ÁLGEBRA CONMUTATIVA BÁSICA

Juan A. Navarro González

25 de mayo de 2014

Prólogo

En palabras de Sancho Guimerá (1927-2011), "la verdadera originalidad en todo saber es siempre paradójicamente la *luz nueva* que engendra la asimilación cada vez más profunda de los fundamentos, no un amontonamiento (que empieza a sobrarnos) de datos a la luz de lo ya conocido". Y las matemáticas son el lenguaje[1] en que se expresa la nueva luz, la nueva forma de ver y entender un mundo descubierto por los griegos hace más de 25 siglos:

> "... un ámbito diáfano que aparece ante la conciencia humana, poblado por objetos y nociones transparentes a la comprensión y cuyo ser se desvela y consiste en su propio sentido, en términos griegos en su propio $\Lambda o\gamma o\sigma$ ... El hombre ya no es un simple animal sujeto a la sinrazón de nacer, vivir y morir, sino un ser abierto a un ámbito de juicio y sabiduría no sometido a la contingencia, antes al contrario tribunal donde la naturaleza y las cosas se juegan su ser como objeto de esta sabiduría.
>
> Con la aparición de este saber aparece la filosofía, y es esta situación la que en frase lapidaria enuncia Parménides[2] diciendo *es lo mismo el ser de las cosas que su sentido* (es decir que su Logos)."

Frase confirmada reiteradamente por el desarrollo de la Ciencia, que al indagar cada vez con más profundidad la realidad íntima de las cosas, descubre que ésta necesita expresarse en el lenguaje matemático, lo que ya había adelantado Platón (427-347 a. de Cristo) al afirmar $o\ \Theta\varepsilon\omega\sigma\ \ \gamma\varepsilon\omega\mu\varepsilon\theta\rho\varepsilon\iota$ (el oficio de Dios es hacer geometría) en un tiempo en que matemáticas y geometría se identificaban. Estudiar matemáticas también es una forma de mirar a Dios, como bien a las claras y nada de soslayo, afirma Alexandre Grothendieck (n. 1928) en *La Llave de los Sueños*:

> ... las leyes matemáticas. Esas leyes pueden ser descubiertas por el hombre, pero no son creadas por el hombre, ni siquiera por Dios. Que

[1] ¡Bah, nada más que un lenguaje! dirán algunos. ¡Oh, nada menos que un lenguaje! decimos otros.

[2] Siglo V antes de Cristo.

> dos y dos son cuatro no es un decreto de Dios, que Él fuera libre de cambiar en dos y dos son tres, o cinco. Siento que las leyes matemáticas forman parte de la naturaleza misma de Dios – una parte ínfima, ciertamente, la más superficial en cierto modo, y la única accesible a la mera razón."

Por eso es tan triste y repugnante dividir las matemáticas en más y más especialidades desconectadas. Se nos ensancha el alma y alegra la mirada cada vez que dos ramas aparentemente separadas se funden en una misma teoría, porque supone un indicio de la esencial unidad de Dios.

A lo largo del siglo XX las matemáticas han vivido un extraordinario proceso de unificación y uno de sus frutos más logrados son los trabajos realizados en los años 60 por Grothendieck. En líneas generales, su obra presenta tres grandes procesos de unificación, cada uno desarrollado en torno a un concepto-clave que recoge, unifica, simplifica y generaliza muchas teorías dispersas anteriores. Así, la noción de *esquema afín* permite unificar la Aritmética y la Geometría afín, el concepto de *esquema* recoge además la Geometría Proyectiva y la Geometría Algebraica abstracta, y los *topos* proporcionan un ámbito común donde también tiene cabida la Topología (Algebraica o General). Estos tres conceptos fundamentales no son independientes, sino que están nucleados por el concepto de *haz*, idea madre de todos ellos, que ha sido el camino seguro que ha permitido aclarar la raíz esencialmente común de diversas teorías matemáticas desarrolladas en etapas anteriores.

Todo intento de enseñar matemáticas en el siglo XXI debería transmitir la perspectiva que se alcanza desde estos tres conceptos, y este libro pretende ser el primero de los tres pasos que deben darse para asimilar la obra de Grothendieck, despojado de todo lo accesorio. Ahora bien, en este primer paso no se introduce el concepto de esquema afín porque esencialmente es equivalente al de anillo conmutativo. Por eso éste último es el centro del libro y por eso éste es un libro de Álgebra Conmutativa, que debería ser continuado por otro de Geometría Algebraica, centrado en la noción de esquema, y un último de Teoría de Topos.

El Álgebra Conmutativa, entendida como estudio de los anillos conmutativos, se nos presentará como la unificación de la Aritmética y la Geometría afín, y el objetivo de este libro es situar al lector en posición de apreciar el significado aritmético y geométrico de los diversos temas que se estudian en Álgebra Conmutativa. Por eso consta de dos partes. La primera[3], centrada en la teoría de congruencias o de paso al cociente (que geométricamente significará pasar a un cerrado), estudia el aspecto aritmético. La segunda[4] aborda el lado geométrico y su núcleo es el proceso de localización, que geométricamente significa pasar a

[3] Los capítulos del 1 al 4.

[4] Los capítulos del 6 al 9, siendo el quinto un capítulo de transición, donde por primera vez se entremezclan el paso al cociente y la localización.

un abierto o a un entorno suficientemente pequeño de un punto. Este libro sólo incluye lo que es estrictamente necesario para alcanzar la comprensión aritmético-geométrica del concepto de anillo conmutativo. No obstante, en un intento de facilitar la asimilación de la teoría, al final se han incluido ejemplos y ejercicios, así como diversos apéndices que pueden estudiarse a partir de la madurez que se va adquiriendo a través de los capítulos del libro.

Por otra parte, la Geometría Algebraica, tal y como ha sido fundamentada por Grothendieck en la noción de esquema, engloba tanto la Geometría Proyectiva como el Álgebra Conmutativa, de forma que la teoría de anillos conmutativos coincide exactamente con el estudio local de los esquemas. La continuación natural de este libro es el estudio de la Geometría Algebraica, entendida como teoría de esquemas. Por tal motivo, los últimos capítulos exponen sistemáticamente el proceso de localización, que es la clave de la inmersión del Álgebra Conmutativa dentro de la Geometría Algebraica así entendida.

Agradezco a mi amigo Juan B. Sancho de Salas sus constantes conversaciones sobre las páginas que siguen, que tanto le deben, y el permiso para reproducir en un apéndice sus notas sobre la clasificación de módulos sobre dominios de ideales principales. Agradezco a María Teresa Sancho de Salas el permiso para incluir en un apéndice su trabajo sobre el grupo de Brauer y a María Ángeles Mulero Díaz y Pedro Sancho de Salas sus provechosos comentarios sobre esta obra.

Me atrevo a dedicar este libro a mis maestros D. Juan Bautista Sancho Guimerá y D. Cristóbal García-Loygorri y Urzaiz, y a mis profesores y compañeros de la Universidad de Salamanca, conmovido por el recuerdo del ambiente en que nos educaron, que tanto bien nos ha hecho.

Ad maiorem Dei gloriam

Badajoz
mayo del 2003

Índice General

Parte I

Teoría

Capítulo 1

Relaciones de Equivalencia

A lo largo de los cursos nuestra actividad fundamental es la de hablar; bueno será que examinemos un poco tan asombrosa facultad humana. Cuando utilizamos nombres (papel, hierro, peso, derecha, etc.) normalmente señalamos primero varios seres a los que ponemos tales nombres, para indicar en lo sucesivo otros similares. Pero, aparte de su capacidad para *señalar* e indicar, al hombre también le es posible delimitar con precisión el significado de algunas palabras, de modo que podamos decidir cuándo son convenientes sin necesidad de ver ejemplos particulares previos. Así, cuando definimos el hidrógeno como elemento de número atómico 1, no es necesario haber visto antes hidrógeno para poder decidir si determinada sustancia que tengamos delante lo es, basta disponer de un procedimiento para hallar el número atómico de los elementos. Igualmente, cuando definimos número primo como el que sólo es divisible por él mismo y la unidad, no necesitamos conocer ningún ejemplo de número primo para decidir si lo es el 11 ó el 12. Sócrates (469-399 a. de Cristo) quedó fascinado por la posibilidad de este modo superior de decir y en los *Diálogos* de Platón (427-347 a. de Cristo) vemos cómo se entregó a la tarea de someter los conceptos a la prueba de fuego de su expresión en él, convencido plenamente de que todo lo verdadero podrá decirse con el nuevo decir (mientras las apariencias se desvanecerán ante sus exigencias) y de que la definición de cada concepto nos mostrará cómo sus propiedades no son meras casualidades sino consecuencias necesarias de su verdadero sentido[1].

La exposición de los conceptos que en alguna parcela de la realidad se yerguen majestuosamente después del demoledor examen de su significado a la luz de las terribles exigencias de este *nuevo decir*, junto con el desarrollo de sus consecuencias absolutamente necesarias, es lo que llamamos *teoría*. Para quien haya vivido la exposición de alguna teoría, *comprender* sólo puede significar ya el des-

[1]Por supuesto nada de lo que estamos diciendo ahora lo es en este sentido más exigente que estamos descubriendo, aún no es teoría, sino sugerencia, indicación.

pliegue del saber como teoría; pues, ante ella, el antiguo modo de decir, que sólo señala, aparece casi como un ruido sin sentido imposible de entender[2]. Más que la búsqueda de lo novedoso, la Ciencia es ante todo una nueva forma de ponerse delante de las afirmaciones comunes. En palabras de Descartes (1596-1650):

> "... y no me precio tampoco de ser el primer inventor de ninguna de ellas, sino solamente de no haberlas admitido, ni porque las dijeran otros, ni porque no las dijeran, sino sólo porque la razón me convenció de su verdad."

Pero, antes de que la razón examine la verdad, falsedad o carencia de sentido de una afirmación, necesita comprender el significado de los conceptos involucrados en la misma. Si decimos que por los vértices de un triángulo pasa una única circunferencia o que hay infinitos números primos, no podemos entender estas afirmaciones sin decir (= definir) previamente qué es un triángulo, qué es una circunferencia y qué es un número primo. El empeño fundamental de las Matemáticas, compartido con las demás Ciencias, es responder con rigor a las preguntas ¿Qué es eso que llamamos ...?, definir los conceptos que continuamente usamos de forma imprecisa.

Conviene advertir que definir un concepto no significa señalar algunas propiedades accidentales que lo caractericen dentro de nuestra experiencia, sino poner de manifiesto su esencia. Es iluminadora la anécdota de un pensador griego que, tras meditar mucho sobre qué es un hombre, en plena plaza pública afirmó su gran descubrimiento: *es* el bípedo implume. Los ciudadanos se maravillaron, pues nadie podía rebatirle ¡no conocemos bípedos implumes que no sean humanos!. Alabaron su inteligencia, con secreta envidia de la eterna fama que su hazaña le daría; aunque muchos debieron sentir en sus tripas ese rescoldo que ante tal respuesta también a nosotros nos susurra: no es eso, no es eso, no es eso, ... Un filósofo, con la rabia del que ha vivido el asombro ante una verdadera definición, desplumó una pobrecita gallina y, lanzándola en medio de la plaza, le espetó: ¡He ahí tu hombre!, pues definir un concepto es desentrañar lo que lo constituye verdaderamente como tal. La definición ha de ser la expresión de su estructura esencial, no una caracterización arbitraria o accidental dentro de nuestra limitada experiencia.

Cuando alcanzamos la definición de algún concepto, en ella incluimos otros conceptos. Si un concepto B se define a partir de otro concepto A, todas las

[2]En modo alguno significa esto menospreciar la manera anterior de hablar y comprender, pues es una etapa absolutamente necesaria para llegar a la claridad y rigor que nos proponemos. Si nos preguntamos ¿qué es una línea recta? ¿qué es un número fraccionario? ¿qué es la dimensión del espacio? ¿qué es el tiempo? etc., será imposible alcanzar definiciones precisas de estos conceptos si previamente no nos hemos sumergido de modo intuitivo en los ámbitos donde tales conceptos se nos presentan "a la vista". Aunque carezcan del rigor que a partir de ahora nos exigiremos, nuestros años de experiencia en Geometría, Aritmética, Física, etc., son un tesoro precioso y requisito imprescindible para entender el desarrollo de la Licenciatura de Matemáticas. La pretensión de la Ciencia es aclarar y fundamentar muchos conceptos que sólo señalamos, y sería empeño vano si de ellos no tenemos amplia experiencia previa y no los poseemos de forma intuitiva.

afirmaciones en que intervenga B quedan transformadas en afirmaciones sobre A. Definir un concepto B a partir de otros conceptos anteriores es *reducirlo* a éstos: para entender B basta comprender los anteriores y todas las propiedades de B lo son de tales conceptos previos. Así, al definir la derivada de una función $f(x)$ en un punto $x = a$ como el límite del cociente de incrementos $(f(x) - f(a))/(x - a)$ cuando $x \to a$, el concepto de derivada queda reducido al de límite. En todas nuestras afirmaciones podríamos sustituir el término derivada por la definición dada sin que por ello cambiase el sentido, por lo que todas las propiedades de la derivada son realmente propiedades del límite. En este sentido podemos decir que el concepto de derivada queda disuelto en el de límite. Análogamente, cuando definimos la circunferencia como la figura formada por los puntos equidistantes de un punto dado, el concepto de circunferencia queda reducido al de equidistancia de puntos.

Lo que no podemos hacer nunca es reducir un concepto B a otro A cuando en la definición de A se haya utilizado B u otros conceptos que se hayan definido a partir de B. Por ejemplo, si definimos el ángulo recto por la condición de que sus lados sean perpendiculares, ya no podremos definir el concepto de rectas perpendiculares por la condición de que se corten formando un ángulo recto, pues tendríamos un *círculo vicioso*: para comprender el concepto de ángulo recto necesitaríamos entender previamente el de perpendicularidad y éste a su vez debería comprenderse a partir del concepto de ángulo. *En la definición de un concepto B no puede intervenir un concepto previamente definido A si en la definición de A hemos introducido B*. Tampoco son admisibles las *autorreferencias*: Un concepto no puede intervenir en su propia definición.

Si nos proponemos definir ciertos conceptos, en este proceso de reducción de unos a otros siempre habrá, debido a la finitud humana, unos conceptos indefinidos a los que hayamos reducido los restantes. Esta finitud del hombre es la que todo niño (tanto mis hijos pequeños como el niño que un día fuimos y yace olvidado en un rincón del alma) descubre cuando ve con regocijo la impotencia de sus mayores ante la reiteración indefinida de la pregunta ¿Por qué?[3], reiteración que sus padres solemos cortar abruptamente con un cambio de tema o con una sonrisa en el mejor de los casos. Finitud que sirve de base fundamental a la Ciencia y nos fuerza a elegir, entre todos los conceptos que utiliza, unos *conceptos primitivos* con los que definiremos los restantes, de modo que sus propiedades no sean más que el reflejo de algunas propiedades de los conceptos primitivos, que han de ser los más cercanos, claros, seguros y sencillos.

Lo que diferencia radicalmente unas ciencias de otras son los conceptos primitivos que se admiten en la fundamentación de cada una. Por eso las separaciones entre las mismas no son algo estable y perenne, sino sujeto a nuestros avances en la aclaración de los conceptos básicos de nuestro pensar. Avances que son los mo-

[3]Ahora estamos involucrados con la pregunta ¿Qué es? y no con la pregunta por las causas; pero la finitud humana que se descubre es esencialmente la misma.

mentos estelares en la aventura del conocimiento humano, como afirma Heidegger en *Ser y Tiempo*:

> "El verdadero movimiento de las ciencias es el de revisión de los conceptos fundamentales,que puede ser más o menos radical y ver a través de sí mismo también más o menos. El nivel de una ciencia se determina por su *capacidad* para experimentar una crisis de sus conceptos fundamentales."

Algo muy similar ocurre con las demostraciones. Cuando hacemos un razonamiento deductivo[4] demostramos que cierta afirmación B es consecuencia racional de otra A, que la razón humana no puede comprender[5] la falsedad de B si acepta la verdad de A. De este modo B queda *reducido* a A. Si nos proponemos demostrar ciertas afirmaciones, de nuevo la finitud del espíritu humano exige la existencia de algunas carentes de demostración (los *principios*) a partir de las cuales demostramos las demás. En la demostración de un enunciado B no puede intervenir un enunciado previamente demostrado A si la demostración de A se basó a su vez en B. Tampoco es admisible la utilización de un resultado en su misma demostración: un teorema no puede darse por válido en su propia demostración.

Todo lo anterior viene a decir que pretendemos seguir el método cartesiano: partiendo de los principios simples que nos sean más claros y evidentes, sólo aceptaremos las consecuencias que podamos derivar mediante deducciones rigurosas, formadas por sucesivos pasos absolutamente indudables. Formaremos parte así de la magna empresa que propuso Descartes en el *Discurso del Método* donde, a renglón seguido de enunciar las cuatro reglas del método, afirma:

> "Esas largas series de trabadas razones muy plausibles y fáciles, que los geómetras acostumbran emplear, para llegar a sus más difíciles demostraciones, habíanme dado ocasión de imaginar que todas las cosas, de que el hombre puede adquirir conocimiento, se siguen unas a otras en igual manera, y que, con sólo abstenerse de admitir como verdadera una que no lo sea y guardar siempre el orden necesario para deducirlas unas de otras, no puede haber ninguna, por lejos que se halle situada o por oculta que esté, que no se llegue a alcanzar y descubrir."

[4] El razonamiento analítico o deductivo es el que pasa de una afirmación a sus consecuencias mediante una argumentación lógica absolutamente indudable. Demuestra la verdad de un enunciado suponiendo la verdad de otros. Su forma arquetípica es "Si A es cierto, entonces B es cierto", donde B es la tesis y A la hipótesis. Actualmente sólo reciben el nombre de demostración las argumentaciones deductivas.

[5] Es verdaderamente increíble y consolador el hecho de que, a pesar de la multitud de experimentos que continuamente se realizan, nunca hayan podido observarse hechos reales con alguna consecuencia racional que no lo sea. Cuando una teoría física ha tenido alguna consecuencia lógica errónea siempre se ha buscado cuál de sus principios es falso; pues es inaceptable que siendo válidos sus principios no lo sea alguna consecuencia racional. Esta confianza, muchas veces inconsciente y siempre maravillosa, la expresamos al decir que la realidad es racional, inteligible y humana.

Ahora debemos buscar, entre los conceptos que a diario usamos intuitivamente, los que nos servirán para fundamentar las Matemáticas, y hemos de elegir los que sean más claros, sencillos y seguros.

Actualmente las Matemáticas se caracterizan por basarse en los conceptos primitivos de **número natural** (0,1,2,3,..., los números que usamos para *contar*) y de **conjunto** o familia de objetos (lo que puede ser *contado*). Partiendo de ellos y de sus propiedades más evidentes (es decir, de la aritmética elemental y la teoría de conjuntos) se definen todos los conceptos que ahora abarcan las Matemáticas y se demuestran sus teoremas, iniciando así el cumplimiento de la fantástica afirmación atribuida a Pitágoras (570?-496? a. de Cristo): *Todo es una música de números.* Es asombroso que todos los conceptos que se han incorporado a las Matemáticas (recta, distancia, ángulo, dimensión, punto, orientación, cercanía, finitud, área, volumen, tiempo, velocidad, aceleración, puntos imaginarios y del infinito, el cálculo literal, las raíces, etc.) no sean más que un entramado de los conceptos de *número natural* y *familia de cosas* u *objetos*, y que todas las propiedades conocidas sean consecuencias lógicas de las propiedades más sencillas y evidentes de estos conceptos primitivos. Es decir, para empezar rechazaremos los demás conceptos (números negativos, fracciones, números imaginarios y todos los conceptos geométricos: recta, área, dimensión, etc.) hasta tanto no hayan podido definirse a partir de los números naturales, al igual que sus propiedades (por más evidentes que parezcan) hasta que hayan sido deducidas de las propiedades elementales de los números naturales. La empresa que ahora se despliega ante cada uno de nosotros es la de volver a entrar, por la fuerza de la razón, en ese Paraíso perdido que habitamos cuando éramos pequeños y con pasmosa seguridad nos movíamos entre semejanzas de triángulos. En este primer capítulo iniciaremos este proceso de reducción del saber matemático a los números naturales y los conjuntos, proceso que se extenderá a lo largo de toda la Licenciatura y, en general, de todo el quehacer matemático.

1.1 Conjunto Cociente

El primer concepto que analizaremos será el de *igualdad*, que solemos representar con el símbolo $=$. A primera vista pudiera parecer que tal concepto no es problemático, que dos objetos son iguales cuando no se distinguen en nada. No obstante, afirmamos que $1/2 = 2/4$ a pesar de que ambas fracciones tienen numeradores distintos y ante la pregunta de si los números 10 y $9'999\ldots$ son iguales pueden surgir dudas: no tienen ninguna cifra común y sin embargo $9'999\ldots = 3(3'333\ldots) = 3(10/3) = 10$. Ante preguntas de este tipo es frecuente dudar o buscar argumentos a favor o en contra de la igualdad en cuestión, sin darse cuenta de que la pregunta carece de sentido mientras no se diga explícitamente qué debe entenderse por "igual". Esta caída en la cuenta de que la igualdad puede decirse de muchos modos, que no es algo dado, que ante un problema tenemos

libertad para elegir la noción de igualdad y debemos aprender cuáles están mejor adaptadas a cada cuestión, es fundamental para librarse de muchas encerronas y preguntas sin sentido que han atenazado a la humanidad durante siglos y aún torturan a algunos.

Partiendo de la relación de igualdad más clara y segura, que es la de igualdad entre los elementos de un conjunto, vamos a estudiar las que puedan reducirse a ella. Si tenemos un conjunto X y fijamos libremente los elementos de X que queremos considerar "iguales" (aunque en X no sean elementos iguales), nuestro problema fundamental es saber si existe alguna aplicación π de X en otro conjunto que identifique las parejas prefijadas y sólo ellas; es decir, que al pasar por π la relación de "igualdad" fijada se transforme en la relación de igualdad entre elementos de un mismo conjunto, que conceptualmente es la más evidente. Veremos que la libertad para fijar tales parejas en X, siendo grande, no es arbitraria, está sometida a ciertas condiciones. Nuestro objetivo es precisamente hallar condiciones necesarias y suficientes para la existencia de tal aplicación π.

Definición: Llamaremos **relación** en un conjunto X a todo subconjunto del producto directo $X \times X$. Dada una relación $R \subseteq X \times X$ en un conjunto X, diremos que dos elementos x, y de X están **relacionados** según R si la pareja (x, y) está en R, y en tal caso escribiremos xRy.

Definición: Diremos que una relación $\equiv$ en un conjunto X es una relación de **equivalencia** si tiene las siguientes propiedades:

1. *Reflexiva*: $x \equiv x$ para todo $x \in X$.
2. *Simétrica*: Sean $x, y \in X$. Si $x \equiv y$, entonces $y \equiv x$.
3. *Transitiva*: Sean $x, y, z \in X$. Si $x \equiv y$ e $y \equiv z$, entonces $x \equiv z$.

Toda aplicación $f\colon X \to Y$ define en el conjunto X una relación

$$x \equiv x' \text{ precisamente cuando } f(x) = f(x')$$

que es una relación de equivalencia en X:

1. Si $x \in X$, entonces $x \equiv x$ porque $f(x) = f(x)$.
2. Sean $x, x' \in X$. Si $x \equiv x'$, entonces $f(x) = f(x')$; luego $f(x') = f(x)$ y concluimos que $x' \equiv x$.
3. Sean $x, x', x'' \in X$. Si $x \equiv x'$ y $x' \equiv x''$, entonces $f(x) = f(x')$ y $f(x') = f(x'')$; luego $f(x) = f(x'')$ y concluimos que $x \equiv x''$.

Dada una relación R en un conjunto X, nuestro propósito es averiguar si podemos identificar los elementos relacionados por R y sólo ellos; es decir, si existe alguna aplicación f de X en otro conjunto tal que:

$$xRx' \Leftrightarrow f(x) = f(x')$$

Es decir, si R es la relación definida en X por alguna aplicación $f\colon X \to Y$. Cuando R no es una relación de equivalencia, acabamos de ver que tal cosa no es posible. La construcción central de este capítulo probará que la respuesta es afirmativa para todas las relaciones de equivalencia: Las propiedades reflexiva, simétrica y transitiva caracterizan las relaciones definidas por aplicaciones, son las condiciones necesarias y suficientes para que exista una aplicación que identifique exactamente los elementos relacionados.

Definición: Dada una relación de equivalencia $\equiv$ en un conjunto X, llamaremos **clase de equivalencia**, respecto de $\equiv$, de un elemento x de X al subconjunto de X formado por todos los elementos equivalentes con x.

La clase de equivalencia de un elemento x suele denotarse $\bar{x}$ ó $[x]$:

$$[x] \ := \ \{y \in X : x \equiv y\}$$

Diremos que un subconjunto C de X es una **clase de equivalencia** de la relación $\equiv$ si es la clase de equivalencia de algún elemento de X; es decir, si existe algún elemento x de X tal que $[x] = C$. Llamaremos **conjunto cociente** de X por $\equiv$ al conjunto de todas las clases de equivalencia de $\equiv$, y lo denotaremos $X/\equiv$. La aplicación π de X en el conjunto cociente $X/\equiv$

$$\pi\colon X \longrightarrow X/\equiv \ ; \qquad \pi(x) = [x]$$

que transforma cada elemento x de X en su clase de equivalencia $\bar{x}$ se llamará aplicación de **paso al cociente** o **proyección canónica**[6] o estructural, para resaltar que pertenece a la estructura misma de lo que estamos estudiando.

Teorema 1.1.1 *Si $\equiv$ es una relación de equivalencia en un conjunto X, la proyección canónica $\pi\colon X \to X/\equiv$, $\pi(x) = [x]$, y se verifica que*[7]

$$x \equiv y \ \Leftrightarrow \ \pi(x) = \pi(y) \ .$$

[6] El adjetivo *canónico* se usa en matemáticas para indicar que algo es natural, como debe ser e independiente de elecciones arbitrarias, que es absoluto e intrínseco, que no depende de un sistema de coordenadas, que pertenece a la estructura propia de lo que estudiamos. Decir de algo que es canónico significa que no es arbitrario, que todos coincidimos en ello si lo miramos con atención. Aunque siempre se use en sentido impreciso, es un concepto central en matemáticas, ciencia que aspira a desentrañar con rigor lo que se entiende por canónico y a sacar la luz todo lo que es canónico. Algunos sinónimos, más o menos lejanos, son: natural, universal, absoluto, intrínseco, general, estructural, independiente; y algunos antónimos son: relativo, arbitrario, particular, usual, ingenioso, por costumbre o convenio. En definitiva, en matemáticas lo canónico es allí donde con más claridad percibimos el rastro de Dios, Su aroma.

[7] Nunca utilizaremos que los elementos del conjunto cociente $X/\equiv$ son las clases de equivalencia de $\equiv$, sólo que tenemos definida una aplicación de X en $X/\equiv$ con las dos propiedades siguientes. Cualquier otro conjunto Y con una aplicación $X \to Y$ que tenga esas dos propiedades puede reemplazar a $X/\equiv$ y ser considerado como cociente de X por la relación $\equiv$; pero la definición anterior muestra que tal conjunto puede darse a la vez para todas las relaciones de equivalencia sin tener que recurrir a una construcción "ad hoc" en cada caso particular.

Demostración: π es epiyectiva porque, por definición, todo elemento de $X/\equiv$ es la clase de algún elemento de X.

En cuanto a la otra propiedad, si $x \equiv y$, al ser reflexiva la relación, para probar que $[x] = [y]$ bastará ver que $[y] \subseteq [x]$. Ahora bien, si $z \in [y]$, entonces $y \equiv z$; luego $x \equiv z$ y $z \in [x]$.

Recíprocamente, si $[x] = [y]$, como $y \in [y]$, tenemos que $y \in [x]$;i.e., $x \equiv y$.

Corolario 1.1.2 *Sea $\equiv$ una relación de equivalencia en un conjunto X. Cada elemento de X pertenece a una única clase de equivalencia de la relación $\equiv$.*

Demostración: Si x es un elemento de X, entonces $[x]$ es una clase de equivalencia de $\equiv$ que contiene a x, porque $x \equiv x$. Además, si x está en otra clase de equivalencia $[y]$, entonces $y \equiv x$, de modo que $[y] = [x]$.

1.2 Relaciones de Orden

Definición: Diremos que una relación $\leq$ en un conjunto X es una relación de **orden** si tiene las propiedades *reflexiva* ($x \leq x$ para todo $x \in X$) *antisimétrica* (si $x \leq y$ e $y \leq x$, entonces $x = y$) y *transitiva* (si $x \leq y$ e $y \leq z$, entonces $x \leq z$).

Diremos que una relación de orden $\leq$ en un conjunto X es **total** cuando $x \leq y$ ó $y \leq x$ para todo par $x, y \in$X.

Diremos que un elemento x de un conjunto ordenado $(X, \leq)$ es **maximal** si verifica que $x \leq y \Rightarrow x = y$. Diremos que es **minimal** cuando $y \leq x \Rightarrow y = x$. Diremos que x es el **primer** elemento de X si $x \leq y$ para todo $y \in X$, y diremos que es el **último** elemento si $y \leq x$ para todo $y \in$X. El primer y último elemento, si existen, son únicos. Se dice que $(X, \leq)$ es un conjunto **bien ordenado** cuando todo subconjunto no vacío de X, con la ordenación inducida por $\leq$, tenga primer elemento.

Principio de Inducción Completa

El **principio de inducción** afirma que, para concluir que todos los números naturales mayores o iguales que un número natural dado r tienen cierta propiedad P, basta probar las dos afirmaciones siguientes:

1. El número r tiene la propiedad P.
2. Sea n un número natural mayor que r. Si todos los números naturales entre r y $n-1$ tienen la propiedad P, entonces n también la tiene.

El principio de inducción es una afirmación sobre los números naturales que es evidentemente cierta (ante la consideración atenta de su sentido nos es imposible

dudar de su veracidad), por lo que lo incluimos entre las propiedades de los números naturales que utilizaremos en la fundamentación de las Matemáticas[8].

Lema de Zorn

Sea Y un subconjunto de un conjunto ordenado $(X, \leq)$. Diremos que $x \in X$ es una **cota superior** (respectivamente **inferior**) de Y si $y \leq x$ (respectivamente $x \leq y$) para todo $y \in$Y. Diremos que Y es una **cadena** si, con la ordenación inducida, Y es un conjunto totalmente ordenado.

Entre las propiedades de los conjuntos que admitiremos para fundamentar las Matemáticas se encuentra la siguiente[9]:

Lema de Zorn (1906-1993)**:** *Sea $(X, \leq)$ un conjunto ordenado no vacío. Si toda cadena de X admite una cota superior, entonces X tiene algún elemento maximal.*

1.3 Números Enteros

Sea $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ el conjunto de los números naturales.

En el producto directo $\mathbb{N} \times \mathbb{N}$ definimos la relación

$$(m, n) \equiv (m', n') \Leftrightarrow m + n' = m' + n$$

y es una relación de equivalencia en $\mathbb{N} \times \mathbb{N}$. El conjunto de los **números enteros** $\mathbb{Z}$ se define[10] como el conjunto cociente de $\mathbb{N} \times \mathbb{N}$ por la anterior relación de equivalencia $\equiv$ y, si $\pi \colon \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ es la proyección canónica, pondremos $m - n$ en lugar de $\pi(m, n)$ y diremos que es la **diferencia** de m y n.

De acuerdo con el teorema 1.1.1, tenemos que

1. Todo número entero b es diferencia de dos números naturales; es decir, $b = m - n$ para alguna pareja (m, n) de números naturales.

[8] Las primeras veces que se utilice este principio puede presentar alguna dificultad, porque su estructura lógica es algo complicada y puede inducir a error. Es un buen ejercicio comprobar que es equivalente a algunas afirmaciones más claras, como *la ordenación de los números naturales es un buen orden* o incluso *en toda familia finita y no vacía de números naturales hay uno que es el primero.*

[9] Dijimos que nos basaríamos únicamente en las propiedades sencillas y claras de los números naturales y los conjuntos; pero el lema de Zorn no puede considerarse en modo alguno como evidente. Puede probarse que es equivalente al **axioma de elección** (el producto directo de cualquier familia, finita o no, de conjuntos no vacíos tiene algún elemento) y al **principio del buen orden** (todo conjunto admite una buena ordenación). Más que su verdad o falsedad, lo que no es nada claro es su sentido para conjuntos infinitos (o, al menos, no numerables). Esto, unido al hecho de que nunca importe el conjunto que tengamos sino la estructura que soporte, hace que en la fundamentación de las Matemáticas la teoría de conjuntos tenga un papel mucho más insatisfactorio (y esperemos que provisional) que los números naturales.

[10] Primero definimos el conjunto $\mathbb{Z}$, luego los números enteros como elementos de tal conjunto.

2. $m - n = m' - n'$ precisamente cuando $m + n' = m' + n$.

Cada número natural n define un número entero

$$\pi(n, 0) = n - 0$$

que también denotaremos n. Obtenemos así una aplicación inyectiva canónica $\mathbb{N} \to \mathbb{Z}$, que nos permite identificar $\mathbb{N}$ con un subconjunto de $\mathbb{Z}$.

Si a y b son dos números enteros, existen números naturales m, n, r, s tales que $a = m - n$, $b = r - s$, y definimos su **suma** y su **producto** del siguiente modo:

$$\begin{aligned} a + b &:= (m + r) - (n + s) \\ a \cdot b &:= (mr + ns) - (nr + ms) \end{aligned}$$

y diremos que $a \leq b$ cuando $m+s$ sea menor o igual que $r+n$. Los números enteros mayores que 0 se llaman **positivos** y los menores que 0 se llaman **negativos**.

Hemos probar que estas definiciones no dependen de los números m, n, r, s elegidos. Si $a = m' - n'$, entonces $m + n' = m' + n$ y

$$\begin{aligned} m + n' + r + s &= m' + n + r + s \\ (m + r) - (n + s) &= (m' + r) - (n' + s) \end{aligned}$$

así que la suma $a + b$ es un número entero que no depende de los representantes m, n, r, s elegidos. Por otra parte tenemos que

$$\begin{aligned} mr + n'r = m'r + nr \quad &, \quad m's + ns = ms + n's \\ mr + n'r + m's + ns &= m'r + nr + ms + n's \\ (mr + ns) - (nr + ms) &= (m'r + n's) - (n'r + m's) \end{aligned}$$

y concluimos que el producto $a \cdot b$ no depende de los representantes elegidos.

Por último, si $b = r' - s'$ para otros números naturales r', s', tenemos que

$$\begin{aligned} m + s \leq n + r \Leftrightarrow m + s + m' + s' &\leq n + r + m' + s' = \\ = m + n' + r' + s &\Leftrightarrow m' + s' \leq n' + r' \end{aligned}$$

así que la relación $a \leq b$ tampoco depende de los representantes elegidos.

De las definiciones anteriores y de las propiedades de los números naturales se deduce fácilmente que la suma y el producto de números enteros son operaciones asociativas y conmutativas, que el producto distribuye respecto de la suma, que la relación $\leq$ es una ordenación total de $\mathbb{Z}$, las igualdades

$$0 + a = a \qquad , \qquad 1 \cdot a = a$$

y las otras propiedades usuales.

La suma, el producto y la ordenación de números enteros coinciden en $\mathbb{N}$ con la suma, el producto y la ordenación de números naturales. Por otra parte, para cada número entero b existe un único número entero, que llamaremos **opuesto** de b y denotaremos $-b$, cuya suma con b es 0. En efecto, si $b = m - n$, entonces $b + (n - m) = 0$, lo que prueba la existencia del opuesto y, en cuanto a la unicidad, si $b + a = 0$ y $b + c = 0$, entonces $a = (c + b) + a = c + (b + a) = c$. En general, si $a, b \in \mathbb{Z}$, diremos que $a - b := a + (-b)$ es la **diferencia** de a y b.

Esta construcción de los números enteros a partir de los números naturales reduce cada enunciado sobre los números enteros a un enunciado equivalente sobre los números naturales. La teoría de números enteros es sólo una parte, una consecuencia lógica, de la teoría de números naturales. *Si los números naturales están libres de contradicción, también los números enteros están libres de contradicción.*

Proposición 1.3.1 *El conjunto de los números enteros es la unión disjunta de* $\mathbb{N}$ *con el conjunto de los opuestos de los números naturales no nulos:*

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Demostración: Si $b \in \mathbb{Z}$, entonces existen $m, n \in \mathbb{N}$ tales que $b = m - n$.

Si $n \leq m$, existe $r \in \mathbb{N}$ tal que $m = n + r$; luego $b = m - n = r - 0$ es un número natural.

Si $m < n$, entonces $n = m + r$ para algún número natural no nulo r, y $b = m - n$ es el opuesto de $r = n - m$.

Por último, la unión es disjunta porque si la suma de dos números naturales es nula, ambos sumandos son nulos.

Este resultado permite definir el **valor absoluto** $|b|$ de un número entero b como el máximo de b y $-b$, que siempre es un número natural, y demostrar fácilmente las siguientes propiedades:

$$ab = 1 \Rightarrow a = \pm 1 \text{ y } b = \pm 1$$
$$ab = 0 \Rightarrow a = 0 \text{ ó } b = 0\ .$$

Ésta última muestra la legitimidad de la simplificación: $ab = ac,\ a \neq 0 \Rightarrow b = c$.

Teorema de División: Sea d un número entero no nulo. Para cada número entero b existe una única pareja de números enteros c, r (llamados **cociente** y **resto** de la división de b por d) tal que:

$$b = c \cdot d + r \quad , \quad 0 \leq r < |d|$$

Demostración: Veamos primero la existencia de tal pareja c, r. El conjunto de números naturales

$$R = \{n \in \mathbb{N}\colon\ n = b + sd \text{ para algún } s \in \mathbb{Z}\}$$

no es vacío (por ejemplo $b + (b^2 d)d$ está en R), así que tiene un primer elemento r. Por definición $r \geq 0$ y existe $s \in \mathbb{Z}$ tal que $r = b + sd$; luego $b = (-s)d + r$. Si $r \geq |d|$, entonces $r - |d| = b + (s \pm 1)d$ está en R y es estrictamente menor que r, en contra de la elección de r. Luego $r < |d|$.

Veamos ahora la unicidad del cociente y el resto. Si c', r' son otros números enteros tales que $b = c'd + r'$ y $0 \leq r' < |d|$, podemos suponer que $r \leq r'$, en cuyo caso $r' - r = (c - c')d$ es un múltiplo no negativo de $|d|$ menor que $|d|$ y se sigue que $r' - r = 0$ y $cd = c'd$. Como d no es nulo, concluimos que $r' = r$ y $c' = c$.

Congruencias módulo un número natural: Sea n un número natural. Diremos que dos números enteros a, b son **congruentes** módulo n cuando su diferencia $b - a$ sea un múltiplo de n (es decir, $b - a = cn$ para algún número entero c) en cuyo caso pondremos

$$a \equiv b \text{ (mód. } n)$$

La relación de congruencia módulo n es una relación de equivalencia en el conjunto de los números enteros y es compatible con la suma y el producto en el siguiente sentido:

$$\text{Si } a \equiv a' \text{ y } b \equiv b' \text{ (mód. } n), \text{ entonces } a + b \equiv a' + b' \text{ y } ab \equiv a'b' \text{ (mód. } n)$$

Los múltiplos de n son exactamente los números enteros congruentes con 0 módulo n, así que esta relación de equivalencia es útil para estudiar la divisibilidad por n.

Corolario 1.3.2 *Sea $n \geq 2$ un número natural. La condición necesaria y suficiente para que dos números enteros sean congruentes módulo n es que tengan el mismo resto al dividir por n.*

Por tanto, la correspondiente clase de equivalencia $[a]_n$ de cualquier número entero a está formada por los números enteros que al dividir por n tienen igual resto que a, y el conjunto cociente de $\mathbb{Z}$ por la relación de congruencia módulo n tiene exactamente n elementos, que son

$$[0]_n,\ [1]_n, \ldots,\ [n-1]_n$$

Demostración: Sean a, b dos números enteros y $a = cn + r$, $b = c'n + r'$ sus respectivas divisiones por n.

Veamos primero la necesidad de la condición. Si $a \equiv b$ (mód. n), entonces $b - a = dn$ para algún número entero d. Luego

$$b = dn + a = (d + c)n + r$$

y, de la unicidad del resto de la división por n, se deduce que $r = r'$.

Veamos ahora que la condición es suficiente. Si $r = r'$, entonces

$$b - a = c'n + r' - cn - r = (c' - c)n$$

y concluimos que $a \equiv b$ (mód. n).

En consecuencia, cada clase de equivalencia $[a]_n$ está formada por todos los números enteros que tengan igual resto que a al dividir por n (por lo que suele decirse que $[a]_n$ es la **clase de restos** de a módulo n). Como los posibles restos de la división de un número entero por n son 0, 1, ..., $n-1$; concluimos que tales clases de equivalencia son $[0]_n, [1]_n, \ldots, [n-1]_n$.

1.4 Números Racionales

Sea S el conjunto de los números enteros no nulos. En el producto directo $\mathbb{Z} \times S$ definimos la relación

$$(a, s) \equiv (b, t) \;\Leftrightarrow\; at = bs$$

y es una relación de equivalencia en $\mathbb{Z} \times S$. Definimos el conjunto $\mathbb{Q}$ de los **números racionales** como el conjunto cociente de $\mathbb{Z} \times S$ por la anterior relación de equivalencia $\equiv$. Sea $\pi\colon \mathbb{Z} \times S \to \mathbb{Q}$ la proyección canónica. Pondremos a/s en vez de $\pi(a, s)$ y diremos que es el **cociente** de los números enteros a, s. De acuerdo con 1.1.1, tenemos que:

1. Todo número racional es el cociente de dos números enteros.
2. $a/s = b/t$ precisamente cuando $at = bs$.

Cada número entero b define un número racional $\pi(b, 1) = b/1$ que también denotaremos b. Obtenemos así una aplicación inyectiva canónica $\mathbb{Z} \to \mathbb{Q}$ que nos permite identificar $\mathbb{Z}$ con un subconjunto de $\mathbb{Q}$.

Si q, r son dos números racionales, existen números enteros a, s, b, t tales que $q = a/s$ y $r = b/t$, y definimos su **suma** y su **producto** como sigue:

$$q + r := \frac{at + bs}{st}$$
$$q \cdot r := \frac{ab}{st}$$

Estas definiciones no dependen de los representantes a, s, b, t elegidos; pues si $q = a'/s'$, entonces $as' = a's$ y concluimos que

$$ats't = a'tst\,;\ \text{luego}\ \ (at + bs)s't = (a't + bs')st$$
$$abs't = a'bst$$

De las definiciones anteriores y de las propiedades de los números enteros se deducen sin dificultad las propiedades usuales de la suma y el producto de números racionales.

Diremos que un número racional $q = a/s$ es **positivo** cuando $as > 0$ y diremos que $q < r$ cuando $r - q$ sea positivo. La aplicación inyectiva canónica $\mathbb{Z} \to \mathbb{Q}$ conserva sumas, productos y la ordenación.

Si q es un número racional no nulo, existe un único número racional cuyo producto con q es 1; tal número se denotará $1/q$ ó q^{-1} y diremos que es el **inverso** de q. En efecto, si $q = a/s$ no es nulo, entonces $a \neq 0$ y $q(s/a) = 1$. Además, si $qu = 1$ y $qv = 1$, entonces $u = u(qv) = (uq)v = v$. En general, llamaremos **cociente** de dos números racionales $q, r \neq 0$ al número racional $q/r = q \cdot r^{-1}$.

Esta construcción de los números racionales a partir de los números enteros reduce los enunciados sobre números racionales a enunciados equivalentes sobre números enteros y, por tanto, a enunciados sobre números naturales. La teoría de números racionales sólo es una parte de la teoría de números naturales. *Si los números naturales no tienen contradicciones, también los números racionales estarán libres de contradicción.*

Igualmente, la construcción de los números reales que se hace en el curso de Análisis y la que, a continuación, daremos para los números complejos, reducen los enunciados sobre números reales y complejos a enunciados equivalentes sobre números naturales.

1.5 Números Complejos

En el curso de Análisis se construye el conjunto de los **números reales** $\mathbb{R}$ como el conjunto cociente de las sucesiones de Cauchy (1789-1857) de números racionales[11] por la siguiente relación de equivalencia:

$$(a_n) \equiv (b_n) \;\Leftrightarrow\; \text{la sucesión } b_n - a_n \text{ converge a cero}$$

se definen la suma, el producto de números reales y una ordenación total de $\mathbb{R}$, y se prueban sus propiedades fundamentales. Cada número racional q define un número real $\pi(q, q, \ldots)$, que se denota también q, obteniéndose así una aplicación inyectiva canónica $\mathbb{Q} \to \mathbb{R}$ que conserva las sumas, los productos y la ordenación, y que nos permite identificar $\mathbb{Q}$ con un subconjunto de $\mathbb{R}$. Sea c un número real y sea n un número natural no nulo. En el curso de Análisis se probará que, cuando

[11] Aunque admitamos números reales definidos por sucesiones arbitrarias de números racionales, es obvio que sólo las que puedan definirse en un número finito de pasos (incluyendo recurrencias) intervienen en las definiciones, enunciados y demostraciones. Algún día esta diferencia crucial entre números reales definibles y números reales fantasmagóricos será un pilar fundamental de las Matemáticas; pero, hasta que llegue, admitiremos sucesiones cualesquiera.

c no es negativo, existe un único número real no negativo cuya potencia n-ésima es c, número real que denotaremos $\sqrt[n]{c}$.

El conjunto $\mathbb{C}$ de los **números complejos** es el conjunto de pares ordenados de números reales $a + bi$, $a, b \in \mathbb{R}$, que se **suman** y **multiplican** del siguiente modo:

$$(a + bi) + (c + di) := (a + c) + (b + d)i$$
$$(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i$$

A partir de estas definiciones y de las propiedades de la suma y el producto de números reales, es inmediato comprobar que tanto la suma como el producto de números complejos son operaciones asociativas y conmutativas, y que el producto distribuye respecto de la suma.

Cada número real x define un número complejo $x+0i$ que también denotaremos x. Obtenemos así una aplicación inyectiva canónica $\mathbb{R} \to \mathbb{C}$ que conserva las sumas y productos, y que permite identificar $\mathbb{R}$ con un subconjunto de $\mathbb{C}$.

Sea $z = a + bi$ un número complejo. Diremos que los números reales a y b son la **parte real** e **imaginaria** de z respectivamente, que $\overline{z} = a - bi$ es el número complejo **conjugado** de z y que el número real no negativo

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}$$

es el **módulo** de z. Llamaremos **distancia** entre dos números complejos al módulo de su diferencia. Se verifica que:

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2 \quad , \quad \overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2 \quad , \quad \overline{\overline{z}} = z \quad , \quad |\overline{z}| = |z|$$
$$|z_1 \cdot z_2| = |z_1| \cdot |z_2| \quad , \quad |z_1 + z_2| \leq |z_1| + |z_2| \quad , \quad |z| = 0 \Leftrightarrow z = 0$$

y si un número complejo z no es nulo, existe un único número complejo cuyo producto con z es 1. Tal número es $\overline{z}/|z|^2$ y se denotará $1/z$ ó z^{-1}.

Exponencial Compleja

En el curso de Análisis se definirán las funciones trigonométricas seno y coseno (en radianes) y para cada número complejo $a + bi$ pondremos

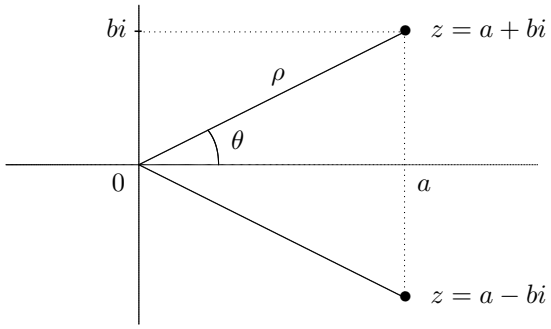
$$e^{a+bi} := e^a(\cos b + i\operatorname{sen} b) \ .$$

De las propiedades de las funciones trigonométricas se sigue

$$e^{2\pi i} = 1$$
$$e^{z+z'} = e^z \cdot e^{z'}$$
$$e^z = e^{z'} \Leftrightarrow z' = z + 2\pi ki \text{ para algún } k \in \mathbb{Z}$$

y que para cada número complejo z de módulo $\rho \neq 0$ existe un número real θ tal que

$$z = \rho(\cos\theta + i \cdot \operatorname{sen}\theta) = \rho e^{i\theta}$$



Este número real θ está bien definido salvo múltiplos enteros de 2π y se llama **argumento** de z (medido en radianes). El producto de dos números complejos no nulos $z = \rho e^{i\theta}$ y $z' = \rho' e^{i\theta'}$ es

$$z \cdot z' = \rho e^{i\theta} \rho' e^{i\theta'} = (\rho\rho') e^{i(\theta+\theta')}$$

así que *el argumento del producto de números complejos es la suma de los argumentos:*

$$\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$$

El **ángulo** (medido en radianes) determinado por dos números complejos no nulos z_1, z_2 se define como el argumento de su cociente z_2/z_1.

Raíces de la Unidad

Sea n un número natural no nulo y sea z un número complejo. Si u es un número complejo tal que $u^n = z$, diremos que u es una **raíz n-ésima** compleja de z. Por ejemplo, una raíz n-ésima de $z = \rho e^{i\theta}$ es claramente $\sqrt[n]{\rho}\, e^{i\theta/n}$. En particular una raíz n-ésima de la unidad $1 = e^{2\pi i}$ es el número complejo

$$e^{\frac{2\pi i}{n}} = \cos\tfrac{2\pi}{n} + i \operatorname{sen}\tfrac{2\pi}{n}$$

de módulo 1 y argumento $2\pi/n$, al igual que sus potencias $e^{\frac{2\pi i}{n}k}$, $k \in \mathbb{Z}$.

Teorema 1.5.1 *Sea n un número natural no nulo. Hay exactamente n raíces n-ésimas complejas de la unidad, que son*

$$e^{\frac{2\pi i}{n}r} = \cos\tfrac{2\pi r}{n} + i \operatorname{sen}\tfrac{2\pi r}{n}\ , \quad 0 \leq r \leq n-1$$

Demostración: Si $u = \rho e^{i\theta}$ es una raíz n-ésima de la unidad, la condición $u^n = 1$ equivale a que $\rho^n = 1$ y $n\theta = 2\pi m$ para algún $m \in \mathbb{Z}$. Es decir, $\rho = 1$ y $\theta = 2\pi m/n$. Dividiendo m por n obtenemos que

$$\theta = \frac{2\pi m}{n} = \frac{2\pi(cn+r)}{n} = 2\pi c + \frac{2\pi r}{n} \ ; \qquad 0 \le r < n \ , \quad c \in \mathbb{Z}$$

y concluimos que $u = e^{i(2\pi c + \frac{2\pi r}{n})} = e^{\frac{2\pi i}{n} r}$, $0 \le r < n$. En resumen, las raíces n-ésimas de la unidad son exactamente:

$$1 = e^{\frac{2\pi i}{n} 0}, \ e^{\frac{2\pi i}{n}} \ , \ e^{\frac{2\pi i}{n} 2}, \ \ldots\ldots \ , \ e^{\frac{2\pi i}{n}(n-1)}$$

Teorema 1.5.2 *Todo número complejo no nulo tiene exactamente n raíces n-ésimas complejas, y se obtienen multiplicando una cualquiera de ellas por las raíces n-ésimas de la unidad.*

Demostración: Todo número complejo no nulo $z = \rho e^{i\theta}$ tiene alguna raíz n-ésima $\alpha = \sqrt[n]{\rho}\, e^{i\theta/n}$. Si β fuera otra raíz n-ésima de z, entonces $\beta^n = z$ y

$$\left(\frac{\beta}{\alpha}\right)^n = \frac{\beta^n}{z} = \frac{z}{z} = 1 \ ; \quad \frac{\beta}{\alpha} = e^{\frac{2\pi i}{n} r} \ , \quad 0 \le r < n$$

Luego z tiene exactamente n raíces n-ésimas, que son

$$\alpha \ , \ e^{\frac{2\pi i}{n}}\alpha \ , \ e^{\frac{2\pi i}{n} 2}\alpha \ , \ \ldots \ , \ e^{\frac{2\pi i}{n}(n-1)}\alpha$$

Corolario 1.5.3 *Sea $z = \rho e^{i\theta}$ un número complejo no nulo. Las raíces n-ésimas complejas de z son los vértices de un polígono regular de n lados inscrito en el círculo de radio $\sqrt[n]{\rho}$ centrado en el 0:*

$$\sqrt[n]{\rho}\left(e^{i\frac{\theta+2\pi r}{n}}\right) \ ; \quad 0 \le r < n$$

Definición: Diremos que una raíz n-ésima de la unidad $e^{\frac{2\pi i}{n} k}$ es **primitiva** si todas las raíces n-ésimas de la unidad complejas son potencias suyas con exponente entero, para lo cual basta que lo sea $e^{\frac{2\pi i}{n}}$ de acuerdo con 1.5.1.

Proposición 1.5.4 *Sea $u = e^{\frac{2\pi i}{n} k}$ una raíz n-ésima de la unidad. Las siguientes condiciones son equivalentes:*

1. u es una raíz n-ésima de la unidad primitiva.

2. La primera potencia de u que es la unidad es u^n; es decir, $u^r \neq 1$ para todo número natural $1 \le r < n$.

3. Todas las potencias u, u^2, $\ldots$, u^n son distintas entre sí.

4. Existe algún $a \in \mathbb{Z}$ tal que $ak \equiv 1$ (módulo n).

Demostración: $(1 \Rightarrow 2)$ Si $u^r = 1$ para algún exponente $1 \leq r < n$, entonces todas las potencias de u son raíces r-ésimas de la unidad: $(u^m)^r = (u^r)^m = 1$. Del teorema 1.5.1 se sigue que las potencias de u no pueden ser las n raíces n-ésimas de la unidad.

$(2 \Rightarrow 3)$ Si $u^i = u^j$ para algunos exponentes $1 \leq i < j \leq n$, entonces $u^{j-i} = 1$ y $1 \leq j - i < n$.

$(3 \Rightarrow 4)$ Como todas las potencias $u, \ldots, u^n$ son raíces n-ésimas de la unidad, y son distintas por hipótesis, del teorema 1.5.1 se sigue que son todas raíces n-ésimas de la unidad. Luego para algún exponente $1 \leq a \leq n$ tendremos

$$e^{\frac{2\pi i}{n}} = \left(e^{\frac{2\pi i}{n}k}\right)^a = e^{\frac{2\pi i}{n}ak} \ .$$

Luego $e^{\frac{ak-1}{n}2\pi i} = 1$ y concluimos que $\frac{ak-1}{n} \in \mathbb{Z}$; i.e., $ak \equiv 1$ (mód. n).

$(4 \Rightarrow 1)$ Si existen números enteros a, c tales que $ak = 1 + cn$, entonces

$$\left(e^{\frac{2\pi i}{n}k}\right)^{ra} = e^{\frac{2\pi i}{n}rak} = e^{\frac{2\pi i}{n}(r+rcn)} = e^{\frac{2\pi i}{n}r}$$

para todo $r \in \mathbb{Z}$. Luego $e^{\frac{2\pi i}{n}k}$ es una raíz n-ésima de la unidad primitiva.

Capítulo 2

Grupos

En el Capítulo anterior hemos comenzado a desarrollar las Matemáticas partiendo del proceso más humilde: el de contar. Este camino se inició hace muchos siglos en la India, nos fue transmitido por los árabes y culmina con el Cálculo Infinitesimal descubierto por Leibnitz (1646-1716). Sus exponentes más logrados son la teoría de funciones de variable compleja y la de ecuaciones en derivadas parciales. Con más o menos rigor, también es éste el camino que hemos seguido desde nuestra infancia. Sin embargo, cuando la Geometría irrumpe luminosamente en Grecia, no lo hace en tal dirección. Parece ineludible que el espíritu humano habla sin definir las palabras que utiliza o, si opta por definirlas, sólo tiene dos posibilidades: caer en círculos viciosos (como ocurre en todos los diccionarios) o reducir todos sus conceptos a unos conceptos primitivos que por el momento carezcan de definición. Posteriormente, tras la consideración atenta de los mismos, tal vez pueda definirlos a partir de otros más fundamentales todavía; pero éstos pasarían a ocupar su lugar y siempre habría un primer peldaño surgiendo de la oscuridad. El genio griego superó en parte esta situación cayendo en la cuenta de que es crucial explicitar las relaciones mutuas entre los conceptos primitivos de cada teoría. Así, alcanzaron a desarrollar toda la geometría plana conocida en su época a partir de unos conceptos (punto, recta, círculo, ángulo...) y de los cinco postulados de Euclides:

1. Por dos puntos pasa una única recta.
2. Toda recta se puede prolongar indefinidamente.
3. Con cualquier centro y cualquier distancia se puede trazar un círculo.
4. Todos los ángulos rectos son iguales.
5. Si una recta, cortando a otras dos, forma los ángulos internos a una misma parte menores que dos rectos, las dos rectas prolongadas indefinidamente se encontrarán de la parte en que los dos ángulos son menores que dos rectos.

Importa mucho resaltar que las consecuencias lógicas de estos axiomas son válidas cualquiera que sea la naturaleza de los conceptos, con tal de que verifiquen todos los axiomas impuestos. Los conceptos primitivos de la Geometría plana quedan definidos por los axiomas: son aquellos que verifiquen los axiomas impuestos. Este punto de vista no se libera de la limitación que hemos indicado al principio, pues en el enunciado de los axiomas han de intervenir conceptos, que previamente deben ser definidos... Actualmente (pero no en la Grecia clásica, como se percibe claramente al leer los 5 postulados anteriores) al establecer los axiomas de una teoría sólo admitiremos conceptos que hayan sido definidos previamente a partir de los números naturales y los conjuntos.

Este punto de vista griego es crucial por dos razones fundamentales:

Principalmente porque nos permite introducir en cada rama de las Matemáticas los conceptos más apropiados, aunque no procedan del desarrollo sistemático del concepto de número (que frecuentemente no es lo más adecuado). Es decir, permite definir conceptos tan sutiles como el de espacio, que en el ejemplo anterior sería la estructura definida por los axiomas de la Geometría euclídea.

En segundo lugar, porque las consecuencias lógicas de los axiomas son válidas para cualquier teoría que los verifique, no sólo para aquella que nos haya llevado a establecerlos. Es decir, la consideración atenta y paciente de cierta estructura que tengamos "a la vista" nos lleva a desentrañar las relaciones básicas que la fundamentan y que explicitamos en forma de axiomas; pero, una vez establecidos, podemos estudiar sus consecuencias lógicas, que obviamente serán ciertas en cualquier otra estructura que cumpla tales axiomas, y éstas pueden ser muy diferentes de la que teníamos "ante los ojos". Por ejemplo, una vez establecidos los axiomas de la Geometría euclídea, deberemos entender que sus puntos, rectas, planos, etc., son cualesquiera objetos que estén dotados de relaciones que verifiquen tales axiomas y Hilbert (1862-1943) observó que los puntos de una geometría euclídea pueden ser objetos sorprendentemente distintos de los que pudiéramos esperar: muchas funciones verifican, con una adecuada definición de la incidencia y la perpendicularidad, los axiomas de la Geometría euclídea, de modo que en tales espacios de funciones son válidos todos los teoremas clásicos de geometría. Esta observación de que muchas funciones son los puntos de una geometría euclídea no es una mera curiosidad, sino que es el punto de arranque del Análisis Funcional y desde principios del siglo XX ha intervenido de una forma u otra en todos los desarrollos del Análisis y la Mecánica Cuántica (donde los estados de un sistema son los puntos de una geometría euclídea, con la salvedad de que los escalares son los números complejos y no los reales). Resumiendo, en muchos conjuntos hay definidas relaciones que satisfacen los axiomas de la Geometría euclídea, de modo que en ellos también hay triángulos, parábolas, etc., y se verifican todos los teoremas de la Geometría clásica. Este es un ejemplo muy claro de la teoría aristotélica de la materia y la forma, donde la materia son los elementos de los conjuntos involucrados y la forma viene dada por unas relaciones limitadas por ciertos axiomas. La

forma es la estructura y, contra nuestra inveterada tendencia a cosificar y mirar sólo la materia, conviene reiterar el descubrimiento platónico de que la forma es lo que importa. En Matemáticas los conjuntos representan ese resto de materia que es tan difícil eliminar; pero trataremos de aprehender esa verdad de que la estructura sólo es la forma[1] definiendo con precisión el concepto de *iso-morfismo* e imponiéndonos la exigencia de hablar siempre salvo isomorfismos.

Ciertos conceptos, como el de punto o el de espacio en Geometría, no se reducen a otros conceptos previos, sino que apuntan directamente a la estructura (por eso son tan cercanos, sutiles y escurridizos cuando se intentan analizar) y deben definirse por el hecho de *estar* en determinado ambiente, de existir dentro de una estructura dada por ciertos axiomas. Los conceptos fundamentales presuponen una estructura previa en la que adquieren su sentido[2]. Incluso pueden tener varios sentidos distintos si la estructura en cuestión admitiera varias posibilidades no isomorfas, que es lo usual. Esta visión de los griegos abre un nuevo camino que exige, en cada rama de la Filosofía (geometría, gramática, ética, mecánica, economía, música, etc.) la aclaración previa de las hipótesis o axiomas que determinan la estructura subyacente, del ámbito que confiere su sentido a todos los conceptos y afirmaciones de la teoría en cuestión.

La cultura griega alcanzó a aplicar el método axiomático a la geometría, en los famosos *Elementos* de Euclides (325?-265? a. de Cristo), y a la estática, en el libro *Del equilibrio de los planos* de Arquímedes (287-212 a. de Cristo). Desde el declive de la Filosofía griega, ninguna otra cultura volvió a vivir esta exigencia de exposición axiomática de todos los ámbitos del conocimiento, y las Matemáticas siguieron el camino de desarrollar sistemáticamente el concepto de número, aplicándolo a todas sus ramas. En el siglo XVII, Descartes (1596-1650) retoma la visión griega y plantea el "método geométrico" como exigencia de todo saber humano verdadero, dando ejemplos de su utilización del método en los tres apéndices *Dióptrica, Meteoros* y *Geometría* de su *Discurso del método* de 1637. El mejor fruto de los esfuerzos de los filósofos racionalistas por dar cumplimiento

[1] La estructura en sí misma, sin ningún soporte material que nos la muestre, la llamaba Platón (427-347 a. de Cristo) *idea* y afirmaba que *las cosas múltiples caen en el campo de los sentidos y no en el del entendimiento; y, en cambio, las ideas son percibidas por el entendimiento, pero no vistas.* Un día que Antístenes le comentó que había visto muchos caballos pero nunca la "caballeidad", Platón le respondió que eso se debía a que siempre miraba con los ojos y nunca con la inteligencia. Ese día Atenas vivió una explosión mayor que la de una bomba nuclear, y ahora tú y yo estamos sufriendo todavía la sacudida de su onda expansiva.

[2] Esto ocurre con casi todos los conceptos importantes de la Ciencia. El razonamiento que pasa de los conceptos a lo que en ellos está implícito, de las consecuencias a sus principios, que desentraña las estructuras subyacentes en nuestro pensamiento, que responde a la pregunta *¿Qué decimos cuando decimos que ...?*, recibe el nombre de *razonamiento dialéctico* y es mucho más humilde, pasivo, femenino y silencioso que el razonamiento deductivo. Sin duda también es mucho más importante. Por desgracia, hoy en día hay un acuerdo tácito y universal de que en los textos matemáticos formales y acabados sólo deben aparecer los razonamientos deductivos, las demostraciones.

a la visión cartesiana es el desarrollo axiomático de la Mecánica expuesto por Newton (1642-1727) en sus *Philosophiae Naturalis Principia Mathematica* de 1687. Descartes considera incluso el desarrollo de cada ciencia a partir de unos principios propios como una situación incompleta que nos invita a considerar atentamente tales principios y reducirlos a otros más generales, claros y simples; aspirando así a la unificación de todo el saber humano absolutamente cierto, que debería obtenerse de un único punto de partida:

> "Si alguna de las cosas de que hablo al principio de la *Dióptrica* o de los *Meteoros* producen extrañeza, porque las llamo suposiciones y no parezco dispuesto a probarlas, ... Y si las he llamado suposiciones, es para que se sepa que pienso poder deducirlas de las primeras verdades que he explicado en este discurso; ..."

Las sucesivas aclaraciones de los principios de una ciencia son sus mejores momentos, sus grandes avances.

En el caso de la Geometría, la exigencia cartesiana de revisión de los principios establecidos en los *Elementos* de Euclides comienza a principios del siglo XIX en Alemania. Los estudios de las hipótesis que subyacen en la geometría realizados por Gauss (1777-1855), Riemann (1826-1866) y Klein (1849-1925) inician un giro copernicano en la orientación de las Matemáticas, considerando que cada rama determina la estructura que le es propia. Con el cambio de siglo, este movimiento de regreso a la visión griega se plantea con total claridad y reconocimiento explícito de sus exigencias por Hilbert (1862-1943) y, tras la obra de Bourbaki[3] a mediados del siglo XX, se ha extendido ya a todas las ramas de las Matemáticas.

De ahí la gran diferencia que el alumno encontrará entre la forma de exposición de las asignaturas de la Licenciatura y la que ha vivido desde sus primeros estudios. Cada asignatura ha de comenzar por la afirmación explícita de los axiomas que definan la estructura que le es propia para, a lo largo del curso, estudiar las consecuencias lógicas de los axiomas y las posibilidades no isomorfas de tal estructura. Por eso los objetos matemáticos no se agrupan según sus semejanzas aparentes, sino por la similitud de sus estructuras subyacentes: los números enteros y los polinomios en una indeterminada se estudiarán simultáneamente porque en ambos casos hallamos la estructura de anillo euclídeo, igualmente las ecuaciones diofánticas de grado 1 y las transformaciones lineales del espacio porque en ambos encontramos la estructura de módulo sobre tales anillos, el concepto de límite de una sucesión junto con el de finitud del espacio porque en ambos subyace una estructura topológica, etc.

En este capítulo nuestro propósito es iniciar la aclaración de la estructura implícita en el concepto de número: ¿qué conceptos y relaciones se dan allí donde los

[3] Autor colectivo francés fundado por A. Weil (1906-1998, hermano mayor de Simone Weil), H. Cartan (1904-2008), J. Dieudonné (1906-1992), C. Chevalley (1909-1984) y C. Ehresmann (1905-1979) entre otros.

hombres hemos llamado número a lo que teníamos ante los ojos? Siempre que tenemos dos números, tenemos ya presente un tercero: su suma, y esta operación de sumar es asociativa, conmutativa, admite elemento neutro (el cero) y todo número tiene un opuesto (salvo en los números naturales). La estructura de *grupo* es la que define cualquier operación que verifique tales condiciones, excepto la conmutatividad[4]. Aprenderemos a definir y razonar dentro de la estructura de grupo, a reconocer estructuras de grupo isomorfas, a relacionar grupos distintos, etc.; para abordar en cursos posteriores las estructuras involucradas en la Geometría y la Física, que forman el núcleo central de esta renovación de la Ciencia a que nos hemos referido.

2.1 Grupos y Subgrupos

Definición: Sea X un conjunto. Llamaremos **operación** o ley de composición interna en X a toda aplicación $X \times X \longrightarrow X$.

Representaremos las operaciones con los símbolos $+$, $\cdot$, $*$, etc., en cuyo caso la imagen de cada pareja $(x, y) \in X \times X$ se denotará respectivamente $x+y$, $x \cdot y$, $x*y$, etc. La suma y el producto de números naturales, enteros, racionales, reales y complejos son operaciones, mientras que la diferencia de números naturales y el cociente de números enteros no lo son.

Axiomas de Grupo: Diremos que una operación $G \times G \stackrel{\cdot}{\longrightarrow} G$ define una estructura de **grupo** en el conjunto G si verifica las siguientes condiciones:

Axioma 1: (*Propiedad asociativa*) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in G$.

Axioma 2: Existe un elemento en G, que se llama **neutro**[5] y se denota 1, tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in G$.

Axioma 3: Si $a \in G$, entonces existe un elemento $a^{-1} \in G$, llamado **inverso**[6] de a, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Si además se verifica que $a \cdot b = b \cdot a$ para todo $a, b \in G$, diremos que el grupo es **abeliano** o **conmutativo**; en cuyo caso a menudo denotaremos $+$ la operación

[4] Aunque nuestro propósito inicial es el estudio de las estructuras de los números y en éstos la suma siempre es conmutativa, eliminaremos esta condición para dar cabida al enorme cúmulo de intuiciones que provienen de todos los contextos en que encontramos simetrías. En el excelente libro *Simetría* de H. Weyl (1885-1955) pueden verse muchos ejemplos donde percibimos regularidad y el autor muestra el grupo que subyace en cada uno.

[5] El elemento neutro es necesariamente único, pues si e fuera otro elemento neutro tendríamos $e = e \cdot 1 = 1$.

[6] Tal elemento es único pues si existiera otro elemento $b \in G$ tal que $a \cdot b = 1$, entonces tendríamos $a^{-1} = a^{-1} \cdot 1 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b$.

del grupo, 0 el elemento neutro y $-a$ el único elemento de G tal que $a+(-a)=0$ (y lo llamaremos **opuesto** en vez de inverso).

El conjunto de los números enteros con la suma es el ejemplo básico de grupo conmutativo.

Definición: Sea $(G,\cdot)$ un grupo. Si H es un subconjunto de G, diremos que H es un **subgrupo** del grupo G cuando H verifique las siguientes condiciones

1. La operación de G induce una operación en H: $a,b\in H \Rightarrow a\cdot b\in H$.
2. El elemento neutro de G está en H: $1\in H$.
3. El inverso de cualquier elemento de H está en H: $a\in H \Rightarrow a^{-1}\in H$.

Por tanto, si H es un subgrupo de un grupo G, la operación de G define en H una estructura de grupo.

Proposición 2.1.1 *La intersección de cualquier familia de subgrupos de un grupo G también es un subgrupo de G.*

Demostración: Sea $\{H_i\}_{i\in I}$ una familia de subgrupos de G y $H=\cap_i H_i$.

Es claro que $1\in H$, porque $1\in H_i$ para todo índice i.

Si $a\in H$, entonces $a\in H_i$ y $a^{-1}\in H_i$ para todo índice $i\in I$; luego $a^{-1}\in H$.

Si $a,b\in H$, entonces $a,b\in H_i$ y $ab\in H_i$ para todo índice $i\in I$; luego $ab\in H$ y se concluye que H es un subgrupo de G. q.e.d.

Como consecuencia directa de esta proposición tenemos que, si X es un subconjunto de un grupo G, la intersección de todos los subgrupos de G que contienen a X es un subgrupo de G y diremos que es el subgrupo de G **engendrado** o **generado** por X (o bien que X es un **sistema de generadores** de tal subgrupo). El subgrupo de G generado por X es un subgrupo de G que contiene a X y que está contenido en cualquier otro subgrupo de G que contenga a X: es el menor subgrupo de G que contiene a X.

Por ejemplo, el subgrupo de $\mathbb{Z}$ generado por un número entero n es

$$n\mathbb{Z}:=\{an:\ a\in\mathbb{Z}\}$$

y el subgrupo de $\mathbb{Z}$ generado por dos números enteros m,n es

$$m\mathbb{Z}+n\mathbb{Z}:=\{am+bn:\ a,b\in\mathbb{Z}\}.$$

2.2 Aritmética Elemental

Teorema 2.2.1 *Si H es un subgrupo del grupo aditivo de los números enteros, entonces existe un único número natural n tal que $H=n\mathbb{Z}$.*

Demostración: Veamos primero la existencia de tal número natural n.

Si $H = 0$, tomamos $n = 0$.

Si $H \neq 0$, en H hay números naturales positivos porque el opuesto de cada número de H también está en H. Sea n el menor número positivo de H. Por definición $n \in H$, así que $n\mathbb{Z} \subseteq H$ por ser H un subgrupo. Ahora bien, si $m \in H$, existen números enteros c y r tales que

$$m = cn + r \ , \quad 0 \leq r \leq n - 1$$

Luego $r = m - cn \in H$, porque H es un subgrupo y $m, n \in H$. De acuerdo con la elección de n tenemos que $r = 0$. Se sigue que $m \in n\mathbb{Z}$ y concluimos que $H = n\mathbb{Z}$.

Por último demostraremos la unicidad del número natural que genera H. Si m y n son dos números naturales tales que $H = m\mathbb{Z} = n\mathbb{Z}$, entonces m es múltiplo de n y n es múltiplo de m; luego $m = n$.

Definición: Sean a, b dos números enteros. Diremos que a es **múltiplo** de b (o que b es **divisor** de a) si $a = bc$ para algún $c \in \mathbb{Z}$; i.e., si $a\mathbb{Z} \subseteq b\mathbb{Z}$.

Diremos que un número natural p mayor que 1 es **primo** cuando no pueda descomponerse en producto de dos números naturales más pequeños (es decir, cuando $p > 1$ y sus únicos divisores naturales son 1 y p).

Definición: Sean a, b dos números enteros. Diremos que un número natural es el **mínimo común múltiplo** de a y b si es un múltiplo común y divide a cualquier otro múltiplo común. Diremos que un número natural es el **máximo común divisor** de a y b si es un divisor común y es múltiplo de cualquier otro divisor común. Diremos que a y b son **primos entre sí** cuando su máximo común divisor sea la unidad.

Si n es un número natural no nulo, $\phi(n)$ denotará el número de números naturales entre 1 y n que son primos con n. Esta función ϕ se llama **indicador de Euler** (1707-1783) y sus primeros valores son:

$$\phi(2) = 1, \ \phi(3) = 2, \ \phi(4) = 2, \ \phi(5) = 4, \ \phi(6) = 2, \ \phi(7) = 6, \ \phi(8) = 4$$
$$\phi(p) = p - 1 \ \text{ cuando } p \text{ es primo}$$

En principio el máximo común divisor o el mínimo común múltiplo de dos números enteros podría no existir; pero veremos que no es el caso:

Proposición 2.2.2 *Sean a y b dos números enteros. La condición necesaria y suficiente para que un número natural m sea el mínimo común múltiplo de a y b es que $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Luego el mínimo común múltiplo de dos números enteros siempre existe y es único.*

Demostración: La condición es suficiente porque $m \in m\mathbb{Z}$.

Veamos la necesidad de la condición. Si $m = \text{m.c.m.}(a, b)$, entonces $a\mathbb{Z} \cap b\mathbb{Z} \subseteq m\mathbb{Z}$ y $m \in a\mathbb{Z} \cap b\mathbb{Z}$; luego $m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$, porque $a\mathbb{Z} \cap b\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$, y concluimos que $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Proposición 2.2.3 *Sean a y b dos números enteros. La condición necesaria y suficiente para que un número natural d sea el máximo común divisor de a y b es que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Por tanto, el máximo común divisor de dos números enteros siempre existe y es único.*

Demostración: La condición es claramente suficiente.

En cuanto a su necesidad, si $d = \text{m.c.d.}(a, b)$, entonces $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ porque $a, b \in d\mathbb{Z}$. Además, en virtud de 2.2.1, existe $c \in \mathbb{N}$ tal que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$, de modo que c es un divisor común de a y b; luego d es múltiplo de c y $d\mathbb{Z} \subseteq c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Se concluye que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Identidad de Bézout (1730-1783)**:** *Sean a y b dos números enteros. Si d es el máximo común divisor de a y b, entonces existen números enteros α y β tales que*

$$d = \alpha a + \beta b$$

Corolario 2.2.4 *La condición necesaria y suficiente para que dos números enteros a, b sean primos entre sí es que existan números enteros α, β tales que*

$$1 = \alpha a + \beta b$$

Demostración: La necesidad de la condición es la Identidad de Bézout cuando $d = 1$. En cuanto a la suficiencia, si $1 = \alpha a + \beta b$, entonces $1 \in a\mathbb{Z} + b\mathbb{Z}$ y $\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. Luego $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ y concluimos que $1 = \text{m.c.d.}(a, b)$.

Corolario 2.2.5 *La condición necesaria y suficiente para que la raíz n-ésima de la unidad $e^{\frac{2\pi i}{n}k}$ sea primitiva es que k y n sean primos entre sí. Por tanto el número de raíces n-ésimas de la unidad primitivas es $\phi(n)$.*

Demostración: Sabemos que $e^{\frac{2\pi i}{n}k}$ es primitiva precisamente cuando $ak \equiv 1$ (módulo n) para algún número entero a; es decir, cuando $1 = ak + bn$, $b \in \mathbb{Z}$, y tal condición equivale a que $\text{m.c.d.}(k, n) = 1$ según 2.2.4.

Corolario 2.2.6 *Si un número entero divide a un producto de dos números enteros y es primo con un factor, entonces divide al otro factor.*

Demostración: Sean $a, b, c \in \mathbb{Z}$. Si bc es múltiplo de a, y b es primo con a, entonces existen $\alpha, \beta \in \mathbb{Z}$ tales que $1 = \alpha a + \beta b$ y concluimos que $c = \alpha ac + \beta bc$ es múltiplo de a por que ambos sumandos lo son.

Lema de Euclides (325?-265? a. de Cristo)**:** *Si un número primo divide a un producto de números enteros, entonces divide a algún factor.*

Demostración: Sea p un número primo. Si un número entero n no es múltiplo de p, entonces p y n son primos entre sí, porque los únicos divisores de p son 1 y p. Ahora el lema de Euclides es consecuencia directa de 2.2.6.

Teorema de Descomposición: *Todo número natural mayor que 1 es producto de números primos. Esta descomposición es única salvo el orden de los factores.*

Demostración: Veamos primero la *existencia* de la descomposición. Si un número natural $n \geq 2$ es primo, no hay nada que probar. Si n no es primo, descompone en producto de dos números menores, $n = ab$. Si algún factor no es primo, descompone en producto de dos números más pequeños. Reiterando el proceso, en algún momento ha de terminar, pues n tiene un número finito de divisores, y obtenemos una descomposición de n en producto de números primos.

Veamos la *unicidad* de la descomposición. Si $n = p^m p_1 \dots p_r$ es una descomposición de un número natural n en producto de primos, donde suponemos que $p_i \neq p$ para todo índice i, del lema de Euclides se sigue que p^{m+1} no divide a n, así que p^m es precisamente la mayor potencia de p que divide a n. Luego el número de veces m que aparece un número primo p no depende de la descomposición elegida: ésta es única salvo el orden de los factores.

Corolario 2.2.7 *Todo número natural mayor que 1 es múltiplo de algún primo.*

Corolario 2.2.8 *Hay infinitos números primos.*

Demostración: Procederemos por reducción al absurdo; es decir, partiendo de la negación del enunciado que pretendemos probar, obtendremos una contradicción, lo que nos permite concluir que tal enunciado es verdadero[7]. Supongamos que sólo hay un número finito de números primos $p_1, \dots, p_r$ y consideremos el número $n = 1 + p_1 \cdots p_r$. Por el corolario anterior, n es múltiplo de algún número primo p, que es distinto de todos los primos $p_1, \dots, p_r$, pues al dividir n por p_i el resto es 1, lo que contradice la suposición de que $p_1, \dots, p_r$ son todos los números primos.

[7]Los razonamientos por reducción al absurdo se basan en dos principios fundamentales: uno es nuestra convicción de que un enunciado y su negación no pueden ser verdaderos a la vez, el otro la de que una afirmación o su contraria ha de ser cierta. El principio de no contradicción, que en nuestro caso se expresa como la imposibilidad de obtener, mediante razonamientos lógicos, un enunciado y su negación a partir de las propiedades elementales de los números naturales, no se basa en nuestra experiencia, pues aunque nuestros razonamientos no hayan derivado "de hecho" ninguna contradicción hasta el presente, sólo representan una parte infinitesimalmente pequeña de la infinitud de razonamientos posibles, que es sobre la que se afirma tal principio. Es admirable nuestra reiterada confianza en la ausencia de absurdos en el camino de la razón humana, similar a la de un bebé en sus padres.

Corolario 2.2.9 *Si un número natural n mayor que 1 no tiene divisores primos menores o iguales que $\sqrt{n}$, entonces n es un número primo.*

Demostración: Probaremos el enunciado contra-recíproco. Si $n > 1$ no es primo, descompone en producto de dos números naturales más pequeños. Algún factor de tal descomposición ha de ser menor o igual que $\sqrt{n}$ y, por tanto, cualquier divisor primo de ese factor es un divisor primo de n menor o igual que $\sqrt{n}$.

Corolario 2.2.10 *Sea $d \geq 2$ un número natural. Si la raíz d-ésima de un número natural n no es entera, entonces es irracional.*

Demostración: Probaremos el enunciado contra-recíproco: si la raíz d-ésima de un número natural n es racional, entonces n es potencia d-ésima de algún número natural. Sea b/c un número racional tal que $n = (b/c)^d$. Dividiendo b y c por su máximo común divisor podemos suponer que b y c son primos entre sí. Como $b^d = nc^d$, del lema de Euclides se sigue que todos los números primos que dividen a c dividen también a b. Luego ningún número primo divide a c, y el teorema anterior permite concluir que $c = 1$, así que b/c es un número entero y n es la potencia d-ésima del número entero b/c.

2.2.11 Todo número natural $n \geq 2$ descompone de la siguiente forma:

$$n = p_1^{n_1} \cdots p_r^{n_r} \ , \quad n_i \geq 1,$$

donde $p_1, \ldots, p_r$ son números primos distintos, y tal descomposición es única salvo el orden de los factores. Del lema de Euclides se sigue que si un número primo p divide a n, entonces $p = p_i$ para algún índice i: *Los únicos factores primos de n son los números $p_1, \ldots, p_r$.*

Si $a = p_1^{a_1} \cdots p_r^{a_r}$ y $b = p_1^{b_1} \cdots p_r^{b_r}$ son descomposiciones de dos números naturales a, b en producto de primos distintos ($a_i, b_i \geq 0$), entonces

$$b \text{ es múltiplo de } a \Leftrightarrow b_i \geq a_i \text{ para todo índice } i$$
$$\text{m.c.d.}(a,b) = p_1^{d_1} \cdots p_r^{d_r} \ , \quad d_i = \min(a_i, b_i)$$
$$\text{m.c.m.}(a,b) = p_1^{m_1} \cdots p_r^{m_r} \ , \quad m_i = \max(a_i, b_i)$$

En particular, $ab = \text{m.c.d.}(a,b) \cdot \text{m.c.m.}(a,b)$.

Algoritmo de Euclides: *Sean $a, b, c, r \in \mathbb{Z}$. Si $a = bc + r$, entonces*

$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r)$$

Demostración: $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$ porque $a = bc + r$ está en $b\mathbb{Z} + r\mathbb{Z}$, y $r = a - bc$ está en $a\mathbb{Z} + b\mathbb{Z}$.

Este algoritmo permite calcular rápidamente el máximo común divisor d de dos números enteros no nulos a, b, y los coeficientes de la Identidad de Bézout. Se efectúan las divisiones:

$$a = c_1 b + r_1 \ , \ b = c_2 r_1 + r_2 \ , \ r_1 = c_3 r_2 + r_3 \ , \ \dots \ , \ r_{n-1} = c_{n+1} r_n + 0$$

hasta que el resto sea nulo, lo que necesariamente ha de ocurrir, pues la sucesión de restos $r_1, r_2, \dots$ es estrictamente decreciente. Según el resultado anterior, el máximo común divisor de a y b coincide con el máximo común divisor de dos términos sucesivos cualesquiera de la sucesión

$$a \, , \ b \, , \ r_1 \, , \ r_2 \, , \ \dots \, , \ r_n \, , \ 0$$

Como m.c.d.$(r_n, 0) = r_n$, concluimos que el máximo común divisor d de a y b es el último resto no nulo r_n.

Además, cuando tengamos una descomposición $d = \gamma r_i + \delta r_{i+1}$ del máximo común divisor d en suma de múltiplos de r_i y r_{i+1}, la división de resto r_{i+1} permite descomponer d como suma de un múltiplo de r_{i-1} y un múltiplo de r_i:

$$d = \gamma r_i + \delta(r_{i-1} - c_i r_i) = \delta r_{i-1} + (\gamma - \delta c_i) r_i$$

Al ser $d = r_n = r_{n-2} - c_n r_{n-1}$, procediendo recurrentemente obtenemos una descomposición del máximo común divisor d como suma de múltiplos de a y b.

2.3 Morfismos de Grupos

Definición: Diremos que una aplicación $f\colon G \to G'$ entre dos grupos es un **morfismo de grupos** cuando para todo $a, b \in G$ se verifique

$$f(a \cdot b) = f(a) \cdot f(b)$$

Diremos que un morfismo de grupos $f\colon G \to G'$ es un **isomorfismo**[8] si existe un morfismo de grupos $g\colon G' \to G$ tal que $f \circ g$ es la identidad de G' y $g \circ f$ es la identidad de G, en cuyo caso diremos que tal morfismo g (que claramente es único, pues es la aplicación inversa de f) es el morfismo **inverso** de f y lo denotaremos f^{-1}. Llamaremos **automorfismos** de un grupo G a los isomorfismos de G en G.

Los morfismos de grupo conservan el neutro y los inversos:

$$f(1) = 1$$
$$f(a^{-1}) = f(a)^{-1}$$

[8] Los isomorfismos cambian los elementos de los grupos, pero respetan la operación, de modo que cualquier afirmación que se refiera sólo a la estructura de grupo (es decir, que se enuncie únicamente con la operación del grupo) es simultáneamente cierta o falsa en ambos grupos. Si dos grupos son isomorfos, tienen las mismas propiedades en la teoría de grupos.

porque $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ implica que $f(1) = 1$ y $1 = f(1) = f(aa^{-1}) = f(a) \cdot f(a^{-1})$ implica que $f(a^{-1})$ es el inverso de $f(a)$.

Proposición 2.3.1 *Si $f\colon G \to G'$ y $g\colon G' \to G''$ son morfismos de grupos, entonces su composición $g \circ f\colon G \to G''$ también es un morfismo de grupos.*

Demostración: Para todo par de elementos $a, b \in G$ tenemos que

$$(gf)(ab) = g(f(ab)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = (gf)(a) \cdot (gf)(b)$$

Definición: Si $f\colon G \to G'$ es un morfismo de grupos, diremos que

$$\operatorname{Ker} f = \{a \in G\colon \ f(a) = 1\}$$
$$\operatorname{Im} f = \{f(a)\colon \ a \in G\}$$

son el **núcleo** y la **imagen** de f respectivamente.

La imagen de f está formada por todos los elementos $b \in G'$ tales que la ecuación $f(x) = b$ tiene alguna solución $x \in G$. Si la operación de G' se denota aditivamente, el núcleo de f está formado por las soluciones de la ecuación homogénea $f(x) = 0\,$.

Proposición 2.3.2 *Si $f\colon G \to G'$ es un morfismo de grupos, entonces*

$$f \text{ es inyectivo} \ \Leftrightarrow \ Ker(f) = 1$$
$$f \text{ es isomorfismo} \ \Leftrightarrow \ f \text{ es biyectivo}$$

Demostración: Las implicaciones directas son inmediatas.

En cuanto a las recíprocas, si $\operatorname{Ker} f = 1$ y $f(a) = f(b)$, entonces $f(a^{-1}b) = 1$; luego $a^{-1}b = 1$ y $a = b$.

Si f es biyectivo, entonces existe la aplicación inversa f^{-1} tal que $f \circ f^{-1}$ y $f^{-1} \circ f$ son la identidad de G' y G respectivamente, así que bastará comprobar que f^{-1} es morfismo de grupos. Ahora bien, $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$ porque f es inyectivo y

$$f\left(f^{-1}(x) \cdot f^{-1}(y)\right) = f\left(f^{-1}(x)\right) \cdot f\left(f^{-1}(y)\right) = x \cdot y = f\left(f^{-1}(xy)\right)$$

Proposición 2.3.3 *Sea $f\colon G \to G'$ un morfismo de grupos.*

Si H es un subgrupo de G, entonces

$$f(H) := \{f(h)\colon \ h \in H\}$$

es un subgrupo de G'. En particular, $\operatorname{Im} f$ *es un subgrupo de G'.*

Si H' es un subgrupo de G', entonces

$$f^{-1}(H') := \{a \in G : \ f(a) \in H'\}$$

es un subgrupo de G. En particular, $\operatorname{Ker} f$ *es un subgrupo de G.*

Demostración: Veamos primero que $f(H)$ es un subgrupo de G':

$1 \in f(H)$ porque $f(1) = 1$ y $1 \in H$.

Si $x, y \in f(H)$, entonces existen $a, b \in H$ tales que $x = f(a)$, $y = f(x)$. Luego $xy = f(ab) \in f(H)$, porque $ab \in H$, y $x^{-1} = f(a^{-1}) \in f(H)$ porque $a^{-1} \in H$.

Veamos ahora que $f^{-1}(H')$ es un subgrupo de G:

$1 \in f^{-1}(H')$, porque $f(1) = 1 \in H'$.

Si $a, b \in f^{-1}(H')$, entonces $f(ab) = f(a)f(b) \in H'$ y se sigue que su producto $ab \in f^{-1}(H')$.

Si $a \in f^{-1}(H')$, entonces $f(a^{-1}) = f(a)^{-1} \in H'$ y se sigue que su inverso $a^{-1} \in f^{-1}(H')$.

Por último, $\operatorname{Im} f = f(G)$ y $\operatorname{Ker} f = f^{-1}(1)$.

2.4 Grupo Cociente

Sea G un grupo. Cada subgrupo H de G define una relación $\equiv$ en G:

$$a \equiv b \;\Leftrightarrow\; a^{-1}b \in H$$

que es una relación de equivalencia en G:

1. Si $a \in G$, entonces $a \equiv a$ porque $a^{-1}a = 1 \in H$ para todo $a \in G$.
2. Sean $a, b \in G$. Si $a \equiv b$, entonces $a^{-1}b \in H$, luego $b^{-1}a = \left(a^{-1}b\right)^{-1}$ está en H y $b \equiv a$.
3. Sean $a, b, c \in G$. Si $a \equiv b$ y $b \equiv c$, entonces $a^{-1}b, b^{-1}c \in H$, luego su producto $(a^{-1}b)(b^{-1}c) = a^{-1}c$ está en H y concluimos que $a \equiv c$.

Respecto de esta relación de equivalencia, la clase de equivalencia de cualquier elemento $a \in G$ es precisamente

$$aH = \{ah\colon\ h \in H\}$$

y el conjunto cociente de G por la relación de equivalencia inducida por el subgrupo H se denotará G/H.

Definición: Llamaremos **orden** de un grupo a su cardinal[9]. Llamaremos **índice** de un subgrupo H de un grupo G al cardinal de G/H; es decir, al número de clases de equivalencia de la relación que H define en G.

[9]El cardinal de un conjunto finito X es el número de elementos de X y se denota $|X|$. En general, aunque los conjuntos sean infinitos, se dice que dos conjuntos tienen el mismo cardinal si existe alguna biyección entre ellos. Los conjuntos numerables son los que tienen el mismo cardinal que el conjunto de los números naturales $\mathbb{N}$.

Ejemplo: Sea n un número natural positivo. La relación de equivalencia que el subgrupo $n\mathbb{Z}$ define en $\mathbb{Z}$ es justamente la relación de congruencia módulo n; así que $\mathbb{Z}/n\mathbb{Z}$ es el conjunto de clases de restos módulo n, que tiene n elementos (luego el índice de $n\mathbb{Z}$ en $\mathbb{Z}$ es n):

$$\mathbb{Z}/n\mathbb{Z} = \{[1], [2], \ldots, [n] = [0]\}$$

Teorema de Lagrange (1736-1813): *Si H es un subgrupo de un grupo finito G, el orden de H divide al orden de G y el cociente es el índice de H en G:*

$$|G/H| = |G| : |H|$$

Demostración: Si $a \in G$, entonces aH y H tienen el mismo número de elementos, porque la aplicación

$$H \xrightarrow{a\cdot} aH \ , \quad h \mapsto ah$$

es biyectiva. En efecto, es epiyectiva por definición de aH y es inyectiva porque, si $ax = ay$, entonces $x = a^{-1}(ax) = a^{-1}(ay) = y$.

Se sigue que todas las clases de equivalencia de la relación de equivalencia que H define en G tienen el mismo número de elementos que H. Ahora bien, al ser G la unión disjunta de tales clases de equivalencia, concluimos que el orden de G es el producto de $|H|$ por el número de clases de equivalencia, que es el índice $|G/H|$ de H en G.

Construcción del Grupo Cociente

Sea H un subgrupo de un grupo G. Veamos cuándo existe alguna estructura de grupo en el conjunto cociente G/H tal que la proyección canónica $\pi\colon G \to G/H$ sea morfismo de grupos. En tal caso $H = \{g \in G\colon \pi(g) = \pi(1)\}$ sería el núcleo del morfismo π, así que verificaría la siguiente condición:

Definición: Sea H un subgrupo de un grupo G. Diremos que H es un subgrupo **normal** de G cuando $aHa^{-1} \subseteq H$ para todo $a \in G$; es decir:

$$h \in H,\, a \in G \Rightarrow aha^{-1} \in H$$

Si un grupo G es conmutativo, todo subgrupo de G es normal en G.

Proposición 2.4.1 *Sea $f\colon G \to G'$ un morfismo de grupos. El núcleo de f es un subgrupo normal de G.*

Demostración: Si $x \in \operatorname{Ker} f$, entonces $f(axa^{-1}) = f(a) \cdot 1 \cdot f(a)^{-1} = 1$ para todo $a \in G$, y se concluye que $axa^{-1} \in \operatorname{Ker} f$.

Teorema 2.4.2 *Si H es un subgrupo normal de un grupo G, en el conjunto cociente G/H existe una única estructura de grupo tal que la proyección canónica $\pi\colon G \to G/H$ es morfismo de grupos.*

Además, $H = \operatorname{Ker}\pi$.

Demostración: Si $x, y \in G/H$, definimos $x \cdot y = \pi(ab)$, donde $a, b \in G$, $x = \pi(a)$, $y = \pi(b)$:

$$[\,a\,]\cdot[\,b\,] \,=\, [\,ab\,]$$

Para ver que así tenemos definida una operación en G/H es necesario probar que $x\cdot y$ no depende de los representantes a, b elegidos: Si $a', b' \in G$ y $x = [a']$, $y = [b']$, entonces $[a'b'] = [ab]$:

Si $[a'] = [a]$, existe $h \in H$ tal que $a' = ah$; luego $a'b = ahb$. Como H es un subgrupo normal de G, se tiene que $h' := b^{-1}hb \in H$ y $hb = bh'$. Luego $a'b = abh' \in abH$ y concluimos que $[a'b] = [ab]$. Si además $b' \in bH$, es claro que $a'b' \in a'bH$ y $[a'b'] = [a'b]$.

Veamos que esta operación define en G/H una estructura de grupo:

$$([\,a\,]\cdot[\,b\,])\cdot[\,c\,]=[\,ab\,]\cdot[\,c\,]=[(ab)c\,]=[\,a(bc)]=[\,a\,]\cdot[\,bc\,]=[\,a\,]\cdot([\,b\,]\cdot[\,c\,])$$

G/H tiene un elemento neutro, que es el $[\,1\,]$:

$$[\,a\,]\cdot[\,1\,] = [\,a\cdot 1\,] = [\,a\,]$$
$$[\,1\,]\cdot[\,a\,] = [\,1\cdot a\,] = [\,a\,]$$

Cada elemento $[\,a\,] \in G/H$ tiene un elemento inverso, que es $[\,a^{-1}]$:

$$[\,a\,]\cdot[\,a^{-1}] = [\,a\cdot a^{-1}] = [\,1\,]$$
$$[\,a^{-1}]\cdot[\,a\,] = [\,a^{-1}\cdot a\,] = [\,1\,]$$

y π es un morfismo de grupos porque, por definición de la operación tenemos $\pi(a)\cdot\pi(b) = [\,a\,]\cdot[\,b\,] = [\,ab\,] = \pi(ab)$ para todo a, $b \in G$.

Por otra parte, si $*$ es otra operación en G/H tal que $\pi\colon G \to (G/H, *)$ es un morfismo de grupos, para todo $[\,a\,]$, $[\,b\,] \in G/H$ tenemos que

$$[\,a\,]\cdot[\,b\,] = \pi(a)\cdot\pi(b) = \pi(ab) = \pi(a) * \pi(b) = [\,a\,] * [\,b\,]$$

Por último, $\operatorname{Ker}\pi = \{a \in G\colon\ \pi(a) = \pi(1)\} = \{a \in G\colon\ a \equiv 1\} = [\,1\,] = H$.

Definición: Sea H un subgrupo normal de un grupo G. Diremos que el conjunto G/H, con la única operación tal que $\pi\colon G \to G/H$ es un morfismo de grupos, es el **grupo cociente** de G por H y lo denotaremos también G/H.

Ejemplo: Si G es un grupo conmutativo, todo subgrupo H de G es normal, y el grupo cociente G/H también es conmutativo.

Sea n un número natural. Como $n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$, en el conjunto cociente $\mathbb{Z}/n\mathbb{Z}$ tenemos una estructura de grupo conmutativo que viene definida por la siguiente operación: $[a]_n + [b]_n := [a+b]_n$. El neutro de $\mathbb{Z}/n\mathbb{Z}$ es $[0]_n$ y el opuesto de cualquier elemento $[a]_n$ es $[-a]_n$.

Propiedad Universal: *Sea H un subgrupo normal de un grupo G y $\pi\colon G \to G/H$ la proyección canónica. Si $f\colon G \to G'$ es un morfismo de grupos y $H \subseteq \operatorname{Ker} f$, entonces existe un único morfismo de grupos $\phi\colon G/H \to G'$ tal que $f = \phi \circ \pi$:*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \searrow & & \nearrow \phi \\ & G/H & \end{array}$$

Demostración: Veamos en primer lugar la existencia de un morfismo de grupos $\phi\colon G/H \to G'$ tal que $f = \phi \circ \pi$.

Si $x \in G/H$, existe algún $a \in G$ tal que $x = \pi(a)$ y definimos $\phi(x) = f(a)$. Veamos que ϕ es una aplicación de G/H en G' (es decir, que $\phi(x)$ no depende del representante $a \in G$ elegido) cuando $H \subseteq \operatorname{Ker} f$. Si $[a] = [b]$, entonces $a \equiv b$ y $a^{-1}b \in H \subseteq \operatorname{Ker} f$; luego $1 = f(a^{-1}b) = f(a)^{-1}f(b)$ y concluimos que $f(a) = f(b)$.

Por definición $\phi(\pi(a)) = f(a)$ para todo $a \in G$, así que $f = \phi \circ \pi$ y para concluir basta probar que ϕ es morfismo de grupos. Si $[a], [b] \in G/H$, entonces

$$\phi([a] \cdot [b]) = \phi(\pi(ab)) = f(ab) = f(a)f(b) = \phi(\pi(a))\phi(\pi(b)) = \phi(x)\phi(y)$$

Por último, si existiera otro morfismo de grupos $\psi\colon G/H \to G'$ tal que $f = \psi \circ \pi$, para todo $[a] \in G/H$ tendríamos que

$$\phi([a]) = f(a) = (\psi \circ \pi)(a) = \psi([a])$$

Teorema de Isomorfía: *Sea $f\colon G \to G'$ un morfismo de grupos. La aplicación $\phi\colon G/\operatorname{Ker} f \to \operatorname{Im} f$; $\phi([a]) = f(a)$, es isomorfismo de grupos:*

$$\boxed{G/\operatorname{Ker} f \;\simeq\; \operatorname{Im} f}$$

Demostración: Sea $\varphi\colon G \to \operatorname{Im} f$ el morfismo de grupos $\varphi(a) = f(a)$. El núcleo de φ coincide con el de f, así que de la propiedad universal del grupo cociente se sigue la existencia de un morfismo de grupos $\phi\colon G/\operatorname{Ker} f \to \operatorname{Im} f$ tal que $\phi([a]) = f(a)$.

Veamos que ϕ es isomorfismo de grupos:

ϕ es epiyectivo: Si $x \in \operatorname{Im} f$, existe $a \in G$ tal que $x = f(a) = \phi([a])$; luego $x \in \operatorname{Im} \phi$.

ϕ es inyectivo: Si $1 = \phi([a]) = f(a)$, entonces $a \in \operatorname{Ker} f$ y $[a] = 1$. Es decir, $\operatorname{Ker} \phi = 1$ y, por 3.2, ϕ es inyectivo.

Corolario 2.4.3 *Si $f\colon G \to G'$ es un morfismo de grupos epiyectivo, entonces el grupo $G/\mathrm{Ker}\, f$ es isomorfo a G'.*

Teorema Chino del Resto: *Si $m, n \in \mathbb{N}$ son primos entre sí, la aplicación*

$$\phi\colon \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}) \quad , \quad \phi([a]_{mn}) = ([a]_m, [a]_n)$$

es un isomorfismo de grupos.

Demostración: Las proyecciones canónicas $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ son morfismos de grupos, de modo que la aplicación

$$f\colon \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \ , \quad f(a) = ([a]_m, [a]_n)$$

es un morfismo de grupos. El núcleo de f es $(m\mathbb{Z}) \cap (n\mathbb{Z}) = nm\mathbb{Z}$, porque el mínimo común múltiplo de m y n es mn, así que, por 2.4.3, basta probar que f es epiyectivo.

Ahora bien, de acuerdo con el teorema de isomorfía, el cardinal de $\mathrm{Im}\, f$ es el de $\mathbb{Z}/nm\mathbb{Z}$, que coincide con el de $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$, y concluimos que el morfismo f es epiyectivo.

2.5 Grupos Cíclicos

Sea $(G, \cdot)$ un grupo. Si $g \in G$, el producto de g consigo mismo m veces lo denotaremos g^m, el producto de g^{-1} consigo mismo m veces lo denotaremos g^{-m} y pondremos que g^0 es el neutro de G (cuando la operación de G se denote aditivamente, pondremos mg en lugar de g^m). Obtenemos así una aplicación

$$f_g : \mathbb{Z} \longrightarrow G \ , \quad f_g(m) = g^m$$

que es un morfismo de grupos porque $g^{m+n} = g^m \cdot g^n$ para todo $m, n \in \mathbb{Z}$. Su imagen es el subgrupo $\{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$, que es claramente el subgrupo generado por g y lo denotaremos (g).

Definición: Diremos que un grupo G es **cíclico** si está generado por alguno de sus elementos; es decir, si existe $g \in G$ tal que $(g) = G$, en cuyo caso diremos que g es un **generador** de G.

Por definición un grupo G es cíclico y $g \in G$ es un generador cuando todo elemento de G es de la forma g^m para algún número entero m. Es claro que los grupos cíclicos son conmutativos.

Clasificación[10] de Grupos Cíclicos: *Sea G un grupo cíclico.*

[10] Se entiende que la clasificación es salvo isomorfismos. Clasificar grupos de cierto tipo significa dar una familia de tales grupos en la que no haya dos isomorfos y tal que cualquier grupo del tipo considerado sea isomorfo a uno de la familia.

1. *Si G es infinito, entonces G es isomorfo al grupo $\mathbb{Z}$.*

   (Si g es un generador de G, la aplicación $\phi\colon \mathbb{Z} \to G$, $\phi(m) = g^m$, es un isomorfismo de grupos).

2. *Si G es finito y su orden es n, entonces G es isomorfo a $\mathbb{Z}/n\mathbb{Z}$.*

   (Si g es un generador de G, la aplicación $\phi\colon \mathbb{Z}/n\mathbb{Z} \to G$, $\phi([m]_n) = g^m$, es un isomorfismo de grupos).

Demostración: Sea g un generador de G, de modo que el morfismo $f_g\colon \mathbb{Z} \to G$, $f_g(m) = g^m$, es epiyectivo. Su núcleo, de acuerdo con 2.2.1, es $\operatorname{Ker} f_g = k\mathbb{Z}$ para algún número natural k. Además, por el teorema de isomorfía, tenemos un isomorfismo de grupos

$$\phi\colon \mathbb{Z}/k\mathbb{Z} \simeq G \quad , \quad \phi([m]) = g^m \ .$$

Ahora, si G es infinito, entonces $\infty = |\mathbb{Z}/k\mathbb{Z}|$, de modo que $k = 0$. Luego f_g es inyectivo, y por tanto es un isomorfismo de grupos.

Si G es finito de orden n, entonces $n = |\mathbb{Z}/k\mathbb{Z}|$, de modo que $k = n$.

Nota: Este teorema de clasificación permite dar una nueva definición del concepto de suma de números enteros, más perfecta que la dada en el capítulo anterior: *Es la única*[11] *operación que define una estructura de grupo cíclico infinito.* Recuperamos así nuestra visión infantil de la suma, cuando no nos importaba qué sumábamos sino cómo sumábamos.

Corolario 2.5.1 *Sea g un generador de un grupo cíclico finito G de orden n. La condición necesaria y suficiente para que g^m genere G es que m y n sean primos entre sí.*

Demostración: De acuerdo con el teorema anterior, basta probar que $[m]$ genera $\mathbb{Z}/n\mathbb{Z}$ si y sólo si m.c.d.$(m, n) = 1$. Ahora bien $[m]$ genera $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $[1] = a[m]$ para algún número entero a; es decir, $1 = am + bn$ para algún $b \in \mathbb{Z}$, y tal condición equivale a que m.c.d.$(m, n) = 1$ según 2.2.4.

Definición: Llamaremos **orden** de un elemento g de un grupo G al orden del subgrupo (g) que genera. El orden de un elemento puede ser infinito.

El único elemento de orden 1 es el neutro del grupo.

De acuerdo con el teorema de Lagrange, el orden de cualquier elemento de un grupo finito divide al orden del grupo.

[11] o cualquier, tanto da, pues es única salvo isomorfismos.

Proposición 2.5.2 *Sea g un elemento de un grupo G. Si g es de orden infinito, entonces $g^n = g^m \Leftrightarrow n = m$. En particular $g^n = 1 \Leftrightarrow n = 0$.*

Si g es de orden d, entonces $(g) = \{g, \ldots, g^d = 1\}$ y $g^n = g^m \Leftrightarrow n \equiv m$ (mód. d)*. En particular*

$$g^n = 1 \Leftrightarrow n \text{ es múltiplo del orden de } g$$

Demostración: El subgrupo $(g) = \{g^m : \ m \in \mathbb{Z}\}$ siempre es cíclico y está generado por g.

Corolario 2.5.3 *El orden de un elemento g de un grupo G es el primer número natural no nulo d tal que $g^d = 1$, si existe tal número natural, y en caso contrario es infinito.*

Corolario 2.5.4 *Si G es un grupo finito de orden n y $g \in G$, entonces $g^n = 1$.*

Demostración: En virtud del teorema de Lagrange, n es múltiplo del orden de (g), que es el orden de g, así que 2.5.2 permite concluir que $g^n = 1$.

2.6 El Grupo Simétrico

El **grupo simétrico** S_n es el grupo de todas las permutaciones de un conjunto X con n elementos, con la estructura de grupo que define la composición de aplicaciones. Supondremos siempre que $n \geq 2$.

Definición: Dados elementos distintos $a_1, \ldots, a_d$; $d \geq 2$, denotaremos $\sigma = (a_1 \ldots a_d)$ la permutación tal que $\sigma(a_i) = a_{i+1}$, entendiendo que $a_{d+1} = a_1$. Diremos que tal permutación $\sigma \in S_n$ es un **ciclo**, y su orden es claramente d. Los ciclos de orden 2 se llaman **trasposiciones**.

Diremos que dos ciclos $(a_1 \ldots a_d)$ y $(b_1 \ldots b_k)$ de S_n son **disjuntos** cuando $a_i \neq b_j$ para todo par de índices i, j.

Lema 2.6.1 *Si dos ciclos σ y τ son disjuntos, entonces $\sigma\tau = \tau\sigma$.*

Demostración: Si $\sigma = (a_1 \ldots a_d)$ y $\tau = (b_1 \ldots b_k)$, entonces las permutaciones $\sigma\tau$ y $\tau\sigma$ coinciden en $a_1, \ldots, a_d, b_1, \ldots, b_k$ y dejan fijos los restantes elementos.

Teorema 2.6.2 *Toda permutación $\sigma \in S_n$ distinta de la identidad descompone en producto de ciclos disjuntos. Salvo el orden de los factores, esta descomposición es única.*

Demostración: Sea a_1 un elemento tal que $\sigma(a_1) \neq a_1$ y consideremos el primer número positivo d tal que $\sigma^d(a_1) = a_1$ (tal número d existe porque el orden de σ es finito). Sea $a_i = \sigma^i(a_1)$. Los números $a_1, a_2, \ldots, a_d$ son todos distintos: si $a_i = a_j$ y $j > i$, entonces $\sigma^{j-i}(a_1) = a_1$ y $0 \leq j - i \leq d - 1$, en contra de la elección del número d. Luego $\alpha_1 = (a_1 \ldots a_d)$ es un ciclo que coincide con σ en $a_1, \ldots, a_d$; pero no en los restantes elementos, si existen, que no queden fijos por σ. Ahora, la permutación $(\alpha_1)^{-1} \cdot \sigma$ deja fijos $a_1, \ldots, a_d$ y todos los elementos que σ deje fijos. Reiterando el proceso obtenemos ciclos disjuntos $\alpha_1, \ldots, \alpha_r$ tales que $(\alpha_r)^{-1} \cdots (\alpha_1)^{-1} \cdot \sigma$ es la identidad. Luego $\sigma = \alpha_1 \cdots \alpha_r$.

Si existieran otros ciclos disjuntos $\beta_1, \ldots, \beta_s$ tales que $\beta_1 \cdots \beta_s = \sigma = \alpha_1 \cdots \alpha_r$, cambiando de orden los factores si fuera preciso podemos suponer que $\beta_1(a_1) \neq a_1$. En tal caso $\beta_1^i(a_1) = \sigma^i(a_1) = \alpha_1^i(a_1)$ para todo $i \geq 0$ y concluimos que $\beta_1 = \alpha_1$. Luego $\beta_2 \cdots \beta_s = \alpha_2 \cdots \alpha_r$ y reiterando el argumento concluimos que, después de reordenar los factores si fuera preciso, los factores $\beta_2, \ldots, \beta_s$ coinciden con los ciclos $\alpha_2, \ldots, \alpha_r$.

Corolario 2.6.3 *Todo ciclo de orden d es producto de $d-1$ trasposiciones. Por tanto, toda permutación es producto de trasposiciones.*

Demostración: $(a_1 \ldots a_d) = (a_1 a_2)(a_2 a_3) \cdots (a_{d-1} a_d)$

Definición: Sea $\sigma = \alpha_1 \cdots \alpha_r$ la descomposición de una permutación $\sigma \neq id$ en producto de ciclos disjuntos y denotemos d_i el orden de α_i, $1 \leq i \leq r$. El lema 2.6.1 nos permite suponer que $d_1 \geq d_2 \geq \cdots \geq d_r$ y diremos que $d_1, \ldots, d_r$ es la **forma** de la permutación σ.

Proposición 2.6.4 *El orden de cualquier permutación de forma $d_1, \ldots, d_r$ es el mínimo común múltiplo de $d_1, \ldots, d_r$.*

Demostración: Si $\sigma = \alpha_1 \cdots \alpha_r$ es la descomposición de σ en producto de ciclos disjuntos, entonces $\sigma^i = \alpha_1^i \cdots \alpha_r^i$. Luego $\sigma^i = 1$ si y sólo si $\alpha_1^i = \ldots = \alpha_r^i = 1$, y concluimos en virtud de 2.5.2.

Definición: Sea G un grupo. Diremos que dos elementos x, y de G son **conjugados** si existe $a \in G$ tal que $y{=}axa^{-1}$.

La relación de conjugación es una relación de equivalencia en el grupo G. Dos elementos conjugados tienen las mismas propiedades en teoría de grupos, porque $\tau_a \colon G \to G$, $\tau_a(x) = axa^{-1}$, es un automorfismo del grupo G.

Proposición 2.6.5 *Sean $\sigma, \tau \in S_n$. La condición necesaria y suficiente para que σ y τ sean conjugadas es que tengan la misma forma.*

Demostración: Sea $\sigma = (a_1 \dots a_{d_1})(b_1 \dots b_{d_2}) \cdots (c_1 \dots c_{d_r})$. Si $\gamma \in S_n$ y ponemos $i' := \gamma(i)$, tenemos que

$$\gamma\sigma\gamma^{-1} = (a'_1 \dots a'_{d_1})(b'_1 \dots b'_{d_2}) \cdots (c'_1 \dots c'_{d_r})$$

Signo de una Permutación

Consideremos el siguiente polinomio con coeficientes enteros:

$$\Delta(x_1, \dots, x_n) = \prod_{i<j}(x_j - x_i)$$

Dada $\sigma \in S_n$, los factores de $\Delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \prod_{i<j}(x_{\sigma(j)} - x_{\sigma(i)})$ coinciden, eventualmente salvo el signo, con los de $\Delta(x_1, \dots, x_n)$. Luego

$$\Delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \pm\Delta(x_1, \dots, x_n)$$

Definición: Llamaremos **signo** de una permutación $\sigma \in S_n$ al número entero $\operatorname{sgn}(\sigma)$ tal que $\Delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \operatorname{sgn}(\sigma) \cdot \Delta(x_1, \dots, x_n)$.

Por definición el signo de una permutación es 1 ó -1.

Proposición 2.6.6 *El signo de cualquier producto de permutaciones es el producto de los signos de los factores.*

El signo de cualquier trasposición es –1.

Demostración: Sean $\sigma, \tau \in S_n$. Por definición

$$\Delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \operatorname{sgn}(\sigma)\,\Delta(x_1, \dots, x_n)$$

y aplicando τ a los índices de las indeterminadas $x_1, \dots, x_n$ de éste polinomio obtenemos que

$$\begin{aligned}\Delta(x_{\tau\sigma(1)}, \dots, x_{\tau\sigma(n)}) &= \operatorname{sgn}(\sigma) \cdot \Delta(x_{\tau(1)}, \dots, x_{\tau(n)}) \\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \cdot \Delta(x_1, \dots, x_n)\end{aligned}$$

Luego $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma)$. Además, un cálculo directo demuestra que el signo de la trasposición (12) es –1. Si σ es otra trasposición, en virtud de 2.6.5 existe una permutación τ tal que $\sigma = \tau \cdot (12) \cdot \tau^{-1}$, y concluimos que

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(12)\operatorname{sgn}(\tau)^{-1} = \operatorname{sgn}(12) = -1$$

Corolario 2.6.7 *El signo de toda permutación de forma $d_1, \dots, d_r$ es*

$$(-1)^{d_1 + \dots + d_r - r}$$

Demostración: De 2.6.3 y 2.6.6 se sigue directamente que el signo de todos los ciclos de orden d es $(-1)^{d-1}$.

Corolario 2.6.8 *Sea $\sigma = \tau_1 \cdots \tau_m$ una descomposición de una permutación σ en producto de trasposiciones. Si $\operatorname{sgn}(\sigma) = 1$, entonces m es par. Si $\operatorname{sgn}(\sigma) = -1$, entonces m es impar.*

Demostración: $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_m) = (-1)^m$.

Definición: Llamaremos permutaciones **pares** a las de signo 1 e **impares** a las de signo –1.

Las permutaciones pares de S_n forman un subgrupo normal de S_n ya que son los elementos del núcleo del morfismo de grupos $\operatorname{sgn}\colon S_n \to \{\pm 1\}$. Este subgrupo se denota A_n y recibe el nombre de **subgrupo alternado**. El índice de A_n en S_n es 2 porque $S_n/A_n \simeq \{\pm 1\}$; así que el teorema de Lagrange permite concluir que el orden de A_n es $n!/2$.

Capítulo 3

Anillos

En el primer capítulo hemos desarrollado el concepto de número, introduciendo los números enteros, racionales, reales y complejos. Este *método constructivo* o *genético* tiene el inconveniente de que frente a un número entero o racional no debemos ver "una clase de equivalencia de ..." sino lo que veíamos de pequeños cuando operábamos inocentemente con ellos, como algo que *está* en un ambiente donde hay unas operaciones, una ordenación, etc., con determinadas propiedades; una estructura en suma. Es decir, lo importante es la estructura que tienen los números racionales y no el conjunto concreto que construimos para que se nos vuelva accesible. En el segundo capítulo hemos presentado el *método axiomático*, que es preferible porque pone de manifiesto la estructura y quita toda importancia a los elementos concretos de los conjuntos en cuestión. Por tanto, sería deseable desarrollar el concepto de número con el método axiomático, como una familia de objetos dotada de operaciones y relaciones sujetas a ciertas condiciones.

Cuando hablamos de números, la suma define una estructura de grupo conmutativo; pero claramente en los números siempre hay más estructura pues, dados dos números cualesquiera, además de su suma tenemos su *producto*. En los números enteros, racionales, reales y complejos disponemos de dos operaciones, usualmente llamadas suma y producto, con las siguientes propiedades: ambas verifican los axiomas de grupo conmutativo, excepto la existencia de inverso para el producto, y el producto distribuye respecto de la suma. Esta estructura recibe el nombre de *anillo conmutativo con unidad*. Vemos así que en todos los contextos en que tradicionalmente se ha hablado de números subyace una estructura de anillo conmutativo con unidad. Recíprocamente, el objetivo del presente capítulo es mostrar cómo en cualquier anillo conmutativo con unidad pueden definirse unos *números ideales* y desarrollar para ellos una teoría de la divisibilidad análoga a la de los números naturales, de modo que en todos los anillos conmutativos con unidad disponemos de una comprensión aritmética de los problemas. Si los elementos

de un anillo se extienden[1] con tales números ideales es inmediata la existencia y unicidad del máximo común divisor y del mínimo común múltiplo, al igual que la demostración de sus propiedades usuales. Además, desarrollaremos la teoría de congruencias módulo un ideal, que generaliza la teoría de congruencias de números enteros expuesta en los capítulos anteriores. Por tanto, en los anillos en que los números ideales se correspondan con los elementos del anillo (anillos que llamaremos *dominios de ideales principales*), éstos gozan de las mismas propiedades. Esta será una consecuencia crucial de este capítulo: que en los dominios de ideales principales es esencialmente válida la teoría de la divisibilidad que hemos estudiado en la Aritmética elemental. Este resultado será fundamental en el estudio de las ecuaciones algebraicas, porque en el próximo capítulo veremos que los polinomios en una indeterminada con coeficientes racionales (o reales o complejos) forman un dominio de ideales principales, resultado que nos permitirá extraer las raíces de los polinomios con coeficientes racionales mediante la teoría de congruencias módulo ideales.

3.1 Anillos y Subanillos

Axiomas de Anillo: Diremos que dos operaciones (que llamaremos suma y producto, y denotaremos $+$ y $\cdot$) en un conjunto A definen una estructura de **anillo conmutativo con unidad**[2] si verifican los siguientes axiomas:

Axioma 1. La suma define en A una estructura de grupo conmutativo.

Axioma 2. El producto es asociativo: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Axioma 3. (*Propiedad distributiva*) $a \cdot (b + c) = a \cdot b + a \cdot c$
$(b + c) \cdot a = b \cdot a + c \cdot a$

Axioma 4. Existe un elemento de A (llamado **unidad** y que denotaremos 1) tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$.

Axioma 5. El producto es conmutativo: $a \cdot b = b \cdot a$

De acuerdo con la propiedad distributiva, las aplicaciones $A \xrightarrow{a\cdot} A$ son morfismos de grupos respecto de la suma, así que en todo anillo A se verifican también las siguientes reglas de cálculo:

$$a \cdot 0 = 0 \ , \quad a \cdot (-b) = -(a \cdot b) \ , \quad (-a) \cdot (-b) = a \cdot b$$

[1] Veremos que cada elemento del anillo define un número ideal; pero, en general, puede haber ideales que no provengan de ningún elemento del anillo.

[2] Suele reservarse el nombre de anillos para las estructuras que verifican los tres primeros axiomas, añadiendo el término "con unidad" o "conmutativo" si verifican además el axioma 4 ó 5 respectivamente. Sin embargo, de ahora en adelante diremos simplemente anillo en lugar de anillo conmutativo con unidad.

Además, la unidad de un anillo es única. Diremos que $a \in A$ es **invertible** si existe algún $b \in A$ tal que $ab = 1$, en cuyo caso tal elemento b es único y se denotará b^{-1} ó $1/b$. Los elementos invertibles de un anillo A forman un grupo conmutativo respecto del producto de A, grupo que se denota A^*. Diremos que un anillo $A \neq 0$ es un **cuerpo** si todo elemento no nulo de A es invertible en A; es decir, si $A^* = A - \{0\}$.

Diremos que un elemento $a \in A$ es un **divisor de cero** si $ab = 0$ para algún elemento no nulo $b \in A$. Diremos que un anillo $A \neq 0$ es **íntegro** o que es un **dominio** si carece de divisores de cero no nulos, es decir, si tiene la propiedad de que el producto de elementos no nulos nunca es nulo. Todos los cuerpos son anillos íntegros: Si en un cuerpo $ab = 0$ y a no es nulo, entonces $0 = a^{-1}ab = b$.

En todo anillo A podemos definir la **resta** $b - a := b + (-a)$, y la **división** $a/b := ab^{-1}$, cuando el divisor b es invertible en A.

La estructura de anillo proporciona el ámbito natural de los conceptos usados en el estudio de la divisibilidad, y ésta es una de las razones de su importancia. Dados dos elementos a, b de un mismo anillo A, diremos que b es un **múltiplo** de a o que a es un **divisor** de b si existe $c \in A$ tal que $b = ca$. Diremos que un elemento de A es el **máximo común divisor** de a y b si es un divisor común que es múltiplo de cualquier otro divisor común, y diremos que es el **mínimo común múltiplo** si es un múltiplo común que divide a cualquier otro múltiplo común. Diremos que un elemento de un anillo es **propio** si no es nulo ni invertible. Por último, diremos que un elemento propio $p \in A$ es **irreducible** en A si en toda descomposición $p = ab$ algún factor es invertible; i.e., si no descompone en producto de dos elementos propios de A.

Sean u, a elementos de un anillo A. Si u es invertible en A, entonces a y ua tienen los mismos divisores y los mismos múltiplos en A. Por tanto, a es irreducible en A si y sólo si lo es ua. Por la misma razón el máximo común divisor y el mínimo común múltiplo de dos elementos $a, b \in A$ no varían al sustituir a por ua.

Definición: Diremos que un subconjunto B de un anillo A es un **subanillo** si es un subgrupo de A estable por el producto (si $a, b \in B$, entonces $ab \in B$) y contiene a la unidad de A.

Es sencillo comprobar que la intersección de subanillos de un anillo A también es un subanillo de A.

Dado un subanillo $B \subset A$ y elementos $a_1, \ldots, a_n \in A$, el menor subanillo de A que los contiene (existe porque es la intersección de todos los subanillos que los contengan) se denotará $B[a_1, \ldots, a_n]$, de modo que

$$B[a_1, \ldots, a_n] \;=\; \{ \sum_{i_1, \ldots, i_n} b_{i_1 \ldots i_n} a_1^{i_1} \ldots a_n^{i_n} : \; b_{i_1 \ldots i_n} \in B\}$$

y diremos que $B[a_1, \ldots, a_n]$ es el subanillo de A **generado** por B y $a_1, \ldots, a_n$.

3.2 Ideales

Definición: Diremos que un subconjunto $\mathfrak{a}$ de un anillo A es un **ideal** si es un subgrupo estable por el producto por elementos arbitrarios de A; es decir:

1. Respecto de la suma, $\mathfrak{a}$ es un subgrupo de A.
2. Si $a \in A$ y $b \in \mathfrak{a}$, entonces $ab \in \mathfrak{a}$.

Dados dos ideales $\mathfrak{a}, \mathfrak{b}$ de un anillo A, diremos que $\mathfrak{a}$ **divide** a $\mathfrak{b}$ cuando $\mathfrak{a} \supseteq \mathfrak{b}$.

Intersección de Ideales: Es fácil comprobar que la intersección de cualquier familia de ideales de un anillo A es también un ideal de A, y es claramente el mayor ideal de A contenido en todos los ideales de la familia dada. Es decir, el ideal $\mathfrak{a} \cap \mathfrak{b}$ divide a cualquier otro ideal de A que sea divisible por $\mathfrak{a}$ y $\mathfrak{b}$.

Suma de Ideales: La **suma** o **máximo común divisor** de dos ideales $\mathfrak{a}, \mathfrak{b}$ de un anillo A es el ideal

$$\mathfrak{a} + \mathfrak{b} = \{a + b\colon\ a \in \mathfrak{a},\ b \in \mathfrak{b}\}$$

y es el menor ideal de A que contiene a los ideales $\mathfrak{a}$ y $\mathfrak{b}$. Es decir, cualquier otro ideal que divida a $\mathfrak{a}$ y a $\mathfrak{b}$ divide también a $\mathfrak{a} + \mathfrak{b}$.

Dados elementos $a_1, \ldots, a_n \in A$, el ideal $a_1A + \ldots + a_nA$ es el menor ideal de A que los contiene y lo denotaremos también $(a_1, \ldots, a_n)$. Diremos que es el ideal de A **engendrado** por $a_1, \ldots, a_n$, ó bien que $a_1, \ldots, a_n$ **generan** tal ideal. El ideal (a) que genera un elemento $a \in A$ está formado por sus múltiplos: $(a) = aA$.

Producto de Ideales: El **producto** de dos ideales $\mathfrak{a}, \mathfrak{b}$ de un anillo A es el ideal generado por los productos de elementos de $\mathfrak{a}$ por elementos de $\mathfrak{b}$:

$$\mathfrak{ab} = \{a_1b_1 + \ldots + a_nb_n\colon\ a_1, \ldots, a_n \in \mathfrak{a},\ b_1, \ldots, b_n \in \mathfrak{b}\}$$

Es fácil comprobar que estas operaciones con ideales tienen las siguientes propiedades, que generalizan las propiedades del máximo común divisor y del mínimo común múltiplo de números enteros:

$$\begin{aligned}
(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) \quad &, \quad \mathfrak{a} + \mathfrak{a} = \mathfrak{a} \\
\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a} \quad &, \quad \mathfrak{a} + 0 = \mathfrak{a} \quad , \quad \mathfrak{a} + A = A \\
(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc}) = \mathfrak{abc} \quad &, \quad \mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} \quad , \quad \mathfrak{ab} = \mathfrak{ba} \\
(a)(b) = (ab) \quad &, \quad \mathfrak{a} \cdot 0 = 0 \quad , \quad \mathfrak{a} \cdot A = \mathfrak{a} \\
\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}) \quad &, \quad \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) \subseteq (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}) \\
\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) \subseteq (\mathfrak{ab}) \cap (\mathfrak{ac}) \quad &, \quad (\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{ac} + \mathfrak{bc} \\
(a_1, \ldots, a_n)(b_1, \ldots, b_m) \ &= (a_1b_1, \ldots, a_1b_m, \ldots, a_nb_1, \ldots, a_nb_m)
\end{aligned}$$

Definición: Diremos que un ideal $\mathfrak{m}$ de un anillo A es **maximal** cuando $\mathfrak{m} \neq A$ y el único ideal de A que contiene estrictamente a $\mathfrak{m}$ es A (es decir, los únicos ideales de A que dividen a $\mathfrak{m}$ son $A = (1)$ y $\mathfrak{m}$). Diremos que un ideal $\mathfrak{p}$ de un anillo A es **primo** cuando $\mathfrak{p} \neq A$ y se verifica que

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ ó } b \in \mathfrak{p}$$

(si un producto está en $\mathfrak{p}$, algún factor está en $\mathfrak{p}$). Por definición, si un ideal primo divide a un producto de elementos del anillo, divide a algún factor.

Ejemplo: El ideal 0 de $\mathbb{Z}$ es primo, porque si un producto de números enteros es nulo, algún factor es nulo. Si un número entero $n \neq 0$ no es primo, el ideal $n\mathbb{Z}$ no es primo. Además, si p es un número primo, el lema de Euclides afirma precisamente que el ideal $p\mathbb{Z}$ es primo; luego los ideales primos de $\mathbb{Z}$ son los ideales $p\mathbb{Z}$, donde p es primo, y el ideal 0.

Los ideales maximales de $\mathbb{Z}$ son los ideales $p\mathbb{Z}$, donde p es un número primo.

Morfismos de Anillos

Definición: Diremos que una aplicación $f\colon A \to B$ entre dos anillos es un **morfismo** de anillos cuando conserva la suma, el producto y la unidad:

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b) \\ f(1) &= 1 \end{aligned}$$

Diremos que un morfismo de anillos $f\colon A \to B$ es un **isomorfismo** de anillos si existe un morfismo de anillos $g\colon B \to A$ tal que $f \circ g$ es la identidad de B y $g \circ f$ es la identidad de A, en cuyo caso diremos que tal morfismo g (que claramente es único, pues es la aplicación inversa de f) es el **inverso** de f y lo denotaremos f^{-1}. Llamaremos **automorfismos** de un anillo A a los isomorfismos de A con A.

Sea $f\colon A \to B$ un morfismo de anillos. En particular f es un morfismo de grupos, así que $f(0) = 0$ y $f(-a) = -f(a)$. Además, si $u \in A$ es invertible en A, es fácil comprobar que $f(u)$ es invertible en B y que $f(u^{-1}) = f(u)^{-1}$. También es sencillo comprobar que la imagen de f es un subanillo de B. Si $h\colon B \to C$ es otro morfismo de anillos, la composición $h \circ f$ también es morfismo de anillos.

Proposición 3.2.1 *Sea $f\colon A \to B$ un morfismo de anillos.*

Si $\mathfrak{b}$ es un ideal de B, entonces $f^{-1}(\mathfrak{b})$ es un ideal de A. Por tanto $\operatorname{Ker} f$ *es un ideal de A.*

Si $\mathfrak{a}$ es un ideal de A y f es epiyectivo, $f(\mathfrak{a})$ es un ideal de B.

Demostración: Si $\mathfrak{b}$ es un ideal de B, por definición $\mathfrak{b}$ es un subgrupo de B, así que $f^{-1}(\mathfrak{b})$ es un subgrupo de A de acuerdo con 2.3.3. Además, si $a \in A$ y $x \in f^{-1}(\mathfrak{b})$, entonces $f(ax) = f(a)f(x) \in \mathfrak{b}$; luego $ax \in f^{-1}(\mathfrak{b})$ y concluimos que $f^{-1}(\mathfrak{b})$ es un ideal de A.

Por otra parte, si $\mathfrak{a}$ es un ideal de A, es un subgrupo de A, así que $f(\mathfrak{a})$ es un subgrupo de B de acuerdo con 2.3.3. Además, si $b \in B$ y $z \in f(\mathfrak{a})$, entonces $z = f(x)$ para algún $x \in \mathfrak{a}$ y existe $a \in A$ tal que $f(a) = b$, porque se supone que f es epiyectivo. Luego $bz = f(a)f(x) = f(ax) \in f(\mathfrak{a})$, porque $ax \in \mathfrak{a}$, y concluimos que $f(\mathfrak{a})$ es un ideal de B.

3.3 Polinomios

Sea A un anillo. El **anillo de polinomios** en una indeterminada x con coeficientes en A es el conjunto de las expresiones

$$\textstyle\sum_i a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots$$

donde los términos a_i son elementos del anillo A y son todos nulos salvo un número finito, con la estructura de anillo que definen las siguientes operaciones:

$$\big(\textstyle\sum_i a_i x^i\big) + \big(\sum_i b_i x^i\big) = \sum_i (a_i + b_i) x^i$$

$$\big(\textstyle\sum_i a_i x^i\big) \cdot \big(\sum_j b_j x^j\big) = \sum\limits_{n \geq 0} \big(\sum\limits_{i+j=n} a_i b_j \big) x^n$$

(compruébese que definen una estructura de anillo) y lo denotaremos $A[x]$.

Dado un polinomio $p(x) = \sum_i a_i x^i$, los términos $a_0, a_1, \dots \in A$ se llaman **coeficientes** del polinomio $p(x)$, y lo determinan completamente. Diremos que un polinomio es **constante** si todos sus coeficientes son nulos, salvo quizás a_0. Cada elemento $a \in A$ define un polinomio constante que también denotaremos a. Obtenemos así un morfismo de anillos canónico $A \to A[x]$.

Si un polinomio $p(x)$ no es nulo, existe un único número natural d tal que $a_d \neq 0$ y $a_r = 0$ para todo $r > d$. Tal número natural recibe el nombre de **grado** del polinomio $p(x)$ y se denotará $\operatorname{gr} p(x)$. Es fácil probar que:

$$\begin{aligned} \operatorname{gr} p(x) = 0 &\Leftrightarrow p(x) \text{ es un polinomio constante no nulo} \\ \operatorname{gr}\big(p(x) + q(x)\big) &\leq \max\big(\operatorname{gr} p(x), \operatorname{gr} q(x)\big) \\ \operatorname{gr}\big(p(x) \cdot q(x)\big) &\leq \operatorname{gr} p(x) + \operatorname{gr} q(x) \end{aligned}$$

Proposición 3.3.1 *Sea A un anillo íntegro. El producto de polinomios no nulos con coeficientes en A nunca es nulo, y su grado es la suma de los grados de los factores. Por tanto, todo múltiplo no nulo de un polinomio $p(x) \in A[x]$ tiene grado mayor o igual que el grado de $p(x)$.*

Demostración: Sean $p(x) = \sum_i a_i x^i$ y $q(x) = \sum_j b_j x^j$ dos polinomios con coeficientes en A. Si $d = \operatorname{gr} p(x)$ y $r = \operatorname{gr} q(x)$, entonces a_d y b_r no son nulos; luego $a_d b_r \neq 0$ y, como es un coeficiente de $p(x)q(x)$, se sigue que $p(x)q(x) \neq 0$ y $\operatorname{gr}\big(p(x)q(x)\big) \geq d + r$. Como siempre $\operatorname{gr}\big(p(x)q(x)\big) \leq d + r$, concluimos que $\operatorname{gr}\big(p(x)q(x)\big) = \operatorname{gr} p(x) + \operatorname{gr} q(x)$.

Definición: Sea A un anillo y n un número natural. Si $n \geq 2$, el **anillo de polinomios** $A[x_1, \ldots, x_n]$ en n indeterminadas con coeficientes en A se define inductivamente del siguiente modo:

$$A[x_1, \ldots, x_n] \ := \ (A[x_1, \ldots, x_{n-1}])[x_n]$$

En particular $A[x, y] = A[x][y]$, así que todo polinomio $p(x, y)$ en dos indeterminadas x, y con coeficientes en A descompone de modo único de la siguiente forma:

$$p(x, y) = \sum_{i \geq 0} \Big(\sum_{j \geq 0} a_{ij} x^i \Big) y^j = \sum_{i,j \geq 0} a_{ij} x^i y^j$$

donde $a_{ij} \in A$. En general, cada polinomio $p(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ descompone de modo único de la siguiente forma:

$$p(x_1, \ldots, x_n) \ = \ \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

donde los elementos $a_{i_1 \ldots i_n} \in A$ son todos nulos, salvo un número finito, y se llaman **coeficientes** del polinomio $p(x_1, \ldots, x_n)$. Si $b_1, \ldots, b_n \in A$, pondremos:

$$p(b_1, \ldots, b_n) \ = \ \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} b_1^{i_1} \cdots b_n^{i_n} \ .$$

Si un polinomio $p(x_1, \ldots, x_n)$ no es nulo, su **grado** es el número

$$\operatorname{gr} p(x_1, \ldots, x_n) = \max\{i_1 + \ldots + i_n : \ a_{i_1 \ldots i_n} \neq 0\}$$

y no debe confundirse con el grado de $p(x_1, \ldots, x_n)$ como polinomio en x_n con coeficientes en el anillo $A[x_1, \ldots, x_{n-1}]$. Diremos que un polinomio $p(x_1, \ldots, x_n)$ es **constante** si todos sus coeficientes son nulos, salvo quizás $a_{0 \ldots 0}$; es decir, los polinomios constantes no nulos son los de grado cero. Cada elemento $a \in A$ define un polinomio constante que denotaremos a, obteniendo así un morfismo de anillos canónico $A \to A[x_1, \ldots, x_n]$.

Proposición 3.3.2 *Sea A un anillo íntegro. El anillo $A[x_1, \ldots, x_n]$ también es íntegro y los elementos invertibles de $A[x_1, \ldots, x_n]$ son los polinomios constantes definidos por invertibles de A:*

$$A[x_1, \ldots, x_n]^* \ = \ A^* \ .$$

Demostración: Procedemos por inducción sobre n. Cuando $n = 1$, se sigue de 3.3.1 que el anillo $A[x]$ es íntegro. Además, si $p(x) \in A[x]$ es invertible en $A[x]$, entonces existe $q(x) \in A[x]$ tal que $p(x)q(x) = 1$; luego $\operatorname{gr}\big(p(x)q(x)\big) = 0$ y, según 3.3.1, tenemos que $\operatorname{gr} p(x) = \operatorname{gr} q(x) = 0$. Es decir, existen $b, c \in A$ tales que $p(x) = b$, $q(x) = c$, de modo que $bc = p(x)q(x) = 1$ y concluimos que b es invertible en A.

Cuando $n > 1$, por hipótesis de inducción $A[x_1, \ldots, x_{n-1}]$ es íntegro y sus elementos invertibles coinciden con A^*. Luego $A[x_1, \ldots, x_{n-1}][x_n]$ es íntegro y

$$A[x_1, \ldots, x_{n-1}][x_n]^* \;=\; A[x_1, \ldots, x_{n-1}]^* \;=\; A^* \ .$$

Teorema de División: *Sea $p(x) = a_0x^n + \ldots + a_n$ un polinomio con coeficientes en un anillo A. Si a_0 es invertible en A, entonces para cada polinomio $q(x) \in A[x]$ existe una única pareja de polinomios $c(x)$, $r(x) \in A[x]$ tales que*

$$q(x) = c(x) \cdot p(x) + r(x) \quad , \qquad \operatorname{gr} r(x) < \operatorname{gr} p(x) \ \text{ ó } \ r(x) = 0$$

Demostración: Veamos primero la *existencia* de tales polinomios $c(x)$, $r(x)$. Procedemos por inducción sobre el grado d del polinomio $q(x)$. Si $d < n$, basta tomar $c(x) = 0$ y $r(x) = q(x)$.

Si $d \geq n$, consideramos los coeficientes de $p(x)$ y $q(x)$:

$$p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$
$$q(x) = b_0x^d + b_1x^{d-1} + \ldots + b_d$$

donde a_0 y b_0 no son nulos. El grado de $\bar{q}(x) = q(x) - (b_0/a_0)x^{d-n} \cdot p(x)$ es menor que d, así que, por hipótesis de inducción, existen $\bar{c}(x)$, $r(x) \in A[x]$ tales que

$$\bar{q}(x) = \bar{c}(x) \cdot p(x) + r(x) \ , \quad \operatorname{gr} r(x) < n \text{ ó } r(x) = 0$$

Luego $q(x) = (b_0a_0^{-1}x^{d-n} + \bar{c}(x)) \cdot p(x) + r(x)$, donde $\operatorname{gr} r(x) < \operatorname{gr} p(x)$ ó $r(x) = 0$.

En cuanto a la *unicidad*, si existieran otros polinomios $\bar{c}(x), \bar{r}(x) \in A[x]$ tales que $q(x) = \bar{c}(x) \cdot p(x) + \bar{r}(x)$ y $\operatorname{gr} \bar{r}(x) < \operatorname{gr} p(x)$ ó $\bar{r}(x) = 0$, entonces

$$p(x)(\bar{c}(x) - c(x)) = r(x) - \bar{r}(x) \ .$$

Por tanto $r(x) - \bar{r}(x)$ es un múltiplo de $p(x)$ que es nulo o de grado menor que el grado de $p(x)$, así que es nulo por ser a_0 invertible, y se sigue que $r(x) = \bar{r}(x)$; luego $p(x)(\bar{c}(x) - c(x)) = 0$, de modo que $\bar{c}(x) - c(x) = 0$ y concluimos que $c(x) = \bar{c}(x)$.

Regla de Ruffini (1765-1822)**:** *Sea $p(x)$ un polinomio con coeficientes en un anillo A. Si $a \in A$, entonces el resto de la división de $p(x)$ por $x - a$ es $p(a)$. Por tanto, la condición necesaria y suficiente para que $p(x)$ sea múltiplo de $x - a$ en el anillo $A[x]$ es que $p(a) = 0$.*

Demostración: Sea $p(x) = q(x)(x - a) + r(x)$ la división de $p(x)$ por $x - a$.

Como $\operatorname{gr} r(x) < 1$ ó $r(x) = 0$, se sigue que el polinomio $r(x)$ es constante, $r(x) = r$, y concluimos que $p(a) = q(a) \cdot 0 + r = r$.

3.4 Polinomios con Coeficientes en un Cuerpo

Definición: Sea $p(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ un polinomio con coeficientes en un cuerpo k. Diremos que un elemento $a \in k$ es una **raíz** de $p(x)$ en k cuando $p(a) = c_0a^n + c_1a^{n-1} + \ldots + c_n = 0$.

Si $p(x)$ descompone en producto de dos polinomios, $p(x) = q(x)r(x)$, entonces la condición necesaria y suficiente para que $a \in k$ sea raíz de $p(x)$ es que sea raíz de $q(x)$ ó de $r(x)$, pues $p(a) = q(a)r(a)$ y k es íntegro.

Teorema 3.4.1 *Si un polinomio $c_0x^n + c_1x^{n-1} + \ldots + c_n$, $c_0 \neq 0$, con coeficientes enteros tiene la raíz $a/b \in \mathbb{Q}$, donde* m.c.d.$(a, b) = 1$*, entonces b divide a c_0 y a divide a c_n.*

En particular, si $c_0 = \pm 1$, todas sus raíces racionales son enteras.

Demostración: Si a/b es una raíz, entonces

$$c_0a^n + c_1a^{n-1}b + \ldots + c_{n-1}ab^{n-1} + c_nb^n = 0$$

de modo que $c_0a^n = -c_1a^{n-1}b - \ldots - c_nb^n$ es un múltiplo de b y a es un divisor de $c_nb^n = -c_0a^m - \ldots - c_{n-1}ab^{n-1}$. Como a y b son primos entre sí por hipótesis, en virtud de II.2.5 concluimos que c_0 es múltiplo de b y c_n es múltiplo de a.

Nota: El teorema 3.4.1 permite hallar todas las raíces racionales de cualquier polinomio con coeficientes racionales, pues podemos suponer que éste tiene coeficientes enteros y el número de divisores de un número entero siempre es finito. Por ejemplo, las posibles raíces racionales del polinomio $3x^4 + x^3 + x^2 + x - 2$ son $\pm 1, \pm 2, \pm 1/3, \pm 2/3$ y sustituyendo en el polinomio se comprueba que sus raíces racionales son -1 y $2/3$.

Teorema 3.4.2 *Sea k un cuerpo. Todo polinomio de grado 1 con coeficientes en k es irreducible en $k[x]$ y tiene una única raíz en k.*

Demostración: Sea $p(x) = ax + b$, $a \neq 0$. Si $p(x) = q(x)r(x)$ para ciertos polinomios $q(x)$, $r(x) \in k[x]$, entonces $\operatorname{gr} q(x) + \operatorname{gr} r(x) = \operatorname{gr} p(x) = 1$, así que algún factor tiene grado cero y es invertible en $k[x]$.

Por otra parte, la única raíz de $p(x)$ en k es claramente $-b/a$.

Proposición 3.4.3 *Todo polinomio irreducible de grado mayor que 1 con coeficientes en un cuerpo k carece de raíces en k.*

Demostración: Si un polinomio irreducible $p(x) \in k[x]$ admite alguna raíz $a \in k$, entonces $p(x) = q(x)(x - a)$ para algún $q(x) \in k[x]$. Como $p(x)$ es irreducible, entonces $q(x)$ ha de ser invertible, luego de grado 0 y concluimos que $\operatorname{gr} p(x) = 1$.

Corolario 3.4.4 *Sea $p(x)$ un polinomio de grado 2 ó 3 con coeficientes en un cuerpo k. La condición necesaria y suficiente para que $p(x)$ sea irreducible en $k[x]$ es que no tenga raíces en k.*

Demostración: La necesidad de la condición se sigue de 3.4.3. Recíprocamente, si $p(x)$ no es irreducible en $k[x]$, tendremos $p(x) = q_1(x)q_2(x)$ donde algún factor tiene grado 1, porque $\operatorname{gr} q_(x) + \operatorname{gr} q_2(x) = 2$ ó 3, y por tanto tiene una raíz en k.

Nota: El teorema 3.4.1 resuelve el problema de hallar las raíces racionales de los polinomios con coeficientes racionales, así que 3.4.4 permite determinar la irreducibilidad en $\mathbb{Q}[x]$ de los polinomios de grado 2 y 3. En cuanto a la irreducibilidad de los polinomios de grado 4 con coeficientes racionales, también puede decidirse usando 3.4.1. En efecto, si una cuártica $x^4+a_3x^3+a_2x^2+a_1x+a_0 \in \mathbb{Q}[x]$ carece de raíces racionales, para determinar si es irreducible basta comprobar la inexistencia de factores de grado 2:

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = (x^2 + b_1x + b_0)(x^2 + c_1x + c_0) \ .$$

Es decir, basta ver si el siguiente sistema de 4 ecuaciones algebraicas carece de soluciones racionales:

$$\begin{cases} a_3 = b_1 + c_1 \\ a_2 = b_0 + b_1c_1 + c_0 \\ a_1 = b_0c_1 + b_1c_0 \\ a_0 = b_0c_0 \end{cases}$$

De la primera ecuación y la última obtenemos que $c_1 = a_3 - b_1$ y $c_0 = a_0/b_0$. Sustituyendo en la tercera ecuación, ésta permite despejar b_1 en función de b_0. Sustituyendo estos valores en la segunda ecuación obtenemos una ecuación polinómica en la indeterminada b_0, polinomio que carece de raíces racionales precisamente cuando la cuártica dada es irreducible.

Corolario 3.4.5 *Sea k un cuerpo. Si $a_1, \ldots, a_r \in k$ son raíces distintas de un polinomio $p(x) \in k[x]$, entonces $p(x)$ es múltiplo de $(x - a_1) \cdots (x - a_r)$ en $k[x]$.*

Demostración: Procedemos por inducción sobre r, pues es la Regla de Ruffini cuando $r = 1$.

Cuando $r > 1$, de acuerdo con la Regla de Ruffini tenemos que $p(x) = q(x)(x - a_r)$ para algún $q(x) \in k[x]$. Como $a_1, \ldots, a_{r-1}$ son raíces de $p(x)$ y no son raíces de $x - a_r$, han de ser raíces de $q(x)$. Por hipótesis de inducción $q(x)$ es múltiplo de $(x-a_1) \cdots (x-a_{r-1})$ en $k[x]$, y concluimos que $p(x) = q(x)(x-a_r)$ es múltiplo de $(x - a_1) \cdots (x - a_r)$.

Teorema 3.4.6 *Si $p(x)$ es un polinomio no nulo con coeficientes en un cuerpo k, el número de raíces de $p(x)$ en k no supera al grado de $p(x)$.*

Demostración: Si $(x-a_1)\cdots(x-a_r)$ divide a $p(x)$ y $p(x)\neq 0$, entonces $r\leq \operatorname{gr} p(x)$.

Fórmula de Interpolación de Lagrange (1736-1813): *Sean $a_1,\ldots,a_n$ elementos distintos de un cuerpo k. Para cada sucesión $b_1,\ldots,b_n$ de elementos de k (no necesariamente distintos), existe un único polinomio $p(x)\in k[x]$ de grado menor que n tal que $p(a_i)=b_i$, $1\leq i\leq n$:*

$$p(x)=\sum_{j=1}^{n} b_j\frac{q_j(x)}{q_j(a_j)}\quad,\quad q_j(x)=\frac{(x-a_1)\cdots(x-a_n)}{(x-a_j)}$$

Demostración: Si $p(x)$, $q(x)\in k[x]$ son dos polinomios de grado menor que n tales que $p(a_i)=q(a_i)=b_i$ para todo $1\leq i\leq n$, entonces $a_1,\ldots,a_n$ son raíces de $p(x)-q(x)$ en k y, por el teorema anterior, concluimos que $p(x)-q(x)=0$; es decir, $p(x)=q(x)$. Por último, con las notaciones del enunciado, es claro que $q_i(a_j)=0$ cuando $i\neq j$; luego:

$$\sum_j b_j\frac{q_j(a_i)}{q_j(a_j)}=b_i\frac{q_i(a_i)}{q_i(a_i)}=b_i$$

Raíces Complejas

Lema 3.4.7 *Sea $p(x)=c_0x^n+c_1x^{n-1}+\ldots+c_{n-1}x+c_n$ un polinomio con coeficientes complejos. Si c es el máximo de los módulos de c_1, $c_2,\ldots,c_n$, entonces para todo número complejo z de módulo $\rho>1$ se verifica que*

$$\rho^n\left(|c_0|-\frac{c}{\rho-1}\right)\leq |p(z)|$$

Demostración: $|p(z)|\geq |c_0z^n|-|c_1z^{n-1}+\ldots+c_n|$
$\geq |c_0|\rho^n-c(\rho^{n-1}+\ldots+1)=|c_0|\rho^n-c(\rho^n-1)/(\rho-1)$
$\geq |c_0|\rho^n-c\rho^n/(\rho-1)=\rho^n\big(|c_0|-c/(\rho-1)\big)$.

Corolario 3.4.8 *Con las notaciones del lema anterior, el módulo de cualquier raíz compleja de $p(x)$ está acotado por $1+\big(c/|c_0|\big)$.*

Definición: Diremos que un cuerpo k es **algebraicamente cerrado** cuando todo polinomio no constante con coeficientes en k tenga alguna raíz en k.

Teorema de D'Alembert (1717-1783)**:** *El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.*

Demostración: Sea $p(x)$ un polinomio no constante con coeficientes en $\mathbb{C}$ y sea r un número real positivo. El disco $D_r=\{z\in\mathbb{C}\colon |z|\leq r\}$ es un conjunto cerrado y

acotado de $\mathbb{C}$; luego es compacto y la función continua $f\colon D_r \to \mathbb{R}$, $f(z) = |p(z)|$, alcanza un mínimo en algún punto $a \in D_r$.

De acuerdo con 3.4.7, podemos elegir r de modo que $|p(z)| > |p(0)|$ para todo número complejo z de módulo r, de modo que el mínimo de f no se alcanza en ningún punto de módulo r, por lo que tal mínimo a tiene que ser un punto interior de D_r. Vamos a probar que $p(a) = 0$. Si $|p(a)| > 0$, consideramos la primera potencia de x que tenga coeficiente no nulo en el polinomio $p(a + x)$:

$$p(a + x) = p(a) + c_d x^d + c_{d+1} x^{d+1} + \ldots + c_n x^n \ , \qquad c_d \neq 0$$

Como $c_d \neq 0$, podemos fijar el argumento de $z \in \mathbb{C}$ de modo que el módulo de $p(a) + c_d z^d$ sea $|p(a)| - |c_d z^d|$. Luego

$$|p(a + z)| \leq |p(a)| - |c_d z^d| + |c_{d+1} z^{d+1} + \ldots + c_n z^n|$$

es menor que $|p(a)|$ cuando

$$|c_{d+1} z^{d+1} + \ldots + c_n z^n| \leq c(n - d)|z|^{d+1}$$

sea menor que $|c_d \cdot z^d|$, donde $c = \max\{|c_i|\}$; lo que nos lleva a contradicción, pues claramente podemos elegir z de modo que $a + z$ esté en el disco D_r, tenga el argumento prefijado y $c(n - d)|z|^{d+1} \leq |c_d| \cdot |z|^d = |c_d z^d|$.

Corolario 3.4.9 *Los polinomios irreducibles en $\mathbb{C}[x]$ son los de grado 1.*

Demostración: Sea $p(x)$ un polinomio irreducible con coeficientes complejos. Por el teorema de D'Alembert $p(x)$ tiene alguna raíz compleja α, así que 3.4.3 nos permite concluir que el grado de $p(x)$ es 1.

Corolario 3.4.10 *Los polinomio irreducible en $\mathbb{R}[x]$ son los de grado 1 y los de grado 2 sin raíces reales.*

Demostración: Sea $p(x)$ un polinomio irreducible en $\mathbb{R}[x]$ de grado mayor que 1 y consideremos $p(x)$ como polinomio con coeficientes complejos. Existe algún número complejo $a + bi$ que es raíz de $p(x)$; luego

$$0 = \overline{p(a + bi)} = p(a - bi)$$

y también $a - bi$ es raíz de $p(x)$. Al ser $b \neq 0$, de 3.4.5 se sigue que

$$\big(x - (a + bi)\big)\big(x - (a - bi)\big) = x^2 - 2ax + (a^2 + b^2)$$

divide a $p(x)$ en $\mathbb{C}[x]$; luego también en $\mathbb{R}[x]$, pues ambos polinomios tienen coeficientes reales. Como $p(x)$ es irreducible en $\mathbb{R}[x]$, su grado ha de ser 2.

3.5 Anillo Cociente

Sea $\mathfrak{a}$ un ideal de un anillo A. Respecto de la suma $\mathfrak{a}$ es un subgrupo de A, así que $\mathfrak{a}$ define una relación de equivalencia en A ($a \equiv b \Leftrightarrow b-a \in \mathfrak{a}$) y el correspondiente conjunto cociente se denotará $A/\mathfrak{a}$. La clase de equivalencia de cualquier elemento $a \in A$ respecto de $\equiv$ es

$$a + \mathfrak{a} = \{a + x\colon \ x \in \mathfrak{a}\}$$

y diremos que es la **clase de restos** de a módulo $\mathfrak{a}$. Tal clase de equivalencia se denotará $\bar{a}$ o $[a]$ cuando no origine confusión.

Teorema 3.5.1 *Sea $\mathfrak{a}$ un ideal de un anillo A. Existe una única estructura de anillo en $A/\mathfrak{a}$ tal que la proyección canónica $\pi\colon A \to A/\mathfrak{a}$ es morfismo de anillos. Además $\mathfrak{a} = \operatorname{Ker}\pi$.*

Demostración: Ya sabemos que la operación $[a] + [b] = [a + b]$ define en $A/\mathfrak{a}$ una estructura de grupo conmutativo y que $\mathfrak{a} = \operatorname{Ker}\pi$. Si $u, v \in A/\mathfrak{a}$, definimos $u \cdot v = [ab]$ donde $[a] = u$, $[b] = v$:

$$[a] \cdot [b] = [ab]$$

Veamos que $u \cdot v$ no depende de los representantes a, b elegidos. Si $[a] = [a']$, entonces existen $c \in \mathfrak{a}$ tales que $a' = a+c$; luego $a'b = ab+cb \in ab+\mathfrak{a}$ y concluimos que $[a'b] = [ab]$.

Es inmediato comprobar que esta operación define en el grupo conmutativo $A/\mathfrak{a}$ una estructura de anillo conmutativo con unidad, que es $[1]$. Además, es claro que con esta estructura de anillo la proyección canónica π es morfismo de anillos.

Para concluir demostraremos la unicidad. Si $\oplus$ y $\odot$ son otras dos operaciones en $A/\mathfrak{a}$ que también definen una estructura de anillo tal que π sea morfismo de anillos, para todo $x, y \in A/\mathfrak{a}$ existen $a, b \in A$ tales que $x = \pi(a)$, $y = \pi(b)$; luego

$$\begin{gathered} x + y = \pi(a) + \pi(b) = \pi(a + b) = \pi(a) \oplus \pi(b) = x \oplus y \\ x \cdot y = \pi(a) \cdot \pi(b) = \pi(ab) = \pi(a) \odot \pi(b) = x \odot y \end{gathered}$$

Ejemplo: Si n es un número natural, $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$, así que en $\mathbb{Z}/n\mathbb{Z}$ tenemos una estructura de anillo, definida por las operaciones:

$$[a]_n + [b]_n = [a + b]_n \qquad , \qquad [a]_n \cdot [b]_n = [ab]_n$$

y la condición necesaria y suficiente para que $[m]_n$ sea invertible en $\mathbb{Z}/n\mathbb{Z}$ es que $mb \equiv 1$ (mód. n) para algún $b \in \mathbb{Z}$; es decir, que m sea primo con n. En tal caso, el inverso de $[m]_n$ en $\mathbb{Z}/n\mathbb{Z}$ puede calcularse con la Identidad de Bézout $1 = \alpha m+\beta n$, pues $1 = [\alpha]_n \cdot [m]_n$, y el inverso de $[m]_n$ en $\mathbb{Z}/n\mathbb{Z}$ es $[\alpha]_n$.

Por tanto, la condición necesaria y suficiente para que el anillo $\mathbb{Z}/n\mathbb{Z}$ sea un cuerpo es que el número n sea primo. Tenemos así para cada número primo p un cuerpo finito con p elementos $\mathbb{Z}/p\mathbb{Z}$, que denotaremos $\mathbb{F}_p$.

Estos anillos $\mathbb{Z}/n\mathbb{Z}$ se usan sistemáticamente en el estudios de las congruencias. Por ejemplo, dos números enteros a, b son solución de cierta congruencia

$$\sum_{i,j\geq 0} a_{ij}x^i y^j \equiv 0 \text{ (mód. } n)$$

precisamente cuando sus clases de restos $\bar{a}, \bar{b}$ son solución de la ecuación

$$\sum_{i,j\geq 0} \bar{a}_{ij}x^i y^j = 0$$

(es decir, $\sum_{ij} \bar{a}_{ij}\bar{a}^i\bar{b}^j = 0$) porque la proyección canónica $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(x) = \bar{x}$, es morfismo de anillos. En particular, si $x = a$, $y = b$ es una solución entera de una ecuación diofántica $\sum_{i,j\geq 0} a_{ij}x^i y^j = 0$, entonces sus clases de restos $\bar{a}, \bar{b}$ son solución de la correspondiente **ecuación reducida** $\sum_{i,j\geq 0} \bar{a}_{ij}x^i y^j = 0$ módulo n, cualquiera que sea el número natural n. Por tanto, si hallamos todas las soluciones en $\mathbb{Z}/n\mathbb{Z}$ de la ecuación reducida, éstas determinan las posibles clases de restos módulo n de las soluciones enteras de la ecuación dada. En particular, si la ecuación reducida carece de soluciones en $\mathbb{Z}/n\mathbb{Z}$, entonces la ecuación diofántica considerada carece de soluciones enteras.

Propiedad Universal: *Sea $\mathfrak{a}$ un ideal de un anillo A y $\pi\colon A \to A/\mathfrak{a}$ la proyección canónica. Si $f\colon A \to B$ es un morfismo de anillos y $\mathfrak{a} \subseteq \operatorname{Ker} f$, entonces existe un único morfismo de anillos $\phi\colon A/\mathfrak{a} \to B$ tal que $f = \phi \circ \pi$:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \searrow & & \nearrow \phi \\ & A/\mathfrak{a} & \end{array}$$

Demostración: Todo anillo A es un grupo (para la suma), todo ideal $\mathfrak{a}$ de A es un subgrupo normal de A y todo morfismo de anillos $f\colon A \to B$ es un morfismo de grupos. En virtud de la propiedad universal del grupo cociente $A/\mathfrak{a}$, si $\mathfrak{a} \subseteq \operatorname{Ker} f$, entonces existe un único morfismo de grupos $\phi\colon A/\mathfrak{a} \to B$ tal que $f = \phi \circ \pi$. Para concluir bastará probar que ϕ es de hecho un morfismo de anillos:

$$\phi([a]\cdot[b]) = \phi([ab]) = f(ab) = f(a)f(b) = \phi([a])\phi([b])$$
$$\phi(1) = \phi(\pi(1)) = f(1) = 1$$

Teorema de Isomorfía: *Si $f\colon A \to B$ es un morfismo de anillos, la aplicación $\phi\colon A/\operatorname{Ker} f \to \operatorname{Im} f$, $\phi([a]) = f(a)$, es isomorfismo de anillos:*

$$\boxed{A/\operatorname{Ker} f \;\simeq\; \operatorname{Im} f}$$

Demostración: Ya sabemos que ϕ es un isomorfismo de grupos, y la demostración del teorema anterior muestra que ϕ es morfismo de anillos; luego es isomorfismo de anillos.

Corolario 3.5.2 *Si $f\colon A \to B$ es un morfismo de anillos epiyectivo, entonces el anillo $A/\mathrm{Ker}\, f$ es isomorfo al anillo B.*

Teorema Chino del Resto: *Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de un anillo A. Si $\mathfrak{a}+\mathfrak{b}=A$, entonces $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{ab}$, y tenemos un isomorfismo de anillos*

$$\phi\colon A/\mathfrak{a}\cap\mathfrak{b} \longrightarrow (A/\mathfrak{a})\times(A/\mathfrak{b}) \quad ; \quad \phi([x]_{\mathfrak{ab}}) = ([x]_{\mathfrak{a}}, [x]_{\mathfrak{b}})$$

Demostración: Por hipótesis existen $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ tales que $1 = a + b$. Ahora, si $c \in \mathfrak{a}\cap\mathfrak{b}$, tenemos que $c = c(a+b) = ca + cb \in \mathfrak{ab}$; así que $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{ab}$, pues la inclusión contraria siempre es válida.

Además, el morfismo de anillos $f\colon A \to (A/\mathfrak{a})\times(A/\mathfrak{b})$, $f(x) = ([x]_{\mathfrak{a}}, [x]_{\mathfrak{b}})$, es epiyectivo, porque $([c]_{\mathfrak{a}}, [d]_{\mathfrak{b}})$ proviene de $x := bc + ad$:

$$\begin{aligned} c = (a+b)c \equiv bc \equiv bc + ad \qquad & (\text{módulo } \mathfrak{a}) \\ d = (a+b)d \equiv ad \equiv bc + ad \qquad & (\text{módulo } \mathfrak{b}) \end{aligned}$$

Como el núcleo de f es $\mathfrak{a}\cap\mathfrak{b}$, el corolario anterior nos permite concluir.

Teorema 3.5.3 *Sea $\mathfrak{a}$ un ideal de un anillo A.*

$$\begin{aligned} \mathfrak{a} \text{ es un ideal primo de } A &\Leftrightarrow \text{el anillo } A/\mathfrak{a} \text{ es íntegro} \\ \mathfrak{a} \text{ es un ideal maximal de } A &\Leftrightarrow \text{el anillo } A/\mathfrak{a} \text{ es un cuerpo} \end{aligned}$$

Demostración: Si el ideal $\mathfrak{a}$ es primo, $A/\mathfrak{a} \neq 0$ porque $\mathfrak{a} \neq A$. Además, si $[a]\cdot[b] = 0$ y $[b] \neq 0$, entonces $ab \in \mathfrak{a}$ y b no está en $\mathfrak{a}$; luego $a \in \mathfrak{a}$ y $[a] = 0$. Recíprocamente, si $A/\mathfrak{a}$ es íntegro, $\mathfrak{a} \neq A$ porque $A/\mathfrak{a} \neq 0$. Además, $ab \in \mathfrak{a} \Rightarrow [a]\cdot[b] = [ab] = 0 \Rightarrow [a] = 0$ ó $[b] = 0 \Rightarrow a \in \mathfrak{a}$ ó $b \in \mathfrak{a}$.

Si el ideal $\mathfrak{a}$ es maximal, $A/\mathfrak{a} \neq 0$ porque $\mathfrak{a} \neq A$. Además, si $[a] \neq 0$, el ideal $\mathfrak{a} + aA$ contiene estrictamente a $\mathfrak{a}$; luego $A = \mathfrak{a} + aA$ y existen $x \in \mathfrak{a}$, $b \in A$ tales que $1 = x + ab$. Se sigue que $[a]\cdot[b] = 1$ y obtenemos que $[a]$ es invertible en $A/\mathfrak{a}$.

Recíprocamente, si $A/\mathfrak{a}$ es un cuerpo, $\mathfrak{a} \neq A$ porque $A/\mathfrak{a} \neq 0$. Además, si $\mathfrak{b}$ es un ideal de A que contiene estrictamente a $\mathfrak{a}$, existe algún $b \in \mathfrak{b}$ que no está en $\mathfrak{a}$; luego $[b] \neq 0$ en $A/\mathfrak{a}$ y existe algún $[a] \in A/\mathfrak{a}$ tal que $[a][b] = 1$. Luego $(1-ab) \in \mathfrak{a}$ y $1 = (1-ab) + ab \in \mathfrak{b}$, de modo que $\mathfrak{b} = A$. q.e.d.

Como todo cuerpo es íntegro, el teorema anterior implica el siguiente resultado, generalización del clásico lema de Euclides (325?-265? a. de Cristo) sobre números primos a los anillos arbitrarios:

Teorema 3.5.4 *Todo ideal maximal es primo.*

Corolario 3.5.5 *Si $a_1, \ldots, a_n$ son elementos de un cuerpo k, entonces*

$$\mathfrak{m} := \{p \in k[x_1, \ldots, x_n] \colon p(a_1, \ldots, a_n) = 0\}$$

es un ideal maximal del anillo $k[x_1, \ldots, x_n]$. Además $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ y el morfismo natural $k \to k[x_1, \ldots, x_n]/\mathfrak{m}$ es un isomorfismo de anillos.

Demostración: El morfismo de anillos natural $k \to k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)$, $a \mapsto [a]$, es inyectivo porque si $a \in (x_1 - a_1, \ldots, x_n - a_n)$, $a = p_1(x - a_1) + \ldots + p_n(x - a_n)$, la sustitución $x_i = a_i$ muestra que $a = 0$; y es epiyectivo porque $[x_i] = [a_i]$ está en la imagen, y ésta es un subanillo. Luego $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal maximal de $k[x_1, \ldots, x_n]$ de acuerdo con 3.5.3.

Como $\mathfrak{m}$ es un ideal que contiene a $(x_1 - a_1, \ldots, x_n - a_n)$, y claramente $\mathfrak{m} \neq k[x_1, \ldots, x_n]$, concluimos que $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$.

Sistemas de Ecuaciones Algebraicas: Cuando planteamos un sistema de ecuaciones polinómicas, digamos con coeficientes racionales, como pueda ser

$$\left.\begin{aligned} -2x^3 + x^3y^2 &= y^4 \\ x^3 - y^2 &= 1 \end{aligned}\right\}$$

y a continuación obtenemos algunas consecuencias

$$y^2 = x^3 - 1 \ , \ (x^3 - 1)^2 = -2x^3 + x^3(x^3 - 1) \ , \ x^3 = -1 \ , \ 2 = -y^2$$

todas estas igualdades son obviamente falsas en el anillo de polinomios $\mathbb{Q}[x, y]$; pero son ciertas en el anillo cociente

$$\mathbb{Q}[x, y]/(-2x^3 + x^3y^2 - y^4, x^3 - y^2 - 1)$$

por el ideal $\mathfrak{a}$ generado por las ecuaciones del sistema considerado, porque la proyección canónica $\pi \colon \mathbb{Q}[x, y] \to \mathbb{Q}[x, y]/\mathfrak{a}$ es morfismo de anillos. Las consecuencias del sistema son las relaciones que se dan en este anillo cociente y, cuando expresan la anulación de un elemento, vienen dadas por los polinomios del ideal $\mathfrak{a}$, porque $\mathfrak{a} = \operatorname{Ker} \pi$. Por ejemplo, los polinomios $x^3 + 1$, $y^2 + 2$ están en el ideal $\mathfrak{a}$: descomponen en suma de un múltiplo de $-2x^3 + x^3y^2 - y^4$ y un múltiplo de $x^3 - y^2 - 1$.

Dos sistemas de ecuaciones deben considerarse equivalentes cuando las ecuaciones de cada sistema sean consecuencias de las del otro sistema. De aquí la importancia crucial de la teoría de ideales en el estudio de los sistemas de ecuaciones algebraicas, pues permite definir con rigor el concepto de sistemas equivalentes: Diremos que dos sistemas de ecuaciones polinómicas en n indeterminadas

$$\left.\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ \cdots\cdots\cdots & \\ p_r(x_1, \ldots, x_n) &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} q_1(x_1, \ldots, x_n) &= 0 \\ \cdots\cdots\cdots & \\ q_s(x_1, \ldots, x_n) &= 0 \end{aligned}\right\}$$

con coeficientes en un anillo A son **equivalentes** si sus ecuaciones generan el mismo ideal $(p_1, \ldots, p_r) = (q_1, \ldots, q_s)$ en el anillo $A[x_1, \ldots, x_n]$. Es decir, cuando

$$p_i(x_1, \ldots, x_n) = \sum_{j=1}^{s} a_{ij}(x_1, \ldots, x_n) q_j(x_1, \ldots, x_n)$$

$$q_j(x_1, \ldots, x_n) = \sum_{i=1}^{r} b_{ji}(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n)$$

para ciertos polinomios $a_{ij}(x_1, \ldots, x_n)$, $b_{ji}(x_1, \ldots, x_n)$ con coeficientes en A. En particular, si dos sistemas son equivalentes, tienen las mismas soluciones en A y en cualquier otro anillo B del que A sea subanillo.

3.6 Congruencia de Euler

Sea n un número natural mayor o igual que 2. Los elementos invertibles del anillo $\mathbb{Z}/n\mathbb{Z}$, que son las clases de restos módulo n de los números primos con n, forman un grupo con el producto de $\mathbb{Z}/n\mathbb{Z}$. Este grupo es conmutativo y su orden es el indicador de Euler $\phi(n)$:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[m]_n : \text{ m.c.d.}(m, n) = 1\}$$

Propiedades del Indicador de Euler (1707-1783)**:**

$$\phi(p^r) = (p-1)p^{r-1} \qquad \text{si } p \text{ es un número primo y } r \geq 1$$
$$\phi(n \cdot m) = \phi(n) \cdot \phi(m) \qquad \text{si } n \text{ y } m \text{ son primos entre sí}$$

Demostración: La primera igualdad se debe a que los números primos con p^r son justamente los que no son múltiplos de p. Luego $p, 2p, \ldots, p^{r-1}p$ son los únicos números entre 1 y p^r que no son primos con p^r.

En cuanto a la segunda igualdad, según el Teorema chino del resto tenemos un isomorfismo de anillos $\mathbb{Z}/nm\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, que induce un isomorfismo de grupos

$$(\mathbb{Z}/nm\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Congruencia de Euler: *Si a y n son números enteros primos entre sí, entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Demostración: Si a es primo con n, entonces $[a]_n$ está en $(\mathbb{Z}/n\mathbb{Z})^*$, que es un grupo finito de orden $\phi(n)$, así que 2.5.4 permite concluir que

$$[1]_n = [a]_n^{\phi(n)} = [a^{\phi(n)}]_n$$

Ejemplo: Si a y n son números enteros primos entre sí, las soluciones enteras de la congruencia $ax \equiv b$ (mód. n) son: $x = a^{\phi(n)-1}b + tn, \quad t \in \mathbb{Z}$.

Congruencia de Fermat (1601-1665)**:** *Sea p un número primo. Si un número entero a no es múltiplo de p, entonces*

$$a^{p-1} \equiv 1 \text{ (mód. } p)$$

Demostración: Si a no es múltiplo de p, entonces m.c.d.$(a, p) = 1$, porque p es primo. Además $\phi(p) = p - 1$ cuando p es primo.

Corolario 3.6.1 *Si p es primo, entonces $a^p \equiv a$* (mód. p) *para todo $a \in \mathbb{Z}$.*

Corolario 3.6.2 *Sea p un número primo impar. Los restos cuadráticos no nulos módulo p forman un subgrupo de $\mathbb{F}_p^*$ de orden $\frac{p-1}{2}$, y son las soluciones de la congruencia*

$$x^{\frac{p-1}{2}} \equiv 1 \quad \text{(módulo } p)$$

Demostración: La aplicación $f\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$, $f(x) = x^2$, es un morfismo de grupos. Su núcleo, que son las raíces del polinomio $x^2 - 1 = (x+1)(x-1)$, es el subgrupo $\{\pm 1\}$, porque $\mathbb{F}_p$ es un cuerpo y $-1 \neq 1$ al ser $p \neq 2$. El teorema de isomorfía permite concluir que la imagen de f, que está formada por los restos cuadráticos no nulos, tiene orden $\frac{p-1}{2}$.

Por otra parte, si $a \in \mathbb{F}_p^*$ es un resto cuadrático, $a = b^2$, entonces $a^{\frac{p-1}{2}} = b^p = 1$ de acuerdo con la congruencia de Fermat. Como el polinomio $x^{\frac{p-1}{2}} - 1$ no puede tener más raíces que el grado, concluimos que todas sus raíces en $\mathbb{F}_p$ son los restos cuadráticos no nulos módulo p.

Corolario 3.6.3 *Sea p un número primo impar. La condición necesaria y suficiente para que -1 sea resto cuadrático módulo p es que $p \equiv 1$* (módulo 4).

Capítulo 4

Anillos Euclídeos

Sabemos determinar todas las raíces racionales de cualquier polinomio con coeficientes racionales; pero puede ocurrir que un polinomio no tenga ninguna raíz racional. En tal caso nuestro propósito es hallar sus raíces en algún cuerpo mayor que $\mathbb{Q}$, de modo análogo al conocido cálculo de las raíces de los polinomios $ax^2 + bx + c$ de grado 2:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

La consideración atenta de esta fórmula muestra que, para los polinomios $x^2 - 2$ y $x^2 + 1$, sólo afirma que $\sqrt{2}$ y $\sqrt{-1}$ son raíces, donde $\sqrt{2}$ y $\sqrt{-1}$ se han definido precisamente por el hecho de que sus cuadrados sean 2 y -1 respectivamente, lo que parece una tautología. En modo alguno consideramos que no sabemos "resolver" la ecuación $x^2 = 2$, a pesar de que para cualquier otro polinomio también podríamos decir una obviedad análoga sin que por ello podamos considerar resuelta la ecuación. Esta perplejidad se debe a que de nuevo estamos ignorando una estructura que pasa desapercibida. En efecto, la fórmula de las soluciones de las ecuaciones cuadráticas sería una tautología inútil si no fuera precedida por el aprendizaje del cálculo con radicales, que nos permite sumarlos, restarlos, multiplicarlos y dividirlos entre sí y con números racionales.

Vemos pues que tal fórmula incluye dos pasos bien diferenciados. El primero, fundamental e implícito, es desentrañar una estructura de cuerpo: la aritmética de radicales. El segundo, bien explícito, es ya la expresión de las raíces mediante radicales y las cuatro operaciones elementales. No es de extrañar que, al permanecer implícito en gran parte el primer paso, históricamente la cuestión de extraer las raíces de los polinomios de grado superior se plantease como el problema de su expresión mediante radicales; pero sin cuestionarse siquiera la conveniencia de la estructura donde limitamos su búsqueda. Ahora bien, esta restricción es artificial y sólo puede explicarse por nuestro manejo desde temprana edad del cálculo

aproximado de radicales, hecho que es externo a la cuestión considerada; pues el problema que pretendemos abordar es el de la expresión exacta de las raíces de los polinomios, y no el de su cálculo aproximado (lo que, por otra parte, es posible realizar para cualquier polinomio con coeficientes racionales con métodos de Cálculo Numérico, sin necesidad de hallar previamente el valor exacto de las raíces). Cierto es que la conocida fórmula de las raíces de los polinomios de grado 2 proporciona tanto una expresión exacta de las raíces como un método para efectuar su cálculo aproximado; pero en el caso de polinomios de grado arbitrario será necesario separar nítidamente ambas cuestiones. La limitación de la búsqueda de las raíces de los polinomios a su expresión por radicales es un ejemplo claro de encerrona intelectual debida a nuestra gran familiaridad con una estructura particular, que nos impide considerar la posibilidad de estructuras alternativas mejor adaptadas al problema en cuestión[1]. La pregunta por las raíces de los polinomios requiere una pregunta previa sobre la estructura en que se han de explicitar éstas, y es un ejemplo claro de lo que afirma Heidegger (1889-1976) en *Ser y Tiempo*:

> "El verdadero progreso de la investigación no consiste tanto en recoger los resultados y recluirlos en tratados, cuanto en ese preguntar por las estructuras fundamentales del dominio del caso, que surge, las más de las veces como una reacción, de semejante acumulación de nociones sobre las cosas."

Para que tenga sentido hablar de las raíces de un polinomio con coeficientes en un cuerpo, éstas deben estar en una extensión del cuerpo de coeficientes (es decir, en un cuerpo que lo contenga como subanillo). Por tanto, el problema general de extraer una raíz de cualquier polinomio $p(x)$ con coeficientes en un cuerpo k incluye dos cuestiones. La primera y más sutil es la construcción de un cuerpo K que extienda al cuerpo de coeficientes k. La segunda es la determinación de un elemento α de K tal que $p(\alpha) = 0$. Puestos ya de manifiesto el verdadero problema y la encerrona mental que nos dificultaba su solución, la respuesta hallada por Kronecker (1823-1891) es maravillosamente sencilla, precisa y general. Por ejemplo, si $q(x)$ es un polinomio con coeficientes racionales y $p(x)$ es un factor irreducible de $q(x)$, veremos que el anillo cociente $\mathbb{Q}[x]/\big(p(x)\big)$ es un cuerpo que contiene a $\mathbb{Q}$, y es obvio que $\alpha = [x]$ es una raíz de $p(x)$, ya que $p(\alpha) = [p(x)] = 0$. Así este teorema de Kronecker pondrá en evidencia que el problema de la extracción de raíces de polinomios con coeficientes en un cuerpo k se reduce esencialmente al problema de descomposición en factores irreducibles de polinomios con coeficientes en k y en extensiones finitas de k, problema al que dedicaremos el próximo capítulo.

[1] Algo similar ocurrió con la Geometría. Durante siglos fue impensable la posibilidad de una estructura geométrica diferente de la geometría euclídea clásica, hasta que a principios del siglo XIX se descubrió la existencia de geometrías no euclídeas y, rompiendo un férreo círculo invisible que nos encerraba, Gauss (1777-1855) planteó la cuestión de la determinación de la estructura geométrica del Universo, abordada por la teoría de la relatividad de Einstein (1879-1955).

4.1 Anillos Euclídeos

Dado un anillo A, cada elemento $a \in A$ define un ideal de A: el ideal aA. Si dos elementos $a, b \in A$ difieren en un invertible de A (es decir, si existe $u \in A^*$ tal que $b = ua$), entonces $aA = bA$. En general, de la igualdad $aA = bA$ no se sigue que a y b difieran en un invertible de A; sin embargo, cuando el anillo A es íntegro, la igualdad $aA = bA$ implica que $b = ua$, $a = vb$ para ciertos $u, v \in A$; luego $b = uvb$ y $b(1 - uv) = 0$, de modo que $uv = 1$ ó $b = 0$. En ambos casos concluimos que $b = ua$ para algún $u \in A$ invertible. *En los anillos íntegros, cada elemento a está determinado, salvo invertibles, por el ideal aA que genera.*

Definición: Diremos que un anillo A es **euclídeo** si es íntegro y existe una aplicación $\delta : A - \{0\} \to \mathbb{N}$ tal que:

1. $\delta(a) \leq \delta(ab)$ para todo par de elementos no nulos $a, b \in$A.
2. Si $a \in A$ no es nulo, para cada $b \in A$ existen[2] $c, r \in A$ tales que

$$b = ac + r \quad , \quad \delta(r) < \delta(a) \text{ ó } r = 0$$

Ejemplos:

1. El anillo de los números enteros $\mathbb{Z}$ es euclídeo, pues basta tomar $\delta(n) = |n|$ y aplicar el teorema de división de números enteros.
2. El anillo $k[x]$ de los polinomios con coeficientes en un cuerpo k es euclídeo, pues nos basta tomar $\delta(p(x)) = \text{gr}\big(p(x)\big)$ y aplicar el teorema de división de polinomios.
3. El anillo de los enteros de Gauss $A = \mathbb{Z}[\,i\,]$ es euclídeo. Para probarlo definimos $\delta(z) = N(z) = z \cdot \bar{z} = |z|^2 = a^2 + b^2$, donde $z = a + bi$. La primera condición es inmediata. En cuanto a la segunda, conviene observar que para cada número complejo $u + vi$ existe algún entero de Gauss $a + bi$ tal que $|(u + vi) - (a + bi)| < 1$, pues podemos elegir dos números enteros a, b tales que $|u - a| \leq 1/2$ y $|v - b| \leq 1/2$. Por tanto, si z es un elemento no nulo de A, para cada $x \in A$ podemos elegir un entero de Gauss c tal que $|(x/z) - c| < 1$. Luego $r = x - cz \in A$ y $|r| = |z(x/z - r)| < |z|$.

Teorema 4.1.1 *Si $\mathfrak{a}$ es un ideal de un anillo euclídeo A, existe algún $a \in A$ tal que $\mathfrak{a} = aA$.*

Demostración: Si $\mathfrak{a} = 0$, basta tomar $a = 0$.

Si $\mathfrak{a} \neq 0$, entre todos los elementos no nulos de $\mathfrak{a}$ existirá alguno a tal que $\delta(a)$ sea mínimo. Entonces $aA \subseteq \mathfrak{a}$ porque $a \in \mathfrak{a}$. Por otra parte, si $b \in \mathfrak{a}$, existen

[2] Nótese que no se exige la unicidad del cociente y el resto.

$c, r \in A$ tales que $b = ac + r$ y $\delta(r) < \delta(a)$ ó $r = 0$. Luego $r = b - ac \in \mathfrak{a}$ y $r = 0$ según la definición de a, de modo que $b = ac \in aA$. Concluimos que $\mathfrak{a} = aA$.

Definición: Sea $p(x) = c_0x^n + \ldots + c_n$ un polinomio de grado n con coeficientes en un cuerpo k. Diremos que $p(x)$ es **unitario** si $c_0 = 1$. Como los elementos invertibles de $k[x]$ son los polinomios de grado cero, para cada polinomio no nulo $p(x) \in k[x]$ existe un único invertible u tal que $up(x)$ es unitario. Además, los múltiplos de $p(x)$ en $k[x]$ coinciden con los múltiplos de $up(x)$.

Corolario 4.1.2 *Sea k un cuerpo y sea $\mathfrak{a}$ un ideal no nulo de $k[x]$. Si $p(x)$ es el polinomio unitario de menor grado que está en $\mathfrak{a}$, entonces $\mathfrak{a}$ está formado por todos los múltiplos de $p(x)$.*

Divisibilidad en los Anillos Euclídeos

Sea A un anillo euclídeo. Las mismas demostraciones que dimos en el caso de la Aritmética elemental (II.2) prueban la existencia (y unicidad salvo invertibles de A) del máximo común divisor de dos elementos cualesquiera $a, b \in A$, pues es el generador del ideal $aA + bA$, y de su mínimo común múltiplo, que es el generador del ideal $aA \cap bA$. En estos anillos es válida la Identidad de Bézout: Si d=m.c.d.(a, b), entonces $dA = aA + bA$ y existen $\alpha, \beta \in A$ tales que $d = \alpha a + \beta b$. En los anillos euclídeos, el algoritmo de Euclides sigue proporcionando un método para calcular el máximo común divisor y los coeficientes de la Identidad de Bézout.

Lema de Euclides: *Sea p un elemento no nulo de un anillo euclídeo A. Las siguientes condiciones son equivalentes:*

1. *p es irreducible en A.*
2. *pA es un ideal maximal de A.*
3. *pA es un ideal primo de A.*

Demostración: $(1 \Rightarrow 2)$ Si p es irreducible en A, entonces $pA \neq A$ porque p no es invertible en A. Si $\mathfrak{b}$ es un ideal de A que contiene a pA, existe $b \in A$ tal que $\mathfrak{b} = bA$. Luego $p = bc$ para algún $c \in A$ y, al ser p irreducible, concluimos que b o c es invertible en A. Si lo es b, entonces $\mathfrak{b} = bA = A$. Si lo es c, tenemos que $\mathfrak{b} = bA = bcA = pA$.

$(2 \Rightarrow 3)$ Todo ideal maximal es primo según afirma 3.5.4.

$(3 \Rightarrow 1)$ Si pA es un ideal primo de A, entonces p no es invertible en A porque $pA \neq A$. Si $p = ab$ es una factorización de p en A, entonces $ab \in pA$ y se sigue que $a \in pA$ o $b \in pA$. Si $a \in pA$, existe $c \in A$ tal que $a = pc$ y $p = ab = pcb$; luego $bc = 1$ y b es invertible en A. Análogamente, si $b \in pA$, entonces a es invertible en A. Concluimos que p es irreducible en A.

Corolario 4.1.3 *Sea $p(x)$ un polinomio con coeficientes en un cuerpo k. La condición necesaria y suficiente para que el anillo cociente $k[x]/(p(x))$ sea un cuerpo es que $p(x)$ sea irreducible en $k[x]$.*

Teorema de Descomposición: *Todo elemento no nulo ni invertible de un anillo euclídeo A descompone, y de modo único salvo el orden y factores invertibles, en producto de elementos irreducibles de A. (Si $b \in A$ no es nulo ni invertible, existen elementos irreducibles $p_1, \ldots, p_r \in A$ tales que $b = p_1 \cdots p_r$. Si $b = q_1 \cdots q_s$ es otra descomposición en producto de irreducibles, entonces $r = s$ y, reordenando los factores si es preciso, $q_i = u_i p_i$ para ciertos elementos invertibles $u_1, \ldots, u_r \in A$).*

Demostración: Probaremos primero la existencia de tal descomposición. Si b no es irreducible, existe en A alguna descomposición $b = ac$ donde ambos factores no son invertibles. Veamos que $\delta(a)$ y $\delta(c)$ son menores que $\delta(b)$. Si $\delta(a) = \delta(b)$, se tiene $a = bd + r$ donde $r = 0$ ó $\delta(r) < \delta(b) = \delta(a)$. Como $r = a - bd = a(1 - cd)$, se tiene $\delta(r) \geq \delta(a)$ cuando $1 - cd \neq 0$; luego $1 = cd$ contra la hipótesis de que c no es invertible en A. Procediendo por inducción sobre $\delta(b)$ podemos suponer que ambos factores a, c descomponen en producto de elementos irreducibles, así que b también descompone en producto de elementos irreducibles en A.

Veamos la unicidad. Si $b = p_1 \cdots p_r$ es una descomposición en producto de irreducibles, para cada elemento irreducible p se verifica que el número de veces que se repite, salvo invertibles, el factor p en la descomposición es el mayor exponente n tal que p^n divide a b. En efecto, si p^n divide a b, por el lema de Euclides p divide a algún factor p_i; luego p coincide con p_i salvo un factor invertible y p^{n-1} divide a $p_1 \ldots \widehat{p_i} \ldots p_r$. Reiterando el argumento, vemos que hay n factores que coinciden con p.

Corolario 4.1.4 *Si $b = p_1 \cdots p_r$, entonces $p_1, \ldots, p_r$ son, salvo factores invertibles de A, los únicos divisores irreducibles de b en A.*

Corolario 4.1.5 *Si $p(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_n$ es un polinomio de grado $n \geq 1$ con coeficientes en un cuerpo k, entonces*

$$p(x) = c_0 \cdot p_1(x)^{n_1} \cdots p_r(x)^{n_r}$$

donde $p_1(x), \ldots, p_r(x) \in k[x]$ son polinomios unitarios irreducibles distintos. Esta descomposición es única salvo el orden.

Demostración: De acuerdo con el teorema anterior existen en $k[x]$ polinomios irreducibles $q_1(x), \ldots, q_s(x)$ tales que $p(x) = q_1(x) \cdots q_s(x)$. Ahora bien, $q_i(x) = a_i p_i(x)$ donde $p_i(x)$ es unitario y $a_i \in k$, así que

$$p(x) = a p_1(x) \cdots p_s(x)$$

donde $a \in k$ y $p_1(x), \ldots, p_s(x)$ son polinomios unitarios irreducibles. Igualando los coeficientes de grado n concluimos que $a = c_0$.

Definición: Se dice que un ideal $\mathfrak{a}$ de un anillo A es **principal** cuando $\mathfrak{a} = aA$ para algún $a \in A$. Diremos que un anillo es un **dominio de ideales principales** si es íntegro y todos sus ideales son principales.

El teorema 4.1.1 afirma precisamente que todos los anillos euclídeos son dominios de ideales principales. El Lema de Euclides (325?-265? a. de Cristo) y el teorema de descomposición en factores irreducibles son válidos en cualquier dominio de ideales principales A; aunque la demostración de la existencia de la descomposición en factores irreducibles ha de modificarse convenientemente (ver apéndice D).

4.2 Extensiones y Raíces

Definición: Sea k un cuerpo. Llamaremos **álgebra** sobre k a todo anillo A dotado de un morfismo de anillos $j\colon k \to A$. Este morfismo estructural j induce en A una estructura de k-espacio vectorial: $\lambda \cdot a := j(\lambda)a$, $\lambda \in k$, $a \in A$. Por eso no distinguiremos cada elemento de k de su imagen en A por j. Es decir, si $\lambda \in k$, entonces $j(\lambda) \in A$ se denotará también λ siempre que no cause confusión.

Dadas dos k-álgebras $j\colon k \to A$ y $j'\colon k \to B$, diremos que una aplicación $f\colon A \to B$ es **morfismo** de k-álgebras si es morfismo de anillos y $f(\lambda) = \lambda$ para todo $\lambda \in k$ (o sea, $j' = f \circ j$). Es decir, si f es morfismo de anillos y es una aplicación k-lineal. Diremos que un morfismo de k-álgebras es un **isomorfismo** si admite un morfismo de k-álgebras inverso.

Es sencillo comprobar que las composiciones de morfismos de k-álgebras también lo son, y que los isomorfismos de k-álgebras son los morfismos biyectivos.

Además, el morfismo estructural $j\colon k \to A$ es inyectivo cuando $A \neq 0$. En efecto, su núcleo es un ideal de k y los únicos ideales de un cuerpo k son 0 y k, de modo que $\operatorname{Ker} j = 0$, ya que $j(1) = 1 \neq 0$.

Definición: Sea k un cuerpo. Diremos que una k-álgebra $j\colon k \to L$ es una **extensión** de k cuando L sea un cuerpo. Diremos que una extensión L es **finita** si lo es la dimensión de L como k-espacio vectorial, en cuyo caso tal dimensión recibe el nombre de **grado** de L sobre k y se denota $[L : k]$.

Diremos que una extensión es **trivial** si su grado es 1; i.e., si el morfismo estructural $k \to L$ es un isomorfismo.

Sea L una extensión de un cuerpo k y $\alpha_1, \ldots, \alpha_n \in L$. Entonces

$$k(\alpha_1, \ldots, \alpha_n) = \{a/b\colon\ a, b \in k[\alpha_1, \ldots, \alpha_n],\ b \neq 0\}$$

es el menor subanillo de L que es cuerpo y contiene a k y a $\alpha_1, \ldots, \alpha_n$. Como contiene a k y es un cuerpo, $k(\alpha_1, \ldots \alpha_n)$ es una extensión de k, y diremos que es la extensión de k **generada** por $\alpha_1, \ldots, \alpha_n$. Está formada por todos los elementos de L que pueden obtenerse a partir de $\alpha_1, \ldots, \alpha_n$ y de elementos de k con un número finito de sumas, restas, productos y divisiones por elementos no nulos.

Definición: Sea $p(x) = c_0x^n + \ldots + c_n$ un polinomio con coeficientes en un cuerpo k. Diremos que un elemento α de una extensión L de k es una **raíz** de $p(x)$ en L si $p(\alpha) = c_0\alpha^n + \ldots + c_n = 0$. En tal caso, la regla de Ruffini afirma que $p(x)$ es múltiplo de $x - \alpha$ en $L[x]$ y, si $p(x)$ no es nulo, llamaremos **multiplicidad** de la raíz α al mayor número natural m tal que $(x - \alpha)^m$ divida a $p(x)$ en $L[x]$.

Las raíces de multiplicidad 1 reciben el nombre de raíces **simples**. Las raíces que no sean simples se denominan **múltiples**.

Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k y sea L una extensión de k. Consideremos la descomposición de $p(x)$ en producto de polinomios irreducibles en $L[x]$:

$$p(x) = c(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} \cdot q_1(x)^{n_1} \cdots q_s(x)^{n_s}$$

donde $x - \alpha_1, \ldots, x - \alpha_r, q_1(x), \ldots, q_s(x)$ son polinomios unitarios irreducibles en $L[x]$ distintos entre sí, y los factores $q_i(x)$ no son de grado 1 (eventualmente r o s puede ser nulo). Las raíces de $p(x)$ en L son precisamente $\alpha_1, \ldots, \alpha_r$ y sus multiplicidades respectivas son $m_1, \ldots m_r$. Tomando grados concluimos que

$$m_1 + \ldots + m_r \leq \operatorname{gr} p(x)$$

y diremos que $p(x)$ tiene **todas sus raíces** en L cuando se dé la igualdad, lo que equivale a que $s = 0$; es decir, a que en la descomposición de $p(x)$ en $L[x]$ no existan factores irreducibles de grado mayor que 1. Resumiendo:

Teorema 4.2.1 *Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k. La suma de las multiplicidades de las raíces de $p(x)$ en cualquier extensión L de k no supera al grado de $p(x)$ y la condición necesaria y suficiente para que coincida con el grado de $p(x)$ es que $p(x)$ descomponga en $L[x]$ en producto de polinomios de grado 1.*

Corolario 4.2.2 *Sea L una extensión de un cuerpo k y sea $p(x) = c_0x^n + \ldots + c_n$ un polinomio de grado $n \geq 1$ con coeficientes en k que tenga todas sus raíces en L. Si $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$ en L, cada una repetida tantas veces como indique su multiplicidad, entonces*

$$p(x) = c_0(x - \alpha_1) \cdots (x - \alpha_n)$$

Corolario 4.2.3 *Sea $p(x) = c_0x^n + \ldots + c_n$ un polinomio con coeficientes complejos de grado $n \geq 1$. Si $\alpha_1, \ldots, \alpha_n$ son las raíces complejas de $p(x)$, cada una repetida tantas veces como indique su multiplicidad, entonces*

$$p(x) = c_0(x - \alpha_1) \cdots (x - \alpha_n)$$

Demostración: Sólo hay que probar que $p(x)$ tiene todas sus raíces complejas. Ahora bien, todo polinomio irreducible en $\mathbb{C}[x]$ es de grado 1, así que todo polinomio con coeficientes complejos no constante descompone en producto de polinomios de grado 1 con coeficientes complejos.

Fórmulas de Cardano

Las fórmulas de Cardano (1501-1576) expresan los coeficientes de cada polinomio $p(x)$ en función de sus raíces. Son muy útiles porque permiten obtener muchas funciones de las raíces de un polinomio en función únicamente de los coeficientes, lo que permite calcularlas sin necesidad de extraer previamente las raíces. Sea $p(x) = c_0x^n + \ldots + c_n$ un polinomio de grado $n \geq 1$ con coeficientes en un cuerpo k. Si $p(x)$ tiene todas sus raíces en k y $\alpha_1, \ldots, \alpha_n$ son sus raíces, cada una repetida tantas veces como indique su multiplicidad, por 4.2.2 tenemos

$$c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n = c_0(x - \alpha_1) \cdots (x - \alpha_n) \ .$$

Igualando coeficientes obtenemos las Fórmulas de Cardano:

$$\boxed{(-1)^r c_r/c_0 = \sum_{i_1 < \cdots < i_r} \alpha_{i_1} \cdots \alpha_{i_r}} \qquad 1 \leq r \leq n$$

4.3 Raíces Múltiples

Definición: Sea $p(x) = \sum_i a_i x^i$ un polinomio con coeficientes en un cuerpo k. Llamaremos **derivada** de $p(x)$ al siguiente polinomio con coeficientes en k (donde $ia_i := a_i + \overset{i}{\ldots} + a_i$ denota la suma i veces de a_i en k):

$$p'(x) = \sum_{i \geq 1} i a_i x^{i-1}$$

Es fácil comprobar que la derivada es una aplicación k-lineal:

$$\begin{aligned} (p(x) + q(x))' &= p'(x) + q'(x) \\ (a \cdot p(x))' &= a \cdot p'(x) \ , \quad a \in k \end{aligned}$$

Teorema 4.3.1 $(p(x) \cdot q(x))' = p'(x) \cdot q(x) + p(x) \cdot q'(x)$.

Demostración: Cuando $p(x) = x^i$ y $q(x) = x^j$ la igualdad se comprueba directamente. En el caso general $p(x) = \sum_i a_i x^i$, $q(x) = \sum_j b_j x^j$ tenemos:

$$(pq)' = \sum_{ij} a_i b_j (x^i x^j)' = \sum_{ij} i a_i b_j x^{i-1} x^j + \sum_{ij} j a_i b_j x^i x^{j-1} =$$
$$= \big(\sum_i i a_i x^{i-1}\big)\big(\sum_j b_j x^j\big) + \big(\sum_i a_i x^i\big)\big(\sum_j j b_j x^{j-1}\big) = p' \cdot q + p \cdot q'$$

Teorema 4.3.2 *Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k. La condición necesaria y suficiente para que una raíz de $p(x)$ sea múltiple es que sea raíz de la derivada $p'(x)$.*

Demostración: Sea α una raíz de $p(x)$ en alguna extensión K de k y sea m su multiplicidad, de modo que en $K[x]$ tenemos

$$p(x) = (x-\alpha)^m q(x) \ , \quad q(\alpha) \neq 0$$

Si $m = 1$, entonces

$$p'(x) = q(x) + (x-\alpha)q'(x) \ , \quad p'(\alpha) = q(\alpha) \neq 0$$

de modo que α no es raíz de $p'(x)$. Si $m \geq 2$, entonces

$$p'(x) = m(x-\alpha)^{m-1} + (x-\alpha)^m q'(x) \ , \quad p'(\alpha) = 0$$

y α es raíz de $p'(x)$.

Corolario 4.3.3 *Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k. Las raíces múltiples de $p(x)$ son las raíces del máximo común divisor de $p(x)$ y su derivada $p'(x)$.*

Demostración: Sea $d(x) = \text{m.c.d.}(p(x), p'(x))$. Si α es una raíz de $d(x)$ en una extensión de k, entonces α es raíz de $p(x)$ y de $p'(x)$ porque ambos polinomios son múltiplos de $d(x)$, así que el teorema anterior permite concluir que α es una raíz múltiple de $p(x)$.

Recíprocamente, si α es una raíz múltiple de $p(x)$, el teorema anterior afirma que también es raíz de $p'(x)$. Concluimos que α es raíz de $d(x)$ porque, según la Identidad de Bézout, existen $a(x)$, $b(x) \in k[x]$ tales que

$$d(x) = a(x)p(x) + b(x)p'(x)$$

Corolario 4.3.4 *Sea $p(x)$ un polinomio con coeficientes en un cuerpo k. Si $p(x)$ es irreducible en $k[x]$, entonces todas las raíces de $p(x)$ son simples o su derivada $p'(x)$ es nula.*

Demostración: Salvo constantes no nulas, los únicos divisores de $p(x)$ en $k[x]$ son 1 y $p(x)$, así que el máximo común divisor de $p(x)$ y $p'(x)$ es 1 ó $p(x)$. Si es 1, en virtud del corolario anterior $p(x)$ no tiene raíces múltiples. Si es $p(x)$, como divide a $p'(x)$ y el grado de $p'(x)$ no puede ser mayor o igual que el grado de $p(x)$, concluimos que $p'(x) = 0$.

Característica de un Anillo

Si $\operatorname{gr} p(x) \geq 1$, por definición de la derivada es evidente que $\operatorname{gr} p'(x) \leq \operatorname{gr} p(x) - 1$; pero el grado de $p'(x)$ puede ser menor que $\operatorname{gr} p(x) - 1$ e incluso puede ocurrir que $p'(x) = 0$. Esto se debe a que un coeficiente ia_i puede ser nulo aunque a_i no lo sea, porque en k la suma iterada i veces de la unidad $i \cdot 1 := 1+ \overset{i}{\ldots} +1$ puede ser nula, suma iterada que denotaremos i cuando no origine confusión con el número natural i. Por ejemplo, si $k = \mathbb{F}_p$, la derivada del polinomio $x^p + 1$ es nula, al igual que la de cualquier polinomio $p(x) = \sum_i a_i x^{pi}$, pues tenemos que $p = 0$ en el cuerpo finito $\mathbb{F}_p$.

Definición: Si A es un anillo, es claro que existe un único morfismo[3] de anillos $\mathbb{Z} \to A$, que transforma cada número natural n en $1+ \overset{n}{\ldots} +1$ y $-n$ en su opuesto. Su núcleo es un ideal de $\mathbb{Z}$; luego es $d\mathbb{Z}$ para cierto número natural d, que recibe el nombre de **característica** de A.

Por definición, la característica de A es nula cuando $n = 1+ \overset{n}{\ldots} +1 \neq 0$ en A para todo número natural no nulo n. Por el contrario, la característica de A es positiva cuando existe algún número natural positivo n tal que $1+ \overset{n}{\ldots} +1 = 0$ en A y, en tal caso, la característica de A es el menor de tales números.

Ejemplos:

1. Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica nula.

2. Si $n \in \mathbb{N}$, la característica del anillo $\mathbb{Z}/n\mathbb{Z}$ es n.

3. Si B es un subanillo de un anillo A, la característica de A coincide con la de B. En particular, la característica de cualquier extensión de un cuerpo k coincide con la de k.

4. Sea b un elemento no nulo de un cuerpo k y $m \in \mathbb{Z}$. Entonces mb es nulo si y sólo si $m = 0$ en k, lo que equivale a que m sea múltiplo de la característica de k. Por tanto, si la característica de k es nula, $\operatorname{gr} p'(x) = \operatorname{gr} p(x) - 1$ para todo polinomio no constante $p(x) \in k[x]$ y, en particular, la derivada $p'(x)$ no es nula.

   Si la característica de k es positiva, la igualdad $\operatorname{gr} p'(x) = \operatorname{gr} p(x) - 1$ sólo es válida cuando el grado de $p(x)$ no sea múltiplo de la característica de k.

[3] Esta propiedad universal caracteriza el anillo $\mathbb{Z}$ salvo isomorfismos, pues si otro anillo B la tuviera también, existirían morfismos $\mathbb{Z} \to B$ y $B \to \mathbb{Z}$, que serían mutuamente inversos en virtud de la unicidad. Obtenemos así una definición, nueva y más profunda, de la suma y el producto de números enteros: Son las únicas operaciones que definen una estructura de anillo con tal propiedad universal.

5. Sea $ax^2 + bx + c = 0$ una ecuación cuadrática con coeficientes en un cuerpo k. La fórmula usual
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$
para sus raíces sólo es válida cuando $\operatorname{car} k \neq 2$, pues exige dividir por $2a$.

Característica Nula

Teorema 4.3.5 *Sea $p(x)$ un polinomio con coeficientes en un cuerpo k de característica nula. Si $p(x)$ es irreducible en $k[x]$, entonces todas las raíces de $p(x)$ son simples.*

Demostración: El grado de $p'(x)$ es $\operatorname{gr} p(x) - 1$ porque la característica de k es nula, así que $p'(x) \neq 0$ y 4.3.4 permite concluir que todas las raíces de $p(x)$ son simples.

Teorema 4.3.6 *Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k de característica nula. Toda raíz múltiple de $p(x)$ de multiplicidad m es una raíz de multiplicidad $m - 1$ de $p'(x)$.*

Demostración: Sea α un elemento de una extensión K de k. Si α es una raíz de multiplicidad m de $p(x)$, en $K[x]$ tendremos $p(x) = (x-\alpha)^m q(x)$, donde $q(\alpha) \neq 0$. Por tanto
$$p'(x) = (x - \alpha)^{m-1}(mq(x) + (x - \alpha)q'(x))$$
y $mq(\alpha)+(\alpha-\alpha)q'(\alpha) = mq(\alpha) \neq 0$, porque $m \neq 0$ en todo cuerpo de característica nula. Luego α es una raíz de $p'(x)$ de multiplicidad $m - 1$.

Regla de Descartes (1596-1650): *Sea $p(x) = a_0 + a_1x + \ldots + a_nx^n$ un polinomio no constante con coeficientes reales. El número $r_+(p(x))$ de raíces reales positivas de $p(x)$, cada una contada tantas veces como indique su multiplicidad, no supera al número de variaciones*[4] *de signo que haya en la sucesión de coeficientes de $p(x)$:*
$$r_+\big(p(x)\big) \leq V(a_0, a_1, \ldots, a_n)$$
y se da la igualdad cuando $p(x)$ tiene todas sus raíces reales.

Demostración: Procederemos por inducción sobre el grado de $p(x)$, pues la regla es evidente para los polinomios de grado 1.

Cuando $p(x)$ tiene grado mayor que 1, cambiando de signo $p(x)$ si fuera preciso y quitándole la raíz nula si la tuviera, podemos suponer que a_0 es positivo. Las

[4] $V(c_0, c_1, \ldots, c_n)$ denotará el número de variaciones de signo entre términos consecutivos de la sucesión $c_0, c_1, \ldots, c_n$; después de eliminar los términos nulos. Así, por ejemplo, $V(1, 0, -1, -2, 1) = V(1, -1, -2, 1) = 2$.

raíces reales positivas $\alpha_1 < \alpha_2 < \ldots < \alpha_r$ de $p(x)$ tendrán ciertas multiplicidades $m_1, m_2, \ldots, m_r$. Si $m_i \geq 2$, entonces α_i es una raíz de $p'(x)$ de multiplicidad $m_i - 1$, según 4.3.6. Además, en virtud del teorema de Rolle, entre cada par de raíces consecutivas α_i, α_{i+1} la derivada $p'(x)$ tiene alguna raíz real más. Se sigue que

$$r_+\big(p'(x)\big) \geq r - 1 + \sum_{i=1}^{r}(m_i - 1) = \Big(\sum_{i=1}^{r} m_i\Big) - 1$$

Por hipótesis de inducción, tenemos que

$$\Big(\sum_{i=1}^{r} m_i\Big) - 1 \leq V(a_1, 2a_2, \ldots, na_n) = V(a_1, \ldots, a_n) = V(a_j, a_{j+1}, \ldots, a_n)$$

donde a_j es el primer término no nulo de la sucesión $a_1, a_2, \ldots, a_n$.

Si a_j es negativo, entonces $V(a_0, a_1, \ldots, a_n) = V(a_j, \ldots, a_n) + 1$ y $\sum_i m_i$ está acotado por $V(a_0, \ldots, a_n)$.

Si a_j es positivo, entonces $p(0) = a_0 > 0$ y la primera derivada no nula de $p(x)$ en 0 es positiva, así que $p(x)$ es creciente a la derecha del 0. Luego el máximo de $p(x)$ entre 0 y α_1 se alcanza en algún punto intermedio, que será una raíz más de $p'(x)$. En este caso $r_+(p')$ es al menos $\sum_i m_i$ y, por hipótesis de inducción, concluimos que

$$\textstyle\sum_i m_i \leq V(a_1, 2a_2, \ldots, na_n) = V(a_j, \ldots, a_n) = V(a_0, a_1, \ldots, a_n)$$

Por último, sea $r_-\big(p(x)\big)$ el número de raíces reales negativas de $p(x)$, cada una contada tantas veces como indique su multiplicidad, que coincide con $r_+\big(p(-x)\big)$. Cuando $p(x)$ tiene todas sus raíces reales, tenemos que $r_+\big(p(x)\big) + r_-\big(p(x)\big) = n$, porque $p(x)$ no tiene la raíz nula al ser $a_0 > 0$. Si $r_+\big(p(x)\big)$ fuera menor que $V(a_0, a_1, \ldots, a_n)$, obtendríamos la siguiente contradicción, :

$$\begin{aligned} n &= r_+\big(p(x)\big) + r_-\big(p(x)\big) = r_+\big(p(x)\big) + r_+\big(p(-x)\big) < \\ &< V(a_0, a_1, \ldots, a_n) + V(a_0, -a_1, a_2, \ldots, (-1)^n a_n) \leq n \end{aligned}$$

Característica Positiva

Teorema 4.3.7 *La característica de todo anillo íntegro es nula o es un número primo.*

Demostración: Sea A un anillo íntegro de característica positiva d. Si d no fuera un número primo, entonces $d = nm$ donde n y m son números naturales menores que d. Luego $0 = d = nm$ en A y, por ser A íntegro, se sigue que $n = 0$ ó $m = 0$ en A, en contra de que d es el menor número positivo tal que $d = 0$ en A. Concluimos que d es un número primo.

Corolario 4.3.8 *El número de elementos de cualquier cuerpo finito k es una potencia de su característica $p = \operatorname{car} k$, que es un número primo.*

Demostración: El morfismo natural $\mathbb{Z} \to k$ no puede ser inyectivo porque el cuerpo k es finito, así que su característica p es un número primo por 4.3.7. Luego k es una extensión finita de $\mathbb{F}_p$ y se concluye al observar que el número de elementos de un $\mathbb{F}_p$-espacio vectorial de dimensión d es precisamente p^d, como puede verse fácilmente sin más que considerar una base.

Lema 4.3.9 *Si la característica de un anillo A es un número primo p, para todo $a, b \in A$ se verifica que:*

$$(a+b)^p = a^p + b^p$$

Demostración: Sea i un número natural entre 1 y $p-1$. Como $i!$ no es múltiplo de p y $p(p-1)\cdots(p-i+1)$ es múltiplo de p, del Lema de Euclides se sigue que

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$$

es múltiplo de p y, por tanto, es nulo en A. Luego

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

Nota: El lema anterior permite dar una demostración directa de la congruencia de Fermat: $a^p = (1+\ldots+1)^p = 1^p + \ldots + 1^p = a$, para todo $a \in \mathbb{F}_p$.

Teorema 4.3.10 *Sea p un número primo y sea $q(x)$ un polinomio con coeficientes en $\mathbb{F}_p$. Si $q(x)$ es irreducible en $\mathbb{F}_p[x]$, entonces todas sus raíces son simples.*

Demostración: Supongamos que $q(x) = \sum_i a_i x^i$ tiene alguna raíz múltiple. Según 4.3.4, tenemos que $0 = q'(x) = \sum_i i a_i x^{i-1}$. Luego $ia = 0$ en $\mathbb{F}_p$ y se sigue que $a_i = 0$ cuando i no es múltiplo de p. Es decir

$$q(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \ldots = \sum_{j \geq 0} a_{jp} x^{jp}$$

Como la congruencia de Fermat (1601-1665) afirma que $a^p = a$ para todo $a \in \mathbb{F}_p$, tenemos que

$$q(x) = \sum_{j \geq 0} a_{jp} x^{jp} = \sum_{j \geq 0} a_{jp}^p x^{jp} = \Big(\sum_{j \geq 0} a_{jp} x^j \Big)^p$$

y $q(x)$ no es irreducible en $\mathbb{F}_p[x]$, lo que nos lleva a contradicción.

Ejemplo: Sea $k = \mathbb{F}_2(t)$ el cuerpo de las fracciones racionales en una indeterminada con coeficientes en $\mathbb{F}_2$. El polinomio $p(x) = x^2 - t$ es irreducible en $k[x]$, porque es de grado 2 y no tiene raíces en k (pruébese). No obstante, todas sus raíces son múltiples, porque $p'(x) = 0$. De hecho, si α es una raíz de $p(x)$, entonces $\alpha^2 = t$ y $x^2 - t = (x-\alpha)^2$.

4.4 Teorema de Kronecker

Lema 4.4.1 *Sea $p(x)$ un polinomio de grado d con coeficientes en un cuerpo k. El cociente $k[x]/\big(p(x)\big)$ es un k-espacio vectorial de dimensión d y una base es*

$$\{\,[\,1\,]\,,\,[\,x\,]\,,\,\ldots\,,\,[\,x\,]^{d-1}\,\}$$

Demostración: Sea V el subespacio vectorial de $k[x]$ generado por los monomios $1, x, .., x^{d-1}$, de modo que $(1, x, \ldots, x^{d-1})$ es una base de V. La aplicación

$$\pi\colon V \to k[x]/\big(p(x)\big),\ \pi\big(q(x)\big) = [q(x)]$$

es k-lineal, es inyectiva, porque V no contiene múltiplos no nulos de $p(x)$, y es epiyectiva, porque en $k[x]/\big(p(x)\big)$ cada polinomio coincide con el resto de su división por $p(x)$ y el grado del resto es menor que d. Por tanto, la dimensión de $k[x]/\big(p(x)\big)$ coincide con la de V, que es d, y una base de $k[x]/\big(p(x)\big)$ es $\{\pi(1), \pi(x), \ldots, \pi(x^{d-1})\}$.

Teorema de Kronecker: *Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo k. Una raíz de $p(x)$ es $\bar{x} \in k[x]/\big(p(x)\big)$. Además, si α es otra raíz de $p(x)$ en una extensión de k, entonces existe un isomorfismo de k-álgebras*

$$k[x]/\big(p(x)\big) \simeq k(\alpha) \quad , \quad [q(x)] \mapsto q(\alpha)$$

que transforma $\bar{x}$ en α. Por tanto, si β es otra raíz de $p(x)$ en otra extensión de k, existe un isomorfismo de k-álgebras $k(\alpha) \simeq k(\beta)$ que transforma α en β.

Demostración: Como $p(x)$ es irreducible, sus múltiplos forman un ideal maximal $(p(x))$ de $k[x]$ en virtud del lema de Euclides; luego el anillo cociente $k[x]/\big(q(x)\big)$ es un cuerpo y, por tanto, es una extensión de k. Vamos a probar que $\bar{x}$ es una raíz de $p(x)$.

Si $a \in k$ y $[r(x)] \in k[x]/\big(p(x)\big)$, por definición $a[r(x)] = [ar(x)]$; luego, si $p(x) = \sum_i a_i x^i$, tenemos que

$$p(\bar{x}) = \textstyle\sum_i a_i [\,x\,]^i = \sum_i a_i [x^i\,] = \sum_i [a_i x^i\,] = \Big[\sum_i a_i x^i\Big] = [p(x)] = 0\ .$$

Ahora, si α es otra raíz de $p(x)$, el morfismo de k-álgebras $k[x] \to k[\alpha]$, $q(x) \mapsto q(\alpha)$, es epiyectivo y su núcleo contiene por hipótesis al ideal $\big(p(x)\big)$, que es maximal según el lema de Euclides. Luego su núcleo es $\big(p(x)\big)$ y el teorema de Isomorfía afirma la existencia de un isomorfismo de k-álgebras $k[x]/\big(p(x)\big) \to k[\alpha]$, $[q(x)] \mapsto q(\alpha)$.

Luego $k[\alpha]$ es cuerpo, porque $k[x]/\big(p(x)\big)$ lo es, y concluimos que $k[\alpha] = k(\alpha)$.

Por último, si β es otra raíz, entonces $k(\alpha) \simeq k[x]/\big(p(x)\big) \simeq k(\beta)$.

Corolario 4.4.2 *Sea $p(x)$ un polinomio irreducible de grado d con coeficientes en un cuerpo k. Si α es una raíz de $p(x)$ en una extensión de k, entonces $p(x)$ divide a todos los polinomios con coeficientes en k que admitan la raíz α, y $k(\alpha)$ es una extensión finita de k de grado d:*

$$k(\alpha) = k \oplus k\alpha \oplus k\alpha^2 \oplus \ldots \oplus k\alpha^{d-1}$$

Teorema 4.4.3 *Todo polinomio no constante con coeficientes en un cuerpo k tiene todas sus raíces en alguna extensión finita de k.*

Demostración: Procedemos por inducción sobre el grado del polinomio $p(x) \in k[x]$. Si $p(x)$ es de grado 1, ya tiene todas sus raíces en k.

Si el grado de $p(x)$ es mayor que 1, considerando un factor irreducible de $p(x)$ en $k[x]$, vemos que el teorema de Kronecker afirma que $p(x)$ tiene una raíz α en alguna extensión finita K de k. Según la regla de Ruffini, existe $q(x) \in K[x]$ tal que $p(x) = (x-\alpha)q(x)$; luego $\operatorname{gr} q(x) = \operatorname{gr} p(x) - 1$ y, por hipótesis de inducción, existe alguna extensión finita L de K en la que $q(x)$ tiene todas sus raíces. Según 4.2.2, $q(x)$ descompone en $L[x]$ en producto de polinomios de grado 1, así que $p(x) = (x-\alpha)q(x)$ también descompone en $L[x]$ en producto de polinomios de grado 1 y concluimos que $p(x)$ tiene todas sus raíces en L, que es una extensión finita de k en virtud del siguiente resultado:

Teorema del Grado: *Si K es una extensión finita de un cuerpo k y L es una extensión finita de K, entonces L es una extensión finita de k de grado*

$$[L:k] \;=\; [L:K]\cdot[K:k]$$

Demostración: Sea $(u_1,\ldots,u_n)$ una base de K sobre k y $(v_1,\ldots,v_m)$ una base de L sobre K. Si $x \in L$, entonces $x = \sum_i \lambda_i v_i$ para ciertos $\lambda_i \in K$. A su vez $\lambda_i = \sum_j a_{ij}u_j$, $a_{ij} \in k$. Luego $x = \sum_{ij} a_{ij}v_iu_j$ y concluimos que los elementos v_iu_j generan L como k-espacio vectorial.

Por otra parte, si alguna combinación lineal $\sum_{ij} a_{ij}v_iu_j$ con coeficientes en k es nula, entonces

$$\sum_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}u_j\Big)v_i = 0$$

y se sigue que $a_{i1}u_1 + \ldots + a_{in}u_n = 0$ para todo índice i. Luego los coeficientes a_{ij} son todos nulos, y los elementos v_iu_j son linealmente independientes sobre k. Concluimos que forman una base de L y, en consecuencia, la dimensión de L como k-espacio vectorial es nm. q.e.d.

Nótese que el teorema de Kronecker (1823-1891) no es meramente existencial, sino que proporciona un método efectivo para calcular una raíz α de un polinomio

no constante $p(x)$ con coeficientes en un cuerpo k, siempre que se conozca algún factor irreducible $\sum_i a_i x^i$ de $p(x)$ en el anillo $k[x]$:

$$\boxed{\alpha = [\,x\,] \quad (\text{módulo } \textstyle\sum_i a_i x^i)}$$

lo que reduce el problema de la extracción de raíces al de la descomposición en factores irreducibles de los polinomios en una indeterminada (con coeficientes en extensiones finitas de k), cuestión a la que nos dedicaremos en breve. Este teorema aporta una contribución fundamental[5], y en cierto sentido definitiva, a la resolución de ecuaciones algebraicas con una incógnita.

A título de ejemplo, veamos cómo este teorema permite probar que *todo polinomio no constante $p(x)$ con coeficientes reales tiene alguna raíz compleja*, y dar así una demostración más algebraica del Teorema de D'Alembert (1717-1783):

Si $\operatorname{gr} p(x) = n = 2^d m$, donde m es impar, procedemos por inducción sobre d. El enunciado es cierto para los polinomios de grado impar según el Teorema de Bolzano (1781-1848), y éste es el punto trascendente de la demostración. Sea L una extensión finita de $\mathbb{C}$ donde el polinomio tenga todas sus raíces, que existe en virtud de 4.4.3. Dado $a \in \mathbb{R}$, formamos el polinomio de raíces $\alpha_i + \alpha_j + a\alpha_i\alpha_j$, donde α_i y α_j recorren las raíces de $p(x)$, que tiene grado $n(n-1)/2 = 2^{d-1}m(n-1)$. Sus coeficientes son reales, porque son funciones simétricas de las raíces de $p(x)$ (v. apéndice A). Por hipótesis de inducción este polinomio tiene alguna raíz compleja: $\alpha_i + \alpha_j + a\alpha_i\alpha_j \in \mathbb{C}$ para ciertos índices i, j. Luego existen índices i, j tales que

$$\alpha_i + \alpha_j + a\alpha_i\alpha_j,\ \alpha_i + \alpha_j + b\alpha_i\alpha_j \in \mathbb{C}$$

donde $a \neq b$. Se sigue que $\alpha_i + \alpha_j,\ \alpha_i\alpha_j \in \mathbb{C}$ y concluimos que α_i y α_j son raíces de un polinomio de grado 2 con coeficientes complejos, polinomios que obviamente tienen todas sus raíces complejas: $\alpha_i,\ \alpha_j \in \mathbb{C}$.

Por último, si $p(x)$ es un polinomio no constante con coeficientes complejos y $\bar{p}(x)$ denota el polinomio de coeficientes conjugados, entonces $p(x)\bar{p}(x) \in \mathbb{R}[x]$; luego $p(x)\bar{p}(x)$ tiene alguna raíz compleja α, que es raíz de $p(x)$ ó de $\bar{p}(x)$, en cuyo caso $\bar{\alpha}$ es raíz de $p(x)$.

[5] La primera vez que nos enfrentamos a este teorema, no es raro que lo percibamos como una "mera tautología", una "formalidad infecunda". Ciertamente es una tautología, al igual que cualquier otro teorema, y justamente eso es lo que muestra la demostración que sigue a cada teorema. Ciertamente es una formalidad, presentada con todo el rigor formal del que somos capaces. Pero, tras la lectura de las restantes páginas de este libro, dejo a juicio del lector la consideración que merecen los calificativos de "mera" e "infecunda". Y es que nuestras preguntas, como pueda ser la búsqueda de las raíces de un polinomio, llevan implícito el horizonte que abarca las posibles respuestas. La aclaración de ese horizonte, su ampliación cuando comprendemos nuestra estrechez de miras, es uno de los momentos fuertes de la aventura del conocimiento humano. Por eso este teorema no es uno más en este libro, sino un Rubicón que se ha de cruzar para entender muchas respuestas que los siglos XIX y XX han dado a viejos problemas.

Elementos Algebraicos

Definición: Sea L una extensión de un cuerpo k. Diremos que un elemento $\alpha \in L$ es **algebraico** sobre k si es raíz de algún polinomio no nulo $q(x)$ con coeficientes en k, y por tanto de algún factor irreducible $p_\alpha(x)$ de $q(x)$ en $k[x]$ que, según 4.4.2, divide a todo polinomio con coeficientes en k que admita la raíz α. Tal polinomio $p_\alpha(x)$ es, salvo factores constantes, el único polinomio irreducible con coeficientes en k que tiene la raíz α y diremos que es el polinomio irreducible o **polinomio mínimo** de α sobre k, pues es el polinomio de menor grado con coeficientes en k que admite la raíz α.

Si $\alpha \in L$ no es algebraico sobre k, diremos es **trascendente** sobre k.

Diremos que una extensión $k \to L$ es **algebraica** cuando todos los elementos de L sean algebraicos sobre k.

Lema 4.4.4 *La condición necesaria y suficiente para que un elemento α de una extensión de un cuerpo k sea algebraico sobre k es que $k(\alpha)$ sea una extensión finita de k. En particular todo elemento de una extensión finita de k es algebraico sobre k.*

Demostración: La necesidad de la condición es consecuencia de 4.4.2.

Recíprocamente, si $k(\alpha)$ es una extensión finita de k, entonces las potencias de α son linealmente dependientes (i.e., $\sum_i a_i\alpha^i = 0$ donde los coeficientes $a_i \in k$ no son todos nulos) y concluimos que α es raíz de un polinomio no nulo con coeficientes en k.

Corolario 4.4.5 *Sea L una extensión de un cuerpo k. Si $\alpha_1, \ldots, \alpha_n \in L$ son algebraicos sobre k, entonces $k(\alpha_1, \ldots, \alpha_n)$ es una extensión finita de k.*

Demostración: Procediendo por inducción sobre n (el caso $n = 1$ se sigue del lema anterior) podemos suponer que $k(\alpha_1, \ldots, \alpha_{n-1})$ es una extensión finita de k. Ahora, como α_n es algebraico sobre k, también es algebraico sobre $k(\alpha_1, \ldots, \alpha_{n-1})$, así que $k(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$ es una extensión finita de $k(\alpha_1, \ldots, \alpha_{n-1})$ y el Teorema del Grado permite concluir que es una extensión finita de k.

Teorema 4.4.6 *Si L es una extensión de un cuerpo k, los elementos de L algebraicos sobre k forman una extensión de k. Es decir, si $\alpha, \beta \in L$ son algebraicos sobre k, entonces también lo son $\alpha + \beta$, $\alpha\beta$ y α/β cuando $\beta \neq 0$.*

Demostración: Si $\alpha, \beta \in L$ son algebraicos sobre k, entonces $k(\alpha, \beta)$ es una extensión finita de k por el corolario anterior, y 4.4.4 permite concluir que todos sus elementos son algebraicos sobre k. En particular lo son $\alpha + \beta$, $\alpha\beta$ y α/β.

Teorema 4.4.7 *Sea K una extensión algebraica de un cuerpo k y sea L una extensión de K. Si $\alpha \in L$ es algebraico sobre K, entonces α es algebraico sobre*

k. En particular, las raíces n-ésimas de cualquier elemento algebraico sobre k también son algebraicas sobre k.

Demostración: Si α es raíz de un polinomio no nulo $c_0x^n + \ldots + c_n$ con coeficientes en K, entonces α es algebraico sobre $k(c_0, \ldots, c_n)$, que es una extensión finita de k por 4.4.5. Luego $k(c_0, \ldots, c_n, \alpha)$ es una extensión finita de $k(c_0, \ldots, c_n)$ y el teorema del grado afirma que $k(c_0, \ldots, c_n, \alpha)$ es una extensión finita de k. Por tanto α, que está en $k(c_0, \ldots, c_n, \alpha)$, es algebraico sobre k por 4.4.4.

Ejemplo: Según los teoremas anteriores, todo número complejo que pueda obtenerse a partir de los números racionales mediante un número finito de sumas, restas, productos, cocientes y radicales es algebraico sobre $\mathbb{Q}$.

Por ejemplo, $((\sqrt[3]{2}/\sqrt{-3}) + 1)^{-1/5}$ es algebraico sobre $\mathbb{Q}$.

Extensiones Finitas de $\mathbb{R}$ y $\mathbb{C}$

En el capítulo 1 definimos un producto en las parejas de números reales

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

construyendo así una extensión $\mathbb{C}$ de $\mathbb{R}$ de grado 2. Pudiera pensarse en la posibilidad de definir en el espacio $\mathbb{R}^3$, o en espacios de dimensión superior, un producto análogo. Veremos ahora que tal cosa no es posible si deseamos obtener una extensión de $\mathbb{R}$. Ningún producto en $\mathbb{R}^n$, $n \geq 3$, puede definir una extensión de los números reales: debe violar alguna de las propiedades básicas de la multiplicación usual (distributiva, asociativa, conmutativa, existencia de unidad y de inverso de todo elemento no nulo). Probaremos incluso que, salvo isomorfismos, el producto de números complejos es el único producto en $\mathbb{R}^2$ que define una extensión de $\mathbb{R}$.

Teorema 4.4.8 *Toda extensión finita $\mathbb{C} \to K$ es trivial: $\mathbb{C} = K$.*

Demostración: Si $\alpha \in K$, de acuerdo con 4.4.4, α es raíz de algún polinomio no nulo $p(x)$ con coeficientes complejos. Según 4.2.3, $p(x)$ tiene todas sus raíces complejas; así que $\alpha \in \mathbb{C}$ y concluimos que el morfismo $\mathbb{C} \to K$ es un isomorfismo.

Teorema 4.4.9 *Toda extensión finita de $\mathbb{R}$ es isomorfa a $\mathbb{R}$ o a $\mathbb{C}$.*

Demostración: Sea $\mathbb{R} \to K$ una extensión finita. Si no es un isomorfismo, existe algún $\alpha \in K$ que no es real. De acuerdo con 4.4.4, α es algebraico sobre $\mathbb{R}$, así que es raíz de un polinomio irreducible $p(x)$ con coeficientes reales. Por el teorema de D'Alembert, $p(x)$ tiene alguna raíz compleja $\beta \in \mathbb{C}$ y el Teorema de Kronecker afirma que existe un isomorfismo $\mathbb{R}(\alpha) \simeq \mathbb{R}(\beta)$, $\alpha \mapsto \beta$.

Como α no es real, tampoco lo es β y obtenemos que $\mathbb{R}(\beta) = \mathbb{C}$. Luego K es una extensión finita de $\mathbb{R}(\alpha) \simeq \mathbb{C}$ y 4.4.8 permite concluir que $K \simeq \mathbb{C}$.

4.5 La Resultante

Consideremos dos polinomios con coeficientes en un cuerpo k:

$$p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$
$$q(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$$

(no excluimos el caso $a_0 = 0$ ó $b_0 = 0$; es decir, el grado de $p(x)$ puede ser menor que n y el de $q(x)$ puede ser menor que m). Daremos ahora criterios para que ambos polinomios tengan raíces comunes (en alguna extensión del cuerpo de coeficientes k).

Teorema 4.5.1 *Las raíces comunes de dos polinomios $p(x)$ y $q(x)$ con coeficientes en un cuerpo k son las raíces de su máximo común divisor. Por tanto, la condición necesaria y suficiente para que tengan alguna raíz común es que admitan en $k[x]$ algún factor común no constante.*

Demostración: Sea $d(x)$ el máximo común divisor de $p(x)$ y $q(x)$. Toda raíz de $d(x)$ es raíz de $p(x)$ y $q(x)$, porque ambos polinomios son múltiplos de $d(x)$. Recíprocamente, de la Identidad de Bézout (1730-1783)

$$d(x) = a(x)p(x) + b(x)q(x)$$

se sigue que toda raíz común de $p(x)$ y $q(x)$ es raíz de $d(x)$. Finalmente, si $d(x)$ no es constante, en virtud del teorema de Kronecker tiene alguna raíz que, por lo anterior, será una raíz común de $p(x)$ y $q(x)$.

Lema 4.5.2 *Si $a_0 \neq 0$, los polinomios $p(x)$ y $q(x)$ tienen algún factor común no constante en $k[x]$ si y sólo si existe alguna relación*

$$a(x)p(x) + b(x)q(x) = 0$$

donde $a(x)$ y $b(x)$ son polinomios no nulos con coeficientes en k de grados menores que m y n respectivamente.

Demostración: Veamos que es condición suficiente. Si existe alguna relación no trivial $a(x)p(x) + b(x)q(x) = 0$ y factorizamos $a(x)p(x)$ y $-b(x)q(x)$ en factores irreducibles en $k[x]$, debemos obtener los mismos factores (salvo constantes no nulas). No todos los factores irreducibles de $p(x)$ pueden dividir a $b(x)$ tantas veces como dividen a $p(x)$, porque $\operatorname{gr} b(x) < n = \operatorname{gr} p(x)$. Luego algún factor irreducible de $p(x)$ aparece en la descomposición de $q(x)$.

Veamos que es condición necesaria. Si $p(x) = b(x)d(x)$, $q(x) = a(x)d(x)$, donde $d(x) \in k[x]$ es un factor no constante común, entonces $a(x)p(x) - b(x)q(x) = 0$, donde $\operatorname{gr} a(x) \leq m - 1$ y $\operatorname{gr} b(x) \leq n - 1$. q.e.d.

La existencia de tal relación $a(x)p(x) + b(x)q(x) = 0$ equivale a decir que los polinomios

$$p(x),\ xp(x),\ \ldots,\ x^{m-1}p(x),\ q(x),\ xq(x),\ \ldots,\ x^{n-1}q(x)$$

son linealmente dependientes; esto es, a la anulación del siguiente determinante:

$$\begin{vmatrix} a_0 & a_1 & \ldots & \ldots & a_n & 0 & \ldots & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & \ldots & \ldots & b_m & 0 & \ldots & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_{m-1} & b_m & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & b_{m-1} & b_m \end{vmatrix}$$

donde hay m filas con los coeficientes de $p(x)$ y n filas con los de $q(x)$.

Este determinante recibe el nombre de **resultante** y, cuando $a_0 \neq 0$ ó $b_0 \neq 0$, su anulación expresa la existencia de un factor no constante común de $p(x)$ y $q(x)$, lo que equivale a la existencia de una raíz común en alguna extensión de k. En resumen, la *resultante se anula precisamente cuando ambos polinomios tienen alguna raíz común o cuando a_0 y b_0 son nulos.* En cualquier caso, si los polinomios dados tienen alguna raíz común, la resultante se anula.

Eliminación de Indeterminadas

Sean $p(x, y)$ y $q(x, y)$ dos polinomios en dos indeterminadas x, y con coeficientes en un cuerpo k. Si los consideramos como polinomios en la indeterminada x con coeficientes en el cuerpo $k(y)$:

$$p(x, y) = a_0(y)x^n + a_1(y)x^{n-1} + \ldots + a_n(y)$$
$$q(x, y) = b_0(y)x^m + b_1(y)x^{m-1} + \ldots + b_m(y)$$

su resultante es un polinomio $r(y)$ con coeficientes en k.

Teorema 4.5.3 *Las raíces de la resultante $r(y)$ son las ordenadas de las soluciones del sistema de ecuaciones*

$$\left.\begin{array}{l} p(x, y) = 0 \\ q(x, y) = 0 \end{array}\right\}$$

en las extensiones de k, junto con las raíces comunes de $a_0(y)$ y $b_0(y)$.

Demostración: Sea β un elemento de una extensión K de k. Es claro que $r(\beta)$ es la resultante de los polinomios (con coeficientes en K):

$$p(x, \beta) = \textstyle\sum_i a_i(\beta)x^{n-i}\ , \quad q(x, \beta) = \sum_j b_j(\beta)x^{m-j}$$

así que la anulación de $r(\beta)$ equivale a la condición $a_0(\beta) = b_0(\beta) = 0$ ó a la existencia de una raíz común α en alguna extensión de L; es decir, a la existencia de alguna solución (α, β) del sistema. q.e.d.

De acuerdo con el teorema anterior, al eliminar una indeterminada x con la resultante, además de las ordenadas de las soluciones del sistema se introducen unas raíces adicionales, que son las raíces comunes de los coeficientes $a_0(y)$ y $b_0(y)$. Si se desea eliminar una indeterminada sin introducir nuevas soluciones, basta efectuar un cambio de variable de la forma $y' = y - \lambda x$, $\lambda \in k$, al menos cuando k es infinito. En efecto, sea

$$p(x, y) = \sum_{i=0}^{d} c_i x^i y^{d-i} + \text{ términos de grado menor que } d$$

Al efectuar el cambio $y = y' + \lambda x$ obtenemos que el coeficiente de x^d en $p(x, y' + \lambda x)$ es precisamente $\sum_i c_i \lambda^{d-i}$. *Si el cuerpo k tiene infinitos elementos*, podemos elegir $\lambda \in k$ de modo que tal coeficiente no sea nulo. En tal caso dicho coeficiente es un polinomio constante no nulo, así que no puede tener raíces comunes con ningún otro polinomio y, si procedemos a eliminar la indeterminada x con la resultante, obtendremos un polinomio $r(y')$ en el que no se han introducidos soluciones extrañas.

Resolución de Sistemas

Consideremos un sistema de dos ecuaciones algebraicas

$$\left.\begin{array}{l} p(x, y) = 0 \\ q(x, y) = 0 \end{array}\right\}$$

con coeficientes en un cuerpo k. De acuerdo con 4.5.3, si para cada raíz $\beta \in k$ de la resultante $r(y)$ hallamos las raíces comunes en k de los polinomios $p(x, \beta)$ y $q(x, \beta)$ las parejas así calculadas son *todas* las soluciones en k del sistema inicial. Como 3.4.1 permite hallar las raíces racionales de cualquier polinomio con coeficientes racionales, podemos calcular todas las soluciones racionales de cualquier sistema de ecuaciones algebraicas con coeficientes racionales en dos incógnitas (si la resultante no es nula) del siguiente modo:

1. Se elimina una indeterminada x, calculando la resultante $r(y)$.

2. Se hallan las raíces racionales β_i de la resultante $r(y)$.

3. Se sustituye cada raíz β_i en el sistema y se determinan las raíces racionales comunes a los dos polinomios en x obtenidos.

Conviene observar que si un número racional β es raíz de la resultante $r(y)$ de un sistema de ecuaciones $p(x,y)=0$, $q(x,y)=0$ con coeficientes racionales, no se sigue necesariamente que β sea la segunda componente de alguna solución racional del sistema, sino que la anulación de $r(\beta)$ significa que el sistema admite alguna solución compleja (α,β) o que β es raíz común de los polinomios $a_0(y)$ y $b_0(y)$.

Por ejemplo, si eliminamos x en el sistema de ecuaciones

$$\left.\begin{aligned} x^2y^2 - x^2 + xy + x = 0 \\ x^2y + xy^2 - x^2 - x + 2y = 0 \end{aligned}\right\}$$

la resultante es $2y^6 - 2y^5 - 2y^4 + 6y^3 - 4y = 2y(y+1)^2(y-1)(y^2-2y+2)$, y sus raíces racionales son $y = 0, 1, -1$.

Sustituyendo y por 0 obtenemos los polinomios $-x^2 + x$ y $-x^2 - x$, que tienen la raíz común $x = 0$.

Sustituyendo y por 1 obtenemos el polinomio $2x$ y el polinomio constante 2, que no tienen ninguna raíz común (por tanto $y = 1$ ha de ser una raíz común de $a_0(y)$ y $b_0(y)$).

Sustituyendo y por –1 obtenemos el polinomio nulo y el polinomio $-2x^2 - 2$, que tienen las raíces comunes $\pm i$, de modo que –1 no es la segunda componente de ninguna solución racional del sistema, aunque sí lo es de dos soluciones complejas: $(i,-1)$ y $(-i,-1)$.

Luego el sistema tiene una única solución racional: $x = 0$, $y = 0$, aunque tiene otras soluciones complejas, por ejemplo $x = \pm i$, $y = -1$ (como ejercicio pueden hallarse las restantes soluciones complejas de este sistema).

Capítulo 5

Factorización Única

Hallar una raíz de un polinomio $p(x)$ consiste, más que en expresar "negro sobre blanco" una raíz, en determinar efectivamente un procedimiento para realizar sumas y productos de las expresiones algebraicas formadas con tal raíz. A la vista del teorema de Kronecker, éste resuelve totalmente la cuestión siempre que seamos capaces de calcular un factor irreducible $q(x)$ de $p(x)$. El procedimiento expuesto para extraer una raíz de un polinomio sólo es efectivo si disponemos de métodos para descomponer cada polinomio en factores irreducibles.

Es claro que el problema de hallar todos los factores de cierto grado de un polinomio dado con coeficientes racionales se reduce al de calcular todas las soluciones racionales de un sistema de ecuaciones algebraicas con coeficientes racionales, sistema del que sabemos que sólo tiene un número finito de soluciones complejas. Tales sistemas pueden siempre resolverse eliminando sucesivamente variables mediante el uso sistemático de resolventes, cuidando de no introducir soluciones extrañas, o bien mediante el cálculo de una base de Gröebner (1899-1980) del sistema de ecuaciones considerado (ver [5]).

Otro método, debido a Kronecker (1823-1892), se basa en el lema de Gauss: al descomponer un polinomio con coeficientes enteros $p(x)$ en factores irreducibles en $\mathbb{Z}[x]$, los factores también son irreducibles en $\mathbb{Q}[x]$. Ahora, para determinar todos los factores de $p(x)$ de cierto grado d basta elegir números enteros $a_0, a_1, \ldots, a_d$ y observar que tales factores se encuentran entre los polinomios con coeficientes enteros que se obtengan al interpolar en los puntos $x = a_1, \ldots, x = a_d$ las sucesiones formadas por divisores de los enteros $p(a_0), p(a_1), \ldots, p(a_d)$.

No obstante, todos estos métodos para descomponer en factores irreducibles polinomios con coeficientes racionales son prácticamente imposibles de realizar con lápiz y papel, a pesar de su extrema sencillez teórica. Por eso, al final del capítulo daremos algunos procedimientos más rápidos, aunque no generales, que a menudo son útiles.

Este capítulo tiene naturaleza más técnica que los anteriores, pues esencialmente está dedicado a la demostración de que en los anillos de polinomios $k[x_1, \ldots, x_n]$ con coeficientes en un cuerpo k y en los anillos de polinomios con coeficientes enteros $\mathbb{Z}[x_1, \ldots, x_n]$ se verifica la existencia y unicidad (salvo el orden e invertibles) de la descomposición en factores irreducibles; a pesar de que no son dominios de ideales principales. En la demostración de este resultado central utilizaremos sistemáticamente la construcción de los anillos de fracciones, introducida por Chevalley (1909-1984), similar a la construcción de los números racionales, a partir de los números enteros, que se expuso en el primer capítulo. Los anillos de fracciones irán adquiriendo una importancia creciente, porque proporcionan el fundamento de la estrecha relación entre el Álgebra y la Geometría. El punto central de la demostración es el llamado lema de Gauss (1777-1855). Como consecuencias de este importante lema veremos algunos criterios de irreducibilidad para polinomios con coeficientes enteros.

5.1 Anillos de Fracciones

Definición: Diremos que un subconjunto S de un anillo A es un **sistema multiplicativo** cuando $1 \in S$ y $a, b \in S \Rightarrow ab \in S$.

Si S es un sistema multiplicativo de un anillo A, vamos a construir el anillo de fracciones con numerador en A y denominador en S; para lo cual consideramos en $A \times S$ la siguiente relación:

$$(a, s) \equiv (b, t) \;\Leftrightarrow\; \text{existen } u, v \in S \text{ tales que } au = bv \text{ y } su = tv$$

que es una relación de equivalencia en el conjunto $A \times S$.

Claramente tiene las propiedades simétrica y reflexiva. En cuanto a la transitiva, si $(a, s) \equiv (b, t)$ y $(b, t) \equiv (c, r)$, existen $u, v, u', v' \in S$ tales que $au = bv$, $su = tv$ y $bu' = cv'$, $tu' = rv'$. Luego $auu' = bvu' = cvv'$ y $suu' = tvu' = rvv'$. Como $uu', vv' \in S$, concluimos que $(a, s) \equiv (c, r)$.

Definición: Sea S un sistema multiplicativo de un anillo A. Llamaremos **anillo de fracciones** o **localización** de A por S, y se denota $S^{-1}A$ ó A_S, al conjunto cociente $(A \times S)/\equiv$ con la estructura de anillo que definen las operaciones:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad , \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

donde $a/s = \pi(a, s)$ y $\pi \colon A \times S \to (A \times S)/\equiv$ es la proyección canónica. Para ver que estas operaciones no dependen de los representantes elegidos, basta comprobarlo cuando la fracción a/s se sustituye por au/su:

$$\frac{au}{su} + \frac{b}{t} = \frac{(at + bs)u}{stu} = \frac{at + bs}{st} \qquad , \qquad \frac{au}{su} \cdot \frac{b}{t} = \frac{abu}{stu} = \frac{ab}{st}$$

Es sencillo comprobar que estas dos operaciones definen en $(A \times S)/\equiv$ una estructura de anillo (conmutativo con unidad). El cero es $0/1$, la unidad es $1/1$ y el opuesto de a/s es $(-a)/s$. Además, una fracción a/s es nula precisamente cuando $ta = 0$ para algún $t \in S$.

La aplicación $\gamma\colon A \to S^{-1}A$, $\gamma(a) = a/1$, es morfismo de anillos

$$\begin{aligned} \gamma(a+b) &= (a+b)/1 = a/1 + b/1 = \gamma(a) + \gamma(b) \\ \gamma(ab) &= ab/1 = (a/1)(b/1) = \gamma(a)\gamma(b) \\ \gamma(1) &= 1/1 \end{aligned}$$

Nótese que $\gamma(s) = s/1$ es invertible en $S^{-1}A$ para todo $s \in S$, pues su inverso es $1/s$. Este morfismo de anillos canónico $\gamma\colon A \to S^{-1}A$ se llamará, por razones que se aclararán en los capítulos VII y VIII, **morfismo de localización**.

Propiedad Universal: *Sea $\gamma\colon A \to S^{-1}A$ el morfismo de localización de un anillo A por un sistema multiplicativo S. Si $f\colon A \to B$ es un morfismo de anillos tal que $f(s)$ es invertible en B para todo $s \in S$, entonces existe un único morfismo de anillos $\psi\colon S^{-1}A \to B$ tal que $f = \psi \circ \gamma$:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\gamma}\searrow & \nearrow{\scriptstyle\psi} & \\ & S^{-1}A & \end{array}$$

Demostración: Si $f(s)$ es invertible en B para todo $s \in S$, entonces la aplicación

$$\psi\colon S^{-1}A \to B\ , \quad \psi(a/s) = f(a)f(s)^{-1}$$

no depende del representante a/s elegido, porque

$$\psi(au/su) = f(au)f(su)^{-1} = f(a)f(u)f(s)^{-1}f(u)^{-1} = f(a)f(s)^{-1}$$

Se comprueba fácilmente que esta aplicación ψ es un morfismo de anillos. Además, si $a \in A$, entonces $(\psi \circ \gamma)(a) = \psi(a/1) = f(a)f(1)^{-1} = f(a)$.

Teorema 5.1.1 *Sea A un anillo íntegro. $S = A - \{0\}$ es un sistema multiplicativo, el anillo de fracciones $S^{-1}A$ es un cuerpo (llamado **cuerpo de fracciones** de A) y el morfismo de localización $\gamma\colon A \to S^{-1}A$ es inyectivo.*

Demostración: Si A es íntegro, $S = A - \{0\}$ es un sistema multiplicativo porque en A el producto de elementos no nulos nunca es nulo y $1 \neq 0$.

Por otra parte, si $a/1 = 0$, existe $s \neq 0$ tal que $sa = 0$; luego $a = 0$ y se sigue que $\gamma\colon A \to S^{-1}A$ es inyectivo. En particular $S^{-1}A \neq 0$. Además, si a/s no es nulo, entonces $a \neq 0$; luego $a \in S$ y $s/a \in S^{-1}A$ verifica que $(a/s)(s/a) = 1$, de modo que a/s es invertible en $S^{-1}A$ y concluimos que $S^{-1}A$ es un cuerpo.

Definición: Sea k un cuerpo. El anillo de polinomios $k[x_1, \ldots, x_n]$ es íntegro y su cuerpo de fracciones se llama **cuerpo de fracciones racionales** en n indeterminadas con coeficientes en k, y se denotará $k(x_1, \ldots, x_n)$.

5.2 Fracciones Racionales

Sea $k(x)$ el cuerpo de las fracciones racionales en una indeterminada x con coeficientes en un cuerpo k.

Lema 5.2.1 *Sean $q_1(x), \ldots, q_r(x)$ polinomios no constantes con coeficientes en k sin factores irreducibles comunes dos a dos. Si $p(x) \in k[x]$, entonces existen polinomios $b_1(x), \ldots, b_r(x) \in k[x]$ tales que:*

$$\frac{p(x)}{q_1(x)\cdots q_r(x)} = \frac{b_1(x)}{q_1(x)} + \cdots + \frac{b_r(x)}{q_r(x)}$$

Demostración: Procederemos por inducción sobre r. Cuando $r = 1$ basta tomar $b_1(x) = p(x)$. Si $r \geq 2$, los polinomios $q(x) = q_1(x)\cdots q_{r-1}(x)$ y $q_r(x)$ no tienen factores comunes no constantes. Según la Identidad de Bézout existen polinomios $s(x)$, $t(x) \in k[x]$ tales que

$$1 = s(x)q(x) + t(x)q_r(x)$$

Luego $p(x) = p(x)s(x)q(x) + p(x)t(x)q_r(x)$ y

$$\frac{p}{q_1\cdots q_r} = \frac{ptq_r}{qq_r} + \frac{psq}{qq_r} = \frac{pt}{q_1\cdots q_{r-1}} + \frac{b_r}{q_r}$$

donde $b_r(x) = p(x)s(x)$. Por hipótesis de inducción, existen polinomios $b_1(x), \ldots, b_{r-1}(x)$ con coeficientes en k tales que:

$$\frac{p(x)t(x)}{q_1(x)\cdots q_{r-1}(x)} = \frac{b_1(x)}{q_1(x)} + \cdots + \frac{b_{r-1}(x)}{q_{r-1}(x)}$$

Lema 5.2.2 *Sea $q(x)$ un polinomio de grado $d \geq 1$ con coeficientes en un cuerpo k. Para cada polinomio $b(x) \in k[x]$ existen polinomios $a_0(x), \ldots, a_n(x) \in k[x]$, de grado menor que d ó nulos, tales que*

$$b(x) = a_0(x) + a_1(x)q(x) + a_2(x)q(x)^2 + \ldots + a_n(x)q(x)^n$$

Demostración: Procederemos por inducción sobre el grado de $b(x)$, pues es obvio cuando $b(x)$ es constante.

Si $\operatorname{gr} b(x) \geq 1$, existen $c(x)$, $r(x) \in k[x]$ tales que $b(x) = q(x)c(x) + r(x)$ y $\operatorname{gr} r(x) < d$ ó $r(x) = 0$. Si $c(x) \neq 0$, entonces $\operatorname{gr} b(x) = d + \operatorname{gr} c(x)$ y, por hipótesis de inducción, tenemos que

$$c(x) = a_1(x) + a_2(x)q(x) + a_3(x)q(x)^2 + \ldots$$

para ciertos $a_1(x)$, $a_2(x)$, $a_3(x), \ldots \in k[x]$ que son nulos o de grado menor que d. Luego todos los polinomios $r(x)$, $a_1(x)$, $a_2(x)$, $a_3(x)$, ... son nulos o de grado menor que d y tenemos que

$$b(x) = r(x) + a_1(x)q(x) + a_2(x)q(x)^2 + a_3(x)q(x)^3 + \ldots$$

Definición: Diremos que una fracción racional en una indeterminada con coeficientes en un cuerpo k es **simple** si es un monomio ax^n, $n \geq 0$, ó es de la forma $p(x)/q(x)^n$, $n \geq 1$, donde $p(x), q(x) \in k[x]$, $q(x)$ es irreducible en $k[x]$ y el grado de $p(x)$ es menor que el grado de $q(x)$.

Teorema 5.2.3 *Toda fracción racional en una indeterminada con coeficientes en un cuerpo k descompone en suma de fracciones simples, y tal descomposición es única salvo el orden de los sumandos.*

Demostración: Veamos primero la *existencia*. Sea $p(x)/q(x) \in k(x)$, donde podemos suponer que $q(x)$ es unitario, y sea $q(x) = q_1(x)^{n_1} \cdots q_r(x)^{n_r}$ la descomposición de $q(x)$ en producto de potencias de polinomios irreducibles en $k[x]$. Según 5.2.1, tenemos que

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{r} \frac{b_i(x)}{q_i(x)^{n_i}}$$

Ahora, según 5.2.2, existen polinomios $a_{i0}(x)$, $a_{i1}(x)$, $\ldots \in k[x]$, nulos o de grado menor que el de $q_i(x)$, tales que:

$$\frac{b_i(x)}{q_i(x)^{n_i}} = \frac{a_{i0}(x) + a_{i1}(x)q_i(x) + a_{i2}(x)q_i(x)^2 + \ldots}{q_i(x)^{n_i}} =$$

$$= \text{Polinomio} + \sum_{j=0}^{n_i-1} \frac{a_{ij}(x)}{q_i^{n_i-j}(x)}$$

que es una suma de fracciones simples.

En cuanto a la *unicidad*, procedemos por inducción sobre el número de sumandos de una descomposición. Consideremos dos descomposiciones

$$\frac{a(x)}{q_1^{n_1}(x)} + \ldots = \frac{b(x)}{q_1^{n_1}(x)} + \ldots \qquad , \qquad a(x) \neq 0$$

donde $q_1^{n_1}(x)$ es la potencia de $q_1(x)$ de mayor exponente que aparece en estas descomposiciones y eventualmente $b(x) = 0$. Multiplicando por el máximo común divisor de los denominadores de todas las fracciones simples obtenemos una igualdad de polinomios

$$\big(a(x) - b(x)\big)q_2^{n_2}(x) \ldots q_r^{n_r}(x) = q_1(x)c(x)$$

y obtenemos que $q_1(x)$ divide a $a(x) - b(x)$. Como $\operatorname{gr} a(x) - b(x) < \operatorname{gr} q_1(x)$, concluimos que $a(x) = b(x)$ y terminamos la demostración al aplicar la hipótesis de inducción.

5.3 Dominios de Factorización Única

Definición: Diremos que un anillo íntegro A es un **dominio de factorización única** si todo elemento no nulo ni invertible de A descompone en producto de elementos irreducibles de A y tal descomposición es única salvo el orden y factores invertibles en A. (Es decir, si $a \in A$ no es nulo ni invertible, existen irreducibles $p_1, \ldots, p_r \in A$, $r \geq 1$, tales que $a = p_1 \cdots p_r$. Si $a = q_1 \cdots q_s$ es otra descomposición de a en producto de irreducibles, entonces $r = s$ y, después de reordenar los factores si fuera preciso, $q_i = u_i p_i$ para ciertos invertibles $u_1, \ldots, u_r \in A$).

Sea A un dominio de factorización única. Si $a = p_1^{n_1} \cdots p_r^{n_r}$ es una descomposición de un elemento $a \in A$ en producto de elementos irreducibles de A, donde $p_i A \neq p_j A$ cuando $i \neq j$, es sencillo comprobar que, salvo invertibles de A, los divisores de a en A son:

$$p_1^{d_1} \ldots p_r^{d_r} \ , \quad 0 \leq d_i \leq n_i \ \ \text{(convenimos que } p_i^0 = 1)$$

Luego el máximo común divisor y el mínimo común múltiplo de dos elementos:

$$a = p_1^{n_1} \ldots p_r^{n_r} \ , \ \ b = p_1^{m_1} \ldots p_r^{m_r} \quad , \qquad m_i, n_i \geq 0$$

siempre existen (y son únicos salvo invertibles de A) y son:

$$\begin{aligned} \text{m.c.d.}(a,b) &= p_1^{d_1} \cdots p_r^{d_r} \quad , \qquad d_i = \min\{m_i, n_i\} \\ \text{m.c.m.}(a,b) &= p_1^{e_1} \cdots p_r^{e_r} \quad , \qquad e_i = \max\{m_i, n_i\} \end{aligned}$$

Diremos que una familia finita $a_1, \ldots, a_n \in A$ no tiene factores irreducibles comunes en A si ningún elemento irreducible de A divide a todos los elementos de tal familia. En los dominios de factorización única es válido el lema de Euclides bajo la siguiente forma: Si un elemento irreducible $p \in A$ divide a un producto de elementos de A, entonces divide a algún factor (es decir, pA es un ideal primo de A). En efecto, $pA \neq A$ porque p no es invertible en A, y si $bc \in pA$, entonces $bc = pa$, $a \in A$. En virtud de la unicidad de la descomposición en factores irreducibles, al descomponer b y c en producto de irreducibles, algún factor debe coincidir, salvo un invertible, con p; luego b o c es múltiplo de p y concluimos que pA es un ideal primo de A. En general, si d divide a bc y no tiene factores irreducibles comunes con b, entonces divide a c.

Por otra parte, si Σ denota el cuerpo de fracciones de A y $a/b \in \Sigma$, tendremos $a = da'$, $b = db'$, donde $d = \text{m.c.d.}(a,b)$; de modo que a' y b' ya no tienen factores irreducibles comunes en A y $a/b = a'/b'$. Es decir, toda fracción de A es equivalente a una fracción cuyo numerador y denominador no tienen factores irreducibles comunes.

Teorema 5.3.1 *Sea $p(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ un polinomio con coeficientes en un dominio de factorización única A y sea Σ el cuerpo de fracciones de A. Si α es una raíz de $p(x)$ en Σ, entonces $\alpha = a/b$ donde a es un divisor de c_n en A y b es un divisor de c_0 en A.*

Demostración: Sea $\alpha = a/b$, donde $a, b \in A$ no tienen factores irreducibles comunes en A. Si α es raíz de $p(x)$, entonces

$$c_0a^n + c_1a^{n-1}b + \ldots + c_{n-1}ab^{n-1} + c_nb^n = 0$$

así que c_nb^n es múltiplo de a. Como b^n no tiene factores irreducibles comunes con a y A es un dominio de factorización única, c_n es múltiplo de a en A. Análogamente c_0a^n es múltiplo de b y concluimos que c_0 es múltiplo de b en A.

Corolario 5.3.2 *Cualquier elemento de Σ que sea raíz de un polinomio unitario con coeficientes en A necesariamente está en A.*

5.4 Lema de Gauss

Lema 5.4.1 *Si p es un elemento irreducible de un dominio de factorización única A, entonces*

$$pA[x] = \{q(x) \in A[x] : \text{los coeficientes de } q(x) \text{ son múltiplos de } p\,\}$$

es un ideal primo del anillo $A[x]$.

Demostración: El núcleo del siguiente morfismo epiyectivo de anillos es $pA[x]$:

$$\phi\colon A[x] \longrightarrow (A/pA)[x]\ , \quad \phi(\textstyle\sum_i a_ix^i) = \sum_i \bar{a}_ix^i$$

Por el teorema de isomorfía, $A[x]/pA[x] \simeq (A/pA)[x]$ y, por 3.5.3, basta probar que el anillo $(A/pA)[x]$ es íntegro. Ahora bien, el anillo $(A/pA)[x]$ es íntegro porque lo es A/pA, al ser pA un ideal primo de A cuando p es irreducible en A.

Lema de Gauss (1777-1855)**:** *Sea A un dominio de factorización única y sea Σ su cuerpo de fracciones. Si un polinomio $q(x) \in A[x]$ descompone, $q(x) = q_1(x)q_2(x)$, en producto de polinomios con coeficientes en Σ, multiplicando los factores por ciertas constantes obtenemos una descomposición $q(x) = q_1'(x)q_2'(x)$ en $A[x]$.*

En particular, si $q(x)$ es irreducible en $A[x]$, entonces es irreducible en $\Sigma[x]$.

Demostración: Reduciendo a común denominador los coeficientes de q_1 y q_2 tenemos

$$\begin{aligned} q(x) &= \frac{1}{a}(a_0x^n + \ldots + a_n) \cdot \frac{1}{b}(b_0x^m + \ldots + b_m) \\ abq(x) &= (a_0x^n + \ldots + a_n)(b_0x^m + \ldots + b_m) \end{aligned}$$

donde $a, a_0, \ldots, a_n, b, b_0, \ldots, b_m \in A$. Si p es un factor irreducible de ab, según 5.4.1 ha de dividir a uno de los dos factores del segundo miembro. Después de suprimir tal factor p en ambos miembros, procedemos del mismo modo con otro factor irreducible, hasta obtener una descomposición en $A[x]$:

$$q(x) = (a'_0 x^n + \ldots + a'_n)(b'_0 x^m + \ldots + b'_m) \ .$$

Corolario 5.4.2 *Si el producto de dos polinomios unitarios con coeficientes racionales tiene coeficientes enteros, ambos polinomios tienen coeficientes enteros.*

Demostración: Sean $p(x) = x^n + \ldots$ y $q(x) = x^m + \ldots$ polinomios unitarios con coeficientes racionales. Si $p(x)q(x)$ tiene coeficientes enteros, por el lema de Gauss existe un número racional c tal que $cp(x) = cx^n + \ldots$ y $c^{-1}q(x) = c^{-1}x^m + \ldots$ tienen coeficientes enteros; luego $c = \pm 1$ y concluimos que $p(x)$ y $q(x)$ tienen coeficientes enteros.

Teorema 5.4.3 *Si A es un dominio de factorización única, los anillos de polinomios $A[x_1, \ldots, x_n]$ también son dominios de factorización única.*

Demostración: Procediendo por inducción sobre n, bastará probar que $A[x]$ es un dominio de factorización única cuando lo es A.

Sabemos que $A[x]$ es íntegro cuando A es íntegro, así que sólo hay que demostrar que todo polinomio $p(x) \in A[x]$ no nulo ni invertible descompone, y de modo único salvo el orden y factores invertibles, en producto de polinomios irreducibles en $A[x]$.

Para demostrar la existencia de la descomposición procedemos por inducción sobre el grado de $p(x)$. Si $\operatorname{gr} p(x) = 0$, el polinomio es constante, $p(x) = c \in A$ y, por hipótesis c descompone en A en producto de elementos irreducibles en A que, obviamente, también son irreducibles en $A[x]$. Si $\operatorname{gr} p(x) \geq 1$ y $d \in A$ es el máximo común divisor de los coeficientes de $p(x)$, tenemos $p(x) = dq(x)$ donde $q(x)$ es un polinomio cuyos coeficientes están en A y ya no tienen factores irreducibles comunes. Si $q(x)$ es irreducible en $A[x]$, entonces $p(x) = dq(x)$ es producto de polinomios irreducibles. Si $q(x)$ no es irreducible, existen $q_1(x), q_2(x) \in A[x]$ que no son invertibles y $q(x) = q_1(x)q_2(x)$. Ni $q_1(x)$ ni $q_2(x)$ son constantes, pues los coeficientes de $q(x)$ no tienen factores irreducibles comunes; luego $\operatorname{gr} q_1(x) < \operatorname{gr} q(x)$ y $\operatorname{gr} q_2(x) < \operatorname{gr} q(x)$. Por hipótesis de inducción $q_1(x)$ y $q_2(x)$ descomponen en producto de polinomios irreducibles en $A[x]$, luego $p(x) = dq_1(x)q_2(x)$ también.

En cuanto a la unicidad, consideremos dos descomposiciones de un polinomio no nulo ni invertible $p(x) \in A[x]$ en producto de polinomios irreducibles en $A[x]$:

$$p(x) = p_1 \cdots p_r p_1(x) \cdots p_s(x) = q_1 \cdots q_m q_1(x) \cdots q_n(x)$$

donde $p_i, q_j \in A$, $\operatorname{gr} p_i(x), \operatorname{gr} q_j(x) \geq 1$. Como $\Sigma[x]$ es un anillo euclídeo, los polinomios $p_i(x)$ y $q_j(x)$ son irreducibles en $\Sigma[x]$, y los polinomios constantes $p_1, \ldots, p_r, q_1, \ldots, q_m$ son invertibles en $\Sigma[x]$, se sigue que $s = n$ y, reordenando los factores si fuera preciso, que $q_i(x) = (a_i/b_i)p_i(x)$, para ciertos $a_i, b_i \in A$ que podemos suponer sin factores irreducibles comunes en A. Luego $b_i q_i(x) = a_i p_i(x)$ y, si b_i tuviera algún factor irreducible p, entonces a_i no sería múltiplo de p y, por 5.4.1, p dividiría a $p_i(x)$, contra el hecho de que $p_i(x)$ es irreducible en $A[x]$. Igualmente se prueba que a_i no tiene factores irreducibles. Es decir, a_i y b_i son invertibles en A. Luego $p_i(x)$ y $q_i(x)$ difieren en un invertible de $A[x]$ y $p_1 \cdots p_r = (uq_1) \cdots q_m$, donde $u \in A$ es invertible. Como A es un dominio de factorización única, se sigue que $r = m$ y que, salvo el orden e invertibles, $p_1, \ldots, p_r$ coinciden con $q_1, \ldots, q_m$. Se concluye que las descomposiciones iniciales coinciden salvo el orden e invertibles de $A[x]$.

Corolario 5.4.4 *Si k es un cuerpo, los anillos de polinomios $k[x_1, \ldots, x_n]$ son dominios de factorización única.*

Los anillos $\mathbb{Z}[x_1, \ldots, x_n]$ son dominios de factorización única.

Corolario 5.4.5 *Si dos polinomios $p(x, y)$, $q(x, y)$ con coeficientes en un cuerpo k no tienen factores comunes no constantes, entonces el sistema*

$$\left.\begin{array}{l} p(x,y) = 0 \\ q(x,y) = 0 \end{array}\right\}$$

tiene un número finito de soluciones en k.

Demostración: Por hipótesis ambos polinomios no tienen factores irreducibles comunes en el anillo $k[x, y]$ y, en virtud del lema de Gauss, tampoco tienen factores comunes no constantes en el anillo $k(y)[x]$; luego su resultante $r(y)$ no es nula. El teorema 4.5.3 afirma que las ordenadas de las soluciones en k del sistema son raíces de $r(y)$, que tiene un número finito de raíces en k.

Análogamente la resultante $\bar{r}(x)$ no es nula y concluimos que sólo hay un número finito de abscisas de soluciones en k del sistema. Luego el sistema tiene un número finito de soluciones en k.

5.5 Polinomios Irreducibles

Sea $q(x)$ un polinomio no constante con coeficientes racionales. Existe $a \in \mathbb{Z}$ tal que $aq(x) \in \mathbb{Z}[x]$ y, si b es el máximo común divisor de los coeficientes de $aq(x)$, entonces los coeficientes de $p(x) = aq(x)/b$ son enteros y carecen de factores primos comunes. En virtud del Lema de Gauss, $q(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si $p(x)$ es irreducible en $\mathbb{Z}[x]$. Además, si $p(x) = p_1(x) \cdots p_r(x)$ es la descomposición

de $p(x)$ en producto de polinomios irreducibles en $\mathbb{Z}[x]$, cada factor $p_i(x)$ es irreducible en $\mathbb{Q}[x]$, así que $q(x) = (bp_1(x)/a)\cdots p_r(x)$ es la descomposición de $q(x)$ en producto de polinomios irreducibles en $\mathbb{Q}[x]$. Por tanto, podemos reducirnos a estudiar la irreducibilidad en $\mathbb{Z}[x]$ de los polinomios con coeficientes enteros.

Sea $q(x) = \sum_i a_i x^i$ un polinomio con coeficientes en un anillo A. Si $f\colon A \to B$ es un morfismo de anillos, entonces $\bar{q}(x) = \sum_i f(a_i)x^i$ es un polinomio con coeficientes en B. Obtenemos así un morfismo de anillos $A[x] \to B[x]$, $q(x) \mapsto \bar{q}(x)$. Nótese que el grado de $\bar{q}(x)$ nunca puede ser mayor que el grado de $q(x)$. Por ejemplo, cuando p es un número primo y

$$f\colon \mathbb{Z} \to \mathbb{F}_p\ , \quad f(a) = \bar{a} = [a]_p$$

es la proyección canónica, $\bar{q}(x) = \sum_i \bar{a}_i x^i$ es la **reducción** del polinomio $q(x)$ módulo p.

Cuando k es un cuerpo y $f\colon k[y] \to k$, $f\big(c(y)\big) = c(\alpha)$, es el morfismo definido por un elemento $\alpha \in k$, el correspondiente morfismo es

$$\begin{gathered} k[x,y] \longrightarrow k[x] \\ q(x,y) = \textstyle\sum_i a_i(y)x^i \ \mapsto\ \bar{q}(x) = q(x,\alpha) = \sum_i a_i(\alpha)x^i \end{gathered}$$

Criterio de Reducción: *Sea $f\colon A \to B$ un morfismo entre anillos íntegros y sea $q(x)$ un polinomio con coeficientes en A tal que el grado de $\bar{q}(x)$ coincida con el grado de $q(x)$. Si $q(x)$ tiene un factor de grado d en $A[x]$, entonces $\bar{q}(x)$ tiene un factor de grado d en $B[x]$.*

En particular, si los coeficientes de $q(x)$ no tienen factores propios comunes en A y $\bar{q}(x)$ es irreducible en $B[x]$, entonces $q(x)$ es irreducible en $A[x]$.

Demostración: Si $q(x) = p(x)r(x)$, donde $p(x), r(x) \in A[x]$, entonces $\bar{q}(x) = \bar{p}(x)\bar{r}(x)$ y $\operatorname{gr}\bar{p}(x) \le \operatorname{gr} p(x)$, $\operatorname{gr}\bar{r}(x) \le \operatorname{gr} r(x)$. Como

$$\operatorname{gr}\bar{p}(x) + \operatorname{gr}\bar{r}(x) = \operatorname{gr}\bar{q}(x) = \operatorname{gr}\bar{q}(x) = \operatorname{gr} p(x) + \operatorname{gr} r(x)$$

concluimos que $\operatorname{gr}\bar{p}(x) = \operatorname{gr} p(x)$ y $\operatorname{gr}\bar{r}(x) = \operatorname{gr} r(x)$. Por último, si $\bar{q}(x)$ es irreducible, entonces $\bar{p}(x)$ ó $\bar{r}(x)$ es invertible en $B[x]$; y por tanto de grado 0. Luego $p(x)$ ó $r(x)$ es de grado 0, e invertible en A, porque los coeficientes de $q(x)$ no tienen factores propios comunes.

Corolario 5.5.1 *Sea $q(x) = c_0x^n + \ldots$ un polinomio con coeficientes enteros y sea p un primo que no divida a c_0. Si la reducción $\bar{c}_0x^n + \ldots$ de $q(x)$ módulo p es irreducible en $\mathbb{F}_p[x]$, entonces $q(x)$ es irreducible en $\mathbb{Q}[x]$.*

Demostración: Consideremos la proyección canónica $\mathbb{Z} \to \mathbb{F}_p$. Por hipótesis $\bar{c}_0 \neq 0$, así que $\operatorname{gr} q(x) = \operatorname{gr}\bar{q}(x)$ y el criterio anterior permite concluir que $q(x)$ no tiene factores de grado $1, \ldots, n-1$ en $\mathbb{Z}[x]$; luego tampoco en $\mathbb{Q}[x]$ por el lema de Gauss.

Corolario 5.5.2 *Sea* $q(x,y) = c_0(y)x^n + c_1(y)x^{n-1} + \ldots + c_{n-1}(y)x + c_n(y)$ *un polinomio en dos indeterminadas* x, y *con coeficientes en un cuerpo* k*. Si* $c_0(y), c_1(y), \ldots, c_n(y)$ *no admiten factores comunes no constantes y para algún elemento* α *de* k*, que no sea raíz de* $c_0(y)$*, se tiene que*

$$q(x,\alpha) = c_0(\alpha)x^n + c_1(\alpha)x^{n-1} + \ldots + c_{n-1}(\alpha)x + c_n(\alpha)$$

es irreducible en $k[x]$*, entonces* $q(x,y)$ *es irreducible en* $k[x,y]$*.*

Demostración: Consideremos el morfismo de anillos $f\colon k[y] \to k$, $y \mapsto \alpha$. Por hipótesis $c_0(\alpha) \neq 0$, así que el grado de $q(x,\alpha)$ es n y se concluye al aplicar el criterio de reducción.

Criterio de Eisenstein (1823-1852)**:** *Sea* $q(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ *un polinomio con coeficientes en un dominio de factorización única* A*. Si existe algún elemento irreducible* $p \in A$ *tal que*

1. $c_0, \ldots, c_n$ *no tienen factores irreducibles comunes en* A
2. p *divide a* $c_1, \ldots, c_n$
3. p^2 *no divide a* c_n

entonces $q(x)$ *es irreducible en* $A[x]$*.*

Demostración: Si $q(x)$ no es irreducible en $A[x]$, entonces descompone en producto de dos polinomios no constantes con coeficientes en A

$$q(x) = (a_0 + a_1x + \ldots + a_rx^r)(b_0 + b_1x + \ldots + b_{n-r}x^{n-r})$$

y reduciendo módulo pA obtenemos la siguiente igualdad entre polinomios con coeficientes en el cuerpo de fracciones de A/pA:

$$\bar{c}_0x^n = (\bar{a}_0 + \ldots + \bar{a}_rx^r)(\bar{b}_0 + \ldots + \bar{b}_{n-r}x^{n-r})$$

Como todo divisor de x^n coincide, salvo factores constantes, con una potencia de x, se sigue que los dos factores del segundo miembro son $\bar{a}_rx^r$ y $\bar{b}_{n-r}x^{n-r}$. Luego $\bar{a}_0$ y $\bar{b}_0$ son nulos. Es decir, a_0 y b_0 son múltiplos de p, y por tanto $c_n = a_0b_0$ es múltiplo de p^2, contra la hipótesis de que no lo es.

Corolario 5.5.3 (Gauss 1777-1855) *Si* p *es un número primo, el polinomio*

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1$$

es irreducible en $\mathbb{Q}[x]$*.*

Demostración: $q(x) = x^{p-1} + \ldots + x + 1$ es irreducible en $\mathbb{Z}[x]$ si y sólo si lo es el polinomio $q(x+1)$:

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{i} x^{p-i-1} + \ldots + \binom{p}{p-1}$$

Ahora bien el número combinatorio $\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{1!}$ es múltiplo de p cuando $1 \leq i \leq p-1$ (porque el numerador lo es y el denominador no) y $\binom{p}{p-1} = p$ no es múltiplo de p^2. Luego $q(x+1)$ es irreducible por el criterio de Eisenstein.

Corolario 5.5.4 *Si p es un número primo, entonces $\mathbb{Q}\big(e^{\frac{2\pi i}{p}}\big)$ es una extensión de $\mathbb{Q}$ de grado $p-1$.*

Demostración: El polinomio irreducible $x^{p-1} + \ldots + x + 1$ admite la raíz $e^{\frac{2\pi i}{p}}$ y se concluye al aplicar 4.4.2.

Ejemplo: Los polinomios $x^n - 2$ son irreducibles en $\mathbb{Z}[x]$ por el criterio de Eisenstein ; luego también en $\mathbb{Q}[x]$ de acuerdo con el lema de Gauss. Según 4.4.2, $\mathbb{Q}(\sqrt[n]{2}\,)$ es una extensión de $\mathbb{Q}$ de grado n. Vemos así que $\mathbb{Q}$ admite extensiones finitas de grado arbitrario.

Capítulo 6

Módulos y Álgebras

En los capítulos anteriores hemos visto cómo en cualquier anillo (conmutativo con unidad) puede desarrollarse una teoría de la divisibilidad para ideales, análoga a la clásica teoría de la divisibilidad de números naturales. Unos anillos particularmente importantes son los anillos de polinomios en varias indeterminadas y en este capítulo iniciaremos el estudio sistemático de tales anillos. Veamos primero los conceptos intuitivos e imprecisos que recoge la correspondiente teoría de ideales. Para fijar ideas consideremos el anillo $\mathbb{R}[x,y]$ de las funciones polinómicas sobre un plano real. Cada lugar geométrico del plano define un ideal $\mathfrak{a}$ de $\mathbb{R}[x,y]$: el ideal formado por todos los polinomios que se anulan en la figura dada. Por ejemplo, el ideal de la recta de ecuación $ax+by=c$ está formado por los múltiplos de $ax+by-c$, el ideal de la parábola de ecuación $y=x^2$ es $(y-x^2)$, el ideal de la curva $x^2+y^2=1$ es (x^2+y^2-1) y el ideal del punto $x=a$, $y=b$ es $(x-a,y-b)$. En estos casos, al igual que en el de las restantes figuras estudiadas en Bachillerato, el ideal está generado por las ecuaciones del lugar geométrico considerado. Este ideal es el núcleo del morfismo natural de restricción $\mathbb{R}[x,y] \to A$, donde A denota el anillo de las funciones algebraicas (es decir, de las funciones definidas por algún polinomio) sobre la figura en cuestión. De acuerdo con el teorema de isomorfía, $\mathbb{R}[x,y]/\mathfrak{a} \simeq A$. Nótese que cuando operamos con la ecuación de un lugar geométrico, por ejemplo $x^2+y^2=1$, no queremos decir que el término de la izquierda sea el polinomio 1, pues claramente su grado es 2 y no es constante: la ecuación significa que tal relación es válida en todos los puntos de la circunferencia considerada, que es una igualdad entre funciones reales definidas sobre tal circunferencia, que es una igualdad en el anillo cociente A. En resumen, cada lugar geométrico del plano real define un ideal $\mathfrak{a}$ del anillo $\mathbb{R}[x,y]$, formado por las funciones polinómicas que se anulan en él, y las manipulaciones algebraicas que hacemos con sus ecuaciones tienen plena validez y sentido en el anillo cociente $\mathbb{R}[x,y]/\mathfrak{a}$, que es isomorfo al anillo de las funciones algebraicas definidas sobre

dicho lugar geométrico.

Hemos dado varios ejemplos que pueden considerarse como subconjuntos de $\mathbb{R}^2$, cada uno formado por los puntos en que se anulan ciertos polinomios; pero esta comprensión como subconjuntos no da cuenta de expresiones clásicas como la recta doble $x^2 = 0$, la cónica imaginaria $x^2 + y^2 = -1$, etc. Aunque cause perplejidad pensar qué lugar geométrico del plano real quiere indicarse en tales casos, es obvio cuáles deben ser sus ideales (los ideales (x^2) y $(x^2 + y^2 - 1)$ respectivamente), sus anillos de funciones algebraicas (los anillos $\mathbb{R}[x, y]/(x^2)$ y $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ respectivamente) y las funciones algebraicas definidas sobre dichos lugares geométricos (los elementos de tales anillos).

Si el lugar geométrico de ecuaciones $p_1(x, y) = 0, \ldots, p_r(x, y) = 0$ puede parecer un concepto confuso e impreciso, no así el ideal de los polinomios que se anulan en él, que es el ideal $(p_1, \ldots, p_r)$ de $\mathbb{R}[x, y]$ generado por sus ecuaciones, ni el anillo de funciones algebraicas sobre el mismo, que es el anillo cociente $\mathbb{R}[x, y]/(p_1, \ldots, p_r)$. Además, si entre dos ideales se da una relación de inclusión $(p_1, \ldots, p_r) \subseteq (q_1, \ldots, q_s)$, entonces se tiene

$$\begin{aligned} p_1(x, y) &= a_{11}(x, y)q_1(x, y) + \ldots + a_{1s}(x, y)q_s(x, y) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_r(x, y) &= a_{r1}(x, y)q_1(x, y) + \ldots + a_{rs}(x, y)q_s(x, y) \end{aligned}$$

para ciertos polinomios $a_{ij}(x, y)$, de modo que los polinomios $p_i(x, y)$ se anulan necesariamente donde se anulen todos los polinomios $q_j(x, y)$. Debemos considerar que entre dos lugares geométricos definidos por ecuaciones polinómicas se da una relación de incidencia precisamente cuando entre sus correspondientes ideales se dé la relación inversa. En particular, la coincidencia entre lugares geométricos definidos por ecuaciones polinómicas debe ser equivalente a la de sus ideales, lo que lleva a establecer las siguientes definiciones:

Sea $k[x_1, \ldots, x_n]$ el anillo de polinomios en n indeterminadas con coeficientes en un cuerpo k. Diremos que el ideal $(p_1, \ldots, p_r)$ generado en $k[x_1, \ldots, x_n]$ por unos polinomios $p_1(x_1, \ldots, x_n)$, $\ldots$, $p_r(x_1, \ldots, x_n)$ es el **ideal de la subvariedad** de ecuaciones

$$\left.\begin{array}{c} p_1(x_1, \ldots, x_n) = 0 \\ \ldots\ldots\ldots \\ p_r(x_1, \ldots, x_n) = 0 \end{array}\right\}$$

y diremos que un polinomio $q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ se **anula** en tal subvariedad cuando $q \in (p_1, \ldots, p_r)$. Llamaremos **anillo de funciones algebraicas** sobre dicha subvariedad al anillo cociente

$$k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$$

y diremos que la clase de restos $[q(x_1,\ldots,x_n)]$ es la **función** definida por el polinomio $q(x_1,\ldots,x_n)$ sobre la subvariedad de ecuaciones $p_1=\ldots=p_r=0$, ó bien que es la **restricción** de $q(x_1,\ldots,x-n)$ a tal subvariedad.

Diremos que la subvariedad definida por el ideal $\mathfrak{a}$ **contiene** a la subvariedad definida por el ideal $\mathfrak{b}$ cuando $\mathfrak{a}\subseteq\mathfrak{b}$. Se llama **intersección** de dos subvariedades a la mayor subvariedad contenida en ambas, así que el ideal de la intersección es la suma de los correspondientes ideales. Se llama **unión** de dos subvariedades a la menor subvariedad que las contiene, de modo que el ideal de la unión es la intersección de los correspondientes ideales. Los ideales A y 0 son los ideales de las subvariedades de ecuaciones $1=0$ y $0=0$, que se denominan **vacío** y **espacio afín** n-dimensional sobre k respectivamente. Las subvariedades definidas por una ecuación no constante $p(x_1,\ldots,x_n)=0$ (por un ideal principal $\neq 0$, A) se llaman **hipersuperficies**. Algunas subvariedades de los espacios afines reales merecen un nombre propio:

Subvariedades de la recta afín real

Nombre	**Ideal**	**Anillo**
punto real $x=a$	$(x-a)$	$\simeq\mathbb{R}$
puntos imaginarios conjugados $x=a\pm bi$	$\big(x^2-2ax+(a^2+b^2)\big)$	$\simeq\mathbb{C}$
punto $x=a$ doble	$\big((x-a)^2\big)$	$\simeq\mathbb{R}[\,\varepsilon\,],\ \varepsilon^2=0$
n puntos confundidos en el punto $x=a$	$\big((x-a)^n\big)$	$\simeq\mathbb{R}[\,t\,]/(t^n)$
recta afín	0	$\mathbb{R}[x]$

Subvariedades del plano afín real

punto real (a,b)	$(x-a,y-b)$	$\simeq\mathbb{R}$
dos puntos imaginarios conjugados (α,β), $(\bar\alpha,\bar\beta)$	$\{p(x,y)\colon\ p(\alpha,\beta)=0\}$	$\simeq\mathbb{C}$
recta $ax+by=c$	$(ax+by-c)$	$\simeq\mathbb{R}[\,t\,]$
recta $ax+by=c$ doble	$(ax+by-c)^2$	$\simeq\mathbb{R}[\,\varepsilon\,][\,t\,]$
r-ésimo entorno infinitesimal del punto (a,b)	$(x-a,y-b)^{r+1}$	$\simeq J_2^r$

Nombre	**Ideal**	**Anillo**
parábola $y = ax^2$	$(y - ax^2)$	$\simeq \mathbb{R}[\,t\,]$
hipérbola $xy = 1$	$(xy - 1)$	$\simeq \mathbb{R}[\,t, t^{-1}]$
par de rectas concurrentes $xy = 0$	(xy)	$\mathbb{R}[x, y]/(xy)$
par de rectas imaginarias conjugadas $x^2 + y^2 = 0$	$(y^2 + x^2)$	$\mathbb{R}[x, y]/(y^2 + x^2)$
dos rectas paralelas $y^2 = 1$	$(y^2 - 1)$	$\simeq \mathbb{R}[t] \oplus \mathbb{R}[t]$
dos rectas imaginarias paralelas $y^2 = -1$	$(y^2 + 1)$	$\simeq \mathbb{C}[\,t\,]$

Subvariedades del espacio afín real de dimensión n

punto real $(a_1, \ldots, a_n)$	$(x_1 - a_1, \ldots, x_n - a_n)$	$\simeq \mathbb{R}$
r-ésimo entorno infinitesimal del punto $(a_1, \ldots, a_n)$	$(x_1 - a_1, \ldots, x_n - a_n)^{r+1}$	$\simeq J_n^r$
Subvariedad lineal $\sum_{j=1}^{n} a_{ij}x_j = 0\,,\ 1 \leq i \leq m$	$\left(\sum_i a_{ij}x_j\right)_{1\leq i\leq m}$	$\mathbb{R}[\,t_1, \ldots, t_d\,]$

donde $J_n^r = \mathbb{R}[t_1, \ldots, t_n]/(t_1, \ldots, t_n)^{r+1}$ es el anillo de los desarrollos de Taylor de orden r en n variables. En resumen, el estudio de los lugares geométricos definidos por la anulación de polinomios en el espacio afín coincide con la teoría de ideales en los anillos de polinomios.

Si $\mathfrak{a}$ es un ideal de un anillo A, es un grupo conmutativo respecto de la suma de A y el producto de A define una aplicación $A \times \mathfrak{a} \to \mathfrak{a}$ que verifica todos los axiomas de espacio vectorial, salvo la condición de que los escalares formen un cuerpo; lo que resumiremos diciendo que es un A-módulo. En este capítulo iniciaremos el estudio de la estructura de módulo sobre un anillo A y veremos que casi todas las definiciones del Álgebra Lineal (aplicaciones lineales y multilineales, submódulos, cocientes, dual, sumas y productos directos, etc.) pueden generalizarse para los A-módulos; aunque la frecuente existencia de módulos que no admiten bases introduzca grandes modificaciones en las hipótesis de los teoremas. La posibilidad de

efectuar muchas operaciones (cocientes, sumas directas, duales, etc.) que carecen de sentido en los ideales hace que la teoría de módulos sea mucho más flexible y natural, por lo que es preferible estudiar los ideales dentro del contexto más general de los módulos. Esta generalidad no complica las demostraciones, sino que la posibilidad de usar las operaciones básicas del Álgebra Lineal las aclara y simplifica. Los módulos son los "espacios vectoriales sobre un anillo de escalares" y en ellos es válida todo el Álgebra Lineal en que no se utilice la propiedad de que todo escalar no nulo es invertible. Puede decirse que valen las definiciones y no los teoremas (existencia de suplementario, bases, etc.); pero lo importante en una teoría, más que los resultados, son las preguntas, aquello de lo que podemos hablar.

6.1 Módulos

Axiomas de Módulo: Sea A un anillo (conmutativo y con unidad) y sea $(M,+)$ un grupo conmutativo. Diremos que una $A\times M \xrightarrow{\cdot} M$ define en M una estructura de A**-módulo** cuando

Axioma 1: $a\cdot(m+n) = a\cdot m + a\cdot n$

Axioma 2: $(a+b)\cdot m = a\cdot m + b\cdot m$

Axioma 3: $(ab)\cdot m = a\cdot(b\cdot m)$

Axioma 4: $1\cdot m = m$

Es decir, dada una aplicación $A\times M\to M$, cada elemento $a\in A$ define una aplicación $a\cdot\colon M\to M$ y el primer axioma expresa que $a\cdot$ es morfismo de grupos. Los tres últimos axiomas expresan que la aplicación $\phi\colon A\to \mathrm{End}(M)$, $\phi(a) = a\cdot$, es morfismo de anillos. Recíprocamente, si M es un grupo abeliano, cada morfismo de anillos $\phi\colon A\to\mathrm{End}(M)$ define una estructura de A-módulo en M tal que $a\cdot m = \phi(a)(m)$. Resumiendo, dar una estructura de A-módulo en un grupo abeliano M es dar un morfismo de anillos de A en el anillo (no conmutativo en general) de los endomorfismos del grupo M. *Los A-módulos son las representaciones de A como anillo de endomorfismos de un grupo abeliano.*

Ejemplos:

1. Todo ideal $\mathfrak{a}$ de un anillo A es estable por el producto por elementos de A, así que el producto de A define en $\mathfrak{a}$ una estructura de A-módulo. En particular, el propio anillo A y el ideal 0 son A-módulos.

2. Sea $\{M_i\}_{i\in I}$ una familia de A-módulos con índices en un conjunto I. Su **producto directo** se denotará $\prod_{i\in I} M_i$, mientras que $\bigoplus_{i\in I} M_i$ denotará el subgrupo de $\prod_{i\in I} M_i$ formado por los elementos (m_i) que tienen todas sus

componentes m_i nulas salvo un número finito y se llamará **suma directa** de tal familia (nótese que $\bigoplus_i M_i = \prod_i M_i$ cuando el conjunto de índices es finito). Tanto la suma directa $\bigoplus_i M_i$ como el producto directo $\prod_i M_i$ son A-módulos con el siguiente producto por elementos de A:

$$a \cdot (m_i)_{i\in I} \;=\; (am_i)_{i\in I}$$

Si todos los módulos M_i son iguales a cierto módulo M, el producto directo $\prod_i M_i$ se denota M^I y la suma directa $\bigoplus_i M_i$ se denota $M^{(I)}$. Cuando el conjunto I es finito y de cardinal n, ambos módulos coinciden y se denotan M^n.

En el caso particular $M = A$, cada elemento $x \in I$ define canónicamente un elemento de $A^{(I)}$: aquél cuyas componentes son todas nulas, excepto la correspondiente a x, que es la unidad. Ahora todo elemento de $A^{(I)}$ descompone, y de modo único, como una suma finita $a_1x_1 + \ldots + a_nx_n$, donde $x_i \in I$, $a_i \in A$. Es decir, $A^{(I)}$ es el módulo de las combinaciones lineales finitas de elementos de I con coeficientes en el anillo A.

Definición: Diremos que una aplicación $f\colon M \to N$ entre dos A-módulos es un **morfismo** de A-módulos cuando sea un morfismo de grupos y conserve el producto por elementos de A:

$$f(m + m') = f(m) + f(m')$$
$$f(a \cdot m) = a \cdot f(m)$$

Diremos que un morfismo de A-módulos $f\colon M \to N$ es un **isomorfismo** de A-módulos si existe algún morfismo de A-módulos $h\colon N \to M$ tal que $f \circ h = Id_N$ y $h \circ f = Id_M$.

La composición de morfismos de A-módulos también es morfismo de A-módulos, la identidad siempre es morfismo de A-módulos, y los isomorfismos de A-módulos son los morfismos biyectivos.

El conjunto de los morfismos de A-módulos de M en N se denota $\mathrm{Hom}_A(M, N)$. Si $f, h\colon M \to N$ son dos morfismos de A-módulos, su suma $f + h$, que es la aplicación

$$(f + h)(m) := f(m) + h(m)$$

también es morfismo de A-módulos, y el producto af por cualquier elemento $a \in A$, que es la aplicación

$$(af)(m) := a\big(f(m)\big)$$

también es morfismo de A-módulos.

Con estas operaciones, $\mathrm{Hom}_A(M, N)$ tiene estructura de A-módulo.

Sea $f\colon M' \to M$ un morfismo de A-módulos y N un A-módulo. La composición con f induce aplicaciones

$$f_*\colon \mathrm{Hom}_A(N, M') \longrightarrow \mathrm{Hom}_A(N, M)\ , \quad f_*(h) := f \circ h$$
$$f^*\colon \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M', N)\ , \quad f^*(h) := h \circ f$$

que son morfismos de A-módulos. Es claro que f^* y f_* son la identidad cuando f lo es y que se verifica:

$$(fh)_* = (f_*) \circ (h_*) \qquad , \qquad (af + bh)_* = a(f_*) + b(h_*)$$
$$(fh)^* = (h^*) \circ (f^*) \qquad , \qquad (af + bh)^* = a(f^*) + b(h^*)$$

Ejemplos:

1. Sea $\{m_i\}_{i\in I}$ una familia de elementos de un A-módulo M. Tal familia define un morfismo de A-módulos $f\colon A^{(I)} \to M$

$$f\big((a_i)_{i\in I}\big) := \sum_{i\in I} a_i m_i$$

Recíprocamente, si $f\colon A^{(I)} \to M$ es un morfismo de A-módulos, tenemos que

$$f\big((a_i)_{i\in I}\big) = f\Big(\sum_{i\in I} a_i e_i\Big) = \sum_{i\in I} a_i f(e_i)$$

donde e_i denota el elemento de $A^{(I)}$ que tiene todas sus componentes nulas salvo la i-ésima, que es la unidad. Luego f es el morfismo correspondiente a la familia $\{f(e_i)\}_{i\in I}$ de elementos de M. Obtenemos así un isomorfismo natural de A-módulos:

$$\mathrm{Hom}_A(A^{(I)}, M) \;=\; M^I$$

2. **Propiedad Universal de la Suma Directa:** Sea $\bigoplus_i M_i$ la suma directa de una familia $\{M_i\}_{i\in I}$ de A-módulos. Para cada índice $j \in I$ tenemos una inclusión canónica

$$u_j\colon M_j \longrightarrow \bigoplus_i M_i$$

que es morfismo de A-módulos. Por tanto, si $f\colon \bigoplus_i M_i \to N$ es un morfismo de A-módulos, para cada índice $j \in I$ tenemos un morfismo de A-módulos $f \circ u_j\colon M_j \to N$. Recíprocamente, si tenemos un morfismo de A-módulos $f_j\colon M_j \to N$ para cada índice $j \in I$, la aplicación

$$f\colon \bigoplus_i M_i \longrightarrow N\ , \quad f\big((m_i)_{i\in I}\big) = \textstyle\sum_i f_i(m_i)$$

es un morfismo de A-módulos tal que $f_j = f \circ u_j$. Concluimos así la existencia de una biyección natural que es isomorfismo de A-módulos

$$\mathrm{Hom}_A\Big(\bigoplus_{i\in I} M_i, N\Big) \;=\; \prod_{i\in I} \mathrm{Hom}_A(M_i, N)$$

3. **Propiedad Universal del Producto Directo:** Sea $\prod_i M_i$ el producto directo de una familia $\{M_i\}_{i\in I}$ de A-módulos. Para cada índice $j \in I$ tenemos la proyección canónica

$$\pi_j\colon \textstyle\prod_i M_i \longrightarrow M_j \ , \quad \pi_j((m_i)_{i\in I}) = m_j$$

que es morfismo de A-módulos. Por tanto, si $f\colon N \to \prod_i M_i$ es un morfismo de A-módulos, para cada índice $j \in I$ tenemos un morfismo de A-módulos $\pi_j \circ f\colon N \to M_j$.

Recíprocamente, dado un morfismo de A-módulos $f_j\colon N \to M_j$ para cada índice $j \in I$, la aplicación

$$f\colon N \longrightarrow \textstyle\prod_i M_i \ , \quad f(n) = (f_i(n))_{i\in I}$$

es un morfismo de A-módulos tal que $f_j = \pi_j \circ f$. Concluimos así la existencia de una biyección natural que es isomorfismo de A-módulos

$$\mathrm{Hom}_A\Big(N, \prod_{i\in I} M_i\Big) \ = \ \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$$

Definición: Sea M un A-módulo. Diremos que un subgrupo N de M es un **submódulo** si es estable por el producto por elementos de A; es decir:

$$a \in A,\ m \in N \ \Rightarrow\ am \in N$$

En tal caso N hereda una estructura de A-módulo.

M y 0 son submódulos de M. Además, la intersección de cualquier familia de submódulos de M también es un submódulo de M. Por tanto, dada una familia $\{m_i\}_{i\in I}$ de elementos de M, la intersección de todos los submódulos de M que la contengan es el menor submódulo de M que la contiene y recibe el nombre de submódulo **generado** por tal familia.

La imagen del morfismo $f\colon A^{(I)} \to M,\ f\big((a_i)_{i\in I}\big) = \sum_i a_i m_i$, es un submódulo de M, que claramente es el submódulo generado por la familia $(m_i)_{i\in I}$, y se denotará

$$\sum_{i\in I} Am_i \ = \ \{\textstyle\sum_i a_i m_i\colon \ a_i \in A\}$$

Módulo Cociente

Si N es un submódulo de un A-módulo M, es un subgrupo normal de M. Es sencillo comprobar que en el grupo cociente M/N existe una única estructura de A-módulo tal que la proyección canónica $\pi\colon M \to M/N$, $\pi(m) = [m]$, sea morfismo de A-módulos. Tal estructura viene definida por el producto

$$a \cdot [m] \ = \ [am]$$

La demostración de la propiedad universal del A-módulo cociente M/N, y la del correspondiente teorema de isomorfía, es similar a la dada para morfismos de grupos y anillos:

Propiedad Universal: *Sea N un submódulo de un A-módulo M y $\pi\colon M \to M/N$ la proyección canónica. Para todo A-módulo M' se verifica que el morfismo*

$$\pi^* \,:\, \mathrm{Hom}_A(M/N, M') \longrightarrow \mathrm{Hom}_A(M, M')$$

es inyectivo, y su imagen está formada por los morfismos que se anulan en N.

Teorema de Isomorfía: *Sea $f\colon M \to N$ un morfismo de A-módulos. La aplicación $\phi\colon M/\mathrm{Ker}\, f \to \mathrm{Im}\, f$, $\phi([m]) = f(m)$, es un isomorfismo de A-módulos.*

Definición: Sea m un elemento de un A-módulo M. Llamaremos **anulador** de m al ideal $\mathrm{Ann}(m) = \{a \in A\colon\ am = 0\}$, que es el núcleo del morfismo $\cdot m\colon A \to M$. De acuerdo con el teorema de isomorfía

$$A/\mathrm{Ann}(m) \,\simeq\, Am$$

Llamaremos **anulador** de un A-módulo M a la intersección de los anuladores de sus elementos:

$$\mathrm{Ann}(M) = \{a \in A\colon\ aM = 0\,\}$$

Si un ideal $\mathfrak{a}$ está contenido en el anulador de M, tenemos en M una estructura de $A/\mathfrak{a}$-módulo, definida por el producto $[a]\cdot m = am$.

Teorema 6.1.1 *Sea M un A-módulo y sea $\pi\colon M \to M/N$ la proyección canónica en el cociente por un submódulo N. Si $\bar{P}$ es un submódulo de M/N, entonces $\pi^{-1}(\bar{P})$ es un submódulo de M que contiene a N. Tenemos así una biyección que conserva inclusiones*

$$\begin{bmatrix}\text{Submódulos}\\ \text{de } M/N\end{bmatrix} \;=\; \begin{bmatrix}\text{Submódulos de } M\\ \text{que contienen a } N\end{bmatrix}$$

Demostración: Es claro que $\pi^{-1}(\bar{P})$ es un submódulo de M que contiene a $\mathrm{Ker}\,\pi = N$ y que $\pi^{-1}(\bar{P}_1) \subseteq \pi^{-1}(\bar{P}_2)$ cuando $\bar{P}_1 \subseteq \bar{P}_2$. Por tanto, basta probar que la aplicación así obtenida del conjunto de los submódulos de M/N en el de los submódulos de M que contienen a N es biyectiva. La aplicación inversa asigna a cada submódulo P de M que contenga a N el submódulo $\pi(P)$ de M/N. En efecto:

Si un submódulo P de M contiene a N, entonces

$$P \subseteq \pi^{-1}\big(\pi(P)\big) \subseteq P + N \subseteq P$$

y $P = \pi^{-1}\big(\pi(P)\big)$. Recíprocamente, si $\bar{P}$ es un submódulo de M/N, entonces $\pi\big(\pi^{-1}(\bar{P})\big) \subseteq \bar{P}$ y se da la igualdad porque π es epiyectivo.

Corolario 6.1.2 *Sea $\mathfrak{a}$ un ideal de un anillo A y sea $\bar{A} = A/\mathfrak{a}$. La proyección canónica $\pi\colon A \to \bar{A}$ establece una correspondencia biyectiva, que conserva inclusiones, entre los ideales de $\bar{A}$ y los ideales de A que contienen a $\mathfrak{a}$. Además, si $\bar{\mathfrak{b}}$ es el ideal de $\bar{A}$ correspondiente a un ideal $\mathfrak{b} \supseteq \mathfrak{a}$, entonces*

$$A/\mathfrak{b} \simeq \bar{A}/\bar{\mathfrak{b}}$$

En particular, ideales primos se corresponden con ideales primos e ideales maximales con ideales maximales.

Demostración: La primera parte es consecuencia del teorema anterior, pues los submódulos del A-módulo $A/\mathfrak{a}$ son sus ideales.

En cuanto al isomorfismo $A/\mathfrak{b} \simeq \bar{A}/\bar{\mathfrak{b}}$, el morfismo de anillos natural $A \to \bar{A}/\bar{\mathfrak{b}}$ es epiyectivo y su núcleo es precisamente el ideal $\mathfrak{b} = \pi^{-1}(\bar{\mathfrak{b}})$. Concluimos al aplicar el teorema de isomorfía para morfismos de anillos.

Teorema 6.1.3 *Todo anillo no nulo tiene algún ideal maximal.*

Demostración: Sea A un anillo y sea X el conjunto de sus ideales distintos de A, ordenado por inclusión. Si $\{\mathfrak{a}_i\}_{i\in I}$ es una cadena de elementos de X, entonces $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$ es claramente un ideal $\neq A$ que contiene a todos los ideales $\mathfrak{a}_i$. Es decir, toda cadena de X admite una cota superior. Si $A \neq 0$, entonces X no es vacío y el lema de Zorn afirma que X tiene algún elemento maximal, que es un ideal maximal de A.

Teorema 6.1.4 *Sea $\mathfrak{a}$ un ideal de un anillo A. Si $\mathfrak{a} \neq A$, entonces $\mathfrak{a}$ está contenido en algún ideal maximal de A.*

Demostración: Si $\mathfrak{a} \neq A$, entonces $A/\mathfrak{a} \neq 0$ y, por 6.1.3, el anillo $A/\mathfrak{a}$ tiene algún ideal maximal que, según 6.1.2, se corresponde con un ideal maximal de A que contiene a $\mathfrak{a}$.

Corolario 6.1.5 *La condición necesaria y suficiente para que un elemento de un anillo A sea invertible es que no pertenezca a ningún ideal maximal de A.*

Demostración: Sea f un elemento de un anillo A. Si f pertenece a un ideal maximal, claramente no puede ser invertible en A. Recíprocamente, si f no es invertible en A, entonces $fA \neq A$ y, según 6.1.4, el ideal fA está contenido en algún ideal maximal de A.

Corolario 6.1.6 *La condición necesaria y suficiente para que un sistema de ecuaciones con coeficientes en un cuerpo k*

$$\left.\begin{aligned} p_1(x_1,\dots,x_n) &= 0 \\ &\cdots\cdots\cdots \\ p_r(x_1,\dots,x_n) &= 0 \end{aligned}\right\}$$

no admita soluciones en ninguna extensión de k (i.e., que sea incompatible), es que existan polinomios $q_1, \ldots, q_r \in k[x_1, \ldots, x_n]$ tales que

$$1 = q_1(x_1, \ldots, x_n)p_1(x_1, \ldots, x_n) + \ldots + q_r(x_1, \ldots, x_n)p_r(x_1, \ldots, x_n)$$

Demostración: La condición es evidentemente suficiente.

En cuanto a la necesidad, si el ideal $(p_1, \ldots, p_r)$ no contiene a la unidad, el anillo $A = k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$ no es nulo y, por 6.1.3, ha de tener algún ideal maximal $\mathfrak{m}$. Luego $A/\mathfrak{m}$ es una extensión de k y las clases de restos $\bar{x}_i \in A/\mathfrak{m}$ son una solución del sistema en tal extensión.

Módulos Libres

Sea $\{m_i\}_{i\in I}$ una familia de elementos de un A-módulo M. Diremos que forman un **sistema de generadores** de M cuando $M = \sum_i Am_i$; es decir, cuando el correspondiente morfismo $\phi\colon A^{(I)} \to M$ sea epiyectivo. Diremos que forman una **base** de M cuando ϕ sea un isomorfismo; es decir, cuando cada elemento de M descomponga, y de modo único, como combinación lineal con coeficientes en A de los elementos $\{m_i\}_{i\in I}$.

Todo módulo admite sistemas de generadores (la familia formada por todos sus elementos, etc.); pero existen módulos que no tienen ninguna base. Por ejemplo, ningún grupo abeliano finito no nulo tiene bases.

Definición: Diremos que un A-módulo es de **tipo finito** si admite algún sistema finito de generadores; es decir, si es isomorfo a un cociente de alguna suma directa finita A^n.

Definición: Diremos que un A-módulo es **libre** si admite alguna base; es decir, si es isomorfo a alguna suma directa $A^{(I)}$. Cuando $A \neq 0$, veremos a continuación que todas las bases de un A-módulo libre L tienen el mismo cardinal, que se llamará **rango** de L.

Lema 6.1.7 *Sea A un anillo no nulo. Si existe algún morfismo epiyectivo de A-módulos $A^{(I)} \to A^{(J)}$, entonces el cardinal de I es mayor o igual que el cardinal de J. En particular todas las bases de un A-módulo libre tienen igual cardinal.*

Demostración: Sea $\mathfrak{m}$ un ideal maximal de A y $k = A/\mathfrak{m}$ su cuerpo residual. Nótese que $\mathfrak{m} \cdot A^{(I)} = \mathfrak{m}^{(I)}$ y que $A^{(I)}/\mathfrak{m}A^{(I)} \simeq (A/\mathfrak{m})^{(I)} = k^{(I)}$. Si algún morfismo de A-módulos $\varphi\colon A^{(I)} \to A^{(J)}$ es epiyectivo, también lo será el morfismo $\bar{\varphi}\colon A^{(I)}/\mathfrak{m}A^{(I)} \to A^{(J)}/\mathfrak{m}A^{(J)}$, $\bar{\varphi}([m]) = [\varphi(m)]$. Como $\bar{\varphi}$ es k-lineal, el cardinal de J no puede superar al cardinal de I.

6.2 Sucesiones Exactas

Definición: Diremos que una sucesión de morfismos de A-módulos

$$\ldots \longrightarrow M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \longrightarrow \ldots$$

es **exacta** cuando $\operatorname{Im} f_n = \operatorname{Ker} f_{n+1}$ para todo índice n.

Teorema 6.2.1 *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ sea exacta es que para todo A-módulo N sea exacta la sucesión*

$$0 \longrightarrow \operatorname{Hom}_A(M'', N) \xrightarrow{p^*} \operatorname{Hom}_A(M, N) \xrightarrow{i^*} \operatorname{Hom}_A(M', N)$$

Demostración: Supongamos que $\operatorname{Im} i = \operatorname{Ker} p$ y que p es epiyectivo.

Si $f \in \operatorname{Hom}_A(M'', N)$ y $fp = 0$, entonces f se anula en $\operatorname{Im} p = M''$; luego $f = 0$, lo que muestra que p^* es inyectivo. Como $pi = 0$, se sigue que $0 = (pi)^* = i^*p^*$; luego $\operatorname{Im} p^* \subseteq \operatorname{Ker} i^*$. Por último, si $h \in \operatorname{Ker} i^*$, entonces el morfismo $h\colon M \to N$ se anula en $\operatorname{Im} i = \operatorname{Ker} p$, así que h factoriza a través de la proyección canónica $\pi\colon M \to M/\operatorname{Ker} p \simeq M''$ de acuerdo con la propiedad universal del cociente. Es decir, $h\operatorname{Im} p^*$.

Veamos que la condición es suficiente. Como p^* es inyectivo cuando $N = M''/\operatorname{Im} p$, se sigue que la proyección canónica $\pi\colon M'' \to N$ es nula; es decir, $\operatorname{Im} p = M''$ y p es epiyectivo. Además, la condición $i^*p^* = (pi)^* = 0$ implica que $pi = (pi)^*(Id) = 0$; luego $\operatorname{Im} i \subseteq \operatorname{Ker} p$. Por último, si $N = M/\operatorname{Im} i$ y $\pi\colon M \to N$ es la proyección canónica, tenemos que $i^*(\pi) = 0$. Luego existe algún morfismo $f\colon M'' \to N$ tal que $\pi = p^*(f) = f \circ p$ y concluimos que $\operatorname{Ker} p \subseteq \operatorname{Ker} \pi = \operatorname{Im} i$.

Corolario 6.2.2 *La condición necesaria y suficiente para que un morfismo de A-módulos $f\colon M \to M''$ sea un isomorfismo es que lo sea el morfismo*

$$f^*\colon \operatorname{Hom}_A(M'', N) \to \operatorname{Hom}_A(M, N)$$

para todo A-módulo N.

Demostración: Un morfismo de A-módulos $g\colon M_1 \to M_2$ es isomorfismo precisamente cuando es exacta la sucesión $0 \to M_1 \xrightarrow{g} M_2 \to 0$.

Teorema 6.2.3 *La condición necesaria y suficiente para que una sucesión de morfismos de A-módulos $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ sea exacta es que para todo A-módulo N sea exacta la sucesión*

$$0 \longrightarrow \operatorname{Hom}_A(N, M') \xrightarrow{i_*} \operatorname{Hom}_A(N, M) \xrightarrow{p_*} \operatorname{Hom}_A(N, M'')$$

Demostración: Es sencillo comprobar la necesidad de la condición. En cuanto a la suficiencia, basta tomar $N = A$, pues para todo A-módulo M tenemos un isomorfismo natural $M = \mathrm{Hom}_A(A, M)$ y, mediante estos isomorfismos, cada morfismo f se corresponde con f_*.

Teorema 6.2.4 *Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta de morfismos de A-módulos. Las siguientes condiciones son equivalentes:*

1. *Existe un morfismo de A-módulos $s\colon M'' \to M$ tal que $p \circ s = Id_{M''}$.*
2. *Existe un morfismo de A-módulos $r\colon M \to M'$ tal que $r \circ i = Id_{M'}$.*
3. *$\mathrm{Hom}_A(N, M) \xrightarrow{p_*} \mathrm{Hom}_A(N, M'')$ es epiyectivo para todo A-módulo N.*
4. *$\mathrm{Hom}_A(M, N) \xrightarrow{i^*} \mathrm{Hom}_A(M', N)$ es epiyectivo para todo A-módulo N.*

Además, si se verifican estas condiciones, M es isomorfo a $M' \oplus M''$.

Demostración: $(1 \Rightarrow 3)$ Porque $p_* s_* = (ps)_* = Id$.

$(3 \Rightarrow 1)$ Basta tomar $N = M''$ y considerar la identidad de M''.

$(2 \Rightarrow 4)$ Porque $i^* r^* = (ri)^* = Id$.

$(4 \Rightarrow 2)$ Basta tomar $N = M'$ y considerar la identidad de M'.

$(1 \Rightarrow 2)$ Basta ver que $\pi i\colon M' \to M/\mathrm{Im}\, s$ es un isomorfismo, pues si ϕ es su inverso y ponemos $r = \phi\pi$, tenemos que $ri = \phi\pi i = Id_{M'}$. Ahora bien, πi es inyectivo porque $(\mathrm{Im}\, i) \cap (\mathrm{Im}\, s) = (\mathrm{Ker}\, p) \cap (\mathrm{Im}\, s) = 0$, y es epiyectivo porque, si $m \in M$, entonces $m - sp(m) \in \mathrm{Ker}\, p = \mathrm{Im}\, i$ y $[m] = [m - sp(m)] = [i(m')]$.

$(2 \Rightarrow 1)$ Tenemos que $(\mathrm{Ker}\, r) \cap (\mathrm{Ker}\, p) = (\mathrm{Ker}\, r) \cap (\mathrm{Im}\, i) = 0$, y que $M = (\mathrm{Ker}\, r) + (\mathrm{Ker}\, p)$, pues si $m \in M$, entonces $m - ir(m) \in \mathrm{Ker}\, r$. Luego $M = (\mathrm{Ker}\, r) \oplus (\mathrm{Ker}\, p)$; así que $p\colon \mathrm{Ker}\, r \to M''$ es un isomorfismo y su inverso define un morfismo $s\colon M'' \to M$ tal que $ps = Id_{M''}$. Además, $M = (\mathrm{Im}\, i) \oplus (\mathrm{Ker}\, r) \simeq M' \oplus M''$.

Definición: Las sucesiones exactas $0 \to M' \to M \to M'' \to 0$ se llaman sucesiones exactas **cortas**. Diremos que una sucesión sucesión exacta corta **escinde** o **rompe** si verifica las condiciones equivalentes del teorema anterior. En tal caso $M \simeq M' \oplus M''$.

Corolario 6.2.5 *Sea k un cuerpo. Toda sucesión exacta corta de aplicaciones k-lineales escinde.*

Demostración: Sea $p\colon E \to F$ una aplicación lineal epiyectiva entre dos k-espacios vectoriales y sea V un subespacio suplementario en E del núcleo de p. La aplicación $p\colon V \to F$ es un isomorfismo y su inverso define una aplicación lineal $s\colon F \to E$ tal que $ps = Id_F$; luego todas las sucesiones exactas cortas satisfacen la primera condición del teorema anterior.

Longitud de un Módulo

Definición: Diremos que un A-módulo $M \neq 0$ es **simple** cuando sus únicos submódulos son los triviales: 0 y M.

Sea M un A-módulo simple. El morfismo $A \to M$ definido por cualquier elemento no nulo de M es epiyectivo, pues su imagen es un submódulo no nulo. Luego $M \simeq A/\mathfrak{a}$ para algún ideal $\mathfrak{a}$ y, de 6.1.2, se sigue que los únicos ideales de A que contienen a $\mathfrak{a}$ son $\mathfrak{a}$ y A. Concluimos que *los A-módulos simples son precisamente los cocientes de A por sus ideales maximales.*

Definición: Sea M un A-módulo. Diremos que una cadena de submódulos

$$0 = M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n = M$$

es una **serie de composición** de M si los cocientes sucesivos M_i/M_{i-1}, $1 \leq i \leq n$, son A-módulos simples; es decir, cuando no pueda refinarse de modo que la sucesión obtenida siga siendo estrictamente creciente. Diremos que un A-módulo M tiene **longitud finita** si admite alguna serie de composición, en cuyo caso todas las series de composición de M tienen igual longitud (número de inclusiones estrictas); longitud común que se llamará **longitud** de M y se denotará $l_A(M)$ ó $l(M)$:

Teorema 6.2.6 *Todas las series de composición de un A-módulo M tienen igual longitud.*

Demostración: Sea $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$ una serie de composición de longitud mínima n. Procederemos por inducción sobre n; pues M es simple cuando $n = 1$, y el teorema es obvio para módulos simples.

Si $0 = M'_0 \subset M'_1 \subset \ldots \subset M'_r = M$ es otra serie de composición, consideramos la proyección canónica $\pi\colon M \to M/M_1$ y pondremos $\bar{N} = \pi(N)$ para todo submódulo N de M, de modo que $0 = \bar{M}_1 \subset \ldots \subset \bar{M}_n = \bar{M}$ es una serie de composición de $\bar{M}$ de longitud $n-1$, y $0 = \bar{M}'_0 \subseteq \bar{M}'_1 \subseteq \ldots \subseteq \bar{M}'_r = \bar{M}$ es otra serie de composición de $\bar{M}$, después de eliminar las repeticiones.

Ahora bien, si $\bar{M}'_i = \bar{M}'_{i+1}$, entonces $M'_i \cap M_1 \subset M'_{i+1} \cap M_1$. Como M_1 es simple, tal cosa sólo ocurre cuando $M'_i \cap M_1 = 0$ y $M_1 \subset M'_{i+1}$. Luego sólo se da una repetición, y los submódulos $\bar{M}_i$ definen una serie de composición de $\bar{M}$ de longitud $r-1$. Por hipótesis de inducción concluimos que $n - 1 = r - 1$. q.e.d.

En el caso particular de los espacios vectoriales sobre un cuerpo k, el concepto de longitud coincide con el de dimensión: $l_k(E) = \dim_k E$. Las demostraciones de muchas propiedades de la dimensión de los espacios vectoriales de dimensión finita permanecen válidas en el contexto más general de los módulos de longitud finita. Así:

1) Sea M un A-módulo de longitud finita. Toda sucesión estrictamente creciente de submódulos de M puede completarse hasta obtener una serie de composición de M. Además, si N es un submódulo de M, entonces N tiene longitud finita y $l(N) \leq l(M)$, dándose la igualdad únicamente cuando $N = M$.

2) *La longitud es aditiva* en el siguiente sentido: dada cualquier sucesión exacta corta $0 \to M' \to M \to M'' \to 0$, la condición necesaria y suficiente para que la longitud de M sea finita es que lo sean las longitudes de M' y M'', en cuyo caso

$$l(M) \;=\; l(M') + l(M'') \;.$$

6.3 Producto Tensorial

Sean M y N dos A-módulos. Si P es un A-módulo, diremos que una aplicación $f\colon M \times N \to P$ es **A-bilineal** cuando

$$\begin{aligned} f(m+m',n) &= f(m,n) + f(m',n) \\ f(m,n+n') &= f(m,n) + f(m,n') \\ f(am,n) &= a \cdot f(m,n) \\ f(m,an) &= a \cdot f(m,n) \end{aligned}$$

El conjunto de todas las aplicaciones A-bilineales de M y N en P se denota $\mathrm{Bil}_A(M,N;P)$ y es un A-módulo con las siguientes operaciones:

$$\begin{aligned} (f+g)(m,n) &= f(m,n) + g(m,n) \\ (a \cdot f)(m,n) &= a \cdot f(m,n) \end{aligned}$$

La condición de que una aplicación $f\colon M \times N \to P$ sea A-bilineal expresa que la aplicación $f_m\colon N \to P$, $f_m(n) = f(m,n)$, es morfismo de A-módulos para cada elemento $m \in M$. Obtenemos así un isomorfismo natural

$$\mathrm{Bil}_A(M,N;P) \;=\; \mathrm{Hom}_A\big(M, \mathrm{Hom}_A(N,P)\big)$$

Definición: Consideremos el A-módulo libre $A^{(M\times N)}$. Identificando $M \times N$ con la base usual de $A^{(M\times N)}$ obtenemos que cada elemento de $A^{(M\times N)}$ descompone de modo único en la forma

$$\sum_{i=1}^{n} a_i \cdot (m_i, n_i) \;, \quad a_i \in A,\, m_i \in M,\, n_i \in N$$

Sea R el submódulo de $A^{(M\times N)}$ generado por los elementos de la forma

$$\begin{aligned} &(m+m',n) - (m,n) - (m',n) \\ &(m,n+n') - (m,n) - (m,n') \\ &(am,n) - a \cdot (m,n) \\ &(m,an) - a \cdot (m,n) \end{aligned}$$

Llamaremos **producto tensorial** de M y N sobre el anillo A al A-módulo cociente $A^{(M\times N)}/R$ y lo denotaremos $M \otimes_A N$. Para cada elemento (m,n) de $M \times N$, entendido como elemento de $A^{(M\times N)}$, su imagen en $M \otimes_A N$ se denotará $m \otimes n$. Por construcción, tales elementos $m \otimes n$ generan el producto tensorial $M \otimes_A N$; es decir, todo elemento de $M \otimes_A N$ descompone (aunque no de modo único) en la forma

$$\sum_{i=1}^{n} a_i(m_i \otimes n_i)$$

En particular, si $\{m_i\}_{i\in I}$ es un sistema de generadores de M y $\{n_j\}_{j\in J}$ es un sistema de generadores de N, entonces $\{m_i \otimes n_j\}_{i\in I,\, j\in J}$ es un sistema de generadores de $M \otimes_A N$. Además, de acuerdo con la definición de R, tenemos que

$$\begin{gathered}(m+m')\otimes n = m\otimes n + m'\otimes n\\ m\otimes(n+n') = m\otimes n + m\otimes n'\\ (am)\otimes n = a(m\otimes n) = m\otimes(an)\end{gathered}$$

de modo que tenemos una aplicación A-bilineal canónica

$$M \times N \xrightarrow{\otimes} M \otimes_A N\ , \quad (m,n) \mapsto m \otimes n$$

Propiedad Universal: *Sean M y N dos A-módulos. Si $f\colon M \times N \to P$ es una aplicación A-bilineal, existe un único morfismo de A-módulos $\phi\colon M \otimes_A N \to P$ tal que $\phi(m \otimes n) = f(m,n)$:*

$$\mathrm{Hom}_A(M \otimes_A N, P) \ = \ \mathrm{Bil}_A(M, N; P)$$

Demostración: La unicidad de tal morfismo se debe a que los elementos $m \otimes n$ generan $M \otimes_A N$ como A-módulo. En cuanto a la existencia, la condición de que f sea A-bilineal expresa precisamente que el morfismo de A-módulos

$$\bar{f}\colon A^{(M\times N)} \longrightarrow P\ ,\ \bar{f}\big(\sum_i a_i(m_i,n_i)\big) = \sum_i a_i f(m_i,n_i)$$

se anula sobre los generadores del submódulo R; luego sobre R y, por la propiedad universal del módulo cociente, induce un morfismo de A-módulos

$$\phi\colon A^{(M\times N)}/R = M \otimes_A N \longrightarrow P\ , \quad \phi(m\otimes n) = \bar{f}(m,n) = f(m,n)$$

Nota: Una construcción análoga puede hacerse para cualquier familia finita de A-módulos $M_1, \ldots, M_n$, obteniéndose un A-módulo $M_1 \otimes_A \cdots \otimes_A M_n$ con una propiedad universal similar.

Como ejemplo de utilización de tal propiedad universal, veamos el comportamiento del producto tensorial frente a los morfismos. Sean $f\colon M \to M'$ y $g\colon N \to N'$ morfismos de A-módulos. La aplicación

$$M \times N \longrightarrow M' \otimes_A N'\ , \quad (m,n) \mapsto f(m) \otimes g(n)$$

es claramente A-bilineal; luego existe un único morfismo de A-módulos

$$f \otimes g \colon M \otimes_A N \longrightarrow M' \otimes_A N'$$

tal que $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. Este producto tensorial de morfismos es compatible, en un sentido obvio, con la suma, el producto por elementos de A y la composición de morfismos:

$$\begin{aligned} (af + bf') \otimes g &= a(f \otimes g) + b(f' \otimes g) \\ f \otimes (ag + bg') &= a(f \otimes g) + b(f \otimes g') \\ (f' \circ f) \otimes (g' \circ g) &= (f' \otimes g') \circ (f \otimes g) \end{aligned}$$

Teorema 6.3.1 *Existen isomorfismos naturales de A-módulos*

1. $(M \otimes_A N) \otimes_A P = M \otimes_A N \otimes_A P = M \otimes_A (N \otimes_A P)$
   $(m \otimes n) \otimes p = m \otimes n \otimes p = m \otimes (n \otimes p)$
2. $M \otimes_A N \;=\; N \otimes_A M \;,\;\; m \otimes n = n \otimes m$
3. $A \otimes_A M \;= M \;,\;\; a \otimes m = am$
4. $\left(\bigoplus_i M_i\right) \otimes_A N \;=\; \bigoplus_i (M_i \otimes_A N) \;,\;\; \left(\sum_i m_i\right) \otimes n = \sum_i (m_i \otimes n)$

Demostración: En cada caso basta definir los correspondientes morfismos, pues entonces es evidente que sus composiciones son la identidad sobre un sistema de generadores. En cuanto a la definición de tales morfismos, haremos las siguientes observaciones:

1) Para cada elemento $p \in P$, la aplicación

$$M \times N \longrightarrow M \otimes_A N \otimes_A P \;, \quad (m, n) \mapsto m \otimes n \otimes p$$

es A-bilineal, así que define un morfismo de A-módulos

$$f_p \colon M \otimes_A N \longrightarrow M \otimes_A N \otimes_A P \;, \quad f_p(m \otimes n) = m \otimes n \otimes p$$

Ahora la aplicación $(M \otimes_A N) \times P \to M \otimes_A N \otimes_A P$, $(x, p) \mapsto f_p(x)$ es bilineal e induce el morfismo de A-módulos $(M \otimes_A N) \otimes_A P \to M \otimes_A N \otimes_A P$ deseado.

3) La aplicación $M \to A \otimes_A M$, $m \mapsto 1 \otimes m$, es un morfismo de A-módulos. Por otra parte, la aplicación $A \times M \to M$, $(a, m) \mapsto am$, es A-bilineal e induce el morfismo de A-módulos $A \otimes_A M \to M$ deseado.

4) Sea $M = \bigoplus_i M_i$. La aplicación A-bilineal

$$M \times N \to \bigoplus_i (M_i \otimes_A N) \;, \quad \left(\sum_i m_i, n\right) \mapsto \sum_i m_i \otimes n$$

induce el morfismo $M \otimes_A N \to \bigoplus_i (M_i \otimes_A N)$ deseado, y las inclusiones canónicas $j_i \colon M_i \to M$ definen morfismos de A-módulos $j_i \otimes 1 \colon M_i \otimes_A N \to M \otimes_A N$ que inducen el morfismo inverso $\bigoplus_i (M_i \otimes_A N) \to M \otimes_A N$.

Corolario 6.3.2 *Si L es un A-módulo libre de base (e_i) y L' es un A-módulo libre de base (e'_j), entonces $L \otimes_A L'$ es un A-módulo libre de base $(e_i \otimes e'_j)$.*

Demostración: Las bases dadas definen isomorfismos $\bigoplus_i A \to L$ y $\bigoplus_j A \to L'$, que inducen un isomorfismo $\bigoplus_{i,j}(A \otimes_A A) \to L \otimes_A L'$, y $A \otimes_A A = A$.

Otra demostración se obtiene observando que los elementos $e_i \otimes e'_j$ claramente generan el A-módulo $L \otimes_A L'$, y que si $\sum_{ij} a_{ij} e_i \otimes e'_j = 0$, considerando las coordenadas $x_i \colon L \to A$, $y_j \colon L' \to A$ en las bases dadas, concluimos que

$$0 = (x_i \otimes y_j)\big(\textstyle\sum_{ij} a_{ij} e_i \otimes e'_j\big) = a_{ij} \ .$$

Teorema 6.3.3 *Sea $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta de morfismos de A-módulos. Para todo A-módulo N tenemos que la siguiente sucesión es exacta:*

$$M' \otimes_A N \xrightarrow{i\otimes 1} M \otimes_A N \xrightarrow{p\otimes 1} M'' \otimes_A N \longrightarrow 0$$

Demostración: Sea $\mathbf{E}$ la sucesión exacta inicial. De acuerdo con 6.2.1,

$$\mathrm{Hom}_A\big(\mathbf{E}, \mathrm{Hom}_A(N,P)\big) \ = \ \mathrm{Bil}_A(\mathbf{E}, N; P) \ = \ \mathrm{Hom}_A(\mathbf{E} \otimes_A N, P)$$

es una sucesión exacta para todo A-módulo P. De nuevo 6.2.1 nos permite concluir que la sucesión $\mathbf{E} \otimes_A N$ es exacta.

Demostración alternativa: $p \otimes 1$ es epiyectiva, porque $\sum_i m''_i \otimes n_i = (p \otimes 1)(\sum_i m_i \otimes n_i)$, donde $m''_i = p(m_i)$. Además $\mathrm{Im}(i \otimes 1) \subset \mathrm{Ker}(p \otimes 1)$ porque $(p \otimes 1)(i \otimes 1) = (pi) \otimes 1 = 0 \otimes 1 = 0$.

Por último, el morfismo natural $\pi \colon M \otimes_A N \to \tilde{M} := (M \otimes_A N)/\mathrm{Im}(i \otimes 1)$ define una aplicación bilineal $f \colon M \times N \to \tilde{M}$, $f(m,n) = [m \otimes n]$, que es nula cuando $m \in \mathrm{Im}\, i = \mathrm{Ker}\, p$. Al ser p epiyectivo, f factoriza por una aplicación bilineal $\bar{f} \colon M'' \times N \to \tilde{M}$, que define un morfismo de A-módulos $\bar{\pi} \colon M'' \otimes_A N \to \tilde{M}$ tal que $\bar{\pi}(p(m) \otimes n) = \pi(m \otimes n)$. Luego $\mathrm{Ker}(p \otimes 1) \subset \mathrm{Ker}\, \pi = \mathrm{Im}(i \otimes 1)$.

Corolario 6.3.4 $(A/\mathfrak{a}) \otimes_A M \ = \ M/\mathfrak{a}M$ *para todo ideal $\mathfrak{a}$ de A.*

Demostración: La sucesión exacta $\mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ induce una sucesión exacta

$$\mathfrak{a} \otimes_A M \longrightarrow A \otimes_A M \longrightarrow (A/\mathfrak{a}) \otimes_A M \longrightarrow 0$$

Para concluir basta observar que $A \otimes_A M = M$ y que la imagen del morfismo $\mathfrak{a} \otimes_A M \to M$, $a \otimes m \mapsto am$, es el submódulo $\mathfrak{a}M$.

Nota: Aunque un morfismo de A-módulos $i \colon M' \to M$ sea inyectivo, puede ocurrir que el morfismo $i \otimes 1 \colon M' \otimes_A N \to M \otimes_A N$ no lo sea. Por ejemplo, si $A = \mathbb{Q}[\,t\,]$, el morfismo $t\cdot \colon A \to A$ es inyectivo mientras que el morfismo

$$t \otimes 1 \colon A \otimes_A (A/tA) \longrightarrow A \otimes_A (A/tA) \ .$$

es nulo. No obstante, el producto tensorial $\otimes_A N$ sí conserva los morfismos inyectivos cuando admiten retracto:

Corolario 6.3.5 *Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta de morfismos de A-módulos. Si la sucesión escinde, para todo A-módulo N tenemos que la siguiente sucesión es exacta y escinde:*

$$0 \longrightarrow M' \otimes_A N \xrightarrow{i\otimes 1} M \otimes_A N \xrightarrow{p\otimes 1} M'' \otimes_A N \longrightarrow 0$$

En particular, si $0 \to E' \xrightarrow{i} E \xrightarrow{p} E'' \to 0$ es una sucesión exacta de espacios vectoriales sobre un cuerpo k, para todo k-espacio vectorial F tenemos que la siguiente sucesión es exacta:

$$0 \longrightarrow E' \otimes_k F \xrightarrow{i\otimes 1} E \otimes_k F \xrightarrow{p\otimes 1} E'' \otimes_k F \longrightarrow 0$$

Demostración: Si la sucesión escinde, de acuerdo con 6.2.4 existe un morfismo de A-módulos $r\colon M \to M'$ tal que $r \circ i = Id_{M'}$, entonces $(r \otimes 1) \circ (i \otimes 1) = Id_{M' \otimes_A N}$ y concluimos que el morfismo $i \otimes 1$ es inyectivo y la sucesión escinde.

En cuanto a la última afirmación, baste observar que toda sucesión exacta corta de k-espacios vectoriales escinde porque todo subespacio vectorial admite un suplementario.

6.4 Cambio de Base

Sea $j\colon A \to B$ un morfismo de anillos y consideremos en B la estructura de A-módulo inducida: $a \cdot b = j(a)b$.

Si M es un A-módulo, cada elemento $b \in B$ define un endomorfismo $1\otimes b\colon M \otimes_A B \to M \otimes_A B$, y así obtenemos una estructura de B-módulo en $M \otimes_A B$, que viene dada por el siguiente producto:

$$b \cdot \left(\textstyle\sum_i m_i \otimes b_i\right) \;=\; \sum_i m_i \otimes (bb_i)$$

Definición: El B-módulo así definido se denotará M_B y diremos que se obtiene de M mediante el **cambio de base** $j\colon A \to B$.

Tenemos un morfismo de A-módulos canónico

$$M \longrightarrow M_B \quad , \quad m \mapsto m \otimes 1$$

llamado morfismo de **cambio de base**, y diremos que $m \otimes 1$ es el elemento m cambiado de base.

Si $f\colon M \to N$ es un morfismo de A-módulos, entonces $f \otimes 1\colon M_B \to N_B$, $(f \otimes 1)(m \otimes b) = f(m) \otimes b$, es un morfismo de B-módulos y diremos que se obtiene de f mediante el cambio de base $j\colon A \to B$.

Propiedad Universal: *Sea $A \to B$ un morfismo de anillos y sea M un A-módulo. Si N es un B-módulo y $f\colon M \to N$ es un morfismo de A-módulos, entonces existe un único morfismo de B-módulos $f'\colon M_B \to N$ tal que $f'(m \otimes 1) = f(m)$:*

$$\mathrm{Hom}_A(M, N) \;=\; \mathrm{Hom}_B(M_B, N)$$

Demostración: De acuerdo con la propiedad universal del producto tensorial, existe un único morfismo de A-módulos $f'\colon M \otimes_A B \to N$ tal que $f'(m \otimes b) = b \cdot f(m)$. Una comprobación directa muestra que f' es morfismo de B-módulos.

Teorema 6.4.1 *Sea $A \to B$ un morfismo de anillos y sea M un A-módulo. Para todo B-módulo N se tiene un isomorfismo natural de B-módulos*

$$(M_B) \otimes_B N \;=\; M \otimes_A N \;; \quad (m \otimes b) \otimes n \;=\; m \otimes (bn)$$

donde $M \otimes_A N$ es B-módulo con la estructura que definen los morfismos

$$1 \otimes b : M \otimes_A N \to M \otimes_A N$$

Demostración: Si $n \in N$, la aplicación $M \to M \otimes_A N$, $m \mapsto m \otimes n$, es un morfismo de A-módulos; así que, por la propiedad universal del cambio de base, tenemos un morfismo de B-módulos $f_n : M_B \to M \otimes_A N$ tal que $f_n(m \otimes b) = b(m \otimes n) = m \otimes bn$. Ahora la aplicación

$$M_B \times N \longrightarrow M \otimes_A N \;, \quad (x, n) \mapsto f_n(x)$$

es B-bilineal e induce el morfismo de B-módulos $(M_B) \otimes_B N \to M \otimes_A N$ deseado. El morfismo inverso viene inducido por la aplicación A-bilineal

$$M \times N \longrightarrow (M \otimes_A B) \otimes_B N \;, \quad (m, n) \mapsto (m \otimes 1) \otimes n$$

Corolario 6.4.2 $(M \otimes_A M')_B \;=\; (M_B) \otimes_B (M'_B)$
$(m \otimes m') \otimes 1 \;=\; (m \otimes 1) \otimes (m' \otimes 1)$

Demostración:

$$(M \otimes_A B) \otimes_B (M' \otimes_A B) = M \otimes_A (M' \otimes_A B) = (M \otimes_A M') \otimes_A B$$

Corolario 6.4.3 $(M_B)_C \;=\; M_C \quad , \quad (m \otimes b) \otimes c = m \otimes bc.$

Demostración: $(M \otimes_A B) \otimes_B C \;=\; M \otimes_A C.$

Ejemplos:

1. Sea $(e_1, \ldots, e_n)$ una base de un A-módulo libre L. El producto tensorial conmuta con sumas directas, de modo que L_B es un B-módulo libre de base $(e_1 \otimes 1, \ldots, e_n \otimes 1)$. Además, si $(a_1, \ldots, a_n)$ son las coordenadas de $e \in L$ en la base dada, entonces las coordenadas de $m \otimes 1$ en la base $\{e_i \otimes 1\}_i$ también son $(a_1, \ldots, a_n)$.

2. Si un A-módulo M está generado por unos elementos $m_1, \ldots, m_n$, entonces M_B está generado claramente por $m_1 \otimes 1, \ldots, m_n \otimes 1$. Además, si las ecuaciones de un morfismo de A-módulos $f\colon M \to N$, respecto de ciertos sistemas de generadores, son
$$f(m_i) = \textstyle\sum_j a_{ij} n_j$$
entonces las ecuaciones del morfismo $f \otimes 1\colon M_B \to N_B$, respecto de los correspondientes sistemas de generadores $\{m_i \otimes 1\}$ y $\{n_j \otimes 1\}$, son
$$(f \otimes 1)(m_i \otimes 1) = \textstyle\sum_j a_{ij}(n_j \otimes 1)$$
Es decir, son las mismas ecuaciones, con la diferencia de que los coeficientes a_{ij} se consideran en el anillo B y no en A. Por ejemplo, si (a_{ij}) es la matriz de un endomorfismo $T\colon E \to E$ de un $\mathbb{R}$-espacio vectorial E en cierta base $(e_1, \ldots, e_n)$, la matriz del endomorfismo $T \otimes 1\colon E_{\mathbb{C}} \to E_{\mathbb{C}}$ en la base $(e_1 \otimes 1, \ldots, e_n \otimes 1)$ de $E_{\mathbb{C}}$ también es (a_{ij}); pero vista como matriz con coeficientes complejos en vez de como matriz con coeficientes reales.

Dado un problema sobre vectores, matrices, aplicaciones lineales, etc., cambiar de base es ese proceso, tan frecuente y humilde como crucial, de"cambiar la mirada" con la que percibimos el problema, viendo todos los coeficientes en el nuevo anillo B y no en el anillo inicial A. Sorprende que algo tan íntimo y sutil pueda ser definido y estudiado con todo rigor y precisión.

6.5 Álgebras

Definición: Sea A un anillo. Llamaremos **álgebra** sobre A a todo anillo B dotado de un morfismo de anillos $j\colon A \to B$. Dada una A-álgebra B, el morfismo estructural j induce en B una estructura de A-módulo: $a \cdot b = j(a)b$, $a \in A$, $b \in B$. Por eso, cuando no origine confusión, $j(a)$ se denotará a.

Dadas dos A-álgebras $j\colon A \to B$ y $j'\colon A \to C$, diremos que una aplicación $f\colon B \to C$ es un **morfismo** de A-álgebras si es morfismo de anillos y $f(a) = a$ para todo $a \in A$ (o sea, $j' = f \circ j$). Es decir, cuando f sea morfismo de anillos y de A-módulos. El conjunto de los morfismos de A-álgebras de B en C se denota
$$\mathrm{Hom}_{A\text{-alg}}(B, C)$$

Diremos que un morfismo de A-álgebras es un **isomorfismo** si admite un morfismo de A-álgebras inverso.

Es sencillo comprobar que las composiciones de morfismos de A-álgebras también lo son y que los isomorfismos de A-álgebras son los morfismos biyectivos.

Definición: Diremos que un subanillo C de una A-álgebra B es una **subálgebra** cuando $a \in C$ para todo $a \in A$; es decir, cuando C contiene la imagen del morfismo estructural $A \to B$.

Es fácil probar que la intersección de cualquier familia de subálgebras de una A-álgebra B es una subálgebra, y que la subálgebra de B generada por unos elementos $b_1, \ldots, b_n \in B$ (i.e., la menor subálgebra que los contiene) es

$$A[b_1, \ldots, b_n] \;:=\; \{p(b_1, \ldots, b_n) \colon\; p \in A[x_1, \ldots, x_n]\}$$

Diremos que una A-álgebra B es de **tipo finito** si $B = A[b_1, \ldots, b_n]$ para algunos elementos $b_1, \ldots, b_n \in A$, y diremos que B es una A-álgebra **finita** cuando sea un A-módulo finito-generado: $B = Ab_1 + \ldots + Ab_n$.

La estructura de álgebra permite enunciar ya con claridad la propiedad universal del anillo de polinomios $A[x_1, \ldots, x_n]$ con coeficientes en un anillo A:

Propiedad Universal de los Polinomios: *Sea A un anillo. Si B es una A-álgebra, para cada sucesión $(b_1, \ldots, b_n) \in B^n$ existe un único morfismo de A-álgebras $\phi \colon A[x_1, \ldots, x_n] \to B$ tal que $\phi(x_1) = b_1, \ldots, \phi(x_n) = b_n$:*

$$\mathrm{Hom}_{A\text{-alg}}(A[x_1, \ldots, x_n], B) \;=\; B^n$$

Demostración: Claramente tal morfismo de A-álgebras ϕ es necesariamente

$$\phi\Big(\sum_{i_1,\ldots,i_n \geq 0} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}\Big) \;=\; \sum_{i_1,\ldots,i_n \geq 0} a_{i_1 \ldots i_n} b_1^{i_1} \cdots b_n^{i_n}$$

Producto Tensorial de Álgebras

Sean B y C dos álgebras sobre un anillo A.

La aplicación $B \times C \times B \times C \to B \otimes_A C$, $(b, c, b', c') \mapsto (bb') \otimes (cc')$, es claramente A-multilineal; luego induce un morfismo de A-módulos

$$B \otimes_A C \otimes_A B \otimes_A C \;\longrightarrow\; B \otimes_A C$$

que se corresponde con una aplicación A-bilineal

$$(B \otimes_A C) \times (B \otimes_A C) \;\stackrel{\cdot}{\longrightarrow}\; B \otimes_A C$$

Obtenemos así una operación en el A-módulo $B \otimes_A C$, que denotaremos multiplicativamente. Por definición tenemos que

$$\big(\sum_i b_i \otimes c_i\big) \cdot \big(\sum_j b_j \otimes c_j\big) \;=\; \sum_{i,j} (b_i b_j) \otimes (c_i c_j)$$

y este producto define en $B \otimes_A C$ una estructura de anillo. Además, la aplicación $A \to B \otimes_A C$, $a \mapsto a \otimes 1 = 1 \otimes a$, es morfismo de anillos. Hemos definido así una estructura de A-álgebra en $B \otimes_A C$.

Además, si $f\colon B \to B'$ y $g\colon C \to C'$ son morfismos de A-álgebras, entonces la aplicación $f \otimes g\colon B \otimes_A C \to B' \otimes_A C'$ también es morfismo de A-álgebras.

Tenemos los siguientes morfismos canónicos de A-álgebras:

$$\begin{aligned} j_1\colon B &\longrightarrow B \otimes_A C\ , \quad j_1(b) = b \otimes 1 \\ j_2\colon C &\longrightarrow B \otimes_A C\ , \quad j_2(c) = 1 \otimes c \end{aligned}$$

Propiedad Universal: *Sea A un anillo. Si $f\colon B \to D$ y $g\colon C \to D$ son morfismos de A-álgebras, existe un único morfismo de A-álgebras $\phi\colon B \otimes_A C \to D$ tal que $f = \phi \circ j_1$ y $g = \phi \circ j_2$; es decir, $\phi(b \otimes 1) = f(b)$, $\phi(1 \otimes c) = g(c)$:*

$$\mathrm{Hom}_{A\text{-alg}}(B \otimes_A C, D) \;=\; \mathrm{Hom}_{A\text{-alg}}(B, D) \times \mathrm{Hom}_{A\text{-alg}}(C, D)$$

Demostración: La unicidad de ϕ se debe a que ha de ser

$$\phi\big(\sum_i b_i \otimes c_i\big) = \sum_i \phi(b_i \otimes 1)\phi(1 \otimes c_i) = \sum_i f(b_i) g(c_i)$$

En cuanto a la existencia, basta considerar la composición del morfismo de A-álgebras $f \otimes g\colon B \otimes_A C \to D \otimes_A D$ con el morfismo $\mu\colon D \otimes_A D \to D$, $\mu(d' \otimes d) = d'd$, inducido por el producto $D \times D \to D$, $(d', d) \mapsto d'd$.

Corolario 6.5.1 $\begin{aligned} A[x_1, \ldots, x_n] \otimes_A A[y_1, \ldots y_m] \;&=\; A[x_1, \ldots, x_n, y_1, \ldots, y_m] \\ p(x_1, \ldots, x_n) \otimes q(y_1, \ldots y_m) \;&=\; p(x_1, \ldots, x_n) q(y_1, \ldots y_m) \end{aligned}$

Definición: Sea A un anillo y C una A-álgebra. Si $A \to C$ es un morfismo de anillos, el morfismo canónico $j_2\colon C \to B \otimes_A C$ define una estructura de C-álgebra en $B \otimes_A C$. Esta C-álgebra se denotará B_C y diremos que se obtiene de la A-álgebra B por el **cambio de base** $A \to C$. Tenemos un morfismo de A-álgebras canónico $j\colon B \to B_C$, $j(b) = b \otimes 1$, llamado morfismo de **cambio de base**.

Sea $f\colon B \to B'$ un morfismo de A-álgebras. El morfismo de A-álgebras

$$f \otimes 1\colon B_C \longrightarrow B'_C \quad , \quad (f \otimes 1)(b \otimes c) = f(b) \otimes c$$

es de hecho un morfismo de C-álgebras, que se denotará f_C y diremos que se obtiene de f mediante el cambio de base $A \to C$.

Propiedad Universal: *Sea B una A-álgebra y $A \to C$ un morfismo de anillos. Si D es una C-álgebra y $f\colon B \to D$ es un morfismo de A-álgebras, entonces existe un único morfismo de C-álgebras $\psi\colon B_C \to D$ tal que $\psi(b \otimes 1) = f(b)$:*

$$\mathrm{Hom}_{A\text{-alg}}(B, D) \;=\; \mathrm{Hom}_{C\text{-alg}}(B_C, D)$$

Demostración: La unicidad se debe a que ψ ha de ser

$$\psi\big(\textstyle\sum_i b_i \otimes c_i\big) = \sum_i \psi\big(c_i \cdot j(b_i)\big) = \sum_i c_i f(b_i)$$

En cuanto a la existencia, el morfismo $f\colon B \to D$ y el morfismo estructural $C \to D$ inducen un morfismo de A-álgebras $\psi\colon B \otimes_A C \to D$ que, de hecho, es morfismo de C-álgebras y verifica que $\psi(b \otimes 1) = f(b)$.

Corolario 6.5.2 $\begin{array}{rcl} A[x_1, \ldots, x_n] \otimes_A C &=& C[x_1, \ldots, x_n] \\ q(x_1, \ldots, x_n) \otimes c &=& cq(x_1, \ldots, x_n) \end{array}$

Corolario 6.5.3 $\begin{array}{rcl} \big(A[x_1, \ldots, x_n]/(p_1, \ldots, p_r)\big) \otimes_A C &=& C[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \\ [q(x_1, \ldots, x_n)] \otimes c &=& [cq(x_1, \ldots, x_n)] \end{array}$

Demostración: Poniendo $\underline{x} = x_1, \ldots, x_n$ y $\underline{p} = p_1, \ldots, p_r$ para abreviar,

$$\begin{aligned} A[\,\underline{x}\,]/(\underline{p}\,) \otimes_A C \;&=\; A[\,\underline{x}\,]/(\underline{p}\,) \otimes_{A[\,\underline{x}\,]} A[\,\underline{x}\,] \otimes_A C \;= \\ &=\; A[\,\underline{x}\,]/(\underline{p}\,) \otimes_{A[\,\underline{x}\,]} C[\underline{x}] \;=\; C[\,\underline{x}\,]/(\underline{p}\,) \end{aligned}$$

Capítulo 7

Espectro Primo

Hemos visto que en el anillo $k[x_1, \dots x_n]$ la teoría de ideales coincide con el estudio de las subvariedades del espacio afín n-dimensional sobre k definidas por ecuaciones polinómicas. Además, la correspondencia natural entre los ideales de un cociente $A/\mathfrak{a}$ y los ideales de A que contienen a $\mathfrak{a}$, muestra que la teoría de ideales en el anillo $k[x_1, \dots, x_n]/(p_1, \dots, p_r)$ coincide con el estudio de las subvariedades contenidas en la subvariedad de ecuaciones

$$\left.\begin{array}{c} p_1(x_1, \dots, x_n) = 0 \\ \cdots\cdots\cdots \\ p_r(x_1, \dots, x_n) = 0 \end{array}\right\} ;$$

es decir, con la geometría intrínseca (sin referencia al espacio afín que la contiene) de tal subvariedad.

Por otra parte, en todos los anillos conmutativos disponemos de una teoría de la divisibilidad de ideales. ¿Podremos entender la teoría de ideales en cualquier anillo conmutativo A como la teoría de los lugares geométricos de cierta geometría y comprender los elementos de A como funciones sobre ese espacio? ¿cuáles serían los puntos de tal espacio? Los puntos deberían ser los lugares geométricos más pequeños posibles, aquellos que sólo contengan al vacío y a ellos mismos; es decir, los que vengan definidos por los ideales maximales de A, por los ideales cuyos únicos divisores son la unidad A y ellos mismos (¡por los números primos!). No obstante, sabemos que la propiedad esencial de los números primos, más que su propia definición, es la que señala el lema de Euclides: en los anillos arbitrarios, el concepto que generaliza al de número primo, más que el de ideal maximal, es el de ideal primo. Por razones que se irán aclarando a lo largo del capítulo, en la comprensión geométrica de los anillos conmutativos el concepto que mejor recoge la noción intuitiva de punto es nuevamente el concepto de ideal primo, no sólo el de ideal maximal. Tenemos así en todo anillo conmutativo una aritmética y una geometría que son lógicamente equivalentes, pues ambas coinciden con la teoría de

ideales del anillo. Todo problema enunciado en términos de ideales admite tanto una comprensión y un tratamiento aritmético como geométrico. La teoría de ideales inicia el cumplimiento del sueño de Kronecker (1823-1891): la unificación de la Aritmética y la Geometría. En esta síntesis asombrosa los conceptos básicos de número primo y de punto quedan asumidos en el de ideal primo.

En este capítulo iniciaremos la comprensión geométrica de cualquier anillo conmutativo A, asociándole un espacio cuyos puntos se corresponden con los ideales primos de A y entendiendo los elementos de A como las funciones sobre tal espacio. Los ideales de A deberán comprenderse entonces como los ideales de las subvariedades cerradas, entendiendo que una función se anula sobre determinada subvariedad cerrada cuando pertenezca al correspondiente ideal; es decir, el ideal de una subvariedad cerrada está formado por todas las funciones que se anulan en la subvariedad.

Daremos así los primeros pasos en el estudio de la aclaración, llevada a cabo por A. Grothendieck (n. 1928) en los años 60, de dos conceptos fundamentales: el de *punto* y el de *función*. Desde esta perspectiva los elementos de cualquier anillo conmutativo pueden entenderse como funciones, no sólo las aplicaciones de un conjunto en $\mathbb{R}$ o $\mathbb{C}$ (o cualquier otro cuerpo). En ella los números enteros, los enteros de Gauss, etc., son verdaderas funciones y les aplicamos nuestras intuiciones y recursos geométricos. En palabras de Grothendieck:

> "Esa vasta visión unificadora puede ser descrita como una *geometría nueva*. Es la que, al parecer, Kronecker había soñado en el siglo pasado[1]. Pero la realidad (que a veces un atrevido sueño hace presentir o entrever, y nos anima a descubrir...) sobrepasa siempre en riqueza y en resonancia al sueño más temerario o más profundo. Seguramente nadie, incluso la víspera del día en que apareció, hubiera soñado muchas de las partes de esa nueva geometría (si no todas) – el obrero mismo no más que los demás.
>
> Puede considerarse que la nueva geometría es ante todo una *síntesis* de dos mundos, hasta entonces contiguos y estrechamente solidarios, aunque separados: el *mundo "aritmético"*, en el que viven los (así llamados) "espacios" sin principio de continuidad, y el *mundo de la magnitud continua*, en que viven los "espacios" en el sentido propio del término, accesibles a los métodos del analista y (por eso mismo) considerados por él como dignos de alojarse en la ciudad matemática. *En la visión nueva, esos dos mundos antes separados forman uno sólo.*

[1] No conocía ese "sueño de Kronecker" más que de oídas, cuando alguien (quizás fuera John Tate) me dijo que estaba realizando ese sueño.

7.1 Espectro Primo y Dimensión

Definición: Llamaremos **espectro primo** de un anillo A al conjunto $\operatorname{Spec} A$ de sus ideales primos[2]. Sus elementos se llamarán **puntos**, así que cada punto $x \in \operatorname{Spec} A$ se corresponde con un ideal primo de A, que denotaremos $\mathfrak{p}_x$.

Llamaremos **funciones** a los elementos del anillo A, y diremos que la clase de $f \in A$ en $A/\mathfrak{p}_x$ es el **valor** de la función f en el punto x:

$$f(x) \;:=\; [f] \;\in\; A/\mathfrak{p}_x$$

de modo que *el ideal primo $\mathfrak{p}_x$ de un punto $x \in \operatorname{Spec} A$ está formado por todas las funciones $f \in A$ que se anulan en x*

$$\mathfrak{p}_x \;=\; \{f \in A\colon\; f(x) = 0\}\ .$$

El hecho de que el ideal $\mathfrak{p}_x$ de un punto $x \in \operatorname{Spec} A$ sea primo significa que:

La función 0 se anula en todos los puntos, y la función 1 en ninguno.
Si dos funciones se anulan en un punto, su suma también.
Si una función se anula en un punto, sus múltiplos también.
Si un producto de funciones se anula en x, algún factor se anula en x.

El teorema 6.1.3 afirma que *todo anillo no nulo tiene espectro no vacío* y 6.1.5 nos dice que *las funciones invertibles son las que no se anulan en ningún punto.*

Definición: Sea A un anillo. Llamaremos **ceros** de una función $f \in A$ al subconjunto $(f)_0$ del espectro de A formado por todos los puntos donde se anule f. Llamaremos **ceros** de un ideal $\mathfrak{a}$ de A al subconjunto de $\operatorname{Spec} A$ formado por los puntos donde se anulen todas las funciones de $\mathfrak{a}$ y lo denotaremos $(\mathfrak{a})_0$:

$$\begin{aligned}(\mathfrak{a})_0 \;=\; \bigcap_{f\in\mathfrak{a}} (f)_0 \;&=\; \{x \in \operatorname{Spec} A\colon\; f(x) = 0,\ \forall f \in \mathfrak{a}\}\\ &=\; \{x \in \operatorname{Spec} A\colon \mathfrak{a} \subseteq \mathfrak{p}_x\} \;=\; \begin{bmatrix}\text{Ideales primos de } A\\ \text{que contienen al ideal } \mathfrak{a}\end{bmatrix}\end{aligned}$$

Ahora, 6.1.4 afirma que si $(\mathfrak{a})_o = \emptyset$, entonces $\mathfrak{a} = A$. Además

$$(0)_0 \;=\; \operatorname{Spec} A \quad ;\quad (A)_0 = \emptyset$$
$$\Big(\sum_{i\in I} \mathfrak{a}_i\Big)_0 \;=\; \bigcap_{i\in I} (\mathfrak{a}_i)_0$$
$$(\mathfrak{a}_1 \ldots \mathfrak{a}_n)_0 = (\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n)_0 = (\mathfrak{a}_1)_0 \cup \ldots \cup (\mathfrak{a}_n)_0$$

[2]Hablando con precisión, no sería necesario pedir que los elementos del espectro sean los ideales primos del anillo, sino que nos bastaría con disponer de una correspondencia biunívoca con tales ideales; pero no lo haremos buscando la claridad de la exposición.

donde la última igualdad, que basta probar cuando $i = 2$, se debe a que si en un punto $x \in \operatorname{Spec} A$ no se anula una función $f_1 \in \mathfrak{a}_1$ y no se anula una función $f_2 \in \mathfrak{a}_2$, entonces $f_1 f_2 \in \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$ y $f_1 f_2$ no se anula en x.

Estas igualdades muestran que los ceros de los ideales de A son los cerrados de una topología sobre $\operatorname{Spec} A$, llamada **topología de Zariski** (1899-1986). De ahora en adelante consideraremos siempre el espectro de un anillo como un espacio topológico. Por definición, si un punto $x \in \operatorname{Spec} A$ no está en un cerrado $C = (\mathfrak{a})_0$, entonces alguna función $f \in \mathfrak{a}$ no se anula en x (y se anula obviamente en C):

Las funciones de A separan puntos de cerrados en $\operatorname{Spec} A$.

Los cerrados de la topología de Zariski son las intersecciones arbitrarias de ceros de funciones, de modo que *los ceros de funciones forman una base de la topología de* $\operatorname{Spec} A$. Luego una base de abiertos de la topología de Zariski de $\operatorname{Spec} A$ está formada por los abiertos

$$U_f := \operatorname{Spec} A - (f)_0 = \{x \in \operatorname{Spec} A \colon f \text{ no se anula en } x\}$$

que llamaremos **abiertos básicos**. Esta base de abiertos es estable por intersecciones finitas, pues

$$U_f \cap U_g = U_{fg}$$

Por otra parte, 6.1.4 afirma que $(\mathfrak{a})_0 = \emptyset$ precisamente cuando $\mathfrak{a} = A$, así que el Teorema chino de los restos admite la siguiente reformulación:

Teorema Chino del Resto: *Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de un anillo A sin ceros comunes, $(\mathfrak{a})_0 \cap (\mathfrak{b})_0 = \emptyset$, entonces $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ y tenemos un isomorfismo de anillos*

$$A/\mathfrak{a} \cap \mathfrak{b} = (A/\mathfrak{a}) \times (A/\mathfrak{b}) \ .$$

Corolario 7.1.1 *Si $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ son ideales maximales distintos de un anillo A, los morfismos naturales $A \to (A/\mathfrak{m}_1^{n_1}) \oplus \ldots \oplus (A/\mathfrak{m}_r^{n_r})$ son epiyectivos.*

Demostración: Sea x_i el punto de $\operatorname{Spec} A$ definido por el ideal maximal $\mathfrak{m}_i$. Como $(\mathfrak{m}_1^{n_1})_0 = (\mathfrak{m}_1)_0 = \{x_1\}$ y $(\mathfrak{m}_2^{n_2} \cap \ldots \cap \mathfrak{m}_r^{n_r})_0 = (\mathfrak{m}_2^{n_2})_0 \cup \ldots \cup (\mathfrak{m}_r^{n_r})_0 = \{x_2, \ldots, x_r\}$, según el teorema chino de los restos tenemos isomorfismos de anillos

$$A/\mathfrak{m}_1^{n_1} \cap \ldots \cap \mathfrak{m}_r^{n_r} = (A/\mathfrak{m}_1^{n_1}) \oplus (A/\mathfrak{m}_2^{n_2} \cap \ldots \cap \mathfrak{m}_r^{n_r}) = \ldots = (A/\mathfrak{m}_1^{n_1}) \oplus \ldots \oplus (A/\mathfrak{m}_r^{n_r})$$

que muestran que el morfismo natural $A \to (A/\mathfrak{m}_1^{n_1}) \oplus \ldots \oplus (A/\mathfrak{m}_r^{n_r})$ es epiyectivo.

Teorema 7.1.2 *El espectro de cualquier anillo es un espacio topológico compacto.*

Demostración: Sea A un anillo y consideremos una familia de cerrados $\{(\mathfrak{a}_i)_0\}_{i \in I}$ de su espectro con intersección vacía

$$\emptyset = \bigcap_{i \in I} (\mathfrak{a}_i)_0 = \Big(\sum_{i \in I} \mathfrak{a}_i \Big)_0$$

De 6.1.4 se sigue que $\sum_i \mathfrak{a}_i = A$. Luego $1 = f_1 + \ldots + f_n$ para ciertas funciones $f_1 \in \mathfrak{a}_{i_1}, \ldots, f_n \in \mathfrak{a}_{i_n}$, de modo que

$$(\mathfrak{a}_{i_1})_0 \cap \ldots \cap (\mathfrak{a}_{i_n})_0 \;=\; (\mathfrak{a}_{i_1} + \ldots + \mathfrak{a}_{i_n})_0 \;=\; (A)_0 \;=\; \emptyset$$

y concluimos que una subfamilia finita tiene intersección vacía. Es decir, el espectro de A es compacto.

Dimensión

Proposición 7.1.3 *El cierre de cada punto x del espectro de un anillo A está formado por los ceros de su ideal primo:*

$$\overline{\{x\}} \;=\; (\mathfrak{p}_x)_0 \;.$$

Luego Spec A *es un espacio topológico T_0 (puntos distintos tienen cierres distintos) y los puntos cerrados de* Spec A *se corresponden con los ideales maximales de A.*

Demostración: La condición de que un cerrado $(\mathfrak{a})_0$ de Spec A pase por x significa que $\mathfrak{a} \subseteq \mathfrak{p}_x$, en cuyo caso $(\mathfrak{p}_x)_0 \subseteq (\mathfrak{a})_0$. Luego $(\mathfrak{p}_x)_0$ es el menor cerrado de Spec A que contiene a x; es decir, $(\mathfrak{p}_x)_0$ es el cierre de x en Spec A.

Definición: Diremos que un espacio topológico es **irreducible** cuando no pueda descomponerse como unión de dos cerrados estrictamente menores. Llamaremos **componentes irreducibles** de un espacio topológico X a los subespacios irreducibles maximales de X, es decir, que no estén contenidos estrictamente en otro subespacio irreducible.

El cierre de un subespacio irreducible también es irreducible y, en particular, el cierre de cualquier punto es un cerrado irreducible. Luego las componentes irreducibles de un espacio siempre son cerradas. Todo espacio irreducible es conexo, así que cada componente irreducible de un espacio X está contenida en una componente conexa de X; pero un punto de X puede pertenecer a varias componentes irreducibles, como es el caso del punto $x = 0$, $y = 0$ en el par de rectas concurrentes Spec $\mathbb{C}[x, y]/(xy)$.

Proposición 7.1.4 *Cada cerrado irreducible del espectro de un anillo A es el cierre de un único punto, llamado* **punto genérico** *de tal cerrado.*

Por tanto, al asociar a cada ideal primo de A sus ceros, obtenemos una correspondencia biyectiva:

$$\begin{bmatrix}\text{Ideales primos}\\ \text{del anillo } A\end{bmatrix} \;=\; \begin{bmatrix}\text{Cerrados irreducibles}\\ \text{de Spec } A\end{bmatrix}$$

que invierte el orden. En particular, las componentes irreducibles de Spec A *se corresponden con los ideales primos minimales de A.*

Demostración: Sea Y un cerrado irreducible de $\operatorname{Spec} A$. Si un producto de dos funciones de A se anula en Y, algún factor se anula en Y, porque Y es irreducible; así que las funciones de A que se anulan en Y forman un ideal primo $\mathfrak{p}$, y tenemos que $Y = (\mathfrak{p})_0$ porque las funciones de A separan puntos de cerrados.

De acuerdo con 7.1.3, concluimos que Y es el cierre del punto de $\operatorname{Spec} A$ definido por el ideal primo $\mathfrak{p}$. La unicidad de tal punto se debe también a 7.1.3.

Definición: Llamaremos **dimensión de Krull** (1899-1971) de un anillo A al supremo de las longitudes de las cadenas crecientes de ideales primos de A. Es decir, un anillo A tiene dimensión finita n cuando admita alguna cadena de ideales primos $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ y cualquier otra cadena de ideales primos de A tenga longitud menor o igual que n.

La dimensión de un anillo A sólo depende de la topología de $\operatorname{Spec} A$, pues es el supremo de las longitudes de las sucesiones $x_0, x_1, \ldots, x_n$ de puntos de $\operatorname{Spec} A$ tales que x_i está en el cierre de x_{i-1} (en cuyo caso se dice que x_i es una *especialización* de x_{i-1} ó que x_{i-1} es una *generalización* de x_i, y pondremos $x_{i+1} > x_i$). Por eso hablaremos de la dimensión de $\operatorname{Spec} A$, entendiendo que es la dimensión de A.

7.2 Aplicación Continua Inducida

Sea $j\colon A \to B$ un morfismo de anillos. Si $\mathfrak{b}$ es un ideal de B, los elementos de A cuya imagen por j está en $\mathfrak{b}$ forman un ideal de A que denotaremos $j^{-1}(\mathfrak{b})$ ó $A \cap \mathfrak{b}$ cuando no cause confusión. Es fácil probar que $A \cap \mathfrak{p}$ es un ideal primo de A cuando $\mathfrak{p}$ es un ideal primo de B. Obtenemos así una aplicación natural

$$\phi : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A \quad ; \quad \phi(\mathfrak{p}) = A \cap \mathfrak{p}$$

Si ϕ y ϕ' son las aplicaciones inducidas por dos morfismos de anillos $j\colon A \to B$ y $j'\colon B \to C$, la aplicación inducida por $j' \circ j$ es $\phi \circ \phi'$.

Por definición, tenemos $x = \phi(y)$ precisamente cuando $\mathfrak{p}_x = j^{-1}(\mathfrak{p}_y)$. Es decir, una función $f \in A$ se anula en el punto $\phi(y)$ justamente cuando $j(f)$ se anula en el punto $y \in \operatorname{Spec} B$:

$$\boxed{\phi^{-1}(f)_0 = \big(j(f)\big)_0 = (fB)_0}$$

Teorema 7.2.1 *La aplicación $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ inducida por cualquier morfismo de anillos $A \to B$ es continua:*

$$\phi^{-1}(\mathfrak{a})_0 = (\mathfrak{a}B)_0$$

Demostración: $\phi^{-1}(\mathfrak{a})_0 = \phi^{-1}\big(\bigcap_{f\in\mathfrak{a}} (f)_0\big) = \bigcap_{f\in\mathfrak{a}} \phi^{-1}(f)_0 = \bigcap_{f\in\mathfrak{a}} (fB)_0 = (\mathfrak{a}B)_0$.

Teorema 7.2.2 *Sea $\mathfrak{a}$ un ideal de un anillo A. La aplicación continua*

$$i\colon \operatorname{Spec}(A/\mathfrak{a}) \to \operatorname{Spec} A$$

inducida por la proyección canónica $\pi\colon A \to A/\mathfrak{a}$ establece un homeomorfismo de $\operatorname{Spec}(A/\mathfrak{a})$ *con su imagen, que son los ceros del ideal $\mathfrak{a}$:*

$$\operatorname{Spec}(A/\mathfrak{a}) \;=\; (\mathfrak{a})_0$$

Demostración: De acuerdo con 6.1.2, la aplicación i establece una biyección entre $\operatorname{Spec} A/\mathfrak{a}$ y los ceros de $\mathfrak{a}$, y es continua en virtud del teorema anterior.

Es un homeomorfismo con la imagen porque para cada cerrado básico $(\bar{f}\,)_0$ de $\operatorname{Spec}(A/\mathfrak{a})$ tenemos que $i^{-1}(f)_0 = (\pi f)_0 = (\bar{f})_0$.

Corolario 7.2.3 $\operatorname{Spec}(A \oplus B) \;=\; (\operatorname{Spec} A) \coprod (\operatorname{Spec} B)$

Demostración: Consideremos en el anillo $A \oplus B$ los ideales $\mathfrak{a} = A \oplus 0$, $\mathfrak{b} = 0 \oplus B$. Como $\mathfrak{a} + \mathfrak{b} = A \oplus B$ y $\mathfrak{a} \cap \mathfrak{b} = 0$, tenemos que $(\mathfrak{a})_0 \cap (\mathfrak{b})_0 = \emptyset$ y $(\mathfrak{a})_0 \cup (\mathfrak{b})_0 = \operatorname{Spec}(A \oplus B)$; es decir, $\operatorname{Spec}(A \oplus B) = (\mathfrak{a})_0 \coprod (\mathfrak{b})_0$.

Para concluir basta observar que, de acuerdo con el teorema anterior,

$$\begin{aligned} (\mathfrak{a})_0 \;&=\; \operatorname{Spec}(A \oplus B)/\mathfrak{a} \;=\; \operatorname{Spec} B \\ (\mathfrak{b})_0 \;&=\; \operatorname{Spec}(A \oplus B)/\mathfrak{b} \;=\; \operatorname{Spec} A \end{aligned}$$

Nótese que cada ideal primo $\mathfrak{p}$ de A se corresponde con el ideal primo $\mathfrak{p} \oplus B$ de $A \oplus B$, y cada ideal primo $\mathfrak{q}$ de B con el ideal primo $A \oplus \mathfrak{q}$ de $A \oplus B$.

Teorema 7.2.4 *Sea S un sistema multiplicativo de un anillo A. La aplicación $i\colon \operatorname{Spec}(S^{-1}A) \to \operatorname{Spec} A$ inducida por el morfismo de localización $\gamma\colon A \to S^{-1}A$ establece un homeomorfismo de* $\operatorname{Spec}(S^{-1}A)$ *con su imagen, que está formada por los puntos donde no se anula ninguna función $f \in S$:*

$$\operatorname{Spec}(S^{-1}A) \;=\; \bigcap_{f \in S} U_f$$

Es decir, los ideales primos de $S^{-1}A$ se corresponden con los ideales primos de A que no cotan al sistema multiplicativo S.

Demostración: Sea $\mathfrak{q}$ un ideal primo de A_S y sea $\mathfrak{p} = A \cap \mathfrak{q}$. Es fácil probar que $\mathfrak{q} = \{b/s \in A_S\colon\ b \in \mathfrak{p}\} = \mathfrak{p}A_S$, así que la aplicación i considerada es inyectiva. Además $\mathfrak{p}$ no corta a S porque, en caso contrario, $\mathfrak{q} = \mathfrak{p}A_S$ tendría elementos invertibles y $\mathfrak{q} = A_S$, contra la hipótesis de que el ideal $\mathfrak{q}$ es primo.

Por otra parte, si $\mathfrak{p}$ es un ideal primo de A que no corta al sistema S, entonces $A \cap (\mathfrak{p}A_S) = \mathfrak{p}$:

$$\frac{a}{1} = \frac{b}{s}\,,\ b \in \mathfrak{p} \;\Rightarrow\; au = bv \in \mathfrak{p}\,,\ u, v \in S \;\Rightarrow\; a \in \mathfrak{p}$$

Se sigue también que $\mathfrak{p}A_S$ es un ideal primo de A_S,

$$(a_1/s_1)(a_2/s_2) \in \mathfrak{p}A_S \;\Rightarrow\; a_1a_2 \in A \cap \mathfrak{p}A_S = \mathfrak{p} \;\Rightarrow\; a_i \in \mathfrak{p} \;\Rightarrow\; a_i/s_i \in \mathfrak{p}A_S$$

y concluimos que el morfismo de localización $\gamma\colon A \to A_S$ establece una biyección entre los ideales primos de A_S y los ideales primos de A que no cortan a S.

Esta biyección es un homeomorfismo porque para cualquier cerrado básico $(f/s)_0$ de $\operatorname{Spec} A_S$ tenemos

$$i^{-1}(f)_0 \;=\; (f/1)_0 \;=\; (f/s)_0\ .$$

Notación: Sea A un anillo. Si $f \in A$, denotaremos A_f la localización de A por el sistema multiplicativo $\{1, f, f^2, \ldots, f^n, \ldots\}$.

Si x es un punto de $\operatorname{Spec} A$ y $\mathfrak{p}$ es su ideal primo, denotaremos A_x ó $A_\mathfrak{p}$ la localización de A por el sistema multiplicativo $S = A - \mathfrak{p}$.

Corolario 7.2.5 *El espectro de A_f es el complementario de $(f)_0$:*

$$U_f = \operatorname{Spec} A_f$$

y A_f coincide con la localización de A por todas las funciones que no se anulan en ningún punto de U_f. Por tanto, si $(f)_0 = (g)_0$, entonces $A_f = A_g$.

Demostración: El homeomorfismo $U_f = \operatorname{Spec} A_f$ se sigue directamente del teorema anterior, porque $(f)_0 = (f^n)_0$.

Por otra parte, si una función $g \in A$ no se anula en ningún punto de U_f, de 6.1.5 se sigue que g es invertible en A_f, así que A_f coincide con la localización de A por las funciones que no se anulan en ningún punto de U_f.

Corolario 7.2.6 *Los ideales primos de $A_\mathfrak{p}$ se corresponden con los ideales primos de A contenidos en $\mathfrak{p}$. En particular, $A_\mathfrak{p}$ tiene un único ideal maximal $\mathfrak{p}A_\mathfrak{p}$.*

Definición: Sea $\mathfrak{a}$ un ideal de un anillo A. Diremos que

$$\mathrm{r}\,(\mathfrak{a}) \;=\; \{f \in A :\; f^n \in \mathfrak{a} \text{ para algún } n \in \mathbb{N}\}$$

es el **radical** de $\mathfrak{a}$. Por abuso del lenguaje, el radical del ideal 0, que está formado por los elementos **nilpotentes** (=con alguna potencia nula), suele denominarse radical del anillo A. Diremos que un anillo es **reducido** si su radical es nulo; es decir, si carece de elementos nilpotentes no nulos.

Teorema 7.2.7 *Las funciones nilpotentes son las que se anulan en todos los puntos del espectro. Es decir, el radical de un anillo es la intersección de todos sus ideales primos.*

Demostración: Es claro que los elementos nilpotentes de un anillo A pertenecen a todos sus ideales primos.

Recíprocamente, si alguna función $f \in A$ se anula en todos los puntos del espectro de A, entonces $\operatorname{Spec} A_f = U_f = \emptyset$ según 7.2.5. De acuerdo con 6.1.3 tenemos que $A_f = 0$; luego $1/1 = 0/1$, de modo que existe una potencia f^n tal que $0 = f^n(1-0) = f^n$.

Corolario 7.2.8 *El radical de un ideal $\mathfrak{a}$ coincide con la intersección de los ideales primos que lo contienen, de modo que su radical $\mathrm{r}(\mathfrak{a})$ es el mayor ideal cuyos ceros coinciden con los ceros de $\mathfrak{a}$.*

Demostración: Es claro que el radical de $\mathfrak{a}$ está contenido en cualquier ideal primo que contenga al ideal $\mathfrak{a}$. Recíprocamente, si una función $f \in A$ pertenece a todos los ideales primos que contienen al ideal $\mathfrak{a}$, entonces $\bar{f}$ se anula en $\operatorname{Spec} A/\mathfrak{a}$ según 7.2.2. El teorema anterior afirma que alguna potencia de $\bar{f}$ es nula, $\bar{f}^n = 0$, y concluimos que $f^n \in \mathfrak{a}$. Es decir, $f \in r(\mathfrak{a})$.

Ejemplo: Dados n elementos $\alpha_1, \ldots, \alpha_n$ de una extensión K de un cuerpo k, el núcleo del correspondiente morfismo $k[x_1, \ldots, x_n] \to K$ es un ideal primo $\mathfrak{p}$ (no necesariamente maximal, pues el morfismo puede no ser epiyectivo) que define un punto del espectro de $k[x_1, \ldots, x_n]$. Por definición, un polinomio $p(x_1, \ldots, x_n)$ se anula en este punto si $p(\alpha_1, \ldots, \alpha_n) = 0$. Por tanto, $\mathfrak{p}$ define un punto del espectro de $A = k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$ cuando $p_i(\alpha_1, \ldots, \alpha_n) = 0$ para todo índice $1 \leq i \leq r$, y diremos que es el punto de $\operatorname{Spec} A$ definido por $(\alpha_1, \ldots, \alpha_n)$, o bien que es el punto $x_1 = \alpha_1, \ldots, x_n = \alpha_n$.

Todos los puntos del espectro de $k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$ son de esta forma, pues cada ideal primo $\mathfrak{p}$ de A es el núcleo del morfismo natural $A \to A/\mathfrak{p} \to \kappa(\mathfrak{p})$, donde $\kappa(\mathfrak{p})$ denota el cuerpo de fracciones de $A/\mathfrak{p}$. Es decir, los puntos del espectro de $k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$ vienen definidos por las soluciones, en extensiones de k, del sistema de ecuaciones $p_1(x_1, \ldots, x_n) = 0, \ldots, p_r(x_1, \ldots, x_n) = 0$; aunque diferentes soluciones puedan definir el mismo punto del espectro de A. Así, cuando $k = \mathbb{R}$, cada solución compleja $(\alpha_1, \ldots, \alpha_n)$ define el mismo punto del espectro que la solución conjugada $(\overline{\alpha}_1, \ldots, \overline{\alpha}_n)$.

Corolario 7.2.9 *Sea k un cuerpo y $\mathfrak{a} = (p_1, \ldots, p_r)$ un ideal del anillo de polinomios $k[x_1, \ldots, x_n]$. El radical del ideal $\mathfrak{a}$ está formado por los polinomios que se anulan en todas las soluciones (en extensiones de k) del sistema de ecuaciones*

$$\left.\begin{array}{c} p_1(x_1, \ldots, x_n) = 0 \\ \cdots\cdots\cdots \\ p_r(x_1, \ldots, x_n) = 0 \end{array}\right\}$$

Por tanto, dos sistemas de ecuaciones en n indeterminadas con coeficientes en k admiten las mismas soluciones justamente cuando los ideales que generan en $k[x_1, \ldots, x_n]$ tienen el mismo radical.

Demostración: Todo punto del espectro de $k[x_1, \dots x_n]$ es de la forma $(\alpha_1, \dots, \alpha_n)$ para ciertos elementos $\alpha_1, \dots, \alpha_n$ de alguna extensión K de k. La condición de que $\mathfrak{a}$ esté contenido en el ideal primo de $(\alpha_1, \dots, \alpha_n)$ significa que $(\alpha_1, \dots, \alpha_n)$ es solución del sistema definido por unos generadores de $\mathfrak{a}$. Según 7.2.7, el radical de $\mathfrak{a}$ está formado por los polinomios $q(x_1, \dots, x_n)$ que se anulan en todas las soluciones de tal sistema.

Fórmula de la Fibra

Definición: Sea $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación continua inducida por un morfismo de anillos $j\colon A \to B$, sea x un punto de $\operatorname{Spec} A$ y sea $\mathfrak{p}$ su ideal primo. Llamaremos **fibra** de ϕ sobre x al subespacio de $\operatorname{Spec} B$ formado por los puntos cuya imagen por ϕ es x:

$$\phi^{-1}(x) = \{y \in \operatorname{Spec} B\colon \ \phi(y) = x\}$$

Por otra parte, la localización del anillo B por la imagen del sistema multiplicativo $A - \mathfrak{p}$ se denotará B_x o $B_{\mathfrak{p}}$ y diremos que es la localización de B en el punto x o en el ideal primo $\mathfrak{p}$.

Lema 7.2.10 $\phi^{-1}(x) = \operatorname{Spec} B/\mathfrak{p}B$ *cuando el punto x es cerrado.*

Demostración: Como x es cerrado, $x = (\mathfrak{p})_0$, y 7.2.1 y 7.2.2 permiten concluir que

$$\phi^{-1}(x) \ = \ (\phi^{-1}((\mathfrak{p})_0) \ = \ (\mathfrak{p}B)_0 \ = \ \operatorname{Spec} B/\mathfrak{p}B$$

Fórmula de la Fibra: $\phi^{-1}(x) = \operatorname{Spec}\left(B_x/\mathfrak{p}B_x\right)$

Demostración: Sea $\mathfrak{q}$ el ideal primo de un punto y de $\operatorname{Spec} B$. La condición $\phi(y) = x$ significa que $\mathfrak{p} = A \cap \mathfrak{q}$, lo que implica que $\mathfrak{q}$ no corta a la imagen de $A - \mathfrak{p}$ en B. Luego, de acuerdo con 7.2.4, la fibra $\phi^{-1}(x)$ está contenida en $\operatorname{Spec} B_x$.

Ahora, el siguiente cuadrado conmutativo

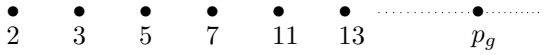
$$\begin{array}{ccc} \operatorname{Spec} B_x & \hookrightarrow & \operatorname{Spec} B \\ \big\downarrow \phi & & \big\downarrow \phi \\ \operatorname{Spec} A_x & \hookrightarrow & \operatorname{Spec} A \end{array}$$

prueba que $\phi^{-1}(x)$ coincide con la fibra de $\phi\colon \operatorname{Spec} B_x \to \operatorname{Spec} A_x$ sobre el único punto cerrado de $\operatorname{Spec} A_x$, definido por $\mathfrak{p}A_x$. Como $(\mathfrak{p}A_x)B_x = \mathfrak{p}B_x$, el lema anterior permite concluir que

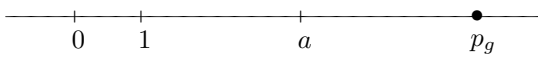
$$\phi^{-1}(x) = \operatorname{Spec}\left(B_x/\mathfrak{p}B_x\right)$$

7.3 Cálculos

(2) El espectro de $\mathbb{Z}$ tiene un punto cerrado por cada número primo y un punto genérico p_g definido por el ideal 0, que debe entenderse como el número primo genérico. Es irreducible y de dimensión 1:



(3) El espectro de $\mathbb{C}[x]$. Cada número complejo a define un punto cerrado, definido por el ideal maximal $(x-a)$. Además tiene un punto genérico p_g definido por el ideal 0. Es irreducible y de dimensión 1 :



(4) El espectro de $k[x]$, donde k es un cuerpo, tiene un punto cerrado por cada polinomio irreducible y unitario $p(x)$ con coeficientes en k, definido por el ideal maximal $\big(p(x)\big)$, y un punto genérico, definido por el ideal primo 0. Es irreducible y de dimensión 1.

(5) El espectro de $k[x]/\big(p(x)\big)$, donde $p(x)$ es un polinomio no constante con coeficientes en el cuerpo k, tiene un punto cerrado por cada factor irreducible y unitario de $p(x)$ en $k[x]$. Su dimensión es 0.

(6) El espectro de $\mathbb{C}[x,y]$. Consideremos la proyección

$$\phi:\ \operatorname{Spec}\mathbb{C}[x,y] \longrightarrow \operatorname{Spec}\mathbb{C}[x]$$

definida por el morfismo de $\mathbb{C}$-álgebras $\mathbb{C}[x] \to \mathbb{C}[x,y]$, $x \mapsto x$. Cada punto de $\operatorname{Spec}\mathbb{C}[x,y]$ está en la fibra de un único punto de $\operatorname{Spec}\mathbb{C}[x]$, así que vamos a calcular tales fibras. Los ideales primos de $\mathbb{C}[x]$ son el ideal 0 y los ideales maximales $(x-a)$, donde $a \in \mathbb{C}$.

Según 7.2.10, la fibra del punto $x = a$ coincide con

$$\operatorname{Spec}\mathbb{C}[x,y]/(x-a)$$

Ahora bien, $\mathbb{C}[x,y]/(x-a) \simeq \mathbb{C}[y]$, donde el isomorfismo transforma x en a, y concluimos que los ideales de los puntos de la fibra del punto $x = a$ son el ideal primo $(x-a)$ y los ideales maximales $(x-a, y-b)$, donde $b \in \mathbb{C}$. Es decir, la fibra del punto $x = a$ está formada por los puntos cerrados $x = a$, $y = b$ junto con el punto genérico de la recta $x = a$.

Según la fórmula de la fibra, la del punto genérico de $\operatorname{Spec}\mathbb{C}[x]$ coincide con el espectro de la localización de $\mathbb{C}[x,y]$ por todos los polinomios en x no nulos; es decir, con

$$\operatorname{Spec}\mathbb{C}(x)[y]$$

Ahora bien, por el lema de Gauss, los ideales primos no nulos de $\mathbb{C}(x)[y]$ son los ideales generados por los polinomios irreducibles en $\mathbb{C}[x,y]$ que sean de grado mayor o igual que 1 en y. Luego los ideales de los puntos de la fibra del punto genérico son el ideal 0 y los ideales primos $\big(p(x,y)\big)$, donde $p(x,y)$ es un polinomio irreducible de grado ≥ 1 en y. Es decir, la fibra del punto genérico de la recta afín está formada por el punto genérico del plano y los puntos genéricos de tales curvas $p(x,y)=0$.

En resumen, $\operatorname{Spec}\mathbb{C}[x,y]$ (o en general $\operatorname{Spec}k[x,y]$ cuando k es algebraicamente cerrado) tiene dimensión 2 y (como los polinomios irreducibles que tienen grado 0 en y son, salvo factores constantes, los polinomios $x-a$) sus puntos son:

–. Los puntos cerrados, que son los puntos $x=a$, $y=b$ donde a, $b\in\mathbb{C}$.

–. Los puntos genéricos de las curvas irreducibles $p(x,y)=0$.

–. El punto genérico del plano afín.

El punto genérico del plano es denso, mientras que las especializaciones del punto genérico de la curva irreducible $p(x,y)=0$ son los puntos cerrados (a,b) tales que $p(a,b)=0$.

Sea $q(x,y)$ un polinomio no constante con coeficientes complejos y sea $q(x,y)=p_1(x,y)^{m_1}\cdots p_r(x,y)^{m_r}$ su descomposición en factores irreducibles que no difieran en factores constantes. Entonces

$$(q)_0=(p_1)_0\cup\ldots\cup(p_r)_0$$

Luego los cerrados de $\operatorname{Spec}\mathbb{C}[x,y]$ son las intersecciones arbitrarias de uniones finitas de curvas irreducibles. De acuerdo con la Teoría de la Eliminación, dos curvas irreducibles distintas se cortan en un número finito de puntos cerrados, así que los cerrados (además del vacío y el total) son las uniones finitas de puntos cerrados y curvas irreducibles.

(7) El espectro de $\mathbb{C}[x,y]/\big(q(x,y)\big)$. Sea $q(x,y)$ un polinomio no constante con coeficientes complejos y sea $q(x,y)=p_1(x,y)^{m_1}\cdots p_r(x,y)^{m_r}$ su descomposición en factores irreducibles que no difieran en factores constantes. De acuerdo con 7.2.2 tenemos que $\operatorname{Spec}\mathbb{C}[x,y]/(q)=(q)_0$, así que la curva plana de ecuación $q(x,y)=0$ tiene dimensión 1 y sus puntos son:

–. Los puntos cerrados (a,b) donde $q(a,b)=0$.

–. Los puntos genéricos de las curvas irreducibles $p_i(x,y)=0$.

Por tanto sus componentes irreducibles son las curvas $p_i(x,y)=0$.

(8) El espectro de $\mathbb{C}[x,y]/(p,q)$. Si dos polinomios $p(x,y)$, $q(x,y)\in\mathbb{C}[x,y]$ no admiten factores comunes no constantes, se sigue que

$$\operatorname{Spec}\mathbb{C}[x,y]/(p,q)=(p)_0\cap(q)_0$$

tiene dimensión 0 y está formado por un número finito de puntos cerrados, que son las soluciones complejas del sistema de ecuaciones $p(x,y)=0$, $q(x,y)=0$.

(9) El espectro de $\mathbb{Z}[x]$. Consideremos el morfismo natural $\mathbb{Z}\to\mathbb{Z}[x]$ y la correspondiente aplicación continua

$$\phi\colon \operatorname{Spec}\mathbb{Z}[x]\longrightarrow \operatorname{Spec}\mathbb{Z}$$

Según 7.2.10, la fibra de cada número primo p coincide con el espectro de $\mathbb{Z}[x]/p\mathbb{Z}[x]$. Ahora bien, tenemos que

$$\mathbb{Z}[x]/p\mathbb{Z}[x]\simeq\mathbb{Z}[x]\otimes_{\mathbb{Z}}\mathbb{F}_p\simeq\mathbb{F}_p[x]$$

donde el isomorfismo transforma $[q(x)]$ en la reducción de $q(x)$ módulo p. Concluimos que los ideales de los puntos de la fibra de p son el ideal primo $p\mathbb{Z}[x]$ y los ideales maximales $(p,q(x))$, donde $q(x)$ es un polinomio cuya reducción módulo p sea irreducible en $\mathbb{F}_p[x]$.

Según la fórmula de la fibra, la del punto genérico de $\operatorname{Spec}\mathbb{Z}$ coincide con $\operatorname{Spec}\mathbb{Q}[x]$. De acuerdo con el lema de Gauss, los ideales primos no nulos de $\mathbb{Q}[x]$ están generados por los polinomios irreducibles en $\mathbb{Z}[x]$ no constantes. Luego los ideales de los puntos de la fibra del punto genérico son el ideal 0 y los ideales primos $(p(x))$ donde $p(x)$ es un polinomio no constante irreducible en $\mathbb{Z}[x]$. Concluimos que $\operatorname{Spec}\mathbb{Z}[x]$ es irreducible y de dimensión 2. Además, como los polinomios irreducibles constantes son, salvo el signo, los números primos, concluimos que los ideales primos de $\mathbb{Z}[x]$ son:

–. Los ideales maximales $(p,q(x))$, donde p es un número primo y $q(x)$ es un polinomio cuya reducción módulo p sea irreducible.

–. Los ideales primos $(p(x))$ generados por un polinomio $p(x)$ irreducible en $\mathbb{Z}[x]$ (lo que incluye los números primos).

–. El ideal primo 0.

7.4 Variedades Algebraicas Afines

Definición: Llamaremos **variedad algebraica afín** sobre un cuerpo k al par (X,A) formado por una k-álgebra de tipo finito A y su espectro $X=\operatorname{Spec}A$. Diremos que la variedad es íntegra, reducida, de dimensión n, etc., si lo es la k-álgebra A, y que es conexa, irreducible, etc., si lo es el espacio topológico X.

Si no origina confusión, tal variedad se denota únicamente X, y la correspondiente k-álgebra se denota $\mathcal{O}(X)$ ó $A(X)$ y se dice que es el anillo de **funciones algebraicas** o el **anillo afín** de X. Así, si A es una k-álgebra de tipo finito, la variedad algebraica afín $(\operatorname{Spec}A,A)$ se denotará $\operatorname{Spec}A$. Llamaremos **espacio**

afín n-dimensional sobre el cuerpo k a la variedad algebraica afín $\mathbb{A}_{n,k}$ definida por el anillo de polinomios $k[x_1, \ldots, x_n]$.

$$\mathbb{A}_{n,k} \;:=\; \operatorname{Spec} k[x_1, \ldots, x_n]$$

Sean X, Y dos variedades algebraicas afines sobre k. Llamaremos **morfismos** de X en Y a los morfismos de k-álgebras de $\mathcal{O}(Y)$ en $\mathcal{O}(X)$. El conjunto de tales morfismos se denotará $\operatorname{Hom}_k(X, Y)$:

$$\operatorname{Hom}_k(X, Y) \;=\; \operatorname{Hom}_{k\text{-}alg}\left(\mathcal{O}(Y), \mathcal{O}(X)\right)$$

Por definición un morfismo $X \to Y$ está determinado por un morfismo de k-álgebras $\mathcal{O}(Y) \to \mathcal{O}(X)$; luego induce una aplicación continua

$$X = \operatorname{Spec} \mathcal{O}(X) \longrightarrow \operatorname{Spec} \mathcal{O}(Y) = Y \;,$$

pero no está determinado por tal aplicación continua. Por ejemplo, la identidad y la conjugación compleja son dos morfismos de variedades algebraicas reales $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} \mathbb{C}$ que inducen la misma aplicación continua, pues el espacio topológico $\operatorname{Spec} \mathbb{C}$ tiene un único punto.

La **composición** de morfismos entre variedades algebraicas afines se define por ser la composición de los correspondientes morfismos de k-álgebras. La **identidad** de una variedad algebraica X es el morfismo $X \to X$ definido por la identidad de $\mathcal{O}(X)$. Diremos que un morfismo $\phi\colon X \to Y$ es un **isomorfismo** si existe algún morfismo $\psi\colon Y \to X$ tal que $\psi \circ \phi$ es la identidad de X y $\phi \circ \psi$ es la identidad de Y. Los isomorfismos de X con Y son los morfismos definidos por isomorfismos de k-álgebras de $\mathcal{O}(Y)$ con $\mathcal{O}(X)$.

Puntos Racionales: Sea x un punto cerrado de una variedad algebraica afín X sobre un cuerpo k y sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}(X)$ formado por las funciones que se anulan en x. Diremos que x es un punto **racional** si el morfismo estructural $k \to \mathcal{O}(X)/\mathfrak{m}$ es un isomorfismo; es decir, si $\mathcal{O}(X)/\mathfrak{m}$ es una extensión trivial de k. Los puntos racionales de X se corresponden con los morfismos de k-álgebras $\delta\colon \mathcal{O}(X) \to k$, pues cada uno de estos morfismos δ está determinado por su núcleo $\mathfrak{m}$, ya que $\delta(f) = a$ justamente cuando $f - a \in \mathfrak{m}$. Es decir:

$$\begin{bmatrix}\text{puntos racionales}\\ \text{de la variedad } X\end{bmatrix} = \operatorname{Hom}_{k\text{-}alg}\big(\mathcal{O}(X), k\big) = \operatorname{Hom}_k(\operatorname{Spec} k, X)$$

Según 3.5.5, cada ideal maximal $(x_1 - a_1, \ldots, x_n - a_n)$ del anillo de polinomios $k[x_1, \ldots, x_n]$ define un punto racional del espacio afín $\mathbb{A}_{n,k}$, que se denota $(a_1, \ldots, a_n)$. Así se obtienen todos los puntos racionales de $\mathbb{A}_{n,k}$, pues si $k = k[x_1, \ldots, x_n]/\mathfrak{m}$ y $a_i = [x_i]$, entonces $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}$ y se concluye que $(x_1 - a_1, \ldots, x_n - a_n) = \mathfrak{m}$, al ser $(x_1 - a_1, \ldots, x_n - a_n)$ un ideal maximal.

Ahora, cuando $\mathcal{O}(X) \simeq k[x_1,\dots,x_n]/(p_1,\dots,p_r)$, de acuerdo con 6.1.2, los puntos racionales de X son las soluciones en k del sistema de ecuaciones

$$\left.\begin{array}{c} p_1(x_1,\dots,x_n)=0 \\ \cdots\cdots\cdots \\ p_r(x_1,\dots,x_n)=0 \end{array}\right\}$$

Es decir, los puntos racionales de una variedad algebraica sobre k son sus puntos con coordenadas en k, mientras que los restantes puntos vienen definidos por soluciones del sistema en otras extensiones de k.

Una variedad algebraica puede carecer de puntos racionales sin que por ello sea vacía, como es el caso de la curva $x^2+y^2=-1$ sobre los números reales, o pasar por todos los puntos racionales del plano afín sin que por eso coincida con el plano, como es el caso de la curva $x^p+y^p=x+y$ sobre el cuerpo finito $\mathbb{F}_p$:

Las variedades algebraicas no están determinadas por sus puntos racionales.

Subvariedades Cerradas: Sea $\mathfrak{a}=(p_1,\dots,p_r)$ un ideal de un anillo de polinomios $k[x_1,\dots,x_n]$. El teorema 7.2.2 afirma que $k[x_1,\dots,x_n]/\mathfrak{a}$ define una estructura de variedad algebraica afín sobre $(\mathfrak{a})_0 \subset \mathbb{A}_{n,k}$, y diremos que es la **subvariedad cerrada** del espacio afín $\mathbb{A}_{n,k}$ definida por el sistema de ecuaciones

$$\left.\begin{array}{c} p_1(x_1,\dots,x_n)=0 \\ \cdots\cdots\cdots \\ p_r(x_1,\dots,x_n)=0 \end{array}\right\}$$

En general, si consideramos una variedad algebraica afín arbitraria X y un ideal $\mathfrak{a}$ de su anillo de funciones algebraicas $\mathcal{O}(X)$, el teorema 7.2.2 muestra que $\mathcal{O}(X)/\mathfrak{a}$ define una estructura de variedad algebraica afín sobre los ceros de $\mathfrak{a}$. Diremos que $Y=((\mathfrak{a})_0,\ \mathcal{O}(X)/\mathfrak{a})$ es la **subvariedad cerrada** de X definida por el ideal $\mathfrak{a}$, y depende del ideal $\mathfrak{a}$, no sólo del cerrado $(\mathfrak{a})_0$.

La **restricción** de una función algebraica $f\in\mathcal{O}(X)$ a esta subvariedad cerrada Y se define por ser su clase de restos $\bar{f}\in\mathcal{O}(X)/\mathfrak{a}$, de modo que la restricción de funciones $\mathcal{O}(X)\to\mathcal{O}(Y)$ es precisamente la proyección canónica. La **inclusión natural** $Y\to X$ se define por ser el morfismo de variedades algebraicas asociado al morfismo de restricción $\mathcal{O}(X)\to\mathcal{O}(Y)$.

Por ejemplo, el punto $t=0$ de la recta afín es el único cero de cualquiera de los ideales (t^n), $n\geq 1$. Sin embargo estos ideales definen diferentes estructuras de variedad algebraica afín sobre tal punto, pues las k-álgebras $k[\,t\,]/(t^n)$ no son isomorfas.

No obstante, dado un cerrado Y de una variedad algebraica afín X, de 7.2.7 se sigue que entre todos los ideales $\mathfrak{a}$ de $\mathcal{O}(X)$ cuyos ceros sean Y existe sólo uno tal que el anillo $\mathcal{O}(X)/\mathfrak{a}$ es reducido, a saber, el ideal formado por todas las funciones algebraicas sobre X que se anulan en Y.

Por tanto, *cada cerrado de una variedad algebraica afín hereda una estructura bien definida de variedad algebraica afín reducida* y, en general, soporta muchas otras subvariedades cerradas que no son reducidas.

Sea X una variedad algebraica afín. Por definición el anillo de funciones $\mathcal{O}(X)$ es una k-álgebra de tipo finito; pero admite diferentes sistemas de generadores $\{\xi_1, \ldots, \xi_n\}$. Cada uno define un morfismo de k-álgebras $k[x_1, \ldots, x_n] \to \mathcal{O}(X)$, $x_i \mapsto \xi_i$, que es epiyectivo e induce un isomorfismo $k[x_1, \ldots, x_n]/\mathfrak{a} \simeq \mathcal{O}(X)$. Es decir, *cada sistema de n generadores de $\mathcal{O}(X)$ define un morfismo $X \to \mathbb{A}_{n,k}$ que induce un isomorfismo de X con una subvariedad cerrada de $\mathbb{A}_{n,k}$.*

Vemos así que toda variedad algebraica afín es isomorfa a una subvariedad cerrada de un espacio afín, pero lo es de muchos modos y ninguno canónico. Además, el menor número n tal que X pueda sumergirse como subvariedad cerrada de $\mathbb{A}_{n,k}$ es el menor cardinal de los sistemas de generadores de $\mathcal{O}(X)$.

Por ejemplo, consideremos la curva plana C de ecuación $y = x^2$. Su anillo de funciones algebraicas $\mathcal{O}(C) = k[\xi, \eta] = k[x, y]/(y - x^2)$ está generado por ξ y el morfismo $k[\,t\,] \to k[\xi, \eta]$, $t \mapsto \xi$, es un isomorfismo, pues su inverso es el morfismo $k[\xi, \eta] \to k[\,t\,]$, $\xi \mapsto t$, $\eta \mapsto t^2$. La curva C es isomorfa a la recta afín.

Abiertos Básicos: Sea U un abierto básico de una variedad algebraica afín X; es decir, $U = U_f = X - (f)_0$ para alguna función $f \in \mathcal{O}(X)$. La localización de $\mathcal{O}(X)$ por el sistema multiplicativo de las funciones que no se anulan en ningún punto de U es, de acuerdo con 7.2.5, una k-álgebra de tipo finito que sólo depende de U, no de f, y cuyo espectro coincide con U. Obtenemos así una estructura natural de variedad algebraica afín en todo abierto básico de una variedad algebraica afín. Por definición

$$\mathcal{O}(U) \,=\, \mathcal{O}(X)\Big[\, f^{-1}\,\Big]$$

La **restricción** de una función algebraica $g \in \mathcal{O}(X)$ a un abierto básico U_f se define por ser su localización $g/1 \in \mathcal{O}(X)_f$, de modo que la restricción de funciones $\mathcal{O}(X) \to \mathcal{O}(U_f)$ es precisamente el morfismo de localización.

La **inclusión natural** $U_f \to X$ se define por ser el morfismo de variedades algebraicas asociado al morfismo de restricción $\mathcal{O}(X) \to \mathcal{O}(U_f)$.

No todos los abiertos de una variedad algebraica afín son básicos. En efecto, sea U el complementario del origen en el plano afín complejo $\mathbb{A}_{2,\mathbb{C}}$. Del teorema de D'Alembert se sigue que todo polinomio no constante se anula en algún punto de U, así que la localización de $\mathbb{C}\,[x, y]$ por los polinomios que no se anulan en ningún punto de U coincide con el propio anillo $\mathbb{C}\,[x, y]$, de modo que su espectro es todo el plano afín: no es U. Luego U no es un abierto básico de $\mathbb{A}_{2,\mathbb{C}}$.

Morfismos: Sea X la subvariedad de $\mathbb{A}_{n,k}$ definida por un sistema de ecuaciones $p_1(x_1, \ldots, x_n) = \ldots = p_r(x_1, \ldots, x_n) = 0$, y sea Y la subvariedad de $\mathbb{A}_{m,k}$ definida por otro sistema de ecuaciones $q_1(y_1, \ldots, y_m) = \ldots = q_s(y_1, \ldots, y_m) = 0$.

Cada morfismo de $\phi\colon X \to Y$ viene dado por un morfismo de k-álgebras $\mathcal{O}(Y) = k[\bar{y}_1, \dots, \bar{y}_m] \to \mathcal{O}(X) = k[\bar{x}_1, \dots, \bar{x}_n]$, definido por ciertas ecuaciones

$$\begin{cases} y_1 = f_1(x_1, \dots, x_n) \\ \cdots\cdots\cdots \\ y_m = f_m(x_1, \dots, x_n) \end{cases}$$

con la condición de que $q_h\big(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\big) = 0$, $1 \le h \le s$.

Si consideramos el punto de X definido por ciertos elementos $(\alpha_1, \dots, \alpha_n)$ de una extensión K de k, entonces su imagen por ϕ es precisamente el punto $(f_1(\alpha_1, \dots, \alpha_n), \dots, f_m(\alpha_1, \dots, \alpha_n))$, por lo que también diremos que ϕ es el morfismo de ecuaciones

$$\phi(x_1, \dots, x_n) = \big(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\big)$$

En efecto, si $\mathfrak{p}$ es el núcleo del morfismo $\mathcal{O}(X) \to K$, $\bar{x}_i \mapsto \alpha_i$, entonces es claro que $\mathcal{O}(Y) \cap \mathfrak{p}$ es el núcleo de la composición $\mathcal{O}(Y) \to \mathcal{O}(X) \to K$, $\bar{y}_j \mapsto f_j(\alpha_1, \dots, \alpha_n)$.

Por ejemplo, hemos visto que el morfismo $\phi\colon \mathbb{A}_1 \to C$, $\phi(t) = (t, t^2)$, de la recta afín en la curva plana $y = x^2$ es un isomorfismo, y el morfismo inverso $\psi\colon C \to \mathbb{A}_1$ es el morfismo $\psi(x, y) = x$.

Sea C la curva plana de ecuación $xy = 1$ y sea $U = \operatorname{Spec} k[t, t^{-1}]$ el abierto complementario del punto $t = 0$ en la recta afín. Consideremos los morfismos

$$\begin{aligned} \phi &: U \longrightarrow C \quad ; \quad \phi(t) = (t, t^{-1}) \\ \psi &: C \longrightarrow U \quad ; \quad \psi(x, y) = x \end{aligned}$$

Como $(\phi\psi)(x, y) = \phi(x) = (x, x^{-1}) = (x, y)$, tenemos que $\phi\psi$ es la identidad. Análogamente $(\psi\phi)(t) = \psi(t, t^{-1}) = t$, así que $\psi\phi$ también es la identidad. Concluimos que ϕ y ψ son isomorfismos mutuamente inversos.

Funciones: Sea X una variedad algebraica afín. Según hemos visto, cada morfismo $X \to \mathbb{A}_1$ viene dado por una ecuación $t = f(x_1, \dots, x_n)$, donde la función $f \in \mathcal{O}(X)$ es arbitraria: *el concepto de función algebraica coincide con el de morfismo valorado en la recta afín:*

$$\operatorname{Hom}_k(X, \mathbb{A}_1) \;=\; \operatorname{Hom}_{k\text{-}alg}\big(k[\,t\,], \mathcal{O}(X)\big) \;=\; \mathcal{O}(X)$$

y la condición de que f se anule en un punto $x \in X$ significa que la imagen de x por el morfismo $f\colon X \to \mathbb{A}_1$ es el punto $t = 0$ de la recta afín.

Entornos Infinitesimales: Sea x un punto cerrado de una variedad algebraica afín X y sea $\mathfrak{m}$ su ideal maximal. La k-álgebra $\mathcal{O}(X)/\mathfrak{m}^{r+1}$ es de tipo finito y la variedad algebraica afín $U_r = \operatorname{Spec}(\mathcal{O}(X)/\mathfrak{m}^{r+1})$ se llama **r-ésimo entorno infinitesimal** de x en X. Cada función $f \in \mathcal{O}(X)$ define una función $\bar{f} \in \mathcal{O}(X)/\mathfrak{m}^{r+1} = \mathcal{O}(U_r)$ llamada **desarrollo de Taylor** de orden r de f en x pues, cuando X es un espacio afín real o complejo y x es un punto racional, coincide con el desarrollo de Taylor clásico.

Desarrollar por Taylor hasta el orden r en un punto x es restringir al entorno infinitesimal U_r de x.

Producto Directo: Sean X, Y dos variedades algebraicas afines sobre un cuerpo k. Si $\mathcal{O}(X) = k[\xi_1, \ldots, \xi_n]$ y $\mathcal{O}(Y) = k[\eta_1, \ldots, \eta_m]$, entonces los productos tensoriales $\xi_i \otimes \eta_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ generan la k-álgebra $\mathcal{O}(X) \otimes_k \mathcal{O}(Y)$. Luego $\mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ es una k-álgebra de tipo finito y define una variedad algebraica afín que se llama **producto directo** de X por Y y se denotará $X \times_k Y$, o simplemente $X \times Y$ si la referencia al cuerpo k se da por supuesta. Por definición

$$\mathcal{O}(X \times_k Y) \;=\; \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$$

y los morfismos naturales $j_1 \colon \mathcal{O}(X) \to \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$, $j_2 \colon \mathcal{O}(Y) \to \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ definen sendos morfismos canónicos

$$\pi_1 : X \times_k Y \longrightarrow X \quad , \quad \pi_2 : X \times_k Y \longrightarrow Y$$

que reciben el nombre de proyecciones de $X \times Y$ sobre sus dos factores.

Cada morfismo $\phi \colon Z \to X \times Y$ de una variedad algebraica afín Z en el producto directo define, por composición con las proyecciones sobre los factores, morfismos $\pi_1 \circ \phi \colon Z \to X$ y $\pi_2 \circ \phi \colon Z \to Y$. La propiedad universal del producto tensorial de álgebras afirma precisamente que así obtenemos biyecciones naturales

$$\operatorname{Hom}_k(Z, X \times_k Y) \;=\; \operatorname{Hom}_k(Z, X) \times \operatorname{Hom}_k(Z, Y)$$

de forma que para definir un morfismo de una variedad Z en $X \times Y$ basta definir un morfismo de Z en X y otro de Z en Y. Con precisión, dado un par de morfismos $f \colon Z \to X$, $g \colon Z \to Y$, existe un único morfismo $f \times g \colon Z \to X \times Y$ tal que su composición con π_1 es f y su composición con π_2 es g. Nótese que cada punto del producto directo $X \times Y$ define un punto de X y otro de Y, sin más que tomar sus imágenes por las proyecciones sobre los factores; pero no está determinado por sus proyecciones: *como conjunto $X \times Y$ no coincide con el conjunto de parejas (x, y) donde $x \in X$, $y \in Y$.* Por ejemplo, el punto genérico del plano afín $\mathbb{A}_2 = \mathbb{A}_1 \times \mathbb{A}_1$ se proyecta sobre el punto genérico de cada factor; pero lo mismo le ocurre al punto genérico de la diagonal $x = y$ o de cualquier otra curva plana irreducible cuya ecuación dependa de ambas indeterminadas.

Dado un morfismo $\psi\colon X \to Y$, existe un único morfismo $X \to X \times Y$ que es la identidad al componer con la primera proyección y coincide con ψ al componer con la segunda proyección. Este morfismo $X \to X \times Y$ recoge nuestra intuición de la gráfica de un morfismo. En particular, cuando $Y = X$ y ψ es la identidad de X, el correspondiente morfismo $X \to X \times X$ se llama **morfismo diagonal** y viene definido por el morfismo de k-álgebras $\mathcal{O}(X) \otimes_k \mathcal{O}(X) \to \mathcal{O}(X)$, $f \otimes g \mapsto fg$. Por otra parte, el isomorfismo $k[x_1, \ldots, x_n] \otimes_k k[y_1, \ldots, y_m] = k[x_1, \ldots, x_n, y_1, \ldots y_m]$ afirma que $\mathbb{A}_{n,k} \times_k \mathbb{A}_{m,k} = \mathbb{A}_{n+m,k}$.

Unión Disjunta: Con las notaciones del apartado anterior, $\mathcal{O}(X) \oplus \mathcal{O}(Y)$ es una k-álgebra generada por los elementos $(\xi_1, 0), \ldots, (\xi_n, 0), (0, \eta_1), \ldots, (0, \eta_m)$. La correspondiente variedad algebraica afín se llamará **unión disjunta** de X e Y, y se denotará $X \coprod Y$. Según 7.2.3, como espacio topológico $X \coprod Y$ coincide con la unión disjunta de X e Y. Por definición

$$\mathcal{O}(X \coprod Y) \;=\; \mathcal{O}(X) \oplus \mathcal{O}(Y)$$

y los morfismos naturales $p_1\colon \mathcal{O}(X) \oplus \mathcal{O}(Y) \to \mathcal{O}(X)$, $p_2\colon \mathcal{O}(X) \oplus \mathcal{O}(Y) \to \mathcal{O}(Y)$ definen sendos morfismos canónicos

$$i_1\colon X \longrightarrow X \coprod Y \quad , \quad i_2\colon Y \longrightarrow X \coprod Y$$

y cada morfismo $\phi\colon X \coprod Y \to Z$ de la unión disjunta en una variedad algebraica afín Z induce dos morfismos $\phi \circ i_1\colon X \to Z$, $\phi \circ i_2\colon Y \to Z$. Obtenemos así una biyección natural

$$\mathrm{Hom}_k(X \coprod Y, Z) \;=\; \mathrm{Hom}_k(X, Z) \times \mathrm{Hom}_k(Y, Z)$$

de forma que para definir un morfismo de $X \coprod Y$ en Z basta definir un morfismo de X en Z y otro de Y en Z. Con precisión, dado un par de morfismos $\psi\colon X \to Z$, $\varphi\colon Y \to Z$, existe un único morfismo $X \coprod Y \to Z$ tal que su composición con j_1 es ψ y su composición con j_2 es φ. En efecto, dado un par de morfismos de k-álgebras $j_1\colon B \to \mathcal{O}(X)$, $j_2\colon B \to \mathcal{O}(Y)$, existe un único morfismo de k-álgebras

$$j_1 \oplus j_2\colon B \longrightarrow \mathcal{O}(X) \oplus \mathcal{O}(Y) \;, \quad (j_1 \oplus j_2)(b) = \big(j_1(b), j_2(b)\big)$$

tal que su composición con p_1 es j_1 y su composición con p_2 es j_2.

Así, el isomorfismo $k[x,y]/(y^2 + y) \simeq k[t] \oplus k[t]$; $\bar{x} \mapsto (t, t)$, $\bar{y} \mapsto (0, -1)$, expresa que el par de rectas paralelas $y(y + 1) = 0$ es la unión disjunta de dos rectas afines.

Cambio del Cuerpo Base: Sea X una variedad algebraica afín sobre un cuerpo k y sea $k \to K$ una extensión de k. Si $\mathcal{O}(X) = k[\xi_1, \ldots, \xi_n]$, entonces $\mathcal{O}(X) \otimes_k K = K[\xi_1 \otimes 1, \ldots, \xi_n \otimes 1]$ es una K-álgebra de tipo finito y define una variedad algebraica

afín sobre K, que denotaremos X_K y diremos que se obtiene de X por el *cambio de base* $k \to K$:

$$\mathcal{O}(X_K) \,=\, \mathcal{O}(X)_K$$

Por ejemplo, el isomorfismo natural

$$k[x_1,\dots,x_n]/(p_1,\dots,p_r) \otimes_k K = K[x_1,\dots,x_n]/(p_1,\dots,p_r)$$

afirma que si X es la subvariedad del espacio afín $\mathbb{A}_{n,k}$ definida por ciertas ecuaciones

$$\left.\begin{array}{c} p_1(x_1,\dots,x_n)=0 \\ \cdots\cdots\cdots \\ p_r(x_1,\dots,x_n)=0 \end{array}\right\}$$

X_K es la subvariedad de $\mathbb{A}_{n,K}$ definida por las mismas ecuaciones.

El isomorfismo $k[x_1,\dots,x_n] \otimes_k K = K[x_1,\dots,x_n]$ afirma que, al cambiar de base el espacio afín $\mathbb{A}_{n,k}$, obtenemos el espacio afín $\mathbb{A}_{n,K}$.

Nota: Nos hemos limitado a considerar álgebras de tipo finito sobre un cuerpo para simplificar la exposición; pero esta restricción es artificial. Los pares (X, A) donde A es un anillo conmutativo con unidad y X es su espectro coinciden esencialmente con los *esquemas afines* introducidos por Grothendieck (n. 1928) a finales de los años 50. El ámbito de los esquemas afines permite tratar de forma unificada la Aritmética y la Geometría afín, pues en él tienen cabida tanto los espacios afines sobre un cuerpo como el espectro de $\mathbb{Z}$ o de los otros anillos que intervienen en la Aritmética, e incluso conceptos tan sorprendentes como el de recta afín sobre los números enteros

$$\mathbb{A}_{1,\mathbb{Z}} \,:=\, \operatorname{Spec}\mathbb{Z}[x]$$

que permiten abordar geométricamente los problemas aritméticos. Los resultados de la teoría de anillos admiten su reformulación en términos de esquemas afines; aunque, por sencillez, sólo hayamos considerado el caso de las álgebras de tipo finito sobre un cuerpo.

Incluso en el estudio de las variedades algebraicas afines es necesario introducir los esquemas afines. Por ejemplo, el anillo local $\mathcal{O}_x = \mathcal{O}(X)_x$ de una variedad algebraica afín X en un punto x, que determina las propiedades de X en el entorno de x, casi nunca es una k-álgebra de tipo finito, ni (cuando x no es cerrado) las álgebras $\mathcal{O}_x/\mathfrak{p}_x^{r+1}$, que determinan el comportamiento infinitesimal de X en el punto x. Es decir, tanto $\operatorname{Spec}(\mathcal{O}_x)$ como $\operatorname{Spec}(\mathcal{O}_x/\mathfrak{p}_x^{r+1})$ no son variedades algebraicas afines, aunque sí son esquemas afines.

Capítulo 8

Localización

Uno de los procesos geométricos más básicos es el de *localizar* la atención en un entorno de un punto; pues nos permite distinguir entre propiedades locales y globales. Una propiedad es *local* cuando sólo depende del comportamiento en un entorno de cada punto. Por ejemplo la continuidad de las funciones consideradas en Topología, la derivabilidad de las funciones estudiadas en Análisis, la conexión local o la compacidad local de los espacios topológicos son propiedades locales. Por el contrario, una propiedad es *global* cuando no es local; es decir, cuando depende de todo el espacio considerado. Por ejemplo el concepto de función acotada no es local, ni el de espacio compacto o conexo. Cuando se pasa a estudiar una cuestión en un abierto U en vez de hacerlo en todo el espacio inicialmente considerado, las funciones que no se anulan en ningún punto de U pasan a ser invertibles. Si, como es lo más usual, no queremos fijar un entorno de un punto dado x, sino considerar un entorno suficientemente pequeño que dependa de los datos en cuestión y no sólo del punto dado, las funciones que no se anulan en x pasan a ser invertibles. Por tanto, dado un anillo A, las fracciones f/g cuyo denominador no se anula en cierto punto $x \in \operatorname{Spec} A$ deben entenderse como funciones definidas en un "entorno suficientemente pequeño" de x. Aunque no tengamos una definición rigurosa del concepto "entorno suficientemente pequeño" que tan a menudo usamos para indicar el significado intuitivo de muchos teoremas, sorprendentemente la construcción de los anillos de fracciones permite introducir con toda precisión un anillo[1] $A_x = \{f/g\}$ de "funciones definidas en un entorno suficientemente pequeño de x".

[1] De nuevo, al igual que en el caso de las variedades algebraicas, no tenemos una definición rigurosa de cierto espacio, en este caso "el entorno suficientemente pequeño de x"; pero disponemos de un anillo de funciones sobre el mismo, que permite introducirlo como el espacio de sus ideales primos. Una y otra vez nos encontramos con una observación crucial: el punto de partida de la Geometría no debe ser el espacio, para introducir luego las funciones, sino las funciones, que determinan el espacio y su estructura. En esto la Geometría coincide con la Física: las observaciones determinan la estructura el Universo.

Este proceso de localización nos permitirá diferenciar los problemas y propiedades locales de los que son globales. Por ejemplo, una propiedad de los módulos (respectivamente de sus morfismos) es local cuando la condición necesaria y suficiente para que un A-módulo M (un morfismo $f\colon M \to N$) tenga tal propiedad es que la tenga el A_x-módulo $M \otimes_A A_x$ (el morfismo $f\colon M \otimes_A A_x \to N \otimes_A A_x$) para todo punto $x \in \operatorname{Spec} A$. Es absolutamente necesario distinguir entre problemas locales (enunciados con propiedades locales) y globales; pues los problemas locales basta estudiarlos después del cambio de base $A \to A_x$ y el anillo A_x es mucho más sencillo que A.

Un resultado central de este capítulo será demostrar que la anulación de un módulo es una cuestión local y que, por tanto, también son locales todos los problemas que puedan reducirse a la anulación de un módulo. Así, la inyectividad y epiyectividad de un morfismo de A-módulos $f\colon M \to N$, que equivalen a la anulación de $\operatorname{Ker} f$ y $N/\operatorname{Im} f$ respectivamente, la inclusión $N \subseteq N'$ entre dos submódulos, que se reduce a la anulación de $(N + N')/N$, etc. Este resultado coloca en el centro de nuestra atención los anillos A_x, porque la mayor parte de los problemas basta estudiarlos después de sustituir el anillo inicial A por su localización A_x en un punto x. Ahora bien, estos anillos A_x no son arbitrarios, sino que están caracterizados por el hecho de tener un único ideal maximal: son los anillos llamados *locales*.

Sea $\mathcal{O}$ un anillo con un único ideal maximal $\mathfrak{m}$. El resultado fundamental en el estudio de los módulos sobre estos anillos es el sorprendente lema de Nakayama (19121964): *La anulación de un $\mathcal{O}$-módulo de tipo finito equivale a la del $(\mathcal{O}/\mathfrak{m})$-espacio vectorial $M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = M/\mathfrak{m}M$*, es una cuestión de Álgebra Lineal. Este lema explica la enorme potencia del Cálculo Diferencial en la resolución de problemas locales. El Cálculo Diferencial, que es el estudio de las relaciones despreciando infinitésimos de segundo orden, es decir, del espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ (o de los espacios vectoriales $\mathfrak{m}^r/\mathfrak{m}^{r+1}$ si se consideran derivadas sucesivas), permite obtener resultados exactos[2] en el anillo local $\mathcal{O}$; o sea, absolutamente válidos en un entorno suficientemente pequeño del punto considerado x. En resumen, este capítulo presenta un procedimiento sistemático para tratar los problemas locales que puedan enunciarse en términos de A-módulos y sus morfismos. Primero se reducen a los anillos A_x; luego, mediante el lema de Nakayama, a cuestiones infinitesimales que se resuelven con el Álgebra Lineal. Ahora bien, para poder aplicar el lema de Nakayama es necesario que los módulos sean de tipo finito, de modo que para estudiar sistemáticamente los ideales con este método es necesario suponer que todos los ideales del anillo son finito-generados. Los anillos que satisfacen tal condición reciben el nombre de *noetherianos*, en honor de E. Noether (1882-1935). La gran importancia de estos anillos radica en el fundamental Teorema de la base de Hilbert (1862-1943): los anillos de polinomios con coeficientes en un cuerpo

[2] No sólo aproximadamente válidos, como pudiera esperarse después de despreciar términos muy pequeños, pero no nulos.

o en $\mathbb{Z}$ son noetherianos, así como sus cocientes y localizaciones. Vemos así que la práctica totalidad de los anillos involucrados en la Geometría Algebraica y la Aritmética son noetherianos, de forma que estos anillos proporcionan el marco natural para desarrollar su estudio unificado. También demostraremos que todo ideal de un anillo noetheriano viene definido por condiciones infinitesimales en un número finito de puntos del espectro, que es el resultado fundamental de la teoría de ideales en los anillos noetherianos.

8.1 Localización de Módulos

Definición: Sea S un sistema multiplicativo de un anillo A. Si M es un A-módulo, denotaremos $S^{-1}M$ ó M_S el cociente de $M \times S$ respecto de la relación de equivalencia

$$(m,s) \equiv (n,t) \;\Leftrightarrow\; \text{existen } u,v \in S \text{ tales que } mu = nv \text{ y } su = tv$$

y la imagen de cada pareja (m,s) en el cociente $S^{-1}M$ se denotará m/s.

Las operaciones

$$\frac{m}{s} + \frac{n}{t} = \frac{tm+sn}{st}$$
$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

definen en $S^{-1}M$ una estructura de $S^{-1}A$-módulo y diremos que es la **localización** de M por S. La aplicación canónica

$$\gamma\colon M \longrightarrow S^{-1}M\ , \quad \gamma(m) = m/1$$

es morfismo de A-módulos y diremos que es el **morfismo de localización**.

También diremos que $\gamma(m) = m/1$ es la localización de m por S. Por definición, *la condición necesaria y suficiente para que la localización de un elemento $m \in M$ por S sea nula es que $sm = 0$ para algún $s \in S$.*

Cada morfismo de A-módulos $f\colon M \to N$ induce de modo natural una aplicación, llamada **localización** de f por S:

$$S^{-1}f\colon S^{-1}M \longrightarrow S^{-1}N\ , \quad (S^{-1}f)(m/s) = f(m)/s$$

que es morfismo de $S^{-1}A$-módulos.

Es inmediato comprobar que la localización de morfismos conserva composiciones y combinaciones A-lineales:

$$S^{-1}(f \circ g) = (S^{-1}f) \circ (S^{-1}g)$$
$$S^{-1}(af + bg) = a(S^{-1}f) + b(S^{-1}g)$$

Propiedad Universal: *Sea S un sistema multiplicativo de un anillo A y sea M un A-módulo. Si N es un $S^{-1}A$-módulo y $f\colon M \to N$ es un morfismo de A-módulos, entonces existe un único morfismo de $S^{-1}A$-módulos $\phi\colon S^{-1}M \to N$ tal que $f = \phi \circ \gamma$; es decir, $\phi(m/1) = f(m)$ para todo $m \in M$:*

$$\mathrm{Hom}_A(M,N) \;=\; \mathrm{Hom}_{S^{-1}A}(S^{-1}M,N)$$

Demostración: La unicidad es evidente, pues tal morfismo ϕ ha de ser $\phi(m/s) = s^{-1}f(m)$. En cuanto a la existencia, veamos que tal igualdad define una aplicación de $S^{-1}M$ en N:

$$\phi(um/us) = (su)^{-1}f(um) = s^{-1}u^{-1}uf(m) = s^{-1}f(m)$$

Ahora es inmediato comprobar que esta aplicación ϕ es morfismo de $S^{-1}A$-módulos.

Teorema 8.1.1 $M \otimes_A (S^{-1}A) \;=\; S^{-1}M$

Demostración: De acuerdo con la propiedad universal del cambio de base, el morfismo de localización $M \to S^{-1}M$, $m \mapsto m/1$, define un morfismo de $S^{-1}A$-módulos

$$M \otimes_A (S^{-1}A) \longrightarrow S^{-1}M \;, \quad m \otimes (a/s) \mapsto am/s$$

Recíprocamente, por la propiedad universal de la localización, el morfismo de cambio de base $M \to M \otimes_A (S^{-1}A)$, $m \mapsto m \otimes 1$, define un morfismo de $S^{-1}A$-módulos

$$S^{-1}M \longrightarrow M \otimes_A (S^{-1}A) \;, \quad m/s \mapsto m \otimes (1/s)$$

Es sencillo comprobar que ambos morfismos son mutuamente inversos.

Corolario 8.1.2 $S^{-1}(\oplus_i M_i) \;=\; \oplus_i (S^{-1}M_i)$
$S^{-1}(M \otimes_A N) \;=\; (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$.

Teorema 8.1.3 *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión exacta de A-módulos. Si S es un sistema multiplicativo de A, entonces también es exacta la sucesión*

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

Demostración: $\mathrm{Im}(S^{-1}f) \subseteq \mathrm{Ker}(S^{-1}g)$ porque

$$(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = 0$$

Recíprocamente, si $m/s \in \mathrm{Ker}(S^{-1}g)$, entonces $g(m)/s = 0$. Luego $0 = tg(m) = g(tm)$ para algún $t \in S$ y, por hipótesis, existe $m' \in M'$ tal que $tm = f(m')$. Por tanto

$$m/s = tm/ts = f(m')/ts = (S^{-1}f)(m'/ts)$$

y $\mathrm{Ker}(S^{-1}g) \subseteq \mathrm{Im}(S^{-1}f)$. Concluimos que $\mathrm{Im}(S^{-1}f) = \mathrm{Ker}(S^{-1}g)$. q.e.d.

Una consecuencia de este teorema es que la localización transforma submódulos en submódulos. Con precisión, si N es un submódulo de un módulo M y consideramos la inclusión $N \to M$, su localización $S^{-1}N \to S^{-1}M$ es inyectiva e induce un isomorfismo de $S^{-1}N$ con su imagen, que también denotaremos $S^{-1}N$:

$$S^{-1}N \;=\; \{m \in S^{-1}M \;:\; m = n/s \text{ para algún } n \in N\}$$

Corolario 8.1.4
$$\begin{aligned}
S^{-1}(M/N) &= (S^{-1}M)/(S^{-1}N)\\
S^{-1}(N+N') &= (S^{-1}N) + (S^{-1}N')\\
S^{-1}(N\cap N') &= (S^{-1}N) \cap (S^{-1}N')\\
S^{-1}(\mathfrak{a}M) &= (S^{-1}\mathfrak{a})(S^{-1}M)\\
S^{-1}(\mathrm{Ker}\, f) &= \mathrm{Ker}\,(S^{-1}f)\\
S^{-1}(\mathrm{Im}\, f) &= \mathrm{Im}\,(S^{-1}f)
\end{aligned}$$

Demostración: La primera afirmación se obtiene localizando la sucesión exacta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

y la segunda es consecuencia directa de la definición de $S^{-1}N$. En cuanto a la tercera, si $n/s = n'/s'$, donde $n \in N$, $n' \in N'$, entonces $un = u'n'$ para ciertos $u', u \in S$; luego un está en $N \cap N'$ y $n/s = (un)/(us) \in S^{-1}(N \cap N')$.

La igualdad $S^{-1}(\mathfrak{a}M) = (S^{-1}\mathfrak{a})(S^{-1}M)$ se sigue de las definiciones.

Si $f\colon M \to N$ es un morfismo de A-módulos, localizando la sucesión exacta

$$0 \longrightarrow \mathrm{Ker}\, f \longrightarrow M \xrightarrow{f} N$$

obtenemos que $S^{-1}(\mathrm{Ker}\, f) = \mathrm{Ker}\,(S^{-1}f)$. La igualdad $S^{-1}(\mathrm{Im}\, f) = \mathrm{Im}\,(S^{-1}f)$ se sigue directamente de las definiciones.

Ejemplo: Sea M un A-módulo. Si $f \in A$, entonces M_f coincide con la localización M_U de M por las funciones $g \in A$ que no se anulen en ningún punto de $U = U_f$, porque $A_f = A_U$ y $S^{-1}M = M \otimes_A S^{-1}A$

8.2 Propiedades Locales

Definición: Llamaremos **soporte** de un elemento m de un A-módulo M al subespacio de $\mathrm{Spec}\, A$ formado por los puntos x donde $m_x \neq 0$ y lo denotaremos

$$\mathrm{Sop}\,(m) \;=\; \{x \in \mathrm{Spec}\, A\colon\; m_x \neq 0\}$$

y pondremos $\mathrm{Sop}\,(M) := \{x \in \mathrm{Spec}\, A\colon\; M_x \neq 0\} = \bigcup_{m\in M} \mathrm{Sop}\,(m)$.

Teorema 8.2.1 *El soporte de un elemento m de un A-módulo M coincide con los ceros de su ideal anulador*

$$\big(\operatorname{Ann}(m)\big)_0 = \{x \in \operatorname{Spec} A : m_x \neq 0\}$$

En particular, la condición necesaria y suficiente para que m sea nulo es que lo sea su localización en todos los puntos cerrados de $\operatorname{Spec} A$.

Demostración: Si $x \in \operatorname{Spec} A$, la condición $m_x = 0$ expresa que $fm = 0$ para alguna función $f \in A$ que no se anula en x; es decir, que x no está en los ceros de $\operatorname{Ann}(m)$. Por último, si $m_x = 0$ en todo punto cerrado $x \in \operatorname{Spec} A$, entonces $\operatorname{Ann}(m)$ no está contenido en ningún ideal maximal de A y, según 6.1.4, tenemos que $\operatorname{Ann}(m) = A$; luego $0 = 1 \cdot m = m$.

Corolario 8.2.2 $\operatorname{Sop} M \subseteq (\operatorname{Ann} M)_0$ *para todo A-módulo M.*

Demostración: $\operatorname{Sop} M = \bigcup_{m\in M} \operatorname{Sop}(m) = \bigcup_{m\in M} \big(\operatorname{Ann}(m)\big)_0 \subseteq (\operatorname{Ann} M)_0$.

Corolario 8.2.3 *Si M es un A-módulo de tipo finito, su soporte es un cerrado que coincide con los ceros de su ideal anulador:* $\operatorname{Sop} M = (\operatorname{Ann} M)_0$.

Demostración: Si M es de tipo finito, $M = Am_1 + \cdots + Am_n$, entonces

$$\operatorname{Sop} M = \bigcup_{i=1}^{n} \operatorname{Sop}(m_i) = \bigcup_{i=1}^{n} \big(\operatorname{Ann}(m_i)\big)_0 = \Big(\bigcap_{i=1}^{n} \operatorname{Ann}(m_i)\Big)_0 = (\operatorname{Ann} M)_0 \ .$$

Corolario 8.2.4 *La condición necesaria y suficiente para que un A-módulo M sea nulo es que lo sea su localización en todos los puntos cerrados de* $\operatorname{Spec} A$.

Demostración: Si $M_x = 0$ para todo punto cerrado $x \in \operatorname{Spec} A$, entonces todo elemento de M se anula al localizar en los puntos cerrados de $\operatorname{Spec} A$ y concluimos que todo elemento de M es nulo.

Teorema 8.2.5 *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión de morfismos de A-módulos. Las siguientes condiciones son equivalentes:*

1. *$M' \xrightarrow{f} M \xrightarrow{g} M''$ es una sucesión exacta.*
2. *$M'_x \xrightarrow{f_x} M_x \xrightarrow{g_x} M''_x$ es exacta en todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración: $1 \Rightarrow 2$ es un caso particular de 8.1.3.

$(2 \Rightarrow 1)$ Si la sucesión es exacta en un punto x, tenemos que

$$(\operatorname{Im} gf)_x = \operatorname{Im}(gf)_x = \operatorname{Im}(g_x f_x) = 0$$

y, de acuerdo con 8.2.4, se sigue que $\operatorname{Im} gf = 0$; es decir, $\operatorname{Im} f \subseteq \operatorname{Ker} g$. Localizando ahora $(\operatorname{Ker} g)/(\operatorname{Im} f)$ obtenemos que

$$(\operatorname{Ker} g/\operatorname{Im} f)_x = (\operatorname{Ker} g)_x/(\operatorname{Im} f)_x = (\operatorname{Ker} g_x)/(\operatorname{Im} f_x) = 0$$

en todo punto cerrado x del espectro de A. De nuevo 8.2.4 permite concluir que $(\operatorname{Ker} g)/(\operatorname{Im} f) = 0$. Es decir, $\operatorname{Ker} g = \operatorname{Im} f$.

Corolario 8.2.6 *La condición necesaria y suficiente para que un morfismo de A-módulos sea inyectivo (respectivamente epiyectivo, isomorfismo) es que lo sea al localizar en todos los puntos cerrados de* $\operatorname{Spec} A$.

Corolario 8.2.7 *Sea N y N' dos submódulos de un A-módulo M. Se verifica que $N' \subseteq N$ si y sólo si $N'_x \subseteq N_x$ en todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración: $N' \subseteq N$ si y sólo si la inclusión $N \to N' + N$ es un isomorfismo.

Teorema de Descomposición: *Si el soporte de un A-módulo M está formado por un número finito de puntos cerrados,* $\operatorname{Sop} M = \{x_1, \ldots, x_n\}$, *entonces M descompone en suma directa de sus localizaciones en los puntos de su soporte*:

$$M \;=\; M_{x_1} \oplus \ldots \oplus M_{x_n}$$

Demostración: Los morfismos canónicos $M \to M_{x_i}$ definen un morfismo de A-módulos $M \to M_{x_1} \oplus \ldots \oplus M_{x_n}$. Según 8.2.6, para probar que es un isomorfismo basta verlo después de localizar en cada punto $y \in \operatorname{Spec} A$. Ahora bien,

$$\big(M_{x_1} \oplus \ldots \oplus M_{x_n}\big)_y \;=\; (M_{x_1})_y \oplus \ldots \oplus (M_{x_n})_y \;=\; \begin{cases} M_{x_i} & \text{cuando } y = x_i \\ 0 & \text{en otro caso} \end{cases}$$

pues en todo punto cerrado $x \in \operatorname{Spec} A$ tenemos que $(M_x)_x = M_x$, y que $(M_x)_y = 0$ cuando $y \neq x$. En efecto, $(M_x)_y$ es un $(A_x)_y$-módulo y su localización en todo punto $z \in \operatorname{Spec}(A_x)_y$ es nula, pues tales puntos z se corresponden con los ideales primos de A contenidos en el ideal maximal de x y en el ideal primo de y, ideales primos que no pueden ser maximales cuando $y \neq x$, de modo que $M_z = 0$.

Corolario 8.2.8 *Si un A-módulo M está anulado por alguna potencia de un ideal maximal $\mathfrak{m}$ de A, entonces $M = M_{\mathfrak{m}}$.*

Demostración: Por hipótesis $\operatorname{Sop} M \subseteq (\operatorname{Ann} M)_0 \subseteq (\mathfrak{m}^n)_0 = (\mathfrak{m})_0 = \{x\}$, así que el soporte de M tiene un único punto x que es cerrado, y el Teorema de Descomposición permite concluir que $M = M_x$.

8.3 Módulos sobre Anillos Locales

Definición: Un anillo es **local** si tiene un único ideal maximal.

Lema de Nakayama (1912-1964)**:** *Sea $\mathcal{O}$ un anillo local y $\mathfrak{m}$ su único ideal maximal. Si M es un $\mathcal{O}$-módulo de tipo finito y $\mathfrak{m}M = M$, entonces $M = 0$.*

Demostración: Si $M \neq 0$, consideramos un sistema finito $\{m_1, \ldots, m_n\}$ de generadores de M tales que $m_2, \ldots, m_n$ no generen M.

Por hipótesis $M = \mathfrak{m}M = \mathfrak{m}(\mathcal{O}m_1 + \ldots + \mathcal{O}m_n) = \mathfrak{m}m_1 + \ldots + \mathfrak{m}m_n$, así que $m_1 = f_1m_1 + f_2m_2 + \ldots + f_nm_n$ para ciertas funciones $f_1, \ldots, f_n \in \mathfrak{m}$. Luego

$$(1 - f_1)m_1 \;=\; f_2m_2 + \ldots + f_nm_n$$

y $1 - f_1$ no está en $\mathfrak{m}$, que es el único ideal maximal de $\mathcal{O}$. En virtud de 6.1.5 concluimos que $1 - f_1$ es invertible en $\mathcal{O}$ y, por tanto, que $m_1 \in \mathcal{O}m_2 + \ldots + \mathcal{O}m_n$. Luego $m_2, \ldots, m_n$ generan M, lo que implica una contradicción.

Corolario 8.3.1 *Sea $\mathcal{O}$ un anillo local, $k = \mathcal{O}/\mathfrak{m}$ el cuerpo residual de su único ideal maximal $\mathfrak{m}$, y sea M un $\mathcal{O}$-módulo de tipo finito.*

La condición necesaria y suficiente para que $m_1, \ldots, m_n \in M$ generen el $\mathcal{O}$-módulo M es que $\bar{m}_1, \ldots, \bar{m}_n$ generen el k-espacio vectorial $M/\mathfrak{m}M$.

Demostración: Sea $N = \mathcal{O}m_1 + \ldots + \mathcal{O}m_n$. La condición de que $\bar{m}_1, \ldots, \bar{m}_n$ generen el k-espacio vectorial $M/\mathfrak{m}M$ significa que $M = N + \mathfrak{m}M$. Pasando al cociente por N obtenemos que $M/N = \mathfrak{m}(M/N)$, y el lema de Nakayama permite concluir que $M/N = 0$. Es decir, $N = M$ y $m_1, \ldots, m_n$ generan el $\mathcal{O}$-módulo M.

Ejemplo: Sea $\mathcal{O}$ el anillo local en el origen del espacio afín $\mathbb{A}_n = \operatorname{Spec} k[x_1, \ldots, x_n]$ sobre un cuerpo k, y sea $\mathfrak{m} = (x_1, \ldots, x_n)$ su único ideal maximal. Según 8.2.8, $\mathfrak{m}/\mathfrak{m}^2$ es un k-espacio vectorial de dimensión n generado por $\{x_1, \ldots, x_n\}$. De acuerdo con el Lema de Nakayama, unos polinomios $f_1, \ldots, f_r \in \mathfrak{m}$

$$f_i(x_1, \ldots, x_n) \;=\; a_{i1}x_1 + \ldots + a_{in}x_n + \text{ términos de grado mayor que } 1$$

generan el ideal $\mathfrak{m}$ si y sólo si sus formas lineales iniciales $a_{i1}x_1 + \ldots + a_{in}x_n$ generan el espacio vectorial de los polinomios homogéneos de grado 1.

Teorema de Bézout

Lema 8.3.2 *Sea k un cuerpo. Toda k-álgebra finita íntegra es un cuerpo. Todo ideal primo de una k-álgebra finita es maximal.*

Demostración: Sea A una k-álgebra finita. Si $a \in A$ no es nulo, la aplicación lineal $h_a\colon A \to A$, $h_a(x) = ax$, es inyectiva cuando A es íntegra. Como A es un k-espacio vectorial de dimensión finita, se sigue que la dimensión de la imagen de h_a coincide con la de A. Luego h_a es epiyectivo y concluimos que $1 = h_a(b) = ab$ para algún $b \in A$. Es decir, a es invertible y A es un cuerpo.

Ahora, si $\mathfrak{p}$ es un ideal primo de A, entonces $A/\mathfrak{p}$ es una k-álgebra finita íntegra; luego es un cuerpo y concluimos que $\mathfrak{p}$ es un ideal maximal.

Teorema 8.3.3 *El espectro de una k-álgebra finita A es un espacio finito y discreto,* $\operatorname{Spec} A = \{z_1, \ldots, z_n\}$*, y A descompone en suma directa de álgebras locales:*

$$A \;=\; A_{z_1} \oplus \ldots \oplus A_{z_n}$$

Demostración: 7.1.1 muestra que el número de ideales maximales de A está acotado por $\dim_k A$. Por el lema anterior, $\operatorname{Spec} A$ es finito y todos sus puntos son cerrados, así que es discreto y el Teorema de descomposición permite concluir.

Definición: Consideremos en el plano afín $\mathbb{A}_2 = \operatorname{Spec} k[x,y]$ dos curvas C_1 y C_2 de ecuaciones $p_1(x,y) = 0$ y $p_2(x,y) = 0$. Si $\mathcal{O}_z$ es el anillo local del plano afín en un punto z, llamaremos **multiplicidad de intersección** de las curvas C_1 y C_2 en el punto z a la longitud del $\mathcal{O}_z$-módulo $\mathcal{O}_z/(p_1,p_2)$:

$$(C_1 \cap C_2)_z \;:=\; l\big(\mathcal{O}_z/(p_1,p_2)\big)\ .$$

Para que la multiplicidad de intersección sea nula es necesario y suficiente que p_1 ó p_2 sea invertible en $\mathcal{O}_z$; i.e., que alguna de las dos curvas no pase por z.

La multiplicidad de intersección es 1 precisamente cuando p_1 y p_2 generan el ideal maximal $\mathfrak{m}_z$ de $\mathcal{O}_z$. Si el punto z es el origen de coordenadas, el Lema de Nakayama muestra que la multiplicidad de intersección es 1 si y sólo si ambas curvas pasan por z y las formas lineales iniciales de $p_1(x,y)$ y $p_2(x,y)$ son linealmente independientes.

Como el único $\mathcal{O}_z$-módulo simple es el cuerpo residual $\kappa(z) := \mathcal{O}_z/\mathfrak{m}_z$ del punto z, tenemos que

$$\dim_k \mathcal{O}_z/(p_1,p_2) \;=\; (C_1 \cap C_2)_z \cdot [\kappa(z) : k]$$

Ahora introducimos tres nuevas indeterminadas x_0, x_1, x_2 y a cada polinomio $q(x,y)$ de grado d le asociamos el polinomio homogéneo de grado d

$$\tilde{q}(x_0,x_1,x_2) := x_0^d q(x_1/x_0, x_2/x_0)\ ,$$

de modo que $q(x,y) = \tilde{q}(1,x,y)$. Diremos que las curvas planas $p_1(x,y) = 0$, $p_2(x,y) = 0$ no se cortan en el infinito cuando la única solución (en extensiones arbitrarias de k) del sistema

$$\left.\begin{aligned} x_0 &= 0 \\ \tilde{p}_1(x_0,x_1,x_2) &= 0 \\ \tilde{p}_2(x_0,x_1,x_2) &= 0 \end{aligned}\right\}$$

sea la solución trivial $x_0 = 0$, $x_1 = 0$, $x_2 = 0$. De acuerdo con 7.2.9, tal condición equivale a que el radical del anillo $k[x_0, x_1, x_2]/(x_0, \tilde{p}_1, \tilde{p}_2)$ sea el ideal maximal (x_0, x_1, x_2); i.e., que alguna potencia de este ideal sea nula.

Teorema de Bézout: *Sea k un cuerpo y $p_1, p_2 \in k[x, y]$ polinomios de grados d_1 y d_2 sin factores irreducibles comunes. El número de puntos de corte de las curvas planas $p_1(x, y) = 0$, $p_2(x, y) = 0$, contado cada uno con su grado y la multiplicidad de intersección, es $\leq d_1 d_2$:*

$$\sum_{z \in C_1 \cap C_2} (C_1 \cap C_2)_z \cdot [\kappa(z) : k] \ \leq \ d_1 d_2$$

y se da la igualdad cuando las curvas no se cortan en el infinito.

Demostración: Sea R_n el subespacio vectorial de $R = k[x_0, x_1, x_2]/(\tilde{p}_1, \tilde{p}_2)$ definido por los polinomios homogéneos de grado n.

Como $\tilde{p}_1(x_0, x_1, x_2)$ y $\tilde{p}_2(x_0, x_1, x_2)$ son polinomios homogéneos de grados d_1 y d_2 sin factores irreducibles comunes, tenemos una sucesión exacta

$$0 \longrightarrow P_{n-d_1-d_2} \xrightarrow{\phi} P_{n-d_2} \oplus P_{n-d_1} \xrightarrow{\psi} P_n \xrightarrow{\pi} R_n \longrightarrow 0$$

donde P_m denota el espacio vectorial de los polinomios homogéneos de grado m en las indeterminadas x_0, x_1, x_2 y $\phi(q) = (\tilde{p}_2 q, -\tilde{p}_1 q)$, $\psi(q_1, q_2) = p_1 q_1 + p_2 q_2$.

Cuando $n \geq d_1 + d_2$, tomando dimensiones sobre k obtenemos que

$$\begin{aligned} \dim_k R_n &= \binom{n+2}{2} - \binom{n-d_1+2}{2} - \binom{n-d_2+2}{2} + \binom{n-d_1-d_2+2}{2} \\ &= d_1 d_2 \end{aligned}$$

Por otra parte, tenemos un isomorfismo de k-álgebras:

$$k[x, y]/(p_1, p_2) \ = \ \bigcup_n \frac{R_n}{x_0^n} \quad , \quad q(x, y) \mapsto q\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right) \ .$$

donde la unión se considera en el anillo de fracciones R_{x_0}. En efecto, tal morfismo claramente es epiyectivo, y si $q(x_1/x_0, x_2/x_0) = 0$, entonces $\tilde{q}(x_0, x_1, x_2) = x_0^d q(x_1/x_0, x_2/x_0) = 0$ en R_{x_0}, de modo que $x_0^r \tilde{q}(x_0, x_1, x_2) = 0$ en R para alguna potencia x_0^r. Luego en el anillo de polinomios $k[x_0, x_2, x_2]$ tenemos una igualdad

$$x_0^r \tilde{q}(x_0, x_1, x_2) \ = \ a(x_0, x_1, x_2)\tilde{p}_1(x_0, x_1, x_2) + b(x_0, x_1, x_2)\tilde{p}_2(x_0, x_1, x_2)$$

y concluimos que $q(x, y) = a(1, x, y)p_1 + b(1, x, y)p_2$ es nulo en $k[x, y]/(p_1, p_2)$.

Esta descomposición del anillo de la intersección en unión creciente de subespacios vectoriales muestra que $\dim_k k[x, y]/(p_1, p_2) = \dim_k (R_n/x_0^n) \leq d_1 d_2$ para

$n >> 0$. Luego $k[x,y]/(p_1,p_2)$ es una k-álgebra finita. Según el teorema anterior, la intersección $C_1 \cap C_2 = \operatorname{Spec} k[x,y]/(p_1,p_2)$ está formada por un número finito de puntos cerrados $z_1,\ldots,z_r$ y tenemos una descomposición

$$\begin{aligned} k[x,y]/(p_1,p_2) &= \mathcal{O}_{z_1}/(p_1,p_2) \oplus \ldots \oplus \mathcal{O}_{z_r}/(p_1,p_2) \\ d_1 d_2 \;\geq\; \dim_k k[x,y]/(p_1,p_2) &= \sum_{z\in C_1\cap C_2} \dim_k \mathcal{O}_z/(p_1,p_2) \\ &= \sum_{z\in C_1\cap C_2} (C_1\cap C_2)_z \cdot [\kappa(z):k] \end{aligned}$$

Para concluir basta ver que el epimorfismo canónico $R_n \to R_n/x_0^n$ es un isomorfismo para $n >> 0$ (i.e., ningún elemento de R_n está anulado por una potencia de x_0) cuando ambas curvas no se cortan en el infinito. Tal condición significa que R_n es nulo en el anillo $k[x_0,x_1,x_2]/(x_0,\tilde{p}_1,\tilde{p}_2) = R/x_0R$ cuando $n >> 0$, de modo que los morfismos $x_0\colon R_n \to R_{n+1}$ son epiyectivos. Como ambos espacios tienen la misma dimensión, concluimos que son inyectivos; luego también lo son los morfismos $x_0^r\colon R_n \to R_{n+r}$ para todo $r \geq 1$.

Nota: Del Teorema de Bézout (1730-1783) se sigue que los cuerpos residuales $\kappa(z)$ son extensiones finitas de k; luego $\kappa(z) = k$ cuando k es algebraicamente cerrado. En tal caso el número de puntos comunes, contados con la multiplicidad de intersección, coincide con el producto de los grados.

8.4 Anillos Noetherianos

Definición: Diremos que un A-módulo es **noetheriano**, en honor de Emmy Noether (1882-1935), si todos sus submódulos son de tipo finito. Diremos que un anillo A es noetheriano si lo es como A-módulo; es decir, si todos sus ideales son de tipo finito.

Si un A-módulo M es noetheriano, es claro que todo submódulo N de M también es noetheriano, al igual que el cociente M/N, ya que cada submódulo de M/N es el cociente de un submódulo de M.

Si un anillo A es noetheriano, también lo es cualquier cociente $A/\mathfrak{a}$ por un ideal $\mathfrak{a}$. Igualmente la localización $S^{-1}A$ por cualquier sistema multiplicativo es un anillo noetheriano, pues cada ideal $\mathfrak{b}$ de $S^{-1}A$ es la localización del ideal $A\cap\mathfrak{b}$ de A, así que $\mathfrak{b}$ es finito-generado cuando lo sea $A\cap\mathfrak{b}$.

Lema 8.4.1 *Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta de A-módulos. La condición necesaria y suficiente para que M sea un A-módulo noetheriano es que M' y M'' sean A-módulos noetherianos.*

Demostración: Si un módulo es noetheriano, también lo son sus submódulos y sus cocientes, así que bastará probar que es condición suficiente. Sea N un submódulo de M. Tenemos una sucesión exacta de A-módulos

$$0 \longrightarrow M' \cap N \longrightarrow N \longrightarrow p(N) \longrightarrow 0$$

Por hipótesis los módulos $M' \cap N$ y $p(N)$ son de tipo finito:

$$M' \cap N = Am'_1 + \ldots + Am'_n \quad , \quad p(N) = Ap(m_1) + \ldots + Ap(m_r)$$

y es sencillo comprobar que $i(m'_1), \ldots, i(m'_n), m_1, \ldots, m_r$ generan N.

Teorema 8.4.2 *Sea A un anillo noetheriano. Todos los A-módulos de tipo finito son noetherianos.*

Demostración: Si A es noetheriano, procediendo por inducción sobre n y aplicando el lema 8.4.1 a las sucesiones exactas

$$0 \longrightarrow A \longrightarrow A^n \longrightarrow A^{n-1} \longrightarrow 0$$

obtenemos que los A-módulos libres de rango finito son noetherianos. Ahora bien, si un A-módulo M está generado por n elementos, éstos definen un epimorfismo $A^n \to M \to 0$ y concluimos que M es noetheriano.

Proposición 8.4.3 *Todo ideal de un anillo noetheriano contiene una potencia de su radical.*

Demostración: Sea $\mathfrak{a}$ un ideal de un anillo noetheriano y sea $\mathfrak{r}$ su radical. Consideremos un sistema finito $\{r_1, \ldots, r_m\}$ de generadores de $\mathfrak{r}$. Por definición de ideal radical, alguna potencia $r_i^{n_i}$ de cada generador r_i ha de estar en $\mathfrak{a}$; luego $\mathfrak{r}^n \subseteq \mathfrak{a}$ cuando $n > n_1 + \ldots + n_m - m$.

Teorema 8.4.4 *La condición necesaria y suficiente para que un A-módulo sea noetheriano, es que toda sucesión estrictamente creciente de submódulos de M sea finita (es decir, que toda familia no vacía de submódulos de M tenga algún elemento maximal).*

Demostración: Supongamos que M es noetheriano. Si

$$N_1 \subseteq N_2 \subseteq \ldots \subseteq N_i \subseteq \ldots$$

es una sucesión creciente de submódulos de M, entonces $N = \bigcup_i N_i$ es un submódulo de M. Luego es de tipo finito: $N = Am_1 + \ldots + Am_r$. Sea n un índice tal que $m_1, \ldots, m_r \in N_n$, de modo que $N \subseteq N_n$. Como $N_n \subseteq \bigcup_i N_i = N$, concluimos que $N_n = N$. Es decir, $N_n = N_{n+j}$ para todo $j \geq 0$, y la sucesión estabiliza a partir del índice n.

Recíprocamente, si M no es noetheriano, algún submódulo $N \subseteq M$ no es de tipo finito. Sea $m_1 \in N$. Como $N \neq Am_1$, existe algún $m_2 \in N$ que no está en Am_1. Como $N \neq Am_1 + Am_2$, existe algún $m_3 \in N$ que no está en $Am_1 + Am_2$. Como $N \neq Am_1 + Am_2 + Am_3$, etc. Procediendo así obtenemos una sucesión estrictamente creciente de submódulos de M:

$$Am_1 \subset Am_1 + Am_2 \subset Am_1 + Am_2 + Am_3 \subset \dots$$

Nota: En la teoría de anillos sólo hemos usado el lema de Zorn en la demostración de la existencia de ideales maximales (6.1.3). En los anillos noetherianos la existencia de ideales maximales se sigue de 8.4.4, así que, en los anillos noetherianos, los resultados de este libro no dependen del lema de Zorn (1906-1993).

Teorema de la Base de Hilbert (1862-1943)**:** *Si un anillo A es noetheriano, el anillo de polinomios $A[x]$ también es noetheriano.*

Demostración: Sea I un ideal de $A[x]$. Los coeficientes dominantes (es decir, de los monomios que dan el grado) de los polinomios de I forman un ideal $\mathfrak{a}$ de A. Por ser A noetheriano, sus ideales son de tipo finito:

$$\mathfrak{a} = a_1A + \dots + a_rA$$

Por definición $a_1, \dots, a_r$ son los coeficientes dominantes de ciertos polinomios $p_1(x), \dots, p_r(x) \in I$ y, después de multiplicarlos por potencias de x adecuadas, podemos suponer que todos tienen igual grado. Sea d su grado común y sea J el ideal de $A[x]$ generado por $p_1, \dots, p_r$.

Sea b el coeficiente dominante de un polinomio $p(x) \in I$. Tenemos que $b = b_1a_1 + \dots + b_ra_r$ para ciertos $b_1, \dots, b_r \in A$ y, si el grado n de $p(x)$ es mayor que $d-1$, entonces el polinomio

$$p(x) - \sum_{i=1}^{r} b_i x^{n-d} p_i(x)$$

está en I y su grado es menor que n. Procediendo de este modo podemos ir restando a $p(x)$ polinomios de J hasta obtener un polinomio de I de grado menor que d; es decir

$$I = J + (I \cap L)$$

donde $L = A \oplus A\,x \oplus \dots \oplus A\,x^{n-1}$ es un A-módulo noetheriano por 8.4.2. Luego $I \cap L$ es un A-módulo noetheriano y, en particular, es de tipo finito:

$$I \cap L = A\,q_1(x) + \dots + A\,q_s(x)$$

Concluimos que $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ generan I.

Corolario 8.4.5 *Si A es un anillo noetheriano, las A-álgebras de tipo finito son noetherianas. Por tanto, si X es una variedad algebraica afín sobre un cuerpo, su anillo de funciones algebraicas $\mathcal{O}(X)$ es noetheriano.*

Demostración: Si un anillo A es noetheriano, procediendo por inducción sobre n obtenemos que los anillos de polinomios $A[x_1, \ldots, x_n]$ también son noetherianos; luego también sus cocientes por ideales, que son precisamente las A-álgebras de tipo finito.

8.5 Espacios Noetherianos

Definición: Diremos que un espacio topológico X es *noetheriano* si toda sucesión estrictamente decreciente de cerrados de X es finita.

Si A es un anillo noetheriano, Spec A *es un espacio topológico noetheriano.*

En efecto, si $Y_1 \supset Y_2 \supset \ldots$ es una sucesión estrictamente decreciente de cerrados de Spec A, y consideramos los ideales $\mathfrak{a}_i := \{f \in A\colon f \text{ se anula en } Y_i\}$, tenemos una sucesión estrictamente creciente de ideales $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ porque las funciones de A separan puntos de cerrados en Spec A; luego, de acuerdo con 8.4.4, ha de ser finita cuando A es un anillo noetheriano.

Teorema 8.5.1 *Todo espacio noetheriano X (en particular, toda variedad algebraica afín) descompone en unión finita de sus componentes irreducibles.*

Demostración: Veamos primero que X *es unión finita de cerrados irreducibles.* En caso contrario X no es irreducible, así que es unión de dos cerrados más pequeños, alguno de los cuales tampoco será unión finita de cerrados irreducibles. Reiterando el argumento con él obtenemos una sucesión infinita estrictamente decreciente de cerrados de X, en contra de la noetherianidad de X.

Consideramos ahora una descomposición $X = Y_1 \cup \ldots \cup Y_r$ en unión de cerrados irreducibles tales que no se den inclusiones $Y_i \subseteq Y_j$ cuando $i \neq j$. Para cualquier cerrado irreducible Y tenemos que $Y = (Y_1 \cap Y) \cup \ldots \cup (Y_r \cap Y)$; luego $Y = Y_i \cap Y$, y por tanto $Y \subseteq Y_i$, para algún índice i. Es decir, $Y_1, \ldots, Y_r$ son precisamente las componentes irreducibles de X.

Corolario 8.5.2 *Todo anillo noetheriano A tiene un número finito de ideales primos minimales y cada ideal primo de A contiene algún ideal primo minimal.*

Demostración: El espacio topológico Spec A es noetheriano, y se concluye al aplicar 7.1.4 y el teorema anterior.

Ejemplo: Toda variedad algebraica afín de dimensión 0 (lo que significa que todos sus puntos son cerrados) está formada por un número finito de puntos aislados.

Si es de dimensión 1, está formada por un número finito de puntos aislados y un número finito de curvas irreducibles, y llamaremos **curvas algebraicas afines** a las variedades algebraicas afines cuyas componentes irreducibles sean todas de dimensión 1. Por tanto, la intersección en el espacio afín $\mathbb{A}_n$ de una curva algebraica C con cualquier subvariedad algebraica que no pase por ninguna componente irreducible de C está formada por un número finito de puntos cerrados.

Teorema 8.5.3 *Todo anillo noetheriano A de dimensión 0 tiene longitud finita, y descompone en suma directa de sus localizaciones en los puntos del espectro, que es finito y discreto:*

$$A \;=\; A_{z_1} \oplus \ldots \oplus A_{z_n}$$

Demostración: Si un anillo tiene dimensión 0, todos sus ideales primos son maximales; luego también son minimales, así que el espectro de A está formado por un número finito de puntos cerrados $z_1, \ldots, z_r$, de acuerdo con 8.5.2. El Teorema de Descomposición afirma que $A = A_{z_1} \oplus \ldots \oplus A_{z_n}$, y para demostrar que A es de longitud finita, podemos suponer que A es local.

Sea $\mathfrak{m}$ el único ideal maximal de A. Los $(A/\mathfrak{m})$-espacios vectoriales $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ son de dimensión finita (porque los ideales $\mathfrak{m}^n$ son finito-generados); luego son A-módulos de longitud finita. Procediendo por inducción sobre n, las sucesiones exactas

$$0 \;\longrightarrow\; \mathfrak{m}^n/\mathfrak{m}^{n+1} \;\longrightarrow\; A/\mathfrak{m}^{n+1} \;\longrightarrow\; A/\mathfrak{m}^n \;\longrightarrow\; 0$$

permiten obtener que los módulos $A/\mathfrak{m}^n$, $n \geq 1$, son de longitud finita. Como $\mathfrak{m}$ es el único ideal primo de A, porque la dimensión de A es 0, alguna potencia $\mathfrak{m}^r$ es nula según 8.4.3. Concluimos que $A = A/\mathfrak{m}^r$ tiene longitud finita.

Corolario 8.5.4 *Los A-módulos de longitud finita son los A-módulos noetherianos con soporte en un número finito de puntos cerrados de* Spec A.

Demostración: Si un A-módulo M es de longitud finita, entonces su longitud $l(M)$ acota la longitud de cualquier cadena de submódulos de M, así que M es noetheriano. Además, si

$$0 = M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n = M$$

es una serie de composición de M, entonces los módulos M_i/M_{i-1} son simples: $M_i/M_{i-1} \simeq A/\mathfrak{m}_i$ para cierto ideal maximal $\mathfrak{m}_i$, correspondiente a un punto cerrado $z_i \in \operatorname{Spec} A$. Luego $(M_i)_y = (M_{i-1})_y$ cuando $y \neq z_i$, y concluimos que

$$M_y \;=\; (M_{n-1})_y \;=\; \ldots \;=\; (M_1)_y \;=\; (M_0)_y \;=\; 0$$

en todo punto $y \in \operatorname{Spec} A$ distinto de los puntos $z_1, \ldots, z_n$.

Recíprocamente, como todo módulo noetheriano M admite un número finito de generadores, $M = Am_1 + \ldots + Am_n$, es un cociente de $Am_1 \oplus \ldots \oplus Am_n$, y

para ver que M es de longitud finita podemos suponer que $M = Am \simeq A/\mathfrak{a}$. Por hipótesis $\mathrm{Sop}(M) = (\mathfrak{a})_0 = \mathrm{Spec}\, A/\mathfrak{a}$ es finito y discreto, y el teorema anterior permite concluir que $A/\mathfrak{a}$ es de longitud finita.

Ejemplo: Sea $C = \mathrm{Spec}\, A$ una curva algebraica del espacio afín $\mathbb{A}_n$ sobre un cuerpo k. Si una hipersuperficie algebraica H de ecuación $f(x_1, \ldots, x_n) = 0$ no pasa por ninguna componente irreducible de C, entonces A/fA es un anillo noetheriano de dimensión 0; luego es de longitud finita y tenemos una descomposición

$$A/fA \;=\; A_{z_1}/fA_{z_1} \oplus \ldots \oplus A_{z_n}/fA_{z_n}$$

donde $z_1, \ldots, z_r$ son los puntos en que H corta a C. Llamaremos **multiplicidades de intersección** de C y H a las longitudes de tales sumandos:

$$(C \cap H)_z \;:=\; l(A_z/fA_z)$$

Proposición 8.5.5 *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión 1 y sea $\mathfrak{m}$ su ideal maximal. Las siguientes condiciones son equivalentes:*

1. *$\mathcal{O}$ es un dominio de ideales principales.*
2. *El $(\mathcal{O}/\mathfrak{m})$-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ es de dimensión 1.*
3. *$\mathfrak{m}$ es un ideal principal: $\mathfrak{m} = t\mathcal{O}$ para algún $t \in \mathcal{O}$.*
4. *Existe $t \in \mathcal{O}$ tal que todo ideal no nulo de $\mathcal{O}$ es de la forma $t^n\mathcal{O}$.*

Demostración: $(1 \Rightarrow 2)$ Si $\mathfrak{m} = t\mathcal{O}$, entonces $\mathfrak{m}/\mathfrak{m}^2$ está generado por $\bar{t}$ y, para concluir que la dimensión de $\mathfrak{m}/\mathfrak{m}^2$ como espacio vectorial es 1, basta probar que $\mathfrak{m}/\mathfrak{m}^2 \neq 0$. En caso contrario, el lema de Nakayama permite concluir que $\mathfrak{m} = 0$, de modo que $\mathcal{O}$ es un cuerpo, contra la hipótesis de que su dimensión es 1.

$(2 \Rightarrow 3)$ Sea $t \in \mathfrak{m}$ tal que $\bar{t} \neq 0$ en $\mathfrak{m}/\mathfrak{m}^2$. Por hipótesis $\bar{t}$ genera $\mathfrak{m}/\mathfrak{m}^2$ y el lema de Nakayama permite concluir que $\mathfrak{m} = t\mathcal{O}$.

$(3 \Rightarrow 4)$ Veamos primero que todo ideal principal no nulo $a\mathcal{O}$ es una potencia de $\mathfrak{m}$. En caso contrario, sea $a\mathcal{O}$ un ideal maximal entre los que no lo sean y pongamos $a = tb$. Entonces $b\mathcal{O}$ tampoco es potencia de $\mathfrak{m}$; luego $b\mathcal{O} = a\mathcal{O} = tb\mathcal{O}$ por el carácter maximal de $a\mathcal{O}$, y el lema de Nakayama afirma que $b\mathcal{O} = 0$, lo que es contradictorio. En el caso general de un ideal no nulo $\mathfrak{a} \subset \mathcal{O}$, consideramos el menor exponente n tal que $\mathfrak{m}^n = a\mathcal{O}$ para algún $a \in \mathfrak{a}$, de modo que $\mathfrak{m}^n \subseteq \mathfrak{a}$ y $\mathfrak{a} \subseteq \mathfrak{m}^n$, y concluimos que $\mathfrak{a} = \mathfrak{m}^n = t^n\mathcal{O}$.

$(4 \Rightarrow 1)$ Sólo hay que probar que el anillo $\mathcal{O}$ es íntegro, y es claro que $\mathfrak{m} = t\mathcal{O}$. Si $a, b \in \mathcal{O}$ no son nulos y $ab = 0$, entonces $a\mathcal{O} = \mathfrak{m}^n$ y $b\mathcal{O} = \mathfrak{m}^m$, de modo que $\mathfrak{m}^{n+m} = ab\mathcal{O} = 0$ y $\dim \mathcal{O} = 0$, en contra de que su dimensión es 1.

Definición: Los anillos locales $\mathcal{O}$ noetherianos de dimensión 1 que verifican las condiciones equivalentes de la proposición anterior reciben el nombre de anillos locales **regulares** de dimensión 1, y diremos que $t \in \mathcal{O}$ es un **parámetro de uniformización** o **coordenada local**, si genera el único ideal maximal $\mathfrak{m}$; es decir, $t\mathcal{O} = \mathfrak{m}$. Si una función $f \in \mathcal{O}$ no es nula, entonces $f\mathcal{O} = \mathfrak{m}^n$ para algún $n \geq 0$, y diremos que tal número n, que coincide con la longitud del $\mathcal{O}$-módulo $\mathcal{O}/f\mathcal{O}$, es el **número de ceros** o la **valoración** de f, y se denota $v(f)$.

Diremos que un punto cerrado z de una curva algebraica afín C es **simple** cuando $\mathcal{O}_{C,x}$ sea un anillo regular de dimensión 1. En caso contrario diremos que x es un punto **singular** de la curva C. En el caso de un punto simple, la multiplicidad de intersección en z de la curva C con una hipersuperficie algebraica H de ecuación $f = 0$ coincide con la valoración de f:

$$v(f) \ = \ (C \cap H)_z$$

8.6 Descomposición Primaria

Definición: Sea A un anillo. Un ideal $\mathfrak{q} \neq A$ es **primario** cuando todo divisor de cero en $A/\mathfrak{q}$ es nilpotente; es decir cuando

$$ab \in \mathfrak{q}\,,\ a \notin \mathfrak{q} \ \Rightarrow\ b^n \in \mathfrak{q} \text{ para algún } n \geq 1$$

El radical de un ideal primario es un ideal primo.

En efecto, sea $\mathfrak{p}$ el radical de un ideal primario $\mathfrak{q}$. Si $ab \in \mathfrak{p}$ y $a \notin \mathfrak{p}$, entonces $a^n b^n \in \mathfrak{q}$ para algún $n \geq 1$. Como $a^n \notin \mathfrak{q}$, se sigue que alguna potencia de b ha de estar en $\mathfrak{q}$, lo que implica que $b \in \mathfrak{p} = r(\mathfrak{q})$.

Sea $\mathfrak{q}$ un ideal primario. Diremos que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario ó que $\mathfrak{p}$ es el ideal primo **asociado** a $\mathfrak{q}$ cuando $\mathfrak{p}$ es el radical de $\mathfrak{q}$. En tal caso, si $B \to A$ es un morfismo de anillos, entonces $B \cap \mathfrak{q}$ es un ideal $(B \cap \mathfrak{p})$-primario de B.

Sea $\mathfrak{m}$ un ideal maximal de un anillo A. Los ideales $\mathfrak{m}$-primarios de A son los ideales de radical $\mathfrak{m}$. En efecto, si $\mathfrak{m}$ es el radical de un ideal $\mathfrak{a}$, es el único ideal primo de A que contiene a $\mathfrak{a}$. Se sigue que el anillo $A/\mathfrak{a}$ tiene un único ideal primo; luego todo elemento de $A/\mathfrak{a}$ es invertible o nilpotente y concluimos que en $A/\mathfrak{a}$ todo divisor de cero es nilpotente. En particular, todas las potencias $\mathfrak{m}^n$ son ideales $\mathfrak{m}$-primarios.

Si el anillo A es noetheriano, cada ideal contiene una potencia de su radical, así que todo ideal $\mathfrak{m}$-primario es de la forma $\pi^{-1}(\bar{\mathfrak{q}})$ para algún ideal $\bar{\mathfrak{q}}$ de $A/\mathfrak{m}^r$: está formado por todas las funciones $f \in A$ cuyo desarrollo de Taylor $\bar{f} \in A/\mathfrak{m}^r$ en el punto definido por $\mathfrak{m}$ satisface las relaciones impuestas por cierto ideal de $A/\mathfrak{m}^r$. Los ideales primarios de radical maximal son los ideales definidos por condiciones infinitesimales en un punto cerrado del espectro. En el caso del anillo

$A = \mathbb{C}[x_1, \ldots, x_n]$, si consideramos el ideal maximal $\mathfrak{m}$ formado por los polinomios que se anulan en cierto punto $(a_1, \ldots, a_n)$ y ponemos $t_i = x_i - a_i$, entonces

$$A/\mathfrak{m}^r = \mathbb{C}[t_1, \ldots, t_n]/(t_1, \ldots, t_n)^r = \begin{bmatrix}\text{Polinomios de grado} \\ < r \text{ en } t_1, \ldots, t_n\end{bmatrix}$$

y la reducción módulo $\mathfrak{m}^r$ de un polinomio es su desarrollo de Taylor hasta el orden $r-1$ en el punto dado. Por tanto, cada ideal $\mathfrak{m}$-primario viene definido por ciertas relaciones lineales entre las derivadas parciales iteradas en el punto $(a_1, \ldots, a_n)$.

En general, sea $\mathfrak{p}$ el ideal primo de un punto $x \in \operatorname{Spec} A$. Los ideales de A_x de radical $\mathfrak{p}_x = \mathfrak{p}A_x$ (que deben llamarse ideales de **condiciones infinitesimales** en el punto x, pues en el caso noetheriano vienen determinados por los ideales de los anillos $A_x/\mathfrak{p}_x^{r+1}$) son precisamente los ideales $\mathfrak{p}_x$-primarios, porque $\mathfrak{p}_x$ es un ideal maximal de A_x. Por tanto, si $\mathfrak{q}_x$ es uno de estos ideales, $A \cap \mathfrak{q}_x$ es un ideal $\mathfrak{p}$-primario de A. Vamos a probar que así se obtienen todos los ideales $\mathfrak{p}$-primarios de A; es decir, *los ideales primarios son los ideales definidos por condiciones infinitesimales en un punto del espectro*:

Proposición 8.6.1 *Sea S un sistema multiplicativo de un anillo A y sea $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario.*

1. *Si $\mathfrak{p}$ corta a S, entonces $\mathfrak{q}(S^{-1}A) = S^{-1}A$.*
2. *Si $\mathfrak{p}$ no corta a S, entonces $\mathfrak{q}(S^{-1}A)$ es un ideal $\mathfrak{p}(S^{-1}A)$-primario y $\mathfrak{q} = A \cap (\mathfrak{q}S^{-1}A)$. En particular:*

$$\boxed{\mathfrak{q} = A \cap (\mathfrak{q}A_{\mathfrak{p}})}$$

Por tanto, para que dos ideales $\mathfrak{p}$-primarios coincidan es suficiente que coincidan al localizar en $\mathfrak{p}$.

Demostración: (1) Si $s \in S \cap \mathfrak{p}$, entonces $\mathfrak{q}$ contiene alguna potencia s^n, que es invertible en $S^{-1}A$; luego $\mathfrak{q}(S^{-1}A) = S^{-1}A$.

(2) Si $S \cap \mathfrak{p} = \emptyset$, entonces $\mathfrak{p}(S^{-1}A)$ es un ideal primo de $S^{-1}A$ y es fácil comprobar que $\mathfrak{q}(S^{-1}A)$ es un ideal $\mathfrak{p}(S^{-1}A)$-primario. Por último, si f está en $A \cap (\mathfrak{q}S^{-1}A)$, entonces $sf \in \mathfrak{q}$ para algún $s \in S$. Como ninguna potencia de s está en $\mathfrak{q}$, se sigue que $f \in \mathfrak{q}$. Luego $\mathfrak{q} = A \cap (\mathfrak{q}S^{-1}A)$, porque la inclusión $\mathfrak{q} \subseteq A \cap (\mathfrak{q}S^{-1}A)$ es evidente.

Ejemplo: Si un ideal primo $\mathfrak{p}$ no es maximal, pueden existir ideales de radical $\mathfrak{p}$ que no son primarios. Fijemos en un plano afín un punto racional y una recta que pase por él. Sea $\mathfrak{m}$ el ideal maximal del punto y $\mathfrak{p}$ el ideal primo del punto genérico de la recta. Consideremos ahora el ideal $\mathfrak{a} = \mathfrak{m}^2 \cap \mathfrak{p}$ formado por los polinomios

que se anulan en el punto genérico de la recta y sus derivadas parciales se anulan en el punto fijado. El radical de $\mathfrak{a}$ es

$$r(\mathfrak{a}) = r(\mathfrak{m}^2) \cap r(\mathfrak{p}) = \mathfrak{m} \cap \mathfrak{p} = \mathfrak{p}$$

pero el ideal $\mathfrak{a}$ no es primario: el producto de la ecuación de la recta fijada por la de otra recta que pase por el punto está en $\mathfrak{a}$, la ecuación de la recta fijada no está en $\mathfrak{a}$ y la ecuación de la otra recta no está en $\mathfrak{p} = r(\mathfrak{a})$. Esto se debe a que el ideal $\mathfrak{a}$ no está definido por condiciones infinitesimales en un solo punto del espectro sino en dos: en el punto fijado y en el punto genérico de la recta dada.

Incluso puede darse el caso de que una potencia de un ideal primo no sea un ideal primario. Por ejemplo, sea A el anillo de las funciones algebraicas sobre un cono en $\mathbb{A}_3$ y sea $\mathfrak{p}$ el ideal primo de A definido por una generatriz.

El ideal $\mathfrak{p}^2$ no viene definido por condiciones infinitesimales en el punto genérico de tal generatriz; i.e., $\mathfrak{p}^2$ no coincide con $A \cap \mathfrak{p}^2 A_{\mathfrak{p}}$ sino que involucra condiciones en el vértice del cono, pues las funciones de $\mathfrak{p}^2$ cumplen además la condición de estar en $\mathfrak{m}^2$, donde $\mathfrak{m}$ denota el ideal maximal del vértice del cono. En efecto, la ecuación del plano tangente al cono a lo largo de la directriz está en $A \cap \mathfrak{p}^2 A_{\mathfrak{p}}$; pero no está en $\mathfrak{p}^2$ porque no pertenece a $\mathfrak{m}^2$. Luego el ideal $\mathfrak{p}^2$ no es primario.

Definición: Sea $\mathfrak{a}$ un ideal de un anillo A. Diremos que una descomposición $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ como intersección de ideales primarios de A es una **descomposición primaria reducida** de $\mathfrak{a}$ cuando no tenga componentes asociadas a un mismo ideal primo ($r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ cuando $i \neq j$) ni componentes redundantes (es decir, $\mathfrak{a} \neq \mathfrak{q}_1 \cap \ldots \cap \widehat{\mathfrak{q}_i} \cap \ldots \cap \mathfrak{q}_n$ para todo $1 \leq i \leq n$).

Si un ideal de un anillo puede descomponerse como intersección finita de ideales primarios, agrupando los términos de igual radical obtenemos una descomposición primaria en que todos los términos tienen radicales diferentes. Eliminando entonces términos redundantes si los hubiera se obtiene una descomposición primaria reducida: *si un ideal admite una descomposición primaria, admite una descomposición primaria reducida.*

Definición: Diremos que un ideal $\mathfrak{q}$ de un anillo A es **irreducible** si no es intersección de dos ideales estrictamente mayores; es decir, si el ideal 0 del anillo cociente $A/\mathfrak{q}$ no es intersección de dos ideales no nulos.

Lema 8.6.2 *Sea A un anillo noetheriano. Todo ideal irreducible $\mathfrak{q} \neq A$ es primario.*

Demostración: Si $b \in A/\mathfrak{q}$, consideramos los morfismos $b^n \colon A/\mathfrak{q} \to A/\mathfrak{q}$:

$$\operatorname{Ker} b \subseteq \operatorname{Ker} b^2 \subseteq \cdots \subseteq \operatorname{Ker} b^n \subseteq \cdots$$

Como $A/\mathfrak{q}$ es noetheriano, $\operatorname{Ker} b^n = \operatorname{Ker} b^{n+1}$ para algún exponente n. Luego $(\operatorname{Ker} b) \cap (\operatorname{Im} b^n) = 0$. Por ser $\mathfrak{q}$ irreducible, $\operatorname{Ker} b$ ó $\operatorname{Im} b^n$ es nulo:

Si $\operatorname{Ker} b = 0$, entonces b no es divisor de cero en $A/\mathfrak{q}$.
Si $\operatorname{Im} b^n = 0$, entonces b es nilpotente en $A/\mathfrak{q}$.
y concluimos que el ideal $\mathfrak{q}$ es primario.

Teorema de Existencia: *Sea A un anillo noetheriano. Todo ideal $\neq A$ es intersección finita de ideales primarios de A; es decir, está definido por condiciones infinitesimales en un número finito de puntos de* $\operatorname{Spec} A$.

Demostración: De acuerdo con el lema anterior, bastará probar que todo ideal de A es intersección finita de ideales irreducibles. En caso contrario, el conjunto de los ideales de A que no son intersección finita de ideales irreducibles no es vacío y tiene algún elemento maximal $\mathfrak{a}$. Este ideal $\mathfrak{a}$ no es irreducible, luego $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ donde $\mathfrak{a} \subset \mathfrak{b}$ y $\mathfrak{a} \subset \mathfrak{c}$. Luego $\mathfrak{b}$ y $\mathfrak{c}$ descomponen en intersección finita de ideales irreducibles y, por tanto, también $\mathfrak{a}$, lo que es contradictorio.

Teorema 8.6.3 *Sea A un anillo y $0 = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ una descomposición primaria reducida del ideal 0. Los divisores de cero de A son las funciones que se anulan en alguno de los puntos definidos por los ideales primos asociados $\mathfrak{p}_i = r(\mathfrak{q}_i)$:*

$$\{\text{Divisores de cero de } A\} \;=\; \bigcup_{i=1}^{n} \mathfrak{p}_i$$

Demostración: Sea $a \in A$ un divisor de cero: $ab = 0$ para algún $b \in A$ no nulo. Luego $b \notin \mathfrak{q}_i$ para algún índice i, porque la descomposición primaria es reducida, y concluimos que $a \in r(\mathfrak{q}_i) = \mathfrak{p}_i$.

Recíprocamente, si $a \in \mathfrak{p}_1$, entonces alguna potencia $a^n \in \mathfrak{q}_1$, de modo que $a^n b = 0$ para cualquier $b \in \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_n$ no nulo, y a es un divisor de cero.

Lema 8.6.4 *Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos de un anillo A. Si $\mathfrak{a}$ es un ideal de A tal que $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$, entonces $\mathfrak{a} \subseteq \mathfrak{p}_i$ para algún índice i. Es decir, si un cerrado $Y \subset \operatorname{Spec} A$ no pasa por ciertos puntos $x_1, \ldots, x_n$, existe una función $f \in A$ que se anula en Y y no se anula en ninguno de los puntos $x_1, \ldots, x_n$.*

Demostración: Podemos suponer que entre los puntos x_i no se dan relaciones de especialización. En tal caso, para cada índice i existe alguna función $f_i \in A$ que se anula en Y y en todos los puntos $x_1, \ldots, x_n$, salvo en x_i, porque x_i no está en el cierre de Y ni de los restantes puntos, y las funciones de A separan puntos de cerrados en $\operatorname{Spec} A$. Luego $f = f_1 + \ldots + f_n$ se anula en Y, y no se anula en ninguno de los puntos $x_1, \ldots, x_n$.

Teorema de Unicidad (de los primos asociados): *Si un ideal $\mathfrak{a}$ de un anillo A admite una descomposición primaria reducida $\mathfrak{a} = \cap_i \mathfrak{q}_i$, los ideales primos asociados $\mathfrak{p}_i = r(\mathfrak{q}_i)$ no dependen de la descomposición.*

Demostración: Veamos primero el caso $\mathfrak{a} = 0$. Sean

$$0 = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \ldots \cap \mathfrak{q}'_m$$

dos descomposiciones primarias reducidas del ideal 0 y sea $\mathfrak{p}$ el ideal primo asociado a una componente de la segunda descomposición. Bastará ver que $\mathfrak{p}$ coincide con $\mathfrak{p}_i = r(\mathfrak{q}_i)$ para algún índice i. Además, por 8.6.1, localizando en $\mathfrak{p}$ podemos suponer que el anillo A es local y que $\mathfrak{p}$ es su único ideal maximal $\mathfrak{m}$. Ahora

$$\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n \; = \; \mathfrak{m}$$

por 8.6.3, pues ambos términos coinciden con el conjunto de los divisores de cero de A, y concluimos al aplicar el lema anterior.

En el caso de un ideal $\mathfrak{a}$ arbitrario, cada ideal $\mathfrak{q} \supseteq \mathfrak{a}$ se corresponde con un ideal $\bar{\mathfrak{q}}$ de $A/\mathfrak{a}$, y $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario precisamente cuando $\bar{\mathfrak{q}}$ es un ideal $\bar{\mathfrak{p}}$-primario, porque $A/\mathfrak{q} = (A/\mathfrak{a})/\bar{\mathfrak{q}}$ y $\bar{\mathfrak{p}}$ es el radical de $\bar{\mathfrak{q}}$. Por tanto, cada descomposición primaria reducida $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ define una descomposición primaria reducida $0 = \bar{\mathfrak{a}} = \bar{\mathfrak{q}}_1 \cap \ldots \cap \bar{\mathfrak{q}}_n$ del ideal 0 del anillo $A/\mathfrak{a}$. Luego los ideales primos $\bar{\mathfrak{p}}_i$ no dependen de la descomposición y concluimos que los ideales primos $\mathfrak{p}_i$ tampoco.

Definición: Sea A un anillo noetheriano. Llamaremos **ideales primos asociados** a un ideal $\mathfrak{a}$ a los radicales de las componentes de cualquier descomposición primaria reducida de $\mathfrak{a}$.

Sea $\mathfrak{a} = \cap_i \mathfrak{q}_i$ una descomposición primaria reducida de un ideal $\mathfrak{a}$ de un anillo A. Como $(\mathfrak{a})_0 = \cup_i (\mathfrak{q}_i)_0$, si un ideal primo $\mathfrak{p}$ es minimal entre los ideales primos de A que contienen a $\mathfrak{a}$, entonces $\mathfrak{p}$ es el radical de alguna componente $\mathfrak{q}_i$ y diremos que $\mathfrak{q}_i$ es una componente **no sumergida**. Una componente $\mathfrak{q}_j$ está **sumergida** cuando sus ceros están contenidos en los de alguna otra componente: $(\mathfrak{q}_j)_0 \subset (\mathfrak{q}_i)_0$.

Las componentes no-sumergidas corresponden a los puntos genéricos de las componentes irreducibles de $(\mathfrak{a})_0$, mientras que las componentes sumergidas están asociadas a puntos más pequeños de $(\mathfrak{a})_0$.

Teorema de Unicidad (de las componentes no-sumergidas): *Sea $\mathfrak{a} = \cap_i \mathfrak{q}_i$ una descomposición primaria reducida de un ideal $\mathfrak{a}$ de un anillo A. Si $\mathfrak{p}$ es el ideal primo de alguna componente irreducible de $(\mathfrak{a})_0$, entonces $\mathfrak{p}$ es el radical de alguna componente $\mathfrak{q}_i$ y*

$$\mathfrak{q}_i = A \cap (\mathfrak{a} A_{\mathfrak{p}})$$

Luego tal componente $\mathfrak{q}_i$ no depende de la descomposición elegida.

Demostración: Cuando $j \neq i$, tenemos que $\mathfrak{q}_j A_{\mathfrak{p}} = A_{\mathfrak{p}}$, porque $r(\mathfrak{q}_j)$ corta al sistema multiplicativo $A - \mathfrak{p}$ por el que localizamos. Luego

$$\mathfrak{a}A_{\mathfrak{p}} = \bigcap_{j=1}^{n} \mathfrak{q}_j A_{\mathfrak{p}} = \mathfrak{q}_i A_{\mathfrak{p}}$$

y, por 8.6.1.2, concluimos que $\mathfrak{q}_i = A \cap (\mathfrak{q}_i A_{\mathfrak{p}}) = A \cap (\mathfrak{a}A_{\mathfrak{p}})$.

Corolario 8.6.5 *Si los ceros de un ideal $\mathfrak{a}$ de un anillo noetheriano son puntos aislados, la descomposición primaria reducida de $\mathfrak{a}$ es única salvo el orden.*

Corolario 8.6.6 *Sea A un anillo noetheriano íntegro de dimensión 1. Todo ideal no nulo $\mathfrak{a} \neq A$ descompone, y de modo único salvo el orden, en producto de ideales primarios con radicales distintos.*

Demostración: Sea $\mathfrak{a}$ un ideal no nulo. Todo ideal primo que contenga a $\mathfrak{a}$ ha de ser maximal, pues la dimensión del anillo es 1. Luego $(\mathfrak{a})_0$ tiene dimensión 0 y la descomposición primaria reducida $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ es única salvo reordenaciones. Para concluir, localizando en los puntos cerrados del espectro de A se prueba que

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_n$$

Definición: Diremos que un anillo íntegro noetheriano A de dimensión 1 es un anillo de **Dedekind** (1831-1916) si su anillo local A_x en cualquier punto cerrado $x \in \operatorname{Spec} A$ es un anillo local regular de dimensión 1.

Corolario 8.6.7 *Sea A un anillo de Dedekind. Todo ideal no nulo $\mathfrak{a} \neq A$ descompone, y de modo único salvo el orden, en producto de potencias de ideales maximales distintos.*

Demostración: Sea $\mathfrak{m}$ un ideal maximal de A. De acuerdo con 8.6.6, bastará probar que todo ideal $\mathfrak{m}$-primario $\mathfrak{q}$ es una potencia de $\mathfrak{m}$. De acuerdo con 8.5.5, $\mathfrak{q}A_{\mathfrak{m}}$ es una potencia del único ideal maximal $\mathfrak{m}A_{\mathfrak{m}}$ de $A_{\mathfrak{m}}$ y, por 8.6.1.2, concluimos que $\mathfrak{q}$ coincide con la correspondiente potencia de $\mathfrak{m}$.

Capítulo 9

Cálculo Diferencial

La comprensión de todo anillo B como un anillo de funciones sobre un espacio $X = \operatorname{Spec} B$ culmina en la posibilidad de desarrollar un cálculo diferencial. El valor $f(p)$ de una función $f(x) \in B$ en el punto $p \in \operatorname{Spec} B$ definido por un ideal primo $\mathfrak{p}$ es la clase de $f(x)$ en $B/\mathfrak{p}$, por lo que el incremento $\Delta_p f = f(x) - f(p)$ en p tiene sentido cuando B es un álgebra sobre un cuerpo k y p es un punto racional, $k = B/\mathfrak{m}_p$, porque en tal caso $f(p) \in k$ puede entenderse como una función constante vía el morfismo estructural $k \to B$. El incremento $\Delta_p f$ es un infinitésimo en p, en el sentido de que está en el ideal maximal $\mathfrak{m}_p$, y los infinitésimos de orden superior son las funciones de $\mathfrak{m}_p^2$. Por tanto la **diferencial** $\mathrm{d}_p f$, entendida por Leibniz (1646-1716) como el incremento despreciando infinitésimos de segundo orden, puede definirse como la clase de restos del incremento módulo $\mathfrak{m}_p^2$:

$$\mathrm{d}_p f \;=\; [\Delta_p f] \in \mathfrak{m}_p/\mathfrak{m}_p^2$$

Para extender esta definición al caso general de un morfismo de anillos $A \to B$, entendiendo A como anillo de funciones constantes, y un punto

$$p\colon T = \operatorname{Spec} C \longrightarrow \operatorname{Spec} B = X$$

de X parametrizado por T, el problema radica en que el valor $f(p)$ de $f \in B$ en p es una función sobre T, y no puede entenderse como función sobre X salvo en el caso $C = A$; es decir, el caso en que el punto p es una sección del morfismo estructural $X \to \operatorname{Spec} A$. No obstante, cambiando de base, es decir, considerando la segunda proyección

$$X \times_A T := \operatorname{Spec}(B \otimes_A C) \;\longrightarrow\; \operatorname{Spec} C = T$$

el punto considerado $p\colon T \to X$ define una sección $p \times Id\colon T \to X \times_A T$ y tiene perfecto sentido considerar la diferencial en p de cualquier función $f \in B$:

1. f se entiende como función sobre $X \times_A T$ por la proyección $X \times_A T \to X$.

2. El valor $f(p)$, que es la imagen de f por el morfismo $B \to C$ definido por el punto p, se entiende como función sobre $X \times_A T$ por la segunda proyección, de modo que el incremento de f en p es $\Delta_p f := f \otimes 1 - 1 \otimes f(p) \in B \otimes_A C$.

3. El núcleo Δ_p del morfismo $B \otimes_A C \to C$ definido por $p \times Id$ se entiende como el ideal de los infinitésimos en p, y la diferencial $\mathrm{d}_p f$ es la clase de restos del incremento en Δ_p/Δ_p^2.

En el caso de la identidad $X \to X$, el valor de una función $f \in B$ coincide con f, su incremento es $\Delta f = f\otimes 1 - 1 \otimes f \in B \otimes_A B$, y el ideal de los infinitésimos es el núcleo $\Delta_{B/A}$ del morfismo diagonal $B \otimes_A B \to B$, $b_1 \otimes b_2 \mapsto b_1 b_2$. En consecuencia la diferencial $\mathrm{d}\, f$ es la clase de restos del incremento $f \otimes 1 - 1 \otimes f$ en $\Delta_{B/A}/\Delta_{B/A}^2$. En este capítulo veremos cómo esta definición de la diferencial permite establecer un cálculo diferencial razonable en anillos arbitrarios.

9.1 Derivaciones

Definición: Sea $A \to B$ un morfismo de anillos. Si M es un B-módulo, diremos que una aplicación $D\colon B \to M$ es una **A-derivación** cuando

1. $D(b + c) = Db + Dc$ para todo $b, c \in B$.
2. $D(bc) = (Db)c + b(Dc)$ para todo $b, c \in B$.
3. $Da = 0$ para todo $a \in A$ (donde a denota también su imagen en B).

Las A-derivaciones son claramente morfismos de A-módulos, y el conjunto $\mathrm{Der}_A(B, M)$ de todas las A-derivaciones de B en M es un B-módulo con las siguientes operaciones

$$(D + D')b = Db + D'b$$
$$(bD)c = b(Dc)$$

Si $f\colon M \to N$ es un morfismo de B-módulos, la aplicación

$$f_*\colon \mathrm{Der}_A(B, M) \longrightarrow \mathrm{Der}_A(B, N) \qquad , \qquad (f_* D)b = f(Db)$$

también es morfismo de B-módulos. Si $j\colon B \to C$ es un morfismo de A-álgebras, para todo C-módulo N tenemos el siguiente morfismo de B-módulos:

$$j^*\colon \mathrm{Der}_A(C, N) \longrightarrow \mathrm{Der}_A(B, N) \qquad , \qquad (j^* D)b = D\big(j(b)\big)$$

Ejemplo 9.1.1 En el caso de un álgebra A sobre un cuerpo k y un punto racional $p \in \operatorname{Spec} A$, las k-derivaciones $D\colon A \to A/\mathfrak{m}_p = k$ son las aplicaciones k-lineales que verifican

$$D(fg) \;=\; (Df)g(p) + f(p)(Dg)\ .$$

Por ejemplo, la **diferencial** $\mathrm{d}_p\colon A \longrightarrow \mathfrak{m}_p/\mathfrak{m}_p^2$, $\mathrm{d}_p f := [\Delta f] = [f - f(p)]$, en el punto dado p es una k-derivación, porque $(\Delta f)(\Delta g) \in \mathfrak{m}_p^2$:

$$\begin{aligned} fg &= \big(f(p) + \Delta f\big)\big(g(p) + \Delta g\big) \\ \Delta(fg) &= f(p)(\Delta g) + g(p)(\Delta f) + (\Delta f)(\Delta g) \\ \mathrm{d}_p(fg) &= f(p)\mathrm{d}_p f + g(p)\mathrm{d}_p f \end{aligned}$$

Ejemplo 9.1.2 En el caso de un anillo de polinomios $B = A[x_1, \ldots, x_n]$ y un B-módulo M, es claro que cada A-derivación $D\colon A[x_1, \ldots, x_n] \to M$ está totalmente determinada por las derivadas Dx_i, así que tenemos

$$D \;=\; \sum_{i=1}^{n} (Dx_i)\frac{\partial}{\partial x_i}$$

donde el significado de la derivación $m\frac{\partial}{\partial x_i}$ es el evidente cuando $m \in M$. Además esta descomposición es única, porque si $D = \sum_j m_j \frac{\partial}{\partial x_j}$, entonces es evidente que $m_i = \big(\sum_j m_j \frac{\partial}{\partial x_j}\big)x_i = Dx_i$. Es decir,

$$\operatorname{Der}_A(A[x_1, \ldots, x_n], M) \;=\; M\,\partial/\partial x_1 \oplus \ldots \oplus M\,\partial/\partial x_n$$

Sucesiones Exactas de Derivaciones

Primera Sucesión Exacta: *Si $j\colon B \to C$ es un morfismo de A-álgebras y N es un C-módulo, entonces la siguiente sucesión es exacta:*

$$0 \;\longrightarrow\; \operatorname{Der}_B(C, N) \;\longrightarrow\; \operatorname{Der}_A(C, N) \;\xrightarrow{\;j^*\;}\; \operatorname{Der}_A(B, N)$$

Demostración: Por definición, una A-derivación $D\colon C \to N$ es una B-derivación precisamente cuando se anule sobre la imagen de j; es decir, cuando $j^*D = 0$.

Segunda Sucesión Exacta: *Sea $p\colon B \to C$ un epimorfismo de A-álgebras de núcleo $\mathfrak{b}$. Si N es un C-módulo, la restricción i^*D a $\mathfrak{b}$ de cualquier derivación $D\colon B \to N$ es un morfismo de B-módulos, y la siguiente sucesión es exacta:*

$$0 \longrightarrow \operatorname{Der}_A(C, N) \xrightarrow{\;p^*\;} \operatorname{Der}_A(B, N) \xrightarrow{\;i^*\;} \operatorname{Hom}_B(\mathfrak{b}, N) = \operatorname{Hom}_B(\mathfrak{b}/\mathfrak{b}^2, N)$$

Demostración: Si $x \in \mathfrak{b}$ y $b \in B$, tenemos que $D(bx) = b(Dx) + x(Db) = b(Dx)$ porque $\mathfrak{b}$ anula a todo $B/\mathfrak{b}$-módulo. Por último, es claro que la condición necesaria y suficiente para que una derivación $D\colon B \to N$ factorice a través de $B/\mathfrak{b}$ es que se anule en $\mathfrak{b}$.

Corolario 9.1.3 *Las A-derivaciones de $B/\mathfrak{b}$ en N se corresponden canónicamente con las A-derivaciones de B en N que se anulen en $\mathfrak{b}$.*

Teorema 9.1.4 *Sea A un álgebra sobre un cuerpo k. Si $p \in \operatorname{Spec} A$ es un punto racional, entonces el morfismo de restricción induce un isomorfismo k-lineal*

$$\operatorname{Der}_k(A, A/\mathfrak{m}_p = k) \xrightarrow{\sim} \operatorname{Hom}_k(\mathfrak{m}_p/\mathfrak{m}_p^2, k) \ .$$

Demostración: La segunda sucesión exacta de derivaciones afirma que la aplicación k-lineal

$$\operatorname{Der}_k(A, A/\mathfrak{m}_p = k) \xrightarrow{i^*} \operatorname{Hom}_A(\mathfrak{m}_p/\mathfrak{m}_p^2, k) = \operatorname{Hom}_k(\mathfrak{m}_p/\mathfrak{m}_p^2, k)$$

es inyectiva. Veamos que es epiyectiva: si $\omega\colon \mathfrak{m}_p/\mathfrak{m}_p^2 \to k$ es una aplicación k-lineal, entonces $Df := \omega(\mathrm{d}_p f)$ es una k-derivación $D\colon A \to k$, y su restricción a $\mathfrak{m}_p$ coincide con ω claramente.

9.2 Diferenciales

Definición: Si $A \to B$ es un morfismo de anillos, existe un único morfismo de B-álgebras $\mu\colon B \otimes_A B \to B$ tal que $\mu(b \otimes c) = bc$, llamado **morfismo diagonal**, y diremos que su núcleo Δ es el **ideal de la diagonal**. Llamaremos **módulo de diferenciales** de B sobre A al B-módulo $\Omega_{B/A} := \Delta/\Delta^2$.

Diremos que la aplicación $\mathrm{d}\colon B \to \Omega_{B/A}$, $\mathrm{d}b = [b \otimes 1 - 1 \otimes b]$, es la **diferencial**, y es una A-derivación:

$$\begin{aligned}\mathrm{d}(bd) &= [bc \otimes 1 - 1 \otimes bc] = (c \otimes 1)[b \otimes 1 - 1 \otimes b] + (1 \otimes b)[c \otimes 1 - 1 \otimes c] \\ &= c(\mathrm{d}b) + b(\mathrm{d}c)\end{aligned}$$

porque la estructura de B-módulo de $\Omega_{B/A}$ es la misma tanto si el morfismo $B \to B \otimes_A B$ se considera por la derecha como por la izquierda, pues está anulado por $b \otimes 1 - 1 \otimes b \in \Delta$.

Lema 9.2.1 *El ideal de la diagonal está generado como B-módulo por los incrementos $b \otimes 1 - 1 \otimes b$ y, por tanto, el B-módulo de diferenciales $\Omega_{B/A}$ está generado por la imagen de la diferencial* $\mathrm{d}\colon B \to \Omega_{B/A}$.

Demostración: Si $\sum_i b_i \otimes c_i \in \Delta$, por definición tenemos que $\sum_i b_i c_i = 0$, y por tanto $\sum_i 1 \otimes b_i c_i = 0$. Luego

$$\textstyle\sum_i b_i \otimes c_i = \sum_i b_i \otimes c_i - \sum_i 1 \otimes b_i c_i = \sum_i c_i (b_i \otimes 1 - 1 \otimes b_i)$$

Corolario 9.2.2 *Si B es una A-álgebra de tipo finito, $B = A[b_1, \ldots, b_n]$, entonces $\Omega_{B/A}$ es un B-módulo de tipo finito*

$$\Omega_{B/A} = B\mathrm{d}b_1 + \ldots + B\mathrm{d}b_n \ .$$

Demostración: De acuerdo con el lema anterior el B-módulo $\Omega_{B/A}$ está generado por la diferenciales

$$\mathrm{d}(b_1^{d_1}\dots b_n^{d_n}) \;=\; b_1^{d_1-1}\dots b_n^{d_n}\mathrm{d}b_1+\dots+b_1^{d_1}\dots b_n^{d_n-1}\mathrm{d}b_n\ .$$

Propiedad Universal: *Sea $A\to B$ un morfismo de anillos y M un B-módulo. Para cada A-derivación $D\colon B\to M$ existe un único morfismo de B-módulos $\phi\colon \Omega_{B/A}\to M$ tal que $\phi(\mathrm{d}b)=Db$ para todo $b\in B$:*

$$\mathrm{Der}_A(B,M) \;=\; \mathrm{Hom}_B(\Omega_{B/A},M)$$

Demostración: La unicidad de tal morfismo ϕ se sigue de 9.2.1, pues un morfismo de B-módulos está totalmente determinado por las imágenes de un sistema de generadores.

En cuanto a la existencia, como D es morfismo de A-módulos y M es un B-módulo, por la propiedad universal del cambio de base existe un morfismo de B-módulos $h\colon B\otimes_A B\to M$ tal que $\phi(b\otimes c)=c(Db)$. La condición de que D sea derivación significa que

$$\phi\big((b\otimes 1-1\otimes b)(c\otimes 1-1\otimes c)\big)=D(bc)-b(Dc)-c(Db)+bc(D1)=0$$

y 9.2.1 permite concluir que ϕ se anula en Δ^2, de modo que ϕ induce un morfismo de B-módulos $\phi\colon \Delta/\Delta^2\to M$ tal que

$$\phi(\mathrm{d}b) \;=\; \phi(b\otimes 1-1\otimes b)=Db-b(D1) \;=\; Db\ .$$

Teorema 9.2.3 *El módulo de diferenciales sobre A del anillo de polinomios $B=A[x_1,\dots,x_n]$ es un B-módulo libre de base $\mathrm{d}x_1,\dots,\mathrm{d}x_n$:*

$$\Omega_{A[x_1,\dots,x_n]/A} \;=\; B\mathrm{d}x_1\oplus\dots\oplus B\mathrm{d}x_n$$

Demostración: Las diferenciales $\mathrm{d}x_1,\dots,\mathrm{d}x_n$ generan el B-módulo $\Omega_{B/A}$ de acuerdo con 9.2.2. Si se diera alguna relación de dependencia lineal $\sum p_i\mathrm{d}x_i=0$, $p_i\in B$, considerando el morfismo de B-módulos $\phi\colon \Omega_{B/A}\to B$ que por la propiedad universal corresponde a la derivación ∂/∂_j concluimos que $0=\phi(\sum_i p_i\mathrm{d}x_i)=\sum_i p_i(\partial x_i/\partial x_j)=p_j$.

Sucesiones Exactas de Diferenciales

(1) Sea $j\colon B\to C$ un morfismo de A-álgebras. La composición de j con la diferencial $\mathrm{d}\colon \Omega_{C/A}$ es una A-derivación, así que, por la propiedad universal, existe un único morfismo de B-módulos $j\colon \Omega_{B/A}\to\Omega_{C/A}$ tal que $j(\mathrm{d}b)=\mathrm{d}j(b)$. Como $\Omega_{C/A}$ es un C-módulo, obtenemos un morfismo de C-módulos

$$j\otimes 1\colon \Omega_{B/A}\otimes_B C \;\longrightarrow\; \Omega_{C/A} \qquad , \qquad (j\otimes 1)(\mathrm{d}b\otimes c)=c\mathrm{d}j(b)$$

Primera Sucesión Exacta: *La siguiente sucesión es exacta:*

$$\Omega_{B/A} \otimes_B C \xrightarrow{j\otimes 1} \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0$$

Demostración: Para todo C-módulo N tenemos que la sucesión inducida

$$\begin{array}{ccccccc} 0 & \to & \operatorname{Hom}_C(\Omega_{C/B}, N) & \to & \operatorname{Hom}_C(\Omega_{C/A}, N) & \to & \operatorname{Hom}_C(\Omega_{B/A} \otimes_B C, N) \\ & & \| & & \| & & \| \\ & & \operatorname{Der}_B(C, N) & & \operatorname{Der}_A(C, N) & & \operatorname{Hom}_B(\Omega_{B/A}, N) \\ & & & & & & \| \\ & & & & & & \operatorname{Der}_A(B, N) \end{array}$$

es la primera sucesión exacta de derivaciones, y 6.2.1 permite concluir.

(2) Cuando $j\colon B \to C$ es un epimorfismo de A-álgebras de núcleo $\mathfrak{b}$, la diferencial $\mathrm{d}\otimes 1\colon \mathfrak{b} \to \Omega_{B/A} \otimes_B C$ es un morfismo de B-módulos porque

$$\mathrm{d}(bf) \otimes 1 = b(\mathrm{d}f \otimes 1) + f(\mathrm{d}b \otimes 1) = b(\mathrm{d}f \otimes 1),$$

así que induce un morfismo de C-módulos

$$\mathrm{d}\otimes 1\colon \mathfrak{b}/\mathfrak{b}^2 = \mathfrak{b} \otimes_B C \longrightarrow \Omega_{B/A} \otimes_B C \qquad , \qquad (\mathrm{d}\otimes 1)[f] = \mathrm{d}f \otimes 1$$

Segunda Sucesión Exacta: *La siguiente sucesión es exacta:*

$$\mathfrak{b}/\mathfrak{b}^2 \xrightarrow{\mathrm{d}\otimes 1} \Omega_{B/A} \otimes_B C \longrightarrow \Omega_{C/A} \longrightarrow 0$$

Demostración: Para todo C-módulo N tenemos que la sucesión inducida

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Hom}_C(\Omega_{C/A}, N) & \longrightarrow & \operatorname{Hom}_C(\Omega_{B/A} \otimes_B C, N) & \longrightarrow & \operatorname{Hom}_C(\mathfrak{b}/\mathfrak{b}^2, N) \\ & & \| & & \| & & \| \\ & & \operatorname{Der}_A(C, N) & & \operatorname{Hom}_B(\Omega_{B/A}, N) & & \operatorname{Hom}_B(\mathfrak{b}, N) \\ & & & & \| & & \\ & & & & \operatorname{Der}_A(B, N) & & \end{array}$$

es la segunda sucesión exacta de derivaciones, y 6.2.3 permite concluir.

Teorema 9.2.4 *Sea A un álgebra sobre un cuerpo k. Si $p \in \operatorname{Spec} A$ es un punto racional, tenemos un isomorfismo k-lineal*

$$\mathrm{d}\otimes 1\colon \mathfrak{m}_p/\mathfrak{m}_p^2 \xrightarrow{\sim} \Omega_{A/k} \otimes_A A/\mathfrak{m}_p$$

Demostración: Para ver que esta aplicación lineal sea un isomorfismo basta probar que lo es su aplicación traspuesta

$$\begin{array}{ccc} \operatorname{Hom}_k(\Omega_{A/k} \otimes_A k, k) & \longrightarrow & \operatorname{Hom}_k(\mathfrak{m}_p/\mathfrak{m}_p^2, k) \\ \| & & \\ \operatorname{Hom}_A(\Omega_{A/k}, A/\mathfrak{m}_p) & & \\ \| & & \\ \operatorname{Der}_k(A, A/\mathfrak{m}_p) & & \end{array}$$

y ésta es un isomorfismo k-lineal de acuerdo con 9.1.4.

9.3 Propiedades de las Diferenciales

Teorema 9.3.1 *Las diferenciales conmutan con cambios de base. Es decir, si $A \to C$ es un morfismo de anillos, para toda A-álgebra B tenemos un isomorfismo de B_C-módulos*

$$\Omega_{B_C/C} \;=\; \Omega_{B/A} \otimes_A C$$

Demostración: Por la propiedad universal del cambio de base, el morfismo de B-módulos natural $\Omega_{B/A} \to \Omega_{B_C/C}$ induce un morfismo de B_C-módulos

$$\Omega_{B/A} \otimes_A C = \Omega_{B/A} \otimes_B (B_C) \;\longrightarrow\; \Omega_{B_C/C} \qquad , \qquad (\mathrm{d}b) \otimes c \mapsto \mathrm{d}(b \otimes c)$$

Por otra parte, por la propiedad universal del cambio de base, la A-derivación $\mathrm{d} \otimes 1 \colon B \to \Omega_{B/A} \otimes_A C$ define una C-derivación $D \colon B_C \to \Omega_{B/A} \otimes_A C$ tal que $D(b \otimes c) = c(\mathrm{d}b \otimes 1) = (\mathrm{d}b) \otimes c$. Por la propiedad universal de las diferenciales obtenemos un morfismo de B_C-módulos

$$\Omega_{B_C/C} \;\longrightarrow\; \Omega_{B/A} \otimes_A C \qquad , \qquad \mathrm{d}(b \otimes c) \mapsto (\mathrm{d}b) \otimes c$$

que claramente es el inverso del anterior.

Corolario 9.3.2 $\Omega_{B \otimes_A C/A} \;=\; \big(\Omega_{B/A} \otimes_A C\big) \oplus \big(B \otimes_A \Omega_{C/A}\big)$.

Demostración: Las sucesiones exactas de diferenciales asociadas a los morfismos naturales $B \to B \otimes_A C$ y $C \to B \otimes_A C$ son

$$\begin{array}{ccccccccc}
 & & \Omega_{B/A} \otimes_A C & \longrightarrow & \Omega_{B \otimes_A C/A} & \longrightarrow & \Omega_{B \otimes_A C/B} & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longleftarrow & \Omega_{B \otimes_A C/C} & \longleftarrow & \Omega_{B \otimes_A C/A} & \longleftarrow & \Omega_{C/A} \otimes_A B & &
\end{array}$$

así que cada una define un retracto de la otra, y concluimos que ambas escinden.

Lema 9.3.3 *Sea B una A-álgebra y S un sistema multiplicativo de B. Si N es un B_S-módulo, cada A-derivación $D \colon B \to N$ factoriza, y de modo único, a través del morfismo de localización $B \to B_S$:*

$$\mathrm{Der}_A(B_S, N) \;=\; \mathrm{Der}_A(B, N)$$

Demostración: La única A-derivación $D \colon B_S \to N$ que puede coincidir con la derivación dada sobre B es

$$D\left(\frac{b}{s}\right) \;=\; \frac{sDb - bDs}{s^2}$$

y tenemos que probar que está bien definida. Si $b/s = c/t$, existe $r \in S$ tal que $rbt = rcs$. Derivando con D y multiplicando por r obtenemos $r^2 D(bt) = r^2 D(cs)$;

luego $D(bt) = D(cs)$ porque N es un B_S-módulo. Es decir, $tDb+bDt = sDc+cDs$ y dividiendo por st se obtiene que

$$\frac{sDb - bDs}{s^2} \;=\; \frac{tDc - cDt}{t^2}$$

Teorema 9.3.4 *Las diferenciales conmutan con la localización. Es decir, si B es una A-álgebra y S es un sistema multiplicativo de B, tenemos un isomorfismo de B_S-módulos*

$$\big(\Omega_{B/A}\big)_S \;=\; \Omega_{B_S/A}$$

Demostración: Por la propiedad universal de la localización, el morfismo de B-módulos $\Omega_{B/A} \to \Omega_{B_S/A}$ define un morfismo de B_S-módulos $(\Omega_{B/A})_S \to \Omega_{B_S/A}$. Ahora, por el lema anterior, para todo B_S-módulo N tenemos que

$$\begin{aligned}\mathrm{Hom}_{B_S}(\Omega_{B_S/A}, N) &= \mathrm{Der}_A(B_S, N) = \mathrm{Der}_A(B, N)\\ &= \mathrm{Hom}_B(\Omega_{B/A}, N) = \mathrm{Hom}_{B_S}\big((\Omega_{B/A})_S, N\big)\end{aligned}$$

y 6.2.2 permite concluir que $\big(\Omega_{B/A}\big)_S = \Omega_{B_S/A}$.

Teorema 9.3.5 *Las diferenciales conmutan con sumas directas finitas:*

$$\Omega_{(B\oplus C)/A} \;=\; \Omega_{B/A} \oplus \Omega_{C/A}$$

Demostración: El ideal de la diagonal Δ en $(B \oplus C) \otimes_A (B \oplus C) = (B \otimes_A B) \oplus (B \otimes_A C) \oplus (C \otimes_A B) \oplus (C \otimes_A C)$es

$$\begin{aligned}\Delta &= \Delta_B \oplus (B \otimes_A C) \oplus (C \otimes_A B) \oplus \Delta_C\\ \Delta^2 &= \Delta_B^2 \oplus (B \otimes_A C) \oplus (C \otimes_A B) \oplus \Delta_C^2\\ \Omega_{(B\oplus C)/A} &= \Delta/\Delta^2 = \Delta_B/\Delta_B^2 \oplus 0 \oplus 0 \oplus \Delta_C/\Delta_C^2 = \Omega_{B/A} \oplus \Omega_{C/A}\end{aligned}$$

Epílogo

Los conceptos más importantes, los que están involucrados en cualquier afirmación humana, los que usamos necesariamente al pensar, son los conceptos metafísicos; como cuando decimos que A es *verdadero*, que A *existe* o que A *es* B. Una profunda justificación de las Matemáticas es su capacidad para iluminar cuestiones tan cruciales, y ya a la entrada de la Academia platónica figuraba la inscripción $\mathit{Μηδεις\ αγεωμετρητος\ εισιτω\ μου\ την\ στεγην}$ (Nadie entre sin Geometría).

Con la experiencia que hemos acumulado a lo largo de este libro, ya es evidente que una afirmación como pueda ser "P *es* el producto directo de $\mathbb{R}$ por $\mathbb{R}$" tiene diferentes sentidos según el contexto en que nos la encontremos:

1. En un texto de teoría de grupos deberemos entender que P es un grupo, que el producto directo de $\mathbb{R}$ por $\mathbb{R}$ es el grupo formado por los pares de números reales con la operación definida por la suma componente a componente, y que el predicado *es* afirma la existencia de un isomorfismo de grupos entre ambos grupos.

2. En una clase de Topología debemos entender que P es un espacio topológico, que el producto directo de $\mathbb{R}$ por $\mathbb{R}$ es el espacio topológico formado por los pares de números reales con la topología usual, y que el predicado *es* afirma la existencia de un homeomorfismo entre ambos espacios topológicos.

3. En un ejercicio de Álgebra Lineal, deberemos entender que P es un espacio vectorial real, que el producto directo de $\mathbb{R}$ por $\mathbb{R}$ está formado por los pares de números reales con la estructura usual de espacio vectorial real, y que el predicado *es* afirma la existencia de un isomorfismo lineal entre ambos espacios vectoriales.

4. En el capítulo 3, dedicado a los anillos, deberíamos entender que P es un anillo, que el producto directo de $\mathbb{R}$ por $\mathbb{R}$ es el anillo formado por los pares de números reales con las operaciones definidas componente a componente, y que el predicado *es* afirma la existencia de un isomorfismo de anillos entre ambos anillos.

5. En un ejercicio sobre variedades algebraicas reales, debemos entender que P es una variedad algebraica real, que $\mathbb{R} = \operatorname{Spec} \mathbb{R}[x]$, que el producto directo de $\mathbb{R}$ por $\mathbb{R}$ es $\mathbb{R} \times \mathbb{R} = \operatorname{Spec} \mathbb{R}[x, y]$, y que el predicado *es* afirma la existencia de un isomorfismo de variedades algebraicas $P \simeq \mathbb{R} \times \mathbb{R}$; es decir, de un isomorfismo de $\mathbb{R}$-álgebras $\mathbb{R}[x, y] \simeq \mathcal{O}(P)$.

Ahora vemos claramente que cada vez que hemos enunciado un teorema, éste se encontraba en un contexto determinado (teoría de grupos, de anillos, de módulos, de espacios topológicos, de variedades algebraicas, etc.) que fijaba el sentido de algunos términos básicos, como pueden ser los de morfismo, cociente, producto directo, ... Ante todo, tal contexto precisa el significado de la afirmación de que cierta estructura A *sea* tal otra B, por lo que estas teorías o ambientes donde exponemos los teoremas y desarrollamos nuestros razonamientos reciben el nombre de categorías, en memoria de Aristóteles (383-321 a. de Cristo) que cayó en la cuenta de que *el ser se predica de diversos modos* y llamó $\kappa\alpha\tau\eta\gamma o\rho\dot{\imath}\alpha\iota$ a los diferentes modos de predicar el verbo ser.

Categorías

Axiomas de Categoría: Dar una **categoría C** es dar

–. Una familia arbitraria, cuyos elementos llamaremos **objetos** de **C**.

–. Unos conjuntos disjuntos $\mathrm{Hom}_{\mathbf{C}}(M,N)$, uno para cada par de objetos M,N de la categoría, cuyos elementos llamaremos **morfismos** de M en N y denotaremos con el símbolo $M \to N$.

–. Para cada terna M,N,P de objetos de la categoría, una aplicación (llamada **composición** de morfismos):

$$\mathrm{Hom}_{\mathbf{C}}(N,P) \times \mathrm{Hom}_{\mathbf{C}}(M,N) \longrightarrow \mathrm{Hom}_{\mathbf{C}}(M,P)\ , \quad (f,g) \mapsto f \circ g$$

Estos tres datos deben satisfacer las siguientes condiciones:

Axioma 1: La composición de morfismos, cuando tenga sentido, es asociativa: $(f \circ g) \circ h = f \circ (g \circ h)$

Axioma 2: Para cada objeto M de **C**, existe un morfismo $\mathrm{id}_M : M \to M$ que actúa como identidad por la izquierda y por la derecha respecto de la composición de morfismos:

$$f \circ \mathrm{id}_M = f \text{ para todo morfismo } f : M \to N$$
$$\mathrm{id}_M \circ g = g \text{ para todo morfismo } g : N \to M$$

Este morfismo $\mathrm{id}_M : M \to M$ es único y se llama **identidad** de M.

Dada una categoría **C**, diremos que un morfismo $f\colon M \to N$ es un **isomorfismo** si existe algún morfismo $g\colon N \to M$ tal que $f \circ g = \mathrm{id}_N$ y $g \circ f = \mathrm{id}_M$, en cuyo caso tal morfismo g es único y se llama **inverso** de f. Los isomorfismos de un objeto M en sí mismo reciben el nombre de **automorfismos** de M.

La identidad de cualquier objeto de una categoría $\mathbf{C}$ es un isomorfismo, el inverso de un isomorfismo es un isomorfismo, y la composición de isomorfismos, cuando tenga sentido, es un isomorfismo. Por tanto, los automorfismos de cualquier objeto M de $\mathbf{C}$ forman un grupo $\mathrm{Aut}_{\mathbf{C}}(M)$ respecto de la composición y el elemento neutro es la identidad id_M .

Cuando hablamos de teoría de grupos, teoría de anillos, teoría de espacios topológicos, etc., esa noción intuitiva de "teoría" queda recogida y precisada en el concepto de categoría. Las categorías proporcionan los ambientes donde desarrollamos nuestros estudios de Matemáticas:

1. La categoría de conjuntos **Sets**: Sus objetos son los conjuntos, sus morfismos son las aplicaciones y la composición es la composición de aplicaciones. La categoría de grupos **Gr**: Sus objetos son los grupos, sus morfismos son los morfismos de grupos y la composición es la composición de aplicaciones. La categoría de anillos **Rings**: Sus objetos son los anillos, sus morfismos son los morfismos de anillos y la composición es la composición de aplicaciones.

2. La categoría de A-módulos **A-mod**: Sus objetos son los A-módulos, sus morfismos son los morfismos A-lineales y la composición es la composición de aplicaciones. Análogamente se define la categoría **A-alg** de A-álgebras con los morfismos de A-álgebras. Por el contrario, no es lícito hablar de la categoría de módulos (o de álgebras), pues no hemos definido el concepto de morfismo entre módulos o álgebras sobre anillos diferentes.

3. La categoría de espacios topológicos **Top**: Sus objetos son los espacios topológicos, sus morfismos son las aplicaciones continuas y la composición es la composición de aplicaciones.

4. La categoría de espacios métricos e isometrías. La categoría de espacios métricos y aplicaciones continuas.

5. La categoría de espacios normados con las aplicaciones lineales continuas.

6. La categoría de conjuntos ordenados **Ord**: Sus objetos son los conjuntos ordenados. Los morfismos de conjuntos ordenados $f\colon X \to Y$ son las aplicaciones que conservan el orden: si $x \leq x'$, entonces $f(x) \leq f(x')$.

7. A partir de cualquier categoría pueden obtenerse nuevas categorías sin más que restringir los objetos y los morfismos, con la única condición de elegir familias de morfismos que contengan la identidad y sean estables por la composición. Así, por ejemplo, tenemos las siguientes categorías:

   (a) La categoría de conjuntos finitos.

   (b) La categoría de conjuntos y aplicaciones epiyectivas.

(c) La categoría de extensiones finitas de un cuerpo dado k.

(d) La categoría de k-espacios vectoriales e isomorfismos k-lineales.

(e) La categoría de espacios topológicos compactos Hausdorff.

8. Las parejas $(A, \mathfrak{a})$, donde A es un anillo y $\mathfrak{a}$ es un ideal de A, forman una categoría, entendiendo que los morfismos $j\colon (A, \mathfrak{a}) \to (B, \mathfrak{b})$ son los morfismos de anillos $j\colon A \to B$ tales que $j(\mathfrak{a}) \subseteq \mathfrak{b}$.

9. Las sucesiones exactas cortas de A-módulos forman una categoría, entendiendo que dar un morfismo de una sucesión exacta corta de A-módulos

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

en otra sucesión exacta corta de A-módulos

$$0 \longrightarrow N' \xrightarrow{j} N \xrightarrow{q} N'' \longrightarrow 0$$

es dar morfismos de A-módulos $h'\colon M' \to N'$, $h\colon M \to N$, $h''\colon M'' \to N''$ tales que el siguiente diagrama sea conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \downarrow h' & & \downarrow h & & \downarrow h'' & & \\ 0 & \longrightarrow & N' & \xrightarrow{j} & N & \xrightarrow{q} & N'' & \longrightarrow & 0 \end{array}$$

10. Cada grupo $(G, \cdot)$ puede entenderse como una categoría con un único objeto M y tal que los elementos de G son los morfismos $M \to M$, siendo la composición de morfismos la operación de G; es decir, $a \circ b = a \cdot b$ para todo $a, b \in G$.

    En este ejemplo la identidad de M es el neutro de G y todos los morfismos son isomorfismos. Además, G es el grupo de los automorfismos del único objeto M.

11. Cada relación R reflexiva y transitiva en un conjunto X puede entenderse como una categoría cuyos objetos son los elementos de X y cuyos morfismos se definen del siguiente modo: Dados $x, x' \in X$, no hay ningún morfismo $x \to x'$ cuando x no esté relacionado con x' y hay un único morfismo $x \to x'$ cuando xRx'.

    En particular, toda relación de equivalencia puede verse como una categoría, al igual que cualquier conjunto ordenado $(X, \leq)$. Así, los abiertos de un espacio topológico, los subespacios vectoriales de un espacio vectorial, los ideales de un anillo, etc., pueden entenderse como categorías.

12. Dada una categoría $\mathbf{C}$, su categoría *opuesta* o *dual* $\mathbf{C^{op}}$ es la categoría que tiene los mismos objetos que $\mathbf{C}$ y tal que los morfismos de M en N en la categoría $\mathbf{C^{op}}$ son los morfismos de N en M en la categoría $\mathbf{C}$:

$$\text{Objetos de } \mathbf{C^{op}} = \text{Objetos de } \mathbf{C}$$
$$\mathrm{Hom}_{\mathbf{C^{op}}}(M,N) = \mathrm{Hom}_{\mathbf{C}}(N,M)$$

siendo la composición $f \circ g$ de dos morfismos $g\colon M \to N$, $f\colon N \to P$ en $\mathbf{C^{op}}$ igual a la composición $g \circ f$ en $\mathbf{C}$.

Funtores

La mayoría de nuestras definiciones se expresan imponiendo alguna propiedad o condición (como ocurre con la definición de número primo, función continua, grupo cíclico, divisor de cero, ideal primario, ...) o estableciendo una aplicación (la suma de números racionales, la derivada, la longitud de un módulo, los ideales primos asociados, ...); pero algunas de las definiciones más importantes no son de esta forma: la construcción del grupo cociente, del espacio dual, del anillo de fracciones, del producto tensorial, del espectro, etc. En todas estas construcciones asociamos a cada objeto de cierta categoría $\mathbf{C}$ un objeto de otra categoría **C'**, y vamos a ver que las construcciones realmente importantes, las que intervienen en nuestros teoremas, no sólo están definidas para los objetos de una categoría $\mathbf{C}$, sino también para todos sus morfismos:

Definición: Sean $\mathbf{C}$ y **C'** dos categorías. Dar un **funtor covariante** $F\colon \mathbf{C} \rightsquigarrow$ **C'** es asignar a cada objeto M de $\mathbf{C}$ un objeto $F(M)$ de $\mathbf{C'}$ y a cada morfismo $f\colon M \to N$ de $\mathbf{C}$ un morfismo $F(f)\colon F(M) \to F(N)$ de **C'**, de modo que se verifiquen las siguientes condiciones:

1. $F(\mathrm{id}_M) = \mathrm{id}_{F(M)}$ para todo objeto M de $\mathbf{C}$.

2. $F(f \circ g) = F(f) \circ F(g)$ para cualquier par de morfismos $M \xrightarrow{g} N$, $N \xrightarrow{f} P$ de la categoría $\mathbf{C}$.

Análogamente se definen los **funtores contravariantes**, que invierten el sentido de los morfismos; es decir, asignan a cada morfismo $f\colon M \to N$ de $\mathbf{C}$ un morfismo $F(f)\colon F(N) \to F(M)$ de $\mathbf{C'}$, sin más que sustituir la condición (2) por la de que $F(f \circ g) = F(g) \circ F(f)$. Dicho de otro modo, los funtores contravariantes de $\mathbf{C}$ en $\mathbf{C'}$ son los funtores covariantes de la categoría opuesta $\mathbf{C^{op}}$ en **C'**, por lo que, en el estudio de los funtores, podemos restringirnos al caso covariante sin pérdida de generalidad.

Los funtores transforman isomorfismos en isomorfismos. Además, los funtores pueden componerse del modo obvio, obteniéndose de nuevo un funtor, covariante o contravariante según la paridad del número de funtores contravariantes que intervengan en la composición.

El concepto de funtor intenta recoger y precisar la noción intuitiva de "construcción natural":

1. Sea k un cuerpo. La construcción del espacio dual $E \rightsquigarrow E^*$ define un funtor contravariante **k-mod** $\rightsquigarrow$ **k-mod**, donde la aplicación lineal $f^*\colon V^* \to E^*$ asociada a una aplicación lineal $f\colon E \to V$ es la aplicación traspuesta:

$$< f^*(\omega), e > = < \omega, f(e) > , \qquad e \in E\,,\ \omega \in V^*$$

   y el bidual $E \rightsquigarrow E^{**}$ es un funtor covariante **k-mod** $\rightsquigarrow$ **k-mod**. El dual puede entenderse como un funtor covariante a condición de restringirse a la categoría de k-espacios vectoriales con isomorfismos, asignando a cada isomorfismo lineal $\tau\colon E \to F$ el isomorfismo $(\tau^*)^{-1}\colon E^* \to V^*$.

2. La construcción $X \rightsquigarrow \mathcal{C}(X)$ del anillo de las funciones reales continuas sobre un espacio topológico X arbitrario define un funtor contravariante **Top** $\rightsquigarrow$ **Rings** de la categoría de espacios topológicos en la categoría de anillos, asignando a cada aplicación continua $h\colon X \to Y$ el morfismo de anillos $\circ h\colon \mathcal{C}(Y) \to \mathcal{C}(X)\,,\ f \mapsto f \circ h\,.$

3. Sea M un A-módulo. La construcción $N \rightsquigarrow \mathrm{Hom}_A(M, N)$ define un funtor covariante

$$\mathrm{Hom}_A(M, -)\colon \textbf{A-mod} \rightsquigarrow \textbf{A-mod}$$

   sin más que asignar a cada morfismo de A-módulos $f\colon N \to N'$ el morfismo de A-módulos $f\circ\colon \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N')\,.$

   Análogamente, la construcción $N \rightsquigarrow \mathrm{Hom}_A(N, M)$ define un funtor contravariante

$$\mathrm{Hom}_A(-, M)\colon \textbf{A-mod} \rightsquigarrow \textbf{A-mod}$$

   sin más que asignar a cada morfismo de A-módulos $f\colon N \to N'$ el morfismo de A-módulos $\circ f\colon \mathrm{Hom}_A(N', M) \to \mathrm{Hom}_A(N, M)\,.$

4. Sea M un A-módulo. La construcción $N \rightsquigarrow N \otimes_A M$ del producto tensorial define un funtor covariante

$$(-) \otimes_A M\colon \textbf{A-mod} \rightsquigarrow \textbf{A-mod}$$

   asignando a cada morfismo de A-módulos $f\colon N \to N'$ el morfismo de A-módulos $f \otimes 1\colon N \otimes M \to N' \otimes M\,.$

5. Sea $A \to B$ un morfismo de anillos. El cambio de base $M \rightsquigarrow M_B$ define un funtor covariante **A-mod** $\rightsquigarrow$ **B-mod** asignando a cada morfismo de A-módulos $f\colon M \to N$ su cambio de base

$$f_B\colon M_B \longrightarrow N_B\ , \quad f_B(m \otimes b) = f(m) \otimes b$$

   Análogamente, el cambio de base $C \rightsquigarrow C_B$ define un funtor covariante **A-alg** $\rightsquigarrow$ **B-alg**. Por otra parte, la restricción de escalares define sendos funtores covariantes **B-mod** $\rightsquigarrow$ **A-mod** y **B-alg** $\rightsquigarrow$ **A-alg**.

6. El espectro es un funtor contravariante Spec : **Rings** $\rightsquigarrow$ **Top** de la categoría de anillos en la de espacios topológicos.

7. Sea S un sistema multiplicativo de un anillo A. La localización $M \rightsquigarrow S^{-1}M$ define un funtor covariante $S^{-1}(-)\colon$ **A-mod** $\rightsquigarrow$ $\mathbf{S^{-1}A}$**-mod** que transforma cada morfismo de A-módulos $f\colon M \to N$ en el morfismo de $S^{-1}A$-módulos $S^{-1}f\colon S^{-1}M \to S^{-1}N$.

8. Si asignamos a cada espacio topológico X el retículo de sus cerrados $A(X)$ y a cada aplicación continua $h\colon X \to Y$ el morfismo de conjuntos ordenados $h^{-1}\colon A(Y) \to A(X)$, obtenemos un funtor contravariante **Top** $\rightsquigarrow$ **Ord** de la categoría de espacios topológicos en la de conjuntos ordenados.

9. Si asignamos a cada A-módulo M el retículo de sus submódulos $Submod(M)$ y a cada morfismo de A-módulos $f\colon M \to N$ el morfismo de conjuntos ordenados $f^{-1}\colon Submod(N) \to Submod(M)$, obtenemos un funtor contravariante **A-mod** $\rightsquigarrow$ **Ord**.

10. Si asignamos a cada anillo A el grupo A^* formado por sus elementos invertibles y a cada morfismo de anillos $f\colon A \to B$ su restricción $f\colon A^* \to B^*$, que es un morfismo de grupos, obtenemos un funtor covariante **Rings** $\rightsquigarrow$ **Ab** de la categoría de anillos en la de grupos abelianos.

11. Si a cada anillo $(A, +, \cdot)$ le asignamos el grupo $(A, +)$ y a cada morfismo de anillos $f\colon (A, +, \cdot) \to (B, +, \cdot)$ le asignamos el morfismo de grupos $f\colon (A, +) \to (B, +)$, obtenemos un funtor covariante **Rings** $\rightsquigarrow$ **Ab**, llamado funtor de *olvido*. También tenemos funtores de olvido **Gr** $\rightsquigarrow$ **Sets**, **Rings** $\rightsquigarrow$ **Sets**, **A-mod** $\rightsquigarrow$ **Ab**, **k-alg** $\rightsquigarrow$ **Rings**, etc.

12. La construcción del A-módulo libre $A^{(I)}$ de base un conjunto I define un funtor contravariante **Sets** $\rightsquigarrow$ **A-mod**, sin más que asignar a cada aplicación $f\colon I \to J$ el morfismo de A-módulos $\phi\colon A^{(J)} \to A^{(I)}$, $\phi\big(\sum_j a_j\big) = \sum_i a_{f(i)}$.

13. La construcción del álgebra de endomorfismos $E \rightsquigarrow \mathrm{End}_k(E)$ de un k-espacio vectorial E define un funtor covariante de la categoría de k-espacios vectoriales e isomorfismos en la de k-álgebras (no conmutativas), sin más que

observar que cada isomorfismo lineal $\tau\colon E \to V$ induce de modo natural un isomorfismo de k-álgebras $\mathrm{End}_k(E) \to \mathrm{End}_k(V)$, $f \mapsto \tau \circ f \circ \tau^{-1}$.

14. Sea **C** la categoría formada por las parejas $(\mathfrak{a}, A)$, donde $\mathfrak{a}$ es un ideal de un anillo A, y donde los morfismos $(\mathfrak{a}, A) \to (\mathfrak{b}, B)$ son los morfismos de anillos $f\colon A \to B$ tales que $f(\mathfrak{a}) \subseteq \mathfrak{b}$. La construcción del anillo cociente $(\mathfrak{a}, A) \rightsquigarrow A/\mathfrak{a}$ define un funtor covariante $\mathbf{C} \rightsquigarrow \mathbf{Rings}$.

15. Sea **C** la categoría formada por las pareja (S, A) donde A es un anillo y S es un sistema multiplicativo de A, entendiendo que los morfismos $(S, A) \to (T, B)$ son los morfismos de anillos $f\colon A \to B$ tales que $f(S) \subseteq T$. La construcción del anillo de fracciones $(S, A) \rightsquigarrow S^{-1}A$ define un funtor covariante $\mathbf{C} \rightsquigarrow \mathbf{Rings}$.

16. Si $A \to B$ es un morfismo de anillos, $M \rightsquigarrow \mathrm{Der}_A(B, M)$ es un funtor covariante de la categoría B-módulos en sí misma.

17. Dada una categoría **C**, el funtor identidad $\mathrm{id}_{\mathbf{C}}\colon \mathbf{C} \rightsquigarrow \mathbf{C}$ es el funtor covariante que transforma cada objeto de **C** el él mismo y cada morfismo de **C** en sí mismo.

Morfismos de Funtores

Al establecer una aplicación, estará definida entre estructuras previamente construidas y, en el apartado anterior, ya hemos señalado que las construcciones matemáticas más importantes son funtoriales. Es mérito fundamental de la Teoría de categorías poner de manifiesto que las transformaciones $F(M) \to G(M)$ entre construcciones funtoriales son naturales, que satisfacen la fortísima condición de ser compatibles con todos los morfismos en el siguiente sentido:

Definición: Sean $F, G\colon \mathbf{C} \rightsquigarrow \mathbf{C'}$ dos funtores covariantes definidos entre ciertas categorías **C** y **C'**. Dar un **morfismo de funtores** $t\colon F \to G$ es dar, para cada objeto M de **C**, un morfismo $t_M\colon F(M) \to G(M)$ de **C'**, de manera que para todo morfismo $f\colon M \to N$ de **C** el siguiente cuadrado conmute:

$$\begin{array}{ccc} F(M) & \xrightarrow{t_M} & G(M) \\ \downarrow {\scriptstyle F(f)} & & \downarrow {\scriptstyle G(f)} \\ F(N) & \xrightarrow{t_N} & G(N) \end{array}$$

Sean F, G, $H\colon \mathbf{C} \rightsquigarrow \mathbf{C'}$ funtores covariantes. Dados morfismo de funtores $t\colon F \to G$, $t'\colon G \to H$, su composición $t' \circ t\colon F \to H$ se define del modo evidente,

$(t' \circ t)_M = t'_M \circ t_M$, y es sencillo comprobar que es un morfismo del funtor F en el funtor H.

Por otra parte, los morfismos identidad $\mathrm{id}_M \colon F(M) \to F(M)$ definen un morfismo de funtores $\mathrm{id}_F \colon F \to F$.

Diremos que un morfismo de funtores $t \colon F \to G$ es un **isomorfismo de funtores** cuando $t_M \colon F(M) \to G(M)$ es un isomorfismo para todo objeto M de $\mathbf{C}$; es decir, cuando existe un morfismo de funtores $t^{-1} \colon G \to F$ tal que $t^{-1} \circ t \colon F \to F$ es la identidad de F y $t \circ t^{-1} \colon G \to G$ es la identidad de G. En tal caso, es evidente que $(t^{-1})_M = (t_M)^{-1}$.

El concepto de morfismo de funtores intenta recoger los términos imprecisos de "morfismo canónico", "operación natural", ... que utilizamos para indicar el carácter general y nada artificioso de una definición; es decir, su pertenencia al ámbito de la $\varphi\dot{\upsilon}\sigma\iota\varsigma$ en el sentido originario que ésta tenía en la cultura griega. En palabras de Heidegger (1889-1976):

> $\Phi\dot{\upsilon}\sigma\iota\varsigma$ significa la fuerza que impera, brota y permanece regulada por ella misma.... Como manifestación opuesta los griegos introdujeron lo que llamaban $\theta\,\dot{\varepsilon}\,\sigma\iota\varsigma$, lo puesto, o $\nu\acute{o}\mu o\varsigma$, regla en el sentido de costumbre.... Ya dentro de la filosofía griega se introdujo pronto un uso más restringido de $\varphi\dot{\upsilon}\sigma\iota\varsigma$, a partir de su oposición a $\tau\dot{\varepsilon}\chi\nu\eta$, que significa "saber", creación y construcción, en tanto que producción a partir de un saber.

Por ejemplo, en los espacios vectoriales, la introducción de definiciones y demostraciones en coordenadas pertenece a la $\theta\dot{\varepsilon}\sigma\iota\varsigma$, la mal llamada base canónica de k^n es $\nu\acute{o}\mu o\varsigma$, y la construcción de un ejemplo que contradiga cierta conjetura famosa pertenece a la $\tau\dot{\varepsilon}\chi\nu\eta$; mientras que la identificación de cada vector con una función lineal sobre el espacio dual es natural, pertenece al ámbito de la $\varphi\dot{\upsilon}\sigma\iota\varsigma$. Esta distinción, que tan claramente percibimos en las entrañas, puede precisarse un poco ahora afirmando que el morfismo $E \to E^{**}$ es funtorial.

1. La aplicación lineal $\phi_E \colon E \to E^{**}$ de cualquier k–espacio vectorial en su bidual, $\phi_E(e)(\omega) = \omega(e)$, es natural en el sentido de que es un morfismo del funtor identidad (de la categoría de k–espacios vectoriales) en el funtor $F(E) = E^{**}$; es decir, para toda aplicación k–lineal $T \colon E \to F$ tenemos que el siguiente cuadrado es conmutativo:

$$\begin{array}{ccc} E & \xrightarrow{\phi_E} & E^{**} \\ \downarrow T & & \downarrow T^{**} \\ F & \xrightarrow{\phi_F} & F^{**} \end{array}$$

2. La inmersión diagonal $\Delta_X\colon X \to X \times X$, $x \mapsto (x,x)$, de cualquier espacio topológico X en el producto directo $X \times X$ es natural en el sentido de que es un morfismo del funtor identidad en el funtor $F(X) = X \times X$; es decir, para toda aplicación continua $h\colon X \to Y$, el siguiente cuadrado conmuta:

$$\begin{array}{ccc} X & \xrightarrow{\Delta_X} & X \times X \\ \downarrow h & & \downarrow h \times h \\ Y & \xrightarrow{\Delta_Y} & Y \times Y \end{array}$$

3. La inmersión canónica $j_E\colon E \to \widehat{E}$ de cualquier espacio normado E en su completación $\widehat{E}$ es un morfismo del funtor identidad en el funtor completación $E \rightsquigarrow \widehat{E}$, entendidos ambos como funtores de la categoría de espacios normados y aplicaciones lineales continuas en sí misma; es decir, para toda aplicación lineal continua $h\colon E \to F$ entre espacios normados se tiene que el siguiente cuadrado es conmutativo:

$$\begin{array}{ccc} E & \xrightarrow{j_E} & \widehat{E} \\ \downarrow h & & \downarrow \widehat{h} \\ F & \xrightarrow{j_F} & \widehat{F} \end{array}$$

4. Cada morfismo de A-módulos $g\colon M_1 \to M_2$ induce un morfismo funtorial $g \otimes 1\colon M_1 \otimes_A N \to M_2 \otimes_A N$; es decir, para todo morfismo de A-módulos $f\colon M \to N$ se verifica que el siguiente cuadrado conmuta:

$$\begin{array}{ccc} M_1 \otimes_A M & \xrightarrow{g\otimes 1} & M_2 \otimes_A M \\ \downarrow 1 \otimes f & & \downarrow 1 \otimes f \\ M_1 \otimes_A N & \xrightarrow{g\otimes 1} & M_2 \otimes_A N \end{array}$$

5. Cada morfismo de A-módulos $g\colon M_1 \to M_2$ induce un morfismo de funtores $g\circ\colon \mathrm{Hom}_A(-,M_1) \to \mathrm{Hom}_A(-,M_2)$ porque para todo morfismo de A-módulos $f\colon M \to N$ se verifica que el siguiente cuadrado conmuta:

$$\begin{array}{ccc} \mathrm{Hom}_A(M,M_1) & \xrightarrow{g\circ} & \mathrm{Hom}_A(M,M_2) \\ \downarrow \circ f & & \downarrow \circ f \\ \mathrm{Hom}_A(N,M_1) & \xrightarrow{g\circ} & \mathrm{Hom}_A(N,M_2) \end{array}$$

También define un morfismo funtorial $\circ g\colon \mathrm{Hom}_A(M_2,-) \to \mathrm{Hom}_A(M_1,-)$.

6. Sean S y T sistemas multiplicativos de un anillo A. Si $S \subseteq T$, los morfismos $S^{-1}M \to T^{-1}M$, $m/s \mapsto m/s$ son funtoriales, entendiendo $S^{-1}(-)$ y $T^{-1}(-)$ como funtores covariantes **A-mod** $\rightsquigarrow$ **A-mod**.

7. La contracción de índices $C^i_j\colon T^q_p(E) \to T^{q-1}_{p-1}(E)$ en los tensores de tipo (p,q) sobre un espacio vectorial E es un morfismo del funtor $T^q_p(-)$ en el funtor $T^{q-1}_{p-1}(-)$, ambos definidos sobre la categoría de k-espacios vectoriales e isomorfismos; es decir, $C^i_j(\tau T^q_p) = \tau(C^i_j T^q_p)$ para todo isomorfismo lineal $\tau\colon E \to V$ y todo tensor $T^q_p \in T^q_p(E)$.

8. En la teoría de grupos, el paso al inverso $G \to G$, $g \mapsto g^{-1}$, y elevar al cuadrado $G \to G$, $g \mapsto g^2$, son operaciones funtoriales, en el sentido de que son morfismos del funtor de olvido en sí mismo. Vemos así que la teoría de categorías nos abre nuevas perspectivas, al hacer posible que podamos comenzar a plantear con rigor y sentido preciso preguntas tales como

   ¿Qué aplicaciones naturales $G \to G$ pueden definirse en los grupos? Es decir, ¿qué morfismos hay del funtor de olvido $\mathbf{Gr} \rightsquigarrow \mathbf{Sets}$ en sí mismo?

   ¿Qué morfismos naturales $G \to G$ pueden definirse en los grupos? Es decir, ¿qué morfismos existen del funtor identidad $\mathrm{id}_{\mathbf{Gr}}\colon \mathbf{Gr} \rightsquigarrow \mathbf{Gr}$ en él mismo?

   ¿Qué operaciones binarias naturales $G \times G \to G$ pueden definirse en los grupos? i.e., ¿qué morfismos hay del funtor $\mathbf{Gr} \rightsquigarrow \mathbf{Sets}$, $G \rightsquigarrow G \times G$, en el funtor de olvido $\mathbf{Gr} \rightsquigarrow \mathbf{Sets}$?

   y no sólo nos permite plantear tales preguntas, sino comenzar a responderlas. Veamos por ejemplo que, en teoría de grupos, toda aplicación funtorial $t\colon G \to G$ ha de ser $t(g) = g^n$ para algún $n \in \mathbb{Z}$. En efecto, consideremos la aplicación $t_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{Z}$ y sea $n = t_{\mathbb{Z}}(1)$. Ahora, dado cualquier elemento g de un grupo G, induce un morfismo de grupos $f_g\colon \mathbb{Z} \to G$, $f_g(r) = g^r$, de modo que el siguiente cuadrado es conmutativo:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{t_{\mathbb{Z}}} & \mathbb{Z} \\ \downarrow f_g & & \downarrow f_g \\ G & \xrightarrow{t_G} & G \end{array}$$

$$t_G(g) = t_G\big(f_g(1)\big) = f_g\big(t_{\mathbb{Z}}(1)\big) = f_g(n) = g^n$$

9. En teoría de grupos, la operación $G \times G \to G$, $(a,b) \mapsto b^5a^8b^{-9}a^6$ es funtorial, en el sentido de que para todo morfismo de grupos $f\colon G \to G'$ se tiene que $f(b^5a^8b^{-9}a^6) = f(b)^5 f(a)^8 f(b)^{-9} f(a)^6$; pero no podemos decir que es una operación canónica en los grupos, pues en modo alguno podemos considerar canónica la sucesión de exponentes $5, 8, -9, 6$ sino totalmente arbitraria. Vemos así que, aunque todo lo canónico debe ser funtorial, los conceptos de funtor y morfismo de funtores no agotan nuestra aguda percepción de lo que ha de ser considerado canónico y natural.

El concepto de isomorfismo de funtores pretende precisar los términos de "isomorfismo canónico", "biyección natural", etc., pues dos construcciones funtorialmente isomorfas son indistinguibles en Matemáticas. Podemos sustituir cualquier

funtor por otro isomorfo en nuestros razonamientos sin que por ello se vean alterados. Por el contrario, si un isomorfismo entre dos estructuras no es funtorial, éstas pueden intervenir de formas bien distintas en las teorías matemáticas, pues nuestros razonamientos involucran constantemente morfismos y la falta de funtorialidad significa precisamente que ambas estructuras tienen comportamientos bien diferentes frente a los morfismos. Por eso los isomorfismos funtoriales se denotan con el símbolo $=$, mientras que se suele reservar el símbolo $\simeq$ para los isomorfismos que no son naturales:

1. Sea S un sistema multiplicativo de un anillo A. Los isomorfismos de $S^{-1}A$-módulos $M \otimes_A S^{-1}A = S^{-1}M$, $m \otimes (a/s) = (am)/s$ son funtoriales; es decir, para todo morfismo de A-módulos $f\colon M \to N$ se verifica que el siguiente cuadrado es conmutativo:

$$\begin{array}{ccc} M \otimes_A S^{-1}A & = & S^{-1}M \\ \downarrow {\scriptstyle f \otimes 1} & & \downarrow {\scriptstyle S^{-1}f} \\ N \otimes_A S^{-1}A & = & S^{-1}N \end{array}$$

2. Todas las propiedades del producto tensorial y, en general, todas las igualdades de este libro son de hecho isomorfismos funtoriales. Por ejemplo, la igualdad $M \otimes_A N = N \otimes_A M$ puede entenderse como un isomorfismo entre los funtores $(-) \otimes_A N$ y $N \otimes_A (-)$, la igualdad $M \otimes_A (A/\mathfrak{a}) = M/\mathfrak{a}M$ como un isomorfismo del funtor $(-) \otimes_A (A/\mathfrak{a})$ con el funtor $M \rightsquigarrow M/\mathfrak{a}M$, y así sucesivamente.

3. La biyección natural

$$\begin{bmatrix}\text{Submódulos} \\ \text{de } M/N\end{bmatrix} = \begin{bmatrix}\text{Submódulos de } M \\ \text{que contienen a } N\end{bmatrix}$$

es un isomorfismo funtorial, donde ambos términos de la igualdad se entienden como funtores contravariantes, definidos sobre la categoría de pares (N, M), donde M es un A-módulo y N es un submódulo de M, y con valores en la categoría de conjuntos ordenados.

4. Todo espacio vectorial de dimensión finita es funtorialmente isomorfo a su bidual, $E = E^{**}$, lo que da cuenta del hecho de que en Álgebra Lineal no sea necesario involucrar duales iterados E^{**}, E^{***}, ... , pues siempre pueden sustituirse por el propio espacio E o su dual E^*. En efecto, el isomorfismo $\phi_E\colon E \to E^{**}$, $< \phi_E(e), \omega > = < \omega, e >$, define un isomorfismo natural del funtor identidad en el funtor bidual $E \rightsquigarrow E^{**}$; es decir, para toda aplicación lineal $f\colon E \to V$ entre espacios vectoriales de dimensión finita, se verifica

que el siguiente cuadrado es conmutativo:

$$\begin{array}{ccc} E & \xrightarrow{\phi_E} & E^{**} \\ \downarrow f & & \downarrow f^{**} \\ V & \xrightarrow{\phi_V} & V^{**} \end{array}$$

$$< f^{**}\phi_E(e), \eta > = < \phi_E(e), f^*(\eta) > = < f^*(\eta), e >$$
$$< \phi_V(f(e)), \eta > = < \eta, f(e) > = < f^*(\eta), e >$$

para todo $e \in E$, $\eta \in V^*$.

5. Por el contrario, cada espacio vectorial de dimensión finita E es isomorfo a su dual, pues ambos tienen la misma dimensión; pero ningún isomorfismo $E \simeq E^*$ puede ser funtorial, lo que explica el hecho de que el dual E^* no pueda sustituirse en Álgebra Lineal por E. En efecto, si existe algún isomorfismo funtorial $\beta\colon E \to E^*$ en la categoría de k-espacios vectoriales de dimensión finita e isomorfismos, para todo automorfismo lineal $\tau\colon E \to E$ el siguiente cuadrado ha de ser conmutativo:

$$\begin{array}{ccc} E & \xrightarrow{\beta} & E^* \\ \downarrow \tau & & \downarrow (\tau^*)^{-1} \\ E & \xrightarrow{\beta} & E^* \end{array}$$

Consideremos una base de E y su base dual en E^*, y sea B la matriz de β en tales bases. La conmutatividad del diagrama anterior expresa que

$$BT = (T^t)^{-1}B$$

para toda matriz invertible T. Tomando determinantes, al ser $|B| \neq 0$, concluimos que $|T| = |T|^{-1}$, lo que es imposible que se verifique para toda matriz invertible T, al menos cuando k tiene más de 3 elementos (es un buen ejercicio analizar los casos $k = \mathbb{F}_2$ y $k = \mathbb{F}_3$, pues todo espacio vectorial E de dimensión 1 sobre $\mathbb{F}_2$ sí es canónicamente isomorfo a su dual: basta identificar el único vector no nulo de E con el único vector no nulo de E^*).

Definición: Diremos que dos funtores covariantes $F\colon \mathbf{C} \rightsquigarrow \mathbf{C'}$ y $G\colon \mathbf{C'} \rightsquigarrow \mathbf{C}$ definen una **equivalencia** de categorías si el funtor $F \circ G$ es isomorfo a la identidad $\mathrm{id}_{\mathbf{C'}}$ y el funtor $G \circ F$ es isomorfo a la identidad $\mathrm{id}_{\mathbf{C}}$.

Si $F : \mathbf{C} \rightsquigarrow \mathbf{C'}$ y $G\colon \mathbf{C'} \rightsquigarrow \mathbf{C}$ definen una equivalencia de categorías, entonces todo objeto M' de $\mathbf{C'}$ es isomorfo a $F(M)$ para algún objeto M de $\mathbf{C}$, pues basta tomar $M = G(M')$. Además, al tener un isomorfismo natural $GF \simeq \mathrm{id}_{\mathbf{C}}$, se sigue que para cada par de objetos M, N de $\mathbf{C}$ la composición

$$\mathrm{Hom}_{\mathbf{C}}(M,N) \xrightarrow{F} \mathrm{Hom}_{\mathbf{C'}}(FM,FN) \xrightarrow{G} \mathrm{Hom}_{\mathbf{C}}(GF(M),GF(N))$$

es biyectiva. Por tanto, las aplicaciones $\mathrm{Hom}_{\mathbf{C}}(M,N) \to \mathrm{Hom}_{\mathbf{C}'}(F(M),F(N))$ inducidas por F, y las aplicaciones $\mathrm{Hom}_{\mathbf{C}'}(M',N') \to \mathrm{Hom}_{\mathbf{C}}(G(M'),G(N'))$ inducidas por G, son biyecciones.

Así como las categorías son las diferentes estructuras: grupos, anillos, espacios topológicos, etc., el concepto de equivalencia de categorías intenta precisar con rigor nuestra noción intuitiva de definiciones equivalentes de una misma estructura:

1. Cuando decimos que los $\mathbb{Z}$-módulos son los grupos abelianos, expresamos sin precisión el hecho riguroso de que el funtor de olvido $\mathbb{Z}$**-mod** $\rightsquigarrow$ **Ab** es una equivalencia de categorías. El funtor inverso asigna a cada grupo abeliano G la única estructura de $\mathbb{Z}$-módulo compatible con su operación de grupo:

$$ng = g + \overset{n}{\ldots} + g \quad , \quad (-n)g = (-g) + \overset{n}{\ldots} + (-g)$$

2. Cuando decimos que dar un endomorfismo de un espacio vectorial sobre un cuerpo k es lo mismo que dar un $k[x]$-módulo, expresamos la existencia de una equivalencia de categorías **k[x]-mod** $\rightsquigarrow$ $\mathbf{C}$, siendo $\mathbf{C}$ la categoría de parejas (E,T), donde E es un k-espacio vectorial y $T\colon E \to E$ es un endomorfismo, donde los morfismos $f\colon (E,T) \to (E',T')$ son las aplicaciones lineales $f\colon E \to E'$ tales que $f \circ T = T' \circ f$.

3. El paso al dual $E \rightsquigarrow E^*$ define una equivalencia de la categoría de k-espacios vectoriales de dimensión finita con su categoría dual, siendo él mismo su propio funtor inverso.

4. Como veremos en la página 370, el teorema de Galois (1811-1832) puede entenderse como una equivalencia de categorías.

El Funtor de Puntos

Sea X un espacio topológico. Si p denota el espacio topológico con un único punto, los puntos de X pueden verse como aplicaciones continuas $p \to X$, mientras que una aplicación continua arbitraria $T \to X$ puede entenderse como un punto de X que depende de un parámetro que recorre el espacio de parámetros T. Esta comprensión de los puntos como morfismos también es adecuada en el caso de la categoría de las variedades algebraicas afines sobre un cuerpo k (que es la categoría opuesta de la categoría de k-álgebras de tipo finito y morfismos de k-álgebras). En efecto, si $X = \operatorname{Spec} k[x_1,\ldots,x_n]/(p_1,\ldots,p_r)$ es la subvariedad algebraica del espacio afín $\mathbb{A}_n$ de ecuaciones $p_1 = \ldots = p_r = 0$, entonces los puntos racionales de X se corresponden con los morfismos $\operatorname{Spec} k \to X$, y para toda extensión L de k

tenemos que los morfismos $\operatorname{Spec} L \to X$ se corresponden con las soluciones en L del sistema de ecuaciones

$$\left.\begin{array}{r} p_1(x_1,\ldots,x_n)=0 \\ \ldots\ldots\ldots\ldots \\ p_r(x_1,\ldots,x_n)=0 \end{array}\right\}$$

por lo que bien merecen el nombre de puntos de X con coordenadas en L. Además, los morfismos $\operatorname{Spec} k[\,t\,] \to X$ se corresponden con los polinomios $x_1(t),\ldots,x_n(t)$ tales que $p_i(x_1(t),\ldots,x_n(t))=0$, por lo que bien merecen el nombre de puntos de X parametrizados por la recta afín $\mathbb{A}_1 = \operatorname{Spec} k[\,t\,]$.

Ahora bien, cuando los puntos se entienden como morfismos, el concepto de punto tiene pleno sentido en cualquier categoría, lo que es tanto como decir en cualquier rama de las matemáticas:

Definición: Fijada una categoría $\mathbf{C}$, diremos que los morfismos $T \to X$ son los **puntos de** X **parametrizados** por T, o bien que son los T-puntos de X. El conjunto de puntos de X parametrizados por T se denotará

$$X^\bullet(T) := \operatorname{Hom}_{\mathbf{C}}(T,X)\ .$$

Cada morfismo $t\colon S \to T$ define una aplicación natural

$$X^\bullet(T) = \operatorname{Hom}_{\mathbf{C}}(T,X) \ \longrightarrow\ \operatorname{Hom}_{\mathbf{C}}(S,X) = X^\bullet(S) \quad , \quad x \ \mapsto\ x|_t := x\circ t$$

de modo que $X^\bullet\colon \mathbf{C} \rightsquigarrow \mathbf{Sets}$ es un funtor contravariante, llamado **funtor de puntos** del objeto X. Diremos que $x|_t$ es la **especialización** del T-punto x al punto t del espacio de parámetros T.

Definición: Dado un objeto X de una categoría $\mathbf{C}$, diremos que la identidad $X \to X$ es el **punto general** de X, porque cualquier otro punto $x\colon T \to X$ es especialización del punto general x_g, pues $x_g|_x = \mathrm{id}_X \circ x = x$.

Por otra parte, cada morfismo $f\colon X \to Y$ induce aplicaciones naturales

$$f\colon X^\bullet(T) \ \longrightarrow\ Y^\bullet(T) \quad , \quad f(x) := f\circ x$$

y diremos que $f(x)$ es la imagen del punto x por el morfismo f. Obtenemos así un morfismo de funtores $f\colon X^\bullet \to Y^\bullet$, porque estas aplicaciones conservan la especialización de puntos: $f(x|_t) = f(x)|_t$ para todo punto t del espacio de parámetros T. En efecto, tenemos que

$$f(x|_t) = f\circ(x\circ t) = (f\circ x)\circ t) = f(x)|_t$$

Teorema: *Cada morfismo de funtores $\phi\colon X^\bullet \to Y^\bullet$ está definido por un único morfismo $X \to Y$:*

$$\operatorname{Hom}_{\mathbf{C}}(X,Y) \ =\ \operatorname{Hom}_{funt}(X^\bullet, Y^\bullet)$$

Demostración: Los morfismos de funtores $\phi\colon X^\bullet \to Y^\bullet$ son compatibles con especializaciones, así que si dos morfismos coinciden en el punto general de X, entonces coinciden en todo punto de X. Sea $f := \phi(x_g) \in Y^\bullet(X) = \mathrm{Hom}_{\mathbf{C}}(X, Y)$. El morfismo de funtores $f\colon X^\bullet \to Y^\bullet$ inducido por f es ϕ porque ambos coinciden en el punto general:

$$f(x_g) = f \circ \mathrm{id}_X = f = \phi(x_g)$$

y es el único morfismo $X \to Y$ que puede definir el morfismo de funtores dado ϕ.

Corolario: *Cada objeto X de una categoría $\boldsymbol{C}$ está totalmente determinado por su funtor de puntos $X^\bullet\colon \boldsymbol{C} \rightsquigarrow$ **Sets**.*

1. En la categoría de espacios topológicos, los T-puntos de un producto directo $\prod_i X_i$ son las sucesiones (x_i) donde cada término x_i es un T-punto de X_i:

   $$(\textstyle\prod_i X_i)^\bullet(T) \;=\; \prod_i X_i^\bullet(T)$$

   y el corolario anterior afirma que esta propiedad determina totalmente la topología del espacio $\prod_i X_i$.

2. Sean $X = \mathrm{Spec}\, A$, $Y = \mathrm{Spec}\, B$ dos variedades algebraicas afines sobre un cuerpo k. La propiedad universal del producto tensorial de álgebras $A \otimes_k B$ afirma que los puntos de $X \times_k Y := \mathrm{Spec}\,(A \otimes_k B)$ son las parejas (x, y) donde x es un punto de X e y es un punto de Y:

   $$(X \times_k Y)^\bullet \;=\; X^\bullet \times Y^\bullet$$

3. Según la propiedad universal del anillo de polinomios $k[x]$, en la categoría de variedades algebraicas afines sobre un cuerpo k, el funtor de puntos de la recta afín $\mathbb{A}_1 = \mathrm{Spec}\, k[x]$ es

   $$\mathbb{A}_1^\bullet(T) \;=\; \mathcal{O}(T)$$

   de modo que las funciones algebraicas $f \in \mathcal{O}(T)$ son morfismos $f\colon T \to \mathbb{A}_1$, y según la propiedad universal del anillo $A[x_1, \ldots, x_n]$, el funtor de puntos del espacio afín $\mathbb{A}_n$ es

   $$\mathbb{A}_n^\bullet(T) \;=\; \mathcal{O}(T)^n$$

4. Sea $i\colon Y = (I)_0 \to X$ una subvariedad cerrada de una variedad algebraica afín $X = \mathrm{Spec}\, A$ sobre un cuerpo k. Las aplicaciones naturales $i\colon Y^\bullet(T) \to X^\bullet(T)$ son inyectivas, así que los puntos de Y pueden verse como un subconjunto de los puntos de X. Ahora, si $Y_1 = (I_1)_0$, $Y_2 = (I_2)_0$ son dos subvariedades cerradas de X, los T-puntos de $Y_1 \cap Y_2 := (I_1 + I_2)_0$ son los T-puntos de Y_1 que también son puntos de Y_2:

   $$(Y_1 \cap Y_2)^\bullet \;=\; Y_1^\bullet \cap Y_2^\bullet$$

5. Sea G una variedad algebraica afín sobre un cuerpo k. Como $(G \times_k G)^\bullet = G^\bullet \times G^\bullet$, dar una estructura de grupo en el conjunto de puntos $G^\bullet(T)$, de modo que $G^\bullet$ sea un funtor valorado en la categoría de grupos, equivale a dar una estructura de **grupo algebraico** en G; es decir, equivale a dar morfismos $m\colon G \times_k G \to G$, $1\colon \operatorname{Spec} k \to G$, $\mathrm{inv}\colon G \to G$ que verifiquen los axiomas de grupo, en el sentido de que los siguientes diagramas sean conmutativos:

$$\begin{array}{ccc} G \times_k G \times_k G & \xrightarrow{m\times \mathrm{id}} & G \times_k G \\ \downarrow \mathrm{id} \times m & & \downarrow m \\ G \times_k G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{\mathrm{inv}\times \mathrm{id}} & G \times_k G \\ \downarrow & & \downarrow m \\ \operatorname{Spec} k & \xrightarrow{1} & G \end{array}$$

y los siguientes morfismos sean la identidad:

$$G = (\operatorname{Spec} k) \times_k G \xrightarrow{1\times \mathrm{id}} G \times_k G \xrightarrow{m} G$$
$$G = G \times_k (\operatorname{Spec} k) \xrightarrow{\mathrm{id}\times 1} G \times_k G \xrightarrow{m} G$$

6. El funtor de puntos de $\mathbb{G}_a := \operatorname{Spec} k[x]$, que es $\mathbb{G}_a(\operatorname{Spec} A) = A$, admite claramente una estructura natural de grupo aditivo, lo que define una estructura de grupo algebraico en $\mathbb{G}_a$. Es el llamado grupo aditivo (sobre el cuerpo k).

7. El funtor de puntos de $\mathbb{G}_m := \operatorname{Spec} k[x, x^{-1}]$, que es $\mathbb{G}_m(\operatorname{Spec} A) = A^*$, admite claramente una estructura natural de grupo multiplicativo, lo que define una estructura de grupo algebraico en $\mathbb{G}_m$. Es el llamado grupo multiplicativo (sobre el cuerpo k).

8. El núcleo del morfismo de grupos $\mathbb{G}_m(T) \to \mathbb{G}_m(T)$, $a \mapsto a^n$, está formado por los T-puntos de $\mu_n := \operatorname{Spec} k[x]/(x^n - 1)$, así que éstos heredan una estructura natural de grupo, lo que define una estructura de grupo algebraico sobre μ_n. Es el llamado grupo multiplicativo de las raíces n-ésimas de la unidad (sobre el cuerpo k).

9. Sea k un cuerpo de característica positiva p y sea $q = p^n$. El núcleo del morfismo de grupos $\mathbb{G}_a(T) \to \mathbb{G}_a(T)$, $a \mapsto a^q - a$, está formado por los T-puntos de $\alpha_n := \operatorname{Spec} k[x]/(x^q - x)$, así que éstos heredan una estructura natural de grupo, lo que define una estructura de grupo algebraico sobre α_n.

Por otra parte, cada objeto X de una categoría $\mathbf{C}$ también define un funtor covariante $\mathrm{Hom}_{\mathbf{C}}(X, -)\colon \mathbf{C} \rightsquigarrow \mathbf{Sets}$:

$$T \rightsquigarrow \mathrm{Hom}_{\mathbf{C}}(X, T)$$
$$T \xrightarrow{f} S \rightsquigarrow \mathrm{Hom}_{\mathbf{C}}(X, T) \xrightarrow{f\circ} \mathrm{Hom}_{\mathbf{C}}(X, S)$$

que es precisamente el funtor de puntos de X en la categoría dual $\mathbf{C^{op}}$.

El teorema anterior permite calcular los morfismos entre dos funtores $\mathbf{C} \rightsquigarrow \mathbf{Sets}$ cuando sean isomorfos a funtores de la forma $\mathrm{Hom}_{\mathbf{C}}(X, -)$ ó $\mathrm{Hom}_{\mathbf{C}}(-, X) = X^{\bullet}$:

1. Sea k un anillo. Para determinar las operaciones funtoriales $A\times \overset{n}{\ldots} \times A \to A$ que pueden definirse en las k-álgebras, basta recordar que el funtor $A \rightsquigarrow A\times \overset{n}{\ldots} \times A$ es el funtor covariante asociado a la k-álgebra $k[x_1, \ldots, x_n]$. Luego, de acuerdo con el teorema anterior, las operaciones funtoriales en cuestión se corresponden canónicamente con los morfismos de k-álgebras

$$k[x] \longrightarrow k[x_1, \ldots, x_n]$$

que claramente están determinados por la imagen de x. Luego toda operación funtorial $A\times \overset{n}{\ldots} \times A \to A$ definida en las k-álgebras es de la forma

$$(a_1, \ldots, a_n) \longmapsto p(a_1, \ldots, a_n)$$

para algún polinomio $p(x_1, \ldots, x_n)$ con coeficientes en k. En particular, los morfismos de anillos funtoriales $A \to A$ se corresponden con los polinomios $p(x) \in k[x]$ tales que

$$p(x + y) = p(x) + p(y)\ , \quad p(xy) = p(x)p(y)\ , \quad p(1) = 1$$

Si la característica de k es nula, la primera condición implica que $p(x) = \lambda x$ para algún $\lambda \in k$, así que la última condición permite concluir que $p(x) = x$; es decir, no hay más morfismo de anillos funtorial $A \to A$ que la identidad. No obstante, cuando la característica de k es positiva, pueden existir otros morfismos de anillos funtoriales. Por ejemplo, si la característica de k es un número primo p, los polinomios x^{p^r} satisfacen las condiciones requeridas, de modo que en las k-álgebras tenemos los morfismos de anillos funtoriales $A \to A$, $a \mapsto a^{p^r}$.

2. Para determinar las operaciones funtoriales $X\times \overset{n}{\ldots} \times X \to X$ que pueden definirse en los espacios topológicos, observamos primero que $X\times \overset{n}{\ldots} \times X = \mathrm{Hom}_{\mathbf{Top}}(\{1, \ldots, n\}, X)$, donde $\{1, \ldots, n\}$ es un espacio topológico discreto con n puntos. De acuerdo con el teorema anterior, las operaciones funtoriales en cuestión se corresponden canónicamente con las aplicaciones continuas $\{1\} \to \{1, \ldots, n\}$: En los espacios topológicos no hay más operaciones funtoriales que las proyecciones canónicas $X\times \overset{n}{\ldots} \times X \to X$, $(x_1, \ldots, x_n) \mapsto x_i$.

3. Sea A un anillo. Vamos a determinar todas las operaciones funtoriales $M\times \overset{n}{\ldots} \times M \to M$ que pueden definirse en los A-módulos. Observamos primero que $M^n = \mathrm{Hom}_A(A^n, M)$. Según el teorema anterior, tales operaciones funtoriales se corresponden canónicamente con los morfismos de A-módulos $A \to A^n$. Todas son de la forma $(m_1, \ldots, m_n) \longmapsto \sum_i a_i m_i$ para ciertos elementos $a_1, \ldots, a_n \in A$.

Funtores Representables

Veamos que la igualdad $\mathrm{Hom}_{\mathbf{C}}(X,Y) = \mathrm{Hom}_{funt}(X^\bullet, Y^\bullet)$ es válida cuando $Y^\bullet$ se sustituye por un funtor contravariante F arbitrario:

Teorema: *Sea $F\colon \boldsymbol{C} \rightsquigarrow \boldsymbol{Sets}$ un funtor contravariante y sea X un objeto de $\boldsymbol{C}$. Para cada elemento $\xi \in F(X)$ existe un único morfismo de funtores $\phi\colon X^\bullet \to F$ tal que $\phi(x_g) = \xi$:*

$$\mathrm{Hom}_{funt}(X^\bullet, F) \;=\; F(X)$$

Demostración: La unicidad se debe a que si dos morfismos $X^\bullet \to F$ coinciden en un punto x, entonces coinciden en sus especializaciones $x|_t$, de modo que cada morfismo $\phi\colon X^\bullet \to F$ está determinado por la imagen $\phi(x_g)$ del punto general de X. En cuanto a la existencia, cada elemento $\xi \in F(X)$ induce aplicaciones

$$\xi\colon \mathrm{Hom}_{\mathbf{C}}(T,X) \to F(T) \quad , \quad \xi(f) := F(f)(\xi)$$

que definen un morfismo natural $\xi\colon X^\bullet \to F$ tal que $\xi(x_g) = F(\mathrm{id}_X)(\xi) = \xi$.

Corolario: *Sea $F\colon \boldsymbol{C} \rightsquigarrow \boldsymbol{Sets}$ un funtor covariante y sea X un objeto de $\boldsymbol{C}$. Si $\xi \in F(X)$, entonces existe un único morfismo de funtores $\phi\colon \mathrm{Hom}_{\boldsymbol{C}}(X,-) \to F$ tal que $\phi(\mathrm{id}_X) = \xi$.*

Definición: Diremos que un funtor contravariante $F\colon \mathbf{C} \rightsquigarrow \mathbf{Sets}$ es **representable** si existe algún objeto X de $\mathbf{C}$ tal que F y $\mathrm{Hom}_{\mathbf{C}}(-,X) = X^\bullet$ sean funtores isomorfos. En tal caso, de acuerdo con el teorema anterior, dicho isomorfismo de funtores debe estar definido por algún elemento $\xi \in F(X)$. Diremos que una pareja (X,ξ), donde $\xi \in F(X)$, **representa** al funtor contravariante F si el correspondiente morfismo de funtores $\xi\colon \mathrm{Hom}_{\mathbf{C}}(-,X) \to F$ es un isomorfismo.

Análogamente, diremos que un funtor covariante $F\colon \mathbf{C} \rightsquigarrow \mathbf{Sets}$ es **representable** si existe algún objeto X de $\mathbf{C}$ tal que F y $\mathrm{Hom}_{\mathbf{C}}(X,-)$ sean funtores isomorfos. En tal caso, de acuerdo con el corolario anterior, dicho isomorfismo de funtores debe estar definido por algún elemento $\xi \in F(X)$. Diremos que una pareja (X,ξ), donde $\xi \in F(X)$, **representa** al funtor covariante F si el correspondiente morfismo de funtores $\xi\colon \mathrm{Hom}_{\mathbf{C}}(X,-) \to F$ es un isomorfismo.

Por definición, decir que un funtor covariante F está representado por una pareja (X,ξ) significa que para cualquier objeto X' de $\mathbf{C}$ y cualquier elemento $\xi' \in F(X')$ existe un único morfismo $f\colon X \to X'$ tal que

$$\xi' = F(f)(\xi)$$

y decir que un funtor contravariante F está representado por una pareja (X,ξ) significa que para cualquier objeto X' de $\mathbf{C}$ y cualquier elemento $\xi' \in F(X')$ existe un único morfismo $f\colon X' \to X$ tal que $\xi' = F(f)(\xi)$.

Teorema: *Si un funtor covariante o contravariante* $F\colon \boldsymbol{C} \rightsquigarrow \textbf{\textit{Sets}}$ *es representable, su representante es único salvo isomorfismos canónicos. Con precisión, si* F *está representado por dos parejas* (X,ξ) *y* (X',ξ')*, entonces existe un único isomorfismo* $f\colon X \to X'$ *tal que* $\xi' = F(f)(\xi)$.

Demostración: Como F está representado por (X,ξ), existe un único morfismo $f\colon X \to X'$ en $\mathbf{C}$ tal que

$$\xi' = F(f)(\xi)$$

y como F está representado por (X',ξ'), existe en $\mathbf{C}$ un único morfismo $g\colon X' \to X$ tal que

$$\xi = F(g)(\xi')$$

Se sigue que $F(f\circ g)(\xi') = \xi'$ y $F(g\circ f)(\xi) = \xi$; luego $f\circ g = \mathrm{id}_{X'}$ y $g\circ f = \mathrm{id}_X$. Concluimos que f es un isomorfismo. q.e.d.

Enunciar la propiedad universal de un objeto X de una categoría $\mathbf{C}$ es afirmar que el funtor $\mathrm{Hom}_{\mathbf{C}}(X,-)$ es isomorfo a cierto funtor covariante $F\colon \mathbf{C} \rightsquigarrow \mathbf{Sets}$ (o que el funtor $\mathrm{Hom}_{\mathbf{C}}(-,X)$ es isomorfo a cierto funtor contravariante $F\colon \mathbf{C} \rightsquigarrow \mathbf{Sets}$); i.e., es afirmar que cierto funtor F es representable y está representado por X. Pero las propiedades universales no sólo afirman la existencia de un isomorfismo funtorial $\mathrm{Hom}_{\mathbf{C}}(X,-) \to F$, sino que determinan un isomorfismo concreto que, según el teorema anterior, vendrá definido por cierto elemento $\xi \in F(X)$. Cada propiedad universal es la afirmación de que cierto funtor F está representado por determinada pareja (X,ξ). Veamos, en las propiedades universales que conocemos, cuál es tal elemento $\xi \in F(X)$, que es el que se corresponde con la identidad de X en la biyección $\mathrm{Hom}_{\mathbf{C}}(X,X) = F(X)$ proporcionada por la propiedad universal en cuestión:

1. La propiedad universal del grupo cociente G/H afirma que, en la categoría de grupos, el funtor

   $$F(G') = \{f \in \mathrm{Hom}_{\mathbf{Gr}}(G,G')\colon\ f(H) = 1\}$$

   está representado por la pareja $(G/H,\pi)$, donde $\pi \in F(G/H)$ es la proyección canónica $\pi\colon G \to G/H$.

2. La propiedad universal del anillo de polinomios $A[x_1,\ldots,x_n]$ afirma que, en la categoría de A-álgebras, el funtor $F(B) = B^n$ está representado por la pareja $(\,A[x_1,\ldots,x_n]\,,\,(x_1,\ldots,x_n)\,)$.

3. La propiedad universal del anillo de fracciones $S^{-1}A$ afirma que, en la categoría de anillos, el funtor

   $$F(B) = \{f \in \mathrm{Hom}_{\mathbf{Rings}}(A,B)\colon\ f(S) \subseteq B^*\}$$

   está representado por $(S^{-1}A,\gamma)$, donde $\gamma\colon A \to S^{-1}A$ es el morfismo de localización: $\gamma(a) = a/1$.

4. Sea $(X_i)_{i\in I}$ una familia de espacios topológicos. En la categoría de espacios topológicos, el funtor

$$F(T) = \textstyle\prod_i \mathrm{Hom}_{\mathbf{Top}}(T, X_i)$$

está representado por la pareja $\big(\prod_i X_i\,,\,(\pi_j)_{j\in I}\big)$, donde las aplicaciones $\pi_j\colon \prod_i X_i \to X_j$ son las proyecciones canónicas: $\pi_j\big((x_i)_{i\in I}\big) = x_j\,.$

5. La propiedad universal de la suma directa $\bigoplus_i M_i$ afirma que, en la categoría de A-módulos, el funtor

$$F(N) = \textstyle\prod_i \mathrm{Hom}_A(M_i, N)$$

está representado por $\big(\bigoplus_i M_i\,,\,(u_j)\big)$, donde los morfismos $u_j\colon M_j \to \bigoplus_i M_i$ son las inclusiones canónicas.

La propiedad universal del producto directo $\prod_i M_i$ afirma que, en la categoría de A-módulos, el funtor

$$F(N) = \textstyle\prod_i \mathrm{Hom}_A(N, M_i)$$

está representado por $\big(\prod_i M_i\,,\,(\pi_j)\big)$, donde los morfismos $\pi_j\colon \prod_i M_i \to M_j$ son las proyecciones canónicas.

6. La propiedad universal del producto tensorial de módulos $M \otimes_A N$ afirma que, en la categoría de A-módulos, el funtor $F(P) = \mathrm{Bil}(M, N; P)$ está representado por $(M\otimes_A N, \otimes)$, donde $\otimes\colon M\times N \to M\otimes_A N$ es la aplicación bilineal canónica.

7. La propiedad universal del cambio de base M_B afirma que, en la categoría de B-módulos, el funtor $F(N) = \mathrm{Hom}_A(M, N)$ está representado por la pareja (M_B, j) donde $j\colon M \to M_B$ es el morfismo de cambio de base: $j(m) = m\otimes 1\,.$

8. La propiedad universal del producto tensorial de álgebras $A\otimes_k B$ afirma que, en la categoría de k-álgebras, el funtor

$$F(C) = \mathrm{Hom}_{k\text{-}alg}(A, C) \times \mathrm{Hom}_{k\text{-}alg}(B, C)$$

está representado por la pareja $\big(A\otimes_k B\,,\,(j_1, j_2)\big)$, donde $j_1\colon A \to A\otimes_k B$ y $j_2\colon B \to A\otimes_k B$ son los morfismos canónicos: $j_1(a) = a\otimes 1$, $j_2(b) = 1\otimes b\,.$

9. La propiedad universal del cambio de base A_K afirma que, en la categoría de K-álgebras, el funtor $F(B) = \mathrm{Hom}_{k\text{-}alg}(A, B)$ está representado por la pareja $(A_K,\, j)$, donde $j\colon A \to A_K$ es el morfismo de cambio de base: $j(a) = a\otimes 1\,.$

10. La propiedad universal de la localización de módulos afirma que, en la categoría de $S^{-1}A$-módulos, el funtor $F(N) = \mathrm{Hom}_A(M, N)$ está representado por la pareja $(S^{-1}M, \gamma)$, donde $\gamma\colon M \to S^{-1}M$ es el morfismo de localización: $\gamma(m) = m/1\,.$

11. Sea X un conjunto. En la categoría de A-módulos, el funtor $F(M) = M^X$ está representado por $\big(A^{(X)}, \iota\big)$, donde $\iota\colon X \to A^{(X)}$ es la identificación canónica de X con una base del A-módulo libre $A^{(X)}$.

12. Sea E un espacio normado. En la categoría de espacios normados completos, el funtor $F(V) = \{\text{Aplicaciones lineales } E \to V \text{ continuas}\}$ está representado por la pareja $(\widehat{E}, j)$, donde $j\colon E \to \widehat{E}$ es la aplicación canónica de E en su completación.

13. Sea $A \to B$ un morfismo de anillos. La propiedad universal del módulo de diferenciales $\Omega_{B/A}$ afirma que, en la categoría de B-módulos, el funtor covariante $F(M) = \mathrm{Der}_A(B, M)$ está representado por la pareja $(\Omega_{B/A}, \mathrm{d})$.

Vemos así que las propiedades universales nos dicen cuáles son los funtores de puntos de las diversas construcciones que realizamos. En cualquier rama de las matemáticas es crucial determinar los puntos de las estructuras involucradas, entendiendo los morfismos $T \to X$ como familias de puntos de X parametrizadas por T. Esta comprensión del concepto de punto es una de las más decisivas aportaciones de Grothendieck (n. 1928), ya que tiene significado en las categorías arbitrarias y permite iniciar un enfoque geométrico de cualquier categoría, culminando el sueño de Kronecker (1823-1891) – la unificación de la geometría y la aritmética – con una comprensión geométrica de todas las matemáticas.

¡Cuánto cambiaría nuestra vida si se viera
que la geometría griega y la fe cristiana
han brotado de la misma fuente!

Simone Weil (1909-1943)

Parte II

Ejemplos y Ejercicios

Ejemplos y Ejercicios

Relaciones de Equivalencia

(*) Estudiemos la divisibilidad por 9 del número $m = 1994^{1996} + 1994$.

1994 es congruente con 5 módulo 9, porque $1994 = 221 \cdot 9 + 5$, así que

$$m \equiv 5^{1996} + 5 \text{ (mód. 9)}$$

Para calcular 5^{1996} módulo 9 efectuamos potencias sucesivas de 5:

$$\begin{aligned} 5^2 &= 25 \equiv -2 && \text{(mód. 9)} \\ 5^3 &\equiv -2 \cdot 5 \equiv -1 && \text{(mód. 9)} \\ 5^6 &\equiv (-1)^2 = 1 && \text{(mód.9)} \end{aligned}$$

Por tanto, al ser $1996 \equiv 4$ (módulo 6), se sigue que

$$5^{1996} = 5^6 \cdots 5^6 \cdot 5^4 \equiv 5^4 \equiv -5 \quad \text{(mód.9)}$$

y concluimos que $m \equiv -5 + 5 = 0$ (mód. 9). Luego m es múltiplo de 9.

(*) La finitud de las clases de restos módulo un número natural no nulo n permite probar la imposibilidad de resolver muchas ecuaciones diofánticas. Por ejemplo, si la ecuación $2x^2 - 5y^2 = 11$ tuviera alguna solución entera, entonces

$$2x^2 \equiv 1 \text{ (mód. 5)}$$

Considerando, módulo 5, todos los casos posibles $x \equiv 0, 1, 2, 3, 4$ comprobamos que $x^2 \equiv 0, 1, 4$ y que $2x^2 \equiv 0, 2, 3$. Se sigue que la congruencia $2x^2 \equiv 1$ (mód. 5) carece de soluciones enteras y, por tanto, también la ecuación $2x^2 - 5y^2 = 11$.

(*) Sea $p(x) = x^n + c_1 x^{n-1} + \ldots + c_n$ un polinomio con coeficientes complejos. Para aumentar las raíces en una constante $a \in \mathbb{C}$, formamos el polinomio $p(x-a)$.

Para multiplicar las raíces por un factor no nulo $a \in \mathbb{C}$, formamos el polinomio

$$x^n + c_1 a x^{n-1} + c_2 a^2 x^{n-2} \ldots + c_n a^n = a^n p\left(\frac{x}{a}\right)$$

Para cambiar de signo las raíces, formamos el polinomio

$$(-1)^n x^n + \ldots - c_{n-1} x + c_n = p(-x)$$

Para invertir las raíces, formamos el polinomio

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + 1 = x^n p\left(\frac{1}{x}\right)$$

(*) Raíces Cúbicas de la Unidad:

Como $x^3-1=(x-1)(x^2+x+1)$, las raíces cúbicas complejas de la unidad distintas de 1 son las raíces complejas del polinomio x^2+x+1, que son $\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$.

La parte imaginaria de $e^{\frac{2\pi i}{3}}$ es positiva y la de $e^{\frac{4\pi i}{3}}$ es negativa, así que las raíces cúbicas complejas de la unidad son

$$1 \quad , \quad e^{\frac{2\pi i}{3}}=\frac{1}{2}+\frac{\sqrt{3}}{2}i \quad , \quad e^{\frac{4\pi i}{3}}=\frac{1}{2}-\frac{\sqrt{3}}{2}i$$

La parte real de dos raíces es $1/2$, así que el lado del triángulo equilátero inscrito en un círculo es la cuerda perpendicular al radio en su punto medio.

Raíces Cuartas de la Unidad:

Como $x^4-1=(x^2-1)(x^2+1)=(x-1)(x+1)(x^2-1)$, las raíces cuartas complejas de la unidad son:

$$1 \quad , \quad e^{\frac{\pi i}{2}}=i \quad , \quad e^{\pi i}=-1 \quad , \quad e^{\frac{3\pi i}{2}}=-i\ .$$

Raíces Quintas de la Unidad:

Sea $x=e^{\frac{2\pi i}{5}}=\cos\frac{2\pi}{5}+i\text{sen}\,\frac{2\pi}{5}$. Vamos a calcular $y:=x+x^{-1}=x+\bar{x}=2\cos\frac{2\pi}{5}$. Como $x^5=1$ y $x\neq 1$, tenemos que

$$\begin{aligned}0&=x^5-1=(x-1)(x^4+x^3+x^2+x+1)\\0&=x^4+x^3+x^2+x+1\\0&=(y^2-2)+y+1=y^2+y-1\end{aligned}$$

porque $y=x+x^{-1}$, $y^2=x^2+x^{-2}+2$. Se sigue que $y=\frac{-1\pm\sqrt{5}}{2}$. Ahora bien, al ser y positivo, concluimos que $\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}$. Luego

$$\begin{aligned}e^{\frac{2\pi i}{5}}&=\frac{\sqrt{5}-1}{4}+i\sqrt{1-\left(\frac{\sqrt{5}-1}{4}\right)^2}\\e^{\frac{8\pi i}{5}}&=\frac{\sqrt{5}-1}{4}-i\sqrt{1-\left(\frac{\sqrt{5}-1}{4}\right)^2}\end{aligned}$$

Las otras dos raíces $e^{\frac{2\pi i}{5}2}$ y $e^{\frac{2\pi i}{5}3}$ pueden hallarse observando que el razonamiento anterior también prueba que $2\cos\frac{4\pi}{5}=-\frac{\sqrt{5}+1}{2}$, de modo que

$$\begin{aligned}e^{\frac{4\pi i}{5}}&=-\frac{\sqrt{5}+1}{4}+i\sqrt{1-\left(\frac{\sqrt{5}+1}{4}\right)^2}\\e^{\frac{6\pi i}{5}}&=\frac{\sqrt{5}+1}{4}-i\sqrt{1-\left(\frac{\sqrt{5}+1}{4}\right)^2}\end{aligned}$$

Raíces Sextas de la Unidad:

Como $x^6 - 1 = (x^3 - 1)(x^3 + 1)$, las raíces sextas complejas de la unidad son las tres raíces cúbicas junto con las raíces complejas del polinomio $x^3 + 1 = (x + 1)(x^2 - x + 1)$, que son $x = -1$ y $x = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Por tanto, las raíces sextas de la unidad son

$$1,\ e^{\frac{\pi i}{3}} = \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i,\ e^{\frac{2\pi i}{3}} = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i,\ e^{\pi i} = -1,\ e^{\frac{4\pi i}{3}} = -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i,\ e^{\frac{5\pi i}{3}} = \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i$$

y vemos que, dado un círculo, los extremos de un diámetro junto con los de las cuerdas perpendiculares a sus dos radios en los puntos medios, son los vértices de un hexágono regular inscrito en el círculo dado.

(*) Raíces Primitivas de la Unidad:

1. $e^{\frac{2\pi i}{n}}$ y $e^{\frac{2\pi i}{n}(n-1)} = e^{\frac{-2\pi i}{n}}$ son raíces n-ésimas de la unidad primitivas.
2. Las raíces quintas de la unidad primitivas son $e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}$ y $e^{\frac{8\pi i}{5}}$.
3. Las raíces sextas de la unidad primitivas son $e^{\frac{2\pi i}{6}}$ y $e^{\frac{-2\pi i}{6}} = e^{\frac{10\pi i}{6}}$.
4. $e^{\frac{2\pi i}{3}} e^{\frac{2\pi i}{5}} = e^{\frac{16\pi i}{15}}$ es una raíz decimoquinta de la unidad primitiva.

(*) Logaritmo Neperiano:

Si u, z son números complejos, pondremos $u = \ln z$ cuando $z = e^u$, y diremos que u es el **logaritmo neperiano** de z, en honor de J. Neper (1550-1617). Como $e^z = 1$ cuando z es múltiplo entero de $2\pi i$, el logaritmo neperiano está bien definido salvo la adición de un múltiplo entero de $2\pi i$.

La exponencial e^{a+bi} nunca es nula, pues su módulo es $e^a \neq 0$, así que el 0 no admite logaritmo neperiano. Si $z = \rho e^{i\theta}$ es un número complejo no nulo de módulo ρ y argumento θ, entonces

$$z = \rho e^{i\theta} = e^{\ln \rho} e^{i\theta} = e^{\ln \rho + i\theta}$$
$$\ln z = \ln \rho + (\theta + 2k\pi)i$$

Vemos así que todo número complejo no nulo z admite infinitos logaritmos neperianos. Ahora las potencias z^w, donde $w \in \mathbb{C}$, pueden definirse a través de la exponencial compleja:

$$z^w := (e^{\ln z})^w := e^{w \ln z}\ .$$

Ejercicios:

1. Sea $n = 1993^{1993} + 1994 \cdot 1995$. ¿Es n múltiplo de 13? ¿Qué resto da al dividir n por 7? ¿y al dividir n por 12?

   Hallar la última cifra decimal del número n^3.

2. Si $a \equiv c\ ,\ b \equiv d\ \pmod{n}$, ¿se sigue necesariamente que $a^b \equiv c^d \pmod{n}$?

3. Si $n = c_0 + c_1 10 + c_2 10^2 + \ldots + c_r 10^r$, $0 \leq c_i \leq 9$, es la expresión en notación decimal de un número natural n, probar que

$$n \equiv c_0 \ \text{ módulo 2, 5 y 10}$$
$$n \equiv c_0 + c_1 10 \ \text{ módulo 4}$$
$$n \equiv c_0 + c_1 10 + c_2 10^2 \ \text{ módulo 8}$$
$$n \equiv c_0 + c_1 + \ldots + c_r \ \text{ módulo 3 y 9}$$
$$n \equiv c_0 - c_1 + c_2 - \ldots + (-1)^r c_r \ \text{ módulo 11}$$
$$n \equiv c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + 2c_8 - \ldots \ \text{ módulo 7}$$

   Usar estas congruencias para dar criterios de divisibilidad por los números 2, 3, 4, ..., 11 y 12.

4. Probar que $10a + b$ es múltiplo de 13 si, y sólo si lo es $a + 4b$; y que $10a + b$ es múltiplo de 7 precisamente cuando lo sea $a - 2b$. Usar estos criterios de divisibilidad para ver si el número 27824342 es múltiplo de 7 y de 13.

5. Determinar los números naturales n tales que $2^n + 1$ sea múltiplo de 3.

   Determinar los números naturales n tales que $2^n - 1$ sea múltiplo de 7.

6. Dar ejemplos de relaciones que verifiquen dos de las propiedades reflexiva, simétrica y transitiva; pero no la tercera.

7. Averiguar si las siguientes relaciones son de equivalencia:

$$X = \mathbb{Z} \times \mathbb{Z}, \quad (x, y) \equiv (x', y') \Leftrightarrow x' - x \text{ e } y' - y \text{ son números impares}$$
$$X = \mathbb{N} \times \mathbb{N}, \quad (x, y) \equiv (x', y') \Leftrightarrow x' = cx,\ y' = cy \text{ para algún } c \in \mathbb{N}$$
$$X = \mathbb{Z} \times \mathbb{N}, \quad (x, y) \equiv (x', y') \Leftrightarrow x' = x$$
$$X = \mathbb{N} \times \mathbb{N}, \quad (x, y) \equiv (x', y') \Leftrightarrow x' + y' = x + y$$

8. ¿Cuántas relaciones de equivalencia diferentes hay en un conjunto con 2 elementos? ¿y con 3 elementos?

9. Probar que ningún número natural congruente con 2 ó 3 módulo 4 es un cuadrado perfecto.

10. Demostrar que la suma de los cuadrados de 4 números naturales consecutivos nunca es un cuadrado perfecto.

11. Hallar el resto de la división de $(116 + 117^{117})^{121}$ por 8, y de la división de 14^{256} por 17.

12. ¿Es siempre $n^3 + 11n$ múltiplo de 6? ¿Es siempre $3n^5 + 5n^3 + 7n$ múltiplo de 15?

13. Si un cuadrado perfecto es suma de dos cuadrados perfectos, $a^2 + b^2 = c^2$, demostrar que a ó b es múltiplo de 3.

14. Averiguar si alguno de los números 11, 111, 1111, ... es un cuadrado perfecto.

15. Demostrar que ningún número de la forma $3 + 4n,\ n \in \mathbb{N}$, es suma de dos cuadrados perfectos.

    Probar que ningún número de la forma $7 + 8n,\ n \in \mathbb{N}$, es suma de tres cuadrados perfectos.

16. Si $2, p_2, \ldots, p_n$ son los n primeros números primos, demostrar que su producto $2p_2 \cdot \ldots \cdot p_n + 1$ no es un cuadrado perfecto.

17. Demostrar que las siguientes ecuaciones no tienen soluciones enteras:

$$\begin{array}{ccc} x^2 - 13y^2 = 275 & x^2 + y^2 + z^2 = 8t + 7 & x^2 + y^2 - 4z = 3 \\ x^2 - y^2 + 4z = 2 & x^2 - 3y^n = 2 & x^2 - 17y = 855 \end{array}$$

    y averiguar si las siguientes ecuaciones tienen alguna solución entera:

$$\begin{array}{ccc} 3x^2 + 2 = y^2 & 7x^3 + y^3 = 5 & 3x^2 - 7y^2 = 2 \\ x^3 - 3y^2 = -11 & x^2 + 2y^2 + 3 = 8z & 11x^2 - 9y^2 = 6 \\ 2x^3 - 7y^3 = 3 & x^2 + y^2 + 1 = 4z & 3x^2 - 14y^2 = 4 \\ x^2 + y^2 + 3 = 4z & 4x^2 + 3 = 5y^2 & x^2 + 21xy + 14y^2 = 3 \end{array}$$

18. Demostrar que la condición necesaria y suficiente para que un número natural n sea suma de tres cuadrados perfectos es que lo sea $4n$.

19. Demostrar que si la ecuación $x^3 + y^3 = z^3$ tuviera alguna solución entera, entonces x, y ó z sería múltiplo de 7.

20. Hallar las raíces cuadradas de -4, -2, $3i$, $-4i$, $1+i$, $-2+3i$, $-2-i$ y $2-3i$. (*Indicación:* Resolver la correspondiente ecuación $(x + yi)^2 = a + bi$).

21. Hallar las raíces cuartas de 1, i, -1, $-i$, $1 + i$ y $-2 + i$. Expresarlas con radicales reales.

22. Hallar las raíces cúbicas de 1, i, -1 y $-i$. Expresarlas con radicales reales.

23. Si un número complejo z de módulo 1 no es real, probar que su argumento duplica al de $z + |z|$, y que

$$\sqrt{z} \;=\; \pm\frac{1+z}{|1+z|}$$

24. Si z es un número complejo no nulo, probar que el argumento de z^{-1} coincide con el de $\bar{z}$ y es el opuesto del argumento de z. Concluir que $z/\bar{z}$ tiene módulo 1 y su argumento es el doble del argumento de z.

25. Sean $x, y \in \mathbb{Q}$. Probar que $x^2 + y^2 = 1$ si y sólo si existen $a, b \in \mathbb{Q}$ tales que

$$x + yi = \frac{a + bi}{a - bi}$$

Hallar infinitas soluciones racionales de la ecuación $x^2 + y^2 = 1$. A partir de ellas, obtener infinitas soluciones enteras de la ecuación $x^2 + y^2 = z^2$.

26. ¿Cuántos ángulos hay cuyo seno y coseno sean números racionales?

27. Si $z \in \mathbb{C}$, demostrar que $z + \bar{z}$ es un número real acotado por $2|z|$. Concluir que $|z_1 + z_2| \leq |z_1| + |z_2|$.

28. Determinar la parte real e imaginaria de los siguientes números complejos:

$$i^i \quad , \quad \ln(-1) \quad , \quad 2^i \quad , \quad \ln i \ .$$

29. Probar que la suma de todas las raíces n-ésimas de la unidad complejas es 0 y su producto es $(-1)^{n+1}$.

30. Si u y v son raíces n-ésimas de la unidad complejas, probar que también lo son uv, u^{-1} y $\overline{u}$.

31. Calcular $\operatorname{sen}(\pi/n) + \operatorname{sen}(2\pi/n) + \operatorname{sen}(3\pi/n) + \ldots + \operatorname{sen}((n-1)\pi/n)$

Calcular $\cos(\pi/11) + \cos(3\pi/11) + \cos(5\pi/11) + \cos(7\pi/11) + \cos(9\pi/11)$.

32. Expresar con radicales cuadráticos las raíces n-ésimas de la unidad complejas cuando $n = 8$, 10 y 12.

33. ¿Es cierto que toda potencia de $e^{2\pi i/n}$ con exponente entero coincide con alguna potencia de exponente natural?

34. Si u es una raíz n-ésima de la unidad primitiva, probar que su inverso u^{-1} y su conjugado $\overline{u}$ también son raíces n-ésimas de la unidad primitivas.

35. Hallar las raíces n-ésimas de la unidad primitivas cuando $n = 9$, 10 y 12.

36. ¿Existe algún número complejo z de módulo 1 tal que $z^n \neq 1$ para todo exponente natural $n \geq 1$?

37. Determinar si las siguientes construcciones de polígonos regulares son exactas y, en caso negativo, acotar el error relativo que se comete.

(a) Dado un círculo, la cuerda perpendicular a un radio por su punto medio es el lado del triángulo equilátero inscrito en el círculo dado.

(b) Dado un círculo, se divide un diámetro AB en 5 partes iguales. Con centro en cada extremo de AB se traza el circulo que pasa por el otro extremo. Se traza la recta que une un punto de corte C con la segunda división del diámetro AB. Esta recta corta al círculo dado en un punto D tal que la longitud del segmento AD es el lado del pentágono regular inscrito en el círculo dado.

(c) El lado del hexágono regular inscrito en un círculo es la cuerda de longitud igual al radio.

(d) Dado un círculo, con centro en el punto medio de un radio se traza un círculo pasando por un extremo A del diámetro perpendicular, que corta al diámetro inicial en un punto B. La longitud del segmento AB es el lado del pentágono regular inscrito en el círculo dado. La longitud del segmento que une B con el centro del círculo dado es el lado del decágono regular inscrito.

(e) El lado del heptágono regular inscrito en un círculo dado es la mitad del lado del triángulo equilátero inscrito.

(f) Dado un círculo con centro O, se trazan dos diámetros perpendiculares AB y JK. El círculo con centro K que pasa por O corta al círculo dado en un punto L. Con centro en J se traza el círculo que pasa por L, que cortará a la prolongación del diámetro AB en un punto M. El círculo con centro M y radio MJ corta al diámetro AB en un punto N tal que AN es el lado del polígono regular de 9 lados inscrito en el círculo dado.

(g) Dado un círculo, se traza el lado AB de un pentágono regular inscrito y a continuación el lado BC de un triángulo equilátero inscrito. El círculo con centro C y radio CA corta al círculo dado en otro punto A' tal que AA' es el lado del polígono regular de 15 lados inscrito en el círculo dado.

Igualmente la cuerda que pasa por C y es perpendicular al diámetro que pasa por A es el lado del polígono regular de 15 lados inscrito en el círculo dado.

Grupos

(*) Grupos:

1. $(\mathbb{Q},+)$, $(\mathbb{R},+)$ y $(\mathbb{C},+)$ son grupos conmutativos.
2. El conjunto $\mathbb{R}_+$ de los números reales positivos con el producto es un grupo conmutativo. También lo es el conjunto $\{1,-1\}$ con el producto.
3. Los números complejos no nulos, con el producto de números complejos, forman un grupo conmutativo.
4. Si $(G,\cdot)$ y $(G',\circ)$ son dos grupos, su producto directo $G\times G'$, con la operación $(a,a')*(b,b')=(a\cdot b, a'\circ b')$ es un grupo, que es conmutativo si y sólo si G y G' son conmutativos.
5. Si un grupo sólo tiene un elemento, es el neutro, por lo que tal grupo se denota 1 ó 0, según que la operación se denote multiplicativamente o aditivamente.

(*) Grupos simétricos:

Sea $\sigma\colon X\to Y$ una aplicación biyectiva. Si $y\in Y$, existe un único elemento $x\in X$ tal que $y=\sigma(x)$, elemento que denotaremos $\sigma^{-1}(x)$. Obtenemos así una aplicación $\sigma^{-1}\colon Y\to X$ que también es biyectiva y verifica que $\sigma^{-1}\circ\sigma$ es la identidad de X y $\sigma\circ\sigma^{-1}$ es la identidad de Y. Por tanto, el conjunto de todas las biyecciones de un conjunto no vacío X en sí mismo, con la composición de aplicaciones, es un grupo cuyo elemento neutro es la identidad de X. Este grupo sólo es conmutativo cuando X tiene 1 ó 2 elementos. Cuando X tiene un número finito n de elementos, este grupo se denota S_n y se llama **grupo simétrico** n-ésimo. Sus elementos también reciben el nombre de **permutaciones** de n elementos. Supondremos siempre que $n\geq 2$. Numerando los elementos de X podemos suponer que $X=\{1,2,\ldots,n\}$, así que una permutación $\sigma\in S_n$ puede denotarse de la siguiente forma:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

donde $a_i=\sigma(i)$. Con esta notación es evidente que el orden del grupo simétrico S_n es el factorial $n\cdot(n-1)\cdots 2\cdot 1=n!$.

También es muy usual la siguiente notación: si $a_1,\ldots,a_d$ son números distintos entre 1 y n, denotaremos $(a_1\ldots a_d)$ la permutación que transforma a_i en a_{i+1} (entendiendo que a_{d+1} es a_1) y deja fijos los restantes elementos. Esta notación es cómoda, pero tiene el inconveniente de que es ambigua, pues (2135) denota tanto un elemento del grupo S_5 como de los grupos S_n con cualquier $n\geq 6$. Además, (2135) es la misma permutación que (1352), (3521) y (5213).

(*) Subgrupos:

1. Todo grupo G admite los subgrupos $\{1\}$ y G, llamados subgrupos *triviales*.

2. Sea a un número entero. El conjunto $a\mathbb{Z} = \{ab\colon\ b \in \mathbb{Z}\}$, formado por todos los múltiplos de a, es un subgrupo de $\mathbb{Z}$.

3. $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son subgrupos del grupo aditivo de los números complejos.

4. Los números racionales no nulos, los números reales positivos y las raíces n-ésimas de la unidad son subgrupos del grupo multiplicativo de los números complejos no nulos.

5. Las permutaciones σ de n puntos dados en un plano que conserven distancias (es decir, tales que la distancia entre P y Q coincida con la distancia entre σP y σQ) forman un subgrupo de S_n, llamado **grupo de simetría** de la figura dada.

   Así, el grupo de simetría de un triángulo equilátero de vértices P_1, P_2, P_3 es claramente S_3. Si el triángulo es isósceles y P_1 es el vértice común de los dos lados iguales, el grupo de simetría es $\{\mathrm{Id}, (23)\}$, mientras que el grupo de simetría se reduce a la identidad cuando el triángulo es escaleno.

6. Si en un conjunto X tenemos una estructura definida por ciertas relaciones entre elementos de X, las biyecciones $X \to X$ que conserven tales relaciones formarán siempre un subgrupo del grupo de todas las biyecciones de X en X. Tal grupo exhibe las simetrías de la estructura de X y su determinación forma parte esencial del estudio de la estructura en cuestión. *En el estudio de cualquier estructura (matemática, física, musical,...) subyace siempre un grupo*: el grupo de todos los automorfismos o simetrías de tal estructura.

7. Sean $\alpha_1, \ldots, \alpha_n$ todas las raíces complejas de un polinomio $p(x)$ con coeficientes racionales. Las permutaciones $\sigma \in S_n$ que conserven todas las relaciones algebraicas que existan entre $\alpha_1, \ldots, \alpha_n$ (es decir, si $r(x_1, \ldots, x_n)$ es un polinomio con coeficientes racionales y $r(\alpha_1, \ldots, \alpha_n) = 0$, entonces $r(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$) forman un subgrupo de S_n, llamado **grupo de Galois** del polinomio $p(x)$. La teoría de Galois (1811-1832) mostrará cómo muchas propiedades de $p(x)$ dependen de la estructura de su grupo de Galois.

(*) Ecuaciones Diofánticas Lineales:

Las ecuaciones con coeficientes enteros se llaman *diofánticas*, en honor del matemático griego Diofanto de Alejandría (200?-284? a. de Cristo), cuando se buscan soluciones enteras.

Dados números enteros a, b, c, el algoritmo de Euclides (325?-265? a. de Cristo) permite hallar todas las soluciones enteras de la ecuación diofántica

$$ax + by = c\ .$$

Sea $d = \text{m.c.d.}(a, b)$. La proposición 2.2.3 afirma que la condición necesaria y suficiente para que la ecuación tenga solución entera es que d divida a c.

Supongamos que $a, b \neq 0$ y que la ecuación tiene alguna solución entera (es decir, $c = dc'$ para algún $c' \in \mathbb{Z}$). Si $d = \alpha a + \beta b$, entonces $x_0 = \alpha c'$, $y_0 = \beta c'$ es una solución particular de la ecuación considerada. Todas las soluciones enteras son

$$\begin{cases} x = x_0 + (b/d)n \\ y = y_0 - (a/d)n \end{cases}$$

donde n recorre todos los números enteros. En efecto, por sustitución directa se comprueba que son soluciones y, para cualquier otra solución x, y se tiene

$$0 = c - c = (ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0)$$

luego $a(x - x_0) = -b(y - y_0)$ y $(a/d)(x - x_0) = -(b/d)(y - y_0)$. De 2.2.6 se sigue que b/d divide a $x - x_0$. Es decir, $x - x_0 = (b/d)n$ para algún $n \in \mathbb{Z}$, así que $y - y_0 = -(a/d)n$.

Como ejemplo vamos a resolver la ecuación diofántica $2000x - 266y = -4$.

Primero hallamos el máximo común divisor de 2000 y 266:

$$\begin{aligned} 2000 &= 8 \cdot 266 - 128 \\ 266 &= 2 \cdot 128 + 10 \\ 128 &= 13 \cdot 10 - 2 \\ 10 &= 5 \cdot 2 \end{aligned}$$

y obtenemos que es 2. Como 2 divide a –4, la ecuación dada tiene soluciones enteras. Para calcular una solución particular descomponemos 2 en suma de un múltiplo de 2000 y un múltiplo de 266:

$$\begin{aligned} 2 &= 13 \cdot 10 - 128 = 13(266 - 2 \cdot 128) - 128 = -27 \cdot 128 + 13 \cdot 266 \\ &= -27(8 \cdot 266 - 2000) + 13 \cdot 266 = -203 \cdot 266 + 27 \cdot 2000 \\ -4 &= (-2) \cdot 2 = (-54) \cdot 2000 - (-406) \cdot 266 \end{aligned}$$

así que una solución es $x_0 = -54$, $y_0 = -406$. Por tanto, todas las soluciones en $\mathbb{Z}$ de la ecuación dada son

$$\begin{cases} x = 133n - 54 \\ y = 1000n - 406 \end{cases}$$

(*) Sea n un número natural. Para determinar todas las soluciones enteras de una congruencia

$$ax \equiv b \pmod{n} \qquad a, b \in \mathbb{Z}$$

basta resolver la ecuación diofántica lineal $ax + ny = b$ y considerar los posibles valores de la indeterminada x. Ahora, para resolver un sistema de congruencias

$$\begin{cases} a_1 x \equiv b_1 \ (\text{mód. } n_1) \\ a_2 x \equiv b_2 \ (\text{mód. } n_2) \end{cases}$$

se calculan todas las soluciones enteras $x = c + dt$ de la primera congruencia (caso de que admita alguna solución) y sustituyendo en la segunda se obtiene una congruencia $a_2 dt \equiv b_2 - a_2 c$ (mód n_2) que se resuelve a su vez.

(*) Morfismos de Grupos:

1. Si H es un subgrupo de un grupo G, la inclusión $i\colon H \to G$, $i(a) = a$, es un morfismo de grupos inyectivo y su imagen es H.

2. Si G es un grupo, existe un único morfismo de grupos $1 \to G$, que es inyectivo, y un único morfismo de grupos $G \to 1$, que es epiyectivo.

3. Sean $a, b \in \mathbb{Z}$. La aplicación $f\colon \mathbb{Z}^2 \to \mathbb{Z}$, $f(x, y) = ax + by$, es un morfismo de grupos. Su imagen está formada por todos los números enteros c tales que la ecuación $ax + by = c$ tiene alguna solución entera, y su núcleo está formado por las soluciones enteras de la ecuación $ax + by = 0$. En general, cada matriz (a_{ij}), de m filas y n columnas con coeficientes enteros, define una aplicación

$$f\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$$
$$f(x_1, \ldots, x_n) = (\textstyle\sum_j a_{1j} x_j, \ldots, \sum_j a_{mj} x_j)$$

   que es un morfismo de grupos. El núcleo de f está formado por todas las soluciones enteras del sistema homogéneo de ecuaciones lineales

$$\sum_{j=1}^{n} a_{ij} x_j = 0 \ , \quad i = 1, \ldots, m$$

   y la imagen de f está formada por las sucesiones $(b_1, \ldots, b_m)$ de números enteros tales que el siguiente sistema de ecuaciones lineales tiene alguna solución entera:

$$\sum_{j=1}^{n} a_{ij} x_j = b_i \ , \quad i = 1, \ldots, m$$

   Las afirmaciones siguen siendo válidas si $\mathbb{Z}$ se reemplaza por $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$.

4. Sea $\mathbb{C}^*$ el grupo de los números complejos no nulos con el producto. La aplicación $e^{it}\colon \mathbb{R} \to \mathbb{C}^*$, $e^{it} = \cos t + i \operatorname{sen} t$, es un morfismo de grupos porque $e^{i(t+s)} = e^{it} e^{is}$. Su imagen son los números complejos de módulo 1 y su núcleo está formado por las soluciones de la ecuación $e^{it} = 1$, que son los múltiplos enteros de 2π.

5. El logaritmo neperiano $\ln\colon (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ es un isomorfismo de grupos y el isomorfismo inverso es la función exponencial $e^t\colon (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot)$.

6. Sea G un grupo. El conjunto $\mathrm{Aut}(G)$ de todos los automorfismos de G, con la composición de aplicaciones, es un grupo. Cada elemento $a \in G$ define una aplicación $\tau_a\colon G \to G$, $\tau_a(x) = axa^{-1}$, que es un automorfismo de G. Obtenemos así una aplicación $\tau\colon G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, que es morfismo de grupos.

7. Si G y G' son dos grupos, las proyecciones $G \times G' \to G$ y $G \times G' \to G'$ son morfismos de grupos. También lo es la aplicación $i\colon G \to G \times G'$, $i(g) = (g, 1)$.

(*) Si m.c.d.(m, n)=1, el Teorema chino de los restos muestra que, para cada par de números enteros b, c, el sistema de congruencias

$$\begin{cases} x \equiv b & (\text{mód. } n) \\ x \equiv c & (\text{mód. } m) \end{cases}$$

siempre tiene alguna solución entera, y ésta es única módulo nm: tal sistema de congruencias tiene una única solución $0 \leq x < nm$.

(*) Grupos Cíclicos:

1. El grupo $\mathbb{Z}$ es cíclico y sus generadores son 1 y –1.

2. Si G es un grupo finito de orden n, la condición necesaria y suficiente para que sea cíclico es que tenga algún elemento de orden n. En tal caso, sus generadores son precisamente los elementos de orden n.

3. Si $n \geq 1$, el grupo $\mathbb{Z}/n\mathbb{Z}$ es cíclico, pues está generado por [1]. De acuerdo con 2.5.3, el orden de $[a]_n$ en $\mathbb{Z}/n\mathbb{Z}$ es el primer número natural $r \neq 0$ tal que ra sea múltiplo de n; es decir, tal que $ra = \text{m.c.m.}(a, n)$. Luego es n/d, donde $d = \text{m.c.d.}(a, n)$. En particular, los generadores de $\mathbb{Z}/n\mathbb{Z}$ son los elementos de la forma $[a]_n$, donde a es primo con n. Luego $\mathbb{Z}/n\mathbb{Z}$ tiene exactamente $\phi(n)$ generadores.

   Ahora, de acuerdo con el teorema de clasificación de grupos cíclicos, todo grupo cíclico finito G de orden n tiene exactamente $\phi(n)$ generadores. Más aún, si g es un generador de G, entonces g^m es un generador de G precisamente cuando m.c.d.(m, n)=1.

4. Si g es un elemento de un grupo G, el subgrupo (g) siempre es cíclico, pues está generado por g.

5. Si G es un grupo finito de orden primo y $g \in G$, el teorema de Lagrange implica que $(g) = 1$ ó $(g) = G$. Si $g \neq 1$, tenemos que $(g) = G$. Es decir, todo grupo finito de orden primo es cíclico y está generado por cualquier elemento $g \neq 1$.

6. El grupo $\mu_n = \{z \in \mathbb{C}\colon\ z^n = 1\}$ de las raíces n-ésimas de la unidad, con el producto de números complejos, está generado por $e^{\frac{2\pi i}{n}}$, así que es un grupo cíclico de orden n. Sus generadores son las raíces n-ésimas de la unidad primitivas y hay $\phi(n)$ raíces n-ésimas de la unidad primitivas. En general, si el orden de una raíz n-ésima de la unidad es d, entonces es una raíz d-ésima de la unidad primitiva, y el subgrupo que genera está formado por todas las raíces d-ésimas de la unidad complejas. Como el orden de un elemento siempre divide al orden del grupo, tenemos que

$$\mu_n \ = \bigcup_{d|n} \{\text{raíces } d\text{-ésimas de la unidad primitivas}\}$$

   y vemos así que $n = \sum_{d|n} \phi(d)$.

7. Los giros que dejan invariante un polígono regular de n lados forman un grupo cíclico de orden n.

8. Si un morfismo de grupos $f\colon G \to G'$ es epiyectivo y g es un generador de G, entonces $f(g)$ genera G'. Por tanto, todo cociente de un grupo cíclico G es cíclico.

Ejercicios:

1. Determinar el grupo de simetría de los triángulos, el cuadrado, los rectángulos, los rombos, los trapecios y el pentágono regular.

2. Sean a, b, c elementos de un grupo G. Probar que $ab = ac \Rightarrow b = c$, $ab = a \Rightarrow b = 1$, $ab = 1 \Rightarrow b = a^{-1}$. Demostrar además que $(a^{-1})^{-1} = a$ y $(ab)^{-1} = b^{-1}a^{-1}$.

3. Sea G un grupo conmutativo. Si H_1 y H_2 son subgrupos de G, probar que

$$H_1H_2 := \{h_1h_2\colon\ h_1 \in H_1,\ h_2 \in H_2\}$$

   es un subgrupo de G, y que es el menor subgrupo de G que contiene a H_1 y H_2. ¿Es cierto este resultado si se elimina la hipótesis de que G sea abeliano? (*Indicación:* Considerar el grupo simétrico S_3).

4. ¿Define la operación $x * y = (x + y)/(1 + xy)$ una estructura de grupo sobre los números reales mayores que -1 y menores que 1?

5. Sea H un subconjunto no vacío de un grupo G. Probar que las siguientes condiciones son equivalentes:

   (a) H es un subgrupo de G.

   (b) $xy^{-1} \in H$ para todo $x, y \in H$.

   (c) $xH = H$ para todo $x \in H$.

6. Sea H un subconjunto finito y no vacío de un grupo G. Probar que H es un subgrupo de G precisamente cuando $x \cdot y \in H$ para todo $x, y \in H$. (*Indicación*: Si $x \in H$, considerar la aplicación $f\colon H \to H\,,\ f(y) := xy$).

7. Sean x, y dos elementos de un grupo G. Si $x^5 = 1$, $y^4 = 1$, $xy = yx^3$, probar que $x^2y = yx$, $xy^3 = y^3x^2$.

8. Demostrar que ningún grupo puede ser la unión de dos subgrupos más pequeños.

9. Sean p, n números naturales. Si p es primo y no divide a n, demostrar que n y p^r son primos entre sí para todo $r \geq 1$.

   Si $b, m, n \in \mathbb{Z}$, demostrar que b es primo con mn si y sólo si es primo con m y con n. Además, $m + bn$ es primo con n si y sólo si m es primo con n.

10. Diremos que un número natural n es *perfecto* si coincide con la suma de sus divisores, incluyendo el 1 y excluyendo el propio n.

    Si la suma de los términos de la progresión geométrica 1, 2, $2^2, \ldots, 2^k$ es un número primo, demostrar que el producto de tal suma por el último término es un número perfecto par (Euclides, proposición 36 del libro IX). Euler (1707-1783) demostró que todos los números perfectos pares son de esta forma; pero aún no se sabe si hay infinitos números perfectos ni si existen números perfectos impares. Los números primos que preceden a una potencia de 2 se llaman *primos de Mersenne* (1588-1648) y cada uno proporciona un número perfecto par.

11. Si $2^n - 1$ es un número primo, demostrar que n es primo. Hallar 5 primos de Mersenne y 5 números perfectos.

    (*Indicación:* $x^d - 1 = (x-1)(x^{d-1} + \ldots + x + 1)$).

12. Si $2^n + 1$ es un número primo, demostrar que n es potencia de 2. Los números primos precedidos por una potencia de 2 se llaman **primos de Fermat** (1601-1665). Hallar 5 primos de Fermat.

    (*Indicación:* Cuando d es impar, $x^d + 1 = (x+1)(x^{d-1} - \ldots - x + 1)$).

13. Resolver las siguientes ecuaciones diofánticas:

$$\begin{array}{ccc} 154x + 110y = -22 & 23x - 17y = 2 & 66x - 54y = -18 \\ (x-3y)(x-2y) = 7 & x^2 - 3xy - 10y^2 = -20 & x^2 - xy - 12y^2 = 11 \end{array}$$

14. ¿Es racional la raíz cuadrada de 3/2? ¿Existen números racionales no nulos a, b tales que $a\sqrt{2} + b\sqrt{3}$ sea racional?

15. Probar que existen infinitos números primos de la forma $4n + 3$.

    (*Indicación:* Modificar adecuadamente la demostración de la existencia de infinitos números primos).

16. Probar que si $n^4 + 64$ es un número primo, entonces n es múltiplo de 5.

17. Determinar todos los subgrupos del grupo simétrico S_3.

18. Hallar, salvo isomorfismos, todos los grupos con 1, 2 ó 3 elementos.

19. Sea c un número entero. Probar que la aplicación $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(x) := cx$, es un morfismo de grupos. Determinar su imagen y su núcleo. ¿Cuándo es un isomorfismo?

20. Sea z un número complejo. ¿Cuándo es un isomorfismo de grupos la aplicación $f\colon \mathbb{C} \to \mathbb{C}$, $f(x) = zx$?

21. Sea n un número natural y sea $\mathbb{C}^*$ el grupo multiplicativo de los números complejos no nulos. Probar que la aplicación $f\colon \mathbb{C}^* \to \mathbb{C}^*$, $f(z) := z^r$, es un morfismo de grupos. Determinar su núcleo y su imagen. Análogamente cuando n es entero. ¿Cuándo es un isomorfismo de grupos?

22. Probar que la aplicación $e^{it}\colon \mathbb{R} \to \mathbb{C}^*$ es morfismo de grupos. Determinar su imagen y su núcleo.

23. Sea G un grupo y sea A un grupo conmutativo. Probar que el conjunto $\mathrm{Hom}(G, A)$ formado por los morfismos de grupos $G \to A$ tiene estructura de grupo con la operación

$$(f \cdot h)(x) = f(x) \cdot h(x) \quad , \qquad f, h \in \mathrm{Hom}(G, A) \ , \quad x \in G$$

    ¿Es siempre conmutativo este grupo?

24. Sea $f\colon \mathbb{Q} \to \mathbb{Q}$ un morfismo de grupos. Demostrar la existencia de un único número racional c tal que $f(x) = cx$ para todo $x \in \mathbb{Q}$.

    (*Indicación:* Tal número c ha de ser $f(1)$ necesariamente).

25. Probar que la condición necesaria y suficiente para que un grupo G sea conmutativo es que su operación $G \times G \to G$ sea un morfismo de grupos.

26. Si H_1, H_2 son subgrupos de un grupo conmutativo G, probar que la aplicación $f\colon H_1 \times H_2 \to G$, $f(a,b) := ab$, es un morfismo de grupos.

27. Sea G un grupo finito y sea

$$1 = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_{n-1} \subset G_n = G$$

una sucesión creciente de subgrupos de G. Si r_i denota el índice de G_{i-1} en G_i, demostrar que $|G| = r_1 r_2 \ldots r_n$.

28. Si G es un grupo, probar que $Z(G) = \{a \in G\colon\ ax = xa, \forall x \in G\}$ es un subgrupo de G. ¿Es siempre $Z(G)$ un subgrupo normal de G?

29. Si H es un subgrupo de un grupo G, probar que

$$N(H) = \{a \in G\ :\ aHa^{-1} = H\}$$

es un subgrupo de G que contiene a H. ¿Es siempre $N(H)$ un subgrupo normal de G? ¿Es siempre H un subgrupo normal de $N(H)$?

30. Determinar todos los subgrupos del grupo $\mathbb{Z}/n\mathbb{Z}$ cuando $n = 3, 4, 5, 6, 7$.

31. Sea G un grupo. Demostrar que $G/G = 1$ y que $G/1$ es isomorfo a G.

32. Sea H un subgrupo normal de un grupo G. Probar que la condición necesaria y suficiente para que el grupo cociente G/H sea conmutativo es que H contenga todos los elementos de G de la forma $aba^{-1}b^{-1}$, donde $a, b \in G$.

33. Sea H un subgrupo de un grupo G. Demostrar que H es normal en G si y sólo si $ab \in H \ \Rightarrow\ a^{-1}b^{-1} \in H$.

34. ¿Es cierto que la intersección de dos subgrupos normales de un grupo G siempre es un subgrupo normal de G?

35. Sea H un subgrupo de un grupo G. Si $gHg^{-1} \subseteq H$ para todo $g \in G$, probar que $gHg^{-1} = H$ para todo $g \in G$

36. Sean H y H' subgrupos de un grupo G. Si H es normal en G, ¿se sigue necesariamente que $H' \cap H$ es un subgrupo normal de H'? ¿y que $H' \cap H$ es un subgrupo normal de G?

37. Sea $f\colon G \to G'$ un morfismo de grupos. Si H' es un subgrupo normal de G', ¿se sigue necesariamente que $f^{-1}(H')$ es un subgrupo normal de G? Si H es un subgrupo normal de G, ¿se sigue necesariamente que $f(H)$ es un subgrupo normal de G'?

38. Sea H un subgrupo de un grupo G. Si en el conjunto cociente G/H existe alguna estructura de grupo tal que la proyección canónica $\pi\colon G \to G/H$ sea morfismo de grupos, demostrar que H es un subgrupo normal de G.

39. Determinar todos los subgrupos del grupo simétrico S_3. ¿Cuáles de estos subgrupos son normales?

40. Determinar todos los subgrupos del grupo $\mathbb{Z}/6\mathbb{Z}$ y del grupo $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$.

41. Sea $\phi\colon G \to G'$ un isomorfismo de grupos, H un subconjunto de G y $H' = \phi(H)$. Probar que H es un subgrupo normal de G precisamente cuando H' es un subgrupo normal de G'.

    En tal caso, demostrar además que G/H y G'/H' son grupos isomorfos.

42. Sea G un grupo. Probar que el conjunto $\mathrm{Aut}(G)$ de los automorfismos de G, con la composición de aplicaciones, es un grupo.

    Si $g \in G$, probar que la aplicación $\tau_g\colon G \to G$, $\tau_g(x) := gxg^{-1}$ es un automorfismo de G.

    Probar que la aplicación $\tau\colon G \to \mathrm{Aut}(G)$, $\tau(g) := \tau_g$, es un morfismo de grupos.

43. Sea $\mathbb{C}^*$ el grupo multiplicativo de los números complejos no nulos y sea U el subgrupo de $\mathbb{C}^*$ formado por los números complejos de módulo 1. Probar que
$$\mathbb{R}/\mathbb{Z} \simeq U \qquad , \qquad \mathbb{C}^*/U \simeq \mathbb{R}_+$$
donde $\mathbb{R}_+$ denota el grupo multiplicativo de los números reales positivos. (*Indicación*: La aplicación $\mathbb{R} \to \mathbb{C}^*$, $t \mapsto e^{2\pi i t}$, es morfismo de grupos).

44. Sea $\mu_n := \{z \in \mathbb{C}\colon\ z^n = 1\}$ el grupo multiplicativo de las raíces n-ésimas de la unidad complejas. Probar que
$$\mathbb{C}^*/\mu_n \simeq \mathbb{C}^* \qquad , \qquad U/\mu_n \simeq U$$

45. ¿Cuándo está bien definida la aplicación $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $f([x]_n) = [x]_m$?

46. Resolver las siguientes congruencias:
$$\begin{array}{cc} 7x \equiv -5 \text{ (mód. } 17) & 6x \equiv 6 \text{ (mód. } 14) \\ 94x \equiv -321 \text{ (mód. } 997) & 22x \equiv 33 \text{ (mód. } 121) \end{array}$$

47. Resolver los siguientes sistemas de congruencias:
$$\left\{\begin{array}{l} x \equiv 3 \text{ (mód. } 8) \\ x \equiv -1 \text{ (mód. } 9) \end{array}\right. \qquad \left\{\begin{array}{l} x \equiv 8 \text{ (mód. } 50) \\ x \equiv 3 \text{ (mód. } 15) \end{array}\right. \qquad \left\{\begin{array}{l} x \equiv 2 \text{ (mód. } 1000) \\ x \equiv 14 \text{ (mód. } 23) \end{array}\right.$$

48. Calcular el resto de la división de 5^{1995} por 1000, por 72 y por 180.

49. Probar que la condición necesaria y suficiente para que un grupo G sea conmutativo es que su operación $G \times G \to G$ sea un morfismo de grupos.

50. Sea a, b elementos de un grupo G. Demostrar que $\text{ord}(a) = \text{ord}(bab^{-1})$. ¿Es cierto que siempre $\text{ord}(ab) = \text{ord}(ba)$?

51. Si todos los elementos de un grupo G, salvo el neutro, tienen orden 2, probar que G es conmutativo. Si además G es finito, entonces su orden es una potencia de 2. (*Indicación:* Proceder por inducción sobre el orden y usar el teorema de Lagrange).

52. (*Clasificación de grupos de orden 4*) Demostrar que todo grupo de orden 4 es isomorfo al grupo cíclico $\mathbb{Z}/4\mathbb{Z}$ o al grupo $V = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, llamado grupo de Klein (1849-1925). Además estos dos grupos no son isomorfos.

53. Determinar si los grupos aditivos $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son cíclicos.

54. Sean G_1 y G_2 dos grupos cíclicos finitos. Probar que la condición necesaria y suficiente para que el grupo $G_1 \times G_2$ sea cíclico es que los órdenes de G_1 y G_2 sean primos entre sí.

55. Determinar si los grupos $(\mathbb{Z}/2n\mathbb{Z}) \times (\mathbb{Z}/3n\mathbb{Z})$ son cíclicos.

    (*Indicación*: Estudiar el orden de sus elementos).

56. Determinar qué grupos simétricos S_n son cíclicos.

57. Sea G un grupo cíclico finito de orden n. Si d es un divisor de n, probar que existe un único subgrupo de G de orden d. Además tal subgrupo de G es cíclico.

58. Determinar los automorfismos del grupo de las raíces n-ésimas de la unidad cuando $n = 2$, 3, 4, 5, 6 y 7.

59. Sea b un elemento de un grupo cíclico finito G de orden n y sea m un número entero no nulo. Demostrar que la condición necesaria y suficiente para que exista algún $a \in G$ tal que $b = a^m$ es que $b^{n/d} = 1$, donde $d = \text{m.c.d.}(n, m)$.

60. Sea H un subgrupo de S_n. Probar que todas las permutaciones $\sigma \in H$ son pares o la mitad son pares y la otra mitad impares.

61. Demostrar que todo subgrupo de índice 2 es normal.

    (*Indicación:* Si $g \notin H$, entonces gH y Hg coinciden con $G - H$).

62. Probar que A_4 y $V = \{id, (12)(34), (13)(24), (14)(23)\}$ son los únicos subgrupos normales no triviales de S_4. Concluir que A_4 no tiene subgrupos de orden 6 (el recíproco del teorema de Lagrange (1736-1813) es falso).

63. Si los únicos subgrupos de un grupo $G \neq 1$ son los triviales, 1 y G, entonces G es un grupo finito y su orden es primo.

64. Si un grupo sólo tiene un número finito de subgrupos, su orden es finito.

    (*Indicación:* Todo grupo es unión de subgrupos cíclicos).

65. Si g es un elemento de orden r de un grupo G, determinar el orden de g^m.

66. Sea G un grupo finito que tenga la propiedad de que para cada par de subgrupos H_1, H_2 se tiene $H_1 \subseteq H_2$ ó $H_2 \subseteq H_1$. Probar que G es cíclico y su orden es una potencia de un número primo.

    (*Indicación:* G está generado por un elemento de orden máximo.)

67. Sea $\equiv$ una relación de equivalencia en un grupo G. Si en el conjunto cociente $G/\equiv$ existe alguna estructura de grupo tal que la proyección canónica $\pi\colon G \to G/\equiv$ sea morfismo de grupos, probar la existencia de un subgrupo normal H de G tal que $\equiv$ es la relación de congruencia módulo H.

68. Calcular σ^{6991} cuando $\sigma = (135)(26478)$. Calcular z^{1996} cuando $z = e^{\frac{6\pi i}{11}}$.

    Calcular A^{2001} cuando

$$A = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

69. Sea $\sigma \in S_n$ y $n \geq 3$. Demostrar que si $\sigma\tau = \tau\sigma$ para todo $\tau \in S_n$, entonces σ es la identidad.

70. ¿Está generado S_n por las trasposiciones $(1i)$, $2 \leq i \leq n$? ¿y por las trasposiciones $(i-1, i)$, $2 \leq i \leq n$? ¿y por los ciclos (ijk) de orden 3? ¿y por el ciclo $(12\ldots n)$ y la trasposición (12)? ¿y por el ciclo $(23\ldots n)$ y la trasposición (12)?

71. Sea G un grupo conmutativo de orden n. Si r es un número entero primo con n, demostrar que para cada $a \in G$, la ecuación $x^r = a$ admite una única solución en G.

    (*Indicación:* Considerar el morfismo de grupos $f\colon G \to G$, $f(x) := x^r$).

    ¿Y cuando G no es conmutativo? (*Indicación:* La identidad de Bézout).

Anillos

(*) Anillos:

1. La suma y el producto usuales definen en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ estructuras de anillo. El anillo $\mathbb{Z}$ es íntegro, pero no es un cuerpo, mientras que $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ sí son cuerpos. Además $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$ y $\mathbb{C}^* = \mathbb{C} - \{0\}$.

2. Los polinomios en una indeterminada x con coeficientes enteros, con la suma y el producto de polinomios, forman un anillo $\mathbb{Z}[x]$. Análogamente si se sustituye $\mathbb{Z}$ por $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$. Estos anillos son íntegros, pero ninguno es un cuerpo. Además $\mathbb{Z}[x]^* = \{\pm 1\}$, $\mathbb{Q}[x]^* = \mathbb{Q}^*$, $\mathbb{R}[x]^* = \mathbb{R}^*$ y $\mathbb{C}\,[x]^* = \mathbb{C}^*$.

3. Las fracciones racionales en una indeterminada x con coeficientes racionales, con la suma y el producto de fracciones, forman un cuerpo que denotaremos $\mathbb{Q}(x)$. Análogamente si se sustituye $\mathbb{Q}$ por $\mathbb{R}$ ó $\mathbb{C}$.

4. Si A y B son dos anillos, las operaciones $(a, b) + (\bar{a}, \bar{b}) = (a + \bar{a}, b + \bar{b})$ y $(a, b) \cdot (\bar{a}, \bar{b}) = (a\bar{a}, b\bar{b})$ definen en $A \times B$ una estructura de anillo.

5. Si $1 = 0$ en un anillo A, todo elemento de A es nulo: $a = a \cdot 1 = a \cdot 0 = 0$. Es decir, en todo anillo $A \neq 0$ se verifica que $1 \neq 0$.

(*) Subanillos:

1. $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, que es un subanillo de $\mathbb{R}$, que es un subanillo de $\mathbb{C}$.

2. Los números complejos con parte real e imaginaria entera se llaman **enteros de Gauss** y forman un subanillo de $\mathbb{C}$, que se denota $\mathbb{Z}[i\,]$.

3. $\mathbb{Z}$ es un subanillo de $\mathbb{Z}[x]$. Igualmente sustituyendo $\mathbb{Z}$ por $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$.

4. $\mathbb{Q}[x]$ es un subanillo de $\mathbb{Q}(x)$. Igualmente sustituyendo $\mathbb{Q}$ por $\mathbb{R}$ o $\mathbb{C}$.

5. Si α es un número complejo, el conjunto $\mathbb{Z}[\,\alpha\,]$ de todos los números complejos que sean sumas de productos de potencias de α por números enteros

$$\mathbb{Z}[\,\alpha\,] = \{a_0 + a_1\alpha + \ldots + a_r\alpha^r + \ldots : \ a_0, a_1, \ldots \in \mathbb{Z}\}$$

   es un subanillo de $\mathbb{C}$ y es el menor subanillo de $\mathbb{C}$ que contiene a $\mathbb{Z}$ y α. El anillo de los enteros de Gauss (1777-1855) es precisamente $\mathbb{Z}[\,i\,]$.

6. Si A y B son anillos y $B \neq 0$, entonces $A \times 0$ no es un subanillo de $A \times B$ porque $A \times 0$ no contiene a la unidad de $A \times B$, que es el par (1,1).

(*) La Ecuación Diofántica $x^2 - dy^2 = n$:

Si $d \in \mathbb{Z}$ es un cuadrado perfecto, $d = a^2$, la ecuación diofántica

$$(x + ay)(x - ay) = x^2 - dy^2 = n$$

se reduce a resolver los sistemas de ecuaciones diofánticas lineales $x - ay = m$, $x + ay = n/m$, donde m recorre los divisores de n.

Si d no es un cuadrado perfecto, $x^2 - dy^2$ no puede descomponerse en factores con coeficientes enteros; pero sí admitiendo coeficientes en el anillo $\mathbb{Z}[\sqrt{d}\,]$:

$$(x + \sqrt{d}\,y)(x - \sqrt{d}\,y) = x^2 - d\,y^2 = n$$

Ahora bien, $\mathbb{Z} + \mathbb{Z}\sqrt{d} = \{x + y\sqrt{d} : \ x, y \in \mathbb{Z}\}$ es un subanillo de $\mathbb{C}$, pues es un subgrupo respecto de la suma, contiene a la unidad y

$$(x + y\sqrt{d}\,)(u + v\sqrt{d}\,) = (xu + dyv) + (xv + yu)\sqrt{d}$$

Este subanillo de $\mathbb{C}$ contiene a $\mathbb{Z}$ y a $\sqrt{d}$, y está contenido en $\mathbb{Z}[\sqrt{d}\,]$, así que

$$\mathbb{Z}[\sqrt{d}\,] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$$

Además, como $\sqrt{d}$ no es un número racional, cada número complejo $z \in \mathbb{Z}[\sqrt{d}\,]$ descompone de modo *único* en la forma $z = x + y\sqrt{d}$; $x, y \in \mathbb{Z}$, y llamaremos **norma** de $z = x + y\sqrt{d}$ en el anillo $\mathbb{Z}[\sqrt{d}\,]$ al número entero:

$$\mathrm{N}(z) = (x + y\sqrt{d}\,)(x - y\sqrt{d}\,) = x^2 - d\,y^2$$

(Si d es negativo, $\mathrm{N}(z)$ es el cuadrado del módulo del número complejo z). Se comprueba directamente que $\mathrm{N}(z_1 z_2) = \mathrm{N}(z_1)\mathrm{N}(z_2)$.

La condición necesaria y suficiente para que una pareja de números enteros x, y sea solución de la ecuación dada $x^2 - d\,y^2 = n$ es que $x + y\sqrt{d}$ tenga norma n en $\mathbb{Z}[\sqrt{d}\,]$; es decir, las soluciones enteras de la ecuación $x^2 - dy^2 = n$ se corresponden con los elementos del anillo $\mathbb{Z}[\sqrt{d}\,]$ de norma n.

Por ejemplo, una solución de la ecuación diofántica $x^2 - 2y^2 = -1$ es $x = y = 1$. Por tanto la norma de $z = 1 + \sqrt{2}$ en $\mathbb{Z}[\sqrt{2}\,]$ es –1 y la norma de z^r es $(-1)^r$, lo que nos permite hallar nuevas soluciones de la ecuación dada y también de la ecuación diofántica $x^2 - 2y^2 = 1$:

$$z^2 = 3 + 2\sqrt{2} \quad , \quad z^4 = 17 + 12\sqrt{2} \quad , \quad z^6 = 99 + 70\sqrt{2} \quad , \quad \ldots$$

(3,2), (17,12), (99,70), ... son soluciones de $x^2 - 2y^2 = 1$

$$z^3 = 7 + 5\sqrt{2} \quad , \quad z^5 = 41 + 29\sqrt{2} \quad , \quad z^7 = 239 + 169\sqrt{2} \quad , \quad \ldots$$

(7,5), (41,29), (239,169), ... son soluciones de $x^2 - 2y^2 = -1$

y estas soluciones son diferentes entre sí porque $z^n \neq 1$ para todo $n \neq 0$.

Ahora, conocida una solución entera $x = a$, $y = b$ de alguna ecuación diofántica $x^2 - 2y^2 = n$, $n \in \mathbb{Z}$, podemos hallar nuevas soluciones multiplicando $a + b\sqrt{2}$ por potencias de $z^2 = 3 + 2\sqrt{2}$. vemos así que la ecuación $x^2 - 2y^2 = n$ carece de soluciones enteras no nulas ó tiene infinitas. Por ejemplo, una solución de la ecuación $x^2 - 2y^2 = 8$ es $x = 4$, $y = 2$; así que la norma de $v = 4 + 2\sqrt{2}$ en $\mathbb{Z}[\sqrt{2}\,]$ es 8. Como la norma de $z^2 = 3 + 2\sqrt{2}$ es 1, concluimos que la norma de $z^{2n}v$ es 8 para todo $n \in \mathbb{Z}$, lo que proporciona nuevas soluciones:

$$z^2v = 20 + 14\sqrt{2}\ ,\ z^4v = 116 + 82\sqrt{2}\ ,\ z^6v = 676 + 478\sqrt{2}\ ,\ \ldots$$
$$(20{,}14),\ (116{,}82),\ (676{,}478),\ \ldots \text{ son soluciones de } x^2 - 2y^2 = 8$$

Estas observaciones no sirven para hallar una solución, sólo para calcular más soluciones cuando ya se conoce una. Si supiéramos calcular los divisores z_i de n en el anillo $\mathbb{Z}[\sqrt{d}\,]$, bastaría resolver los sistemas de ecuaciones lineales

$$x + \sqrt{d}\,y = z_i \quad , \quad x - \sqrt{d}\,y = n/z_i$$

para hallar las posibles soluciones enteras de la ecuación $x^2 - dy^2 = n$. Si en este anillo fuera cierto que todo elemento descompone de modo único, salvo el orden y factores invertibles, en producto de elementos irreducibles, los divisores de un elemento serían (salvo factores invertibles) los productos de los factores irreducibles de su descomposición; pero pocos de estos anillos tienen tal propiedad. No obstante, en los anillos pueden introducirse unos números ideales y sí es cierto que en muchos de los anillos asociados a ecuaciones diofánticas cada ideal no nulo descompone, de modo único salvo el orden, en producto de ideales primos. Este fue el origen histórico de la teoría de ideales desarrollada por Kummer (1810-1893) y Dedekind (1831-1916).

(*) Ideales:

1. Si A es un anillo, los subgrupos 0 y A son ideales de A, llamados ideales *triviales*.

2. Sea A un anillo. Si $b \in A$, sus múltiplos forman un ideal de A que denotaremos $bA = \{ba\colon a \in A\}$, ó simplemente (b) cuando el anillo A se supone. Es el ideal de A más pequeño que contiene a b y no debe confundirse con el subgrupo de A generado por b, que en el capítulo anterior también se denotó (b).

3. Todo ideal de $\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$, así que, en virtud de 2.2.1, si $\mathfrak{a}$ es un ideal de $\mathbb{Z}$, existe un único número natural n tal que $\mathfrak{a} = n\mathbb{Z}$: *Los ideales de $\mathbb{Z}$ se corresponden con los números naturales.*

4. La condición necesaria y suficiente para que un anillo $A \neq 0$ sea un cuerpo es que no tenga más ideales que los triviales: 0 y A.

5. Los polinomios con coeficientes racionales que admiten la raíz $\sqrt{2}$ forman un ideal del anillo $\mathbb{Q}[x]$. En general, dado un número complejo α, los polinomios con coeficientes racionales que admiten la raíz α forman un ideal de $\mathbb{Q}[x]$.

6. Sea A un anillo. Si $u \in A$ es invertible, entonces todo elemento de A está en uA. Luego un elemento $a \in A$ es invertible precisamente cuando $aA = A$.

7. En el anillo de polinomios $\mathbb{Z}[x]$ el ideal (x) es claramente primo; pero no es maximal, porque está contenido estrictamente en el ideal $(2, x) \neq \mathbb{Z}[x]$.

(*) Morfismos de Anillos:

1. Si B es un subanillo de A, la inclusión $B \to A$ es morfismo de anillos.

2. Si A es un anillo, existe un único morfismo de anillos $\mathbb{Z} \to A$, que transforma cada número natural n en la suma de n términos iguales a la unidad 1 de A y transforma $-n$ en la suma de n términos iguales a –1.

3. La conjugación compleja $\tau\colon \mathbb{C} \to \mathbb{C}$, $\tau(z) = \bar{z}$, es un automorfismo de $\mathbb{C}$.

4. Si $\alpha \in \mathbb{C}$, la aplicación $\mathbb{Z}[x] \to \mathbb{C}$ que asigna a cada polinomio $p(x)$ su valor en α es un morfismo de anillos. Su núcleo está formado por los polinomios con coeficientes enteros que admiten la raíz α, y su imagen es precisamente el subanillo $\mathbb{Z}[\alpha]$.

5. Si A y B son anillos, las proyecciones naturales de $A \times B$ en A y B son morfismos de anillos; pero las inclusiones $A \to A \times B$ y $B \to A \times B$ no.

6. Sea $I = [a, b]$ un intervalo cerrado de $\mathbb{R}$ y sea $\mathcal{C}(I)$ el anillo de todas las funciones continuas de I en $\mathbb{R}$. Si $x_0 \in I$, la aplicación $\mathcal{C}(I) \to \mathbb{R}$ que asigna a cada función su valor en x_0 es un morfismo de anillos epiyectivo cuyo núcleo está formado por las funciones continuas en I que se anulan en x_0.

7. Si $\phi\colon I \to I'$ es una aplicación continua entre dos intervalos, entonces la aplicación $\mathcal{C}(I') \to \mathcal{C}(I)$, $f \mapsto f \circ \phi$, es morfismo de anillos.

(*) Según el teorema 3.4.1, los únicos números racionales que pueden ser raíces del polinomio $p(x) = 6x^4 + x^3 + 11x^2 + 2x - 2$ son ± 1, ± 2, $\pm 1/2$, $\pm 1/3$, $\pm 2/3$, $\pm 1/6$. Por comprobación directa se obtiene que sólo $-1/2$ y $1/3$ son raíces de $p(x)$, así que éstas son las únicas raíces racionales de $p(x)$.

(*) Cálculo de Raíces con Radicales:

Veamos cómo pueden expresarse con radicales las raíces de un polinomio con coeficientes complejos cuando el grado es ≤ 4:

Ecuación Cuadrática: $ax^2 + bx + c = 0$, $a \neq 0$.

Como $4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$, las únicas soluciones son

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

y $b^2 - 4ac$ recibe el nombre de discriminante, pues es $\neq 0$ precisamente cuando la ecuación considerada admita dos soluciones complejas distintas.

Ecuación Cúbica: $x^3 + c_1x^2 + c_2x + c_3 = 0$.

Mediante el cambio de variable $x = y - c_1/3$ se obtiene una ecuación de la forma

$$(*) \qquad y^3 + py + q = 0$$

así que las soluciones de la ecuación inicial se obtienen restando $c_1/3$ a las soluciones de $(*)$. Si $p = 0$, sus soluciones son las raíces cúbicas de $-q$.

Si $p \neq 0$, con el cambio de variable $y = z - (3z)^{-1}p$ se transforma en la ecuación

$$0 = z^6 + qz^3 - \frac{p^3}{27} = u^2 + qu - \frac{p^3}{27} \quad , \qquad u = z^3$$

así que cada raíz α de $z^6 + qz^3 - p^3/27$ da una solución $\alpha - 3/p\alpha$ de $(*)$. Considerando las tres raíces cúbicas α, $\omega\alpha$, $\omega^2\alpha$ de una de las raíces del polinomio $u^2 + qu - p^3/27$ obtenemos tres soluciones de $(*)$. Si se consideran las raíces cúbicas β, $\omega\beta$, $\omega^2\beta$ de la otra raíz de $u^2 + qu - p^3/27$ se obtienen las mismas soluciones de $(*)$, porque, eligiendo β de modo que $\alpha\beta = p/3$, es claro que β (respectivamente $\omega\beta$, $\omega^2\beta$) proporciona la misma solución que α (respectivamente $\omega^2\alpha$, $\omega\alpha$).

Ecuación Cuártica: $x^4 + c_1x^3 + c_2x^2 + c_3x + c_4 = 0$.

Las soluciones de esta ecuación son las abscisas de las soluciones del sistema

$$\begin{cases} 0 = y^2 + c_1xy + c_2y + c_3x + c_4 \\ y = x^2 \end{cases}$$

lo que reduce el problema al de la determinación de los puntos de corte de dos cónicas, cuestión que puede resolverse del siguiente modo:

Entre las cónicas del haz $(y^2 + c_1xy + c_2y + c_3x + c_4) + \lambda(x^2 - y) = 0$, $\lambda \in \mathbb{C}$, se elige una que esté formada por un par de rectas (esto exige resolver una ecuación cúbica en λ); es decir, tal que su ecuación sea $(y - ax - b)(y - a'x - b') = 0$, lo que significa que, considerada como polinomio en y con coeficientes en el cuerpo $\mathbb{C}(x)$, tenga en $\mathbb{C}(x)$ las raíces $ax + b$, $a'x + b'$. Cortando las rectas $y = ax + b$, $y = a'x + b'$ con una cónica cualquiera del haz (por ejemplo con la cónica $y = x^2$)

se obtienen los puntos de corte de las dos cónicas consideradas, y sus abscisas son las soluciones de la cuártica dada.

(*) Vamos a calcular, con el método anterior, las soluciones complejas de la ecuación $x^4+x+2=0$, que son las abscisas de las soluciones del sistema $y=x^2$, $y^2+x+2=0$:

$$y^2+x+2+\lambda(y-x^2)=y^2+\lambda y+(-\lambda x^2+x+2)=0$$

$$y=\frac{-\lambda+\sqrt{\lambda^2+4(\lambda x^2-x-2)}}{2}$$

y la condición de que estas raíces sean polinomios de grado 1 en x significa que $4\lambda x^2-4x+\lambda^2-8$ debe ser el cuadrado de algún polinomio de grado 1; es decir, su discriminante ha de ser nulo:

$$0=16-16\lambda(\lambda^2-8)=\lambda^3-8\lambda-1$$

Si $\alpha\in\mathbb{C}$ es solución de esta ecuación, entonces $4\alpha x^2-4x+\alpha^2-8=(cx+d)^2$. Igualando coeficientes se sigue que $c=2\sqrt{\alpha}$, $d=-1/\sqrt{\alpha}$; es decir, las soluciones se obtienen cortando la cónica $y=x^2$ con las dos rectas

$$y=\frac{-\alpha\pm 2\sqrt{\alpha}x\mp\frac{1}{\sqrt{\alpha}}}{2}$$

Las soluciones son las raíces de los dos polinomios $2x^2\mp 2\sqrt{\alpha}x+\alpha\pm 1/\sqrt{\alpha}$, que son los 4 números complejos

$$x=\frac{\pm\sqrt{\alpha}\pm\sqrt{-\alpha\mp\frac{2}{\sqrt{\alpha}}}}{2}$$

(*) Congruencias:

1. El anillo $\mathbb{Z}/4\mathbb{Z}$ no es íntegro, porque $[2]\cdot[2]=0$ y $[2]\neq 0$. En general, si un número natural $n\geq 4$ no es primo, el anillo $\mathbb{Z}/n\mathbb{Z}$ no es íntegro. Por otra parte, si p es un número primo, el anillo $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo (luego íntegro).

2. Consideremos la posibilidad de descomponer un número natural dado n en suma de dos potencias cuartas de números enteros: $x^4+y^4=n$.

   Si reducimos esta ecuación módulo 5, al ser $x^4=1$ para todo elemento no nulo x del anillo $\mathbb{Z}/5\mathbb{Z}$, se sigue que la ecuación reducida no tiene soluciones en $\mathbb{Z}/5\mathbb{Z}$ cuando $\bar{n}=\bar{3}$ ó $\bar{n}=\bar{4}$. Es decir, la ecuación inicial no tiene soluciones enteras cuando n es congruente con 3 ó 4 módulo 5. Además, cuando $\bar{n}=0$, la única solución en $\mathbb{Z}/5\mathbb{Z}$ de la ecuación reducida es $x=0$, $y=0$; de modo que si a, b es una solución entera de la ecuación inicial y n es un múltiplo de 5, también a y b son múltiplos de 5: si un múltiplo de 5 es suma de dos potencias cuartas, necesariamente es múltiplo de $5^4=625$.

(*) Consideremos el morfismo de anillos $f\colon \mathbb{R}[x] \to \mathbb{C}$ que a cada polinomio con coeficientes reales $p(x)$ le asigna el número complejo $p(i)$. Este morfismo es epiyectivo, pues cada número complejo $a+bi$ proviene del polinomio $a+bx$, y su núcleo está formado por los polinomios que admiten la raíz $x = i$. Ahora bien, si un polinomio con coeficientes reales tiene la raíz i, también tiene la raíz $-i$ y ha de ser múltiplo de $(x-i)(x+i) = x^2+1$. En resumen, el núcleo de f es el ideal (x^2+1) y el teorema de isomorfía permite concluir que $\mathbb{C}$ se obtiene al adjuntar a $\mathbb{R}$ una indeterminada x que verifique la relación $x^2 = -1$:

$$\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}\ , \qquad [x] \mapsto i$$

(*) Congruencia de Wilson (1741-1793)**:** *Si p es un número primo, entonces*

$$(p-1)! \equiv -1 \text{ (mód. } p).$$

Los elementos de $\mathbb{F}_p$ que coinciden con su inverso son precisamente las raíces del polinomio $x^2 - 1 = (x+1)(x-1)$ en $\mathbb{F}_p$; así que son $x = \pm[1]$ (y son distintos cuando $p \neq 2$, lo cual supondremos en adelante, pues la congruencia es obvia cuando $p = 2$). Luego en el producto

$$[(p-1)!] = [1]\cdot[2]\cdots[p-1]$$

los factores desde el $[2]$ hasta el $[p-2]$ pueden agruparse cada uno con su inverso y concluimos que

$$[(p-1)!] = [1]\cdot[p-1] = [-1]\ .$$

Una demostración alternativa, que me ha comunicado J. Arboleda Castilla, se basa en la congruencia de Fermat (1601-1665), que afirma que los elementos no nulos de $\mathbb{F}_p^*$ son raíces de $x^{p-1}-1$; luego, de acuerdo con 3.4.5, tenemos

$$x^{p-1} - 1 \ = \ (x-1)(x-2)\ldots(x-(p-1))$$

en $\mathbb{F}_p[x]$, y la congruencia de Wilson (1741-1793) se obtiene al igualar los coeficientes de grado cero (que están en $\mathbb{F}_p$):

$$-1 \ = \ (-1)^{p-1}(p-1)!$$

(*) Un buen método para calcular el indicador de Euler (1707-1783) de un número natural n consiste en descomponerlo en producto de números primos:

$$\phi(2000) = \phi(2^4 5^3) = \phi(2^4)\phi(5^3) = 2^3 5^2 (5-1) = 2^5 5^2$$
$$\phi(1995) = \phi(3\cdot 5\cdot 7\cdot 19) = 2\cdot 4\cdot 6\cdot 18 = 864$$

(*) Para calcular el resto de $n = 29^{2022}$ módulo 92, podemos utilizar la congruencia de Euler porque 29 y 92 son primos entre sí. Como $\phi(92) = \phi(4\cdot 23) = \phi(2^2)\cdot \phi(23) = 2\cdot 22 = 44$, en el anillo $\mathbb{Z}/92\mathbb{Z}$ tenemos que $[29]^{44} = 1$; luego:

$$[n] = [29]^{2022} = [29]^{46\cdot 44 - 2} = [29]^{46\cdot 44}\cdot [29]^{-2} = [29]^{-2}$$

El inverso de 29 módulo 92 se calcula con la Identidad de Bézout (1730-1783):

$$1 = 6 \cdot 92 - 19 \cdot 29 \ .$$

En el anillo $\mathbb{Z}/92\mathbb{Z}$ tenemos que $[29]^{-1} = [-19]$ y concluimos que

$$[n] = [29]^{-2} = [-19]^2 = [361] = [85]$$

(*) Partes de un Conjunto: Fijado un conjunto X, cada subconjunto $A \subseteq X$ está totalmente determinado por su **función característica** $\chi_A \colon X \to \{0,1\}$:

$$\chi_A(x) := \begin{cases} 1 \text{ cuando } x \in A \\ 0 \text{ cuando } x \notin A \end{cases}$$

y obtenemos así una biyección natural entre el conjunto $\mathcal{P}(X)$ de subconjuntos de X y el conjunto de las funciones sobre X valoradas en el cuerpo $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Las operaciones usuales con subconjuntos admiten la siguiente traducción en términos de funciones (donde la función característica de cada subconjunto se denota con la correspondiente letra minúscula):

	Función característica
$A^c = X - A$	$1 + a$
$A \cap B$	ab
$A \cup B$	$a + b + ab$
$A - B = A \cap B^c$	$a(1 + b)$
$A \triangle B = (A - B) \cup (B - A)$	$a + b$
X	1
$\emptyset$	0

Ahora, para demostrar igualdades entre subconjuntos, basta comprobar la coincidencia de sus funciones características, con la ventaja de nuestra gran familiaridad con el cálculo de funciones. Además, de regalo tenemos que $f^2 = f$ y $f + f = 0$ para toda función valorada en $\mathbb{F}_2 = \{0,1\}$. Por ejemplo, el carácter asociativo de la suma de funciones, $(a+b)+c = a+(b+c)$, demuestra la propiedad asociativa de la diferencia simétrica: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$; y la ley de Morgan (1806-1871) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ se sigue directamente del cálculo de las correspondientes funciones características:

$A \cap (B \cup C)$	$a(b + c + bc) = ab + ac + abc$
$(A \cap B) \cup (A \cap C)$	$ab + ac + abac = ab + ac + abc$

Este procedimiento también puede usarse para demostrar inclusiones entre subconjuntos, pues la condición $A \subseteq B$ equivale a la igualdad $A \cap B = A$. Además, permite dar condiciones necesarias y suficientes para que sea válida cierta igualdad

entre subconjuntos, pues equivale a la igualdad de sus funciones características. Así, el cálculo de las funciones características de $(A-B)-C$ y $A-(B-C)$:

$$\begin{array}{ll} (A-B)-C & a(1+b)(1+c) = a+ab+ac+abc \\ A-(B-C) & a[1+b(1+c)] = a+ab+abc \end{array}$$

muestra que $(A-B)-C = A-(B-C)$ precisamente cuando

$$a+ab+ac+abc = a+ab+abc \quad , \quad ac = 0$$

es decir, cuando $A \cap C = \emptyset$.

(*) Cálculo Proposicional: Si 0 y 1 representan los valores lógicos *verdadero* y *falso*, los enunciados de una teoría pueden entenderse como funciones valoradas en el cuerpo $\mathbb{F}_2 = \{0,1\}$, y las operaciones lógicas como operaciones con funciones (o sea, con funciones sobre $(\mathbb{F}_2)^n$, donde n es el número de variables que intervengan en la operación):

	Función asociada
$\neg p$	$1+p$
$p \vee q$	pq
$p \wedge q$	$p+q+pq$
$p \Rightarrow q$	$(1+p)q$
$p \Leftrightarrow q$	$p+q$

Las *tautologías* son las operaciones lógicas con función asociada idénticamente nula.

Por ejemplo, a $(p \wedge q) \Leftrightarrow (\neg r)$ le corresponde la función sobre $(\mathbb{F}_2)^3$:

$$p+q+pq+r+1 = (1+p)(1+q)+r \ ,$$

y proporciona directamente su tabla de valores lógicos (recuérdese que 0=*verdadero*, 1=*falso*):

p	q	r	$(p \wedge q) \Leftrightarrow (\neg r)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Además, la función $\delta_{a_1,\ldots,a_n} = (p_1 - a_1^*)\ldots(p_n - a_n^*)$, donde $a_i^* = 1+a_i$, se anula siempre, salvo cuando $p_1 = a_1, \ldots, p_n = a_n$, lo que permite resolver el *Problema de*

Post: la determinación de una operación lógica f que tenga una tabla de valores predeterminada:

$$f = \sum_{a_1,\ldots,a_n} f(a_1,\ldots,a_n)\,\delta_{a_1,\ldots,a_n}\ .$$

Ejercicios:

1. Hallar los elementos invertibles en los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Q}(x)$ y $\mathbb{Z}[\,i\,]$. Probar que el anillo $\mathbb{Z}[\sqrt{2}\,]$ tiene infinitos elementos invertibles.

2. Si A es un anillo, probar que el producto de A define una estructura de grupo conmutativo en A^*. Además $(A \times B)^* = A^* \times B^*$.

3. Determinar los elementos irreducibles de los anillos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$.

4. Sea b un elemento de un anillo A. Si $u \in A$ es invertible en A, probar que b es irreducible en A precisamente cuando ub sea irreducible en A.

5. Determinar las relaciones de inclusión entre los siguientes subanillos de los números complejos:

   $$\mathbb{Z}\ ,\ \mathbb{Z}[\,i\,]\ ,\ \mathbb{Z}[\,2\,]\ ,\ \mathbb{Z}[\,2i\,]\ ,\ \mathbb{Z}[\,i-2\,]\ ,\ \mathbb{Z}[1-2i\,]\ ,\ \mathbb{Z}[\,i/2\,]\ ,\ \mathbb{Z}[1/2\,]$$

   y probar que $\sqrt[3]{2}$ no está en $\mathbb{Z}[\sqrt{2}\,]$. (*Indicación:* $\mathbb{Z}[\sqrt{d}\,] = \mathbb{Z} + \mathbb{Z}\sqrt{d}\,$).

6. Determinar el número de soluciones enteras de las ecuaciones:

$x^2 - 3y^2 = 1$	$x^2 - 3y^2 = -1$	$x^2 - 5y^2 = -1$	$x^2 - 5y^2 = 1$
$x^2 - 4y^2 = -1$	$x^2 - 7y^2 = -1$	$x^2 - 8y^2 = -2$	$x^2 - 8y^2 = 4$
$x^2 - 5y^2 = -11$	$x^2 - 7y^2 = 7$	$x^2 - 20y^2 = -11$	$x^2 - 7y^2 = 18$
$x^2 - 3y^2 = 16$	$x^2 - 3y^2 = 18$	$x^2 - 5y^2 = 20$	$x^2 - 5y^2 = 55$

7. Sea d un número entero que no sea cuadrado perfecto. Pruébese que la condición necesaria y suficiente para que un número complejo $z \in \mathbb{Z}[\sqrt{d}\,]$ sea invertible en $\mathbb{Z}[\sqrt{d}\,]$ es que su norma en $\mathbb{Z}[\sqrt{d}\,]$ sea 1 ó –1.

8. Si la norma de un elemento $z \in \mathbb{Z}[\sqrt{d}\,]$ es un número primo, probar que z es irreducible en el anillo $\mathbb{Z}[\sqrt{d}\,]$.

9. Demostrar que un número primo p es irreducible en $\mathbb{Z}[\sqrt{d}\,]$ precisamente cuando las ecuaciones $x^2 - dy^2 = p$, $x^2 - dy^2 = -p$ no tienen soluciones enteras.

10. ¿Son irreducibles en el anillo $\mathbb{Z}[\sqrt{2}\,]$ los números 2, 3, 5, 7, 11, 13 y 17?

11. ¿Son cuerpos los anillos $\mathbb{Z}[\sqrt{2}\,]$ y $\mathbb{Q}[\sqrt{2}\,]$?
    ¿Coincide $\mathbb{Q}[\sqrt{2}\,]$ con $\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{z \in \mathbb{C}\colon\ z = a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$?

12. Determinar un generador de cada uno de los siguientes ideales del anillo $\mathbb{Z}$: $\big((6)\cap(22)\big)+(15)$, $(6,15)\cap(22)$, $\big((6)\cap(22)\big)+\big((6)\cap(15)\big)$.

13. Sea $\mathfrak{a}$ un ideal de un anillo A. Probar que la condición necesaria y suficiente para que $\mathfrak{a}=A$ es que $\mathfrak{a}$ contenga algún elemento invertible en A.

14. Si $a_1,\ldots,a_n,b_1,\ldots,b_m$ son elementos de un anillo A, demostrar que

$$(a_1,\ldots,a_n)=a_1A+\ldots+a_nA$$
$$\big(\sum_i a_iA\big)\cdot\big(\sum_j b_jA\big) \;=\; \sum_{i,j} a_ib_jA$$

15. Si la unión de dos ideales de un anillo A es un ideal de A, probar que uno de los dos ideales está contenido en el otro.

16. Consideremos en el anillo $A=\mathbb{Z}[\,2i\,]$ los ideales $\mathfrak{a}=2A$, $\mathfrak{b}=2iA$. Determinar las relaciones de inclusión entre los siguientes ideales de A:

$$\mathfrak{a}\ ,\ \mathfrak{b}\ ,\ 4A\ ,\ \mathfrak{a}^2\ ,\ \mathfrak{b}^2\ ,\ \mathfrak{ab}\ ,\ \mathfrak{a}+\mathfrak{b}\ ,\ \mathfrak{a}\cap\mathfrak{b}$$

17. Probar que $4=2\cdot2=(-2i)(2i)$ son, salvo invertibles, descomposiciones distintas del número 4 en producto de elementos irreducibles del anillo $\mathbb{Z}[\sqrt{-4}\,]$, y que $6=2\cdot3=(1+\sqrt{-5}\,)(1-\sqrt{-5}\,)$ son, salvo invertibles, descomposiciones distintas del 6 en producto de elementos irreducibles de $\mathbb{Z}[\sqrt{-5}\,]$. Además, en el anillo $\mathbb{Z}[\sqrt{-5}\,]$, el ideal $\mathfrak{a}=(2,1+\sqrt{-5}\,)$ no está generado por un elemento y su cuadrado es el ideal (2).

18. Sea p un número primo. ¿Es irreducible el número 2 en el anillo $A=\mathbb{Z}[\sqrt{-p}\,]$? ¿Es primo el ideal $2A$?

    (*Indicación:* $1+p=(1+\sqrt{-p}\,)(1-\sqrt{-p}\,)$ es par cuando p es impar.)

19. Sea p un elemento no nulo de un anillo íntegro A. Probar que si el ideal pA es primo, entonces p es irreducible en A. ¿Es cierto el recíproco?

    (*Indicación:* El ejercicio anterior).

20. Probar que si un ideal primo $\mathfrak{p}$ divide a un producto $\mathfrak{ab}$ de dos ideales, entonces divide a $\mathfrak{a}$ o a $\mathfrak{b}$. Si un ideal primo $\mathfrak{p}$ divide al mínimo común múltiplo $\mathfrak{a}_1\cap\ldots\cap\mathfrak{a}_n$ de unos ideales, entonces $\mathfrak{p}$ divide a $\mathfrak{a}_i$ para algún índice i.

21. Sean a,b dos elementos de un anillo íntegro A. Demostrar que: $aA=bA \;\Leftrightarrow\; b=ua$ para algún elemento $u\in A$ invertible.

22. La condición necesaria y suficiente para que un anillo A sea un cuerpo es que tenga exactamente dos ideales (los ideales triviales: 0 y A).

23. Probar que todo anillo íntegro finito A es cuerpo.

    (*Indicación*: Considerar las aplicaciones $A \xrightarrow{\cdot a} A$).

24. Sea $f\colon A \to B$ un morfismo de anillos. ¿Es cierto que la imagen de f es siempre un ideal de B? ¿y un subanillo de B? Responder a las mismas preguntas para el núcleo de f.

25. Demostrar que el único automorfismo de anillos del cuerpo $\mathbb{Q}$ es la identidad. ¿Es cierta esta afirmación para los cuerpos $\mathbb{R}$ y $\mathbb{C}$? (*Indicación:* Probar que todo automorfismo de $\mathbb{R}$ transforma números positivos en números positivos).

26. Sea $f\colon A \to B$ un morfismo de anillos. Averiguar si son ciertas las siguientes afirmaciones?

    Si $\mathfrak{p}$ es un ideal primo de B, entonces $f^{-1}(\mathfrak{p})$ es un ideal primo de A.

    Si $\mathfrak{m}$ es un ideal maximal de B, entonces $f^{-1}(\mathfrak{m})$ es un ideal maximal de A.

27. Sea $f\colon A \to B$ un morfismo epiyectivo de anillos.

    Si $\mathfrak{p}$ es un ideal primo de A que contiene al núcleo de f, probar que $f(\mathfrak{p})$ es un ideal primo de B.

    Si $\mathfrak{m}$ es un ideal maximal de A que contiene al núcleo de f, probar que $f(\mathfrak{m})$ es un ideal maximal de B.

28. Sean $p(x)$ y $q(x)$ polinomios con coeficientes racionales. Si $p(x)$ es múltiplo de $q(x)$ en $\mathbb{C}[x]$ ¿se sigue que $p(x)$ es múltiplo de $q(x)$ en $\mathbb{Q}[x]$?

    Si un polinomio con coeficientes enteros $p(x)$ es múltiplo de $x^3 - 3$ en $\mathbb{C}[x]$, ¿se puede concluir que $p(x)$ es múltiplo de $x^3 - 3$ en $\mathbb{Z}[x]$?

29. Sea k un cuerpo y $a \in k$. Demostrar que $p(x)$ es irreducible en $k[x]$ si y sólo si lo es $p(x + a)$.

30. Hallar todas las raíces racionales de los siguientes polinomios: x^3+2x^2+x+2 , $2x^3 - 4x^2 - x - 15$, $6x^4 - x^3 - 7x^2 + x + 1$, $x^2(1 + x)^2 + x^2 - 8(1 + x)^2$.

31. Si $p_1, \ldots, p_r$ son números primos diferentes, probar que $(p_1 \cdots p_r)^{1/m}$ es irracional para todo número natural $m \geq 2$.

32. Determinar si los siguientes polinomios son irreducibles en el anillo $\mathbb{Q}[x]$: $x^3 - x - 1$, $2x^3 + x + 2$, $3x^3 - 3x + 2$, $4x^3 - 3x - 1/2$, $x^4 - x - 1$, $2x^4 + 1$, $x^4 + x^3 + 1$, $x^4 + 3x^2 + 44$, $x^4 + 4$, $x^4 - x^2 - 1$, $x^4 + 3x^3 + 1$, $x^4 - x^2 + 18x + 7$.

33. ¿Es cierto que todo polinomio de grado 4 con coeficientes racionales y sin raíces en $\mathbb{Q}$ es irreducible en $\mathbb{Q}[x]$?

34. Sea $p(x) \in \mathbb{Q}[x]$. Si $p(x^n)$ es múltiplo de $x-1$, concluir que $p(x^n)$ es múltiplo de $x^n - 1$.

35. Hallar un polinomio con coeficientes racionales de grado ≤ 3 que tome los valores –3, 7, 35, 125 cuando $x = 1, 2, 3, 4$.

36. Sea $p(x, y)$ un polinomio con coeficientes en un anillo A. Probar que $p(x, x) = 0$ precisamente cuando $p(x, y)$ es múltiplo de $y - x$ en $A[x, y]$.

37. Sea $\equiv$ una relación de equivalencia en un anillo A. Si existe una estructura de anillo en el conjunto cociente $A/\equiv$ tal que la proyección canónica $\pi\colon A \to A/\equiv$ es morfismo de anillos, probar la existencia de un ideal $\mathfrak{a}$ de A tal que $\equiv$ es la relación de congruencia módulo $\mathfrak{a}$.

38. Hallar todos los restos cuadráticos y cúbicos módulo 3, 4, 5, 6, 7, 8, 9 y 10.

39. Demostrar que $1993^{1993} \pm 993$ no es un cubo ni un cuadrado perfecto.

40. Determinar los posibles valores entre 1 y 10 que puede tomar la función $x^3 + y^3 + z^3$ cuando x, y, z son números enteros.

41. Hallar todos los polinomios irreducibles de grado menor que 5 en $(\mathbb{F}_2)[x]$.
Hallar todos los polinomios irreducibles de grado menor que 4 en $(\mathbb{F}_3)[x]$.

42. Probar que $\mathbb{R}[x]/(x^2+x+1) \simeq \mathbb{C}$, $k[x]/(x-a) \simeq k$ y $\mathbb{R}[x]/(x^2-1) \simeq \mathbb{R} \oplus \mathbb{R}$

43. Demostrar que $k[x, y]/(x - a) \simeq k[y]$. Concluir que en el anillo $k[x, y]$ se verifica $\big(p(x, y), x - a\big) = \big(p(a, y), x - a\big)$.

44. Sea p un número primo. Demostrar que las ecuaciones $x^2 - dy^2 = \pm p$ no tienen soluciones enteras cuando el número entero d no es resto cuadrático módulo p.

45. En el anillo $\mathbb{Z}/993\mathbb{Z}$, hallar el inverso de $[248]$ y de $[4]^{13}$. Calcular el resto de la división de 248^{1993} por 993.

46. Calcular todas las soluciones de la reducción módulo 11 de las ecuaciones:
$$14x^2 - 5y^2 = 22 \qquad 11x^2 - 17y^2 = -3$$
$$13x^2 - 6x + 22y^2 = 4 \qquad 4x^2 + 7xy - 5y^2 = 33$$

47. Sea n un número natural mayor que 1. Si $a^{n-1} \equiv 1$ (mód. n) para todo número entero a que no sea múltiplo de n, probar que n es un número primo.

48. Sea n un número natural mayor que 1. Si $(n - 1)! \equiv -1$ (mód. n), probar que n es un número primo.

49. Sea $q(x) = (2x - 3)(3x - 2)$. Si p^r es una potencia de un número primo, probar que la congruencia $q(x) \equiv 0$ (mód. p^r) tiene alguna solución entera. Concluir, usando el teorema chino de los restos, que todas las congruencias $q(x) \equiv 0$ (mód. n) tienen solución entera, aunque la ecuación $q(x) = 0$ carece de soluciones enteras.

50. Sea p un número primo. Si a, $b \in \mathbb{F}_p$ no son restos cuadráticos, probar que ab sí es un resto cuadrático módulo p.

    Probar que el polinomio $q(x) = (x^2 - 17)(x^2 + 1)(x^2 + 17)$ no tiene raíces racionales y que su reducción $\bar{q}(x)$ módulo p tiene alguna raíz en $\mathbb{F}_p$ para todo número primo p.

    Probar que el polinomio $q(x) = x^8 - 16$ no tiene raíces racionales y que su reducción $\bar{q}(x)$ módulo p tiene alguna raíz en $\mathbb{F}_p$ para todo número primo p.

    (*Indicación:* Sus raíces complejas son funciones racionales de $\sqrt{2}$, i y $\sqrt{2}i$.)

51. Demostrar que el número 17 es resto cuadrático módulo 2^n para todo $n \geq 1$.

    (*Indicación:* Proceder por inducción sobre n.)

    Sea p un número primo impar. Si un número entero a es resto cuadrático módulo p, probar que a también es resto cuadrático módulo p^n para todo $n \geq 2$.

    Usando el teorema chino de los restos y el ejercicio anterior, concluir que el polinomio $q(x) = (x^2-17)(x^2+1)(x^2+17)$ no tiene raíces racionales aunque la congruencia $q(x) \equiv 0$ (módulo n) tenga soluciones para todo número natural $n \geq 2$.

52. Sea p un número primo impar. Demostrar que:

    (a) Si $p-1$ no es múltiplo de 3, todo elemento de $\mathbb{F}_p$ es resto cúbico.

    (b) Si $p-1$ es múltiplo de 3, en $\mathbb{F}_p$ hay exactamente $(p-1)/3$ restos cúbicos no nulos. (*Indicación:* Si $p - 1 = 3d$, probar que $x^{p-1} - 1$ es múltiplo de $x^3 - 1$ y aplicar la congruencia de Fermat).

53. Demostrar que el polinomio $q(x) = (x^3 - 2)(x^2 + x + 1)$ no tiene raíces racionales y que su reducción $\bar{q}(x)$ módulo p tiene alguna raíz en $\mathbb{F}_p$ para todo número primo p.

54. Sean A y B dos anillos. Probar que todo ideal de $A \times B$ es de la forma $\mathfrak{a} \times \mathfrak{b}$ para ciertos ideales $\mathfrak{a} \subseteq A$, $\mathfrak{b} \subseteq B$. Además:

$$(A \times B)/\mathfrak{a} \times \mathfrak{b} \;=\; (A/\mathfrak{a}) \times (B/\mathfrak{b})$$

55. De los siguientes sistemas en dos incógnitas con coeficientes reales, determinar los que son equivalentes:

$$\left.\begin{aligned} x^2 - y^2 &= x^3 \\ y + x &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} x &= 0 \\ y &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} x^3 &= 0 \\ y + x &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} x^3 &= 0 \\ y^2 &= x^2 \end{aligned}\right\}$$

$$\left.\begin{aligned} x^2 &= 0 \\ y + x &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} x^2 + y^2 &= x^3 \\ y + x &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} x &= y \\ -x &= y \end{aligned}\right\} \qquad \left.\begin{aligned} x^3 &= 0 \\ x &= y \\ -x &= y \end{aligned}\right\}$$

56. De los siguientes sistemas en dos incógnitas con coeficientes racionales, determinar los que son equivalentes:

$$\left.\begin{matrix} xy - x = 1 \\ x^2 + y^2 = 1 \end{matrix}\right\} \qquad \left.\begin{matrix} x(y-1) = 1 \\ x^4 + 2x + 1 = 0 \end{matrix}\right\} \qquad \left.\begin{matrix} xy - x = 1 \\ y^4 - 2y^3 + 2y = 0 \end{matrix}\right\}$$

57. Considérese en $\mathbb{C}[x, y]$ el ideal $\mathfrak{a} = \big(xy,\, (x+y)^2 - x\big)$. Determinar si están en $\mathfrak{a}$ los siguientes polinomios: $x,\ y,\ (x-y)^2 - x,\ (x-y)^2,\ x^2 - x,\ x^2 - xy$.

58. Sean a, b elementos de un anillo A. Si a es múltiplo de ab en A, ¿se sigue necesariamente que b es invertible en A? (*Indicación:* Considerar en el anillo cociente $\mathbb{Z}[x, y, z]/(x - xyz)$ los elementos $a = \bar{x}$, $b = \bar{y}$.)

59. Demostrar las siguiente igualdades:

$$\begin{gathered} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \vartriangle C) = (A \cap B) \vartriangle (A \cap C) \\ (A \vartriangle B) - C = (A - C) \vartriangle (B - C) \\ (A \cap B) \cup (B \cap C) \cup (C \cap A) = (A \cup B) \cap (B \cup C) \cap (C \cup A) \end{gathered}$$

60. Demostrar que las siguientes condiciones son equivalentes:

    (a) $A \vartriangle (B \cap C) = (A \vartriangle B) \cap (A \vartriangle C)$

    (b) $A \cap B = A \cap C$

    (c) $A \vartriangle (B \cup C) = (A \vartriangle B) \cup (A \vartriangle C)$

61. ¿Cómo ha de ser un subconjunto $A \subseteq X$ para que $A \cup (B \vartriangle C) = (A \cup B) \vartriangle (A \cup C)$ para cualesquiera subconjuntos $B, C \subseteq X$?

62. Se dice que un anillo A es de **Boole** (1815-1864) cuando $a^2 = a$ para todo $a \in A$. En tal caso, probar que $2a = 0$, que todo ideal primo $\mathfrak{p}$ de A es maximal y que $A/\mathfrak{p} = \mathbb{F}_2$.

Anillos Euclídeos

(*) Sea $\omega = (-1+\sqrt{3}i)/2$, que es una raíz cúbica primitiva de la unidad. Veamos que el anillo $\mathbb{Z}[\omega] = \{a+b\omega\colon\ a,b\in\mathbb{Z}\}$ es euclídeo. Para probarlo definimos

$$\delta(z) = z\cdot\bar{z} = |z|^2 = (a+b\omega)(a+b\bar{\omega}) = a^2-ab+b^2 \in \mathbb{N}\ ,$$

y la comprobación de que el anillo $\mathbb{Z}[\omega]$ es euclídeo es análoga a la dada para $\mathbb{Z}[\,i\,]$, pues de nuevo todo número complejo dista menos de la unidad de algún elemento de $\mathbb{Z}[\omega]$.

(*) Vamos a calcular el máximo común divisor, en el anillo euclídeo $\mathbb{F}_5[x]$, de los polinomios $p(x) = x^4+2x^3-x^2+2x+2$ y $q(x) = 2x^2-1$, aplicando el algoritmo de Euclides (325?-265? a. de Cristo):

$$\begin{aligned} p(x) &= q(x)(3x^2+x+1)+(3x-2)\\ q(x) &= (3x-2)(4x+1)+1 \end{aligned}$$

Luego $p(x)$ y $q(x)$ son primos entre sí, y la Identidad de Bézout (1730-1783) es

$$\begin{aligned} 1 &= q(x)-(4x+1)(3x-2) = q(x)-(4x+1)\big(p(x)-q(x)(3x^2+x+1)\big)\\ &= (x-1)\cdot p(x)+(2x^3+2x^2+2)\cdot q(x) \end{aligned}$$

(*) Para calcular el máximo común divisor de $5+5i$ y $3+6i$ en el anillo euclídeo $\mathbb{Z}[\,i\,]$, dividimos $5+5i$ por $3+6i$. Como

$$\frac{5+5i}{3+6i} = \frac{(5+5i)(3-6i)}{45} = \frac{1-i}{3}$$

dista menos de la unidad de los enteros de Gauss 1 y $1-i$, el cociente de tal división es 1 ó $1-i$. Si elegimos 1, el resto es $5+5i-(3+6i) = 2-i$. Dividiendo ahora $3+6i$ por $2-i$ obtenemos que $3+6i = (3i)(2-i)$ y el resto es nulo. Luego el máximo común divisor de $5+5i$ y $3+6i$ en $\mathbb{Z}[\,i\,]$ es $2-i$.

(*) Clases de Restos de Polinomios:

Sea $p(x) = x^n+c_1x^{n-1}+\ldots+c_n$ un polinomio con coeficientes en un cuerpo k. Para determinar si un polinomio $q(x)\in k[x]$ es múltiplo de $p(x)$ no es necesario efectuar la división de $q(x)$ por $p(x)$, que suele ser laboriosa. Basta calcular la imagen $[q(x)]$ de $q(x)$ en el anillo cociente $K = k[x]/\big(p(x)\big)$, pues la condición de que $q(x)$ sea múltiplo de $p(x)$ equivale a que la clase de restos de $q(x)$ módulo $p(x)$ sea nula. Sea $\alpha = [x]$ y denotemos c la clase $[c]$ de cualquier constante $c\in k$. Para calcular $[q(x)] = q([x]) = q(\alpha)$ utilizamos reiteradamente la relación

$$\alpha^n \ = \ -(c_1\alpha^{n-1}+\ldots+c_{n-1}\alpha+c_n)$$

que nos permite expresar las sucesivas potencias α^m, $m \geq n$, como combinaciones lineales de 1, α, ..., α^{n-1} con coeficientes en k. Obtendremos así que

$$[q(x)] = [a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}]$$

donde $a_i \in k$, de modo que $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ es precisamente el resto de la división de $q(x)$ por $p(x)$ y su anulación significa que $p(x)$ divide a $q(x)$.

Del lema de Euclides se sigue que K es un cuerpo precisamente cuando el polinomio $p(x)$ es irreducible en $k[x]$. En tal caso, el inverso de cualquier elemento no nulo $\sum_i a_i\alpha^i$ puede calcularse mediante la Identidad de Bézout: Como $a(x) = \sum_i a_i x^i$ no es múltiplo de $p(x)$ y $p(x)$ es irreducible en $k[x]$, el máximo común divisor de $p(x)$ y $a(x)$ en $k[x]$ es 1; luego $1 = a(x)b(x) + p(x)q(x)$ para ciertos polinomios $b(x), q(x) \in k[x]$ y concluimos que $1 = a(\alpha)b(\alpha)$ en K. Es decir, $b(\alpha)$ es el inverso de $a(\alpha)$ en el cuerpo K.

(*) Consideremos los polinomios $p(x) = x^2 + x + 1$, $q(x) = x^6 + x^4 + x^3 + x + 1$ con coeficientes en el cuerpo $\mathbb{F}_2$. Para averiguar si $q(x)$ es múltiplo de $p(x)$ calculamos las potencias necesarias de $\alpha = [x]$ en el anillo $\mathbb{F}_2[x]/\big(p(x)\big)$, partiendo de la relación $\alpha^2 = -\alpha - 1 = \alpha + 1$:

$$\begin{aligned}
\alpha^3 &= \alpha^2 + \alpha = 2\alpha + 1 = 1 \\
\alpha^4 &= \alpha \\
\alpha^6 &= \alpha^3 = 1
\end{aligned}$$

Ahora $[q(x)] = q(\alpha) = \alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 1 + \alpha + 1 + \alpha + 1 = 2\alpha + 3 = 1$ y concluimos que $q(x)$ no es múltiplo de $p(x)$, pues el resto de la división es 1.

(*) Sumas de Dos Cuadrados Perfectos:

La posibilidad de descomponer un número natural n en suma de dos cuadrados perfectos está relacionada con el anillo de los enteros de Gauss $\mathbb{Z}[\,i\,]$ porque la condición $n = a^2 + b^2$ equivale a que $n = (a + bi)(a - bi)$ descomponga en producto de un entero de Gauss por su conjugado. Ahora, en virtud del teorema de descomposición en factores irreducibles en el anillo euclídeo $\mathbb{Z}[\,i\,]$, hemos de descomponer primero n en producto de enteros de Gauss irreducibles y estudiar luego la posibilidad de agrupar los factores de modo que se obtenga un entero de Gauss (1777-1855) y su conjugado.

En cuanto al primer paso, descomponiendo n en producto de números primos, basta saber efectuar la descomposición de los números primos. Ahora bien, si un número primo p es suma de dos cuadrados perfectos, $p = a^2 + b^2 = (a + bi)(a - bi)$, entonces no es irreducible en $\mathbb{Z}[\,i\,]$, y ambos factores $a + bi$ y $a - bi$ son irreducibles porque su norma es un número primo. Recíprocamente, si un número primo p no es irreducible en $\mathbb{Z}[\,i\,]$, $p = (a + bi)(c + di)$, tomando normas obtenemos que $p^2 = (a^2 + b^2)(c^2 + d^2)$; luego $p = a^2 + b^2$ es suma de dos cuadrados perfectos.

Por ejemplo, para descomponer 14625 en suma de dos cuadrados perfectos de todas las formas posibles, hallamos primero su descomposición en producto de enteros de Gauss irreducibles, para lo cual lo descomponemos en producto de números primos y luego cada factor primo que sea suma de dos cuadrados perfectos se descompone en producto de dos enteros de Gauss irreducibles:

$$14625 = 3^2 \cdot 5^3 \cdot 13 = 3^2(2+i)^3(2-i)^3(3+2i)(3-2i)$$

Ahora ponemos 14625 como producto de un entero de Gauss por su conjugado:

$$3(2+i)^3(3+2i)\cdot 3(2-i)^3(3-2i) = (-48+111i)(-48-111i) = 48^2+111^2$$
$$3(2+i)^3(3-2i)\cdot 3(2-i)^3(3+2i) = (84+87i)(84-87i) = 84^2+87^2$$
$$3(2+i)^2(2-i)(3+2i)\cdot 3(2-i)^2(2+i)(3-2i) = 60^2+105^2$$
$$3(2+i)^2(2-i)(3-2i)\cdot 3(2-i)^2(2+i)(3+2i) = 120^2+15^2$$

Para aplicar este algoritmo conviene disponer de un criterio para saber cuándo un número primo p es irreducible en $\mathbb{Z}[\,i\,]$.

Veamos que *un número primo p no descompone en suma de dos cuadrados perfectos (i.e., es irreducible en $\mathbb{Z}[\,i\,]$) precisamente cuando $p \equiv 3$* (módulo 4):

En efecto, si p es suma de dos cuadrados perfectos, $p = a^2 + b^2$, entonces $a^2, b^2 \equiv 0, 1$ (mód. 4) y concluimos que p no es congruente con 3 módulo 4.

Recíprocamente, si $p \equiv 0, 1, 2$ (mód. 4), entonces el caso $p \equiv 0$ es imposible porque p es primo, el caso $p \equiv 2$ implica que $p = 2 = 1^2 + 1^2$ es suma de dos cuadrados, y en el caso $p \equiv 1$ tenemos que -1 es resto cuadrático módulo p de acuerdo con 3.6.3. Luego existen números enteros n, c tales que $cp = n^2 + 1 = (n+i)(n-i)$. Si p fuera irreducible en $\mathbb{Z}[\,i\,]$, por el lema de Euclides tendríamos $n \pm i = p(a+bi)$ para algún entero de Gauss $a+bi$, lo que es contradictorio, y concluimos que también en este caso p es suma de dos cuadrados perfectos.

En resumen, *la condición necesaria y suficiente para que un número natural sea suma de dos cuadrados perfectos es que al descomponerlo en producto de números primos sean pares los exponentes de los primos congruentes con 3 módulo 4.*

(*) Operadores: Sea $T\colon E \to E$ un endomorfismo de un k-espacio vectorial (usualmente de dimensión infinita). Si $p(x) = a_0x^d + a_1x^{d-1} + \ldots + a_d$ es un polinomio con coeficientes en k, pondremos $p(T) := a_0T^d + a_1T^{d-1} + \ldots + a_d\mathrm{I}$, donde I es la identidad. Cuando dos polinomios $p(x), q(x) \in k[x]$ son primos entre sí, la identidad de Bézout $1 = a(x)p(x) + b(x)q(x)$ muestra que tenemos

$$e = a(T)p(T)e + b(T)q(T)e$$

para todo $e \in E$; luego $0 = \operatorname{Ker} p(T) \cap \operatorname{Ker} q(T)$. Además, $a(T)p(T)e \in \operatorname{Ker} q(T)$ y $b(T)q(T)e \in \operatorname{Ker} p(T)$ cuando $e \in \operatorname{Ker} p(T)q(T)$, así que

$$\boxed{\operatorname{Ker} p(T)q(T) = \operatorname{Ker} p(T) \oplus \operatorname{Ker} q(T)} \qquad \text{m.c.d.}\big(p(x), q(x)\big) = 1$$

Por ejemplo, las sucesiones de Fibonacci (1170–1250) son las sucesiones (y_n) tales que cada término es la suma de los dos anteriores: $y_{n+2} = y_{n+1} + y_n$. Para resolver esta ecuación en diferencias finitas introducimos el $\mathbb{C}$-espacio vectorial E de todas las sucesiones de números complejos y consideramos el operador "siguiente" $\nabla\colon E \to E$, $\nabla(y_n) := (y_{n+1})$. Ahora nuestra ecuación es

$$(\nabla^2 - \nabla - 1)(x_n) = 0\ .$$

Si $x^2 - x - 1 = (x - \alpha)(x - \beta)$, la igualdad

$$\operatorname{Ker}(\nabla^2 - \nabla - 1) = \operatorname{Ker}(\nabla - \alpha) \oplus \operatorname{Ker}(\nabla - \beta)$$

afirma que cada sucesión de Fibonacci (x_n) descompone, y de modo único, en suma de una progresión geométrica de razón α y otra de razón β:

$$x_n = \lambda \left(\frac{1+\sqrt{5}}{2}\right)^n + \mu \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Vemos así que, cuando las raíces del polinomio $p(x) = x^d + a_1 x^{d-1} + \ldots + a_d$ son simples, $p(x) = (x - \alpha_1)\ldots(x - \alpha_d)$, las soluciones de la ecuación homogénea $y_{n+d} + a_1 y_{n+d-1} + \ldots + a_d y_n = 0$ descomponen en suma de progresiones geométricas de razones $\alpha_1, \ldots, \alpha_d$. En el caso general, cuando $p(x)$ tenga raíces múltiples, la ecuación se reduce al cálculo del núcleo de los operadores $(\nabla - \alpha)^r$. No trataremos este caso; pero diremos que tal núcleo está generado por las sucesiones (α^n), $(n\alpha^n), \ldots, (n^{r-1}\alpha^n)$.

Por otra parte, si E denota el $\mathbb{C}$-espacio vectorial de las funciones complejas de variable real y clase $\mathcal{C}^\infty$, y consideramos el operador "derivada" $D\colon E \to E$, $Df(t) = f'(t)$, tenemos que las soluciones de la ecuación $(D - \alpha)y = 0$ son las funciones $y(t) = \lambda e^{\alpha t}$, donde $\alpha, \lambda \in \mathbb{C}$. En efecto, si $y'(t) = \alpha y(t)$, es inmediato comprobar que $D(y(t)e^{-\alpha t}) = 0$. Vemos así que, cuando las raíces del polinomio $p(x) = x^d + a_1 x^{d-1} + \ldots + a_d$ son simples, $p(x) = (x - \alpha_1)\ldots(x - \alpha_d)$, las soluciones de la ecuación diferencial lineal $y^{(n+d} + \ldots + a_{d-1}y' + a_d y = 0$ son combinaciones lineales con coeficientes complejos $y(t) = \lambda_1 e^{\alpha_1 t} + \ldots + \lambda_d e^{\alpha_d t}$.

En el caso general, cuando $p(x)$ tenga raíces múltiples, la ecuación se reduce al cálculo del núcleo de los operadores $(D - \alpha)^r$. Tampoco trataremos este caso; pero diremos que tal núcleo está generado por las funciones $e^{\alpha t}$, $te^{\alpha t}, \ldots, t^{r-1}e^{\alpha t}$.

(*) Extensiones:

1. El morfismo natural $\mathbb{Q} \to \mathbb{R}$ es una extensión infinita, porque todo espacio vectorial de dimensión finita sobre $\mathbb{Q}$ es de cardinal numerable, mientras que el cardinal de $\mathbb{R}$ no es numerable.

2. El morfismo natural $\mathbb{R} \to \mathbb{C}$ es una extensión finita de grado 2, porque una base de $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$ es $\{1, i\}$.

3. Si k es un cuerpo, la identidad $k \to k$ es una extensión de grado 1, y toda extensión de k de grado 1 es isomorfa a esta extensión trivial.

4. Si k es un cuerpo y $k(t)$ es el cuerpo de las fracciones racionales en una indeterminada t con coeficientes en k, el morfismo natural $k \to k(t)$ es una extensión infinita, porque las potencias de t forman una familia infinita linealmente independiente sobre k.

5. Si $\alpha \in \mathbb{C}$, el menor subanillo de $\mathbb{C}$ que es cuerpo y contiene a $\mathbb{Q}$ y a α es

$$\mathbb{Q}(\alpha) = \{p(\alpha)/q(\alpha)\colon\ p(x),\, q(x) \in \mathbb{Q}[x],\ q(\alpha) \neq 0\}$$

   Como $\mathbb{Q}(\alpha)$ es un cuerpo que contiene a $\mathbb{Q}$, la inclusión $\mathbb{Q} \to \mathbb{Q}(\alpha)$ es una extensión de $\mathbb{Q}$. Por definición, la extensión $\mathbb{Q}(\alpha)$ está formada por todos los números complejos que puedan obtenerse a partir de α y de números racionales con un número finito de sumas, restas, productos y cocientes.

6. Si $p(x)$ es un polinomio irreducible con coeficientes en un cuerpo k, los múltiplos de $p(x)$ en $k[x]$ forman un ideal maximal; luego $k[x]/(p(x))$ es un cuerpo y el morfismo natural $k \to k[x]/(p(x))$, $c \mapsto [c]$, es una extensión de k.

7. Si K es un cuerpo de característica 0, entonces existe un único morfismo de anillos $\mathbb{Q} \to K$ (porque el único morfismo de anillos $\mathbb{Z} \to K$ es inyectivo), de modo que todo cuerpo de característica 0 es una extensión de $\mathbb{Q}$. Esta propiedad universal caracteriza al cuerpo $\mathbb{Q}$, lo que nos da una nueva y más profunda definición de la suma y producto de números racionales: *Son las únicas operaciones que definen una estructura de cuerpo de característica 0 que admite un único morfismo de anillos en cualquier otro cuerpo de característica nula.*

8. Si K es un cuerpo de característica positiva p, entonces $p\mathbb{Z}$ es el núcleo del único morfismo de anillos $\mathbb{Z} \to K$. Luego éste morfismo induce un morfismo de anillos $\mathbb{F}_p \to K$ y vemos así que K es una extensión de $\mathbb{F}_p$.

(*) Consideremos el polinomio $p(x) = x^4 + 2x^3 + 5x^2 + 4x + 4$ con coeficientes racionales. Para hallar sus raíces múltiples calculamos el máximo común divisor de $p(x)$ y su derivada $p'(x)$ mediante el algoritmo de Euclides:

$$p(x) = \left(\frac{x}{4} + \frac{1}{8}\right)(4x^3 + 6x^2 + 10x + 4) + \frac{7}{4}(x^2 + x + 2)$$
$$p'(x) = 4x^3 + 6x^2 + 10x + 4 = (4x + 2)(x^2 + x + 2) + 0$$

Obtenemos que el máximo común divisor de $p(x)$ y $p'(x)$ es $x^2 + x + 2$; luego las raíces múltiples de $p(x)$ son precisamente las raíces del polinomio $x^2 + x + 2$.

(*) Consideremos el polinomio $p(x) = x^6 + x^2 + x$ con coeficientes en el cuerpo $\mathbb{F}_3$. De acuerdo con 4.3.2, la raíz $x = 1$ es múltiple, porque $p'(x) = -x + 1$. De hecho es una raíz doble: $p(x) = (x-1)^2(x^4 - x^3 + x)$.

(*) En el caso de un polinomio $ax^2 + bx + c$ de grado 2, de raíces α_1, α_2, las fórmulas de Cardano son

$$\begin{aligned} -b/a &= \alpha_1 + \alpha_2 \\ c/a &= \alpha_1\alpha_2 \end{aligned}$$

y, en el caso de un polinomio unitario $x^3 + px^2 + qx + r$ de grado 3, de raíces α_1, α_2, α_3, las fórmulas de Cardano son

$$\begin{aligned} -p &= \alpha_1 + \alpha_2 + \alpha_3 \\ q &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \\ -r &= \alpha_1\alpha_2\alpha_3 \end{aligned}$$

(*) Sea p un número primo y sea d un divisor de $p-1$. Veamos que la condición necesaria y suficiente para que un número entero n primo con p sea resto d-ésimo módulo p es que $n^{(p-1)/d} \equiv 1$ (mód. p).

Si $[n] = a^d$ para algún $a \in \mathbb{F}_p$, entonces $a \neq 0$ y $[n^{(p-1)/d}] = a^{p-1} = 1$ según la congruencia de Fermat. Recíprocamente, si $n^{(p-1)/d} \equiv 1$ (mód. p) y α es una raíz del polinomio $x^d - [n]$ en una extensión finita de $\mathbb{F}_p$ (que existe en virtud del Teorema de Kronecker), $\alpha^{p-1} = [n^{(p-1)/d}] = 1$. Luego α es una raíz de $x^{p-1} - 1$, que tiene todas sus raíces en $\mathbb{F}_p$ según la congruencia de Fermat, así que $\alpha \in \mathbb{F}_p$. Como $[n] = \alpha^d$, concluimos que n es resto d-ésimo módulo p.

(*) Sea p un número primo y sea k el cuerpo de las fracciones racionales en una indeterminada t con coeficientes en $\mathbb{F}_p$. Consideremos el polinomio $p(x) = x^p - t$ con coeficientes en k. Este polinomio no tiene raíces en k: si $a(t)/b(t) \in k$ fuera una raíz, donde $a(t)$, $b(t) \in \mathbb{F}_p[t]$ pueden elegirse sin factores irreducibles comunes, tendríamos $a(t)^p = b(t)^p t$, luego $a(t)$ sería múltiplo de t, $a(t)^p$ múltiplo de t^p, $b(t)^p$ múltiplo de t y $b(t)$ múltiplo de t, contra el hecho de que $a(t)$ y $b(t)$ no tienen factores irreducibles comunes.

Veamos que $p(x) = x^p - t$ es irreducible en $k[x]$. En virtud del teorema de Kronecker, $p(x)$ tiene una raíz α en alguna extensión K de k. Como $\alpha^p = t$, tenemos que $x^p - t = (x-\alpha)^p$ en $K[x]$. Si $p(x)$ tuviera en $k[x]$ algún factor no constante $q(x)$ de grado menor que p, que podemos suponer unitario, en $K[x]$ se tendría $q(x) = (x-\alpha)^i$ para algún $1 \leq i \leq p-1$. Como $(x-\alpha)^i = x^i - i\alpha x^{i-1} + \ldots$, se seguiría que $i\alpha \in k$ y, al ser $i \neq 0$ en k, concluiríamos que $\alpha \in k$ y $p(x)$ tendría una raíz en k. Por tanto $p(x)$ es irreducible en $k[x]$ y, al ser $p'(x) = 0$, todas las raíces de $x^p - t$ son múltiples. De hecho $x^p - t$ tiene una única raíz de multiplicidad p, pues si α es una raíz de $x^p - t$, entonces $x^p - t = (x-\alpha)^p$ según 4.3.9.

(*) Veamos que el polinomio $xy+x+y$ no pertenece al ideal (x^2+x-y, x^2y-y^2-1) del anillo $\mathbb{Q}[x,y]$. Una solución del sistema de ecuaciones

$$\left.\begin{array}{r} x^2+x=y \\ x^2y-y^2=1 \end{array}\right\}$$

es $x=\alpha$, $y=\alpha^2+\alpha$, donde α es una raíz de x^3+x^2+1, así que bastará comprobar que no es solución de la ecuación $xy+x+y=0$.

Consideremos la raíz $\alpha=[x]$ (mód. x^3+x^2+1) que nos proporciona el teorema de Kronecker, de modo que 1, α, α^2 son linealmente independientes sobre $\mathbb{Q}$:

$$\begin{aligned}\alpha(\alpha^2+\alpha)+\alpha+(\alpha^2+\alpha)&=\alpha^3+2\alpha^2+2\alpha= \\ &=(-\alpha^2-1)+2\alpha^2+2\alpha=\alpha^2+2\alpha-1\neq 0\end{aligned}$$

(*) Elementos Algebraicos:

1. Todos los elementos de un cuerpo k son algebraicos sobre k, pues $c\in k$ es obviamente raíz del polinomio $x-c\in k[x]$.

2. Las raíces de cualquier polinomio no nulo con coeficientes en k son elementos algebraicos sobre k.

3. Las raíces n-ésimas de la unidad $e^{\frac{2\pi i}{n}k}$ son algebraicas sobre $\mathbb{Q}$.

4. El número real π es trascendente sobre $\mathbb{Q}$ (*teorema de Lindemann* 1852-1939) y el número real e también es trascendente sobre $\mathbb{Q}$; pero en este libro no daremos demostraciones de estos resultados.

5. Es sencillo comprobar que el cardinal del conjunto de los números reales algebraicos sobre $\mathbb{Q}$ es numerable, porque lo es el cardinal de $\mathbb{Q}[x]$ y cada polinomio con coeficientes racionales tiene a lo sumo un número finito de raíces reales. Como el cardinal de $\mathbb{R}$ no es numerable, se concluye que el cardinal del conjunto de los números reales trascendentes sobre $\mathbb{Q}$ no es numerable.

6. $\sqrt[n]{2}$ es raíz del polinomio x^n-2, que es irreducible en $\mathbb{Q}[x]$ según el criterio de Eisenstein. Luego el polinomio irreducible de $\sqrt[n]{2}$ sobre $\mathbb{Q}$ es x^n-2.

7. Sea p un número primo. El polinomio $(x^p-1)/(x-1)=x^{p-1}+\ldots+x+1$ es irreducible en $\mathbb{Q}[x]$ según 5.5.3 y admite la raíz $x=e^{\frac{2\pi i}{p}}$; luego es el polinomio irreducible de $e^{\frac{2\pi i}{p}}$ sobre $\mathbb{Q}$.

8. Sea α el número real $\sqrt{2}-\sqrt{3}$. Como tenemos que

$$\begin{aligned}2&=(\alpha+\sqrt{3})^2=\alpha^2+2\sqrt{3}\alpha+3 \\ 0&=(\alpha^2+2\sqrt{3}\alpha+1)(\alpha^2-2\sqrt{3}\alpha+1)=\alpha^4-10\alpha^2+1\end{aligned}$$

α es raíz del polinomio $p(x) = x^4 - 10x^2 + 1$ y $p(x)$ es múltiplo del polinomio irreducible $p_\alpha(x)$ de α sobre $\mathbb{Q}$. Es sencillo comprobar que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y que el grado de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$ es 2. Del teorema del grado se sigue que el grado de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ es 4, luego el grado de $p_\alpha(x)$ es 4 y tenemos que $p_\alpha(x) = p(x)$. En particular $p(x)$ es irreducible en $\mathbb{Q}[x]$.

9. El concepto de elemento algebraico o trascendente depende del cuerpo base k considerado. Por ejemplo, todos los números complejos son algebraicos sobre $\mathbb{R}$ aunque muchos sean trascendentes sobre $\mathbb{Q}$.

(*) Teorema de Galois:

El Teorema de Kronecker (1823-1891) permite dar una presentación elemental del teorema de Galois (1811-1832), al menos para cualquier cuerpo k de característica nula, hipótesis que mantendremos en todo este apartado.

Dadas dos extensiones $k \to K$, $k \to L$ de un mismo cuerpo base k y un morfismo de k-álgebras $\tau\colon K \to L$, si $\alpha \in K$ es raíz de un polinomio $\sum_i a_i x^i$ con coeficientes en k, entonces $\tau(\alpha)$ es raíz del mismo polinomio porque $\tau(a_i) = a_i$:

$$0 = \tau\Big(\textstyle\sum_i a_i \alpha^i\Big) = \sum_i \tau(a_i)(\tau\alpha)^i = \sum_i a_i(\tau\alpha)^i \ .$$

Dado un polinomio no constante $p(x) \in k[x]$, diremos que una extensión finita $k \to L$ es un **cuerpo de descomposición** de $p(x)$ sobre k si $p(x)$ tiene todas sus raíces en L y éstas generan L sobre k. Es decir:

$$L = k(\alpha_1, \ldots, \alpha_n) \quad , \qquad p(x) = (x - \alpha_1) \ldots (x - \alpha_n)$$

Tal extensión siempre existe, pues basta considerar la extensión generada por las raíces de $p(x)$ en una extensión donde tenga todas sus raíces. Por ejemplo, cuando $k = \mathbb{Q}$, el cuerpo de descomposición de un polinomio $p(x)$ es la extensión generada por todas las raíces complejas de $p(x)$. Una propiedad fundamental del cuerpo de descomposición es que *si un polinomio irreducible $q(x)$ con coeficientes en k admite una raíz $\alpha = r(\alpha_1, \ldots, \alpha_n)$ en L, entonces tiene todas sus raíces en L,* porque divide al polinomio

$$\prod_{\sigma \in S_n} \big(x - r(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})\big)$$

ya que éste tiene coeficientes en k, pues son funciones simétricas de $\alpha_1, \ldots, \alpha_n$, (véase el apéndice A) y admite la raíz α; luego es múltiplo de $q(x)$ por 4.4.2.

Llamaremos **grupo de Galois** de $p(x)$ sobre k al grupo de los automorfismos de k-álgebras de su cuerpo de descomposición. La definición tiene sentido porque el cuerpo de descomposición es único salvo isomorfismos:

(1) *Si L y L' son dos cuerpos de descomposición de $p(x)$ sobre k, entonces existe algún isomorfismo de k-álgebras $L \simeq L'$.*

Procedemos por inducción sobre el grado $[L : k]$. Si $k = L$, entonces $p(x)$ tiene todas sus raíces en k y, como la extensión L' está generada por raíces de $p(x)$, concluimos que $L' = k$.

Si $k \neq L$, consideramos un factor irreducible $q(x)$ de $p(x)$ de grado > 1 y sendas raíces $\alpha \in L$, $\alpha' \in L'$ de $q(x)$. Por el Teorema de Kronecker existe un isomorfismo $k(\alpha) \simeq k(\alpha')$. La extensión $k(\alpha) \simeq k(\alpha') \to L'$ es un cuerpo de descomposición de $p(x)$ sobre $k(\alpha)$. Como también lo es L y $[L : k(\alpha)] < [L : k]$, por hipótesis de inducción existe un isomorfismo de $k(\alpha)$-álgebras $L \simeq L'$, que también es un isomorfismo de k-álgebras.

Aplicando este mismo razonamiento al caso en que $L' = L$ y α, α' son dos raíces de un mismo polinomio irreducible con coeficientes en k, obtenemos que

(2) *Si un polinomio irreducible $q(x)$ con coeficientes en k tiene una raíz $\alpha \in L$ (y por tanto $q(x)$ tiene todas sus raíces en L), entonces el grupo de Galois G actúa transitivamente sobre las raíces de $q(x)$ en L (i.e., si $\beta \in L$ es otra raíz de $q(x)$, entonces $\beta = \sigma(\alpha)$ para algún $\sigma \in G$).*

Ahora bien, como la característica de k es nula, todas las raíces de $q(x)$ son simples (4.3.5), y al transformar α con el grupo de Galois G obtenemos tantos elementos distintos como el grado de $q(x)$. Luego

$$|G| = |H| \cdot \operatorname{gr} q(x) = |H| \cdot [k(\alpha) : k]$$

donde $H = \{\tau \in G\colon\ \tau(\alpha) = \alpha\}$ es el grupo de Galois de $p(x)$ sobre $k(\alpha)$. Procediendo por inducción sobre el grado del cuerpo de descomposición obtenemos que *el orden del grupo de Galois es el grado del cuerpo de descomposición:*

$$|G| \ = \ [L : k] \ .$$

(3) Teorema de Galois: *Sea L el cuerpo de descomposición sobre k de un polinomio $p(x) \in k[x]$, y sea G su grupo de Galois. Si a cada subgrupo H de G le asignamos el cuerpo intermedio $L^H := \{\alpha \in L\colon \tau(\alpha) = \alpha, \forall \tau \in H\}$, obtenemos una biyección*

$$\begin{bmatrix}\text{Subgrupos}\\ \text{de } G\end{bmatrix} \longrightarrow \begin{bmatrix}\text{Cuerpos intermedios}\\ \text{entre } k \text{ y } L\end{bmatrix}$$

que invierte inclusiones. La biyección inversa asigna a cada cuerpo intermedio L' el subgrupo $\operatorname{Aut}(L/L') := \{\tau \in G\colon \tau(\alpha) = \alpha, \forall \alpha \in L'\}$. Además $|H| = [L : L^H]$.

Demostración: Si L' es un cuerpo intermedio, entonces L es el cuerpo de descomposición de $p(x)$ sobre L' y $H = \operatorname{Aut}(L/L')$ es el grupo de Galois de $p(x)$ sobre L'. Por tanto, si $\alpha \in L^H$, se sigue del punto 2 que el polinomio irreducible de α sobre L' tiene una única raíz; luego es de grado 1 por 4.3.5 y concluimos que $\alpha \in L'$. Es decir, $L' = L^H$. Además, por el punto 2 tenemos que

$$|H| \ = \ [L : L'] \ = \ [L : L^H] \ .$$

Por otra parte, sea H un subgrupo de G y sea $\sigma \in \mathrm{Aut}(L/L^H)$. Si $\alpha \in L$, el polinomio

$$q_\alpha(x) := \textstyle\prod_{\tau\in H}\big(x - \tau(\alpha)\big)$$

tiene sus coeficientes en L^H, así que son invariantes por σ, y $\sigma(\alpha)$ es una raíz de $q_\alpha(x)$. Luego $\sigma(\alpha) = \tau(\alpha)$ para algún $\tau \in H$:

$$L = \textstyle\bigcup_{\tau\in H} \mathrm{Ker}\,(\sigma - \tau)\ .$$

Como el cuerpo k es infinito, porque $\mathrm{car}\, k = 0$, ningún k-espacio vectorial es unión finita de subespacios vectoriales propios (G.4.2), así que $\mathrm{Ker}\,(\sigma - \tau) = L$ para algún $\tau \in G$; es decir, $\sigma = \tau \in H$ y concluimos que $H = \mathrm{Aut}(L/L^H)$.

(*) Eliminación:

La teoría de la Eliminación permite resolver múltiples problemas. Veamos algunos ejemplos:

(1) Para hallar todas las soluciones racionales del sistema de ecuaciones

$$\begin{cases} 4 = 2x^2y + 2xy^2 - 4xy + x^2 + y^3 \\ 0 = 2x^2 + y^2 + 2xy - 5x + 2 \end{cases}$$

eliminamos x, para lo que formamos la resultante

$$\begin{vmatrix} 2y+1 & 2y^2-4y & y^3-4 & 0 \\ 0 & 2y+1 & 2y^2-4y & y^3-4 \\ 2 & 2y-5 & y^2+2 & 0 \\ 0 & 2 & 2y-5 & y^2+2 \end{vmatrix} = y^4 + 13y^3 + 56y^2 + 80y$$

Las raíces racionales no nulas de este polinomio dividen a 80. Por comprobación directa vemos que las raíces racionales de la resultante son $y = 0, -4, -5$.

Sustituyendo $y = 0$ en el sistema inicial obtenemos $x^2 = 4$, $2x^2 - 5x + 2 = 0$, que sólo tienen en común la raíz $x = 2$.

Sustituyendo $y = -4$ obtenemos $-7x^2 + 48x - 64 = 4$, $2x^2 - 13x + 18 = 0$, que sólo tienen en común la raíz $x = 2$.

Sustituyendo $y = -5$ obtenemos $-9x^2 + 70x - 125 = 4$, $2x^2 - 15x + 27 = 0$, que sólo tienen en común la raíz $x = 3$.

Concluimos que las soluciones racionales del sistema son $(2, 0), (2, -4), (3, -5)$.

(2) Dado un polinomio de grado 5 con coeficientes racionales, la determinación de sus factores de grado 2 puede hacerse resolviendo un sistema de 2 ecuaciones algebraicas con dos incógnitas, lo que nos permite descomponer el polinomio dado

en factores irreducibles. Por ejemplo, el polinomio $x^5+x^4+x^3-1$ no tiene factores de grado 1 en $\mathbb{Q}[x]$ porque no tiene raíces racionales. Para hallar los posibles factores de grado 2

$$x^5+x^4+x^3-1=(x^3+ax^2+bx+c)(x^2+(1-a)x-1/c)$$

determinamos las soluciones racionales del sistema

$$\left\{\begin{array}{l} 1=c^{-1}+a(1-a)+b \\ 0=-ac^{-1}+b(1-a)+c \\ 0=-bc^{-1}+c(1-a) \end{array}\right.$$

De la última ecuación obtenemos $b=c^2(1-a)$ y sustituimos en las otras dos

$$\left\{\begin{array}{l} 0=-ca^2+(c-c^3)a+c^3-c+1 \\ 0=c^3a^2-(2c^3+1)a+c^3+c^2 \end{array}\right.$$

Eliminamos a formando la resultante

$$\begin{vmatrix} -c & c-c^3 & c^3-c+1 & 0 \\ 0 & -c & c-c^3 & c^3-c+1 \\ c^3 & -2c^3-1 & c^3+c^2 & 0 \\ 0 & c^3 & -2c^3-1 & c^3+c^2 \end{vmatrix} = c^{11}+c^9+c^8+2c^6+2c^5+c^4+c^2+c$$

cuyas raíces racionales son $c=0$, $c=-1$. Sustituyendo $c=0$ obtenemos $0=-1$, $0=-a$, que no tienen ninguna solución común. Sustituyendo $c=-1$ obtenemos $0=a^2-1$, $0=-a^2+a$, que tienen en común la raíz $a=1$, y de la igualdad $b=c^2(1-a)$ se sigue que $b=0$. El polinomio admite la descomposición

$$x^5+x^4+x^3-1=(x^3+x^2-1)(x^2+1)$$

(3) Dado un polinomio $p(x)\in k[x]$ de raíces $\alpha_1,\ldots,\alpha_n$ y un polinomio $q(x)\in k[x]$, para hallar un polinomio no nulo con coeficientes en k que admita las raíces $q(\alpha_1),\ldots,q(\alpha_n)$ basta eliminar x en el sistema:

$$\left.\begin{array}{l} p(x)=0 \\ q(x)=y \end{array}\right\}$$

Por ejemplo, si α,β,γ son las tres raíces complejas del polinomio $2x^3-3x+1$, un polinomio no nulo con coeficientes racionales que admita las raíces $q(\alpha)$, $q(\beta)$, $q(\gamma)$, donde $q(x)=x^2/(1+x)$, se obtiene eliminando x en el sistema

$$\left.\begin{array}{r} 2x^3-3x+1=0 \\ x^2/(1+x)=y \end{array}\right\} \qquad \left.\begin{array}{r} 2x^3-3x+1=0 \\ (1+x)y-x^2=0 \end{array}\right\}$$

La resultante es

$$\begin{vmatrix} 2 & 0 & -3 & 1 & 0 \\ 0 & 2 & 0 & -3 & 1 \\ -1 & y & y & 0 & 0 \\ 0 & -1 & y & y & 0 \\ 0 & 0 & -1 & y & y \end{vmatrix} = -4y^3 - 18y^2 + 12y - 1$$

(4) Sean α y β raíces de sendos polinomios $p(x)$ y $q(x)$ con coeficientes en un cuerpo k. para hallar un polinomio no nulo con coeficientes en k que admita la raíz $f(\alpha, \beta)$, donde $f(x, y) \in k[x, y]$, basta eliminar x e y en el sistema

$$\left.\begin{aligned} p(x) &= 0 \\ q(y) &= 0 \\ f(x, y) &= z \end{aligned}\right\}$$

Por ejemplo, para calcular un polinomio con coeficientes racionales que tenga la raíz $\sqrt[3]{2} - \omega\sqrt[3]{2}$, donde ω denota una raíz cúbica primitiva de la unidad, eliminamos x e y en el sistema

$$\left.\begin{aligned} x^2 + x + 1 &= 0 \\ y^3 - 2 &= 0 \\ y - xy &= z \end{aligned}\right\}$$

Como $y = z/(1 - x)$, sustituyendo en la segunda ecuación eliminamos y:

$$\left.\begin{aligned} x^2 + x + 1 &= 0 \\ 2x^3 - 6x^2 + 6x + z^3 - 2 &= 0 \end{aligned}\right\}$$

Ahora, para eliminar x, formamos la resultante

$$\begin{vmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 2 & -6 & 6 & z^3 - 2 & 0 \\ 0 & 2 & -6 & 6 & z^3 - 2 \end{vmatrix} = z^6 + 108$$

(*) Racionalización de Expresiones Algebraicas:

Sea α una raíz de un polinomio no constante $p(x)$ con coeficientes en un cuerpo k. Si $q(x) \in k[x]$ y $q(\alpha) \neq 0$, el problema de racionalizar la expresión algebraica $1/q(\alpha)$ es el de hallar un polinomio $b(x) \in k[x]$ tal que $1/q(\alpha) = b(\alpha)$.

Dividiendo $p(x)$ y $q(x)$ por su máximo común divisor, podemos suponer que no tienen factores comunes no constantes y, en tal caso, el algoritmo de Euclides (325?-265? a. de Cristo) permite hallar polinomios $a(x)$, $b(x) \in k[x]$ tales que:

$$1 = a(x)p(x) + b(x)q(x)$$

Sustituyendo ahora x por α concluimos que $1/q(\alpha) = b(\alpha)$, porque $p(\alpha) = 0$.

El hecho de que el inverso de todo elemento no nulo de $k[\alpha]$ ya esté en $k[\alpha]$ significa que $k[\alpha]$ es un cuerpo. Es decir, $k[\alpha] = k(\alpha)$.

Cuando $p(x)$ es irredcible en $k[x]$ y de grado d, según 4.4.2 tenemos que una base de $k(\alpha)$ sobre k es $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Por tanto, para racionalizar $1/q(\alpha)$ basta resolver el siguiente sistema de ecuaciones lineales con d incógnitas $a_0, \ldots, a_{d-1}$:

$$q(\alpha)(a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1}) = 1$$

(1) Por ejemplo, para racionalizar (quitar los radicales del denominador) la expresión $\beta = 1/(\sqrt[3]{4} + 2\sqrt[3]{2} + 2)$, observamos que $\beta = 1/q(\alpha)$, donde $q(x) = x^2 + 2x + 2$ y $\alpha = \sqrt[3]{2}$ es raíz del polinomio $x^3 - 2$, que tiene coeficientes racionales. Mediante el algoritmo de Euclides obtenemos la identidad de Bézout (1730-1783):

$$\begin{aligned} 1 &= \left(\frac{x^2 - x}{2}\right) q(x) - \left(\frac{x+1}{2}\right) p(x) \\ 1 &= \left(\frac{\alpha^2 - \alpha}{2}\right) q(\alpha) \\ \beta &= \frac{1}{q(\alpha)} = \frac{\alpha^2 - \alpha}{2} = \frac{\sqrt[3]{4} - \sqrt[3]{2}}{2} \end{aligned}$$

También podemos resolver el siguiente sistema de ecuaciones lineales:

$$\begin{aligned} 1 &= (2 + 2\alpha + \alpha^2)(a + b\alpha + c\alpha^2) \\ &= (2a + 2b + 4c) + 2(a + b + c)\alpha + (a + 2b + 2c)\alpha^2 \end{aligned}$$

$$\begin{cases} 1 = 2a + 2b + 4c \\ 0 = a + b + c \\ 0 = a + 2b + 2c \end{cases}$$

y obtenemos que $a = 0$, $b = -1/2$, $c = 1/2$. Luego $q(\alpha)^{-1} = (\sqrt[3]{4} - \sqrt[3]{2})/2$.

(2) Otro procedimiento para racionalizar una expresión con radicales consiste en ir eliminando sucesivamente los diferentes radicales. Por ejemplo, para racionalizar $1/(\sqrt[3]{2} + \sqrt[5]{3})$ consideramos primero el cuerpo $k = \mathbb{Q}(\sqrt[5]{3})$ y $\alpha = \sqrt[3]{2}$, de modo que α es raíz del polinomio $x^3 - 2 \in k[x]$ y tenemos que racionalizar $1/q(\alpha)$, donde $q(x) = x + \sqrt[5]{3} \in k[x]$. La Identidad de Bézout para $x^3 - 2$ y $x + \sqrt[5]{3}$ es:

$$\begin{aligned} \sqrt[5]{27} + 2 &= (x^2 - \sqrt[5]{3}x + \sqrt[5]{3})(x + \sqrt[5]{3}) - (x^3 - 2) \\ \frac{1}{\sqrt[3]{2} + \sqrt[5]{3}} &= \frac{1}{\alpha + \sqrt[5]{3}} = \frac{\sqrt[3]{4} - \sqrt[5]{3}\sqrt[3]{2} + \sqrt[5]{3}}{\sqrt[5]{27} + 2} \end{aligned}$$

Para concluir se racionaliza el denominador $1/(\sqrt[5]{27}+2)$:

$$1 = (x+2)\frac{x^4-2x^3+4x^2-8x+16}{59} - \frac{x^5-27}{59}$$
$$\frac{1}{\sqrt[5]{27}+2} = \frac{\sqrt[5]{27^4}-2\sqrt[5]{27^3}+4\sqrt[5]{27^2}-8\sqrt[5]{27}+16}{59}$$

Ejercicios:

1. Sea b un elemento no nulo de un anillo euclídeo A. Probar que $\delta(1) \leq \delta(b)$ y $\delta(1) = \delta(b)$ si y sólo si b es invertible en A.

2. Determinar los elementos invertibles de $\mathbb{Z}$, $\mathbb{Z}[\,i\,]$, $\mathbb{Z}[\omega]$.

3. Demostrar que $\mathbb{Z}[\sqrt{-2}\,]$ es un anillo euclídeo.

4. ¿Es invertible $\sqrt[3]{2}$ en el anillo $\mathbb{Z}[\sqrt[3]{2}\,]$?

5. ¿Es cierto que $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha$ cuando $\alpha = \sqrt{2}/2,\ 2\sqrt{2},\ 2+\sqrt{2},\ \sqrt[3]{2}$?

6. Demostrar que los enteros de Gauss irreducibles son los de la forma $a+bi$ donde su norma a^2+b^2 es un número primo, y los de la forma $\pm p$ ó $\pm pi$ donde p es un número primo que no descompone en suma de dos cuadrados perfectos.

7. Demostrar que dos descomposiciones $n = a^2+b^2 = c^2+d^2$ de un número natural n en suma de dos cuadrados perfectos coinciden (es decir $a^2 = c^2$ ó $a^2 = d^2$) precisamente cuando $a+bi$ difiere de $c+di$ o de $c-di$ en un entero de Gauss invertible.

8. Demostrar que ningún número primo puede descomponerse de dos formas distintas en suma de dos cuadrados perfectos.

9. Hallar las descomposiciones de 1991, 1992, 1993, 157300, 100, 1000 y 11111 en producto de enteros de Gauss (1777-1855) irreducibles. Calcular todas sus descomposiciones en suma de dos cuadrados perfectos.

10. ¿De cuántos modos distintos puede descomponerse 10^n en suma de dos cuadrados perfectos?

    (*Indicación:* $1+i$ y $1-i$ difieren en un entero de Gauss invertible.)

11. Sea $n \geq 2$ un número natural. Si p es un factor primo impar de n^2+1, probar que $(p-1)/2$ es par. Concluir que existen infinitos números primos de la forma $4m+1$.

12. Sean n, m números naturales primos entre sí. Demostrar que todo número primo que divida a $n^2 + m^2$ es suma de dos cuadrados perfectos.

13. Sea d un número impar mayor que 1. Probar que el anillo $\mathbb{Z}[\sqrt{-d}\,]$ no es euclídeo. (*Indicación*: $(1 + \sqrt{-d}\,)(1 - \sqrt{-d}\,)$ es par).

14. Sea $A = \mathbb{Q}[x]/(x^3 - x - 1)$ y $\alpha = [x]$. ¿Es $3\alpha + 1$ el inverso de $\alpha^2 + 2\alpha + 1$ en el anillo A? Hallar el inverso de $\alpha + 2$ en A. ¿Es 2 el cubo de $\alpha + 2$? Calcular un polinomio no nulo $p(x)$ con coeficientes racionales tal que $p(\alpha^2 + 1) = 0$.

15. Sea $K = \mathbb{Q}[x]/(x^2 - 2x - 2)$ y sea $\alpha = [x]$. Probar que K es una extensión de $\mathbb{Q}$ de grado 2 y que $\{1, \alpha\}$ es una base de K como $\mathbb{Q}$-espacio vectorial. Determinar si el opuesto de $1 + \alpha$ es el inverso de $1 - \alpha$ y si $(2 + \alpha)^3$ es la unidad. Hallar las raíces en K de los polinomios $x^2 - 2$, $x^2 - 3$, $x^2 + 1$ y $x^3 - 3$. Calcular un polinomio no nulo con coeficientes racionales que admita la raíz $\alpha + \alpha^2$.

16. Probar que $K = \mathbb{Q}[x]/(x^3 - 6x - 6)$ es una extensión de $\mathbb{Q}$. Sea $\alpha = [x]$. Comprobar si $\alpha + 1$ es raíz de $x^2 - 3$, si $\alpha^2 - \alpha - 4$ es raíz de $x^3 - 2$ y si $\alpha^2 - 2\alpha - 4$ es raíz de $x^3 + 4$. Calcular un polinomio no nulo con coeficientes racionales que admita las raíces $1 - \alpha$ y $\alpha^2 + 2$.

17. Demostrar que la condición necesaria y suficiente para que una extensión $j\colon k \to K$ tenga grado 1 es que j sea un isomorfismo.

18. Si $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, entonces $p(x)p(-x)$ es un polinomio en x^2:

$$p(x)p(-x) = q(x^2)$$

y $q(x)$ es el polinomio de raíces α_i^2; es decir, $q(x) = \prod_i (x - \alpha_i^2)$.

19. Si α, β, γ son las raíces complejas de $x^3 - 3x + 1$, determinar un polinomio cuyas raíces sean $\alpha + \alpha^{-1}$, $\beta + \beta^{-1}$ y $\gamma + \gamma^{-1}$.

20. Si α, β, γ son las raíces complejas del polinomio $x^3 + 2x^2 - x + 1$, hallar

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 \ , \ \alpha\beta\gamma^3 + \alpha\beta^3\gamma + \alpha^3\beta\gamma \ , \ (\alpha + \beta)^2 + (\alpha + \gamma)^2 + (\beta + \gamma)^2$$

21. Si $\alpha_1, \ldots, \alpha_5$ son las raíces complejas del polinomio $x^5 - x - 1$, calcular

$$\sum_{i=1}^{5} \alpha_i^2 \quad , \quad \sum_{i=1}^{5} \alpha_i^{-1} \quad , \quad \sum_{i=1}^{5} \alpha_i^{-2}$$

22. Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo. Si $p(x)$ tiene una raíz simple ¿es cierto que todas sus raíces son simples? Si $p(x)$ tiene una raíz múltiple ¿es cierto que todas sus raíces son múltiples?

23. Hallar las raíces múltiples de los siguientes polinomios con coeficientes racionales, así como sus respectivas multiplicidades ¿y si los coeficientes están en $\mathbb{F}_2$? ¿y en $\mathbb{F}_3$?

$$x^6 + x^4 - 4x^3 + 4x^2 - 4x + 4 \quad , \quad 2x^6 - 9x^4 + 20x^3 - 24x + 28$$

24. Si $d \in \mathbb{Q}$ no es un cuadrado, demostrar que $\mathbb{Q}(\sqrt{d}\,)$ es una extensión de grado 2 de $\mathbb{Q}$. Si $a, b \in \mathbb{Q}$, demostrar que $\mathbb{Q}(\sqrt{a}\,) = \mathbb{Q}(\sqrt{b}\,)$ precisamente cuando a/b sea un cuadrado en $\mathbb{Q}$.

25. Demostrar que $[\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}] = 3$. ¿Está $\sqrt{2}$ en $\mathbb{Q}(\sqrt[3]{2}\,)$?

26. Demostrar que una base de $\mathbb{Q}(\sqrt[4]{2}\,)$ sobre $\mathbb{Q}$ es $\{1,\ \sqrt[4]{2},\ \sqrt{2},\ \sqrt[4]{8}\}$.

27. Determinar las relaciones de inclusión entre los siguientes subcuerpos de $\mathbb{C}$:

$$\mathbb{Q}\ ,\ \mathbb{Q}(1/2)\ ,\ \mathbb{Q}(\sqrt{2}\,)\ ,\ \mathbb{Q}(\sqrt[3]{2}\,)\ ,\ \mathbb{Q}(i)\ ,\ \mathbb{Q}(i+\sqrt{2}\,)\ ,\ \mathbb{Q}(\sqrt{-2}\,)$$

28. ¿Están $x^3 + 1$ y $x^4 - 1$ en el ideal $(xy - x - 1, x^2 + y^2 - 1)$ de $\mathbb{Q}[x, y]$?

29. Determinar si en el ideal (x^2+y^2-x, x^2y^2-x) de $\mathbb{Q}[x, y]$ están los siguientes polinomios:

$$x^4 - x^3 + x\ , \quad x^3 - x^2 + 1\ , \quad x^3 + y^3 - x - y$$
$$y^4 - x(y^2 - 1)\ , \quad (x^2y^2 + y)^2 - xy(2 + xy)$$

30. Hallar todas las soluciones racionales de los siguientes sistemas de ecuaciones:

$$\left.\begin{aligned} 2x^2 + 2xy + y^2 - 5x &= -2 \\ 2xy^2 + 2xy^2 + y^3 + x^2 - 4xy &= 4 \end{aligned}\right\} \qquad \left.\begin{aligned} x^3 + y^2 - x &= 0 \\ x^2 + y^2 + y &= 1 \end{aligned}\right\}$$

$$\left.\begin{aligned} x^2 + y^4 &= 0 \\ yx^3 + y^3x &= -1 \end{aligned}\right\} \qquad \left.\begin{aligned} x^2y^2 + y^4 + 1 &= 0 \\ x^2y + xy^2 + y^3 &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} x^2y^2 + y^5 &= 0 \\ x^2y + y^2x + 1 &= 0 \end{aligned}\right\}$$

31. Racionalizar $(\sqrt[3]{4} + \sqrt[4]{3}\,)^{-1}$, $(\sqrt[5]{2} - \sqrt{3} + 1)^{-1}$, $(\sqrt[6]{10} - \sqrt{2} - 1)^{-1}$.

32. Determinar si los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$: $x^5 - x - 1$, $x^5 + 4$, $x^5 - x^2 - 1$, $x^5 + 3x^3 + 1$, $x^5 - x^2 + 18x + 7$.

33. Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo k. Si el grado de una extensión finita $k \to L$ no es múltiplo del grado de $p(x)$, probar que $p(x)$ no tiene raíces en L.

34. Hallar el grado de $\mathbb{Q}(\sqrt{3} + \sqrt{5}\,)$ sobre $\mathbb{Q}$.

35. Demostrar que x^3-3 no tiene raíces en $k=\mathbb{Q}(\sqrt{2})$. Concluir que $\mathbb{Q}(\sqrt{2},\sqrt[3]{3})$ es una extensión de grado 6 de $\mathbb{Q}$ y hallar una base sobre $\mathbb{Q}$.

    Sea $\alpha=\sqrt{2}+\sqrt[3]{3}$. Probar que el grado de un polinomio irreducible en $\mathbb{Q}[x]$ que admita la raíz α es 1, 2, 3, ó 6. Analizando las relaciones de dependencia lineal entre las sucesivas potencias de α, concluir que α es raíz de un polinomio irreducible de grado 6 con coeficientes racionales. Calcular tal polinomio.

36. Hallar el grado sobre $\mathbb{Q}$ y una base de las siguientes extensiones:

$$\mathbb{Q}(\sqrt{2},\sqrt{3})\ ,\quad \mathbb{Q}(\sqrt{3},\sqrt[3]{2})\ ,\quad \mathbb{Q}(i,\sqrt{2})$$

37. ¿Está i en la extensión $\mathbb{Q}(\omega,\sqrt[3]{2})$? ¿Está $\sqrt{2}$ en $\mathbb{Q}(\sqrt{3},\sqrt[3]{2})$?

38. Determinar un polinomio irreducible con coeficientes racionales que admita la raíz $\sqrt{2}+\sqrt{3}$. Análogamente para

$$\begin{gathered}\sqrt{3}+\sqrt[4]{3}\ ,\quad \sqrt{2}+i\ ,\quad \sqrt[3]{2}+\omega\sqrt[3]{2}\ ,\quad \sqrt[3]{7+5\sqrt{2}}\\ \sqrt[3]{1+\sqrt{2}i}\ ,\quad \sqrt{6+4\sqrt{3}}\ ,\quad \sqrt{21+12\sqrt{3}}\ ,\quad \sqrt[3]{2-2i}\\ i-\omega\ ,\quad 2i+\omega,\ i\omega\ ,\quad i/\omega\ ,\quad i/(2\omega+1)\\ \tfrac{\sqrt{-2}}{1+\sqrt{2}}\ ,\quad \tfrac{\sqrt{3}}{\sqrt{2}}-\sqrt{2}\ ,\quad \tfrac{\sqrt{3}}{\sqrt[3]{2}}-1\ ,\quad \tfrac{1}{i-\sqrt{2}}\ ,\quad \tfrac{\omega}{1-\sqrt[3]{-2}}\end{gathered}$$

39. Construir un cuerpo con 4 elementos, otro con 8 y otro con 9.

40. Hallar los números racionales q tales que $\operatorname{sen} q\pi$ es algebraico sobre $\mathbb{Q}$.

41. Si dos números complejos son trascendentes sobre $\mathbb{Q}$, entonces su suma o su producto es también trascendente sobre $\mathbb{Q}$.

42. Si p es un número primo, todo cuerpo de cardinal p es isomorfo a $\mathbb{F}_p$.

43. Sea $k\to L$ una extensión de grado 2. Si la característica de k no es 2, probar que $L=k(\sqrt{a})$ para algún $a\in k$. ¿Es cierto también cuando $\operatorname{car} k=2$?

44. Dado un sistema de ecuaciones

$$\left.\begin{aligned}p(x,y)&=0\\ q(x,y)&=0\end{aligned}\right\}$$

    con coeficientes en un cuerpo k, probar que su resultante $r(y)$ está en el ideal (p,q) de $k[x,y]$:

$$r(y)=a(x,y)p(x,y)+b(x,y)q(x,y)$$

    Indicación: Sean $C_0,\dots,C_{m+n}$ las columnas de la matriz que nos proporciona la resultante. Calcular $C=x^{m+n-1}C_0+\ldots+1\cdot C_{m+n}$ y utilizar que

$$r(y)=\det(C_0,\dots,C_{m+n})=\det(C_0,\dots,C_{m+n-1},C)$$

Factorización Única

(*) Anillos de Fracciones:

1. El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, y el de $\mathbb{Z}[\,i\,]$ es $\mathbb{Q}(\,i\,)$.

2. Los números impares forman un sistema multiplicativo S en $\mathbb{Z}$ y el correspondiente anillo de fracciones $S^{-1}\mathbb{Z}$ es el subanillo de $\mathbb{Q}$ formado por todos los números racionales que pueden representarse con una fracción cuyo denominador sea impar.

   En general, si p es un número primo, entonces $S = \mathbb{Z} - p\mathbb{Z}$ es un sistema multiplicativo de $\mathbb{Z}$ y el anillo de fracciones $S^{-1}\mathbb{Z}$ es el subanillo de $\mathbb{Q}$ formado por todos los números racionales que pueden representarse con una fracción cuyo denominador no sea múltiplo de p.

3. Sea k un cuerpo. En el anillo $A = k[x, y]$ los polinomios no nulos en x forman un sistema multiplicativo $S = \{q(x) \neq 0\}$ y el correspondiente anillo de fracciones $S^{-1}A$ es isomorfo al anillo de polinomios en una indeterminada con coeficientes en el cuerpo $k(x)$; es decir, $S^{-1}A \simeq k(x)[y]$.

4. Si S es un sistema multiplicativo de un anillo A y $a \in A$, entonces $a/1 = 0$ en $S^{-1}A$ si y sólo si existe $s \in S$ tal que $sa = 0$. Es decir, el núcleo del morfismo de localización $\gamma\colon A \to S^{-1}A$ está formado por los elementos de A que están anulados por algún elemento de S. En particular, si A es íntegro y el 0 no está en S, el morfismo de localización γ es inyectivo.

(*) Descomposición en Fracciones Simples:

Para descomponer la fracción racional $(x^4+1)/(x^4+x^2)$ en suma de fracciones simples en $\mathbb{R}(x)$

$$\frac{x^4+1}{x^4+x^2} = 1 + \frac{1-x^2}{x^4+x^2} = 1 + \frac{ax+b}{x^2+1} + \frac{c}{x} + \frac{d}{x^2}$$

basta identificar coeficientes en la igualdad

$$1 - x^2 = (ax+b)x^2 + cx(x^2+1) + d(x^2+1)$$

Resolviendo el sistema de ecuaciones lineales así obtenido concluimos que $a = 0$, $b = -2$, $c = 0$ y $d = 1$.

Para descomponer la fracción racional $(x^2+1)/x^2(x^3-x^2+1)$ con coeficientes en el cuerpo $\mathbb{F}_7$

$$\frac{x^2+1}{x^2(x^3-2)} = \frac{ax^2+bx+c}{x^3-2} + \frac{d}{x} + \frac{e}{x^2}$$

basta resolver en $\mathbb{F}_7$ el sistema de ecuaciones lineales

$$x^2+1=(ax^2+bx+c)x^2+dx(x^3-2)+e(x^3-2)$$

Si no se desea resolverlo por los métodos usuales del Álgebra Lineal, podemos dar los valores $x=0$, $x=\alpha$ y $x=1$, donde α es la raíz de x^3-2 que nos proporciona el teorema de Kronecker (la clase de restos de x módulo x^3-2, de forma que $\alpha^3=2$ y 1, α, α^2 son linealmente independientes sobre $\mathbb{F}_7$):

$$\begin{aligned} 1&=-2e\ ;\quad e=-1/2=3\\ \alpha^2+1&=(a\alpha^2+b\alpha+c)\alpha^2=c\alpha^2+2a\alpha+2b\ ;\quad c=1,\ a=0,\ b=1/2=4\\ 2&=(a+b+c)-d-e\ ;\quad d=a+b+c-e=4+1-3=2\end{aligned}$$

(*) Dominios de Factorización Única:

1. Todos los cuerpos y todos los anillos euclídeos ($\mathbb{Z}$, $\mathbb{Z}[\,i\,]$, $k[x],\ldots$) son dominios de factorización única.

2. Consideremos el anillo $\mathbb{Z}[\sqrt{d}\,]$, donde d es un número entero que no sea cuadrado perfecto. Si d es par, entonces 2 divide a $d=\sqrt{d}\cdot\sqrt{d}$ mientras que 2 no divide a $\sqrt{d}$ en $\mathbb{Z}[\sqrt{d}\,]$. Si d es impar, 2 divide a $1-d=(1+\sqrt{d}\,)(1-\sqrt{d}\,)$, mientras que 2 no divide a $1+\sqrt{d}$ ni a $1-\sqrt{d}$ en $\mathbb{Z}[\sqrt{d}\,]$. Luego $\mathbb{Z}[\sqrt{d}\,]$ no es un dominio de factorización única cuando 2 sea irreducible en $\mathbb{Z}[\sqrt{d}\,]$, lo que equivale a que la ecuación $x^2-d\,y^2=\pm2$ no tenga soluciones enteras.

   En efecto, si $2=\pm(x+y\sqrt{d}\,)(x-y\sqrt{d}\,)$ tiene alguna solución entera, claramente 2 no es irreducible en $\mathbb{Z}[\sqrt{d}\,]$. Recíprocamente, si

   $$2=(a+b\sqrt{t}\,)(u+v\sqrt{t}\,)$$

   y ningún factor es invertible en $\mathbb{Z}[\sqrt{d}\,]$, al tomar normas obtenemos que $2^2=(a^2-b^2d)(u^2-v^2d)$. Luego $a^2-b^2d=\pm2$, porque $a^2-b^2d\neq\pm1$ y $u^2-v^2d\neq\pm1$, al no ser $a+b\sqrt{d}$ ni $u+v\sqrt{d}$ invertibles en $\mathbb{Z}[\sqrt{d}\,]$.

   En resumen, si la ecuación $x^2-d\,y^2=\pm2$ carece de soluciones enteras, el anillo $\mathbb{Z}[\sqrt{d}\,]$ no es un dominio de factorización única. Por ejemplo, tal ecuación carece de soluciones enteras cuando $d\leq-3$. Tampoco tiene soluciones enteras cuando $d\equiv1$ módulo 4, porque su reducción módulo 4 no tiene soluciones en $\mathbb{Z}/4\mathbb{Z}$.

3. En el cuerpo de fracciones del anillo íntegro $A=\mathbb{Z}[ni\,]$, está $i=ni/n$, que es raíz del polinomio $x^2+1\in A[x]$. Como i no está en $\mathbb{Z}[ni\,]$ cuando $n\geq2$, en tal caso 5.3.2 proporciona otra demostración de que $\mathbb{Z}[ni\,]$ no es un dominio de factorización única.

4. Consideremos el polinomio $y^2 - x^{2n+1}$ con coeficientes en un cuerpo k. En virtud del lema de Gauss (1777-1855), este polinomio es irreducible en $k[x, y]$, porque $y^2 - a^{2n+1}$ es irreducible en $k(a)[\,y\,]$, ya que es de grado 2 y no tiene raíces en $k(a)$. Luego $A = k[x, y]/(y^2 - x^{2n+1}) = k[\xi, \eta]$ es un anillo íntegro. En su cuerpo de fracciones $k(\xi, \eta)$ tenemos que

$$(\eta/\xi)^2 \;=\; \xi^{2n-1}$$

así que η/ξ es raíz del polinomio unitario $p(t) = t^2 - \xi^{2n-1} \in A[\,t\,]$. Ahora bien, η/ξ no está en A, pues en tal caso tendríamos $\eta = \xi q(\xi, \eta)$ para algún $q(\xi, \eta) \in A$; luego $y - xq(x, y)$ sería un múltiplo de $y^2 - x^{2n+1}$ en $k[x, y]$, lo que llevaría a contradicción igualando los coeficientes de y. De acuerdo con 5.3.2, concluimos que A no es un dominio de factorización única.

(*) Polinomios Irreducibles:

(1) Veamos que el polinomio $q(x) = x^4 - x^3 + x^2 + 1$ es irreducible en $\mathbb{Z}[x]$. No tiene factores de grado 0 porque sus coeficientes no tienen factores primos comunes. No tiene factores de grado 1 porque no tiene raíces en $\mathbb{Q}$. Si tuviera algún factor de grado dos, $q(x) = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$, entonces $b = -a$, y el coeficiente de x^3 en $q(x)$ sería nulo. En virtud del lema de Gauss, $q(x)$ también es irreducible en $\mathbb{Q}[x]$.

(2) Veamos que los polinomios $x^2 + y^n - 1$ son irreducibles en $\mathbb{C}[x, y]$. Consideremoslos como polinomios $q(x)$ en una indeterminada x con coeficientes en el anillo de polinomios $A = \mathbb{C}[a]$ en otra indeterminada, que no denotaremos y sino a para resaltar que A es ahora el anillo de las constantes. Es decir

$$q(x) = x^2 + a^n - 1$$

Sus coeficientes 1, 0, $a^n - 1$ claramente no tienen factores irreducibles comunes en A (pues la unidad no tiene factores irreducibles). Este polinomio $q(x)$ es irreducible en $\Sigma[x]$, donde $\Sigma = \mathbb{C}(a)$ es el cuerpo de fracciones de $A = \mathbb{C}[a]$, porque Σ es un cuerpo y $q(x)$ es un polinomio de grado 2 sin raíces en Σ, dado que $a^n - 1$ no es un cuadrado en Σ (por ejemplo porque tiene una raíz simple). El lema de Gauss permite concluir que $x^2 + y^n - 1$ es irreducible en $\mathbb{C}[x, y]$.

(3) El polinomio $p(x) = x^5 - x^2 + 1$ es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$, porque sus coeficientes no tienen factores primos comunes y su reducción módulo 2 es irreducible en $\mathbb{F}_2[x]$. En efecto, $\bar{p}(x)$ no admite factores de grado 1 en $\mathbb{F}_2[x]$ porque no tiene raíces en $\mathbb{F}_2$, así que, si no fuera irreducible tendría algún factor irreducible de grado 2. Ahora bien, el único polinomio irreducible de grado 2 con coeficientes

en $\mathbb{F}_2$, que es x^2+x+1, no divide a x^5+x^2+1, pues no es nula la clase de restos de x^5+x^2+1 módulo x^2+x+1. En efecto, poniendo $\alpha=[x]$ tenemos:

$$\alpha^2=\alpha+1\ ,\ \alpha^4=\alpha^2+1=\alpha\ ,\ \alpha^5=\alpha^2$$
$$\alpha^5+\alpha^2+1=\alpha^2+\alpha^2+1=1\neq 0$$

(4) El polinomio con coeficientes enteros $p(x)=x^5-6x^4+2x^3+5x^2-x-2$ no tiene raíces racionales, así que no admite factores de grado 1 en $\mathbb{Q}[x]$ y, por tanto, tampoco en $\mathbb{Z}[x]$. Su reducción módulo 2 es el polinomio

$$\bar{p}(x)=x^5+x^2+x=x(x^4+x+1)$$

que no admite factores de grado 2, pues x^4+x+1 es irreducible en $\mathbb{F}_2[x]$. Luego $p(x)$ no admite factores de grado 2 en $\mathbb{Z}[x]$ y concluimos que $p(x)$ es irreducible en $\mathbb{Z}[x]$ y, en virtud del lema de Gauss, también es irreducible en $\mathbb{Q}[x]$.

(5) Consideremos el polinomio $p(x)=-5x^6+6x^4-3x^2-6x+7$. Su reducción módulo 2 no admite factores de grado 1 ni 2 en $\mathbb{F}_2[x]$:

$$x^6+x^2+1=(x^3+x+1)^2$$

En consecuencia, $p(x)$ no admite factores de grado 1 ni 2 en $\mathbb{Z}[x]$. Por otra parte, la reducción de $p(x)$ módulo 3 no admite factores de grado 3 en $\mathbb{F}_3[x]$:

$$x^6+1=(x^2+1)^3$$

Luego $p(x)$ no admite factores de grado 3 en $\mathbb{Z}[x]$ y concluimos que $p(x)$ no tiene factores de grado 1,2 ni 3 en $\mathbb{Z}[x]$. Como sus coeficientes no tienen factores primos comunes, $p(x)$ no tiene factores irreducibles de grado cero, así que $p(x)$ es irreducible en $\mathbb{Z}[x]$ y también es irreducible en $\mathbb{Q}[x]$.

(6) Veamos, usando el criterio de reducción, que el polinomio x^5+y^3-1 es irreducible en $\mathbb{Q}[x,y]$. Si se considera como polinomio en una indeterminada y con coeficientes en el anillo de polinomios $A=\mathbb{Q}[a]$ en otra indeterminada

$$p(y)=y^3+(a^5-1)$$

sus coeficientes 1, 0, 0, a^5-1 no tienen factores irreducibles comunes en $\mathbb{Q}[a]$. Al considerar el caso particular $a=-1$ obtenemos el polinomio $\bar{p}(y)=y^3-2$, que es irreducible en $\mathbb{Q}[y]$, y concluimos que y^3+a^5-1 es irreducible en $A[y]=\mathbb{Q}[a,y]$.

(7) Si un número entero d es múltiplo de un número primo p y no es múltiplo de p^2, el criterio de Eisenstein (1823-1852) prueba que los polinomios x^n-d son irreducibles en $\mathbb{Z}[x]$ y, por tanto, también en $\mathbb{Q}[x]$.

Por ejemplo, los polinomios x^n-2, x^n+3 , ... son irreducibles en $\mathbb{Q}[x]$

Ejercicios:

1. Sea S un sistema multiplicativamente cerrado de un anillo A. Probar que
   (a) $a/s = b/t$ si y sólo si $r(ta - sb) = 0$ para algún $r \in S$.
   (b) El morfismo canónico de localización $A \to S^{-1}A$ es un isomorfismo precisamente cuando todo elemento de S es invertible en A.
   (c) La condición necesaria y suficiente para que $S^{-1}A = 0$ es que $0 \in S$.

2. Sean S y T dos sistemas multiplicativos de un anillo A. Probar que $(A_S)_T = A_{ST}$. Si $S \subseteq T$, concluir que $A_T = (A_S)_T$.

3. ¿Es cierto que el cuerpo de fracciones de $\mathbb{Z}[x]$ es isomorfo a $\mathbb{Q}(x)$?
   Si $\alpha \in \mathbb{C}$, ¿es cierto que el cuerpo de fracciones de $\mathbb{Z}[\alpha]$ es isomorfo a $\mathbb{Q}(\alpha)$?

4. Sea p un número primo y d un número entero. Si d es resto cuadrático módulo p y las ecuaciones $x^2 - dy^2 = \pm p$ carecen de soluciones enteras, demostrar que el anillo $\mathbb{Z}[\sqrt{d}\,]$ no es un dominio de factorización única.
   Cuando $p = 2$, comprobar que la hipótesis se verifica en los casos $d = -5,\ -4,\ 5,\ 8,\ 10$.

5. Si k es un cuerpo, determinar los elementos de $k(x_1, \ldots, x_n)$ que son algebraicos sobre k.

6. Calcular el grado sobre $\mathbb{Q}$ de la extensión que generan las raíces complejas del polinomio $x^4 - 2$. Análogamente para $x^3 + 3$, $x^5 - 1$ y $x^4 + 1$.

7. Calcular un polinomio irreducible con coeficientes en $\mathbb{Q}(i)$ que admita la raíz $\sqrt[4]{2}$. Análogamente sustituyendo $\mathbb{Q}(i)$ por $\mathbb{Q}(\sqrt{2}\,)$, $\mathbb{Q}(\sqrt[3]{2}\,)$ y $\mathbb{Q}(\sqrt{3}\,)$.

8. Hallar el grado sobre $\mathbb{Q}$ de la extensión que generan todas las raíces complejas del polinomio $x^3 + 2$. Análogamente para los polinomios $x^4 - 3$, $x^4 + 3$, $x^4 - x^2 + 1$, $x^4 + x^2 - 2$, $x^3 - 4x^2 + 5$, $x^4 + 3$, $x^4 - 3$.

9. Descomponer en factores irreducibles los siguientes polinomios con coeficientes complejos (respectivamente en $\mathbb{F}_2$ y en $\mathbb{F}_3$): $x^2 + y^2 - 1$, $xy^2 + x^2y - x - y$, $y^2 + x^2 - y^3$, $x^2y^2 - x^2z^2 - y^2z^2 + z^2$, $x^3 + y^3 + 1$, $x^3y^3 + 1$, $x^6 - y^3$, $x^3y + yz^3 + x - z$.

10. Estudiar la irreducibilidad en $\mathbb{Q}[x]$ del polinomio $x^5 - nx - 1$, donde $n\mathbb{Z}$.

11. Sea α una raíz racional de un polinomio con coeficientes enteros $p(x)$. Si $\alpha = a/b$, donde a y b son números enteros primos entre sí, demostrar que todos los coeficientes de $p(x)/(bx - a)$ son enteros. Concluir que $p(1)$ es múltiplo de $a - b$ y $p(-1)$ lo es de $a + b$.

12. Sea k un cuerpo y $p(x) \in k[x]$. Probar que $y^2 - p(x)$ es irreducible en $k[x, y]$ si, y sólo si, $p(x)$ no es un cuadrado en $k[x]$.

13. Descomponer en factores irreducibles los siguientes polinomios con coeficientes racionales: $x^4y^4 + x^2y^3 - x^4 - x^2 + y^2 - 1$, $x^4 + 3x^3 + x^2 + x + (2n+1)$, $x^5 - x^2 + 1$, $x^5 - 2x^3 + x^2 - 3x + 1$, $x^6 - 6x^5 - 5x^3 + 4x^2 + 3x + 2$.

14. Sea $p(x) = x^4 + 4x^3 + 3x^2 + 2x + 3$.

    Descomponer en factores irreducibles la reducción de $p(x)$ módulo 2 y 3.

    Descomponer $p(x)$ en factores irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

15. Sea $p(x) = 33x^5 - 6x^4 + 3x^2 - 3x + 6$.

    Descomponer en factores irreducibles la reducción módulo 2 de $p(x)$.

    Descomponer $p(x)$ en factores irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

16. *Criterio de Nietsnesie* (3281-2581): Sea $a_0 + a_1x + \ldots + a_nx^n$ un polinomio no constante con coeficientes enteros. Si sus coeficientes no admiten factores primos comunes y existe un número primo p que divide a $a_1, \ldots, a_n$ y p^2 no divide a a_n, entonces el polinomio es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

17. Sea $q(x)$ un polinomio irreducible con coeficientes racionales y sea $k = \mathbb{Q}[x]/(q(x))$. Dado un polinomio $p(x)$ con coeficientes racionales, probar que los siguientes problemas pueden reducirse al de calcular todas las soluciones racionales de un número finito de sistemas de ecuaciones algebraicas con coeficientes racionales:

    (a) Hallar todas las raíces de $p(x)$ en k.

    (b) Decidir si $p(x)$ es irreducible en $k[x]$.

    (c) Hallar la descomposición de $p(x)$ en producto de polinomios irreducibles en $k[x]$.

Módulos y Álgebras

(*) Módulos:

1. Si k es un cuerpo, los k-módulos son los k-espacios vectoriales.

2. Sea $j\colon A \to B$ un morfismo de anillos. El producto $a \cdot b = j(a)b$ define en B una estructura de A-módulo. En general, en todo B-módulo N tenemos una estructura de A-módulo, definida por el producto $a \cdot n = j(a)n$; y diremos que tal estructura de A-módulo se obtiene por **restricción de escalares**.

   En particular, si $\mathfrak{a}$ es un ideal de un anillo A, la proyección canónica $A \to A/\mathfrak{a}$ define en $A/\mathfrak{a}$ una estructura de A-módulo: $a \cdot [\,b\,] = [ab]\,$. Si S es un sistema multiplicativo de A, el morfismo de localización $A \to A_S$ define en A_S una estructura de A-módulo: $a \cdot (b/s) = (a/1)(b/s) = ab/s\,$.

3. Cada grupo abeliano G admite una única estructura de $\mathbb{Z}$-módulo, pues para cada $n \in \mathbb{N},\ g \in G$ el producto $n \cdot g$ ha de ser la suma iterada n veces de g, y $(-n) \cdot g$ ha de ser el opuesto de $n \cdot g$. En resumen, los $\mathbb{Z}$-módulos son los grupos conmutativos. Cuando un grupo abeliano se considera como $\mathbb{Z}$-módulo, los submódulos son los subgrupos.

4. Sea $\mathfrak{a}$ un ideal de un anillo A. La inclusión $\mathfrak{a} \to A$ y la proyección canónica $A \to A/\mathfrak{a}$ son morfismos de A-módulos.

5. Sea M un A-módulo. Cada elemento $a \in A$ define una aplicación $a\cdot\colon M \to M$ que es morfismo de A-módulos. La aplicación natural $A \to \mathrm{Hom}_A(M, M)$ así obtenida es un morfismo de A-módulos.

6. Los submódulos del anillo A son precisamente los ideales de A.

7. Sea $f\colon M \to N$ un morfismo de A-módulos. Si M' es un submódulo de M, entonces $f(M')$ es un submódulo de N. Si N' es un submódulo de N, entonces $f^{-1}(N')$ es un submódulo de M. En particular, $\mathrm{Im}\, f = f(M)$ es un submódulo de N y $\mathrm{Ker}\, f = f^{-1}(0)$ es un submódulo de M.

8. Sea $\mathfrak{a}$ un ideal de A y M un A-módulo. El subgrupo

   $$\mathfrak{a}M = \{m = \textstyle\sum_i a_i m_i\colon\ a_i \in \mathfrak{a},\, m_i \in M\}$$

   generado por los productos de elementos de $\mathfrak{a}$ por elementos de M es un submódulo de M.

9. Sean N_1, N_2 submódulos de un A-módulo M. Los morfismos de inclusión naturales $N_i \to M$ definen un morfismo de A-módulos $N_1 \bigoplus N_2 \to M$. En consecuencia, su imagen $N_1 + N_2 = \{n_1 + n_2\colon\ n_i \in N_i\}$ es un submódulo de M y claramente es el submódulo generado por N_1 y N_2.

(*) Geometría Intrínseca de las Subvariedades:

Consideremos la subvariedad del espacio afín n-dimensional sobre un cuerpo k definida por un ideal $\mathfrak{a}$ de $k[x_1,\ldots,x_n]$. El corolario 6.1.2 muestra que las relaciones de incidencia entre las subvariedades contenidas en ella están determinadas por el anillo $k[x_1,\ldots,x_n]/\mathfrak{a}$. En este sentido el anillo de funciones algebraicas determina la geometría intrínseca de cada subvariedad. En particular, si el anillo $k[x_1,\ldots,x_n]/\mathfrak{a}$ es isomorfo a un anillo de polinomios $k[t_1,\ldots,t_d]$, dichas relaciones de incidencia coinciden con las de las subvariedades de un espacio afín de dimensión d. Veamos unos ejemplos:

1. Consideremos la curva plana $y = ax + b$ sobre un cuerpo k. Las ecuaciones
$$\begin{cases} x = t \\ y = at + b \end{cases}$$
definen un isomorfismo $k[x,y]/(y - ax - b) \simeq k[\,t\,]$. Tal curva es una recta afín.

   Si $k = \mathbb{R}$, la intersección de la curva $x^2 + y^2 = 1$ con la recta $y = 1$, que es la subvariedad definida por el ideal $(x^2 + y^2 - 1, y - 1)$, se corresponde con la subvariedad de la recta afín definida por el ideal $(t^2 + 1 - 1) = (t^2)$: se cortan en dos puntos confundidos en $t{=}0$. La intersección con la recta $y = x$ es la subvariedad definida por el ideal $(t^2 + t^2 - 1) = (\sqrt{2}\,t - 1)(\sqrt{2}\,t + 1)$: son los dos puntos reales $t = \pm 1/\sqrt{2}$. La intersección con la recta $y = 2$ es la subvariedad definida por el ideal $(t^2 + 3)$: es el par de puntos complejos conjugados $t = \pm\sqrt{3}\,i$.

2. El isomorfismo $k[x,y,z]/(z{-}ax{-}by{-}c) \simeq k[\,t_1,t_2]$ definido por las ecuaciones
$$\begin{cases} x = t_1 \\ y = t_2 \\ z = at_1 + bt_2 + c \end{cases}$$
muestra que la subvariedad $z = ax + by + c$ es un plano afín.

   Si $k = \mathbb{R}$, la intersección de la superficie $x^2 + y^2 + z^2 = 1$ con el plano $z = 1$ es la subvariedad definida por el ideal $(t_1^2 + t_2^2 + 1 - 1) = (t_1^2 + t_2^2)$: es el par de rectas imaginarias conjugadas $t_1^2 + t_2^2 = 0$.

3. Consideremos la curva plana de ecuación $y = x^4$. Las ecuaciones
$$\begin{cases} x = t \\ y = t^4 \end{cases}$$
definen un isomorfismo $k[x,y]/(y - x^4) \simeq k[\,t\,]$. La intersección de esta curva con la de ecuación $y = -x^4$ está definida por el ideal $(y - x^4, y + x^4)$, y se corresponde con la subvariedad de la recta afín definida por el ideal $(t^4 + t^4) = (t^4)$: se cortan en 4 puntos confundidos en $t = 0$.

(*) Sea $\mathfrak{a}$ un ideal de un anillo A. El anulador del A-módulo $A/\mathfrak{a}$ es $\mathfrak{a}$. En general, si M es un A-módulo, el anulador de $M/\mathfrak{a}M$ contiene al ideal $\mathfrak{a}$.

(*) Sea $\mathfrak{m}$ un ideal maximal de un anillo A. El A-módulo $\mathfrak{m}/\mathfrak{m}^2$ está anulado por el ideal $\mathfrak{m}$, así que el producto $\bar{a}\cdot[x]=a[x]=[ax]$ define en $\mathfrak{m}/\mathfrak{m}^2$ una estructura de espacio vectorial sobre el cuerpo residual $A/\mathfrak{m}$. En general, si M es un A-módulo, $M/\mathfrak{m}M$ es un espacio vectorial sobre $A/\mathfrak{m}$ con el producto $\bar{a}\cdot[m]=a[m]=[am]$.

(*) Consideremos el grupo abeliano $(\mathbb{Z}/6\mathbb{Z})\oplus\mathbb{Z}$. El anulador de cualquier elemento (a,b) es 0 cuando $b\neq 0$. El anulador de $(\bar{1},0)$ y $(\bar{5},0)$ es $6\mathbb{Z}$, el anulador de $(\bar{2},0)$ y $(\bar{4},0)$ es $3\mathbb{Z}$, el anulador de $(\bar{3},0)$ es $2\mathbb{Z}$ y el anulador de $(0,0)$ es $\mathbb{Z}$. En particular el anulador de este grupo abeliano es 0.

(*) Sea M un A-módulo. Cada morfismo $A\to M$ viene definido por algún elemento $m\in M$ y la condición necesaria y suficiente para que su núcleo contenga cierto ideal $\mathfrak{a}$ es que m esté anulado por $\mathfrak{a}$. En virtud de la propiedad universal del módulo cociente concluimos que

$$\mathrm{Hom}_A(A/\mathfrak{a},M) \;=\; \begin{bmatrix}\text{Elementos de } M\\ \text{anulados por } \mathfrak{a}\end{bmatrix}$$

(*) Sea I un conjunto. El A-módulo $A^{(I)}$ es libre y una base está formada por los elementos de I (que se identifican canónicamente con elementos de $A^{(I)}$). Luego el rango de $A^{(I)}$ coincide con el cardinal de I.

(*) Sea A un anillo íntegro. Si $\mathfrak{a}\neq 0$ es un ideal principal de A, entonces $\mathfrak{a}=aA$ para algún elemento no nulo $a\in A$. Luego el morfismo $a\cdot\colon A\to\mathfrak{a}$ es un isomorfismo de A-módulos y concluimos que $\mathfrak{a}$ es un A-módulo libre de rango 1. Recíprocamente, si un ideal no nulo $\mathfrak{a}$ de A es un A-módulo libre, su rango ha de ser 1 (pues dos elementos a,b de una base verificarían la relación $ba-ab=0$) y concluimos que $\mathfrak{a}$ es un ideal principal de A. Es decir, los ideales de A que son módulos libres son precisamente los ideales principales y todos, salvo el 0, son de rango 1.

Cuando A es un anillo de polinomios sobre un cuerpo k, obtenemos que las únicas subvariedades del espacio afín cuyo ideal es un módulo libre no nulo son las hipersuperficies.

(*) El anulador de cualquier A-módulo libre no nulo es el ideal 0. Si el anillo A es íntegro, el anulador de cualquier elemento no nulo de un módulo libre es 0.

(*) Sea $\mathfrak{a}$ un ideal no nulo de un anillo A. El A-módulo cociente $A/\mathfrak{a}$ nunca es libre, porque su anulador es $\mathfrak{a}$, que no es nulo. Sin embargo, $A/\mathfrak{a}$ es un $A/\mathfrak{a}$ -módulo libre de rango 1.

(*) El anulador del grupo abeliano $(\mathbb{Z}/n\mathbb{Z})\oplus\mathbb{Z}$ es el 0; pero no es un grupo libre cuando $n\geq 2$, porque $(\bar{1},0)$ no es nulo y su anulador es $n\mathbb{Z}\neq 0$.

(*) Sea A un anillo íntegro que no sea cuerpo y sea $a \in A$ un elemento no nulo de A que no sea invertible; es decir, tal que el morfismo $a\cdot\colon A \to A$ no sea epiyectivo. Para todo A-módulo libre no nulo L es claro que el morfismo $a\cdot\colon L \to L$ tampoco es epiyectivo. Sea Σ el cuerpo de fracciones de A. Como el morfismo $a\cdot\colon \Sigma \to \Sigma$ es epiyectivo, concluimos que Σ no es un A-módulo libre.

En particular, $\mathbb{Q}$ no es un grupo abeliano libre. Si k es un cuerpo, el cuerpo de fracciones racionales $k(x_1, \ldots, x_n)$ no es un $k[x_1, \ldots, x_n]$-módulo libre.

(*) Cálculos de Longitudes:

(1) Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo k. Los ideales del anillo $k[x]/(p(x)^n)$ se corresponden con los ideales de $k[x]$ que contienen a $p(x)^n$, que son precisamente los ideales generados por sus divisores:

$$\big(p(x)^n\big) \subset \big(p(x)^{n-1}\big) \subset \cdots \subset \big(p(x)^2\big) \subset \big(p(x)\big) \subset k[x]$$

Luego la longitud de $k[x]/(p(x)^n)$ es exactamente n.

Si $p_1(x), \ldots, p_r(x)$ son polinomios irreducibles en $k[x]$, primos entre sí dos a dos, entonces $k[x]/(p_1(x)^{n_1} \cdots p_r(x)^{n_r}) \simeq k[x]/(p_1(x)^{n_1}) \oplus \cdots \oplus k[x]/(p_r(x)^{n_r})$ y, por la aditividad de la longitud, concluimos que

$$l\left(k[x]/\big(p_1(x)^{n_1} \cdots p_r(x)^{n_r}\big)\right) \;=\; n_1 + \ldots + n_r$$

(2) Consideremos la recta de ecuación $y = ax + b$ sobre un cuerpo k. La parametrización $x = t$, $y = at + b$ define un isomorfismo $k[x, y]/(y - ax - b) \simeq k[\,t\,]$, así que para cada polinomio $p(x, y)$ con coeficientes en k tenemos un isomorfismo

$$k[x, y]/\big(y - ax - b, p(x, y)\big) \;\simeq\; k[\,t\,]/\big(p(t, at + b)\big)$$

que nos permite calcular la longitud del anillo de funciones algebraicas de la intersección de la curva plana $p(x, y) = 0$ con cualquier recta.

Por ejemplo, el anillo de la intersección de la curva plana $x^2 + y^2 = 1$ con la recta $x = 1$ es isomorfo a $k[\,t\,]/(t^2)$ y su longitud es 2, lo que recoge nuestra idea intuitiva de que tal recta la corta en dos puntos infinitamente próximos.

(3) La parametrización $x = t$, $y = t^2$ define un isomorfismo $\mathbb{R}[x, y]/(y - x^2) \simeq \mathbb{R}[\,t\,]$. Luego el anillo de funciones algebraicas de la intersección de la parábola $y = x^2$ con la circunferencia centrada en el punto $(0, 1/2)$ que pasa por el origen es

$$\mathbb{R}[x, y]/(y - x^2, x^2 + y^2 - y) \;\simeq\; \mathbb{R}[\,t\,]/(t^4)$$

y su longitud es 4; recogiendo así nuestra intuición de que ambas cónicas se cortan en 4 puntos confundidos en $t = 0$.

(4) Sea k un cuerpo y consideremos el anillo $k[\xi, \eta] = k[x, y]/(x^2, y^2)$. Su dimensión como k-espacio vectorial es 4, pues una base es $\{1, \xi, \eta, \xi\eta\}$. Todo ideal es

un subespacio vectorial, así que la longitud de $k[\xi,\eta]$ no puede ser mayor que 4. Ahora bien, los ideales de este anillo se corresponden con los ideales de $k[x,y]$ que contienen a (x^2,y^2). La siguiente sucesión estrictamente creciente de ideales muestra que la longitud de $k[\xi,\eta]$ es 4:

$$(x^2,y^2) \subset (x,y)^2 \subset (x,y^2) \subset (x,y) \subset k[x,y]$$

(5) La longitud de cualquier anillo íntegro A que no sea cuerpo es infinita porque admite cadenas de ideales de longitud arbitraria:

$$\cdots \subset f^n A \subset \cdots \subset f^2 A \subset fA \subset A$$

donde $f \in A$ no es nulo ni invertible. Además, cualquier ideal no nulo de A tiene longitud infinita, pues contiene algún ideal principal no nulo, que es isomorfo al propio anillo A y, por tanto, de longitud infinita.

(6) Veamos que el anillo $A = \mathbb{C}[x,y]/\big(p(x,y)\big)$ de funciones algebraicas de una curva plana compleja $p(x,y) = 0$ tiene longitud infinita. Si $q(x,y)$ es un factor irreducible de $p(x,y)$, tenemos que $\mathbb{C}[x,y]/\big(q(x,y)\big) = A/qA$, así que podemos suponer que $p(x,y)$ es irreducible, en cuyo caso A es íntegro y para concluir bastará probar que no es cuerpo. En virtud del Teorema de D'Alembert, existen números complejos a,b tales que $p(a,b) = 0$, de modo que $(x-a, y-b)$ define un ideal maximal de A. Ahora bien, es claro que $x-a$ ó $y-b$ no es nulo en A, así que A tiene un ideal maximal no nulo y concluimos que no es un cuerpo.

(7) Sea G un grupo abeliano de longitud finita. Si $g \in G$ no es nulo, su orden ha de ser finito, pues en caso contrario $(g) \simeq \mathbb{Z}$ sería un subgrupo de G de longitud infinita. Luego el subgrupo (g) es finito y, procediendo por inducción sobre la longitud, la sucesión exacta corta

$$0 \longrightarrow (g) \longrightarrow G \longrightarrow G/(g) \longrightarrow 0$$

nos permite concluir que G es un grupo finito. Los grupos abelianos de longitud finita son precisamente los de orden finito.

(*) Producto Tensorial de Espacios Vectoriales: Sea E un espacio vectorial de dimensión finita n sobre un cuerpo k, y sea $T^q_p E$ el espacio de los tensores de tipo (p,q) sobre E; es decir, de las aplicaciones multilineales

$$T^q_p \colon E\times \overset{p}{\ldots} \times E \times E^*\times \overset{q}{\ldots} \times E^* \longrightarrow k \ ,$$

Cada sucesión $(\omega_1,\ldots,\omega_p,e_1,\ldots,e_q)$ de p formas lineales y q vectores define un tensor de tipo (p,q):

$$(\omega_1\otimes\ldots\omega_p\otimes e_1\ldots\otimes e_q)(v_1,\ldots,v_p,\eta_1,\ldots,\eta_q) := \omega_1(e_1)\ldots\omega_p(v_p)\eta_1(e_1)\ldots\eta_q(e_q)$$

y la aplicación $E^*\times \overset{p}{\ldots} \times E^*\times E\times \overset{q}{\ldots}\times E \to T^q_p E$ así definida es A-multilineal. La propiedad universal del producto tensorial permite obtener una aplicación lineal

$$E^*\otimes_k \overset{p}{\ldots} \otimes_k E^* \otimes_k E\otimes_k \overset{q}{\ldots}\otimes_k E \longrightarrow T^q_p E$$

que es un isomorfismo porque ambos espacios vectoriales tienen dimensión n^{p+q} y la imagen contiene una base de $T^q_p E$ (por ejemplo los productos tensoriales de los vectores de una base de E y de su base dual). Estos isomorfismos permite definir de manera muy directa la contracción de índices. En efecto la aplicación

$$\begin{aligned} E^*\times \overset{p}{\ldots} \times E^*\times E\times \overset{q}{\ldots}\times E &\longrightarrow T^{q-1}_{p-1}E \\ (\omega_1,\ldots,\omega_p,e_1,\ldots,e_q) &\mapsto \omega_1(e_1)(\omega_2\otimes\ldots\otimes\omega_p\otimes e_2\otimes\ldots\otimes e_q) \end{aligned}$$

es multilineal, así que define una aplicación lineal $C^1_1\colon T^q_p E \to T^{q-1}_{p-1}$ tal que

$$C^1_1(\omega_1\otimes\ldots\otimes\omega_p\otimes e_1\otimes\ldots\otimes e_q) = \omega_1(e_1)(\omega_2\otimes\ldots\otimes\omega_p\otimes e_2\otimes\ldots\otimes e_q)$$

Por ejemplo, tenemos que $\mathrm{End}_k E = T^1_1 E = E^*\otimes_k E$ y la aplicación lineal $C^1_1\colon \mathrm{End}_k E = T^1_1 E \to T^0_0 E = k$ es precisamente la traza de los endomorfismos.

(*) Álgebras:

1. Sea A un anillo. El cociente $A/\mathfrak{a}$ por un ideal $\mathfrak{a}$ y el anillo de fracciones $S^{-1}A$ por un sistema multiplicativo S son A-álgebras.

2. Sea k un anillo y A una k-álgebra. Si B es una A-álgebra, la composición de los morfismos estructurales $k\to A\to B$ define en B una estructura de k-álgebra y diremos que se obtiene por *restricción de escalares*. En particular, todos los cocientes y localizaciones de una k-álgebra son k-álgebras.

3. Cada anillo A admite una única estructura de $\mathbb{Z}$-álgebra; pues existe un único morfismo de anillos $j\colon \mathbb{Z}\to A$, que es el morfismo que transforma cada número natural n en la suma iterada n veces de la unidad de A y $-n$ en la suma iterada n veces de -1. Además todo morfismo de anillos es un morfismo de $\mathbb{Z}$-álgebras. El concepto de $\mathbb{Z}$-álgebra coincide con el de anillo.

4. Sea $A = k[x_1,\ldots x_n]/\mathfrak{a}$ y denotemos ξ_i la clase de restos de x_i módulo $\mathfrak{a}$. La k-álgebra A es de tipo finito porque los elementos $\xi_1,\ldots,\xi_n$ forman un sistema de generadores de $A = k[\xi_1,\ldots,\xi_n]$. Recíprocamente, si una k-álgebra A admite un sistema de generadores con n elementos, éstos definen un morfismo epiyectivo $k[x_1,\ldots,x_n]\to A$ y por tanto

   $$A \simeq k[x_1,\ldots,x_n]/\mathfrak{a}$$

   para algún ideal $\mathfrak{a}$. Es decir, *las k-álgebras de tipo finito son precisamente los cocientes por ideales de los anillos de polinomios con coeficientes en k.*

El anillo de funciones algebraicas de cualquier subvariedad de un espacio afín sobre un cuerpo k definida por ecuaciones polinómicas es una k-álgebra de tipo finito, y la condición de ser de tipo finito caracteriza las k-álgebras de funciones algebraicas de tales subvariedades, lo que nos permitirá reducir totalmente el estudio de las variedades algebraicas afines al de las k-álgebras de tipo finito. Esta reducción es absolutamente crucial.

5. Sea k un anillo. Cada morfismo de k-álgebras

$$f\colon k[y_1,\dots,y_m]/\mathfrak{b} \longrightarrow k[x_1,\dots,x_n]/\mathfrak{a}$$

está totalmente determinado por las imágenes $f_i(\bar{x}_1,\dots,\bar{x}_n) = f(\bar{y}_i)$ de los generadores $\bar{y}_1,\dots,\bar{y}_m$ de $k[y_1,\dots,y_m]/\mathfrak{b}$, en cuyo caso diremos que

$$\begin{cases} y_1 = f_1(x_1,\dots,x_n) \\ \quad\cdots\cdots\cdots \\ y_m = f_m(x_1,\dots,x_n) \end{cases}$$

son las ecuaciones del morfismo f considerado. La propiedad universal del anillo cociente afirma que las ecuaciones de un morfismo son totalmente arbitrarias, con la única condición de que se verifique

$$q_h\big(f_1(\bar{x}_1,\dots,\bar{x}_n),\dots,f_m(\bar{x}_1,\dots,\bar{x}_n)\big) = 0$$

para un sistema de generadores $\{q_h(y_1,\dots,y_m)\}$ del ideal $\mathfrak{b}$.

(*) En el isomorfismo natural de K-álgebras del corolario 6.5.3

$$\big(k[x_1,\dots x_n]/(p_1,\dots,p_r)\big)\otimes_k K = K[x_1,\dots,x_n]/(p_1,\dots,p_r)$$
$$[q(x_1,\dots,x_n)]\otimes\lambda = [\lambda q(x_1,\dots,x_n)]$$

ha de entenderse que, en el segundo término de esta fórmula, los coeficientes de los polinomios $p_i(x_1,\dots,x_n)$ se han sustituido por sus imágenes según el morfismo estructural $k\to K$. En particular, cuando $q(x)$ es un polinomio con coeficientes enteros y $\bar{q}(x)$ denota su reducción módulo un número primo p, tenemos que

$$\mathbb{Z}[x]/\big(q(x)\big)\otimes_{\mathbb{Z}}\mathbb{F}_p \;=\; \mathbb{F}_p[x]/\big(\bar{q}(x)\big)$$

(*) Sean $A = k[x_1,\dots,x_n]/(p_1,\dots,p_r)$ y $B = k[y_1,\dots,y_m]/(q_1,\dots,q_s)$. De acuerdo con 6.5.3, tenemos que

$$A\otimes_k B \;=\; k[x_1,\dots,x_n,y_1,\dots,y_m]/(p_1,\dots,p_r,q_1,\dots,q_s)$$
$$[p(x_1,\dots,x_n)]\otimes[q(y_1,\dots,y_m)] = [p(x_1,\dots,x_n)q(y_1,\dots,y_m)]$$

(*) Los números complejos son las sumas formales $a+bi$, donde $i^2=-1$ y $a,b\in\mathbb{R}$. Cambiar de base a $\mathbb{C}$ esta $\mathbb{R}$-álgebra significa considerar la $\mathbb{C}$-álgebra de las sumas

formales $\alpha+\beta i$, donde $i^2=-1$ y $\alpha,\beta\in\mathbb{C}$. La determinación de este anillo $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ se realiza con el teorema de Kronecker y el teorema Chino de los Restos:

$$\begin{aligned}\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} &= \big(\mathbb{R}[x]/(x^2+1)\big)_{\mathbb{C}} = \mathbb{C}[x]/(x^2+1) = \mathbb{C}[x]/(x-i)(x+i) = \\ &= \mathbb{C}[x]/(x-i)\oplus\mathbb{C}[x]/(x-i) = \mathbb{C}\oplus\mathbb{C}\end{aligned}$$

donde $\alpha\otimes\beta=(\alpha\beta,\bar{\alpha}\beta)$, y el producto en $\mathbb{C}\oplus\mathbb{C}$ es componente a componente.

(*) Álgebra Tensorial de un Módulo: Si M es un A-módulo, pondremos $T^dM := M\otimes_A \overset{d}{\ldots}\otimes_A M$ (entendiendo que $T^0M=A$ y $T^1M=M$), de modo que el producto tensorial de elementos define en

$$T^\bullet M := \bigoplus_{d\geq 0} T^dM$$

una estructura de A-álgebra graduada con unidad (¡pero no conmutativa!). El morfismo natural $t\colon M\to T^\bullet M$, $t(m)=m\in T^1M$, claramente tiene la propiedad universal de que todo morfismo de A-módulos $f\colon M\to B$ en una A-álgebra B (no necesariamente conmutativa) factoriza de modo único a través de t:

$$M \xrightarrow{t} T^\bullet M \xrightarrow{\phi} B$$

i.e., $f=\phi t$, donde ϕ es morfismo de A-álgebras.

(*) Álgebra Simétrica: Si M es un A-módulo, el **álgebra simétrica** $S^\bullet M$ de M es el cociente del álgebra tensorial $T^\bullet M$ por el ideal (bilátero) que generan los elementos $x\otimes y-y\otimes x$:

$$S^\bullet M := T^\bullet M/(x\otimes y - y\otimes x)$$

Es claro que $S^\bullet M$ es una A-álgebra graduada conmutativa, y que el morfismo de A-módulos canónico $\sigma\colon M\to S^\bullet M$, $\sigma(m)=[t(m)]$, tiene la propiedad universal de que todo morfismo de A-módulos $f\colon M\to B$ en una A-álgebra conmutativa B factoriza de modo único a través de σ:

$$M \xrightarrow{\sigma} S^\bullet M \xrightarrow{\phi} B$$

i.e., $f=\phi\sigma$ donde ϕ es morfismo de A-álgebras. De esta propiedad universal se sigue directamente que[1]

$$\begin{aligned}S^\bullet(M\oplus N) &= (S^\bullet M)\otimes_A (S^\bullet N)\\ S^\bullet(\oplus_n A) &= A[x_1,\ldots,x_n]\\ (S^\bullet_A M)_B &= S^\bullet_B(M_B)\end{aligned}$$

[1] En particular, obtenemos una definición del concepto de polinomio más satisfactoria que decir "las expresiones de la forma ...": El anillo de polinomios en n indeterminadas con coeficientes en un anillo A es el álgebra simétrica de un módulo libre de rango n.

Cuando E es un espacio vectorial de dimensión finita sobre un cuerpo k de característica nula, si consideramos el espacio vectorial TS^dE de los tensores contravariantes simétricos de orden d, tenemos que el morfismo natural

$$TS^dE \longrightarrow T^dE \longrightarrow S^dE$$

es un isomorfismo lineal, como puede comprobarse directamente, sin más que elegir una base en E. Estos isomorfismos canónicos inducen un producto conmutativo en los tensores simétricos.

Sin embargo, cuando la característica de k es positiva, aunque la potencia simétrica S^dE tenga igual dimensión que el espacio vectorial TS^dE de los tensores contravariantes simétricos de orden d, no es posible definir isomorfismos intrínsecos $TS^dE = S^dE$. Por ejemplo, si la característica de k es 2, los tensores hemisimétricos son simétricos; así que, cuando E es un plano, TS^2E contiene una recta invariante por la acción natural del grupo lineal $\mathrm{Gl}(E)$, mientras que el espacio S^2E de los polinomios homogéneos de grado 2 no contiene rectas invariantes (al menos cuando todo polinomio homogéneo se anule en algún vector no nulo, como es el caso cuando k es algebraicamente cerrado).

Ejercicios:

1. Sea $C = \{(a, b) \in \mathbb{R}^2 \colon\ ab = 1\}$. Demostrar que todo polinomio con coeficientes reales que se anule en todos los puntos de C es divisible por $xy - 1$ y que el anillo $\mathbb{R}[x, y]/(xy - 1)$ es isomorfo al anillo de las aplicaciones $C \to \mathbb{R}$ definidas por polinomios con coeficientes reales.

   Análogamente para el polinomio $x^2 - y^2$ y el conjunto $C = \{(a, b) \colon\ a^2 = b^2\}$.

2. Determinar si las siguientes afirmaciones son verdaderas:

   (a) La unión de la recta $x = 0$ con la recta $y = 0$ es el par de rectas $xy = 0$.

   (b) La intersección de la curva $y = x^2$ con la recta $y = 0$ es el punto $x = y = 0$.

   (c) La intersección del par de rectas $xy = 0$ con el par de rectas $y(x-y) = 0$ es la recta $y = 0$.

   (d) La intersección de dos rectas planas paralelas es vacía.

   (e) La intersección de la curva $x^2 + y^2 = 1$ con la recta $x = 2$ es vacía.

   (f) La intersección de la curva $x^2+y^2 = 1$ con la recta $x = 0$ es la unión del punto $x = 0$, $y = 1$ con el punto $x = 0$, $y = -1$. (*Indicación*: Aplicar el Teorema chino del resto a los ideales de ambos puntos).

   (g) La intersección del par de rectas $xy = 0$ con el par de rectas $y(x+y-1) = 0$ es la unión de la recta $y = 0$ con el punto $x = 0$, $y = 1$. (*Indicación*: Sea $\mathfrak{m}$ el ideal del punto $(0, 1)$. Probar que $(xy, y(x + y - 1)) = y\mathfrak{m}$).

(h) La intersección de la curva $x^2+y^2=1$ con la recta doble $x^2=0$ coincide con su intersección con el par de rectas paralelas $y^2=1$.

(i) La intersección del par de planos $zx=0$ con el par de planos $zy=0$ es la unión del plano $z=0$ con la recta $x=0, y=0$. (*Indicación*: El ideal (x,y) es primo).

3. Si k es un cuerpo, demostrar que $k[x,y]/\,(y-p(x)) \simeq k[\,t\,]$ y que

$$k[x,y]/\,(q(x)y-p(x)) \simeq S^{-1}k[\,t\,]\ ,$$

donde $S=\{q(x)^n,\ n\in\mathbb{N}\}$, cuando $p(x)$ y $q(x)$ son primos entre sí.

Indicación: Si $1=ap+bq$, entonces $q^{-1}=a(p/q)+b$.

4. Sea A un anillo y sea $\bar{A}=A/aA$. Probar que $A/(aA+bA)\simeq \bar{A}/\bar{b}\bar{A}$.

5. Determinar si el ideal $(x^2+x-y, y^2+y-x^4-3x-2)$ de $\mathbb{Q}[x,y]$ contiene los siguientes polinomios: $xy+y-(x^3+x+2)\,,\ x^2+y^2-(2xy+1)\,,$ $y^2-2xy-y+x-1\,,\ x^2y-2y-x^3+2x+1\,.$

6. Determinar si en el ideal $(xy+y-1,\ x^2y^2-4y^3+3y^2+y-1)$ del anillo $\mathbb{R}[x,y]$ están los siguientes polinomios: $x^2-1\,,\ x^2-2x-1\,,\ 2y-1\,,\ y^2-4y+1\,.$

7. Sean $\alpha_1,\ldots,\alpha_n$ números complejos, no todos reales. Demostrar que los polinomios con coeficientes reales $p(x_1,\ldots,x_n)$ tales que $p(\alpha_1,\ldots,\alpha_n)=0$ forman un ideal maximal $\mathfrak{m}$ de $\mathbb{R}[x_1,\ldots,x_n]$ y que $\mathbb{R}[x_1,\ldots,x_n]/\mathfrak{m}\simeq\mathbb{C}$, donde $[q(x_1,\ldots,x_n)]$ se corresponde con $q(\alpha_1,\ldots,\alpha_n)$.

Hallar un sistema finito de generadores de $\mathfrak{m}$ cuando los números complejos son 2 y $1+i$. Análogamente cuando son $-i$ y $-1+i$.

8. Demostrar que todo módulo es cociente de un módulo libre. ¿Es cierto que todo módulo libre de tipo finito tiene rango finito? ¿y que cualquier sistema linealmente independiente con n elementos en un módulo libre de rango n es una base?

9. Si L es un A-módulo libre, probar que toda sucesión exacta de morfismos de A-módulos $0\to N\to M\to L\to 0$ escinde.

10. Demostrar que una sucesión exacta de A-módulos $0\to M'\to M\to M''\to 0$ escinde precisamente cuando M' admite un suplementario en M (i.e. un submódulo $N\subseteq M$ tal que $M'\cap N=0$ y $M'+N=M$).

11. Demostrar que $(N+N')/N=N'/(N\cap N')$ y que

$$M/(N+N')\ =\ \frac{(M/N)}{(N+N')/N}$$

12. Demostrar que $M_1 \oplus M_2)/(N_1 \oplus N_2) = (M_1/N_1) \oplus (M_2/N_2)$.

13. Demostrar que $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$, donde $d =$m.c.d.(m, n).

14. Si E es un k-espacio vectorial, probar que el producto tensorial $\otimes_k E$ transforma sucesiones exactas de aplicaciones k-lineales en sucesiones exactas.

15. Sean E y F dos k-espacios vectoriales de dimensión finita. Probar la existencia de un isomorfismo lineal canónico $\mathrm{Hom}_k(E, F) = E^* \otimes_k F$.

16. Sea L un A-módulo libre y $0 \to M' \to M \to L \to 0$ una sucesión exacta de A-módulos. Probar que la sucesión $0 \to M' \otimes_A N \to M \otimes_A N \to L \otimes_A N \to 0$ es exacta para todo A-módulo N.

17. Sea k un cuerpo. Si $\mathfrak{m}$ es un ideal maximal de $k[x_1, \ldots, x_n]$ tal que la k-álgebra $k[x_1, \ldots, x_n]/\mathfrak{m}$ es isomorfa a k, probar que existen $a_1, \ldots, a_n \in k$ tales que $\mathfrak{m} = (x - a_1, \ldots, x - a_n)$. Análogamente, si $\mathfrak{m}$ es un ideal maximal de una k-álgebra de tipo finito $k[\xi_1, \ldots, \xi_n]$ y $k[\xi_1, \ldots, \xi_n]/\mathfrak{m} \simeq k$, probar que $\mathfrak{m} = (\xi_1 - a_1, \ldots, \xi_n - a_n)$ para ciertos $a_1, \ldots, a_n \in k$.

18. Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de un anillo A y sea M un A-módulo. Si $\mathfrak{a} + \mathfrak{b} = A$, aplicar el teorema chino de los restos para probar que tenemos un isomorfismo de A-módulos natural $M/\mathfrak{a}\mathfrak{b}M = (M/\mathfrak{a}M) \oplus (M/\mathfrak{b}M)$.

19. Demostrar la existencia de isomorfismos de anillos:

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &\simeq \mathbb{C} \oplus \mathbb{C} \\ \mathbb{Q}(\sqrt[3]{2}\,) \otimes_{\mathbb{Q}} \mathbb{R} &\simeq \mathbb{R} \oplus \mathbb{C} \\ \mathbb{Q}(\omega) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}\,) &\simeq \mathbb{Q}(\omega, \sqrt[3]{2}\,) \ , \qquad \omega^2 + \omega + 1 = 0 \\ \mathbb{Q}(\sqrt[3]{2}\,) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}\,) &\simeq \mathbb{Q}(\sqrt[3]{2}\,) \oplus \mathbb{Q}(\omega, \sqrt[3]{2}\,) \end{aligned}$$

20. Determinar los elementos invertibles, los divisores de cero, los nilpotentes y los idempotentes de los siguientes anillos:

$$\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(i) \quad , \quad \mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \quad , \quad \mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2})$$

21. Sea A un álgebra sobre un cuerpo k. Probar que el morfismo de cambio de base $A \to A_K$ es inyectivo para toda k-álgebra K.

22. Sean $p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polinomios con coeficientes en un cuerpo k y sea K una extensión de k. Si $q(x_1, \ldots, x_n)$ pertenece al ideal generado por $p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n)$ en $K[x_1, \ldots, x_n]$, demostrar que $q(x_1, \ldots, x_n)$ está en el ideal de $k[x_1, \ldots, x_n]$ generado por los polinomios $p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n)$.

    (*Indicación*: Considerar el morfismo natural $A \to A_K$, donde A es el anillo de funciones algebraicas de la subvariedad $p_1 = 0, \ldots, p_r = 0$).

Espectro Primo

(*) Puntos del Espectro:

1. Consideremos un anillo de polinomios $k[x_1, \ldots, x_n]$ con coeficientes en un cuerpo k. Si $a_1, \ldots, a_n \in k$, el ideal $\mathfrak{m} = (x - a_1, \ldots, x - a_n)$ es maximal, luego define un punto cerrado del espectro del anillo $k[x_1, \ldots, x_n]$ y diremos que es el punto $(a_1, \ldots, a_n)$. Un polinomio $q(x_1, \ldots, x_n)$ se anula en este punto cuando $q(a_1, \ldots, a_n) = 0$. Nótese que $k[x_1, \ldots, x_n]/\mathfrak{m} = k$.

2. Sean $\alpha_1, \ldots, \alpha_n$ números complejos y supongamos que algún α_i no es real. En tal caso el correspondiente morfismo de anillos $\mathbb{R}[x_1, \ldots, x_n] \to \mathbb{C}$ es epiyectivo, así que su núcleo $\mathfrak{m}$ es un ideal maximal y $\mathbb{R}[x_1, \ldots, x_n]/\mathfrak{m} = \mathbb{C}$. Luego $\mathfrak{m}$ define un punto cerrado del espectro de $\mathbb{R}[x_1, \ldots, x_n]$ que no es de los construidos en el ejemplo anterior. Análogamente, $\mathfrak{m}$ define un punto cerrado del espectro de $\mathbb{R}[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$ cuando $p_j(\alpha_1, \ldots, \alpha_n) = 0$ para todo $1 \leq j \leq r$. Nótese que $\alpha_1, \ldots, \alpha_n$ definen el mismo punto que sus conjugados $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$.

3. Sea $p(x_1, \ldots, x_n)$ un polinomio irreducible con coeficientes en un cuerpo k. El ideal $(p(x_1, \ldots, x_n))$ del anillo $k[x_1, \ldots, x_n]$ es primo y define por tanto un punto de su espectro. Su cierre $(p)_0$ está formado por todos los puntos en que se anula $p(x_1, \ldots, x_n)$, así que es el punto genérico de la hipersuperficie de ecuación $p(x_1, \ldots, x_n) = 0$.

   El ideal 0 también es primo, porque el anillo $k[x_1, \ldots, x_n]$ es íntegro, y su cierre es todo el espectro. En general, si un anillo es íntegro, su espectro es irreducible y su punto genérico viene definido por el ideal 0, que es primo.

4. Sea k un cuerpo y $H = (q)_0$ el cerrado del espacio afín $\mathbb{A}_{n,k}$ definido por la anulación de un polinomio no constante $q(x_1, \ldots, x_n)$. Si

   $$q(x_1, \ldots, x_n) = p_1^{m_1} \cdots p_r^{m_r}$$

   es su descomposición en producto de potencias de polinomios irreducibles que no difieran en factores constantes, entonces

   $$(p_1^{m_1} \cdots p_r^{m_r})_0 = (p_1^{m_1})_0 \cup \ldots \cup (p_r^{m_r})_0$$

   Como $(p_i^{m_i})_0 = (p_i)_0$, tenemos que $H = (p_1)_0 \cup \ldots \cup (p_r)_0$. Ahora bien, el ideal (p_i) del anillo $k[x_1, \ldots, x_n]$ es primo, así que sus ceros forman un cerrado irreducible del espectro, y concluimos que H es unión de los cerrados irreducibles $(p_1)_0, \ldots, (p_r)_0$, que son por tanto las componentes irreducibles de H.

5. Vamos a calcular el espectro del anillo $\mathbb{Z}[\sqrt{-5}\,] \simeq \mathbb{Z}[x]/(x^2+5)$ aplicando la fórmula de la fibra a la aplicación continua natural $\operatorname{Spec}\mathbb{Z}[\sqrt{-5}\,] \to \operatorname{Spec}\mathbb{Z}$. Por el lema 7.2.10, la fibra de cada número primo p es el espectro de

$$\mathbb{Z}[\sqrt{-5}\,]/p\mathbb{Z}[\sqrt{-5}\,] \simeq \mathbb{Z}[x]/(p, x^2+5) \simeq \mathbb{F}_p[x]/(x^2+5)$$

Cuando la reducción módulo p de x^2+5 sea irreducible (es decir, cuando –5 no sea resto cuadrático módulo p, lo que ocurre en los primos $p = 11, 13, \ldots$) la fibra de p tiene un único punto, definido por el ideal maximal $p\mathbb{Z}[\sqrt{-5}\,]$.

Cuando la reducción de x^2+5 tenga una raíz doble en $\mathbb{F}_p$ (lo que ocurre sólo en los números primos $p = 2,\ 5$) la fibra de p tiene un único punto; pero el ideal $p\mathbb{Z}[\sqrt{-5}\,]$ no es maximal. Si $p = 2$, tal punto viene definido por el ideal maximal $(2, 1+\sqrt{-5}\,)$. Si $p = 5$, está definido por el ideal maximal $(5, \sqrt{-5}) = (\sqrt{-5}\,)$.

Cuando la reducción de x^2+5 tenga dos raíces simples (lo que ocurre en los números primos $p = 3,\ 7, \ldots$), la fibra de p tiene dos puntos, definidos por los ideales maximales $(p, \sqrt{-5}+a)$ y $(p, \sqrt{-5}-a)$, donde $a^2 \equiv -5$ (mód. p).

Según la fórmula de la fibra, la del punto genérico de $\operatorname{Spec}\mathbb{Z}$ coincide con el espectro de $\mathbb{Q}[\sqrt{-5}] = \mathbb{Q}(\sqrt{-5})$, así que tiene un único punto, definido por el ideal 0. Los ideales primos no nulos de $\mathbb{Z}[\sqrt{-5}\,]$ son maximales, y son:

$$(2, 1+\sqrt{-5}\,)\ , \quad (\sqrt{-5}\,)$$

$$(p)\ , \quad \text{si } -5 \text{ no es resto cuadrático módulo } p$$

$$(p, \sqrt{-5}+a)\ , \ (p, \sqrt{-5}-a) \quad \text{donde } a^2 \equiv -5 \text{ (mód. } p).$$

(*) Conexión del Espectro: De acuerdo con 7.2.3 cada descomposición $A = B_1 \oplus B_2$ de un anillo en suma directa induce una descomposición de su espectro en unión disjunta de dos abiertos:

$$\operatorname{Spec} A \;=\; (\operatorname{Spec} B_1) \coprod (\operatorname{Spec} B_2)$$

Recíprocamente, cada descomposición $\operatorname{Spec} A = U \coprod V$ del espectro en unión disjunta de dos abiertos induce una descomposición de A en suma directa de dos anillos.

En efecto, como U y V son cerrados, tenemos que $U = (\mathfrak{a})_0$ y $V = (\mathfrak{b})_0$ para ciertos ideales $\mathfrak{a}$, $\mathfrak{b}$ de A. Luego $(\mathfrak{a}+\mathfrak{b})_0 = U \cap V = \emptyset$ y se sigue que $\mathfrak{a}+\mathfrak{b} = A$; es decir,

$$1 = f + h \qquad , \quad f \in \mathfrak{a}\ , \quad h \in \mathfrak{b}\ .$$

así que f y h no pueden tener ceros comunes. Luego f se anula en todos los puntos de U y no se anula en ningún punto de V, mientras que h se anula en todos los

puntos de V y no se anula en ningún punto de U. En particular fh se anula en todos los puntos del espectro, y es nilpotente por el teorema 7.2.7; es decir, $f^n h^n = 0$. Ahora bien, como $(f^n)_0 \cap (h^n)_0 = U \cap V = \emptyset$, el Teorema chino de los restos permite concluir que el morfismo natural $A = A/f^n h^n A \to (A/f^n A) \oplus (A/h^n A)$ es un isomorfismo. En particular U y V son abiertos básicos de $\operatorname{Spec} A$.

(*) Variedades Algebraicas: Cuando hablamos de modo impreciso e intuitivo de algún lugar geométrico, lo que casi siempre tenemos claro son sus ecuaciones, así que podemos definirlo rigurosamente como variedad algebraica. Del grupo de las raíces n-ésimas de la unidad, lo que es obvio es que viene definido por la ecuación $x^n = 1$. Por tanto, la variedad algebraica μ_n de las raíces n-ésimas de la unidad sobre un cuerpo k debe definirse como

$$\mu_n = \operatorname{Spec} k[x]/(x^n - 1)$$

y sus puntos racionales son las raíces n-ésimas de la unidad en k; pero puede tener otros puntos, como ya ocurre cuando $k = \mathbb{Q}$, debido a la existencia de otras raíces n-ésimas de la unidad en extensiones no triviales de k.

Un polinomio $a_0 + a_1 x + \ldots + a_n x^n$ de grado $\leq n$ con coeficientes en un cuerpo k viene dado por sus coeficientes $(a_0, a_1, \ldots, a_n)$, así que la variedad algebraica de los polinomios de grado menor o igual que n sobre un cuerpo k debe definirse como el espacio afín $\operatorname{Spec} k[a_0, a_1, \ldots, a_n]$ donde $a_0, \ldots, a_n$ son indeterminadas. Ahora, los polinomios de grado n vienen dados por la condición $a_n \neq 0$, así que la variedad algebraica de los polinomios de grado n sobre un cuerpo k debe definirse como el abierto básico $U_{a_n} = \operatorname{Spec} k[a_0, a_1, \ldots, a_n, a_n^{-1}]$. La variedad algebraica de los polinomios de grado n con alguna raíz múltiple, caracterizados por la anulación del discriminante $\Delta(a_0, a_1, \ldots, a_n)$, debe definirse como

$$\operatorname{Spec} k[a_0, \ldots, a_n, a_n^{-1}]/(\Delta)$$

y la variedad algebraica de los polinomios de grado n sin raíces múltiples se define como

$$\operatorname{Spec} k[a_0, \ldots, a_n, a_n^{-1}, \Delta^{-1}]$$

Como último ejemplo citemos el grupo lineal general $\mathbf{Gl}_n$ (el grupo de las matrices $n \times n$ invertibles) que claramente debe definirse como

$$\mathbf{Gl}_n = \operatorname{Spec} k[\, a_{ij}, |a_{ij}|^{-1}] \,, \quad 1 \leq i, j \leq n$$

donde $|a_{ij}|$ denota el determinante de la matriz (a_{ij}), y el grupo unitario $\mathbf{U}_n$, que es la subvariedad de $\mathbf{Gl}_n$ de ecuación $|a_{ij}| = 1$; es decir,

$$\mathbf{U}_n = \operatorname{Spec} k[a_{ij}, |a_{ij}|^{-1}]/(|a_{ij}| - 1)$$

(*) Álgebras de Boole: Un álgebra de Boole (1815-1864) es un conjunto A dotado de dos operaciones $\wedge$, $\vee$ que verifican las propiedades del cálculo proposicional (ver página 220):

1. Ambas operaciones son asociativas, conmutativas, y admiten neutro:
$$a \wedge 0 = a \quad , \quad a \vee 1 = A$$
2. Distributiva: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad , \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.
3. Absorción: $a \vee 0 = 0 \quad , \quad a \wedge 1 = 1$.
4. Idempotencia: $a \vee a = a \quad , \quad a \wedge a = a$.
5. Negación: Si $a \in A$, existe $\bar{a} \in A$ tal que $\bar{a} \wedge a = 1$ y $\bar{a} \vee a = 0$.

El ejemplo fundamental de álgebra de Boole lo proporcionan el álgebra $\mathcal{P}(X)$ de las partes de un conjunto X, donde $\wedge$ es la intersección y $\vee$ es la unión, de modo que $0 = X$, $1 = \emptyset$ y $\bar{a}$ es el complementario de a . También los enunciados de cualquier teoría lógica formalizada (que incluya los conectores "no", "y", "o") siempre que se identifiquen los enunciados equivalentes (i.e., identificamos α y β cuando $\alpha \Leftrightarrow \beta$ sea un teorema de tal teoría).

En las álgebras de Boole se definen la implicación $\Rightarrow$ y la equivalencia $\Leftrightarrow$ del siguiente modo:

$$a \Rightarrow b \ := \ \bar{a} \vee b \qquad , \qquad a \Leftrightarrow b \ := \ (\bar{a} \vee b) \wedge (a \vee \bar{b})$$

y es sencillo comprobar que en todo álgebra de Boole $(A; \vee, \wedge)$, las operaciones

$$a + b \ := \ a \Leftrightarrow b \qquad , \qquad a \cdot b \ := \ a \vee b$$

definen una estructura de anillo conmutativo con unidad en el que todo elemento es idempotente: $a^2 = a$. Tales anillos reciben el nombre de anillos de **Boole**. Recíprocamente, si $(A; +, \cdot)$ es un anillo de Boole, obtenemos en A una estructura de álgebra de Boole (donde la negación es $\bar{a} = 1 + a$) sin más que definir

$$a \wedge b \ := \ a + b + ab \qquad , \qquad a \vee b \ := \ a \cdot b$$

Los anillos de Boole son de característica 2 porque $2^2 = 2$. Además, todo anillo de Boole íntegro es el cuerpo $\mathbb{F}_2$, porque la condición $a(a-1) = a^2 - a = 0$ implica que $a = 0$ ó $a = 1$. Luego en todo anillo de Boole A los ideales primos $\mathfrak{p}$ son maximales y de cuerpo residual $A/\mathfrak{p} = \mathbb{F}_2$.

Como cada morfismo de anillos $A \to \mathbb{F}_2$ está totalmente determinado por su núcleo, tenemos que

$$\operatorname{Spec} A \ = \ \operatorname{Hom}(A, \mathbb{F}_2)$$

Es decir, los puntos $x \in X := \operatorname{Spec} A$ del espectro de un anillo de Boole A se corresponden con los morfismos $v_x \colon A \to \mathbb{F}_2$, que son las valoraciones o interpretaciones coherentes de A como familia de proposiciones verdaderas o falsas. Por tanto, cada elemento $f \in A$ define una función $f \colon X \to \mathbb{F}_2$, sin más que poner $f(x) := v_x(f)$, que se anula precisamente en $(f)_0$. Si consideramos en el cuerpo $\mathbb{F}_2$ la topología

discreta, estas funciones son continuas, pues $U_f = (1+f)_0$. Además, así se obtiene toda función continua $X \to \mathbb{F}_2$, porque dar tal función equivale a descomponer el espectro como unión de dos cerrados disjuntos, $X = Y_0 \coprod Y_1$, de modo que Y_0 son los ceros de algún $f \in A$, según se ha visto en el apartado anterior.

Como la condición $f^2 = f$ claramente implica que todo elemento nilpotente de un anillo de Boole A es nulo, el teorema 7.2.7 muestra que cada elemento de A está totalmente determinado por la función que define sobre el espectro, de modo que A puede entenderse como el anillo de las funciones continuas sobre su espectro X con valores en $\mathbb{F}_2$. Como además cada función con valores en $\mathbb{F}_2$ está determinada por sus ceros, vemos así que todo álgebra de Boole A es un álgebra de partes de su espectro X (a saber, los cerrados abiertos de X).

Según 7.2.8 cada ideal I de un anillo de Boole A está formado por todas las funciones continuas $X \to \mathbb{F}_2$ que se anulan en el cerrado $(I)_0$. Así pues, fijada una familia de axiomas $B \subset A$, el ideal que genera B está formado por las funciones $f \in A$ que se anulan en el cerrado $\bigcap_{b\in B}(b)_0$; i.e., por los enunciados que son verdaderos en cualquier interpretación coherente que verifique los axiomas fijados:

$$v(f) = 0 \text{ siempre que } v(b) = 0 \text{ para todo } b \in B$$
$$f \text{ es verdadero siempre que lo sea todo } b \in B$$

En principio eso no significa que el enunciado f pueda derivarse de los axiomas fijados y tautologías (el 0), usando sólo el "Modus Ponens"; enunciados que forman el menor subconjunto B' que, incluyendo a B y al 0, tenga la siguiente propiedad:

$$\text{Si } a \in B' \text{ y } (a \Rightarrow b) \in B' \text{ , entonces } b \in B'$$

Tal conjunto B' está contenido en el ideal de A generado por B, pues claramente los ideales tienen la propiedad anterior, ya que $(a \Leftrightarrow b) = a + b$ y $b = a + (a + b)$. De hecho B' coincide con el ideal generado por B; es decir, B' es un ideal:

Si $a \in A$ y $b \in B'$, como $b \Rightarrow (a \vee b)$ es nulo, tenemos que $ab = (a \vee b) \in B'$.

Si $a, b \in B'$, como $a \Rightarrow (b \Rightarrow (a \Leftrightarrow b))$ es nulo, tenemos que $b \Rightarrow (a \Leftrightarrow b)$ está en B' y concluimos que $a + b = (a \Leftrightarrow b) \in B'$.

En resumen, si un enunciado es cierto en todas las interpretaciones coherentes que satisfagan la familia de axiomas B, entonces puede deducirse en un número finito pasos usando tautologías y el "Modus Ponens".

Ejercicios:

1. Sea A un anillo reducido. Probar que $\operatorname{Spec} A$ es irreducible si y sólo si A es íntegro. ¿Es cierto el resultado si se elimina la hipótesis de que A sea reducido?

2. Probar que la condición necesaria y suficiente para que un punto x' sea una especialización de un punto x es que x esté en todos los entornos de x'.

3. Sea A un anillo y $f, g \in A$. Probar que $U_f \subseteq U_g \Leftrightarrow g$ divide a alguna potencia de f.

4. Sea $\mathfrak{a}$ un ideal de un anillo A. Probar que la condición necesaria y suficiente para que $\operatorname{Spec}(A/\mathfrak{a}) = \operatorname{Spec} A$ es que el ideal $\mathfrak{a}$ esté generado por elementos nilpotentes. Concluir que $\operatorname{Spec} A$ es irreducible precisamente cuando el cociente de A por su radical sea un anillo íntegro.

5. Hallar el espectro, determinar sus componentes irreducibles, sus componentes conexas y calcular la dimensión de los anillos:

   $\mathbb{R}[x]/(x^4+x^2)$, $\mathbb{R}[x]/(x^4+x^2) \otimes_{\mathbb{R}} \mathbb{C}$, $\mathbb{C}[x]/(x^4+x^2) \otimes_{\mathbb{C}} \mathbb{C}[y]/(y^2+1)$,
   $\mathbb{C}[x,y]/(x^2+y^2)$, $\mathbb{C}[x,x^{-1}]$, $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{R}$, $\mathbb{C}[x,y]/(y^2+x, y^2-xy+x)$,
   $\mathbb{C}[x,y]/(xy+2, x^3-x+y^2x)$.

6. Demostrar que todo elemento de un ideal primo minimal es un divisor de cero. (*Indicación*: Localizar en el punto definido por el ideal primo).

7. Si un morfismo de anillos $A \to B$ es epiyectivo y $\mathfrak{a}$ es su núcleo, probar que la correspondiente aplicación continua $\operatorname{Spec} B \to \operatorname{Spec} A$ es un homeomorfismo de $\operatorname{Spec} B$ con $(\mathfrak{a})_0$.

8. Si un morfismo de anillos $j\colon A \to B$ es inyectivo, probar que la correspondiente aplicación continua $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ tiene imagen densa.

   (*Indicación*: Si un cerrado $(\mathfrak{a})_0$ contiene a la imagen de ϕ, entonces $\mathfrak{a}B \subseteq \operatorname{rad} B$ y por tanto $\mathfrak{a} \subseteq \operatorname{rad} A$).

9. Sea $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación continua inducida por un morfismo de anillos $A \to B$. Probar que el cierre de la imagen de ϕ es $(\operatorname{Ker} j)_0$.

   En general, si $\mathfrak{b}$ es un ideal de B, el cierre de $\phi(\mathfrak{b})_0$ coincide con $(\mathfrak{b} \cap A)_0$.

10. Sea A un anillo y $X = \operatorname{Spec} A$. Probar que un punto $x \in X$ es denso precisamente cuando su ideal primo $\mathfrak{p}_x$ coincide con el radical $\mathrm{r}(A)$ de A. Concluir que X tiene un punto denso si y sólo si $\mathrm{r}(A)$ es un ideal primo.

11. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales de un anillo A. Demostrar que $(\mathfrak{a})_0 \subseteq (\mathfrak{b})_0$ precisamente cuando $\mathrm{r}(\mathfrak{b}) \subseteq \mathrm{r}(\mathfrak{a})$.

12. Sea A un anillo. Si una función $f \in A$ es idempotente, $f^2 = f$, demostrar que sus ceros son un abierto cerrado de $\operatorname{Spec} A$. Concluir que $\operatorname{Spec} A$ no es conexo cuando existe algún idempotente $f \neq 0, 1$.

13. Probar, usando el lema de Zorn, que todo espacio topológico es unión de sus componentes irreducibles. Concluir que todo ideal primo de un anillo A contiene algún ideal primo minimal de A.

14. Sea S un sistema multiplicativo de un anillo A. Probar que el morfismo canónico $\gamma\colon A \to A_S$ es un isomorfismo precisamente cuando la aplicación continua $\operatorname{Spec} A_S \to \operatorname{Spec} A$ inducida por γ es un homeomorfismo.

15. Sean S y T dos sistemas multiplicativos de un anillo A. Probar que si $\operatorname{Spec} A_S = \operatorname{Spec} A_T$ (como subespacios de $\operatorname{Spec} A$), entonces $A_S = A_T$.

16. Sea $\mathfrak{m}$ el ideal maximal de A definido por un punto cerrado $x \in \operatorname{Spec} A$. Probar que $A_x = A_{1+\mathfrak{m}}$.

17. Hallar la fibra de todos los puntos en los siguientes morfismos entre variedades algebraicas complejas:

    (a) La parametrización $x = t^2$, $y = t^3$ de la curva $y^2 = x^3$.

    (b) La parametrización $x = t^2 - 1$, $y = t^3 - t$ de la curva $y^2 = x^3 + x^2$.

    (c) La proyección $\pi\colon \mathbb{A}_2 \to \mathbb{A}_1$, $\pi(x, y) = xy$.

18. Calcular el espectro del anillo $\mathbb{Z}[\sqrt{d}\,]$ cuando $d = 2, 3, 5, -1, -2, -3$. Calcular el espectro de $\mathbb{Z}[\omega]$, donde ω denota una raíz cúbica primitiva de la unidad, y las fibras del morfismo natural $\operatorname{Spec} \mathbb{Z}[\,\omega\,] \to \operatorname{Spec} \mathbb{Z}[\sqrt{-3}\,]$.

19. Sean I, J ideales de un anillo A. Probar que el morfismo natural

$$A/(I \cap J) \;\longrightarrow\; (A/I) \times_{A/(I+J)} (A/J)$$

    es un isomorfismo, donde

$$(A/I) \times_{A/(I+J)} (A/J) := \{(\bar{a}, \bar{b}) \in (A/I) \times (A/J)\colon\ \bar{a} = \bar{b} \text{ en } A/(I+J)\}$$

    Sean $Y_1 = (I_1)_0$, $Y_2 = (I_2)_0$ dos subvariedades algebraicas cerradas de una variedad algebraica afín X. Dadas funciones algebraicas f_1, f_2 sobre Y_1 e Y_2 respectivamente, que coincidan en $Y_1 \cap Y_2$ (la subvariedad definida por $I_1 + I_2$), probar que existe una única función algebraica sobre $Y_1 \cup Y_2$ (la subvariedad definida por $I_1 \cap I_2$) que coincide con f_1 en Y_1 y con f_2 en Y_2.

20. Sea $\mu_6 = \operatorname{Spec} k[x]/(x^6 - 1)$ el grupo de las raíces sextas de la unidad sobre un cuerpo k. Determinar si es una variedad íntegra o reducida, y calcular el número de componentes irreducibles cuando $k = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$.

21. Sea $\mathbf{P}_2 = \operatorname{Spec} k[\,a, b, c, a^{-1}]$ la variedad algebraica de los polinomios de grado dos $at^2 + bt + c$ con coeficientes en un cuerpo k y sea X la subvariedad cerrada de $\mathbf{P}_2$ de ecuación $b^2 = 4ac$ (es decir, la subvariedad de los polinomios de

grado 2 con alguna raíz múltiple). Determinar si X es íntegra o reducida, y calcular sus componentes conexas y sus componentes irreducibles cuando $k = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$.

Definir la variedad $\mathbf{P}_1$ de los polinomios de grado 1 con coeficiente en k y el morfismo "elevar al cuadrado" $\phi\colon \mathbf{P}_1 \to X$. Calcular la fibra de ϕ sobre el punto racional de X correspondiente al polinomio $t^2 + 2t + 1$ y sobre el punto genérico de X. ¿Es ϕ un isomorfismo?

22. Sea $\mathbf{U}_2 = \operatorname{Spec} k[\,b, c\,]$ la variedad algebraica afín de los polinomios unitarios $t^2 + bt + c$ de grado 2 con coeficientes en un cuerpo k y sea Y la subvariedad cerrada de ecuación $b^2 = 4c$. Definir la variedad algebraica $\mathbf{U}_1$ de los polinomios unitarios de grado 1 con coeficientes en k y comprobar si el morfismo "elevar al cuadrado" $\mathbf{U}_1 \to Y$ es un isomorfismo. Calcular la fibra de cada punto en el morfismo $\mathbf{U}_1 \times \mathbf{U}_1 \to \mathbf{U}_2$ definido por el producto de polinomios cuando $k = \mathbb{C}$, y la fibra del punto correspondiente al polinomio $x^2 + 1$ cuando $k = \mathbb{F}_2$.

23. Sea X una variedad algebraica afín íntegra sobre un cuerpo. Si dos morfismos de X en otra variedad algebraica afín Y coinciden en un abierto básico no vacío de X, probar que coinciden en X.

24. Sea C la curva plana $y^2 = x^2 - 2x$. Si consideramos el punto de intersección variable con las rectas $y = tx$, ¿en qué abierto U de $\operatorname{Spec} k[\,t\,]$ tenemos definido un morfismo $U \to C$? Análogamente para las curvas $y^2 = x^2 - x^3$, $x^n = y^{n+1}$, $x^{n+1} = y^n$.

25. Sea C una curva $p(x, y) = 0$ del plano afín complejo. Si a cada punto de C le asignamos la recta $y = tx$ que pasa por él, ¿en qué abierto U de C tenemos definido un morfismo $U \to \operatorname{Spec} \mathbb{C}\,[\,t\,]$? (discutir separadamente el caso en que C pase por el origen).

26. Definir la variedad algebraica afín $\mathbf{G}_m$ de los elementos no nulos de un cuerpo k, y los morfismos $\mathbf{G}_m \times \mathbf{G}_m \to \mathbf{G}_m$, $\mathbf{G}_m \to \mathbf{G}_m$ correspondientes al producto y el paso al inverso.

    Análogamente para el grupo aditivo $\mathbf{G}_a$ definido por la suma de k. Si la característica de k es 3, demostrar que $\mathcal{P}\colon \mathbf{G}_a \to \mathbf{G}_a$, $\mathcal{P}(x) = x^3 - x$, es un morfismo de grupos. Calcular su núcleo y la fibra del punto genérico de $\mathbf{G}_a$.

Localización

(*) Localización:

1. Sea A un anillo. Los elementos de A que no son divisores de cero forman un sistema multiplicativo S en A, y la localización $S^{-1}A$ se llama *anillo total de fracciones* de A.

2. Sea $j\colon A \to B$ un morfismo de anillos y sea S un sistema multiplicativo de A. La localización de B por S coincide con la localización de B por el sistema multiplicativo $j(S)$; es decir, $S^{-1}B = j(S)^{-1}B$.

   En particular, la localización B_x de B en un punto $x \in \operatorname{Spec} A$ coincide con la localización del A-módulo B por el sistema multiplicativo de las funciones $f \in A$ que no se anulan en x.

3. Si $\mathfrak{a}$ es un ideal de un anillo A, entonces $S^{-1}\mathfrak{a}$ es un ideal de $S^{-1}A$, que coincide con $\mathfrak{a}(S^{-1}A)$. Así se obtienen todos los ideales de $S^{-1}A$: si $\mathfrak{b}$ es un ideal de $S^{-1}A$, entonces $\mathfrak{b} = S^{-1}\mathfrak{a}$, donde $\mathfrak{a} = \mathfrak{b} \cap A$.

   En particular, si A es un dominio de ideales principales (respectivamente un anillo noetheriano), también lo es $S^{-1}A$.

4. En la correspondencia entre ideales primos de un anillo A que no corten a cierto sistema multiplicativo S e ideales primos de $S^{-1}A$ (ver 7.2.4), cada ideal primo $\mathfrak{p}$ de A que no corte a S se corresponde con el ideal primo $S^{-1}\mathfrak{p} = \mathfrak{p}(S^{-1}A)$ del anillo $S^{-1}A$.

5. Sea A un anillo y U un abierto básico de $\operatorname{Spec} A$. La localización de un A-módulo M por el sistema multiplicativo de las funciones $f \in A$ que no se anulan en ningún punto de U se denotará M_U. Diremos que dos elementos de M coinciden en el abierto U cuando coinciden en M_U.

   Sea x un punto de $\operatorname{Spec} A$ y $\mathfrak{p}$ su ideal primo. La localización de M por el sistema multiplicativo $A - \mathfrak{p}$ de las funciones $f \in A$ que no se anulan en x se denotará M_x o $M_{\mathfrak{p}}$ y diremos que es la localización de M en el punto x o en el ideal primo $\mathfrak{p}$. La imagen de cada elemento $m \in M$ por el correspondiente morfismo de localización se denotará m_x. Por definición, la condición $m_x = 0$ significa que $fm = 0$ para alguna función $f \in A$ que no se anula en x; de modo que m se anula en M_{U_f}. Por tanto, *la condición necesaria y suficiente para que la localización de m en x sea nula es que m se anule en algún entorno básico de x*. Las relaciones que se dan en M_x son las relaciones válidas en algún entorno de x. Diremos que A_x es el *anillo local* en el punto x. A la luz de esta comprensión, el paso de $\mathbb{Z}$ a $\mathbb{Q}$, de importancia evidente, significa pasar de todo el espectro de $\mathbb{Z}$ a un entorno suficientemente pequeño del número primo genérico.

6. Sea $\mathcal{C}(X)$ el anillo de las funciones reales continuas sobre un espacio metrizable X. Sea U un abierto de X y consideremos el sistema multiplicativo S formado por las funciones que no se anulen en ningún punto de U. Si $g \in S$, la restricción g_U de g a U es invertible, así que el morfismo de restricción $\mathcal{C}(X) \to \mathcal{C}(U)$ induce un morfismo de anillos

$$S^{-1}\mathcal{C}(X) \longrightarrow \mathcal{C}(U) \quad ; \qquad f/g \mapsto f_U\,(g_U)^{-1}$$

que es un isomorfismo. En efecto, si $f_U = 0$, entonces $fd = 0$, donde d denota la función "distancia a $X - U$", y concluimos que $f/1 = 0$. Además, si $h \in \mathcal{C}(U)$, entonces la función

$$g = \min\big(d, (1+h^2)^{-1}\big)$$

prolongada por 0 fuera de U, es continua y no se anula en ningún punto de U. También la función $f = hg$, prolongada por 0 fuera de U, es continua y claramente tenemos que $h = f_U\,(g_U)^{-1}$.

Por otra parte, se dice que dos funciones continuas definidas en algún entorno de un punto $x \in X$ tienen el mismo **germen** en x si coinciden en algún entorno x. Del razonamiento anterior se sigue que, bajo las hipótesis consideradas, cada función continua definida en algún entorno de x tiene el mismo germen en x que un cociente de dos funciones continuas sobre X, donde el denominador no se anula en x. Ahora es fácil concluir que el anillo de los gérmenes en x de funciones continuas coincide con la localización de $\mathcal{C}(X)$ por el sistema multiplicativo $S = \{f \in \mathcal{C}(X) \colon\ f(x) \neq 0\}$.

7. Sea X una variedad algebraica afín sobre un cuerpo. El anillo local en un punto $x \in X$ se denota $\mathcal{O}_{X,x}$, o bien $\mathcal{O}_x$ si no hay lugar a confusión. Por definición $\mathcal{O}_{X,x}$ es la localización de $\mathcal{O}(X)$ por las funciones sobre X que no se anulan en el punto x, así que cada elemento $g/f \in \mathcal{O}_x$ viene dado por una función algebraica definida en algún entorno básico U_f de x.

   Cuando el anillo $\mathcal{O}(X)$ es íntegro, el anillo local de X en su punto genérico, que es el cuerpo de fracciones de $\mathcal{O}(X)$, lo denotaremos Σ_X y diremos que es el cuerpo de **funciones racionales** de X. Cada función racional $g/f \in \Sigma_X$ viene dada por una función algebraica definida en algún abierto no vacío de X, pues todo abierto básico no vacío es un entorno del punto genérico de X. En este caso los morfismos de localización son inyectivos, por lo que podemos considerar los anillos $\mathcal{O}(U_f)$ y los anillos $\mathcal{O}_{X,x}$ como subálgebras de Σ_X .

(*) Anillos Locales de Curvas Planas:

Sea $k[\xi,\eta]$ el anillo de funciones algebraicas de una curva plana C sobre un cuerpo k de ecuación $p(x,y) = 0$ y supongamos que esta curva pasa por un punto racional (a,b), de modo que $\mathfrak{m} = (\xi - a, \eta - b)$ es un ideal maximal de $k[\xi,\eta]$. Veamos la simplificación que supone pasar del anillo $k[\xi,\eta]$ al anillo local $\mathcal{O}$ de la curva C

en el punto (a, b). La condición de que una función $q(\xi, \eta)$ se anule al localizar en tal punto es que $q(x, y)r(x, y)$ sea múltiplo de $p(x, y)$ para algún polinomio $r(x, y)$ que no se anule en (a, b). Considerando una descomposición $p(x, y) = p_1 \cdots p_r$ en producto de factores irreducibles, concluimos que la localización de $q(\xi, \eta)$ es nula precisamente cuando $q(x, y)$ sea múltiplo del producto de todos los factores irreducibles $p_i(x, y)$ que se anulen en (a, b). Si en la descomposición no aparecen factores que difieran en una constante, esta condición equivale a que $q(\xi, \eta)$ se anule en todas las componentes irreducibles de la curva que pasen por el punto (a, b). Al localizar en un punto nos desentendemos del comportamiento de las funciones en las componentes irreducibles que no pasen por tal punto.

(*) Fórmula de la Fibra:

Sea x un punto del espectro de un anillo A y sea $\mathfrak{p}$ su ideal primo. Llamaremos **cuerpo residual** del punto x al cuerpo de fracciones del anillo íntegro $A/\mathfrak{p}$ y se denota $\kappa(x)$ ó $\kappa(\mathfrak{p})$:

$$\kappa(x) = (A/\mathfrak{p})_x = A_x/\mathfrak{p}A_x$$

Si B es una A-álgebra, se llama **anillo de la fibra** de x a la $\kappa(x)$-álgebra

$$B \otimes_A \kappa(x) = (B/\mathfrak{p}B)_x = B_x/\mathfrak{p}B_x$$

pues, de acuerdo con la fórmula de la fibra, la fibra de la aplicación continua $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ inducida por un morfismo de anillos $A \to B$ coincide con el espectro del anillo de la fibra:

$$\phi^{-1}(x) = \operatorname{Spec}\big(B \otimes_A \kappa(x)\big)$$

En el caso de una variedad algebraica afín X sobre un cuerpo k, un punto $x \in X$ es racional precisamente cuando $k = \kappa(x)$. Si X es la subvariedad de un espacio afín $\mathbb{A}_n$ definida por un sistema de ecuaciones y x es el punto de X definido por cierta solución $(\alpha_1, \ldots, \alpha_n)$ del sistema en una extensión de k, entonces

$$\begin{aligned} \mathcal{O}(X)/\mathfrak{p} &\simeq k[\alpha_1, \ldots, \alpha_n] \\ \kappa(x) &\simeq k(\alpha_1, \ldots, \alpha_n) \end{aligned}$$

Además, si $\phi\colon Y \to X$ es un morfismo de variedades algebraicas afines, la $\kappa(x)$-álgebra $\mathcal{O}(Y) \otimes_{\mathcal{O}(X)} \kappa(x)$ es de tipo finito y define sobre la fibra $\phi^{-1}(x)$ una estructura de variedad algebraica afín sobre el cuerpo residual $\kappa(x)$. Las fibras de los puntos racionales son variedades algebraicas sobre k, mientras que las fibras de los otros puntos son variedades algebraicas sobre extensiones del cuerpo base k.

(*) Sea $\mathfrak{m}$ un ideal maximal de un anillo A y sea x el correspondiente punto cerrado de $\operatorname{Spec} A$. De acuerdo con 8.2.8:

$$\mathfrak{m}^r/\mathfrak{m}^n \;=\; \mathfrak{m}_x^r/\mathfrak{m}_x^n\;, \quad n \geq r$$

En particular $A/\mathfrak{m}^n = A_x/\mathfrak{m}_x^n$. Luego $\mathfrak{m}^n = A \cap \mathfrak{m}^n A_x$ y vemos que el problema de decidir si una función $f \in A$ pertenece a cierta potencia de $\mathfrak{m}$ es una cuestión local en x: basta resolver el problema en la localización A_x.

Por ejemplo, consideremos el anillo local $\mathcal{O}_p$ del espacio afín $\mathbb{A}_{n,k}$ en un punto racional $p = (a_1, \ldots, a_n)$. Poniendo $t_i = x_i - a_i$ tenemos que

$$\mathcal{O}_p/\mathfrak{m}^{r+1}\mathcal{O}_p = k[x_1, \ldots, x_n]/\mathfrak{m}^{r+1} = \begin{bmatrix}\text{Polinomios de grado} \\ \leq r \text{ en } t_1, \ldots, t_n\end{bmatrix}$$

y la clase de restos $\bar{f}$ de cualquier función $f \in \mathcal{O}_p$ en $\mathcal{O}_p/\mathfrak{m}^{r+1}\mathcal{O}_p$ se llama **desarrollo de Taylor** (1685-1731) de f hasta el orden r en el punto p pues, cuando $k = \mathbb{C}$, de hecho $f = h(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ define una función (en el sentido del Análisis) en un entorno de $(a_1, \ldots, a_n)$ y el desarrollo de Taylor clásico de orden r de esta función en tal punto difiere de f en un elemento de $\mathfrak{m}^{r+1}$.

Sgún el Lema de Nakayama, para que $\mathfrak{m}^r\mathcal{O}_p$ esté contenido en un ideal dado $\mathfrak{a}$ del anillo $\mathcal{O}_p$ es necesario y suficiente que

$$\mathfrak{m}^r/\mathfrak{m}^{r+1} = \{\text{Polinomios homogéneos de grado } r \text{ en } t_1, \ldots, t_n\}$$

esté contenido en el ideal $\bar{\mathfrak{a}}$ de $\mathcal{O}_p/\mathfrak{m}^{r+1}$ formado por los desarrollos de Taylor hasta el orden r de las funciones de $\mathfrak{a}$ (es decir, $\bar{\mathfrak{a}}$ es la imagen de $\mathfrak{a}$ por la proyección canónica $\pi\colon \mathcal{O}_p \to \mathcal{O}_p/\mathfrak{m}^{r+1}\mathcal{O}_p$). Nótese que $\bar{\mathfrak{a}}$ está formado por las combinaciones lineales con coeficientes en k de los desarrollos de Taylor de un sistema de generadores de $\mathfrak{a}$ y sus productos por monomios en $t_1, \ldots, t_n$ de grado $\leq r$.

(*) Anillos Noetherianos:

1. Los cuerpos y dominios de ideales principales son anillos noetherianos.

2. Sea $\mathcal{C}(X)$ el anillo de las funciones reales continuas sobre un espacio topológico metrizable X, sea x un punto de X y sea $\mathfrak{m}$ el ideal maximal de $\mathcal{C}(X)$ formado por las funciones que se anulan en x. Si $f \in \mathfrak{m}$, entonces

$$f = f_+ - f_- = \left(\sqrt{f_+}\right)^2 - \left(\sqrt{f_-}\right)^2 \,, \quad f_+ = \sup(f, 0)\,,\ f_- = \sup(-f, 0)$$

   Luego $f \in \mathfrak{m}^2$ y obtenemos que $\mathfrak{m} = \mathfrak{m}^2$. Si $\mathfrak{m}\mathcal{O}$ fuera un ideal finito-generado, el lema de Nakayama (19121964) permitiría concluir que $\mathfrak{m}\mathcal{O} = 0$, donde $\mathcal{O} = \mathcal{C}(X)_{\mathfrak{m}}$ denota el anillo de gérmenes en x de funciones continuas. Ahora bien, si el germen en x de la función continua "distancia a x" es nulo, entonces x es un punto aislado de X. En resumen, si algún punto x de X no está aislado, entonces el ideal $\mathfrak{m}\mathcal{O}$ no es finito-generado y los anillos $\mathcal{O}$ y $\mathcal{C}(X)$ no son noetherianos.

3. Todo elemento no nulo ni invertible de un anillo noetheriano íntegro A descompone en producto de elementos irreducibles. En efecto, en caso contrario entre los ideales generados por elementos no nulos ni invertibles para los que fuera falsa tal afirmación habría alguno maximal aA. Luego a descompone en producto de dos elementos no invertibles, $a = bc$. Por ser A íntegro, los ideales bA y cA contienen estrictamente al ideal aA, así que b y c descomponen en producto de elementos irreducibles y lo mismo ha de ocurrir con a, lo que lleva a contradicción. En particular, todo dominio de ideales principales es un dominio de factorización única, pues la demostración de la unicidad de la descomposición en factores irreducibles dada en los anillos euclídeos sigue siendo válida en los dominios de ideales principales.

(*) Ideales Primarios:

1. Los ideales primarios de $\mathbb{Z}$ son los ideales engendrados por una potencia de un número primo. Los ideales primarios del anillo de polinomios $k[x]$ con coeficientes en un cuerpo k son los ideales engendrados por una potencia de un polinomio irreducible. En general, los ideales primarios de un dominio de ideales principales son los ideales engendrados por una potencia de un elemento irreducible.

2. Toda intersección $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ de ideales $\mathfrak{p}$-primarios es un ideal $\mathfrak{p}$-primario. En efecto, tenemos que

$$r(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n) = r(\mathfrak{q}_1) \cap \ldots \cap r(\mathfrak{q}_n) = \mathfrak{p} \cap \ldots \cap \mathfrak{p} = \mathfrak{p}$$

   y, si $ab \in \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ y $a \notin \mathfrak{q}_i$ para algún índice i, entonces $b \in r(\mathfrak{q}_i) = \mathfrak{p}$ porque el ideal $\mathfrak{q}_i$ es primario.

3. Sea A un dominio de factorización única y p un elemento irreducible de A. El ideal $\mathfrak{p} = pA$ es primo y los ideales $p^r A$, $r \geq 1$, son $\mathfrak{p}$-primarios, pues su radical es pA y si un producto ab es múltiplo de p^r y un factor no lo es, el otro factor ha de ser múltiplo de p. Más aún, éstos son los únicos ideales $\mathfrak{p}$-primarios de A: si p^r es la primera potencia de p que está en un ideal $\mathfrak{p}$-primario $\mathfrak{q}$, entonces $\mathfrak{q} = p^r A$, pues si $ap^m \in \mathfrak{q}$ y $a \notin pA$, entonces $p^m \in \mathfrak{q}$, de modo que $m \geq r$ y $ap^m \in p^r A$.

   En particular, si $p(x_1, \ldots, x_n)$ es un polinomio irreducible con coeficientes en un cuerpo k, los únicos ideales (p)-primarios de $k[x_1, \ldots, x_n]$ son los ideales (p^r). Es usual decir que los polinomios del ideal (p^r) son los que se anulan r veces en la hipersuperficie $p(x_1, \ldots, x_n) = 0$.

(*) Ideales de $\mathbb{C}[x,y]$:

De acuerdo con el teorema de existencia de descomposiciones primarias, todo ideal no nulo $\mathfrak{a}$ de $\mathbb{C}[x,y]$ es de la forma:

$$\mathfrak{a} = (p_1^{n_1}) \cap \ldots \cap (p_r^{n_r}) \cap \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$$

donde $p_1(x,y), \ldots, p_r(x,y)$ son polinomios irreducibles en $\mathbb{C}[x,y]$ y $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ son ideales primarios cuyos radicales $\mathfrak{m}_i = r(\mathfrak{q}_i)$ son ideales maximales, de modo que cada uno de estos ideales $\mathfrak{m}_i$ está formado por todos los polinomios que se anulen en cierto punto (a_i, b_i). Es decir, el ideal $\mathfrak{a}$ está formado por los polinomios que se anulen determinado número de veces en unas curvas irreducibles $p_j(x,y) = 0$ y cuyos desarrollos de Taylor en unos puntos (a_i, b_i) verifiquen ciertas condiciones. La condición de que la componente $\mathfrak{q}_i$ esté sumergida significa que alguna de las curvas $p_j(x,y) = 0$ pasa por el punto (a_i, b_i).

(*) Sea $\mathfrak{a}$ un ideal de un anillo noetheriano A y sean $x_1, \ldots, x_r$ los puntos genéricos de las componentes irreducibles de sus ceros $(\mathfrak{a})_0$. En cualquier descomposición primaria reducida de $\mathfrak{a}$ aparecen unas componentes $\mathfrak{q}_i$ asociadas a los puntos x_i, y no dependen de la descomposición, pues $\mathfrak{q}_i = A \cap \mathfrak{a}A_{x_i}$. Sin embargo, si $\mathfrak{a}$ no coincide con $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$, en cualquier descomposición primaria reducida de $\mathfrak{a}$ han de aparecer otras componentes sumergidas, asociadas a otros puntos de $(\mathfrak{a})_0$, y éstas sí pueden depender de la descomposición elegida. Por ejemplo, sea $\mathfrak{a}$ el ideal de $\mathbb{C}[x,y]$ formado por los polinomios $p(x,y)$ que se anulan en la recta $x = 0$ y que se anulan en el origen junto con sus derivadas parciales $\partial p/\partial x$, $\partial p/\partial y$:

$$\mathfrak{a} = (x,y)^2 \cap (x)$$

Los ceros de $\mathfrak{a}$ coinciden con la recta $x = 0$, de modo que la componente (x) debe aparecer en cualquier otra descomposición primaria reducida de $\mathfrak{a}$. No así la componente sumergida $(x,y)^2$, pues su radical, que es el ideal maximal del origen, no corresponde a una componente irreducible de los ceros de $\mathfrak{a}$. En efecto, si un polinomio $p(x,y)$ se anula en la recta $x = 0$, necesariamente su derivada $\partial p/\partial y$ se anula en el origen; luego la componente $(x,y)^2$ se puede sustituir por el ideal de los polinomios que se anulen en el origen junto con su derivada $\partial p/\partial x$:

$$\mathfrak{a} = (x^2, y) \cap (x)$$

(*) Sea $\mathfrak{m}$ un ideal maximal de un anillo noetheriano A. Si $\mathfrak{q}$ es un ideal $\mathfrak{m}$-primario, entonces $\mathfrak{q}$ contiene alguna potencia $\mathfrak{m}^n$. Para determinar si $\mathfrak{q}$ contiene cierta potencia $\mathfrak{m}^n$ dada, de acuerdo con el lema de Nakayama (19121964) basta desarrollar por Taylor (1685-1731):

$$\mathfrak{m}^n \subseteq \mathfrak{q} \;\Leftrightarrow\; \pi(\mathfrak{m}^n) \subseteq \pi(\mathfrak{q}) \text{ en } A/\mathfrak{m}^{n+1}$$

En efecto, si $\pi(\mathfrak{q})$ contiene un sistema de generadores de $\mathfrak{m}^n/\mathfrak{m}^{n+1}$, el Lema de Nakayama afirma que $\mathfrak{m}^n A_{\mathfrak{m}} \subseteq \mathfrak{q}A_{\mathfrak{m}}$ y, al ser $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario, concluimos que $\mathfrak{m}^n \subseteq \mathfrak{q}$.

(*) Consideremos en el anillo $A = \mathbb{C}[x, y]$ el ideal $\mathfrak{a} = (xy\,, -y + x^2 + y^2)$. Sus ceros son los puntos $z_1 = (0, 0)$ y $z_2 = (0, 1)$, así que su descomposición primaria reducida no tiene componentes sumergidas y ha de ser

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$$

donde $(\mathfrak{q}_1)_0 = z_1$ y $(\mathfrak{q}_2)_0 = z_2$. Sea $\mathcal{O}_2$ el anillo local del plano en z_2. El ideal $\mathfrak{a}\mathcal{O}_2$ es el ideal maximal $\mathfrak{m}_2$ de $\mathcal{O}_2$, porque las curvas $xy = 0$, $x^2 + y^2 - y = 0$ son simples en z_2 y tienen rectas tangentes distintas. Luego $\mathfrak{q}_2$ es el ideal de todos los polinomios que se anulan en z_2:

$$\mathfrak{q}_2 = A \cap (\mathfrak{a}\mathcal{O}_2) = A \cap \mathfrak{m}_2 = (x, y - 1)$$

Sea ahora $\mathcal{O}_1$ el anillo local del plano en z_1 y sea $\mathfrak{m}_1$ su ideal maximal. Vamos a determinar la primera potencia de $\mathfrak{m}_1$ contenida en $\mathfrak{a}\mathcal{O}_1$.

El ideal $\bar{\mathfrak{a}}$ de $\mathcal{O}_1/\mathfrak{m}_1^3$ formado por los desarrollos de Taylor de orden 2 en el punto z_1 de las funciones del ideal $\mathfrak{a}\mathcal{O}_1$ es:

$$\bar{\mathfrak{a}} = < xy, -y + x^2 + y^2, -xy, -y^2 > = < -y + x^2, xy, y^2 >$$

y no contiene a $\mathfrak{m}_1^2/\mathfrak{m}_1^3 = < x^2, xy, y^2 >$, así que $\mathfrak{a}\mathcal{O}_1$ no contiene a $\mathfrak{m}_1^2$.

Los desarrollos de Taylor de orden 3 en el punto z_1 de las funciones del ideal $\mathfrak{a}\mathcal{O}_1$ forman el siguiente ideal de $\mathcal{O}_1/\mathfrak{m}_1^4$:

$$< x^2y, xy^2, xy, y^3, -xy + x^3, y^2, -y + x^2 >$$

que claramente contiene a $\mathfrak{m}_1^3/\mathfrak{m}_1^4$. Según el Lema de Nakayama, $\mathfrak{a}\mathcal{O}_1$ contiene a $\mathfrak{m}_1^3$ y obtenemos que $\mathfrak{a}\mathcal{O}_1$ está formado por todas las funciones $f \in \mathcal{O}_1$ cuyo desarrollo de Taylor en z_1 hasta el orden 2 está en $\bar{\mathfrak{a}} \subset \mathcal{O}_1/\mathfrak{m}_1^3$. Ahora bien, como $\mathfrak{q}_1 = A \cap \mathfrak{a}\mathcal{O}$, concluimos que

$$\mathfrak{q}_1 = \{-ay + ax^2 + bxy + cy^2 + \text{términos de grado mayor que } 2\,\}$$

(*) Ideales en Curvas Simples:

Diremos que una curva algebraica C es **simple** cuando carezca de puntos singulares. Cuando la curva es íntegra, tal condición equivale a que su anillo de funciones algebraicas $\mathcal{O}(C)$ sea un dominio de Dedekind (1831-1916), en cuyo caso todo ideal no nulo $\mathfrak{a}$ de $\mathcal{O}(C)$ es de la forma:

$$\mathfrak{a} = \mathfrak{m}_1^{r_1} \cdots \mathfrak{m}_n^{r_n} = \mathfrak{m}_1^{r_1} \cap \ldots \cap \mathfrak{m}_n^{r_n}$$

para ciertos ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ de $\mathcal{O}(C)$, que definen ciertos puntos cerrados $x_1, \ldots, x_n$ de la curva C. Es decir, $\mathfrak{a}$ está formado por las funciones $f \in \mathcal{O}(C)$ que se anulen al menos r_i veces en cada punto x_i. En efecto, la igualdad 8.6.1

$$\mathfrak{m}_i^r = \mathcal{O}(C) \cap (\mathfrak{m}_i \mathcal{O}_{C,x_i})^r$$

expresa precisamente que cada potencia $\mathfrak{m}_i^r$ está formada por las funciones f que se anulan al menos r veces en el punto x_i.

(*) Multiplicidades de Intersección de Curvas Planas:

Sean C y C' dos curvas planas, de ecuaciones $p(x,y) = 0$ y $p'(x,y) = 0$ respectivamente, sin componentes irreducibles comunes. Si se cortan en un punto z, la multiplicidad de intersección

$$(C \cap C')_z = l\big(k[x,y]/(p,p')\big)_z = l\big(\mathcal{O}/p'\mathcal{O}\big) = l\big(\mathcal{O}'/p\mathcal{O}'\big)$$

(donde $\mathcal{O}$ y $\mathcal{O}'$ denotan los anillos locales de C y C' en z respectivamente) es finita en virtud del teorema de Bézout. Si z es un punto no singular de C, la multiplicidad de intersección puede calcularse determinando el primer término no nulo del desarrollo de Taylor de $p'(x,y) = a_r t^r + \ldots$, donde t es una coordenada local de C en z, pues en tal caso $(C \cap C')_z = l(\mathcal{O}/t^r\mathcal{O}) = r$.

En general, las multiplicidades de intersección pueden calcularse a partir de la descomposición primaria del ideal $(p,p') = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$, pues los ceros de los ideales primarios $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ son los puntos de corte, de modo que

$$k[x,y]/(p,p') \;=\; k[x,y]/\mathfrak{q}_1 \oplus \ldots \oplus k[x,y]/\mathfrak{q}_r$$

y las multiplicidades de intersección son las longitudes de los anillos $k[x,y]/\mathfrak{q}_i$.

Ejercicios:

1. En M_S, probar que $m/s = n/t$ si y sólo si $r(tm - sn) = 0$ para algún $r \in S$.

2. Sean S y T dos sistemas multiplicativos de un anillo A, y sea M un A-módulo. Demostrar que $S^{-1}(S^{-1}M) = S^{-1}M$, y que $T^{-1}(S^{-1}M) = T^{-1}M$ cuando $S \subseteq T$.

3. Sea C una curva plana de ecuación $p(x,y) = 0$ que pase por el punto $(0,0)$. Probar que el anillo local de C en el origen no es un cuerpo.

4. Sea $\mathcal{O}$ el anillo local de la recta afín $\mathbb{A}_{1,k}$ en el origen. Determinar si el anillo local del plano afín $\mathbb{A}_{2,k}$ en el origen es isomorfo a $\mathcal{O} \otimes_k \mathcal{O}$.

5. Si $\mathfrak{a}$ es un ideal de un anillo A, entonces $S^{-1}\mathfrak{a}$ es un ideal de $S^{-1}A$. Cuando $\mathfrak{a} = a_1A + \ldots + a_nA$, probar que $S^{-1}\mathfrak{a} = a_1(S^{-1}A) + \ldots + a_n(S^{-1}A)$; es decir, un sistema de generadores de $S^{-1}\mathfrak{a}$ se obtiene localizando un sistema de generadores de $\mathfrak{a}$.

6. Sea $p(x_1, \ldots, x_n)$ un polinomio irreducible con coeficientes en un cuerpo k y sea $\mathcal{O}$ el anillo local del espacio afín $\mathbb{A}_n$ en el punto genérico de la hipersuperficie $p(x_1, \ldots, x_n) = 0$. Probar que $\mathcal{O}$ es un anillo local regular de dimensión 1.

7. Sea $\mathfrak{a}$ un ideal de un anillo A y sea x un punto de $\operatorname{Spec} A$. Probar que las siguientes condiciones son equivalentes:

   (a) $(A/\mathfrak{a})_x = 0$

   (b) $\mathfrak{a}_x = A_x$

   (c) Alguna función $f \in \mathfrak{a}$ no se anula en x.

   (d) El punto x está en el abierto complementario de $(\mathfrak{a})_0$.

8. Sea $\mathfrak{a}$ un ideal de un anillo A y sea x un punto de $\operatorname{Spec} A$. Probar que las siguientes condiciones son equivalentes:

   (a) $\mathfrak{a}_x = 0$

   (b) $(A/\mathfrak{a})_x = A_x$

   (c) Cada función del ideal $\mathfrak{a}$ se anula en algún entorno de x.

   Además, si el ideal $\mathfrak{a}$ es finito-generado, estas condiciones equivalen a que x esté en el interior del cerrado $(\mathfrak{a})_0$.

9. Probar que todo abierto cerrado U del espectro de un anillo A es básico: $U = U_f$ para alguna función $f \in A$. Además, $(A_f)_x = A_x$ cuando $x \in U_f$, y $(A_f)_x = 0$ en caso contrario.

   (*Indicación*: Si $U = (\mathfrak{a})_0$ y $U^c = (\mathfrak{b})_0$, entonces $\mathfrak{a} + \mathfrak{b} = A$ y $1 = a + b$ para ciertos $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Tomar $f = b$).

10. Si el espectro de un anillo A no es conexo, $\operatorname{Spec} A = U_1 \coprod U_2$, probar que los abiertos cerrados U_i son básicos, $U_i = U_{f_i}$, donde $f_1 f_2$ es nilpotente.

    Si $x \in \operatorname{Spec} A$, deducir que f_i es nilpotente en A_x cuando f_i se anula en x, y obtener que

$$(A_{f_i})_x = \begin{cases} A_x & \text{cuando } x \in U_i \\ 0 & \text{cuando } x \in U_j = (f_i)_0 \end{cases} \quad , \quad i \neq j$$

    Concluir que el morfismo natural $A \to A_{f_1} \oplus A_{f_2}$ es un isomorfismo.

11. Demostrar que una variedad algebraica afín X es conexa si y sólo si toda función algebraica $f \in \mathcal{O}(X)$ idempotente es $f = 0$ ó 1.

12. La condición de pertenecer a un submódulo dado es local. Con precisión, sea N un submódulo de un A-módulo M y sea $m \in M$. Si $m_x \in N_x$ para todo $x \in \operatorname{Spec} A$, demostrar que $m \in N$.

13. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales de un anillo A. Si $\mathfrak{a}_x \subseteq \mathfrak{b}_x$ en todo punto $x \in \operatorname{Spec} A$, probar que $\mathfrak{a} \subseteq \mathfrak{b}$.

14. Si A es un anillo íntegro, probar que (la intersección se considera en el cuerpo de fracciones Σ de A):
$$A = \bigcap_{x \in \operatorname{Spec} A} A_x$$
(*Indicación*: Si $a/b \in \Sigma$ está en todos los anillos A_x, probar que $bA \subseteq aA$).

15. Demostrar que la condición necesaria y suficiente para que un sistema de ecuaciones lineales diofánticas tenga alguna solución entera es que, para cada número primo p, admita alguna solución racional con denominadores que no sean múltiplos de p.

16. Sea $\mathfrak{a}$ un ideal de un anillo A y sea M un A-módulo finito-generado. Probar que $\mathfrak{a}M = M$ precisamente cuando $M_{1+\mathfrak{a}} = 0$.

17. Demostrar que cualquier sistema de n generadores de un A-módulo libre de rango n forman una base. (*Indicación*: Aplicar el lema de Nakayama al núcleo del epimorfismo $A^n \to A^n$ para demostrar que es nulo).

18. Sea M un A-módulo de tipo finito y sea N un A-módulo. Si $M \simeq M \oplus N$, probar que $N = 0$. ¿Es cierta esta afirmación si se elimina la hipótesis de que M sea finito-generado.

19. Probar que si existe un morfismo de A-módulos inyectivo $A^m \to A^n$, entonces $m \leq n$. (*Indicación:* Localizando en un primo minimal, puede suponerse que A tiene un único ideal primo $\mathfrak{p}$, y en tal caso el morfismo $(A/\mathfrak{p})^m \to (A/\mathfrak{p})^n$ es inyectivo).

20. Sea $p(x, y)$ un polinomio no constante con coeficientes en un cuerpo k. Demostrar que todas las componentes irreducibles de $C = \operatorname{Spec} k[x, y]/(p(x, y))$ tienen dimensión 1.

21. Probar que si el anillo $A[x]$ es noetheriano, entonces el anillo A también es noetheriano.

22. Sean N y N' dos submódulos de un A-módulo M tales que $M = N' + N$. Probar que M es un A-módulo noetheriano si y sólo si N y N' son A-módulos noetherianos.

23. Sean N y N' dos submódulos de un A-módulo M tales que $0 = N' \cap N$. Probar que M es un A-módulo noetheriano si y sólo si M/N y M/N' son A-módulos noetherianos.

24. Sea M un A-módulo noetheriano y N un A-módulo de tipo finito. Probar que $\mathrm{Hom}_A(N, M)$ es un A-módulo noetheriano.

25. ¿Es noetheriano el anillo $\prod_\infty \mathbb{Z}$?

26. Probar que todo endomorfismo epiyectivo f de un A-módulo noetheriano es un isomorfismo. (*Indicación:* Considerar los submódulos $\mathrm{Ker}\, f^n$.)

27. Sea $\mathfrak{a}$ el ideal anulador de un A-módulo M. Si M es finito-generado, probar que $A/\mathfrak{a}$ es un submódulo de $M \oplus \ldots \oplus M$. Concluir que el anillo $A/\mathfrak{a}$ es noetheriano cuando M es un A-módulo noetheriano.

28. Probar que todo espacio noetheriano es compacto, y todo subespacio de un espacio noetheriano es noetheriano.

29. Probar que un espacio topológico es noetheriano precisamente cuando todos sus abiertos son compactos.

30. Dar un ejemplo de un anillo no noetheriano A tal que su espectro sea un espacio topológico noetheriano.

31. Probar que el soporte $\mathrm{Sop}\,(M)$ de un A-módulo noetheriano es un subespacio cerrado noetheriano de $\mathrm{Spec}\, A$.

32. Sea $\{U_{f_i}\}$ un recubrimiento de $\mathrm{Spec}\, A$ por abiertos básicos. Probar que un A-módulo M es noetheriano si y sólo si M_{f_i} es un A_{f_i}-módulo noetheriano para todo índice i.

33. Sea $\mathfrak{n}$ el ideal de $\mathcal{C}^\infty(\mathbb{R})$ formado por las funciones que se anulan en algún entorno del punto $x = 0$. Demostrar que el ideal $\mathfrak{n}$ no es finito-generado y concluir que los anillos $\mathcal{C}^\infty(\mathbb{R}^n)$ no son noetherianos cuando $n \geq 1$.

34. Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{C}^\infty(\mathbb{R})$ formado por las funciones que se anulan en el punto $x = 0$. Probar que $\mathcal{O} = \mathcal{C}^\infty(\mathbb{R})_\mathfrak{m}$ es el anillo de gérmenes de funciones diferenciables en el punto $x = 0$. Sea I el ideal $\mathcal{O}$ formado por los gérmenes cuya serie de Taylor en $x = 0$ es nula. Probar que $xI = I$ y concluir que el anillo $\mathcal{O}$ no es noetheriano.

35. Hallar los puntos singulares de las siguientes curvas planas complejas: $y^2 = x^3$, $y^2 = x(x-a)(x-b)$, $y^2x^3 + ax^2 + bx = 0$, $1 = x^n + y^n$, $3axy = x^3 + y^3$, $x^3 = y^2(a-x)$, $y^2(a-x) = x^2(a+x)$, $(x^2+y^2)^2 = (x^2-y^2)$.

36. Hallar un generador del ideal maximal del anillo local de la curva plana compleja $y^2 = x^2 + x^3$ en el punto $(-1, 0)$.

    Análogamente en los puntos $(1, -\sqrt{2})$, $(1, \sqrt{2})$, $(-2, -2i)$.

37. Calcular el desarrollo de Taylor en el origen hasta el orden 3, cuando $k = \mathbb{C}$, $\mathbb{Q}$ y $\mathbb{F}_2$, de las funciones racionales

$$\frac{2 + x^2}{(1 + y)(1 - x^3)} \ , \ \frac{x^2 - y^2}{1 - x^3 + y^3} \ , \ \frac{1}{1 - y + x^2}$$

38. Elegir un generador t del ideal maximal $\mathfrak{m}$ del anillo local $\mathcal{O}$ en el origen de la curva plana $x - 2xy + y^3 - y^4 + x^3 = 0$ y calcular el desarrollo de Taylor en el origen hasta el orden 6 de la función x sobre tal curva. ¿Para qué valores $a \in k$ pertenece la función $xy^2 + ay^5$ al ideal $\mathfrak{m}^6$?

39. Sea $\mathcal{O}$ el anillo local en el origen del plano afín sobre un cuerpo k. Determinar si el ideal maximal $\mathfrak{m}$ de $\mathcal{O}$ está generado por $x+y+x^2$, $x+y^3$. Análogamente para $1 + x + y^4$, $x + y^2$ y para $x/(1 - y + x^2)$, $y/(2 + x - y)$.

    Hallar la primera potencia de $\mathfrak{m}$ contenida en el ideal $(y - x^2, xy)$. Análogamente para los ideales $(x^2 + y^2 - 2y, y + x^2)$, $\big(x/(1 + y), (x + y^2)/(1 - x)\big)$.

40. Probar que la función x genera el ideal maximal $\mathfrak{m}$ del anillo local en el origen de la curva plana compleja $y = x^2 + y^3$, calcular el desarrollo de Taylor en el origen hasta el orden 5 de las funciones y, $y + x^2y$, $y - x^2$, $xy - x^3$ sobre tal curva, y determinar la potencia de $\mathfrak{m}$ que genera cada una de estas funciones.

41. Sea $\mathfrak{a}$ un ideal con ceros aislados de un anillo noetheriano A y sea $\mathfrak{a} = \mathfrak{q} \cap \ldots$ una descomposición primaria reducida de $\mathfrak{a}$. Sea $\mathfrak{m}$ el radical de $\mathfrak{q}$. Probar que $\mathfrak{q} = \mathfrak{a} + \mathfrak{m}^r$ para algún exponente $r \geq 1$. De hecho, podemos tomar r como el exponente de la primera potencia de $\mathfrak{m}\mathcal{O}$ que esté contenida en $\mathfrak{a}\mathcal{O}$. Además, $\mathfrak{m}^r\mathcal{O} \subseteq \mathfrak{a}\mathcal{O}$ precisamente cuando $\mathfrak{m}^r \subseteq \mathfrak{a} + \mathfrak{m}^{r+1}$ (*Indicación:* Aplicar el lema de Nakayama para demostrar que $\mathfrak{a} \cap \mathfrak{m}^r$ genera $\mathfrak{m}^r$).

42. Hallar la componente primaria correspondiente al origen del ideal (p, q) del anillo $\mathbb{C}[x, y]$, y la multiplicidad de intersección en el origen de la curva $p(x, y) = 0$ con la curva $q(x, y) = 0$, en los siguientes casos:

$$\begin{array}{ll} p(x,y) = y^2 - x^2 + x^3 \ , & q(x,y) = y^2 - x^3 \\ p(x,y) = y^2 - x^2 + x^3 \ , & q(x,y) = x^2 - y^3 \\ p(x,y) = y - x^2 \ , & q(x,y) = y + yx - x^2 - y^2 \\ p(x,y) = y + x + y^2 + 2xy \ , & q(x,y) = y + x - y^2 - 2xy \end{array}$$

43. Sea A el anillo de funciones algebraicas de la curva plana compleja $x^3 + x = y^2$. Probar que A es un dominio de Dedekind y calcular la descomposición

en producto de potencias de ideales maximales del ideal de A generado por cada una de las funciones x, y, $x+y$, xy, x^2+y^2, x^3+y, así como del ideal generado por dos de tales funciones.

44. Sean $\mathfrak{a} = \mathfrak{m}_1^{a_1} \cdots \mathfrak{m}_n^{a_n}$ y $\mathfrak{b} = \mathfrak{m}_1^{b_1} \cdots \mathfrak{m}_n^{b_n}$, $a_i, b_i \geq 0$, las descomposiciones en producto de potencias de ideales maximales de dos ideales de un dominio de Dedekind. Probar que

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \mathfrak{m}_1^{d_1} \cdots \mathfrak{m}_n^{d_n} \quad , \quad d_i = \min(a_i, b_i) \\ \mathfrak{a} \cap \mathfrak{b} &= \mathfrak{m}_1^{m_1} \cdots \mathfrak{m}_n^{m_n} \ , \quad m_i = \max(a_i, b_i) \\ \mathfrak{a} \cdot \mathfrak{b} &= \mathfrak{m}_1^{a_1+b_1} \cdots \mathfrak{m}_n^{a_n+b_n} \\ \mathfrak{a} \cdot \mathfrak{b} &= (\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) \end{aligned}$$

45. Sea A un anillo noetheriano. Probar que los ideales primos asociados al ideal 0 son los ideales primos de A que coinciden con el anulador de algún elemento de A. (*Indicación*: Si $\mathfrak{p} = \mathrm{Ann}(a)$, entonces

$$\mathfrak{p} = \bigcap_{a \notin \mathfrak{q}_i} \mathfrak{p}_i$$

Recíprocamente, sea $a \in \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_n$ no nulo. Entonces $\mathfrak{q}_1 \subseteq \mathrm{Ann}(a) \subseteq \mathfrak{p}_1$ y $\mathrm{Ann}(a)$ contiene alguna potencia de $\mathfrak{p}_1$. Sea $\mathfrak{p}_1^r$ la primera potencia contenida en $\mathrm{Ann}(a)$ y sea $b \in \mathfrak{p}_1^{r-1}$, $b \notin \mathrm{Ann}(a)$. El anulador de ab es $\mathfrak{p}_1$).

46. Hallar la descomposición primaria del ideal generado en $\mathbb{C}[x, y]$ por las ecuaciones de un par de rectas y una recta. Igualmente para una recta doble y una recta, una cónica no singular y una recta, una cónica no singular y un par de rectas, una cónica no singular y una recta doble.

47. Determinar si los siguientes sistemas de ecuaciones con coeficientes racionales son equivalentes al sistema $x^2 + y^2 = 1$, $x^2y^2 = 0$:

$$\left.\begin{matrix} x^2+y^2=1 \\ x^4-x^2=0 \end{matrix}\right\} \qquad \left.\begin{matrix} x^2-y^2=1 \\ x^2y^2=0 \end{matrix}\right\} \qquad \left.\begin{matrix} x^2-y^2=1 \\ x^2+y^2=1 \end{matrix}\right\}$$

$$\left.\begin{matrix} x^2+y^2=1 \\ (x+y+1)^2(x+y-1)^2=0 \end{matrix}\right\} \qquad \left.\begin{matrix} x^2+y^2=1 \\ (x+y+1)^2(x+y-1)=0 \end{matrix}\right\}$$

$$\left.\begin{matrix} x^2+y^2=1 \\ (x+y+1)(x+y-1)(x-y+1)(x-y-1)=0 \end{matrix}\right\}$$

48. En la curva plana compleja de ecuación $x^2+y^2=9$, determinar si la función $f(x,y) = (y-3)(x-5)$ divide a la función $g(x,y) = x(y^2-16)$ ¿divide $f(x,y)$ a alguna potencia de $g(x,y)$? ¿y si sustituimos el cuerpo de los números complejos por el de los números racionales?

49. Calcular la multiplicidad de intersección en el origen de la curva $y^2 = x^2 + y^3$ con las curvas $x = 0$, $y = 0$, $y = x^2 + y^3$, $x + y = x^3 + y^4$, $x^2 = -y^3$.

Cálculo Diferencial

(*) Desarrollos de Taylor:

Sea $p = (a_1, \ldots, a_n)$ un punto racional del espacio afín $\operatorname{Spec} k[x_1, \ldots, x_n]$ sobre un cuerpo k. Según 3.5.5 su ideal maximal es $\mathfrak{m}_p = (x_1 - a_1, \ldots, x_n - a_n)$. Como $\mathrm{d}_p x_i = [\Delta_p x_i] = [x_i - a_i] \in \mathfrak{m}_p/\mathfrak{m}_p^2$, se sigue que $\{\mathrm{d}_p x_1, \ldots, \mathrm{d}_p x_n\}$ es una base del k-espacio vectorial $\mathfrak{m}_p/\mathfrak{m}_p^2$.

Además la diferencial $\mathrm{d}_p \colon A \to \mathfrak{m}_p/\mathfrak{m}_p^2$, $\mathrm{d}_p f = [\Delta_p f]$, es una k-derivación, y por 9.1.2 tenemos que

$$\mathrm{d}_p f \;=\; \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a_1, \ldots, a_n) \cdot \mathrm{d}_p x_i$$

Por otra parte, realizando la sustitución $t_i = x_i - a_i = \Delta_p x_i$ vemos que

$$k[x_1, \ldots, x_n]/\mathfrak{m}^{r+1} = \begin{bmatrix} \text{Polinomios en } t_1, \ldots, t_n \\ \text{de grado menor que } r+1 \end{bmatrix}$$

y la expresión de cualquier polinomio $f(x_1, \ldots, x_n)$, módulo $\mathfrak{m}_p^{r+1}$, como polinomio de grado $\leq r$ en $\Delta_p x_1, \ldots, \Delta_p x_n$ es el **desarrollo de Taylor** (1685-1731) de orden r de $f(x_1, \ldots, x_n)$ en el punto $p = (a_1, \ldots, a_n)$:

$$f(x_1, \ldots, x_n) \equiv \sum_{i_1 + \ldots + i_n \leq r} c_{i_1 \ldots i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} \quad (\text{mód. } \mathfrak{m}_p^{r+1})$$

En el caso particular en que $f \in \mathfrak{m}_p^r$ y $f \notin \mathfrak{m}_p^{r+1}$, la clase de restos de un polinomio $f(x_1, \ldots, x_n)$ en $\mathfrak{m}_p^r/\mathfrak{m}_p^{r+1}$ recibe el nombre de **forma inicial** de f en el punto $p = (a_1, \ldots, a_n)$ y es un polinomio homogéneo de grado r en $\Delta_p x_1, \ldots, \Delta_p x_n$:

$$f(x_1, \ldots, x_n) \equiv \sum_{i_1 + \ldots + i_n = r} c_{i_1 \ldots i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} \quad (\text{mód. } \mathfrak{m}_p^{r+1})$$

En el caso de una curva plana $f(x, y) = 0$ que pase por un punto racional $x = a$, $y = b$, la forma inicial descompone en producto de factores de grado 1

$$\sum_{i+j=r} c_{ij} t^i u^j = \prod_{i=1}^{r} (\lambda_i t + \mu_i u)$$

donde $t = x - a$, $u = y - b$, y los coeficientes $\lambda_i,\ \mu_i$ están en una extensión finita de k. Diremos que las rectas $\lambda_i(x - a) + \mu_i(y - b) = 0$, $1 \leq i \leq r$ son las **rectas tangentes** a la curva $f(x, y) = 0$ en el punto $p = (a, b)$.

Nótese que, por definición, $r = 1$ precisamente cuando $\mathrm{d}_p f \neq 0$, de modo que la curva tiene una única recta tangente en p cuando la diferencial $\mathrm{d}_p f$ no es nula.

(*) Puntos Simples de Curvas Planas:

Sea $k[\xi,\eta] = k[x,y]/\big(f(x,y)\big)$ el anillo de funciones algebraicas de una curva plana $f(x,y) = 0$ que pase por el punto racional $p = (a,b)$, sea $\mathfrak{m} = (\xi - a, \eta - b)$, y sea $\bar{\mathfrak{m}} = (x-a, y-b)$ el correspondiente ideal maximal de $k[x,y]$. Tenemos una sucesión exacta de k-espacios vectoriales:

$$0 \;\longrightarrow\; < \mathrm{d}_p f > \;\longrightarrow\; \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 \;\longrightarrow\; \mathfrak{m}/\mathfrak{m}^2 \;\longrightarrow\; 0$$

Como $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 =< \mathrm{d}_p x, \mathrm{d}_p y >$ es un espacio vectorial de dimensión 2, vemos que $\mathrm{d}_p f \neq 0$ si y sólo si la dimensión de $\mathfrak{m}/\mathfrak{m}^2$ es 1. Además, si $\mathcal{O}_p$ denota el anillo local en p de la curva dada, en virtud de 8.2.8 tenemos que $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}\mathcal{O}_p/\mathfrak{m}^2\mathcal{O}_p$, y de 8.5.5 se sigue que la condición de que p sea un punto simple de la curva equivale a que la diferencial $\mathrm{d}_p f$ no sea nula.

En tal caso el ideal $\mathfrak{m}\mathcal{O}_p$ es principal y, de acuerdo con el lema de Nakayama, está generado por cualquier polinomio $t \in \bar{\mathfrak{m}}$ cuya diferencial $\mathrm{d}_p t$ no sea proporcional a $\mathrm{d}_p f$. Luego $\mathfrak{m}^n\mathcal{O}_p = t^n\mathcal{O}_p$, de modo que todos los espacios vectoriales $\mathfrak{m}^n\mathcal{O}_p/\mathfrak{m}^{n+1}\mathcal{O}_p$ tienen dimensión 1. Ahora, si $h \in \mathcal{O}_p = k + \mathfrak{m}\mathcal{O}_p$, tendremos $h = c_0 + th_1$ donde $c_0 \in k$, $h_1 \in \mathcal{O}_p$, y por tanto

$$h = c_0 + t(c_1 + th_2) = c_0 + c_1 t + t^2 h_2 = c_0 + c_1 t + c_2 t^2 + t^3 h_3 = \ldots$$
$$k[\,t\,]/(t^n) \;=\; \mathcal{O}_p/\mathfrak{m}^n\mathcal{O}_p \;=\; k[\xi,\eta]/\mathfrak{m}^n$$

lo que determina la estructura de los entornos infinitesimales $\mathrm{Spec}\,(k[\xi,\eta]/\mathfrak{m}^n)$ del punto simple p. Cuando $h = c_m t^m + c_{m+1}t^{m+1} + \ldots$, $c_m \neq 0$, tenemos que h está en $\mathfrak{m}^m\mathcal{O}_p$ y genera $\mathfrak{m}^m\mathcal{O}_p/\mathfrak{m}^{m+1}\mathcal{O}_p$. El lema de Nakayama permite concluir que $h\mathcal{O}_p = \mathfrak{m}^m\mathcal{O}_p$, así que el número de ceros o valoración en p es $v(h) = m$.

(*) El origen de coordenadas es un punto simple de la curva $0 = y - x^2 + xy^2$. Un parámetro local es la función x, porque la recta $x = 0$ no es tangente a la curva en tal punto, así que $v(x) = 1$. Si queremos determinar la valoración de otra función $h(x,y)$, iniciamos su desarrollo en serie de potencias del parámetro x. Para ello es suficiente desarrollar la función y:

$$\begin{aligned} y &= x^2 - xy^2 = x^2 - x(x^2 - xy^2)^2 = \\ &= x^2 - x^5 + 2x^4(x^2 - xy^2)^2 - x^3(x^2 - xy^2)^4 = \\ &= x^2 - x^5 + 2x^8 + \text{ términos de orden} \geq 11 \end{aligned}$$

pues cualquier otro polinomio h puede desarrollarse conociendo el desarrollo de y hasta un orden adecuado:

$$\begin{aligned} y^2 - x^2 y + x^8 &= (x^2 - x^5 + 2x^8 + \ldots)^2 - x^2(x^2 - x^5 + 2x^8 + \ldots) + x^8 \\ &= -x^7 + x^8 + 3x^{10} + \text{términos de orden} \geq 11 \\ 7 &= v(y^2 - x^2 y + x^8) \end{aligned}$$

(*) Puntos Singulares en Aritmética

En general, dado un anillo A y un punto cerrado $x \in \operatorname{Spec} A$, definido por un ideal maximal $\mathfrak{m}$ de A, la diferencial en x de una función f sólo podemos definirla cuando ésta se anula en el punto, $f \in \mathfrak{m}$, porque en tal caso f coincide con su incremento en x y podemos definir $\mathrm{d}_x f$ como la clase de f en $\mathfrak{m}/\mathfrak{m}^2$, que es un espacio vectorial sobre el cuerpo residual $\kappa(x) = A/\mathfrak{m}$. Ahora, si $\bar{A} = A/(f_1, \ldots, f_n)$, donde las funciones f_i se anulan en x, tenemos una sucesión exacta

$$0 \longrightarrow < \mathrm{d}_x f_1, \ldots, \mathrm{d}_x f_n > \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 \longrightarrow 0$$

que permite calcular la dimensión de $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$. Por ejemplo, veamos los puntos singulares del espectro del anillo $\mathbb{Z}[\sqrt{5}\,] = \mathbb{Z}[x]/(x^2-5)$. De acuerdo con el cálculo de $\operatorname{Spec}\mathbb{Z}[x]$ realizado en la página 131, los puntos cerrados de $\operatorname{Spec}\mathbb{Z}[\sqrt{5}\,]$ se corresponden con los siguientes ideales maximales de $\mathbb{Z}[x]$:

$$\begin{aligned} \mathfrak{m}_y &= (p, x^2-5) \quad \text{donde } x^2-5 \text{ es irreducible módulo } p \\ \mathfrak{m}_z &= (p, x-a) \quad \text{donde } a^2 \equiv 5 \text{ (mód. } p) \end{aligned}$$

En el primer caso $\mathfrak{m}_y/\mathfrak{m}_y^2$ es un espacio vectorial de dimensión 2 generado por $\mathrm{d}_y p$ y $\mathrm{d}_y(x^2-5)$; luego la diferencial de x^2-5 no es nula y concluimos que en este caso $\bar{\mathfrak{m}}_y/\bar{\mathfrak{m}}_y^2$ es de dimensión 1. Tal punto $y \in \operatorname{Spec}\mathbb{Z}[\sqrt{5}\,]$ es simple en el sentido de que $\mathbb{Z}[\sqrt{5}\,]_y$ es un anillo local regular.

En el segundo caso $\mathfrak{m}_z/\mathfrak{m}_z^2$ es un espacio vectorial de dimensión 2 sobre el cuerpo residual $\mathbb{Z}[x]/(p, x-a) = \mathbb{F}_p$, generado por $\mathrm{d}_z p$ y $\mathrm{d}_z(x-a)$. Ahora, si $a^2 = 5 + bp$, tenemos

$$x^2 - 5 \;=\; (x-a)(x+a) + bp \;=\; (x-a)^2 + 2a(x-a) + bp$$

de modo que $\mathrm{d}_z(x^2-5) = 2a\mathrm{d}_z(x-a) + b\mathrm{d}_z p$, y obtenemos que z es un punto no singular de $\operatorname{Spec}\mathbb{Z}[\sqrt{5}\,]$, salvo cuando $2a$ y b sean múltiplos de p. Si $p \neq 2$, entonces a es múltiplo de p y 5 también. Pero cuando $p = 5$, tenemos que $a \equiv 0$; luego $b \equiv -1$ no es múltiplo de p. Cuando $p = 2$, tenemos que $a \equiv 1$ y $b \equiv 0$. Concluimos que el único punto singular de $\operatorname{Spec}\mathbb{Z}[\sqrt{5}\,]$ está definido por el ideal maximal $\mathfrak{m} = (2, x-1)$.

(*) Derivaciones de Funciones Diferenciables:

Sea $p = (a_1, \ldots, a_n)$ un punto de un abierto U de $\mathbb{R}^n$ y sea $\mathfrak{m}_p$ el ideal maximal de $\mathcal{C}^\infty(U)$ formado por las funciones que se anulan en p. La diferencial $\mathrm{d}_p f$ de cualquier función infinitamente diferenciable $f \in \mathcal{C}^\infty(U)$ es la clase de restos del incremento $f - f(p)$ en $\mathfrak{m}_p/\mathfrak{m}_p^2$. Desarrollando por Taylor (1685-1731) en p cualquier función diferenciable

$$f(x_1, \ldots, x_n) = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} (x_i - a_i) f_i \qquad , \qquad f_i \in \mathcal{C}^\infty(U)$$

vemos que el ideal $\mathfrak{m}_p$ está generado por los incrementos $x_i - a_i$ de las coordenadas x_i. Luego $\mathfrak{m}_p/\mathfrak{m}_p^2$ está generado por las diferenciales $\mathrm{d}_p x_i$. De hecho son linealmente independientes, porque tenemos derivaciones

$$\left(\frac{\partial}{\partial x_i}\right)_p : \mathcal{C}^\infty(U) \longrightarrow \mathcal{C}^\infty(U)/\mathfrak{m}_p = \mathbb{R} \qquad , \qquad \left(\frac{\partial}{\partial x_i}\right)_p f := \frac{\partial f}{\partial x_i}(p)$$

que, entendidas mediante 9.1.4 como aplicaciones lineales sobre $\mathfrak{m}_p/\mathfrak{m}_p^2$, verifican que $(\partial/\partial x_i)_p(\mathrm{d}_p x_j) = \delta_{ij}$. En resumen:

$$\mathfrak{m}_p/\mathfrak{m}_p^2 = \mathbb{R}\mathrm{d}_p x_1 \oplus \ldots \oplus \mathbb{R}\mathrm{d}_p x_n$$
$$\mathrm{Der}_{\mathbb{R}}\big(\mathcal{C}^\infty(U), \mathcal{C}^\infty(U)/\mathfrak{m}_p\big) = \mathbb{R}(\partial/\partial x_1)_p \oplus \ldots \oplus \mathbb{R}(\partial/\partial x_n)_p$$

En particular, una $\mathbb{R}$-derivación $D_p\colon \mathcal{C}^\infty(U) \to \mathcal{C}^\infty(U)/\mathfrak{m}_p = \mathbb{R}$ es nula precisamente cuando se anula en las coordenadas $x_1, \ldots, x_n$. Ahora cada $\mathbb{R}$-derivación $D\colon \mathcal{C}^\infty(U) \to \mathcal{C}^\infty(U)$ induce una $\mathbb{R}$-derivación $D_p\colon \mathcal{C}^\infty(U) \to \mathcal{C}^\infty(U)/\mathfrak{m}_p = \mathbb{R}$, $D_p f := (Df)(p)$, y vemos que $D = 0$ si y sólo si $Dx_1 = \ldots = Dx_n = 0$. Por tanto

$$D = (Dx_1)\frac{\partial}{\partial x_1} + \ldots + (Dx_n)\frac{\partial}{\partial x_n}$$

porque ambas derivaciones coinciden sobre las coordenadas $x_1, \ldots, x_n$, y concluimos que $\mathrm{Der}_{\mathbb{R}}\big(\mathcal{C}^\infty(U), \mathcal{C}^\infty(U)\big)$ es un $\mathcal{C}^\infty(U)$-módulo libre de base las derivaciones $\partial/\partial x_1, \ldots, \partial/\partial x_n$.

Ejercicios:

1. Sea A una k-álgebra y M un $A[x]$-módulo. Si $D\colon A \to M$ es una k-derivación, para cada elemento $m \in M$ existe una única k-derivación $\bar{D}\colon A[x] \to M$ que extiende a D y $\bar{D}x = m$.

2. Calcular $\mathrm{Der}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q})$ y $\mathrm{Der}_{\mathbb{Z}}(\mathbb{Z}[\,i\,], \mathbb{Z}[\,i\,])$.

3. Sea k un cuerpo, $A = k[x,y]/(x - y^2 - y^3)$ y $\mathfrak{m}$ el ideal maximal del punto $x = 0, y = 0$. ¿Existe alguna k-derivación $D\colon A \to A/\mathfrak{m}$ tal que $Dx = 1$?

   Estudiar también los casos $A = k[x,y]/(x^2 - y^2 - y^3)$, $A = k[x,y]/(x - y - y^3)$.

4. Sea $A = \mathbb{Z}[\,i\,]$ y $\mathfrak{m} = (1+i)A$. Calcular $\mathrm{Der}_{\mathbb{Z}}(A, A)$ y $\mathrm{Der}_{\mathbb{Z}}(A, A/\mathfrak{m})$.

5. Calcular $\Omega_{\mathbb{C}/\mathbb{R}}$, $\Omega_{k(x)/k}$ y $\Omega_{\mathbb{Z}[\,i\,]/\mathbb{Z}}$.

6. Sea $p(x)$ un polinomio con coeficientes en un anillo A y sea $B = A[x]/\big(p(x)\big)$. Demostrar que $\Omega_{B/A} = \big(B/p'(x)B\big)\,\mathrm{d}x$.

7. Sean $A \to B$ y $A \to C$ morfismos de anillos. La aplicación natural

$$\mathrm{Der}_A(B \otimes_A C, M) \longrightarrow \mathrm{Der}_A(B, M) \times \mathrm{Der}_A(C, M)$$

es biyectiva para todo $B \otimes_A C$-módulo M. Obtener así otra demostración del isomorfismo de $B \otimes_A C$-módulos

$$\Omega_{B \otimes_A C/A} \;=\; \big(\Omega_{B/A} \otimes_A C\big) \oplus \big(B \otimes_A \Omega_{C/A}\big)$$

8. Sea $B \to C$ un morfismo de A-álgebras. La condición necesaria y suficiente para que la sucesión

$$0 \;\longrightarrow\; \Omega_{B/A} \otimes_B C \;\xrightarrow{j \otimes 1}\; \Omega_{C/A} \;\longrightarrow\; \Omega_{C/B} \;\longrightarrow\; 0$$

sea exacta y escinda, es que toda A-derivación $B \to M$ en un C-módulo M pueda extenderse a una A-derivación $C \to M$.

9. Si $A \to B$ es un morfismo de anillos y $C = B[x_1, \ldots, x_n]$, entonces

$$\Omega_{C/A} \;=\; (\Omega_{B/A} \otimes_A C) \oplus C\mathrm{d}x_1 \oplus \ldots \oplus C\mathrm{d}x_n$$

10. Si $B = A[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$, entonces $\Omega_{B/A}$ es el cociente del B-módulo libre de base $(\mathrm{d}x_1, \ldots, \mathrm{d}x_n)$ por el submódulo generado por los elementos

$$(\partial p_i/\partial x_1)\mathrm{d}x_1 + \ldots + (\partial p_i/\partial x_n)\mathrm{d}x_n \qquad , \qquad 1 \leq i \leq r$$

11. Sea k un cuerpo y $A = k[x, y]/(x^2 - y^3)$. Calcular $\Omega_{A/k}$ y determinar si es un A-módulo libre y si su torsión es nula.

    Análogamente cuando $A = k[x, y]/(1 - x^2 - x^2y^2)$.

12. Sea k un cuerpo, $k \to k(\alpha)$ una extensión, E un $k(\alpha)$-espacio vectorial y $D\colon k \to E$ una derivación. Si α es trascendente sobre k, demostrar que para cada vector $e \in E$ existe una única derivación $\bar{D}\colon k(\alpha) \to E$ que extiende a D y $\bar{D}\alpha = e$.

13. Sea k un cuerpo, $k \to k(\alpha)$ una extensión, E un $k(\alpha)$-espacio vectorial y $D\colon k \to E$ una derivación. Supongamos que α es algebraico sobre k y sea $p(x) = \sum_i a_i x^i \in k[x]$ su polinomio irreducible.

    (a) Cuando $p'(x) \neq 0$, existe una única derivación $\bar{D}\colon k(\alpha) \to E$ que extiende a D.

    (b) Cuando $p'(x) = 0$ y $\sum_i \alpha^i(Da_i) \neq 0$, no existe ninguna derivación $\bar{D}\colon k(\alpha) \to E$ que extienda a D.

(c) Cuando $p'(x) = 0$ y $\sum_i \alpha^i (Da_i) = 0$, para cada vector $e \in E$ existe una única derivación $\bar{D}\colon k(\alpha) \to E$ que extiende a D y $\bar{D}\alpha = e$.

14. Sea k un cuerpo de característica nula y $k \to L$ una extensión. La condición necesaria y suficiente para que un elemento $\alpha \in L$ sea trascendente sobre k es que exista alguna k-derivación $D\colon L \to L$ tal que $D\alpha \neq 0$.

    (*Indicación:* El Lema de Zorn y los dos ejercicios anteriores).

15. Sea $\mathcal{C}(X)$ el anillo de funciones reales continuas sobre un espacio topológico X y sea $\mathfrak{m}_p$ el ideal maximal de $\mathcal{C}(X)$ formado por las funciones que se anulan en un punto dado $p \in X$. Demostrar que $\mathfrak{m}_p = \mathfrak{m}_p^2$ y que por tanto toda $\mathbb{R}$-derivación $D\colon \mathcal{C}(X) \to \mathcal{C}(X)/\mathfrak{m}_p = \mathbb{R}$ es nula. Concluir que toda $\mathbb{R}$-derivación $D\colon \mathcal{C}(X) \to \mathcal{C}(X)$ es nula.

    (*Indicación:* Toda función continua es diferencia de dos cuadrados).

16. Sea p un punto de un espacio topológico X y sea $\mathcal{O}$ el anillo de gérmenes en p de funciones reales continuas definidas en algún entorno de p en X. Si un germen $f \in \mathcal{O}$ no es constante, probar la existencia de un ideal primo $\mathfrak{p} \subset \mathcal{O}$ tal que la clase de restos $\bar{f} \in \mathcal{O}/\mathfrak{p}$ no es nula, en cuyo caso $\bar{f}$ es trascendente sobre $\mathbb{R}$. Obtener la existencia de una $\mathbb{R}$-derivación $\mathcal{O} \to \Sigma$ que no se anula en f, donde Σ denota el cuerpo de fracciones de $\mathcal{O}/\mathfrak{p}$.

    Concluir que el núcleo de la diferencial $\mathrm{d}\colon \mathcal{O} \longrightarrow \Omega_{\mathcal{O}/\mathbb{R}}$ está formado por los gérmenes constantes.

Parte III

Apéndices

Apéndice A

Polinomios Simétricos

A.1 Teorema Fundamental

Definición: Diremos que un polinomio $p(x_1, \ldots, x_n)$ con coeficientes en un anillo A es **simétrico** cuando, para toda permutación $\sigma \in S_n$ se tenga

$$p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = p(x_1, \ldots, x_n)$$

Definición: En $A[x_1, \ldots, x_n]$ llamaremos **funciones simétricas elementales** a los polinomios simétricos

$$\begin{aligned} s_1(x_1, \ldots, x_n) &= x_1 + \ldots + x_n \\ &\ldots\ldots\ldots\ldots \\ s_r(x_1, \ldots, x_n) &= \sum_{i_1 < \ldots < i_r} x_{i_1} \cdots x_{i_r} \\ &\ldots\ldots\ldots\ldots \\ s_n(x_1, \ldots, x_n) &= x_1 \cdots x_n \end{aligned}$$

Ejemplos:

1. Los polinomios $\sigma_r(x_1, \ldots, x_n) = x_1^r + \ldots + x_n^r$ son simétricos.
2. Si $p(x) \in A[x]$, los polinomios $p(x_1) + \ldots + p(x_n)$ y $p(x_1) \cdots p(x_n)$ son simétricos.
3. El polinomio $\Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_j - x_i)$ no es simétrico; pero Δ^2 sí.
4. Todos los polinomios constantes son simétricos. Además las sumas y productos de polinomios simétricos en las mismas indeterminadas también son polinomios simétricos. Luego, si $q(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$, entonces el polinomio $q(s_1, \ldots, s_n)$ es simétrico.

5. El polinomio $x_1 + x_2$ es simétrico en $A[x_1, x_2]$; pero no en $A[x_1, x_2, x_3]$. Cuando hablamos de polinomios simétricos, debe quedar claro el número de indeterminadas que consideramos.

Teorema de los Polinomios Simétricos: *Si $p(x_1, \ldots, x_n)$ es un polinomio simétrico con coeficientes en un anillo A, existe un único polinomio $q(x_1, \ldots, x_n)$ con coeficientes en A tal que*

$$p(x_1, \ldots, x_n) = q(s_1, \ldots, s_n) \ , \qquad s_r := s_r(x_1, \ldots, x_n)$$

Demostración: Veamos primero la existencia de tal polinomio $q(x_1, \ldots, x_n)$, para lo que ordenamos los monomios según su grado y, a igualdad de grado, según el orden léxico-gráfico. Es decir, decimos que $x_1^{m_1} \ldots x_n^{m_n}$ es mayor que $x_1^{r_1} \ldots x_n^{r_n}$ cuando su grado sea mayor ó, caso de ser iguales sus grados, cuando la sucesión de exponentes $(m_1, \ldots, m_n)$ sea mayor que $(r_1, \ldots, r_n)$ en el orden léxico-gráfico (en el sentido de que la primera diferencia $m_i - r_i$ no nula es positiva). Llamaremos **monomio inicial** de un polinomio al mayor (en esta ordenación) de sus monomios con coeficiente no nulo.

En esta ordenación es claro que el número de monomios menores que cierto monomio dado siempre es finito, pues es finito el número de monomios de grado menor que cierto número dado, así que podemos demostrar el teorema procediendo por inducción sobre el monomio inicial $x_1^{m_1} \ldots x_n^{m_n}$ del polinomio simétrico $p(x_1, \ldots, x_n)$, de modo que

$$p(x_1, \ldots, x_n) = a x_1^{m_1} \ldots x_n^{m_n} + \text{ términos con monomios menores } \ ,$$

y necesariamente $m_1 \geq m_2 \geq \ldots \geq m_n$ porque $p(x_1, \ldots, x_n)$ es simétrico. Por otra parte, el monomio inicial de $s_1^{r_1} s_2^{r_2} \ldots s_n^{r_n}$ es claramente

$$x_1^{r_1 + r_2 + \ldots + r_n} x_2^{r_2 + \ldots + r_n} \ldots x_n^{r_n} \ .$$

Eligiendo adecuadamente los exponentes $r_1, \ldots, r_n$ podemos conseguir que el monomio inicial de $s_1^{r_1} \ldots s_n^{r_n}$ coincida con el de $p(x_1, \ldots, x_n)$, de modo que el monomio inicial del polinomio simétrico

$$p(x_1, \ldots, x_n) - a s_1^{r_1} \ldots s_n^{r_n}$$

sea estrictamente menor que $x_1^{m_1} \ldots x_n^{m_n}$. Por hipótesis de inducción, existe un polinomio $\bar{q}(x_1, \ldots, x_n)$ con coeficientes en A tal que

$$p(x_1, \ldots, x_n) - a s_1^{r_1} \ldots s_n^{r_n} = \bar{q}(s_1, \ldots, s_n)$$

y concluimos que $p(x_1, \ldots, x_n) = q(s_1, \ldots, s_n)$, donde

$$q(x_1, \ldots, x_n) := a x_1^{r_1} \ldots x_n^{r_n} + \bar{q}(x_1, \ldots, x_n) \ .$$

Por último, la unicidad es consecuencia directa del siguiente teorema:

Teorema A.1.1 *Sea* $q(x_1,\ldots,x_n) \in A[x_1,\ldots,x_n]$. *Si* $q(s_1,\ldots,s_n)=0$, *entonces* $q(x_1,\ldots,x_n)=0$.

Demostración: Procedemos por inducción sobre n, pues es evidente cuando $n=1$.

Si $n \geq 2$, suponemos que el teorema es falso y consideramos un polinomio no nulo $q(x_1,\ldots,x_n) \in A[x_1,\ldots,x_n]$ de grado mínimo en x_n tal que $q(s_1,\ldots,s_n)=0$:

$$q = q_0(x_1,\ldots,x_{n-1}) + q_1(x_1,\ldots,x_{n-1})x_n + \ldots + q_d(x_1,\ldots,x_{n-1})x_n^d$$

Sustituyendo ahora x_n por 0 en la identidad $q(s_1,\ldots,s_n)=0$, obtenemos la igualdad $q_0(\bar{s}_1,\ldots,\bar{s}_{n-1})=0$, donde $\bar{s}_r := s_r(x_1,\ldots,x_{n-1})$. Por hipótesis de inducción $q_0(x_1,\ldots,x_{n-1})=0$; luego

$$q(x_1,\ldots,x_n) = x_n \cdot (q_1 + \ldots + q_d x_n^{d-1}) = x_n \cdot h(x_1,\ldots,x_n)$$

y concluimos que $h(x_1,\ldots,x_n)$ es un polinomio no nulo con coeficientes en A, de grado menor que $q(x_1,\ldots,x_n)$, tal que $h(s_1,\ldots,s_n)=0$, en contra de la elección de $q(x_1,\ldots,x_n)$.

Ejemplos:

1. $\sigma_2(x_1,\ldots,x_n) = x_1^2+\ldots+x_n^2 = s_1^2 - 2s_2$.

2. Sigamos la demostración del teorema cuando $p(x_1,x_2) = x_1^4 + x_2^4$. En tal caso el monomio inicial es x_1^4, que es el monomio inicial de s_1^4, y tenemos que

$$\begin{aligned} p(x_1,x_2) - s_1^4 = x_1^4 + x_2^4 - (x_1+x_2)^4 &= -4x_1^3x_2 - 6x_1^2x_2^2 - 4x_1x_2^3 \\ &= -(4x_1^2 + 4x_2^2 + 6x_1x_2)x_1x_2 \\ &= -(4s_1^2 - 8s_2 + 6s_2)s_2 = 2s_2^2 - 4s_1^2s_2 \end{aligned}$$

   Luego $\sigma_4(x_1,x_2) = s_1^4 + 2s_2^2 - 4s_1^2s_2$.

3. Consideremos $\sigma_3 = x_1^3+\ldots+x_n^3$. Como $s_1^{r_1}\ldots s_n^{r_n}$ es un polinomio homogéneo de grado $r_1+2r_2+\ldots+nr_n$, de acuerdo con el teorema de los polinomios simétricos existen $a,b,c \in \mathbb{Z}$ tales que $\sigma_3 = as_1^3 + bs_1s_2 + cs_3$.

   Tomando $1 = x_1$ y $0 = x_2 = \ldots = x_n$ obtenemos que $a=1$, tomando $1 = x_1 = x_2$ y $0 = x_3 = \ldots = x_n$ obtenemos que $2 = 8 - 2b$, y tomando $1 = x_1 = x_2 = x_3$ y $0 = x_4 = \ldots = x_n$ se obtiene que $3 = 27 - 9b - c$. Luego $b=-3$, $c=3$, y concluimos que $\sigma_3 = s_1^3 - 3s_1s_2 + 3s_3$.

A.2 Funciones Simétricas de las Raíces

Sea $p(x)$ un polinomio de grado n con coeficientes en un cuerpo k y sean $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$, cada una repetida tantas veces como indique su multiplicidad, en una extensión de k donde $p(x)$ tenga todas sus raíces. Si $r(x_1, \ldots, x_n)$ es un polinomio simétrico con coeficientes en k, el teorema de los polinomios simétricos afirma la existencia de un polinomio $q(x_1, \ldots, x_n)$ con coeficientes en k tal que $r(x_1, \ldots, x_n) = q(s_1, \ldots, s_n)$. Por las fórmulas de Cardano, tenemos que

$$r(\alpha_1, \ldots, \alpha_n) = q\big(-c_1/c_0, \ldots, (-1)^n c_n/c_0\big)$$

y concluimos que $r(\alpha_1, \ldots, \alpha_n)$ es una función racional de los coeficientes del polinomio dado $p(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_n$, así que puede calcularse sin necesidad de hallar previamente las raíces α_i. Veamos ahora el cálculo de algunas de las funciones simétricas más importantes de las raíces de un polinomio:

Fórmula de Girard: Vamos a calcular las sumas de las potencias de las raíces

$$\sigma_r = \sum_{i=1}^{n} \alpha_i^r \ , \quad r \in \mathbb{N}$$

donde convenimos que $\alpha_i^0 = 1$; es decir, que $\sigma_0 = n$. Como $\alpha_1, \ldots, \alpha_n$ son todas las raíces de $p(x)$, cada una contada con su multiplicidad, tenemos que

$$p(x) = c_0(x - \alpha_1) \cdots (x - \alpha_n)$$
$$\frac{p'(x)}{p(x)} = \sum_{i=1}^{n} \frac{1}{x - \alpha_i}$$

Es inmediato comprobar que[1]:

$$\frac{1}{x - \alpha_i} = \frac{1}{x} + \frac{\alpha_i}{x^2} + \frac{\alpha_i^2}{x^3} + \ldots = \frac{1}{x} \cdot \left(\sum_{r \geq 0} \frac{\alpha_i^r}{x^r} \right)$$

y obtenemos la **fórmula de Girard** (1590–1634) para el cálculo de las sumas de potencias de las raíces de un polinomio:

$$\frac{p'(x)}{p(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \frac{\sigma_2}{x^3} + \ldots \ , \quad \sigma_r := \sum_{i=1}^{n} \alpha_i^r$$

Ejemplo: Si $p(x) = x^3 + 2x + 1$, entonces

$$\frac{p'(x)}{p(x)} = \frac{3x^2 + 2}{x^3 + 2x + 1} = \frac{3}{x} - \frac{4}{x^3} - \frac{3}{x^4} + \ldots$$

y obtenemos que $\sigma_0 = 3,\ \sigma_1 = 0,\ \sigma_2 = -4,\ \sigma_3 = -3,\ \ldots$

[1] La siguiente igualdad afirma que $1 = (x - \alpha_i)(1/x + \alpha_i/x^2 + \ldots)$, donde el producto de series formales con coeficientes en un cuerpo k se realiza según la definición del producto de polinomios. A diferencia de los polinomios, las series formales pueden tener infinitos coeficientes no nulos.

Ejemplo: Sea k un cuerpo y $\Sigma = k(x_1, \ldots, x_n)$ el cuerpo de fracciones racionales con coeficientes en k en n indeterminadas. El siguiente polinomio $p(x)$ con coeficientes en Σ

$$p(x) = \prod_{i=1}^{n}(x - x_i) = x^n + \sum_{r=1}^{n}(-1)^r s_r(x_1, \ldots, x_n) \cdot x^{n-r}$$

tiene en Σ las raíces $x_1, \ldots, x_n$. En este caso $\sigma_r = x_1^r + \ldots + x_n^r$, así que podemos expresar estos polinomios simétricos en función de los polinomios simétricos elementales $s_r(x_1, \ldots, x_n)$ dividiendo $p'(x) = nx^{n-1} - (n-1)s_1x^{n-2} + (n-2)s_2x^{n-3} - \ldots$ por $p(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \ldots$.

Fórmulas de Newton: La fórmula de Girard afirma que

$$p'(x) = \sum_{i=0}^{n-1}(n-i)c_ix^{n-i-1} = \left(\sum_{i=0}^{n}c_ix^{n-i}\right)\left(\sum_{j\geq 0}\sigma_j x^{-j-1}\right)$$

Igualando los coeficientes de x^{n-r-1}, $r \geq 1$, obtenemos que

$$(n-r)c_r = \sum_{i+j=r} c_i\sigma_j = \sum_{i=0}^{r} c_i\sigma_{r-i}\ , \quad 1 \leq r \leq n-1$$

$$0 = \sum_{i+j=r} c_i\sigma_j = \sum_{i=0}^{n} c_i\sigma_{r-i}\ , \qquad r \geq n$$

que son las **fórmulas de Newton** (1643–1727):

$$c_0\sigma_r + c_1\sigma_{r-1} + \ldots + c_{r-1}\sigma_1 + rc_r = 0\ , \quad r \leq n$$
$$c_0\sigma_r + c_1\sigma_{r-1} + c_2\sigma_{r-2} + \ldots + c_n\sigma_{r-n} = 0\ , \quad r \geq n$$

Ejemplos:

1. Para el polinomio $x^3 + x^2 - 1$ las fórmulas de Newton dan

$$\begin{aligned} \sigma_1 + 1 &= 0\ , & \sigma_1 &= -1 \\ \sigma_2 + \sigma_1 &= 0\ , & \sigma_2 &= 1 \\ \sigma_3 + \sigma_2 - 3 &= 0\ , & \sigma_3 &= 2 \\ \sigma_4 + \sigma_3 - \sigma_1 &= 0\ , & \sigma_4 &= -3 \\ \sigma_5 + \sigma_4 - \sigma_2 &= 0\ , & \sigma_5 &= 4 \\ \ldots\ldots\ldots & & \ldots & \end{aligned}$$

2. En el caso del polinomio $x^n - 1$, las fórmulas de Newton son

$$\sigma_1 = 0\ ,\ \sigma_2 = 0\ ,\ \ldots\ ,\sigma_{n-1} = 0\ ,\ \sigma_n - n = 0$$
$$\sigma_{n+1} - \sigma_1 = 0\ ,\ \sigma_{n+2} - \sigma_2 = 0\ ,\ \ldots\ ,\sigma_{2n-1} - \sigma_{n-1} = 0\ ,\ \sigma_{2n} - \sigma_n = 0$$
$$\ldots\ldots\ldots\ldots\ldots$$

así que $\sigma_r = 0$ cuando r no es múltiplo de n y $\sigma_r = n$ cuando r es múltiplo de n.

3. Para cualquier polinomio de grado dos $x^2 - s_1x + s_2$ tenemos

$$\begin{aligned} \sigma_1 - s_1 &= 0\ , & \sigma_1 &= s_1 \\ \sigma_2 - s_1\sigma_1 + 2s_2 &= 0\ , & \sigma_2 &= s_1^2 - 2s_2 \\ \sigma_3 - s_1\sigma_2 + s_2\sigma_1 &= 0\ , & \sigma_3 &= s_1^3 - 3s_1s_2 \\ \sigma_4 - s_1\sigma_3 + s_2\sigma_2 &= 0\ , & \sigma_4 &= s_1^4 - 5s_1^2s_2 + 2s_2^2 \\ \cdots\cdots & & \cdots\cdots & \end{aligned}$$

4. Para cualquier cúbica $x^3 - px^2 + qx - r$ tenemos que

$$\begin{aligned} \sigma_1 - p &= 0\ , & \sigma_1 &= p \\ \sigma_2 - p\sigma_1 + 2q &= 0\ , & \sigma_2 &= p^2 - 2q \\ \sigma_3 - p\sigma_2 + q\sigma_1 - 3r &= 0\ , & \sigma_3 &= p^3 - 3pq + 3r \\ \sigma_4 - p\sigma_3 + q\sigma_2 - r\sigma_1 &= 0\ , & \sigma_4 &= p^4 - 4p^3q + 4pr + 2q^2 \\ \cdots\cdots & & \cdots\cdots & \end{aligned}$$

A.3 El Discriminante

Definición: Sea $p(x) = c_0x^n + \ldots + c_n$ un polinomio de grado $n \geq 1$ con coeficientes en un cuerpo k y sean $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$ en una extensión K de k donde tenga todas sus raíces, cada una repetida tantas veces como indique su multiplicidad. Llamaremos **discriminante** de $p(x)$ a

$$\Delta = c_0^{2n-2} \prod_{i<j} (\alpha_j - \alpha_i)^2$$

de modo que la *condición necesaria y suficiente para que $p(x)$ tenga alguna raíz múltiple es que su discriminante sea nulo.* Según el teorema de los polinomios simétricos, existe un polinomio con coeficientes enteros $D(x_1, \ldots, x_n)$ tal que

$$\prod_{i<j} (x_j - x_i)^2 = D(s_1, \ldots, s_n)$$

Por las fórmulas de Cardano, $\Delta = c_0^{2n-2} D(-c_1/c_0, c_2/c_0, \ldots, (-1)^n c_n/c_0)$ y se concluye que *el discriminante Δ es un elemento del cuerpo de coeficientes k que no depende de la extensión elegida K.* De hecho tenemos que

$$\Delta = c_0^{2n-2} \begin{vmatrix} 1 & 1 & .. & 1 \\ \alpha_1 & \alpha_2 & .. & \alpha_n \\ . & . & .. & . \\ \alpha_1^{n-1} & \alpha_2^{n-1} & .. & \alpha_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & \alpha_1 & .. & \alpha_1^{n-1} \\ 1 & \alpha_2 & .. & \alpha_2^{n-1} \\ . & . & .. & . \\ 1 & \alpha_n & .. & \alpha_n^{n-1} \end{vmatrix} =$$

$$= c_0^{2n-2} \begin{vmatrix} n & \sigma_1 & .. & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & .. & \sigma_n \\ . & . & .. & . \\ \sigma_{n-1} & \sigma_n & .. & \sigma_{2n-2} \end{vmatrix}$$

Discriminante de la Cúbica $x^3 - px^2 + qx - r$.

$\sigma_1 = p,\ \sigma_2 = p^2 - 2q,\ \sigma_3 = p^3 - 3pq + 3r,\ \sigma_4 = p^4 - 4p^2q + 4pr + 2q^2$; luego:

$$\Delta = \begin{vmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{vmatrix} = -4p^3r - 27r^2 + 18pqr - 4q^3 + p^2q^2$$

En particular, el discriminante de la cúbica $x^3 + qx - r$ es $\Delta = -4q^3 - 27r^2$.

Discriminante de la Cuártica $x^4 - px^3 + qx^2 - rx + s$.

Si $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son las raíces de una cuártica (cada una repetida tantas veces como indique su multiplicidad), llamaremos **cúbica resolvente** de la cuártica al polinomio unitario cuyas raíces son

$$\vartheta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4\ ,\ \vartheta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4\ ,\ \vartheta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

Es decir, la cúbica resolvente es

$$(y - \vartheta_1)(y - \vartheta_2)(y - \vartheta_3) = y^3 - qy^2 + (pr - 4s)y - (s(p^2 - 4q) + r^2)$$

y el discriminante de la cuártica coincide con el de su cúbica resolvente:

$$(\vartheta_2 - \vartheta_1)(\vartheta_3 - \vartheta_1)(\vartheta_3 - \vartheta_2) = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_4 - \alpha_2)(\alpha_1 - \alpha_2)(\alpha_4 - \alpha_3)$$

A.4 El Polinomio Genérico

Definición: Sea k un cuerpo y n un número natural no nulo. El polinomio

$$\sum_{i=0}^{n} c_i x^{n-i} = c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n$$

con coeficientes en el cuerpo $k(c_0, c_1, \ldots, c_n)$ de fracciones racionales en $n+1$ indeterminadas se llamará **polinomio genérico** de grado n con coeficientes en k (aunque no sea un polinomio con coeficientes en k).

También diremos que $x^n + c_1x^{n-1} + \ldots + c_n$ es el **polinomio unitario genérico** de grado n con coeficientes en k.

Sea $L = k(x_1, \ldots, x_n)$ el cuerpo de fracciones racionales en n indeterminadas con coeficientes en el cuerpo k, y sean $s_1, \ldots, s_n$ las funciones simétricas elementales en $x_1, \ldots, x_n$. El morfismo de anillos $k[c_1, \ldots, c_n] \to k(x_1, \ldots x_n)$ que transforma c_r en $(-1)^r s_r$ y es la identidad sobre k, es inyectivo en virtud del teorema

de los polinomios simétricos; luego induce un morfismo de anillos

$$\Sigma = k(c_1, \ldots, c_n) \to k(x_1, \ldots, x_n) = L$$

cuya imagen es $k(s_1, \ldots, s_n)$. De acuerdo con las fórmulas de Cardano

$$x^n + c_1 x^{n-1} + \ldots + c_n = (x - x_1) \cdots (x - x_n)$$

y concluimos que el polinomio unitario genérico tiene todas sus raíces en L y que sus raíces son $x_1, \ldots, x_n$. Por tanto, *las raíces del polinomio unitario genérico de grado n con coeficientes en un cuerpo k son simples.*

Si $L = k(c_0, x_1, \ldots, x_n)$ es el cuerpo de fracciones racionales en $n+1$ indeterminadas con coeficientes en un cuerpo k, análogamente se define un morfismo de anillos $k(c_0, c_1, \ldots, c_n) \to k(c_0, x_1, \ldots, x_n) = L$ que transforma c_r en $(-1)^r s_r(x_1, \ldots, x_n)c_0$ y c_0 en c_0, de modo que

$$c_0 x^n + c_1 x^{n-1} + \ldots + c_n = c_0(x - x_1) \cdots (x - x_n)$$

y concluimos que el polinomio genérico de grado n tiene todas sus raíces en L. También las raíces del polinomio genérico de grado n con coeficientes en un cuerpo son simples.

Teorema A.4.1 *El polinomio genérico de grado n con coeficientes en un cuerpo k es irreducible*

Demostración: El polinomio genérico es irreducible en $k(c_0, \ldots, c_{n-1}, x)[c_n]$ porque es de grado 1 en c_n. Luego es irreducible en $k[c_0, \ldots, c_n, x]$ y el lema de Gauss (1777-1855) permite concluir que es irreducible en $k(c_0, \ldots, c_n)[x]$.

Apéndice B

Irracionales Cuadráticos

B.1 Irracionales Cuadráticos

Definición: Diremos que un número complejo α es un **irracional cuadrático** si existen números complejos $\alpha_1, \ldots, \alpha_n$ tales que $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ y α_i^2 está en $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ para todo índice $1 \leq i \leq n$.

Diremos que un polinomio con coeficientes racionales es **resoluble por radicales cuadráticos** si todas sus raíces complejas son irracionales cuadráticos.

Ejemplos:

1. Los irracionales cuadráticos son los números complejos que pueden expresarse, a partir de los números racionales, mediante un número finito de sumas, productos, cocientes y raíces cuadradas. Según 4.4.6 y 4.4.7, todo irracional cuadrático es algebraico sobre $\mathbb{Q}$.

2. Toda ecuación cuadrática $ax^2 + bx + c = 0$ es resoluble por radicales cuadráticos, porque sus raíces son $(-b \pm (b^2 - 4ac)^{1/2})/2$.

3. Toda ecuación bicuadrada $ax^4 + bx^2 + c = 0$ es resoluble por radicales cuadráticos, pues sus raíces son $\pm\sqrt{z_1}$ y $\pm\sqrt{z_2}$, donde z_1 y z_2 son las raíces de $az^2 + bz + c$.

4. Toda cuártica recíproca $ax^4 + bx^3 + cx^2 + bx + a = 0$ es resoluble por radicales cuadráticos. En efecto, no tiene la raíz nula porque $a \neq 0$ y, dividiendo por x^2, obtenemos:

$$\begin{aligned} a(x^2 + x^{-2}) + b(x + x^{-1}) + c &= 0 \\ a(y^2 - 2) + by + c &= 0 \qquad y = x + x^{-1} \end{aligned}$$

y concluimos que las raíces de la cuártica dada son las soluciones de las ecuaciones cuadráticas $x^2 - y_1 x + 1 = 0$, $x^2 - y_2 x + 1 = 0$; donde y_1, y_2 son las raíces de $ay^2 + by + c - 2a$. Luego son irracionales cuadráticos.

5. Las raíces de la unidad $e^{\frac{2\pi i}{3}}$, $e^{\frac{2\pi i}{4}}$, $e^{\frac{2\pi i}{5}}$ y $e^{\frac{2\pi i}{6}}$ son irracionales cuadráticos, porque son raíces de los polinomios $x^2 + x + 1$, $x^2 + 1$, $x^4 + x^3 + x^2 + x + 1$ y $x^2 - x + 1$ respectivamente.

Lema B.1.1 *Sea K una extensión de un cuerpo k. Si existe $\alpha \in K$ tal que $K = k(\alpha)$ y $\alpha^2 \in k$, entonces el grado de K sobre k es 1 ó 2.*

Demostración: Sea $a = \alpha^2 \in k$. Como α es raíz de $x^2 - a \in k[x]$, su polinomio irreducible $p_\alpha(x)$ sobre k divide a $x^2 - a$ y por tanto su grado es 1 ó 2. Concluimos ya que $[k(\alpha) : k] = \operatorname{gr} p_\alpha(x)$ de acuerdo con 4.4.2.

Teorema B.1.2 *Los irracionales cuadráticos forman una extensión de $\mathbb{Q}$ estable por raíces cuadradas. Además, el grado sobre $\mathbb{Q}$ de cualquier extensión generada por un número finito de irracionales cuadráticos es una potencia de 2.*

Demostración: Sean α, β dos irracionales cuadráticos. Por definición α está en la extensión de $\mathbb{Q}$ generada por unos números complejos $\alpha_1, \ldots, \alpha_n$, donde

$$\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$$

y β está en la extensión generada por ciertos $\beta_1, \ldots, \beta_m$, donde

$$\beta_j^2 \in \mathbb{Q}(\beta_1, \ldots, \beta_{j-1}) \ .$$

Es claro que el cuadrado de cada término de la sucesión $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ está en la extensión generada por los anteriores. Como $\alpha + \beta$, $\alpha\beta$ y α/β están en $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ se sigue que son irracionales cuadráticos. Es decir, los irracionales cuadráticos forman una extensión de $\mathbb{Q}$.

Además, es evidente que $\sqrt{\alpha}$ es un irracional cuadrático cuando α lo es.

Por otra parte, si K es una extensión de $\mathbb{Q}$ generada por un número finito de irracionales cuadráticos, el argumento anterior muestra que

$$K \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$$

donde $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ para todo índice i. Según el lema anterior, el grado de $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ sobre $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ es 1 ó 2; así que el teorema del grado prueba que el grado de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ sobre $\mathbb{Q}$ es potencia de 2. De nuevo el teorema del grado afirma que el grado de K sobre $\mathbb{Q}$ divide al grado de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, lo que nos permite concluir que el grado de K sobre $\mathbb{Q}$ es potencia de 2.

Corolario B.1.3 *El grado del polinomio irreducible de cualquier irracional cuadrático es una potencia de 2.*

Demostración: Sea α un irracional cuadrático. El grado del polinomio irreducible de α sobre $\mathbb{Q}$ coincide con el grado de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$, que es una potencia de 2 según el teorema anterior.

Corolario B.1.4 *Si un polinomio irreducible es resoluble por radicales cuadráticos, su grado es potencia de 2.*

Demostración: Todo polinomio irreducible en $\mathbb{Q}[x]$ es el polinomio irreducible sobre $\mathbb{Q}$ de cualquiera de sus raíces.

Corolario B.1.5 *Si un polinomio es resoluble por radicales cuadráticos, entonces el grado de la extensión generada por sus raíces complejas es potencia de 2.*

Ejemplos:

1. El número complejo $e^{\frac{2\pi i}{7}}$ no es un irracional cuadrático, porque su polinomio irreducible sobre $\mathbb{Q}$, que es $x^6 + \ldots + x + 1$ en virtud de 5.5.3, tiene grado 6, que no es potencia de 2.

2. El número complejo $e^{\frac{2\pi i}{9}}$ es raíz del polinomio $p(x) = x^6 + x^3 + 1$ porque $(e^{\frac{2\pi i}{9}})^3 = e^{\frac{2\pi i}{3}}$ es raíz del polinomio $x^2 + x + 1$. La reducción de $p(x)$ módulo 2 es irreducible porque no tiene raíces en $\mathbb{F}_2$, no es múltiplo de $x^2 + x + 1$, $x^3 + x + 1$ ni $x^3 + x^2 + 1$, que son los únicos polinomios irreducibles de grado 2 y 3 con coeficientes en $\mathbb{F}_2$.

   Luego $p(x)$ es irreducible en $\mathbb{Z}[x]$ y, por el lema de Gauss, en $\mathbb{Q}[x]$; así que $p(x)$ es el polinomio irreducible de $e^{\frac{2\pi i}{9}}$ sobre $\mathbb{Q}$. Como su grado no es potencia de 2, se concluye que $e^{\frac{2\pi i}{9}}$ no es un irracional cuadrático.

3. Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ las cuatro raíces complejas de la cuártica irreducible

$$p(x) = x^4 - x^3 + x^2 + 1$$

   Su cúbica resolvente es $y^3 - y^2 - 4y + 3$, que no tiene raíces racionales y es por tanto irreducible. Una raíz de la cúbica resolvente es $\vartheta = \alpha_1\alpha_2 + \alpha_3\alpha_4$, así que el grado de $\mathbb{Q}(\vartheta)$ sobre $\mathbb{Q}$ es 3. Como $\mathbb{Q}(\vartheta)$ está contenido en $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, el teorema del grado permite concluir que el grado de $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ sobre $\mathbb{Q}$ es un múltiplo de 3. Luego el polinomio $p(x)$ no es resoluble por radicales cuadráticos.

   Nótese que los números complejos α_i no son irracionales cuadráticos, a pesar de que su polinomio irreducible, que es $p(x)$, tiene grado 4.

B.2 Construcciones con Regla y Compás

Definición: Dado un segmento OP en un plano euclídeo, los puntos, rectas y círculos **constructibles con regla y compás** a partir de O y P se definen inductivamente mediante la aplicación reiterada de un número finito de las construcciones siguientes:

1. Los puntos dados O y P son constructibles.
2. Si dos puntos distintos son constructibles, la recta que pasa por ellos es constructible.
3. El círculo con centro en un punto constructible y radio congruente con un segmento determinado por dos puntos constructibles es constructible.
4. Los puntos de corte de dos líneas (rectas o círculos) constructibles distintas son constructibles.

Las siguientes construcciones pueden realizarse con regla y compás:

–. Trazar la perpendicular por su punto medio a un segmento dado.
–. Trazar la paralela a una recta dada por un punto exterior dado.
–. Trazar el círculo que pasa por tres puntos dados no alineados.
–. Trazar la bisectriz de un ángulo dado.

Dado un segmento de extremos O, P en un plano euclídeo, la recta OP y su perpendicular por el punto O forman unos ejes cartesianos en el plano, de modo que cada punto A se corresponde con un par ordenado de números reales (a, b) y, por tanto, con un número complejo $a + bi$. Identificaremos sin más cada punto del plano con el correspondiente número complejo y diremos que un número complejo $\alpha \in \mathbb{C}$ es **constructible** cuando el correspondiente punto del plano sea constructible con regla y compás a partir de O y P.

El punto O se identifica con el número 0, el punto P con el número 1, los puntos de la recta OP con los números reales y los puntos de la recta perpendicular a OP por O con los números imaginarios puros.

Lema B.2.1 *La condición necesaria y suficiente para que un número complejo $a + bi$ sea constructible es que lo sean a y b.*

Demostración: Es consecuencia directa de la posibilidad de trazar paralelas y perpendiculares con regla y compás.

Lema B.2.2 *Los números complejos constructibles forman una extensión de $\mathbb{Q}$ estable por raíces cuadradas. Por tanto, todos los irracionales cuadráticos son constructibles.*

Demostración: Veamos primero que los números complejos constructibles forman un cuerpo. Como los números 0 y 1 son constructibles, basta probar que si dos números complejos a, b son constructibles, $a - b$ y a/b también lo son. Según el lema anterior podemos suponer que a y b son números reales. La diferencia $a - b$ es obviamente constructible. En cuanto al cociente a/b, el círculo con centro en O que pasa por ai, $-b$ y $-i$ corta al eje real en a/b.

Para concluir veremos que la raíz cuadrada de cualquier número complejo constructible también lo es. Si el número es real y positivo, basta observar que el círculo con centro en $(a-1)/2$ que pasa por -1 corta al eje imaginario en $\sqrt{a}i$. En el caso de un número complejo arbitrario z, basta cortar las bisectrices de la recta que lo une con el origen y el eje real, con el círculo centrado en el origen y de radio igual a la raíz cuadrada del módulo de z.

Lema B.2.3 *Si el punto de coordenadas (a, b) es constructible con regla y compás, entonces los números reales a y b son irracionales cuadráticos.*

Si la recta de ecuación $y = ax + b$ ó $x = ay + b$ es constructible con regla y compás, entonces los números reales a y b son irracionales cuadráticos.

Si el círculo de ecuación $x^2 + y^2 + ax + by + c = 0$ es constructible con regla y compás, entonces los números reales a, b, c son irracionales cuadráticos.

Demostración: Los puntos dados O y P, que tienen coordenadas (0,0) y (1,0), verifican el enunciado porque 0 y 1 son irracionales cuadráticos.

Procediendo inductivamente, bastará probar que si unos puntos, rectas o círculos constructibles verifican el enunciado y se efectúa alguna de las construcciones de la definición, los puntos, rectas o círculos que se obtienen también verifican el enunciado:

1) Sean (a, b) y (c, d) dos puntos distintos. La ecuación de la única recta que pasa por ellos (cuando $c \neq a$) es $y = b + (d - b)(x - a)/(c - a)$, así que todos sus coeficientes son irracionales cuadráticos cuando a, b, c, d lo son.

2) La ecuación del círculo con centro en un punto de coordenadas (a, b) y radio congruente con el segmento determinado por dos puntos de coordenadas (c, d) y (e, f) es $(x - a)^2 + (y - b)^2 = r$, donde $r = (e - c)^2 + (f - d)^2$, así que todos sus coeficientes son irracionales cuadráticos cuando a, b, c, d, e, f lo son.

3) Si $ax+by = c\,,\ dx+ey = f$ son dos rectas distintas, entonces las coordenadas de su punto de corte son $(ce-bf)/(ae-bd)$ y $(af-bc)/(ae-bf)$, que son irracionales cuadráticos cuando a, b, c, d, e, f lo son.

4) Sean $y = ax + b\,,\ x^2 + y^2 + cx + dy + e = 0$ una recta y un círculo. Las coordenadas de sus puntos de corte son $(\alpha, a\alpha + b)$, donde α recorre las raíces reales del polinomio $(1 + a^2)x^2 + (c + 2ab + ad)x + (b^2 + bd + e) = 0$; luego son irracionales cuadráticos cuando a, b, c, d, e lo son.

5) Si $x^2+y^2+ax+by+c=0$ y $x^2+y^2+dx+ey+f=0$ son dos círculos distintos, sus puntos de corte son los de uno de ellos con la recta

$$(x^2+y^2+ax+by+c)-(x^2+y^2+dx+ey+f)=(a-d)x+(b-e)y+(c-f)=0$$

Si a,b,c,d,e,f son irracionales cuadráticos, también lo son los coeficientes de la ecuación de esta recta; luego, según el apartado anterior, concluimos que las coordenadas de todos los puntos de corte son irracionales cuadráticos.

Teorema B.2.4 *La condición necesaria y suficiente para que un número complejo sea constructible es que sea un irracional cuadrático.*

Demostración: El lema B.2.2 afirma que tal condición es suficiente.

Recíprocamente, si $\alpha=a+bi\in\mathbb{C}$ es constructible, B.2.3 afirma que a y b son irracionales cuadráticos; luego también lo es $\alpha=a+bi$.

Ejemplos:

1. Construir el lado de un cubo con volumen doble que el de un cubo de lado dado OP significa construir un segmento cuya proporción con OP sea la raíz cúbica de 2, lo que equivale a construir el punto correspondiente al número $\sqrt[3]{2}$. Tal construcción sólo es posible si $\sqrt[3]{2}$ es un irracional cuadrático, lo que no es el caso: no es posible duplicar un cubo con regla y compás.

2. Construir el lado de un cuadrado de área igual a la de un círculo de radio dado equivale a construir el punto correspondiente a $\sqrt{\pi}$. La trascendencia de π (teorema de Lindemann (1852-1939) que no probaremos en este libro), implica que $\sqrt{\pi}$ es trascendente y, por tanto, no es un irracional cuadrático: La cuadratura del círculo con regla y compás es imposible.

3. Construir un ángulo de α radianes equivale a construir el punto que corresponde al número complejo $\cos\alpha+i\,\mathrm{sen}\,\alpha$. El ángulo de $2\pi/3$ radianes puede construirse con regla y compás, porque

   $$\cos(2\pi/3)+i\,\mathrm{sen}\,(2\pi/3)=e^{\frac{2\pi i}{3}}=(-1+\sqrt{3}i)/2$$

   es un irracional cuadrático. Sin embargo, el ángulo de $2\pi/9$ radianes no se puede construir con regla y compás, porque $e^{\frac{2\pi i}{9}}$ no es un irracional cuadrático: Es imposible trisecar todos los ángulos con regla y compás.

B.3 Construcción de Polígonos Regulares

Dado un número natural $n\geq 3$, construir con regla y compás un polígono regular de n lados inscrito en un círculo de radio dado equivale a construir el punto

correspondiente al número complejo $e^{\frac{2\pi i}{n}} = \cos(2\pi/n) + i\,\mathrm{sen}\,(2\pi/n)$, que es una raíz n-ésima primitiva de la unidad. En consecuencia, la condición necesaria y suficiente para que la construcción de tal polígono sea posible es que $e^{\frac{2\pi i}{n}}$ sea un irracional cuadrático.

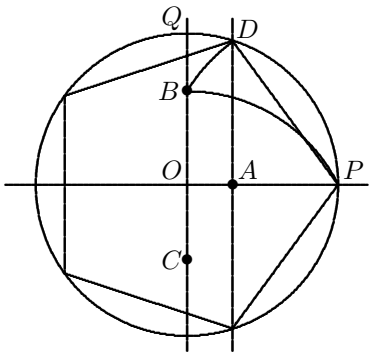
El triángulo equilátero inscrito en un círculo de radio dado puede construirse con regla y compás, pues $e^{\frac{2\pi i}{3}} = (-1+\sqrt{3}i)/2$ es un irracional cuadrático. Como la parte real de $e^{\frac{2\pi i}{3}}$ es $-1/2$, para construir tal triángulo basta cortar el círculo dado con la perpendicular por el punto medio al segmento de extremos -1 y 0.

Las raíces quintas de la unidad primitivas son las soluciones complejas de la ecuación recíproca $x^4 + x^3 + x^2 + x + 1 = 0$, que con el cambio $y = x + x^{-1}$ se transforma en $y^2+y-1 = 0$. Las raíces de este polinomio son y_1, $y_2 = (-1\pm\sqrt{5})/2$, así que las raíces quintas de la unidad primitivas son

$$\frac{y_i \pm \sqrt{y_i^2 - 4}}{2}$$

que son irracionales cuadráticos. Por tanto, se puede construir con regla y compás el pentágono regular inscrito en un círculo de radio dado.

Esta determinación de las raíces quintas de la unidad puede utilizarse para dar una construcción efectiva del pentágono regular. Nótese que la parte real de $e^{\frac{2\pi i}{5}}$ es $\alpha = (-1+\sqrt{5})/4$. Dado un segmento OP, se construye el punto $C = -i/2$. Como la distancia entre P y C es $\sqrt{5}/2$, el punto equidistante de C en el segmento OQ es $B = 2\alpha i$. Luego el círculo con centro en O que pasa por el punto medio de OB corta al segmento OP en el punto $A = \alpha$ y la perpendicular a OP en A corta al círculo de radio OP en $D = e^{\frac{2\pi i}{5}}$, que es un vértice del pentágono regular inscrito con vértice en P (Una construcción más sencilla se obtiene observando que PB es congruente con el lado del pentágono):



La posibilidad de trazar bisectrices con regla y compás muestra que, si el polígono regular de n lados es constructible, también lo es el polígono regular

de $2n$ lados. Por otra parte, si n y m son números naturales primos entre sí, entonces

$$e^{\frac{2\pi i}{n}} e^{\frac{2\pi i}{m}} = e^{\frac{2\pi i}{nm}(n+m)}$$

es una raíz nm-ésima primitiva de la unidad y, por tanto, $e^{\frac{2\pi i}{nm}}$ es una potencia de $e^{\frac{2\pi i}{n}} e^{\frac{2\pi i}{m}}$; luego $e^{\frac{2\pi i}{nm}}$ es un irracional cuadrático cuando $e^{\frac{2\pi i}{n}}$ y $e^{\frac{2\pi i}{m}}$ lo son. Es decir, si los polígonos regulares de n y m lados son constructibles con regla y compás, también lo es el polígono regular de nm lados. En resumen: *Los polígonos regulares de* 2^n, 2^n3, 2^n5 *y* 2^n15 *lados inscritos en un círculo de radio dado pueden construirse con regla y compás.*

Teorema B.3.1 *Sea p un número primo. Si puede construirse con regla y compás el polígono regular de p lados inscrito en un círculo de radio dado, entonces p es un primo de Fermat (es decir, está precedido por una potencia de 2).*

Demostración: Si el polígono regular de p lados inscrito en un círculo de radio dado es constructible con regla y compás, entonces $e^{\frac{2\pi i}{p}}$ es un irracional cuadrático. Luego el grado de su polinomio irreducible sobre $\mathbb{Q}$, que es $x^{p-1} + \ldots + x + 1$, es una potencia de 2.

Corolario B.3.2 *Es imposible construir con regla y compás los polígonos regulares de 7, 11, 13, 19, 23, 29,... lados inscritos en un círculo de radio dado.*

B.4 Raíces de la Unidad

Sea n un número natural no nulo. Las raíces n-ésimas de la unidad complejas forman, respecto del producto de números complejos, un grupo cíclico de orden n que denotaremos μ_n. Los generadores de μ_n son las raíces n-ésimas de la unidad **primitivas** .

El número de raíces n-ésimas de la unidad primitivas es el indicador de Euler $\phi(n)$. Una raíz n-ésima de la unidad primitiva es $e^{\frac{2\pi i}{n}} = \cos(2\pi/n) + i \operatorname{sen}(2\pi/n)$, así que las raíces n-ésimas de la unidad primitivas son $e^{\frac{2\pi i}{n}m}$, donde $1 \leq m \leq n$ y m es primo con n.

Definición: Llamaremos **polinomio ciclotómico** n-ésimo al polinomio unitario $\Phi_n(x)$ que tiene como raíces simples las raíces n-ésimas de la unidad primitivas:

$$\Phi_n(x) = \prod_{\substack{\text{m.c.d.}(m,n)=1 \\ 1 \leq m \leq n}} (x - e^{\frac{2\pi i}{n}m})$$

Sea d un divisor de n. Las raíces d-ésimas de la unidad primitivas son los elementos de orden d del grupo μ_n. Como el orden de cualquier elemento de μ_n

es un divisor de n, concluimos que

$$\mu_n = \bigcup_{d|n} \{ \text{ raíces } d\text{-ésimas de la unidad primitivas} \}$$

y esta unión es disjunta. Luego:

$$x^n - 1 = \prod_{\alpha \in \mu_n} (x - \alpha) = \prod_{d|n} \Phi_d(x) \tag{B.1}$$

Ejemplos: $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$, $\Phi_{2p}(x) = \Phi_p(-x) = x^{p-1} - x^{p-2} + \ldots - x + 1$, donde p denota un número primo impar.

Teorema B.4.1 (Kronecker 1823-1891) *Los polinomios ciclotómicos son polinomios irreducibles con coeficientes enteros.*

Demostración: Para demostrar que $\Phi_n(x)$ tiene coeficientes enteros para todo $n \geq 1$ procedemos por inducción sobre n, porque es evidente cuando $n = 1$. Cuando $n \geq 2$, tenemos

$$x^n - 1 = \Phi_n(x) \cdot \textstyle\prod_d \Phi_d(x)$$

donde d recorre los divisores positivos de n menores que n. Por hipótesis de inducción, $q(x) = \prod_d \Phi_d(x)$ tiene coeficientes enteros y es unitario; luego $\Phi_n(x)$ tiene coeficientes enteros, porque es el cociente de un polinomio con coeficientes enteros por un polinomio unitario con coeficientes enteros.

En cuanto a la irreducibilidad de $\Phi_n(x)$ en $\mathbb{Z}[x]$, consideremos la descomposición de $\Phi_n(x)$ en producto de polinomios irreducibles en $\mathbb{Z}[x]$ y el factor irreducible $q(x)$ que tenga la raíz $e^{\frac{2\pi i}{n}}$. Podemos suponer que $q(x)$ es unitario y bastará probar que $q(x) = \Phi_n(x)$. Como ambos polinomios son unitarios, es suficiente demostrar que todas las raíces n-ésimas de la unidad primitivas son raíces de $q(x)$. Ahora bien, tales raíces primitivas son de la forma $e^{\frac{2\pi i}{n} m}$ donde m es un número natural primo con n, así que m es producto de números primos que no dividen a n y bastará probar que: *si α es una raíz de $q(x)$ y p es un número primo que no divide a n, entonces α^p también es raíz de $q(x)$.*

Supongamos que α^p no es raíz de $q(x)$. En tal caso, si $x^n - 1 = q(x)c(x)$, se sigue que α^p es raíz de $c(x)$, porque es raíz de $x^n - 1$. Luego α es raíz de $c(x^p)$, así que $c(x^p)$ y $q(x)$ no son primos entre sí en $\mathbb{Q}[x]$ y, al ser $q(x)$ irreducible en $\mathbb{Q}[x]$, obtenemos que $c(x^p) = q(x)r(x)$ para algún $r(x) \in \mathbb{Q}[x]$ que, por 5.4.2, tiene coeficientes enteros. Reduciendo módulo p (vía el morfismo $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ inducido por la proyección canónica $\mathbb{Z} \to \mathbb{F}_p$) tenemos:

$$\bar{q}(x) \cdot \bar{r}(x) = \bar{c}(x^p) = \bar{c}(x)^p$$

donde la última igualdad se debe a la congruencia de Fermat:

$$c(x) = \sum_i a_i x^i$$
$$\bar{c}(x^p) = \sum_i \bar{a}_i x^{pi} = \sum_i \bar{a}_i{}^p (x^i)^p = \left(\sum_i \bar{a}_i x^i\right)^p = \bar{c}(x)^p$$

Por tanto, cualquier factor irreducible de $\bar{q}(x)$ divide a $\bar{c}(x)$, y el polinomio $x^n - 1 = \bar{q}(x)\bar{c}(x)$ no es primo con su derivada nx^{n-1}, lo que implica que $n = 0$ en $\mathbb{F}_p$, en contra de la hipótesis de que n no es múltiplo de p.

Corolario B.4.2 *El polinomio irreducible de $e^{\frac{2\pi i}{n}}$ sobre $\mathbb{Q}$ es $\Phi_n(x)$ y el grado de $\mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big)$ sobre $\mathbb{Q}$ es $\phi(n)$. Por tanto, si $\phi(n)$ no es potencia de 2, entonces $e^{\frac{2\pi i}{n}}$ no es un irracional cuadrático.*

Teorema B.4.3 *Si el polígono regular de n lados inscrito en un círculo de radio dado es constructible con regla y compás, entonces n es producto de una potencia de 2 y de números primos de Fermat distintos.*

Demostración: Si el polígono regular de n lados inscrito en un círculo de radio dado es constructible con regla y compás, entonces $e^{\frac{2\pi i}{n}}$ es un irracional cuadrático y el grado de su polinomio irreducible $\Phi_n(x)$ sobre $\mathbb{Q}$ ha de ser una potencia de 2. Sea $n = 2^m p^a q^b \cdots$ la descomposición de n en producto de potencias de primos distintos. Tenemos que

$$\phi(n) = 2^{m-1} p^{a-1}(p-1) q^{b-1}(q-1)\cdots$$

y, cuando $\phi(n)$ es potencia de 2, se sigue que $1 = a = b = \ldots$ y que $p-1$, $q-1, \ldots$ son potencias de 2; es decir, los factores primos impares de n son primos de Fermat y ninguno está repetido.

Nota: Si $2^n + 1$ es un número primo, es sencillo probar que n es potencia de 2. Los únicos primos de Fermat (1601-1665) conocidos son 3, 5, 17, $257 = 2^8 + 1$ y $2^{16} + 1 = 65537$. La teoría de Galois (1811-1832) permitirá probar que la condición necesaria y suficiente para que $e^{\frac{2\pi i}{n}}$ sea un irracional cuadrático es que $[\mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big) : \mathbb{Q}] = \phi(n)$ sea potencia de 2. Luego una consecuencia de tal teoría (ver H.3.3) es la posibilidad de construir con regla y compás los polígonos regulares de p lados, inscritos en un círculo de radio dado, cuando p es un primo de Fermat (en particular la de construir el polígono regular de 17 lados).

Apéndice C

Módulos Proyectivos, Inyectivos y Planos

C.1 Módulos Proyectivos

Definición: Sea A un anillo. Diremos que un A-módulo P es **proyectivo** si el funtor $\mathrm{Hom}_A(P,-)$ conserva sucesiones exactas; es decir, si para toda sucesión exacta corta de A-módulos

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

se verifica que la correspondiente sucesión

$$0 \longrightarrow \mathrm{Hom}_A(P,M') \xrightarrow{i_*} \mathrm{Hom}_A(P,M) \xrightarrow{p_*} \mathrm{Hom}_A(P,M'') \longrightarrow 0$$

también es exacta. Como la anterior sucesión siempre es exacta salvo por lo que se refiere a la epiyectividad del morfismo $p_*\colon \mathrm{Hom}_A(P,M) \longrightarrow \mathrm{Hom}_A(P,M'')$, la condición de que P sea un A-módulo proyectivo equivale a que, para todo epimorfismo de A-módulos $p\colon M \to M''$, también sea epiyectivo el correspondiente morfismo $p_*\colon \mathrm{Hom}_A(P,M) \longrightarrow \mathrm{Hom}_A(P,M'')$.

Proposición C.1.1 *La condición necesaria y suficiente para que una suma directa $P = \bigoplus_i P_i$ de A-módulos sea un A-módulo proyectivo es que cada sumando P_i sea un A-módulo proyectivo.*

Demostración: Esta afirmación es consecuencia del isomorfismo natural

$$\mathrm{Hom}_A\big(\textstyle\bigoplus_i P_i, M\big) \;=\; \prod_i \mathrm{Hom}_A(P_i,M)$$

que muestra que el funtor $\mathrm{Hom}_A(P,-)$ es exacto si y sólo si todos los funtores $\mathrm{Hom}_A(P_i,-)$ son exactos.

Corolario C.1.2 *Todo A-módulo libre es proyectivo.*

Demostración: El A-módulo A es proyectivo, porque $\mathrm{Hom}_A(A, M) = M$ para todo A-módulo M, y la proposición anterior nos permite concluir.

Proposición C.1.3 *La condición necesaria y suficiente para que un A-módulo P sea proyectivo es que escinda toda sucesión exacta corta de A-módulos*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow P \longrightarrow 0$$

Demostración: Sea $0 \to M' \longrightarrow M \xrightarrow{p} P \to 0$ una sucesión exacta. Si P es proyectivo, por definición existe un morfismo de A-módulos $s\colon P \to M$ tal que $p \circ s = id_P$ y concluimos que la sucesión exacta escinde.

Para demostrar el recíproco consideramos un epimorfismo $p\colon L \to P$ donde L es un A-módulo libre. La sucesión exacta $0 \to \mathrm{Ker}\, p \to L \to P \to 0$ escinde por hipótesis, así que P es un sumando directo de L y concluimos que P es proyectivo en virtud de la proposición C.1.1.

C.2 Módulos Inyectivos

Definición: Sea A un anillo. Diremos que un A-módulo I es **inyectivo** si el funtor $\mathrm{Hom}_A(-, I)$ conserva sucesiones exactas; es decir, si para toda sucesión exacta corta de A-módulos

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

se verifica que la correspondiente sucesión

$$0 \longrightarrow \mathrm{Hom}_A(M'', I) \xrightarrow{p^*} \mathrm{Hom}_A(M, I) \xrightarrow{i^*} \mathrm{Hom}_A(M', I) \longrightarrow 0$$

también es exacta. Como la anterior sucesión siempre es exacta salvo por lo que se refiere a la epiyectividad del morfismo $i^*\colon \mathrm{Hom}_A(M, I) \longrightarrow \mathrm{Hom}_A(M', I)$, la condición de que I sea un A-módulo inyectivo equivale a que, para todo morfismo de A-módulos inyectivo $i\colon M' \to M$, sea epiyectivo el correspondiente morfismo de A-módulos $i^*\colon \mathrm{Hom}_A(M, I) \longrightarrow \mathrm{Hom}_A(M', I)$.

Proposición C.2.1 *Si un A-módulo I es inyectivo, entonces escinden todas las sucesiones exactas de la forma*

$$0 \longrightarrow I \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

Demostración: Se prueba de modo análogo al caso de los módulos proyectivos.

Criterio del Ideal: *Sea I un A-módulo. Si para cada morfismo de A-módulos $f\colon \mathfrak{a} \to I$, donde $\mathfrak{a}$ es un ideal de A, existe algún $x \in I$ tal que $f(a) = ax$ para todo $a \in \mathfrak{a}$, entonces I es un A-módulo inyectivo.*

Demostración: Sea $i\colon M' \to M$ un morfismo inyectivo de A-módulos y $h\colon M' \to I$ un morfismo de A-módulos arbitrario. Sustituyendo M' por $i(M')$ podemos suponer que M' es un submódulo de M, y hemos de extender h hasta obtener un morfismo de A-módulos $M \to I$.

Consideremos el conjunto X de todas las parejas (N, g) donde N es un submódulo de M que contiene a M' y $g\colon N \to I$ es una extensión de h. Este conjunto no es vacío porque en él está la pareja (M', h). Si definimos en X la relación de orden

$$(N, g) \leq (N', g') \quad \text{cuando} \quad N \subseteq N' \text{ y } g' = g \text{ en } N$$

es claro que satisface las hipótesis del lema de Zorn, así que en X existen elementos maximales. Sea (N, g) un elemento maximal de X.

Si $N = M$, entonces g es la extensión de h buscada. Si $N \neq M$, existe $m \in M$ tal que $N' = N + Am$ contiene estrictamente a N. Consideremos el ideal $\mathfrak{a} = \{a \in A\colon\ am \in N\}$ y el morfismo $f\colon \mathfrak{a} \to I$, $f(a) = g(am)$. Por hipótesis existe $x \in I$ tal que $f(a) = ax$, lo que permite construir una aplicación

$$g'\colon N' \longrightarrow I\ , \quad g'(n + am) = g(n) + ax$$

bien definida: Si $n + am = \bar{n} + bm$, entonces $\bar{n} - n = (a - b)m$ y $a - b \in \mathfrak{a}$; luego $g(\bar{n} - n) = (b - a)x$ y concluimos que $g(n) + ax = g(\bar{n}) + bx$. Es sencillo comprobar que g' es morfismo de A-módulos, así que $(N, g) < (N', g')$ en contra del carácter maximal de (N, g).

Corolario C.2.2 *Sea A un dominio de ideales principales. La condición necesaria y suficiente para que un A-módulo I sea inyectivo es que sea* divisible*; es decir, que el morfismo $a\cdot\colon I \to I$ sea epiyectivo para todo $a \in A$ no nulo.*

Demostración: Supongamos que un A-módulo I es inyectivo. Si $a \in A$ no es nulo, define un morfismo inyectivo $a\colon A \to A$; luego es epiyectivo el morfismo

$$I = \mathrm{Hom}_A(A, I) \xrightarrow{\ a\ } \mathrm{Hom}_A(A, I) = I$$

Recíprocamente, si I es divisible y $f\colon \mathfrak{a} \to I$ es un morfismo de A-módulos, donde $\mathfrak{a} = aA$ es un ideal no nulo de A, por hipótesis existe $x \in I$ tal que $f(a) = ax$. Luego $f(ab) = abx$ para todo $ab \in aA$ y el criterio del ideal permite concluir que I es un A-módulo inyectivo.

C.3 Módulos Planos

Definición: Diremos que un A-módulo N es **plano** si el funtor $N \otimes_A (-)$ es exacto; i.e., si para toda sucesión exacta $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ de A-módulos se verifica que también es exacta la sucesión

$$0 \longrightarrow N \otimes_A M' \xrightarrow{1\otimes i} N \otimes_A M \xrightarrow{1\otimes p} N \otimes_A M'' \longrightarrow 0$$

Como la anterior sucesión siempre es exacta salvo por lo que se refiere a la inyectividad del morfismo $1 \otimes i \colon N \otimes_A M' \to N \otimes_A M$, la condición de que N sea plano significa que para todo morfismo inyectivo $i \colon M' \to M$ se tiene que el morfismo $1 \otimes i \colon N \otimes_A M' \to N \otimes_A M$ también es inyectivo.

-. El isomorfismo natural $A \otimes_A M = M$ muestra que el A-módulo A es plano.

-. El producto tensorial conmuta con sumas directas. Luego una suma directa de A-módulos es plana si y sólo si lo es cada sumando. En particular todos los A-módulos libres y proyectivos son planos.

-. El isomorfismo natural $(N_1 \otimes_A N_2) \otimes_A M = N_1 \otimes_A (N_2 \otimes_A M)$ muestra que el producto tensorial de A-módulos planos también es plano.

-. Sea S un sistema multiplicativo de un anillo A. El funtor de localización $S^{-1}(-)$ es exacto, de modo que el isomorfismo natural $M \otimes_A (S^{-1}A) = S^{-1}M$ muestra que $S^{-1}A$ es un A-módulo plano.

-. Si B es una A-álgebra plana y C es una B-álgebra plana, entonces C es una A-álgebra plana, como demuestra el isomorfismo natural $(M_B)_C = M_C$.

Proposición C.3.1 *Los módulos planos son estables por cambios de base. Es decir, si N es un A-módulo plano, para todo morfismo de anillos $A \to B$ se verifica que N_B es un B-módulo plano.*

Demostración: Para todo B-módulo M tenemos que $(N_B) \otimes_B M = N \otimes_A M$, así que el funtor $(N_B) \otimes_B (-)$ es exacto cuando lo sea el funtor $N \otimes_A (-)$.

Proposición C.3.2 *La condición necesaria y suficiente para que un A-módulo N sea plano es que N_x sea un A_x-módulo plano para todo $x \in \operatorname{Spec} A$.*

Demostración: Si N es plano sobre A, entonces $N_x = N \otimes_A A_x$ es plano sobre A_x de acuerdo con la proposición anterior.

Recíprocamente, sea $i \colon M' \to M$ un morfismo de A-módulos inyectivo. En todos los puntos $x \in \operatorname{Spec} A$ se tiene que $i_x \colon M'_x \to M_x$ es inyectivo; luego, por hipótesis, también es inyectivo el morfismo

$$(1 \otimes i)_x \colon (N \otimes_A M')_x = N_x \otimes_{A_x} M'_x \longrightarrow (N \otimes_A M)_x = N_x \otimes_{A_x} M_x$$

Como la inyectividad de un morfismo es una cuestión local, concluimos que el morfismo $1 \otimes i \colon N \otimes_A M' \to N \otimes_A M$ es inyectivo, lo que significa que N es un A-módulo plano.

Apéndice D

Módulos sobre Dominios de Ideales Principales

Este apéndice reproduce las notas de unas lecciones que a principios de los años 90 impartió Juan B. Sancho de Salas en el 2º curso de la Licenciatura de Matemáticas de la Universidad de Extremadura.

Definición: Un **dominio de ideales principales** es un anillo íntegro donde cada ideal es principal, es decir, está generado por un elemento.

En este apéndice A denotará un dominio de ideales principales.

Ejemplos de dominios de ideales principales son los anillos euclídeos, en particular $\mathbb{Z}$, $\mathbb{Z}[\,i\,]$ y el anillo de polinomios $k[x]$ con coeficientes en un cuerpo k . La localización de un dominio de ideales principales también es un dominio de ideales principales. El anillo local de una curva íntegra en un punto cerrado es un dominio de ideales principales cuando el punto es simple.

Definición: Un elemento **propio** (no nulo ni invertible) se dice que es **irreducible** si no descompone en producto de dos elementos propios. Se dice que dos elementos propios son **primos entre sí** si carecen de divisores propios comunes.

Nótese que un elemento a es divisor de otro b si y sólo si $bA \subseteq aA$.

Dados elementos $a, b \in A$, consideremos un generador d del ideal $aA + bA$. Como $a, b \in aA + bA = dA$, resulta que d es divisor de a y b. Por otra parte, si c es divisor de a y b, entonces $dA = aA + bA \subseteq cA$, luego c es divisor de d. En conclusión, d es el máximo común divisor de a y b en A.

De la igualdad $dA = aA + bA$ se deduce directamente la

Identidad de Bézout (1730-1783)**:** *Sea d el máximo común divisor de dos elementos a, b. Existen elementos $\alpha, \beta \in A$ tales que*

$$d = \alpha a + \beta b$$

Como caso particular resulta:

Corolario D.0.3 *Si a, b son primos entre sí, existen $\alpha, \beta \in A$ tales que*

$$1 \;=\; \alpha a + \beta b \;.$$

Lema D.0.4 *Si a divide a bc y es primo con b, entonces divide a c.*

Demostración: Sean $\alpha, \beta \in A$ tales que $1 = \alpha a + \beta b$. Multiplicando por c resulta $c = \alpha ac + \beta bc$; como a divide a los dos sumandos se concluye que divide también a la suma c.

Lema de Euclides (325?-265? a. de Cristo)**:** *Si un elemento irreducible divide un producto, divide algún factor.*

Proposición D.0.5 *Toda cadena de ideales de A estabiliza.*

Demostración: (Esta propiedad es válida en los anillos noetherianos; pero vamos a probarla en este caso particular). Dada una cadena de ideales $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ consideremos el generador c del ideal $\cup_i \mathfrak{a}_i$. Se cumple $c \in \mathfrak{a}_n$ para algún n. Las inclusiones $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+j} \subseteq \cup_i \mathfrak{a}_i = cA \subseteq \mathfrak{a}_n$ prueban que $\mathfrak{a}_n = \mathfrak{a}_{n+j}$ para todo $j > 0$.

Teorema de Descomposición: *Todo elemento propio $a \in A$ descompone en producto de factores irreducibles: $a = p_1 \cdots p_n$. Además, la descomposición es única salvo el orden y factores invertibles.*

Demostración: Si a es irreducible no hay nada que decir. En caso contrario descompone en producto de dos factores propios $a = q_1 q_2$. Si tales factores son irreducibles acabamos, en caso contrario los descomponemos a su vez: $a = (q_{11}q_{12})(q_{21}q_{22})$. Y así sucesivamente. El proceso termina porque en caso contrario tendríamos una cadena infinita de ideales $aA \subset q_i A \subset q_{ij} A \subset q_{ijk} A \subset \cdots$ en contradicción con la proposición anterior.

Veamos ahora la unicidad. Sean $a = p_1 \cdots p_n = q_1 \cdots q_m$ dos descomposiciones. Por el lema de Euclides, q_1 divide algún factor p_i, luego coincide con él (salvo un factor invertible) por ser p_i irreducible. Pongamos $q_1 = p_1$ (salvo invertibles). Simplificando la identidad original tenemos $p_2 \cdots p_n = q_2 \cdots q_m$. Razonando con q_2 como hicimos antes con q_1 llegamos a que q_2 coincide con algún p_i. Reiterando el argumento obtendremos que las dos descomposiciones son iguales (salvo el orden y factores invertibles).

D.1 Teoremas de Descomposición

Denotaremos Σ el cuerpo de fracciones de A; es decir, Σ es la localización de A por el sistema multiplicativo $S = A - \{0\}$. Luego los elementos de Σ son las fracciones a/b de elementos de A (con $b \neq 0$) módulo la relación usual de equivalencia de fracciones.

Definición: Se llama **rango** de un A-módulo M a la dimensión de $S^{-1}M$ como espacio vectorial sobre Σ. Nótese que para un A-módulo libre $L = A \oplus \overset{r}{\ldots} \oplus A$ el rango es justamente el número r de sumandos isomorfos a A.

Proposición D.1.1 *Todo submódulo M de un A-módulo libre L de rango finito es también libre de rango finito.*

Demostración: Procederemos por inducción sobre el rango r de L.

Si $r = 1$, entonces $L \simeq A$ y en consecuencia M es isomorfo a un ideal aA de A. Como $aA = 0$ ó $aA \simeq A$ se concluye.

Si $r > 1$, descomponemos L en suma directa de dos libres de rango menor que r, digamos $L = L' \oplus L''$. Llamando $\pi\colon L \to L''$ a la proyección natural, tenemos las sucesiones exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L' & \longrightarrow & L & \xrightarrow{\pi} & L'' & \longrightarrow & 0 \\ & & \cup & & \cup & & \cup & & \\ 0 & \longrightarrow & M \cap L' & \longrightarrow & M & \xrightarrow{\pi} & \pi(M) & \longrightarrow & 0 \end{array}$$

Por hipótesis de inducción, $M \cap L'$ y $\pi(M)$ son libres de rango finito. Además, por ser $\pi(M)$ libre, la segunda sucesión exacta rompe, luego M es suma directa de dos libres de rango finito y se concluye.

Corolario D.1.2 *Todo submódulo M' de un A-módulo finito generado M también es finito generado.*

Demostración: Por ser M finito generado, existe un epimorfismo $\pi\colon L \to M$ siendo L libre de rango finito. Por la proposición anterior, el submódulo $L' = \pi^{-1}(M')$ es libre de rango finito; en particular L' es finito generado. Como M' es un cociente de L' (es decir, $\pi\colon L' \to M'$ es epiyectivo) se concluye que M' también es finito generado.

Definición: Un elemento m de un A-módulo M se dice de **torsión** si existe un elemento no nulo $a \in A$ tal que $am = 0$; es decir, cuando el morfismo $A \to \overset{\cdot m}{} M$ no es inyectivo. Tal condición equivale a que la localización $m/1$ sea nula, al localizar por el sistema multiplicativo $S = A - \{0\}$.

El conjunto $T(M)$ de los elementos de torsión de M es un submódulo, llamado **submódulo de torsión**, pues coincide con el núcleo del morfismo natural de localización $M \to S^{-1}M = M \otimes_A \Sigma$.

Diremos que un A-módulo M es *de torsión* si $M = T(M)$. Diremos que M **carece de torsión** si $T(M) = 0$.

Las siguientes propiedades son elementales:

1. $T(M \oplus N) = T(M) \oplus T(N)$
2. $M/T(M)$ carece de torsión.
3. Todo A-módulo libre L carece de torsión: $T(L) = 0$.
4. M es de torsión precisamente cuando $M_\Sigma = 0$.

Proposición D.1.3 *Todo A-módulo M finito generado y sin torsión es libre.*

Demostración: Bastará probar que M se inyecta en un A-módulo libre de rango finito. Como M carece de torsión, tenemos una inyección $M \to S^{-1}M$. Si $m_1, \ldots, m_s$ es un sistema de generadores de M, entonces $m_1/1, \ldots, m_s/1$ es un sistema de generadores de $S^{-1}M$ como espacio vectorial sobre Σ. De dicho sistema de generadores podemos extraer una base, digamos $m_1/1, \ldots, m_r/1$. Podemos escribir entonces:

$$\frac{m_i}{1} = \sum_{j=1}^{r} \frac{a_{ij}}{b_{ij}} \frac{m_j}{1} \qquad \text{con} \;\; a_{ij}, b_{ij} \in A$$

y reduciendo a común denominador podemos suponer que todos los b_{ij} son iguales, digamos $b_{ij} = b$, así que

$$\frac{m_i}{1} = \sum_{j=1}^{r} \frac{a_{ij}}{b} \frac{m_j}{1}$$

Se concluye entonces que los generadores de M se inyectan en el A-módulo libre $L = A(m_1/b) \oplus \ldots \oplus A(m_r/b)$, luego $M \subseteq L$.

Primer Teorema de Descomposición: *Todo A-módulo finito generado descompone de modo único (salvo isomorfismos) en suma directa de un A-módulo libre y un A-módulo de torsión. En concreto, si r es el rango de M, se verifica*

$$M \simeq (A \oplus \overset{r}{\ldots} \oplus A) \oplus T(M)$$

Demostración: Consideremos la sucesión exacta

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0$$

Por la proposición anterior $M/T(M)$ es libre, así que esta sucesión exacta rompe y obtenemos la descomposición buscada:

$$M \simeq (M/T(M)) \oplus T(M)$$

Veamos ahora la unicidad de la descomposición: Sea $M \simeq L \oplus T$ donde L es libre y T es de torsión. Localizando por S resulta $S^{-1}M \simeq S^{-1}L$, luego M y L tienen el mismo rango; es decir, $L \simeq A \oplus \overset{r}{\ldots} \oplus A$ donde r es el rango de M. Finalmente, tomando torsión en la descomposición $M \simeq L \oplus T$ resulta

$$T(M) \simeq T(L) \oplus T(T) = 0 \oplus T = T\,.$$

Definición: Sea M un A-módulo. Diremos que $\mathfrak{a} = \{a \in A\colon\ aM = 0\}$ es el **ideal anulador** de M, y el generador de $\mathfrak{a}$ se llamará **anulador** de M.

Por definición $\mathfrak{a}M = 0$, así que el A-módulo M admite una estructura natural de $A/\mathfrak{a}$-módulo: $[\,a\,] \cdot m := am$.

Como el generador de un ideal es único salvo un factor invertible, resulta que el anulador de un módulo está bien definido salvo un factor invertible.

Es claro que el ideal anulador de $A/\mathfrak{a}$ es $\mathfrak{a}$.

La siguiente propiedad será utilizada más adelante: El anulador de $M_1 \oplus M_2$ es el mínimo común múltiplo de los anuladores de M_1 y M_2:

$$\mathrm{Ann}(M_1 \oplus M_2) = \mathrm{Ann}(M_1) \cap \mathrm{Ann}(M_2)$$

Lema D.1.4 *Sea M un A-módulo de anulador $a = pq$, siendo p y q primos entre sí. Entonces M descompone de modo único en suma directa de un submódulo de anulador p y otro submódulo de anulador q. En concreto se verifica*

$$M = \ker p \oplus \ker q$$

Demostración: Veamos primero la existencia de la descomposición. De acuerdo con la Identidad de Bézout existen $\lambda, \mu \in A$ tales que $1 = \lambda p + \mu q$. Luego para cada $m \in M$ se cumple

$$m = 1 \cdot m = \lambda pm + \mu qm$$

donde $\lambda pm \in \ker q$ porque $q(\lambda pm) = \lambda am = 0$, y análogamente $\mu qm \in \ker p$. Por consiguiente $M = \ker p + \ker q$.

Veamos ahora que $\ker p \cap \ker q = 0$. Si $m \in \ker p \cap \ker q$ entonces

$$m = 1 \cdot m = \lambda pm + \mu qm = 0 + 0 = 0$$

De todo lo anterior se deduce que $M = \ker p \oplus \ker q$.

Determinemos ahora los anuladores de $\ker p$ y $\ker q$. Denotemos por p' y q' los respectivos anuladores. Como p anula a $\ker p$ se cumple $p = \alpha p'$ (y análogamente $q = \beta q'$). Por otra parte $p'q'$ anula a $M = \ker p \oplus \ker q$, así que

$$p'q' = \gamma a = \gamma pq = \gamma\alpha\beta p'q'$$

y α, β son invertibles. Luego p', q' coinciden con p, q (salvo factores invertibles).

En cuanto a la unicidad de la descomposición, sea $M = M_p \oplus M_q$ donde M_p es un submódulo de M de anulador p y M_q es un submódulo de anulador q. Entonces $M_p \subseteq \ker p$ y $M_p \subseteq \ker p$, y ninguna de estas inclusiones puede ser estricta porque entonces también sería estricta la inclusión

$$M = M_p \oplus M_q \subset \ker p \oplus \ker q = M$$

lo que es absurdo.

Segundo Teorema de Descomposición: *Sea $a = p_1^{n_1} \cdots p_s^{n_s}$ la descomposición en factores irreducibles del anulador de un A-módulo M. Entonces M descompone de modo único en suma directa de submódulos M_i de anuladores respectivos $p_i^{n_i}$. En concreto se cumple*

$$M = \ker p_1^{n_1} \oplus \ldots \oplus \ker p_s^{n_s}$$

Demostración: Basta aplicar el lema anterior sucesivamente:

$$M = \ker p_1^{n_1} \oplus \ker (p_2^{n_2} \cdots p_s^{n_s}) = \cdots = \ker p_1^{n_1} \oplus \ldots \oplus \ker p_s^{n_s} \ .$$

q.e.d.

A partir de ahora p será un elemento *irreducible* de A.

Lema D.1.5 *Los ideales de A/p^nA son de la forma $(\bar{p}^{\,m})$ con $0 \leq m \leq n$.*

Demostración: Sea $\pi\colon A \to A/p^nA$ el morfismo de paso al cociente. Si $\bar{\mathfrak{a}}$ es un ideal de A/p^nA, entonces $\mathfrak{a} = \pi^{-1}(\bar{\mathfrak{a}})$ es un ideal de A que contiene a p^n (porque $\pi(p^n) = 0$). Por lo tanto, el generador de $\mathfrak{a}$ debe ser un divisor de p^n, luego $\mathfrak{a} = p^mA$ para algún $0 \leq m \leq n$. En conclusión, $\bar{\mathfrak{a}} = \pi(\mathfrak{a}) = \pi(p^mA) = (\bar{p}^{\,m})$.

Lema D.1.6 *Se cumple que A/p^nA es un (A/p^nA)-módulo inyectivo.*

Demostración: Usemos el criterio del ideal. Sea $f\colon \bar{\mathfrak{a}} = (\bar{p}^{\,m}) \to A/p^nA$ un morfismo de (A/p^nA)-módulos. El generador $\bar{p}^{\,m}$ de $\bar{\mathfrak{a}}$ está anulado por $\bar{p}^{\,n-m}$, así que lo mismo ocurrirá con su imagen $f(\bar{p}^{\,m})$. Luego $f(\bar{p}^{\,m}) = \bar{a}\bar{p}^{\,m}$ para algún $\bar{a} \in A/p^nA$. Es claro que la homotecia $\bar{f}\colon A/p^nA \to A/p^nA$ de razón $\bar{a}$ extiende a f, esto es $\bar{f}(\bar{b}) = \bar{a}\bar{b}$.

Definición: Un A-módulo M se dice **monógeno** si esta generado por un elemento. Tales módulos son de la forma $M \simeq A/aA$ siendo a el anulador de M. En efecto, sea m un generador de M y consideremos el morfismo $\pi\colon A \to M$ definido por $\pi(b) = bm$. Es claro que π es epiyectivo y que su núcleo es el ideal anulador de M, con lo que se concluye.

Tercer Teorema de Descomposición: *Sea M un A-módulo finito generado de anulador p^n. Entonces M descompone de modo único (salvo isomorfismos) en suma directa de monógenos*

$$M \simeq (A/p^{n_1}A) \oplus \ldots \oplus (A/p^{n_s}A)$$

con $n = n_1 \geq \cdots \geq n_s$.

Demostración: Consideremos un sistema minimal de generadores de M y sea m un elemento de tal sistema de anulador p^n (¡existe!). En la sucesión exacta

$$0 \longrightarrow Am = A/p^nA \longrightarrow M \longrightarrow M/Am \longrightarrow 0$$

los términos están anulados por p^n, así que pueden ser considerados como (A/p^nA)-módulos. Por el lema anterior $Am = A/p^nA$ es un (A/p^nA)-módulo inyectivo, luego la sucesión exacta rompe y resulta

$$M \simeq A/p^nA \oplus M/Am$$

Procediendo por inducción sobre el mínimo número de generadores, podemos suponer que el teorema es cierto para M/Am y se obtiene una descomposición

$$M \simeq (A/p^{n_1}A) \oplus \ldots \oplus (A/p^{n_s}A)$$

Veamos ahora la unicidad de la descomposición. Sea $k := A/pA$ y observemos que $(p^iA/p^jA) \otimes_A k \simeq k$ para todo $0 \leq i < j$. Si denotemos por ν_j el número de sumandos iguales a A/p^jA que aparezcan en una descomposición de M, tenemos

$$\begin{aligned}
&\dim_k(M \otimes k) = \nu_1 + \ldots + \nu_n \\
&\dim_k((pM) \otimes_A k) = \nu_2 + \ldots + \nu_n \\
&\qquad \ldots\ldots\ldots\ldots\ldots \\
&\dim_k((p^{n-1}M) \otimes_A k) = \nu_n
\end{aligned}$$

Estas igualdades permiten despejar las ν_j a partir de las dimensiones de los espacios vectoriales $(p^iM) \otimes_A k$; luego tales números no dependen de la particular descomposición de M elegida.

Definición: Según el primer teorema de descomposición, todo A-módulo M finito generado descompone en suma directa de un módulo libre y otro de torsión. Aplicando a la parte de torsión el segundo y tercer teoremas de descomposición, resulta que todo A-módulo M finito generado descompone de modo único (salvo isomorfismos) en la forma

$$M \simeq (A \oplus \overset{r}{\ldots} \oplus A) \oplus \Big(\bigoplus_{i,j} A/p_i^{n_{ij}}A \Big)$$

donde los p_i son elementos irreducibles de A y r es el rango del módulo M. Además consideramos los exponentes ordenados de mayor a menor: $n_{i1} \geq n_{i2} \geq \cdots$ para cada índice i. A las potencias $p_i^{n_{ij}}$ se les llama **divisores elementales** del módulo M. Nótese que están bien definidos salvo factores invertibles.

Como consecuencia directa de la descomposición obtenida para los módulos finito generados resulta el siguiente

Teorema de Clasificación (1^a versión): *Dos A-módulos finito generados son isomorfos si y sólo si poseen el mismo rango y los mismos divisores elementales.*

D.2 Factores Invariantes

Teorema Chino del Resto: *Sea $a = p_1^{n_1} \cdots p_s^{n_s}$ la descomposición en factores irreducibles de un elemento $a \in A$. Existe un isomorfismo de A-módulos*

$$A/aA = (A/p^{n_1}A) \oplus \ldots \oplus (A/p^{n_s}A)$$

Demostración: Por el segundo teorema de descomposición, aplicado a A/aA, se tiene

$$A/aA = \ker p_1^{n_1} \oplus \ldots \oplus \ker p_s^{n_s}$$

Ahora bien, cada sumando $\ker p_i^{n_i}$ es un cociente de A/aA y por lo tanto es monógeno. Como el anulador de $\ker p_i^{n_i}$ es $p_i^{n_i}$ se concluye que $\ker p_i^{n_i} = A/p_i^{n_i}A$.

Proposición D.2.1 *Dado un A-módulo M finito generado, existe una única sucesión creciente de ideales $\phi_1 A \subseteq \phi_2 A \subseteq \ldots \subseteq \phi_m A$ tal que*

$$M \simeq A/\phi_1 A \oplus \ldots \oplus A/\phi_m A \ .$$

Demostración: Sabemos que

$$M \simeq (A \oplus \overset{r}{\ldots} \oplus A) \oplus \Big(\bigoplus_{i,j} A/p_i^{n_{ij}} A \Big)$$

siendo los $p_i^{n_{ij}}$ los divisores elementales de M y r el rango. Definamos

$$\phi_1 = \cdots = \phi_r = 0 \ , \quad \phi_{r+j} = p_1^{n_{1j}} \cdots p_s^{n_{sj}}$$

Agrupando sumandos en la descomposición de M por medio del teorema chino del resto se obtiene directamente que

$$M \simeq A/\phi_1 A \oplus \ldots \oplus A/\phi_m A$$

Para la unicidad se razona a la inversa descomponiendo cada sumando de la igualdad de arriba por medio del teorema chino del resto.

Definición: A los elementos $\phi_1, \cdots, \phi_m$ de la proposición anterior (cada uno múltiplo del siguiente y bien definidos salvo factores invertibles de A) se les llama **factores invariantes** del módulo M.

Nótese que ϕ_1 es el anulador del módulo, y que la sucesión de factores invariantes puede considerarse infinita sin más que tomar $1 = \phi_{m+1} = \phi_{m+2} = \cdots$. En la demostración de la proposición anterior hemos definido los factores invariantes a partir del rango y de los divisores elementales. Recíprocamente, es evidente que los factores invariantes determinan el rango y los divisores elementales del módulo. Luego podemos reenunciar el teorema de clasificación de la siguiente manera:

Teorema de Clasificación (2^a versión): *Dos A-módulos finito generados son isomorfos si y sólo si poseen los mismos factores invariantes.*

Cálculo de los Factores Invariantes

Consideremos un A-módulo finito generado M y una presentación de M con una sucesión exacta

$$0 \longrightarrow L'_n \xrightarrow{\psi} L_m \longrightarrow M \longrightarrow 0$$

donde L'_n y L_m son A-módulos libres (los subíndices indican los rangos). Fijadas sendas bases $(e'_1, \ldots, e'_n)$ y $(e_1, \ldots, e_m)$ de L'_n y L_m, escribimos $\psi(e'_j) = \sum_i a_{ij} e_i$; así que (a_{ij}) es la matriz de ψ. Definimos entonces los siguientes ideales:

Definición: Se llama i-ésimo **ideal de Fitting** (1906-1938) de M al ideal $F_i(M)$ generado por los menores de orden $m-i$ de la matriz de ψ (entendiendo que $F_i = 0$ cuando $m - i > n$, y que $F_i = A$ cuando $m - i < 1$).

Veamos que los ideales de Fitting de un módulo no dependen de las bases elegidas: Consideremos otra base $(\bar{e}_1, \ldots, \bar{e}_n)$ de L'_n y escribamos $\psi(\bar{e}_j) = \sum_i \bar{a}_{ij} e_i$, así que la nueva matriz de ψ es $(\bar{a}_{ij})$. Denotemos $F_i(M)$ y $\bar{F}_i(M)$ a los respectivos ideales i-ésimos de Fitting de las matrices (a_{ij}) y $(\bar{a}_{ij})$. Cada $\bar{e}_j$ es combinación lineal de la antigua base $(e'_1, \ldots, e'_n)$ y, por lo tanto, cada columna de $(\bar{a}_{ij})$ es combinación lineal de las columnas de (a_{ij}). En consecuencia, los menores de orden $m - i$ de $(\bar{a}_{ij})$ son combinación lineal de los menores de (a_{ij}), es decir, $\bar{F}_i(M) \subseteq F_i(M)$. Por simetría también se cumple $F_i(M) \subseteq \bar{F}_i(M)$; luego en conclusión $F_i(M) = \bar{F}_i(M)$. Si la que cambiamos es la base de L_m se razona de modo similar (por filas en vez de por columnas).

Denotemos c_i al generador del ideal $F_i(M)$, es decir, c_i es el máximo común divisor de los menores de orden $m - i$ de la matriz de ψ (entendiendo que $c_i = 0$ cuando $m - i > n$, y $c_i = 1$ cuando $m - i < 1$).

Proposición D.2.2 *Para todo A-módulo finito generado M se verifica*

$$c_i = \phi_{i+1} \cdots \phi_m$$
$$\phi_i = \begin{cases} c_{i-1}/c_i & \text{cuando } c_i \neq 0 \\ 0 & \text{cuando } c_i = 0 \end{cases}$$

Demostración: Dos elementos de A son iguales si al localizar en cada punto cerrado del espectro son iguales. Por lo tanto podemos suponer que A es un anillo local. En tal caso A tiene un único ideal maximal y en consecuencia sólo existe un elemento irreducible (salvo invertibles), que denotaremos p.

Los factores invariantes se escribirán en la forma

$$\phi_1 = \ldots = \phi_r = 0 \ , \ \phi_{r+1} = p^{n_1}, \ldots, \phi_{r+s} = p^{n_s}$$

con $n_1 \geq \ldots \geq n_s$. Por lo tanto

$$M = A \oplus \overset{r}{\ldots} \oplus A \oplus A/p^{n_1}A \oplus \ldots \oplus A/p^{n_s}A$$

Tomemos un sistema mínimo de generadores $\{m_1, \ldots, m_{r+s}\}$ de M (un generador en cada sumando), y consideremos también la presentación dada:

$$0 \longrightarrow L'_n \xrightarrow{\psi} L_m \xrightarrow{\pi} M \longrightarrow 0$$

Como el morfismo natural $L_m/pL_m \to M/pM$ es epiyectivo, el lema de Nakayama nos permite elegir una base $(e_1, \ldots, e_m)$ de L_n tal que $\pi(e_i) = m_i$, $1 \leq i \leq r+s$. El resto de los elementos de la base verificarán relaciones, digamos

$$\pi(e_{r+s+j}) = \textstyle\sum_i a_{ij} m_i \ .$$

Cambiando los elementos e_{r+s+j} por $e_{r+s+j} - \sum_i a_{ij} e_i$ obtenemos una base $e_1, \ldots, e_m$ de L_m que verifica $\pi(e_i) = m_i$ para $i \leq r+s$, y $\pi(e_{r+s+j}) = 0$ para $j > 0$. Es claro entonces que los elementos $e'_i = p^{n_i} e_{r+i}$, $e'_{s+j} = e_{r+s+j}$ forman una base de $\ker \pi = L'_n$. La correspondiente matriz de ψ es

$$\begin{pmatrix} 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ & \ldots & \ldots & \ldots & \ldots & \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ p^{n_1} & & & & & \\ & \ddots & & & & \\ & & p^{n_s} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

Recordando que $n_1 \geq \ldots \geq n_s$, es fácil comprobar que el máximo común divisor c_i de los menores de orden $m-i$ de esta matriz es nulo cuando $i < r$ (luego coincide con $\phi_{i+1} \cdots \phi_n$) y, cuando $i \geq r$, vale

$$c_{r+j} = p^{n_{j+1}} \cdots p^{n_s} \cdot 1 \cdots 1 = \phi_{r+j+1} \cdots \phi_n$$

Corolario D.2.3 *El mínimo número de generadores de M coincide con el número de factores invariantes.*

Demostración: La proposición anterior muestra que el número de generadores m acota al número de factores invariantes. Por otra parte, si $\phi_1, \ldots, \phi_m$ son los factores invariantes, entonces $M \simeq A/\phi_1 A \oplus \ldots \oplus A/\phi_m A$ claramente admite un sistema de m generadores.

Observación: De la proposición anterior se deduce que los ideales $F_i(M)$ no dependen de la presentación particular elegida. No es difícil probar que tal afirmación también es válida para presentaciones $L'_n \to L_m \to M \to 0$ con $L'_n \to L_m$ no necesariamente inyectivo.

D.3 Clasificación de Endomorfismos

Sea E un espacio vectorial de dimensión finita sobre un cuerpo k.

Definición: Se dice que dos endomorfismos T, T' de E son **equivalentes** o **semejantes** si existe un automorfismo lineal τ de E tal que $T' = \tau \circ T \circ \tau^{-1}$. Esta igualdad significa la conmutatividad del cuadrado

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ \downarrow \tau & & \downarrow \tau \\ E & \xrightarrow{T'} & E \end{array}$$

Cada endomorfismo T induce una estructura de $k[x]$-módulo en E del siguiente modo

$$p(x) \cdot e = p(T)(e)$$

y en particular $x \cdot e = T(e)$. Este $k[x]$-módulo se denotará E_T.

Proposición D.3.1 *Dos endomorfismos T, T' son equivalentes si y sólo si inducen estructuras de $k[x]$-módulos isomorfas sobre E.*

Demostración: Si T y T' son equivalentes, existe un automorfismo lineal τ tal que $\tau \circ T = T' \circ \tau$. Veamos que $\tau \colon E_T \to E_{T'}$ es un isomorfismo de $k[x]$-módulos.

Como τ es un isomorfismo k-lineal, bastará ver que conmuta con la multiplicación por x:

$$\tau(x \cdot e) = \tau\left(T(e)\right) = T'\left(\tau(e)\right) = x \cdot \tau(e)$$

Para el recíproco se razona de modo similar. q.e.d.

Según la proposición anterior la clasificación de endomorfismos se reduce a la de $k[x]$-módulos. Llamemos factores invariantes de un endomorfismo T de un k-espacio vectorial de dimensión finita E a los factores invariantes del $k[x]$-módulo E_T, que es finito generado. El teorema de clasificación de $k[x]$-módulos implica directamente el siguiente

Teorema de Clasificación: *Dos endomorfismos de un k-espacio vectorial de dimensión finita E son equivalentes si y sólo si poseen los mismos factores invariantes.*

Cálculo de los Factores Invariantes

Sea E un k-espacio vectorial de dimensión n. Consideremos un endomorfismo T y la correspondiente estructura de $k[x]$-módulo sobre E. Sea (λ_{ij}) la matriz de T en una base $(e_1, \ldots, e_n)$ de E. Vamos a determinar los factores invariantes de T a partir de su matriz.

Consideremos la sucesión exacta

$$0 \longrightarrow k[x,y] \xrightarrow{(x-y)\cdot} k[x,y] \longrightarrow k[x] \longrightarrow 0$$

Mediante el isomorfismo $k[x] \otimes_k k[x] = k[x,y]$, $x \otimes 1 \mapsto x$, $1 \otimes x \mapsto y$, la sucesión anterior se expresa en la forma

$$0 \longrightarrow k[x] \otimes_k k[x] \xrightarrow{(x\otimes 1 - 1 \otimes x)\cdot} k[x] \otimes_k k[x] \longrightarrow k[x] \longrightarrow 0$$

Consideremos $k[x] \otimes_k k[x]$ como $k[x]$-módulo por el segundo factor. Entonces la sucesión anterior es una sucesión exacta de $k[x]$-módulos que rompe porque el último término es libre. Aplicando ahora $(-) \otimes_{k[x]} E_T$ resulta la sucesión exacta

$$0 \longrightarrow k[x] \otimes_k E \xrightarrow{(x\otimes 1 - 1 \otimes T)\cdot} k[x] \otimes_k E \longrightarrow E_T \longrightarrow 0$$

Considerando $k[x] \otimes_k E$ como $k[x]$-módulo por el primer factor resulta ser libre de base $(1 \otimes e_1, \ldots, 1 \otimes e_n)$. Por lo tanto, la sucesión anterior es una presentación de E_T como $k[x]$-módulo. La matriz del morfismo $(x \otimes 1 - 1 \otimes T)\cdot$ es $x\mathrm{Id} - (\lambda_{ij})$. Luego

Teorema D.3.2 *Sea (λ_{ij}) la matriz $n \times n$ de un endomorfismo T. Sea $c_i(x)$ el máximo común divisor de los menores de orden $n-i$ de la matriz $x\mathrm{Id} - (\lambda_{ij})$. Se verifica*

$$c_i(x) = \phi_{i+1}(x) \cdots \phi_n(x)$$
$$\phi_i(x) = c_{i-1}(x)/c_i(x)$$

siendo $\phi_1(x), \ldots, \phi_n(x)$ los factores invariantes de T.

Observaciones:

1. El polinomio $c_0(x) = det\left(x\mathrm{Id} - (\lambda_{ij})\right)$ se llama **polinomio característico** de T. Según el teorema anterior, el polinomio característico es igual al producto de los factores invariantes.
2. Un caso particular es el **Teorema de Hamilton-Cayley** (1805-1865 y 1821-1895)**:** *El polinomio característico de un endomorfismo es múltiplo del polinomio anulador, y ambos tienen los mismos factores irreducibles.*
3. Si el polinomio característico de un endomorfismo no tiene factores irreducibles repetidos, entonces coincide con el polinomio anulador, y los restantes factores invariantes son la unidad: $\phi_2 = \ldots = 1$.

D.4 Matrices de Jordan

Cuerpo Algebraicamente Cerrado

Lema D.4.1 $\{\overline{1}, \overline{(x-\lambda)}, \ldots, \overline{(x-\lambda)}^{\,n-1}\}$ *es una base de* $k[x]/\big((x-\lambda)^n\big)$.

Demostración: Las clases $\overline{1}, \bar{y}, \ldots, \bar{y}^{\,n-1}$ forman una base de $k[y]/(y^n)$. Haciendo el cambio $y = x - \lambda$ concluimos.

Sea ahora T un endomorfismo de un k-espacio vectorial E. Supongamos que E_T es monógeno, es decir, se cumple:

$$E_T \simeq k[x]/\big((x-\lambda)^n\big)$$

Tomemos entonces la base $\{e_j = (x-\lambda)^{j-1}\}$ con $0 \leq j \leq n-1$. Se tiene

$$T(e_j) = x \cdot (x-\lambda)^{j-1} = (x-\lambda)(x-\lambda)^{j-1} + \lambda(x-\lambda)^{j-1} = e_{j+1} + \lambda e_j$$

Por lo tanto, la matriz de T vale

$$\begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

En el caso general, la descomposición de E será

$$E_T \simeq \bigoplus_{i,j} k[x]/\big((x-\lambda_i)^{n_{ij}}\big)$$

siendo $(x-\lambda_i)^{n_{ij}}$ los divisores elementales del endomorfismo T. Tomando una base en cada sumando $k[x]/\big((x-\lambda_i)^{n_{ij}}$, elegida como en el caso monógeno, obtendremos una base de E en la que la matriz de T es de la **forma de Jordan** (1838-1922)

$$\begin{pmatrix} (B_{11}) & & & \\ & \ddots & & \\ & & (B_{ij}) & \\ & & & \ddots \end{pmatrix}$$

siendo (B_{ij}) la siguiente matriz $n_{ij} \times n_{ij}$

$$(B_{ij}) = \begin{pmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

El Cuerpo $\mathbb{R}$

Lema D.4.2 *Sea E un espacio vectorial complejo de base $(e_1, \ldots, e_n)$. Entonces $(e_1, ie_1, \ldots, e_n, ie_n)$ es una base de E como espacio vectorial real.*

Demostración: Teniendo en cuenta que $\mathbb{C} = \mathbb{R}1 \oplus \mathbb{R}i$, resulta

$$E = \mathbb{C}e_1 \oplus \ldots \oplus \mathbb{C}e_n = (\mathbb{R}e_1 \oplus \mathbb{R}ie_1) \oplus \ldots \oplus (\mathbb{R}e_n \oplus \mathbb{R}ie_n)$$

lo que permite concluir. q.e.d.

Consideremos un número complejo $\alpha = a + bi$ y su conjugado $\bar{\alpha} = a - bi$, donde se supone $b \neq 0$. Observemos que $(x-\alpha)(x-\bar{\alpha}) = x^2 - 2ax + (a^2+b^2)$ es un polinomio irreducible con coeficientes reales.

Lema D.4.3 *Existe un isomorfismo de $\mathbb{R}[x]$-módulos*

$$\mathbb{R}[x]/\big((x-\alpha)^n(x-\bar{\alpha})^n\big) = \mathbb{C}[x]/\big((x-\alpha)^n\big)$$

Demostración: Ambos módulos tienen dimensión $2n$ sobre $\mathbb{R}$. Sea $< \bar{1} >$ el $\mathbb{R}[x]$-submódulo de $\mathbb{C}[x]/\big((x-\alpha)^n\big)$ generado por la clase $\bar{1}$. Determinemos el anulador de esta clase: Por una parte, es claro que $(x-\alpha)^n(x-\bar{\alpha})^n$ anula a $\bar{1}$; por otra parte, el anulador deberá ser múltiplo de $(x-\alpha)^n$ y, dado que todo polinomio con

coeficientes reales que tiene una raíz compleja tiene también la conjugada (con igual multiplicidad) se concluye que el polinomio anulador es $(x-\alpha)^n(x-\bar{\alpha})^n$.

Se tiene entonces una inclusión

$$\mathbb{R}[x]/\big((x-\alpha)^n(x-\bar{\alpha})^n\big) = <\bar{1}> \subseteq \mathbb{C}[x]/\big((x-\alpha)^n\big)$$

y como ambos espacios son de la misma dimensión sobre $\mathbb{R}$ se concluye que la anterior inclusión es una igualdad. q.e.d.

Sea ahora T un endomorfismo de un espacio vectorial real E.

Supongamos primero que E_T es monógeno, de la forma

$$E_T \simeq \mathbb{R}[x]/\big((x-\alpha)^n(x-\bar{\alpha})^n\big) = \mathbb{C}[x]/\big((x-\alpha)^n\big)$$

Tomemos la base $\{e_j = (x-\alpha)^{j-1},\ e'_j = i(x-\alpha)^{j-1}\}$. Calculemos:

$$\begin{aligned}
T(e_j) &= x\cdot(x-\alpha)^{j-1} = (x-\alpha)^j + \alpha(x-\alpha)^{j-1} = \\
&= (x-\alpha)^j + a(x-\alpha)^{j-1} + bi(x-\alpha)^{j-1} = e_{j+1} + ae_j + be'_j \\
T(e'_j) &= x\cdot i(x-\alpha)^{j-1} = i(x-\alpha)^j + i\alpha(x-\alpha)^{j-1} = \\
&= i(x-\alpha)^j + ai(x-\alpha)^{j-1} - b(x-\alpha)^{j-1} = e'_{j+1} + ae'_j - be_j
\end{aligned}$$

luego la matriz de T vale

$$\begin{pmatrix}
\begin{pmatrix} a & -b \\ b & a \end{pmatrix} & & & \\
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & & \\
& \ddots & \ddots & \\
& & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} a & -b \\ b & a \end{pmatrix}
\end{pmatrix}$$

En el caso general, la descomposición de E en monógenos será de la forma

$$E_T \simeq \bigoplus_{i,j} \mathbb{R}[x]/\big(p_i(x)^{n_{ij}}\big)$$

donde los polinomios $p_i(x)$ son irreducibles y por lo tanto son de la forma $p_i(x) = x-\lambda_i$ ó bien $p_i(x) = (x-\alpha_i)(x-\bar{\alpha}_i)$ con $\alpha_i = a_i + b_i i$. Tomando como antes una base en cada monógeno $\mathbb{R}[x]/\big(p_i(x)^{n_{ij}}\big)$ obtendremos una base de E en la que la matriz de T es reducida (**matriz de Jordan**):

$$\begin{pmatrix}
(B_{11}) & & & \\
& \ddots & & \\
& & (B_{ij}) & \\
& & & \ddots
\end{pmatrix}$$

donde el valor de la matriz (B_{ij}) depende de $p_i(x)^{n_{ij}}$. Si $p_i(x) = x - \lambda_i$ entonces (B_{ij}) es la siguiente matriz $n_{ij} \times n_{ij}$

$$(B_{ij}) = \begin{pmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

Si $p_i(x) = (x - \alpha_i)(x - \bar{\alpha}_i)$ entonces (B_{ij}) es la siguiente matriz $2n_{ij} \times 2n_{ij}$

$$(B_{ij}) = \begin{pmatrix} \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} & & & \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} & & \\ & \ddots & \ddots & \\ & & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} \end{pmatrix}$$

D.5 Clasificación de Autoproyectividades

Denotaremos $\tilde{T}\colon \mathbb{P}(E) \to \mathbb{P}(E)$ la proyectividad inducida por un automorfismo lineal $T\colon E \to E$.

Definición: Diremos que dos proyectividades $\tilde{T}, \tilde{T}'$ son **equivalentes** si existe alguna proyectividad $\tilde{\tau}$ tal que $\tilde{T}' = \tilde{\tau} \circ \tilde{T} \circ \tilde{\tau}^{-1}$. Esta igualdad significa la conmutatividad del cuadrado

$$\begin{array}{ccc} \mathbb{P}(E) & \xrightarrow{\tilde{T}} & \mathbb{P}(E) \\ \downarrow \tilde{\tau} & & \downarrow \tilde{\tau} \\ \mathbb{P}(E) & \xrightarrow{\tilde{T}'} & \mathbb{P}(E) \end{array}$$

La igualdad $\tilde{T}' = \tilde{\tau} \circ \tilde{T} \circ \tilde{\tau}^{-1}$ significa que los representantes lineales verifican $\lambda T' = \tau \circ T \circ \tau^{-1}$ para cierta constante no nula $\lambda \in k$. Por consiguiente, los endomorfismos T y $\lambda T'$ son equivalentes. La equivalencia de endomorfismos viene determinada por los factores invariantes, así que nos es necesario determinar cómo varían los factores invariantes cuando se multiplica el endomorfismo por una constante.

Lema D.5.1 *Sean $\{\phi_i(x)\}$ los factores invariantes de un endomorfismo T y sean $\{\phi'_i(x)\}$ los factores invariantes de λT (con $\lambda \neq 0$). Se verifica*

$$\phi'_i(x) = \phi_i(x/\lambda)$$

Demostración. Considerando en E la estructura de $k[x]$-módulo inducida por T se cumple

$$E \simeq k[x]/\big(\phi_1(x)\big) \oplus \ldots \oplus k[x]/\big(\phi_n(x)\big)$$

Realizando el cambio de variable $x = y/\lambda$ obtenemos el siguiente isomorfismo de $k[y]$-módulos

$$E \simeq k[y]/\big(\phi_1(y/\lambda)\big) \oplus \ldots \oplus k[y]/\big(\phi_n(y/\lambda)\big)$$

Como $y = \lambda x$, la estructura de $k[y]$-módulo que posee E en el isomorfismo anterior es justamente la correspondiente al endomorfismo λT. El isomorfismo anterior nos dice entonces que los factores invariantes de λT son los polinomios $\{\phi_i(y/\lambda)\}$. q.e.d.

Es fácil comprobar que las raíces de $\phi_i(x/\lambda)$ son las de $\phi_i(x)$ multiplicadas por la constante λ. Por lo tanto, al multiplicar un endomorfismo por una constante sus factores invariantes quedan multiplicados en sus raíces por la constante.

Como consecuencia del último lema y de la clasificación de endomorfismos, obtenemos directamente el siguiente

Teorema de Clasificación: *Dos proyectividades $\tilde{T}$, $\tilde{T}'$ de un espacio proyectivo $\mathbb{P}(E)$ son equivalentes si y sólo si existe una constante no nula $\lambda \in k$ tal que*

$$\phi'_i(x) = \phi_i(x/\lambda)$$

siendo $\{\phi_i(x)\}$, $\{\phi'_i(x)\}$ los respectivos factores invariantes de los representantes lineales T y T'.

D.6 Clasificación de Grupos Abelianos

Todo grupo conmutativo $(G, +)$ tiene una estructura natural de $\mathbb{Z}$-módulo:

$$n \cdot g = g + \overset{n}{\ldots} + g$$
$$(-n) \cdot g = -g - \overset{n}{\ldots} - g$$

donde $g \in G$ y $n \in \mathbb{N}$. Recíprocamente, todo $\mathbb{Z}$-módulo posee por definición una estructura subyacente de grupo abeliano. Además, los morfismos de grupos (abelianos) son justamente los morfismos de $\mathbb{Z}$-módulos. Por lo tanto, la clasificación de grupos abelianos equivale a la clasificación de $\mathbb{Z}$-módulos. Así pues, todo grupo abeliano finito generado G viene determinado (salvo isomorfismos) por sus factores invariantes:

$$G \simeq \mathbb{Z}/\phi_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\phi_m\mathbb{Z}$$

Teorema de Clasificación: *Dos grupos abelianos finito generados son isomorfos si y sólo si poseen los mismos factores invariantes.*

Corolario D.6.1 *Todo grupo abeliano finito generado descompone, y de modo único, en suma directa de grupos cíclicos infinitos y de grupos cíclicos de órdenes potencias de números primos.*

Corolario D.6.2 *Todo grupo abeliano finito G descompone, y de modo único, en suma directa de grupos cíclicos de órdenes potencias de números primos.*

Corolario D.6.3 *Si un número natural d divide al orden de un grupo abeliano finito G, entonces G tiene algún subgrupo de orden d.*

Demostración: $p^{n-i}\mathbb{Z}/p^n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}/p^n\mathbb{Z}$ de orden p^i.

Corolario D.6.4 *Si G es un grupo abeliano finito-generado, las siguientes condiciones son equivalentes:*

1. *G es un grupo finito.*
2. *El rango de G es nulo.*
3. *El primer factor invariante ϕ_1 (i.e. el anulador) de G no es nulo.*

en cuyo caso su orden es el producto de los factores invariantes: $|G| = \phi_1 \dots \phi_m$.

Corolario D.6.5 *Un sistema de ecuaciones diofánticas lineales $AX = B$ admite solución entera precisamente cuando el rango r de la matriz A coincide con el de la matriz ampliada $(A|B)$ y el ideal de Fitting $F_r(A)$ coincide con $F_r(A|B)$.*

Demostración: Consideremos el morfismo $\mathbb{Z}$-lineal $f\colon \mathbb{Z}^n \to \mathbb{Z}^m$, $f(X) = AX$, y su conúcleo $M = \mathbb{Z}^m/\operatorname{Im} f$, de modo que $\operatorname{rg}(M) = m - \operatorname{rg}(A)$. Además, según D.2.2, el orden $\phi_{r+1} \cdots \phi_m$ del subgrupo de torsión de M coincide con $c_r(A)$.

Si el sistema tiene alguna solución entera, entonces $B \in \operatorname{Im} f$ y tenemos que $M = M/\mathbb{Z}B$. Ahora D.2.2 permite concluir que $F_i(A) = F_i(A|B)$ para todo índice i. En particular $F_r(A) = F_r(A|B)$.

Recíprocamente, si el sistema no tiene solución entera, entonces $B \neq 0$ en M. Si B no es de torsión en M, entonces $\operatorname{rg}(M/\mathbb{Z}B) = \operatorname{rg}(M) - 1$ y concluimos que $\operatorname{rg}(A|B) = \operatorname{rg}(A)+1$. Si B es de torsión en M, entonces $\operatorname{rg}(A|B) = \operatorname{rg}(A) = r$; pero el orden del subgrupo de torsión de $M/\mathbb{Z}B$ (que coincide con $c_r(A|B)$ en virtud de D.2.2) es estrictamente menor que el orden $c_r(A)$ del subgrupo de torsión de M. Luego $F_r(A) \neq F_r(A|B)$.

Transformaciones Elementales

Veamos otro método para clasificar un grupo abeliano G (o, más en general, un módulo sobre un anillo euclídeo) a partir de una presentación

$$L' \xrightarrow{f} L \longrightarrow G \longrightarrow 0$$

Elegidas bases $(e_1, \ldots, e_m)$ y $(e'_1, \ldots, e'_n)$ de los grupos libres L y L', el morfismo f vendrá dado por una matriz $A = (a_{ij})$ de m filas y n columnas con coeficientes enteros: $f(e'_j) = \sum_i a_{ij} e_i$. Las siguientes operaciones con las columnas C_j de A, que corresponden a cambios de base en L', y con las filas F_i de A, que corresponden a cambios de base en L, se llaman **transformaciones elementales**:

Transformación Elemental	Cambio de Base
Trasponer C_i y C_j	Trasponer e'_i y e'_j
Trasponer F_i y F_j	Trasponer e_i y e_j
Sustituir C_i por $C_i + \lambda C_j$	Sustituir e'_i por $e'_i + \lambda e'_j$
Sustituir F_i por $F_i + \lambda F_j$	Sustituir e_j por $e_j - \lambda e_i$

donde $i \neq j$ y $\lambda \in \mathbb{Z}$. A veces también es cómodo considerar como transformaciones elementales los cambios de signo de columnas o filas, pues claramente se corresponden con los cambios de signo de los vectores de las bases elegidas.

Mediante transformaciones elementales (i.e., cambios de base en L' y L) podemos conseguir que todos los coeficientes a_{ij} de la matriz de f sean múltiplos de a_{11}, y por tanto anular los restantes coeficientes de la primera fila y columna. Obtenemos así matrices invertibles con coeficientes enteros B y C tales que

$$\bar{A} = C^{-1}AB = \begin{pmatrix} a_1 & & & & 0 & \cdot \\ & a_2 & & & \cdot & \cdot \\ & & \ddots & & \cdot & \cdot \\ & & & a_m & 0 & \cdot \end{pmatrix}$$

es una matriz diagonal donde a_{i+1} es múltiplo de a_i. En particular, los factores invariantes de $L/\mathrm{Im}\, f \simeq G$ coinciden con los coeficientes de la diagonal de $\bar{A}$ (completados con ceros cuando $m > n$); es decir, $\phi_1 = a_m$, $\phi_2 = a_{m-1}, \ldots, \phi_m = a_1$.

Por otra parte, para resolver un sistema de ecuaciones diofánticas lineales $AX = Y$, basta calcular las soluciones $\bar{X}$ del sistema trivial $\bar{A}\bar{X} = \bar{Y}$, donde $\bar{Y} = C^{-1}Y$, pues las soluciones del inicial son $X = B\bar{X}$, y la matriz de cambio de base B se calcula aplicando a la base inicial de L' las transformaciones elementales por columnas que se hayan realizado (i.e. los cambios de base en L').

Ejemplo: Para hallar las soluciones del sistema de ecuaciones diofánticas lineales

$$\left.\begin{aligned} 5x_1 - 2x_2 - 11x_3 &= 2 \\ 3x_1 + 2x_2 - 5x_3 &= -2 \end{aligned}\right\}$$

reducimos la matriz del sistema mediante transformaciones elementales:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \qquad \left(\begin{array}{ccc:c}5&-2&-11&2\\3&2&-5&-2\end{array}\right)$$

$$\begin{pmatrix}1&0&0\\-1&1&0\\0&0&1\end{pmatrix} \qquad \left(\begin{array}{ccc:c}7&-2&-11&2\\1&2&-5&-2\end{array}\right)$$

$$\text{„} \qquad \left(\begin{array}{ccc:c}1&2&-5&-2\\7&-2&-11&2\end{array}\right)$$

$$\text{„} \qquad \left(\begin{array}{ccc:c}1&2&-5&-2\\0&-16&24&16\end{array}\right)$$

$$\begin{pmatrix}1&-2&5\\-1&3&-5\\0&0&1\end{pmatrix} \qquad \left(\begin{array}{ccc:c}1&0&0&-2\\0&-16&24&16\end{array}\right)$$

$$B=\begin{pmatrix}1&3&-4\\1&-2&1\\0&1&-2\end{pmatrix} \qquad \left(\begin{array}{ccc:c}1&0&0&-2\\0&8&0&16\end{array}\right)$$

de modo que el sistema inicial es equivalente al sistema $\bar{A}\bar{X}=\bar{Y}$:

$$\begin{pmatrix}1&0&0\\0&8&0\end{pmatrix}\begin{pmatrix}\bar{x}_1\\\bar{x}_2\\\bar{x}_3\end{pmatrix}=\begin{pmatrix}-2\\16\end{pmatrix}$$

Sus soluciones son $\bar{x}_1=-2$, $\bar{x}_2=2$, $\bar{x}_3=\lambda$, y las del sistema inicial son

$$\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=B\bar{X}=\begin{pmatrix}1&3&-4\\1&-2&1\\0&1&-2\end{pmatrix}\begin{pmatrix}-2\\2\\\lambda\end{pmatrix} \quad , \quad \left\{\begin{array}{l}x_1=4-4\lambda\\x_2=-2+\lambda\\x_3=2-2\lambda\end{array}\right. \quad , \quad \lambda\in\mathbb{Z}$$

Nota: Para estudiar la compatibilidad de un sistema, no es necesario calcular la matriz de cambio de base B. Así, para estudiar la compatibilidad del sistema

$$\left.\begin{array}{r}5x_1-2x_2-11x_3=a\\3x_1+2x_2-5x_3=b\end{array}\right\}$$

realizando transformaciones elementales

$$\left(\begin{array}{ccc|c} 5 & -2 & -11 & a \\ 3 & 2 & -5 & b \end{array}\right) \quad , \quad \cdots\cdots \quad , \quad \left(\begin{array}{ccc|c} 1 & 0 & 0 & b \\ 0 & 8 & 0 & a-7b \end{array}\right)$$

vemos que el sistema dado es equivalente al sistema

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \end{pmatrix} \begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \bar{x}_3 \end{pmatrix} = \begin{pmatrix} b \\ a-7b \end{pmatrix}$$

que sólo es compatible cuando $a-7b$ es múltiplo de 8. El sistema dado es compatible precisamente cuando $a+b$ sea múltiplo de 8.

Ejemplo: Para hallar las matrices de cambio de base B y C tales que $\bar{A} = C^{-1}AB$, efectuamos las transformaciones elementales en las bases de L' y L (según que sean transformaciones de A por columnas o filas). Obtenemos así las coordenadas de la nueva base de L' en la inicial (i.e., la matriz B) y las de la base inicial de L en la nueva base (i.e., la matriz C^{-1}):

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A = \begin{pmatrix} 5 & -2 & -11 \\ 3 & 2 & -5 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 7 & -2 & -11 \\ 1 & 2 & -5 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{"}$$

$$\text{"} \quad \begin{pmatrix} 1 & 2 & -5 \\ 7 & -2 & -11 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\text{"} \quad \begin{pmatrix} 1 & 2 & -5 \\ 0 & -16 & 24 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -2 & 5 \\ -1 & 3 & -5 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -16 & 24 \end{pmatrix} \quad \text{"}$$

$$B = \begin{pmatrix} 1 & 3 & -4 \\ 1 & -2 & 1 \\ 0 & 1 & -2 \end{pmatrix} \quad \bar{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix} = C^{-1}$$

Ejemplo: Sea G el grupo abeliano generado por 3 elementos con las relaciones

$$\left.\begin{aligned} 8a + 10b + 12c = 0 \\ 8a + 4b + 6c = 0 \end{aligned}\right\}$$

i.e., G es el conúcleo del morfismo $f\colon \mathbb{Z}^2 \to \mathbb{Z}^3$, $f(x_1, x_2) = x_1(8, 10, 12) + x_2(8, 4, 6)$. Aplicando transformaciones elementales a la matriz de f:

$$A = \begin{pmatrix} 8 & 8 \\ 10 & 4 \\ 12 & 6 \end{pmatrix} \ , \ \begin{pmatrix} -2 & 4 \\ 10 & 4 \\ 12 & 6 \end{pmatrix} \ , \ \begin{pmatrix} -2 & 0 \\ 10 & 24 \\ 12 & 30 \end{pmatrix} \ , \ \begin{pmatrix} -2 & 0 \\ 0 & 24 \\ 0 & 30 \end{pmatrix} \ , \ \begin{pmatrix} 2 & 0 \\ 0 & 6 \\ 0 & 0 \end{pmatrix} = \bar{A}$$

vemos que $G = \mathbb{Z}^3/\operatorname{Im} f \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus \mathbb{Z}$. Los factores invariantes de G son $\phi_1 = 0$, $\phi_2 = 6$ y $\phi_3 = 2$; es decir, G es un grupo abeliano de rango $r = 1$ y sus divisores elementales son 2, 2, 3. Un método alternativo es calcular el máximo común divisor c_i de los menores de orden $3 - i$ de la matriz A:

$$\begin{aligned} c_0 &= 0 \\ c_1 &= \text{m.c.d.}(-48,\, -48,\, 12) = 12 \\ c_2 &= \text{m.c.d.}(8,\, 10,\, 4,\, 12,\, 6) = 2 \\ c_3 &= c_4 = \ldots = 1 \end{aligned}$$

de modo que $\phi_1 = c_0/c_1 = 0$, $\phi_2 = c_1/c_2 = 6$, $\phi_3 = c_2/c_3 = 2$.

En particular, G es un grupo infinito de rango 1, no es un grupo cíclico (de hecho, no puede ser generado con menos de 3 elementos), su anulador es 0 y su subgrupo de torsión $T(G) \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z})$ tiene 12 elementos.

Apéndice E

Módulos Localmente Libres

Definición: Sea M un A-módulo de tipo finito. Diremos que un sistema finito de generadores de M es **mínimo** si no contiene estrictamente ningún otro sistema de generadores de M.

Sea $\mathcal{O}$ un anillo local, $\mathfrak{m}$ su ideal maximal y $k = \mathcal{O}/\mathfrak{m}$. En virtud del lema de Nakayama, la condición necesaria y suficiente para que una familia $\{m_1, \ldots, m_r\}$ de elementos de un $\mathcal{O}$-módulo de tipo finito M sea un sistema mínimo de generadores es que $m_1 \otimes 1, \ldots, m_r \otimes 1$ formen una base del k-espacio vectorial $M \otimes_{\mathcal{O}} k$; es decir, que el morfismo $\mathcal{O}^r \to M$ definido por $m_1, \ldots, m_r$ induzca un isomorfismo

$$\mathcal{O}^r \otimes_{\mathcal{O}} k = k^r \simeq M \otimes_{\mathcal{O}} k$$

Por tanto, todos los sistemas mínimos de generadores de M tienen el mismo número de elementos y este número común, que coincide con la dimensión del k-espacio vectorial $M \otimes_{\mathcal{O}} k$, lo denotaremos $\mathrm{g}(M)$.

Ejercicio: Si M es un A-módulo de tipo finito, la función $f(x) := \mathrm{g}(M_x)$ es semicontinua sobre $\operatorname{Spec} A$; es decir, $U_n := \{x \in \operatorname{Spec} A\colon\ \mathrm{g}(M_x) < n\}$ es un abierto de $\operatorname{Spec} A$ para todo número natural n.

Lema E.0.6 *Sea M un módulo de tipo finito sobre un anillo local $\mathcal{O}$. Si el morfismo natural $\mathfrak{a} \otimes_A M \to M$ es inyectivo para todo ideal finito-generado $\mathfrak{a}$ de $\mathcal{O}$, entonces M es un $\mathcal{O}$-módulo libre.*

Demostración: Sea $\{m_1, \ldots, m_r\}$ un sistema mínimo de generadores de M. Dada una relación $a_1 m_1 + \ldots + a_r m_r = 0$, consideramos el ideal $\mathfrak{a} = (a_1, \ldots, a_r)$, que es de tipo finito. Por hipótesis el morfismo natural $\mathfrak{a} \otimes_{\mathcal{O}} M \to M$ es inyectivo, así que $a_1 \otimes m_1 + \ldots + a_r \otimes m_r = 0$. Cambiando de base al cuerpo residual k del

único ideal maximal $\mathfrak{m}$ de $\mathcal{O}$, obtenemos la relación $\bar{a}_1 \otimes \bar{m}_1 + \ldots + \bar{a}_r \otimes \bar{m}_r = 0$ en el k-espacio vectorial

$$(\mathfrak{a} \otimes_{\mathcal{O}} M) \otimes_{\mathcal{O}} k = (\mathfrak{a}/\mathfrak{m}\mathfrak{a}) \otimes_k (M/\mathfrak{m}M) = \bigoplus_{i=1}^{r} (\mathfrak{a}/\mathfrak{m}\mathfrak{a}) \otimes_k (k\bar{m}_i)$$

Luego $\bar{a}_1 = \ldots = \bar{a}_r = 0$. Es decir, $\mathfrak{a}/\mathfrak{m}\mathfrak{a} = 0$ y, en virtud del lema de Nakayama, concluimos que $\mathfrak{a} = 0$. Es decir, $a_1 = \ldots = a_r = 0$ y el epimorfismo $\mathcal{O}^r \to M$ definido por $m_1, \ldots, m_r$ es un isomorfismo.

Criterio de Platitud del Ideal: *Sea M un A-módulo de tipo finito. Si el morfismo natural $\mathfrak{a} \otimes_A M \to M$ es inyectivo para todo ideal finito-generado $\mathfrak{a}$ de A, entonces M es un A-módulo plano.*

Demostración: En cada punto $x \in \operatorname{Spec} A$ tenemos que el morfismo natural

$$\mathfrak{a}_x \otimes_{A_x} M_x = (\mathfrak{a} \otimes_A M)_x \longrightarrow M_x$$

es inyectivo. Como cada ideal finito-generado de A_x es la localización de un ideal finito-generado de A, el lema anterior permite concluir que M_x es un A_x-módulo libre y, por tanto, plano. Luego M es un A-módulo plano porque la platitud es una propiedad local.

Teorema E.0.7 *En los módulos de tipo finito sobre un anillo local $\mathcal{O}$, las condiciones de ser libre, proyectivo y plano son equivalentes.*

Demostración: Sólo hay que probar que todo $\mathcal{O}$-módulo de tipo finito plano M es libre. Ahora bien, para cualquier ideal $\mathfrak{a}$ de $\mathcal{O}$ se verifica que el morfismo natural $\mathfrak{a} \otimes_{\mathcal{O}} M \to M$ es inyectivo, porque lo es la inclusión $\mathfrak{a} \to \mathcal{O}$ y M es plano. El lema anterior permite concluir que M es un $\mathcal{O}$-módulo libre.

Definición: Diremos que un A-módulo M es de **presentación finita** si admite alguna presentación $A^s \to A^r \to M \to 0$, es decir si existe algún epimorfismo $A^r \to M$ cuyo núcleo sea de tipo finito.

En particular, todo módulo de presentación finita es de tipo finito. Cuando el anillo A es noetheriano, todo A-módulo de tipo finito es de presentación finita.

Lema E.0.8 *Sea M un A-módulo de presentación finita. Para todo A-módulo N y todo punto $x \in \operatorname{Spec} A$ tenemos que* $\operatorname{Hom}_A(M, N)_x = \operatorname{Hom}_{A_x}(M_x, N_x)$.

Demostración: El enunciado es claramente cierto cuando M es un A-módulo libre de rango finito. En el caso general, por hipótesis existe una presentación finita

$A^s \to A^r \to M \to 0$ y concluimos al considerar el siguiente diagrama conmutativo de filas exactas:

$$\begin{array}{ccccccc}
\mathrm{Hom}_A(A^s,N)_x & \longleftarrow & \mathrm{Hom}_A(A^r,N)_x & \longleftarrow & \mathrm{Hom}_A(M,N)_x & \longleftarrow & 0 \\
\| & & \| & & \downarrow & & \\
\mathrm{Hom}_{A_x}(A^s_x,N_x) & \longleftarrow & \mathrm{Hom}_{Ax}(A^r_x,N_x) & \longleftarrow & \mathrm{Hom}_{A_x}(M_x,N_x) & \longleftarrow & 0
\end{array}$$

Teorema E.0.9 *En los A-módulos de presentación finita, la condición de ser proyectivo equivale a la de ser plano.*

Demostración: Todo módulo proyectivo es siempre plano.

Recíprocamente, si un A-módulo de presentación finita M es plano, entonces M_x es un A_x-módulo plano en todos los puntos $x \in \operatorname{Spec} A$. Por el teorema anterior, M_x es un A_x-módulo proyectivo, así que el funtor

$$N \rightsquigarrow \mathrm{Hom}_{A_x}(M_x,N_x) = \mathrm{Hom}_A(M,N)_x$$

es exacto. Luego $\mathrm{Hom}_A(M,-)$ es un funtor exacto, porque la exactitud de una sucesión es una propiedad local, y M es un A-módulo proyectivo.

Definición: Diremos que un A-módulo M es **localmente libre** si cada punto $x \in \operatorname{Spec} A$ admite un entorno básico U tal que M_U sea un A_U-módulo libre.

Teorema E.0.10 *Si M es un A-módulo de tipo finito, las siguientes condiciones son equivalentes:*

1. *M es proyectivo.*
2. *M es localmente libre.*
3. *M es plano y la función $f(x) := \mathrm{g}\,(M_x)$ es localmente constante sobre el espectro de A.*

Demostración: Si M es un A-módulo plano de tipo finito, en cada punto x tenemos que M_x es un A_x-módulo libre de rango finito. Sean $m_1,\ldots,m_r$ elementos de M que formen un sistema mínimo de generadores de M_x y sea $\phi\colon A^r \to M$ el correspondiente morfismo, de modo que $\phi_x\colon A^r_x \to M_x$ es un isomorfismo. Tenemos una sucesión exacta:

$$0 \longrightarrow N \longrightarrow A^r \xrightarrow{\phi} M \longrightarrow K \longrightarrow 0$$

donde $N_x = K_x = 0$. Como K es de tipo finito (por ser un cociente de M, que es de tipo finito) de acuerdo con 8.2.3 tendremos $K_U = 0$ en algún entorno básico U de x. Es decir, la siguiente sucesión es exacta

$$0 \longrightarrow N_U \longrightarrow A^r_U \xrightarrow{\phi_U} M_U \longrightarrow 0$$

Ahora bien, si M es proyectivo, entonces M_U es un A_U-módulo proyectivo y esta sucesión exacta escinde. Luego N_U es un A_U-módulo de tipo finito y, al ser

$N_x = 0$, podemos sustituir U por un entorno básico de x más pequeño de forma que $N_U = 0$. En tal caso $A_U^r \to M_U$ es un isomorfismo y concluimos que $1 \Rightarrow 2$.

Por otra parte, si la función $f(x) = \mathrm{g}(M_x)$ es localmente constante, sustituyendo U por un entorno básico más pequeño si fuera necesario, podemos suponer que $f(x)$ es constante en U. En tal caso, en cualquier punto $y \in U$ tenemos que $\phi_y\colon A_y^r \to M_y$ es un epimorfismo entre A_y-módulos libres del mismo rango; luego es un isomorfismo. Se sigue que $\phi_U\colon A_U^r \to M_U$ es un isomorfismo y $3 \Rightarrow 2$.

La implicación $2 \Rightarrow 3$ es inmediata, pues si M_U es un A_U-módulo libre entonces M_x es un A_x-módulo libre para todo $x \in U$ y la función $f(x)$ es constante en U.

Para concluir basta probar que $2 \Rightarrow 1$. Si M es de tipo finito, existe alguna una sucesión exacta $0 \to N \to A^r \to M \to 0$. Si además M es localmente libre, al ser $\operatorname{Spec} A$ un espacio compacto, admite un recubrimiento abierto finito, $\operatorname{Spec} A = U_1 \cup \ldots \cup U_n$, tal que cada M_i es un A_i-módulo libre (donde el subíndice i denota la localización por todas las funciones que no se anulen en ningún punto de U_i). Por tanto, las sucesiones exactas

$$0 \longrightarrow N_i \longrightarrow A_i^r \longrightarrow M_i \longrightarrow 0$$

escinden. Luego N_i es un cociente de A_i^r, de modo que N_i es un A_i-módulo de tipo finito. Elegimos ahora elementos $n_1, \ldots, n_s \in N$ que, al localizar en cada abierto U_i, generen el A_i-módulo N_i. El correspondiente morfismo $A^s \to N$ es epiyectivo, porque lo es en un recubrimiento abierto de $\operatorname{Spec} A$, así que N es de tipo finito. Luego M es de presentación finita y el teorema anterior permite concluir que M es proyectivo.

Nota: La condición 3 puede sustituirse por la siguiente: M es plano y $\mathrm{g}(M_x)$ es localmente constante sobre el subespacio de puntos cerrados de $\operatorname{Spec} A$.

Ejemplo: Todo ideal $\mathfrak{a}$ de un dominio de Dedekind A satisface claramente la condición 3 del teorema anterior, luego $\mathfrak{a}$ es un A-módulo proyectivo.

Ejemplo (M. Pisonero): Sea $\mathcal{C}(X)$ el anillo de las funciones reales continuas sobre un espacio metrizable X, sea $\mathfrak{m}$ el ideal maximal de $\mathcal{C}(X)$ formado por las funciones que se anulan en un punto dado $x \in X$ y sea $\mathcal{O}_x = \mathcal{C}(X)_{\mathfrak{m}}$. Entonces:

1. El morfismo de localización $\mathcal{C}(X) \to \mathcal{O}_x$ es epiyectivo y su núcleo es el ideal $\mathfrak{n}_x = \{f \in \mathcal{C}(X)\colon\ f \text{ se anula en un entorno de } x\}$.

2. Si x no es un punto aislado ($\mathfrak{n}_x \neq \mathfrak{m}_x$), entonces $\mathcal{O}_x$ es un $\mathcal{C}(X)$-módulo plano de tipo finito que no es proyectivo.

3. Sea $\mathfrak{a}$ un ideal de $\mathcal{C}(X)$. El $\mathcal{C}(X)$-módulo $\mathcal{C}(X)/\mathfrak{a}$ es plano si y sólo si existe un cerrado Y de X tal que $\mathfrak{a} = \bigcap_{y \in Y} \mathfrak{n}_y$. (*Indicación*: Sea Y el cerrado de X formado por los puntos donde se anulen todas las funciones de $\mathfrak{a}$. Si $\mathcal{C}(X)/\mathfrak{a}$ es plano, entonces $\mathfrak{a}\mathcal{O}_x = 0$ cuando $x \in Y$, mientras que $\mathfrak{a}\mathcal{O}_x = \mathcal{O}_x$ cuando $x \notin Y$).

Apéndice F

Grupos Finitos

F.1 G-conjuntos

Definición: Sea G un grupo y X un conjunto. Llamaremos **acción** (por la izquierda[1]) de G en X a toda aplicación $G \times X \dashrightarrow X$ tal que

1. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ para todo $g_1, g_2 \in G$, $x \in X$.

2. $1 \cdot x = x$ para todo $x \in X$.

Dar una acción de G en X es dar un morfismo de grupos $\rho\colon G \to \mathrm{Biy}(X)$, $\rho(g)(x) = g \cdot x$, en el grupo $\mathrm{Biy}(X)$ de todas las biyecciones de X, en cuyo caso diremos que X es un **G-conjunto**.

Si X e Y son G-conjuntos, diremos que una aplicación $f\colon X \to Y$ es un **morfismo de G-conjuntos** cuando $f(g \cdot x) = g \cdot f(x)$ para todo $g \in G$, $x \in X$. Los isomorfismos de G-conjuntos son los morfismos biyectivos.

Cada acción de un grupo G en un conjunto X define una relación de equivalencia en X sin más que considerar equivalentes dos elementos $x, y \in X$ cuando exista algún $g \in G$ tal que $y = gx$. Llamaremos **órbita** de $x \in X$ a su clase de equivalencia

$$Gx := \{gx\colon\ g \in G\}$$

y Llamaremos **subgrupo de isotropía** de $x \in X$ al subgrupo

$$I_x := \{g \in G\colon\ gx = x\}\ .$$

[1] Análogamente puede definirse el concepto de acción por la derecha; pero sólo es necesario estudiar una de estas dos clases de acciones, porque las acciones por la izquierda y por la derecha de G en X se corresponden sin más que poner $g \cdot x = x \cdot g^{-1}$.

De la definición se sigue directamente la igualdad

$$\boxed{I_{gx} = gI_xg^{-1}} \tag{F.1}$$

Diremos que una acción es **transitiva** cuando tenga una única órbita, y diremos que $x \in X$ es un punto fijo o invariante cuando $Gx = \{x\}$; es decir, cuando $I_x = G$. El conjunto de puntos fijos se denotará X^G.

Ejemplos:

1. G actúa en sí mismo por traslaciones: $g \cdot a = ga$. Esta acción es transitiva y sin puntos fijos (salvo cuando $G = 1$). Además la isotropía es trivial, $I_a = 1$, y por tanto el morfismo de grupos $G \to S_n$ que define esta acción es inyectivo: *Todo grupo finito es isomorfo a un subgrupo de un gruo simétrico.* (**Teorema de Cayley** 1821-1895).

2. G actúa en sí mismo por conjugación: $g \cdot a := gag^{-1}$. El **centro** de G:

$$Z(G) := \{a \in G\colon\ ab = ba,\ \forall b \in G\}\ ,$$

   que es un subgrupo normal de G, coincide con el conjunto de puntos fijos de esta acción.

3. G actúa en el conjunto de sus subgrupos por conjugación: $g \cdot H = gHg^{-1}$. La órbita de un subgrupo H está formada por los subgrupos conjugados de H, y el subgrupo de isotropía es el **normalizador** de H en G:

$$N(H) := \{g \in G\colon\ H = gHg^{-1}\}\ ,$$

   que es el mayor subgrupo de G tal que $H \lhd N(H)$ (el símbolo $H_1 \lhd H_2$ significa que H_1 es un subgrupo normal de H_2).

4. Si H es un subgrupo de G, entonces G actúa en el conjunto cociente G/H del siguiente modo: $g \cdot [a] := [ga]$. Esta acción es transitiva y el subgrupo de isotropía de $[a]$ es precisamente aHa^{-1}.

5. Si H es un subgrupo de G, todo G-conjunto hereda una estructura de H-conjunto sin más que restringir a H la acción de G. En particular H actúa en G/H' cualquiera que sea el subgrupo H'.

Teorema F.1.1 *Si X es un G-conjunto, para todo $x \in X$ se tiene un isomorfismo de G-conjuntos*

$$G/I_x \ = \ Gx \qquad , \qquad [g] \mapsto gx\ .$$

En particular, si G es un grupo finito, el cardinal de cualquier órbita es un divisor del orden de G.

Demostración: La aplicación $G/I_x \to Gx$, $[g] \mapsto gx$, está bien definida porque $I_x x = x$, es claramente morfismo de G-conjuntos y es epiyectiva por definición de Gx. Para concluir, veamos que es inyectiva:

$$g_1 x = g_2 x \;\Rightarrow\; g_1^{-1} g_2 x = x \;\Rightarrow\; g_1^{-1} g_2 \in I_x \;\Rightarrow [g_1] = [g_2]$$

Fórmula de Clases: *Si un grupo finito G de orden n actúa en un conjunto finito X, entonces*

$$|X| = |X^G| + \sum_{x_i} [G : I_{x_i}] = |X^G| + \sum_i d_i \quad , \quad 1 < d_i | n$$

donde $\{x_i\}$ tiene un punto en cada órbita de cardinal mayor que 1.

Demostración: X es la unión disjunta de las órbitas, porque son las clases de equivalencia de una relación de equivalencia, $|X^G|$ es el número de órbitas con un único punto, y por el teorema anterior los cardinales de las restantes órbitas coinciden con los índices $d_i = [G : I_{x_i}]$, que dividen a n por el teorema de Lagrange.

Corolario F.1.2 *Si el orden de un grupo finito G es potencia de un número primo p, entonces para todo G-conjunto finito X tenemos que*

$$|X| \equiv |X^G| \quad (\text{módulo } p)$$

Teorema de Cauchy (1789-1857)**:** *Si un número primo p divide al orden de un grupo finito G, entonces G tiene algún elemento de orden p; i.e., G tiene algún subgrupo de orden p.*

Demostración: El grupo $\mathbb{Z}/p\mathbb{Z}$ actúa en $X = \{(g_1, \ldots, g_p) \in G^p \colon\ g_1 \ldots g_p = 1\}$ permutando cíclicamente los factores:

$$g_1 \ldots g_p = 1 \;\Rightarrow\; g_1 \ldots g_{p-1} = g_p^{-1} \;\Rightarrow\; g_p g_1 \ldots g_{p-1} = 1$$

Como el cardinal $|X| = |G|^{p-1}$ es múltiplo de p, F.1.2 permite obtener que $|X^{\mathbb{Z}/p\mathbb{Z}}| \equiv 0$ (módulo p). Luego existe algún punto fijo $(g, \ldots, g) \in X$ que no es $(1, \ldots, 1)$. Es decir, $g^p = 1$ y $g \neq 1$; luego el orden de g es p.

F.2 p-grupos

Definición: Sea p un número primo. Diremos que un grupo finito es un **p-grupo** si su orden es potencia de p.

Teorema F.2.1 *Si $G \neq 1$ es un p-grupo, su centro no es trivial: $Z(G) \neq 1$.*

Demostración: Si consideramos la acción de G en sí mismo por conjugación, entonces $Z(G)$ es el conjunto de puntos invariantes y F.1.2 permite obtener que el orden del centro es múltiplo de p. Luego $|Z(G)| \neq 1$.

Teorema F.2.2 *Si G es un p-grupo, existe una sucesión creciente de subgrupos normales*

$$1 = H_0 \ \subset \ H_1 \ \subset \ \ldots \ \subset \ H_{n-1} \ \subset \ H_n = G$$

tales que H_i es de orden p^i.

Demostración: Por F.2.1 tenemos que $Z(G) \neq 1$, y el teorema de Cauchy (o bien D.6.3, pues $Z(G)$ es abeliano) asegura la existencia de un subgrupo $H \subseteq Z(G)$ de orden p, que es normal en G. Consideremos la proyección canónica $\pi\colon G \to G/H$. Procediendo por inducción sobre el orden de G, podemos suponer la existencia de una sucesión de subgrupos normales de G/H

$$1 = \bar{H}_0 \ \subset \ \bar{H}_1 \ \subset \ \ldots \ \subset \ \bar{H}_{n-1} = G/H$$

tal que $|\bar{H}_i| = p^i$. Los subgrupos $H_i = \pi^{-1}(\bar{H}_{i-1})$ son normales en G y $H_i/H \simeq \bar{H}_{i-1}$, de modo que $|H_i| = p^i$, $1 \leq i \leq n$.

Corolario F.2.3 *Si G es un p-grupo y p^i divide al orden de G, entonces existe algún subgrupo normal de G de orden p^i.*

F.3 Subgrupos de Sylow

Definición: Sea p un número primo. Si p^n es la mayor potencia de p que divide al orden de un grupo finito G, llamaremos **p-subgrupo de Sylow** (1832-1918) de G a todo subgrupo de orden p^n.

Primer Teorema de Sylow: *Si G es un grupo finito y p un número primo, existen p-subgrupos de Sylow de G.*

Demostración: Procedemos por inducción sobre el orden de G y usamos la fórmula de clases para la acción de G en sí mismo por conjugación:

$$p^n m = |G| = |Z(G)| + \sum_i [G : I_{x_i}]$$

Si algún sumando $[G : I_{x_i}]$ no es múltiplo de p, entonces $|I_{x_i}| = p^n m'$ y cualquier p-subgrupo de Sylow de I_{x_i}, que existe por hipótesis de inducción, también es un p-subgrupo de Sylow de G.

En caso contrario la fórmula de clases muestra que p divide al orden de $Z(G)$. Por el teorema de Cauchy (o por D.6.3, al ser $Z(G)$ abeliano) existe un subgrupo

$H \subseteq Z(G)$ de orden p, que será normal en G. Consideremos el grupo cociente $\pi\colon G \to G/H$. Por hipótesis de inducción, existe un p-subgrupo de Sylow $\bar{P}$ de G/H, y $\pi^{-1}(\bar{P})$ es un p-subgrupo de Sylow de G.

Corolario F.3.1 *Si una potencia p^i de un número primo p divide al orden de un grupo finito G, entonces G tiene algún subgrupo de orden p^i.*

Demostración: Se sigue directamente del primer teorema de Sylow y de F.2.3.

Segundo Teorema de Sylow: *Si G es un grupo finito y p un número primo, entonces todos los p-subgrupos de Sylow de G son conjugados.*

Demostración: Sean P y P' dos p-subgrupos de Sylow de G. Como el cardinal de G/P no es múltiplo de p y P' actúa en G/P, la fórmula de clases muestra la existencia de algún punto fijo $[g] \in G/P$. Como el subgrupo de isotropía de $[g]$ para la acción de G sobre G/P es gPg^{-1}, se sigue que $P' \subseteq gPg^{-1}$ y concluimos que $P' = gPg^{-1}$ al tener ambos subgrupos el mismo orden.

Tercer Teorema de Sylow: *Si p es un número primo y G un grupo finito de orden $p^n m$, donde $p \nmid m$, entonces el número de p-subgrupos de Sylow de G divide al índice común m y es congruente con 1 módulo p.*

Demostración: Sea X el conjunto de p-subgrupos de Sylow de G y sea P un p-subgrupo de Sylow de G. La acción de G en X por conjugación es transitiva, por el segundo teorema, y el subgrupo de isotropía de P es su normalizador $N(P)$. Por F.1.1 tenemos que $|X| = [G : N(P)]$, que divide a $[G : P] = m$.

Consideremos ahora la acción de P en X por conjugación y veamos que el único punto fijo es P. En efecto, si $gP'g^{-1} = P'$ para todo $g \in P$, entonces $P \subset N(P')$; luego P y P' son p-subgrupos de Sylow de $N(P)$, y el segundo teorema afirma que $P' = P$. Usando F.1.2 concluimos que $|X| \equiv |X^P| = 1$ (módulo p).

F.4 Grupos Simples

Definición: Diremos que un grupo G es **simple** si todo subgrupo normal $N \lhd G$ es trivial: $N = 1$ ó $N = G$.

Ejemplos:

1. Todo grupo de orden primo es simple en virtud del teorema de Lagrange. De hecho es cíclico e isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

2. Por el teorema de Cauchy, todo grupo abeliano simple tiene orden primo. *Los grupos abelianos simples son los grupos cíclicos de orden primo.*

3. Los grupos simétricos S_n no son simples, cuando $n \geq 3$, porque A_n es un subgrupo normal no trivial de S_n.

4. Usando los teoremas de Sylow, puede comprobarse caso a caso que todo grupo simple de orden menor que 60 es de orden primo, y por tanto abeliano.

5. El grupo alternado A_4 no es simple, porque un subgrupo normal de A_4 es el grupo de Klein $V = \{id, (12)(34), (13)(24), (14)(23)\}$; pero a continuación veremos que A_5 es un grupo simple de orden 60.

6. Si un grupo G tiene un subgrupo no trivial H de índice n, la acción de G en $X = G/H$ define un morfismo de grupos $G \to \mathrm{Biy}(X) = S_n$ cuyo núcleo es la intersección de todos los subgrupos conjugados de H. Ahora bien, cuando $n! < |G|$, tal morfismo no puede ser inyectivo, y concluimos que tal núcleo es un subgrupo normal no trivial de G: *Un grupo simple G no puede tener subgrupos no triviales de índice n cuando $n! < |G|$.*

   En particular, el grupo simple A_5 no tiene subgrupos de índice 2, ni 3 ni 4.

Lema F.4.1 *Si $n \geq 3$, toda permutación par es producto de ciclos de orden 3*

Demostración: Bastará probar que el producto $(a_1a_2)(b_1b_2)$ de dos trasposiciones siempre es producto de 3-ciclos. Ahora bien, tenemos que

$$\begin{aligned} (a_1a_2)(b_1b_2) &= (a_1a_2b_1)(a_2b_1b_2) && \text{cuando las trasposiciones son disjuntas} \\ (a_1a_2)(b_1b_2) &= (a_2a_1b_2) && \text{cuando } a_1 = b_1 \end{aligned}$$

Teorema F.4.2 *El grupo alternado A_n es simple cuando $n \neq 4$.*

Demostración: Si $n \leq 3$, el orden de A_n es 1 ó 3, así que los únicos subgrupos de A_n son los triviales.

Si $n \geq 5$ y $H \neq 1$ es un subgrupo normal de A_n, vamos a probar que $H = A_n$. Sea α un elemento de H que deje fijos el mayor número de elementos, exceptuando la identidad, y consideremos su descomposición en producto de ciclos disjuntos. Volviendo a numerar los elementos si fuera preciso podemos suponer que

$$\alpha = (1, 2, \ldots, d_1)(d_1 + 1, \ldots, d_1 + d_2)(\ldots$$

y que $d_1, d_2, \ldots$ es una sucesión decreciente. Sea $s \geq 1$ el número de elementos que α no deja fijos. Es claro que $s \geq 3$ y vamos a ver que $s \geq 4$ es imposible:

$s \geq 5$. Sea $\beta = (345)$. Como $\beta \in A_n$ y H es un subgrupo normal de A_n, $\beta\alpha\beta^{-1} \in H$ y $\beta\alpha\beta^{-1}\alpha^{-1} \in H$. Ahora bien, $\beta\alpha\beta^{-1}\alpha^{-1}$ deja fijos el 2 y también todos los elementos que α deje fijos; luego $\beta\alpha\beta^{-1}\alpha^{-1} = 1$ y $\alpha\beta = \beta\alpha$. Se sigue que $\alpha(2) \neq 3$, de modo que $\alpha(2) = 1$ y $\alpha = (12)(34)(56)\ldots \Rightarrow \alpha\beta(3) \neq \beta\alpha(3)$; luego $\alpha\beta \neq \beta\alpha$ y concluimos que este caso es imposible.

$s = 4$. En este caso $\alpha = (12)(34)$ porque la permutación (1234) es impar. Sea $\beta = (345)$. De nuevo $\beta\alpha\beta^{-1}\alpha^{-1} \in H$ y $\beta\alpha\beta^{-1}\alpha^{-1} = (354)$ deja fijos más elementos que α, en contradicción con la elección de α. Este caso también es imposible.

Luego $\alpha = (123)$ y concluimos que H contiene un ciclo de orden 3.

De acuerdo con el lema anterior, para concluir que $H = A_n$ basta probar que H contiene todos los 3-ciclos. Sea $\sigma = (ijk)$ un 3-ciclo 3 y consideremos una permutación τ que transforme 1,2,3 en i, j, k:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ i & j & k & l & m & \dots \end{pmatrix}$$

Intercambiando l y m si fuera preciso podemos suponer que τ es par; luego $\sigma = (ijk) = \tau(123)\tau^{-1} = \tau\alpha\tau^{-1} \in H$ y todos los 3-ciclos están en H.

Corolario F.4.3 *Si $n \neq 4$, el único subgrupo normal no trivial de S_n es A_n.*

Demostración: Si $H \lhd S_n$, entonces $(H \cap A_n) \lhd A_n$ y pueden darse dos casos:

1. $H \cap A_n = A_n$. En este caso $A_n \subseteq H$ y concluimos que $H = A_n$ ó $H = S_n$, porque el índice de A_n en S_n es 2.

2. $H \cap A_n = 1$. En este caso los elementos de H, salvo la identidad, son permutaciones impares. Luego H sólo puede tener un elemento $\sigma \neq 1$, así que toda permutación que tenga la misma forma que σ coincide con σ, lo cual es imposible cuando $n \geq 3$. Concluimos que $H = 1$.

Corolario F.4.4 *Cuando $n > 4$, el único subgrupo no trivial de S_n de índice menor que n es A_n.*

Demostración: Si H es un subgrupo de índice m, la acción de S_n en S_n/H define un morfismo de grupos $S_n \to S_m$, que no puede ser inyectivo cuando $m < n$. Luego su núcleo es A_n ó S_n en virtud del corolario anterior. Como evidentemente tal núcleo está contenido en H, concluimos que $H = A_n$ ó $H = S_n$.

Nota: Los únicos subgrupos normales no triviales del grupo simétrico S_4 son A_4 y $V = \{id, (12)(34), (13)(24), (14)(23)\}$, llamado grupo de Klein (1849-1925).

Por otra parte, cualquier 2-subgrupo de Sylow (1832-1918) de S_4 tiene índice 3.

F.5 Grupos Resolubles

Todo grupo finito G admite una sucesión $1 = H_0 \lhd H_1 \lhd \dots \lhd H_{n-1} \lhd H_n = G$ de subgrupos tal que los cocientes sucesivos H_i/H_{i-1}, $1 \leq i \leq n$, son grupos simples.

En este sentido todo grupo finito está compuesto de grupos simples, y los que estén compuestos por grupos simples abelianos se llaman resolubles:

Definición: Un grupo finito G es **resoluble** si existe alguna sucesión de subgrupos

$$1 = H_0 \ \lhd \ H_1 \ \lhd \ \ldots \ \lhd \ H_{n-1} \ \lhd \ H_n = G$$

tal que los cocientes sucesivos H_i/H_{i-1}, $1 \leq i \leq n$, son grupos cíclicos de orden primo. Tales sucesiones reciben el nombre de resoluciones de G.

Los grupos S_2 y S_3 son claramente resolubles, y una resolución de S_4 es

$$1 \ \lhd \ \{\, \mathrm{id}\,,\, (12)(34)\,\} \ \lhd \ V \ \lhd \ A_4 \ \lhd \ S_4 \ .$$

Teorema F.5.1 *El grupo simétrico S_n no es resoluble cuando $n \geq 5$.*

Demostración: Es obvio a partir de F.4.2 y F.4.3; pero también es consecuencia directa de que todo 3-ciclo (ijk) es el conmutador de otros dos 3-ciclos:

$$(ijk) = \sigma\tau\sigma^{-1}\tau^{-1} \qquad , \qquad \sigma = (ijl) \ , \ \tau = (ikm)$$

Si existiera una sucesión de subgrupos $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_{d-1} \lhd H_d = S_n$ tal que los cocientes H_i/H_{i-1} fueran abelianos, entonces H_{i-1} contiene el conmutador de dos elementos cualesquiera de H_i para todo $1 \leq i \leq d$. Luego H_{i-1} contiene todos los 3-ciclos cuando H_i los contiene, y se llegaría al absurdo de que el subgrupo 1 contiene todos los 3-ciclos.

Teorema F.5.2 *Si un grupo finito es resoluble, todos sus subgrupos también son resolubles.*

Demostración: Sea $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ una resolución de un grupo finito G. Si H es un subgrupo de G y ponemos $H'_i = H_i \cap H$, entonces H'_{i-1} es un subgrupo normal de H'_i y H'_i/H'_{i-1} es (isomorfo a) un subgrupo de H_i/H_{i-1} para todo $1 \leq i \leq n$. Como el orden de H_i/H_{i-1} es primo, el teorema de Lagrange afirma que $H'_i/H'_{i-1} = 1$ ó $H'_i/H'_{i-1} = H_i/H_{i-1}$. Eliminando las repeticiones en la cadena $1 = H'_0 \subseteq H'_1 \subseteq \ldots \subseteq H'_n = H$ obtenemos una sucesión cuyos cocientes sucesivos son de orden primo, y concluimos que H es resoluble.

Teorema F.5.3 *Sea H un subgrupo normal de un grupo finito G. La condición necesaria y suficiente para que G sea resoluble es que H y G/H sean resolubles.*

Demostración: Si G es resoluble, H es resoluble por F.5.2. En cuanto a G/H, consideremos una resolución $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$, la proyección canónica $\pi\colon G \to G/H$, y pongamos $\bar{H}_i := \pi(H_i)$. Entonces $\bar{H}_{i-1}$ es un subgrupo normal de $\bar{H}_i$ y $\bar{H}_i/\bar{H}_{i-1}$ es (isomorfo a) un cociente de H_i/H_{i-1} para todo $1 \leq i \leq n$. Como

el orden de H_i/H_{i-1} es primo, el teorema de Lagrange (1736-1813) afirma que $\bar{H}_i/\bar{H}_{i-1} = 1$ ó $\bar{H}_i/\bar{H}_{i-1} = H_i/H_{i-1}$. Eliminando ahora las posibles repeticiones en la cadena $1 = \bar{H}_0 \lhd \bar{H}_1 \lhd \ldots \lhd \bar{H}_n = G/H$ obtenemos una sucesión cuyos cocientes sucesivos son de orden primo, y concluimos que G/H es resoluble.

Recíprocamente, si H y G/H son resolubles, consideramos la proyección canónica $\pi\colon G \to G/H$ y sendas resoluciones

$$\begin{aligned} 1 = H_0 \ &\lhd\ H_1 \ \lhd\ \ldots\ \lhd\ H_{n-1} \ \lhd\ H_n = H \\ 1 = \bar{H}_0 \ &\lhd\ \bar{H}_1 \ \lhd\ \ldots\ \lhd\ \bar{H}_{d-1} \ \lhd\ \bar{H}_d = G/H \end{aligned}$$

Es sencillo comprobar que en la sucesión creciente de subgrupos

$$1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = \pi^{-1}(\bar{H}_0) \lhd \pi^{-1}(\bar{H}_1) \lhd \ldots \lhd \pi^{-1}(\bar{H}_d) = G$$

los cocientes sucesivos son de orden primo, y concluimos que G es resoluble.

Corolario F.5.4 *Todo grupo finito abeliano es resoluble.*

Demostración: Procediendo por inducción sobre el orden, si H es un subgrupo de orden primo de un grupo abeliano finito G, entonces $H \lhd G$ y el grupo G/H es resoluble por hipótesis de inducción, así que F.5.3 permite concluir.

Corolario F.5.5 *Sea G un grupo finito. Si existe una sucesión de subgrupos $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ tal que los cocientes sucesivos H_i/H_{i-1} son grupos abelianos, entonces G es resoluble.*

El Grupo Metacíclico

Definición: Sea p un número primo y $\mathrm{Af}_p(1)$ el grupo de las afinidades $ax + b$, de una recta afín sobre $\mathbb{F}_p$, que puede verse como subgrupo de orden $p(p-1)$ del grupo S_p de todas las permutaciones de la recta afín. Las traslaciones $x+b$ forman un subgrupo T de orden p, que es el subgrupo generado por el ciclo $(1, 2, \ldots, p)$.

Lema F.5.6 *Sea p un número primo. El grupo $\mathrm{Af}_p(1)$ de las afinidades $ax+b$ de una recta afín sobre el cuerpo $\mathbb{F}_p$ es un grupo resoluble de orden $p(p-1)$, y visto como subgrupo del grupo S_p de todas las biyecciones de la recta afín, coincide con el normalizador del grupo de las traslaciones T en S_p.*

Demostración: El morfismo de grupos $\mathrm{Af}_p(1) \to \mathbb{F}_p^*$, $ax + b \mapsto a$, es epiyectivo y su núcleo es el grupo T de las traslaciones $x + b$, que es un grupo cíclico de orden p. Como $\mathbb{F}_p^*$ es un grupo abeliano de orden $p - 1$, F.5.5 afirma que $\mathrm{Af}_p(1)$ es un grupo resoluble de orden $p(p-1)$.

Por otra parte T es un subgrupo normal de $\mathrm{Af}_p(1)$ porque es el núcleo de un morfismo de grupos, así que $\mathrm{Af}_p(1) \subseteq N(T)$. Además, por el segundo teorema de

Sylow, todos los subgrupos de orden p de S_p son conjugados; luego el índice de $N(T)$ en S_p coincide con el número de subgrupos de orden p, que es

$$\frac{\text{número de } p\text{-ciclos}}{p-1} \;=\; \frac{(p-1)!}{p-1} \;=\; (p-2)!$$

y concluimos que el orden de $N(T)$ es $p(p-1)$; es decir, $\mathrm{Af}_p(1) = N(T)$.

Teorema F.5.7 *Sea p un número primo. Todo subgrupo resoluble y transitivo de S_p es, salvo conjugación, un subgrupo del grupo $\mathrm{Af}_p(1)$ de las afinidades de una recta afín sobre $\mathbb{F}_p$ que contiene a las traslaciones. En particular su orden es pd para algún divisor d de $p-1$.*

Demostración: Si $G \subseteq S_p$ es un subgrupo transitivo, su orden es múltiplo de p por F.1.1. Si N es un subgrupo normal de G no trivial, entonces N también es transitivo y su orden es múltiplo de p. En efecto, los subgrupos de isotropía $I_1, \ldots, I_p$ de la acción de G son conjugados entre sí porque la acción es transitiva, así que también lo son los subgrupos $I_1 \cap N, \ldots, I_p \cap N$, que son los subgrupos de isotropía de la acción de N; luego todas las órbitas de la acción de N tienen igual cardinal y, al ser p primo, concluimos que N actúa transitivamente.

Si además G es resoluble y $1 \lhd H_1 \lhd \ldots \lhd H_n = G$ es una resolución, se sigue que el orden de H_1 es múltiplo de p; luego es p y, sustituyendo G por un subgrupo conjugado si fuera necesario, podemos suponer que $H_1 = T$. Ahora T es un p-subgrupo de Sylow de estos grupos H_i, $2 \leq i \leq n$. Como $T \lhd H_2$, del segundo teorema de Sylow se sigue que T es el único subgrupo de orden p en H_2, como $H_2 \lhd H_3$, se sigue que T es el único subgrupo de orden p en H_3, como $H_3 \lhd H_4$, $\ldots$ y obtenemos que $T \lhd G$. Luego $G \subseteq N(T) = \mathrm{Af}_p(1)$.

Corolario F.5.8 *Sea p un número primo y $G \subset S_p$ un subgrupo resoluble y transitivo. Si $\tau \in G$ tiene dos puntos fijos, entonces $\tau = id$.*

Demostración: $G \subseteq \mathrm{Af}_p(1)$ y la única afinidad con dos puntos fijos es la identidad.

Corolario F.5.9 *Sea p un número primo. La condición necesaria y suficiente para que un subgrupo transitivo $G \subset S_p$ sea resoluble es que su orden sea pq para algún $q < p$.*

Demostración: La necesidad es parte de F.5.7.

Recíprocamente, si $|G| = pq$ y $q < p$, entonces G contiene algún subgrupo de orden p y, sustituyendo G por un subgrupo conjugado, podemos suponer que $T \subseteq G$. Por el tercer teorema de Sylow, el número de subgrupos de orden p en G divide a q y es congruente con 1 módulo p. Como $q < p$, se sigue que T es el único subgrupo de orden p en G; luego $G \subseteq N(T) = \mathrm{Af}_p(1)$ y concluimos que G es resoluble.

Apéndice G

Álgebras Finitas

En este apéndice k denotará un cuerpo arbitrario.

G.1 Espectro de un Álgebra Finita

Definición: Llamaremos **grado** de una k-álgebra A a su dimensión como k-espacio vectorial y se denota $[A : k]$. Diremos que una k-álgebra A es **finita** si lo es su grado.

Propiedades de las Álgebras Finitas:

1. *Subálgebras, cocientes sumas directas y productos tensoriales de k-álgebra finitas son k-álgebras finitas y*

$$[A \oplus B : k] = [A : k] + [B : k] \quad , \quad [A \otimes_k B : k] = [A : k] \cdot [B : k]$$

2. *Si A es una k-álgebra finita y L es una extensión de k, entonces $A_L := A \otimes_k L$ es una L-álgebra finita y* $[A_L : L] = [A : k]$.

Demostración: Son propiedades sencillas de la dimensión de los espacios vectoriales y del producto tensorial.

Lema G.1.1 *Toda k-álgebra finita íntegra es un cuerpo.*

Demostración: Si $a \in A$ no es nulo, la aplicación lineal $h_a \colon A \to A$, $h_a(x) = ax$, es inyectiva porque A es íntegro. Como A es un k-espacio vectorial de dimensión finita, se sigue que la dimensión de la imagen de h_a coincide con la de A. Luego h_a es epiyectivo y concluimos que $1 = h_a(b) = ab$ para algún $b \in A$. Es decir, a es invertible y A es un cuerpo.

Lema G.1.2 *Todo ideal primo de una k-álgebra finita A es maximal.*

Demostración: Si $\mathfrak{p}$ es un ideal primo de A, entonces $A/\mathfrak{p}$ es una k-álgebra finita íntegra; luego es un cuerpo y concluimos que $\mathfrak{p}$ es un ideal maximal. q.e.d.

Ahora, si $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ son ideales maximales de una k-álgebra finita A, entonces

$$(\mathfrak{m}_1)_o \cap (\mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_r)_o \;=\; (\mathfrak{m}_1)_o \cap \big((\mathfrak{m}_2)_o \cup \ldots \cup (\mathfrak{m}_r)_o\big) \;=\; \emptyset$$

y el Teorema Chino de los Restos nos proporciona un isomorfismo de k-álgebras

$$\boxed{A/(\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r) \;=\; (A/\mathfrak{m}_1) \oplus \ldots \oplus (A/\mathfrak{m}_r)}$$

Lema G.1.3 *El número de ideales maximales de una k-álgebra finita A está acotado por el grado de A.*

Demostración: El isomorfismo anterior muestra claramente que

$$r \leq [A/\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r : k] \leq [A : k]$$

Teorema G.1.4 *El espectro de una k-álgebra finita A es un espacio topológico discreto de cardinal acotado por el grado de A sobre k.*

Demostración: En virtud de los lemas anteriores $\operatorname{Spec} A$ es finito (A sólo tiene un número finito de ideales primos) y de cardinal acotado por el grado de A, y todos sus puntos son cerrados; luego es un espacio discreto.

Definición: Si $\mathfrak{m}$ es un ideal maximal de una k-álgebra A, diremos que la extensión $A/\mathfrak{m}$ de k es el **cuerpo residual** de $\mathfrak{m}$ o del correspondiente punto $x \in \operatorname{Spec} A$, y diremos que $\mathfrak{m}$ (o el correspondiente punto x de $\operatorname{Spec} A$) es **racional** cuando su cuerpo residual sea una extensión de grado 1; es decir, cuando $k = A/\mathfrak{m}$.

Diremos que una k-álgebra finita es **racional** cuando todos los puntos de su espectro sean racionales.

Teorema G.1.5 *Toda k-álgebra finita reducida A descompone en suma directa de extensiones finitas, que son los cuerpos residuales de los puntos de su espectro:*

$$A \;=\; (A/\mathfrak{m}_1) \oplus \ldots \oplus (A/\mathfrak{m}_n) \quad , \quad \operatorname{Spec} A = \{x_1, \ldots, x_n\}$$

Demostración: Si $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ son todos los ideales maximales de una k-álgebra finita reducida A, entonces son todos los ideales primos de A por G.1.2. Luego $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ es el radical de A en virtud de 7.2.7, que es nulo por hipótesis. Concluimos que

$$A \;=\; (A/\mathfrak{m}_1) \oplus \ldots \oplus (A/\mathfrak{m}_n)$$

Corolario G.1.6 *Si una k-álgebra finita A es reducida, todos sus cocientes A/I son k-álgebras finitas reducidas.*

Demostración: Todo ideal I de una suma directa finita de cuerpos $A = L_1 \oplus \ldots \oplus L_n$ es de la forma $I = L_1 \oplus \ldots \oplus L_r \oplus 0 \oplus \ldots \oplus 0$, después de reordenar las componentes si fuera necesario; luego $A/I = L_{r+1} \oplus \ldots \oplus L_n$ es un anillo reducido. Hemos usado el siguiente resultado elemental:

Lema G.1.7 *Si A_1 y A_2 son dos anillos, todo ideal de $A_1 \oplus A_2$ es de la forma $\mathfrak{a}_1 \oplus \mathfrak{a}_2$, donde $\mathfrak{a}_1$ es un ideal de A_1 y $\mathfrak{a}_2$ es un ideal de A_2.*

Demostración: Sea $\mathfrak{a}$ un ideal de $A_1 \oplus A_2$. Si ponemos $\mathfrak{a}_1 := \{a_1 \in A_1 \colon (a_1, 0) \in \mathfrak{a}\}$ y $\mathfrak{a}_2 := \{a_2 \in A_2 \colon (0, a_2) \in \mathfrak{a}\}$, es claro que $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \subseteq \mathfrak{a}$. Ahora bien, si $(a_1, a_2) \in \mathfrak{a}$, entonces $a_1 \in \mathfrak{a}_1$ porque $(a_1, 0) = (1, 0)(a_1, a_2) \in \mathfrak{a}$ y $a_2 \in \mathfrak{a}_2$ porque $(0, a_2) = (0, 1)(a_1, a_2) \in \mathfrak{a}$.

G.2 Álgebras Triviales

Definición: Diremos que una k-álgebra finita A es **trivial** si descompone en suma directa de extensiones de grado 1; es decir, si $A \simeq k \oplus \ldots \oplus k$.

Caracterización de las Álgebras Triviales: *Si A es una k-álgebra finita, las siguientes condiciones son equivalentes:*

1. *A es una k-álgebra trivial, $A = k \oplus \ldots \oplus k$.*
2. *El número de puntos de* $\operatorname{Spec} A$ *coincide con el grado de A sobre k.*
3. *A es una k-álgebra racional reducida.*

Demostración: Sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ los ideales maximales de A, y consideremos la descomposición $A/\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r = (A/\mathfrak{m}_1) \oplus \ldots \oplus (A/\mathfrak{m}_r)$.

($2 \Rightarrow 3$) Si $r = [A : k]$, entonces $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r = 0$ y todos los cuerpos residuales $A/\mathfrak{m}_i$ son de grado 1.

($3 \Rightarrow 1$) Si A es reducida y racional, entonces $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r = 0$ y $k = A/\mathfrak{m}_i$ para todo $1 \leq i \leq r$, y la descomposición anterior muestra que A es trivial.

($1 \Rightarrow 2$) Si $A = k \oplus \overset{n}{\ldots} \oplus k$ es trivial, entonces los núcleos de las proyecciones naturales $p_i \colon A \to k$ definen n puntos de $\operatorname{Spec} A$. Como el número de puntos no puede superar al grado, concluimos que ambos coinciden.

Lema G.2.1 *La aplicación continua $\phi \colon \operatorname{Spec} A \to \operatorname{Spec} B$ inducida por cualquier morfismo de k-álgebras $j \colon B \to A$ transforma puntos racionales de* $\operatorname{Spec} A$ *en puntos racionales de* $\operatorname{Spec} B$.

Demostración: Sea $\mathfrak{m}$ el ideal maximal de A definido por un punto racional $x \in \operatorname{Spec} A$. Si $\mathfrak{p}$ denota el ideal primo de B correspondiente al punto $\phi(x)$, por definición $\mathfrak{p} = j^{-1}(\mathfrak{m})$, así que el morfismo natural

$$B/\mathfrak{p} \longrightarrow A/\mathfrak{m}$$

es inyectivo. Por hipótesis $k = A/\mathfrak{m}$; luego $B/\mathfrak{p} = k$ y concluimos que $\phi(x)$ es un punto racional de $\operatorname{Spec} B$.

Propiedades de las Álgebras Triviales:

1. *Subálgebras, cocientes sumas directas y productos tensoriales de k-álgebras triviales son k-álgebras triviales.*

2. *El concepto de álgebra trivial es estable por cambios del cuerpo base (i.e., si A es una k-álgebra trivial y L es una extensión de k, entonces $A_L = A \otimes_k L$ es una L-álgebra trivial).*

Demostración: Sea B una subálgebra de una k-álgebra trivial $A = \oplus k$. Como B es reducida, al serlo A, bastará ver que B es racional. Sea $\mathfrak{m}$ un ideal maximal de B. Por 7.2.4 cualquier ideal maximal de $A_{\mathfrak{m}}$ se corresponde con un ideal maximal $\mathfrak{m}'$ de A que no corta a $S = B - \mathfrak{m}$; así que $\mathfrak{m} = \mathfrak{m}' \cap B$. Por hipótesis $k = A/\mathfrak{m}'$ y G.2.1 permite concluir que $k = B/\mathfrak{m}$.

Además, si I es un ideal de $A = k\oplus \overset{d}{\ldots} \oplus k$, reordenando las componentes si fuera necesario, podemos suponer que $I = k\oplus \overset{r}{\ldots} \oplus k \oplus 0 \oplus \ldots \oplus 0$. Luego $A/I = k\oplus \overset{n-r}{\ldots} \oplus k$ es una k-álgebra finita trivial.

Las demás propiedades son evidente por las propiedades del producto tensorial.

Definición: Diremos que una k-álgebra finita A es trivial sobre una extensión L de k, ó que L trivializa a la k-álgebra A, cuando A_L sea una L-álgebra trivial.

De las propiedades de las álgebras triviales deducen inmediatamente las siguientes propiedades de las extensiones trivializantes:

1. Subálgebras, cocientes, sumas directas y productos tensoriales de k-álgebras finitas triviales sobre L son triviales sobre L.

2. Si una k-álgebra finita es trivial sobre L, también es trivial sobre cualquier extensión de L.

El Ejemplo Fundamental: De acuerdo con 4.4.1, si $p(x) \in k[x]$ es un polinomio no constante de grado d, entonces $A = k[x]/(p(x))$ es una k-álgebra finita de grado d, y una base de A como k-espacio vectorial es $(1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{d-1})$. Si $p(x) = p_1(x)^{m_1} \ldots p_r(x)^{m_r}$ es su descomposición en factores irreducibles en $k[x]$, entonces:

1. Los ideales maximales de A son $\mathfrak{m}_1 = (p_1(x)), \ldots, \mathfrak{m}_r = (p_r(x))$, de modo que los puntos de $\operatorname{Spec} A$ se corresponden con los factores irreducibles de $p(x)$, y los cuerpos residuales son las extensiones $k[x]/(p_i(x))$, cuyos grados coinciden con los de los factores irreducibles de $p(x)$.

   En particular, los puntos racionales de A se corresponden con los factores irreducibles $p_i(x)$ de grado 1; es decir, con las raíces de $p(x)$ en k.

2. A es una k-álgebra racional precisamente cuando todos los factores irreducibles $p_i(x)$ son de grado 1, lo que significa que $p(x)$ descompone en $k[x]$ en factores de grado 1 (eventualmente repetidos). Es decir, A es racional si y sólo si $p(x)$ tiene todas sus raíces en k: el número de raíces de $p(x)$ en k, contadas con su multiplicidad, iguala al grado de $p(x)$.

3. El radical del álgebra A es $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r = (p_1(x) \ldots p_r(x))$, así que A es reducida precisamente cuando $m_1 = \ldots = m_n = 1$.

4. A es trivial si y sólo si $p(x)$ tiene todas sus raíces en k y son simples.

5. Si L es una extensión de k, por las propiedades del cambio de base tenemos que $A_L = L[x]/(p(x))$. Luego A es trivial sobre L precisamente cuando $p(x)$ tiene todas sus raíces en L y son simples.

G.3 Puntos de un Álgebra

Definición: Si A es una k-álgebra y L es una extensión de k, llamaremos **puntos** de A con valores en L, ó L-puntos de A, a los morfismos de k-álgebras $p\colon A \to L$. Si $f \in A$, diremos que $f(p) := p(f) \in L$ es el **valor** de la función f en el punto p.

Ejemplos:

1. Cada morfismo de k-álgebras $k[x_1, \ldots, x_n] \to L$ está totalmente determinado por las imágenes α_i de las indeterminadas x_i. Los puntos de $k[x_1, \ldots, x_n]$ con valores en cualquier extensión L de k son las sucesiones $(\alpha_1, \ldots, \alpha_n) \in L^n$.

2. Si $A = k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$, los morfismos de k-álgebras $A \to L$, de acuerdo con la propiedad universal del cociente, se corresponden con los morfismos de k-álgebras $k[x_1, \ldots, x_n] \to L$ que se anulen en $(p_1, \ldots, p_r)$. Es decir, con las sucesiones $(\alpha_1, \ldots, \alpha_n) \in L^n$ tales que

$$p_1(\alpha_1, \ldots, \alpha_n) = \ldots = p_r(\alpha_1, \ldots, \alpha_n) = 0.$$

$$\operatorname{Hom}_{k\text{-alg}}(A, L) \;=\; \begin{bmatrix}\text{Soluciones en } L \text{ del sistema de} \\ \text{ecuaciones } p_1 = \ldots = p_r = 0\end{bmatrix}$$

En particular, cuando $A = k[x]/(p(x))$, obtenemos que los puntos de A con valores en L son las raíces de $p(x)$ en L. *El concepto de raíz de un polinomio es un caso particular del concepto de punto.*

3. Si L es una extensión finita de un cuerpo k, todo morfismo de k-álgebras $L \to L$ es un automorfismo porque necesariamente es inyectivo, al ser L un cuerpo, y L es un k-espacio vectorial de dimensión finita. Luego los puntos de L con valores en L son precisamente los automorfismos de L que son la identidad sobre k. *El concepto de automorfismo de una extensión finita es un caso particular del concepto de punto.*

El núcleo de cualquier morfismo de k-álgebras $p\colon A \to L$ es un ideal primo de A, porque L es íntegro, así que cada L-punto de A define un punto de $\operatorname{Spec} A$. Pero diferentes L-puntos pueden definir el mismo punto del espectro. No obstante, en el caso de un punto $A \to k$ con valores en el cuerpo base k, el correspondiente punto de $\operatorname{Spec} A$ es un punto racional, y vamos a probar que tal correspondencia entre k-puntos de A y puntos racionales de $\operatorname{Spec} A$ es biyectiva:

Lema G.3.1 *Si A es una k-álgebra, los puntos de A con valores en k se corresponden biunívocamente con los puntos racionales de* $\operatorname{Spec} A$.

Demostración: Cada ideal maximal $\mathfrak{m}$ de un punto racional de $\operatorname{Spec} A$ es el núcleo de la proyección canónica $\pi\colon A \to A/\mathfrak{m} = k$, que es un k-punto de A; luego tal correspondencia es epiyectiva.

Por otra parte, si otro morfismo de k-álgebras $p\colon A \to k$ tiene núcleo $\mathfrak{m}$, de la propiedad universal del cociente se sigue que $p = \phi \circ \pi$ para algún automorfismo de k-álgebras $\phi\colon k \to k$. Pero el único automorfismo de k-álgebras $k \to k$ es la identidad, así que $p = \pi$ y concluimos que tal correspondencia es inyectiva.

Fórmula de los Puntos: *Sea A una k-álgebra y sea L una extensión de k. Si a cada L-punto $p\colon A \to L$ se le asigna el punto racional $p \otimes 1\colon A \otimes_k L \to L$ del espectro de $A_L = A \otimes_k L$, se obtiene una correspondencia biyectiva:*

$$\begin{bmatrix}\text{Puntos de } A\\ \text{con valores en } L\end{bmatrix} = \begin{bmatrix}\text{Puntos racionales}\\ \text{de la } L\text{-álgebra } A_L\end{bmatrix}$$

Demostración: Por la propiedad universal del cambio de base de álgebras, tenemos que $\operatorname{Hom}_{k\text{-alg}}(A, L) = \operatorname{Hom}_{L\text{-alg}}(A_L, L)$, y se concluye al aplicar el lema anterior a la L-álgebra A_L.

Corolario G.3.2 *El número de puntos de una k-álgebra finita A con valores en una extensión L de k está acotado por el grado $[A : k]$, y coincide con él precisamente cuando A es trivial sobre L: $A \otimes_k L = L \oplus \ldots \oplus L$.*

Demostración: El número de puntos racionales de la L-álgebra finita A_L está acotado por $[A_L : L] = [A : k]$ (porque lo está el número de puntos del espectro de A_L). Se da la coincidencia si y sólo si A_L es L-álgebra trivial, en virtud de la caracterización de las álgebras triviales.

Corolario G.3.3 *El número de automorfismos de una extensión finita L de un cuerpo k está acotado por el grado $[L : k]$. Se da la coincidencia si y sólo si $L \otimes_k L$ es L-álgebra trivial: $L \otimes_k L = L \oplus \ldots \oplus L$.*

Ejemplo: Sea A una k–álgebra finita y sean $\phi_1, \ldots, \phi_n \colon A \to L$ los puntos de A con valores en una extensión L de k. Los correspondientes puntos racionales de A_L son los morfismos $\phi_i \otimes 1 \colon A_L \to L$, así que, cuando el número de puntos iguala al grado de A, el isomorfismo $A_L = L \oplus \ldots \oplus L$ es $a \otimes \lambda \mapsto (\lambda\phi_1(a), \ldots, \lambda\phi_n(a))$.

Cuando $A = k[x]/(p(x))$, los puntos de A con valores en L se corresponden con las raíces $\alpha_1, \ldots, \alpha_n$ de $p(x)$ en L. Si el número de raíces iguala al grado de $p(x)$, el isomorfismo $A_L = L \oplus \ldots \oplus L$ es $q(x) \otimes \lambda \mapsto (\lambda q(\alpha_1), \ldots, \lambda q(\alpha_n))$.

Cuando $A = L$ y el número de automorfismos $\tau_1, \ldots, \tau_n$ de L sobre k iguala al grado de L, el isomorfismo $L \otimes_k L = L \oplus \ldots \oplus L$ es $\mu \otimes \lambda \mapsto (\lambda\tau_1(\mu), \ldots, \lambda\tau_n(\mu))$.

Teorema de Independencia: *Si A es una k-álgebra finita y L es una extensión de k, toda familia de morfismos de k-álgebras $A \to L$ es linealmente independiente sobre L.*

Demostración: Si $\{p_i \colon A \to L\}_{i \in I}$ es una familia de morfismos de k-álgebras, define morfismos de L-álgebras $p_i \otimes 1 \colon A_L \to L$. Si existen elementos $\lambda_i \in L$ tales que $\lambda_1 p_1 + \ldots + \lambda_n p_n = 0$, entonces $\lambda_1(p_1 \otimes 1) + \ldots + \lambda_n(p_n \otimes 1) = 0$, así que basta considerar el caso $k = L$.

Si $k = L$, por G.3.1 los morfismos p_i se corresponden con ciertos puntos racionales $x_i \in \operatorname{Spec} A$, que son cerrados. Como las funciones de A separan puntos de cerrados, para cada índice $i = 1, \ldots, n$ existe una función $f \in A$ que se anula en tales puntos, salvo en x_i. Es decir, $f(p_i) \neq 0$ y $f(p_j) = 0$ cuando $j \neq i$. Como $0 = \sum_j \lambda_j f(p_j) = \lambda_i f(p_i)$, concluimos que $\lambda_i = 0$.

Corolario G.3.4 *Los automorfismos de una extensión finita L de un cuerpo k son linealmente independientes sobre L.*

Compuestos

Definición: Sean L_1 y L_2 dos extensiones de un cuerpo k. Si E es una extensión común, de modo que tenemos sendos morfismos de k-álgebras $L_1 \to E$ y $L_2 \to E$, llamaremos **compuesto** de L_1 y L_2 en E al menor subanillo de E que sea cuerpo y contenga a (las imágenes de) L_1 y L_2, y se denotará L_1L_2. Es decir, L_1L_2 está

formado por los elementos de E que se obtienen a partir de elementos de L_1 y L_2 mediante un número finito de sumas, restas, multiplicaciones y divisiones.

Diremos que E es un compuesto de L_1 y L_2 sobre k cuando $E = L_1L_2$.

Siempre existe algún compuesto L_1L_2.

Basta tomar el cuerpo residual $(L_1 \otimes_k L_2)/\mathfrak{m}$ de un ideal maximal de $L_1 \otimes_k L_2$.

Los compuestos de una extensión finita $k \to L$ con cualquier extensión $k \to E$ son las extensiones de E isomorfas a los cuerpos residuales de los puntos del espectro de $L \otimes_k E$, así que son extensiones finitas de E de grado

$$[LE : E] \ \leq \ [L : k]$$

En efecto, los morfismos $L \to LE$, $E \to LE$ definen un morfismo $L \otimes_k E \to LE$ que ha de ser epiyectivo, pues su imagen es un cuerpo, al ser una E-álgebra finita (es un cociente de $L \otimes_k E$) íntegra (porque es un subanillo de un cuerpo). Luego LE es isomorfo al cociente de $L \otimes_k E$ por un ideal maximal.

Ejemplo: Sea $L = \mathbb{Q}(\sqrt[4]{2}\,)$. Los compuestos de L consigo mismo sobre $\mathbb{Q}$ son $\mathbb{Q}(\sqrt[4]{2}\,)$ y $\mathbb{Q}(\sqrt[4]{2}, i)$, porque son (isomorfos a) los cuerpos residuales de

$$\begin{aligned} L \otimes_{\mathbb{Q}} L &= L \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x^4-2) = L[x]/(x^4-2) = \\ &= L[x]/((x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2})) \simeq \\ &\simeq L[x]/(x-\sqrt[4]{2}) \oplus L[x]/(x+\sqrt[4]{2}) \oplus L[x]/(x^2+\sqrt{2}) \simeq \\ &\simeq L \oplus L \oplus L(i\sqrt[4]{2}) = L \oplus L \oplus \mathbb{Q}(\sqrt[4]{2}, i)\ . \end{aligned}$$

G.4 Álgebras Separables

Definición: Diremos que una k-álgebra finita A es **separable** si es geométricamente reducida; es decir, si $A_L = A \otimes_k L$ es reducida para toda extensión $k \to L$. En caso contrario diremos que es **inseparable**.

Diremos que un polinomio no nulo $p(x) \in k[x]$ es **separable** cuando lo sea la k-álgebra $k[x]/(p(x))$; es decir, cuando su descomposición en factores irreducibles en $L[x]$ carezca de factores repetidos, para toda extensión $k \to L$. Tal condición claramente significa que todas las raíces de $p(x)$ son simples, lo que equivale a decir que $\text{m.c.d.}(p(x), p'(x)) = 1$.

Caracterización de las Álgebras Separables: *Una k-álgebra finita A es separable si y sólo si es trivial sobre alguna extensión L de k; i.e., $A_L = L \oplus \ldots \oplus L$.*

Demostración: Si A es separable, procedemos por inducción sobre el grado $d = [A : k]$, pues A es trivial sobre k cuando $d = 1$. Cuando $d > 1$, consideramos un

morfismo de k-álgebras $A \to E$ en alguna extensión finita K de k (basta tomar un cuerpo residual $K = A/\mathfrak{m}$). La fórmula de los puntos asegura que A_K tiene algún punto racional y, al ser A_K reducida, G.1.5 muestra que $A_K = K \oplus B$, de modo que $[B : K] < [A : k] = d$ y B es una K-álgebra separable, pues para toda extensión E de K tenemos que B_E es una subálgebra de $(A_K)_E = A_E$, que es reducida. Por hipótesis de inducción existe alguna extensión L de K tal que $B \otimes_K L = \oplus L$, y concluimos que

$$A \otimes_k L = (A \otimes_k K) \otimes_K L = (K \oplus B) \otimes_K L = L \oplus (B \otimes_K L) = \oplus L$$

Recíprocamente, si $A_L = \oplus L$, tenemos que demostrar que A_E es reducida para toda extensión $k \to E$. Consideremos un compuesto LE de L y E sobre k. Como A es trivial sobre L, también es trivial sobre LE. Luego $A_{LE} = LE \oplus \ldots \oplus LE$ y, en particular, es reducida. Como el morfismo natural $A \otimes_k E \to A \otimes_k (LE)$ es inyectivo, porque lo es el morfismo $E \to LE$ y k es un cuerpo, concluimos que A_E es reducida.

Propiedades de las Álgebras Separables:

1. *Subálgebras, cocientes sumas directas y productos tensoriales de k-álgebras finitas separables son k-álgebras finitas separables.*
2. *El concepto de álgebra finita separable es estable por cambios del cuerpo base (si A es una k-álgebra finita separable y L es una extensión de k, entonces A_L es una L-álgebra finita separable).*
3. *Si A es una k-álgebra finita y para alguna extensión L del cuerpo base k se verifica que la L-álgebra finita A_L es separable, entonces la k-álgebra finita A es separable.*

Demostración: La propiedad 1 se sigue directamente de las propiedades de las álgebras triviales. En cuanto a la propiedad 2, si A es una k-álgebra finita separable, para toda extensión $L \to E$ tenemos que $(A_L)_E = A_E$ es reducida; luego la L-álgebra finita A_L es separable.

Por último, si la L-álgebra finita A_L es separable para alguna extensión L de k, entonces existe una extensión $L \to E$ tal que $A_E = (A_L)_E = E \oplus \ldots \oplus E$, y concluimos que A es separable por el teorema de caracterización.

Propiedades de las Extensiones Separables:

1. *La condición necesaria y suficiente para que dos extensiones finitas $k \to L_1$ y $L_1 \to L_2$ sean separables es que lo sea $k \to L_2$.*
2. *Si $k \to L_1$ y $k \to L_2$ son extensiones separables, cualquier compuesto L_1L_2 es una extensión separable de k.*
3. *Si $k \to L$ es una extensión separable, cualquier compuesto LE de L con una extensión E de k es una extensión separable de E.*

Demostración: 1. Si $k \to L_2$ es separable, también lo es $k \to L_1$, porque L_1 es una subálgebra de L_2, y $L_1 \to L_2$ es separable porque, para toda extensión E de L_1 se tiene que $L_2 \otimes_{L_1} E$ es un cociente de $L_1 \otimes_k E$; luego es reducida.

Recíprocamente, si las extensiones finitas $K \to L_1$ y $L_1 \to L_2$ son separables, para toda extensión $k \to E$ tenemos que $L_1 \otimes_k E$ es reducida; luego descompone en suma directa de cuerpos, $(L_1)_E = K_1 \oplus \ldots \oplus K_n$, que son extensiones de L_1, y concluimos que

$$L_2 \otimes_k E = L_2 \otimes_{L_1} (L_1 \otimes_k E) = (L_2 \otimes_{L_1} K_1) \oplus \ldots \oplus (L_2 \otimes_{L_1} K_n)$$

es reducida, porque es suma directa de álgebras reducidas, al ser L_2 separable sobre L_1. Es decir, la extensión $k \to L_2$ es separable.

2. Cualquier compuesto L_1L_2 es separable sobre k porque es un cociente de $L_1 \otimes_k L_2$, que es una k-álgebra finita separable.

3. Cualquier compuesto LE es separable sobre E porque es un cociente de $L \otimes_k E$, que es una E-álgebra finita separable.

Construcción de las Álgebras Separables

Teorema G.4.1 *Sea k un cuerpo infinito. Toda k-álgebra finita separable es isomorfa a $k[x]/(p(x))$ para algún polinomio separable $p(x)$,*

Demostración: Sea A una k-álgebra finita separable de grado d y sea $k \to L$ una extensión que la trivialice, de modo que existen d puntos $\phi_1, \ldots, \phi_d \colon A \to L$. Para cada par de índices $i \neq j$, los elementos $a \in A$ tales que $\phi_i(a) = \phi_j(a)$ forman un subespacio vectorial propio de A, así que el siguiente lema afirma la existencia de algún $a \in A$ tal que los morfismos $\phi_1, \ldots, \phi_d \colon k[a] \to L$ son distintos entre sí.

Como el grado acota el número de puntos, el grado de $k[a]$ es $\geq d$ y obtenemos que $A = k[a]$. Concluimos al observar que $k[a] \simeq k[x]/(p(x))$, donde $p(x)$ denota el generador del núcleo del morfismo $k[x] \to A$, $q(x) \mapsto q(a)$.

Lema G.4.2 *Si k es un cuerpo infinito, ningún k-espacio vectorial es unión de un número finito de subespacios vectoriales propios.*

Demostración: Si un espacio vectorial E sobre un cuerpo k es unión finita de subespacios vectoriales propios, $E = V_1 \cup \ldots \cup V_n$, podemos suponer que $V_2 \cup \ldots \cup V_n \neq E$, de modo que existe algún vector $e_1 \in V_1$ que no está en $V_2 \cup \ldots \cup V_n$ y algún vector $e_2 \in V_2 \cup \ldots \cup V_n$ que no está en V_1. Ahora, para cada índice i, a lo sumo puede existir un escalar $\lambda \in k$ tal que $\lambda e_1 + e_2 \in V_i$; luego el cardinal de k está acotado por n y concluimos que el cuerpo k es finito.

Teorema del Elemento Primitivo: *Si $k \to L$ es una extensión finita y separable, existe algún $\alpha \in L$ tal que $L = k(\alpha)$.*

Demostración: Si el cuerpo k es infinito, es un caso particular del teorema anterior. Si k es finito, también L es un cuerpo finito y el siguiente lema afirma que el grupo multiplicativo $L^* = L - \{0\}$ es cíclico. Si α es un generador de L^*, todo elemento no nulo de L es una potencia de α, y en particular $L = k(\alpha)$.

Lema G.4.3 *Si k es un cuerpo, todo subgrupo finito del grupo multiplicativo k^* es cíclico.*

Demostración: Sea G un subgrupo finito de k^*, de modo que G es un grupo abeliano finito. Si n es el anulador de G, tenemos que $a^n = 1$ para todo $a \in G$; así que todos los elementos de G son raíces del polinomio $x^n - 1$ y se sigue que el orden de G está acotado por n. Como el orden de un grupo abeliano es múltiplo del anulador, el orden de G es n y el teorema de clasificación de grupos abelianos finitos permite concluir que G es un grupo cíclico.

Cuerpos Perfectos

Definición: Diremos que un elemento a de una k-álgebra finita A es **separable** cuando lo sea la subálgebra $k[a]$ que genera en A.

Teorema G.4.4 *La condición necesaria y suficiente para que una k-álgebra finita A sea separable es que lo sean todos sus elementos.*

Demostración: La necesidad es obvia porque $k[a]$ es una subálgebra de A.

Recíprocamente, si todos los elementos de A son separables, consideramos un sistema finito de generadores, $A = k[a_1, \ldots, a_r]$, de modo que el morfismo natural

$$k[a_1] \otimes_k \ldots \otimes_k k[a_r] \longrightarrow A$$

es epiyectivo. Luego A es separable, porque es isomorfa a un cociente de un producto tensorial de álgebras separables.

Definición: Diremos que un cuerpo k es **perfecto** si todas sus extensiones finitas son separables; es decir, si todas la k-álgebras finitas reducidas son separables.

Lema G.4.5 *La condición necesaria y suficiente para que un cuerpo k sea perfecto es que todos los polinomios irreducibles en $k[x]$ sean separables.*

Demostración: Si α es un elemento de una extensión finita de k, tenemos que $k(\alpha) \simeq k[x](p_\alpha(x))$. Luego k es perfecto si y sólo si todos los elementos de las extensiones finitas de k son separables, y el teorema anterior permite concluir.

Teorema G.4.6 *Todo cuerpo de característica nula es perfecto.*

Demostración: 4.3.5.

Definición: Si la característica de un anillo A es un número primo p, de acuerdo con 4.3.9 la aplicación $F\colon A \to A$, $F(a) = a^p$, es un morfismo de anillos, llamado **morfismo de Frobënius** (1849–1917) del anillo A.

Lema G.4.7 *Un cuerpo k de característica positiva p es perfecto precisamente cuando el morfismo de Frobënius $F\colon k \to k$, $F(a) = a^p$, es epiyectivo.*

Demostración: Si k es perfecto y $a \in k$, entonces el polinomio $x^p - a$ no puede ser irreducible en $k[x]$ porque su derivada es nula. Si α es una raíz de este polinomio en una extensión de k, tenemos que $(x-\alpha)^p = x^p - \alpha^p = x^p - a$, así que algún factor $(x-\alpha)^m$, $0 < m < p$, ha de tener todos sus coeficientes en k. Como

$$(x-\alpha)^m = x^m - m\alpha x^{m-1} + \ldots \in k[x]$$

y $m \neq 0$ en k, concluimos que $\alpha \in k$. Luego $a = F(\alpha)$ y F es epiyectivo.

Recíprocamente, si F es epiyectivo y $p(x) = \sum_i a_i x^i \in k[x]$ tiene derivada nula, entonces

$$p(x) = \textstyle\sum_i a_{ip} x^{ip} = \sum_i b_i^p x^{ip} = \left(\sum_i b_i x^i\right)^p$$

donde $a_{ip} = F(b_i)$, y concluimos que $p(x)$ no es irreducible. Luego k es un cuerpo perfecto.

Teorema G.4.8 *Todos los cuerpos finitos son perfectos.*

Demostración: El morfismo de Frobënius $F\colon k \to k$ siempre es inyectivo, porque es un morfismo de anillos y k es un cuerpo; luego es epiyectivo cuando el cardinal de k es finito.

Apéndice H

Teoría de Galois

En este apéndice k denotará un cuerpo arbitrario, y usaremos sin mención previa el hecho de que si $\tau\colon L \to E$ es un morfismo de k-álgebras entre dos extensiones de k y $\alpha \in L$ es raíz de un polinomio $\sum_i a_i x^i \in k[x]$, entonces $\tau(\alpha)$ también es raíz del mismo polinomio:

$$\textstyle\sum_i a_i\, \tau(\alpha)^i \;=\; \sum_i a_i \tau(\alpha^i) \;=\; \tau\big(\sum_i a_i \alpha^i\big) \;=\; 0\ .$$

H.1 Extensiones de Galois

Definición: Sea $p(x)$ un polinomio no constante con coeficientes en k. Diremos que una extensión finita $k \to L$ es un **cuerpo de descomposición** de $p(x)$ sobre k si $p(x)$ tiene todas sus raíces en la extensión L y éstas la generan; es decir, cuando $L = k(\alpha_1, \ldots, \alpha_n)$ y $p(x) = (x-\alpha_1)^{m_1} \ldots (x-\alpha_n)^{m_n}$.

El cuerpo de descomposición de un polinomio $p(x)$ siempre existe, pues basta tomar la extensión de k generada por las raíces de $p(x)$ en una extensión donde éste tenga todas sus raíces (existe en virtud de 4.4.3). Así, por ejemplo, cuando $k = \mathbb{Q}$, un cuerpo de descomposición de $p(x) \in \mathbb{Q}[x]$ es la extensión $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son todas las raíces complejas de $p(x)$.

Lema del Hueco Único: *Sean L y L' dos cuerpos de descomposición de un polinomio no constante $p(x) \in k[x]$. Dos morfismos de k-álgebras cualesquiera $j : L \to E$, $j' : L' \to E$ en una extensión E de k tienen la misma imagen.*

En particular, L y L' son extensiones de k isomorfas.

Demostración: Tanto $j(L)$ como $j'(L')$ son subcuerpos de E donde $p(x)$ tiene todas sus raíces y están generados sobre k por raíces de $p(x)$; luego ambos coinciden con el subcuerpo de E generado sobre k por todas las raíces de $p(x)$ en E.

Por último, como siempre existe tal extensión común, por ejemplo $E = (L' \otimes_k L)/\mathfrak{m}$, se sigue que $L \simeq j(L) = j'(L') \simeq L'$ y concluimos que L y L' son extensiones de k isomorfas.

Definición: Diremos que una extensión finita $k \to L$ es de **Galois** (1811-1832) cuando el orden de su grupo de automorfismos $\mathrm{Aut}(L/k) := \mathrm{Aut}_{k\text{-alg}}(L, L)$ coincida con el grado de la extensión:

$$|G| \;=\; [L : k]$$

lo que, de acuerdo con G.3.3, equivale a que la L-álgebra $L \otimes_k L$ sea trivial

$$L \otimes_k L \;=\; L \oplus \ldots \oplus L \;,$$

En tal caso diremos que $G = \mathrm{Aut}(L/k) = \mathrm{Hom}_{k\text{-alg}}(L, L)$ es el **grupo de Galois** de L sobre k.

Caracterización de las Extensiones de Galois: *Si $k \to L$ es una extensión finita separable, las siguientes condiciones son equivalentes:*

1. *L es el cuerpo de descomposición de algún polinomio con coeficientes en k.*
2. *Todo compuesto de L consigo mismo es isomorfo a L.*
3. *L es una extensión de Galois: $L \otimes_k L = \oplus L$.*
4. *Todo polinomio irreducible en $k[x]$ que tenga alguna raíz en L tiene todas sus raíces en L.*

Demostración: $(1 \Rightarrow 2)$ Es un caso particular del lema del hueco único, cuando $L' = L$.

$(2 \Rightarrow 3)$ El cuerpo residual $\kappa(x)$ de cualquier punto x del espectro de $L \otimes_k L$ es un compuesto de L consigo mismo, así que $\kappa(x) = L$ por hipótesis, y concluimos que $L \otimes_k L$ es una L-álgebra racional. Como L es una extensión separable, concluimos que $L \otimes_k L$ es trivial.

$(3 \Rightarrow 4)$ Si un polinomio irreducible $p(x) \in k[x]$ tiene una raíz α en L, ésta define un morfismo de k-álgebras

$$k[x]/(p(x)) \;\xrightarrow{x=\alpha}\; L$$

que necesariamente es inyectivo, porque $k[x]/(p(x))$ es un cuerpo. Por hipótesis, L es trivial sobre L, así que $k[x]/(p(x))$ también es trivial sobre L, lo que significa que $p(x)$ tiene todas sus raíces en L.

$(4 \Rightarrow 1)$ Sea $L = k(\alpha_1, \ldots, \alpha_r)$ y sea $p_i(x) \in k[x]$ el polinomio anulador de α_i, donde $i = 1, \ldots, r$. Éstos polinomios $p_i(x)$ son irreducibles, porque L es un

cuerpo, y tienen alguna raíz en L; luego, por hipótesis, tienen todas sus raíces en L. Concluimos que el polinomio $p(x) = p_1(x) \dots p_r(x) \in k[x]$ tiene todas sus raíces en L y éstas generan L; i.e., L es el cuerpo de descomposición de $p(x)$ sobre k.

Ejemplo: El cuerpo de descomposición $L = k(\alpha_1, \dots, \alpha_n)$ de cualquier polinomio separable $p(x) \in k[x]$ es una extensión separable de k, pues claramente tenemos un morfismo epiyectivo $k[x]/(p(x)) \otimes_k \dots \otimes_k k[x]/(p(x)) \to k(\alpha_1, \dots, \alpha_n)$; luego L es una extensión de Galois de k.

Si un cuerpo k es perfecto, el cuerpo de descomposición de cualquier polinomio con coeficientes en k es una extensión de Galois de k.

Definición: Llamaremos **grupo de Galois** sobre k de un polinomio separable $p(x) \in k[x]$ al grupo de Galois G de su cuerpo de descomposición L sobre k:

$$\boxed{G \,=\, \mathrm{Aut}(L/k) \,=\, \mathrm{Hom}_{k\text{-alg}}(L, L)}$$

En virtud del teorema del hueco único, tal grupo no depende, salvo isomorfismos, del cuerpo de descomposición L elegido. Además, cada automorfismo $\tau \in G$ permuta las raíces $\alpha_1, \dots \alpha_n$ de $p(x)$ en L, y está totalmente determinado por tal permutación porque $L = k(\alpha_1, \dots \alpha_n)$. Es decir, *el grupo de Galois de un polinomio $p(x)$ es, de modo canónico, un subgrupo de permutaciones de las raíces de $p(x)$ en su cuerpo de descomposición.*

Toda vez que se numeren las raíces de $p(x)$ en L, el grupo de Galois G puede entenderse como un subgrupo del grupo simétrico S_n, bien definido salvo conjugación. Además, por ser $p(x)$ un polinomio separable, las raíces $\alpha_1, \dots \alpha_n$ de $p(x)$ en L son todas simples, así que su número n coincide con el grado de $p(x)$:

$$G \;\subseteq\; S_n \qquad\qquad n = \mathrm{grad}\, p(x)$$

Propiedades de las Extensiones de Galois: *Sea $k \to L$ una extensión de Galois.*

1. *L es una extensión de Galois de cualquier cuerpo intermedio $k \to L' \to L$.*
2. *Si $k \to E$ es una extensión arbitraria, cualquier compuesto LE es una extensión de Galois de E.*
3. *Si L' es una extensión de Galois de k, cualquier compuesto $L'L$ es una extensión de Galois de k.*

Demostración: Estas propiedades se siguen de las propiedades de las extensiones separables, pues si L es el cuerpo de descomposición sobre k de un polinomio $p(x) \in k[x]$, entonces:

1. L es el cuerpo de descomposición de $p(x)$ sobre L'.

2. LE es el cuerpo de descomposición de $p(x)$ sobre E.

3. Si L' es el cuerpo de descomposición de $q(x) \in k[x]$ sobre k, entonces LL' es el cuerpo de descomposición de $p(x)q(x)$ sobre k.

Ejemplo: De acuerdo con el teorema de D'Alembert, todo polinomio con coeficientes complejos $p(x)$ tiene todas sus raíces complejas. Luego su cuerpo de descomposición sobre $\mathbb{C}$ es $L = \mathbb{C}$, así que el grupo de Galois sobre $\mathbb{C}$ de cualquier polinomio con coeficientes complejos es trivial: $G = 1$.

Si un polinomio con coeficientes reales tiene todas sus raíces reales, entonces su cuerpo de descomposición sobre $\mathbb{R}$ es $L = \mathbb{R}$, y su grupo de Galois sobre $\mathbb{R}$ es trivial: $G = 1$. Por el contrario, si tiene alguna raíz imaginaria, su cuerpo de descomposición sobre $\mathbb{R}$ es $L = \mathbb{C}$, y su grupo de Galois es cíclico de orden 2; i.e., $G = \{\mathrm{id}, \tau\}$, donde τ denota la conjugación compleja.

Grupo de Galois de las ecuaciones cuadráticas:

Sea $p_2(x) = ax^2 + bx + c \in k[x]$ un polinomio separable de grado 2 y denotemos $\alpha_1,\ \alpha_2 = -\alpha_1 - b/a$ sus dos raíces en su cuerpo de descomposición L.

Si $p_2(x)$ tiene alguna raíz en k, entonces tiene las dos raíces en k; luego $L = k$ y su grupo de Galois sobre k es $G = \{\mathrm{id}\}$.

Si $p_2(x)$ no tiene raíces en k, entonces es irreducible en $k[x]$ y su cuerpo de descomposición $L = k(\alpha_1, \alpha_2) = k(\alpha_1) = k(\alpha_2)$ es una extensión de grado 2 de k. Además, existe un automorfismo $k(\alpha_1) \simeq k[x]/(p_2(x)) \simeq k(\alpha_2)$ que transforma α_1 en α_2, y concluimos que su grupo de Galois sobre k es $G = S_2$.

Ejemplo H.1.1 El cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^4 - 2$ es $L = \mathbb{Q}(\sqrt[4]{2}, i)$. El grado de $\mathbb{Q}(\sqrt[4]{2})$ sobre $\mathbb{Q}$ es 4 porque $x^4 - 2$ es irreducible en $\mathbb{Q}[x]$, y el grado de L sobre $\mathbb{Q}(\sqrt[4]{2})$ es 2 porque x^2+1 no tiene raíces en $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. Luego $[L : \mathbb{Q}] = 8$ y el grupo de Galois G de $x^4 - 2$ sobre $\mathbb{Q}$ es de orden 8.

Si $\tau \in G$, entonces $\tau(\sqrt[4]{2}) = \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ y $\tau(i) = \pm i$; luego éstas 8 posibilidades son todos los elementos de G. Los 8 automorfismos τ_i, $1 \le i \le 8$, de L son

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Las raíces complejas $\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$ de $x^4 - 2$ son los vértices de un cuadrado, $\gamma := \tau_2$ es el giro de ángulo recto y $\sigma := \tau_5$ es la simetría respecto del eje horizontal. Como esos dos movimientos generan las 8 simetrías del cuadrado, el grupo de Galois es el grupo de simetrías de un cuadrado:

$$G = \{id,\ \gamma,\ \gamma^2,\ \gamma^3,\ \sigma,\ \sigma\gamma,\ \sigma\gamma^2,\ \sigma\gamma^3\} \quad , \quad \gamma^4 = \sigma^2 = id,\ \gamma\sigma = \sigma\gamma^3$$
$$G = \{id,\ (1234),\ (13)(24),\ (1432),\ (24),\ (14)(23),\ (13),\ (12)(34)\}$$

H.2 Teorema de Galois

Lema H.2.1 *Si G es un grupo de automorfismos de un cuerpo L, entonces $L^G := \{\alpha \in L\colon\ \tau(\alpha) = \alpha\,,\ \forall \tau \in G\,\}$ es un cuerpo.*

Demostración: Si $\alpha, \beta \in L^G$, para todo $\tau \in G$ tenemos que $\tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta) = \alpha + \beta$, $\tau(\alpha\beta) = \tau(\alpha)\tau(\beta) = \alpha\beta$, y $\tau(\alpha^{-1}) = \tau(\alpha)^{-1} = \alpha^{-1}$.

Teorema H.2.2 *Si $k \to L$ es una extensión de Galois de grupo $G = \mathrm{Aut}(L/k)$, entonces $k = L^G$.*

Demostración: Como los elementos de G son automorfismos de L sobre L^G, de acuerdo con la fórmula de los puntos el orden de G está acotado por el grado de L sobre L^G. Por otra parte, al ser L una extensión de Galois de k, el orden de G coincide con el grado de L sobre k. Como $[L : k] = [L : L^G] \cdot [L^G : k]$, se sigue que $[L^G : k] = 1$ y concluimos que $L^G = k$.

Corolario H.2.3 *Sea $k \to L$ una extensión de Galois de grupo G. La órbita de cada elemento $\alpha \in L$ bajo la acción de G está formada por todas las raíces del polinomio irreducible de α sobre k, y su cardinal es el grado de $k(\alpha)$ sobre k.*

Demostración: Sea $q(x)$ el polinomio irreducible de α sobre k. La órbita de α está formada por raíces de $q(x)$, porque $q(\tau\alpha) = 0$ para todo $\tau \in G$. Por otra parte, de acuerdo con el teorema anterior, el polinomio

$$\prod_{\tau \in G} (x - \tau\alpha)$$

tiene todos sus coeficientes en k, pues claramente son invariantes por la acción de G. Como este polinomio tiene en común con el polinomio irreducible $q(x)$ la raíz $x = \alpha$, se sigue que este polinomio es múltiplo de $q(x)$, y concluimos que las raíces de $q(x)$ en L forman la órbita $G\alpha$.

Por último, como $q(x)$ es separable y tiene todas sus raíces en L, el número de tales raíces es su grado, que es $[k(\alpha) : k]$ por 4.4.2.

Corolario H.2.4 *Sea $p(x) \in k[x]$ un polinomio separable, y sea G su grupo de Galois sobre k. Las órbitas de la acción de G en las raíces de $p(x)$ están formadas por las raíces de los factores irreducibles de $p(x)$ en $k[x]$.*

En particular, el orden del grupo de Galois G es múltiplo de los grados de los factores irreducibles de $p(x)$.

Corolario H.2.5 *El grupo de Galois de cualquier polinomio irreducible actúa transitivamente sobre las raíces, y su orden es múltiplo del grado del polinomio.*

Corolario H.2.6 *Sea k un cuerpo de característica distinta de 2 y sea $p(x) \in k[x]$ un polinomio separable de grado n. La condición necesaria y suficiente para que el grupo de Galois G de $p(x)$ sobre k esté contenido en el grupo alternado A_n es que el discriminante Δ de $p(x)$ sea un cuadrado en k:*

$$G \subseteq A_n \;\Leftrightarrow\; \sqrt{\Delta} \in k$$

Demostración: Sea σ una permutación de las raíces de $p(x)$. Por definición del signo de una permutación, tenemos que $\sigma\sqrt{\Delta} = (\operatorname{sgn}\sigma)\sqrt{\Delta}$. Por tanto, cuando $-1 \neq 1$ en k, tenemos que $\sigma\sqrt{\Delta} = \sqrt{\Delta}$ si y sólo si σ es una permutación par.

Si $G \subseteq A_n$, se sigue que $\tau\sqrt{\Delta} = \sqrt{\Delta}$ para todo automorfismo $\tau \in G$, y el teorema anterior permite concluir que $\sqrt{\Delta} \in k$.

Recíprocamente, si $\sqrt{\Delta} \in k$, entonces $\tau\sqrt{\Delta} = \sqrt{\Delta}$ para todo $\tau \in G$, y concluimos que todo automorfismo $\tau \in G$ define una permutación par de las raíces de $p(x)$; es decir, $\tau \in A_n$.

Corolario H.2.7 (Grupo de Galois de las cúbicas) *Sea G el grupo de Galois de una cúbica $x^3 + px^2 + qx + r$ irreducible y separable sobre un cuerpo k de característica distinta de 2.*

Si el discriminante $\Delta = -4p^3r - 27r^2 + 18pqr - 4q^3 + p^2q^2$ es un cuadrado en k, entonces $G = A_3$.

Si el discriminante Δ no es un cuadrado en k, entonces $G = S_3$.

Demostración: Los únicos subgrupos de S_3 cuyo orden es múltiplo de 3 son A_3 y S_3, y el corolario anterior muestra que el discriminante del polinomio permite distinguir entre ambos casos.

Ejemplo: El grupo de Galois de $x^3 - x + 1$ sobre $\mathbb{Q}$ es el grupo simétrico S_3, porque no tiene raíces racionales y $\Delta = -27 + 4 = -23$ no es un cuadrado en $\mathbb{Q}$. El grupo de Galois de $x^3 - 3x + 1$ sobre $\mathbb{Q}$ es el grupo alternado A_3, porque no tiene raíces racionales y $\Delta = -27 + 108 = 81$ es un cuadrado en $\mathbb{Q}$.

H.2.8 (Grupo de Galois del Polinomio Genérico) Sean $s_1, \ldots, s_n$ las funciones simétricas elementales en n indeterminadas $x_1 \ldots, x_n$. La extensión

$$k(s_1, \ldots, s_n) \;\longrightarrow\; k(x_1, \ldots, x_n)$$

es de Galois porque es el cuerpo de descomposición del polinomio

$$x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n \;=\; \prod_{i=1}^{n} (x - x_i)$$

que es separable, pues obviamente tiene todas sus raíces distintas. Además, cualquier permutación de sus raíces $x_1, \ldots, x_n$ define un automorfismo del cuerpo

$k(x_1,\ldots,x_n)$ que es la identidad sobre $k(s_1,\ldots,s_n)$. Luego el grupo de Galois de esta extensión de Galois es todo el grupo simétrico S_n, y el teorema anterior afirma que toda función racional simétrica es función racional de las funciones simétricas elementales:

$$k(x_1,\ldots,x_n)^{S_n} \;=\; k(s_1,\ldots,s_n)$$

Además, este polinomio $x^n - s_1x^{n-1} + \ldots + (-1)^n s_n$ es el polinomio unitario genérico de grado n con coeficientes en k, porque las funciones simétricas elementales son algebraicamente independientes (A.1.1). *El polinomio genérico de grado n con coeficientes en cualquier cuerpo k es separable y su grupo de Galois es el grupo simétrico S_n.*

Como el grupo S_n actúa transitivamente en las raíces del polinomio genérico, obtenemos otra demostración de que éste es irreducible (A.4.1).

Teorema de Artin (1898-1962)**:** *Si G es un grupo finito de automorfismos de un cuerpo L, entonces L es una extensión de Galois de L^G y su grupo de Galois es G.*

Demostración: Si vemos que $[L : L^G] \leq |G|$, entonces G.3.3 permite concluir que L es una extensión de Galois de L^G y que $G = \mathrm{Aut}(L/L^G)$.

Si $\alpha \in L$, pondremos $\phi(\alpha) = (\tau(\alpha))_{\tau\in G} \in \oplus_G L$. Veamos que toda familia $\alpha_1,\ldots,\alpha_m \in L$, donde $m > |G|$, es linealmente dependiente sobre L^G. Si n es el primer índice tal que $\phi(\alpha_1),\ldots,\phi(\alpha_{n+1})$ son L-linealmente dependientes, existe una única relación de dependencia lineal $\phi(\alpha_{n+1}) = \lambda_1\phi(\alpha_1) + \ldots + \lambda_n\phi(\alpha_n)$, $\lambda_i \in L$:

$$\tau(\alpha_{n+1}) = \lambda_1\tau(\alpha_1) + \ldots + \lambda_n\tau(\alpha_n) \quad , \quad \forall\tau \in G$$

Aplicando $\sigma \in G$ obtenemos que

$$(\sigma\tau)(\alpha_{n+1}) = \sigma(\lambda_1)(\sigma\tau)(\alpha_1) + \ldots + \sigma(\lambda_n)(\sigma\tau)(\alpha_n) \quad , \quad \forall\tau \in G$$

y la unicidad de la relación de dependencia lineal muestra que $\sigma(\lambda_i) = \lambda_i$ para todo índice i y todo $\sigma \in G$. Luego $\alpha_{n+1} = \sum_i \lambda_i\alpha_i$ donde $\lambda_i \in L^G$, y concluimos que la familia dada es linealmente dependiente sobre L^G.

Teorema de Galois (según Artin)**:** *Sea $k \to L$ una extensión finita de Galois y sea $G = \mathrm{Aut}(L/k)$ su grupo de Galois. Si a cada subgrupo H de G le asignamos el cuerpo intermedio L^H, obtenemos una correspondencia biunívoca*

$$\begin{bmatrix}\text{Subgrupos}\\ \text{de } G\end{bmatrix} \longrightarrow \begin{bmatrix}\text{Cuerpos intermedios}\\ \text{entre } k \text{ y } L\end{bmatrix}$$

que invierte inclusiones. La correspondencia inversa asigna a cada cuerpo intermedio L' el grupo de Galois $\mathrm{Aut}(L/L')$ de L sobre L', y tenemos que

$$[L : L^H] \;=\; |H| \qquad , \qquad [L^H : k] \;=\; [G : H]$$

Además, L^H es una extensión de Galois de k si y sólo si H es un subgrupo normal de G, en cuyo caso el grupo de Galois de L^H sobre k es isomorfo a G/H.

Demostración: Las correspondencias $H \mapsto L^H$ y $L' \mapsto \mathrm{Aut}(L/L')$ claramente invierten inclusiones y, para probar que son mutuamente inversas, hemos de ver que $H = \mathrm{Aut}(L/L^H)$ para todo subgrupo H de G y que $L' = L^{\mathrm{Aut}(L/L')}$ para todo cuerpo intermedio L'.

La igualdad $L' = L^{\mathrm{Aut}(L/L')}$ se sigue del teorema H.2.2, porque $L' \to L$ es una extensión de Galois y su grupo de Galois es $\mathrm{Aut}(L/L')$.

La igualdad $H = \mathrm{Aut}(L/L^H)$ es consecuencia del teorema de Artin, que afirma que H es el grupo de Galois de la extensión $L^H \to L$.

La igualdad $|H| = [L : L^H]$ se debe a que, por el teorema de Artin, L es una extensión de Galois de grupo H y a que el número de automorfismos de cualquier extensión de Galois coincide con el grado. Ahora,

$$|G| \;=\; [L:k] \;=\; [L:L^H]\cdot[L^H:k] \;=\; |H|\cdot[L^H;k]$$

y obtenemos que $[L^H : k] = |G|/|H| = [G : H]$.

Por último, es sencillo comprobar que para todo subgrupo H de G y todo automorfismo $\tau \in G$ tenemos que

$$L^{\tau H\tau^{-1}} \;=\; \tau(L^H)\ .$$

Ahora, si L^H es una extensión de Galois de k, el lema del hueco único asegura que $L^H = \tau(L^H)$; luego $L^H = L^{\tau H\tau^{-1}}$ y concluimos que $H = \tau H\tau^{-1}$ para todo $\tau \in G$. Es decir, el subgrupo H es normal en G.

Recíprocamente, si H es normal en G, entonces $\tau(L^H) = L^{\tau H\tau^{-1}} = L^H$ para todo $\tau \in G$. Es decir, cada automorfismo de L induce, por restricción, un automorfismo de L^H, obteniendo así un morfismo de grupos

$$G = \mathrm{Aut}(L/k) \;\longrightarrow\; \mathrm{Aut}(L^H/k)$$

cuyo núcleo es H en virtud del teorema de Artin. Luego el grupo cociente G/H es isomorfo a la imagen, que es un subgrupo de $\mathrm{Aut}(L^H/k)$. Como ya sabemos que el orden de G/H coincide con el grado de L^H sobre k, concluimos que el número de automorfismos de la extensión $k \to L^H$ es mayor o igual que el grado: es una extensión de Galois y su grupo de Galois $\mathrm{Aut}(L^H/k)$ es isomorfo a G/H.

Teorema de los Irracionales Naturales: *Sea $k \to L$ una extensión finita de Galois de grupo $G = \mathrm{Aut}(L/k)$. Si $k \to E$ es una extensión arbitraria, cualquier compuesto $E \to EL$ es una extensión finita de Galois y su grupo es isomorfo al grupo de Galois de L sobre $L \cap E$:*

$$\mathrm{Aut}(EL/E) \;=\; \mathrm{Aut}(L/L\cap E)\ .$$

Demostración: Ya sabemos que EL es una extensión de Galois de E. Sea $G' = \mathrm{Aut}(EL/E)$ su grupo de Galois. Por el Lema del Hueco único, tenemos que $\tau(L) = L$ para todo $\tau \in G'$, así que la restricción de automorfismos define un morfismo de grupos $G' \hookrightarrow G$, que es inyectivo porque los elementos de L generan EL sobre E. Por el Teorema de Galois, para concluir basta observar que

$$L^{G'} \;=\; L \cap (EL)^{G'} \;=\; L \cap E \;.$$

La Equivalencia de Galois

Dada una extensión de Galois $k \to L$ de grupo G, el teorema de Galois (1811-1832) determina los cuerpos intermedios a partir del grupo G. Luego determina, salvo isomorfismos, las extensiones finitas de k triviales sobre L, pues tales extensiones admiten algún morfismo en L (necesariamente inyectivo) y son por tanto isomorfas a algún cuerpo intermedio entre k y L. Más en general, como toda k-álgebras finita A trivial sobre L descompone en suma directa de extensiones triviales sobre L, vemos que el teorema de Galois determina las k-álgebras finitas triviales sobre L, pues nos muestra que son de la forma

$$A \;=\; L^{H_1} \oplus \ldots \oplus L^{H_r}$$

donde $H_1, \ldots, H_r$ son subgrupos de G. Ahora bien, las k-álgebras finitas triviales sobre L forman evidentemente una categoría, y determinar una categoría, más que dar sus objetos, es dar sus morfismos. Vamos a completar ahora el teorema de Galois, exponiendo su comprensión por Grothendieck (n. 1928) como equivalencia de categorías.

Teorema H.2.9 *Si G es un grupo de automorfismos de una k-álgebra A, entonces el álgebra de invariantes es estable por cambios de base. Es decir, para toda k-álgebra B tenemos*

$$A^G \otimes_k B \;=\; (A \otimes_k B)^G$$

donde G actúa en $A \otimes_k B$ mediante su acción por la izquierda:

$$g(a \otimes b) := (ga) \otimes b \;.$$

Demostración: Si $\{e_i\}_{i \in I}$ es una base de B como k-espacio vectorial, tenemos que

$$(A \otimes_k B)^G = \big(\oplus_i (A \otimes_k ke_i)\big)^G = \oplus_i (A \otimes_k ke_i)^G = \oplus_i (A^G \otimes_k ke_i) = A^G \otimes_k B$$

q.e.d.

Si A es una k-álgebra finita trivial sobre L, el grupo de Galois $G = \mathrm{Aut}(L/k)$ actúa de modo natural sobre el conjunto

$$P(A) \;=\; \mathrm{Hom}_{k\text{-alg}}(A, L)$$

de puntos de A con valores en L, donde la acción es: $\tau(p) := \tau \circ p$. De acuerdo con la fórmula de los puntos, al ser $A \otimes_k L$ una L-álgebra trivial tenemos que

$$A \otimes_k L \;=\; L \oplus \overset{P(A)}{\ldots} \oplus L \;=\; \mathrm{Hom}(P(A), L)$$

(donde Hom denota las aplicaciones de meros conjuntos) y este isomorfismo es compatible con las respectivas acciones de G, actuando en $A \otimes_k L$ por su acción sobre L y en $\mathrm{Hom}(P(A), L)$ del siguiente modo: $\tau \cdot f := \tau \circ f \circ \tau^{-1}$. Por tanto, éste G-conjunto $P(A)$ permite recuperar la k-álgebra inicial A porque

$$A = A \otimes_k L^G = (A \otimes_k L)^G = \big(\mathrm{Hom}(P(A), L)\big)^G = \mathrm{Hom}_G(P(A), L)$$

Por eso, a cada G-conjunto finito X le asociamos la k-álgebra finita

$$R(X) \;:=\; \big(\mathrm{Hom}(X, L)\big)^G \;=\; \mathrm{Hom}_G(X, L)$$

que es trivial sobre L, al ser una subálgebra de $\mathrm{Hom}(X, L) = \oplus_X L$.

Teorema de Galois (según Grothendieck)**:** *Si $k \to L$ es una extensión finita de Galois de grupo $G = \mathrm{Aut}(L/k)$, el funtor de puntos*

$$P : \begin{bmatrix} k\text{-álgebras finitas} \\ \text{triviales sobre } L \end{bmatrix} \rightsquigarrow \begin{bmatrix} G\text{-conjuntos} \\ \text{finitos} \end{bmatrix}$$

establece una equivalencia de la categoría (dual) de las k-álgebras finitas triviales sobre L con la categoría de G-conjuntos finitos, siendo R el funtor inverso.

En particular, si A y B son k-álgebras finitas triviales sobre L, el funtor de puntos P define una biyección

$$\mathrm{Hom}_{k\text{-alg}}(A; B) \;=\; \mathrm{Hom}_G(P(B), P(A))$$

Demostración: Sea A una k-álgebra finita trivial sobre la extensión L. Cada función $f \in A$ define de modo natural una aplicación $f\colon P(A) \to L$, $f(p) := p(f)$, que es claramente G-invariante:

$$(\tau f)(p) = \tau(f(\tau^{-1}p)) = \tau\left(\tau^{-1}p(f)\right) = p(f) = f(p)\ .$$

Obtenemos así un morfismo de k-álgebras $A \to R(P(A))$ que define una transformación natural $\mathrm{Id} \to R \circ P$, y vamos a ver que es un isomorfismo de funtores.

Por otra parte, si X es un conjunto finito, cada punto $p \in X$ define de modo natural un punto $p\colon R(X) = \mathrm{Hom}_G(X, L) \to L$, $p(f) := f(p)$. Esto define una aplicación $X \to P(R(X))$ que es un morfismo de G-conjuntos, pues $(\tau p)(f) = f(\tau p) = \tau(f(p))$. Obtenemos así una transformación natural $\mathrm{Id} \to P \circ R$ y vamos a ver que es un isomorfismo de funtores.

El funtor de puntos P transforma sumas directas en uniones disjuntas y el funtor R transforma uniones disjuntas en sumas directas,

$$P(A \oplus B) \;=\; P(A) \sqcup P(B) \qquad , \qquad R(X \sqcup Y) \;=\; R(X) \oplus R(Y)\ ,$$

así que es suficiente probar que $L' \to R(P(L'))$ es un isomorfismo para todo cuerpo intermedio L' (es decir, $L' = L^H$ para algún subgrupo H de G), y que $X \to P(R(X))$ es un isomorfismo cuando el G-conjunto finito X sólo tiene una órbita (es decir, $X = G/H$).

Ahora bien, el teorema de prolongación de morfismos que demostraremos a continuación prueba que $P(L^H) = G/H$, lo que permite concluir:

$$\begin{aligned} R(P(L^H)) \;&=\; \mathrm{Hom}_G(P(L^H), L) \;=\; \mathrm{Hom}_G(G/H, L) \;=\; L^H \\ P(R(G/H)) \;&=\; P(\mathrm{Hom}_G(G/H, L)) \;=\; P(L^H) \;=\; G/H \end{aligned}$$

Lema H.2.10 *Sea $j\colon A \to B$ un morfismo inyectivo de k-álgebras. Si B es una k-álgebra finita, entonces la aplicación continua inducida $\phi\colon \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ es epiyectiva.*

Demostración: Sea $a \in A$ una función que se anule en la imagen de ϕ. Entonces $j(a)$ se anula en todo $\mathrm{Spec}\, B$; luego es una función nilpotente, $0 = j(a)^n = j(a^n)$, según 7.2.7. Al ser j inyectivo, se sigue que $a^n = 0$, de modo que a es nilpotente y se anula en todo $\mathrm{Spec}\, A$. Es decir, la imagen de ϕ es densa en $\mathrm{Spec}\, A$ y, al ser éste un espacio discreto, concluimos que tal imagen coincide con $\mathrm{Spec}\, A$.

Teorema de Prolongación: *Sea A una k-álgebra finita racional sobre cierta extensión L de k. Si B es una subálgebra de A, todo morfismo de k-álgebras $B \to L$ es restricción de algún morfismo de k-álgebras $A \to L$.*

Demostración: Como B también es racional sobre L, la fórmula de los puntos afirma que $\mathrm{Hom}_{k\text{-alg}}(A, L) = \mathrm{Spec}\, A_L$ y $\mathrm{Hom}_{k\text{-alg}}(B, L) = \mathrm{Spec}\, B_L$. Ahora H.2.10 permite concluir que la aplicación

$$\mathrm{Hom}_{k\text{-alg}}(A, L) = \mathrm{Spec}\, A_L \longrightarrow \mathrm{Spec}\, B_L = \mathrm{Hom}_{k\text{-alg}}(B, L)$$

es epiyectiva, y es sencillo comprobar que transforma cada morfismo $A \to L$ en su restricción a B.

Corolario H.2.11 *Sea $k \to L$ una extensión normal. Si L' es un cuerpo intermedio, entonces el grupo $\mathrm{Aut}(L/k)$ actúa transitivamente en $\mathrm{Hom}_{k\text{-alg}}(L', L)$.*

Demostración: Sea $i\colon L' \to L$ el morfismo de inclusión. Si $j\colon L' \to L$ es otro morfismo de k-álgebras, por el teorema de prolongación existe existe algún automorfismo $\tau\colon L \to L$ tal que $j = \tau \circ i$.

H.3 Aplicaciones

Irracionales Cuadráticos

Lema H.3.1 *Sea $k \to L$ una extensión de grado 2. Si la característica de k no es 2, entonces $L = k(\alpha)$, donde $\alpha^2 \in k$.*

Demostración: Si $\beta \in L$ no está en k, entonces β es raíz de un polinomio x^2+bx+c con coeficientes en k, y la fórmula de las raíces de los polinomios de grado 2 (válida en característica distinta de 2) muestra que $L = k(\sqrt{b^2-4c}\,)$.

Teorema H.3.2 *La condición necesaria y suficiente para que un polinomio con coeficientes racionales $p(x)$ sea resoluble por radicales cuadráticos es que el orden del grupo de Galois de $p(x)$ sobre $\mathbb{Q}$ sea potencia de 2.*

Demostración: La necesidad de la condición es consecuencia de B.1.5, porque el orden del grupo de Galois coincide con el grado del cuerpo de descomposición.

Recíprocamente, si el orden del grupo de Galois G es potencia de 2, existe una sucesión de subgrupos

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots H_{n-1} \supset H_n = 1$$

tal que $|H_i| = 2^{n-i}$. Por el teorema de Galois estos subgrupos se corresponden con ciertos subcuerpos K_i de la extensión L de $\mathbb{Q}$ generada por las raíces complejas de $p(x)$:

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_{n-1} \subset K_n = L$$

tales que $[K_i : K_{i-1}] = 2$. Aplicando reiteradamente el lema anterior concluimos que $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ para todo índice $i = 1, \ldots, n$. Luego todas las raíces complejas de $p(x)$, al estar en L, son irracionales cuadráticos.

Corolario H.3.3 *La condición necesaria y suficiente para que $e^{\frac{2\pi i}{n}}$ sea un irracional cuadrático es que el indicador de Euler $\phi(n)$ sea potencia de 2.*

Demostración: La necesidad de la condición es B.4.2.

Recíprocamente, el cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(e^{\frac{2\pi i}{n}})$; luego, si $\phi(n) = [\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}]$ es potencia de 2, el teorema anterior permite concluir que $e^{\frac{2\pi i}{n}}$ es un irracional cuadrático.

Corolario H.3.4 *Un número complejo algebraico es irracional cuadrático si y sólo si el orden del grupo de Galois de su polinomio irreducible es potencia de 2.*

Demostración: De acuerdo con H.3.2, basta probar que si $\alpha \in \mathbb{C}$ es un irracional cuadrático, entonces toda raíz compleja β de su polinomio irreducible $p_\alpha(x)$ también es irracional cuadrático.

Por hipótesis $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_r) \subset \mathbb{C}$ donde $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ para todo $1 \leq i \leq r$. Consideremos un cuerpo $\mathbb{Q}(\alpha_1, \ldots, \alpha_r) \subset L \subset \mathbb{C}$ que sea extensión de Galois de $\mathbb{Q}$. De acuerdo con H.2.3, $\beta \in L$ y existe un automorfismo $\tau\colon L \to L$ tal que $\tau(\alpha) = \beta$; luego $\beta \in \mathbb{Q}(\tau\alpha_1, \ldots, \tau\alpha_r)$ donde $(\tau\alpha_i)^2 \in \mathbb{Q}(\tau\alpha_1, \ldots, \tau\alpha_{i-1})$ para todo $1 \leq i \leq r$, y concluimos que β es un irracional cuadrático.

Ejemplo: La teoría de Galois permite dar una nueva demostración del Teorema de D'Alembert. De acuerdo con el Teorema de Kronecker, basta probar que toda extensión finita L de $\mathbb{C}$ es trivial. Como toda extensión finita está contenida en el cuerpo de descomposición de algún polinomio, podemos suponer que L es una extensión de Galois de $\mathbb{R}$ de grupo G. Sea H un 2-subgrupo de Sylow de G, de modo que $[L^H : \mathbb{R}]$ es impar. Si $\alpha \in L^H$, entonces $\operatorname{gr} p_\alpha(x) = [\mathbb{R}(\alpha) : \mathbb{R}]$ divide a $[L^H : \mathbb{R}]$; luego es impar, y tiene alguna raíz real en virtud del Teorema de Bolzano, lo que permite concluir que α es real: $L^H = \mathbb{R}$ y $H = G$.

Se sigue que el orden del subgrupo $G' = \operatorname{Aut}(L/\mathbb{C}) \subset G$ es una potencia de 2. Si $G' \neq 1$, entonces tiene algún subgrupo de índice 2 que, por el Teorema de Galois, se corresponde con una extensión $\mathbb{C} \to K$ de grado 2. De acuerdo con H.3.1, tenemos que $K = \mathbb{C}(\alpha)$, donde $\alpha^2 \in \mathbb{C}$, lo que es absurdo porque todo número complejo tiene raíz cuadrada compleja. Luego $G' = 1$ y $\mathbb{C} = L$.

Raíces de la Unidad

Fijado un cuerpo k, para cada número natural $n \geq 2$ llamaremos raíces n-ésimas de la unidad a las raíces del polinomio $x^n - 1$ en su cuerpo de descomposición, y claramente forman un grupo abeliano multiplicativo que denotaremos μ_n, que es cíclico de acuerdo con G.4.3. Si n es múltiplo de la característica p de k, $n = pm$, entonces $x^n - 1 = (x^m - 1)^p$ y por tanto $\mu_n = \mu_m$. Por eso nos limitaremos al caso en que n es primo con p. En tal caso el polinomio $x^n - 1$ es separable, porque no tiene raíces comunes con su derivada nx^{n-1}, así que en su cuerpo de descomposición tiene n raíces distintas y concluimos que μ_n es un grupo cíclico de orden n. Los generadores de μ_n reciben el nombre de raíces n-ésimas de la unidad **primitivas** sobre el cuerpo k. Por tanto, si ε_n es una raíz n-ésima de la unidad primitiva, tendremos que

$$\mu_n \;=\; \{\varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^n = 1\}\ .$$

Teorema H.3.5 *Si ε_n es una raíz n-ésima de la unidad primitiva y n es primo con la característica de k, entonces $k \to k(\varepsilon_n)$ es una extensión de Galois y su grupo es un subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$. En particular su grado divide a $\phi(n)$.*

Demostración: $k(\varepsilon_n)$ es una extensión de Galois de k porque es el cuerpo de descomposición del polinomio separable $x^n - 1$, pues todas sus raíces son potencias de ε_n. Sea G su grupo de Galois.

Cada automorfismo $\tau \in G$ induce un automorfismo del grupo cíclico μ_n; luego transforma ε_n en otro generador ε_n^i, donde i es primo con n y está bien definido módulo n. Obtenemos así morfismo de grupos $G \to (\mathbb{Z}/n\mathbb{Z})^*$, $\tau \mapsto i$. Es inyectivo porque cada k-automorfismo de $k(\varepsilon_n)$ está determinado por su acción sobre ε_n.

Teorema H.3.6 *$\mathbb{Q}(e^{\frac{2\pi i}{n}})$ es una extensión de Galois de $\mathbb{Q}$ y su grupo es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$.*

Demostración: El grado de $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ sobre $\mathbb{Q}$ es $\phi(n)$ según B.4.2, y el teorema anterior permite concluir que su grupo de Galois es $(\mathbb{Z}/n\mathbb{Z})^*$.

Cuerpos Finitos

Sea k un cuerpo finito con q elementos.

Es claro que la característica p de k es positiva y que k es una extensión finita de $\mathbb{F}_p$. Si d es el grado de k sobre $\mathbb{F}_p$, entonces existe un isomorfismo $\mathbb{F}_p$–lineal entre k y $\mathbb{F}_p^d$ y concluimos que $q = p^d$. El cardinal de un cuerpo finito es una potencia de su característica.

Teorema H.3.7 *Sea $q = p^d$ una potencia de un número primo p. Salvo isomorfismos, existe un único cuerpo $\mathbb{F}_q$ con q elementos, que es el cuerpo de descomposición sobre $\mathbb{F}_p$ del polinomio $x^q - x$.*

Demostración: Sea k un cuerpo con q elementos. Los elementos no nulos de k forman un grupo multiplicativo de orden $q-1$, así que son raíces del polinomio $x^{q-1} - 1$ según 2.5.4, y todo elemento de k es raíz de $x^q - x$. Luego $x^q - x$ tiene todas sus raíces en k y k es el cuerpo de descomposición del polinomio $x^q - x$ sobre $\mathbb{F}_p$. En particular es único salvo isomorfismos.

Para demostrar la existencia de un cuerpo con q elementos observamos que el polinomio $x^q - x$ con coeficientes en $\mathbb{F}_p$ es separable porque es primo con su derivada (que es -1), de modo que tiene q raíces distintas en su cuerpo de descomposición k sobre $\mathbb{F}_p$. Además el automorfismo $F\colon k \to k$, $F(a) = a^q$, deja fijas todas las raíces de $x^q - x$; luego F es la identidad sobre k y se sigue que todos los elementos de k son raíces de $x^q - x$. Concluimos que k está formado por las raíces de $x^q - x$ y su cardinal es q.

Corolario H.3.8 *La condición necesaria y suficiente para que $\mathbb{F}_{q'}$ sea una extensión de $\mathbb{F}_q$ es que q' sea potencia de q.*

Demostración: Si $\mathbb{F}_{q'}$ es una extensión de $\mathbb{F}_q$ de grado d, entonces es un espacio vectorial de dimensión d sobre $\mathbb{F}_q$; luego su cardinal es $q' = q^d$.

Recíprocamente, si $q' = q^d$, entonces toda solución de la ecuación $x^q = x$ es solución de $x^{q'} = ((x^q)^q)^{\cdots q} = x$. Luego el cuerpo de descomposición $\mathbb{F}_{q'}$ de $x^{q'} - x$ sobre $\mathbb{F}_p$ contiene al cuerpo de descomposición $\mathbb{F}_q$ de $x^q - x$ sobre $\mathbb{F}_p$.

Corolario H.3.9 *En el anillo de polinomios $\mathbb{F}_q[x]$ hay polinomios irreducibles de grado arbitrario.*

Demostración: Sea $d \geq 1$ un número natural. Por el corolario anterior $\mathbb{F}_{q^d}$ es una extensión finita de $\mathbb{F}_q$, que es separable y de grado d. Por el teorema del elemento primitivo esta extensión está generada por un elemento $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha)$, y el polinomio irreducible de α sobre $\mathbb{F}_q$ es precisamente un polinomio irreducible de grado d.

Definición: Sea k un cuerpo finito con q elementos. Si L es una extensión finita de k, diremos que el automorfismo $F\colon L \to L$, $F(\alpha) = \alpha^q$, es el **automorfismo de Frobënius** (1849-1917) de L sobre k, y claramente es la identidad sobre k.

Teorema H.3.10 *Si k es un cuerpo finito, toda extensión finita $k \to L$ es de Galois, y su grupo de Galois es un grupo cíclico generado por el automorfismo de Frobënius de L sobre k.*

Demostración: Sea q el número de elementos de k y sea G el grupo de automorfismos de L generado por el automorfismo de Frobënius $F(\alpha) = \alpha^q$. Los elementos de L que quedan fijos por F son las raíces del polinomio $x^q - x$, que están todas en k. Luego $L^G = k$ y el teorema de Artin permite concluir que L es una extensión de Galois de k y su grupo de Galois es G.

Corolario H.3.11 *Sea $p(x)$ un polinomio separable con coeficientes en $\mathbb{F}_q$ y sea $p(x) = p_1(x)\dots p_r(x)$ su descomposición en factores irreducibles en $\mathbb{F}_q[x]$. El grupo de Galois de $p(x)$ sobre $\mathbb{F}_q$ es un grupo cíclico generado por el automorfismo de Frobënius $F(\alpha) = \alpha^q$, que entendido como permutación de las raíces de $p(x)$ tiene forma $(n_1, \dots, n_r)$, donde $n_i = \operatorname{gr} p_i(x)$.*

Demostración: Si la permutación de la raíces de $p(x)$ que define F es producto de ciclos disjuntos de órdenes $d_1, \dots, d_s$, entonces la acción del grupo (F) en las raíces tiene s órbitas y $d_1, \dots, d_s$ son los cardinales de tales órbitas. Ahora H.2.4 permite concluir que $d_1, \dots, d_s$ coinciden con $n_1, \dots, n_r$.

Ejemplo: Si $p(x)$ es un polinomio irreducible de grado n con coeficientes en $\mathbb{F}_q$ y α es una raíz de $p(x)$, entonces $\mathbb{F}_q(\alpha)$ ya es el cuerpo de descomposición de $p(x)$ sobre $\mathbb{F}_q$, porque es una extensión de Galois. Todas las raíces de $p(x)$ son α^q, $\alpha^{q^2}, \dots, \alpha^{q^n} = \alpha$ y, con esta ordenación de las raíces, el grupo de Galois de $p(x)$ está generado por la permutación $(1, 2, \dots, n)$.

Así, en el caso del polinomio irreducible $x^4 + x + 1$ con coeficientes en $\mathbb{F}_2$, de acuerdo con el teorema de Kronecker una raíz en el cuerpo

$$\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1) = \mathbb{F}_2 \oplus \mathbb{F}_2\alpha \oplus \mathbb{F}_2\alpha^2 \oplus \mathbb{F}_2\alpha^3 \quad , \quad \alpha = [x]$$

es α. Luego las raíces de $p(x)$ en su cuerpo de descomposición $\mathbb{F}_{16}$ son

$$\alpha^2\ ,\ \alpha^4 = 1+\alpha\ ,\ \alpha^8 = (1+\alpha)^2 = 1+\alpha^2\ ,\ \alpha^{16} = \alpha\ .$$

Ley de Reciprocidad Cuadrática

Sea p un número primo y sea ε_n una raíz n-ésima de la unida primitiva sobre el cuerpo $\mathbb{F}_p$. De acuerdo con B.1 tenemos que $\Phi_n(\varepsilon_n) = 0$, porque claramente $\Phi_d(\varepsilon_n) \neq 0$ cuando $d < n$. Según B.4.1 los polinomios ciclotómicos $\Phi_n(x)$ son irreducibles en $\mathbb{Z}[x]$, así que *todas las relaciones algebraicas con coeficientes enteros que satisfaga $e^{2\pi i/n}$ también las verifica ε_n* (aunque pude admitir relaciones adicionales, porque $\Phi_n(x)$ no es necesariamente irreducible en $\mathbb{F}_p[x]$).

Si $p \neq 2$, como $i^2 = -1$, tenemos que $\varepsilon_4^2 = -1$ y $\sqrt{-1} \in \mathbb{F}_p(\varepsilon_4)$. Si consideramos el automorfismo de Frobënius $F(\alpha) = \alpha^p$ de $\mathbb{F}_p(\varepsilon_4)$ sobre $\mathbb{F}_p$, concluimos que -1 es resto cuadrático módulo p si y sólo si $p \equiv 1$ (mód. 4), resultado que ya vimos en 3.6.3. Si introducimos el **símbolo de Legendre** (1752-1833)

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si } a \text{ es resto cuadrático módulo } p \\ -1 & \text{si } a \text{ no es resto cuadrático módulo } p \end{cases}$$

(donde se supone que a no es múltiplo de p), tenemos que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Sea q otro primo impar. Las raíces del polinomio $f(x) = x^q - 1$ son $\alpha_1 = \varepsilon_q$, $\alpha_2 = \varepsilon_q^2$, $\ldots$, $\alpha_q = \varepsilon_q^q = 1$; así que su discriminante Δ es

$$\begin{aligned} \Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2 &= (-1)^{\frac{q(q-1)}{2}} \prod_{i\neq j}(\alpha_i - \alpha_j) = \\ &= (-1)^{\frac{q-1}{2}} \prod_i f'(\alpha_i) = (-1)^{\frac{q-1}{2}} q^q \prod_i \alpha_i^{q-1} = (-1)^{\frac{q-1}{2}} q^q \\ \sqrt{\Delta} &= q^{\frac{q-1}{2}} \sqrt{(-1)^{\frac{q-1}{2}} q} \end{aligned}$$

y $\mathbb{Q}(\sqrt{\Delta})$ es una extensión de grado 2 de $\mathbb{Q}$, contenida en $\mathbb{Q}(\varepsilon_q)$. Según H.3.6, $\mathbb{Q}(\varepsilon_q)$ es una extensión de Galois de $\mathbb{Q}$ de grupo $(\mathbb{Z}/q\mathbb{Z})^*$, que es cíclico de acuerdo con G.4.3. Luego, al ser $q-1$ es par, contiene un único subgrupo de índice 2. Por tanto, $\mathbb{Q}(\sqrt{\Delta})$ se corresponde con el subgrupo de $(\mathbb{Z}/q\mathbb{Z})^*$ formado por los restos cuadráticos no nulos módulo q, de modo que

$$\prod_{i<j}(\alpha_i^p - \alpha_j^p) \ = \ \begin{cases} \sqrt{\Delta} & \text{si } p \text{ es resto cuadrático módulo } q \\ -\sqrt{\Delta} & \text{si } p \text{ no es resto cuadrático módulo } q \end{cases}$$

Ahora, módulo p tendremos que $\sqrt{\Delta} \in \mathbb{F}_p(\varepsilon_q)$ y que $F(\sqrt{\Delta}) = \sqrt{\Delta}$ si y sólo si p es resto cuadrático módulo q. Es decir, $(-1)^{\frac{q-1}{2}} q$ es resto cuadrático módulo p) si

y sólo si p es resto cuadrático módulo q. Obtenemos así la **Ley de Reciprocidad Cuadrática** de Gauss (1777-1855) para dos primos impares $p \neq q$:

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

Esta ley no es válida cuando $q = 2$. En tal caso hemos de considerar las raíces octavas de la unidad, porque $e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, de modo que $\sqrt{2} = e^{2\pi i/8} + e^{-2\pi i/8}$. Por tanto, si ε_8 es una raíz octava de la unidad primitiva sobre $\mathbb{F}_p$, tendremos que

$$\sqrt{2} = \varepsilon_8 + \varepsilon_8^{-1} \in \mathbb{F}_p(\varepsilon_8) \ .$$

Se sigue que 2 es resto cuadrático módulo p si y sólo si

$$\varepsilon_8 + \varepsilon_8^{-1} = F(\varepsilon_8 + \varepsilon_8^{-1}) = \varepsilon_8^p + \varepsilon_8^{-p} \ .$$

Como $\varepsilon_8^3 + \varepsilon_8^{-3} = \varepsilon_8^5 + \varepsilon_8^{-5} = \varepsilon_8^4(\varepsilon_8 + \varepsilon_8^{-1}) = -(\varepsilon_8 + \varepsilon_8^{-1})$, esta condición equivale a que $p \equiv \pm 1$ (módulo 8):

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \ .$$

Ejemplo: Sea $p \neq 2$ un número primo. Como $\sqrt{2} = \varepsilon_8 + \varepsilon_8^{-1}$, las 8 raíces del polinomio $x^8 - 2^4$ son

$$\varepsilon_8 + \varepsilon_8^{-1} \ , \ \varepsilon_8^2 + 1 \ , \ \varepsilon_8^3 + \varepsilon_8 \ , \ \varepsilon_8^4 + \varepsilon_8^2 \ , \ \varepsilon_8^5 + \varepsilon_8^3 \ , \ \varepsilon_8^6 + \varepsilon_8^4 \ , \ \varepsilon_8^7 + \varepsilon_8^5 \ , \ \varepsilon_8^8 + \varepsilon_8^6$$

así que el automorfismo de Frobënius $F(\varepsilon_8) = \varepsilon_8^p$ siempre deja fija alguna raíz:

Si $F(\varepsilon_8) = \varepsilon_8$, deja fijas las 8 raíces.
Si $F(\varepsilon_8) = \varepsilon_8^3$, deja fijas las raíces $\varepsilon_8^3 + \varepsilon_8$ y $\varepsilon_8^7 + \varepsilon_8^5$.
Si $F(\varepsilon_8) = \varepsilon_8^5$, deja fijas las raíces $\varepsilon_8^2 + 1$, $\varepsilon_8^4 + \varepsilon_8^2$, $\varepsilon_8^6 + \varepsilon_8^4$ y $\varepsilon_8^8 + \varepsilon_8^6$.
Si $F(\varepsilon_8) = \varepsilon_8^7$, deja fijas las raíces $\varepsilon_8 + \varepsilon_8^{-1}$ y $\varepsilon_8^5 + \varepsilon_8^3$.

Por tanto, si $p \equiv 1$ (mód. 8), el 16 tiene 8 raíces octavas módulo p; si $p \equiv 3$ (mód. 8), tiene 2 raíces octavas módulo p; si $p \equiv 5$ (mód. 8), tiene 4 raíces octavas módulo p; y si $p \equiv 7$ (mód. 8), tiene 2 raíces octavas módulo p.

En particular, $x^8 - 16$ tiene raíz modular en todo primo p (pues obviamente también la tiene cuando $p = 2$), aunque tal polinomio no tiene ninguna raíz racional.

Extensiones Cíclicas

Definición: Sea $k \to L$ una extensión de Galois de grupo $G = \{\tau_1, \ldots, \tau_n\}$. Si $\alpha \in L$, diremos que $\mathrm{N}(\alpha) = \tau_1(\alpha) \cdot \ldots \cdot \tau_n(\alpha)$ es la **norma** de α. Nótese que $\mathrm{N}(\alpha) \in L^G = k$, y que $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

Teorema 90 de Hilbert (1862-1943)**:** *Sea $k \to L$ una extensión de Galois cíclica y sea σ un generador de su grupo de Galois. La condición necesaria y suficiente para que un elemento $\beta \in L$ tenga norma 1 es que $\beta = \alpha/\sigma(\alpha)$ para algún $\alpha \in L$.*

Demostración: Sea n el orden del grupo de Galois de L sobre k. Si $\beta = \alpha/\sigma(\alpha)$, es inmediato comprobar que $N(\beta) = (\sigma\beta)(\sigma^2\beta)\dots(\sigma^n\beta) = 1$.

Recíprocamente, los automorfismos $\sigma, \sigma^2, \dots, \sigma^n$ son linealmente independientes sobre L por el teorema de independencia, así que, si $\beta \in L$, existe algún $\theta \in L$ tal que la *resolvente de Lagrange* de θ por β:

$$\alpha \;:=\; \beta(\sigma\theta) + \beta(\sigma\beta)(\sigma^2\theta) + \dots + \beta(\sigma\beta)(\sigma^2\theta)\dots(\sigma^{n-2}\beta)(\sigma^{n-1}\theta) + N(\beta)\theta$$

no es nula. Es claro que $\beta = \alpha/\sigma(\alpha)$ cuando $N(\beta) = 1$.

Teorema H.3.12 *Sea n un número primo con la característica de un cuerpo k que contenga todas las raíces n–ésimas de la unidad. Si L es una extensión cíclica de k de grado n, entonces existe $\alpha \in L$ tal que $L = k(\alpha)$ y $\alpha^n \in k$.*

Recíprocamente, si una extensión L de k está generada por un elemento α tal que $\alpha^n \in k$, entonces L es una extensión cíclica de k de grado un divisor d de n y $\alpha^d \in k$.

Demostración: Sea $\varepsilon_n \in k$ una raíz n–ésima de la unidad primitiva.

Si $k \to L$ es una extensión cíclica de grado n, es claro que $N(\varepsilon_n^{-1}) = 1$, así que, en virtud del teorema 90 de Hilbert, existe $\alpha \in L$ tal que $\sigma(\alpha) = \varepsilon_n\alpha$, donde σ es un generador del grupo de Galois de L sobre k. Como

$$\sigma(\alpha^n) \;=\; (\sigma\alpha)^n \;=\; (\varepsilon_n\alpha)^n \;=\; \alpha^n \;,$$

tenemos que $\alpha^n \in k$. Además $L = k(\alpha)$ porque no hay dos elementos distintos en el grupo de Galois que coincidan en α, pues $\sigma^i(\alpha) = \varepsilon_n^i\alpha$ y ε_n es raíz primitiva.

Recíprocamente, si $L = k(\alpha)$ y $a := \alpha^n \in k$, entonces L es el cuerpo de descomposición sobre k del polinomio $x^n - a$, porque k contiene todas las raíces n–ésimas de la unidad. Además este polinomio es separable porque n es primo con la característica de k; luego L es una extensión de Galois de k. Sea G su grupo de Galois.

Si $\tau \in G$, tenemos $(\tau\alpha)^n = \tau(\alpha^n) = a$, así que $\tau(\alpha) = u\alpha$ para alguna raíz n–ésima de la unidad $u \in \mu_n$. Obtenemos así un morfismo de grupos $G \to \mu_n$, que es inyectivo porque cada automorfismo de $L = k(\alpha)$ sobre k está totalmente determinado por su acción sobre α. Al ser μ_n un grupo cíclico de orden n, concluimos que G es un grupo cíclico de orden un divisor d de n. Además, si σ es un generador de G, tenemos que $\sigma(\alpha) = v\alpha$ donde $v^d = 1$. Luego $\alpha^d \in k$ porque

$$\sigma(\alpha^d) \;=\; (\sigma\alpha)^d \;=\; (v\alpha)^d \;=\; \alpha^d \;.$$

Ecuaciones Resolubles por Radicales

Definición: Sea k un cuerpo de característica nula. Diremos que una extensión finita $k \to L$ es una **extensión por radicales** si $L = k(\alpha_1, \ldots, \alpha_r)$ donde alguna potencia $\alpha_i^{n_i}$, $n_i \geq 2$, está en $k(\alpha_1, \ldots, \alpha_{i-1})$ para todo índice $i = 1, \ldots, r$.

Diremos que un polinomio $p(x)$ con coeficientes en k es **resoluble por radicales** cuando todas sus raíces puedan expresarse con radicales; es decir, cuando su cuerpo de descomposición L sobre k admita una extensión finita $L \to E$ tal que E es una extensión de k por radicales.

Lema H.3.13 *Sea $k \to L$ una extensión de Galois de grupo G. Si $k \to E$ es una extensión de Galois abeliana, entonces el grupo de Galois sobre E de cualquier compuesto EL es un subgrupo normal $H \lhd G$ tal que G/H es abeliano.*

Demostración: Como E es una extensión abeliana de k, por el Teorema de Galois, $E \cap L$ es una extensión de Galois de k y su grupo es abeliano; luego se corresponde con un subgrupo normal $H \lhd G$ tal que G/H es abeliano. Ahora bien, el Teorema de los Irracionales Naturales afirma precisamente que H es el grupo de Galois de EL sobre E.

Teorema de las Ecuaciones Resolubles: *Sea k un cuerpo de característica nula. La condición necesaria y suficiente para que un polinomio con coeficientes en k sea resoluble por radicales es que su grupo de Galois sea resoluble.*

Demostración: Sea L el cuerpo de descomposición sobre k de un polinomio con coeficientes en k y sea $G = \mathrm{Aut}(L/k)$ su grupo de Galois.

Supongamos que L puede incluirse en una extensión por radicales $k(\alpha_1, \ldots, \alpha_r)$, donde $\alpha_i^{n_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$, y consideremos la extensión $E_i = k(\varepsilon_n, \alpha_1, \ldots, \alpha_i)$, donde $n = \text{m.c.m.}(n_1, \ldots, n_r)$. En virtud de H.3.5 E_0 es una extensión abeliana de k, y E_i es una extensión abeliana de E_{i-1} por H.3.12. Si H_i denota el grupo de Galois de E_iL sobre E_i,

$$\begin{array}{ccccccccc} L & \to & E_0L & \to & E_1L & \to & \ldots & \to & E_rL \\ \uparrow G & & \uparrow H_0 & & \uparrow H_1 & & \ldots & & \uparrow H_r \\ k & \to & E_0 & \to & E_1 & \to & \ldots & \to & E_r \end{array}$$

el lema anterior afirma que $H_i \lhd H_{i-1}$ y el cociente H_{i-1}/H_i es abeliano. Como $H_r = 1$, porque $L \subset E_r$, concluimos que G es resoluble.

Recíprocamente, supongamos que G es resoluble, y sea n el producto de los números primos que dividan al orden de G. El Teorema de los irracionales naturales afirma que el grupo de Galois $L(\varepsilon_n)$ sobre $k(\varepsilon_n)$ es un subgrupo H de G; luego es resoluble por F.5.2, así que admite una sucesión decreciente de subgrupos $H = H_0 \rhd H_1 \rhd \ldots \rhd H_r = 1$ tal que los cocientes sucesivos H_{i-1}/H_i, $1 \leq i \leq r$,

son grupos cíclicos de orden un número primo p_i que divide a n. El teorema de Galois y H.3.12 permiten concluir que $L(\varepsilon_n)$ es una extensión de $k(\varepsilon_n)$ por radicales, y por tanto también es una extensión de k por radicales. El polinomio dado es resoluble por radicales. q.e.d.

Cuando el grupo de Galois de una ecuación algebraica $q(x) = 0$ es resoluble, y la descomposición en factores primos del orden del grupo de Galois es $|G| = p_1 p_2 \dots p_r$, la demostración anterior prueba además que tal ecuación puede resolverse con r radicales $\sqrt[p_1]{}, \dots, \sqrt[p_r]{}$ junto con raíces de la unidad de órdenes $p_1, \dots, p_r$.

Corolario H.3.14 *La ecuación general de grado 3, con coeficientes en un cuerpo k de característica nula, puede resolverse con una raíz cuadrada, una raíz cúbica y las raíces cúbicas de la unidad.*

La ecuación general de grado 4 puede resolverse con 3 raíces cuadradas, una raíz cúbica y las raíces cúbicas de la unidad.

Las ecuaciones generales de grado mayor o igual que 5 no pueden resolverse por radicales.

Demostración: De acuerdo con H.2.8, el grupo de Galois del polinomio genérico de grado n es el grupo simétrico S_n, que no es resoluble cuando $n \geq 5$ (véase F.5.1).

Ejemplo: La imposibilidad de resolver por radicales el polinomio genérico de grado n con coeficientes en k (que, recuérdese, no tiene coeficientes en k sino en el cuerpo $k(c_1, \dots, c_n)$ de funciones racionales en n indeterminadas) no implica la existencia de algún polinomio particular $p(x) \in k[x]$ que no pueda resolverse por radicales, sino que afirma la imposibilidad de expresar las raíces, a partir de los coeficientes, mediante un número finito de sumas, productos, cocientes y radicales. Por ejemplo, la ecuación general de grado 5 con coeficientes reales no es resoluble por radicales, mientras que cualquier polinomio particular con coeficientes reales puede resolverse con una raíz cuadrada (a saber $\sqrt{-1}$) pues todas sus raíces son complejas.

Por eso el corolario anterior no implica por sí solo la existencia de ecuaciones irresolubles con coeficientes racionales. Para ver una de tales ecuaciones, consideremos el polinomio $q(x) = x^5 - 4x + 2$, que es irreducible (criterio de Eisenstein) y tiene dos raíces reales positivas y una negativa (por la regla de Descartes no puede tener más de 3 raíces reales, y $q(-2) < 0$, $q(0) > 0$, $q(1) < 0$, $q(2) > 0$). Como tiene tres raíces reales y dos complejas conjugadas, el siguiente lema prueba que su grupo de Galois es S_5, que no es resoluble.

Lema H.3.15 *Sea $q(x) \in \mathbb{Q}[x]$ un polinomio irreducible de grado primo p. Si $q(x)$ sólo tiene 2 raíces imaginarias, entonces su grupo de Galois es el grupo simétrico S_p. En particular, $q(x)$ no es resoluble por radicales cuando $p \geq 5$.*

Demostración: Sea G el grupo de Galois de $q(x)$. Por hipótesis la conjugación compleja define una trasposición, así que bastará probar que un subgrupo transitivo $G \subseteq S_p$ que contenga una trasposición es todo el grupo simétrico S_p. Consideremos la siguiente relación de equivalencia en el conjunto $\{1, 2, \ldots, p\}$:

$$i \equiv j \text{ cuando } (ij) \in G$$

Todas las clases de equivalencia tienen el mismo cardinal, porque G es transitivo, y alguna clase tiene más de un elemento porque G contiene una trasposición. Como p es primo, se sigue que sólo hay una clase de equivalencia: G contiene todas las trasposiciones y concluimos que $G = S_p$.

Proposición H.3.16 *La condición necesaria y suficiente para que un polinomio irreducible y separable de grado primo p tenga grupo de Galois resoluble es que su cuerpo de descomposición esté generado por dos raíces cualesquiera.*

Demostración: El grupo de Galois G es un subgrupo transitivo de S_p porque el polinomio es irreducible. Si G es resoluble, F.5.8 afirma que la identidad es el único automorfismo $\tau \in G$ que deja fijas dos raíces; luego el cuerpo de descomposición está generado por dos raíces cualesquiera.

Recíprocamente, si el cuerpo de descomposición está generado por dos raíces, entonces su grado es pq, donde $q < p$. Luego $|G| = pq$ y F.5.9 permite concluir que G es resoluble.

Corolario H.3.17 (Galois 1811-1832) *Si un polinomio irreducible y de grado primo con coeficientes racionales tiene grupo de Galois resoluble y dos raíces reales, entonces todas sus raíces son reales.*

Envolvente de Galois

Teorema H.3.18 *Sea A una k-álgebra finita. Existe una extensión finita $k \to L$, única salvo isomorfismos, llamada* ***envolvente normal*** *de A sobre k, tal que*

1. *A es racional sobre L.*
2. *L es cociente de algún producto tensorial iterado $A^{\otimes n} = A \otimes_k \overset{n}{\ldots} \otimes_k A$.*

Demostración: Para ver la existencia, fijamos el grado y procedemos por inducción descendente sobre el número de puntos racionales de $\operatorname{Spec} A$, porque cuando A es racional basta tomar $L = k$. Si algún punto $x \in \operatorname{Spec} A$ no es racional, consideramos su cuerpo residual $\pi\colon A \to \kappa(x)$. Por la fórmula de los puntos el número de puntos racionales de $\operatorname{Spec} A_{\kappa(x)}$ es mayor que el número de puntos racionales de $\operatorname{Spec} A$, porque cada punto $A \to k$ define obviamente un punto $A \to \kappa(x)$ y aún tenemos uno más π. Por hipótesis de inducción $A_{\kappa(x)}$ es racional sobre una extensión finita $\kappa(x) \to L$ que es cociente de $(A_{\kappa(x)})^{\otimes n} = (A^{\otimes n}) \otimes_k \kappa(x)$. Como $\kappa(x)$ es un cociente de A, concluimos que L es un cociente de $A^{\otimes(n+1)}$.

En cuanto a la unicidad, si L y L' son dos envolventes de A, entonces L es racional sobre L' porque es un cociente de $A^{\otimes n}$, que es racional sobre L'; luego, por la fórmula de los puntos, existe algún morfismo $L \to L'$ y $[L : k] \leq [L' : k]$. Por la misma razón existe un morfismo $L' \to L$ y ambas extensiones tienen igual grado, de modo que tal morfismo $L' \to L$ es un isomorfismo.

Corolario H.3.19 *La envolvente de una k-álgebra finita A es una extensión normal de k, y es una extensión de Galois cuando A es separable.*

Demostración: Por definición A es racional sobre su envolvente L, luego también lo son las álgebras $A^{\otimes n}$ y sus cocientes, así que L es racional sobre L: es una extensión normal.

Si además es separable también lo son las álgebras $A^{\otimes n}$ y sus cocientes, así que L es una extensión normal separable: es de Galois.

Corolario H.3.20 *La envolvente normal L de una k-álgebra finita A es la menor extensión de k que la racionaliza, en el sentido de que cualquier otra extensión de k que la racionalice es extensión de L.*

Demostración: Si A es racional sobre una extensión L' de k, también lo son las álgebras $A^{\otimes n}$ y sus cocientes, así que L es racional sobre L' y la fórmula de los puntos permite concluir la existencia de algún morfismo $L \to L'$.

Corolario H.3.21 *La envolvente normal de $k[x]/\big(p(x)\big)$ sobre k es el cuerpo de descomposición del polinomio $p(x)$ sobre k.*

Corolario H.3.22 *Si K es una extensión finita de k, existe una extensión finita L de K tal que L es extensión normal de k y L es un compuesto iterado de K.*

Demostración: Si L es la envolvente normal de K sobre k, entonces K es racional sobre L y, por la fórmula de los puntos, existe algún morfismo $K \to L$, que necesariamente es inyectivo al ser K un cuerpo.

Corolario H.3.23 *Toda extensión finita separable $k \to K$ admite una extensión finita $K \to L$ tal que L es una extensión de Galois de k y L es un compuesto iterado de K. En particular el número de cuerpos intermedios entre k y K es finito.*

Demostración: En una extensión de Galois el número de cuerpos intermedios es finito por el teorema de Galois.

Grupo de Galois de las Cuárticas

Sea $p_4(x) = x^4 + px^3 + qx^2 + rx + s$ una cuártica *separable* e *irreducible* sobre un cuerpo k de característica distinta de 2, sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ sus raíces en su cuerpo de descomposición $L = k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ y sea G su grupo de Galois, que es un subgrupo de S_4 bien definido salvo conjugación.

La cúbica resolvente de $p_4(x)$, que es el polinomio de raíces $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$, también es separable, y es

$$r(y) \;=\; y^3 - qy^2 + (pr - 4s)y - (p^2s - 4qs + r^2)$$

Es inmediato comprobar que una permutación σ de las raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ deja fijos β_1, β_2 y β_3 si y sólo si σ está en el grupo de Klein (1849-1925)

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\},$$

de modo que $G \cap V$ es el grupo de Galois de L sobre $k(\beta_1, \beta_2, \beta_3)$:

$$k \;\xrightarrow{\;d\;}\; k(\beta_1, \beta_2, \beta_3) \;\xrightarrow{\;G\cap V\;}\; k(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = L$$

Por otra parte, al ser $p_4(x)$ irreducible en $k[x]$, el orden de su grupo de Galois G sobre k es múltiplo de 4. Luego el morfismo natural $G \to S_4/V$ no puede ser inyectivo, ya que $|S_4/V| = 6$, y se sigue que su núcleo $G \cap V$ tiene orden 2 ó 4:

$$|G \cap V| \;=\; 2 \text{ ó } 4 \qquad , \qquad |G| \;=\; 2d \text{ ó } 4d$$

Distingamos ahora los casos posibles según el grado d sobre k del cuerpo de descomposición $k(\beta_1, \beta_2, \beta_3)$ de la cúbica resolvente, que coincide con el orden del grupo de Galois de $r(y)$ sobre k y ya sabemos calcular (H.2.7):

$\boxed{d = 6}$

En este caso el orden de G es 12 ó 24, así que $G = A_4$ ó $G = S_4$, porque A_4 es el único subgrupo de orden 12 de S_4. En ambos casos G contiene a V; luego $|G \cap V| = 4$ y concluimos que $|G| = 24$. El grupo de Galois de la cuártica es el simétrico $G = S_4$.

$\boxed{d = 3}$

En este caso el orden de G es 6 ó 12; luego es 12 porque ha de ser múltiplo de 4. El grupo de Galois es el alternado $G = A_4$, porque éste es el único subgrupo de orden 12 del grupo simétrico S_4 .

$\boxed{d = 2}$

En este caso el orden de G es 4 ó 8.

- Si $|G| = 8$, entonces G es un 2-subgrupo de Sylow de S_4. Como el grupo diédrico D_8 (el grupo de las simetrías de un cuadrado) es un 2-subgrupo de Sylow de S_4, todos los subgrupos de Sylow son conjugados, y el grupo de Galois está bien definido salvo conjugación, concluimos que su grupo de Galois es D_8. Con una adecuada numeración de las raíces de la cuártica

$$G = D_8 = \{\, \mathrm{id}\,,\ (1234)\,,\ (13)(24)\,,\ (1432)\,,\ (12)(34)\,,\ (14)(23)\,,\ (13)\,,\ (24)\,\}.$$

- Si $|G| = 4$, entonces $|G \cap V| = 2$. Como G es un subgrupo transitivo de S_4 de orden 4, si una permutación $\tau \in G$ deja fija alguna raíz, necesariamente es la identidad. Luego toda permutación de G es de tipo 2,2 ó de tipo 4. Si todas son de tipo 2,2, tenemos que $G = V$, lo que contradice que $|G \cap V| = 2$. Concluimos que el grupo de Galois es cíclico, generado por un 4-ciclo. Es decir, salvo conjugación,

$$G = C_4 = \{\, \mathrm{id}\,,\ (1234)\,,\ (13)(24)\,,\ (1432)\,\}\ .$$

$\boxed{d = 1}$

En este caso el orden de G es 2 ó 4; luego es 4, porque ha de ser múltiplo de 4, y tenemos que $|G \cap V| = 4$. Concluimos que el grupo de Galois es el grupo de Klein $G = V$.

Vemos así que el grupo de Galois G de una cuártica irreducible está totalmente determinado por el de su cúbica resolvente, salvo cuando $d = 2$, que es el caso en que la cúbica resolvente tiene una única raíz en k, y G puede ser el grupo diédrico D_8 o el grupo cíclico C_4:

$$C_4 = \{\, \mathrm{id}\,,\ (1234)\,,\ (13)(24)\,,\ (1432)\,\}$$
$$D_8 = \{\, \mathrm{id}\,,\ (1234)\,,\ (13)(24)\,,\ (1432)\,,\ (12)(34)\,,\ (14)(23)\,,\ (13)\,,\ (24)\,\}$$

En ambos casos, la única raíz en k de la cúbica resolvente es $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, que denotaremos a. Pero, al ser $C_4 \cap V = \{\mathrm{id}, (13)(24)\}$ y $D_8 \cap V = V$, tenemos que $G = C_4$ si y sólo si $\alpha_1\alpha_3$, $\alpha_2\alpha_4$, $\alpha_1+\alpha_3$ y $\alpha_2+\alpha_4$ quedan invariantes por $G \cap V$, lo que equivale a que estén en el cuerpo de descomposición $L^{G\cap V} = k(\beta_1, \beta_2, \beta_3)$ de la cúbica resolvente.

Por tanto, cuando $d = 2$, la condición necesaria y suficiente para que el grupo de Galois sea $G = C_4$ es que los polinomios

$$(x - \alpha_1\alpha_3)(x - \alpha_2\alpha_4) = x^2 - ax + s$$
$$(x - (\alpha_1 + \alpha_3))(x - (\alpha_2 + \alpha_4)) = x^2 + px + q - a$$

tengan sus raíces en el cuerpo de descomposición $k(\beta_1, \beta_2, \beta_3)$ de la cúbica resolvente, que es una extensión cuadrática de k, porque $r(y)$ tiene una raíz en k. De

hecho es la extensión $k(\sqrt{\Delta})$, donde Δ es el discriminante de $r(y) = (y-a)p_2(y)$, porque éste se diferencia en un cuadrado del discriminante de $p_2(y)$.

d	G	
6	S_4	
3	A_4	
2	C_4	Si $x^2 - ax + s$ y $x^2 + px + q - a$ descomponen sobre $k(\sqrt{\Delta})$
2	D_8	En caso contrario
1	V	

Veamos que todos estos casos son posibles cuando el cuerpo base es $\mathbb{Q}$:

$G = V$. Una extensión de Galois de grado 4 que no es cíclica es $\mathbb{Q}(i, \sqrt{2})$. Como $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}((1+i)/\sqrt{2})$, el grupo de Galois del polinomio irreducible de $(1+i)/\sqrt{2} = e^{\frac{2\pi i}{8}}$ es V, porque es de orden 4 y no es cíclico. Es decir, V es el grupo de Galois de $x^4 + 1$ sobre $\mathbb{Q}$.

$G = D_8$. En H.1.1 hemos visto que el grupo de Galois de $x^4 - 2$ sobre $\mathbb{Q}$ es de orden 8; luego es D_8.

$G = C_4$. Una extensión cíclica de $\mathbb{Q}$ de grado 4 es $\mathbb{Q}(e^{\frac{2\pi i}{5}})$; luego el grupo de Galois de $x^4 + x^3 + x^2 + x + 1$ sobre $\mathbb{Q}$ es C_4.

$G = A_4$. Busquemos una cuártica cuyo discriminante sea un cuadrado, porque en general es de esperar que su cúbica resolvente sea irreducible y el grupo de Galois será A_4. La cúbica resolvente de $x^4 - px^3 + s$ es $y^3 - 4sy - sp^2$, cuyo discriminante

$$\Delta = 4^4 s^2 (s - 27(p/4)^4)$$

es un cuadrado cuando $p = 4$, $s = 28$. En este caso la cúbica resolvente, que es $y^3 - 4 \cdot 28y - 4^2 \cdot 28$, es irreducible (criterio de Eisenstein para el primo 7), y concluimos que una cuártica de grupo A_4 sobre $\mathbb{Q}$ es $x^4 - 4x^3 + 28$.

$G = S_4$. En general es de esperar que una cuártica tenga grupo S_4. Así la cúbica resolvente de la cuártica irreducible $x^4 - x + 1$ es $y^3 - 4y - 1$, que es irreducible y su discriminante $\Delta = 229$ no es un cuadrado.

H.4 El Automorfismo de Frobënius

Teorema de Reducción: *Sea $q(x) = x^n + c_1 x^{n-1} + \ldots + c_n$ un polinomio unitario con coeficientes enteros y G su grupo de Galois sobre $\mathbb{Q}$. Sea p un número primo, $\bar{q}(x) = x^d + \bar{c}_1 x^{d-1} + \ldots + \bar{c}_n \in \mathbb{F}_p[x]$ la reducción módulo p y $\bar{G}$ su grupo de Galois sobre $\mathbb{F}_p$. Existe un subgrupo $G' \subseteq G$ y un epimorfismo $\varphi\colon G' \to \bar{G}$.*

Además, numerando adecuadamente las raíces α_i de $q(x)$ y las raíces $\bar\alpha_i$ de $\bar q(x)$, si $\bar g = \varphi(g)$, entonces $(\bar g)(\bar\alpha_i) = \bar\alpha_j$ cuando $g(\alpha_i) = \alpha_j$.

Si $\bar q(x)$ es separable (y por tanto $q(x)$ también), entonces φ es un isomorfismo.

Demostración: Consideremos el cuerpo de descomposición $L := \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ de $q(x) = (x-\alpha_1)\dots(x-\alpha_n)$ sobre $\mathbb{Q}$ y el anillo $A := \mathbb{Z}[\alpha_1, \dots, \alpha_n]$. La demostración se descompone en los siguientes pasos:

1. $A = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$ es un $\mathbb{Z}$-módulo de tipo finito, porque está generado por los monomios $\alpha_1^{d_1} \dots \alpha_n^{d_n}$ donde todos los exponentes d_i son menores que n, pues $\alpha_i^n = -c_1\alpha_i^{n-1} - \dots - c_n$.

2. $\mathbb{Z}[\alpha_1, \dots, \alpha_n]^G = \mathbb{Z}$.

   En efecto, si $a/b \in A^G = A \cap L^G = A \cap \mathbb{Q}$, entonces $\mathbb{Z}[a/b]$ es un $\mathbb{Z}$-módulo de tipo finito porque es un submódulo de A. Se sigue que todos los elementos de $\mathbb{Z}[a/b]$ tienen denominador acotado por cierta constante, lo que es absurdo si a/b no es un número entero.

3. $A' = A/pA$ es una $\mathbb{F}_p$-álgebra finita por el paso 1. Sea $A' = A_1 \oplus \dots \oplus A_r$ su descomposición en álgebras locales, y sean $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ los correspondientes ideales maximales de A. Si $a \in A$, representaremos por a' su clase en $A' = A/pA$ y por $\bar a$ su clase en $K_1 := A/\mathfrak{m}_1$.

   Nótese que $K_1 = \mathbb{F}_p[\bar\alpha_1, \dots, \bar\alpha_n]$, y por tanto es el cuerpo de descomposición sobre $\mathbb{F}_p$ de $\bar q(x) = (x-\bar\alpha_1)\dots(x-\bar\alpha_n)$. Sea G' el subgrupo de los elementos de G que dejan invariante el ideal $\mathfrak{m}_1$, de modo que G' actúa sobre el cuerpo $K_1 = A/\mathfrak{m}_1$ y obtenemos un morfismo natural

   $$\varphi\colon G' \longrightarrow \bar G$$

4. Veamos que φ siempre es epiyectivo. Por el teorema del elemento primitivo $K_1 = \mathbb{F}_p[\bar\theta]$. Sea $\bar r(x)$ el polinomio irreducible de $\bar\theta$ sobre $\mathbb{F}_p$. Todo automorfismo $\bar g \in \bar G$ está determinado por $\bar g(\bar\theta)$, que es raíz de $\bar r(x)$. Fijemos un representante $\theta' = (\theta_1, 0, \dots, 0) \in A'$ de $\bar\theta$ y un representante $\theta \in A$ de θ'.

   El polinomio $h(x) = \prod_{g\in G}\big(x - g(\theta)\big)$ tiene coeficientes enteros por el paso 2, y su reducción $\bar h(x)$ módulo p admite la raíz $\bar\theta$; luego es múltiplo de $\bar r(x)$. Por tanto, dado $\bar g \in \bar G$, existe $g \in G$ tal que $\overline{g(\theta)} = \bar g(\bar\theta)$. Para terminar basta ver que $g \in G'$. Sea $g(\mathfrak{m}_i) = \mathfrak{m}_1$. Si $\mathfrak{m}_i = \mathfrak{m}_1$ hemos terminado, y en caso contrario

   $$\theta \in \mathfrak{m}_2 \cap \dots \cap \mathfrak{m}_r \;\Rightarrow\; g(\theta) \in g(\mathfrak{m}_2) \cap \dots \cap g(\mathfrak{m}_r) \subset \mathfrak{m}_1$$

   de modo que $\overline{g(\theta)} = 0$, y por tanto $\bar g(\bar\theta) = 0$, lo que es absurdo.

5. Por último, cuando $q(x)$ y $\bar{q}(x)$ son separables, cada automorfismo $g' \in G'$ viene dado por una permutación de las raíces α_i de $q(x)$, y $\varphi(g')$ define la *misma* permutación de las raíces $\bar{\alpha}_i$. Luego φ es claramente inyectivo, y el punto anterior permite concluir que es un isomorfismo.

Corolario H.4.1 *Sea $q(x)$ un polinomio unitario separable con coeficientes enteros y sea p un número primo. Si la reducción $\bar{q}(x)$ módulo p es separable y descompone en factores irreducibles de grados $n_1, \ldots, n_r$, entonces el grupo de Galois de $q(x)$ sobre $\mathbb{Q}$ contiene una permutación de forma $(n_1, \ldots, n_r)$.*

Demostración: El grupo de Galois G de $\bar{q}(x)$ sobre $\mathbb{F}_p$ está generado por el automorfismo de Frobënius F, y por el teorema anterior existe algún automorfismo $g \in G' \subseteq G \subseteq S_d$ tal que $\varphi(g) = F$. Además, al ser $\bar{q}(x)$ separable, la forma de la permutación g coincide con la forma de la permutación $\varphi(g) = F$, que es precisamente $(n_1, \ldots, n_r)$ por H.3.11.

Corolario H.4.2 *Para cada número natural n existe un polinomio con coeficientes racionales de grado n cuyo grupo de Galois es el grupo simétrico S_n.*

Demostración: Sea $q_2(x) \in \mathbb{F}_2[x]$ un polinomio unitario irreducible de grado n, que existe por H.3.9. Sea $q_3(x) \in \mathbb{F}_3[3]$ un polinomio unitario que tiene un factor irreducible de grado $n-1$ y una raíz en $\mathbb{F}_3$. Sea $q_p(x) \in \mathbb{F}_p[x]$ un polinomio unitario que tenga un factor irreducible de grado 2 y $n-2$ raíces distintas en $\mathbb{F}_p$, donde $p \neq 2, 3$ es número primo $\geq n-2$.

Como $\mathbb{Z}/6p\mathbb{Z} = \mathbb{F}_2 \oplus \mathbb{F}_3 \oplus \mathbb{F}_p$ por el teorema chino de los restos, existe un polinomio unitario con coeficientes enteros $q(x)$ cuyas reducciones módulo 2,3 y p son $q_2(x)$, $q_3(x)$ y $q_p(x)$ respectivamente. En particular $q(x)$ es irreducible, y su grupo de Galois G es un subgrupo transitivo de S_n por H.2.5. Además, por el corolario anterior, G contiene un $(n-1)$-ciclo y una trasposición. Podemos suponer que $(2, \ldots, n)$, $(ij) \in G$. Ahora, al ser G un subgrupo transitivo, contiene una trasposición $(1k)$. Conjugando $(1k)$ con $(2, \ldots, n)$ y sus potencias obtenemos que (12), $(13), \ldots,$ $(1n) \in G$. Es sencillo ver que estas trasposiciones generan todo el grupo simétrico S_n y concluimos que $G = S_n$.

Corolario H.4.3 *Para todo grupo finito G existe un polinomio $p(x) \in \mathbb{Q}[x]$ tal que su grupo de Galois sobre cierta extensión finita K de $\mathbb{Q}$ es isomorfo a G.*

(Es un problema abierto saber si puede tomarse $K = \mathbb{Q}$.)

Demostración: Según el ejemplo 1 de la página 340, todo grupo finito G es isomorfo a un subgrupo de un grupo simétrico S_n y, por H.4.2, existe alguna extensión de Galois L de $\mathbb{Q}$ de grupo S_n. Basta considerar un polinomio $p(x)$ cuyo cuerpo de descomposición sea L y tomar $K := L^G$.

Definición: Cuando la reducción $\bar{q}(x)$ módulo p es separable, tenemos un isomorfismo $\varphi\colon G' \to \bar{G}$. Ahora bien, $\bar{G}$ tiene un generador canónico, el automorfismo de Frobënius $\bar{F}(\bar{a}) = \bar{a}^p$, y llamaremos **automorfismo de Frobënius** (1849-1917) asociado al primo p al único elemento $F_p \in G'$ tal que $\varphi(F_p) = \bar{F}$; es decir,

$$F_p(a) \equiv a^p \quad (\text{módulo } \mathfrak{m}_1)$$

para todo $a \in A$. Este automorfismo de Frobënius F_p no sólo depende del primo p, sino también del ideal maximal $\mathfrak{m}_1$ elegido en la demostración del teorema de reducción. Como el grupo de Galois actúa transitivamente en $\operatorname{Spec} A'$, si se elige otro maximal $\tau(\mathfrak{m}_1)$, entonces el automorfismo de Frobënius asociado a p es $\tau F_p \tau^{-1}$: *El automorfismo de Frobënius asociado a un número primo es un elemento del grupo de Galois G bien definido salvo conjugación.*

Veamos en efecto que el grupo de Galois actúa transitivamente en $\operatorname{Spec} A'$, que es la fibra de la aplicación $\operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z}$ sobre el punto p. Si tal fibra tuviera más de una órbita, elegimos una función $f \in A$ que se anule en los puntos de una órbita y no se anule en los restantes puntos de tal fibra (la existencia de f se sigue del Teorema chino de los restos). Luego $N(f) = \prod_{\tau \in G} \tau(f)$ se anula en unos puntos de la fibra y en otros no, lo que es absurdo porque $N(f) \in A^G = \mathbb{Z}$.

Notas: **(1)** Si un polinomio $q(x) = x^n + c_1 x^{n-1} + \ldots + c_n$ tiene coeficientes racionales y S denota el conjunto de números primos que dividen al denominador de algún coeficiente c_i, entonces la reducción $\bar{q}(x)$ módulo p está bien definida para todo primo $p \notin S$, y la demostración del teorema de reducción sigue siendo válida si $\mathbb{Z}$ se sustituye por la localización de $\mathbb{Z}$ en los números primos que están en S.

(2) La reducción $\bar{q}(x)$ módulo p es separable precisamente cuando el primo p no divida al discriminante $\Delta = \prod_{i<j}(\alpha_j - \alpha_i)^2$ del polinomio $q(x)$. Por tanto, *si un polinomio con coeficientes enteros $q(x)$ es separable, sólo hay un número finito de primos en los que la reducción $\bar{q}(x)$ es inseparable.*

Ejemplos: **(1)** Sea $q(x) = x^n + \ldots$ un polinomio irreducible con coeficientes enteros. *Si su grupo de Galois sobre $\mathbb{Q}$ no contiene ciclos de orden n, entonces no existe ningún número primo p tal que la reducción $\bar{q}(x)$ sea irreducible.*

En efecto, si $\bar{q}(x)$ no es separable, entonces no es irreducible por 4.3.10. Si $\bar{q}(x)$ es separable, entonces no puede ser irreducible, porque en caso de serlo el grupo de Galois de $q(x)$ tendría un ciclo de orden n según H.4.1.

Por ejemplo, si el grupo de Galois de una cuártica con coeficientes enteros es $V = \{id, (12)(34), (13)(24), (14)(23)\}$ entonces es irreducible aunque no lo sea su reducción módulo ningún primo. Tal es el caso de $x^4 + 1$ y de $x^4 - 2x^2 + 9$.

(2) Si todo automorfismo $g \in G$ deja fija alguna raíz de $q(x)$, el Teorema de reducción muestra que el generador de $\bar{G}$ deja fija alguna raíz de $\bar{q}(x)$, de modo que $\bar{q}(x)$ tiene una raíz en $\mathbb{F}_p$ para casi todo primo p.

Por ejemplo, sea $L = \mathbb{Q}(\sqrt{2}, i)$. Cada elemento de su grupo de Galois deja fijo i, $\sqrt{2}$ ó $i\sqrt{2}$, así que deja fija alguna raíz del polinomio $q(x) = x^8 - 2^4$, pues sus raíces son $\pm\sqrt{2}$, $\pm(1+i)$, $\pm\sqrt{2}i$ y $\pm(1-i)$. Por tanto su reducción $\bar{q}(x)$ módulo cualquier primo p admite alguna raíz en $\mathbb{F}_p$ cuando $\bar{q}(x)$ sea separable (i.e. cuando $p \neq 2$), lo que ya habíamos visto en el ejemplo de la página 377.

(3) La reducción de $x^n - 1$ módulo p es separable cuando p no divide a n. En tal caso, si $\varepsilon_n := e^{2\pi i/n}$, tenemos que $\overline{\varepsilon}_n^i \neq \overline{\varepsilon}_n^j$ cuando $1 \leq i, j \leq n$, $i \neq j$; es decir, $\varepsilon_n^i - \varepsilon_n^j \notin \mathfrak{m}_1$. Por tanto $F_p(\varepsilon) = \varepsilon^p$ y, al identificar (v. H.3.5) el grupo de Galois G de $x^n - 1$ con un subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$, el automorfismo F_p se corresponde con la clase de p. Luego G contiene la clase de cualquier primo que no divide a n y concluimos que $G = (\mathbb{Z}/n\mathbb{Z})^*$, lo que proporciona otra demostración de la irreducibilidad de los polinomios ciclotómicos B.4.1.

(4) Sea G el grupo de Galois de un polinomio con coeficientes racionales. El teorema de Tchebotarev, que no probaremos en este libro , afirma que cada automorfismo $g \in G$ es el automorfismo de Frobënius asociado a infinitos números primos. Veamos algunas consecuencias de este resultado fundamental:

1. *Dado un polinomio $q(x)$ con coeficientes racionales, existen infinitos números primos p tales que la reducción $\bar{q}(x)$ módulo p tiene grupo de Galois trivial,* i.e., $\bar{q}(x)$ tiene todas sus raíces en $\mathbb{F}_p$.

   En efecto, el automorfismo de Frobënius asociado a un primo p es la identidad precisamente cuando $\bar{q}(x)$ tiene todas sus raíces en $\mathbb{F}_p$. Aunque no demostremos el teorema de Tchebotarev, este corolario se probará en N.3.6.

2. Sea $q(x)$ un polinomio con coeficientes racionales. *Si en casi todo número primo p la reducción $\bar{q}(x)$ módulo p tiene grupo de Galois trivial, entonces el grupo de Galois de $q(x)$ es trivial.* Es decir, si en todo número primo p, salvo un número finito, la reducción $\bar{q}(x)$ tiene todas sus raíces en $\mathbb{F}_p$, entonces $q(x)$ tiene todas sus raíces racionales. (Este corolario del teorema de Tchebotarev se probará en N.3.8).

   Por ejemplo, si un número entero a es resto cuadrático módulo casi todos los números primos, entonces a es un cuadrado perfecto.

3. Sea $q(x) = x^n + \ldots$ un polinomio con coeficientes racionales. *La condición necesaria y suficiente para que exista algún número primo p tal que la reducción $\bar{q}(x)$ módulo p sea irreducible es que el grupo de Galois G de $q(x)$ sobre $\mathbb{Q}$ contenga algún ciclo de orden n. Además, en tal caso hay infinitos números primos en que la reducción $\bar{q}(x)$ es irreducible.*

   En efecto, si la reducción $\bar{q}(x)$ módulo p es irreducible, entonces el automorfismo de Frobënius asociado a p es un ciclo de orden n. Recíprocamente, si G contiene un ciclo de orden n, éste será el automorfismo de Frobënius

asociado a algún número primo p (y de hecho a infinitos) y concluimos que la reducción $\bar{q}(x)$ módulo p es irreducible.

4. *Si un polinomio $q(x) \in \mathbb{Q}[x]$ es irreducible y de grado primo, existen infinitos números primos tales que la reducción $\bar{q}(x)$ es irreducible.*

   En efecto, como $q(x)$ es irreducible en $\mathbb{Q}[x]$, el orden de su grupo de Galois G es múltiplo del grado p. Por el teorema de Cauchy, G contiene alguna permutación $\tau \in S_p$ de orden p, que necesariamente es un ciclo de orden p al ser p un número primo (2.6.4).

5. *Si un polinomio $q(x) \in \mathbb{Q}[x]$ es irreducible, existen infinitos números primos p tales que la reducción $\bar{q}(x)$ no tiene raíces en $\mathbb{F}_p$.*

   En efecto, sea $G \subseteq S_n$ el grupo de Galois de $q(x)$ sobre $\mathbb{Q}$ y sea $H_i = \{\tau \in G\colon \tau(i) = i\}$. Tenemos que $[G : H_i] = n$ porque $q(x)$ es irreducible (H.2.5); luego $H_1 \cup \ldots \cup H_n \neq G$, ya que la unión de subgrupos nunca es disjunta. Cualquier número primo p cuyo automorfismo de Frobënius no esté en $H_1 \cup \ldots \cup H_n$ verifica que la reducción $\bar{q}(x)$ carece de raíces en $\mathbb{F}_p$.

6. Si una cúbica con coeficientes racionales tiene una raíz modular en casi todos los números primos, entonces tiene alguna raíz racional. En particular, si un número entero es resto cúbico módulo casi todo primo, es un cubo perfecto.

Ejercicios:

1. $\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es una extensión de Galois de $\mathbb{Q}$ de grado 32.

2. Decidir si las raíces de la cúbica x^3+2x+1 son irracionales cuadráticos sobre el cuerpo $\mathbb{Q}(e^{2\pi i/7})$.

3. Si L y L' son dos extensiones de Galois de un cuerpo k, entonces $L \otimes_k L'$ descompone en suma directa de extensiones de k isomorfas entre sí.

4. Sean K_1 y K_2 dos extensiones de Galois de un cuerpo k, de grupos G_1 y G_2 respectivamente. Si L es un compuesto de K_1 y K_2, entonces $\bar{K} := K_1 \cap K_2$ y L son extensiones de Galois de k, y si $\bar{G}$ y G denotan sus respectivos grupos de Galois, entonces $G = G_1 \times_{\bar{G}} G_2 := \{(g_1, g_2) \in G_1 \times G_2\colon g_1|_{\bar{K}} = g_2|_{\bar{K}}\}$.

5. Si p es un número primo p, existen polinomios $q(x) \in \mathbb{Q}[x]$ cuyo grupo de Galois es cíclico de orden p. Hallar uno cuando $p = 5$.

6. ¿Qué parte del siguiente razonamiento es falaz? Si $k \to L'$ y $L' \to L$ son extensiones de Galois, entonces $k \to L$ también es una extensión de Galois:

$$L' \otimes_k L = L' \otimes_k L' \otimes_{L'} L = (\oplus L') \otimes_{L'} L = \oplus L$$
$$L \otimes_k L = L \otimes_{L'} (L' \otimes_k L) = L \otimes_{L'} (\oplus L) = \oplus(L \otimes_{L'} L) = \oplus(\oplus L)$$

7. Sean $k \to L'$ y $L' \to L$ extensiones de Galois. Si todo automorfismo de L' sobre k puede extenderse a un automorfismo de L sobre k, entonces L es una extensión de Galois de k.

8. Sea $k \to L$ una extensión de Galois de grupo G. Si H y H' son subgrupos de G, demostrar las siguientes afirmaciones:

   (a) $\mathrm{Aut}(L^H/k) = N(H)/H$.

   (b) La condición necesaria y suficiente para que L^H y $L^{H'}$ sean k-álgebras isomorfas es que H y H' sean subgrupos conjugados de G.

   (c) Si $j\colon L^H \to L^{H'}$ es un morfismo de k-álgebras, entonces existe un automorfismo $\tau \in G$ tal que $j(\alpha) = \tau(\alpha)$ para todo $\alpha \in L^H$

9. Determinar si $\mathbb{Q}(\sqrt{2+\sqrt{2}}\,)$ es una extensión de Galois de $\mathbb{Q}$.

10. Sea α una raíz de una cuártica irreducible $p(x) \in \mathbb{Q}[x]$. Demostrar que no existen cuerpos intermedios propios entre $\mathbb{Q}$ y $\mathbb{Q}(\alpha)$ si y sólo si el grupo de Galois de $p(x)$ es el grupo simétrico S_4 o el grupo alternado A_4.

11. Si una cuártica irreducible tiene exactamente dos raíces reales, probar que su grupo de Galois sobre $\mathbb{Q}$ es el grupo simétrico S_4 o el diédrico D_8.

12. El grupo de Galois sobre $\mathbb{Q}$ de una bicuadrada irreducible $x^4 + ax^2 + b$ es

    (a) El grupo de Klein V si b es un cuadrado.

    (b) El grupo cíclico C_4 si b no es un cuadrado, pero $a^2b - 4b^2$ sí lo es.

    (c) El grupo diédrico D_8 en cualquier otro caso.

13. El grupo de Galois sobre el cuerpo $\mathbb{Q}$ de una cuártica recíproca irreducible $x^4 + ax^3 + bx^2 + ax + 1$ es

    (a) El grupo de Klein V si $b^2 + 4b + 4 - 4a^2$ es un cuadrado.

    (b) El grupo cíclico C_4 cuando $b^2 + 4b + 4 - 4a^2$ no es un cuadrado, pero sí lo es $(b^2 + 4b + 4 - 4a^2)(a^2 - 4b + 8)$.

    (c) El grupo diédrico D_8 en cualquier otro caso.

14. Determinar el grupo de Galois de la bicuadrada genérica $x^4 + ax^2 + b$ y de la cuártica recíproca genérica $x^4 + ax^3 + bx^2 + ax + 1$ sobre $\mathbb{C}$.

15. Si p, q son números primos distintos, entonces p genera el grupo cíclico $(\mathbb{Z}/q\mathbb{Z})^*$ si y sólo si el polinomio $x^{q-1} + \ldots + x + 1$ es irreducible en $\mathbb{F}_p[x]$.

16. Sea L una extensión de Galois de $\mathbb{Q}$ de grupo G. Si G no es cíclico, L es el cuerpo de descomposición de un polinomio $q(x) \in \mathbb{Q}[x]$ sin raíces racionales que admite raíz modular en casi todo primo.

17. Sea $p(x)$ un polinomio de grado n con coeficientes racionales y sin raíces racionales. Si cada automorfismo de su grupo de Galois deja fija alguna raíz de $p(x)$, entonces $n \geq 5$ (i.e., si $p(x)$ admite raíces modulares en casi todo primo, entonces su grado es mayor que 4).

18. Dado un número natural $n \geq 2$, considérese la siguiente afirmación (que sabemos es falsa cuando $n = 8$, véase el ejemplo de la página 377 y el ejercicio 49 en la página 225):

    Si un polinomio con coeficientes enteros $x^n - b$ tiene raíz modular en casi todo número primo, entonces b es potencia n-ésima de algún número entero.

    Usando el teorema de Tchebotarev (y por supuesto el teorema H.3.12) probar que la afirmación es cierta cuando $n \leq 7$ y cuando n es primo. (*Indicación:* Si n es primo, $x^n - b$ es irreducible o su grupo de Galois es cíclico.)

    Además, en el caso $n = 8$, la afirmación sólo es falsa cuando $b = 2^4 a^8$ para algún número entero a.

Apéndice I

Separabilidad

En este apéndice k denotará un cuerpo arbitrario.

I.1 Álgebras Racionales

Teorema de Descomposición: *Toda k-álgebra finita A descompone en suma directa de k-álgebras locales, que son las localizaciones en los puntos de su espectro:*

$$A = A_{x_1} \oplus \ldots \oplus A_{x_n} \qquad , \qquad \operatorname{Spec} A = \{x_1, \ldots, x_n\}$$

Demostración: Los morfismos de localización $A \to A_x$, $a \mapsto a/1$, inducen un morfismo de k-álgebras canónico

$$A \longrightarrow A_{x_1} \oplus \ldots \oplus A_{x_n}$$

y vamos a probar que es un isomorfismo. Basta probar que lo es después de localizar en cualquier punto $y \in \operatorname{Spec} A$. Ahora bien,

$$(A_{x_1} \oplus \ldots \oplus A_{x_n})_y = (A_{x_1})_y \oplus \ldots \oplus (A_{x_n})_y = A_y$$

porque $(A_y)_y = A_y$ y $(A_x)_y = 0$ cuando $x \neq y$. En efecto, los puntos del espectro de $(A_x)_y$ se corresponde con los ideales primos de A contenidos en $\mathfrak{m}_x$ y $\mathfrak{m}_y$, ideales que no existen al ser maximales todos los ideales primos de A. Luego tal espectro es vacío y por 6.1.3 concluimos que $(A_x)_y = 0$.

Lema I.1.1 *Sea A una k-álgebra finita y sea I un ideal de A contenido en todos los ideales maximales de A. La condición necesaria y suficiente para que A sea k-álgebra racional es que lo sea A/I.*

Demostración: De acuerdo con 6.1.2, cada ideal maximal $\mathfrak{m}$ de A se corresponde con un ideal maximal $\bar{\mathfrak{m}}$ de $\bar{A} = A/I$, y $A/\mathfrak{m} = \bar{A}/\bar{\mathfrak{m}}$.

Lema I.1.2 *El concepto de álgebra finita local y racional es estable por cambios del cuerpo base. Es decir, si A es una k-álgebra finita local y racional y L es una extensión de k, entonces $A_L = A \otimes_k L$ es una L-álgebra finita local y racional.*

Demostración: Si $\mathfrak{m}$ es el único ideal maximal de A, por hipótesis $k = A/\mathfrak{m}$; luego

$$A_L/\mathfrak{m}A_L \;=\; (A/\mathfrak{m}) \otimes_A (A \otimes_k L) \;=\; (A/\mathfrak{m}) \otimes_k L \;=\; k \otimes_k L \;=\; L$$

es un cuerpo y obtenemos que $\mathfrak{m}A_L$ es un ideal maximal de A_L cuyo cuerpo residual es L. Además todos los elementos de $\mathfrak{m}$ son nilpotentes, así que $\mathfrak{m}A_L$ es un ideal generado por elementos nilpotentes y ha de estar contenido en todos los ideales maximales de A_L. Concluimos que $\mathfrak{m}A_L$ es el único ideal maximal de A_L y que A_L es L-álgebra racional.

Propiedades de las Álgebras Racionales:

1. *Subálgebras, cocientes sumas directas y productos tensoriales de k-álgebras racionales son k-álgebras racionales.*

2. *El concepto de álgebra racional es estable por cambios del cuerpo base (es decir, si A es una k-álgebra racional y L es una extensión de k, entonces $A_L = A \otimes_k L$ es una L-álgebra racional).*

Demostración: (1) Sea A una subálgebra de una k-álgebra finita racional B. La aplicación $\operatorname{Spec} B \to \operatorname{Spec} A$ inducida por el morfismo de inclusión $A \to B$ es epiyectiva por H.2.10 y transforma puntos racionales en puntos racionales por G.2.1. Como todos los puntos de $\operatorname{Spec} B$ son racionales por hipótesis, concluimos que también lo son todos los puntos de $\operatorname{Spec} A$.

Sea A una k-álgebra finita racional y sea I un ideal de A. Si $\bar{\mathfrak{m}}$ es un ideal maximal de $\bar{A} := A/I$, por 6.1.2 se corresponde con un ideal maximal $\mathfrak{m}$ de A que contiene a I tal que $A/\mathfrak{m} = \bar{A}/\bar{\mathfrak{m}}$. Por hipótesis $k = A/\mathfrak{m} = \bar{A}/\bar{\mathfrak{m}}$ y concluimos que A/I es una k-álgebra finita racional.

Por 7.2.3, $\operatorname{Spec}(A \oplus B) = (\operatorname{Spec} A) \sqcup (\operatorname{Spec} B)$, así que todos los puntos de $\operatorname{Spec}(A \oplus B)$ son racionales cuando lo son los de $\operatorname{Spec} A$ y $\operatorname{Spec} B$.

En cuanto a la demostración de que $A \otimes_k B$ es k-álgebra racional, en virtud del teorema de descomposición y el carácter distributivo de la suma directa respecto del producto tensorial, podemos reducirnos al caso en que A y B son k-álgebras finitas locales y racionales. Sea $\mathfrak{m}$ el único ideal maximal de A. Como el ideal $\mathfrak{m}(A \otimes_k B)$ está generado por elementos nilpotentes, según I.1.1 basta probar que

$$(A \otimes_k B)/\mathfrak{m}(A \otimes_k B) = (A/\mathfrak{m}) \otimes_A (A \otimes_k B) = (A/\mathfrak{m}) \otimes_k B = k \otimes_k B = B$$

es k-álgebra racional, y lo es por hipótesis.

(2) Sea A una k-álgebra finita. Por el teorema de descomposición tenemos que $A = A_1 \oplus \ldots \oplus A_n$ donde las componentes A_i son k-álgebras finitas locales. Si A

es racional, tales componentes son k-álgebras finitas locales y racionales; luego las L-álgebras $(A_i)_L$ son racionales en virtud de I.1.2. El apartado 1 permite concluir que la L-álgebra finita $A_L = (A_1)_L \oplus \ldots \oplus (A_n)_L$ también es racional.

Teorema I.1.3 *Toda k-álgebra finita A es racional sobre alguna extensión finita L de k (i.e., A_L es L-álgebra racional).*

Demostración: Procedemos por inducción sobre el grado $d = [A : k]$, porque el morfismo estructural $k \to A$ es un isomorfismo cuando $d = 1$, de modo que en tal caso A es racional sobre k.

Cuando $d > 1$, siempre existe algún punto de A con valores en una extensión finita K de k (por ejemplo, basta tomar como K el cuerpo residual de un punto del espectro de A). Por la fórmula de los puntos, $\operatorname{Spec} A_K$ tiene algún punto racional, y el teorema de descomposición permite obtener que $A_K = B \oplus C$, donde B es una K-álgebra finita local y racional.

Como $[C : K] < [A_K : K] = d$, por hipótesis de inducción C es racional sobre una extensión finita L de K, de modo que $A_L = (A_K)_L = B_L \oplus C_L$ es L-álgebra racional (B_L es L-álgebra racional porque B es K-álgebra racional). Concluimos que A es racional sobre L, que es una extensión finita de k.

I.2 Métrica de la Traza

Definición: Sea A una k-álgebra finita. Cada elemento $a \in A$ define un endomorfismo k-lineal $h_a \colon A \to A$, $h_a(b) = ab$, y diremos que la traza y el determinante de h_a son la **traza** y la **norma** de a:

$$\operatorname{tr}_{A/k}(a) := \operatorname{tr}(h_a)$$
$$\mathrm{N}_{A/k}(a) := \det(h_a)$$

La traza y la norma son invariantes por cambios del cuerpo base, en el sentido de que para toda extensión $k \to L$ tenemos

$$\operatorname{tr}_{A/k}(a) := \operatorname{tr}_{A_L/L}(a \otimes 1)$$
$$\mathrm{N}_{A/k}(a) := \mathrm{N}_{A_L/L}(a \otimes 1)$$

porque la matriz de h_a en cualquier base $(e_1, \ldots, e_d)$ de A coincide con la matriz de $h_{a\otimes 1}$ en la base $(e_1 \otimes 1, \ldots, e_d \otimes 1)$ de A_L.

La traza $\operatorname{tr} \colon A \to k$ es una aplicación lineal y permite definir en A una métrica (aplicación bilineal simétrica)

$$T_2(a, b) := \operatorname{tr}(ab)$$

llamada **métrica de la traza** . El radical de la métrica de la traza

$$\operatorname{Rad}(A/k) := \{a \in A \colon \operatorname{tr}(ab) = 0,\ \forall b \in A\}$$

es un ideal de A, y contiene a los elementos nilpotentes de A

$$\operatorname{rad} A \ \subseteq \ \operatorname{Rad}(A/k)$$

porque la traza de los endomorfismos nilpotentes es nula (pues su polinomio característico es una potencia de x según el teorema de Hamilton-Cayley). Además, como la traza es invariante por cambios del cuerpo base, $\operatorname{tr}(a\otimes 1) = \operatorname{tr}(a)$, también la métrica de la traza y su radical son estables por cambios del cuerpo base; i.e., para toda extensión $k \to L$ tenemos que

$$\operatorname{Rad}(A_L/L) \ = \ \operatorname{Rad}(A) \otimes_k L \ .$$

Ejemplo I.2.1 En el caso de una k-álgebra finita trivial $A = k\oplus\ldots\oplus k$, si consideramos la base $e_1 = (1,0,\ldots,0),\ldots,\ e_d = (0,\ldots,0,1)$, la matriz del endomorfismo h_a definido por $a = (\lambda_1,\ldots,\lambda_n)$ es la matriz diagonal $\operatorname{diag}(\lambda_1,\ldots,\lambda_n)$. Luego

$$\begin{aligned} \operatorname{tr}(a) &= \lambda_1 + \ldots + \lambda_n \\ \mathrm{N}(a) &= \lambda_1 \cdot \ldots \cdot \lambda_n \\ T_2(e_i,e_j) &= \operatorname{tr}(e_i e_j) = \delta_{ij} \end{aligned}$$

y vemos que la métrica de la traza no es singular: $\operatorname{Rad}(A/k) = 0$.

En el caso de una k-álgebra finita separable A, es trivial sobre alguna extensión L de k, así que el número de puntos $\sigma_1,\ldots,\sigma_d\colon A \to L$ iguala al grado y

$$A_L = L \oplus \ldots \oplus L \qquad , \qquad a \otimes 1 = \big(\sigma_1(a),\ldots,\sigma_d(a)\big)$$

porque las proyecciones de A_L sobre sus componentes definen d morfismos $A \to L$; luego son todos los morfismos porque su número nunca supera al grado. Como la traza y la norma son invariantes por cambios de base, obtenemos que

$$\begin{aligned} \operatorname{tr}(a) &= \sigma_1(a) + \ldots + \sigma_d(a) \\ \mathrm{N}(a) &= \sigma_1(a) \cdot \ldots \cdot \sigma_d(a) \end{aligned}$$

Teorema I.2.2 *La condición necesaria y suficiente para que una k-álgebra finita A sea separable es que su métrica de la traza no sea singular; es decir, que*

$$\operatorname{Rad}(A/k) = 0 \ .$$

Demostración: Si el radical de la métrica de la traza $\operatorname{Rad}(A/k)$ es nulo, entonces para toda extensión $k \to L$ tenemos que el álgebra A_L es reducida porque

$$\operatorname{rad}(A_L) \ \subseteq \ \operatorname{Rad}(A_L/L) \ = \ \operatorname{Rad}(A/k)_L = 0 \ .$$

Recíprocamente, si A es separable, entonces es trivial sobre alguna extensión L de k, de modo que en A_L la métrica de la traza no es singular. Luego

$$\operatorname{Rad}(A/k)_L = \operatorname{Rad}(A_L/L) = 0$$

y concluimos que $\operatorname{Rad}(A/k) = 0$.

Corolario I.2.3 *La condición necesaria y suficiente para que una extensión finita sea separable es que tenga algún elemento de traza no nula.*

Demostración: Sea $k \to L$ una extensión finita. Si la traza $\mathrm{tr}\colon L \to k$ es nula, entonces $\mathrm{Rad}(L/k) = L$ y el teorema anterior permite concluir que la extensión es inseparable.

Recíprocamente, si existe $\alpha \in L$ tal que $\mathrm{tr}(\alpha) \neq 0$, entonces $\mathrm{Rad}(L/k) = 0$ porque es un ideal del cuerpo L que no contiene a α, y el teorema anterior permite concluir que la extensión es separable.

Corolario I.2.4 *Si una extensión finita de k es inseparable, entonces su grado es múltiplo de la característica de k.*

Demostración: Si $k \to L$ es una extensión finita inseparable, por el corolario anterior tenemos $0 = \mathrm{tr}(1) = [L : k]$.

I.3 Álgebras Inseparables

Lema I.3.1 *Sea A una k-álgebra finita racional. Si $\Omega_{A/k} = 0$, entonces A es trivial.*

Demostración: Descomponiendo A en suma directa de álgebras locales podemos suponer que tiene un único ideal maximal $\mathfrak{m}$. Por hipótesis el único punto del espectro de A es racional, así que $\mathfrak{m}/\mathfrak{m}^2 = \Omega_{A/k} \otimes_A k = 0$ por 9.2.4, y el lema de Nakayama permite concluir que $\mathfrak{m} = 0$ y $A = k$.

Teorema I.3.2 *La condición necesaria y suficiente para que una k-álgebra finita A sea separable es que $\Omega_{A/k} = 0$.*

Demostración: Si A es separable, en particular es reducida y descompone en suma directa de extensiones de k por G.1.5; luego $A \otimes_k A$ es reducida, porque A_L es reducida para toda extensión L de k. Luego $A \otimes_k A = L_1 \oplus \ldots \oplus L_n$ para ciertas extensiones L_i de k, y se sigue que el ideal de la diagonal es de la forma $\Delta = L_1 \oplus \ldots \oplus L_r \oplus 0 \ldots \oplus 0$ después de reordenar las componentes si fuera necesario. Ahora es evidente que $\Delta^2 = \Delta$ y concluimos que $\Omega_{A/k} = \Delta/\Delta^2 = 0$.

Recíprocamente, si $\Omega_{A/k} = 0$, entonces $\Omega_{A_L/L} = 0$ para toda extensión L de k. Por el teorema de Kronecker podemos elegir L de modo que A_L sea L-álgebra racional, en cuyo caso el lema anterior afirma que A_L es L-álgebra trivial y concluimos que A es separable.

Grado de Separabilidad

Definición: Por G.4.4, cada k-álgebra finita A contiene una única subálgebra separable maximal, formada por todos sus elementos separables, que denotaremos $\pi_0^k(A)$. Llamaremos **grado de separabilidad** de A sobre k al grado de $\pi_0^k(A)$ y lo denotaremos

$$[A:k]_s := [\pi_0^k(A):k] \ .$$

Sean A, B dos k-álgebras finitas. Si $f\colon A \to B$ es un morfismo de k-álgebras, entonces $f(\pi_0^k(A))$ es una subálgebra separable de B, porque es un cociente de $\pi_0^k(A)$, así que está contenida en $\pi_0^k(B)$ y f define un morfismo de k-álgebras $f\colon \pi_0^k(A) \to \pi_0^k(B)$. Por tanto π_0^k es un funtor covariante de la categoría de k-álgebras finitas en la categoría de k-álgebras finitas separables.

Teorema I.3.3 *La subálgebra separable maximal es estable por cambios del cuerpo base. Es decir, si A es una k-álgebra finita y L es una extensión de k, entonces*

$$\pi_0^k(A) \otimes_k L \ = \ \pi_0^L(A \otimes_k L)$$

Demostración:[1] El núcleo A_1 de la diferencial $d\colon A \to \Omega_{A/k}$ contiene a $\pi_0^k(A)$ de acuerdo con I.3.2. Si definimos recursivamente A_{n+1} como el núcleo de la diferencial $d\colon A_n \to \Omega_{A_n/k}$, tenemos que $\pi_0^k(A) \subseteq \bigcap_n A_n$. Cuando se dé una igualdad $A_{n+1} = A_n$, por I.3.2 la k-álgebra A_n es separable y $A_n \subseteq \pi_0^k(A)$, Concluimos que

$$\pi_0^k(A) = \bigcap_n A_n \ .$$

Ahora el enunciado es evidente, porque la subálgebra $\bigcap_n A_n$ es estable por cambios del cuerpo base al serlo el módulo de las diferenciales (9.3.1).

Corolario I.3.4 *Sea A una k-álgebra finita y L una extensión de k tal que A_L es L-álgebra racional. El grado de separabilidad $[A:k]_s$ coincide con el número de puntos de A con valores en L.*

Demostración: Por el teorema anterior $[A:k]_s = [A_L:L]_s$, así que podemos suponer que A es una k-álgebra racional y $k = L$. En tal caso, por la fórmula de los puntos, el número n de puntos $A \to k$ coincide con el número de puntos de $\operatorname{Spec} A$, así que A descompone en suma directa de n álgebras racionales. El morfismo natural $\pi_0^k(A) \to A/\operatorname{rad} A = k^n$ es inyectivo porque un álgebra separable es reducida, y es epiyectivo porque claramente $k^n \subseteq \pi_0^k(A)$; luego

$$[A:k]_s = [\pi_0^k(A):k] = n \ .$$

[1] Esta demostración se debe a Juan B. Sancho de Salas en el ya lejano 1976, cuando cursaba el segundo curso de la licenciatura.

Corolario I.3.5 $[A \oplus B : k]_s = [A : k]_s + [B : k]_s$
$[A \otimes_k B : k]_s = [A : k]_s [B : k]_s$

Demostración: Basta considerar una extensión $k \to L$ que racionalice a ambas k-álgebras finitas A, B y aplicar I.3.4.

Corolario I.3.6 $\pi_0^k(A \oplus B) = \pi_0^k(A) \oplus \pi_0^k(B)$
$\pi_0^k(A \otimes_k B) = \pi_0^k(A) \otimes \pi_0^k(B)$

Demostración: Las inclusiones $\pi_0^k(A) \oplus \pi_0^k(B) \subseteq \pi_0^k(A \oplus B)$ y $\pi_0^k(A) \otimes \pi_0^k(B) \subseteq \pi_0^k(A \otimes_k B)$ son inmediatas, y los dos términos de cada inclusión tienen el mismo grado por I.3.5

Corolario I.3.7 *La condición necesaria y suficiente para que una k-álgebra finita A sea local es que $\pi_0^k(A)$ sea un cuerpo.*

Demostración: Si A es local, también lo son todas sus subálgebras por H.2.10; luego son cuerpos si además son separables.

Recíprocamente, si A descompone en suma directa de dos o más álgebras locales, $A = A_1 \oplus \ldots \oplus A_n$, entonces $\pi_0^k(A) = \pi_0^k(A_1) \oplus \ldots \oplus \pi_0^k(A_n)$ tampoco es local, y en particular no es un cuerpo.

Corolario I.3.8 *El grado de separabilidad sobre k del álgebra $k[x]/\big(p(x)\big)$ coincide con el número de raíces diferentes del polinomio $p(x)$ en una extensión donde tenga todas sus raíces.*

Demostración: Es consecuencia directa de I.3.4.

Corolario I.3.9 *Sean A y B dos k-álgebras finitas. Si un morfismo de k-álgebras $A \to B$ es epiyectivo, el correspondiente morfismo $\pi_0^k(A) \to \pi_0^k(B)$ también es epiyectivo.*

Demostración: Como la subálgebra separable maximal es estable por cambios del cuerpo base, por el teorema de Kronecker podemos suponer que la k-álgebra finita A es racional. Como el funtor π_0^k conserva sumas directas, podemos suponer además que A es una k-álgebra local racional, caso en que el enunciado es trivial.

Corolario I.3.10 *Sea L el cuerpo residual de una k-álgebra finita local A. Si L es una extensión separable de k, entonces existe una única subálgebra $L' \subset A$ tal que la proyección natural $L' \to L$ es un isomorfismo.*

Demostración: El proyección natural $\pi_0^k(A) \to \pi_0^k(L) = L$ es epiyectiva por I.3.9, y es inyectiva por I.3.7. Cualquier otra subálgebra L' tal que la proyección $L' \to L$ sea un isomorfismo es separable; luego $L' \subseteq \pi_0^k(A)$ y coinciden porque el grado de ambas álgebras coincide con el grado de L.

I.4 Álgebras Puramente Inseparables

Definición: Diremos que una k-álgebra finita A es **puramente inseparable** si es geométricamente local; es decir, si $A_L = A \otimes_k L$ es local para toda extensión $k \to L$.

Las k-álgebras locales y racionales son puramente inseparables por I.1.2.

Caracterización de las Álgebras Puramente Inseparables: *Si A es una k-álgebra finita, las siguientes condiciones son equivalentes:*

1. *A es puramente inseparable.*
2. *Existe una extensión $k \to L$ tal que la L-álgebra A_L es local y racional.*
3. *$\pi_0^k(A) = k$.*

Demostración: Por el teorema de Kronecker existe una extensión $k \to L$ tal que A_L es racional. Si A es puramente inseparable, entonces A_L es local y racional.

Si A_L es local y racional para alguna extensión $k \to L$, entonces $\pi_0^k(A)_L = \pi_0^L(A_L) = L$ y concluimos que $\pi_0^k(A) = k$.

Por último, si $\pi_0^k(A) = k$, entonces para toda extensión $k \to L$ tenemos que $\pi_0^L(A_L) = \pi_0^k(A)_L = L$ y I.3.7 permite concluir que A_L es local.

Propiedades de las Álgebras Puramente Inseparables:

1. *Subálgebras, cocientes y productos tensoriales de k-álgebras puramente inseparables son k-álgebras puramente inseparables.*
2. *Sea $k \to L$ una extensión. La condición necesaria y suficiente para que una k-álgebra finita A sea puramente inseparable es que la L-álgebra finita A_L sea puramente inseparable.*

Demostración: La primera propiedad se sigue de que subálgebras y cocientes de álgebras finitas locales son locales (H.2.10) y $\pi_0^k(A \otimes_k B) = \pi_0^k(A) \otimes_k \pi_0^k(B)$.

Por último, la igualdad $\pi_0^L(A_L) = \pi_0^k(A)_L$ muestra que una k-álgebra finita A es puramente inseparable precisamente cuando la L-álgebra A_L es puramente inseparable.

Ejemplo: Diremos que un polinomio $p(x) \in k[x]$ es puramente inseparable cuando lo sea la k-álgebra finita $k[x]/\big(p(x)\big)$; es decir, cuando todas las raíces de $p(x)$ sean iguales, en el sentido de que en alguna extensión de k tengamos $p(x) = (x-\alpha)^n$.

Cuando k es un cuerpo de característica positiva p, todos los polinomios $x^{p^n} - a$ son puramente inseparables, pues si α es una raíz, $\alpha^{p^n} = a$, entonces

$$x^{p^n} - a = x^{p^n} - \alpha^{p^n} = (x-\alpha)^{p^n} \ .$$

Lema I.4.1 *Sea k es un cuerpo de característica positiva p. La condición necesaria y suficiente para que una extensión finita $k \to k(\alpha)$ sea puramente inseparable es que α sea raíz de algún polinomio $x^{p^n} - a$.*

Demostración: Sea $q_\alpha(x)$ el polinomio irreducible de α sobre k. Si α es raíz de $x^{p^n} - a$ entonces $q_\alpha(x)$ divide a $x^{p^n} - a = (x - \alpha)^{p^n}$; luego todas sus raíces son iguales y $k(\alpha) = k[x]/\big(q_\alpha(x)\big)$ es puramente inseparable.

Recíprocamente, sea p^n la mayor potencia de p tal que $q_\alpha(x) = q(x^{p^n})$ para algún polinomio $q(x)$, que necesariamente será separable al ser irreducible y $q'(x) \neq 0$. Si $k(\alpha)$ es una extensión puramente inseparable, entonces $a := \alpha^{p^n} \in k$ y concluimos que α es raíz del polinomio $x^{p^n} - a$.

De hecho $q_\alpha(x) = x^{p^n} - a$ porque el grado de $q_\alpha(x)$ es obviamente $\geq p^n$.

Teorema I.4.2 *La condición necesaria y suficiente para que una extensión finita $k \to L$ sea puramente inseparable es que esté generada por raíces de polinomios de la forma $x^{p^n} - a$, donde p es la característica de k.*

Demostración: Es consecuencia directa de I.4.1, y de que toda subálgebra de una k-álgebra finita puramente inseparable también es puramente inseparable.

Extensiones Normales

Definición: Diremos que una extensión finita $k \to L$ es **normal** si $L \otimes_k L$ es L-álgebra racional.

Caracterización de las Extensiones Normales: *Si $k \to L$ es una extensión finita, las siguientes condiciones son equivalentes:*

1. *L es el cuerpo de descomposición de algún polinomio con coeficientes en k.*
2. *Todo compuesto de L consigo mismo es isomorfo a L.*
3. *$L \otimes_k L$ es L-álgebra racional.*
4. *Todo polinomio irreducible en $k[x]$ que tenga alguna raíz en L tiene todas sus raíces en L.*

Demostración: Totalmente análoga a la demostración de la caracterización de las extensiones de Galois dada en la página 362.

Propiedades de las Extensiones Normales: *Sea $k \to L$ una extensión normal.*

1. *Si $k \to L' \to L$ es un cuerpo intermedio, entonces L es una extensión normal de L'.*

2. *Si $k \to E$ es una extensión arbitraria, cualquier compuesto LE es una extensión normal de E.*

3. *Si L' es una extensión normal de k, cualquier compuesto $L'L$ es una extensión normal de k.*

Demostración: Totalmente análoga a la demostración de las propiedades de las extensiones de Galois dada en la página 363.

Teorema I.4.3 *Toda extensión finita normal $k \to L$ de grupo $G := \mathrm{Aut}(L/k)$ descompone de modo canónico en producto tensorial de una extensión de Galois de grupo G y una extensión puramente inseparable:*

$$L \;=\; \pi_0^k(L) \otimes_k L^G \;.$$

Demostración: Pongamos $L_s := \pi_0^k(L)$, $L_i := L^G$. La extensión L_i es racional sobre L, porque lo es L, y admite un único morfismo de k-álgebras $L_i \to L$ en virtud de H.2.11. Luego es una extensión puramente inseparable de k por I.3.4.

Se sigue que $L_s \otimes_k L_i$ es una k-álgebra local y, como es reducida porque L_s es separable, tenemos que es un cuerpo. Luego el morfismo natural $L_s \otimes_k L_i \to L$ es inyectivo. Es epiyectivo porque el orden de G coincide con $[L : L^G] = [L : L_i]$ según el teorema de Artin, y coincide con $[L_s : k] = [L_s \otimes_k L_i : L_i]$ por I.3.4. Luego $L = L_s \otimes_k L_i$.

Se sigue que el morfismo de restricción $G \to \mathrm{Aut}(L_s/k)$ es inyectivo y, al coincidir el orden de G con $[L_s : k]$, concluimos que L_s es una extensión de Galois de grupo G.

Apéndice J

Extensiones Algebraicas y Trascendentes

J.1 Cierre Algebraico

Teorema J.1.1 *Sea k un cuerpo. Las siguientes condiciones son equivalentes:*

1. *Todo polinomio no constante $p(x) \in k[x]$ tiene todas sus raíces en k.*
2. *Todo polinomio no constante $p(x) \in k[x]$ tiene alguna raíz en k.*
3. *Todo polinomio irreducible $q(x) \in k[x]$ es de grado 1.*
4. *Toda extensión algebraica de k es trivial (i.e., de grado 1).*

Demostración: $(1 \Rightarrow 2)$ es evidente.

$(2 \Rightarrow 3)$ Por la regla de Ruffini, si un polinomio irreducible en $k[x]$ tiene una raíz en k, su grado ha de ser 1.

$(3 \Rightarrow 4)$ Sea α un elemento de una extensión algebraica K de k. Por hipótesis su polinomio irreducible $p_\alpha(x)$ sobre k tiene grado 1. Ahora bien, un polinomio de grado 1 sólo puede tener una raíz en K y, si sus coeficientes están en k, tiene una raíz en k. Luego $\alpha \in k$ y concluimos que el morfismo estructural $k \to K$ es un isomorfismo.

$(4 \Rightarrow 1)$ Por el teorema de Kronecker, $p(x)$ tiene todas sus raíces en alguna extensión finita K de k. Toda extensión finita es algebraica, luego, por hipótesis, $K = k$ y concluimos que $p(x)$ tiene todas sus raíces en k.

Definición: Diremos que un cuerpo es **algebraicamente cerrado** cuando satisface las condiciones equivalentes del teorema anterior. Diremos que una extensión $\bar{k}$ de un cuerpo k es un **cierre algebraico** de k si es una extensión algebraica y $\bar{k}$ es un cuerpo algebraicamente cerrado.

Ejemplos:

1. Por el teorema de D'Alembert (1717-1783) el cuerpo de los números complejos es algebraicamente cerrado y, al ser una extensión finita de los números reales, se sigue que $\mathbb{C}$ es un cierre algebraico de $\mathbb{R}$.

2. Los números complejos algebraicos sobre $\mathbb{Q}$ forman, de acuerdo con 4.4.6, una extensión algebraica $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ y, por 4.4.7, el cuerpo $\bar{\mathbb{Q}}$ es algebraicamente cerrado. Luego $\bar{\mathbb{Q}}$ es un cierre algebraico de $\mathbb{Q}$.

   El grado de $\bar{\mathbb{Q}}$ sobre $\mathbb{Q}$ es infinito, porque contiene extensiones de grado arbitrariamente grande como, por ejemplo, $\mathbb{Q}(\sqrt[n]{2}\,)$.

3. Ningún cuerpo algebraicamente cerrado puede ser finito. Para demostrarlo consideremos un cuerpo finito $\mathbb{F}_q$ con q elementos. El grupo multiplicativo de sus elementos no nulos tiene orden $q-1$, así que todo $a \in \mathbb{F}_q$ no nulo es raíz de $x^{q-1}-1$. Se sigue que todos los elementos de $\mathbb{F}_q$ son raíces del polinomio $x^q - x$; luego $x^q - x - 1$ no tiene raíces en $\mathbb{F}_q$ y concluimos que $\mathbb{F}_q$ no es algebraicamente cerrado.

Teorema de Existencia: *Todo cuerpo admite un cierre algebraico.*

Demostración: Sea k un cuerpo. Según el teorema de Kronecker, cada polinomio irreducible $p(x)$ con coeficientes en k tiene todas sus raíces en alguna extensión finita K_p de k. Para cada familia finita $\{p_1, \ldots, p_r\}$ de polinomios irreducibles con coeficientes en k consideraremos la k-álgebra finita $K_{p_1} \otimes_k \cdots \otimes_k K_{p_r}$. Cuando $\{p_1, \ldots, p_r\} \subseteq \{q_1, \ldots, q_s\}$, el morfismo natural

$$K_{p_1} \otimes_k \cdots \otimes_k K_{p_r} \longrightarrow K_{q_1} \otimes_k \cdots \otimes_k K_{q_s}$$

es inyectivo y nos permite identificar $K_{p_1} \otimes_k \cdots \otimes_k K_{p_r}$ con una subálgebra de $K_{q_1} \otimes_k \cdots \otimes_k K_{q_s}$, identificación que haremos en lo sucesivo sin más indicación. Consideremos ahora la k-álgebra

$$A = \bigcup_{\{p_1,\ldots,p_r\}} K_{p_1} \otimes_k \cdots \otimes_k K_{p_r}$$

y el cuerpo residual $\bar{k} = A/\mathfrak{m}$ de un ideal maximal $\mathfrak{m}$ de A. Por construcción tenemos morfismos de k-álgebras $K_p \to A \to \bar{k}$, así que cada polinomio irreducible $p(x)$ con coeficientes en k tiene todas sus raíces en $\bar{k}$. Además, $\bar{k}$ está generado como k-álgebra por las clases de restos de los elementos $1 \otimes \cdots \otimes \lambda_i \otimes \cdots \otimes 1 \in A$, que son algebraicos sobre k; luego $\bar{k}$ es una extensión algebraica de k.

Para concluir que $\bar{k}$ es un cierre algebraico de k bastará ver que toda extensión algebraica K de $\bar{k}$ es trivial. Si $\alpha \in K$, por 4.4.7 tenemos que α es algebraico sobre k; luego es raíz de algún polinomio irreducible $p_\alpha(x)$ con coeficientes en k. Como $p_\alpha(x)$ tiene todas sus raíces en $\bar{k}$, se sigue que $\alpha \in \bar{k}$ y concluimos que $\bar{k} = K$.

Teorema J.1.2 *Sea $\bar{k}$ un cierre algebraico de un cuerpo k. Toda extensión algebraica K de k puede sumergirse en $\bar{k}$; es decir, existe algún morfismo (necesariamente inyectivo) de k-álgebras $K \to \bar{k}$.*

Demostración: Consideremos el cuerpo residual $K\bar{k} = (K \otimes_k \bar{k})/\mathfrak{m}$ de algún ideal maximal $\mathfrak{m}$ de $K \otimes_k \bar{k}$, y los morfismos naturales $\bar{k} \to K\bar{k}$, $K \to K\bar{k}$. Todo elemento de $K\bar{k}$ proviene de algún elemento $\sum_i \alpha_i \otimes \beta_i$, $\alpha_i \in K$, $\beta_i \in \bar{k}$, así que $K\bar{k}$ es una extensión de $\bar{k}$ generada por los elementos de K, que son algebraicos sobre k y, por tanto, sobre $\bar{k}$. Luego $K\bar{k}$ es una extensión algebraica de $\bar{k}$ y concluimos que el morfismo natural $\bar{k} \to K\bar{k}$ es un isomorfismo de k-álgebras, de modo que el morfismo natural $K \to K\bar{k}$ define un morfismo $K \to \bar{k}$.

Teorema de Unicidad: *El cierre algebraico de un cuerpo k es único salvo isomorfismos (no canónicos) de k-álgebras.*

Demostración: Sean $\bar{k}$ y $\bar{k}'$ dos cierres algebraicos de k. De acuerdo con el teorema anterior, existe un morfismo de k-álgebras $\bar{k}' \to \bar{k}$; luego $\bar{k}$ es una extensión algebraica de $\bar{k}'$ y concluimos que $\bar{k}' \to \bar{k}$ es un isomorfismo porque el cuerpo $\bar{k}'$ es algebraicamente cerrado.

J.2 Extensiones Trascendentes

Definición: Sea Σ una extensión de un cuerpo k. Diremos que unos elementos $\alpha_1, \ldots, \alpha_n \in \Sigma$ son **algebraicamente independientes** sobre k cuando el correspondiente morfismo de k-álgebras $k[x_1, \ldots, x_n] \to \Sigma$, $x_i \mapsto \alpha_i$, sea inyectivo; es decir, cuando cualquier relación algebraica

$$\sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n} = 0$$

con coeficientes en k tenga todos sus coeficientes nulos. En particular los elementos $\alpha_1, \ldots, \alpha_n$ son trascendentes sobre k. Diremos que $\alpha_1, \ldots, \alpha_n$ forman una **base de trascendencia** de Σ sobre k cuando sean algebraicamente independientes y Σ sea una extensión algebraica de $k(\alpha_1, \ldots, \alpha_n)$; es decir, si son algebraicamente independientes sobre k y no pueden ampliarse con ningún elemento de Σ de modo que sigan siendo algebraicamente independientes sobre k.

Teorema J.2.1 *Sea Σ una extensión de un cuerpo k generada por un número finito de elementos. Existen bases de trascendencia de Σ sobre k y todas tienen el mismo número de elementos, llamado* ***grado de trascendencia*** *de Σ sobre k.*

Demostración: Sea $\Sigma = k(\alpha_1, \ldots, \alpha_r)$. Reordenando los generadores si fuera preciso, podemos suponer que $\alpha_1, \ldots, \alpha_n$ son algebraicamente independientes sobre k y que $\alpha_1, \ldots, \alpha_n, \alpha_i$ son algebraicamente dependientes para todo $n+1 \leq i \leq r$, de

modo que α_i es algebraico sobre $k(\alpha_1,\dots,\alpha_n)$. Por 4.4.6, $k(\alpha_1,\dots,\alpha_n,\dots,\alpha_r) = \Sigma$ es una extensión algebraica de $k(\alpha_1,\dots,\alpha_n)$ y concluimos que $\{\alpha_1,\dots,\alpha_n\}$ es una base de trascendencia de Σ sobre k.

Por otra parte, si $\{\beta_1,\dots,\beta_m\}$ es otra base de trascendencia de Σ sobre k, probaremos por inducción sobre i que, reordenándola si fuera preciso, Σ es una extensión algebraica de $k(\alpha_1,\dots,\alpha_i,\beta_{i+1},\dots,\beta_m)$. Cuando $i=0$ es cierto, pues Σ es una extensión algebraica de $k(\beta_1,\dots,\beta_m)$. Si $i\geq 1$, por hipótesis de inducción α_i es algebraico sobre $k(\alpha_1,\dots,\alpha_{i-1},\beta_i,\dots,\beta_m)$, así que $\alpha_1,\dots,\alpha_i,\beta_i,\dots,\beta_m$ son algebraicamente dependientes sobre k. Como $\alpha_1,\dots,\alpha_i$ son algebraicamente independientes, reordenando $\beta_i,\dots,\beta_m$ podemos suponer que β_i es algebraico sobre $k(\alpha_1,\dots,\alpha_i,\beta_{i+1},\dots,\beta_m)$. Por hipótesis de inducción Σ es algebraico sobre $k(\alpha_1,\dots,\alpha_i,\beta_i,\dots,\beta_m)$ y concluimos que Σ también es algebraico sobre el cuerpo $k(\alpha_1,\dots,\alpha_i,\beta_{i+1},\dots,\beta_m)$. Ahora, si m fuera menor que n, tendríamos que Σ es algebraico sobre $k(\alpha_1,\dots,\alpha_m)$, contra la hipótesis de que $\alpha_1,\dots,\alpha_m,\alpha_{m+1}$ son algebraicamente independientes. Luego $m\geq n$. Por igual razón $n\geq m$ y $n=m$.

Ejemplos:

1. Sea k un cuerpo. El cuerpo $k(x_1,\dots,x_n)$ de las funciones racionales en el espacio afín $\mathbb{A}_{n,k}$ tiene grado de trascendencia n porque las funciones $x_1,\dots,x_n$ forman claramente una base de trascendencia sobre k.

2. Sea $p(x_1,\dots,x_n)$ un polinomio irreducible con coeficientes en un cuerpo k. Si el grado de p en x_n es ≥ 1, entonces el cuerpo $k(\xi_1,\dots,\xi_n)$ de las funciones racionales sobre la hipersuperficie $p(x_1,\dots,x_n)=0$ tiene grado de trascendencia $n-1$ sobre k, porque una base de trascendencia es $\{\xi_1,\dots,\xi_{n-1}\}$.

3. Sean X, Y variedades algebraicas íntegras sobre un cuerpo k y sean Σ_X, Σ_Y sus respectivos cuerpos de funciones racionales. Si $\phi\colon Y\to X$ es un morfismo que transforma el punto genérico de Y en el punto genérico de X (lo que equivale a que tenga imagen densa), entonces induce un morfismo de k-álgebras $\Sigma_X\to\Sigma_Y$. Diremos que ϕ es un morfismo de **grado** n cuando Σ_Y sea una extensión finita de grado n de Σ_X. Los morfismos de grado 1 se llaman morfismos **birracionales** . Diremos que X e Y son **birracionalmente equivalentes** si sus cuerpos de funciones racionales son extensiones de k isomorfas: $\Sigma_X\simeq\Sigma_Y$. Las variedades algebraicas birracionalmente equivalentes a un espacio afín se llaman **racionales**. Es decir, una variedad algebraica sobre k es racional si su cuerpo de funciones racionales es isomorfo a un cuerpo de fracciones racionales $k(x_1,\dots,x_n)$ con coeficientes en k.

4. Sea C la cúbica plana $y^2=x^2+x^3$. El haz de rectas $y=tx$ define un morfismo birracional $\mathbb{A}_1\to C$, $x=t^2-1$, $y=t^3-t$.

5. Sea C la cúbica plana $y^2=x^3$. El haz de rectas $y=tx$ define un morfismo birracional $\mathbb{A}_1\to C$, $x=t^2$, $y=t^3$.

Apéndice K

Grupo de Brauer

En este apéndice estudiamos las álgebras finitas, eventualmente no conmutativas, sobre un cuerpo conmutativo k. La analogía con el caso conmutativo es notable. Si convenimos en llamar triviales a las álgebras $M_n(k)$ de matrices cuadradas de orden n con coeficientes en k, entonces las álgebras de Azumaya son las álgebras triviales sobre alguna extensión (K.2.3). Si $k \to L$ es una extensión finita de Galois de grupo G, el teorema de Galois (1811-1832) afirma que las k-álgebras conmutativas triviales sobre L están clasificadas por las acciones de G en los conjuntos finitos, pues tales acciones se corresponden con las operaciones de G en las L-álgebras triviales L^n compatibles con su acción en L. Análogamente el teorema central K.3.3 afirma que las k-álgebras no conmutativas triviales sobre L están clasificadas por las acciones de G en los L-espacios proyectivos de dimensión finita, pues tales acciones se corresponden con las operaciones de G en las L-álgebras triviales $M_n(L)$ compatibles con la acción natural de G en L. Por eso siempre he considerado esta presentación de M$^{\text{a}}$ Teresa Sancho de Salas de la teoría del grupo de Brauer (1901-1977) como un excelente complemento de la teoría de Galois. De ella la aprendí y, entre todas la lecciones del programa que en 1983 presenté para optar a la cátedra de Álgebra, la elegí como lección magistral. Mi agradecimiento por su generosidad conmigo hace veinte años, y por permitirme exponer aquí su desarrollo de esta bella teoría.

En este apéndice los anillos tendrán unidad y serán eventualmente no conmutativos. Salvo mención expresa, siempre supondremos que todos los módulos e ideales lo son por la izquierda. Diremos que un ideal $\mathfrak{a}$ de un anillo A es bilátero cuando $A\mathfrak{a}A \subseteq \mathfrak{a}$. Además, k será un cuerpo conmutativo, y llamaremos k-álgebra a todo morfismo de anillos $k \to A$ tal que las imágenes de los elementos de k conmuten con todos los elementos de A. Diremos que una k-álgebra es finita cuando lo sea su dimensión como k-espacio vectorial.

K.1 Álgebras Simples

Definición: El centro de un anillo A es el subanillo $Z(A)$ formada por los elementos que conmutan con todos los elementos de A:

$$Z(A) := \{a \in A\colon\ xa = ax\,,\ \forall x \in A\}\ .$$

Diremos que un anillo $A \neq 0$ es de **división** cuando todo elemento no nulo sea invertible, y diremos que una k-álgebra A es **central** cuando $k = Z(A)$.

El anillo **inverso** de un anillo A es el anillo A^o que se obtiene al modificar el producto de A del siguiente modo: $a * b := ba$, donde $*$ denota el producto de A^o. Cada elemento $a \in A^o$ define un morfismo de A-módulos $R_a\colon A \to A$, $R_a(x) = xa$, y es sencillo comprobar que así se obtiene un isomorfismo de anillos

$$A^o\ =\ \mathrm{End}_A(A)\ .$$

Definición: Diremos que un A-módulo E es **simple** cuando el único submódulo no nulo sea E. Diremos que un anillo A es **simple** cuando, como A-módulo, sea isomorfo a una suma directa iterada de un módulo simple: $A \simeq E \oplus \ldots \oplus E$.

Diremos que un A-módulo M es **fiel** cuando su anulador, el ideal bilátero $\{a \in A\colon aM = 0\}$, sea nulo.

Ejemplo (álgebras de cuaterniones): Sean $a, b \in k$ no nulos y consideremos la k-álgebra A generada por dos elementos i, j con las relaciones

$$i^2 = a \quad , \quad j^2 = b \quad , \quad ij = -ji$$

que es una k-álgebra finita de dimensión 4, porque una base es $\{1, i, j, ij\}$, y es directo comprobar que el centro de A es k. Si $z = x_0 + x_1 i + x_2 j + x_3 ij$, donde $x_i \in k$, pondremos $\bar{z} := x_0 - x_1 i - x_2 j - x_3 ij$, y se define su norma como

$$N(z) := z\bar{z} = x_0^2 - ax_1^2 - bx_2^2 - abx_3^2$$

Si el índice de esta forma cuadrática es nulo (es decir, si el 0 es el único elemento de norma nula) entonces A es un álgebra de división, pues $a^{-1} = \bar{a}/N(a)$.

Cuando $k = \mathbb{R}$, es sencillo comprobar que, salvo isomorfismos, con este procedimiento sólo se obtiene un álgebra de división central, que es el álgebra de **cuaterniones**, y corresponde al caso $a = b = -1$.

Cuando $k = \mathbb{Q}$, obtenemos infinitas álgebras de división centrales no isomorfas entre sí (considérense los números racionales que admiten raíz cuadrada en A).

Ejemplo (álgebras de matrices): *Si E es un espacio vectorial de dimensión finita n sobre un anillo de división D, entonces $A := \mathrm{End}_D(E) \simeq M_n(D^o)$ es un anillo simple y $D = \mathrm{End}_A(E)$, donde $\lambda \in D$ se identifica con la homotecia $h_\lambda(e) = \lambda e$ de razón λ. Además el centro de D es el centro de* $\mathrm{End}_D(E)$.

En primer lugar observemos que E es claramente un A-módulo simple, y que la elección de una base $(e_1, \dots, e_n)$ de E permite definir un isomorfismo de A-módulos por la izquierda

$$\mathrm{End}_D(E) \xrightarrow{\sim} E\oplus \overset{n}{\cdots} \oplus E \quad , \quad T \mapsto (Te_1, \dots, Te_n) \ ,$$

así que el anillo $\mathrm{End}_D(E)$ es simple. Además, como $E \simeq D^n$, tenemos que

$$A \simeq \mathrm{Hom}_D(D^n, D^n) = \bigoplus_{ij} \mathrm{Hom}_D(D, D) = M_n(D^o)$$

donde cada matriz (a_{ij}) opera en D^n según la ley $(a_{ij})(b_i) = \left(\sum_j b_j a_{ij}\right)$. Nótese que la trasposición define un isomorfismo de anillos $M_n(D)^o \simeq M_n(D^o)$. En particular, cuando k es un cuerpo conmutativo, tenemos que $M_n(k)^o = M_n(k)$.

Si $f\colon E \to E$ es un morfismo de A-módulos, entonces $\oplus f\colon A = \oplus E \to \oplus E = A$, es un morfismo de A-módulos; luego es multiplicar por la derecha por cierta matriz $(a_{ij}) \in A = M_n(D^o)$. La condición de que respete las columnas nulas significa que tal matriz es diagonal, y la de que sea el mismo morfismo en todos los sumandos afirma que todos los elementos de la diagonal son un mismo $\lambda \in D^o$. Luego $f(e) = \lambda e$, y concluimos que $D = \mathrm{End}_A(E)$.

Por último, si $T \in \mathrm{End}_D(E)$ está en el centro, para cada vector no nulo $e \in E$ elegimos una aplicación lineal $\bar{T}$ que sólo deje fijos los vectores del subespacio ke. La condición $\bar{T}(Te) = T(\bar{T}e) = Te$ muestra que todos los subespacios vectoriales de dimensión 1 son invariantes por T, y el siguiente lema afirma que T es una homotecia h_λ (y, al ser k-lineal, su razón λ ha de estar en el centro de D):

Lema K.1.1 *Sea E un k-espacio vectorial de dimensión mayor que 1. Si un morfismo de grupos $S\colon E \to E$ deja invariantes todos los subespacios vectoriales de dimensión 1, entonces S es una homotecia: $S = h_\lambda$ para algún $\lambda \in k$.*

Demostración: (No usaremos que el cuerpo k es conmutativo). Si $e \in E$ no es nulo, por hipótesis existe $\lambda_e \in k$ tal que $S(e) = \lambda_e e$. Si dos vectores no nulos $e, v \in E$ son linealmente independientes, entonces

$$\lambda_{e+v} = S(e+v) = S(e) + S(v) = \lambda_e e + \lambda_v v$$

y concluimos que $\lambda_e = \lambda_v$. Si son linealmente dependientes, podemos elegir $w \in E$ que sea independiente de e y v, porque $\dim E > 1$. Luego $\lambda_e = \lambda_w = \lambda_v$.

Lema de Schur (1875-1941)**:** *Si M y N son A-módulos simples, todo morfismo de A-módulos no nulo $f\colon M \to N$ es un isomorfismo. En particular,* $\mathrm{End}_A(M)$ *es un anillo de división.*

Demostración: Si f no es nulo, entonces $\mathrm{Ker}\, f \neq M$ y $\mathrm{Im}\, f \neq 0$. Luego $\mathrm{Ker}\, f = 0$ y $\mathrm{Im}\, f = N$ porque M y N son simples.

Lema K.1.2 *Sea A un anillo simple. Salvo isomorfismos, existe un único módulo simple E y todo A-módulo de tipo finito descompone en suma directa de submódulos isomorfos a E.*

Demostración: Por definición, existe un A-módulo simple E y $A \simeq \oplus E$. Luego, si M es un A-módulo de tipo finito, existe un epimorfismo $f\colon E \oplus \ldots \oplus E \to M$. Podemos suponer que $f(E_{i+1})$ no está contenido en $f(E_1 \oplus \ldots \oplus E_i)$, de modo que al ser $f(E_{i+1}) \simeq E$ simple, tenemos $f(E_1 \oplus \ldots \oplus E_i) \cap f(E_{i+1}) = 0$ y concluimos que f es un isomorfismo. Cuando M es simple, se concluye que $M \simeq E$.

Teorema K.1.3 *Todo anillo simple A es un anillo de matrices con coeficientes en un anillo de división. De hecho, si E es un A-módulo simple y ponemos $D := \mathrm{End}_A(E)$, entonces*

$$A = M_n(D^o)\ .$$

Demostración: Por definición $A \simeq E^n$, así que

$$A^o = \mathrm{Hom}_A(A,A) \simeq \mathrm{Hom}_A(E^n,E^n) = \bigoplus_{ij} \mathrm{Hom}_A(E,E) = M_n(D)$$

y concluimos que $A \simeq M_n(D)^o = M_n(D^o)$ es un anillo de matrices, y $D = \mathrm{End}_A(E)$ es un anillo de división por el lema de Schur.

Corolario K.1.4 *Sea A un anillo simple. Si E es un A-módulo simple y ponemos $D := \mathrm{End}_A(E)$, entonces $A = \mathrm{End}_D(E)$.*

Demostración: $A = M_n(D^o) = \mathrm{End}_D(D^n) = \mathrm{End}_D(E)$ porque D^n es un $A = M_n(D^o)$-módulo simple y todos los A-módulos simples son isomorfos: $D^n \simeq E$.

Corolario K.1.5 *Sea k un cuerpo algebraicamente cerrado. Si A es una k-álgebra finita simple, entonces $A = M_n(k)$ para algún $n \geq 1$.*

Demostración: Sea D una k-álgebra finita de división. Si $\alpha \in D$, entonces $k[\alpha]$ es una k-álgebra finita conmutativa íntegra; luego es una extensión finita de k y $k[\alpha] = k$. Es decir, $D = k$.

Corolario K.1.6 *Sea A una k-álgebra finita. Si existe un A-módulo simple y fiel E, entonces A es simple, y por tanto $A = \mathrm{End}_D(E)$, donde $D := \mathrm{End}_A(E)$.*

Demostración: El morfismo de k-álgebras $A \to \mathrm{End}_k(E)$ que define E es inyectivo, porque E es un módulo fiel. Ahora bien, tenemos $\mathrm{End}_k(E) = E \oplus \ldots \oplus E$ como módulos sobre $\mathrm{End}_k(E)$ y, por tanto, también como A-módulos. Luego A es un submódulo de E^m y, al ser E un A-módulo simple, es sencillo concluir que $A \simeq E^n$.

Corolario K.1.7 *La condición necesaria y suficiente para que una k-álgebra finita A sea simple es que todo ideal bilátero de A sea trivial.*

Demostración: Sea I un ideal bilátero de un anillo simple A, y sea E un A-módulo simple. Como el ideal I es bilátero, anula a A/I. Por K.1.2, tenemos $A/I \simeq E \oplus \ldots \oplus E$; luego I anula a E, así que también anula a $A \simeq E \oplus \ldots \oplus E$, y concluimos que $I = 0$.

Recíprocamente, si A es una k-álgebra finita, cualquier ideal mínimo no nulo I de A es un A-módulo simple. Como el núcleo del morfismo natural $A \to \mathrm{End}_k(I)$ es un ideal bilátero, si éstos son triviales tenemos que I es un A-módulo simple fiel, y K.1.6 permite concluir que A es simple.

Definición: Sea E un k-espacio vectorial. Diremos que un morfismo de grupos $S\colon E \to E$ es una aplicación **semilineal** si existe un automorfismo de anillos $g\colon k \to k$ tal que $S(\lambda e) = g(\lambda)S(e)$ para todo $\lambda \in k$, $e \in E$. Cuando $S \neq 0$, tal automorfismo g es claramente único, y se dice que S y g están **asociados**. Las aplicaciones lineales son las aplicaciones semilineales asociadas a la identidad.

Cada automorfismo semilineal $S\colon E \to E$ induce un automorfismo de anillos $\mathrm{End}_k(E) \to \mathrm{End}_k(E)$, $T \mapsto STS^{-1}$, que en el centro $k\mathrm{Id}$ coincide precisamente con el automorfismo asociado a S.

Definición: Sea $\mathbb{P}_m = \mathbb{P}(E)$ un espacio proyectivo de dimensión $m := \dim E - 1$ sobre el cuerpo k. Llamaremos **proyectividades** a las proyectivizaciones de los automorfismos k-lineales $T\colon E \to E$ y llamaremos **colineaciones** a las proyectivizaciones de los automorfismos semilineales $S\colon E \to E$. El grupo de todas las proyectividades de $\mathbb{P}_m$ se denota $PGL_{m+1}n(k)$, y el de las colineaciones $PS_{m+1}(k)$.

Diremos que dos colineaciones son proyectivamente equivalentes si son conjugadas respecto de alguna proyectividad.

Teorema de Skolem-Noether(1887-1963 y 1882-1935)**:** *Sea E un k-espacio vectorial de dimensión finita $n > 1$. Todo automorfismo del anillo* $\mathrm{End}_k(E)$ *está asociado a algún automorfismo semilineal de E, y el grupo de los automorfismos del anillo* $\mathrm{End}_k(E)$ *es el grupo de las colineaciones $PS_n(k)$.*

En particular todo automorfismo de la k-álgebra $\mathrm{End}_k(E)$ *es interno, y el grupo de los automorfismos de k-álgebras de* $\mathrm{End}_k(E)$ *es el grupo de las proyectividades $PGL_n(k)$.*

Demostración: Sea $A := \mathrm{End}_k(E)$. Cada automorfismo de anillos $\tau\colon : A \to A$ define en E una nueva estructura de A-módulo, $T * e := (\tau T)(e)$, que denotaremos E_*. Como E y E_* son A-módulos simples, de K.1.2 se sigue la existencia de un isomorfismo de A-módulos $S\colon E \xrightarrow{\sim} E_*$. Es decir, S es morfismo de grupos y $S(Te) = T * S(e) = (\tau T)(Se)$, o lo que es lo mismo, $\tau(T) = STS^{-1}$.

Veamos que S es semilineal. Como el centro de A coincide con $k\mathrm{Id}$, al ser k conmutativo, τ induce un automorfismo $g\colon k \to k$ tal que $h_{g(\lambda)} = \tau(h_\lambda) = Sh_\lambda S^{-1}$. Es decir, $h_{g(\lambda)}S = Sh_\lambda$, lo que significa que S es semilineal y g es el automorfismo

asociado. (Además esto prueba que τ es isomorfismo de k-álgebras precisamente cuando S es k-lineal).

Por último, si una transformación S induce la identidad en $\mathrm{End}_k(E)$, entonces $ST = TS$ para todo $T \in \mathrm{End}_k(E)$. Eligiendo T de modo que el subespacio de vectores fijos tenga dimensión 1 vemos que S deja invariantes tales subespacios; luego S induce la identidad en $\mathbb{P}(E)$. Recíprocamente, si la proyectivización de S es la identidad, K.1.1 afirma que $S = h_\lambda$, así que S induce el automorfismo identidad en $\mathrm{End}_k(E)$.

Teorema de Wedderburn (1882-1948)**:** *Sea A un anillo simple. Si E es un A-módulo simple, entonces el funtor covariante $P(M) := \mathrm{Hom}_A(E, M)$ establece una equivalencia entre la categoría de A-módulos de tipo finito y la categoría de espacios vectoriales de dimensión finita sobre el álgebra de división $K := \mathrm{End}_A(E)^o$.*

Demostración: La estructura natural de E como módulo por la izquierda sobre $D := \mathrm{End}_(E)$ define en E una estructura de módulo por la derecha sobre $K = D^o$. El funtor inverso es $\bar{P}(V) := E \otimes_K V$, donde la estructura de A-módulo se define a partir de la estructura de A-módulo del primer factor. Ambos funtores P, $\bar{P}$ conservan sumas directas finitas, así que para demostrar que las transformaciones naturales

$$\begin{aligned} E \otimes_K \mathrm{Hom}_A(E, M) &\longrightarrow M \quad , \qquad e \otimes f \mapsto f(e) \\ V &\longrightarrow \mathrm{Hom}_A(E, E \otimes_K V) \quad , \qquad v \mapsto f_v \quad \text{donde } f_v(e) = e \otimes v \end{aligned}$$

son isomorfismos podemos reducirnos, en virtud de K.1.2, a los casos $M = E$ y $V = D$, que son inmediatos.

Nota: De hecho los funtores P y $\bar{P}$ establecen una equivalencia de la categoría de A-módulos arbitrarios con la de K-espacios vectoriales, pues ambos funtores conservan sumas directas arbitrarias (P porque E es un A-módulo monógeno al ser simple), y todo A-módulo M es suma directa de módulos simples. En efecto, en virtud de K.1.2 M es suma de submódulos simples ($M = \sum_i E_i$ donde $E_i \simeq E$) y, usando el Lema de Zorn, puede obtenerse que M es suma directa de submódulos simples: $M \simeq \oplus E$.

K.2 Álgebras de Azumaya

Definición: Las k-álgebras finitas centrales y simples reciben el nombre de k-álgebras de **Azumaya** (n. 1920).

Si A es una k-álgebra, cada par $a, b \in A$ define un endomorfismo k-lineal $x \mapsto axb$ de A, obteniendo así un morfismo canónico de k-álgebras f_A, que define en A una estructura de $A \otimes_k A^o$-módulo:

$$f_A \colon A \otimes_k A^o \longrightarrow \mathrm{End}_k(A) \qquad , \qquad f_A(a \otimes b)(x) = axb$$

Caracterización de las Álgebras de Azumaya: *La condición necesaria y suficiente para que una k-álgebra finita A sea de Azumaya es que f_A sea un isomorfismo.*

Demostración: Los ideales biláteros de A son precisamente los $A\otimes_k A^o$-submódulos de A y tenemos que

$$Z(A) = \mathrm{End}_{A\otimes_k A^o}(A) \subseteq \mathrm{End}_A(A) = A^o$$

Por tanto, A es un álgebra simple cuando lo sea como $A\otimes_k A^o$-módulo, y es central cuando $k = \mathrm{End}_{A\otimes_k A^o}(A)$. Como A siempre es un $\mathrm{End}_k(A)$-módulo simple, se sigue que A es un álgebra simple cuando f_A es un isomorfismo. Más aún, en este caso tenemos que

$$Z(A) = \mathrm{End}_{A\otimes_k A^o}(A) = Z(\mathrm{End}_k(A)) = k\ .$$

Recíprocamente, si A es una k-álgebra de Azumaya y $B = \mathrm{Im}\, f_A$, entonces A es un B-módulo simple y fiel. De acuerdo con K.1.6, se sigue que $B = \mathrm{End}_D(A)$ donde $D = \mathrm{End}_{A\otimes_k A^o}(A) = Z(A) = k$. Luego $B = \mathrm{End}_k(A)$ y f_A es epiyectivo. Como ambas álgebras tienen igual dimensión sobre k, concluimos que f_A es un isomorfismo.

Corolario K.2.1 *Sea $k \to L$ una extensión. La condición necesaria y suficiente para que una k-álgebra A sea de Azumaya es que lo sea la L-álgebra $A_L = A\otimes_k L$.*

Demostración: $f_{A_L} = f_A \otimes 1$.

Corolario K.2.2 *Si A y B son k-álgebras de Azumaya, también lo es $A\otimes_k B$.*

Demostración: $f_{A\otimes_k B} = f_A \otimes f_B$.

Corolario K.2.3 *La condición necesaria y suficiente para que una k-álgebra A sea de Azumaya es que exista alguna extensión $k \to L$ tal que A_L sea un álgebra de matrices sobre L; es decir, $A_L = M_n(L)$.*

Demostración: Si A es una k-álgebra de Azumaya y $\bar{k}$ es el cierre algebraico de k, entonces $A_{\bar{k}} = M_n(\bar{k})$ en virtud de K.2.1 y K.1.5. Recíprocamente, si A_L es un álgebra de matrices, entonces es una L-álgebra de Azumaya y K.2.1 permite concluir que A es una k-álgebra de Azumaya.

Corolario K.2.4 *La dimensión de cualquier álgebra de Azumaya es un cuadrado perfecto.*

Neutralización de Álgebras de Azumaya

Vamos a probar que para cada k-álgebra de Azumaya A existe alguna extensión finita de Galois $k \to L$ tal que A_L es un álgebra de matrices sobre L (en cuyo caso diremos que A está **neutralizada** por L). Este resultado se basa en la siguiente caracterización de las álgebras de matrices:

Definición: Si A es una k-álgebra de Azumaya de dimensión n^2, llamaremos subálgebras **diagonales** de A a las subálgebras conmutativas triviales de grado n.

Teorema K.2.5 *La condición necesaria y suficiente para que una k-álgebra de Azumaya A sea un álgebra de matrices es que contenga alguna subálgebra diagonal.*

Demostración: Si $A = M_n(k)$, entonces las matrices diagonales forman una subálgebra conmutativa trivial de grado n.

Recíprocamente, si B es una subálgebra diagonal de un álgebra de Azumaya A, para cada ideal maximal $\mathfrak{m}_i$ de B tenemos que el A-módulo $E_i := A \otimes_B (B/\mathfrak{m}_i)$ define un morfismo $A \to \mathrm{End}_k(E_i)$, que es inyectivo porque A es simple. Luego $n^2 = \dim A \leq (\dim E_i)^2$. Además, al ser $B = \oplus_i (B/\mathfrak{m}_i)$, tenemos que

$$A = A \otimes_B B = E_1 \oplus \ldots \oplus E_n$$

de modo que $n^2 = \dim E_1 + \ldots + \dim E_n$, así que $n = \dim E_i$ y $A = \mathrm{End}_k(E_i)$.

Proposición K.2.6 *Toda k-álgebra de Azumaya de dimensión n^2 contiene alguna subálgebra conmutativa separable de grado n.*

Demostración: Si $a \in A$, la subálgebra $k[a] \simeq k[x]/(p_a(x))$ es separable y de grado n si y sólo si el polinomio anulador $p_a(x)$ es separable y de grado n.

Si $\bar{k}$ es un cierre algebraico de k, tenemos que $A_{\bar{k}} = M_n(\bar{k})$ por K.1.5. Como el polinomio anulador de $a \otimes 1$ también es $p_a(x)$, basta probar que podemos elegir a de modo que el polinomio característico de $a \otimes 1$ no tenga raíces múltiples, porque en tal caso el polinomio característico coincide con el anulador. Ahora bien, el discriminante del polinomio característico de $a \otimes 1$ es una función polinómica sobre el k-espacio vectorial A, y este polinomio no es nulo porque no se anula en $A_{\bar{k}} = M_n(\bar{k})$. Si el cuerpo k es infinito, podemos concluir que tal polinomio no se anula en algún elemento $a \in A$, de modo que $p_a(x)$ es separable y de grado n.

Si el cuerpo k es finito, entonces es perfecto y, en virtud de K.1.3, basta probar que, cuando A es de división, contiene un subcuerpo conmutativo de grado n. Sea L un subcuerpo conmutativo de A y sea d su grado sobre k, de modo que $L_{\bar{k}} = \oplus \bar{k} = \bar{k}[T]$ donde el polinomio anulador del endomorfismo T es separable y de grado d. En particular $d \leq n$. Se comprueba sin dificultad que el conmutador de $L_{\bar{k}}$ en $A_{\bar{k}}$ (la subálgebra formada por los elementos de $A_{\bar{k}}$ que conmutan con todos los elementos de $L_{\bar{k}}$) tiene dimensión mayor que d cuando $d < n$. Por tanto, si $d < n$, podemos elegir $a \in A$ tal que $L[a]$ sea conmutativo y estrictamente mayor que L. Se concluye la existencia de un subcuerpo de A de grado n.

Teorema K.2.7 *Toda álgebra de Azumaya A está neutralizada por alguna extensión finita de Galois.*

Demostración: Sea $n^2 = \dim_k A$ y sea B una subálgebra conmutativa separable de grado n. Si L es la envolvente de Galois de B, entonces $B_L = \oplus L$ es una subálgebra diagonal de A_L y K.2.5 permite concluir que $A_L = M_n(L)$.

K.3 Construcción de las Álgebras de Azumaya

Sea $k \to L$ una extensión finita de Galois de grupo G. Vamos a exponer un método para construir todas las k-álgebras de Azumaya neutralizadas por L.

Definición: Sea E un L-espacio vectorial. Dar una **operación** de G en E es dar un morfismo de grupos $\rho\colon G \to \mathrm{Aut}_k(E)$ tal que $\rho(g)$ sea una transformación semilineal de automorfismo g. Es decir, las operaciones de G en E son las secciones del morfismo de grupos $G' \to G$, donde G' denota el grupo de los automorfismos semilineales de E asociados a elementos de G (y que por tanto son k-lineales). Diremos que dos operaciones de G en sendos L-espacios vectoriales son equivalentes si existe algún isomorfismo L-lineal que conmute con las respectivas operaciones de G.

Si en esta definición los morfismos k-lineales y L-lineales se sustituyen por morfismos de k-álgebras y L-álgebras, se obtiene la definición de operación de G en una L-álgebra A y de equivalencia de tales operaciones. Es decir, las operaciones de G en una L-álgebra A son las secciones del morfismo de grupos $G' \to G$, donde G' denota el grupo de los automorfismos de anillo semilineales asociados a elementos de G (y que por tanto son morfismos de k-álgebras).

Sea $L[G]$ el L-espacio vectorial de base G dotado del producto $(\lambda g)(\mu s) := \lambda g(\mu) gs$, donde $\lambda, \mu \in L$ y $g, s \in G$, de modo que $L[g]$ es una L-álgebra finita y cada operación de G en un L-espacio vectorial E define en E una estructura de $L[G]$-módulo:

$$\left(\textstyle\sum_i \lambda_i g_i\right) \;:=\; \textstyle\sum_i \lambda_i (g_i \cdot e)$$

Recíprocamente, cada $L[G]$-módulo M está definido por una única operación de G en el L-espacio vectorial M. Además dos operaciones son equivalentes precisamente cuando los correspondientes $L[G]$-módulos son isomorfos.

Lema K.3.1 $L[G] \;=\; \mathrm{End}_k(L)$ *y, por tanto, es una k-álgebra simple central.*

Demostración: La operación natural de G en L define un morfismo de k-álgebras $L[G] \to \mathrm{End}_k(L)$ que es L-lineal. Este morfismo es inyectivo en virtud de G.3.4 y, al tener ambos términos igual dimensión, es un isomorfismo.

Corolario K.3.2 *Si G opera en un L-espacio vectorial de dimensión finita E, entonces el morfismo natural $E^G \otimes_k L \to E$ es un isomorfismo.*

Demostración: Es obvio que L es un $L[G]$-módulo simple, así que K.1.2 permite reducirse al caso $E = L$, que es consecuencia directa de la igualdad $L^G = k$.

Teorema de Construcción: *Sea $k \to L$ una extensión finita de Galois de grupo G. Salvo isomorfismos, las k-álgebras de Azumaya de dimensión n^2 neutralizada por L son las álgebras de invariantes de las operaciones de G en la L-álgebra $M_n(L)$. Además dos operaciones de G en $M_n(L)$ son equivalentes precisamente cuando sus álgebras de invariantes son k-álgebras isomorfas.*

Demostración: Sea A una k-álgebra de Azumaya de dimensión n^2 neutralizada por L. Si consideramos la operación de G en $A_L \simeq M_n(L)$ inducida por su acción natural sobre el segundo factor de A_L, tenemos

$$M_n(L)^G \;=\; (A \otimes_k L)^G \;=\; A \otimes_k (L^G) \;=\; A$$

porque $L^G = k$. Es obvio que esta operación de G en $M_n(L)$ depende del isomorfismo de L-álgebras $A_L \simeq M_n(L)$ elegido, así que está bien definida salvo equivalencia.

Las operaciones de G en $M_n(L)$ que define la k-álgebra $M_n(k)$ se llaman **triviales** y son las operaciones equivalentes a la que define la acción natural de G en los coeficientes de las matrices.

Recíprocamente, si G opera en la L-álgebra $M_n(L)$ y $A := M_n(L)^G$, entonces el morfismo de L-álgebras $A_L \to M_n(L)$ es un isomorfismo por K.3.2. Luego, según K.2.1, A es una k-álgebra de Azumaya de dimensión n^2 neutralizada por L. Más aún, es claro que este isomorfismo $A_L \to M_n(L)$ conmuta con las respectivas operaciones de G, así que la operación considerada es la que define A. Esto permite concluir la demostración del teorema, pues operaciones equivalentes claramente tienen álgebras de invariantes isomorfas.

Definición: Dar una **geometría** (en el sentido de Klein) de grupo G en un espacio proyectivo $\mathbb{P}_m$ sobre L es dar un morfismo de grupos $\rho\colon G \to PS_{m+1}(L)$ tal que cada automorfismo $g \in G$ esté asociado a la colineación $\rho(g)$. Es decir, son las secciones del morfismo natural $PS_{m+1}(L) \to \mathrm{Aut}(L)$ definidas sobre G. Diremos que dos geometrías son proyectivamente equivalentes cuando sean subgrupos conjugados respecto de alguna proyectividad.

Teorema K.3.3 *Sea $k \to L$ una extensión finita de Galois de grupo G y sea $\mathbb{P}_m$ un espacio proyectivo de dimensión m sobre L. Las geometrías de grupo G en $\mathbb{P}_m$, salvo equivalencia proyectiva, se corresponden canónicamente con las k-álgebras de Azumaya de dimensión $(m+1)^2$ neutralizadas por L, salvo isomorfismos.*

Demostración: Sea $n = m + 1$. Por el teorema de construcción, las k-álgebras de Azumaya de dimensión n^2 neutralizadas por L, salvo isomorfismos, se corresponden con las secciones, salvo equivalencia, del morfismo $G' \to G$, donde G' denota el grupo de los automorfismos de anillo semilineales $M_n(L) \to M_n(L)$ asociados a elementos de G. Ahora bien, por el teorema de Skolem-Noether, todos los automorfismos del anillo $M_n(L)$ son semilineales y se corresponden canónicamente con las colineaciones de $\mathbb{P}_m$. Es decir, las operaciones de G en $M_n(L)$ se corresponden con las geometrías de grupo G en $\mathbb{P}_m$. Además, el teorema de Skolem-Noether también muestra que la equivalencia de operaciones se corresponde con la equivalencia proyectiva de geometrías.

Ejemplo K.3.4 La extensión $\mathbb{R} \to \mathbb{C}$ es de Galois y su grupo es $G = \{1, g\}$ donde g denota la conjugación compleja. Como el cuerpo $\mathbb{C}$ es algebraicamente cerrado, todas las $\mathbb{R}$-álgebras de Azumaya están neutralizadas por $\mathbb{C}$. Para construir todas las $\mathbb{R}$-álgebras de Azumaya de dimensión 4 basta determinar (salvo equivalencia proyectiva) las involuciones de automorfismo g de la recta proyectiva compleja. Dos de tales involuciones son

$$\begin{array}{ll} x_0 = \bar{x}_0 & \\ x_1 = \bar{x}_1 & \end{array} \quad , \quad \begin{array}{ll} x_0 = -\bar{x}_1 & \\ x_1 = \bar{x}_0 & \end{array}$$

La primera involución define una operación de G en $M_2(\mathbb{C})$ tal que la subálgebra de invariantes es $M_2(\mathbb{R})$. La operación que define la segunda involución es

$$g\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \bar{d} & -\bar{c} \\ -\bar{b} & \bar{a} \end{pmatrix}$$

y en este caso la subálgebra de invariantes es

$$\mathbb{H} \;=\; \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;,\; a, b \in \mathbb{C} \right\}$$

Una base de $\mathbb{H}$ sobre $\mathbb{R}$ es

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad , \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad , \quad ij = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

y se tiene que $i^2 = j^2 = -1$, $ij = -ji$. Luego $\mathbb{H}$ es el álgebra de los cuaterniones.

Definición: Diremos que una colineación es **cíclica** si su orden es finito y coincide con el de su automorfismo asociado.

Cuando la extensión de Galois $k \to L$ es cíclica, K.3.3 reduce la construcción de las k-álgebras de Azumaya neutralizadas por L a la clasificación proyectiva de las colineaciones cíclicas cuyo automorfismo asociado sea un generador dado del grupo de Galois.

Sea d el orden del grupo de Galois y sea g un generador. Si τ es una colineación cíclica de automorfismo τ y orden d, y elegimos una transformación semilineal T que represente a τ, entonces $T^d = \lambda$ para algún $\lambda \in L^*$. Como $\lambda T = T^d T = TT^d = T\lambda$, se sigue que $g(\lambda) = \lambda$. Luego $\lambda \in k^*$ y lo denotaremos $\mathrm{inv}(T)$. No es un invariante de τ porque depende del representante elegido:

$$\mathrm{inv}(\mu T) = (\mu T)^d = \mu(g\mu)\dots(g^{d-1}\mu)T^d = N(\mu)\mathrm{inv}(T)$$

Así que la clase de $\mathrm{inv}(T)$ módulo el subgrupo de normas $N(L^*)$ es un invariante de τ, bien definido en $k^*/N(L)^*$.

Teorema K.3.5 (Clasificación de Colineaciones Cíclicas) *La condición necesaria y suficiente para que dos colineaciones cíclicas con igual automorfismo asociado sean proyectivamente equivalentes, es que tengan el mismo invariante.*

Demostración: Sea E un L-espacio vectorial de dimensión finita y sean τ, τ' dos colineaciones cíclicas en $\mathbb{P}(E)$ con el mismo automorfismo asociado g. Si T, T' son representantes semilineales de τ y τ' respectivamente, entonces τ y τ' son proyectivamente equivalentes si y sólo si T' es equivalente a μT para algún $\mu \in L$. Luego basta probar que T y T' son equivalentes cuando $\mathrm{inv}(T) = \mathrm{inv}(T')$.

Sea $L_g[x]$ el anillo de polinomios con coeficientes en L, donde el producto se define por la condición $x\lambda = g(\lambda)x$. Las transformaciones semilineales $T\colon E \to E$ de automorfismo g tales que $T^d = \lambda$ se corresponden con las estructuras de $L_g[x]/(x^d - \lambda)$-módulo en E: $xe = T(e)$. Además dos de tales transformaciones semilineales son equivalentes precisamente cuando los correspondientes módulos son isomorfos. Luego basta probar que, salvo isomorfismos, sólo puede existir una estructura de $L_g[x]/(x^d - \lambda)$-módulo en E, cuando d es el orden de g. En virtud de K.1.2 es suficiente ver que $L_g[x]/(x^d - \lambda)$ es simple.

Sea $k = L^G$ y sea $\bar{k}$ un cierre algebraico de k. Entonces $A = L \otimes_k \bar{k}$ es una $\bar{k}$-álgebra trivial de grado d y la acción natural de g sobre A (vía su acción sobre el primer factor) es $g(a_1, \dots, a_d) = (a_d, a_1, \dots)$. Si $\mu \in \bar{k}$ es una raíz d-ésima de λ, entonces μg es un endomorfismo $\bar{k}$-lineal de A y define un morfismo de $\bar{k}$-álgebras

$$(L_g[x]/(x^d - \lambda)) \otimes_k \bar{k} = A_g[x]/(x^d - \lambda) \longrightarrow \mathrm{End}_{\bar{k}}(A)$$

porque $(\mu g)^d = \lambda$. Es sencillo comprobar que es un isomorfismo, y K.2.1 permite concluir que $L_g[x]/(x^d - \lambda)$ es simple.

Ejemplo K.3.6 Los invariantes de las involuciones consideradas en el ejemplo K.3.4 son 1 y -1 respectivamente. Como las normas de los números complejos no nulos son los números reales positivos, tenemos $\mathbb{R}^*/N(^*) = \{\pm 1\}$. Luego $M_2(\mathbb{R})$ y el álgebra $\mathbb{H}$ de los cuaterniones son las únicas $\mathbb{R}$-álgebras de Azumaya de dimensión 4.

Ahora bien, toda subálgebra conmutativa de un álgebra de división es una extensión finita. Como $\mathbb{C}$ es la única extensión finita no trivial de $\mathbb{R}$, de K.2.6 se sigue que toda $\mathbb{R}$-álgebra de división central no trivial tiene dimensión 4, así que el álgebra de los cuaterniones $\mathbb{H}$ es la única $\mathbb{R}$-álgebra de división central no trivial: *Las únicas -álgebras finitas de división son* $\mathbb{R}$, $\mathbb{C}$ *y* $\mathbb{H}$ (Teorema de Frobënius).

En virtud de K.1.3 podemos concluir que *las* $\mathbb{R}$*-álgebras de Azumaya son las álgebras* $M_n(\mathbb{R})$ *y* $M_n(\mathbb{H})$.

Ejemplo K.3.7 Si $\mathbb{F}_q$ es un cuerpo finito, toda extensión finita $\mathbb{F}_q \to \mathbb{F}_{q^d}$ es cíclica y un generador del grupo de Galois es el automorfismo de Frobënius $F(x) = x^q$. Luego la norma es

$$N(x) = xF(x)F^2(x)\dots F^{d-1}(x) = xx^q x^{q^2}\dots x^{q^{d-1}} = x^{1+q+q^2+\dots+q^{d-1}} = x^{\frac{q^d-1}{q-1}}$$

y el número de elementos de norma 1, i.e. de soluciones de la ecuación $x^{\frac{q^d-1}{q-1}} = 1$, es $\leq \frac{q^d-1}{q-1}$. Se sigue que la norma $N\colon \mathbb{F}_{q^d}^* \to \mathbb{F}_q^*$ es epiyectiva y concluimos que todo álgebra de Azumaya sobre un cuerpo finito $\mathbb{F}_q$ es un álgebra de matrices $M_n(\mathbb{F}_q)$. En particular, *todo anillo de división finito es conmutativo* (Teorema de Wedderburn).

Ejemplo K.3.8 Con las notaciones de K.3.5, el invariante de la colineación cíclica

$$x_0 = \lambda\bar{x}_d \quad , \quad x_1 = \bar{x}_0 \quad , \dots , \quad x_d = \bar{x}_{d-1}$$

donde $\bar{x} := g(x)$, es precisamente $\lambda \in k^*/N(L^*)$. En consecuencia, *las* k*-álgebras de Azumaya de dimensión* d^2 *neutralizadas por* L *se corresponden biunívocamente con* $k^*/N(L^*)$; pero tal correspondencia depende del generador g del grupo de Galois elegido. La operación de G en $M_d(L)$ definida por g y $\lambda \in k^*/N(L^*)$ es

$$g\begin{pmatrix} a_{11} & \dots & a_{1d} \\ \dots & \dots & \dots \\ a_{d1} & \dots & a_{dd} \end{pmatrix} = \begin{pmatrix} \bar{a}_{dd} & \lambda\bar{a}_{d1} & \dots & \lambda\bar{a}_{dm} \\ \bar{a}-1d/\lambda & \bar{a}_{11} & \dots & \bar{a}_{1m} \\ \dots & \dots & \dots & \dots \\ \bar{a}_{md}/\lambda & \bar{a}_{m1} & \dots & \bar{a}_{mm} \end{pmatrix}$$

donde $m = d-1$. El álgebra de invariantes es la k-álgebra de Azumaya de dimensión d^2 correspondiente a g y λ.

Nota: El Teorema de Skolem-Noether admite la siguiente generalización en las álgebras de Azumaya:

Si B *y* B' *son subálgebras simples de una* k*-álgebra de Azumaya* A*, entonces cualquier isomorfismo de* k*-álgebras* $B \to B'$ *está inducido por un automorfismo interno de* A*. En particular todo automorfismo de* k*-álgebras de* A *es interno.*

En efecto, sean $f, g\colon B \to A$ dos morfismos inyectivos de k-álgebras.

Si $A = \mathrm{End}_k(E)$ para algún k-espacio vectorial E, entonces E adquiere dos estructuras de B-módulo que son isomorfas en virtud de K.1.2, pues ambas tienen igual dimensión sobre k. Luego existe $T \in \mathrm{Aut}_k(E) \subset A$ tal que $T \cdot f(b) = g(b) \cdot T$ para todo $b \in B$, lo que permite concluir en este caso.

Si A no es un álgebra de matrices, el funtor $\otimes_k A^o$ nos reduce al caso anterior:

$$f \otimes 1, g \otimes 1 \colon B \otimes_k A^o \xrightarrow{\sim} A \otimes_k A^o = \mathrm{End}_k(A)$$

de modo que existe $T \in \mathrm{Aut}_k(A)$ tal que $T(f(b) \otimes a)T^{-1} = g(b) \otimes a$. Ahora bien, T es un isomorfismo de $B \otimes_k A^o$-módulos, así que T está en $\mathrm{End}_{A^o}(A) = A$ y concluimos la demostración.

K.4 Ideales de las Álgebras de Azumaya

Vamos a determinar los ideales de un álgebra de Azumaya en términos de su geometría finita. Primero calcularemos los ideales de las álgebras de matrices:

Lema K.4.1 *Sea E un k-espacio vectorial de dimensión finita. Si V es un subespacio vectorial de E, entonces* $\mathrm{Hom}_k(E/V, E) = \{T \in \mathrm{End}_k(E) \colon V \subseteq \mathrm{Ker}\, T\}$ *es un ideal por la izquierda de* $\mathrm{End}_k(E)$*, y* $\mathrm{Hom}_k(E, V) = \{T \in \mathrm{End}_k(E) \colon \mathrm{Im}\, T \subseteq V\}$ *es un ideal por la derecha. Así se obtienen todos los ideales de* $\mathrm{End}_k(E)$*.*

Demostración: Si $T \colon E \to E$ es un endomorfismo tal que $\mathrm{Im}\, T \subseteq V$, entonces $\mathrm{Im}\, TS \subseteq V$ para todo endomorfismo $S \colon E \to E$, así que $\mathrm{Hom}_k(E, V)$ es un ideal por la derecha de $\mathrm{End}_k(E)$. Recíprocamente, como todo ideal por la derecha es suma directa de ideales minimales por la derecha, basta probar que tales ideales minimales son de la forma $\mathrm{Hom}_k(E, V_1)$ para algún subespacio vectorial V_1 de dimensión 1. Esto se debe a que el ideal por la derecha generado por un endomorfismo T es precisamente $\mathrm{Hom}_k(E, \mathrm{Im}\, T)$.

La demostración para ideales por la izquierda es similar.

K.4.2 Sea $k \to L$ una extensión finita de Galois de grupo G y sea E un L-espacio vectorial de dimensión n. Consideremos una operación de G en la L-álgebra $\mathrm{End}_L(E)$ y la correspondiente acción (K.3.3) de G en el espacio proyectivo $\mathbb{P}(E)$, de modo que $A = \mathrm{End}_L(E)^G$ es una k-álgebra de Azumaya de dimensión n^2 neutralizada por L.

Lema K.4.3 *Existe una correspondencia biunívoca, que invierte inclusiones, entre los ideales por la izquierda de A y las subvariedades lineales G-invariantes de $\mathbb{P}(E)$. El ideal correspondiente a la subvariedad lineal invariante $\mathbb{P}(V)$ es* $\mathrm{Hom}_L(E/V, E)^G$*.*

Demostración: Si $\mathbb{P}(V)$ es una subvariedad lineal G-invariante, entonces el ideal $\mathrm{Hom}_L(E/V, E)$ de $\mathrm{End}_L(E)$ es invariante por la acción de G, y $\mathrm{Hom}_L(E/V, E)^G$ es un ideal de A.

Recíprocamente, si I es un ideal de A, entonces I_L es un ideal G-invariante de $A_L = \mathrm{End}_L(E)$. De acuerdo con K.4.1 tenemos que $I_L = \mathrm{Hom}_L(E/V, E)$ para algún subespacio vectorial $V \subseteq E$, y $\mathbb{P}(V)$ es G-invariante porque $\mathrm{Hom}_L(E/V, E)$ lo es. Además $\mathrm{Hom}_L(E/V, E)^G = (I_L)^G = I$. q.e.d.

Análogamente se prueba que *el retículo de subvariedades lineales G-invariantes de $\mathbb{P}(E)$ es isomorfo al retículo de ideales por la derecha de A, donde el ideal correspondiente a $\mathbb{P}(V)$ es precisamente* $\mathrm{Hom}_L(E, V)^G$.

Corolario K.4.4 *Los retículos de ideales por la izquierda y por la derecha de A son duales. A cada ideal por la izquierda le corresponde su anulador por la derecha, y a cada ideal por la derecha le corresponde su anulador por la izquierda.*

Corolario K.4.5 *Las subvariedades lineales de $\mathbb{P}(E)$ generadas por alguna órbita de la acción de G se corresponden con los ideales maximales por la izquierda de A (y con los ideales no nulos minimales por la derecha).*

Corolario K.4.6 *A es un álgebra de división precisamente cuando $\mathbb{P}(E)$ es la única subvariedad lineal no vacía invariante.*

Corolario K.4.7 *Si I, J son los ideales por la izquierda y derecha de A correspondientes a una subvariedad lineal G-invariante $\mathbb{P}(V)$ y $n^2 = \dim_k A$, entonces* $\dim_k I = n(n - \dim_k V)$ *y* $\dim_k J = n(\dim_k V)$.

Demostración: En efecto, tenemos que $\dim_k I = \dim_L I_L = \dim_L \mathrm{Hom}_L(E/V, E)$ y que $\dim_k J = \dim_L J_L = \dim_L \mathrm{Hom}_L(E, V)$.

Corolario K.4.8 *La condición necesaria y suficiente para que A sea un álgebra de matrices sobre k es que en $\mathbb{P}(E)$ exista algún punto invariante (resp. algún hiperplano invariante).*

Demostración: Este corolario es consecuencia directa del anterior y de la siguiente caracterización de las álgebras de matrices:

Lema K.4.9 *La condición necesaria y suficiente para que una k-álgebra simple de dimensión n^2 sea $M_n(k)$ es que tenga algún ideal por la izquierda (resp. por la derecha) de dimensión n.*

Demostración: La necesidad de la condición se sigue de K.4.1. Recíprocamente, si $I \subset A$ es un ideal por la izquierda de dimensión n, su estructura de A-módulo define un morfismo de k-álgebras $A \to \mathrm{End}_k(I)$ que, por ser A simple, es inyectivo. Como ambas k-álgebras tienen igual dimensión, concluimos que es un isomorfismo.

Si $J \subset A$ es un ideal por la derecha de dimensión n, el morfismo de k-álgebras $A^o \to \mathrm{End}_k(J)$ es un isomorfismo, de modo que A es un álgebra de matrices.

K.5 El Grupo de Brauer

Toda k-álgebra de Azumaya es, según K.1.3, un álgebra de matrices sobre una k-álgebra de división bien definida salvo isomorfismos. Diremos que dos k-álgebras de Azumaya son **equivalentes** si sus correspondientes álgebras de división son isomorfas. Es claro que en cada clase de equivalencia hay, salvo isomorfismos, una única álgebra de división, y que sólo puede haber un álgebra de dimensión dada. La clase de equivalencia de una k-álgebra de Azumaya A se denotará $[A]$.

Sean A, A' dos k-álgebras de Azumaya, que serán álgebras de matrices sobre sendas álgebras de división D, D'. Si $D \otimes_k D'$ es un álgebra de matrices sobre D'', también lo es $A \otimes_k A'$. Luego la clase $[A \otimes_k A']$ está bien determinada por las clases $[A]$ y $[A']$, lo que nos permite definir una operación

$$[A] \cdot [A'] \;=\; [A \otimes_k A']$$

en el conjunto $\mathrm{Br}(k)$ de las clases de equivalencia de k-álgebras de Azumaya, conjunto que coincide con el de k-álgebras finitas centrales de división (salvo isomorfismos). Este producto es claramente asociativo, conmutativo y $1 = [k]$ es un elemento neutro. Además el teorema de caracterización de las álgebras de Azumaya afirma que $[A] \cdot [A^o] = 1$. Luego este producto define una estructura de grupo abeliano en $\mathrm{Br}(k)$, llamado **grupo de Brauer** (1901-1977) de k.

Cada extensión $k \to L$ induce una aplicación $\mathrm{Br}(k) \to \mathrm{Br}(L)$, $[A] \mapsto [A_L]$, que es morfismo de grupos porque $(A \otimes_k A')_L = (A_L) \otimes_L (A'_L)$. El núcleo de este morfismo se denota $\mathrm{Br}(L/k)$ y es el subgrupo de $\mathrm{Br}(k)$ formado por las clases de las k-álgebras de Azumaya neutralizadas por L. De acuerdo con K.2.7, el grupo $\mathrm{Br}(k)$ es la unión de los subgrupos $\mathrm{Br}(L/k)$ cuando L recorre las extensiones finitas de Galois de k, así que para determinar el grupo de Brauer $\mathrm{Br}(k)$ basta calcular $\mathrm{Br}(L/k)$ cuando $k \to L$ es una extensión finita de Galois.

Ejemplos: La construcción de las álgebras de cuaterniones muestra que el grupo de Brauer del cuerpo de los números racionales es infinito.

Cuando el cuerpo k es algebraicamente cerrado, K.1.3 afirma que $\mathrm{Br}(k) = 1$.

Cuando la extensión de Galois $k \to L$ es cíclica, K.3.8 y la clasificación de colineaciones cíclicas prueban que $\mathrm{Br}(L/k) = k^*/N(L^*)$.

K.3.6 afirma que $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

Cuando el cuerpo k es finito, K.3.7 afirma que $\mathrm{Br}(k) = 1$.

Apéndice L

Morfismos Finitos

L.1 Dependencia Entera

Definición: Sea $A \to B$ un morfismo de anillos. Diremos que un elemento $b \in B$ es **entero** sobre A si verifica alguna relación

$$b^n + a_1 b^{n-1} + \ldots + a_{n-1} b + a_n = 0 \ , \quad a_i \in A$$

(nótese que el coeficiente de b^n es la unidad) y diremos que B es **entero** sobre A, ó que $A \to B$ es un morfismo **entero** cuando todos los elementos de B sean enteros sobre A.

Recuérdese que se dice que un morfismo de anillos $A \to B$ es **finito** si la estructura de A-módulo que define en B es de tipo finito: $B = Ab_1 + \ldots + Ab_n$. En tal caso todo B-módulo de tipo finito $M = Bm_1 + \ldots + Bm_r$ es, por restricción de escalares, un A-módulo de tipo finito:

$$M = \textstyle\sum_j (\sum_i Ab_i) m_j = \sum_{ij} Ab_i m_j$$

Caracterización de los Elementos Enteros: *Sea $A \to B$ un morfismo de anillos. Si $b \in B$, las siguientes condiciones son equivalentes:*

1. *b es entero sobre A.*
2. *$A[\,b\,]$ es un A-módulo de tipo finito.*
3. *b pertenece a una subálgebra C de B que es A-módulo de tipo finito.*

Demostración: $(1 \Rightarrow 2)$ Si b es entero sobre A, alguna potencia es combinación lineal de las anteriores, $b^n = -a_1 b^{n-1} - \ldots - a_{n-1} b - a_n$, $a_i \in A$, de modo que las sucesivas potencias b^{n+j} también son combinaciones lineales de $1, b, \ldots, b^{n-1}$ con coeficientes en A y concluimos que

$$A[\,b\,] = A + Ab + \ldots + Ab^{n-1}$$

($2 \Rightarrow 3$) Es evidente, pues $A[b]$ es una subálgebra de B y $b \in A[b]$.

($3 \Rightarrow 1$) Sea $C = Ae_1 + \ldots + Ae_n$. Por hipótesis $b \in C$ y C es una subálgebra, así que $be_i = \sum_{j=1}^{n} a_{ij}e_j$ para ciertos $a_{ij} \in A$:

$$0 = \sum_{j=1}^{n} (\delta_{ij}b - a_{ij})e_j \ , \quad 1 \leq i \leq n$$

donde $\delta_{ii} = 1$ y $\delta_{ij} = 0$ cuando $i \neq j$. Multiplicando por la izquierda por la matriz adjunta de $(\delta_{ij}b - a_{ij})$ se sigue que el determinante $|\delta_{ij}b - a_{ij}|$ anula a cada e_i; luego anula a C y concluimos que es nulo porque $1 \in C$. Desarrollando el determinante obtenemos una relación de dependencia entera $b^n + \sum_{i=1}^{n} a_i b^{n-i} = 0$, $a_i \in A$.

Corolario L.1.1 *Si $b_1, \ldots, b_n \in B$ son enteros sobre A, entonces $A[b_1, \ldots, b_n]$ es un A-módulo de tipo finito.*

Demostración: Procedemos por inducción sobre n. Si $n = 1$, se sigue directamente de la caracterización anterior. Si $n > 1$, por hipótesis de inducción $A[b_1, \ldots, b_{n-1}]$ es un A-módulo de tipo finito. Ahora bien, como b_n es entero sobre A, también es entero sobre $A[b_1, \ldots, b_{n-1}]$, luego $A[b_1, \ldots, b_n]$ es $A[b_1, \ldots, b_{n-1}]$-módulo de tipo finito y concluimos que $A[b_1, \ldots, b_n]$ es A-módulo de tipo finito.

Corolario L.1.2 *Los elementos de B enteros sobre A forman una subanillo, llamado* ***cierre entero*** *de A en B.*

Demostración: Si $b_1, b_2 \in B$ son enteros sobre A, entonces $A[b_1, b_2]$ es un A-módulo de tipo finito y se sigue que todos sus elementos son enteros sobre A. En particular $b_1 + b_2$ y $b_1 b_2$ son enteros sobre A.

Corolario L.1.3 *La dependencia entera es estable por cambios de base: Si B es entero sobre A, entonces $B \otimes_A C$ es entero sobre C para toda A-álgebra C.*

Demostración: La C-álgebra $B \otimes_A C$ está generada por los elementos $b \otimes 1$, $b \in B$, que son enteros sobre C. En efecto, si $b^n + a_1 b^{n-1} + \ldots + a_n = 0$, $a_i \in A$, entonces

$$(b\otimes 1)^n + (a_1 \otimes 1)(b \otimes 1)^{n-1} + \ldots + (a_n \otimes 1) = (b^n + a_1 b^{n-1} + \ldots + a_n) \otimes 1 = 0$$

y se sigue que $b \otimes 1$ es entero sobre $A \otimes_A C = C$. El corolario anterior permite concluir que $B \otimes_A C$ es entero sobre C.

Corolario L.1.4 *Sean $A \to B \to C$ morfismos de anillos. Si B es entero sobre A, entonces todo elemento de C entero sobre B también es entero sobre A.*

En particular, si C es entero sobre B y B es entero sobre A, entonces C es entero sobre A.

Demostración: Si un elemento $c \in C$ es entero sobre B, satisface alguna relación de dependencia entera $c^n + b_1 c^{n-1} + \ldots + b_n$, $b_i \in B$. Luego c es entero sobre $B' = A[b_1, \ldots, b_n]$ y, por tanto, $B'[c]$ es un B'-módulo de tipo finito. Por L.1.1, B' es un A-módulo de tipo finito, y se sigue que $B'[c]$ es un A-módulo de tipo finito; luego c es entero sobre A.

Ejemplos:

1. Sea K una extensión de un cuerpo k. Los elementos de K enteros sobre k son precisamente los elementos algebraicos sobre k. Es decir, el cierre entero de k en K es el cierre algebraico de k en K. Por tanto, si K es una extensión algebraica de k, de L.1.3 se sigue que $K[x_1, \ldots, x_n]$ es entero sobre $k[x_1, \ldots, x_n]$. En particular $\bar{k}[x_1, \ldots, x_n]$ es entero sobre $k[x_1, \ldots, x_n]$.

2. Los números complejos enteros sobre $\mathbb{Z}$ se llaman **enteros algebraicos** sin más y, por definición, son las raíces de los polinomios unitarios con coeficientes en $\mathbb{Z}$. Cada número algebraico $\alpha \in \mathbb{C}$ es raíz de un único polinomio irreducible unitario $p_\alpha(x)$ con coeficientes racionales y, según 5.4.2, la condición necesaria y suficiente para que α sea entero es que $p_\alpha(x)$ tenga coeficientes en $\mathbb{Z}$. Así, $\sqrt{2}$ es entero, porque es raíz del polinomio $x^2 - 2$; pero $\sqrt{2}/2$ no es entero, pues su polinomio irreducible $x^2 - 1/2$ no tiene coeficientes en $\mathbb{Z}$.

3. Sea C la curva plana de ecuación $p(x, y) = 0$ y consideremos la proyección $\pi\colon C \to \mathbb{A}_1$, $\pi(x, y) = x$, en la dirección de las rectas verticales $x = c$. Vamos a ver que π es un morfismo finito precisamente cuando la curva carece de asíntotas verticales (es decir, rectas tangentes a la curva en el punto $x = 0$, $z = 0$ que no sean la recta del infinito $z = 0$).

   Sea $k[\xi, \eta]$ el anillo de funciones algebraicas de C. Según la caracterización de los elementos enteros, la condición necesaria y suficiente para que π sea un morfismo finito es que η sea entero sobre $k[\xi]$. Ahora bien, cualquier relación de dependencia entera de η sobre $k[\xi]$ ha de venir dada por un múltiplo de $p(x, y)$, así que tal condición equivale a que, considerando $p(x, y)$ como polinomio en y:

   $$p(x, y) = p_0(x)y^n + p_1(x)y^{n-1} + \ldots + p_n(x) \ , \quad p_0(x) \neq 0$$

   el coeficiente $p_0(x)$ sea constante. Homogeneizando con una indeterminada z, para obtener la ecuación proyectiva de la curva, y deshomogeneizando respecto de y para estudiar sus tangentes en el punto $(0, 1, 0)$, tal condición expresa que la ecuación de la curva sea de la forma

   $$0 = z^{d-n} + \text{ (términos de grado mayor que } d - n)$$

donde d es el grado de $p(x,y)$; es decir, que la curva no pase por el punto $(0,1,0)$ o, si pasa (cuando $d > n$), que la única recta tangente en tal punto sea la recta $z = 0$; es decir, que no tenga asíntotas verticales. Análogamente se prueba que la proyección $\pi\colon C \to \mathbb{A}_1$, $\pi(x,y) = ax+by$, en la dirección de las rectas $ax+by = c$, es un morfismo finito si y sólo si C no tiene asíntotas en tal dirección.

4. Sea C la curva plana $y^2 = x^3$. La parametrización $x = t^2$, $y = t^3$, define un morfismo finito $\mathbb{A}_1 \to C$, porque t satisface la relación de dependencia entera $t^2 - x = 0$ sobre $\mathcal{O}(C)$.

5. Si C es la curva $y^2 = x^2+x^3$, la parametrización $x = t^2-1$, $y = t^3-t$, define un morfismo finito $\mathbb{A}_1 \to C$, porque t satisface la relación de dependencia entera $t^2 - (1+x) = 0$ sobre $\mathcal{O}(C)$.

6. Sea B un anillo entero sobre otro anillo A. Si $\mathfrak{b}$ es un ideal de B, entonces $B/\mathfrak{b}$ es entero sobre A, pues para obtener una relación de dependencia entera de $[b] \in B/\mathfrak{b}$ basta reducir módulo $\mathfrak{b}$ cualquier relación de dependencia entera de b sobre el anillo A.

7. Según L.1.1, si un morfismo $A \to B$ es de tipo finito, $B = A[b_1,\dots,b_n]$, la condición de ser entero equivale a la de ser finito.

L.2 Teorema del Ascenso

Lema L.2.1 *Sea $A \to B$ un morfismo entero e inyectivo entre anillos íntegros. La condición necesaria y suficiente para que B sea cuerpo es que A sea cuerpo.*

Demostración: Supongamos que B es un cuerpo. Si $a \in A$ no es nulo, su imagen en B no es nula; luego a es invertible en B y a^{-1} es entero sobre A:

$$a^{-n} + a_1 a^{-n+1} + \ldots + a_{n-1}a^{-1} + a_n = 0\ , \quad a_i \in A$$

Multiplicando por a^{n-1} obtenemos que $a^{-1} \in A$. Luego A es un cuerpo.

Recíprocamente, si A es cuerpo, el cuerpo de fracciones K de B es una extensión algebraica de A. Luego toda subálgebra de K (en particular B) es cuerpo.

Corolario L.2.2 *Sea $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación continua inducida por un morfismo de anillos $A \to B$ y sea $y \in \operatorname{Spec} B$. Si B es entero sobre A, entonces*

$$y \text{ es un punto cerrado de } \operatorname{Spec} B \ \Leftrightarrow\ \phi(y) \text{ es un punto cerrado de } \operatorname{Spec} A$$

Demostración: Sea $\mathfrak{q}$ el ideal primo de y, y $\mathfrak{p} = \mathfrak{q} \cap A$ el ideal primo de $\phi(y)$, de modo que $A/\mathfrak{p} \to B/\mathfrak{q}$ es un morfismo entero e inyectivo entre anillos íntegros. El lema anterior permite concluir que $\mathfrak{q}$ es un ideal maximal de B si y sólo si $\mathfrak{p}$ es un ideal maximal de A.

Corolario L.2.3 *Sea $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación continua inducida por un morfismo de anillos $A \to B$. Si B es entero sobre A, entonces las fibras de ϕ tienen dimensión 0. Si además el morfismo $A \to B$ es finito, entonces las fibras de ϕ son finitas y discretas.*

Demostración: Sea $x \in \operatorname{Spec} A$. La fórmula de la fibra afirma que

$$\phi^{-1}(x) \;=\; \operatorname{Spec}\left(B_x/\mathfrak{p}_x B_x\right) \;=\; \operatorname{Spec}\left(B \otimes_A \kappa(x)\right)$$

donde $\kappa(x)$ es el cuerpo residual de x. Si B es entero sobre A, entonces $B \otimes_A \kappa(x)$ es entero sobre $\kappa(x)$ por L.1.3, y el corolario anterior afirma que todos los puntos de $\operatorname{Spec} B \otimes_A \kappa(x)$ son cerrados, así que su dimensión es 0. Si, además, B es finito sobre A, entonces $B \otimes_A \kappa(x)$ es una $\kappa(x)$-álgebra finita, así que su espectro es finito y discreto.

Corolario L.2.4 *Sea $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ la aplicación continua inducida por un morfismo de anillos $A \to B$. Si B es entero sobre A, entonces*

$$\dim B_y \leq \dim A_{\phi(y)}$$

para todo punto $y \in \operatorname{Spec} B$. En particular, $\dim B \leq \dim A$.

Demostración: Sea $y_0 > \ldots > y_n = y$ una cadena de especializaciones en $\operatorname{Spec} B$. Como ϕ es una aplicación continua, $\phi(y_i)$ está en el cierre de $\phi(y_{i-1})$. Si se diera alguna coincidencia $\phi(y_{i-1}) = \phi(y_i)$, la fibra de $\phi(y_i)$ tendría dimensión ≥ 1, en contra de L.2.3. Luego $\dim B_y \leq \dim A_{\phi(y)}$.

Teorema del Ascenso: *Sea $j\colon A \to B$ un morfismo de anillos y sea $\mathfrak{a}$ su núcleo. Si B es entero sobre A, la aplicación continua $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ inducida por j es cerrada y su imagen son los ceros de $\mathfrak{a}$.*

Demostración: Veamos primero que si un morfismo $A \to B$ es inyectivo y entero, entonces la aplicación inducida $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectiva. En tal caso, sea $x \in \operatorname{Spec} A$ y consideremos el siguiente cuadrado conmutativo:

$$\begin{array}{ccc} \operatorname{Spec} B_x & \xrightarrow{\phi} & \operatorname{Spec} A_x \\ \downarrow & & \downarrow \\ \operatorname{Spec} B & \xrightarrow{\phi} & \operatorname{Spec} A \end{array}$$

El morfismo $A_x \to B_x$ es inyectivo; luego $B_x \neq 0$ y su espectro tiene algún punto cerrado y. Por L.1.3, B_x es entero sobre A_x, así que L.2.2 permite obtener que $\phi(y)$ es un punto cerrado de $\operatorname{Spec} A_x$. Luego $x = \phi(y)$, porque x es el único punto cerrado de $\operatorname{Spec} A_x$, y concluimos que $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectiva.

Demostremos ahora el caso general. Sea $\mathfrak{b}$ un ideal de B. Bastará probar que $\phi((\mathfrak{b})_0) = (\mathfrak{b} \cap A)_0$. Consideremos el siguiente cuadrado conmutativo:

$$\begin{array}{ccc} (\mathfrak{b})_0 = \operatorname{Spec} B/\mathfrak{b} & \xrightarrow{\phi} & \operatorname{Spec} A/(\mathfrak{b} \cap A) = (\mathfrak{b} \cap A)_0 \\ \downarrow & & \downarrow \\ \operatorname{Spec} B & \xrightarrow{\phi} & \operatorname{Spec} A \end{array}$$

Como el morfismo natural $A/(\mathfrak{b} \cap A) \to B/\mathfrak{b}$ es inyectivo y entero, la aplicación $\operatorname{Spec} B/\mathfrak{b} \to \operatorname{Spec} A/(\mathfrak{b} \cap A)$ es epiyectiva y concluimos que $\phi((\mathfrak{b})_0) = (\mathfrak{b} \cap A)_0$. Luego $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es cerrada y

$$\phi(\operatorname{Spec} B) = \phi((0)_0) = (0 \cap A)_0 = (\mathfrak{a})_0$$

Corolario L.2.5 *En las hipótesis del teorema del ascenso, si $x = \phi(y)$ y x' es una especialización de x, entonces existe una especialización y' de y tal que $x' = \phi(y')$.*

Demostración: $\overline{\{x\}} = \overline{\{\phi(y)\}} \subseteq \phi\big(\overline{\{y\}}\big)$ porque la aplicación ϕ es cerrada.

Corolario L.2.6 *Si un morfismo entero $A \to B$ es inyectivo, entonces la aplicación inducida $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectiva y $\dim A = \dim B$.*

Demostración: Sea $x_0 > x_1 > \ldots > x_n$ una cadena de especializaciones en $\operatorname{Spec} A$. Como el núcleo del morfismo $A \to B$ es nulo por hipótesis, el teorema del ascenso afirma que ϕ es epiyectiva, así que $x_0 = \phi(y_0)$ para algún $y_0 \in \operatorname{Spec} B$.

Aplicando ahora L.2.5 obtenemos especializaciones $y_0 > y_1 > \ldots > y_n$ en $\operatorname{Spec} B$ tales que $\phi(y_i) = x_i$, $0 \le i \le n$. Luego $\dim B \ge \dim A$ y, por L.2.4, concluimos que $\dim A = \dim B$.

Nota: Si el morfismo $A \to B$ es finito, los resultados de esta sección se obtienen directamente de la fórmula de la fibra $\phi^{-1}(x) = \operatorname{Spec} B \otimes_A \kappa(x)$:

Las fibras de ϕ son de dimensión 0 porque $B \otimes_A \kappa(x)$ es una $\kappa(x)$-álgebra finita (8.3.3 ó G.1.4). Además, si $j\colon A \to B$ es inyectivo, tenemos que $B_x \neq 0$ porque $j_x\colon A_x \to B_x$ es inyectivo. Al ser B_x un A_x-módulo de tipo finito, $\mathfrak{p}_x B_x \neq B_x$ por el lema de Nakayama; luego la fibra $\phi^{-1}(x) = \operatorname{Spec}(B_x/\mathfrak{p}_x B_x)$ no es vacía y concluimos que la aplicación $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectiva.

Ejemplos:

1. Sea U un abierto básico de una variedad algebraica afín X. Si U no es cerrado, la inclusión $U \to X$ no es un morfismo finito, aunque sus fibras son obviamente finitas, porque viola la tesis del Teorema del ascenso.

2. Sea C la curva plana compleja $x = y^2$ y sea U el abierto complementario del punto $(1,1)$ en C. La proyección $\pi\colon U \to \mathbb{A}_1$, $\pi(x,y) = x$, no es un morfismo finito: si $\mathcal{O}(U)$ fuera finito sobre $\mathbb{C}[x]$, sería finito sobre $\mathcal{O}(C)$; pero el morfismo $U \to C$ no es finito. No obstante, la proyección $\pi\colon U \to \mathbb{A}_1$ es cerrada, epiyectiva y sus fibras son finitas y discretas; incluso es abierta.

L.3 Lema de Normalización

Lema de Normalización de Noether (1882-1935)**:** *Sea A un álgebra de tipo finito sobre un cuerpo k. Existen elementos $x_1, \ldots, x_d \in A$ algebraicamente independientes sobre k tales que A es finita sobre $k[x_1, \ldots, x_d]$.*

Demostración: Sea $A = k[\xi_1 \ldots, \xi_n]$. Procedemos por inducción sobre n. Si $n = 0$, entonces $A = k$ y no hay nada que probar.

Sea $n \geq 1$. Si $\xi_1, \ldots, \xi_n$ son algebraicamente independientes sobre k, entonces A es finita sobre $k[\xi_1 \ldots, \xi_n] = A$. En caso contrario, verificarán alguna relación de dependencia algebraica, que escribimos en orden lexicográfico decreciente:

$$a\xi_1^{r_1}\xi_2^{r_2}\cdots\xi_n^{r_n} + \ldots \quad , \qquad a \neq 0$$

Sean $\xi_i' = \xi_i - \xi_n^{d_i}$, $1 \leq i \leq n-1$, donde $d_1 \gg d_2 \gg \ldots \gg d_{n-1}$. Es claro que $k[\xi_1, \xi_2, \ldots, \xi_n] = k[\xi_1', \ldots \xi_{n-1}', \xi_n]$ y, realizando las sustituciones $\xi_i = \xi_i' + \xi_n^{d_i}$ en la relación anterior, obtenemos una relación algebraica entre $\xi_1', \ldots, \xi_{n-1}', \xi_n$ en la que el término de mayor grado en ξ_n es

$$a\xi_n^{d_1 r_1 + \ldots + d_{n-1} r_{n-1} + r_n} \quad , \qquad a \neq 0$$

de modo que ξ_n es entero sobre $k[\xi_1', \ldots, \xi_{n-1}']$. Luego $A = k[\xi_1', \ldots, \xi_{n-1}', \xi_n]$ es finita sobre la subálgebra $k[\xi_1', \ldots, \xi_{n-1}']$. Por hipótesis de inducción existen elementos $x_1, \ldots, x_d \in k[\xi_1', \ldots, \xi_{n-1}']$ algebraicamente independientes sobre k tales que $k[\xi_1', \ldots, \xi_{n-1}']$ es finita sobre $k[x_1, \ldots, x_d]$. Concluimos que $A = k[\xi_1, \ldots, \xi_n]$ es finita sobre $k[x_1, \ldots, x_d]$.

Nota: Cuando k es infinito, la demostración se simplifica tomando $\xi_i' = \xi_i - \lambda_i \xi_n$, donde $\lambda_i \in k$. Es decir, la proyección finita $X \to \mathbb{A}_d$ es una proyección lineal genérica.

Corolario L.3.1 *La dimensión de $\mathbb{A}_{n,k}$ es n:* $\dim k[x_1, \ldots, x_n] = n$.

Demostración: Procedemos por inducción sobre n, y ya lo sabemos cuando $n \leq 1$. Si $0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m$ es una cadena de ideales primos en $k[x_1, \ldots, x_n]$, basta probar que $m \leq n$, porque claramente existe una cadena de longitud n:

$$0 \subset (x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n)$$

Sea $p(x_1, \ldots, x_n) \in \mathfrak{p}_1$ no nulo, y sea $k[\xi_1, \ldots, \xi_n] := k[x_1, \ldots, x_n]/(p)$, de modo que $k[\xi_1, \ldots, \xi_n]$ tiene dimensión $\geq m-1$. Por el lema de normalización existe un morfismo finito e inyectivo

$$k[y_1, \ldots, y_d] \longrightarrow k[\xi_1, \ldots, \xi_n]$$

donde $d < n$, porque $\xi_1, \ldots, \xi_n$ son algebraicamente dependientes. Por L.2.6 tenemos que $\dim k[\xi_1, \ldots, \xi_n] = \dim k[y_1, \ldots, y_d] = d$; luego $m - 1 \leq d \leq n - 1$.

Corolario L.3.2 *Toda variedad algebraica afín tiene dimensión finita.*

Demostración: $\dim k[x_1,\dots,x_n]/\mathfrak{a} \le \dim k[x_1,\dots,x_n] = n$.

En vista de estos corolarios y de L.2.6, el lema de normalización admite la siguiente reformulación geométrica:

Lema de Normalización: *Toda variedad algebraica afín X admite un morfismo finito y epiyectivo $X \to \mathbb{A}_d$ sobre un espacio afín de dimensión $d = \dim X$.*

Corolario L.3.3 *Sea A una k-álgebra de tipo finito íntegra y Σ su cuerpo de fracciones. La dimensión de Krull de A es el grado de trascendencia de Σ.*

Demostración: Por el lema de normalización tenemos un morfismo finito inyectivo $k[x_1,\dots,x_d] \to A$, donde $d = \dim A$. Luego Σ es una extensión finita de $k(x_1,\dots,x_d)$, y concluimos que su grado de trascendencia sobre k es d.

Corolario L.3.4 *Sea X una variedad algebraica afín sobre un cuerpo k. Si L es una extensión k, entonces*

$$\dim X = \dim X_L$$

Demostración: Por el lema de normalización tenemos un morfismo finito inyectivo $k[x_1,\dots,x_d] \to \mathcal{O}(X)$, donde $d = \dim X$. El morfismo

$$L[x_1,\dots,x_d] = k[x_1,\dots,x_d] \otimes_k L \longrightarrow \mathcal{O}(X) \otimes_k L = \mathcal{O}(X_L)$$

también es finito e inyectivo, y L.2.6 permite concluir que $d = \dim X_L$.

Corolario L.3.5 *Si X, Y son variedades algebraicas afines sobre un cuerpo k, entonces* $\dim (X \times_k Y) = \dim X + \dim Y$.

Demostración: Consideremos morfismos finitos inyectivos $k[x_1,\dots,x_d] \to \mathcal{O}(X)$ y $k[y_1,\dots,y_n] \to \mathcal{O}(Y)$, donde $d = \dim X$ y $n = \dim Y$. El morfismo

$$k[x_1,\dots,x_{d+n}] = k[x_1,\dots,x_d] \otimes_k k[y_1,\dots,y_n] \longrightarrow \mathcal{O}(X) \otimes_k \mathcal{O}(Y) = \mathcal{O}(X \times_k Y)$$

es finito e inyectivo, y L.2.6 permite concluir que $d + n = \dim (X \times_k Y)$.

Corolario L.3.6 *Toda variedad algebraica afín X de dimensión no nula tiene infinitos puntos cerrados.*

Demostración: El lema de normalización proporciona un morfismo finito y epiyectivo $\pi\colon X \to \mathbb{A}_d$, donde $1 \le \dim X = d$. Como $\mathbb{A}_d = \operatorname{Spec} k[x_1,\dots,x_d]$ tiene infinitos puntos cerrados, se concluye al aplicar L.2.2 al morfismo finito π.

Teorema de los Ceros de Hilbert (1862-1943)

Teorema de los Ceros: *Sea k un cuerpo y $\mathfrak{m}$ un ideal maximal de una k-álgebra finito-generada A. El cuerpo $A/\mathfrak{m}$ es una extensión finita de k.*

Demostración: Por el lema de normalización, existe un morfismo inyectivo finito

$$k[x_1, \ldots, x_d] \longrightarrow A/\mathfrak{m}$$

donde $d = \dim A/\mathfrak{m} = 0$. Luego $A/\mathfrak{m}$ es una extensión finita de k.

Corolario L.3.7 *Todo punto cerrado x de una variedad algebraica X sobre un cuerpo algebraicamente cerrado k es racional. En particular, si $\mathfrak{m}$ es un ideal maximal de $\mathbb{C}[x_1, \ldots, x_n]$, entonces existen $a_1, \ldots, a_n \in \mathbb{C}$ tales que*

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \ .$$

Demostración: Si k es algebraicamente cerrado, la extensión finita $k \to \kappa(x)$ es trivial, $k = \kappa(x)$, de modo que x es un punto racional de X.

Corolario L.3.8 *Toda variedad algebraica afín no vacía sobre un cuerpo algebraicamente cerrado tiene algún punto racional.*

Demostración: Si el espectro de un anillo no es vacío, tiene algún punto cerrado, y se aplica el corolario anterior.

Ejemplo: Si un sistema $p_1(x_1, \ldots, x_n) = \ldots = p_r(x_1, \ldots, x_n) = 0$ de ecuaciones polinómicas con coeficientes en un cuerpo algebraicamente cerrado k no admite soluciones en k, entonces $k[x_1, \ldots, x_n]/(p_1, \ldots, p_r) = 0$ de acuerdo con L.3.8. Es decir, existen polinomios $q_1, \ldots, q_r \in k[x_1, \ldots, x_n]$ tales que:

$$1 = q_1(x_1, \ldots, x_n)p_1(x_1, \ldots, x_n) + \ldots + q_r(x_1, \ldots, x_n)p_r(x_1, \ldots, x_n)$$

Corolario L.3.9 *Si X es una variedad algebraica afín de dimensión 0 sobre un cuerpo k, entonces su anillo de funciones algebraicas $\mathcal{O}(X)$ es un k-espacio vectorial de dimensión finita.*

Demostración: Como $\mathcal{O}(X)$ es un anillo de longitud finita, basta probar que todos los $\mathcal{O}(X)$-módulos simples son k-espacios vectoriales de dimensión finita. Ahora bien, los $\mathcal{O}(X)$-módulos simples son precisamente los cuerpos residuales de los puntos de X, que son extensiones finitas de k por el teorema de los ceros.

Corolario L.3.10 *Todo morfismo $X \to Y$ entre variedades algebraicas afines sobre un cuerpo k transforma puntos cerrados de X en puntos cerrados de Y.*

Demostración: Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}(X)$ formado por las funciones que se anulan en cierto punto cerrado x de X. La imagen de la composición

$$\mathcal{O}(Y) \longrightarrow \mathcal{O}(X) \longrightarrow \kappa(x)$$

es un cuerpo, porque $\kappa(x)$ es una extensión finita de k. Luego $\mathfrak{m} \cap \mathcal{O}(Y)$ es un ideal maximal de $\mathcal{O}(Y)$ y concluimos que la imagen de x en Y es un punto cerrado.

Teorema de los Ceros (forma fuerte)**:** *Sea A un álgebra de tipo finito sobre un cuerpo k. La intersección de todos los ideales maximales de A coincide con el radical de A (formado por los elementos nilpotentes).*

Demostración: Si $f \in A$ se anula en todos los puntos cerrados de $X = \operatorname{Spec} A$, el corolario anterior muestra que la variedad algebraica $U_f = X - (f)_0$ carece de puntos cerrados. Luego U_f es vacía; así que f se anula en todos los puntos de X y concluimos que f es nilpotente.

Corolario L.3.11 *Sea X una variedad algebraica afín sobre un cuerpo algebraicamente cerrado. Si una función algebraica se anula en todos los puntos racionales de X, entonces es nilpotente.*

Corolario L.3.12 *Sean Y_1 e Y_2 dos cerrados de una variedad algebraica afín X sobre un cuerpo algebraicamente cerrado k. La condición necesaria y suficiente para que Y_1 contenga a Y_2 es que pase por todos los puntos racionales de Y_2.*

En particular, cada cerrado de X (y por tanto cada abierto) está determinada por sus puntos racionales.

Demostración: La necesidad de la condición es obvia. Recíprocamente, si Y_1 pasa por todos los puntos racionales de Y_2, entonces todas las funciones algebraicas $f \in \mathcal{O}(X)$ que se anulen en Y_1 se anulan en los puntos cerrados de Y_2; luego se anulan en Y_2 por el teorema de los ceros, y concluimos que Y_1 contiene a Y_2.

Corolario L.3.13 *Si X e Y son variedades algebraicas afines reducidas (resp. conexas, irreducibles, íntegras) sobre un cuerpo algebraicamente cerrado k, entonces $X \times_k Y$ también es reducida (resp. conexa, irreducible, íntegra).*

Demostración: (Pedro Sancho) Si $X = \operatorname{Spec} A$ e $Y = \operatorname{Spec} B$ son reducidas, consideremos una base $\{h_i\}$ de B como k-espacio vectorial.

Si $\sum_i f_i \otimes h_i \in A \otimes_k B$ es nilpotente, entonces en todo punto racional $x \in X$ tenemos que $\sum_i f_i(x) h_i \in B$ es nilpotente; luego nula por hipótesis, y obtenemos que las funciones f_i se anulan en todos los puntos racionales de X. Por el teorema de los ceros, las funciones f_i son nilpotentes; luego son nulas y concluimos que $\sum_i f_i \otimes h_i = 0$.

Por otra parte, si X e Y son irreducibles y tenemos $X \times_k Y = C_1 \cup C_2$, donde C_1 y C_2 son cerrados, entonces en el espacio topológico Y_r formado por los puntos racionales de Y consideramos los subespacios

$$Y_i \;=\; \{y \in Y_r \colon X \times y \subseteq C_i\}$$

que son cerrados según L.3.14 . Como $Y_r = Y_1 \cup Y_2$, y Y_r es irreducible en virtud del corolario anterior, se sigue que $Y_r = Y_i$ para algún índice i. Luego C_i contiene todos los puntos racionales de $X \times_k Y$ y concluimos que $C_i = X \times_k Y$.

Análogamente se prueba que $X \times_k Y$ es conexa cuando X e Y lo son. Por último, las variedades íntegras son las variedades irreducibles reducidas.

Lema L.3.14 *Si C es un cerrado de $X \times_k Y$, entonces $Y_C := \{y \in Y_r \colon X \times y \subseteq C\}$ es un cerrado de Y_r.*

Demostración: Si $y \in Y_r$ no está en Y_C, entonces C no contiene a $X \times y$. Luego C no pasa por algún punto racional $x \times y$; así que $f(x \times y) \neq 0$ para alguna función $f \in \mathcal{O}(X \times_k Y)$ que se anula en C. Se sigue la existencia de algún entorno V de y en Y tal que f no se anula en $x \times V$, de modo que V no corta a Y_C.

L.4 Teorema del Descenso

Teorema de Cohen-Seidenberg (1917-1955 y 1916-1988)**:** *Sea A un anillo íntegramente cerrado en su cuerpo de fracciones Σ y sea Σ' una extensión normal de Σ. Si una subálgebra B de Σ' es entera sobre A y es estable por el grupo $G = \mathrm{Aut}_{\Sigma\text{-}alg}(\Sigma')$, entonces G actúa transitivamente en las fibras de la proyección $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$.*

Demostración: Sea $G = \{\sigma_1, \ldots, \sigma_n\}$. Consideremos dos puntos y, y' de la fibra de ϕ sobre un punto $x \in \operatorname{Spec} A$. Si $y' \neq \sigma_i(y)$ para todo índice i, según 8.6.4 existe una función $f \in B$ que se anula en y' y no se anula en ninguno de los puntos $\sigma_i(y)$, porque la fibra de ϕ sobre x tiene dimensión nula. Sea $p_f(x)$ el polinomio irreducible de f sobre Σ. Por hipótesis Σ' es una extensión normal de Σ, así que $p_f(x)$ tiene todas sus raíces en Σ' y éstas son de la forma $\sigma_i(f)$; en particular son enteras sobre A. Se sigue que el término independiente de

$$p_f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$$

que es el producto de todas las raíces cada una contada con su multiplicidad, es entero sobre A; luego $c_n \in A$, porque A es íntegramente cerrado en Σ. Además c_n se anula en $x = \phi(y')$ porque es múltiplo de f, que se anula en y'. Se sigue que $c_n = \prod \sigma_i(f)$ se anula en y, porque $\phi(y) = x$. Por tanto, existe $\sigma \in G$ tal que $\sigma(f)$ se anula en y, de modo que f se anula en $\sigma(y)$, lo que contradice la elección de la función f.

Teorema del Descenso: *Sea $A \to B$ un morfismo inyectivo y finito entre anillos íntegros. Si A es íntegramente cerrado en su cuerpo de fracciones Σ, entonces la correspondiente proyección $\phi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es abierta.*

Demostración: Sea Σ' una extensión del cuerpo de fracciones de B que sea extensión normal de Σ (tal extensión existe porque el cuerpo de fracciones de B es una extensión finita de Σ) y sea $G = \operatorname{Aut}_{\Sigma\text{-}alg}(\Sigma')$, que es un grupo finito. Sea $B = A[b_1, \ldots, b_n]$ y sea

$$B' = A[\sigma_i(b_j)]\ , \quad \sigma_i \in G\ ,\ 1 \leq j \leq n$$

Es claro que B' es estable por la acción de G y que B' es finito sobre A, porque sus generadores $\sigma_i(b_j)$ son enteros sobre A y podemos aplicar L.1.1. Consideremos las aplicaciones continuas

$$\operatorname{Spec} B' \xrightarrow{\psi} \operatorname{Spec} B \xrightarrow{\phi} \operatorname{Spec} A$$

inducidas por los morfismos estructurales $A \to B$ y $B \to B'$, y sea U un abierto de $\operatorname{Spec} B$. Por el teorema del ascenso, ψ es epiyectiva, de modo que $U = \psi\big(\psi^{-1}(U)\big)$ y para concluir que

$$\phi(U) = (\phi \circ \psi)\big(\psi^{-1}(U)\big)$$

es un abierto de $\operatorname{Spec} A$ bastará probar que la aplicación $\phi \circ \psi$ es abierta. En resumen, podemos suponer que B es estable por G. En tal caso, el teorema de Cohen-Seidenberg afirma que

$$\operatorname{Spec} A - \phi(U) = \phi\Big(\operatorname{Spec} B - \bigcup_{\sigma \in G} \sigma(U)\Big)$$

Por el teorema del ascenso ϕ es cerrada, así que el segundo término de la igualdad anterior es un cerrado de $\operatorname{Spec} A$ y concluimos que $\phi(U)$ es un abierto de $\operatorname{Spec} A$.

Corolario L.4.1 *En las hipótesis del teorema del descenso, si x' es una generalización de $x = \phi(y)$, entonces $x' = \phi(y')$ para alguna generalización y' de y.*

Demostración: La fibra $\phi^{-1}(x')$ es finita, así que su cierre Y está formado por las especializaciones de sus puntos, y bastará probar que $y \in Y$. Sea U el abierto complementario de Y en $\operatorname{Spec} B$. Si $y \notin Y$, entonces $x \in \phi(U)$, mientras que x' no está en $\phi(U)$. Ahora bien, por el teorema del descenso $\phi(U)$ es un abierto de $\operatorname{Spec} A$, lo que contradice la hipótesis de que x está en el cierre de x'.

Corolario L.4.2 *En las hipótesis del teorema del descenso, si $x = \phi(y)$, entonces*

$$\dim B_y = \dim A_x$$

Demostración: Si $x = x_0 < \ldots < x_n$ es una cadena de generalizaciones en $\operatorname{Spec} A$, L.4.1 permite obtener una cadena de generalizaciones $y = y_0 < \ldots < y_n$ en $\operatorname{Spec} B$ tal que $\phi(y_i) = x_i$ para todo $0 \leq i \leq n$. Luego $\dim B_y \geq \dim A_x$ y, de acuerdo con L.2.4, concluimos que $\dim B_y = \dim A_x$.

Corolario L.4.3 *Sea $X = \operatorname{Spec} A$ una variedad algebraica afín íntegra sobre un cuerpo. Si x es un punto cerrado de X, entonces* $\dim X = \dim A_x$.

Demostración: Procedemos por inducción sobre $d = \dim X$, pues el enunciado es evidente cuando $d = 0$.

En el caso general, considerando una proyección finita $X \to \mathbb{A}_d$ sobre un espacio afín, L.2.2 y L.4.2 permiten reducirse al caso $A = k[t_1, \ldots, t_d]$. Sea $p(t_1, \ldots, t_d)$ un polinomio no nulo que se anule en el punto x. Descomponiendo $p(t_1, \ldots, t_d)$ en factores irreducibles podemos suponer que $p(t_1, \ldots, t_d)$ es irreducible. Ahora A/pA es íntegro y L.3.3 muestra que $\dim A/pA = d - 1$; luego, por hipótesis de inducción, $\dim A_x/pA_x = d - 1$ y obtenemos que $d \leq \dim A_x$. Como siempre es cierta la desigualdad $\dim A_x \leq \dim A$, concluimos que $d = \dim A_x$.

Ejemplo: En el teorema del descenso, la hipótesis de que el anillo A sea íntegramente cerrado en su cuerpo de fracciones Σ no es superflua: Sea C la cúbica plana $y^2 = x^2 + x^3$ y sea $\psi\colon \mathbb{A}_1 \to C$ la parametrización $x = t^2 - 1$, $y = t^3 - t$, que es un morfismo finito birracional. La proyección finita

$$\phi = \psi \times (Id)\colon \mathbb{A}_1 \times \mathbb{A}_1 \longrightarrow C \times \mathbb{A}_1 \ , \quad \phi(t, u) = (t^2 - 1, t^3 - t, u)$$

satisface todas las hipótesis del teorema del descenso (¡incluso es birracional!), excepto la de que $\mathcal{O}(C \times \mathbb{A}_1) = k[x, y, z]/(y^2 - x^2 - x^3)$ sea íntegramente cerrado en su cuerpo de fracciones, y vamos a ver que la aplicación ϕ no es abierta.

Sea $y' = (t, t)$ el punto genérico de la diagonal de $\mathbb{A}_1 \times \mathbb{A}_1$ y sea $x' = \phi(y')$. Como ϕ es un isomorfismo fuera de la recta $x = y = 0$, se sigue que y' es el único punto de $\phi^{-1}(x')$, porque $x' = (t^2 - 1, t^3 - t, t)$ no es un punto de la recta $x = y = 0$. Luego x' no está en $\phi(U)$, donde U denota el abierto complementario de la diagonal. Ahora bien, y' es una generalización del punto cerrado $y = (1, 1)$, así que x' es una generalización del punto $x = (0, 0, 1)$. Como $x \in \phi(U)$, porque $x = \phi(-1, 1)$, concluimos que $\phi(U)$ no es un abierto de $C \times \mathbb{A}_1$.

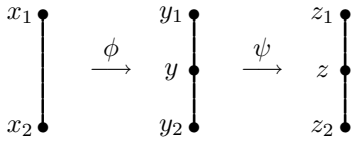
Lema L.4.4 *Sea $\phi\colon X \to Y$ un morfismo finito entre variedades algebraicas afines sobre un cuerpo k. Si $x_0 > x_1 > \ldots > x_n$ es una cadena irrefinable de especializaciones en X, entonces $\phi(x_0) > \phi(x_1) > \ldots > \phi(x_n)$ es una cadena irrefinable de especializaciones en Y.*

Demostración: (Pedro Sancho) Según L.2.3, no se dan igualdades $\phi(x_i) = \phi(x_{i+1})$; luego basta probar que las especializaciones $\phi(x_i) > \phi(x_{i+1})$ son irrefinables.

Supongamos que existe en X una especialización irrefinable $x_1 > x_2$ tal que $y_1 > y_2$ pueda refinarse en Y (donde $\phi(x_i) = y_i$): $y_1 > y > y_2$. Sea X_1 el cierre de x_1 en X y sea Y_1 el cierre de y_1 en Y, de modo que

$$\phi\colon X_1 \longrightarrow Y_1$$

es una proyección finita entre variedades algebraicas íntegras. Sea $\psi\colon Y_1 \to \mathbb{A}_d$ una proyección finita:



Ahora, $\psi\phi\colon X_1 \to \mathbb{A}_d$ es una proyección finita entre variedades íntegras. De acuerdo con el teorema del descenso, se sigue la existencia de una generalización x de x_2 en $X_1 = \overline{\{x_1\}}$ tal que $\psi\phi(x) = z$, en contradicción con el carácter irrefinable de la especialización $x_1 > x_2$.

Definición: Diremos que un anillo de dimensión finita A es **catenario** si para cada par de ideales primos $\mathfrak{p} \subset \mathfrak{p}'$ se verifica que todas las cadenas irrefinables $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \ldots \subset \mathfrak{p}_n = \mathfrak{p}'$ tienen igual longitud.

Para que un anillo de dimensión finita sea catenario, basta que verifique tal condición cuando $\mathfrak{p}$ es un ideal primo minimal y $\mathfrak{p}'$ es un ideal maximal.

Teorema L.4.5 *Las variedades algebraicas afines sobre un cuerpo son catenarias.*

Demostración: Procedemos por inducción sobre la dimensión de la variedad algebraica, pues es evidente que los anillos de dimensión 0 son catenarios.

En el caso general, considerando una proyección finita sobre un espacio afín, el lema anterior permite reducirlo al caso del espacio afín $\mathbb{A}_d$. En tal caso, consideremos una cadena irrefinable de ideales primos de $k[t_1, \ldots, t_d]$:

$$0 = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_r = \mathfrak{m}$$

y un polinomio $p(t_1, \ldots, t_d) \in \mathfrak{p}_1$ no nulo. Descomponiendo p en factores irreducibles, podemos suponer que p es irreducible. En tal caso (p) es un ideal primo, de modo que $\mathfrak{p}_1 = (p)$ en virtud del carácter irrefinable de la cadena elegida. Ahora L.3.3 muestra que $\dim k[t_1, \ldots, t_d]/\mathfrak{p}_1 = d - 1$; luego, por hipótesis de inducción, $k[t_1, \ldots, t_d]/\mathfrak{p}_1$ es un anillo catenario, y L.4.3 permite obtener que $r - 1 = d - 1$. Concluimos que tales cadenas irrefinables tienen todas longitud $r = d$.

Apéndice M

Morfismos Finitos Birracionales

M.1 Anillos de Valoración Discreta

Definición: Sea Σ un cuerpo. Una **valoración discreta** (no trivial) de Σ es una aplicación epiyectiva $v\colon \Sigma - \{0\} \to \mathbb{Z}$ tal que

1. $v(fg) = v(f) + v(g)$.
2. $v(f+g) \geq \min\big(v(f), v(g)\big)$.

A menudo es conveniente extender v a todo Σ poniendo $v(0) = +\infty$, de modo que $\{f \in \Sigma\colon\ v(f) \geq 0\}$ es un anillo, llamado anillo de v.

Diremos que un dominio de integridad $\mathcal{O}$ es un **anillo de valoración discreta** si es el anillo de alguna valoración discreta v de su cuerpo de fracciones.

Los elementos invertibles de un anillo de valoración discreta $\mathcal{O}$ son los de valor nulo, así que $\mathcal{O}$ es un anillo local y su único ideal maximal es

$$\mathfrak{m} = \{f \in \Sigma\colon\ v(f) > 0\}\ .$$

Además, $\mathfrak{m} = t\mathcal{O}$ justamente cuando $v(t) = 1$ (existen elementos de valor 1 porque $v\colon \Sigma - \{0\} \to \mathbb{Z}$ es epiyectiva por definición).

Nótese que, para todo $f \in \Sigma$ se tiene que $f \in \mathcal{O}$ ó $f^{-1} \in \mathcal{O}$. Por otra parte, si $\mathfrak{a}$ es un ideal no nulo de $\mathcal{O}$ y n es el mínimo valor de sus elementos, entonces

$$\mathfrak{a} \ = \ t^n\mathcal{O} \ = \ \mathfrak{m}^n\ .$$

En particular, $\mathcal{O}$ es un anillo local regular de dimensión 1.

Teorema M.1.1 *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión 1. Las siguientes condiciones son equivalentes:*

1. *$\mathcal{O}$ es regular.*

2. *$\mathcal{O}$ es un anillo de valoración discreta.*

3. *$\mathcal{O}$ es íntegramente cerrado en su cuerpo de fracciones Σ.*

Demostración: $(1 \Rightarrow 2)$ Sea t un parámetro local de $\mathcal{O}$. Si f es un elemento no nulo de $\mathcal{O}$, entonces $f\mathcal{O} = t^n\mathcal{O}$ para un único número natural n, y definimos $v(f) = n$. Extendemos v a $\Sigma - \{0\}$ poniendo $v(f/g) = v(f) - v(g)$. Es sencillo comprobar que v está bien definida, que es una valoración discreta de Σ y que su anillo $\{f \in \Sigma\colon\ v(f) \geq 0\}$ es precisamente $\mathcal{O}$.

$(2 \Rightarrow 3)$ Sea $f \in \Sigma$ entero sobre $\mathcal{O}$:

$$f^n + a_1 f^{n-1} + \ldots + a_n = 0 \quad , \qquad a_i \in \mathcal{O}$$

Si $f \notin \mathcal{O}$, entonces $f^{-1} \in \mathcal{O}$ y $f = -a_1 + a_2 f^{-1} - \ldots - a_n f^{1-n} \in \mathcal{O}$.

$(3 \Rightarrow 1)$ Sea f un elemento no nulo del único ideal maximal $\mathfrak{m}$ de $\mathcal{O}$. Como $\mathfrak{m}$ es el único ideal primo no nulo de $\mathcal{O}$, es el radical de $f\mathcal{O}$; así que tendremos $\mathfrak{m}^n \not\subseteq f\mathcal{O}$ y $\mathfrak{m}^{n+1} \subseteq f\mathcal{O}$ para algún exponente n. Sea $g \in \mathfrak{m}^n$ tal que $g \notin f\mathcal{O}$ y sea $x = g/f$, de modo que

$$x\mathfrak{m} \subseteq \mathcal{O} \quad , \qquad x \notin \mathcal{O}$$

y para concluir que $\mathfrak{m}$ es un ideal principal bastará ver que $x\mathfrak{m} = \mathcal{O}$. En caso contrario $x\mathfrak{m} \subseteq \mathfrak{m}$ y x define un endomorfismo $x\cdot\colon \mathfrak{m} \to \mathfrak{m}$, así que ha de satisfacer el correspondiente polinomio característico. Luego x es entero sobre $\mathcal{O}$, contra la hipótesis de que $\mathcal{O}$ es íntegramente cerrado en su cuerpo de fracciones.

Ejemplos:

1. Sea p un elemento irreducible de un dominio de ideales principales A. Si $a \in A$, definimos $v_p(a) = n$ cuando $a = p^n a'$, donde a' no es múltiplo de p, y extendemos v_p al cuerpo de fracciones Σ de A definiendo $v_p(a/b) = v_p(a) - v_p(b)$. Es sencillo comprobar que v_p es una valoración discreta de Σ, llamada *valoración p-ádica*, y que su anillo es A_p.

2. Sea x un punto no-singular de una curva C sobre un cuerpo k. Para cada función racional $f \in \Sigma_C$ denotaremos $v_x(f)$ el número de ceros de f en x (que es negativo si f tiene polos en x), obteniendo así una valoración discreta v_x de Σ_C. Su anillo coincide con el anillo local $\mathcal{O}_{C,x}$ de la curva C en x.

3. Sea k un cuerpo. La valoración discreta v_∞ del cuerpo $k(t)$ asociada al punto $u = 0$ de la recta afín $\operatorname{Spec} k[u]$, donde $u = t^{-1}$, recibe el nombre de valoración del infinito, porque mide "el número de ceros de una función racional $p(t)/q(t)$ en el punto $t = \infty$":

$$v_\infty\left(\frac{p(t)}{q(t)}\right) = \operatorname{gr} q(t) - \operatorname{gr} p(t)$$

4. Por abuso de lenguaje, a veces se dice que la aplicación $v\colon \Sigma - \{0\} \to \mathbb{Z}$, $v(f) = 0$ para todo $f \in \Sigma - \{0\}$, es una valoración discreta de Σ, llamada **valoración trivial**, aunque no responda a nuestra definición por no ser epiyectiva.

M.2 Anillos Normales

Definición: Diremos que un anillo íntegro es **normal** si es íntegramente cerrado en su cuerpo de fracciones.

Lema M.2.1 *Sea $A \to B$ un morfismo de anillos y sea C el cierre entero de A en B. Si S es un sistema multiplicativo de A, entonces $S^{-1}C$ es el cierre entero de $S^{-1}A$ en $S^{-1}B$.*

Demostración: Sabemos que $S^{-1}C$ es entero sobre $S^{-1}A$. Por otra parte, si $b/s \in S^{-1}B$ es entero sobre $S^{-1}A$, ha de verificar alguna relación

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \ldots + (a_n/s_n) = 0 \quad , \qquad a_i \in A\,,\ s_i \in S$$

Sea $t = s_1 \cdots s_n$. Multiplicando la relación anterior por $s^n t^n$ obtenemos una relación de dependencia entera de bt sobre A; luego $bt \in C$ y $b/s = bt/st \in S^{-1}C$.

Corolario M.2.2 *Si A es un anillo íntegro, las siguientes condiciones son equivalentes:*

1. *A es normal.*
2. *A_x es normal para todo punto cerrado $x \in \operatorname{Spec} A$.*

Demostración: Sea $\bar{A}$ el cierre entero de A en su cuerpo de fracciones. La condición de que A sea normal equivale a la anulación del A-módulo $\bar{A}/A$, que es una cuestión local. De acuerdo con M.2.1, la condición $0 = (\bar{A}/A)_x = \bar{A}_x/A_x$ significa que A_x es normal.

Corolario M.2.3 *Todo anillo normal noetheriano A es regular en codimensión 1. Es decir, A_x es un anillo local regular cuando* $\dim A_x = 1$.

Corolario M.2.4 *Sea A un anillo íntegro noetheriano de dimensión 1. La condición necesaria y suficiente para que A sea un dominio de Dedekind es que sea normal.*

Teorema M.2.5 *Sea B un anillo de Dedekind de cuerpo de fracciones Σ. Los anillos de valoración discreta de Σ que contienen a B son los anillos locales B_x en los puntos $x \in \operatorname{Spec} B$, y B es la intersección de todos los anillos de valoración discreta que lo contienen:*

$$B = \bigcap_x B_x$$

Demostración: Los anillos locales B_x son anillos de valoración discreta porque son normales y de dimensión 1, y obviamente contienen a B.

Recíprocamente, si un anillo de valoración discreta $\mathcal{V}$ de Σ contiene a B, entonces $\mathfrak{m}_x = \mathfrak{m}_{\mathcal{V}} \cap B$ es un ideal maximal de B y $B_x \subseteq \mathcal{V}$. Si no se diera la igualdad $B_x = \mathcal{V}$, al ser B_x un anillo de valoración discreta, existiría $f \in \mathcal{V}$ tal que $v_x(f) < 0$; luego $f^{-1} \in \mathfrak{m}_x \subseteq \mathfrak{m}_{\mathcal{V}}$, en contra de que $f \in \mathcal{V}$.

Por último, la igualdad $B = \bigcap B_x$ es válida para todo anillo íntegro. En efecto, la condición $a/b \in \bigcap B_x$ significa que $aB_x \subseteq bB_x$ para todo $x \in \operatorname{Spec} B$, lo que equivale a que $aB \subseteq bB$ de acuerdo con 8.2.7; es decir, a que $a/b \in B$.

M.3 Finitud del Cierre Entero

Teorema de Finitud: *Sea A un anillo normal noetheriano y L una extensión finita separable de su cuerpo de fracciones Σ. El cierre entero B de A en L es un A-módulo de tipo finito.*

Demostración: Como la extensión finita $\Sigma \to L$ es separable, la métrica de la traza $T_2(\alpha, \beta) = \operatorname{tr}(\alpha\beta)$ tiene radical nulo (I.2.2). Además, $\operatorname{tr}(\beta) = \sigma_1(\beta) + \ldots + \sigma_d(\beta)$ donde $\sigma_1, \ldots, \sigma_d \colon L \to L'$ son los puntos de L con valores en una extensión L' que la trivialice (I.2.1). Luego, si $b \in B$, entonces $\operatorname{tr}(b)$ es entero sobre A, de modo que $\operatorname{tr}(b) \in B \cap \Sigma = A$.

Por otra parte, todo elemento $\beta \in L$ es algebraico sobre Σ, así que satisface una ecuación de la forma

$$a_0\beta^m + a_1\beta^{m-1} + \ldots + a_m = 0\ , \quad a_i \in A$$

Multiplicando esta relación por a_0^{m-1} vemos que $a_0\beta$ es entero sobre A. Luego, dada una base de L sobre Σ, podemos multiplicar sus elementos por elementos convenientes de A de modo que se obtenga una base $b_1, \ldots, b_n$ formada por elementos de B. Consideremos su base dual $b_1^*, \ldots, b_n^*$ respecto de la métrica de la traza, de modo que $\operatorname{tr}(b_i \cdot b_j^*) = \delta_{ij}$. Si $x \in B$, entonces las coordenadas de x en

la base dual coinciden con los valores de x (entendido como forma lineal sobre L mediante la métrica de la traza) sobre los vectores de la base:

$$x = \sum_{i=1}^{n} \mathrm{tr}(x \cdot b_i)\, b_i^*$$

Como $xb_i \in B$, se sigue que $\mathrm{tr}(xb_i) \in A$. Luego B es un submódulo del A-módulo de tipo finito $Ab_1^* + \ldots + Ab_n^*$ y, al ser A noetheriano, concluimos que B es un A-módulo de tipo finito.

Teorema M.3.1 *Sea k un cuerpo, A una k-álgebra de tipo finito íntegra y Σ su cuerpo de fracciones. El cierre entero de A en cualquier extensión finita L de Σ es un A-módulo finito y, por tanto, también es una k-álgebra de tipo finito.*

Demostración: En virtud del lema de normalización, existe un morfismo inyectivo y finito $k[x_1, \ldots, x_n] \to A$. Luego el cierre entero de A en L coincide con el cierre entero de $k[x_1, \ldots, x_n]$ en L, que es una extensión finita de $k(x_1, \ldots, x_n)$, así que podemos suponer que $A = k[x_1, \ldots, x_n]$ y $\Sigma = k(x_1, \ldots, x_n)$.

Si la característica de k es nula, se concluye al aplicar el teorema anterior, pues $k[x_1, \ldots, x_n]$ es un anillo normal noetheriano.

Si la característica p de k es positiva, fijamos una extensión finita $L \to \bar{L}$ tal que $\bar{L}$ sea extensión normal de Σ (ver H.3.22), y bastará probar que el cierre entero de A en $\bar{L}$ es A-módulo finito, porque el cierre entero de A en L es un submódulo y A es noetheriano. Si $G = \mathrm{Aut}(\bar{L}/\Sigma)$, entonces $\bar{L}$ es una extensión separable de $\bar{L}^G$ por el teorema de Artin, y $\bar{L}^G$ es una extensión puramente inseparable de Σ (ver I.4.3). Si demostramos que el cierre entero B de A en $\bar{L}^G$ es A-módulo finito, entonces B es un anillo normal noetheriano, y el teorema de finitud permitiría concluir que el cierre entero de B en $\bar{L}$, que es el cierre entero de A en $\bar{L}$, es un B-módulo finito y por tanto un A-módulo finito.

En resumen basta probar el teorema en el caso en que $A = k[x_1, \ldots, x_n]$ y L es una extensión finita puramente inseparable de $\Sigma = k(x_1, \ldots, x_n)$. En este caso, por I.4.2 existe una potencia $q = p^r$ tal que $L = \Sigma(\alpha_1, \ldots, \alpha_r)$ y $\alpha_i^q \in \Sigma$, $1 \le i \le r$. Si $\alpha_i^q = p_i/q_i$, entonces $(q_i\alpha_i)^q = p_i q_i^{q-1}$, así que podemos suponer que $\alpha_i^q \in A$:

$$\begin{aligned} \alpha_i^q &= \sum_{j_1 \ldots j_n} a_{i,j_1\ldots j_n} x_1^{j_1} \ldots x_n^{j_n} \\ \alpha_i &= \sum_{j_1 \ldots j_n} \sqrt[q]{a_{i,j_1\ldots j_n}}\, y_1^{j_1} \ldots y_n^{j_n} \qquad , \qquad y_j := \sqrt[q]{x_j} \end{aligned}$$

Si K denota la extensión finita de k que se obtiene adjuntando las raíces q-ésimas de los coeficientes $a_{i,j_1\ldots j_n}$, entonces $L = k(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_r)$ está contenida en $K(y_1, \ldots, y_n)$. Como el anillo $K[y_1, \ldots, y_n]$ es normal y es finito sobre $k[x_1, \ldots, x_n] = k[y_1^q, \ldots, y_n^q]$, se sigue que es el cierre entero de $A = k[x_1, \ldots, x_n]$

en $K(y_1, \ldots, y_n)$. Luego el cierre entero de A en $K(y_1, \ldots, y_n)$, y por tanto el cierre entero de A en L, es un A-módulo finito.

Corolario M.3.2 *Sea k un cuerpo. Si A es una k-álgebra de tipo finito íntegra, entonces el cierre entero $\bar{A}$ de A en su cuerpo de fracciones es un A-módulo de tipo finito. En particular $\bar{A}$ también es una k-álgebra de tipo finito.*

M.4 Desingularización de Curvas

Sea $C = \operatorname{Spec} A$ una curva íntegra sobre un cuerpo k (i.e., A es una k-álgebra de tipo finito íntegra de dimensión 1) y sea $\bar{A}$ el cierre entero de A en su cuerpo de fracciones Σ_C.

Teorema M.4.1 *El A-módulo $\bar{A}/A$ tiene longitud finita.*

Demostración: La localización de $\bar{A}/A$ en el punto genérico p_g de C es nula

$$(\bar{A}/A)_{p_g} = \bar{A}_{p_g}/A_{p_g} = \Sigma_C/\Sigma_C = 0$$

así que el soporte del A-módulo $\bar{A}/A$ está formado por puntos cerrados. Según M.3.2, el A-módulo $\bar{A}/A$ es de tipo finito y concluimos al aplicar 8.5.4.

Teorema M.4.2 *El número de puntos singulares de C es finito.*

Demostración: La condición de que un punto cerrado x de C sea no-singular equivale a la anulación de $(\bar{A}/A)_x$, porque $(\bar{A})_x$ es el cierre entero de $A_x = \mathcal{O}_{C,x}$ en su cuerpo de fracciones. Luego los puntos singulares de C son los del soporte de $\bar{A}/A$, formado por un número finito de puntos cerrados según 8.5.4.

Definición: De acuerdo con M.3.2, el cierre entero $\bar{A}$ es una k-álgebra de tipo finito; luego $\bar{C} = \operatorname{Spec} \bar{A}$ es una curva íntegra no-singular sobre el cuerpo k, y diremos que el morfismo natural $\bar{C} \to C$, que es finito y birracional, es la **desingularización** de la curva C.

Definición: Diremos que una valoración discreta v del cuerpo Σ_C está **centrada** en un punto x de C, y lo denotaremos con el símbolo $v \to x$, cuando su anillo $\mathcal{V} = \{f \in \Sigma_C \colon\ v(f) \geq 0\}$ **domine** al anillo local A_x de C en x, en el sentido de que

$$A_x \subseteq \mathcal{V} \qquad \text{y} \qquad \mathfrak{m}_x = \mathfrak{m}_{\mathcal{V}} \cap A_x$$

donde $\mathfrak{m}_x$ y $\mathfrak{m}_{\mathcal{V}}$ denotan los ideales maximales de A_x y $\mathcal{V}$ respectivamente.

Para que v centre en x es suficiente que $A_x \subseteq \mathcal{V}$, porque los únicos ideales primos de A_x son el ideal maximal y el ideal nulo, y la igualdad $0 = \mathfrak{m}_{\mathcal{V}} \cap A_x$ implicaría que el cuerpo de fracciones Σ_C de A_x estaría contenido en $\mathcal{V}$.

Corolario M.4.3 *Las valoraciones discretas de Σ_C con centro en un punto x de C son los anillos locales de $\bar{C}$ en los puntos de su fibra sobre x.*

Demostración: En virtud de M.1.1, los anillo de valoración discreta de Σ_C que contienen a A_x son los que contienen al cierre entero $\bar{A}_x$. Ahora el teorema M.2.5 permite conluir, pues los anillos locales de $\bar{A}_x$ son los anillos locales de $\bar{A}$ en los puntos de la fibra de x.

Además, M.2.5 también permite concluir que

Corolario M.4.4 *El cierre entero de A_x en su cuerpo de fracciones Σ_C es la intersección de todos los anillos de valoración discreta de Σ_C con centro en x.*

Corolario M.4.5 *Para toda función no nula $f \in A_x$ tenemos que*

$$l(A_x/fA_x) \;=\; \sum_{v_i \to x} v_i(f) \cdot [\kappa(x_i)\colon \kappa(x)]$$

donde x_i es el centro de la valoración discreta v_i en $\bar{C}$.

Demostración: El morfismo $\bar{A}_x/A_x \xrightarrow{f\cdot} f\bar{A}_x/fA_x$ es un isomorfismo, así que ambos A_x-módulos tienen la misma longitud. Considerando el siguiente cuadrado conmutativo:

$$\begin{array}{ccc} fA_x & \to & f\bar{A}_x \\ \downarrow & & \downarrow \\ A_x & \to & \bar{A}_x \end{array}$$

el carácter aditivo de la longitud permite obtener que

$$l(A_x/fA_x) = l(\bar{A}_x/f\bar{A}_x)$$

Ahora bien, cuando f es invertible en A_x, el teorema es obvio, así que podemos suponer que f se anula en x. En tal caso el anillo $\bar{A}_x/f\bar{A}_x$ tiene dimensión 0 y descompone en suma directa de sus localizaciones en los puntos $x_1, \ldots, x_n$ de su espectro, que son los puntos de $\bar{C}$ sobre x:

$$\bar{A}_x/f\bar{A}_x = \bigoplus_{i=1}^{n} \bar{A}_{x_i}/f\bar{A}_{x_i}$$
$$l(A_x/fA_x) = \sum_{v_i \to x} l(\bar{A}_{x_i}/f\bar{A}_{x_i})$$

Ahora bien la longitud del A_x-módulo $\bar{A}_{x_i}/f\bar{A}_{x_i}$ es el producto de su longitud como $\bar{A}_{x_i}$-módulo por la longitud del cuerpo residual $\kappa(x_i)$ (el único $\bar{A}_{x_i}$-módulo simple), que es $[\kappa(\bar{x}_i)\colon \kappa(x)]$:

$$l(\bar{A}_{x_i}/f\bar{A}_{x_i}) \;=\; \bar{l}(\bar{A}_{x_i}/f\bar{A}_{x_i}) \cdot [\kappa(x_i) : \kappa(x)]$$

donde $\bar{l}$ denota la longitud como $\bar{A}_{x_i}$-módulo. Para concluir basta observar que, si $f\bar{A}_{x_i} = \mathfrak{m}_{x_i}^n$, entonces $\bar{l}(\bar{A}_{x_i}/f\bar{A}_{x_i}) = n = v_i(f)$.

Corolario M.4.6 *La multiplicidad de intersección de una curva íntegra C con una hipersuperficie H de ecuación $f = 0$, en un punto $x \in C$, es*

$$(C \cap H)_x \;=\; \sum_{v_i \to x} v_i(f) \cdot [\kappa(x_i)\colon \kappa(x)]$$

Transformaciones Cuadráticas

Dada una valoración discreta v centrada en x, las funciones $f \in \mathfrak{m}_x$ que no tienen valor $v(f)$ mínimo forman un subespacio vectorial $\neq \mathfrak{m}_x$. Si suponemos que *el cuerpo base k es infinito*, la unión de un número finito de subespacios vectoriales $\neq \mathfrak{m}_x$ no puede coincidir con $\mathfrak{m}_x$; luego ha de existir alguna función $f \in \mathfrak{m}_x$ con valor mínimo para todas las valoraciones discretas v_i centradas en x. Sea $\{f_1, \ldots, f_d\}$ un sistema de generadores del ideal maximal $\mathfrak{m}_x$. Llamaremos **transformación cuadrática** o **explosión** del anillo A_x al anillo

$$A_1 = A_x\left[f_1 f^{-1}, \ldots, f_d f^{-1}\right]$$

y la condición de que las valoraciones $v_i(f)$ son mínimas significa que $v_i(f_j f^{-1}) \geq 0$ para todo par de índices i, j. Es decir, $f_j f^{-1} \in \bar{A}_x$, de modo que la transformación cuadrática $A_x \to A_1$ es un morfismo finito birracional:

$$A_x \subseteq A_1 \subseteq \bar{A}_x$$

La explosión $A_x \to A_1$ nunca es un isomorfismo, salvo cuando x sea un punto no-singular de C, ya que de la igualdad $A_x = A_1$ se sigue que $f_j/f \in A_x$, lo que significa que $\mathfrak{m}_x = f A_x$ es un ideal principal.

Si A_1 no coincide con el cierre entero $\bar{A}_x$, algún punto de su espectro ha de ser singular. En tal caso, consideramos los anillos locales de A_1 en sus puntos singulares y en cada uno efectuamos la transformación cuadrática. Reiterando el proceso (que debe terminar después de un número finito de pasos al ser finita la longitud de $\bar{A}_x/A_x$) *con un número finito de transformaciones cuadráticas obtenemos todas las valoraciones discretas de Σ_C centradas en el punto x.*

La explosión $A_1 = A_x[f_1 f^{-1}, \ldots, f_d f^{-1}]$ claramente no depende de los generadores $f_1, \ldots, f_d$ de $\mathfrak{m}_x$ elegidos. Tampoco depende de la función f. En efecto, si $g \in \mathfrak{m}_x$ es otra función con valores $v_i(g)$ mínimos, entonces $v_i(g) = v_i(f)$, de modo que $g f^{-1} \in A_1$ no se anula en los puntos cerrados $\bar{x}_i$ de $\operatorname{Spec} \bar{A}_x$. Como el morfismo $A_1 \to \bar{A}_x$ es finito, se sigue que $g f^{-1}$ no se anula en ningún punto cerrado de $\operatorname{Spec} A_1$ y $g f^{-1}$ es invertible en A_1:

$$A_x\left[f_1 g^{-1}, \ldots, f_d g^{-1}\right] \subseteq A_1 = A_x\left[f_1 f^{-1}, \ldots, f_d f^{-1}\right]$$

porque $f_j g^{-1} = (f_j f^{-1})(f g^{-1}) \in A_x[f_1 f^{-1}, \ldots, f_d f^{-1}]$. Análogamente se demuestra la inclusión contraria.

Nota: Si se desea desingularizar la curva afín $C = \operatorname{Spec} A$; es decir, obtener su cierre entero $\bar{A}$ y no sólo los anillos locales de $\bar{A}$, debe modificarse ligeramente el proceso anterior. Elegido un punto singular x de C, se consideran generadores de su ideal maximal $\mathfrak{m} = (f_1, \ldots, f_d)$ y una función $f \in \mathfrak{m}$ que tome valor mínimo en todas la valoraciones discretas de Σ_C centradas en x y que no se anule en los demás puntos singulares de C. Ahora no podemos asegurar que las funciones $f_j f^{-1}$ sean enteras sobre A, porque f puede tener otros ceros $x_1, \ldots, x_r$ en C además del punto singular x fijado. En tal caso se elige una función $g \in A$ que no se anule en ningún punto singular de C y que en los puntos $x_1, \ldots, x_r$ tenga igual número de ceros que f (existe por 7.1.1). Por construcción las funciones $f_j g f^{-1}$ tienen valor ≥ 0 en todas las valoraciones discretas centradas en puntos de C; luego son enteras sobre A y el morfismo

$$A \longrightarrow A_1 = A\left[f_1 g f^{-1}, \ldots, f_d g f^{-1}\right]$$

es finito y birracional. Si $A = A_1$, entonces $f_j g \in fA$. Como la función g no se anula en x, es invertible en A_x y concluimos que $\mathfrak{m}A_x = fA_x$ es un ideal principal, contra la hipótesis de que el punto x es singular. Luego la longitud de A_1/A no es nula y $l(\bar{A}_1/A_1) = l(\bar{A}/A_1) < l(\bar{A}/A)$. Reiterando el proceso, después de un número finito de pasos obtenemos el cierre entero $\bar{A}$ de A.

Curvas planas: Consideremos un punto racional singular de una curva plana C sobre un cuerpo infinito. Después de un cambio de coordenadas lineal podemos suponer que el punto es el origen de coordenadas y que la recta $x = 0$ no es tangente a C en el origen:

$$0 = a_0 y^r + a_1 x y^{r-1} + \ldots + a_r x^r + \sum_{i+j>r} a_{ij} x^i y^j \ , \quad a_0 \neq 0$$

Dividiendo por x^r obtenemos una relación de dependencia entera

$$0 = \left(a_0 + \sum_{i+j>r,\, j\geq r} a_{ij} x^i y^{j-r}\right)\left(y x^{-1}\right)^r + \ldots$$

de yx^{-1} sobre el anillo local $\mathcal{O}$ de la curva C en el origen. Luego ninguna valoración discreta de Σ_C centrada en el origen toma valor negativo en yx^{-1}, de modo que el valor de x es el mínimo entre los de las funciones que se anulan en el origen, y la transformación cuadrática de $\mathcal{O}$ es precisamente

$$\mathcal{O}_1 = \mathcal{O}\left[\, y x^{-1} \,\right]$$

Por ejemplo, sea C la curva plana compleja de ecuación

$$0 = y^7 - x^9 y - x^{10} y + x^{11} + x^{12} = p(x, y)$$

C es íntegra porque $p(x,y)$ es un polinomio irreducible (aplíquese el criterio de Eisenstein al polinomio $p(a,y)$ con coeficientes en $\mathbb{C}[a]$). Sea $\mathcal{O}$ el anillo local de C en el origen, que es un punto singular. Vamos a determinar las valoraciones discretas del cuerpo de funciones racionales Σ_C centradas en el origen. Como la recta $x=0$ no es tangente a C en el origen y

$$\boxed{z = y/x}$$

$$\begin{aligned} 0 = p(x,xz) =& x^7z^7 - x^{10}z - x^{11}z + x^{11} + x^{12} \\ =& x^7(z^7 - x^3z - x^4z + x^4 + x^5) \\ 0 = p_1(x,z) =& x^4 - x^3z + x^5 - x^4z + z^7 \end{aligned}$$

la transformación cuadrática $\mathcal{O}_1 = \mathcal{O}[y/x]$ de $\mathcal{O}$ es la localización del anillo de funciones algebraicas de la curva $p_1(x,z)=0$ por las funciones $f(x,y)$ que no se anulan en el punto $x=y=0$. Luego la fibra de la explosión sobre el punto $x=y=0$ son los puntos de corte de $p_1(x,z)=0$ con la recta $x=0$, porque $y \in x\mathcal{O}_1$. En nuestro caso sólo se cortan en el punto $x=z=0$, que es un punto singular de la curva $p_1(x,z)=0$. Efectuemos la explosión de la curva $p_1(x,z)=0$ en tal punto (donde la recta $x=0$ es tangente; pero no $z=0$):

$$\boxed{s = x/z}$$

$$\begin{aligned} 0 = p_1(zs,z) &= z^4s^4 - z^4s^3 + z^5s^5 - z^5s^4 + z^7 \\ &= z^4(s^4 - s^3 + zs^5 - zs^4 + z^3) \\ 0 = p_2(z,s) &= z^3 - s^3 + s^4 - zs^4 + zs^5 \end{aligned}$$

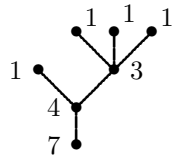
y la fibra de la curva $p_2(z,s)=0$ sobre el punto $x=0$, $z=0$, que es el corte con la recta $z=0$, tiene dos puntos: el punto $z=0$, $s=0$, que es singular, y el punto $z=0$, $s=1$, que no es singular, pues $\partial p/\partial s$ no se anula en él. Este punto no-singular define una valoración discreta v_1 de Σ_C que domina a $\mathcal{O}$. Un parámetro local es z; es decir, $v_1(z)=1$. Explotemos ahora el punto $z=s=0$:

$$\boxed{u = s/z}$$

$$\begin{aligned} 0 = p_2(z,zu) &= z^3 - z^3u^3 + z^4u^4 - z^5u^4 + z^6u^5 \\ &= z^3(1 - u^3 + zu^4 - z^2u^4 + z^3u^5) \\ 0 = p_3(z,u) &= 1 - u^3 + zu^4 - z^2u^4 + z^3u^5 \end{aligned}$$

La fibra del punto explotado, que es el corte de la curva $p_3(z,u)=0$ con la recta $z=0$, tiene tres puntos: el punto $z=0$, $u=1$, el punto $z=0$, $u=\omega$ y el punto $z=0$, $u=\omega^2$ (donde ω es una raíz cúbica primitiva de la unidad). Los tres son puntos no-singulares de la curva $p_3(z,u)=0$; luego definen tres valoraciones discretas v_2, v_3, v_4 de Σ_C que dominan a $\mathcal{O}$. La función z también es un parámetro local de estas valoraciones: $v_2(z)=v_3(z)=v_4(z)=1$.

Como ya todos los puntos obtenidos son no-singulares, v_1, v_2, v_3, v_4 son todas las valoraciones discretas de Σ_C con centro en el punto singular $x=0$, $y=0$. El diagrama o árbol de las explosiones realizadas es el siguiente (donde al lado de cada punto figura el grado de la forma inicial de la ecuación de la transformada):



Ahora, para calcular la multiplicidad de intersección en el punto $x=y=0$ de C con otra curva plana $f(x,y)=0$, sea irreducible o no, basta determinar $v_1(f)+v_2(f)+v_3(f)+v_4(f)$. A título de ejemplo, calculemos la multiplicidad de intersección en el origen de C con la curva $y^2=x^3$:

$$\begin{aligned} v_1(y^2-x^3) &= v_1(x^2z^2-x^3) = v_1(z^4s^2-z^3s^3) \\ &= v_1(z^3)+v_1(s^2)+v_1(z-s) = 3+0+0=3 \end{aligned}$$

porque $v_1(z)=1$ y las funciones s^2 y $z-s$ no se anulan en el punto $z=0$, $s=1$.

$$\begin{aligned} v_3(y^2-x^3) &= v_3(z^4s^2-z^3s^3) = v_3(z^6u^2-z^6u^3) \\ &= v_3(z^6)+v_3(u^2)+v_3(1-u) = 6+0+0=6 \end{aligned}$$

porque $v_3(z)=1$ y las funciones u^2 y $1-u$ no se anulan en el punto $z=0$, $u=\omega$. Análogamente $v_4(y^2-x^3)=6$. Por último,

$$v_2(y^2-x^3) = v_2(z^6)+v_2(u^2)+v_2(1-u) = 6+0+v_2(1-u)$$

y debemos calcular $v_2(1-u)$, lo que puede hacerse desarrollando $1-u$ en potencias de z (que es el procedimiento sistemático y general) o bien directamente:

$$\begin{aligned} v_2(1-u) &= v_2(-1+u^3) = v_2(zu^4-z^2u^4+z^3u^5) \\ &= v_2(z)+v_2(u^4-zu^4+z^2u^5) = 1+0=1 \end{aligned}$$

Luego $v_2(y^2-x^3)=7$ y concluimos que la multiplicidad de intersección en cuestión es precisamente $3+6+6+7=22$. No obstante, para calcular la multiplicidad de intersección en el origen de estas curvas $p(x,y)=0$, $y^2=x^3$ es más sencillo desingularizar la segunda, porque al explotar el origen

$$\boxed{t = y/x}$$

$$0 = y^2 - x^3 = x^2t^2 - x^3 = x^2(t^2 - x)$$
$$x = t^2$$

sobre el punto explotado aparece un único punto que ya es no-singular:

En el cuerpo de funciones racionales de la curva $y^2 = x^3$, que es $\mathbb{C}(t)$, sólo hay una valoración discreta v centrada en el punto $x = y = 0$. Un parámetro local de v es t; es decir, $v(t) = 1$. Ahora

$$v(y^7 - x^9y - x^{10}y + x^{11} + x^{12}) = v(t^{21} - t^{21} - t^{23} + t^{22} + t^{24}) = 22$$

porque $x = t^2$, $y = xt = t^3$.

Apéndice N

Teoría de Números

N.1 Tres Lemas Previos

Definición: Diremos que un subgrupo aditivo Γ de un espacio vectorial euclídeo E es una **red** si $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_d$ para alguna base $e_1, \ldots, e_d$ de E. En tal caso E/Γ es compacto y de volumen finito, $\mathrm{Vol}(E/\Gamma) < \infty$.

Lema N.1.1 *Sea $\Gamma \subset E$ una red y X un compacto de E. Si $\mathrm{Vol}(X) \geq \mathrm{Vol}(E/\Gamma)$, entonces existen dos puntos distintos $x, y \in X$ tales que $y - x \in \Gamma$.*

Demostración: Si la proyección natural $i\colon X \to E/\Gamma$ es inyectiva, entonces es un homeomorfismo con su imagen, y $i(X) \neq E/\Gamma$ porque la proyección $E \to E/\Gamma$ no admite secciones continuas: la imagen de tal sección sería abierta y cerrada en el espacio conexo E. Luego $\mathrm{Vol}(E/\Gamma - i(X)) > 0$, y $\mathrm{Vol}(X) < \mathrm{Vol}(E/\Gamma)$.

Teorema de Minkowski (1864-1909)**:** *Sea $\Gamma \subset E$ una red y X un compacto de E convexo y simétrico respecto del origen. Si $\mathrm{Vol}(X) \geq 2^d \mathrm{Vol}(E/\Gamma)$, entonces X contiene algún vector no nulo de la red Γ.*

Demostración: Como $\mathrm{Vol}(X/2) \geq \mathrm{Vol}(E/\Gamma)$, por N.1.1 existen $x, y \in X$ tales que $e = (y - x)/2 \in \Gamma$ no es nulo. Como X es convexo y simétrico, $e \in X$.

Lema N.1.2 *Todo subgrupo discreto Γ de un grupo de Lie conmutativo $G \times \mathbb{R}^d$, donde G es compacto, es de la forma $\Gamma \simeq U \times \mathbb{Z}^r$, donde U es un grupo finito y $r \leq d$. Además $r = d$ si y sólo si $G \times \mathbb{R}^d = X + \Gamma$ para algún compacto X (i.e., $(G \times \mathbb{R}^d)/\Gamma$ es compacto).*

Demostración: Γ es un subgrupo cerrado, pues si una sucesión $v_n \in \Gamma$ converge, $v_n \to v$, entonces $v_n - v_m \in \Gamma$ y $v_n - v_m \to v - v = 0 \in \Gamma$ y, al ser Γ discreto, se sigue que $v_n - v_m = 0$ cuando $n, m \gg 0$. Luego $v_n = v_m$ y por tanto $v \in \Gamma$.

Veamos primero el caso $G = 1$. Sustituyendo $\mathbb{R}^d$ por el subespacio vectorial que genera Γ, podemos suponer que Γ contiene una base una base de $\mathbb{R}^r$ y, aplicando un automorfismo lineal si fuera necesario, que $\mathbb{Z}^r \subseteq \Gamma$. Consideremos la proyección natural $\pi\colon \mathbb{R}^r \to \mathbb{R}^r/\mathbb{Z}^r = S_1^r$, que es una aplicación continua abierta. Ahora $\pi(\Gamma)$ es un subgrupo cerrado, porque lo es $\pi^{-1}(\pi(\Gamma)) = \Gamma + \mathbb{Z}^r = \Gamma$, y discreto. En efecto, si $v \in \Gamma$ y U es un abierto tal que $U \cap \Gamma = \{v\}$, entonces

$$\pi(\Gamma) \cap \pi(U) = \pi\pi^{-1}\big(\pi(\Gamma) \cap \pi(U)\big) = \pi\big(\Gamma \cap (v + \mathbb{Z}^r)\big) = \pi(v + \mathbb{Z}^r) = \pi(v)$$

y concluimos que $\pi(\Gamma) = \Gamma/\mathbb{Z}^r$ es cerrado y discreto en el compacto S_1^r. Luego es finito y obtenemos que Γ es un grupo finito-generado. Por el primer teorema de descomposición (apéndice D) tenemos que $\Gamma \simeq \mathbb{Z}^r$, pues $\mathbb{R}^r$ carece de torsión, así que $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r$.

En el caso general consideramos la segunda proyección $\pi\colon G \times \mathbb{R}^d \to \mathbb{R}^d$ y la correspondiente sucesión exacta

$$0 \longrightarrow \Gamma \cap G \longrightarrow \Gamma \longrightarrow \pi(\Gamma) \longrightarrow 0$$

El grupo $U := \Gamma \cap G$ es finito porque es un subgrupo discreto del grupo compacto G. Por otra parte, $\pi(\Gamma) = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r$ para ciertos vectores linealmente independientes $e_1, \ldots, e_r \in \mathbb{R}^d$, porque es un subgrupo discreto de $\mathbb{R}^d$. Ahora, como $\pi(\Gamma)$ es un grupo abeliano libre, la sucesión exacta escinde y $\Gamma \simeq U \times \mathbb{Z}^r$.

Por último, es obvio que $\mathbb{R}^d = X + \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r$ para algún compacto X precisamente cuando $r = d$.

Proposición N.1.3 *Sea X un compacto de una subvariedad diferenciable de codimensión r en un espacio vectorial real E dotado de un producto escalar. Si X_ε denota el abierto de puntos a distancia menor que ε de X, entonces existe una constante c tal que* $\mathrm{Vol}(X_\varepsilon) < c\varepsilon^r \;\;,\;\; \varepsilon \ll 1$.

Demostración: Recubriendo X con bolas podemos suponer que el borde de X es una subvariedad compacta de codimensión $r+1$. Si para un punto $x \in X_\varepsilon$ la distancia mínima se alcanza en un punto del interior de X, entonces x está en el entorno tubular N_ε de radio ε, porque la esfera centrada en x ha de ser tangente al interior de X. Si la distancia se alcanzase en el borde de X, entonces x está en $(\partial X)_\varepsilon$, cuyo volumen es un infinitésimo $O(\varepsilon^{r+1})$ por inducción sobre la dimensión, y no afecta. Basta ver que el volumen de N_ε es un infinitésimo $O(\varepsilon^r)$, y se concluye al integrar por Fubini (1879-1943) la forma de volumen en N_ε.

Lema N.1.4 *Sea U un abierto acotado de un espacio vectorial real E de dimensión d y sea $\Gamma \subset E$ una red. Si U está limitado por un número finito de hipersuperficies diferenciables, entonces el número $P(\lambda)$ de puntos de la red contenidos en λU es*

$$P(\lambda) = v\lambda^d + O(\lambda^{d-1}) \qquad , \qquad \lambda \gg 1$$

donde v es una constante no nula y $|O(\lambda^{d-1})| \leq a\lambda^{d-1}$ para cierta constante a.

Demostración: Podemos suponer que $E = \mathbb{R}^d$ y $\Gamma = \mathbb{Z}^d$. En tal caso $P(\lambda)$ es justamente el número de puntos de la red $\lambda^{-1}\Gamma$ en U. Asociando a cada uno de estos puntos el cubo de volumen λ^{-d} que en él determinan los vectores $(0, \ldots, \lambda^{-1}, \ldots 0)$, obtenemos una figura que casi coincide con U, aunque le falten algunos puntos de U y pueda tener algunos puntos fuera de U; pero tales puntos están a distancia menor que $\sqrt{d}/\lambda$ del borde X de U. Luego

$$\mathrm{Vol}(U) - \mathrm{Vol}(X_{\sqrt{d}/\lambda}) \leq P(\lambda)\lambda^{-d} \leq \mathrm{Vol}(U) + \mathrm{Vol}(X_{\sqrt{d}/\lambda})$$

y el lema anterior permite concluir.

N.2 Tres Teoremas Fundamentales

Sea K una extensión finita de $\mathbb{Q}$ de grado d y sea A el cierre entero de $\mathbb{Z}$ en K. Por el teorema de finitud, A es un dominio de Dedekind, y por M.2.1 tenemos

$$A = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_d$$

donde $a_1, \ldots, a_d$ es una base de K como $\mathbb{Q}$-espacio vectorial. Por tanto, A es una red en $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}a_1 \oplus \ldots \oplus \mathbb{R}a_d$, mediante el morfismo natural

$$\begin{array}{rcll} A & \longrightarrow & K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \oplus \mathbb{C}^s & , \qquad (r + 2s = d) \\ a & \mapsto & \big(\sigma_1(a), \ldots, \sigma_r(a), \sigma_{r+1}(a), \ldots, \sigma_{r+s}(a)\big) & \end{array}$$

donde $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}, \sigma_{r+s+1} = \bar{\sigma}_{r+1}, \ldots, \sigma_{r+2s} = \bar{\sigma}_{r+s}$ son todos los morfismos de $\mathbb{Q}$-álgebras $K \to \mathbb{C}$, y los r primeros son los que valoran en $\mathbb{R}$.

En $K_{\mathbb{R}}$ tenemos la métrica de la traza (ver sección I.2)

$$\begin{aligned} T_2\big((x_1, \ldots, x_r, z_1, \ldots, z_s), (y_1, \ldots, y_r, w_1, \ldots, w_s)\big) = \\ = \mathrm{tr}(x_1y_1, \ldots, x_ry_r, z_1w_1, \ldots, z_sw_s) = \\ = \textstyle\sum_i x_iy_i + \sum_j (z_jw_j + \bar{z}_j\bar{w}_j) \end{aligned}$$

que es no-singular (por cálculo directo o por I.2.2); luego tiene asociada una forma de volumen bien definida salvo un signo (en los factores complejos es el doble del área usual que define la base $\{1, i\}$). Si $a, b \in A$, tenemos que

$$T_2(a, b) = \mathrm{tr}(ab) = \sigma_1(a)\sigma_1(b) + \ldots + \sigma_d(a)\sigma_d(b)$$

Cuando se considera una métrica no-singular T_2, el cuadrado del volumen determinado por unos vectores $e_1, \ldots, e_d$ es el valor absoluto del determinante de la matriz $\big(T_2(e_i, e_j)\big)$. Luego el volumen de $K_{\mathbb{R}}/A$ es la raíz cuadrada del valor absoluto del determinante de la matriz $\big(T_2(a_i, a_j)\big) = (\sigma_i a_j)^t(\sigma_i a_j)$, Es decir, es la raíz cuadrada del valor absoluto del **discriminante** Δ_K de la extensión:

$$\mathrm{Vol}(K_{\mathbb{R}}/A) = \sqrt{|\Delta_K|} \qquad , \qquad \Delta_K := \det\big((\sigma_i a_j)^2\big)$$

Ejemplo N.2.1 Si α es una raíz compleja de un polinomio irreducible $q(x)$ con coeficientes racionales, tenemos que $K = \mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/\big(q(x)\big)$ es una extensión de $\mathbb{Q}$ de grado $d = \operatorname{gr} q(x)$ y los morfismos $\sigma_i\colon K \to \mathbb{C}$ se corresponden con las raíces complejas $\alpha_i = \sigma_i(\alpha)$ de $q(x)$. Si además $q(x) = x^d + c_1x^{d-1} + \ldots + c_d$ es un polinomio unitario con coeficientes enteros, entonces α es entero sobre $\mathbb{Z}$ y

$$\mathbb{Z}[x]/\big(q(x)\big) \simeq \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \ldots \oplus \mathbb{Z}\alpha^{d-1} \ \subseteq \ A \ .$$

Si se da la igualdad, entonces por 7.2.10 la fibra de la proyección natural $\operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z}$ sobre cada número primo p coincide con el espectro de

$$A/pA = \mathbb{F}_p[x]/\big(\bar{q}(x)\big) \ .$$

Es decir, los ideales maximales de A se corresponden con los factores irreducibles $\bar{q}_j(x)$ de las distintas reducciones $\bar{q}(x)$ módulo p. El ideal maximal de A correspondiente a un factor irreducible $\bar{q}_j(x)$ es $\mathfrak{m} = \big(p, q_j(x)\big)$ y el cuerpo residual $A/\mathfrak{m} \simeq \mathbb{F}_p[x]/\big(\bar{q}_j(x)\big)$ es el cuerpo finito con p^f elementos, donde $f = \operatorname{gr} \bar{q}_j(x)$. Además, el discriminante de K es

$$\Delta_K = \det\big((\sigma_i\alpha^{j-1})^2\big) = \det\big((\alpha_i^{j-1})^2\big) \ ,$$

y coincide (ver sección A.3) con el discriminante $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$ del polinomio $q(x)$. Por tanto la reducción $\bar{q}(x)$ módulo p es separable precisamente cuando el primo p no divide al discriminante Δ_K.

Si la inclusión $\mathbb{Z}[\alpha] \subset A$ es estricta, entonces $A/\mathbb{Z}[\alpha]$ es un grupo finito; luego es nulo al localizar en cualquier primo p que no divida a su orden, y

$$\mathbb{Z}_p[x]/\big(q(x)\big) \simeq \mathbb{Z}_p[\alpha] = \mathbb{Z}_p \oplus \mathbb{Z}_p\alpha \oplus \ldots \oplus \mathbb{Z}_p\alpha^{d-1} \ = \ A_p \ .$$

Por tanto, la correspondencia entre maximales de A que contienen a p y factores irreducibles de la reducción $\bar{q}(x)$ módulo p es válida para casi todo número primo p. Además tendremos $\alpha^{j-1} = \sum_k c_{kj}a_k$ para cierta matriz (c_{kj}) con coeficientes enteros. Luego $\alpha_i^{j-1} = \sum_k c_{kj}\sigma_i(a_k)$ y, tomando determinantes, vemos que el discriminante Δ del polinomio $q(x)$ es $\Delta = c^2\Delta_K$, donde $c = \det(c_{ij}) \in \mathbb{Z}$. En este caso la reducción $\bar{q}(x)$ no es separable en los primos que dividen al discriminante Δ_K y, eventualmente el algún primo adicional (los factores primos de c).

En general, cuando $q(x)$ es un polinomio unitario con coeficientes racionales, todas las afirmaciones anteriores son ciertas después de localizar por el sistema multiplicativo $S = \{p_1^{n_1} \ldots p_r^{n_r}\}$, donde $p_1, \ldots, p_r$ son los números primos que dividen a algún denominador de los coeficientes de $q(x)$. Luego son ciertas en casi todos los números primos.

Definición: Se llama **norma** de un ideal no nulo $\mathfrak{a} \subset A$ al cardinal $[A : \mathfrak{a}]$ del anillo cociente $A/\mathfrak{a}$, que es finito y se denota $N(\mathfrak{a})$.

Todo ideal no nulo $\mathfrak{a}$ de A también es una red en $K_\mathbb{R}$, y como la proyección natural $K_\mathbb{R}/\mathfrak{a} \to K_\mathbb{R}/A$ es un revestimiento no ramificado de grado igual al cardinal de $A/\mathfrak{a}$, tenemos que

$$\mathrm{Vol}(K_\mathbb{R}/\mathfrak{a}) \;=\; N(\mathfrak{a})\mathrm{Vol}(K_\mathbb{R}/A)$$

En el caso de los ideales principales $\mathfrak{a} = aA$, tenemos que $N(aA)$ coincide con el determinante del endomorfismo $h_a(x) = ax$, que es precisamente la norma $N(a) = \prod_i \sigma_i(a)$ del elemento $a \in K$ (ver sección I.2). Si $\mathfrak{m}$ es un ideal maximal de A, tenemos que $\mathfrak{m}^n/\mathfrak{m}^{n+1} \simeq A/\mathfrak{m}$, porque $\mathfrak{m}$ es localmente principal; luego

$$N(\mathfrak{m}_1^{n_1} \ldots \mathfrak{m}_r^{n_r}) \;=\; q_1^{n_1} \ldots q_r^{n_r} \qquad , \qquad q_i = N(\mathfrak{m}_i)$$

y por tanto la norma es multiplicativa: $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Lema Fundamental: *En todo ideal no nulo $\mathfrak{a} \subset A$ hay algún elemento no nulo $a \in \mathfrak{a}$ tal que* $N(a) \leq \sqrt{|\Delta_K|}N(\mathfrak{a})$.

Demostración: Todos los elementos de $\mathfrak{a}$ que estén en el convexo simétrico

$$\{|x_1| \leq c_1\} \times \ldots \times \{|x_r| \leq c_r\} \times \{|z_1| \leq c_{r+1}\} \times \ldots \times \{|z_s| \leq c_{r+s}\}$$

tienen norma $\leq c := c_1 \ldots c_r c_{r+1}^2 \ldots c_{r+s}^2$. Como el volumen de tal convexo es $2^{r+s}\pi^s c \geq 2^d c$, el teorema de Minkowski permite concluir la existencia en la red $\mathfrak{a}$ de un elemento no nulo de norma $\leq c$ siempre que

$$2^d c \;\geq\; 2^d \mathrm{Vol}(K_\mathbb{R}/\mathfrak{a}) \;=\; 2^d N(\mathfrak{a})\mathrm{Vol}(K_\mathbb{R}/A) \;=\; 2^d N(\mathfrak{a})\sqrt{|\Delta_K|}$$

Definición: El grupo $\mathrm{Div}(A)$ de los **divisores** de A es el grupo abeliano libre generado por los puntos cerrados de $\mathrm{Spec}(A)$; i.e., por los ideales maximales de A. Cada función racional no nula $f \in K$ define un divisor, llamado **principal**

$$D(f) := \textstyle\sum_x v_x(f) \cdot x$$

y el cociente del grupo de divisores por el subgrupo de divisores principales se denotará $\mathrm{Pic}(A)$ y se llamará grupo de **clases de ideales** de A o grupo de Picard (1856-1941) de A.

Los ideales $\mathfrak{m}_{x_1}^{n_1} \ldots \mathfrak{m}_{x_r}^{n_r}$ pueden verse como los divisores $D = n_1x_1 + \ldots + n_rx_r$ efectivos (en el sentido de que los coeficientes n_i son positivos), y es claro que todo divisor es equivalente a algún divisor efectivo. Además, la norma puede extenderse a los divisores arbitrarios sin más que poner

$$N(n_1x_1 + \ldots + n_rx_r) \;=\; N(x_1)^{n_1} \cdot \ldots \cdot N(x_r)^{n_r}$$

Teorema N.2.2 *El grupo* $\mathrm{Pic}(A)$ *de clases de ideales es finito.*

Demostración: El número de ideales de A de norma dada n es finito, porque han de ser ideales del anillo finito A/nA, así que basta ver que en cada clase de divisores hay un representante $D = \sum_i n_i x_i$ efectivo de norma $\leq \sqrt{|\Delta_K|}$.

Ahora bien, dado un ideal $\mathfrak{a}$ de A (i.e., un divisor efectivo D), el lema fundamental afirma la existencia de un elemento no nulo $\alpha \in \mathfrak{a}$ (i.e., el divisor $D(\alpha) - D$ es efectivo) tal que $N(D(\alpha) - D) \leq \sqrt{|\Delta_K|}$. Luego la clase $[-D]$ tiene un representante efectivo de norma $\leq \sqrt{|\Delta_K|}$.

Toda clase está representada por un divisor efectivo, luego también por el opuesto de un divisor efectivo, lo que permite concluir.

Teorema N.2.3 (Hermite 1822-1901) *Sólo hay un número finito de extensiones de $\mathbb{Q}$ de grado y discriminante dados.*

Demostración: Sea K una extensión de discriminante Δ y grado d. Si $r \neq 0$, el volumen del convexo simétrico

$$|x_1| \leq 2^d \sqrt{|\Delta|}\ ,\ |x_i| \leq 1/2\ ,\ |z_j| \leq 1/2$$

(donde $2 \leq i \leq r$, $1 \leq j \leq s$) es $\geq 2^d\sqrt{|\Delta|}$. Por el teorema de Minkowski existe $\alpha \in A$ tal que $|\sigma_i(\alpha)| < 1/2$ cuando $i \neq 1$. Como $N(\alpha)$ es entero, $2 < |\sigma_1(\alpha)|$ y obtenemos que $\sigma_i(\alpha) \neq \sigma_1(\alpha)$ cuando $i \neq 1$. Luego $K = \mathbb{Q}(\alpha)$.

Además, los coeficientes del polinomio irreducible de α sobre $\mathbb{Q}$ están acotados porque lo está el módulo de los números complejos $\sigma_i(\alpha)$, y al ser números enteros concluimos que sólo hay un número finito de tales polinomios.

El caso $r = 0$ se trata de modo similar, sin más que considerar el convexo simétrico $\mathrm{Im}(z_1) < 2^d\sqrt{|\Delta|}$, $\mathrm{Re}(z_1) < 1/2$, $|z_i| < 1/2$, $i = 2, \ldots, s$, que tiene volumen $\geq 2^d\sqrt{|\Delta|}$.

Nota: Considerando los convexos simétricos $\sum_i |x_i| + \sum_j |z_j| \leq t$, que tienen volumen $2^r\pi^s t^d/d!$, el teorema de Minkowski y la acotación de la media geométrica por la media aritmética muestran que en cada ideal no nulo $\mathfrak{a}$ existe un elemento no nulo $a \in \mathfrak{a}$ de norma $N(a) \leq cN(\mathfrak{a})$, donde $c = d!d^{-d}(4/\pi)^s\sqrt{|\Delta_K|}$. Como c ha de ser ≥ 1, se sigue que, fijado el discriminante Δ de la extensión, el grado d está acotado, por lo que realmente sólo hay un número finito de extensiones finitas de $\mathbb{Q}$ de discriminante dado. Esta acotación también permite obtener el teorema de Minkowski: $\Delta_K \neq \pm 1$ *para toda extensión finita K no trivial de* $\mathbb{Q}$. Es decir, todo polinomio unitario $q(x)$ con coeficientes enteros tiene reducción $\bar{q}(x)$ inseparable en algún primo.

Teorema N.2.4 *El grupo A^* de elementos invertibles en A es un grupo abeliano finito-generado de rango $r + s - 1$ (su torsión es obviamente el grupo μ_K de las raíces de la unidad contenidas en K):*

$$A^* \simeq \mu_K \oplus \mathbb{Z}^{r+s-1}$$

Demostración: Sea $U(1) \subset \mathbb{C}^*$ el grupo de los números complejos de módulo 1. Vía la inmersión $A \to K_{\mathbb{R}}$, tenemos que A^* es un subgrupo discreto del grupo

$$(K_{\mathbb{R}})^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s = G \times (\mathbb{R}_+)^{r+s}$$

donde G es el grupo de Lie (1842-1899) compacto $G = (\mathbb{Z}/2\mathbb{Z})^r \times U(1)^s$, y el isomorfismo $\mathbb{C}^* = U(1) \times \mathbb{R}_+$ transforma z en $(z/|z|, z\bar{z})$.

Como la norma $N\colon (\mathbb{R}_+)^{r+s} \to \mathbb{R}_+$, $N(x_i) := \prod_i x_i$ tiene la sección obvia $t \mapsto (t^{1/n}, \ldots, t^{1/n})$, $n = r + s$, tenemos que

$$(K_{\mathbb{R}})^* = G \times H \times (\mathbb{R}_+) \quad , \quad H := \{(x_i)\colon\ x_1 \ldots x_{r+s} = 1\} \simeq (\mathbb{R}_+)^{r+s-1}$$

Las unidades de A tienen norma ± 1, así que A^* es un subgrupo discreto del grupo $G \times H \simeq G \times \mathbb{R}^{r+s-1}$ de elementos de norma ± 1. El lema N.1.2 permite concluir que es un grupo finito-generado de rango $\leq r + s - 1$. Para ver que se da la igualdad basta probar la existencia de un compacto X tal que los compactos uX recubran $G \times H$ cuando $u \in A^*$. Consideremos un cubo

$$Q := \{(x_1, \ldots, x_r, z_1, \ldots, z_s)\colon\ |x_i| \leq a_i,\ |z_j| \leq b_j\}$$

cuyo volumen supere $2^d\sqrt{|\Delta_K|}$. Si $y \in G \times H$, entonces $N(y) = \pm 1$ y el volumen del cubo yQ coincide con el de Q. Por el teorema de Minkowski existe algún elemento no nulo $\alpha \in A \cap yQ$, y tendremos $|N(\alpha)| \leq a_1 \ldots a_r b_1^2 \ldots b_s^2 |N(y)| = c$, donde $c := a_1 \ldots a_r b_1^2 \ldots b_s^2$.

Ahora bien, salvo unidades sólo hay un número finito de elementos de A de norma $\leq c$, porque sólo hay un número finito de ideales de norma $\leq c$. Eligiendo generadores $\alpha_1, \ldots, \alpha_n$ de los ideales principales de norma $\leq c$, tendremos $\alpha = u\alpha_i$ para alguna unidad $u \in A^*$; luego $u\alpha_i \in yQ$. Es decir, $y^{-1} \in u^{-1}(\alpha_i^{-1}Q)$ y concluimos que el compacto $X := \alpha_1^{-1}Q \cup \ldots \cup \alpha_n^{-1}Q$ tiene la propiedad requerida: $G \times H \subset \bigcup uX$, donde $u \in A^*$.

Proposición N.2.5 *Sea $S(n)$ el número de ideales de A de norma $\leq n$. Existe una constante no nula v tal que $S(n) = vn + O(n^{1-1/d})$.*

Demostración: En virtud de la finitud del grupo de clases de ideales, basta probar el enunciado para el número $S(n)$ de ideales de norma $\leq n$ en una clase dada C. Fijado un ideal $\mathfrak{a}$ en la clase inversa, tales ideales son $\alpha\mathfrak{a}^{-1}$ donde $\alpha \in \mathfrak{a}$ tiene norma $N(\alpha) \leq nN(\mathfrak{a})$. Es decir, es el número de elementos de norma $\leq nN(\mathfrak{a})$, salvo unidades, en cierto ideal dado $\mathfrak{a}$.

Fijado un paralelogramo fundamental P de la red que A^* define en H, salvo unidades cada elemento de A tiene exactamente w representantes en $G \times P \times \mathbb{R}_+$. donde w es el número de raíces de la unidad en K, que es finito. Luego $wS(n)$ es el número de elementos de la red $\mathfrak{a}$ en el conjunto

$$U_n := G \times P \times (0, nN(\mathfrak{a})]$$

Este conjunto está acotado en $K_{\mathbb{R}}$ porque está contenido en el transformado de un compacto (P está en un compacto de H) por todas las homotecias de razón entre 0 y $nN(\mathfrak{a})$. Como $U_n = n^{1/d}U_1$, se concluye al aplicar el lema N.1.4.

N.3 La Función Zeta

Teorema N.3.1 *La serie $\sum_n n^{-s}$ converge uniformemente en los compactos de la semirrecta $s > 1$, y define una función continua $\zeta(s)$ en $(1, \infty)$ tal que*

$$1 = \lim_{s\to 1}(s-1)\zeta(s) \qquad , \qquad \zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Demostración: Es una serie de términos positivos y tenemos

$$\frac{1}{s-1} = \int_1^\infty \frac{\mathrm{d}t}{t^s} < \sum_{n\geq 1} \frac{1}{n^s} < 1 + \int_1^\infty \frac{\mathrm{d}t}{t^s} = 1 + \frac{1}{s-1}$$

Por último, la igualdad $\sum_n n^{-s} = \prod_p (1 + p^{-s} + p^{-2s} + \ldots) = \prod_p (1 - p^{-s})^{-1}$ expresa la unicidad de la descomposición de n en producto de números primos.

Corolario N.3.2 *Sea $f \geq 2$ un número natural y P cualquier conjunto de números primos. El producto $\prod_{p\in P}(1 - (p^f)^{-s})^{-1}$ define una función continua en la semirrecta $s > 1/f$.*

Demostración: La serie $\zeta(fs) = \sum_n (n^f)^{-s}$ define una función continua en la semirrecta $s > 1/f$, y la serie formada por los términos correspondientes a números con todos sus factores primos en P coincide con el producto considerado.

Definición: Si K es una extensión finita de $\mathbb{Q}$, su **función zeta** (de Riemann 1826-1866) es

$$\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

donde $\mathfrak{a}$ recorre todos los ideales no nulos del cierre entero A de $\mathbb{Z}$ en K.

Lema N.3.3 *Sea (a_n) una sucesión de números reales y sea $b_n := a_1 + \ldots + a_n$. Si $b_n = O(n^\varepsilon)$, entonces la serie $\sum_n a_n/n^s$ converge uniformemente en los compactos de la semirrecta $s > \varepsilon$.*

Demostración: Por hipótesis existe una constante c tal que $|b_n| \le cn^\varepsilon$. Ahora, para cada pareja $m < r$ de números naturales tenemos

$$\sum_{n=m}^{r} \frac{b_n - b_{n-1}}{n^s} = \frac{b_r}{r^s} - \frac{b_{m-1}}{m^s} + \sum_{n=m}^{r-1} b_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$$

$$\left| b_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| \le cn^\varepsilon s \int_n^{n+1} \frac{\mathrm{d}t}{t^{s+1}} \le cs \int_n^{n+1} \frac{\mathrm{d}t}{t^{s+1-\varepsilon}}$$

$$\left| \sum_{n=m}^{r} \frac{a_n}{n^s} \right| \le \frac{2c}{m^{s-\varepsilon}} + cs \int_m^\infty \frac{\mathrm{d}t}{t^{s+1-\varepsilon}} = \left(2c + \frac{cs}{s-\varepsilon} \right) \frac{1}{m^{s-\varepsilon}}$$

Notación: Dadas dos funciones continuas $f(s)$ y $g(s)$ en la semirrecta $s > 1$, pondremos $f(s) \sim g(s)$ cuando $g(s) = u(s)f(s)$ para alguna función continua $u(s)$ en un entorno del punto $s = 1$ que no se anule en el mismo.

Definición: Llamaremos **grado** de un ideal primo $\mathfrak{p}$ de A al grado de $A/\mathfrak{p}$ sobre $\mathbb{F}_p$ y lo denotaremos $\operatorname{gr}\mathfrak{p}$. Es decir, $N(\mathfrak{p}) = p^f$ cuando $\mathfrak{p}$ es un ideal primo de grado f que está en la fibra del número primo p.

De acuerdo con el ejemplo N.2.1, si $q(x)$ es un polinomio unitario e irreducible con coeficientes enteros, los primos de grado 1 de $\mathbb{Z}[x]/\big(q(x)\big)$ en la fibra de p se corresponden con los factores de grado 1 de la reducción $\bar{q}(x)$ módulo p.

Teorema N.3.4 *$\zeta_K(s)$ es una función continua en la semirrecta $s > 1$ y*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = v \neq 0, \infty$$

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s} \right)^{-1} \sim \prod_{\operatorname{gr}\mathfrak{p}=1} \left(1 - \frac{1}{p^s} \right)^{-1}$$

Demostración: De acuerdo con la proposición N.2.5 el número de ideales de norma n es $v + a_n$, donde $v > 0$ y $s_n := a_1 + \ldots + a_n = O(n^{1-\frac{1}{d}})$. El lema anterior permite concluir que

$$\zeta_K(s) = v\zeta(s) + \sum_n \frac{a_n}{n^s} = v\zeta(s) + h(s)$$

donde $h(s)$ es una función continua en $s > 1 - \frac{1}{d}$. Luego $\zeta_K(s)$ es una función continua en $s > 1$ y

$$\lim_{s\to 1}(s-1)\zeta_K(s) = v \lim_{s\to 1}(s-1)\zeta(s) = v.$$

La igualdad $\sum N(\mathfrak{a})^{-s} = \prod (1 - N(\mathfrak{p})^{-s})^{-1}$ expresa la unicidad de la descomposición de cada ideal de A en producto de ideales primos.

Por último, los ideales primos de grado $f \ge 2$ definen un número finito de factores de la forma $\prod_{p\in P}(1-(p^f)^{-s})^{-1}$ para ciertas familias P de números primos, factores que definen funciones continuas en la semirrecta $s > 1/f$ según N.3.2.

Corolario N.3.5 *Toda extensión finita de $\mathbb{Q}$ tiene infinitos primos de grado 1. Todo polinomio con coeficientes racionales tiene infinitas raíces modulares.*

Demostración: Si una extensión finita K sólo tuviera un número finito de primos de grado 1, entonces

$$\lim_{s\to 1}\zeta_K(s) = \lim_{s\to 1}\prod_{\mathrm{gr}\,\mathfrak{p}=1}\left(1-\frac{1}{p^s}\right)^{-1} < \infty$$

y $\lim_{s\to 1}(s-1)\zeta_K(s) = 0$, en contra del teorema anterior.

Ahora, si un polinomio con coeficientes racionales $q(x)$ es irreducible, tenemos que $K = \mathbb{Q}[x]/(q(x))$ tiene infinitos primos de grado 1, y N.2.1 permite concluir que hay infinitos números primos p tales que la reducción $\bar{q}(x)$ módulo p tiene algún factor de grado 1 (i.e., alguna raíz en $\mathbb{F}_p$).

Corolario N.3.6 *Si $q(x) \in \mathbb{Q}[x]$ no es constante, existen infinitos números primos p tales que la reducción $\bar{q}(x)$ módulo p descompone en factores de grado 1 (i.e., el grupo de Galois de $\bar{q}(x)$ sobre $\mathbb{F}_p$ es trivial.).*

Demostración: Sea $L = \mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ el cuerpo de descomposición de $q(x)$ sobre $\mathbb{Q}$ y sea A el cierre entero de $\mathbb{Z}$ en L. Cuando $q(x)$ es unitario y tiene coeficientes enteros, tenemos que $\mathbb{Z}[\alpha_1,\ldots,\alpha_n] \subseteq A$ y el teorema de finitud del cierre entero muestra que las fibras de estos dos anillos coinciden en casi todos los números primos. Como A tiene infinitos primos de grado 1 de acuerdo con el corolario anterior, se sigue que lo mismo es cierto en $\mathbb{Z}[\alpha_1,\ldots,\alpha_n]$, y la demostración del teorema de reducción permite concluir que el grupo de Galois de la reducción $\bar{q}(x)$ es trivial en tales primos.

El caso de un polinomio arbitrario $q(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ con coeficientes enteros se reduce fácilmente al del polinomio unitario

$$c_0^{n-1}q(x) = c_0^nx^n + c_1c_0^{n-1}x^{n-1} + \ldots + c_nc_0^{n-1} = y^n + c_1y^{n-1} + \ldots + c_nc_0^{n-1}$$

donde $y = c_0x$, o bien se sustituye $\mathbb{Z}$ por su localización por las potencias de c_0.

Corolario N.3.7 *Para cada número natural n existen infinitos números primos congruentes con 1 módulo n.*

Demostración: De acuerdo con el ejemplo (3) de la página 389, el automorfismo de Frobënius F_p del polinomio $x^n - 1$ en un primo p que no sea divisor de n se identifica con la clase de p en $(\mathbb{Z}/n\mathbb{Z})^*$.

Corolario N.3.8 *Sea $K \to L$ una extensión finita. Si casi todos los primos de grado 1 de K descomponen totalmente en L, entonces $K = L$.*

La condición necesaria y suficiente para que un polinomio $q(x) \in \mathbb{Q}[x]$ tenga todas sus raíces racionales es que para casi todo número primo p la reducción $\bar{q}(x)$ módulo p tenga todas sus raíces en $\mathbb{F}_p$.

Es decir, el grupo de Galois de $q(x)$ sobre $\mathbb{Q}$ es trivial si y sólo si la reducción $\bar{q}(x)$ tiene grupo de Galois trivial para casi todo primo p.

Sea $d = [L : K]$. Por hipótesis la fibra de casi todos los primos de grado 1 de K está formada por d primos de L, que necesariamente han de tener grado 1. Además cada primo de L de grado 1 está sobre un primo de K de grado 1; luego $\zeta_L(s) \sim \zeta_K(s)^d$, y si $d > 1$ se obtiene la contradicción

$$\lim_{s\to 1}(s-1)\zeta_L(s) = \lim_{s\to 1}(s-1)\zeta_K(s)^d = \infty \ .$$

Por último, si $q(x) \in \mathbb{Q}[x]$ es irreducible y la reducción $\bar{q}(x)$ descompone en producto de factores de grado 1 para casi todo primo p, de N.2.1 se sigue que casi todos los números primos descomponen totalmente en la extensión $L = \mathbb{Q}[x]/(q(x))$. Luego $L = \mathbb{Q}$ y concluimos que $q(x)$ es de grado 1.

Corolario N.3.9 *Sean $K \to L$ y $K \to L'$ extensiones de Galois. Si casi todos los primos de grado 1 de K que descomponen totalmente en L también descomponen totalmente en L', entonces $L' \subseteq L$. En particular, si los primos de grado 1 de K que descomponen totalmente en L y en L' son los mismos, salvo un número finito, entonces $L = L'$; i.e., cada extensión de Galois $K \to L$ está determinada por el conjunto de primos de grado 1 de K que descomponen totalmente en L.*

Cada extensión de Galois $K \to L$ está determinada por el conjunto de primos de K que descomponen totalmente en L.

Demostración: Salvo en la ramificación, la condición de que un primo de grado 1 descomponga totalmente en una extensión finita dada significa que todos los puntos de su fibra también son de grado 1, lo que equivale a decir que el número de puntos de la fibra iguala al grado de la extensión. En el caso de las extensiones de Galois, tal condición equivale a que la isotropía de cualquier punto de la fibra sea trivial, porque el grupo de Galois actúa transitivamente en las fibras.

En virtud de corolario anterior, basta probar que casi todo primo $\mathfrak{p}$ de grado 1 de L descompone totalmente en LL'; es decir que es trivial la isotropía de cualquier primo $\mathfrak{q}$ de su fibra. Sea $\sigma \in \mathrm{Aut}(LL'/L)$ tal que $\sigma\mathfrak{q} = \mathfrak{q}$. Si $\mathfrak{p}' := L' \cap \mathfrak{q}$, entonces $\mathfrak{p}'$ es de grado 1 por hipótesis; luego σ es la identidad sobre L', ya que la isotropía de $\mathfrak{p}'$ bajo la acción del grupo de Galois de L' es trivial, y concluimos que σ es la identidad sobre LL'.

Corolario N.3.10 *Si $q(x), r(x) \in \mathbb{Q}[x]$, la condición necesaria y suficiente para que todas las raíces de $q(x)$ sean expresiones racionales de las raíces de $r(x)$ es que la reducción $\bar{q}(x)$ descomponga en factores de grado 1 en casi todos los números primos en que $\bar{r}(x)$ descompone en factores de grado 1.*

Estos pocos resultados, junto con las consecuencias del teorema de reducción que en su momento vimos, son indicio de lo que, desde la introducción por Gauss (1777–1855) de las congruencias, es cada vez más patente: *que muchos problemas esenciales de la Aritmética, adecuadamente entendidos, se reducen al estudio de la Aritmética módulo p.* Además, también señalan que el sueño de Kronecker (1823–1891), la unificación de la Aritmética y la Geometría, es mucho más que una analogía o unificación de métodos, *que el comportamiento de las soluciones modulares de un sistema de ecuaciones diofánticas está íntimamente relacionado con la geometría de sus soluciones complejas.* Vaya pues como broche final de este libro una generalización de N.3.5 que, entre otros temas y con motivo de su doctorado *honoris causa* por la Universidad Complutense, expuso Jean Pierre Serre (n. 1927) en Madrid el 28 de abril del 2006:

La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas $q_1(x_1,\ldots,x_n)=0,\ldots,q_r(x_1,\ldots,x_n)=0$ *tenga alguna solución compleja es que admita soluciones modulares en infinitos números primos.*

En efecto, si el sistema no tiene soluciones complejas, el teorema de los ceros de Hilbert afirma que el anillo

$$\mathbb{C}[x_1,\ldots,x_n]/(q_1,\ldots,q_r) \;=\; \mathbb{Q}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)\otimes_{\mathbb{Q}}\mathbb{C}$$

carece de ideales maximales. Luego $\mathbb{C}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=0$ de acuerdo con 6.1.3, así que $\mathbb{Q}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)=0$ y existen polinomios $h_1,\ldots,h_r\in\mathbb{Q}[x_1,\ldots,x_n]$ tales que

$$h_1q_1+\ldots+h_rq_r=1\ .$$

Ahora es evidente que, salvo en los primos que dividan a algún denominador de los coeficientes de tales polinomios h_i, la reducción $\bar{q}_1=\ldots=\bar{q}_r=0$ módulo p del sistema dado carece de soluciones en $\mathbb{F}_p$.

Recíprocamente, si el sistema considerado tiene alguna solución compleja, entonces $\mathbb{C}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)\neq 0$; luego $\mathbb{Q}[x_1,\ldots,x_n]/(q_1,\ldots,q_r)\neq 0$ y el teorema de los ceros de Hilbert afirma que el sistema admite solución en alguna extensión finita L de $\mathbb{Q}$. Sea A el cierre entero de $\mathbb{Z}$ en L. Como $L=A\otimes_{\mathbb{Z}}\mathbb{Q}$, tal solución será

$$x_1=\frac{\alpha_1}{d_1}\ ,\ \ldots\ ,\ x_n=\frac{\alpha_n}{d_n}$$

donde $\alpha_1,\ldots,\alpha_n\in A$ y $d_1,\ldots,d_n\in\mathbb{Z}$.

Ahora bien, cada primo de A de grado 1 define un morfismo de anillos $A\to\mathbb{F}_p$, y por tanto una solución del sistema en $\mathbb{F}_p$ siempre que ningún denominador d_i sea múltiplo del primo p. Como N.3.5 afirma precisamente la existencia de infinitos primos de grado 1 en A, se concluye la existencia de infinitos números primos p tales que el sistema considerado tiene solución en $\mathbb{F}_p$.

Bibliografía

[1] M. Atiyah, I. G. Macdonald: *Introducción al Álgebra Conmutativa*, Ed. Reverté, Barcelona (1973).

[2] N. Bourbaki: *Algèbre Commutative*, Ed. Hermann, Paris (1961).

[3] A. Chambert–Loir: *A Field Guide to Algebra*, Undergraduate Texts in Mathematics, Springer (2005).

[4] A. Clark: *Elementos de Álgebra abstracta*, Ed. Alhambra, Madrid (1974).

[5] D. Eisenbud: *Commutative Algebra*, Graduate Texts in Math. **150**, Springer-Verlag, NuevaYork (1995).

[6] J. P. Lafon: *Algèbre Commutative*, Enseignement des Sciences **24**. Ed. Hermann, Paris 1998).

[7] M. Reid: *Undergraduate Commutative Algebra*, London Math. Soc. Student Texts **29**, Cambridge Univ. Press., Cambridge (1995).

[8] R. Y. Sharp: *Steps in Commutative Algebra* 2ª ed., London Math. Soc. Student Texts **51**, Cambridge Univ. Press., Cambridge (2001).

Índice de Materias