Álgebra Conmutativa

Grado en Matemáticas

Segunda Edición

Colección manuales uex - 111

Pedro
Sancho de Salas

111

ÁLGEBRA CONMUTATIVA

GRADO EN MATEMÁTICAS

Segunda Edición

MANUALES UEX

111

PEDRO SANCHO DE SALAS

ÁLGEBRA CONMUTATIVA

GRADO EN MATEMÁTICAS

Segunda Edición

UNIVERSIDAD DE EXTREMADURA

2024

Edita

Universidad de Extremadura. Servicio de Publicaciones
C./ Caldereros, 2 - Planta 2ª - 10071 Cáceres (España)
Telf. 927 257 041 - Fax 927 257 046
publicac@unex.es
www.unex.es/ publicaciones

ISSN XXX
ISBN de méritos XXX

Índice general

Introducción

El presente manual está concebido por el autor como el manual de la asignatura cuatrimestral Álgebra Conmutativa, del segundo curso del Grado en Matemáticas de la UEX. Introducimos estructuras básicas del Álgebra como las de grupo, anillo y módulo, herramientas fundamentales como el cociente de un grupo por un subgrupo, cociente de un anillo por un ideal, cociente de un módulo por un submódulo y la localización de un anillo o un módulo por un sistema multiplicativo. Estudiamos los dominios de factorización única, cuyos ejemplos fundamentales son el anillo de los números enteros y los anillos de polinomios. Introducimos la teoría del exceso para la separación de las raíces reales y complejas de los polinomios con coeficientes complejos. Clasificamos los módulos sobre dominios de ideales principales y en particular obtenemos la clasificación de los grupos abelianos y la clasificación de los endomorfismos de un espacio vectorial.

El manual está divido en cinco temas. En cada tema incluimos un cuestionario, una lista de problemas (con sus soluciones) y la biografía de un matemático relevante (en inglés).

Comentemos algunos de los conceptos y contenidos fundamentales del curso.

Los inicios de la filosofía griega (los presocráticos) fueron también los inicios de la matemática griega (los pitagóricos). El descubrimiento de que en el conjunto de los números naturales destacaban los números primos y de que todo número era producto de números primos de modo único, la observación de que las notas musicales dependían de las proporciones enteras de las longitudes de las cuerdas musicales, etc, se vivió como la aparición de un nuevo mundo independiente de toda contingencia que regía y explicaba el mundo real. En la escuela aprendimos la aritmética elemental de $\mathbb{Z}$. Si elevamos un poco la vista observaremos que en $\mathbb{Z}$ es fundamental la existencia de dos operaciones + y $\cdot$, la existencia de elementos primos (o irreducibles) y que esta estructura es igualmente existente en otros anillos (por ejemplo, en los anillos de polinomios). En el curso hablaremos de los anillos y fundamentalmente de los anillos euclídeos. Probaremos que en los anillos euclídeos ($\mathbb{Z}$, $k[x]$, el anillo de los enteros de Gauss, etc.) todo elemento se escribe de modo único como producto de irreducibles (salvo multiplicación por invertibles y orden). La propiedad aritmética fundamental de los anillos euclídeos es que sus ideales son principales, es decir, generados por un elemento (el de "grado" mínimo). Del mismo modo que en anillos euclídeos, probamos que si A es un dominio de ideales principales entonces todo elemento $a \in A$ (no nulo ni invertible) se escribe de modo único como producto de irreducibles (salvo multiplicación por invertibles y orden),

$$a = p_1 \cdots p_n, \quad (p_i \text{ irreducibles}).$$

Veremos que

$$a \cdot A + b \cdot A = m.c.d.(a,b) \cdot A$$
$$a \cdot A \cap b \cdot A = m.c.m.(a,b) \cdot A$$

Mediante el algoritmo de Euclides, calcularemos $\lambda, \mu \in A$, tales que

$$\lambda \cdot a + \mu \cdot b = m.c.d.(a,b).$$

Esta igualdad, "identidad de Bezout", tendrá múltiples aplicaciones tanto en Álgebra como para la resolución de ciertas ecuaciones diferenciales y ecuaciones en diferencias finitas.

Consideremos ahora el anillo de polinomios en una variable con coeficientes complejos. Probaremos el teorema fundamental del Álgebra, que nos dice que para todo polinomio $p(x) \in \mathbb{C}[x]$ existen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ de modo que

$$p(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

O dicho de otro modo, salvo multiplicación por $c \in \mathbb{C}$ no nulo, los polinomios irreducibles de $\mathbb{C}[x]$ son los polinomios $x - \alpha$. Con mayor generalidad, el teorema de Kronecker nos dice que dado $p(x) \in k[x]$ existe un cuerpo mayor $k \hookrightarrow K$ y $\alpha_1, \ldots, \alpha_n \in K$ de modo que $p(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$. La teoría del exceso nos permitirá calcular las raíces de los polinomios con coeficientes reales, o más generalmente con coeficientes complejos.

Un concepto fundamental en Matemáticas es el concepto de equivalencia y es fundamental también el proceso de identificar las cosas que consideramos equivalentes. Un concepto y herramienta fundamental en el curso va a ser el concepto de cociente. Pongamos un par de ejemplos.

Si en $\mathbb{Z}$ considero equivalentes dos números cuando difieran en un múltiplo de 9 e igualo entre sí los números que considero equivalentes obtengo un nuevo conjunto de "números" que denotamos por $\mathbb{Z}/9\mathbb{Z}$, que por definición es el conjunto

$$\mathbb{Z}/9\mathbb{Z} := \{\bar{n}, \forall\, n \in \mathbb{Z} \colon \bar{n} = \bar{m} \iff n - m \in 9\mathbb{Z}\}.$$

Este nuevo conjunto, $\mathbb{Z}/9\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{8}\}$ es de modo natural un anillo, podemos definir como se suman y multiplican sus elementos:

$$\bar{r} + \bar{s} := \overline{r+s}$$
$$\bar{r} \cdot \bar{s} := \overline{rs}$$

Si tenemos un número natural $n_r n_{r-1} \ldots n_0 := \sum_i n_i 10^i$ escrito en base decimal, entonces en $\mathbb{Z}/9\mathbb{Z}$ tenemos que

$$\overline{n_r n_{r-1} \ldots n_0} = \overline{\sum_i n_i 10^i} = \sum_i \bar{n}_i \bar{10}^i = \sum_i \bar{n}_i \bar{1}^i = \sum_i \bar{n}_i = \overline{\sum_i n_i}.$$

Por tanto, $n_r n_{r-1} \ldots n_0$ es divisible por 9 (es decir, $\overline{n_r n_{r-1} \ldots n_0} = \bar{0}$) si y solo si $\sum_i n_i$ es divisible por 9.

Si en $\mathbb{R}[x]$ considero equivalentes dos polinomios cuando difieran en un múltiplo de x^2+1 e igualo entre sí los polinomios que sean equivalentes obtengo un nuevo conjunto que denotamos $\mathbb{R}[x]/(x^2+1)$, que por definición es el conjunto

$$\mathbb{R}[x]/(x^2+1) := \{\overline{p(x)}, \forall\, p(x) \in \mathbb{R}[x] \colon \overline{p(x)} = \overline{q(x)} \iff p(x) - q(x) \in (x^2+1) \cdot \mathbb{R}[x]\}.$$

Este nuevo conjunto es de modo natural un anillo: podemos definir como se suman y multiplican sus elementos

$$\overline{p(x)} + \overline{q(x)} := \overline{p(x)+q(x)}$$
$$\overline{p(x)} \cdot \overline{q(x)} = \overline{p(x)\cdot q(x)}$$

Observemos que $\bar{x}\cdot\bar{x} = \overline{x^2} = \overline{-1}$. La aplicación, $\mathbb{C} \to \mathbb{R}[x]/(x^2+1)$, $a+bi \mapsto \overline{a+bx}$ es un isomorfismo de anillos.

Una vez que hemos estudiado los anillos euclídeos, o más generalmente los anillos de ideales principales, pasamos a estudiar los módulos sobre dominios de ideales principales. Un A-módulo es un A-espacio vectorial, salvo que no se supone que A sea un cuerpo sino que se supone que es solo un anillo. Igual que en la teoría de espacios vectoriales, puede hablarse de submódulos, cocientes por submódulos, sumas y productos directos de módulos, aplicaciones A-lineales, sistemas de generadores, pero no puede afirmarse en general la existencia de bases en los A-módulos. Demos dos ejemplos fundamentales de A-módulos. Si $(G,+)$ es un grupo abeliano entonces G es un $\mathbb{Z}$-módulo, porque además de que sabemos sumar los elementos de G, podemos definir la multiplicación de los elementos g de G por los enteros n de $\mathbb{Z}$:

$$n\cdot g := \begin{cases} g+\overset{n}{\cdots}+g, \text{ si } n>0 \\ (-g)+\overset{-n}{\cdots}+(-g), \text{ si } n<0 \\ 0, \text{ si } n=0 \end{cases}$$

Si E un k-espacio vectorial y $T\colon E\to E$ es un endomorfismo k-lineal, entonces E es un $k[x]$-módulo, porque además de que sabemos sumar los vectores de E, podemos definir la multiplicación de los vectores e de E por los polinomios $p(x)=\sum_i a_i x^i$ de $k[x]$:

$$(\sum_i a_i x^i)\cdot e := \sum_i a_i \cdot T^i(e).$$

Casos concretos de endomorfismos lineales que estudiaremos son:

1. $E=\{f\colon \mathbb{R}\to\mathbb{R} : f \text{ infinito derivable}\}$ y $T\colon E\to E$, $T(f):=f'$.
2. $E :=$ {sucesiones (a_n) de números reales} y $T\colon E\to E$, $T(a_n):=(a_{n+1})-(a_n)$.

Como hemos dicho, en los A-módulos no existen bases, en general. Si M es un A-módulo finito generado no existe en general un isomorfismo de A-módulos $A^n \simeq M$, como sucede con los espacios vectoriales. Existe un epimorfismo $A^n \to M$ y si A es un dominio de ideales principales existe un morfismo de A-módulos $\phi\colon A^m\to A^n$ de modo que $A^n/\mathrm{Im}\,\phi \simeq M$. Además, probaremos que existen bases en A^m y en A^n de modo que la matriz asociada a ϕ en estas bases es (a_{ij}) con $a_{ij}=0$ si $i\neq j$. Como consecuencia probaremos que si A es un dominio de ideales principales y M es un A-módulo finito generado existen elementos irreducibles únicos $p_1,\dots,p_r\in A$ y números naturales $n\geq 0$, $n_{ij}>0$ únicos de modo que

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A\oplus\cdots\oplus A/p_1^{n_{1s_1}}A)\oplus\cdots\oplus(A/p_r^{n_{r1}}A\oplus\cdots\oplus A/p_r^{n_{rs_r}}A).$$

Como corolario clasificaremos los grupos abelianos. También clasificaremos los endomorfismos lineales de un espacio vectorial. Aplicaremos esta teoría a la resolución de los sistemas de ecuaciones lineales diofánticas y la resolución de los sistemas de ecuaciones diferenciales lineales con coeficientes constantes.

Capítulo 1

Teoría de grupos

1.1. Introducción

La estructura más básica y fundamental en Álgebra es la estructura de grupo (y semigrupo). Los anillos, los espacios vectoriales, los módulos, etc. necesitan para su definición de la noción de grupo.

Demos una justificación de carácter muy general para la introducción de la teoría de grupos, siguiendo a Felix Klein en su Erlanger Programm. Dar una teoría (geométrica) es dar una estructura, un espacio con cierta estructura. En esta teoría es fundamental el estudio del grupo de automorfismos de la estructura, es decir, de aquellas biyecciones del espacio que respetan la estructura del espacio. Las nociones y objetos de este espacio, o de la teoría, serán aquéllos que queden invariantes por el grupo de automorfismos recién mencionado. El estudio de las funciones, campos diferenciables, etc., que quedan invariantes por el grupo y el estudio de las relaciones que verifican éstos, son todos los teoremas de la teoría. Es pues el estudio de los grupos (y la teoría de invariantes) un tópico fundamental en Matemáticas.

En el cálculo de las raíces de un polinomio, es conveniente conocer el grupo de aquellas permutaciones de las raíces, que respetan las relaciones algebraicas que verifican éstas. Este grupo se denomina grupo de Galois del polinomio. En el curso "Álgebra I"de tercero del grado de Matemáticas, se estudiará con profundidad este grupo.

1.2. Grupos

1. Definición: Sea X un conjunto. Diremos que una aplicación $m: X \times X \to X$ es una operación (interna) en X. Seguiremos las notaciones[1] $m(x,x') = x \cdot x' = xx'$.

2. Definición: Sea G un conjunto. Diremos que una operación

$$G \times G \to G, (g,g') \mapsto g \cdot g'$$

dota a G de estructura de grupo si cumple las siguientes condiciones:

[1] La operación $\cdot$, a veces, se denota con otros símbolos: $*$, $\circ$, etc.

1. Propiedad asociativa: $g\cdot(g'\cdot g'')=(g\cdot g')\cdot g''$, para todo $g,g',g''\in G$.

2. Existencia de elemento neutro: Existe un elemento de G, que denotamos por 1 y denominamos elemento neutro, tal que $1\cdot g=g\cdot 1=g$, para todo $g\in G$.

3. Existencia de inversos: Para cada $g\in G$ existe un elemento de G, que denotamos por g^{-1} y denominamos inverso de g, tal que $g\cdot g^{-1}=g^{-1}\cdot g=1$.

Si además se cumple que $g\cdot g'=g'\cdot g$, para todo $g,g'\in G$, diremos que G es un grupo abeliano o conmutativo; en cuyo caso, a menudo denotaremos la operación del grupo por $+$, al elemento neutro por 0 y al inverso de cada g por $-g$ (y lo denominaremos opuesto de g).

Si 1 y $1'$ son elementos neutros del grupo G entonces $1=1'$: $1=1\cdot 1'=1'$. Si h y h' son inversos de $g\in G$, entonces $h=h'$: $h=h\cdot 1=hgh'=1\cdot h'=h'$.

3. Ejemplos: 1. El conjunto de los números enteros, $\mathbb{Z}$, con la suma es un ejemplo básico de grupo conmutativo.

2. El conjunto de todas las biyecciones de un conjunto X en sí mismo, $BiyX$, con la operación composición de aplicaciones, es un grupo no conmutativo (cuando X contenga más de dos elementos).

3. $(\mathbb{Q},+)$, $(\mathbb{R},+)$ y $(\mathbb{C},+)$ son grupos abelianos.

4. $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$ y $(\mathbb{C}^*,\cdot)$ son grupos abelianos.

5. El conjunto de las sucesiones de números reales con la suma es un grupo abeliano.

6. El conjunto de las funciones reales de variable real (es decir, el conjunto de las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$) con la suma de funciones es un grupo abeliano.

7. El conjunto de las matrices, $M_{n\times m}(\mathbb{R})$ con la suma de matrices es un grupo abeliano.

8. El conjunto de las matrices cuadradas de orden n invertibles con coeficientes reales, con el producto de matrices, es un grupo (que no es abeliano para $n>1$).

9. **Producto directo de grupos:** Sean $(G,\cdot)$ y $(G',\cdot')$ dos grupos. Podemos dotar al producto cartesiano de G y G', $G\times G'$, de estructura de grupo definiendo la siguiente operación

$$(g,g')*(h,h'):=(g\cdot h,g'\cdot' h'),\text{ para todo }(g,g'),(h,h')\in G\times G'.$$

Si 1 es el elemento neutro de G y $1'$ es elemento neutro de G', entonces $(1,1')$ es el elemento neutro de $G\times G'$. Dado $(g,g')\in G\times G'$, entonces $(g,g')^{-1}=(g^{-1},g'^{-1})$.

Sea $\{G_i\}_{i\in I}$ un conjunto de grupos (la operación en cada uno de los G_i la denotaremos $\cdot$). Podemos dotar al producto cartesiano de todos los G_i, $\prod_{i\in I} G_i$ de estructura de grupo definiendo la siguiente operación

$$(g_i)_{i\in I}\cdot(h_i)_{i\in I} := (g_i\cdot h_i)_{i\in I}, \text{ para todo } (g_i)_{i\in I},(h_i)_{i\in I} \in \prod_{i\in I} G_i.$$

Si 1_i es el elemento neutro de G_i, entonces $(1_i)_{i\in I}$ es el elemento neutro de $\prod_{i\in I} G_i$. Dado $(g_i)_{i\in I} \in \prod_{i\in I} G_i$, entonces $((g_i)_{i\in I})^{-1} = (g_i^{-1})_{i\in I}$.

1.3. Subgrupos

1. Definición: Sea $(G,\cdot)$ un grupo. Diremos que un subconjunto $H \subseteq G$ es un subgrupo de G si cumple las siguientes condiciones:

1. Si $h,h' \in H$ entonces $h\cdot h' \in H$.
2. $1 \in H$.
3. Si $h \in H$ entonces $h^{-1} \in H$.

Si H es un subgrupo de G, entonces la operación de G define en H una estructura de grupo. Recíprocamente, si H es un subconjunto de un grupo G y la operación de G define en H una estructura de grupo entonces H es un subgrupo.

2. Proposición: *La intersección de cualquier familia de subgrupos de un grupo es un subgrupo.*

3. Definición: Dado un subconjunto X de un grupo G, llamaremos subgrupo generado por X y lo denotaremos $\langle X\rangle$, al mínimo subgrupo de G que contiene a X, es decir, a la intersección de todos los subgrupos de G que contienen a X.

4. Notación: Sea $(G,\cdot)$ un grupo y $g \in G$. Si $n > 0$, se define $g^n := g\overset{n}{\cdots}g$; si $n < 0$, se define $g^n := g^{-1}\overset{-n}{\cdots}g^{-1}$; y $g^0 := 1$. Dado $g \in G$, entonces $\langle g\rangle = \{g^n, \text{ con } n \in \mathbb{Z}\}$.

Si $(G,+)$ es un grupo conmutativo escribiremos $n\cdot g$, en vez de g^n (como es natural).

Por ejemplo, el subgrupo de $(\mathbb{Z},+)$ generado por $n \in \mathbb{Z}$, es igual a

$$\langle n\rangle = \{m\cdot n, m \in \mathbb{Z}\} =: n\mathbb{Z}.$$

El subgrupo de $\mathbb{Z}$ generado por $n,n' \in \mathbb{Z}$, es $\langle n,n'\rangle = \{mn+m'n', m,m' \in \mathbb{Z}\}$.

Sea $(G,+)$ un grupo abeliano y $G_1,G_2 \subseteq G$ dos subgrupos. El lector puede comprobar que $\langle G_1 \cup G_2\rangle = G_1 + G_2$, donde $G_1+G_2 := \{g_1+g_2,\ g_1 \in G_1\ g_2 \in G_2\}$.

5. Ejercicio: Sea G un grupo y $X \subseteq G$ un subconjunto. Prueba que

$$\langle X\rangle = \text{El conjunto de todas las “palabras” formadas con las letras } \{g,g^{-1}\}_{g\in X}.$$

(dos palabras con letras distintas pueden representar el mismo elemento de G, por ejemplo, $gg^{-1} = 1$).

Dado un número entero $z \in \mathbb{Z}$, llamaremos valor absoluto de z y denotaremos $|z|$, al máximo entre z y $-z$.

6. Teorema de división de números enteros: *Sean n y $d \neq 0$ dos números enteros. Existe una única pareja de números enteros c y r (denominados cociente y resto de dividir n por d), tales que $0 \leq r < |d|$ y*

$$n = c \cdot d + r.$$

Demostración. Procedamos por inducción sobre $|n|$, para probar la existencia de c y r.

Si $|n| = 0$, entonces $c = 0$ y $r = 0$. Podemos suponer que $|n| > 0$. El teorema es cierto para d si y solo si lo es para $-d$ (solo hay que cambiar c por $-c$), luego podemos suponer que $d > 0$.

Supongamos $n > 0$. Si $n < d$, entonces $c = 0$ y $r = n$. Si $n \geq d$, sea $n' = n - d$, luego $|n'| = n - d < n = |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' + 1)d + r'$ y hemos concluido.

Supongamos, ahora, $n < 0$. Si $-n \leq d$, sea $c = -1$ y $r = d + n$. Si $-n > d$, sea $n' = n + d$. luego $|n'| < |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' - 1)d + r'$ y hemos concluido.

Veamos la unicidad de c y r. Sea $n = cd + r = c'd + r'$, cumpliendo c, c', r, r' lo exigido. Podemos suponer $r \geq r'$. Entonces, $(c - c')d + (r - r') = 0$ y $|c - c'| \cdot |d| = |(c - c')d| = r - r' \leq r < |d|$, luego $c - c' = 0$. Por tanto, $c = c'$ y $r = n - cd = r'$.

□

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

Demostración. Si $H = \{0\}$ entonces $H = 0 \cdot \mathbb{Z}$.

Supongamos $H \neq \{0\}$. Existen naturales positivos en H, porque el opuesto de cada número entero de H pertenece a H. Sea $n \in H$ el mínimo número natural no nulo contenido en H. Veamos que $H = n\mathbb{Z}$: Obviamente, $n\mathbb{Z} \subseteq H$. Dado $m \in H \subset \mathbb{Z}$, existen números enteros c y r tales que

$$m = cn + r, \quad 0 \leq r < n.$$

Luego, $r = m - cn \in H$, porque $m, -cn \in H$. Por la definición de n, se tiene que $r = 0$. Luego, $m \in n\mathbb{Z}$, $H \subseteq n\mathbb{Z}$ y $H = n\mathbb{Z}$.

Por último, demostremos la unicidad: observemos que si un número natural m pertenece a $n\mathbb{Z}$, entonces $m \geq n$. Por tanto, si $m\mathbb{Z} = n\mathbb{Z}$, $m \geq n$ y $n \geq m$, luego $m = n$.

□

1.4. Morfismos de grupos

1. Definición: Sean $(G, \cdot)$ y $(G', \cdot)$ dos grupos. Diremos que una aplicación $f : G \to G'$ es un morfismo de grupos si para todo $g, g' \in G$ se cumple que

$$f(g \cdot g') = f(g) \cdot f(g').$$

Diremos que f es un isomorfismo de grupos si f es biyectiva (en tal caso la aplicación inversa f^{-1} es un isomorfismo de grupos). Diremos que es un epimorfismo (resp. monomorfismo) de grupos si f es epiyectiva (resp. inyectiva).

Si $f: G \to G'$ es un morfismo de grupos entonces $f(1) = 1$: $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ y multiplicando por $f(1)^{-1}$ obtenemos $1 = f(1)$. Además, $f(g^{-1}) = f(g)^{-1}$: $1 = f(1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$ y multiplicando por $f(g)^{-1}$ obtenemos $f(g)^{-1} = f(g^{-1})$.

2. Ejemplo: Sea G un grupo y $g \in G$. La aplicación $\tau_g: G \to G$ "conjugar por g", definida por

$$\tau_g(g') := gg'g^{-1}, \quad \text{para todo } g' \in G,$$

es un morfismo de grupos: $\tau_g(g_1g_2) = gg_1g_2g^{-1} = gg_1g^{-1}gg_2g^{-1} = \tau_g(g_1)\tau_g(g_2)$. Además es isomorfismo porque $(\tau_g)^{-1} = \tau_{g^{-1}}$. En efecto,

$$\tau_g(\tau_{g^{-1}}(g')) = g(g^{-1}g'g)g^{-1} = g' \text{ y } \tau_{g^{-1}}(\tau_g(g')) = g^{-1}(gg'g^{-1})g = g'.$$

3. Ejemplo: $\mathbb{Z} \to \mathbb{Z}$, $n \mapsto 3n$ es un morfismo de grupos.

4. Notación: Denotaremos $\mathrm{Hom}_{grp}(G, G')$ al conjunto de todos los morfismos de grupos de G en G'.

5. Ejemplo: Sean G_1 y G_2 dos grupos. La aplicación $\pi_1: G_1 \times G_2 \to G_1$, $\pi_1(g_1, g_2) := g_1$ es un morfismo de grupos. Igualmente, la aplicación $\pi_2: G_1 \times G_2 \to G_2$, $\pi_2(g_1, g_2) := g_2$ es un morfismo de grupos. Sea G otro grupo, se cumple que la aplicación

$$\mathrm{Hom}_{grp}(G, G_1 \times G_2) \to \mathrm{Hom}_{grp}(G, G_1) \times \mathrm{Hom}_{grp}(G, G_2),\ f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$$

es biyectiva.

6. Definición: Sea $f: G \to G'$ un morfismo de grupos. Llamaremos núcleo de f y lo denotaremos $\mathrm{Ker}\, f$, al subconjunto de G

$$\mathrm{Ker}\, f := f^{-1}(1) = \{g \in G : f(g) = 1\}.$$

Llamaremos imagen de f, que denotaremos $\mathrm{Im}\, f$, a la imagen de la aplicación f, es decir,

$$\mathrm{Im}\, f := \{f(g) \in G', g \in G\}.$$

7. Proposición: *$\mathrm{Ker}\, f$ es un subgrupo de G e $\mathrm{Im}\, f$ es un subgrupo de G'. Más aún, la antimagen por un morfismo de grupos de un subgrupo es subgrupo y la imagen de un subgrupo es subgrupo.*

8. Notación: Sean $(G, \cdot)$ un grupo y $H \subset G$ un subgrupo. Dado $g \in G$, denotaremos $gH := \{gh, \forall\, h \in H\}$.

9. Proposición: *Sea $f: G \to G'$ un morfismo de grupos. Dados $g, g' \in G$, se cumple que $f(g) = f(g')$ si y solo si $g' \in g \cdot \mathrm{Ker}\, f$.*

Demostración. Tenemos que $f(g) = f(g')$ si y solo si $1 = f(g)^{-1} \cdot f(g') = f(g^{-1} \cdot g')$, es decir, si y solo si $g^{-1} \cdot g' \in \operatorname{Ker} f$, que equivale a decir que $g' \in g \cdot \operatorname{Ker} f$. □

10. Proposición: *Un morfismo de grupos $f : G \to G'$ es inyectivo si y solo si* $\operatorname{Ker} f = \{1\}$.

Si identificamos los elementos de G cuando tengan la misma imagen, obtenemos un conjunto biyectivo con la imagen. De hecho esta biyección es un isomorfismo de grupos como veremos.

1.5. Cocientes por subgrupos

Sea $H \subseteq G$ un subgrupo y $g, g' \in G$.

Si $g' \in gH$ entonces $g'H = gH$: Sea $h \in H$, tal que $g' = gh$. Entonces, $g'H = ghH = gH$.

Si $g' \notin gH$, entonces $g'H \cap gH = \emptyset$, pues si $z \in g'H \cap gH$, entonces $g'H = zH = gH$.

En conclusión, dados $g, g' \in G$, o $gH = g'H$ o bien $gH \cap g'H = \emptyset$. Además, $gH = g'H$ si y solo si $g' \in gH$.

1. Definición: Sea $H \subseteq G$ un subgrupo. Dado $g \in G$, denotemos $\bar{g} := gH$. Llamaremos conjunto cociente de G por H, que denotaremos G/H, al conjunto

$$G/H := \{\bar{g}, \forall\, g \in G\}.$$

Recordemos que hemos probado que

$$\bar{g} = \bar{g'} \iff g' \in gH.$$

"Si en G identificamos cada $g \in G$ con todos los elementos de $gH \subseteq G$, obtenemos el conjunto G/H; todos los elementos de H los identificamos con 1."

2. Notación: Se dice que g es congruente con g' módulo H y se denota $g \equiv g' \, mod \, H$, cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g'H$ (o $g'^{-1}g \in H$). En notaciones aditivas, si $(G, +)$ es un grupo abeliano y $H \subset G$ es un subgrupo, entonces $g \equiv g' \, mod \, H$ cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g' + H$ (o $-g' + g \in H$).

La aplicación $G \to G/H$, $g \mapsto \bar{g}$, se denomina el morfismo de paso cociente (por H).

3. Ejemplo: $G/\{1\}$ es biyectivo con G. En efecto, estamos identificando cada $g \in G$ solo con $g \cdot 1 = g$. Con rigor, la aplicación de paso al cociente $\pi : G \to G/\{1\}$, $\pi(g) = \bar{g}$ es biyectiva: Es epiyectiva, pues dado $\bar{g} \in G/\{1\}$, $\pi(g) = \bar{g}$. Es inyectiva, porque si $\bar{g} = \bar{g'}$, entonces $g' = g \cdot 1 = g$.

4. Ejemplo: G/G es biyectivo con $\{1\}$. En efecto, estamos identificando cada $g \in G$ con todos los elementos de $g \cdot G = G$. Es decir, hacemos iguales todos los elementos de G. Con rigor, la aplicación $\{1\} \to G/G$, $1 \mapsto \bar{1}$ es biyectiva: Dado $\bar{g} \in G/G$ tenemos que $\bar{g} = \bar{1}$ porque $g = 1 \cdot g$.

5. Definición: Llamaremos orden de un conjunto X, que denotaremos $|X|$, al número de elementos del conjunto. Si el conjunto tiene un número infinito de elementos diremos que es de cardinal infinito.

6. Ejemplo: Si $n > 0$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un conjunto de orden n, explícitamente $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \ldots, \overline{n-1}\}$: Dado $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$, por el teorema de división de números enteros, existen números enteros únicos c y r, con $0 \leq r < n$, de modo que $m = cn + r$. Por tanto, existe un único $r \in \{0, \ldots, n-1\}$, tal que $\bar{m} = \bar{r}$.

7. Teorema de Lagrange: *Sea G un grupo de orden finito. Si H es un subgrupo de G entonces*

$$|G| = |G/H| \cdot |H|.$$

En particular, el orden de H divide al de G.

Demostración. $G = \coprod_{\bar{g} \in G/H} g \cdot H$ y $|gH| = |H|$ (porque la aplicación $H \to gH$, $h \mapsto gh$ es biyectiva). Por tanto, $|G| = |G/H| \cdot |H|$.

□

8. Definición: Se dice que un subgrupo $H \subseteq G$ es normal (en G) cuando $gHg^{-1} \subseteq H$, para todo $g \in G$, es decir, $ghg^{-1} \in H$, para todo $g \in G$ y todo $h \in H$.

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

10. Ejemplo: Los subgrupos de G, $\{1\}$ y G son normales.

11. Ejemplo: $H = \{\mathrm{Id}, (1,2)\} \subset S_3$ no es un subgrupo normal.

Si H es un subgrupo normal de G y tomamos $g^{-1} \in G$, tendremos $g^{-1}Hg \subseteq H$, luego $H \subseteq gHg^{-1} \subseteq H$ y $gHg^{-1} = H$ (para todo $g \in G$). Por tanto, $gH = Hg$, para todo $g \in G$, y recíprocamente si un subgrupo cumple esta condición el subgrupo es normal.

Sea $H \subseteq G$ un subgrupo normal. Definamos en G/H la operación

$$\bar{g} \cdot \bar{g'} := \overline{gg'},$$

que está bien definida porque $gHg'H = gg'HH = gg'H$. La propiedad asociativa se cumple de modo obvio, $\bar{1}$ es el elemento neutro y $\overline{g^{-1}}$ es el inverso de $\bar{g} \in G/H$. Luego, G/H es grupo. Además, el morfismo de paso al cociemte $\pi : G \to G/H$ es morfismo de grupos, pues $\pi(g \cdot g') = \overline{gg'} = \bar{g} \cdot \bar{g'} = \pi(g) \cdot \pi(g')$.

12. Proposición: *Sea $f : G \to G'$ un morfismo de grupos. Se cumple que* $\mathrm{Ker}\, f$ *es un subgrupo normal de G.*

Demostración. Al lector. □

13. Teorema de isomorfía: *Sea $f : G \to G'$ un morfismo de grupos. La aplicación, $\bar{f} : G/\mathrm{Ker}\, f \to \mathrm{Im}\, f$, $\bar{f}(\bar{g}) := f(g)$, es un isomorfismo de grupos.*

Demostración. La aplicación $\bar{f}$ está bien definida: dado $\overline{gh} = \bar{g} \in G/H$ (con $h \in H$), tenemos que $f(gh) = f(g)f(h) = f(g)1 = f(g)$.

Veamos que $\bar{f}$ es inyectiva: si $1 = \bar{f}(\bar{g}) = f(g)$, entonces $g \in \operatorname{Ker} f$ y $\bar{g} = \bar{1}$, luego $\operatorname{Ker} \bar{f} = \{\bar{1}\}$. Veamos que es epiyectiva: dado $f(g) \in \operatorname{Im} f$, tenemos que $\bar{f}(\bar{g}) = f(g)$.

Dejamos que el lector compruebe que $\bar{f}$ es morfismo de grupos. □

Observemos que dado un morfismo de grupos $f : G \to G'$ tenemos el diagrama conmutativo

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \pi} & & \uparrow \\ G/\operatorname{Ker} f & \xrightarrow{\bar{f}} & \operatorname{Im} f \end{array} \qquad \begin{array}{ccc} g & \xmapsto{f} & f(g) \\ \downarrow{\scriptstyle \pi} & & \uparrow \\ \bar{g} & \xmapsto{\bar{f}} & f(g) \end{array}$$

14. Ejemplo: Cuando hablamos de un ángulo hablamos de un número real y además decimos que dos ángulos son iguales si difieren en 2π por un número entero. Sabemos sumar ángulos. Con más rigor: Consideremos el grupo $(\mathbb{R}, +)$ y el subgrupo $2\pi\mathbb{Z} \subset \mathbb{R}$. El grupo de todos los ángulos es $\mathbb{R}/2\pi\mathbb{Z}$.

Sea $S^1 \subset \mathbb{R}^2$ la circunferencia de radio 1 centrada en el origen. Observemos que la aplicación

$$\mathbb{R}/2\pi\mathbb{Z} \to S^1,\ \bar{\theta} \mapsto (\cos\theta, \operatorname{sen}\theta)$$

es una biyección. Por tanto, vía esta biyección S^1 es un grupo abeliano. Si $*$ es la operación definida en S^1, puede comprobarse que $(x, y) * (x', y') = (xx' - yy', xy' + yx')$.

15. Ejercicio: Prueba que $\mathbb{R}/\mathbb{Z}$ es un grupo isomorfo al grupo $[0, 1)$, donde $[0, 1)$ es un grupo con la siguiente operación

$$\alpha * \beta = \begin{cases} \alpha + \beta, & \text{si } \alpha + \beta < 1. \\ \alpha + \beta - 1, & \text{si } \alpha + \beta \geq 1. \end{cases}$$

16. Ejercicio: Sea $f : G \to G'$ un morfismo de grupos. Sea H un subgrupo normal de G y supongamos que $H \subseteq \operatorname{Ker} f$. Demuestra que la aplicación $\bar{f} : G/H \to G'$ definida por $\bar{f}(\bar{g}) = f(g)$ está bien definida y es un morfismo de grupos.

1.6. Grupos cíclicos

1. Definición: Diremos que un grupo G es cíclico si está generado por uno de sus elementos, es decir, existe $g \in G$ de modo que $G = \langle g \rangle$.

2. Proposición: *Un grupo G es cíclico si y solo si es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, para algún número natural n.*

Demostración. $\mathbb{Z}/n\mathbb{Z}$ es un grupo (aditivo) cíclico, generado por $\bar{1}$.

Supongamos que $G = \langle g \rangle$ es cíclico. Sea $f : \mathbb{Z} \to G$, la aplicación definida por $f(n) := g^n$. Es fácil comprobar que f es un morfismo de grupos. $\operatorname{Im} f$ es un subgrupo de G, que contiene a g, luego $\operatorname{Im} f = G$ y f es epiyectivo. $\operatorname{Ker} f$ es un subgrupo de $\mathbb{Z}$, luego existe $n \in \mathbb{N}$ tal que $\operatorname{Ker} f = n\mathbb{Z}$. Por el teorema de isomorfía $\mathbb{Z}/n\mathbb{Z} \simeq G$. □

$\mathbb{Z}/n\mathbb{Z}$ es un grupo conmutativo, pues es cociente de $\mathbb{Z}$ que es conmutativo. Por tanto, todo grupo cíclico es conmutativo.

3. Definición: Llamaremos orden de un elemento g de un grupo G, y lo denotaremos $\mathrm{ord}(g)$, al orden del subgrupo $\langle g\rangle$ de G que genera.

En la proposición anterior hemos dado el isomorfismo $\mathbb{Z}/n\mathbb{Z} \simeq \langle g\rangle$, $\bar{m} \mapsto g^m$. Por tanto, si $n > 0$, el orden de g es igual a $|\langle g\rangle| = |\mathbb{Z}/n\mathbb{Z}| = n$, $\langle g\rangle = \{1, g^1, \ldots, g^{n-1}\}$ y n es el mínimo número natural positivo tal que $g^n = 1$, además, si $g^m = 1$, entonces m es un múltiplo del orden de g. Si $n = 0$, entonces el orden de g es $|\langle g\rangle| = |\mathbb{Z}| = \infty$ y $\langle g\rangle = \{\ldots, g^{-m}, \ldots, 1, g^1, \ldots, g^m, \ldots\}$ (cumpliendo $g^i \neq g^j$, para todo $i, j \in \mathbb{Z}$, $i \neq j$).

4. Si G es un grupo de orden $m < \infty$, entonces el orden de todo elemento $g \in G$ divide a m, ya que el orden de todo subgrupo $\langle g\rangle$ divide al orden del grupo G, por el teorema de Lagrange. Es decir, $g^{|G|} = 1$.

5. Proposición: *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Sea $G = \langle g\rangle$ un grupo cíclico y $\pi\colon \mathbb{Z} \to G$, $\pi(n) := g^n$ un epimorfismo de grupos. Dado un subgrupo $H \subseteq G$, se cumple que $H = \pi(\pi^{-1}(H))$. Ahora bien, $\pi^{-1}(H)$ es un subgrupo de $\mathbb{Z}$, luego es cíclico, es decir, generado por un elemento z. Por tanto, $H = \pi(\pi^{-1}(H))$ está generado por $\pi(z)$ y es cíclico. □

1.7. Grupo simétrico

El grupo simétrico de un conjunto X es el grupo de todas las biyecciones (o "permutaciones") de X en sí mismo, con la operación composición de aplicaciones.

Comentario: Una biyección entre dos conjuntos $\tau\colon X \to Y$, puede entenderse como una identificación de X con Y: "a $x \in X$ lo llamamos $\tau(x)$ en Y". Dada una aplicación $f\colon X \to X$, que aplica x en $f(x)$, tenemos la correspondiente aplicación en Y: "la que aplica $\tau(x)$ en $\tau(f(x))$, es decir, la aplicación $\tau \circ f \circ \tau^{-1}\colon Y \to Y$". Así el grupo de las permutaciones de X se identifica con el grupo de las permutaciones de Y (vía la identificación de X con Y). Con mayor precisión, el morfismo

$$BiyX \to BiyY, \quad \sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$$

es un isomorfismo de grupos (como el lector puede comprobar).

Sea Y es un conjunto de orden n. Entonces, Y es biyectivo con $\{1, \ldots, n\}$ y por lo tanto $BiyY = Biy\{1, \ldots, n\} =: S_n$. El número de permutaciones de n elementos es $n!$, luego $|S_n| = n!$.

1. Proposición (Cayley): *Sea G un grupo. La aplicación $G \to \mathrm{Biy}(G)$, $g \mapsto L_g$, donde $L_g(g') := gg'$ es un morfismo de grupos inyectivo, luego "G es isomorfo a un subgrupo de un grupo simétrico".*

2. Definiciones: Dados r elementos distintos $x_1,\dots,x_r \in X$, con $r > 1$, denotaremos $(x_1,\dots,x_r) = \sigma \in Biy X$ a la permutación definida por $\sigma(x_i) = x_{i+1}$, para todo $i < r$; $\sigma(x_r) = x_1$; y $\sigma(x) = x$, para todo $x \notin \{x_1,\dots,x_r\}$. Diremos que $(x_1,\dots,x_r)$ es un ciclo y observemos que es de orden r. Si $r = 2$, diremos que el ciclo (x_1,x_2) es una transposición. Diremos que dos ciclos $(x_1,\dots,x_r),(x'_1,\dots,x'_{r'})$ de $Biy X$ son disjuntos si $x_i \neq x'_j$ para todo i,j.

3. Lema: *Si $\sigma = (x_1,\dots,x_r)$ y $\sigma' = (x'_1,\dots,x'_{r'})$ son disjuntos, entonces conmutan, es decir, $\sigma \circ \sigma' = \sigma' \circ \sigma$.*

Demostración. Para $x \in \{x_1,\dots,x_r\}$, $(\sigma \circ \sigma')(x) = \sigma(x) = (\sigma' \circ \sigma)(x)$. Para $x \in \{x'_1,\dots,x'_r\}$, $(\sigma \circ \sigma')(x) = \sigma'(x) = (\sigma' \circ \sigma)(x)$. Para $x \notin \{x_i,x'_j\}_{i,j}$, $(\sigma \circ \sigma')(x) = x = (\sigma' \circ \sigma)(x)$.

De otro modo (siguiendo el comentario anterior): $\sigma' \circ \sigma \circ \sigma'^{-1} = (\sigma'(x_1),\dots,\sigma'(x_r)) = (x_1,\dots,x_r) = \sigma$, luego $\sigma \circ \sigma' = \sigma' \circ \sigma$.

□

4. Teorema: *Toda permutación $\sigma \in S_n$, distinta de la identidad, es igual a un producto de ciclos disjuntos, de modo único salvo el orden de los factores.*

Demostración. Sea $x \in X$, tal que $\sigma(x) \neq x$. Sea r el mínimo número natural positivo tal que $\sigma^r(x) = x$ (tal número existe porque el orden de σ, que divide al orden de S_n, es finito). Para todo $0 \leq s < s' < r$, se cumple que $\sigma^{s'}(x) \neq \sigma^s(x)$: pues componiendo con σ^{-s} son distintos, pues $\sigma^{s'-s}(x) \neq x$, porque $0 < s' - s < r$. Sea $\sigma_1 = (x,\sigma(x),\dots,\sigma^{r-1}(x))$. Entonces, como σ_1 y σ coinciden sobre $\{x,\sigma(x),\dots,\sigma^{r-1}(x)\}$ y σ_1 es la identidad sobre $X\setminus\{x,\sigma(x),\dots,\sigma^{r-1}(x)\}$, se cumple que $\sigma_1^{-1} \circ \sigma$ deja fijos $\{x,\sigma(x),\dots,\sigma^{r-1}(x)\}$ y los que dejaba fijos σ. Reiterando el proceso obtenemos ciclos disjuntos $\sigma_1,\dots,\sigma_s$ tales que $\sigma_s^{-1} \circ \cdots \circ \sigma_1^{-1} \circ \sigma = \mathrm{Id}$. Luego, $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$.

Sea otra descomposición $\sigma = \tau_1 \circ \cdots \tau_t$ en producto de ciclos disjuntos. Reordenando, podemos suponer que $\tau_1(x) \neq x$. Es decir, x "aparece" en el ciclo τ_1 (y en el de σ_1). Luego, $\tau_1(x) = \sigma(x) = \sigma_1(x)$. Obviamente, $\tau_1(x) = \sigma(x) = \sigma_1(x)$ "aparece" en ciclo de τ_1 y en el de σ_1. Luego, $\tau_1^2(x) = \sigma^2(x) = \sigma_1^2(x)$. Así sucesivamente, $\tau_1^i(x) = \sigma^i(x) = \sigma_1^i(x)$, para todo i. Por tanto, $\tau_1 = \sigma_1$ y $\sigma_2 \circ \cdots \circ \sigma_s = \tau_2 \circ \cdots \circ \tau_t$. Reiterando el argumento concluimos que, después de reordenar los factores, $\sigma_2,\dots,\sigma_s$ coinciden con $\tau_2,\dots,\tau_t$.

□

5. Definición: Sea $\sigma \in S_n$ una permutación distinta de la identidad. Sea $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ una descomposición en producto de ciclos disjuntos y d_i el orden de σ_i. Reordenando podemos suponer que $d_1 \geq d_2 \geq \cdots \geq d_s$. Diremos que $d_1,\dots,d_s$ es la forma de σ.

6. Definición: Dado un elemento $g \in G$, diremos que el morfismo $\tau_g : G \to G$, $\tau_g(g') := gg'g^{-1}$, es la conjugación en G por g. Diremos que $h,h' \in G$ son conjugados si y solo si existe $g \in G$, de modo que $\tau_g(h) = h'$.

7. Teorema: *La condición necesaria y suficiente para que $\sigma,\sigma' \in S_n$ sean conjugadas es que tengan la misma forma.*

Demostración. Sea $\sigma = (x_{11},\dots,x_{1d_1})\circ\cdots\circ(x_{s1},\cdots,x_{sd_s})$ una descomposición en producto de ciclos disjuntos y $\tau \in S_n$. Entonces,

$$\tau\circ\sigma\circ\tau^{-1} = (\tau(x_{11}),\dots,\tau(x_{1d_1}))\circ\cdots\circ(\tau(x_{s1}),\cdots,\tau(x_{sd_s}))$$

tiene la misma forma que σ. Sea $\sigma' = (x'_{11},\dots,x'_{1d_1})\circ\cdots\circ(x'_{s1},\cdots,x'_{sd_s})$. Si τ es cualquier permutación que cumpla $\tau(x_{ij}) = x'_{ij}$, para todo i,j, entonces $\tau\circ\sigma\circ\tau^{-1} = \sigma'$. □

8. Proposición: *Si $d_1,\dots,d_s$ es la forma de $\sigma \in S_n$, entonces el orden de σ es el mínimo común múltiplo de $d_1,\dots,d_s$.*

Demostración. Escribamos $\sigma = \sigma_1\cdots\sigma_s$ como producto de ciclos disjuntos. Entonces, $\sigma^n = \sigma_1^n\cdots\sigma_s^n$ y σ_i^n es "disjunta" con σ_j^n, para $i \neq j$. Luego, $\sigma^n = \mathrm{Id}$ si y solo si $\sigma_1^n = \cdots = \sigma_s^n = \mathrm{Id}$. Luego el orden de σ es el mínimo común múltiplo de los órdenes de los σ_i. □

9. Proposición: *Todo permutación $\sigma \in S_n$ es producto de transposiciones.*

Demostración. Como toda permutación es producto de ciclos, basta probar que todo ciclo es producto de transposiciones. Sea, pues, un ciclo $(x_1,\dots,x_r) \in S_n$. Obviamente,

$$(x_1,\dots,x_r) = (x_1,x_2)(x_2,\dots,x_r) = (x_1,x_2)(x_2,x_3)(x_3,\dots,x_r) = \cdots = (x_1,x_2)(x_2,x_3)\cdots(x_{r-1},x_r).$$

□

Signo de una permutación

Cada permutación $\sigma \in S_n = Biy(\{1,2,\dots,n\})$ define una biyección del anillo de polinomios en n variables con coeficientes números racionales: $\mathbb{Q}[x_1,\dots,x_n] \to \mathbb{Q}[x_1,\dots,x_n]$, $p(x_1,\dots,x_n) \mapsto p(x_1,\dots,x_n)^\sigma := p(x_{\sigma(1)},\dots,x_{\sigma(n)})$.

Sea $\delta(x_1,\dots,x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Q}[x_1,\dots,x_n]$. Dada una permutación $\sigma \in S_n = Biy(\{1,2,\dots,n\})$, es fácil comprobar que $\delta(x_1,\dots,x_n)^\sigma = \delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \pm\delta(x_1,\dots,x_n)$.

10. Definición: Dada $\sigma \in S_n$, llamaremos signo de σ, que denotaremos $\mathrm{sign}(\sigma)$, al número entero 1 ó -1 tal que $\delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \mathrm{sign}(\sigma)\cdot\delta(x_1,\dots,x_n)$.

11. Proposición: *Consideremos el grupo (multiplicativo) $\{1,-1\}$. El morfismo natural*

$$\mathrm{sign}\colon S_n \to \{1,-1\},\ \sigma \mapsto \mathrm{sign}(\sigma)$$

es un morfismo de grupos.

Demostración. $\mathrm{sign}(\sigma'\sigma)\cdot\delta = \delta^{\sigma'\sigma} = (\delta^\sigma)^{\sigma'} = (\mathrm{sign}(\sigma)\delta)^{\sigma'} = \mathrm{sign}(\sigma')\cdot\mathrm{sign}(\sigma)\cdot\delta$. Luego, $\mathrm{sign}(\sigma)\cdot\mathrm{sign}(\sigma') = \mathrm{sign}(\sigma\cdot\sigma')$. □

Es fácil ver que $\text{sign}(\text{Id}) = 1$ y que $\text{sign}((1,2)) = -1$.

Observemos que el signo es invariante por conjugaciones, es decir,

$$\text{sign}(\tau\sigma\tau^{-1}) = \text{sign}(\tau)\cdot\text{sign}(\sigma)\cdot\text{sign}(\tau)^{-1} = \text{sign}(\sigma).$$

En particular, el signo de toda transposición es -1, porque todas son conjugadas de la transposición $(1,2)$.

12. Proposición: *Si la forma de una permutación $\sigma \in S_n$ es $d_1,\dots,d_r$, entonces*

$$\text{sign}(\sigma) = (-1)^{d_1-1}\cdots(-1)^{d_r-1} = (-1)^{d_1+\cdots+d_r-r}.$$

Demostración. Si $\sigma = (x_1,\dots,x_r)$ es un ciclo, entonces

$$(x_1,\dots,x_r) = (x_1,x_2)(x_2,x_3)\cdots(x_{r-1},x_r)$$

es producto de $r-1$ transposiciones. Como el morfismo sign es un morfismo de grupos, $\text{sign}(\sigma) = (-1)^{r-1}$.

En general, $\sigma = \sigma_1\cdots\sigma_r$, donde σ_i es un ciclo de orden d_i. Por tanto, $\text{sign}(\sigma) = \text{sign}(\sigma_1)\cdots\text{sign}(\sigma_r) = (-1)^{d_1-1}\cdots(-1)^{d_r-1}$. □

Evidentemente, sign es un epimorfismo (para $n > 1$).

13. Definición: Llamaremos subgrupo alternado de S_n, que denotaremos A_n, al núcleo del morfismo sign, es decir, al subgrupo (normal) de S_n formado por las permutaciones de signo positivo.

Por el teorema de isomorfía $S_n/A_n \simeq \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Por el teorema de Lagrange, $|A_n| = |S_n|/2 = n!/2$ $(n > 1)$.

1.8. Cuestionario

1. ¿Es $(\mathbb{N},+)$ un grupo?¿Y $(\mathbb{Q},\cdot)$?

2. ¿Es S_3 con la composición de permutaciones un grupo abeliano?¿Es el grupo de las matrices $2x2$ con coeficientes reales invertibles, con la multiplicación de matrices, un grupo abeliano?

3. Sean g_1,g_2,g_3 tres elementos de un grupo G. Calcula $(g_1\cdot g_2\cdot g_3)^{-1}$ en términos de productos de los elementos g_1^{-1}, g_2^{-1} y g_3^{-1}.

4. Sean g,g' dos elementos de un grupo $(G,\cdot)$. Prueba que si $g\cdot g' = g'$ entonces $g = 1$.

5. Sean x e y dos elementos de un grupo G. Si $x^5 = 1$, $y^4 = 1$ y $xy = yx^3$, prueba que $x^2y = yx$ y $xy^3 = y^3x^2$.

6. Sea $(G,\cdot)$ un grupo. Definamos la operación interna $\diamond$ en G como sigue: $g\diamond g' := g'\cdot g$, para todo $g,g' \in G$. Prueba que $(G,\diamond)$ es un grupo.

7. Consideremos los grupos $(\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$. Consideremos el grupo producto directo $\mathbb{Z}\times\mathbb{R}^*$ y $(3,3)\in\mathbb{Z}\times\mathbb{R}^*$. Calcula $(3,3)^{-1}$.

8. Sea $A=\begin{pmatrix}0&0&-1\\-1&-0&0\\0&1&0\end{pmatrix}$. Calcula A^{2001}.

9. Sea $(G,\cdot)$ un grupo ¿Son $\{1\}$ y G subgrupos de G?

10. Sea $(G,\cdot)$ un grupo ¿Es la aplicación $G\to G$, $g\mapsto g^2$, un morfismo de grupos?

11. Sea $M_2(\mathbb{R})^*$ el conjunto de las matrices cuadradas de orden 2 invertibles, que es un grupo con la multiplicación de matrices ¿Es la aplicación $M_2(\mathbb{R})\to M_2(\mathbb{R})$, $g\mapsto g^2$, un morfismo de grupos?

12. Sea $f:G\to G'$ un morfismo de grupos. Prueba que $\operatorname{Im} f$ es un subgrupo de G'.

13. Sea $f:G\to G'$ un morfismo de grupos. Demuestra que $\operatorname{Ker} f$ es un subgrupo de G.

14. Sea G el conjunto de los enteros que son múltiplos de 6 y 10 ¿Es G es un subgrupo de $(\mathbb{Z},+)$?¿Es G el conjunto de los múltiplos de algún número natural?

15. ¿Existe $(n,m)\in\mathbb{Z}\times\mathbb{Z}$ de modo que $\mathbb{Z}\times\mathbb{Z}=\langle(n,m)\rangle$?

16. Consideremos el subrgupo $H=\langle(2,3),(4,5)\rangle\subseteq\mathbb{Z}\times\mathbb{Z}$. Prueba que $H=2\mathbb{Z}\times\mathbb{Z}$.

17. Sea G un grupo abeliano. Prueba que G es abeliano si y solo si $gg'g^{-1}g'^{-1}=1$ para todo $g,g'\in G$. Prueba que la aplicación $G\to G$, $g\mapsto g^{-1}$, para todo g, es un morfismo de grupos si y solo si G es abeliano.

18. Defínase una biyección entre $\mathbb{R}/\mathbb{Z}$ y $(0,1]$.

19. Sea $f:\mathbb{Z}\to\mathbb{C}^*$, $f(n):=e^{\frac{n\cdot 2\cdot\pi\cdot i}{5}}$. Prueba que f es un morfismo de grupos. Calcula $\operatorname{Ker} f$. Calcula $\operatorname{Im} f$. Prueba que $\mathbb{Z}/5\mathbb{Z}\simeq\operatorname{Im} f$.

20. Demuestra que G/G es un grupo isomorfo al grupo $\{1\}$. Demuestra que $G/\{1\}$ es un grupo isomorfo a G.

21. Sea $H=\{\mathrm{Id},(1,2)\}\subset S_3$ ¿Es H un subgrupo normal de S_3?¿Es H conmutativo?

22. Sea $H=\{\mathrm{Id},(1,2)\}\subset S_3$. Demuestra que H es un grupo isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

23. Prueba que todo grupo de orden primo es cíclico.

24. Sea $f:G\to G'$ un morfismo de grupos epiyectivo. Si G es cíclico prueba que G' es cíclico.

25. ¿Es $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ un grupo cíclico?

26. ¿Es $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ un grupo cíclico?

27. ¿Qué elementos de $\mu_6 := \{e^{\frac{2\cdot\pi\cdot i\cdot n}{6}} \in \mathbb{C}$, con n natural y $0 \leq n < 6\}$ lo generan?

28. Sea $g \in M_2(\mathbb{R})^*$ el giro de 60 grados alrededor del origen. Calcular los generadores del grupo $\langle g \rangle$.

29. Resuelve el problema 9.

30. Escribir la permutación $\sigma = \binom{123456789}{935726481}$ como producto de ciclos disjuntos.

31. ¿Es $\langle (1,2) \rangle$ un subgrupo normal de S_4?

32. ¿Es S_n un grupo abeliano?

33. Escribir la permutación $\sigma = \binom{12345678}{74582163}$ como producto de transposiciones.

34. Sea $H = \langle (1,2),(1,3) \rangle \subseteq S_3$ ¿Es $H = S_3$?

35. Explicítense todos los elementos de S_4 de signo positivo.

36. Explicítense todos los elementos de S_4 de orden 2.

37. Sea $\sigma \in S_7$ la permutación definida por $\sigma(1) = 7$, $\sigma(2) = 6$, $\sigma(3) = 4$, $\sigma(4) = 5$, $\sigma(5) = 3$, $\sigma(6) = 2$ y $\sigma(7) = 1$. Calcula $\text{ord}(\sigma)$ y $\text{sign}(\sigma)$.

38. Prueba que $S_5 = \langle (1,2),(1,2,3,4,5) \rangle$.

1.9. Biografía de Georg Fröbenius

FRÖBENIUS BIOGRAPHY

Georg Fröbenius's father was Christian Ferdinand Fröbenius, a Protestant parson, and his mother was Christine Elizabeth Friedrich. Georg was born in Charlottenburg which was a district of Berlin which was not incorporated into the city until 1920. He entered the Joachimsthal Gymnasium in 1860 when he was nearly eleven years old and graduated from the school in 1867. In this same year he went to the University of Göttingen where he began his university studies but he only studied there for one semester before returning to Berlin.

Back at the University of Berlin he attended lectures by Kronecker, Kummer and Weierstrass. He continued to study there for his doctorate, attending the seminars of Kummer and Weierstrass, and he received his doctorate (awarded with distinction) in 1870 supervised by Weierstrass. In 1874, after having taught at secondary school level first at the Joachimsthal Gymnasium then at the Sophienrealschule, he was appointed to the University of Berlin as an extraordinary professor of mathematics.

For the description of Fröbenius's career so far, the attentive reader may have noticed that no mention has been made of him receiving his habilitation before being appointed to a teaching position. This is not an omission, rather it is surprising given

the strictness of the German system that this was allowed. We should say that it must ultimately have been made possible due to strong support from Weierstrass who was extremely influential and considered Fröbenius one of his most gifted students.

Fröbenius was only in Berlin for a year before he went to Zürich to take up an appointment as an ordinary professor at the Eidgenössische Polytechnikum. For seventeen years, between 1875 and 1892, Fröbenius worked in Zürich. He married there and brought up a family and did much important work in widely differing areas of mathematics. We shall discuss some of the topics which he worked on below, but for the moment we shall continue to describe how Fröbenius's career developed.

In the last days of December 1891 Kronecker died and, therefore, his chair in Berlin became vacant. Weierstrass, strongly believing that Fröbenius was the right person to keep Berlin in the forefront of mathematics, used his considerable influence to have Fröbenius appointed. However, for reasons which we shall discuss in a moment, Fröbenius turned out to be something of a mixed blessing for mathematics at the University of Berlin.

The positive side of his appointment was undoubtedly his remarkable contributions to the representation theory of groups, in particular his development of character theory, and his position as one of the leading mathematicians of his day. The negative side came about largely through his personality which is described as:

"*... occasionally choleric, quarrelsome, and given to invectives.*"

Biermann described the strained relationships which developed between Fröbenius and his colleagues at Berlin:

"*... suspected at every opportunity a tendency of the Ministry to lower the standards at the University of Berlin, in the words of Fröbenius, to the rank of a technical school ... Even so, Fuchs and Schwarz yielded to him, and later Schottky, who was indebted to him alone for his call to Berlin. Fröbenius was the leading figure, on whom the fortunes of mathematics at Berlin university rested for 25 years. Of course, it did not escape him, that the number of doctorates, habilitations, and docents slowly but surely fell off, although the number of students increased considerably. That he could not prevent this, that he could not reach his goal of maintaining unchanged the times of Weierstrass, Kummer and Kronecker also in their external appearances, but to witness helplessly these developments, was doubly intolerable for him, with his choleric disposition.*"

We should not be too hard on Fröbenius for, as Haubrich explained:

"*They all felt deeply obliged to carry on the Prussian neo-humanistic tradition of university research and teaching as they themselves had experienced it as students. This is especially true of Fröbenius. He considered himself to be a scholar whose duty it was to contribute to the knowledge of pure mathematics. Applied mathematics, in his opinion, belonged to the technical colleges.*"

The view of mathematics at the University of Göttingen was, however, very different. This was a time when there was competition between mathematians in the University of Berlin and in the University of Göttingen, but it was a competition that Göttingen won, for there mathematics flourished under Klein, much to Fröbenius's annoyance. Biermann wrote:

"*The aversion of Fröbenius to Klein and S. Lie knew no limits ...*"

Fröbenius hated the style of mathematics which Göttingen represented. It was a new approach which represented a marked change from the traditional style of German universities. Fröbenius, as we said above, had extremely traditional views. In a letter to Hurwitz, who was a product of the Göttingen system, he wrote on 3 February 1896:

"*If you were emerging from a school, in which one amuses oneself more with rosy images than hard ideas, and if, to my joy, you are also gradually becoming emancipated from that, then old loves don't rust. Please take this joke facetiously.*"

One should put the other side of the picture, however, for Siegel, who knew Fröbenius for two years from 1915 when he became a student until Fröbenius's death, related his impression of Fröbenius as having a warm personality and expresses his appreciation of his fast-paced varied and deep lectures. Others would describe his lectures as solid but not stimulating.

To gain an impression of the quality of Fröbenius's work before the time of his appointment to Berlin in 1892 we can do no better than to examine the recommendations of Weierstrass and Fuchs when Fröbenius was elected to the Prussian Academy of Sciences in 1892. We quote a short extract to show the power, variety and high quality of Fröbenius's work in his Zürich years. Weierstrass and Fuchs listed 15 topics on which Fröbenius had made major contributions:

"*-On the development of analytic functions in series.*

-On the algebraic solution of equations, whose coefficients are rational functions of one variable.

-The theory of linear differential equations.

-On Pfaff's problem.

-Linear forms with integer coefficients.

-On linear substitutions and bilinear forms...

-On adjoint linear differential operators...

-The theory of elliptic and Jacobi functions...

-On the relations among the 28 double tangents to a plane of degree 4.

-On Sylow's theorem.

-On double cosets arising from two finite groups.

-On Jacobi's covariants...

-On Jacobi functions in three variables.

-The theory of biquadratic forms.

-On the theory of surfaces with a differential parameter."

In his work in group theory, Fröbenius combined results from the theory of algebraic equations, geometry, and number theory, which led him to the study of abstract groups. He published Über Gruppen von vertauschbaren Elementen in 1879 (jointly with Stickelberger, a colleague at Zürich) which looks at permutable elements in groups. This paper also gives a proof of the structure theorem for finitely generated abelian groups. In 1884 he published his next paper on finite groups in which he proved Sylow's theorems for abstract groups (Sylow had proved his theorem as a result about permutation groups in his original paper). The proof which Fröbenius gives is the one, based on conjugacy classes, still used today in most undergraduate courses.

In his next paper in 1887 Fröbenius continued his investigation of conjugacy classes in groups which would prove important in his later work on characters. In the introduction to this paper he explains how he became interested in abstract groups, and this was through a study of one of Kronecker's papers. It was in the year 1896, however, when Fröbenius was professor at Berlin that his really important work on groups began to appear. In that year he published five papers on group theory and one of them Über die Gruppencharactere on group characters is of fundamental importance. He wrote in this paper:

"*I shall develop the concept [of character for arbitrary finite groups] here in the belief that through its introduction, group theory will be substantially enriched.*"

This paper on group characters was presented to the Berlin Academy on July 16 1896 and it contains work which Fröbenius had undertaken in the preceding few months. In a series of letters to Dedekind, the first on 12 April 1896, his ideas on group characters quickly developed. Ideas from a paper by Dedekind in 1885 made an important contribution and Fröbenius was able to construct a complete set of representations by complex numbers. It is worth noting, however, that although we think today of Fröbenius's paper on group characters as a fundamental work on representations of groups, Fröbenius in fact introduced group characters in this work without any reference to representations. In was not until the following year that representations of groups began to enter the picture, and again it was a concept due to Fröbenius. Hence 1897 is the year in which the representation theory of groups was born.

Over the years 1897-1899 Fröbenius published two papers on group representations, one on induced characters, and one on tensor product of characters. In 1898 he introduced the notion of induced representations and the Fröbenius Reciprocity Theorem. It was a burst of activity which set up the foundations of the whole of the machinery of representation theory.

In a letter to Dedekind on 26 April 1896 Fröbenius gave the irreducible characters for the alternating groups A_4, A_5, the symmetric groups S_4, S_5 and the group $PSL(2,7)$ of order 168. He completely determined the characters of symmetric groups in 1900 and of characters of alternating groups in 1901, publishing definitive papers on each. He continued his applications of character theory in papers of 1900 and 1901 which studied the structure of Fröbenius groups.

Only in 1897 did Fröbenius learn of Molien's work which he described in a letter to Dedekind as "very beautiful but difficult". He reformulated Molien's work in terms of matrices and then showed that his characters are the traces of the irreducible representations. This work was published in 1897. Fröbenius's character theory was used with great effect by Burnside and was beautifully written up in Burnside's 1911 edition of his Theory of Groups of Finite Order.

Fröbenius had a number of doctoral students who made important contributions to mathematics. These included Edmund Landau who was awarded his doctorate in 1899, Issai Schur who was awarded his doctorate in 1901, and Robert Remak who was awarded his doctorate in 1910. Fröbenius collaborated with Schur in representation theory of groups and character theory of groups. It is certainly to Fröbenius's credit that he so quickly spotted the genius of his student Schur. Fröbenius's representation theory for finite groups was later to find important applications in quantum mechanics

and theoretical physics which may not have entirely pleased the man who had such "pure" views about mathematics.

Among the topics which Fröbenius studied towards the end of his career were positive and non-negative matrices. He introduced the concept of irreducibility for matrices and the papers which he wrote containing this theory around 1910 remain today the fundamental results in the discipline. The fact so many of Fröbenius's papers read like present day text-books on the topics which he studied is a clear indication of the importance that his work, in many different areas, has had in shaping the mathematics which is studied today. Having said that, it is also true that he made fundamental contributions to fields which had already come into existence and he did not introduce any totally new mathematical areas as some of the greatest mathematicians have done.

Haubrich gave the following overview of Fröbenius's work:

"*The most striking aspect of his mathematical practice is his extraordinary skill at calculations. In fact, Fröbenius tried to solve mathematical problems to a large extent by means of a calculative, algebraic approach. Even his analytical work was guided by algebraic and linear algebraic methods. For Fröbenius, conceptual argumentation played a somewhat secondary role. Although he argued in a comparatively abstract setting, abstraction was not an end in itself. Its advantages to him seemed to lie primarily in the fact that it can lead to much greater clearness and precision.*"

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

1.10. Problemas

1. Las siguientes condiciones sobre un grupo G son equivalentes:

   a) G es un grupo abeliano.

   b) La aplicación $\phi\colon G \to G$, $\phi(g) = g^{-1}$, es morfismo de grupos.

   c) La aplicación $\phi\colon G \to G$, $\phi(g) = g^2$, es morfismo de grupos.

   d) La aplicación $\phi\colon G \times G \to G$, $\phi(g,g') = gg'$, es morfismo de grupos.

2. Sea G un grupo. Si $a, g \in G$, se dice que aga^{-1} es el *conjugado* de g por a. La conjugación $\tau_a\colon G \to G$, $\tau_a(g) = aga^{-1}$ es un automorfismo de grupos (tales automorfismos de G reciben el nombre de *automorfismos internos*), y la aplicación $G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, es un morfismo de grupos.

3. Sea H un subconjunto finito y no vacío de un grupo G. Prueba que H es un subgrupo de G precisamente cuando $x \cdot y \in H$ para todo $x, y \in H$. ¿Sigue siendo cierto el enunciado cuando H no es finito?

4. Sea H un subconjunto no vacío de un grupo G. Prueba que H es un subgrupo de G si y solo si $xH = H$ para todo $x \in H$.

5. Determina los siguientes subgrupos:

a) El subgrupo de $\mathbb{Z}$ generado por $X = \{3,5\}$.

b) El subgrupo de $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ generado por $X := \{(2,0),(0,5)\}$ y el generado por $Y = \{(2,3),(4,5)\}$.

c) El subgrupo de S_3 generado por $X = \{(1,2),(1,3)\}$.

d) El subgrupo de $\mathbb{Q}$ generado por $X = \{1\}$, el generado por $Y = \{1/2\}$ y el generado por $Z = \{1/6, 1/8\}$.

6. Sea G un grupo de orden primo. Prueba que G es un grupo cíclico.

7. Si los únicos subgrupos de un grupo G, no trivial, son el trivial, $\{1\}$ y G, prueba que G es un grupo finito y su orden es primo.

8. Sean a, b elementos de un grupo G. Demuestra que $ord(a) = ord(bab^{-1})$. ¿Es cierto que siempre $ord(ab) = ord(ba)$?

9. Sea $\mu_n := \{z \in \mathbb{C} : z^n = 1\}$ el conjunto de las raíces n-esimas de la unidad. Prueba que

   a) μ_n es un subgrupo de $(\mathbb{C}^*, \cdot)$.

   b) μ_n es un grupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

10. Sea G un grupo abeliano y $\pi : G \to G'$ un morfismo de grupos. Si $s : G' \to G$ es un morfismo de grupos tal que $\pi \circ s = \mathrm{Id}$ (es decir, "s es una sección de π"), prueba que G es isomorfo a $\mathrm{Ker}\,\pi \times G'$.

11. Sea G' un grupo abeliano. Sea $i : G \to G'$ un morfismo de grupos. Si existe un morfismo de grupos $r : G' \to G$ tal que $r \circ i = \mathrm{Id}$ (es decir, "r es un retracto de i"), prueba que G' es isomorfo a $G \times \mathrm{Ker}\, r$.

12. Prueba que si G es un grupo cíclico finito de orden n, entonces para cada divisor d de n existe un único subgrupo $H \subseteq G$ de orden d.

13. Sea $F : S_n \to \{\pm 1\}$ un morfismo de grupos. Prueba que $F(\sigma) = 1$ para todo σ ó $F = \mathrm{sign}$.

14. Sea $F : S_n \to G$ un morfismo de grupos y supongamos que $(G, \cdot)$ es un grupo abeliano de orden impar. Prueba que $F(\sigma) = 1$ para todo $\sigma \in S_n$.

15. Sea E un espacio vectorial y $\{e_1, \ldots, e_n\}$ una base. Dada $\sigma \in S_n$, sea $\tilde{\sigma} : E \to E$ el endomorfismo lineal tal que $\tilde{\sigma}(e_i) := e_{\sigma(i)}$, para todo i. Prueba que $\det(\tilde{\sigma}) = \mathrm{sign}(\sigma)$.

16. Prueba que toda $\sigma \in A_n \subset S_n$ es producto de ciclos de orden 3.

Capítulo 2

Dominios de factorización única

2.1. Introducción

El anillo por excelencia es el anillo de los números enteros, $\mathbb{Z}$. Clásicamente la rama de las Matemáticas que estudia el anillo de los números enteros es la Aritmética, actualmente la Teoría de Números.

Hay otros anillos también muy importantes. Dado un conjunto con cierta estructura se puede considerar el anillo formado por las funciones del conjunto que respeten la estructura considerada en el conjunto. Por ejemplo, dado $\mathbb{R}^n$ podemos estudiar el anillo de las funciones continuas reales de $\mathbb{R}^n$, o el anillo de las funciones infinito diferenciables de $\mathbb{R}^n$, o el anillo $\mathbb{R}[x_1,\ldots,x_n]$ de las funciones algebraicas de $\mathbb{R}^n$. Así desde este punto de vista, la Topología es la rama de las Matemáticas que estudia los anillos de las funciones continuas reales de los espacios topológicos, la Geometría Diferencial es la rama de las Matemáticas que estudia los anillos de las funciones infinito diferenciables reales de las variedades diferenciables, la Geometría Algebraica es la rama de las Matemáticas que estudia los anillos de las funciones algebraicas de las variedades algebraicas.

En este capítulo vamos a estudiar los anillos euclídeos o más generalmente los anillos de factorización única, es decir, los anillos donde todo elemento se escribe de modo único como producto de elementos irreducibles. Se introducirán también herramientas básicas como el cociente de un anillo por un ideal y la localización de un anillo por un sistema multiplicativo.

2.2. Anillos. Cuerpos

Comencemos con una revisión rápida de la definición y propiedades elementales de los anillos.

1. Definición: Un anillo A es un conjunto dotado con dos operaciones

$$A\times A\xrightarrow{+}A,\ (a,a')\mapsto a+a',\quad A\times A\xrightarrow{\cdot}A,\ (a,a')\mapsto a\cdot a',$$

que denominamos suma y producto[1], tales que

[1] Será usual utilizar la notación $a\cdot a'=aa'$.

1. A es un grupo abeliano con respecto a la suma (luego tiene un elemento neutro, que se denota por 0, y cada $a \in A$ tiene un opuesto que se denota por $-a$).
2. La multiplicación es asociativa ($(a \cdot b) \cdot c = a \cdot (b \cdot c)$) y distributiva ($a \cdot (b + c) = a \cdot b + a \cdot c$).

   Además, solo consideraremos anillos conmutativos con unidad, es decir, cumpliendo:

3. $ab = ba$, para todo $a, b \in A$.
4. Existe un elemento $1 \in A$ tal que $a1 = 1a = a$, para todo $a \in A$.

A lo largo del libro entenderemos anillo por anillo conmutativo con unidad.

Observemos que $a \cdot 0 = 0$, porque $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Observemos también que $-1 \cdot a = -a$, porque $0 = 0 \cdot a = (1 + (-1)) \cdot a = a + (-1 \cdot a)$.

2. Ejemplos: 1. El anillo de los números enteros, $\mathbb{Z}$. El anillo de los números racionales $\mathbb{Q}$. El anillo de los números reales $\mathbb{R}$. El anillo de los números complejos, $\mathbb{C}$.

2. El anillo de funciones reales continuas, $C(X)$ de un espacio topológico X, con la suma y producto de funciones.

3. Los anillos de polinomios $\mathbb{C}[x_1, \ldots, x_n]$.

4. Dado $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotamos $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Sea A un anillo, se define el "anillo de series formales en las variables $x_1, \ldots, x_n$ con coeficientes en A", que denotamos $A[[x_1, \ldots, x_n]]$, como

$$A[[x_1, \ldots, x_n]] := \{ \sum_{\alpha \in \mathbb{N}^n} a_\alpha \cdot x^\alpha,\ a_\alpha \in A \},$$

donde dadas $s(x) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \cdot x^\alpha$, $t(x) = \sum_{\alpha \in \mathbb{N}^n} b_\alpha \cdot x^\alpha \in A[[x_1, \ldots, x_n]]$, se define

$$\begin{aligned} s(x) + t(x) &:= \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) \cdot x^\alpha \\ s(x) \cdot t(x) &:= \sum_{\alpha \in \mathbb{N}^n} \Big(\sum_{\beta + \beta' = \alpha} a_\beta \cdot b_{\beta'} \Big) \cdot x^\alpha \end{aligned}$$

3. Definición: Un elemento $a \in A$, diremos que es un divisor de cero, si existe $b \in A$, no nulo tal que $ab = 0$. Diremos que un anillo es íntegro si el único divisor de cero es el cero.

4. Ejemplos: $\mathbb{Z}$ es un anillo íntegro. Si A es un anillo íntegro entonces el anillo de polinomios con coeficientes en A, $A[x]$ es un anillo íntegro.

5. Definición: Diremos que un elemento de un anillo es invertible si tiene inverso (en el anillo con la multiplicación).

6. Definición: Diremos que un anillo es un cuerpo si todo elemento no nulo es invertible.

Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

Los cuerpos son anillos íntegros: si $a \cdot b = 0$ y $b \neq 0$, entonces $0 = a \cdot b \cdot b^{-1} = a$.

2.2.1. Anillos euclídeos

7. Definición: Un anillo íntegro A se dice que es euclídeo si existe una aplicación $\delta: A\setminus\{0\}\to\mathbb{N}$, que cumple

1. $\delta(a)\leq\delta(ab)$, para todo $a,b\in A\setminus\{0\}$.[2]

2. Para cada $a\in A$ y $b\in A$ no nulo, existen $c,r\in A$, de modo que $a=bc+r$, y r es nulo ó $\delta(r)<\delta(b)$.

8. Ejercicio: Sea (A,δ) un anillo euclídeo y $a\in A\setminus\{0\}$. Prueba:

1. a es invertible si y solo si $\delta(a)=\delta(1)$.

2. a no es invertible si y solo si $\delta(a)>\delta(1)$.

3. Sea $\delta': A\setminus\{0\}\to\mathbb{N}$, $\delta'(a):=\delta(a)-\delta(1)$, entonces (A,δ') es un anillo euclídeo y que a es invertible si y solo si $\delta'(a)=0$.

Veamos algunos ejemplos de anillos euclídeos.

9. El anillo de los números enteros: *Definimos $\delta:\mathbb{Z}\setminus\{0\}\to\mathbb{N}$, $\delta(n):=|n|$, donde $|n|=n$ si n es positivo y $|n|=-n$ si n es negativo. Por el teorema 1.3.6, es fácil comprobar que $(\mathbb{Z},\delta)$ es un anillo euclídeo.*

10. Los anillos de polinomios: *Sea A un anillo. Diremos que el grado de un polinomio con coeficientes en A*

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in A[x],\ \textit{con}\ a_n\neq 0$$

es n y denotaremos $gr(p(x))=n$.

Si A es un anillo íntegro, entonces el grado es una función aditiva, es decir, se cumple la fórmula

$$gr(p(x)q(x))=gr(p(x))+gr(q(x))\ .$$

para cada par de polinomios $p(x),q(x)\in A[x]$ (seguimos la convención: $gr(0)=-\infty$). Por tanto, si $p(x)\neq 0$ es múltiplo de $q(x)$, entonces $gr\,p(x)\geq gr\,q(x)$.

Algoritmo de división *en el anillo de polinomios: Sea $A=k$ un cuerpo. Para cada par de polinomios no nulos $p(x),q(x)\in k[x]$, existen otros dos, $c(x),r(x)$, que denominaremos* cociente *y* resto *de dividir $p(x)$ por $q(x)$, únicos con las condiciones:*

1. $p(x)=c(x)\cdot q(x)+r(x)$.

2. $gr(r(x))<gr(q(x))$.

[2] El problema 11 muestra que esta condición no es necesaria.

Demostración. Existencia: Si $\operatorname{gr} q(x) > \operatorname{gr} p(x)$ entonces $c(x) = 0$ y $r(x) = p(x)$. Supongamos $\operatorname{gr} q(x) = m \leq n = \operatorname{gr} p(x)$ y escribamos $p(x) = a_0x^n + \ldots + a_n$ y $q(x) = b_0x^m + \cdots + b_m$. Procedemos por inducción sobre $\operatorname{gr} p(x)$. Si $\operatorname{gr} p(x) = 0$, entonces $\operatorname{gr} q(x) = 0$ y $c(x) = \frac{a_0}{b_0}$ y $r(x) = 0$. Sea, pues, $\operatorname{gr}(p(x)) > 0$. El polinomio $p'(x) := p(x) - \frac{a_0}{b_0} \cdot x^{n-m} \cdot q(x)$ es de grado menor que el de $p(x)$, luego por hipótesis de inducción, existen $c'(x)$ y $r'(x)$ tales que $p'(x) = c'(x) \cdot q(x) + r'(x)$ y $gr(r'(x)) < gr(q(x))$. Entonces, $c(x) := c'(x) + \frac{a_0}{b_0} \cdot x^{n-m}$ y $r(x) := r'(x)$ cumplen lo exigido.

Unicidad: Al lector. □

Por lo tanto, $(k[x], \operatorname{gr})$ *es un anillo euclídeo.*

11. El anillo de los enteros de Gauss: *Sea* $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$. $\mathbb{Z}[i]$ *es un anillo (subanillo de* $\mathbb{C}$*) y se denomina el anillo de los enteros de Gauss.* $\mathbb{Z}[i]$ *con la aplicación*

$$\delta : \mathbb{Z}[i] \to \mathbb{N}, \quad \delta(a + bi) := (a + bi) \cdot (a - bi) = a^2 + b^2$$

es un anillo euclídeo:

Dados $z, z' \in \mathbb{Z}[i]$ no nulos se cumple que $\delta(zz') = \delta(z)\delta(z') \geq \delta(z)$. Dado un número complejo $a + bi \in \mathbb{C}$, denotemos $|a + bi| = a^2 + b^2 \in \mathbb{R}$. Consideremos el número complejo $z/z' \in \mathbb{C}$ y consideremos un entero de Gauss $c \in \mathbb{Z}[i]$ lo más cercano posible a z/z'. Tenemos que $|z/z' - c| < 1$. Sea $r := z - z'c$, si $r \neq 0$ entonces

$$\delta(r) = \delta(z - z'c) = |z'(z/z' - c)| = |z'||z/z' - c| < |z'|$$

Tenemos, pues, que $z = z'c + r$ con $r = 0$ ó $\delta(r) < \delta(z')$.

2.3. Ideales de un anillo. Dominios de ideales principales

1. Definición: Un subconjunto $I \subseteq A$ diremos que es un ideal del anillo A si es un subgrupo para la suma y cumple que $a \cdot i \in I$, para todo $a \in A$ y todo $i \in I$.

Los subconjuntos $\{0\}$ y A son ideales del anillo A.

Dado $a \in A$, el conjunto $a \cdot A := \{a \cdot b \in A, \forall b \in A\}$ es un ideal de A. Si $I \subseteq \mathbb{Z}$ es un ideal, entonces existe un $n \in \mathbb{Z}$ tal que $I = n \cdot \mathbb{Z}$ (por el teorema 1.3.7).

Un anillo es un cuerpo si y solo si los únicos ideales del anillo son el (0) y todo el anillo: Si A es un cuerpo e $I \subset A$ es un ideal no nulo, entonces existe $a \in I$ no nulo; como $a \cdot A = A$ tendremos que $I = A$. Recíprocamente, si A no contiene más ideales que $\{0\}$ y A, dado $a \in A$ no nulo tendremos que $a \cdot A = A$, lo que implica que $1 \in a \cdot A$, luego a es invertible.

2. Ejercicio: Sea X un conjunto y $\operatorname{Aplic}(X, \mathbb{R})$ el conjunto de las aplicaciones de X en $\mathbb{R}$. Con la suma y producto ordinarios de funciones $\operatorname{Aplic}(X, \mathbb{R})$ es un anillo. Sea $Y \subset X$ un subconjunto, prueba que $\{f \in \operatorname{Aplic}(X, \mathbb{R}) : f(y) = 0, \forall y \in Y\}$ es un ideal de $\operatorname{Aplic}(X, \mathbb{R})$.

La intersección de ideales es un ideal. Dado un subconjunto $F \subseteq A$, denotaremos por (F) al ideal mínimo de A que contiene a F (que es la intersección de todos los ideales que contienen a F). Diremos que el ideal (F) está generado por F. Explícitamente $(F) = \{a \in A : a = \sum_{i=0}^{n} a_i f_i \text{ con } f_i \in F, a_i \in A \text{ y } n \in \mathbb{N} \text{ cualesquiera}\}$. Dado $a \in A$, tenemos que $(a) = aA$. Dados dos ideales I_1 e I_2 de A, llamaremos suma de los dos ideales, que denotaremos por $I_1 + I_2$, al ideal de A definido por $I_1 + I_2 := \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$, que es el mínimo ideal de A que contiene a I_1 y I_2.

3. Definición: Sea A un anillo. Diremos que un ideal $I \subseteq A$ es principal si existe $a \in A$ tal que $I = aA$. Diremos que un anillo es un dominio de ideales principales si es un anillo íntegro cuyos ideales son principales.

$\mathbb{Z}$ es un dominio de ideales principales.

4. Proposición: *Los anillos euclídeos son dominios de ideales principales.*

Demostración. Sea (A, δ) un anillo euclídeo e $I \subset A$ un ideal no nulo. Sea $i \in I$ un elemento no nulo tal que $\delta(i) = \min\{\delta(j)\}_{j \in I \setminus \{0\}}$. Veamos que $I = i \cdot A$: Dado $j \in I$ no nulo, existen $c, r \in A$ de modo que $j = c \cdot i + r$ y $r = 0$ ó $\delta(r) < \delta(i)$. Observemos que $r \in I$, luego no es posible que $\delta(r) < \delta(i)$. En conclusión, $j = c \cdot i$. Por tanto, $I = i \cdot A$.

□

El ideal $\mathfrak{p} = (2, x_1)$ del anillo $\mathbb{Z}[x_1, \ldots x_n]$ no es principal: un generador de $\mathfrak{p}$ sería un divisor de 2 y éstos son ± 1 y ± 2, y $1 \cdot \mathbb{Z}[x_1, \ldots, x_n]$ y $2 \cdot \mathbb{Z}[x_1, \ldots, x_n]$ son ideales distintos de $\mathfrak{p}$. En consecuencia, los anillos $\mathbb{Z}[x_1, \ldots, x_n]$ no son dominios de ideales principales.

Análogamente, si k es un cuerpo, el ideal (x_1, x_2) del anillo $k[x_1, \ldots, x_n]$ no es principal, así que los anillos $k[x_1, \ldots, x_n]$ no son dominios de ideales principales (para $n > 1$).

2.3.1. Morfismo de anillos. Cociente por un ideal

5. Definición: Una aplicación $f : A \to B$ entre los anillos A y B, diremos que es un morfismo de anillos si cumple

1. $f(a + a') = f(a) + f(a')$, para todo $a, a' \in A$.
2. $f(aa') = f(a)f(a')$, para todo $a, a' \in A$.
3. $f(1) = 1$.

6. Ejemplos: La aplicación $\mathbb{C}[x] \to \mathbb{C}$, $p(x) \mapsto p(33)$, es un morfismo de anillos. Dada una aplicación continua $\phi : X \to Y$ entre espacios topológicos, la aplicación inducida $\tilde{\phi} : C(Y) \to C(X)$, $f \mapsto f \circ \phi$ es un morfismo de anillos.

La composición de morfismos de anillos es un morfismo de anillos. La imagen de un morfismo de anillos $f : A \to B$, $\operatorname{Im} f$, es un subanillo de B, es decir, un subconjunto de B que con las operaciones de B es anillo y la unidad de B pertenece al subanillo.

El núcleo de un morfismo de anillos f, $\operatorname{Ker} f := \{a \in A : f(a) = 0\}$, es un ideal. La antimagen por un morfismo de anillos de un ideal es un ideal. Si un morfismo de anillos es epiyectivo la imagen de un ideal es un ideal.

Sea $I \subseteq A$ un ideal. Como I es un subgrupo (aditivo) de A, podemos considerar el grupo cociente A/I, donde

$$A/I := \{\bar{a} \text{ (donde } \bar{a} := a + I), \forall\, a \in A\},$$

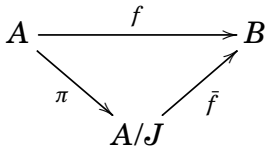
y $\bar{a} + \bar{b} := \overline{a+b}$. Recordemos que $\bar{a} = \bar{b}$ si y solo si $a - b \in I$. Podemos definir en A/I la operación "producto", $\bar{a} \cdot \bar{a'} := \overline{a \cdot a'}$, que dota a A/I de estructura de anillo (compruébese), y es la única estructura de anillo que podemos definir en A/I, de modo que el morfismo de paso al cociente $\pi : A \to A/I$, $a \mapsto \bar{a}$, sea un morfismo de anillos.

7. Ejemplo: Consideremos el ideal $9 \cdot \mathbb{Z} \subseteq \mathbb{Z}$. En $\mathbb{Z}/9 \cdot \mathbb{Z}$ tenemos que $\overline{10^n} = \overline{10}^n = \bar{1}^n = \bar{1}$. Por tanto, dado un número natural cualquiera, por ejemplo $7836 \in \mathbb{N}$, tenemos que

$$\overline{7836} = \overline{7 \cdot 10^3 + 8 \cdot 10^2 + 3 \cdot 10 + 6} = \overline{7} \cdot \overline{10^3} + \overline{8} \cdot \overline{10^2} + \overline{3} \cdot \overline{10} + \overline{6} = \overline{7} + \overline{8} + \overline{3} + \overline{6} = \overline{7 + 8 + 3 + 6}$$

Por tanto, 7836 es divisible por 9 (es decir, $\overline{7836} = \bar{0}$) si y solo si $7 + 8 + 3 + 6$ es divisible por 9 (es decir, $\overline{7 + 8 + 3 + 6} = \bar{0}$). En general, un número natural $n = n_1 n_2 \ldots n_r$, escrito en base decimal, es divisible por nueve si y solo si la suma de sus cifras, $n_1 + \cdots + n_r$ es divisible por nueve.

Sea $f : A \to B$ un morfismo de anillos. Si $J \subseteq A$ es un ideal incluido en $\operatorname{Ker} f$, entonces existe un único morfismo de anillos $\bar{f} : A/J \to B$ (definido por $\bar{f}(\bar{a}) = f(a)$) de modo que el diagrama



es conmutativo, siendo π el morfismo de paso al cociente, $\pi(a) = \bar{a}$. Como consecuencia del teorema de isomorfía para morfismos de grupos obtenemos el siguiente teorema.

8. Teorema de isomorfía: *Sea $f : A \to B$ un morfismo de anillos. La aplicación*

$$\bar{f} : A/\operatorname{Ker} f \to \operatorname{Im} f,\ \bar{f}(\bar{a}) := f(a)$$

es un isomorfismo de anillos.

9. Ejemplo: El cuerpo de los números complejos es isomorfo a $\mathbb{R}[x]/(x^2 + 1)$: Consideremos el morfismo de anillos $f : \mathbb{R}[x] \to \mathbb{C}$, $f(p(x)) := p(i)$. El morfismo f es epiyectivo. Sea $\operatorname{Ker} f = (p(x))$. Obviamente, $x^2 + 1 \in \operatorname{Ker} f$, luego $p(x)$ ha de dividir a $x^2 + 1$. Como no existe ningún polinomio de grado 1 en $\operatorname{Ker} f$, concluimos que $\operatorname{Ker} f = (x^2 + 1)$ y por el teorema de isomorfía $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

10. Ejemplo: Sea K un cuerpo, $k \subseteq K$ un subcuerpo, y sea $\alpha \in K$. Se denota $k[\alpha] := \{p(\alpha) \in K$, para todo $p(x) \in k[x]\}$. Consideremos el morfismo $\phi : k[x] \to K$, $\phi(p(x)) := p(\alpha)$. Se cumple que ϕ es un morfismo de anillos y $\operatorname{Im} \phi = k[\alpha]$. $\operatorname{Ker} \phi$ es un ideal de

$k[x]$. Si $\mathrm{Ker}\,\phi \neq \{0\}$, entonces está generado por el polinomio $p(x)$ no nulo mónico[3] de grado más pequeño tal que $p(\alpha)=0$. Por tanto, por el teorema de isomorfía

$$k[\alpha]=\begin{cases} k[x], & \text{si no existe ningún polinomio no nulo } p(x) \text{ tal que } p(\alpha)=0.\\ k[x]/(p(x)), & \text{donde } p(x)\in k[x] \text{ es el pol. no nulo mónico mín. anulador de } \alpha.\end{cases}$$

Observemos que el polinomio mínimo anulador de α, $p(x)$, es irreducible (es decir, no es producto de dos polinomios de grado menor que el de $p(x)$), porque si no lo es entonces $p(x)=p_1(x)\cdot p_2(x)$, con $\mathrm{gr}(p_1(x)), \mathrm{gr}(p_2(x)) < \mathrm{gr}(p(x))$ y $p_1(x)$ ó $p_2(x)$ anula a α. Recíprocamente, si $p(x)$ es mónico, anula a α y es irreducible, entonces es el polinomio mónico mínimo anulador de α.

$k[x]/(p(x))$ es un k-espacio vectorial de base $\{\bar{1},\bar{x},\cdots,\bar{x}^{n-1}\}$, con $n=\mathrm{gr}(p(x))$: En efecto dado $\overline{q(x)}\in k[x]/(p(x))$, como $q(x)=c(x)\cdot p(x)+r(x)$, con $\mathrm{gr}(r(x))<n$, tenemos que $\overline{q(x)}=\overline{r(x)}$. Como $r(x)$ es combinación lineal de $1,\cdots,x^{n-1}$, $\{\bar{1},\bar{x},\cdots,\bar{x}^{n-1}\}$ es un sistema generador. Veamos que $\bar{1},\bar{x},\cdots,\bar{x}^{n-1}$ son linealmente independientes. Si

$$0=\sum_{i=0}^{n-1}\lambda_i\bar{x}^i=\overline{\sum_{i=0}^{n-1}\lambda_i x^i}.$$

Entonces, $\sum_{i=0}^{n-1}\lambda_i x^i$ es múltiplo de $p(x)$, lo cual es imposible, salvo que $\sum_{i=0}^{n-1}\lambda_i x^i=0$, es decir, $\lambda_i=0$ para todo i.

Consideremos la inclusión $\mathbb{Q}\subset\mathbb{C}$ y $\sqrt[3]{2}\in\mathbb{C}$. El polinomio con coeficientes racionales mínimo anulador de $\sqrt[3]{2}$ es x^3-2, porque es irreducible ya que si no lo es x^3-2 tendría raíces en $\mathbb{Q}$, que es imposible. Por tanto,

$$\mathbb{Q}[x]/(x^3-2)=\mathbb{Q}[\sqrt[3]{2}].$$

Por tanto, $\mathbb{Q}[\sqrt[3]{2}]$ es un $\mathbb{Q}$-espacio vectorial de dimensión 3, de base $\{1,\sqrt[3]{2},\sqrt[3]{2}^2\}$.

Dados dos ideales $I_1,I_2\subset A$, denotamos por I_1+I_2 el mínimo ideal de A que contiene a I_1 e I_2. Puede comprobarse que

$$I_1+I_2=\{i_1+i_2,\ \forall i_1\in I_1,\forall i_2\in I_2\}.$$

11. Teorema chino de los restos: *Sea A un anillo e $I_1,I_2\subseteq A$ dos ideales tales que $I_1+I_2=A$. Entonces, el morfismo natural*

$$A/(I_1\cap I_2)\to A/I_1\times A/I_2,\quad \bar{a}\mapsto(\bar{a},\bar{a})$$

es un isomorfismo

Demostración. El núcleo del morfismo $f: A\to A/I_1\times A/I_2$, $f(a)=(\bar{a},\bar{a})$ es claramente $I_1\cap I_2$. Por el teorema de isomorfía, solo nos falta probar que es epiyectivo. Sea $(\bar{a},\bar{b})\in A/I_1\times A/I_2$. Observemos que en A/I_2, $A/I_2=\overline{a+I_1+I_2}=\overline{a+I_1}$. Por tanto, existe $i_1\in I_1$ de modo que $\overline{a+i_1}=\bar{b}$ en A/I_2. Por tanto, $f(a+i_1)=(\overline{a+i_1},\overline{a+i_1})=(\bar{a},\bar{b})$. □

Dados dos ideales $I_1,I_2\subset A$, denotamos por $I_1\cdot I_2$ el mínimo ideal de A que contiene al conjunto $\{i_1\cdot i_2,\ \forall i_1\in I_1,\forall i_2\in I_2\}$. Si $I_1+I_2=A$ entonces $I_1\cap I_2=I_1\cdot I_2$: Evidentemente $I_1\cdot I_2\subseteq I_1\cap I_2$. Sea $i_1\in I_1$ e $i_2\in I_2$, tales que $i_1+i_2=1$. Dado $i\in I_1\cap I_2$, se cumple que $i=i\cdot 1=i\cdot i_1+i\cdot i_2\in I_1\cdot I_2$. Por tanto, $I_1\cap I_2\subseteq I_1\cdot I_2$.

[3] Se dice que un polinomio $p(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ de grado n es mónico si $a_0=1$.

2.3.2. Ideales primos. Ideales maximales

12. Definición: Un ideal $\mathfrak{p} \underset{\neq}{\subset} A$, diremos que es un ideal primo de A, si cumple que si $ab \in \mathfrak{p}$ entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

13. Proposición: *Un ideal $\mathfrak{p} \underset{\neq}{\subset} A$ es un ideal primo si y solo si $A/\mathfrak{p}$ es un anillo íntegro.*

Demostración. Supongamos que $\mathfrak{p} \subset A$ es un ideal primo. Si $\bar{a} \cdot \bar{a'} = 0$ en $A/\mathfrak{p}$ entonces $\overline{a \cdot a'} = 0$, luego $a \cdot a' \in \mathfrak{p}$. Por tanto, o $a \in \mathfrak{p}$ o $a' \in \mathfrak{p}$, luego o $\bar{a} = 0$ o $\bar{a'} = 0$. En conclusión $A/\mathfrak{p}$ es íntegro.

Recíprocamente, supongamos que $A/\mathfrak{p}$ es íntegro. Si $a \cdot a' \in \mathfrak{p}$, entonces $\overline{a \cdot a'} = 0$ en $A/\mathfrak{p}$. Por tanto, $\bar{a} \cdot \bar{a'} = 0$, luego o $\bar{a} = 0$ o $\bar{a'} = 0$. Es decir, o $a \in \mathfrak{p}$ o $a' \in \mathfrak{p}$. En conclusión, $\mathfrak{p}$ es un ideal primo. □

14. Ejercicio: Sea $\mathfrak{p} = (2, x) \subset \mathbb{Z}[x, y]$. Prueba que $\mathbb{Z}[x, y]/\mathfrak{p} \simeq \mathbb{Z}/2\mathbb{Z}[y]$. Prueba que $\mathfrak{p}$ es un ideal primo.

15. Definición: Diremos que un ideal $\mathfrak{m} \underset{\neq}{\subset} A$ es maximal si los únicos ideales que contienen a $\mathfrak{m}$ son $\mathfrak{m}$ y A.

16. Proposición: *En todo anillo $A \neq 0$ existen ideales maximales.*

Demostración. La demostración es una aplicación típica del lema de Zorn (que puede evitarse en anillos noetherianos). Sea X el conjunto de los ideales de A, distintos de A. En X podemos definir una relación de orden: decimos que un ideal I es menor o igual que otro I' cuando $I \subseteq I'$. Observemos que toda cadena de ideales, distintos de A tiene una cota superior: la unión de los ideales de la cadena (que es distinto de A, pues el 1 no está en ninguno de ellos, ni por tanto en la unión). El lema de Zorn nos dice que existen elementos de X maximales, es decir, existen ideales maximales. □

17. Ejercicio: Se dice que un ideal primo es minimal si no contiene estrictamente ningún ideal primo. Prueba que en todo anillo $A \neq 0$ existen ideales primos minimales.

18. Lema: *Sea $\pi : A \to A/I$ el morfismo de paso al cociente. Las aplicaciones*

$$\begin{array}{rcl} \left\{\begin{array}{l}\text{Ideales de } A \\ \text{que contienen a } I\end{array}\right\} & = & \{\text{Ideales de } A/I\} \\ J & \longmapsto & \pi(J) \\ \pi^{-1}(J') & \longleftarrow & J' \end{array}$$

son inversas entre sí (y conservan inclusiones).

Demostración. Observemos que $\pi(\pi^{-1}(J')) = J'$ porque π es epiyectiva, y $\pi^{-1}(\pi(J)) = J + I = J$. □

19. Corolario: *Todo ideal $I \underset{\neq}{\subset} A$ está incluido en un ideal maximal.*

Demostración. Por el lema anterior, los ideales maximales de A que contienen a I se corresponden con los ideales maximales de A/I, que no es vacío por la proposición anterior. □

Un elemento $a \in A$ es invertible si y solo si $(a) = A$. Por tanto, $a \in A$ es invertible si y solo si no está incluido en ningún ideal maximal (suponemos $A \neq 0$).

20. Proposición: *Un ideal $\mathfrak{m} \subsetneq A$ es maximal si y solo si $A/\mathfrak{m}$ es un cuerpo. En particular, por la proposición 2.3.13, los ideales maximales son ideales primos.*

Demostración. $A/\mathfrak{m}$ es cuerpo si y solo si el único ideal maximal es el (0). Que equivale a decir que el único ideal maximal de A que contiene a $\mathfrak{m}$ es $\mathfrak{m}$, es decir, $\mathfrak{m}$ es maximal. □

21. Definiciones: Sea A un anillo íntegro y $a \in A$. Se dice que a es propio si no es nulo ni invertible. Se dice que a es irreducible si es propio y no descompone en producto de dos elementos propios. Se dice que a es primo (en A) si es propio y (a) es un ideal primo.

22. Nota: Observemos que decimos que -5 es un elemento primo de $\mathbb{Z}$.

23. Proposición: *Sea A un anillo íntegro. Si $a \in A$ es primo, entonces es irreducible.*

Demostración. Si $a = b \cdot c$, entonces $b \in (a)$ (o $c \in (a)$) porque (a) es un ideal primo. Luego, $b = ad$ para cierto $d \in A$. Por tanto, $a = bc = adc$ y $dc = 1$. Es decir, c es invertible y a es irreducible. □

24. Proposición: *Sea p un elemento no nulo de un dominio de ideales principales A. Las siguientes condiciones son equivalentes:*

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

Demostración. 3. $\Rightarrow$ 2. Obvio.

2. $\Rightarrow$ 1. Es consecuencia de 2.3.23.

1. $\Rightarrow$ 3. Si $pA \subseteq I = aA \subsetneq A$, entonces existe $b \in A$ tal que $ab = p$. Luego, b es invertible y $I = pA$. En conclusión, pA es maximal.

□

2.3.3. Congruencias de Wilson y Fermat

25. Notaciones: Escribiremos $m \equiv m' \, mod \, n$ y leeremos m es congruente con m' módulo n, cuando $\bar{m} = \bar{m'}$ en $\mathbb{Z}/n\mathbb{Z}$ (es decir, el resto de dividir m por n coincide con el resto de dividir m' por n).

Dado un anillo A, denotaremos A^* al grupo (con la multiplicación) formado por los elementos invertibles de A.

Si $p \in \mathbb{Z}$ es un número primo entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, porque $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ por la proposición 2.3.24

26. Congruencia de Wilson: *Si p es un número natural primo, entonces:*

$$(p-1)! \equiv -1 \, mod \, p.$$

Demostración. $(p-1)! \, mod \, p$ es el producto de todos los elementos del grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Si $\bar{m} \in (\mathbb{Z}/p\mathbb{Z})^*$ no es igual a su inverso, entonces en este producto ambos se cancelan (dando 1) luego en el producto mencionado solo permanecen aquellos $\bar{m}$ que verifiquen que son igual a su inverso. Ahora bien, $1 = \bar{m} \cdot \bar{m} = \bar{m}^2$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\bar{m}$ es raíz del polinomio $x^2 - \bar{1} \in \mathbb{Z}/p\mathbb{Z}[x]$. Como $x^2 - \bar{1} = (x+\bar{1}) \cdot (x-\bar{1})$, $\bar{m}$ es igual a su inverso si y solo si $\bar{m} = \pm\bar{1}$. Por tanto, $(p-1)! = 1 \cdot (-1) = -1$ en $\mathbb{Z}/p\mathbb{Z}$. □

27. Congruencia de Fermat: *Si p es un número natural primo y m no es divisible por p, entonces*

$$m^{p-1} \equiv 1 \, mod \, p.$$

Demostración. Es consecuencia de 1.6.4, aplicado al caso $G = (\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ y $g = \bar{m}$. □

2.4. Dominios de factorización única

1. Definición: Un anillo íntegro se dice que es un dominio de factorización única si todo elemento propio (no nulo ni invertible) del anillo es producto de elementos irreducibles, de modo único salvo orden de los factores y multiplicación de éstos por invertibles. DFU significará dominio de factorización única.

En la demostración de que todo número natural es producto de irreducibles es esencial observar que toda sucesión de números naturales $n_1, n_2, \ldots, n_r, \ldots$ tal que n_{i+1} divide a n_i estabiliza, es decir, existe m tal que $n_m = n_{m+1} = n_{m+2} = \cdots$. Para demostrar la unicidad es esencial probar que los números naturales irreducibles son los números (naturales) primos.

Diremos que una cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ estabiliza si existe m, tal que $I_m = I_{m+1} = I_{m+2} = \cdots$.

2. Lema: *Sea A un anillo íntegro y $a, b \in A$. Entonces, $(a) = (b)$ si y solo si $a = b \cdot i$ para cierto invertible $i \in A$.*

Demostración. $\Rightarrow$) Si $(a)=(b)$ existen $i,i' \in A$ tales que $a=bi$ y $b=ai'$. Por tanto, $a=ai'i$. Como A es íntegro, $1=ii'$, luego i es invertible.

□

3. Teorema de descomposición única en factores irreducibles: *Sea A un anillo íntegro. A es un dominio de factorización única si y solo si toda cadena ascendente de ideales principales estabiliza y todo elemento irreducible es primo.*

Demostración. $\Rightarrow$) Si $a=p_1\cdots p_r$ (p_i irreducibles para todo i) y $aA \subsetneq bA$ entonces reordenando los factores $b=p_1\cdots p_s\cdot inv$ con $s<r$. Ahora, es claro que toda cadena ascendente de ideales principales es estable.

Sea $a \in A$ irreducible. Si $b\cdot c \in (a)$, entonces existe $d \in A$ tal que $bc=ad$. Sea $b=b_1\cdots b_r$, $c=c_1\cdots c_s$ y $d=d_1\cdots d_t$ las descomposiciones en factores irreducibles de b,c,d. Entonces,

$$b_1\cdots b_r\cdot c_1\cdots c_s = a\cdot d_1\cdots d_t.$$

Como A es un dominio de factorización única, a ha de coincidir, salvo multiplicación por un invertible, con algún b_i o algún c_j. Luego, a divide a b, es decir. $b \in (a)$; o a divide a c, es decir, $c \in (a)$. En conclusión, (a) es un ideal primo.

$\Leftarrow$) Empecemos probando que a todo elemento $a \in A$ lo divide algún elemento irreducible: Si a no es irreducible entonces $a=a_1\cdot b_1$, a_1,b_1 elementos propios. Si a_1 no es irreducible, entonces $a_1=a_2\cdot b_2$, con a_2,b_2 elementos propios. Así sucesivamente, vamos obteniendo una cadena de ideales principales $(a)\subsetneq(a_1)\subsetneq(a_2)\subsetneq\dots$ que ha de ser finita y terminará cuando a_n sea irreducible, para cierto n. Con lo que tenemos un irreducible, a_n, que divide a a.

Ahora ya, sea a_1 irreducible que divide a a y escribamos $a=a_1\cdot b_1$. Si b_1 no es irreducible sea a_2 irreducible, que divide a b_1 y escribamos $a=a_1\cdot b_1=a_1\cdot a_2\cdot b_2$. Así sucesivamente, vamos obteniendo la cadena $(a)\subsetneq(b_1)\subsetneq(b_2)\subsetneq\dots$ que ha de ser finita y terminará cuando b_n sea irreducible. En tal caso, $a=a_1\cdots a_{n-1}\cdot b_n$ que es producto de irreducibles.

Sean $p_1\cdots p_n=q_1\cdots q_m$ dos descomposiciones en factores irreducibles. Entonces, q_1 divide algún factor p_i, luego coincide con él (salvo multiplicación por un invertible). Reordenando los factores podemos decir que $p_1=q_1$ (salvo invertibles). Simplificando la igualdad original tenemos $p_2\cdots p_n=q_2\cdots q_m$ (salvo multiplicación por un invertible). Razonando con q_2 como hemos hecho 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 orden y factores invertibles).

□

4. Teorema: *Los dominios de ideales principales son dominios de factorización única.*

Demostración. Si $p \in A$ es irreducible entonces es primo, por la proposición 2.3.24. Sea $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$ una cadena ascendente de ideales. Sea $I=\cup_{i=1}^{\infty} I_i$, que es un ideal de A, luego $I=a\cdot A$. Sea I_m tal que $a\in I_m$, entonces $I=I_m=I_{m+1}=\cdots$. Por el teorema 2.4.3, hemos terminado. □

5. Corolario: *Los anillos euclídeos son dominios de factorización única.*

Demostración. Recordemos que los anillos euclídeos son dominios de ideales principales (ver 2.3.4). □

2.4.1. Máximo común divisor

6. Definición: Se dice que dos elementos de un anillo íntegro son primos entre sí si no existe un elemento propio que los divida a los dos.

Sea A un dominio de factorización única, $a,b \in A$ y escribamos $a = u \cdot p_1^{n_1} \cdots p_r^{n_r}$, $b = v \cdot p_1^{m_1} \cdots p_r^{m_r}$, con u,v invertibles, $n_i, m_i \geq 0$ y $p_1,\ldots,p_r$ irreducibles y primos entre sí. Definimos (salvo multiplicación por invertibles) el máximo común divisor de a y b, que denotaremos $m.c.d.(a,b)$ y el mínimo común múltiplo de a y b, que denotaremos $m.c.m.(a,b)$ como sigue:

$$m.c.d.(a,b) := p_1^{\text{mín}(n_1,m_1)} \cdots p_r^{\text{mín}(n_r,m_r)}$$
$$m.c.m.(a,b) := p_1^{\text{máx}(n_1,m_1)} \cdots p_r^{\text{máx}(n_r,m_r)}$$

Observemos que $m.c.d.(a,b)$ divide á a y b y si m divide a a y b, entonces m divide a $m.c.d.(a,b)$. Estas dos propiedades caracterizan al máximo común divisor, porque si d las cumple entonces d divide a $m.c.d.(a,b)$ y recíprocamente, luego salvo multiplicación por un invertible d es igual a $m.c.d.(a,b)$.

Observemos que $m.c.m.(a,b)$ es múltiplo de a y b y si m es múltiplo de a y b, entonces m es múltiplo de $m.c.m.(a,b)$. Estas dos propiedades caracterizan al mínimo común múltiplo.

7. Teorema: *Un anillo A es DIP (dominio de ideales principales) si y solo si es DFU (dominio de factorización única) y todo ideal primo no nulo es maximal.*

Demostración. $\Rightarrow$) Es consecuencia del teorema 2.4.4 y la proposición 2.3.24.

$\Leftarrow$) Sea $\mathfrak{p}$ un ideal primo no nulo. Dado $0 \neq a \in \mathfrak{p}$, tenemos que $a = p_1 \cdots p_r$, con p_i irreducibles, luego algún irreducible $p_i \in \mathfrak{p}$, luego $(p_i) = \mathfrak{p}$. Si $a,b \in A$, no nulos, son primos entre sí, entonces (a,b) no está incluido en ningún ideal primo, luego $(a,b) = A$. Dados $a,b \in A$ no nulos, tenemos que $a = m.c.d(a,b) \cdot c$ y $b = m.c.d(a,b) \cdot d$ para ciertos $c,d \in A$ y

$$(a,b) = (m.c.d(a,b) \cdot c, m.c.d(a,b) \cdot d) = m.c.d(a,b) \cdot (c,d) = m.c.d(a,b) \cdot A.$$

Dado un ideal I no nulo y distinto de A, sea $a = p_1 \cdots p_r \in I$ con p_i irreducibles con r mínimo posible. Dado $b \in I$ no nulo, tenemos que $m.c.d(a,b) \in (a,b) \subseteq I$ y divide a a, luego $m.c.d.(a,b) = a \cdot inv$. En conclusión, $b \in (a)$ y $I = (a)$.

□

Si A es un dominio de ideales principales y $a,b \in A$, entonces $aA + bA = dA$, siendo d "el máximo común divisor de a y b": Si c divide á a y b entonces divide á d y obviamente d divide á a y b. Igualmente, el mínimo común múltiplo de a y b es el generador del ideal $aA \cap bA$.

8. Identidad de Bézout: *Sea A un dominio de ideales principales y sean $a, b \in A$. Sea d el máximo común divisor de a y b. Existen elementos $\alpha, \beta \in A$ tales que*

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

9. Algoritmo de Euclides: Este algoritmo nos permite calcular en anillos euclídeos el máximo común divisor de dos elementos del anillo. Dados $a_1, a_2 \in A$ definimos por recurrencia a_{i+1}, como el resto de dividir a_{i-1} por a_i. Entonces, escribimos

$$\begin{aligned} a_1 &= a_2 c_1 + a_3 \\ a_2 &= a_3 c_2 + a_4 \\ a_3 &= a_4 c_3 + a_5 \\ &\cdots \\ a_{s-2} &= a_{s-1} c_{s-2} + a_s \end{aligned}$$

y terminamos cuando s sea el primero tal que $a_s = 0$.

Observemos que d divide á a_1 y a_2 si y solo si divide a a_2 y a_3, si y solo si ... divide a a_{s-2} y a_{s-1}, si y solo si divide a a_{s-1}. Luego, $m.c.d(a_1, a_2) = a_{s-1}$ (único salvo multiplicación por invertibles).

Además, el algoritmo de Euclides nos permite calcular λ, μ tales que $\lambda \cdot a_1 + \mu \cdot a_2 = m.c.d(a_1, a_2)$: Sabemos expresar a_3 como combinación A-lineal de a_1 y a_2, luego sabemos expresar a_4 como combinación A-lineal de a_1 y a_2, y así sucesivamente sabremos expresar a_{s-1} como combinación A-lineal de a_1 y a_2.

10. Sean $n, m \in \mathbb{Z}$ primos entre sí (luego $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ y $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$). Por el teorema chino de los restos se tiene el isomorfismo

$$\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \bar{r} \mapsto (\bar{r}, \bar{r})$$

Calculemos el morfismo inverso: Sabemos calcular $\lambda, \mu \in \mathbb{Z}$ de modo que $\lambda \cdot n + \mu \cdot m = 1$. Luego, $\lambda \cdot n \mapsto (\bar{0}, \bar{1})$ y $\mu \cdot m \mapsto (\bar{1}, \bar{0})$. Luego, el morfismo $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/nm\mathbb{Z}$, $(\bar{r}, \bar{s}) \mapsto \overline{r \cdot \mu \cdot m + s \cdot \lambda \cdot n}$ es el morfismo inverso buscado.

11. Calculemos las soluciones enteras de la siguiente ecuación diofántica (es decir, ecuación con coeficientes enteros),

$$2000x - 266y = -4.$$

Primero calculemos mediante el algoritmo de Euclides, $n, m \in \mathbb{Z}$, tales que

$$2000n + 266 \cdot (-m) = m.c.d(2000, 266).$$

a. $2000 = 7 \cdot 266 + 138$. b. $266 = 1 \cdot 138 + 128$. c. $138 = 1 \cdot 128 + 10$. d. $128 = 12 \cdot 10 + 8$ e. $10 = 1 \cdot 8 + 2$. Luego, $m.c.d(2000, 266) = 2$. Lo cual era evidente, pero ahora sabremos calcular n y m: $2 = 10 - 1 \cdot 8 = 10 - 1 \cdot (128 - 12 \cdot 10) = -128 + 13 \cdot 10 = -128 + 13(138 - 128) = 13 \cdot 138 - 14 \cdot 128 = 13 \cdot 138 - 14(266 - 138) = -14 \cdot 266 + 27 \cdot 138 = -14 \cdot 266 + 27(2000 - 7 \cdot 266) = 27 \cdot 2000 - 203 \cdot 266$.

Por tanto, una solución particular de nuestro sistema de ecuaciones diofánticas es $x_0 = -2 \cdot 27 = -54$, $y_0 = -2 \cdot 203 = -406$. Las soluciones de la ecuación homogénea $2000x - 266y = 0$ son las soluciones de $1000x - 133y = 0$, que son $x = n \cdot 133$, $y = n \cdot 1000$. Todas las soluciones de nuestro sistema de ecuaciones diofánticas son

$$\begin{cases} x = -54 + n \cdot 133 \\ y = -406 + n \cdot 1000 \end{cases}$$

2.4.2. Congruencia de Euler

12. Proposición: *El elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es un generador del grupo $(\mathbb{Z}/n\mathbb{Z}, +)$ si y solo m es primo con n.*

Demostración. Consideremos el epimorfismo natural $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(z) = \bar{z}$. Es claro que $\pi^{-1}(\langle \bar{m} \rangle) = m\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$, donde r es el máximo común divisor de m y n. Por otra parte, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$, es decir, $\langle \bar{m} \rangle = \mathbb{Z}/n\mathbb{Z}$, si y solo $\pi^{-1}(\langle \bar{m} \rangle) = \mathbb{Z}$. Por tanto, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y solo si $r = 1$. □

Así pues, si $G = \langle g \rangle$ es un grupo cíclico de orden $n > 0$, entonces g^m es un generador de G si y solo si m y n son primos entre sí.

13. Proposición: *$\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*$ si y solo si m es primo con n.*

Demostración. Un elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es invertible si y solo si existe $\bar{m}' \in \mathbb{Z}/n\mathbb{Z}$ tal que $\bar{m}' \cdot \bar{m} = \bar{1}$, para esto es necesario y suficiente que exista m' tal que $m' \cdot \bar{m} = \bar{1}$, o equivalentemente, $\mathbb{Z} \cdot \bar{m} = \mathbb{Z}/n\mathbb{Z}$. Es decir, $\bar{m}$ es un invertible de $\mathbb{Z}/n\mathbb{Z}$ si y solo si $\bar{m}$ genera el grupo aditivo $\mathbb{Z}/n\mathbb{Z}$. Por 2.4.12, $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es invertible si y solo si m es primo con n.

□

De estas proposiciones obtendremos la congruencia de Euler.

14. Definición: Sea $\phi\colon \mathbb{N}^* \to \mathbb{N}$ la aplicación definida por

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

A la aplicación ϕ la denominaremos operador de Euler.

Es decir, $\phi(n) = |$Conjunto de los números naturales inferiores a n y primos con él$|$.

15. Congruencia de Euler: *Si n, m son números naturales primos entre sí, entonces*

$$m^{\phi(n)} \equiv 1 \, mod \, n.$$

Demostración. Es consecuencia de 1.6.4, aplicado al caso $G = (\mathbb{Z}/n\mathbb{Z})^*$ y $g = \bar{m}$. □

Calculemos $\phi(n)$.

16. Proposición: *Si n, m son números naturales primos entre sí, entonces*

$$\phi(nm) = \phi(n)\phi(m).$$

Demostración. Por el teorema chino de los restos tenemos el isomorfismo de anillos $\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Tomando los invertibles de los anillos

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

luego $\phi(nm) = |(\mathbb{Z}/nm\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^*| \cdot |(\mathbb{Z}/m\mathbb{Z})^*| = \phi(n)\phi(m)$. □

17. Proposición: *Si p es un número natural primo, entonces:*

$$\phi(p^n) = p^{n-1}(p-1).$$

Demostración. Un número r es primo con p^n si y solo si es primo con p. Obviamente $1 \cdot p, 2 \cdot p, \ldots, p^{n-1} \cdot p$ son los números naturales m, con $0 < m \leq p^n$, que no son primos con p^n. Luego, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

18. Teorema: *Si $n = p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición de $n \in \mathbb{N}$ en producto de potencias de números naturales primos, entonces:*

$$\phi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1 - 1) \cdots (p_r - 1).$$

2.5. Anillos de fracciones

1. Definición: Sea A un anillo y $S \subseteq A$ un subconjunto. Diremos que S es un sistema multiplicativo de A si cumple

1. $1 \in S$.
2. Si $s, s' \in S$ entonces $s \cdot s' \in S$.

2. Ejemplos: $\mathbb{Z}\backslash\{0\}$ es un sistema multiplicativo de $\mathbb{Z}$. Si A es un anillo íntegro, entonces $A\backslash\{0\}$ es un sistema multiplicativo. Si $\mathfrak{p} \subset A$ es un ideal primo, entonces $A\backslash\mathfrak{p}$ es un sistema multiplicativo. Dado $a \in A$, $S = \{1, a, a^2, \ldots, a^n, \ldots\}$ es un sistema multiplicativo.

Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. Podemos definir en el conjunto $A \times S$ la siguiente relación de equivalencia:

$$(a,s) \sim (a',s') \iff \text{existen } s_1, s_2 \in S \text{ tales que } (as_1, ss_1) = (a's_2, s's_2).$$

Denotaremos $\frac{a}{s}$ a la clase de equivalencia de (a,s).

3. Definición: Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. La localización de A por S, A_S, es el conjunto

$$A_S := \left\{ \frac{a}{s},\ \forall\, a \in A \text{ y } \forall\, s \in S \right\}$$

Observemos que $\frac{a}{s} = \frac{a'}{s'}$ si y solo si existen $s_1, s_2 \in S$ tales que $as_1 = a's_2$ y $ss_1 = s's_2$. Luego, $\frac{a}{s} = \frac{as_1}{ss_1} = \frac{a's_2}{s's_2} = \frac{a'}{s'}$, donde las fracciones del medio tienen igual numerador y denominador. Ahora es fácil probar la siguiente afirmación:

> Sea B un conjunto. Dar una aplicación $\phi\colon A_S \to B$ es asignar a cada $\frac{a}{s} \in A_S$ un elemento $\varphi(a,s) \in B$ de modo que $\varphi(at,st) = \varphi(a,s)$ para todo $t \in S$.

Con mayor generalidad, dar una aplicación $\phi\colon A_S \times \overset{n}{\cdots} \times A_S \to B$ es asignar a cada elemento $(\frac{a_1}{s_1}, \ldots, \frac{a_n}{s_n}) \in A_S \times \overset{n}{\cdots} \times A_S$ un elemento $\varphi(a_1, s_1, \ldots, a_n, s_n) \in B$ de modo que $\varphi(t_1a_1, t_1s_1, \ldots, t_na_n, t_ns_n) = \varphi(a_1, s_1, \ldots, a_n, s_n)$ para todo $t_1, \ldots, t_n \in S$.

Con la suma y producto ordinarios de fracciones (bien definidos)

$$\frac{a}{s} + \frac{a'}{s'} := \frac{s'a + sa'}{ss'}$$
$$\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

A_S es un anillo. El elemento unidad de A_S es la fracción $\frac{1}{1}$. Si $s \in S$ entonces la fracción $\frac{s}{1}$ es invertible, de inverso $\frac{1}{s}$. La fracción $\frac{0}{s} = \frac{0 \cdot s}{1 \cdot s} = \frac{0}{1}$ es el elemento nulo de A_S.

4. Definición: Al morfismo natural de anillos $A \to A_S$, $a \mapsto \frac{a}{1}$ se le denomina morfismo de localización por S.

Denotaremos $\frac{a}{1} = a$, cuando no sea causa de confusión.

5. Definición: Si A es un anillo íntegro, obviamente $A_{A\setminus\{0\}}$ es un cuerpo y diremos que es el cuerpo de fracciones de A.

6. Ejemplos: 1. $\mathbb{Q} = \mathbb{Z}_{\mathbb{Z}\setminus\{0\}}$,

2. $\mathbb{Q}(x) := \mathbb{Q}[x]_{\mathbb{Q}[x]\setminus\{0\}}$

3. $k(x) := k[x]_{k[x]\setminus\{0\}} = \{p(x)/q(x)\colon\ p(x), q(x) \in k[x], q(x) \neq 0\}$, o con mayor generalidad, el cuerpo de funciones racionales en n-variables con coeficientes en k,

$$k(x_1, \ldots, x_n) := k[x_1, \ldots, x_n]_{k[x_1,\ldots,x_n]\setminus\{0\}} = \{\frac{p(x)}{q(x)}\colon 0 \neq q(x), p(x) \in k[x_1, \ldots, x_n]\}$$

7. Proposición: *Sea A_S la localización de A por S. Entonces,*

1. *$\frac{a}{s} = 0$ si y solo si existe $s' \in S$ tal que $s' \cdot a = 0$ (en A).*

2. *$\frac{a}{s} = \frac{a'}{s'}$ en A_S si y solo si existe un $t \in S$ de modo que $t \cdot (as' - a's) = 0$.*

Demostración. 1. $\Rightarrow$) $0 = \frac{0}{1} = \frac{a}{s}$ luego existen $t, t' \in S$ tales que $t \cdot 0 = t' \cdot a$ (y $t \cdot 1 = t' \cdot s$), luego $t' \cdot a = 0$.

$\Leftarrow$) $\frac{a}{s} = \frac{as'}{ss'} = \frac{0}{ss'} = \frac{0}{1} = 0$.

2. $\Rightarrow$) $0 = \frac{a}{s} - \frac{a'}{s'} = \frac{as' - a's}{ss'}$, existe un $t \in S$ de modo que $t \cdot (as' - a's) = 0$, por el punto 1.

$\Leftarrow$) Si $t \cdot (as' - a's) = 0$, entonces $0 = \frac{as' - a's}{ss'} = \frac{a}{s} - \frac{a'}{s'}$, entonces $\frac{a}{s} = \frac{a'}{s'}$.

□

8. Ejercicio: Sea A un anillo y $S \subseteq A$ un sistema multiplicativo. Entonces, $A_S = \{0\} \iff 0 \in S$.

9. Ejercicio: Sea A un anillo íntegro y $S \subseteq A\setminus\{0\}$ un sistema multiplicativo. Entonces, $\frac{a}{s} = \frac{a'}{s'}$ en A_S si y solo si $as' - a's = 0$ (en A).

10. Ejercicio: Prueba que $(\mathbb{Z}[x])_{\mathbb{Z}\setminus\{0\}} = \mathbb{Q}[x]$.

11. Descomposición en suma de fracciones simples: Sea (A,δ) un anillo euclídeo. Sean $a,p,q \in A$ y supongamos que p y q son primos entre sí. Entonces,

1. Existen $a_1, a_2 \in A$ de modo que $\frac{a}{pq} = \frac{a_1}{p} + \frac{a_2}{q}$.
2. Existen $a_0,\dots,a_n \in A$, con $a_i = 0$ ó $\delta(a_i) < \delta(p)$, para cada $i \geq 1$, de modo que

$$\frac{a}{p^n} = \sum_{i=0}^{n} \frac{a_i}{p^i}.$$

Demostración. 1. Sean $\lambda,\mu \in A$ tales que $\lambda p + \mu q = 1$. Entonces

$$\frac{a}{pq} = \frac{a(\lambda p + \mu q)}{pq} = \frac{a\mu}{p} + \frac{a\lambda}{q}$$

2. $a = c_0 p + b_0$, para ciertos c_0 y b_0, con $b_0 = 0$ ó $\delta(b_0) < \delta(p)$. Igualmente, $c_0 = c_1 p + b_1$, para ciertos c_1 y b_1, con $b_1 = 0$ ó $\delta(b_1) < \delta(p)$. Luego, $a = b_0 + b_1 p + c_1 p^2$. De nuevo, $c_1 = c_2 p + b_2$, para ciertos c_2 y b_2, con $b_2 = 0$ ó $\delta(b_2) < \delta(p)$. Luego, $a = b_0 + b_1 p + b_2 p^2 + c_2 p^3$. Así sucesivamente obtenemos que $a = (\sum_{i=0}^{n-1} b_i p^i) + c_{n-1} p^n$. Si tomamos $a_i = b_{n-i}$, para $1 \leq i \leq n$, y $a_0 = c_{n-1}$ concluimos que $\frac{a}{p^n} = \sum_{i=0}^{n} \frac{a_i}{p^i}$.

□

2.6. Lema de Gauss. $K[x_1,\dots,x_n]$ es DFU

Probaremos que $k[x,y]$ es un dominio de factorización única usando que $k[x,y] \subset k(x)[y]$ y que $k(x)[y]$ es dominio de factorización única.

1. Definición: Un polinomio $p(x) \in A[x]$ se dice *primitivo* cuando sus coeficientes no admiten un divisor común no invertible, es decir, si $p(x) = a \cdot q(x)$ con $a \in A$, entonces a es invertible.

2. Lema: *Sea A un dominio de factorización única de cuerpo de fracciones $\Sigma = A_{A\setminus 0}$. Entonces,*

1. *Si $p(x), q(x) \in A[x]$ son dos polinomios primitivos entonces $p(x)\cdot q(x)$ es primitivo.*
2. *Para cada $h(x) \in \Sigma[x]$ existen $v \in \Sigma$ y $p(x) \in A[x]$ primitivo, únicos salvo multiplicación por un invertible de A, tales que*

$$h(x) = v \cdot p(x).$$

Demostración. 1. Supongamos que $p(x)\cdot q(x) = a\cdot r(x)$, con $r(x)\in A[x]$ y $a\in A$ no invertible. Sea $p\in A$ irreducible que divida a a. Pasando al cociente $A[x]\to (A/pA)[x]$, tenemos que

$$\overline{p(x)}\cdot\overline{q(x)} = 0 \in (A/pA)[x].$$

Lo cual es contradictorio, porque $(A/pA)[x]$ es íntegro y $\overline{p(x)}$ y $\overline{q(x)}$ son no nulos.

2. Sea $u\in A$ el producto de todos los denominadores de los coeficientes de $h(x)$. Entonces, $u\cdot h(x)\in A[x]$. Sea u' el máximo común divisor de todos los coeficientes de $u\cdot h(x)$. Entonces, $p(x) := \frac{u}{u'}h(x)\in A[x]$ es primitivo. Si definimos $v := \frac{u'}{u}$, entonces $h(x) = v\cdot p(x)$.

Sea otra descomposición $h(x) = v'\cdot p(x)'$. Basta probar que $v = v'$ salvo multiplicación por un invertible. Sea $w\in A$ tal que $w\cdot v, w\cdot v'\in A$. Observemos que $w\cdot v\cdot p(x) = w\cdot v'\cdot p(x)'$. Ahora bien, el máximo común divisor de los coeficientes del polinomio $w\cdot v\cdot p(x)$ es $w\cdot v$ (salvo multiplicación por un invertible) y el de $w\cdot v'\cdot p(x)$ es $w\cdot v'$. Luego, $v = v'$ salvo multiplicación por un invertible. □

3. Lema de Gauss: *Sea A un dominio de factorización única con cuerpo de fracciones Σ y $p(x)\in A[x]$ un polinomio primitivo. Entonces, $p(x)$ es irreducible en $A[x]$ si y solo si es irreducible en $\Sigma[x]$.*

Demostración. Supongamos que $p(x)$ es irreducible en $\Sigma[x]$. Si $p(x) = p_1(x)\cdot p_2(x)$, con $p_1(x), p_2(x)\in A[x]$, entonces como $p(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $p_1(x)$ o $p_2(x)$ ha de ser de grado cero, digamos $p_1(x) = a$. Como $p(x)$ es primitivo $p_1(x) = a\in A$ es invertible. En conclusión, $p(x)$, es irreducible en $A[x]$.

Supongamos que $p(x)$ es irreducible en $A[x]$. Supongamos que $p(x) = \tilde{p}_1(x)\cdot\tilde{p}_2(x)$, siendo $\tilde{p}_1(x)$ y $\tilde{p}_2(x)$ dos polinomios de $\Sigma[x]$. Sean $v_1, v_2\in\Sigma$ y $p_1(x), p_2(x)\in A[x]$ primitivos, salvo multiplicación por invertibles de A, tales que $\tilde{p}_1(x) = v_1\cdot p_1(x)$ y $\tilde{p}_2(x) = v_2\cdot p_2(x)$. Entonces,

$$p(x) = (v_1\cdot v_2)\cdot(p_1(x)\cdot p_2(x)).$$

Por el lema 2.6.2 1., $p_1(x)\cdot p_2(x)$ es primitivo. Por el lema 2.6.2 2., $v_1\cdot v_2$ es un invertible de A. Luego $p(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

4. Corolario: *Si A es un dominio de factorización única, entonces $A[x]$ también lo es.*

Demostración. Sea $\Sigma = A_{A\setminus\{0\}}$ el cuerpo de fracciones. Sea $p(x)\in A[x]$ y escribamos $p(x) = a\cdot q(x)$, con $a\in A$ y $q(x)\in A[x]$ primitivo. Sea

$$q(x) = \widetilde{q}_1(x)\cdots\widetilde{q}_r(x)$$

la descomposición en irreducibles en $\Sigma[x]$. Por el lema 2.6.2 se puede escribir $\widetilde{q}_i(x) = v_i\cdot q_i(x)$ con $v_i\in\Sigma$ y $q_i(x)\in A[x]$ primitivos. Luego,

$$q(x) = v\cdot q_1(x)\cdots q_r(x).$$

• Por el lema 2.6.2 1., $q_1(x)\cdots q_r(x)$ es primitivo. Por el lema 2.6.2 2., v es un invertible de A.

• Cada $q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por 2.6.3.

Descomponiendo $a = p_1\cdots p_s$ en producto de irreducibles en A, se obtiene una descomposición en producto de irreducibles

$$p(x) = a\cdot q(x) = v\cdot p_1\cdots p_s q_1(x)\cdots q_r(x)$$

en $A[x]$.

Unicidad: Si $p(x) = q_1\cdots q_l p_1(x)\cdots p_t(x)$, entonces cada $p_i(x)$ es irreducible en $\Sigma[x]$ por 2.6.3. $\Sigma[x]$ es DFU, por tanto, los polinomios $p_i(x)$ (una vez reordenados) son iguales a los $q_i(x)$, salvo multiplicación por un elemento de Σ, que ha de ser un invertible de A. Tachando los términos polinómicos comunes se obtiene salvo multiplicación por invertibles de A la igualdad $q_1\cdots q_l = p_1\cdots p_s$, de donde $q_i = p_i$ (salvo permutación de los factores y multiplicación de éstos por invertibles de A).

□

Como corolario del teorema anterior, se obtiene el siguiente teorema.

5. Teorema : *Los anillos $\mathbb{Z}[x_1,\ldots,x_n]$ y $k[x_1,\ldots,x_n]$ (k un cuerpo) son dominios de factorización única.*

2.7. Cuestionario

1. Consideremos el conjunto $A = \{0\}$ y consideremos las dos operaciones internas:

   $$0+0 := 0 \text{ y } 0\cdot 0 := 0$$

   ¿Es $(A,+,\cdot)$ un anillo?

2. Sean $(A,+,\cdot)$ y $(B,+,\cdot)$ dos anillos. Dota a $A\times B$ de estructura de anillo.

3. ¿La serie $1+x \in \mathbb{Q}[[x]]$ tiene inverso?

4. Sean A y B dos anillos y consideremos en $A\times B$ la estructura de anillo usual ¿Es $A\times B$ un anillo íntegro?

5. ¿Son los cuerpos anillos íntegros?

6. Sea A un anillo íntegro. Sean $a,b,c\in A$ y $a\neq 0$. Si $ab = ac$, prueba que $b = c$.

7. Sea A un anillo y p un número primo. Si $1+\overset{p}{\cdots}+1 = 0$ en A, prueba que $(a+b)^p = a^p + b^p$, para todo $a,b\in A$.

8. Sea $I\subset A$ un ideal. Prueba que $A[x]/(I)\simeq (A/I)[x]$.

9. Sean I_1, I_2 dos ideales de A. Prueba que $I_1+I_2 := \{i_1+i_2\in A : i_1\in I_1, i_2\in I_2\}$ es un ideal de A. Prueba que $\bar{I}_2 := \{\bar{i}_2\in A/I_1 : i_2\in I_2\}$ es un ideal de A/I_1. Prueba que

   $$(A/I_1)/\bar{I}_2 = A/(I_1+I_2).$$

10. Sea A un anillo íntegro. Prueba que $(A[x])^* = A^*$ (definimos B^* como el conjunto de los invertibles de B).

11. Calcula los ideales primos de $A = \{0\}$.

12. Sea K un cuerpo. Calcula los ideales de K.

13. Da un criterio para saber cuándo un número entero escrito en base dos es divisible por $3 \in \mathbb{Z}$.

14. ¿Es el ideal $(x,y) \subset \mathbb{Q}[x,y]$ principal?

15. ¿Es el ideal $(2,x) \subset \mathbb{Z}[x]$ principal?

16. Prueba que $(x_1,\ldots,x_n,\ldots) \subset \mathbb{Q}[x_1,\ldots,x_n,\ldots]$ no es un ideal finito generado.

17. Sea (A,δ) un anillo euclídeo. Dado $a \in A$ no nulo prueba que $\delta(a) \geq \delta(1)$. Prueba que a es invertible si y solo si $\delta(a) = \delta(1)$.

18. Dados $p(x) = x^3+x^2+x+1, q(x) = 2x^2+3x+1 \in \mathbb{Q}[x]$, calcula $c(x), r(x)$ de modo que $p(x) = q(x)c(x)+r(x)$ y $r(x) = 0$ ó $\mathrm{gr}(r(x)) < \mathrm{gr}(q(x)$.

19. Dados $22+7i, 2+2i \in \mathbb{Z}[i]$. Calcula $c, r \in \mathbb{Z}[i]$, tales que $22+7i = (2+2i)\cdot c + r$, de modo que $r = 0$ ó $|r| < |2+2i|$.

20. ¿Es $2 \in \mathbb{Z}[i]$ irreducible? Descompóngase 2 en producto de irreducibles de $\mathbb{Z}[i]$.

21. Sean $p(x) = x^3 - x^2 + x - 1$ y $q(x) = x^3 - 3x^2 + 3x - 1 \in \mathbb{Q}[x]$. Calcula mediante el algoritmo de Euclides el máximo común divisor de $p(x)$ y $q(x)$, calcula $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ de modo que $\lambda(x)p(x) + \mu(x)q(x) = m.c.d.(p(x), q(x))$.

22. Sea A DFU y $a, b \in A$. Prueba que si $a^{33} = b^{33}$ entonces a es igual a b salvo un factor invertible.

23. Sea A DFU y $a, b \in A$. Prueba que $m.c.d(a,b) \cdot m.c.m.(a,b)$ es igual a $a \cdot b$ salvo multiplicación por un invertible.

24. Sea A DFU y $a, b \in A$. Prueba que $m.c.d.(a^2, b^2) = m.c.d.(a,b)^2$ salvo un factor invertible.

25. Prueba que en $\mathbb{Z}$ hay infinitos números primos.

26. Sea K un cuerpo. Prueba que un polinomio no constante $p(x) \in K[x]$ es irreducible si y solo si $K[x]/(p(x))$ es un cuerpo.

27. Calcula el inverso de $\bar{7}$ en $\mathbb{Z}/982\mathbb{Z}$.

28. Sea p un número primo y $q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Prueba que $q(x)^p = q(x^p)$.

29. Calcula el inverso de $\overline{1+x+x^2} \in \mathbb{Q}[x]/(x^3-2)$. Calcula el inverso de $1+\sqrt[3]{2}+\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$.

30. Calcula la clase de 12^{13} en $\mathbb{Z}/5\mathbb{Z}$, en $\mathbb{Z}/7\mathbb{Z}$ y en $\mathbb{Z}/35\mathbb{Z}$.

31. Descompóngase $12x^3 - 12x^2 - 3x + 3 \in \mathbb{Z}[x]$ como producto de irreducibles.

2.8. Biografía de Leonhard Euler

EULER BIOGRAPHY

Leonhard Euler's father was Paul Euler. Paul Euler had studied theology at the University of Basel and had attended Jacob Bernoulli's lectures there. In fact Paul Euler and Johann Bernoulli had both lived in Jacob Bernoulli's house while undergraduates at Basel. Paul Euler became a Protestant minister and married Margaret Brucker, the daughter of another Protestant minister. Their son Leonhard Euler was born in Basel, but the family moved to Riehen when he was one year old and it was in Riehen, not far from Basel, that Leonard was brought up. Paul Euler had, as we have mentioned, some mathematical training and he was able to teach his son elementary mathematics along with other subjects.

Leonhard was sent to school in Basel and during this time he lived with his grandmother on his mother's side. This school was a rather poor one, by all accounts, and Euler learnt no mathematics at all from the school. However his interest in mathematics had certainly been sparked by his father's teaching, and he read mathematics texts on his own and took some private lessons. Euler's father wanted his son to follow him into the church and sent him to the University of Basel to prepare for the ministry. He entered the University in 1720, at the age of 14, first to obtain a general education before going on to more advanced studies. Johann Bernoulli soon discovered Euler's great potential for mathematics in private tuition that Euler himself engineered. Euler's own account given in his unpublished autobiographical writings, is as follows:

... I soon found an opportunity to be introduced to a famous professor Johann Bernoulli. ... True, he was very busy and so refused flatly to give me private lessons; but he gave me much more valuable advice to start reading more difficult mathematical books on my own and to study them as diligently as I could; if I came across some obstacle or difficulty, I was given permission to visit him freely every Sunday afternoon and he kindly explained to me everything I could not understand ...

In 1723 Euler completed his Master's degree in philosophy having compared and contrasted the philosophical ideas of Descartes and Newton. He began his study of theology in the autumn of 1723, following his father's wishes, but, although he was to be a devout Christian all his life, he could not find the enthusiasm for the study of theology, Greek and Hebrew that he found in mathematics. Euler obtained his father's consent to change to mathematics after Johann Bernoulli had used his persuasion. The fact that Euler's father had been a friend of Johann Bernoulli's in their undergraduate days undoubtedly made the task of persuasion much easier.

Euler completed his studies at the University of Basel in 1726. He had studied many mathematical works during his time in Basel. They include works by Varignon,

Descartes, Newton, Galileo, van Schooten, Jacob Bernoulli, Hermann, Taylor and Wallis. By 1726 Euler had already a paper in print, a short article on isochronous curves in a resisting medium. In 1727 he published another article on reciprocal trajectories and submitted an entry for the 1727 Grand Prize of the Paris Academy on the best arrangement of masts on a ship.

The Prize of 1727 went to Bouguer, an expert on mathematics relating to ships, but Euler's essay won him second place which was a fine achievement for the young graduate. However, Euler now had to find himself an academic appointment and when Nicolaus (II) Bernoulli died in St Petersburg in July 1726 creating a vacancy there, Euler was offered the post which would involve him in teaching applications of mathematics and mechanics to physiology. He accepted the post in November 1726 but stated that he did not want to travel to Russia until the spring of the following year. He had two reasons to delay. He wanted time to study the topics relating to his new post but also he had a chance of a post at the University of Basel since the professor of physics there had died. Euler wrote an article on acoustics, which went on to become a classic, in his bid for selection to the post but he was not chosen to go forward to the stage where lots were drawn to make the final decision on who would fill the chair. Almost certainly his youth (he was 19 at the time) was against him. However Calinger suggests:

This decision ultimately benefited Euler, because it forced him to move from a small republic into a setting more adequate for his brilliant research and technological work.

As soon as he knew he would not be appointed to the chair of physics, Euler left Basel on 5 April 1727. He travelled down the Rhine by boat, crossed the German states by post wagon, then by boat from Lübeck arriving in St Petersburg on 17 May 1727. He had joined the St Petersburg Academy of Sciences two years after it had been founded by Catherine I the wife of Peter the Great. Through the requests of Daniel Bernoulli and Jakob Hermann, Euler was appointed to the mathematical-physical division of the Academy rather than to the physiology post he had originally been offered. At St Petersburg Euler had many colleagues who would provide an exceptional environment for him. Youschkevitch wrote:

Nowhere else could he have been surrounded by such a group of eminent scientists, including the analyst, geometer Jakob Hermann, a relative; Daniel Bernoulli, with whom Euler was connected not only by personal friendship but also by common interests in the field of applied mathematics; the versatile scholar Christian Goldbach, with whom Euler discussed numerous problems of analysis and the theory of numbers; F Maier, working in trigonometry; and the astronomer and geographer J-N Delisle.

Euler served as a medical lieutenant in the Russian navy from 1727 to 1730. In St Petersburg he lived with Daniel Bernoulli who, already unhappy in Russia, had requested that Euler bring him tea, coffee, brandy and other delicacies from Switzerland. Euler became professor of physics at the Academy in 1730 and, since this allowed him to become a full member of the Academy, he was able to give up his Russian navy post.

Daniel Bernoulli held the senior chair in mathematics at the Academy but when he left St Petersburg to return to Basel in 1733 it was Euler who was appointed to this se-

nior chair of mathematics. The financial improvement which came from this appointment allowed Euler to marry which he did on 7 January 1734, marrying Katharina Gsell, the daughter of a painter from the St Petersburg Gymnasium. Katharina, like Euler, was from a Swiss family. They had 13 children altogether although only five survived their infancy. Euler claimed that he made some of his greatest mathematical discoveries while holding a baby in his arms with other children playing round his feet. D. Cameron wrote:

... after 1730 he carried out state projects dealing with cartography, science education, magnetism, fire engines, machines, and ship building. ... The core of his research program was now set in place: number theory; infinitary analysis including its emerging branches, differential equations and the calculus of variations; and rational mechanics. He viewed these three fields as intimately interconnected. Studies of number theory were vital to the foundations of calculus, and special functions and differential equations were essential to rational mechanics, which supplied concrete problems.

The publication of many articles and his book Mechanica (1736-37), which extensively presented Newtonian dynamics in the form of mathematical analysis for the first time, started Euler on the way to major mathematical work.

Euler's health problems began in 1735 when he had a severe fever and almost lost his life. However, he kept this news from his parents and members of the Bernoulli family back in Basel until he had recovered. In his autobiographical writings Euler says that his eyesight problems began in 1738 with overstrain due to his cartographic work and that by 1740 he wrote:

... lost an eye and [the other] currently may be in the same danger.

However, Calinger argued that Euler's eyesight problems almost certainly started earlier and that the severe fever of 1735 was a symptom of the eyestrain. He also argued that a portrait of Euler from 1753 suggests that by that stage the sight of his left eye was still good while that of his right eye was poor but not completely blind. Calinger suggested that Euler's left eye became blind from a later cataract rather than eyestrain.

By 1740 Euler had a very high reputation, having won the Grand Prize of the Paris Academy in 1738 and 1740. On both occasions he shared the first prize with others. Euler's reputation was to bring an offer to go to Berlin, but at first he preferred to remain in St Petersburg. However political turmoil in Russia made the position of foreigners particularly difficult and contributed to Euler changing his mind. Accepting an improved offer Euler, at the invitation of Frederick the Great, went to Berlin where an Academy of Science was planned to replace the Society of Sciences. He left St Petersburg on 19 June 1741, arriving in Berlin on 25 July. In a letter to a friend Euler wrote:

I can do just what I wish [in my research] ... The king calls me his professor, and I think I am the happiest man in the world.

Even while in Berlin Euler continued to receive part of his salary from Russia. For this remuneration he bought books and instruments for the St Petersburg Academy, he continued to write scientific reports for them, and he educated young Russians.

Maupertuis was the president of the Berlin Academy when it was founded in 1744 with Euler as director of mathematics. He deputised for Maupertuis in his absence

and the two became great friends. Euler undertook an unbelievable amount of work for the Academy:

... he supervised the observatory and the botanical gardens; selected the personnel; oversaw various financial matters; and, in particular, managed the publication of various calendars and geographical maps, the sale of which was a source of income for the Academy. The king also charged Euler with practical problems, such as the project in 1749 of correcting the level of the Finow Canal ... At that time he also supervised the work on pumps and pipes of the hydraulic system at Sans Souci, the royal summer residence.

This was not the limit of his duties by any means. He served on the committee of the Academy dealing with the library and of scientific publications. He served as an advisor to the government on state lotteries, insurance, annuities and pensions and artillery. On top of this his scientific output during this period was phenomenal.

During the twenty-five years spent in Berlin, Euler wrote around 380 articles. He wrote books on the calculus of variations; on the calculation of planetary orbits; on artillery and ballistics (extending the book by Robins); on analysis; on shipbuilding and navigation; on the motion of the moon; lectures on the differential calculus; and a popular scientific publication Letters to a Princess of Germany (3 vols., 1768-72).

In 1759 Maupertuis died and Euler assumed the leadership of the Berlin Academy, although not the title of President. The king was in overall charge and Euler was not now on good terms with Frederick despite the early good favour. Euler, who had argued with d'Alembert on scientific matters, was disturbed when Frederick offered d'Alembert the presidency of the Academy in 1763. However d'Alembert refused to move to Berlin but Frederick's continued interference with the running of the Academy made Euler decide that the time had come to leave.

In 1766 Euler returned to St Petersburg and Frederick was greatly angered at his departure. Soon after his return to Russia, Euler became almost entirely blind after an illness. In 1771 his home was destroyed by fire and he was able to save only himself and his mathematical manuscripts. A cataract operation shortly after the fire, still in 1771, restored his sight for a few days but Euler seems to have failed to take the necessary care of himself and he became totally blind. Because of his remarkable memory he was able to continue with his work on optics, algebra, and lunar motion. Amazingly after his return to St Petersburg (when Euler was 59) he produced almost half his total works despite the total blindness.

Euler of course did not achieve this remarkable level of output without help. He was helped by his sons, Johann Albrecht Euler who was appointed to the chair of physics at the Academy in St Petersburg in 1766 (becoming its secretary in 1769) and Christoph Euler who had a military career. Euler was also helped by two other members of the Academy, W. L. Krafft and A J. Lexell, and the young mathematician N. Fuss who was invited to the Academy from Switzerland in 1772. Fuss, who was Euler's grandson-in-law, became his assistant in 1776. Yushkevich wrote:

.. the scientists assisting Euler were not mere secretaries; he discussed the general scheme of the works with them, and they developed his ideas, calculating tables, and sometimes compiled examples.

For example Euler credits Albrecht, Krafft and Lexell for their help with his 775

page work on the motion of the moon, published in 1772. Fuss helped Euler prepare over 250 articles for publication over a period on about seven years in which he acted as Euler's assistant, including an important work on insurance which was published in 1776.

Yushkevich described the day of Euler's death:

On 18 September 1783 Euler spent the first half of the day as usual. He gave a mathematics lesson to one of his grandchildren, did some calculations with chalk on two boards on the motion of balloons; then discussed with Lexell and Fuss the recently discovered planet Uranus. About five o'clock in the afternoon he suffered a brain haemorrhage and uttered only Ï am dying"before he lost consciousness. He died about eleven o'clock in the evening.

After his death in 1783 the St Petersburg Academy continued to publish Euler's unpublished work for nearly 50 more years.

Euler's work in mathematics is so vast that an article of this nature cannot but give a very superficial account of it. He was the most prolific writer of mathematics of all time. He made large bounds forward in the study of modern analytic geometry and trigonometry where he was the first to consider sin, cos etc. as functions rather than as chords as Ptolemy had done.

He made decisive and formative contributions to geometry, calculus and number theory. He integrated Leibniz's differential calculus and Newton's method of fluxions into mathematical analysis. He introduced beta and gamma functions, and integrating factors for differential equations. He studied continuum mechanics, lunar theory with Clairaut, the three body problem, elasticity, acoustics, the wave theory of light, hydraulics, and music. He laid the foundation of analytical mechanics, especially in his Theory of the Motions of Rigid Bodies (1765).

We owe to Euler the notation $f(x)$ for a function (1734), e for the base of natural logs (1727), i for the square root of -1 (1777), π for pi, $\sum$ for summation (1755), the notation for finite differences Δy and $\Delta^2 y$ and many others.

Let us examine in a little more detail some of Euler's work. Firstly his work in number theory seems to have been stimulated by Goldbach but probably originally came from the interest that the Bernoullis had in that topic. Goldbach asked Euler, in 1729, if he knew of Fermat's conjecture that the numbers $2n+1$ were always prime if n is a power of 2. Euler verified this for $n = 1, 2, 4, 8$ and 16 and, by 1732 at the latest, showed that the next case $2^{32}+1 = 4294967297$ is divisible by 641 and so is not prime. Euler also studied other unproved results of Fermat and in so doing introduced the Euler ϕ function $\phi(n)$, the number of integers k with $1 \le k \le n$ and k coprime to n. He proved another of Fermat's assertions, namely that if a and b are coprime then a^2+b^2 has no divisor of the form $4n-1$, in 1749.

Perhaps the result that brought Euler the most fame in his young days was his solution of what had become known as the Basel problem. This was to find a closed form for the sum of the infinite series $\zeta(2) = \sum(1/n^2)$, a problem which had defeated many of the top mathematicians including Jacob Bernoulli, Johann Bernoulli and Daniel Bernoulli. The problem had also been studied unsuccessfully by Leibniz, Stirling, de Moivre and others. Euler showed in 1735 that $\zeta(2) = \frac{\pi^2}{6}$ but he went on to

prove much more, namely that $\zeta(4) = \pi^4/90, \zeta(6) = \frac{\pi^6}{945}$, $\zeta(8) = \frac{\pi^8}{9450}, \zeta(10) = \frac{pi^{10}}{93555}$ and $\zeta(12) = \frac{691\pi^{12}}{638512875}$. In 1737 he proved the connection of the zeta function with the series of prime numbers giving the famous relation

$$\zeta(s) = \sum(1/n^s) = \prod(1 - p^{-s})^{-1}.$$

Here the sum is over all natural numbers n while the product is over all prime numbers.

By 1739 Euler had found the rational coefficients C in $\zeta(2n) = C\pi^{2n}$ in terms of the Bernoulli numbers.

Other work done by Euler on infinite series included the introduction of his famous Euler's constant γ, in 1735, which he showed to be the limit of

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + 1/n - \log_e n$$

as n tends to infinity. He calculated the constant γ to 16 decimal places. Euler also studied Fourier series and in 1744 he was the first to express an algebraic function by such a series when he gave the result

$$\frac{\pi}{2} - \frac{x}{2} = \sin x + \frac{\sin 2x}{2} + \frac{\sin 3x}{3} + \ldots$$

in a letter to Goldbach. Like most of Euler's work there was a fair time delay before the results were published; this result was not published until 1755.

Euler wrote to James Stirling on 8 June 1736 telling him about his results on summing reciprocals of powers, the harmonic series and Euler's constant and other results on series. In particular he wrote:

Concerning the summation of very slowly converging series, in the past year I have lectured to our Academy on a special method of which I have given the sums of very many series sufficiently accurately and with very little effort.

He then goes on to describe what is now called the Euler-MacLaurin summation formula. Two years later Stirling replied telling Euler that Maclaurin:

... will be publishing a book on fluxions. ... he has two theorems for summing series by means of derivatives of the terms, one of which is the self-same result that you sent me.

Euler replied:

... I have very little desire for anything to be detracted from the fame of the celebrated Mr Maclaurin since he probably came upon the same theorem for summing series before me, and consequently deserves to be named as its first discoverer. For I found that theorem about four years ago, at which time I also described its proof and application in greater detail to our Academy.

Some of Euler's number theory results have been mentioned above. Further important results in number theory by Euler included his proof of Fermat's Last Theorem for the case of $n = 3$. Perhaps more significant than the result here was the fact that he introduced a proof involving numbers of the form $a + b\sqrt{-3}$ for integers a and b. Although there were problems with his approach this eventually led to Kummer's major work on Fermat's Last Theorem and to the introduction of the concept of a ring.

One could claim that mathematical analysis began with Euler. In 1748 in Introductio in analysin infinitorum Euler made ideas of Johann Bernoulli more precise in defining a function, and he stated that mathematical analysis was the study of functions. This work bases the calculus on the theory of elementary functions rather than on geometric curves, as had been done previously. Also in this work Euler gave the formula

$$e^{ix} = \cos x + i \sin x.$$

In Introductio in analysin infinitorum Euler dealt with logarithms of a variable taking only positive values although he had discovered the formula

$$\ln(-1) = \pi i$$

in 1727. He published his full theory of logarithms of complex numbers in 1751.

Analytic functions of a complex variable were investigated by Euler in a number of different contexts, including the study of orthogonal trajectories and cartography. He discovered the Cauchy-Riemann equations in 1777, although d'Alembert had discovered them in 1752 while investigating hydrodynamics.

In 1755 Euler published Institutiones calculi differentialis which begins with a study of the calculus of finite differences. The work makes a thorough investigation of how differentiation behaves under substitutions.

In Institutiones calculi integralis (1768-70) Euler made a thorough investigation of integrals which can be expressed in terms of elementary functions. He also studied beta and gamma functions, which he had introduced first in 1729. Legendre called these 'Eulerian integrals of the first and second kind' respectively while they were given the names beta function and gamma function by Binet and Gauss respectively. As well as investigating double integrals, Euler considered ordinary and partial differential equations in this work.

The calculus of variations is another area in which Euler made fundamental discoveries. His work Methodus inveniendi lineas curvas ... published in 1740 began the proper study of the calculus of variations. In [12] it is noted that Carathéodory considered this as:

... one of the most beautiful mathematical works ever written.

Problems in mathematical physics had led Euler to a wide study of differential equations. He considered linear equations with constant coefficients, second order differential equations with variable coefficients, power series solutions of differential equations, a method of variation of constants, integrating factors, a method of approximating solutions, and many others. When considering vibrating membranes, Euler was led to the Bessel equation which he solved by introducing Bessel functions.

Euler made substantial contributions to differential geometry, investigating the theory of surfaces and curvature of surfaces. Many unpublished results by Euler in this area were rediscovered by Gauss. Other geometric investigations led him to fundamental ideas in topology such as the Euler characteristic of a polyhedron.

In 1736 Euler published Mechanica which provided a major advance in mechanics. As Yushkevich wrote:

The distinguishing feature of Euler's investigations in mechanics as compared to those of his predecessors is the systematic and successful application of analysis. Previously the methods of mechanics had been mostly synthetic and geometrical; they demanded too individual an approach to separate problems. Euler was the first to appreciate the importance of introducing uniform analytic methods into mechanics, thus enabling its problems to be solved in a clear and direct way.

In Mechanica Euler considered the motion of a point mass both in a vacuum and in a resisting medium. He analysed the motion of a point mass under a central force and also considered the motion of a point mass on a surface. In this latter topic he had to solve various problems of differential geometry and geodesics.

Mechanica was followed by another important work in rational mechanics, this time Euler's two volume work on naval science. D. cameron wrote:

Outstanding in both theoretical and applied mechanics, it addresses Euler's intense occupation with the problem of ship propulsion. It applies variational principles to determine the optimal ship design and first established the principles of hydrostatics ... Euler here also begins developing the kinematics and dynamics of rigid bodies, introducing in part the differential equations for their motion.

Of course hydrostatics had been studied since Archimedes, but Euler gave a definitive version.

In 1765 Euler published another major work on mechanics Theoria motus corporum solidorum in which he decomposed the motion of a solid into a rectilinear motion and a rotational motion. He considered the Euler angles and studied rotational problems which were motivated by the problem of the precession of the equinoxes.

Euler's work on fluid mechanics is also quite remarkable. He published a number of major pieces of work through the 1750s setting up the main formulae for the topic, the continuity equation, the Laplace velocity potential equation, and the Euler equations for the motion of an inviscid incompressible fluid. In 1752 he wrote:

However sublime are the researches on fluids which we owe to Messrs Bernoulli, Clairaut and d'Alembert, they flow so naturally from my two general formulae that one cannot sufficiently admire this accord of their profound meditations with the simplicity of the principles from which I have drawn my two equations ...

Euler contributed to knowledge in many other areas, and in all of them he employed his mathematical knowledge and skill. He did important work in astronomy, theory of music and cartography.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

2.9. Problemas

1. Calcula todos los automorfismos de anillos de $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$.

2. Sea A un anillo, $a \in A$ y $p(x) \in A[x]$. Prueba que $p(a) = 0$ si y solo si $p(x)$ es múltiplo de $x - a$. Prueba que $A[x]/(x-a) \simeq A$.

3. Prueba que $\mathbb{R}[x]/((x^2+1)\cdot(x^2-1)) \simeq \mathbb{C} \times \mathbb{R} \times \mathbb{R}$.

4. Prueba

   a) $s(x) = \sum_{i=0}^{n} a_i x^i \in k[[x]]$ es invertible si y solo si $a_0 \neq 0$.

   b) El morfismo $k[x]/(x^n) \to k[[x]]/(x^n)$, $\overline{p(x)} \mapsto \overline{p(x)}$ es un isomorfismo.

5. Sea $I \subseteq A$, $J \subseteq B$ dos ideales. Prueba que $I \times J \subseteq A \times B$ es un ideal. Prueba que $(A \times B)/I \times J \simeq A/I \times B/J$.

6. Sea $n = n_r n_{r-1} \dots n_1 n_0$ un número natural escrito en base 10. Prueba que n es divisible por 7 si y solo si $n_r n_{r-1} \dots n_1 - 2 \cdot n_0$ es divisible por 7.

7. Sea $n = n_r n_{r-1} \dots n_1 n_0$ un número natural escrito en base 10. Prueba que n es divisible por 13 si y solo si $n_r n_{r-1} \dots n_1 + 4 \cdot n_0$ es divisible por 13.

8. Prueba que el anillo de los enteros de Eisenstein $\mathbb{Z}[e^{\frac{2\pi i}{3}}] := \{a + be^{\frac{2\pi i}{3}} \in \mathbb{C}, \forall a, b \in \mathbb{Z}\}$ es un anillo euclídeo.

9. Sea (A, δ) un anillo euclídeo. Sean $(a) \subseteq (b)$ ideales no nulos de A. Prueba que $\delta(b) \leq \delta(a)$ y que $\delta(a) = \delta(b)$ si y solo si $(a) = (b)$.

10. Sea (A, δ) un anillo euclídeo y A^* los invertibles de A. Sea $n = \text{mín}\{\delta(a), \text{ para } a \in A \setminus A^* \text{ y no nulo}\}$. Prueba que si $\delta(a) = n$ entonces a es irreducible.

11. Sea A un anillo íntegro y $\delta' \colon A \setminus \{0\} \to \mathbb{N}$ una aplicación que cumple: para cada $a \in A$ y $b \in A$ no nulo, existen $c, r \in A$, de modo que $a = bc + r$, y r es nulo ó $\delta'(r) < \delta'(b)$. Sea $\delta \colon A \setminus \{0\} \to \mathbb{N}$ definida por $\delta(a) := \text{mín}\{\delta'(ab), \text{ con } b \in A \setminus \{0\}\}$. Prueba que (A, δ) es un anillo euclídeo.

12. Sea A un anillo íntegro y consideremos la relación $\leq$ en A definida por $a \leq b$ si a divide a b. Demuestra

    a) $\leq$ es un preorden parcial (es decir, cumple la propiedad reflexiva y la transitiva).

    b) $a \leq b$ y $b \leq a$ si y solo si $a = b \cdot i$ con i invertible.

    c) Si $a \leq b$ entonces $a \cdot c \leq b \cdot c$, para todo $c \in A$. Si $a \cdot c \leq b \cdot c$ para algún c no nulo, entonces $a \leq b$.

    d) Si A es DFU entonces $m.c.d.(a, b)$ es el máximo común divisor de a y b (salvo multiplicación por invertibles) y $m.c.m.(a, b)$ es el mínimo común múltiplo de a y b (salvo multiplicación por invertibles)

13. Sea A un anillo íntegro. Prueba que A es un dominio de factorización si y solo si toda cadena ascendente de ideales principales estabiliza. Prueba $k[x_1, \dots, x_n]$ y $k[[x_1, \dots, x_n]]$ son dominios de factorización.

14. Prueba que $k[x_1, \dots, x_n, \dots]$ es DFU, pero no es un anillo noetheriano

15. Sea A un anillo de ideales principales. Prueba que $A = A_1 \times \cdots \times A_n$, con A_i DIP ó $A_i = B_i/(p_i^{n_i})$ donde $(p_i) \subset B_i$ es maximal.

16. Prueba que $\sqrt{2} \notin \mathbb{Q}$.

17. Calcula el mínimo común múltiplo de los polinomios $x^4+x^3+x-1, x^4+x^3+2x^2+x+1 \in \mathbb{Q}[x]$.

18. Calcula el máximo común divisor de $6, -1+3i \in \mathbb{Z}[i]$.

19. Resuelve el sistema de ecuaciones diofánticas

$$\begin{aligned} 2x+4y+3z &= 6 \\ 4x+6y+3z &= 4 \end{aligned}$$

20. Prueba que $N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$, $N(a+b\sqrt{-5}) := (a+b\sqrt{-5})\cdot(a-b\sqrt{-5}) = a^2+5b^2$ cumple que $N(z\cdot z') = N(z)\cdot N(z')$. Prueba que 2, 3, $1+\sqrt{-5}$ y $1-\sqrt{-5}$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Comprueba que $2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$ y concluye que el anillo de enteros de Kummer $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única.

21. El morfismo $c\colon \mathbb{C}[z,\frac{1}{z}] \to \mathbb{C}[z,\frac{1}{z}]$, $c(\sum_{i=m}^{n} a_i z^i) := \sum_{i=m}^{n} \bar{a}_i z^{-i}$ (donde $\bar{a}_i$ es el conjugado de a_i) es un isomorfismo de anillos.

    a) Sea $\mathbb{C}[z,\frac{1}{z}]^c := \{f \in \mathbb{C}[z,\frac{1}{z}]\colon c(f) = f\}$. Prueba que $\mathbb{C}[z,\frac{1}{z}]^c = \{\frac{p(z)}{z^n}\colon \ p(z) = a_0 z^{2n} + \cdots + a_{2n} \in \mathbb{C}[z],\ a_{2n}, a_0 \neq 0,\ a_n \in \mathbb{R}$, y si $\alpha \in \mathbb{C}$ es una raíz de multiplicidad r de $p(z)$ entonces $\frac{1}{\bar{\alpha}}$ es una raíz de multiplicidad r de $p(z)\}$.

    b) Prueba que $\frac{p(z)}{z^n} \in \mathbb{C}[z,\frac{1}{z}]^c$ es irreducible si y solo si $\mathrm{gr}(p(z)) = 2$; es además primo si las raíces de $p(z)$ no son de módulo 1.

    c) Prueba que la igualdad $\mathbb{C}[z,\frac{1}{z}] = \mathbb{C}[x,y]/(x^2+y^2-1)$, $(z = x+iy,\ x = \frac{z+z^{-1}}{2},\ y = \frac{z-z^{-1}}{2i})$, establece un isomorfismo de $\mathbb{C}[z,\frac{1}{z}]^c$ con $\mathbb{R}[x,y]/(x^2+y^2-1)$. Prueba que los elementos irreducibles de $\mathbb{C}[x,y]/(x^2+y^2-1)$ son los elementos $\overline{ax+by+c}$ y que éste es primo si y solo si $ax+by+c=0$ no corta en a $x^2+y^2-1=0$ en ningún punto (real).

22. Calcula el inverso de $\bar{7} \in \mathbb{Z}/982\mathbb{Z}$.

23. Calcula el inverso de $\overline{1+x+x^2} \in \mathbb{Q}[x]/(x^3-2)$. Calcula el inverso de $1+\sqrt[3]{2}+\sqrt[3]{2}^2$ (expresado como polinomio en $\sqrt[3]{2}$).

24. Calcula los puntos de corte de las dos curvas planas

$$\begin{aligned} x^2+y^2-1 &= 0 \\ x^3+y^3-1 &= 0 \end{aligned}$$

25. Prueba que la aplicación :

$$(\mathbb{Z}/n\mathbb{Z})^* \to Aut_{grp}(\mathbb{Z}/n\mathbb{Z}),\ \bar{m} \mapsto h_{\bar{m}},$$

donde $h_{\bar{m}}(\bar{i}) := \bar{m}\cdot\bar{i}$, es un isomorfismo.

26. Sea A un anillo.

    a) Sea $p(x,y) \in A[x,y]$. Prueba que $p(x,x) = 0$ si y solo si $p(x,y)$ es un múltiplo de $x-y$.

    b) Prueba que $A[x,y]/(x-y) = A[x]$.

27. Prueba la igualdad

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j).$$

28. Prueba que $n^3(n^3-1)(n^3+1)$ es divisible por 504, para todo número entero n.

29. Consideremos los números primos 31 y 37 y $1147 = 31 \cdot 37$. Calcular la aplicación inversa de la aplicación $\mathbb{Z}/1147\mathbb{Z} \to \mathbb{Z}/1147\mathbb{Z}$, $\bar{n} \mapsto \bar{n}^{73}$ (El sistema de encriptación RSA se basa en que la aplicación inversa es difícil de calcular cuando no se conoce la descomposición de 1147 como producto de dos primos, descomposición y aplicación inversa que son muy difíciles de calcular cuando los primos son muy grandes).

30. Calcula 17^{2023} mód 2023 (observa que $2023 = 7 \cdot 17^2$).

31. Sean $p \in \mathbb{N}$ un número primo impar y $a \in \mathbb{N}$ no divisible por p. Prueba que existe $b \in \mathbb{N}$ tal que $a = b^2 \mod p$ si y solo si $a^{\frac{p-1}{2}} = 1 \mod p$.

32. Prueba que *un número primo $p \in \mathbb{N}$ descompone en suma de dos cuadrados perfectos si y solo si p no es irreducible en $\mathbb{Z}[i]$*. Prueba que p descompone en suma de dos cuadrados perfectos si y solo si $p \equiv 1 \mod 4$ ó $p = 2$.

33. Sea A un dominio de factorización única y supongamos que $2 \in A$ es invertible. Sean $a, b \in A$ y supongamos que a es irreducible. Prueba que

$$b^2 = 1 \mod a^m \ (\text{con } m \in \mathbb{N}) \iff b = \pm 1 \mod a^m.$$

34. Resuelve la ecuación diofántica $a^2 + b^2 = 2178$.

35. Prueba que la aplicación $A_S \times A_S \to A_S$, $(\frac{a}{s}, \frac{a'}{s'}) \mapsto \frac{as'+a's}{ss'}$ está bien definida.

36. Sea S un sistema multiplicacativo del anillo A, $i : A \to A_S$ el morfismo de localización y $f : A \to B$ un morfismo de anillos. Prueba que existe un morfismo (único) $g : A_S \to B$ tal que $f = g \circ i$ si y solo si $f(s)$ es invertible para todo $s \in S$.

37. Sean S y S' dos sistemas multiplicativos de un anillo A y denotemos $S \cdot S' = \{ss', \forall\, s \in S, \forall\, s' \in S'\}$. Probar que $A_{S \cdot S'}$ es un anillo isomorfo a $(A_S)_{S'}$.

38. Sea A un anillo íntegro y $S \subset A$ un sistema multiplicativo. Prueba:

a) Si $ab = s \in S$, entonces $\frac{a}{1} \in A_S$ es invertible.

b) Si $p \in A$ es primo y p no divide a ningún elemento de S entonces $\frac{p}{1} \in A_S$ es primo.

c) Si A es DFU entonces A_S es DFU.

39. Prueba que A es un anillo noetheriano (ver 5.2.2) si y solo si toda cadena creciente de ideales de A,
$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$
estabiliza, es decir, existe $r >> 0$ tal que $I_r = I_{r+1} = I_{r+2} = \cdots$.

40. Sea A un anillo noetheriano íntegro. Prueba que A es un dominio de ideales principales si y solo si todo ideal maximal de A es principal.

41. Calcula $\int \frac{x^5}{x^4+2x^2+1}\,dx$.

42. Calcula $p(t), q(t) \in \mathbb{C}[t]$, tales que
$$\int \frac{\cos(x)\cdot\sin(x)}{\sin(x)^2\cdot\cos(3x)}\cdot dx = \int \frac{p(t)}{q(t)}\cdot dt,$$
donde $t = e^{ix}$.

Capítulo 3

Raíces de un polinomio

3.1. Introducción

Simplificando, puede afirmarse que el Álgebra es la disciplina que estudia las soluciones de los sistemas de ecuaciones algebraicas. Para la resolución de estos sistemas es necesario saber calcular las raíces de un polinomio.

El teorema de Kronecker dice que para todo polinomio $p(x) \in k[x]$ existe una extensión de cuerpos $k \hookrightarrow K$ y $\alpha_1, \ldots, \alpha_n \in K$, de modo que

$$p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

El teorema fundamental del Álgebra, que probaremos, afirma que todas las raíces de un polinomio con coeficientes complejos son complejas. En este capítulo introduciremos algunos algoritmos para el cálculo de las raíces (complejas) de un polinomio con coeficientes complejos.

Sea $p(x) \in \mathbb{R}[x]$. Primero calcularemos una cota superior M e inferior I del conjunto de todas las raíces reales de $p(x)$. Vía la teoría del exceso probaremos el teorema de Sturm, que nos permitirá calcular el número de raíces reales distintas de $p(x)$ en (I, M). Tras sucesivas bisecciones de este intervalo podremos calcular, usando el teorema de Sturm, intervalos (a_i, b_i) donde $p(x)$ solo tiene una raíz. Por último, una vez que sabemos que en un intervalo (a, b) solo hay una raíz (supongamos que no es múltiple), calculamos aproximadamente la raíz mediante sucesivas bisecciones del intervalo, o mediante la régula falsi o por el método de Newton (estudiados en Análisis o Métodos Numéricos).

Todos estos resultados los obtendremos también cuando $p(x)$ sea un polinomio con coeficientes complejos: Daremos una cota $r \in \mathbb{R}$, tal que toda raíz de $p(x)$ sea de módulo menor que r. Mediante la teoría del exceso calcularemos el número de raíces complejas de $p(x)$ que están incluidos en el interior de un rectángulo (del plano de los números complejos).

Por último, resolveremos los sistemas de ecuaciones algebraicas eliminando variables vía la resultante.

3.2. Teorema de Kronecker

El anillo de polinomios $k[x]$ es un anillo euclídeo, luego es un dominio de factorización única. Un polinomio no nulo $p(x) \in k[x]$ es invertible si y solo si es de grado cero. Si $p(x) = ax+b$ es de grado 1 entonces es irreducible, además $p(\frac{-b}{a}) = 0$ y $p(x) = a\cdot(x-\frac{-b}{a})$.

1. Definición: Sea $p(x) \in k[x]$ un polinomio y $\alpha \in k$. Se dice que α es una raíz de $p(x)$ si $p(\alpha) = 0$.

2. Proposición: *Sea $p(x) \in k[x]$ un polinomio. Entonces, $\alpha \in k$ es una raíz de $p(x)$ si y solo si $p(x)$ es múltiplo de $x-\alpha$.*

Demostración. Por el algoritmo de Euclides, existen $c(x) \in k[x]$ y $\lambda \in k$, tales que $p(x) = c(x)(x-\alpha)+\lambda$. Si α es una raíz de $p(x)$ entonces $0 = p(\alpha) = \lambda$ y $p(x)$ es múltiplo de $x-\alpha$. El recíproco es obvio. □

La siguiente proposición nos muestra cómo calcular las raíces racionales de un polinomio con coeficientes racionales.

3. Proposición: *Sea $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$ un polinomio de grado n con coeficientes racionales. Supongamos que es de coeficientes enteros, multiplicando por un número entero conveniente. Si una fracción irreducible $\frac{r}{s} \in \mathbb{Q}$ (r y s son números enteros primos entre sí) es una raíz de $p(x)$, entonces r divide a a_n y s a a_0*

Demostración. $0 = (\frac{r}{s})^n a_0 + (\frac{r}{s})^{n-1}a_1 + \cdots + a_n$, luego $0 = r^n a_0 + r^{n-1}sa_1 + \cdots + s^n a_n$. Por tanto, $s^n a_n$ es múltiplo de r y $r^n a_0$ es múltiplo de s. Luego, a_n es múltiplo de r y a_0 es múltiplo de s. □

4. El cálculo de las raíces de un polinomio en función de los coeficientes es problemático y difícil incluso para polinomios de grado pequeño. Calculemos las raíces de una cúbica, las soluciones de $x^3+a_1x^2+a_2x+a_3 = 0$. Con el cambio de variable $y = x+\frac{a_1}{3}$ obtenemos $y^3+py+q = 0$, donde $p = a_2-\frac{a_1^2}{3}$ y $q = a_3-\frac{a_1a_2}{3}+\frac{2a_1^3}{27}$. Con el cambio, $y = z-\frac{p}{3z}$, obtenemos $z^3-\frac{p^3}{27z^3}+q = 0$ y multiplicando por z^3, $z^6+qz^3-\frac{p^3}{27} = 0$, luego $z^3 = \frac{-q\pm\sqrt{q^2+\frac{4p^3}{27}}}{2}$. Dejamos que el lector obtenga, con todo, las raíces de $x^3+a_1x^2+a_2x+a_3$.

El primer matemático en resolver la ecuación cúbica fue el italiano Scipione del Ferro (1465-1526), en 1515. Del Ferro mantuvo su descubrimiento en secreto y solo lo compartió en su lecho de muerte con su discípulo Antonio Maria Fiore. Años después, otro matemático italiano, Niccolò Tartaglia (c. 1500-1557), redescubrió una solución. Tartaglia también mantuvo su método en secreto, pero finalmente fue persuadido de compartirlo con el matemático Girolamo Cardano (1501-1576). Cardano, impresionado por la solución, prometió no divulgarla, aunque más tarde rompió su promesa al publicarla en su obra Ars Magna en 1545, atribuyendo el método a Tartaglia y a del Ferro. Lodovico Ferrero (1522-1565) dió la fórmula general de las raíces de una cuártica. La imposibilidad de una fórmula general (que use sumas, restas, multiplicaciones, divisiones y radicales) para ecuaciones de quinto grado (y superiores) son una consecuencia del teorema de Abel-Ruffini y de la teoría de Galois, que explica cómo las

propiedades de simetría en las raíces de las ecuaciones polinómicas determinan si pueden resolverse por radicales.

5. Definición: Dado un morfismo de anillos $k \to K$ entre cuerpos, diremos que K es una extensión (de cuerpos) de k.

En todo cuerpo k no hay más ideales que el ideal $\{0\}$ y todo k. Por lo tanto, todo morfismo de anillos $k \to K$ entre cuerpos (con $K \neq \{0\}$) es inyectivo. Dado un morfismo de cuerpos $k \to K$, escribiremos habitualmente $\lambda \mapsto \lambda$. Tenemos el morfismo de anillos obvio $k[x] \hookrightarrow K[x]$, $\sum_i \lambda_i x^i \mapsto \sum_i \lambda_i x^i$, todo polinomio $p(x) \in k[x]$ es obviamente un polinomio con coeficientes en K.

6. Teorema de Kronecker: *Sea $p(x) \in k[x]$ un polinomio de grado $n > 0$. Existe una extensión de cuerpos K de k en la que $p(x)$ descompone en factores simples, es decir, existen $\alpha_1, \ldots, \alpha_n \in K$ tales que*

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n), \qquad \lambda \in k.$$

Demostración. Procedamos por inducción sobre n. Si $n = 1$, basta tomar $K = k$, pues $p(x) = \lambda(x - \alpha)$, con $\alpha \in k$. Supongamos que $n > 1$. Sea $p_1(x) \in k[x]$ un polinomio irreducible que divida a $p(x)$. Sea $K_1 = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = p_1(\bar{x}) = \overline{p_1(x)} = 0$, luego $p(\alpha_1) = 0$. Por tanto, en $K_1[x]$ tenemos que $p(x) = (x - \alpha_1) \cdot p_2(x)$. Por hipótesis de inducción, existe una extensión $K_1 \hookrightarrow K$ de modo que $p_2(x) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Luego en K, que es una extensión de k,

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

□

Observemos que si $\lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n) = \mu \cdot (x - \beta_1) \cdots (x - \beta_n)$, entonces reordenando convenientemente los β_i, tendremos que $\alpha_i = \beta_i$, para todo i.

Dadas dos k-extensiones de cuerpos K y K', puede probarse que existe una extensión de cuerpos de k, L, que contiene a K y K' (véase problema 3). Por tanto, si K y K' son dos k-extensiones de cuerpos que contienen todas las raíces de $p(x)$ y consideramos una k-extensión L que contenga a K y K', entonces las raíces de $p(x)$ en K y K' han de coincidir en L.

El teorema fundamental del Álgebra, que probaremos más adelante, afirma que para todo polinomio $p(x) = a_0 x^n + \cdots + a_n \in \mathbb{C}[x]$ (con $a_0 \neq 0$ y $n > 0$) existen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ de modo que

$$p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

7. Definición: Sea $p(x) \in k[x]$ un polinomio y $\alpha \in k$. Se dice que $\alpha \in k$ es una raíz múltiple de $p(x)$ si $p(x)$ es múltiplo de $(x - \alpha)^2$. Se dice que $r > 0$ es la multiplicidad de una raíz de $p(x)$ si $p(x) = (x - \alpha)^r \cdot q(x)$, con $q(\alpha) \neq 0$.

8. Proposición: *Si $\alpha_1, \ldots, \alpha_s$ son raíces distintas de $p(x)$ con multiplicidad $n_1, \ldots, n_s$ respectivamente, entonces $p(x) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_s)^{n_s} \cdot q(x)$, con $q(\alpha_i) \neq 0$ para todo i. En particular el número de raíces de $p(x)$ en k, contando multiplicidades, es menor o igual que el grado de $p(x)$.*

9. Proposición: *Sea $p(x) \in k[x]$ un polinomio. Entonces, $\alpha \in k$ es una raíz múltiple de $p(x)$ si y solo si es raíz de $p(x)$ y $p'(x)$ (la derivada "formal" de $p(x)$).*

Demostración. Tenemos que α es una raíz de $p(x)$, entonces $p(x) = (x-\alpha)\cdot q(x)$ y $p'(x) = q(x) + (x-\alpha)\cdot q'(x)$. Por tanto, α es una raíz de $p'(x)$ si y solo si es raíz de $q(x)$, es decir, si y solo si α es una raíz múltiple de $p(x)$. □

Sea $k \hookrightarrow K$ una extensión de cuerpos y $p(x) \in k[x]$. Se dice que $\alpha \in K$ es raíz de $p(x)$ si $p(\alpha) = 0$. Igualmente, diremos que $\alpha \in K$ es una raíz de multiplicidad r si es una raíz de multiplicidad r de $p(x) \in K[x]$. Si $\alpha \in k$, la multiplicidad de $p(x)$ en α no varía si consideramos $\alpha \in k$ o $\alpha \in K$.

10. Proposición : *Sean $p(x), q(x) \in k[x]$ dos polinomios y $k \hookrightarrow K$ una extensión de cuerpos. El máximo común divisor de $p(x)$ y $q(x)$ en $k[x]$ coincide con el máximo común divisor de $p(x)$ y $q(x)$ en $K[x]$.*

Demostración. El máximo común divisor de dos polinomios $p(x)$ y $q(x)$ se puede calcular por el algoritmo de Euclides, cálculo que es el mismo si consideramos que estamos en $k[x]$ o si consideramos que estamos en $K[x]$.

□

11. Proposición: *Sean $p(x), q(x) \in k[x]$ dos polinomios y K una extensión de cuerpos de k donde estén todas las raíces de $p(x)$ y $q(x)$. Escribamos en $K[x]$*

$$p(x) = a_0 \cdot (x-\alpha_1)^{n_1} \cdots (x-\alpha_r)^{n_r}$$
$$q(x) = b_0 \cdot (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r}$$

con $\alpha_1, \ldots, \alpha_r \in K$ y $n_i, m_i \geq 0$, para todo i. Entonces,

$$m.c.d.(p(x), q(x)) = (x-\alpha_1)^{\min\{n_1,m_1\}} \cdots (x-\alpha_r)^{\min\{n_r,m_r\}}$$

Además, $p(x)$ y $q(x)$ son primos entre sí si y solo si no tienen raíces comunes (en K).

3.3. Teorema de las funciones simétricas

Sea $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = c(x-\alpha_1)\cdots(x-\alpha_n)$. Desarrollando el último término e igualando coeficientes de los x^i se obtiene las fórmulas de Cardano:

$$\begin{aligned}
a_0 &= c \\
a_1 &= -c\cdot(\alpha_1 + \cdots + \alpha_n) \\
&\cdots \\
a_i &= (-1)^i c \cdot \sum_{1\leq j_1<\cdots<j_i\leq n} \alpha_{j_1}\cdots\alpha_{j_i} \\
&\cdots \\
a_n &= (-1)^n c\cdot\alpha_1\cdots\alpha_n
\end{aligned}$$

1. Definición: Llamaremos *funciones simétricas elementales* (o polinomios simétricos elementales) en las letras $x_1,\dots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\dots,x_n]$ $(i = 1,\dots,n)$ definidos por:

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ &\cdots \\ s_i &= \sum_{1\le j_1<\cdots<j_i\le n} x_{j_1}\cdots x_{j_i} \\ &\cdots \\ s_n &= x_1\cdots x_n \end{aligned}$$

Se cumple la igualdad:

$$\prod_i (x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n.$$

Sea S_n el grupo de las permutaciones de n letras. Para cada $\sigma \in S_n$ consideremos el morfismo de anillos, $\sigma\colon A[x_1,\dots,x_n] \to A[x_1,\dots,x_n]$ definido por

$$\sigma(p(x_1,\dots,x_n)) := p(x_{\sigma(1)},\dots,x_{\sigma(n)}).$$

2. Definición: Diremos que un polinomio $p(x_1,\dots,x_n) \in A[x_1,\dots x_n]$ es simétrico cuando $\sigma(p(x_1,\dots,x_n)) = p(x_1,\dots,x_n)$ para toda $\sigma \in S_n$. Al conjunto de las funciones simétricas las denotaremos $A[x_1,\dots x_n]^{S_n}$.

3. Teorema de las funciones simétricas: *Se cumple la igualdad:*

$$A[x_1,\dots,x_n]^{S_n} = A[s_1,\dots,s_n].$$

Es decir, un polinomio en $x_1,\dots,x_n$ con coeficientes en el anillo A es invariante por todas las permutaciones de las variables si y solo si es un polinomio en las funciones simétricas elementales.

Demostración. Evidentemente todo polinomio en las funciones simétricas elementales es invariante por el grupo de las permutaciones. Por tanto, basta probar el recíproco.

Procedemos por inducción sobre el número n de variables. Para $n = 1$ es trivial. Sea $p(x_1,\dots,x_n) \in A[x_1,\dots,x_n]^{S_n}$. Descomponiendo $p(x_1,\dots,x_n)$ en la suma de sus componentes homogéneas, podemos suponer que $p(x_1,\dots,x_n)$ es homogéneo de grado m. Haciendo cociente por x_n se obtiene que $p(x_1,\dots,x_{n-1},0)$ es un polinomio homogéneo de grado m en $n-1$ variables e invariante por las permutaciones de éstas, luego $p(x_1,\dots,x_{n-1},0) = q'(s'_1,\dots,s'_{n-1})$, siendo s'_i la i-ésima función simétrica en las $n-1$ primeras variables. Cada sumando $\lambda_{m_1,\dots,m_{n-1}} s'^{m_1}_1 \cdots s'^{m_{n-1}}_{n-1}$ de $q'(s'_1,\dots,s'_{n-1})$ es un polinomio homogéneo en las variables $x_1,\dots,x_{n-1}$, de grado $m_1 + 2m_2 + \cdots + (n-1)m_{n-1}$. Podemos suponer que $\lambda_{m_1,\dots,m_{n-1}} = 0$, cuando $m_1 + 2m_2 + \cdots + (n-1)m_{n-1} \neq m$. Por tanto, $q'(s_1,\dots,s_{n-1})$ es un polinomio homogéneo en las variables $x_1,\dots,x_n$ de grado m. Sea $h(x_1,\dots,x_n) = p(x_1,\dots,x_n) - q'(s_1,\dots,s_{n-1})$. Se verifica que $h(x_1,\dots,x_n)$ es simétrico y homogéneo de grado m y se anula para $x_n = 0$ (ya que $s_i = s'_i \, mod\, x_n$), luego es múltiplo de x_n y por ser simétrico es múltiplo de $x_1\cdots x_n = s_n$, es decir,

$h(x_1,\dots,x_n) = s_n \cdot h'(x_1,\dots,x_n)$ y, por tanto, $h'(x_1,\dots,x_n)$ es simétrico también y homogéneo de grado $gr(h') = gr(h) - n = gr(p) - n < gr(p)$, luego por recurrencia sobre el grado m de p se concluye que $h'(x_1,\dots,x_n) = \widetilde{q}(s_1,\dots,s_n)$ y $h(x_1,\dots,x_n) = s_n \cdot \widetilde{q}(s_1,\dots,s_n)$. Por tanto,

$$p(x_1,\dots x_n) = q'(s_1,\dots,s_{n_1}) + h(x_1,\dots,x_n) = q'(s_1,\dots,s_{n-1}) + s_n \cdot \widetilde{q}(s_1,\dots,s_n)$$

con lo que se concluye. □

3.3.1. Teorema fundamental del Álgebra

4. Teorema: *Para todo polinomio $p(x) \in \mathbb{C}[x]$ de grado n existen $\alpha_1,\dots,\alpha_n \in \mathbb{C}$ de modo que*

$$p(x) = c \cdot (x-\alpha_1)\cdots(x-\alpha_n).$$

Demostración. Dado un polinomio cualquiera, $0 \neq p(x) \in \mathbb{C}[x]$, tenemos que probar que tiene una raíz en $\mathbb{C}$. Basta probar que todo polinomio con coeficientes reales tiene una raíz compleja, porque el producto de $p(x)$ por su conjugado, $q(x) = p(x) \cdot \overline{p(x)}$, es un polinomio con coeficientes reales y si α es una raíz de $q(x)$, entonces α o su conjugada es una raíz de $p(x)$. Si $q(x) \in \mathbb{R}[x]$ es un polinomio de grado impar entonces

$$\lim_{x\to+\infty} q(x) = -\lim_{x\to-\infty} q(x), \quad (\text{y } |\lim_{x\to+\infty} q(x)| = +\infty).$$

Luego por el teorema de Bolzano existe un $\alpha \in \mathbb{R}$ tal que $q(\alpha) = 0$. Supongamos que $\operatorname{gr} q(x) = r = 2^n \cdot m$, con m impar. Para probar que $q(x)$ tiene una raíz compleja procedamos por inducción sobre n. Para $n = 0$ lo hemos probado. Supongamos $n > 0$. Sean $\alpha_1,\dots,\alpha_r$ las raíces de $q(x)$ y fijado $\lambda \in \mathbb{R}$ sean $\beta_{ij} := \alpha_i + \alpha_j + \lambda\alpha_i \cdot \alpha_j$. El polinomio $h(x) := \prod_{i<j}(x-\beta_{ij}) \in \mathbb{R}[x]$, porque los coeficientes de $h(x)$ son funciones simétricas en $\alpha_1,\dots,\alpha_r$, luego por el teorema de las funciones simétricas, los coeficientes de $h(x)$ son polinomios en los coeficientes de $q(x)$. Observemos que $h(x)$ es un polinomio de grado $\binom{r}{2} = 2^{n-1} \cdot m \cdot (r-1) = 2^{n-1} \cdot m'$ con m' impar. Por inducción sobre n, cierto $\beta_{rs} = \alpha_r + \alpha_s + \lambda\alpha_r \cdot \alpha_s \in \mathbb{C}$. Variando el número real λ fijado (tómese $\binom{r}{2} + 1$ distintos), existirán $\lambda \neq \lambda'$, para los que existen r, s, de modo que

$$\alpha_r + \alpha_s + \lambda\alpha_r \cdot \alpha_s,\ \alpha_r + \alpha_s + \lambda'\alpha_r \cdot \alpha_s \in \mathbb{C}.$$

Luego $a := \alpha_r + \alpha_s$ y $b := \alpha_r \cdot \alpha_s \in \mathbb{C}$. Como α_r y α_s son las raíces de $(x-\alpha_r)(x-\alpha_s) = x^2 - ax + b$, tenemos que $\alpha_r, \alpha_s = (a \pm \sqrt{a^2-4b})/2 \in \mathbb{C}$. □

Se dice que un cuerpo k es algebraicamente cerrado si todas las raíces de todo polinomio $p(x) \in k[x]$ están en k. Entonces, el teorema fundamental del Álgebra dice que $\mathbb{C}$ es un cuerpo algebraicamente cerrado.

5. Corolario: *Si $\mathbb{R} \hookrightarrow K$ es una extensión de cuerpos tal que $\dim_{\mathbb{R}} K < \infty$, entonces $K = \mathbb{R}$ ó $\mathbb{C}$.*

Demostración. Supongamos que $\mathbb{R} \subsetneq K$. Sea $\alpha \in K - \mathbb{R}$ y $n = \dim_{\mathbb{R}} K$, entonces una combinación $\mathbb{R}$-lineal de $1, \alpha, \ldots, \alpha^n$ igual a cero, luego existe un polinomio de grado n que anula a α. Sea $p(x) \in \mathbb{R}[x]$ el polinomio mónico irreducible que anule a α. Sea $a+bi \in \mathbb{C}$, tal que $p(a+bi) = 0$. Tenemos el isomorfismo $\mathbb{R}[\alpha] = \mathbb{R}[x]/(p(x)) = \mathbb{R}[a+bi] = \mathbb{C}$. En conclusión, podemos suponer que $\mathbb{C} = \mathbb{R}[\alpha] \subseteq K$. Sea $\beta \in K$ y $q(x) \in \mathbb{C}[x]$ un polinomio mónico irreducible tal que $q(\beta) = 0$. Como $q(x)$ es mónico irreducible, $q(x) = x - c$, luego $\beta = c \in \mathbb{C}$. Luego, $K = \mathbb{C}$. □

3.4. Factorización en $\mathbb{Q}[x]$

1. Proposición: *Sean A y B anillos íntegros, $p(x) = \sum_{i=0}^{n} a_i \cdot x^{n-i} \in A[x]$ un polinomio primitivo y $f : A \to B$ un morfismo de anillos. Si $f(a_0) \neq 0$ y $q(x) = \sum_{i=0}^{n} f(a_i) \cdot x^{n-i} \in B[x]$ es irreducible, entonces $p(x)$ es irreducible.*

Demostración. La aplicación $F : A[x] \to B[x]$, $F(\sum_i c_i x^i) := \sum_i f(c_i) x^i$ es un morfismo de anillos. Supongamos que $p(x) = p_1(x) \cdot p_2(x)$. Entonces,

$$q(x) = F(p(x)) = F(p_1(x)) \cdot F(p_2(x)).$$

Como $q(x)$ tiene grado n y es irreducible, entonces podemos decir que $F(p_1(x))$ es de grado cero y $F(p_2(x))$ es de grado n. Por tanto, $p_1(x)$ tiene grado cero y $p_2(x)$ tiene grado n. Como $p(x)$ es primitivo, $p_1(x)$ es un invertible de A. En conclusión, $p(x)$ es irreducible.

□

2. Ejercicio: Calcula todos los polinomios de grado dos irreducibles de $\mathbb{Z}/2\mathbb{Z}[x]$. Demuestra que $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ es irreducible.

3. Criterio de Eisenstein: *Sea A un dominio de factorización única, $p \in A$ irreducible y $p(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in A[x]$ un polinomio. Si se cumple que*

1. *$p(x)$ es primitivo,*
2. *$a_1, \ldots, a_n$ son múltiplos de p*
3. *a_n no es múltiplo de p^2.*

entonces $p(x)$ es irreducible.

Demostración. Si $p(x) = c(x) \cdot d(x)$ es una descomposición propia, entonces por ser $p(x)$ primitivo es $n > gr\, c(x), gr\, d(x) > 0$. Sean $\overline{p(x)}, \overline{c(x)}, \overline{d(x)} \in (A/(p))[x]$ las clases de $p(x), c(x)$ y $d(x)$ módulo p. Por 2., es $\overline{p(x)} = \overline{a}_0 x^n$. Por tanto (ejercicio), $\overline{c(x)} = \overline{c}_{n-i} x^i$ y $\overline{d(x)} = \overline{d}_i x^{n-i}$ (con $n > n-i$ y $n > i$, es decir, $i, n-i > 0$). En particular, los términos independientes de $c(x), d(x)$ son múltiplos de p y, por tanto, el de $p(x)$ es múltiplo de p^2, lo que contradice 3.

□

4. Ejercicio: Prueba que $x^n - 2 \in \mathbb{Q}[x]$ es un polinomio irreducible, para todo $n > 0$.

5. Fórmula de interpolación de Lagrange: *Dados $\alpha_0, \ldots, \alpha_n \in k$ distintos entre sí y $\beta_0, \ldots, \beta_n \in k$ existe un único polinomio $p(x)$ de grado menor o igual que n tal que $p(\alpha_i) = \beta_i$, para todo i. Además,*

$$p(x) = \sum_{i=0}^{n} \beta_i \cdot \frac{(x-\alpha_0)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)}{(\alpha_i-\alpha_0)\cdots\widehat{(\alpha_i-\alpha_i)}\cdots(\alpha_i-\alpha_n)}.$$

Diremos que $p(x)$ es el polinomio de interpolación de $\alpha_0, \ldots, \alpha_n$ con valores $\beta_0, \ldots, \beta_n$.

Demostración. $p(x)$ es de grado menor o igual que n y $p(\alpha_i) = \beta_i$, para todo i.

Si $q(x)$ fuese otro polinomio tal que $q(\alpha_i) = \beta_i$ para todo i, entonces $p(x) - q(x)$ sería un polinomio de grado menor o igual que n con $n+1$ raíces:$\alpha_0, \ldots, \alpha_n$. Por tanto, $p(x) - q(x) = 0$ y $q(x) = p(x)$. □

6. Descomposición de un polinomio con coeficientes racionales en producto de polinomios irreducibles:

1. Dado $p(x) \in \mathbb{Q}[x]$, escribamos $p(x) = m \cdot q(x)$, con $m \in \mathbb{Q}$ y $q(x) \in \mathbb{Z}[x]$ primitivo. Para descomponer $p(x)$ en factores irreducibles basta descomponer $q(x)$ en factores irreducibles en $\mathbb{Z}[x]$.

2. Calculemos los polinomios $q_n(x) \in \mathbb{Z}[x]$, con $n = \operatorname{gr} q_n(x) \leq \operatorname{gr}(q(x))/2$, que dividen a $q(x)$: Todo polinomio de grado n, $r(x)$, coincide con el polinomio de interpolación de $0, 1, \ldots, n$ con valores $r(0), \ldots, r(n)$. Si $q(x) = q_n(x) \cdot q'(x)$, entonces $q_n(i)$ divide a $q(i)$. Observemos que solo hay un número finito de enteros que dividen al entero $q(i)$. Sea $Y = \{(\beta_0, \ldots, \beta_n) \in \mathbb{Z}^{n+1}\colon\ \beta_i$ divide a $q(i)$, para todo $i\}$, y para cada $y = (\beta_0, \ldots, \beta_n) \in Y$ sea $q_y(x)$ el polinomio de interpolación de $0, 1, \ldots, n$ con valores $\beta_0, \ldots, \beta_n$. $Y' = \{q_y(x)\colon\ y \in Y$ y $q_y(x)$ divide a $q(x)\}$ es el conjunto buscado que sabemos calcular.

3.4.1. Polinomios ciclotómicos

7. Definición: Sea k un cuerpo. Se dice que $\alpha \in k$ es una raíz n-ésima de la unidad si $\alpha^n = 1$. Se dice que α es una raíz n-ésima primitiva de la unidad si $\alpha^n = 1$ y $\alpha^m \neq 1$, para todo $0 < m < n$.

Sea α una raíz n-ésima de la unidad y $r = \operatorname{ord}(\alpha)$ el mínimo número natural (no nulo) tal que $\alpha^r = 1$, entonces el grupo (multiplicativo) generado por α es $\langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ y tiene orden r. Si $x^n - 1$ no tiene raíces múltiples (es decir, $n \neq 0$ en k), α es una raíz primitiva de la unidad si y solo si $\langle\alpha\rangle$ es el grupo de todas las raíces n-ésimas de la unidad.

Consideremos ahora $k = \mathbb{C}$. Observemos que

$$\mu_n := \{e^{k\cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i\,sen\,\frac{2k\pi}{n} \in \mathbb{C},\ 0 \leq k < n\},$$

es el conjunto de todas las raíces n-ésimas de la unidad, que es un subgrupo (multiplicativo) de $\mathbb{C}^*$, de orden n. El morfismo

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n,\ \bar{m} \mapsto e^{m\cdot 2\pi i/n}$$

es un isomorfismo de grupos. Vía este isomorfismo, el conjunto de generadores $\mathbb{Z}/n\mathbb{Z}$ se identifica con el conjunto $R_n \subset \mu$, de todas las raíces n-ésimas primitivas de la unidad ($R_n = \{\varepsilon \in \mu_n$ tales que $\varepsilon^m \neq 1$ para cada $m < n\}$). El conjunto de generadores de $\mathbb{Z}/n\mathbb{Z}$ se identifica con los invertibles de $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z}, (k,n) = (1)\}$. Luego,

$$R_n = \{e^{k\cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i\,sen\,\frac{2k\pi}{n},\ \text{con}\ \ 0 < k < n \text{ y } (k,n) = (1)\}.$$

8. Definición: Para cada $n \in \mathbb{N}$ se denomina n-ésimo *polinomio ciclotómico* al polinomio mónico

$$\Phi_n(x) = \prod_{k<n,(k,n)=(1)} (x - e^{k\cdot 2\pi i/n}).$$

Se cumple $\xi \in \mathbb{C}$ es una raíz n-ésima de la unidad si y solo si ξ es una raíz primitiva d-ésima de la unidad para algún $d|n$. Por tanto,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Luego,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n,d|n} \Phi_d(x)}.$$

Por recurrencia se demuestra que $\Phi_n(x) \in \mathbb{Z}[x]$ (obsérvese que $\Phi_1(x) = x - 1$).

Dejamos que el lector pruebe la siguiente proposición.

9. Proposición: *Se cumple*

1. $\Phi_1(x) = x - 1$.
2. $\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = x + 1$.
3. $\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = x^2 + x + 1$.
4. $\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\cdot\Phi_2(x)} = x^2 + 1$.
5. $\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1$.
6. $\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\cdot\Phi_2(x)\cdot\Phi_3(x)} = x^2 - x + 1$.
7. *Si* $p > 0$ *es primo,* $\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = x^{p-1} + x^{p-2} + \cdots + x + 1$.
8. *Si* $p > 0$ *es primo,* $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}}) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1$. *También,* $\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1}$.

9. *Si $p>0$ es primo y r no es divisible por p, $\Phi_{r\cdot p^n}(x)=\frac{\Phi_r(x^{p^n})}{\Phi_r(x^{p^{n-1}})}$: Las raíces de $\Phi_r(x^{p^n})$ son aquellas $\alpha\in\mathbb{C}$ tales que $\operatorname{ord}(\alpha^{p^n})=r$, es decir, aquellas $\alpha\in\mathbb{C}$ tales que $\operatorname{ord}(\alpha)=r\cdot p^i$, con $i\leq n$. Por tanto,*

$$\begin{aligned}\{\textit{Raíces de } \Phi_r(x^{p^n})\}\setminus\{\textit{Raíces de } \Phi_r(x^{p^{n-1}})\}&=\{\alpha\in\mathbb{C}\colon \operatorname{ord}(\alpha)=r\cdot p^n\}\\&=\{\textit{Raíces de } \Phi_{r\cdot p^n}(x)\}\end{aligned}$$

y hemos terminado.

10. *Si r es impar, $\Phi_{2r}(x)=\pm\Phi_r(-x)$: Si $\operatorname{ord}(\alpha)=2r$ entonces $\alpha^r=-1$, luego $(-\alpha)^r=1$ y $\operatorname{ord}(-\alpha)=r$. Por tanto, las raíces de $\Phi_{2r}(x)$ son raíces de $\Phi_r(-x)$ y como $\operatorname{gr}(\Phi_{2r}(x))=\phi(2r)=\phi(2)\phi(r)=\phi(r)=\operatorname{gr}\Phi_r(-x)$ hemos terminado.*

10. Lema: *Sea $p\in\mathbb{N}$ un número primo. Para todo $q(x)\in\mathbb{Z}/p\mathbb{Z}[x]$ se cumple que*

$$q(x)^p=q(x^p).$$

Demostración. Para cada $a\in\mathbb{Z}/p\mathbb{Z}$ es $a^p=a$ y $(r(x)+s(x))^p=r(x)^p+s(x)^p$, para cada $r(x),s(x)\in\mathbb{Z}/p\mathbb{Z}[x]$, luego

$$q(x)^p=(a_0+a_1x+\cdots a_nx^n)^p=a_0^p+a_1^px^p+\cdots a_n^p(x^p)^n=q(x^p).$$

□

11. Teorema: *Los polinomios ciclotómicos $\Phi_n(x)\in\mathbb{Z}[x]$ son polinomios irreducibles.*

Demostración. Supongamos que $\Phi_n(x)=p(x)\cdot q(x)$. Sea p un número primo que no divida a n. Veamos que si ε es raíz de $p(x)$ entonces ε^p es también raíz de $p(x)$: Observemos que ε^p es una raíz n-ésima primitiva de la unidad, luego es raíz de $\Phi_n(x)$. Si ε^p es raíz de $q(x)$, entonces, los polinomios $p(x)$ y $q(x^p)$ tienen la raíz ε en común, luego no son primos entre sí. Entonces, en $\mathbb{Z}/p\mathbb{Z}[x]$, $\overline{p(x)}$ y $\overline{q(x^p)}=\overline{q(x)}^p$ no son primos entre sí. Por tanto, $\overline{p(x)}$ y $\overline{q(x)}$ no son primos entre sí, y $\overline{\Phi_n(x)}=\overline{p(x)}\cdot\overline{q(x)}$ tiene raíces múltiples. Entonces, $x^n-\bar{1}\in\mathbb{Z}/p\mathbb{Z}[x]$ tiene raíces múltiples. Pero, $x^n-\bar{1}$ es primo con su derivada $\bar{n}\cdot x^{n-1}$ (donde $\bar{n}\neq 0$, porque p no divide a n), lo que implica que no tiene raíces múltiples. Hemos llegado a contradicción, luego ε^p no es raíz de $q(x)$ y ha de ser raíz de $p(x)$.

Sin pérdida de generalidad, podemos suponer que $e^{\frac{2\pi i}{n}}$ es raíz de $p(x)$. Sea $e^{\frac{2m\pi i}{n}}$ una raíz primitiva de la unidad, luego m es primo con n y $m=p_1\cdots p_r$, donde los primos p_i no dividen a n. Por el párrafo anterior, $e^{\frac{2p_1\pi i}{n}}$ es raíz de $p(x)$, luego $e^{\frac{2p_1p_2\pi i}{n}}$ es raíz de $p(x)$ y así sucesivamente obtenemos que $e^{\frac{2m\pi i}{n}}$ es raíz de $p(x)$. En conclusión, $\Phi_n(x)=p(x)$.

□

12. Proposición: $\mathbb{Q}[e^{\frac{2\pi i}{n}}]\simeq\mathbb{Q}[x]/(\Phi_n(x))$.

Demostración. El polinomio mónico con coeficientes en $\mathbb{Q}$ mínimo anulador de $e^{\frac{2\pi i}{n}}$ es $\Phi_n(x)$, por el teorema 3.4.11 y el lema 2.6.3. Luego, $\mathbb{Q}[e^{\frac{2\pi i}{n}}]\simeq\mathbb{Q}[x]/(\Phi_n(x))$. □

3.5. Separación de las raíces

3.5.1. Acotación de las raíces

1. Sea $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{C}[x]$ no nulo. Queremos encontrar un número real $L > 0$, que llamaremos cota (de las raíces) de $P(x)$, de modo que si $\alpha \in \mathbb{C}$ es una raíz de $P(x)$ entonces $|\alpha| < L$.

Cota de MacLaurin: Una cota de $P(x)$ es $L = 1 + \text{máx}\{|a_1|, \ldots, |a_n|\}$, porque si $|z| \geq L$,

$$|P(z)| \geq |z|^n - |a_1||z|^{n-1} - \cdots - |a_n| \geq |z|^n - (|z|-1)|z|^{n-1} - \cdots - (|z|-1) = 1.$$

2. Sea $P(x) = x^n + a_1 x^{n-1} \cdots + a_n \in \mathbb{R}[x]$ no nulo. Queremos encontrar un número real L, que llamaremos cota superior (de las raíces reales) de $P(x)$, de modo que si $r \in \mathbb{R}$ es una raíz de $P(x)$ entonces $r < L$.

Cota superior de Newton: Si $P(a), P'(a), \ldots, P^{n)}(a) \geq 0$, entonces $L = a$ es una cota superior: $P(x) = \sum_{i=0}^{n} P^{i)}(a)\frac{(x-a)^i}{i!}$, luego $P(r) > 0$, para todo $r \geq a$.

Cota superior de Lagrange: Sea $N = \text{máx}\{|a_i| : a_i \leq 0\}$. Si a_s es el primer coeficiente negativo, una cota superior de $P(x)$ es $L = 1 + \sqrt[s]{N}$, porque si $r \geq L$,

$$P(r) = r^n + a_1 r^{n-1} + \cdots + a_n \geq r^n - (r-1)^s r^{n-s} - \cdots - (r-1)^s = r^n - \frac{(r-1)^s r^{n-s+1} - (r-1)^s}{r-1}$$
$$= r^n - (r-1)^{s-1} \cdot (r^{n-s+1} - 1) > r^n - r^{s-1} \cdot r^{n-s+1} = 0.$$

Observación Se dice que $I \in \mathbb{R}$ es una cota inferior (de las raíces reales) de $P(x) \in \mathbb{R}[x]$, si I es menor o igual que toda raíz real de $P(x)$. I es una cota inferior de $P(x)$ si y solo si $-I$ es una cota superior de $P(-x)$.

3.5.2. Exceso de una función racional real

En esta sección los polinomios considerados son con coeficientes reales.

Sea una función racional $f(x) = \frac{P(x)}{Q(x)}$ (con P y Q primos entre sí). Diremos que $f(x)$ tiene un polo en $a \in \mathbb{R}$ cuando a sea raíz de Q. Diremos que la multiplicidad de f en el polo a es n si ésta es la multiplicidad de a como raíz de Q.

Escribamos $f(x) = \tilde{f}(x) \cdot \frac{1}{(x-a)^n}$ siendo n la multiplicidad de f en el polo a y $0 \neq \tilde{f}(a) \in \mathbb{R}$.

3. Definición: Llamaremos exceso de $f(x) = \frac{P(x)}{Q(x)}$ en $a \in \mathbb{R}$, al número:

$$E_a(f) = \begin{cases} 1 \text{ si } a \text{ es un polo de } f \text{ de multiplicidad impar y } \tilde{f}(a) > 0. \\ -1 \text{ si } a \text{ es un polo de } f \text{ de multiplicidad impar y } \tilde{f}(a) < 0. \\ 0 \text{ si } f(x) \text{ no tiene polo en } a \text{ o es de multiplicidad par.} \end{cases}$$

De otro modo: el exceso de f en a es 1, si $f(x)$ pasa de $-\infty$ a ∞ al pasar x por a de izquierda a derecha; el exceso de f en a es 1, si $f(x)$ pasa de ∞ a $-\infty$ al pasar x por a

de izquierda a derecha el exceso es -1; y el exceso de f en a es cero en cualquier otro caso.

4. Definición: Dados $a,b\in\mathbb{R}$ y $f(x)$ una función racional, llamaremos exceso de $f(x)$ entre a y b a la suma de los excesos de $f(x)$ en sus polos contenidos en (a,b):

$$E_a^b(f)=\sum_{t\in(a,b)}E_t(f).$$

5. Evidentemente, si $a<c<b$ y $f(x)$ no tiene polos en c, entonces

$$E_a^b(f)=E_a^c(f)+E_c^b(f).$$

Si f y g son dos funciones racionales sin polos comunes en (a,b) entonces

$$E_a^b(f+g)=E_a^b(f)+E_a^b(g).$$

Si P es un polinomio entonces $E_a^b(P)=0$.

Veamos qué relación hay entre las raíces de un polinomio y el exceso.

6. Proposición: *Sean $a<b$ números reales y $P\in\mathbb{R}[x]$. Entonces,*

$$E_a^b(\frac{P'}{P})=N^o \text{ de raíces reales distintas de } P \text{ en } (a,b).$$

Demostración. Sean $\alpha_1,\dots,\alpha_r$ las raíces complejas (distintas) de P. Entonces $P(x)=a_0\cdot\prod_{i=1}^{r}(x-\alpha_i)^{n_i}$ y $P'(x)=a_0\cdot\sum_{i=1}^{r}n_i\cdot(x-\alpha_i)^{n_i-1}\prod_{j\neq i}(x-\alpha_j)^{n_j}$ y

$$\frac{P'}{P}=\sum_i\frac{n_i}{x-\alpha_i}.$$[1]

Por tanto, si α_i es real, entonces $E_{\alpha_i}\frac{P'}{P}=1$. Luego, el número de raíces distintas en (a,b) coincide con $E_a^b\frac{P'}{P}$.

□

Por tanto, el cálculo del número de raíces de P se reduce al cálculo de $E_a^b(\frac{P'}{P})$. El teorema 3.5.9 (y su corolario: el teorema de Sturm) resolverá este problema.

Dado un número real no nulo $r\in\mathbb{R}$, diremos que $\operatorname{sign}(r)=1$ si $r>0$ y $\operatorname{sign}(r)=-1$ si $r<0$.

7. Definiciones: Dados dos números reales no nulos a,b se define

$$V(a,b):=\begin{cases}1 \text{ si } \operatorname{sign}a\neq\operatorname{sign}b.\\ 0 \text{ si } \operatorname{sign}a=\operatorname{sign}b.\end{cases}$$

Dados números reales no nulos $a_1,\dots,a_n$ llamaremos variaciones de signo de dicha sucesión al número:

$$V(a_1,\dots,a_n):=\sum_i V(a_i,a_{i+1}),$$

[1] De otro modo: $\frac{P'}{P}=(\ln P)'=(\sum_i n_i\ln(x-\alpha_i))'=\sum_i\frac{n_i}{x-\alpha_i}$.

Si algunos términos a_i (con $1 < i < n$) son nulos se define las variaciones de signo $V(a_1,\dots,a_n)$ suprimiendo los términos nulos. Por ejemplo,

$$V(1,0,0,-1,0,3,1) = V(1,-1,3,1) = 2.$$

Dados dos números reales a,b y n polinomios reales $P_1,\dots,P_n$ (supongamos que P_1 y P_n no se anulan en a ni en b), definimos

$$V_a^b(P_1,\dots,P_n) := V(P_1(a),\dots,P_n(a)) - V(P_1(b),\dots,P_n(b)).$$

8. Evidentemente, dados tres números reales a,b,c (suponemos que P_1 y P_n no se anulan en a, ni en b ni en c) se cumple que

$$V_a^b(P_1,\dots,P_n) = V_a^c(P_1,\dots,P_n) + V_c^b(P_1,\dots,P_n).$$

9. Teorema : *Sean $a < b$ dos números reales y P,Q dos polinomios reales que no se anulan en a ni en b, entonces*

$$E_a^b(\frac{P}{Q}) + E_a^b(\frac{Q}{P}) = V_a^b(P,Q).$$

Demostración. Se puede suponer que P y Q son primos entre sí, pues los factores comunes se pueden suprimir sin que altere la fórmula. Sean $a = a_1 < a_2 < \cdots < a_n = b$ tales que $P\cdot Q$ tiene a lo más una raíz (múltiple o no) en (a_i,a_{i+1}) y $(P\cdot Q)(a_i) \neq 0$, para todo i. Basta probar que

$$E_{a_i}^{a_{i+1}}(\frac{P}{Q}) + E_{a_i}^{a_{i+1}}(\frac{Q}{P}) = V_{a_i}^{a_{i+1}}(P,Q),$$

para todo i, por 3.5.5 y 3.5.8. Intercambiando P por Q si es necesario, podemos suponer que P no tiene raíces en (a_i,a_{i+1}), luego $E_{a_i}^{a_{i+1}}(\frac{Q}{P}) = 0$. Cambiando, si es necesario, P y Q por $-P$ y $-Q$ podemos suponer que $P > 0$ en (a_i,a_{i+1}). Tenemos

$$E_{a_i}^{a_{i+1}}(\frac{P}{Q}) + E_{a_i}^{a_{i+1}}(\frac{Q}{P}) = E_{a_i}^{a_{i+1}}(\frac{P}{Q}) \overset{*}{=} V_{a_i}^{a_{i+1}}(P,Q),$$

donde $\overset{*}{=}$ es fácil de probar. □

10. Sea $P(x) \in \mathbb{R}[x]$ y supongamos que $P'(x)$ no tiene raíces en (a,b) y que $P(a)\cdot P(b) \neq 0$. Entonces,

$$\text{Nº de raíces de } P(x) \text{ en } (a,b) = E_a^b(\frac{P'}{P}) = |E_a^b(\frac{1}{P})| = |V_a^b(P,1)| = V(P(a),P(b))$$

De otro modo: $P(x)$ es estrictamente creciente (o decreciente) en el intervalo (a,b), luego tendrá una (resp. ninguna) raíz si $V(P(a),P(b)) = 1$ (resp. $V(P(a),P(b)) = 0$).

Si $P(x)$ no tiene raíces múltiples, entonces las raíces reales de $P'(x)$ separan las raíces reales de $P(x)$. La dificultad está en el cálculo de las raíces α_i de $P'(x)$ (y en el cálculo de $P(\alpha_i)$).

3.5.3. Número de raíces reales en un intervalo

Veamos que el teorema anterior nos da un modo de calcular, vía el algoritmo de Euclides, el exceso de una función racional y por ende un modo de calcular el número de raíces de un polinomio en un intervalo.

Sean P,Q dos polinomios con coeficientes reales y consideremos los restos R_i obtenidos en el algoritmo de Euclides (cambiados de signo):

$$\begin{aligned} P &= C_1Q - R_1\\ Q &= C_2R_1 - R_2\\ &\cdots\\ R_{n-2} &= C_nR_{n-1} - R_n\\ R_{n-1} &= C_{n+1}R_n \end{aligned}$$

Se dice que los $\{R_i\}$ son los restos de Sturm de P y Q.

11. Teorema : *Sean $a<b$ dos números reales, P,Q dos polinomios con coeficientes reales y supongamos que P no se anula en a ni en b, entonces:*

$$E_a^b\frac{Q}{P} = V_a^b(P,Q,R_1,\ldots,R_n).$$

Demostración. (1) Supongamos que Q y los restos de Sturm no se anulan en a ni en b.

Procedamos por inducción sobre n. Para $n=0$, es decir, P es múltiplo de Q, $E_a^b\frac{Q}{P} \overset{3.5.9}{=} V_a^b(P,Q) - E_a^b\frac{P}{Q} = V_a^b(P,Q)$. Sea $n>0$. De la igualdad $P = C_1Q - R_1$ se obtiene $\frac{P}{Q} = C_1 - \frac{R_1}{Q}$, luego $E_a^b\frac{P}{Q} = -E_a^b\frac{R_1}{Q}$. Aplicando esta igualdad e inducción se obtiene:

$$\begin{aligned} E_a^b\frac{Q}{P} &\overset{3.5.9}{=} V_a^b(P,Q) - E_a^b\frac{P}{Q} = V_a^b(P,Q) + E_a^b\frac{R_1}{Q}\\ &= V_a^b(P,Q) + V_a^b(Q,R_1,\ldots,R_n) = V_a^b(P,Q,R_1,\ldots,R_n). \end{aligned}$$

(2) Supongamos que $Q =: R_0$ o algún resto de Sturm se anula en a o en b.

Se observa que no puede haber dos términos consecutivos $R_i(a) = R_{i+1}(a) = 0$, pues entonces $x-a$ sería divisor del máximo común divisor de R_i y R_{i+1}, y por tanto de P, contradiciendo la hipótesis del teorema. Igualmente, no puede ser que $R_i(b) = R_{i+1}(b) = 0$. Por la misma razón $R_n(a)\neq 0$ y $R_n(b)\neq 0$. Por otro lado, si $R_i(a)=0$, como $R_{i-1} = C_{i+1}R_i - R_{i+1}$, se tiene que $R_{i-1}(a)$ y $R_{i+1}(a)$ son de signo contrario. Igualmente, si $R_i(b)=0$, entonces $R_{i-1}(b)$ y $R_{i+1}(b)$ son de signo contrario.

Modifiquemos $a \rightsquigarrow a' = a+\epsilon$ y $b \rightsquigarrow b' = b-\epsilon$ ligeramente de manera que: $E_a^b\frac{Q}{P} = E_{a'}^{b'}\frac{Q}{P}$, $R_i(a')\neq 0$ (y $R_i(b')\neq 0$) para todo i, y $\operatorname{sign}(R_j(a)) = \operatorname{sign}(R_j(a'))$ cuando $R_j(a)\neq 0$ (y $\operatorname{sign}(R_j(b)) = \operatorname{sign}(R_j(b'))$ cuando $R_j(b)\neq 0$). Si $R_i(a)=0$ entonces

$$V(R_{i-1}(a'),R_i(a'),R_{i+1}(a')) = 1 = V(R_{i-1}(a),R_{i+1}(a)) = V(R_{i-1}(a),R_i(a),R_{i+1}(a)),$$

ya que $\operatorname{sign}(R_{i-1}(a')) = \operatorname{sign}(R_{i-1}(a)) = -\operatorname{sign}(R_{i+1}(a)) = -\operatorname{sign}(R_{i+1}(a'))$. Igualmente, si $R_i(b)=0$ entonces $V(R_{i-1}(b'),R_i(b'),R_{i+1}(b')) = V(R_{i-1}(b),R_i(b),R_{i+1}(b))$. Por tanto,

$$E_a^b\frac{Q}{P} = E_{a'}^{b'}\frac{Q}{P} \overset{(1)}{=} V_{a'}^{b'}(P,Q,R_1,\ldots,R_n) = V_a^b(P,Q,R_1,\ldots,R_n).$$

□

12. Teorema de Sturm: *Sean $a < b$ dos números reales, P un polinomio con coeficientes reales que no se anula en a ni en b y $\{R_1,\dots,R_n\}$ los restos de Sturm para P y su derivada P'. Entonces,*

$$N^o \text{ de raíces reales distintas de } P \text{ en } (a,b) = V_a^b(P,P',R_1,\dots,R_n).$$

Demostración. Es consecuencia del teorema anterior y la proposición 3.5.6.

□

13. Una vez que sabemos que todas las raíces reales de $P(x)$ están incluidas en un intervalo (a,b), el teorema de Sturm nos da el procedimiento para separarlas[2]: Supongamos que $P(x)$ no tiene raíces múltiples en (a,b). Consideremos los intervalos $(a,\frac{a+b}{2})$ y $(\frac{a+b}{2},b)$ (supongamos por sencillez que $P((a+b)/2) \neq 0$). Por el teorema de Sturm sabemos calcular el número de raíces reales de $P(x)$ en cada uno de los dos intervalos. Dividiendo sucesivamente en dos los intervalos que contengan más de una raíz, consiguiremos separar las raíces.

14. Observación: Sean P y Q primos entre sí, supongamos que P no se anula en a ni en b y sea $r_a^b(P)$ el número de raíces reales de P (contadas con su multiplicidad) en (a,b). Entonces,

$$\pm E_a^b \frac{Q}{P} \leq r_a^b(P).$$

Además, como $1 = -1 mod\, 2$, se cumple la igualdad $E_a^b \frac{Q}{P} = r_a^b(P) \mod 2$.

En particular,

$$r_a^b(P) = E_a^b(\frac{1}{P}) \mod 2 = V_a^b(P,1) \mod 2 = V(P(a),P(b)) \mod 2.$$

15. Si P en un intervalo (a,b) tiene una raíz o ninguna (contando multiplicidades) y $(c,d) \subset (a,b)$ (y suponemos $P(c),P(d) \neq 0$), entonces $r_c^d(P) = V(P(c),P(d))$.

16. Si $V(P(a),P(b)) = 1$ y $P(a),P(b) \neq 0$, entonces $P(x)$ tiene un número impar de raíces en el intervalo (a,b). Consideremos los intervalos $(a,\frac{a+b}{2})$ y $(\frac{a+b}{2},b)$ (supongamos por sencillez que $P((a+b)/2) \neq 0$). Entonces, o $V(P(a),P(\frac{a+b}{2})) = 1$, o bien $V(P(\frac{a+b}{2}),P(b)) = 1$. De nuevo, $P(x)$ tiene un número impar de raíces en $(a,\frac{a+b}{2})$, o bien en $(\frac{a+b}{2},b)$. Reiterando este proceso calcularemos aproximadamente una raíz de $P(x)$ en (a,b). Existen otros métodos de aproximación, como el método de aproximación de Newton o *regula falsi* que el lector conocerá del Análisis Numérico.

17. Si sabemos calcular las raíces reales de un polinomio real entonces sabemos calcular las raíces reales de un polinomio complejo: Sea $P(x) \in \mathbb{C}[x]$ y consideremos el producto de este polinomio por su conjugado, $Q(x) = P(x) \cdot \overline{P(x)} \in \mathbb{R}[x]$ (o consideremos $Q(x) = m.c.d.(P(x),\overline{P(x)}) \in \mathbb{R}[x]$). Las raíces reales de $P(x) \in \mathbb{C}[x]$ coinciden con las raíces reales de $Q(x) \in \mathbb{R}[x]$.

[2] No hacemos un análisis de la dificultad intrínseca del cálculo de los polinomios de Sturm.

18. Teorema de Budan-Fourier: *Sea P un polinomio con coeficientes reales de grado n que no se anula en a ni en b, y r_a^b el número de raíces reales de P en $[a,b]$ (contadas con su multiplicidad).. Se cumple la acotación:*

$$r_a^b(P) \le V_a^b(P,P',P'',\dots,P^{n)}).$$

Además esta desigualdad es una igualdad módulo 2.

Demostración. Procedemos por recurrencia sobre el grado n del polinomio P. Si $n=1$ entonces $r_a^b(P) \overset{3.5.12}{=} V_a^b(P,P')$.

(1) Supongamos que todas las raíces reales de P son simples y que P y sus derivadas iteradas no se anulan en a ni en b. Entonces,

$$\begin{aligned} r_a^b(P) &\overset{3.5.6}{=} E_a^b\frac{P'}{P} \overset{3.5.9}{=} V_a^b(P,P') - E_a^b\frac{P}{P'} \le V_a^b(P,P') + r_a^b(P') \\ &\le V_a^b(P,P') + V_a^b(P',P'',\dots,P^{n)}) = V_a^b(P,P',P'',\dots,P^{n)}). \end{aligned}$$

Las desigualdades son igualdades módulo 2 por serlo la primera (por la observación 3.5.14) y serlo la segunda por recurrencia.

(2) Supongamos ahora que P y sus derivadas iteradas no se anulan en a ni en b. Sustituyendo cada factor $(x-\alpha_i)^{s+1}$ de P (con $\alpha_i \in \mathbb{R}$) por $(x-\alpha_i)(x-\alpha_i-\epsilon)\cdots(x-\alpha_i-s\epsilon)$ con ϵ pequeño, se obtiene otro polinomio Q con raíces simples tal que $r_a^b Q = r_a^b P$ y $V_a^b(Q,Q',Q'',\dots,Q^{n)}) = V_a^b(P,P',P'',\dots,P^{n)})$. Por tanto,

$$r_a^b(P) = r_a^b Q \overset{(1)}{\le} V_a^b(Q,Q',Q'',\dots,Q^{n)}) = V_a^b(P,P',P'',\dots,P^{n)})$$

y se cumple la igualdad módulo 2.

(3) Por último, supongamos que alguna derivada iterada de P se anula en a (igualmente en b). Vamos a ver que cambiando infinitesimalmente a (y b), estamos en las condiciones de (2) y no cambia el número de raíces de P (evidentemente) ni el número de las variaciones de signo de P y sus derivadas iteradas. Haciendo el cambio de variable $x' = x-a$ se puede suponer $a=0$. Haciendo el cambio $a=0 \rightsquigarrow a=\epsilon>0$ se puede suponer que $\operatorname{sign}(P^{i)}(0) = \operatorname{sign}(P^{i)}(\epsilon))$, para todo ϵ pequeño, cuando $P^{i)}(0)\neq 0$. Supongamos que

$$P^{i-1)}(0)\neq 0, \quad P^{i)}(0) = \cdots = P^{i+h-1)}(0) = 0, \quad P^{i+h)}(0)\neq 0.$$

Entonces es $P^{i)}(x) = x^h(\mu+\gamma x+\cdots)$ y por tanto $P^{i+r)}(x) = c_r x^{h-r}(\mu+\gamma' x+\cdots)$ (siendo $c_r = h(h-1)\cdots(h-r+1)>0$) para $r\le h$. Por tanto, para ϵ suficientemente pequeño y $r\le h$ es $\operatorname{sign} P^{i+r)}(\epsilon) = \operatorname{sign}\mu$, de donde

$$\begin{aligned} &V(P^{i-1)}(\epsilon),P^{i)}(\epsilon),\dots,P^{i+h-1)}(\epsilon),P^{i+h)}(\epsilon)) = V(P^{i-1)}(\epsilon),\mu,\dots,\mu,\mu) \\ &= V(P^{i-1)}(0),0,\dots,0,P^{i+h)}(0)) = V(P^{i-1)}(0),P^{i)}(0),\dots,P^{i+h-1}(0),P^{i+h)}(0)). \end{aligned}$$

Luego, $V(P(\epsilon),P'(\epsilon),\dots,P^{n)}(\epsilon)) = V(P(0),P'(0),\dots,P^{n)}(0))$ y se concluye. □

19. Teorema de Descartes: *Sea $P(x) = a_0x^n + \cdots a_{n-1}x + a_n$ un polinomio con coeficientes reales de grado n sin la raíz 0 (i.e. $a_n \neq 0$). Entonces,*

$$r_0^{+\infty}(P) \leq V(a_0, a_1, \ldots, a_n)$$

y es una igualdad módulo 2 (es decir, ambos números tienen la misma paridad).

Demostración. Basta aplicar el teorema de Budan-Fourier teniendo en cuenta que $a_i = P^{n-i)}(0)/(n-i)!$ y que $\operatorname{sign} P^{i)}(+\infty) = \operatorname{sign} a_0$ (es decir, no depende de i y, por tanto, sus variaciones son nulas).

□

Haciendo el cambio $x \mapsto -x$ y aplicando el teorema de Descartes se concluye que

$$r_{-\infty}^0(P(x)) = r_0^{+\infty}(P(-x)) \leq V(a_0, -a_1, \ldots, (-1)^n a_n)$$

y es una igualdad módulo 2.

20. Corolario: *Si todas las raíces de P son reales (y no nulas), entonces:*

$$r_0^{+\infty}(P) = V(a_0, a_1, \ldots, a_n) \quad y \quad r_{-\infty}^0(P) = V(a_0, -a_1, \ldots, (-1)^n a_n)$$

y además $P(x)$ no puede tener dos coeficientes consecutivos nulos.

Demostración. Por el teorema de Descartes,

$$n = r_0^{+\infty}(P) + r_{-\infty}^0(P) \leq V(a_0, a_1, \ldots, a_n) + V(a_0, -a_1, \ldots, (-1)^n a_n)$$

Es fácil ver que el último sumando es siempre menor o igual que n, y que si es n no puede haber dos coeficientes consecutivos nulos. Ahora es fácil concluir. □

Este corolario se usa en Álgebra Lineal para determinar cuándo una métrica simétrica es euclídea: Todos los autovalores de las matrices simétricas con coeficientes reales son reales, y la matriz simétrica es euclídea si y solo si todos los autovalores son estrictamente positivos. Por el corolario, la métrica simétrica es euclídea si y solo si $V(a_0, a_1, \ldots, a_n) = n$, donde $P(x) = a_0x^n + \cdots + a_{n-1}x + a_n$ es el polinomio característico asociado a la matriz.

3.5.4. Número de raíces complejas en un rectángulo

Orientemos S^1 en sentido anti-horario. Dados $a, b \in S^1$ denotemos $[a, b]$ el arco bien orientado de S^1 que empieza en a y acaba en b.

Sea $f\colon S^1 \to S^1 = \mathbb{R} \amalg \infty$ una función continua tal que $f^{-1}(\infty)$ sea unión de un número finito (o nulo) de intervalos cerrados.

Si p es un polo aislado de f, es decir, p es un abierto de $f^{-1}(\infty)$, definimos $E_p(f)$ del modo usual: $E_p(f) = 1$ si $\lim_{x \to p^-} f(x) = -\infty$ y $\lim_{x \to p^+} f(x) = +\infty$, etc. Si $[p, b]$ es un abierto de $f^{-1}(\infty)$, diremos que $E_p(f) = \frac{1}{2}$ si $\lim_{x \to p^-} f(x) = -\infty$ y diremos que $E_p(f) = \frac{-1}{2}$ si $\lim_{x \to p^-} f(x) = +\infty$. Si $[a, p]$ es un abierto de $f^{-1}(\infty)$, diremos que $E_p(f) = \frac{1}{2}$ si $\lim_{x \to p^+} f(x) =$

$+\infty$ y diremos que $E_p(f) = \frac{-1}{2}$ si $\lim_{x\to p^+} f(x) = -\infty$. Si p no es un polo o $f^{-1}(\infty)$ es un entorno de p, entonces diremos que $E_p(f) = 0$

Dado un intervalo $[a,b]$, tal que a y b no son polos, se define $E_a^b(f) = \sum_{p\in[a,b]} E_p(f)$. Si $c \in [a,b]$ no es un polo, entonces $E_a^b(f) = E_a^c(f) + E_a^c(f)$. Si f y g no tienen polos comunes, entonces $E_a^b(f+g) = E_a^b(f) + E_a^b(g)$ Por último, argumentando como la demostración de teorema 3.5.9, tenemos que

$$E_a^b(f) + E_a^b(\frac{1}{f}) = V_a^b(f,1)$$

(f sin polos ni ceros en a y b, $f^{-1}(0)$ como $f^{-1}(\infty)$ es igual a un número finito de intervalos cerrados). Por tanto, tomando $b \to a^-$

$$E_{S^1}(f) + E_{S^1}(\frac{1}{f}) = 0.$$

21. Definición: Llamaremos **curva racional** en $\mathbb{C}$ a cualquier aplicación continua

$$\sigma : [a,b] \to \mathbb{C}$$

definida a trozos por funciones racionales, es decir, una aplicación continua $\sigma(t) = u(t) + iv(t)$ tal que existen un número finito de números reales $a = a_0 < a_1 < \cdots < a_n = b$ de manera que las funciones u, v en cada intervalo $[a_i, a_{i+1}]$ son de la forma $u(t) = \frac{P_i(t)}{Q_i(t)}$ y $v(t) = \frac{S_i(t)}{H_i(t)}$ con $P_i(t), Q_i(t), S_i(t), H_i(t)$ polinomios. Diremos que es **circuito** cuando $\sigma(a) = \sigma(b)$.

Es claro que la unión de dos curvas racionales (a trozos) tal que la segunda empieza en el punto donde termina la primera, es otra curva racional.

22. Ejemplos: Las circunferencias son circuitos. En efecto: basta ver que las semicircunferencias son curvas racionales, pues la circunferencia es unión de dos semicircunferencias. Sea (c_1, c_2) el centro y $r \in \mathbb{R}^+$ el radio de una circunferencia. Consideremos el haz de rectas que pasan por el punto de la circunferencia $p_1 = (c_1 + r, c_2)$, es decir, $y = t(x - c_1 - r) + c_2$. Para cada pendiente t, la correspondiente recta, corta a la circunferencia en un único punto (aparte de p_1). Computando, dicho punto es:

$$(r\frac{t^2-1}{t^2+1} + c_1, r\frac{-2t}{t^2+1} + c_2).$$

Luego para $t \in [-1,1]$ parametriza la semicircunferencia (con $x \le c_1$).[3]

Otro ejemplo trivial es un segmento en $\mathbb{C}$ (usando las ecuaciones paramétricas de las rectas). Por tanto, cualquier polígono es un circuito.

23. Definición: Diremos que una curva σ pasa por un punto $z \in \mathbb{C}$ cuando $z \in \operatorname{Im}\sigma$.

[3] Podemos considerar $t \in (-\infty, \infty)$, que parametriza la circunferencia (salvo el punto $(c_1 + r, c_2)$) y para $t \to \pm\infty$ obtenemos el punto $(c_1 + r, c_2)$.

24. Definición: Dado un circuito $\sigma\colon [a,b]\to\mathbb{C}$, $\sigma(t)=u(t)+iv(t)$ que no pasa por el origen, llamaremos número de vueltas alrededor del origen (en el sentido de las agujas del reloj) al número

$$\mathrm{v}(\sigma)=\frac{1}{2}E_a^b\frac{v(t)}{u(t)}.$$

25. Observaciones: (1) El exceso de la fracción $\frac{v(t)}{u(t)}$ es 1 en $t=t_0$ cuando $u(t_0)=0$ (es decir la curva corta el eje OY) y la fracción pasa de negativa a positiva, es decir: (i) si $v(t_0)$ es negativo, entonces u pasa de positivo a negativo (o equivalentemente, $\sigma(t)$ pasa del cuarto cuadrante al tercero); (ii) si $v(t_0)$ es positivo u pasa de negativo a positivo (es decir $\sigma(t)$ pasa del segundo cuadrante al primero). Por tanto, es claro que cada vez que la curva da una vuelta alrededor del origen el exceso es 2, y queda justificada la definición.

(2) Análogamente se puede definir $\mathrm{v}(\sigma)=-\frac{1}{2}E_a^b\frac{u(t)}{v(t)}$ contabilizando el número de cortes con el eje OX. En efecto, ambos números coinciden, pues como sabemos

$$E_a^b\frac{v(t)}{u(t)}+E_a^b\frac{u(t)}{v(t)}=V_a^b(u,v)=V(u(a),v(a))-V(u(b),v(b))=0,$$

porque $u(a)=u(b), v(a)=v(b)$.

(3) Realmente, en el número de vueltas lo que se cuenta es el número de vueltas en el sentido de las agujas del reloj menos el número de vueltas en sentido contrario.

26. Lema: *Si $\sigma_1,\sigma_2\colon [a,b]\to\mathbb{C}$ son dos circuitos (que no pasan por el origen), entonces el número de vueltas de $\sigma_1\cdot\sigma_2$ es igual a la suma de las vueltas que da cada uno de ellos:*

$$v(\sigma_1\cdot\sigma_2)=v(\sigma_1)+v(\sigma_2).$$

Demostración. Supongamos que $\sigma_1(t),\sigma_2(t)$ no cortan simultáneamente al eje OX para ningún valor de t. Escribamos el número de vueltas por $\mathrm{v}(\sigma)=-\frac{1}{2}E_a^b\frac{u(t)}{v(t)}=\frac{1}{2}E_a^b f(t)$ (siendo $\sigma(t)=u(t)+v(t)i$ y $f(t)=-\frac{u(t)}{v(t)}$). Se verifica que la parte real e imaginaria de $\sigma_1(t)\cdot\sigma_2(t)$ es $u_1u_2-v_1v_2$ y $u_1v_2+v_1u_2$ y por tanto el número de vueltas es

$$\mathrm{v}(\sigma_1\cdot\sigma_2)=-\frac{1}{2}E_a^b\frac{u_1u_2-v_1v_2}{u_1v_2+v_1u_2}=-\frac{1}{2}E_a^b\frac{\frac{u_1}{v_1}\frac{u_2}{v_2}-1}{\frac{u_1}{v_1}+\frac{u_2}{v_2}}=\frac{1}{2}E_a^b\frac{f_1f_2-1}{f_1+f_2}.$$

Ahora bien, si f_1 ó f_2 tiene polo en un punto t_0, la fracción $\frac{f_1f_2-1}{f_1+f_2}$ no tiene polo en t_0 (toma el valor finito $f_2(t_0)$ ó $f_1(t_0)$ respectivamente), luego los polos se dan exactamente cuando se anula el denominador, es decir, cuando $f_1(t_0)=-f_2(t_0)$ y en tales puntos el numerador es estrictamente negativo ($f_1(t_0)f_2(t_0)-1=-f_1(t_0)^2-1<0$), es decir,

$$\frac{1}{2}E_a^b\frac{f_1f_2-1}{f_1+f_2}=-\frac{1}{2}E_a^b\frac{1}{f_1+f_2}=\frac{1}{2}E_a^b(f_1+f_2)=\frac{1}{2}E_a^bf_1+\frac{1}{2}E_a^bf_2=\mathrm{v}(\sigma_1)+\mathrm{v}(\sigma_2).$$

En particular, si $\sigma_2(t)=cte=:z$ entonces $v(\sigma_1(t))=v(\sigma_1(t)\cdot z)$. En el caso de que $\sigma_1(t),\sigma_2(t)$ corten simultáneamente el eje OX, entonces para casi todo $z\in\mathbb{C}$,

$$v(\sigma_1\cdot\sigma_2)=v(\sigma_1\cdot\sigma_2\cdot z)=v(\sigma_1)+v(\sigma_2\cdot z)=v(\sigma_1)+v(\sigma_2).$$

□

27. Teorema : *Sea $P(z)$ un polinomio con coeficientes complejos y $\sigma\colon [a,b] \to \mathbb{C}$ un rectángulo (por sencillez) recorrido en el sentido de las agujas del reloj y no pasando por ninguna raíz de $P(z)$. Entonces el número $r_\sigma(P(z))$ de raíces de $P(z)$ (contadas con su multiplicidad) contenidas en el interior del rectángulo coincide con el número de vueltas $v(P(\sigma(t)))$ de $P(\sigma(t))$ alrededor del origen:*

$$r_\sigma(P(z)) = v(P(\sigma(t))) := \frac{1}{2} E_a^b \frac{[P(\sigma(t))]_{Im}}{[P(\sigma(t))]_{Re}},$$

donde $[P(\sigma(t))]_{Im}$ es la parte imaginaria de $P(\sigma(t))$ y $[P(\sigma(t))]_{Re}$ la parte real.

Demostración. Escribamos $P(z) = H(z) \cdot \prod_i (z-\alpha_i)^{r_i}$ siendo α_i las raíces de $P(z)$ contenidas en el rectángulo y $H(z)$ sin raíces en el mismo. Por el lema anterior, $\mathrm{v}(P(\sigma(t))) = \mathrm{v}(H(\sigma(t))) + \sum_i r_i \cdot \mathrm{v}(\sigma(t)-\alpha_i) = \mathrm{v}(H(\sigma(t))) + \sum_i r_i$.

Solo tenemos que probar que si un polinomio $H(z)$ no tiene raíces en el rectángulo entonces $\mathrm{v}(H) = 0$. Supongamos que $\mathrm{v}(H(\sigma(t))) \neq 0$ y lleguemos a contradicción.

Se observa que si dos polígonos tienen un tramo en común pero recorridos en sentido contrario, entonces la suma de los excesos sobre estos estos dos coincide con el exceso en el contorno de la unión, pues en el tramo común el exceso de uno se cancela con el del otro. Por tanto si el interior de un polígono es unión de los interiores de varios polígonos de modo que cada dos de ellos tengan como mucho un tramo de su borde en común y éste está recorrido en sentido contrario en cada uno, entonces el exceso en el borde del polígono es la suma de los excesos en los bordes de los polígonos en los que descompone.

En particular cuadriculando el rectángulo (de manera que los ejes verticales y horizontales no pasen por las raíces) se puede suponer que dichos rectángulos son todo lo pequeños que se quiera.

Como el número de vueltas es no nulo, se puede elegir una cadena de rectángulos $\sigma_n(t)$ de manera que cada uno está contenido en el siguiente y el tamaño (de sus lados) es menor que $\frac{1}{2^n}$ y tal que el número de vueltas en él es no nulo. Estos rectángulos se intersecan en un punto α. $H(\alpha) = \lambda \neq 0$, entonces existe n tal que $H(\sigma_n(t))$ corta como mucho con uno de los ejes. Por lo tanto, por las observaciones (1) y (2), el número de vueltas de $H(\sigma_n(t))$ es nulo y hemos llegado a contradicción.

□

Este teorema permite separar las raíces de un polinomio complejo cualquiera. En efecto, $M = 1 + \mathrm{máx}\{|a_1|, \ldots, |a_n|\}$ es una cota de $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n$. Comencemos con un cuadrado centrado en el origen y lado de longitud $2M$. Éste contendrá todas las raíces de $P(z)$. Subdividiendo este cuadrado en cuadrados con lado de longitud la mitad y calculando el número de vueltas en cada uno de ellos se va aproximando y separando las raíces.

Por otro lado permite demostrar de nuevo el teorema fundamental del Álgebra.

28. Teorema de D'Alembert: *Todo polinomio con coeficientes complejos tiene todas sus raíces complejas.*

Demostración. Sea $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n$. Se trata de ver que eligiendo un cuadrado σ centrado en el origen y de lado suficientemente grande es $\mathrm{v}(P(\sigma)) = n$. Basta

elegir un cuadrado σ centrado en el origen y con lado de longitud mayor que $2nM$ (siendo M como arriba). En efecto, sea $f(z) = \frac{P(z)}{z^n}$. Se tiene $P(z) = z^n f(z)$, luego $\mathrm{v}(P(\sigma)) = \mathrm{v}(\sigma^n) + \mathrm{v}(f(\sigma)) = n + \mathrm{v}(f(\sigma))$, luego basta ver que sobre σ es $\mathrm{v}(f(\sigma)) = 0$. Ahora bien, $|\sigma(t)| > nM$, y para todo z tal que $|z| > nM$ se cumple que $|f(z) - 1| = |\frac{P(z)}{z^n} - 1| = |a_1 z^{-1} + \cdots + a_n z^{-n}| < \frac{1}{n} + \cdots + \frac{1}{n} = 1$. En particular $f(\sigma(t))$ no corta al eje OY, por tanto, el número de vueltas de $f(z)$ al recorrer σ es nulo.

□

29. Lema : *Sean $\sigma_1(t), \sigma_2(t)\colon [a,b] \to \mathbb{C}$ dos curvas racionales (que no pasan por el origen) y $\sigma_3(t) := \sigma_1(t) \cdot \sigma_2(t)$. Denotemos $\sigma_j(t) = u_j(t) + v_j(t) \cdot i$. Entonces,*

$$E_a^b \frac{u_3(t)}{v_3(t)} = E_a^b \frac{u_1(t)}{v_1(t)} + E_a^b \frac{u_2(t)}{v_2(t)} - V_a^b(v_1 v_2, v_3),$$

donde suponemos que v_1, v_2, v_3 no se anulan ni en a ni en b.

Demostración. Supongamos que $\sigma_1(t), \sigma_2(t)$ no cortan simultáneamente al eje OX para ningún valor de t. Tenemos que $\sigma_3(t) = (u_1 u_2 - v_1 v_2) + (u_1 v_2 + v_1 u_2) \cdot i$. Denotemos $f_i = \frac{u_i}{v_i}$. Entonces,

$$E_a^b \frac{u_3}{v_3} = E_a^b \frac{u_1 u_2 - v_1 v_2}{u_1 v_2 + v_1 u_2} = E_a^b \frac{f_1 f_2 - 1}{f_1 + f_2}$$

Ahora bien, si f_1 ó f_2 tiene polo en un punto t_0, la fracción $\frac{f_1 f_2 - 1}{f_1 + f_2}$ no tiene polo en t_0 (toma el valor finito $f_2(t_0)$ ó $f_1(t_0)$ respectivamente), luego los polos se dan exactamente cuando se anula el denominador, es decir, cuando $f_1(t_0) = -f_2(t_0)$ y en tales puntos el numerador es estrictamente negativo ($f_1(t_0) f_2(t_0) - 1 = -f_1(t_0)^2 - 1 < 0$), es decir,

$$\begin{aligned} E_a^b \frac{f_1 f_2 - 1}{f_1 + f_2} &= -E_a^b \frac{1}{f_1 + f_2} = E_a^b(f_1 + f_2) - V_a^b(f_1 + f_2, 1) = E_a^b f_1 + E_a^b f_2 - V_a^b(f_1 + f_2, 1) \\ &= E_a^b \frac{u_1}{v_1} + E_a^b \frac{u_2}{v_2} - V_a^b(u_1 v_2 + u_2 v_1, v_1 v_2) = E_a^b \frac{u_1}{v_1} + E_a^b \frac{u_2}{v_2} - V_a^b(v_3, v_1 v_2) \end{aligned}$$

y obtendremos la fórmula requerida.

En particular, para casi todo número complejo 1_ϵ muy próximo a 1 (de parte imaginaria no nula), si $\sigma_2(t) = 1_\epsilon$, entonces se cumplirá que $E_a^b(\frac{u_3}{v_3}) = E_a^b(\frac{u_1}{v_1})$.

En general, existe un número complejo 1_ϵ muy próximo a 1, de modo que si definimos $\sigma_1' = \sigma_1$, $\sigma_2' = 1_\epsilon \cdot \sigma_2$ y $\sigma_3' = 1_\epsilon \cdot \sigma_3 = \sigma_1' \cdot \sigma_2'$, entonces los σ_i' están en las hipótesis del teorema y en las del párrafo primero de la demostración, $E_a^b \frac{u_i}{v_i} = E_a^b \frac{u_i'}{v_i'}$ y $V_a^b(v_1 v_2, v_3) = V_a^b(v_1' v_2', v_3')$. Con lo que concluimos fácilmente.

□

30. Observación : Si tomamos las curvas $\sigma_1' = i \cdot \sigma_1$, $\sigma_2' = \sigma_2$ y $\sigma_3' = \sigma_1' \cdot \sigma_3' = i \cdot \sigma_3$, entonces obtendremos que

$$E_a^b \frac{v_3(t)}{u_3(t)} = E_a^b \frac{v_1(t)}{u_1(t)} - E_a^b \frac{u_2(t)}{v_2(t)} + V_a^b(u_1 v_2, u_3),$$

donde suponemos que u_1, v_2, u_3 no se anulan ni en a ni en b

31. Teorema: *Sea $p(z) = z^n + a_1 z^{n-1} + \cdots + a_n \in \mathbb{C}[x]$ un polinomio mónico y escribamos $p(x+iy) = u(x,y) + v(x,y)\cdot i$. Sea $a \in \mathbb{R}$ y supongamos que la recta del plano complejo $y = a$ no pasa por ninguna raíz de $p(z)$. Entonces,*

$$[N^o \text{ de raíces de } p(z) \text{ contenidas en el semiplano } y < a\ ] = \frac{n}{2} + \frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{v(t,a)}{u(t,a)}$$

Demostración. Probemos que para todo $A >> 0$, $E_{-\infty}^{+\infty}\frac{v(t,A)}{u(t,A)} = n$. Si definimos $q(z) = 1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$, entonces $p(z) = q(z)\cdot z^n$. Observemos $q(z)$ es un número complejo muy próximo a 1, cuando $|z| >> 0$. Denotemos $\sigma_1(t) = q(t+Ai) = u_1(t) + v_1(t)\cdot i$ y $\sigma_2(t) = (t+Ai)^n = u_2(t) + v_2(t)\cdot i$. Entonces,

$$\begin{aligned} E_{-\infty}^{\infty}\frac{v(t,A)}{u(t,A)} &= E_{-\infty}^{\infty}\frac{v_1(t,A)}{u_1(t,A)} - E_{-\infty}^{\infty}\frac{u_2(t,A)}{v_2(t,A)} + V_{-\infty}^{\infty}(u_1 v_2, u) \\ &= -E_{-\infty}^{\infty}\frac{u_2(t,A)}{v_2(t,A)} + V_{-\infty}^{\infty}(t^{n-1}, t^n) = -E_{-\infty}^{\infty}\frac{u_2(t,A)}{v_2(t,A)} + 1. \end{aligned}$$

Tenemos que probar que $E_{-\infty}^{\infty}\frac{u_2(t,A)}{v_2(t,A)} = -(n-1)$. Sea $\sigma_1'(t) = t + Ai = u_1' + v_1'\cdot i$ y $\sigma_2'(t) = (t+Ai)^{n-1} = u_2' + v_2'\cdot i$, entonces

$$\begin{aligned} E_{-\infty}^{\infty}\frac{u_2(t,A)}{v_2(t,A)} &= E_{-\infty}^{\infty}\frac{u_1'(t,A)}{v_1'(t,A)} + E_{-\infty}^{\infty}\frac{u_2'(t,A)}{v_2'(t,A)} - V_{-\infty}^{\infty}(v_1' v_2', v_2) \\ &= E_{-\infty}^{\infty}\frac{u_2'(t,A)}{v_2'(t,A)} - V_{-\infty}^{\infty}(t^{n-2}, t^{n-1}) = E_{-\infty}^{\infty}\frac{u_2'(t,A)}{v_2'(t,A)} - 1, \end{aligned}$$

y recurrentemente concluimos.

Procedamos ahora con toda generalidad. Sea $A >> 0$ y $B >> A$. Si definimos $q(z) = 1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$, entonces $p(z) = z^n \cdot q(z)$. Observemos $q(z)$ es un número complejo muy próximo a 1, cuando $|z| >> 0$. $\pm B + ti$, con $|t| \le A$, es un número complejo de argumento muy próximo a cero o π, y módulo grande, luego $(\pm B + ti)^n$ también y $p(\pm B + ti)$ también; luego, la parte real de $p(\pm B + ti)$ es no nula. Sea m el número de raíces de $p(z)$ que yacen en el semiplano $y < a$. Entonces,

$$\frac{1}{2}\cdot\left(E_{-B}^{B}\frac{v(t,A)}{u(t,A)} - E_{a}^{A}\frac{v(B,t)}{u(B,t)} - E_{-B}^{B}\frac{v(t,a)}{u(t,a)} + E_{a}^{A}\frac{v(-B,t)}{u(-B,t)}\right) = n - m$$

Luego, $\frac{1}{2}\cdot(n - 0 - E_{-B}^{B}\frac{v(t,a)}{u(t,a)} + 0) = n - m$ y por tanto $m = \frac{n}{2} + \frac{1}{2}E_{-\infty}^{+\infty}\frac{v(t,a)}{u(t,a)}$.

□

32. Observaciones: 1. En el teorema hemos supuesto que $a_0 = 1$, podíamos haber supuesto con mayor generalidad que $a_0 \in \mathbb{R}^*$.

2. Evidentemente, dados $a > b$, si $p(z)$ no tiene raíces en las rectas $y = a$ e $y = b$, entonces

$$[\text{Nº de raíces de } p(z) \text{ en la banda } b < y < a\ ] = \frac{1}{2}\cdot\left(E_{-\infty}^{+\infty}\frac{v(t,a)}{u(t,a)} - E_{-\infty}^{+\infty}\frac{v(t,b)}{u(t,b)}\right).$$

3. Supongamos que $p(z)$ no tiene raíces en la recta $x = a$. Las raíces de $p(z)$ contenidas en el semiplano $x > a$ se corresponden biunívocamente con las raíces de $p(i \cdot z)$ contenidas en el semiplano $y < -a$. Observemos que $p(iz) = p(i(x+yi)) = p(-y+xi) = u(-y,x) + v(-y,x)i$.

   Si n es par, el primer coeficiente de $p(i \cdot z)$ es igual a ± 1, luego

$$[\text{Nº de raíces de } p(z) \text{ contenidas en el semiplano } x > a\ ] = \frac{n}{2} + \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{v(a,t)}{u(a,t)}$$

   Si n es impar, observemos que el primer coeficiente de $i \cdot p(i \cdot z)$ es igual a ± 1 y $ip(iz) = -v(-y,x) + u(-y,x)i$, luego

$$[\text{Nº de raíces de } p(z) \text{ contenidas en el semiplano } x > a\ ] = \frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{u(a,t)}{v(a,t)}$$

33. Sea ahora $p(z) \in \mathbb{R}[z]$. Entonces $p(0+ti) = \sum_{r=0}^{n} i^{n-r} a_r t^{n-r}$. Si $n = 2m$ es par entonces

$$u(0,t) = (-1)^m \sum_{s=0}^{m} (-1)^s a_{2s} t^{n-2s} \quad \text{y} \quad v(0,t) = (-1)^m \sum_{s=1}^{m} (-1)^s a_{2s-1} t^{n-2s+1}.$$

Si $n = 2m+1$ es impar entonces

$$u(0,t) = (-1)^m \sum_{s=0}^{m} (-1)^s a_{2s+1} t^{n-2s-1} \quad \text{y} \quad v(0,t) = (-1)^m \sum_{s=0}^{m} (-1)^s a_{2s} t^{n-2s}.$$

Supongamos que $p(x)$ no tiene raíces imaginarias puras. Entonces,

$$(*) \qquad \left[\begin{array}{c} \text{Nº de raíces de } p(x) \in \mathbb{R}[x] \text{ contenidas} \\ \text{en el semiplano } x > 0 \end{array} \right] = \frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} \frac{\phi_1(t)}{\phi_0(t)}$$

con

$$\phi_1(t) = a_1 t^{n-1} - a_3 t^{n-3} + a_5 t^{n-5} - \cdots$$
$$\phi_0(t) = a_0 t^n - a_2 t^{n-2} + a_4 t^{n-4} - \cdots$$

Este cálculo es importante en el problema de la estabilidad en los sistemas de ecuaciones diferenciales (lineales). Si $a_1 \neq 0$, el primer resto de Sturm de la pareja ϕ_0, ϕ_1 es

$$R_1(t) = -(\phi_0(t) - \frac{a_1}{a_0} \cdot t \cdot \phi_1(t)) = (a_2 - \frac{a_0}{a_1} \cdot a_3) t^{n-2} - (a_4 - \frac{a_0}{a_1} \cdot a_5) t^{n-4} + (a_6 - \frac{a_0}{a_1} \cdot a_7) t^{n-6} - \cdots.$$

34. Lema: *Si $a_1 \neq 0$, entonces*

$$\left[\frac{n}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} (\frac{\phi_1(t)}{\phi_0(t)}) \right] = \left[\frac{n-1}{2} - \frac{1}{2} \cdot E_{-\infty}^{+\infty} (\frac{R_1(t)}{\phi_1(t)}) \right] + V(a_0, a_1).$$

Demostración. Para todo $b >> 0$,

$$E_{-b}^{b} \frac{\phi_1(t)}{\phi_0(t)} + E_{-b}^{b} \frac{\phi_0(t)}{\phi_1(t)} = V_{-b}^{b}(\phi_1, \phi_0) = V(a_1 \cdot (-1)^{n-1}, (-1)^n a_0) - V(a_1, a_0) = \text{sign}(a_0 \cdot a_1) \cdot 1.$$

Luego, $E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = -E_{-\infty}^{+\infty}\frac{\phi_0(t)}{\phi_1(t)} + \operatorname{sign}(a_0\cdot a_1)\cdot 1 = E_{-\infty}^{+\infty}\frac{R_1(t)}{\phi_1(t)} + \operatorname{sign}(a_0a_1)$. Por tanto,

$$\frac{n}{2}-\frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = \frac{n-1}{2}+\frac{1}{2}-\frac{1}{2}(E_{-\infty}^{+\infty}\frac{R_1(t)}{\phi_1(t)}+\operatorname{sign}(a_0a_1)) = \frac{n-1}{2}-\frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{R_1(t)}{\phi_1(t)}+V(a_0,a_1).$$

□

35. Proposición: *Sea $p(x)=\sum_{i=0}^{n}a_ix^{n-i}\in\mathbb{R}[x]$ (con $a_0\neq 0$), $R_1,\dots,R_m$ los restos de Sturm de la pareja ϕ_0,ϕ_1 y c_i el coeficiente de grado máximo de R_i. Si $m=n-1$, el número de raíces de $p(x)$ de parte real positiva es igual a $V(a_0,a_1,c_1,c_2,\dots,c_{n-1})$.*

Demostración. Observemos que ha de ser $\operatorname{gr}\phi_1 = n-1$ y $\operatorname{gr}(R_i) = n-i-1$, para todo i. En particular, $a_1\neq 0$. Además, ϕ_0 y ϕ_1 han de ser primos entre sí, luego $p(x)$ no tiene ninguna raíz imaginaria pura. Por la fórmula $(*)$, solo tenemos que probar que $\frac{n}{2}-\frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = V(a_0,a_1,c_1,c_2,\dots,c_{n-1})$. Procedamos por inducción sobre n. El caso $n=1$ es de comprobación inmediata. Por el lema de 3.5.34 e inducción

$$\begin{aligned}\frac{n}{2}-\frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} &= \frac{n-1}{2}-\frac{1}{2}\cdot E_{-\infty}^{+\infty}\frac{R_1(t)}{\phi_1(t)}+V(a_0,a_1) = V(a_1,c_1,c_2,\dots,c_{n-1})+V(a_0,a_1)\\ &= V(a_0,a_1,c_1,c_2,\dots,c_{n-1}).\end{aligned}$$

□

36. Teorema: *Sea $p(x)=\sum_{i=0}^{n}a_ix^{n-i}\in\mathbb{R}[x]$ (con $a_0\neq 0$) y consideremos la matriz*

$$H(\phi_0,\phi_1) := \begin{pmatrix} a_1 & a_0 & 0 & 0 & \dots & 0\\ a_3 & a_2 & a_1 & a_0 & \dots & 0\\ a_5 & a_4 & a_3 & a_2 & \dots & \\ \vdots & \vdots & \vdots & \vdots & & \vdots\\ a_{2n-1} & a_{2n-2} & a_{2n-3} & a_{2n-4} & \dots & a_n \end{pmatrix}$$

(con $a_m=0$ para todo $m>n$) y sea D_i el menor principal de orden i de $H(\phi_0,\phi_1)$. Si $D_i\neq 0$ para todo i, entonces el número de raíces de $p(x)$ de parte real positiva es igual a $V(a_0,D_1,\frac{D_2}{D_1},\frac{D_3}{D_2},\dots,\frac{D_n}{D_{n-1}})$, que es igual a

$$V(a_0,D_1,D_3,D_5,\dots)+V(1,D_2,D_4,D_6,\dots).$$

Demostración. Probemos la primera afirmación. Sean $R_1,\dots,R_m$ los restos de Sturm de la pareja ϕ_0,ϕ_1. Sigamos las notaciones del teorema anterior. Basta que probemos que $m=n-1$ y que $c_i=\frac{D_{i+1}}{D_i}$. Procedamos por inducción sobre n. El caso $n=1$ es de comprobación inmediata. Observemos que $\operatorname{gr}\phi_1 = n-1$, porque $a_1 = D_1\neq 0$, y que los restos de Sturm de la pareja ϕ_1,R_1 son $R_2,\dots,R_m$. Denotemos $D_i(\phi_0,\phi_1)$ el menor principal de orden i de $H(\phi_0,\phi_1)$. Si a las columnas pares les restamos $\frac{a_0}{a_1}$ veces la columna anterior, los menores principales no cambian y si a continuación eliminamos la primera fila y la primera columna obtenemos la matriz $H(\phi_1,R_1)$. Luego $D_i(\phi_0,\phi_1) = a_1\cdot D_{i-1}(\phi_1,R_1)$. Por inducción, $m-1=n-1$ y $\frac{D_{i+1}(\phi_0,\phi_1)}{D_i(\phi_0,\phi_1)} = \frac{D_i(\phi_1,R_1)}{D_{i-1}(\phi_1,R_1)} = c_i$.

Por último, observemos que $V(D_1,\frac{D_2}{D_1}) = V(D_1^2,D_2) = V(1,D_2)$ y que $V(\frac{D_i}{D_{i-1}},\frac{D_{i+1}}{D_i}) = V(\frac{D_i^2}{D_{i-1}},D_{i+1}) = V(D_{i-1},D_{i+1})$.

□

37. Definición: Se dice que un polinomio $p(x) \in \mathbb{R}[x]$ es de Hurwitz si la parte real de todas sus raíces es negativa.

38. Proposición: *Sea* $p(x) = \sum_{i=0}^{n} a_i x^{n-i}$, *con* $a_0 > 0$. *Las siguientes afirmaciones son equivalentes*

1. $p(x)$ *es de Hurwitz.*
2. $E_{-\infty}^{+\infty}(\frac{\phi_1(t)}{\phi_0(t)}) = n$.

Si $p(x)$ *es de Hurwitz entonces* $a_1, \ldots, a_n > 0$.

Demostración. Si $p(x)$ tiene alguna raíz imaginaria pura entonces no sería de Hurwitz y ϕ_1 y ϕ_0 tendrían raices comunes, luego el número de polos de ϕ_1/ϕ_0 sería menor que n, luego $E_{-\infty}^{+\infty}(\frac{\phi_1(t)}{\phi_0(t)}) < n$. Por la fórmula previa $(*)$, $p(x)$ es de Hurwitz si y solo si $E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = n$.

Supongamos que $p(x)$ es de Hurwitz. Entonces, $E_{-\infty}^{+\infty}\frac{\phi_1(t)}{\phi_0(t)} = n$, y por el lema 3.5.34 $E_{-\infty}^{+\infty}(\frac{R_1(t)}{\phi_1(t)}) = n-1$ (y $a_0, a_1 > 0$). Por tanto, $\phi_0(t)$ tiene n raíces reales y $\phi_1(t)$ tiene $n-1$ raíces reales. Por la regla de Descartes $a_{2i} > 0$ para todo i y $a_{2i+1} > 0$ para todo i.

□

39. Criterio de Hurwitz: *El polinomio* $p(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{R}[x]$ *(con* $a_0 > 0$*) es de Hurwitz si y solo si todos los menores principales de la matriz*

$$\begin{pmatrix} a_1 & a_0 & 0 & 0 & \ldots & 0 \\ a_3 & a_2 & a_1 & a_0 & \ldots & 0 \\ a_5 & a_4 & a_3 & a_2 & \ldots & \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{2n-1} & a_{2n-2} & a_{2n-3} & a_{2n-4} & \ldots & a_n \end{pmatrix}$$

(con $a_m = 0$ *para todo* $m > n$*) son positivos.*

Demostración. Es consecuencia inmediata del teorema 3.5.36. □

3.6. Teoría de la eliminación

El objetivo principal de esta sección es la resolución de los sistemas de ecuaciones algebraicas, vía la eliminación sucesiva de variables, como sabemos hacer con los sistemas de ecuaciones lineales.

3.6.1. Resultante de dos polinomios

Sean $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m$ variables $\mathbb{Z}$-algebraicamente independientes y sean $P(x) := a_0x^n + a_1x^{n-1} + \cdots + a_n$ y $Q(x) := b_0x^m + b_1x^{m-1} + \cdots + b_m$ polinomios genéricos de grados n y m.

Sean $x_1, \ldots, x_n$ las raíces de $P(x)$ e $y_1, \ldots, y_m$ las raíces de $Q(x)$. Observemos que $a_0, b_0, x_1, \ldots, x_n, y_1, \ldots, y_m$ son $\mathbb{Z}$-algebraicamente independientes: Sea una relación $\mathbb{Z}$-algebraica $f(a_0, b_0, , x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$. Por el teorema de las funciones simétricas $0 = g := a_0^N \prod_{\sigma \in S_n} f(a_0, b_0, , x_{\sigma(1)}, \ldots, x_{\sigma(n)}, y_1, \ldots, y_m) \in \mathbb{Q}[a_0, \ldots, a_n, b_0, y_1, \ldots, y_m]$ y de nuevo $0 = b_0^N \prod_{\sigma \in S_m} g(a_0, \ldots, a_n, b_0, y_{\sigma(1)}, \ldots, y_{\sigma(m)}) \in \mathbb{Q}[a_0, \ldots, a_n, b_0, \ldots, b_m]$, luego $f = 0$.

1. Definición: Llamaremos resultante genérica (de dos polinomios de grados n y m), que denotaremos $R(P,Q)$, a

$$R(P,Q) := a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

2. Propiedades: *1.* $R(P,Q) = (-1)^{nm} R(Q,P)$.

2. $R(P,Q) = a_0^m \prod_{i=1}^{n} Q(x_i)$

3. $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$.

Demostración. (1)

$$\begin{aligned} R(P,Q) &= a_0^m b_0^n \textstyle\prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (-1)(y_i - x_j) \\ &= (-1)^{nm} b_0^n a_0^m \textstyle\prod_{j=1}^{m} \prod_{i=1}^{n} (y_i - x_j) = (-1)^{nm} R(Q,P). \end{aligned}$$

(2)

$$R(P,Q) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) = a_0^m \prod_{i=1}^{n} b_0 \prod_{j=1}^{m} (x_i - y_j) = a_0^m \prod_{i=1}^{n} Q(x_i).$$

(3) Por el apartado anterior se obtiene que $R(P,Q)$ es un polinomio en las $\{b_i\}$ y en a_0 y simétrico en las $\{x_i\}$, luego $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]_{a_0}$. De (1) se obtiene por la misma razón que $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]_{b_0}$. Por tanto, $R(P,Q) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$. □

Sea $\bar{A}$ un anillo cualquiera y

$$\left.\begin{aligned} \overline{P}(x) &= \overline{a}_0 x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_n \\ \overline{Q}(x) &= \overline{b}_0 x^m + \overline{b}_1 x^{m-1} + \cdots + \overline{b}_m \end{aligned}\right\} \in \bar{A}[x], \quad \overline{a}_0, \overline{b}_0 \neq 0$$

3. Definición: $R(\overline{P}, \overline{Q}) \in \bar{A}$ es el valor obtenido en la resultante genérica $R(P,Q)$ dando a las variables $\{a_0, \ldots, a_n, b_0, \ldots, b_m\}$ los valores $\{\overline{a}_0, \ldots, \overline{a}_n, \overline{b}_0, \ldots, \overline{b}_m\}$.

Estabilidad por cambio de anillo base: Si $i\colon \bar{A} \to \bar{B}$ es un morfismo de anillos tal que $i(\bar{a}_0) \neq 0$ y $i(\bar{b}_0) \neq 0$, entonces $i(R(\bar{P},\bar{Q})) = R(P',Q')$, donde $P' = i(\overline{a_0})x^n + \cdots + i(\overline{a}_n)$ y $Q' := i(\overline{b}_0)x^m + \cdots + i(\overline{b}_m)$.

Evidentemente, $R(\bar{P},\bar{Q}) = (-1)^{nm}R(\bar{Q},\bar{P})$.

Esta definición da sentido a la resultante de polinomios cualesquiera (de grados positivos) aunque no se conozcan sus raíces, incluso sin hacer presunción de que éstas existan. Ahora bien, si $\bar{P} = \bar{a}_0(x-\bar{x}_1)\cdots(x-\bar{x}_n)$ y $\bar{Q} = \bar{b}_0(x-\bar{y}_1)\cdots(x-\bar{y}_n)$, entonces

$$R(\overline{P},\overline{Q}) = \bar{a}_0^m \bar{b}_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\bar{x}_i - \bar{y}_j)$$

ya que ya si damos a las variables x_i el valor $\bar{x}_i$ y a a_0 el valor $\bar{a}_0$ (luego a a_i el valor $\bar{a}_i$) y si damos a las variables y_i el valor $\bar{y}_i$ y a b_0 el valor $\bar{b}_0$ (luego a b_i el valor $\bar{b}_i$), entonces el valor de $R(P,Q) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j)$ es lo requerido.

Igualmente, si $\bar{P} = \bar{a}_0(x-\bar{x}_1)\cdots(x-\bar{x}_n)$, entonces $R(\overline{P},\overline{Q}) = \bar{a}_0^m \prod_{i=1}^{n}\bar{Q}(\bar{x}_i)$,

El interés de la resultante lo da el siguiente teorema.

4. Teorema: *Sea k un cuerpo. Dos polinomios $\overline{P}(x),\overline{Q}(x) \in k[x]$, tienen alguna raíz en común si y solo si $R(\overline{P},\overline{Q}) = 0$.*

5. Proposición: *$R(P_1(x),Q_1(x)\dot{Q}_2(x)) = R(P(x),Q_1(x))\cdot R(P(x),Q_2(x))$, (si $\operatorname{gr}Q_1(x) = m_1$ y $\operatorname{gr}Q_2(x) = m_2$, suponemos que $\operatorname{gr}(Q_1Q_2) = m_1 + m_2$).*

Demostración. Podemos suponer que $P(x)$ es el polinomio genérico, de raíces $x_1,\ldots,x_n$. Entonces,

$$\begin{aligned} R(P(x),Q_1(x)\cdot Q_2(x)) &= a_0^{m_1+m_2}\prod_{i=1}^{n}Q(x_i) = a_0^{m_1+m_2}\prod_{i=1}^{n}Q_1(x_i)\cdot Q_2(x_i) \\ &= a_0^{m_1}\prod_{i=1}^{n}Q_1(x_i)\cdot a_0^{m_2}\prod_{i=1}^{n}Q_2(x_i) = R(P(x),Q_1(x))\cdot R(P(x),Q_2(x)). \end{aligned}$$

□

3.6.2. Métodos de cómputo de la resultante

Demos diversos algoritmos para el cómputo de la resultante.

A. Método directo mediante el algoritmo de Euclides:

En este apartado, supondremos que el anillo de coeficientes de los polinomios es íntegro. Este método se basa en el siguiente lema.

6. Proposición: *Sean $C(x),R(x)$ polinomios tales que $P(x) = C(x)\cdot Q(x) + R(x)$. Entonces, se cumple la igualdad*

$$R(P,Q) = (-1)^{nm}b_0^{n-grR}R(Q,R),$$

siendo n,m los grados de P, Q respectivamente y b_0 el coeficiente en grado máximo de Q.

Demostración. De la igualdad del enunciado se obtiene $P(y_j) = R(y_j)$, siendo $\{y_j\}$ las raíces de Q, luego:

$$R(P,Q) = (-1)^{nm} R(Q,P) = (-1)^{nm} b_0^n \prod_j P(y_j)$$
$$= (-1)^{nm} b_0^n \prod_j R(y_j) = (-1)^{nm} b_0^n b_0^{-grR} R(Q,R).$$

□

Con el algoritmo de división de Euclides y la aplicación reiterada de esta proposición podemos calcular la resultante de dos polinomios.

B. Resultante de Bézout:

7. Teorema: *Sean* $P(x) = \sum_{i=0}^{n} a_i x^{n-i}$, $Q(x) = \sum_{i=1}^{m} b_i x^{m-i}$ *polinomios con coeficientes en un cuerpo k, de grados n y m respectivamente. El determinante del endomorfismo k-lineal*

$$Q(x)\cdot : k[x]/(P(x)) \to k[x]/(P(x)), \overline{H(x)} \mapsto \overline{Q(x)\cdot H(x)},$$

multiplicado por a_0^m*, es igual a* $R(P,Q)$*.*

Demostración. Podemos suponer que P y Q son polinomios genéricos y que k es algebraicamente cerrado. En este caso, $P(x) = a_0 \cdot (x - x_1) \cdots (x - x_n)$. Por el teorema chino de los restos $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, $\overline{H(x)} \mapsto (H(x_1), \ldots, H(x_n))$. Por tanto, $\overline{Q(x)}$ es igual a $(Q(x_1), \ldots, Q(x_n))$ en $k[x]/(P(x)) = k \times \overset{n}{\cdots} \times k$, y el determinante $|Q(x)\cdot| = Q(x_1) \cdots Q(x_n)$. Luego, $a_0^m \cdot |Q(x)\cdot| = R(P,Q)$. □

8. Supongamos que $n = m$. Consideremos en $k[x]/(P(x))$ las dos bases siguientes $B = \{a_0, a_0 \cdot x + a_1, \ldots, a_0 x^{n-1} + \cdots + a_{n-1}\}$ y $B' = \{x^{n-1}, \ldots, x, 1\}$. Observemos que

$$Q(x) \cdot (a_0 x^i + \cdots + a_i) - P(x) \cdot (b_0 x^i + \cdots + b_i) = \sum_{j=1}^{n} c_{i+1,j} x^{n-j} \qquad (*)$$

para ciertos $c_{i+1,j} \in k$. Entonces, la matriz de $Q(x)\cdot$ en las bases B, B' es (c_{ij}) y el determinante de la matriz de cambio de base de B a B' es a_0^n. Luego,

$$R(P,Q) = (a_0)^n \cdot |Q(x)\cdot| = |(c_{ij})|.$$

Es fácil comprobar que $\boxed{c_{ij} = \sum_{\substack{r+s=i+j-1 \\ r<i, s \geq i}} a_r b_s - a_s b_r}$.

Supongamos ahora que $\mathrm{gr}P(x) = n > m = \mathrm{gr}Q(x)$. Entonces, P y $x^{n-m}Q$ tienen grado n y $R(P, x^{n-m}Q) = R(P,Q) \cdot R(P,x)^{n-m} = a_n^{n-m} R(P,Q)$.

9. Observación: Como los coeficientes c_{ij} se obtienen algebraicamente a partir de los de P y Q es fácil ver que la fórmula $R(P,Q) = |(c_{ij})|$ es válida para polinomios con coeficientes en un anillo cualquiera (no necesariamente un cuerpo).

10. Observación: $c_{1j} = a_0 b_j - b_0 a_j$, para todo j, luego $R(P,Q) \in (a_0, b_0)$.

C: Resultante de Sylvester:

11. Teorema: *Sean* $P(x)=\sum_{i=0}^{n} a_i x^{n-i}$, $Q(x)=\sum_{i=1}^{m} b_i x^{m-i}$ *y*

$$S(P,Q):=\begin{vmatrix} a_0 & \cdots & \cdots & a_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & \cdots & \cdots & a_n \\ b_0 & \cdots & \cdots & \cdots & b_m & & \\ & \ddots & & & & \ddots & \\ & & b_0 & \cdots & \cdots & \cdots & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \Big\} m \\ \Big\} n \end{matrix}$$

Entonces, $S(P,Q)=R(P,Q)$.

Demostración. Procedemos por inducción sobre $n+m$. Podemos suponer que los polinomios son genéricos. Como $S(P,Q)=(-1)^{nm}S(Q,P)$, nos bastaría probar que $S(Q,P)=R(Q,P)$. Permutando P y Q, si es necesario, podemos suponer que $n\le m$. Tenemos $Q(x)=\frac{b_0}{a_0}x^{m-n}\cdot P(x)+Q'(x)$. Escribamos $Q'(x)=b'_0x^{m-1}+\cdots+b'_{m-1}$ Si a la fila $i+m$ (para todo $i\le n$) le restamos la fila i multiplicada por $\frac{b_0}{a_0}$, obtenemos

$$\begin{vmatrix} a_0 & \cdots & \cdots & a_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & \cdots & \cdots & a_n \\ b_0 & \cdots & \cdots & \cdots & b_m & & \\ & \ddots & & & & \ddots & \\ & & b_0 & \cdots & \cdots & \cdots & b_m \end{vmatrix} = \begin{vmatrix} a_0 & \cdots & \cdots & a_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & \cdots & \cdots & a_n \\ 0 & b'_0 & \cdots & \cdots & b'_{m-1} & & \\ & \ddots & \ddots & & & \ddots & \\ & & 0 & b'_0 & \cdots & \cdots & b'_{m-1} \end{vmatrix}$$

$$= a_0 \cdot \begin{vmatrix} a_0 & \cdots & \cdots & a_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & \cdots & \cdots & a_n \\ b'_0 & \cdots & \cdots & \cdots & b'_{m-1} & & \\ & \ddots & & & & \ddots & \\ & & b'_0 & \cdots & \cdots & \cdots & b'_{m-1} \end{vmatrix} = a_0 \cdot R(P,Q') = R(P,Q).$$

□

3.6.3. Aplicaciones de la resultante

A. Intersección de dos curvas planas.

Sean $P(x,y),Q(x,y)\in k[x,y]$ dos polinomios en dos variables primos entre sí y sea el sistema de ecuaciones:

$$\begin{aligned} P(x,y)&=a_0(y)\cdot x^n+\cdots+a_{n-1}(y)\cdot x+a_n(y)=0 \\ Q(x,y)&=b_0(y)\cdot x^m+\cdots+b_{m-1}(y)\cdot x+b_m(y)=0 \end{aligned} \qquad (a_0(y),b_0(y)\neq 0)$$

que son las ecuaciones de la intersección de las curvas $P(x,y)=0$ y $Q(x,y)=0$.

12. Proposición: *Sea $R(y)$ la resultante de P y Q entendidos respectivamente como polinomios en x con coeficientes en $k[y]$. Entonces, β es una raíz de $R(y)$ si y solo si β es una raíz común de $a_0(y)$ y $b_0(y)$, o existe α tal que (α,β) es un punto de corte de las curvas $P(x,y)=0$ y $Q(x,y)=0$.*

Demostración. Por la observación 3.6.10, $R(y)\subseteq(a_0(y),b_0(y))$, luego si β es una raíz de común de $a_0(y)$ y $b_0(y)$ lo es de $R(y)$. Si β no es una raíz $a_0(y)$, por la resultante de Bezout, $R(\beta)=a_0(\beta)^{m-\mathrm{gr}Q(x,\beta)}\cdot R(P(x,\beta),Q(x,\beta))$. Por tanto, si $R(\beta)=0$, tenemos que $R(P(x,\beta),Q(x,\beta)=0$ y existe α tal que $P(\alpha,\beta)=Q(\alpha,\beta)=0$.

□

Si $\{(\alpha_1,\beta_1),\ldots,(\alpha_n,\beta_n)\}$ son los puntos de corte de las curvas $P(x,y)=0$ y $Q(x,y)=0$, entonces $\{(\alpha_1,\ldots,\alpha_n\},\{\beta_1,\ldots,\beta_n\}$ son respectivamente raíces de $R(x)$ y $\overline{R}(y)$.

B. Cálculo de las raíces complejas de un polinomio complejo.

Sea $P(z)\in\mathbb{C}[z]$ y escribamos $z=x+i\cdot y$. Entonces, $P(z)=U(x,y)+V(x,y)\cdot i$, con $U(x,y),V(x,y)\in\mathbb{R}[x]$. El número complejo $a+b\cdot i$ es una raíz compleja de $P(z)$ si y solo si (a,b) es una solución del sistema de ecuaciones reales

$$\begin{aligned}U(x,y)&=0\\V(x,y)&=0\end{aligned}$$

Por el apartado anterior, si (a,b) es una solución real del sistema de ecuaciones, entonces a es una raíz real de la resultante, $R(x)=R(U(x,y),V(x,y))$, considerados como polinomios en y; y b es una raíz real de la resultante de $\bar{R}(y)=R(U(x,y),V(x,y))$, considerados como polinomios en x. Para calcular las raíces complejas de $P(z)$ basta calcular las raíces reales de $R(x)$ y $\bar{R}(y)$.

C. Solución de un sistema de ecuaciones algebraicas

Consideremos un sistema de ecuaciones algebraicas

$$\begin{aligned}&P_1(x_1,\ldots,x_n)=0\\&\cdots\\&P_n(x_1,\ldots,x_n)=0\end{aligned}$$

Sea $R_i(x_2,\ldots,x_n):=R(P_1(x_1,\ldots,x_n),P_i(x_1,\ldots,x_n))$, para todo $1<i\leq n$, considerados P_1 y P_i como polinomios en x_1. Si $(\alpha_1,\ldots,\alpha_n)$ es una solución del sistema de ecuaciones $P_1=\ldots=P_n=0$ entonces $(\alpha_2,\ldots,\alpha_n)$ es una solución del sistema de ecuaciones $R_2=\ldots=R_n=0$.

D. Discriminante.

Sea $P(x)=x^n+a_1x^{n-1}+\cdots+a_n$.

13. Teorema: *Si denotamos por $P'(x)=nx^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$ la derivada (formal) de $P(x)$, entonces:*

$$\Delta(P)=(-1)^{\binom{n}{2}}R(P,P').$$

Demostración. Como $P(x)=\prod_{i=1}^{n}(x-x_i)$, entonces $P'(x)=\sum_{j=1}^{n}\prod_{i\neq j}^{n}(x-x_i)$ y $P'(x_j)=\prod_{i\neq j}^{n}(x_j-x_i)$. Por tanto:

$$R(P,P')=\prod_{j=1}^{n}P'(x_j)=\prod_{j=1}^{n}\prod_{i\neq j}^{n}(x_j-x_i)=\prod_{i<j}(x_i-x_j)(x_j-x_i)$$
$$=\prod_{i<j}-(x_i-x_j)^2=(-1)^{\binom{n}{2}}\prod_{i<j}(x_i-x_j)^2=(-1)^{\binom{n}{2}}\Delta(P).$$

□

E. Racionalización.

Dados $P,Q\in k[x]$ primos entre sí y dada una raíz α de P se trata de *calcular* $\frac{1}{Q(\alpha)}$ *como polinomio en* α. Observemos que

$$R(P,Q)=R(\frac{P(x)}{x-\alpha}(x-\alpha),Q(x))=R(\frac{P(x)}{x-\alpha},Q(x))\cdot R(x-\alpha,Q(x))=R(\frac{P(x)}{x-\alpha},Q(x))\cdot Q(\alpha).$$

Luego,

$$\boxed{\frac{1}{Q(\alpha)}=\frac{1}{R(P,Q)}\cdot R(\frac{P(x)}{x-\alpha},Q)}$$

F. Polinomio de raíces una función de las raíces de otro polinomio.

Sea $P(x)\in k[x]$ y $\alpha_1,\ldots,\alpha_n$ las raíces de $P(x)$ y, sea $f(x)=\frac{A(x)}{B(x)}\in k(x)$ una función racional, tal que B es primo con P (para que tenga sentido hacer $x=\alpha_i$ en $f(x)$). *Se trata de calcular otro polinomio* $Q(x)\in k[x]$ *cuyas raíces sean* $f(\alpha_1),\ldots,f(\alpha_n)$.

Para ello se considera el sistema de ecuaciones:

$$\left.\begin{aligned}P(x)&=0\\A(x)-B(x)y&=0\end{aligned}\right\}$$

Las raíces del polinomio $R(y):=R(P(x),A(x)-B(x)y)$ son $f(\alpha_1),\ldots,f(\alpha_n)$: La condición necesaria y suficiente para que $R(\beta)=0$ es que los polinomios $\{P(x),A(x)-B(x)\beta\}$ tengan una raíz común α. Esto es que exista α tal que

$$\left.\begin{aligned}P(\alpha)&=0\\\beta&=\frac{A(\alpha)}{B(\alpha)}\end{aligned}\right\}$$

es decir, que $\beta=f(\alpha)$ para alguna raíz α de $P(x)$.

14. Ejemplo: Sea $P(x)\in k[x]$ de raíces $\alpha_1,\ldots,\alpha_n\in K$. Sea ξ una raíz r-ésima primitiva de la unidad. El polinomio cuyas raíces son $\alpha_1^r,\ldots,\alpha_n^r$ es:

$$\boxed{R(y)=R(P(x),x^r-y)=\prod_{i=1}^{r}P(\xi^i\cdot\sqrt[r]{y})}$$

Si $r=2$, el polinomio cuyas raíces son los cuadrados de las de $P(x)$ es

$$Q(x)=P(\sqrt{x})\cdot P(-\sqrt{x})$$

(conviene calcular $P(z)\cdot P(-z)$ y después hacer el cambio $x=z^2$.)

3.7. Cuestionario

1. Calcula las raíces racionales de $2x^5 - \frac{3}{2}x^3 + \frac{1}{8}$.

2. Calcula las raíces múltiples de $x^4 + x^3 + x^2 + x - 1 \in \mathbb{R}[x]$.

3. Sea $p(x) \in \mathbb{R}[x]$. Prueba que si $a + bi \in \mathbb{C}$ es una raíz de $p(x)$, entonces $a - bi$ es raíz de $p(x)$.

4. Escribe $x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2$ como polinomio en las funciones simétricas elementales.

5. Sean α_1, α_2 las raíces de $x^2 + 3x + 2$. Calcula el polinomio de raíces α_1^2, α_2^2.

6. Prueba que $p(x) \in \mathbb{C}[x]$ es mónico e irreducible si y solo si $p(x) = x - \alpha$.

7. El polinomio $x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ ¿es irreducible?¿tiene raíces en $\mathbb{Q}$?

8. Prueba que el polinomio $y^2 - x^2 + x^3 \in \mathbb{R}[x, y]$ es irreducible.

9. Prueba que $\frac{1}{7}x^{33} - \frac{2}{7} \in \mathbb{Q}[x]$ es irreducible.

10. Calcula un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 3 tal que $p(0) = 1$, $p(1) = 2$, $p(2) = -1$ y $p(3) = -2$.

11. Calcula $\Phi_{18}(x)$.

12. Prueba que $\operatorname{gr}\Phi_n(x) = \phi(n)$.

13. Si $\alpha_1, \alpha_2, \alpha_3$ son las raíces del polinomio $x^3 + x^2 + 2x + 3$, calcula un polinomio de raíces $\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}$.

14. Si L es una cota superior de $p(-x) \in \mathbb{R}[x]$ prueba que $-L$ es una cota inferior de $p(x)$.

15. Calcula $E_0^1(\frac{x-1}{x^2-3x+1})$.

16. ¿Cuántas raíces reales tiene $x^3 - 2x^2 - 2x - 1$?

17. ¿Es la métrica simétrica de $\mathbb{R}^3$ de matriz $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 1 \\ 3 & 1 & 0 \end{pmatrix}$ en la base usual, un producto escalar?

18. Sea $p(x) = \sum_{i=0}^{n} a_{n-i}x^i \in \mathbb{C}[x]$ y $\overline{p(x)} = \sum_{i=0}^{n} \bar{a}_{n-i}x^i$. Prueba que $p(x) \cdot \overline{p(x)} \in \mathbb{R}[x]$.

3.8. Biografía de D'Alembert

D'ALAMBERT BIOGRAPHY

D'Alembert was the illegitimate son from one of Mme de Tencin 'amorous liaisons'. His father, Louis-Camus Destouches, was out of the country at the time of d'Alembert's birth and his mother left the newly born child on the steps of the church of St Jean Le Rond. When his father returned to Paris he made contact with his young son and arranged for him to be cared for by the wife of a glazier, Mme Rousseau. She would always be d'Alembert's mother in his own eyes, particularly since his real mother never recognised him as her son, and he lived in Mme Rousseau's house until he was middle-aged.

The Destouches family continued to look after d'Alembert's education and they arranged for him to enter the Jansenist Collège des Quatre Nations. The Collège des Quatre Nations was an excellent place for d'Alembert to study mathematics and d'Alembert was able to make use of the excellent mathematics library at the Collège. As well as the mathematical training, he learnt about Descartes' physical ideas at the Collège but, when he formed his own ideas later in his life, he would have little respect for the views of Descartes.

The main aim of the Jansenist Collège des Quatre Nations was to produce scholars who could become experts in theology and argue the Jansenist case against the Jesuits. However, d'Alembert was turned off the study of theology at the Collège. After graduating in 1735 he decided that he would make a career in law but his real passion was for mathematics and he continued to work in his spare time on that subject. In 1738 d'Alembert qualified as an advocate but he seems to have decided that this was not the career for him. The following year d'Alembert studied medicine but this was a topic that he found even worse than theology. Of all the topics he had studied the one that he had real enthusiasm for was mathematics and his progress in this was quite remarkable, particularly given that he had studied almost exclusively on his own and at a time when he was supposed to be studying for other qualifications.

In July 1739 d'Alembert read his first paper to the Paris Academy of Science on some errors he had found in Reyneau's standard text Analyse démontrée which were not of great significance but marked the start of his mathematical career. In 1740 he submitted a second work on the mechanics of fluids which was praised by Clairaut. In May 1741 d'Alembert was admitted to the Paris Academy of Science, on the strength of these and papers on the integral calculus. It took some determination on his part, submitting three unsuccessful applications in quick succession, before his appointment.

Despite this tendency to quarrel with all around him, his contributions were truly outstanding. D'Alembert helped to resolve the controversy in mathematical physics over the conservation of kinetic energy by improving Newton's definition of force in his Traité de dynamique which he published in 1743. This also contains d'Alembert's principle of mechanics. This is an important work and the preface contains a clear statement by d'Alembert of an attempt to lay a firm foundation for mechanics. D'Alembert

thought mechanics should be made into a completely rationalistic mathematical system. D'Alembert had begun to read parts of his Traité de dynamique to the Academy in late 1742 but soon afterwards Clairaut began to read his own work on dynamics to the Academy. Clearly a rivalry quickly sprung up and d'Alembert stopped reading the work to the Academy and rushed into print with the treatise. The two mathematicians had come up with similar ideas and indeed the rivalry was to become considerably worse in the next few years.

D'Alembert stated his position clearly that he believed mechanics to be based on metaphysical principles and not on experimental evidence. He seems not to have realised in his reading of Newton's Principia how strongly Newton based his laws of motion on experimental evidence. For d'Alembert these laws of motion were logical necessities.

In 1744 d'Alembert applied his results to the equilibrium and motion of fluids and published Traité de l'équilibre et du mouvement des fluides. This work gave an alternative treatment of fluids to the one published by Daniel Bernoulli. D'Alembert thought it a better approach, of course, as one might expect, Daniel Bernoulli did not share this view.

Until 1746 he had been satisfied to lead a retired but mentally active existence at the house of his foster-mother. In 1746 he was introduced to Mme Geoffrin, the rich, imperious, unintellectual but generous founder of a salon to which d'Alembert was suddenly invited. He soon entered a social life in which, surprisingly enough, he began to enjoy great success and popularity. Around the same time d'Alembert began to become involved in a major project, namely editing the Encyclopédie with Diderot. He was contracted as an editor to cover mathematics and physical astronomy but his work covered a wider field. When the first volume appeared in 1751 it contained a Preface written by d'Alembert which was widely acclaimed as a work of great genius. D'Alembert worked on the Encyclopédie for many years. In fact he wrote most of the mathematical articles in this 28 volume work. However, he continued his mathematical work while working on the Encyclopédie. He was a pioneer in the study of partial differential equations and he pioneered their use in physics. His work on this topic first appeared in an article which he submitted for the 1747 prize of the Prussian Academy Réflexions sur la cause générale des vents which indeed he won the prize. Euler, however, saw the power of the methods introduced by d'Alembert and soon developed these far further than had d'Alembert.

The year 1747 was an important one for d'Alembert in that a second important work of his appeared in that year, namely his article on vibrating strings. The article contains the first appearance of the wave equation in print but again suffers from the defect that he used mathematically pleasing simplifications of certain boundary conditions which led to results which were at odds with observation.

The Paris Academy had not been a place for d'Alembert to publish after he fell out with colleagues there and he was sending his mathematical papers to the Berlin Academy during the 1750s. However Euler was unhappy to publish these works and d'Alembert stopped publishing his mathematical articles, collecting them together and publishing them as Opuscules mathématiques which appeared in eight volumes between 1761 and 1780.

D'Alembert made other important contributions to mathematics which we have not yet mentioned. In an article entitled Différentiel in volume 4 of Encyclopédie written in 1754, he suggested that the theory of limits be put on a firm foundation. He was one of the first to understand the importance of functions and, in this article, he defined the derivative of a function as the limit of a quotient of increments. His ideas on limits led him to the test for convergence, known today as d'Alembert's ratio test, which appears in Volume 5 of Opuscules mathématiques.

In the latter part of his life d'Alembert turned more towards literature and philosophy. D'Alembert's philosophical works appear mainly in the five volume work Mélanges de littérature et de philosophie which appeared between 1753 and 1767. In this work he sets out his skepticism concerning metaphysical problems. He accepts the argument in favour of the existence of God, based on the belief that intelligence cannot be a product of matter alone. However, although he took this public view in his books, evidence from his friends showed that he was persuaded by Diderot towards materialism before 1770.

3.9. Problemas

1. Sea $p(x) \in k[x]$ un polinomio de grado n y supongamos que $n! \neq 0 \in k$. Prueba que $p(x) = \sum_{i=0}^{n} \frac{p^{i)}(0)}{i!} \cdot x^i$.

2. Sea $p(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in k[x]$, con $\alpha_1, \ldots, \alpha_n \in k$ distintos.

   a) Prueba que
   $$\frac{1}{p(x)} = \sum_{i=1}^{n} \frac{1}{p'(\alpha_i)} \cdot \frac{1}{x-\alpha_i}$$

   b) Prueba que $\sum_i \frac{\alpha_i^r}{p'(\alpha_i)} = 0$, si $r \leq n-1$ y $\sum_i \frac{\alpha_i^{n-1}}{p'(\alpha_i)} = 1$.

3. Sean K y K' dos k-extensiones de cuerpos. Prueba que existe una k-extensión de cuerpos L que contiene a K y K'.

4. Sea $p(x) \in \mathbb{R}[x]$ un polinomio irreducible. Prueba que $\mathrm{gr}(p(x)) \leq 2$.

5. Sea $p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in k[x]$. Demuestra que existe un polinomio $q(x) \in k[x]$ tal que $q(x^2) = p(x) \cdot p(-x)$. Si $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$ prueba que $\alpha_1^2, \ldots, \alpha_n^2$ son las raíces de $q(x)$. Calcula $q(x)$.

6. Sean α_1, α_2 las raíces de $p(x) = x^2 + a_1x + a_2$. Escribe el discriminante de $p(x)$, $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$, como función de los coeficientes del polinomio.

7. Sean $\alpha_1, \alpha_2, \alpha_3$ las raíces de $p(x) = x^3 + a_1x^2 + a_2x + a_3$. Escribe el discriminante $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$ del polinomio como función de los coeficientes del polinomio.

8. Sea $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in k[x]$ un polinomio de grado n y $\alpha_1, \ldots, \alpha_n$ sus raíces. Sea $\sigma_i = \alpha_1^i + \cdots + \alpha_n^i$, para cada $i \in \mathbb{N}$. Prueba la fórmula de Girard

$$\frac{p'(x)}{p(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \cdots + \frac{\sigma_n}{x^{n+1}} + \cdots$$

Multiplicando por $p(x)$ en esta igualdad prueba las **fórmulas de Newton**

$$0 = a_0\sigma_r + a_1\sigma_{r-1} + \cdots + a_{r-1}\sigma_1 + ra_r, \quad r \leq n$$
$$0 = a_0\sigma_r + a_1\sigma_{r-1} + \cdots + a_{r-n}\sigma_n, \quad r \geq n$$

9. Sea $p(x) = x^4 + 4x^3 + 3x^2 + 2x + 3$.

   a) Descompón en factores irreducibles la reducción módulo 2 de $p(x)$.

   b) Descompón en factores irreducibles la reducción módulo 3 de $p(x)$.

   c) Descompón $p(x)$ en factores irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

10. (Criterio de Nietsnesie) Sea $a_0 + a_1x + \cdots + a_nx^n$ 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 $\mathbb{Q}[x]$.

11. Sea $p > 2$ un número primo. Prueba que $x^p - px + 1 \in \mathbb{Q}]x]$ es irreducible. Pista: hágase el cambio de variable $x = y - 1$.

12. Descompón en producto de factores irreducibles el polinomio $x^5 - 2x^4 + x + 1 \in \mathbb{Q}[x]$.

13. Sea $p(x)$ un polinomio con coeficientes racionales. Prueba que si $\sqrt{2}$ es raíz de $p(x)$, entonces $p(x)$ es múltiplo de $x^2 - 2$, y que si $\sqrt[3]{2}$ es raíz de $p(x)$, entonces $p(x)$ es múltiplo de $x^3 - 2$.

14. Prueba que $n = \sum_{d|n} \phi(d)$.

15. Prueba que un grupo finito es cíclico si y solo si para cada divisor d de su orden admite como mucho un subgrupo de orden d.

16. Acota las raíces reales de los polinomios $x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3$, $x^4 - 2x^2 + 4x + 1$, $x^3 + 2x^2 + 3x - 1$, $24x^3 - 27x^2 + 9x - 1$.

17. Calcula todas las raíces reales de $x^3 + 3x^2 - 1$ con un error de una décima.

18. Calcula el número de las raíces reales positivas de $x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3$.

19. Calcula los excesos de la fracción $\frac{-4x^5+26x^4+4x^3-33x^2+98x+5}{2x^4-13x^3+10x-49}$ en los intervalos siguientes $(-\infty, -3)$, $(-3, 0)$, $(0, 3)$ y $(3, \infty)$.

20. Calcula el número de vueltas alrededor del origen de la curva cerrada

$$x = \frac{t^2}{t^2+1}, \; y = \frac{t^4 + 2t^3 + 5t^2 - 2t - 1}{t^2 + 1} \quad (-1 \leq t \leq 1).$$

21. Calcula el número de vueltas alrededor del punto $(1,1)$ de la curva cerrada

$$x = \frac{t^4-1}{t^4+1},\ y = \frac{t^2}{t^2+1} \quad (-1 \le t \le 1).$$

22. Calcula el número de vueltas alrededor del origen de la curva cerrada

$$w = z^5 + z + 1,\ |z| = 1.$$

23. Prueba que:

    a) $a_0t^2 + a_1t + a_2$ es de Hurwitz si y solo si a_0, a_1, a_2 tienen el mismo signo.

    b) $a_0t^3 + a_1t^2 + a_2t + a_3$ es de Hurwitz si y solo si a_0, a_1, a_2, a_3 tienen el mismo signo y $a_1a_2 - a_0a_3 > 0$.

    c) $a_0t^4 + a_1t^3 + a_2t^2 + a_3t + a_4$ es de Hurwitz si y solo si a_0, a_1, a_2, a_3, a_4 tienen el mismo signo y $(a_1a_2a_3 - a_3^2a_0 - a_1^2a_4)/a_0 > 0$.

24. Dado un polinomio $P(x) \in k[x]$, de raíces α_i, calcula un polinomio de raíces $\alpha_i + \frac{1}{\alpha_i}$.

25. Calcula el polinomio cuyas raíces son

$$cos\,\frac{2k\pi}{5} \quad , \ k = 0,1,2,3,4$$

26. Dado un polinomio $P(x) \in k[x]$, de raíces α_i, calcula el polinomio de raíces $\alpha_i - \frac{1}{\alpha_i}$.

27. Generalización de 24 y 26: Calcula el polinomio de raíces $a\alpha_i + \frac{b}{\alpha_i}$, con $a, b \in k$.

28. Sea $P(x) \in k[x]$ y $\alpha_1, \ldots, \alpha_n \in k$ sus raíces. Sea $F(\alpha, \beta) = 0$ una relación de dependencia algebraica sobre k entre dos raíces $\alpha = \alpha_1$ y $\beta = \alpha_2$ (es decir, $F(x,y)$ es un polinomio con coeficientes en k). Calcula α, β.

29. Prueba que el discriminante de $x^2 + ax + b$ es $\Delta = a^2 - 4b$.

30. Prueba que el discriminante de $x^3 + px + q$ es $\Delta = -(4p^3 + 27q^2)$.

Capítulo 4

Módulos

4.1. Introducción

El espacio vectorial es el ejemplo más sencillo y usual de espacio geométrico. Muchos problemas se resuelven linealizándolos, lo que permite aplicarles además la intuición geométrica. Añadamos que muchas de las estructuras usuales en Matemáticas son estructuras de espacios vectoriales.

Sea A un anillo. Sin precisar, un A-módulo es un A-espacio vectorial, pero donde A es un anillo y no necesariamente un cuerpo. En esta capítulo iniciaremos el estudio de la estructura de módulo sobre un anillo A y veremos que casi todas las definiciones del Álgebra Lineal (subespacios, sistemas generadores, cocientes, 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 la teoría de módulos. La posibilidad de efectuar estas operaciones (cocientes, sumas directas, etc.) aclara y simplifica muchos enunciados y demostraciones.

Los módulos aparecen también con frecuencia en Matemáticas. Ya veremos que los grupos abelianos y los espacios vectoriales con un endomorfismo lineal son ejemplos de módulos, y que su clasificación es la clasificación de la estructura de módulo.

4.2. Módulos

1. Definición: Sea A un anillo y M un conjunto. Diremos que una operación

$$M \times M \xrightarrow{+} M, (m, m') \mapsto m + m' \text{ y una aplicación } A \times M \xrightarrow{\cdot} M, (a, m) \mapsto a \cdot m,$$

definen en M una estructura de A-módulo cuando cumplen

1. $(M, +)$ es un grupo conmutativo.
2. $a \cdot (m + n) = a \cdot m + a \cdot n$, para todo $a \in A$ y $m, n \in M$.
3. $(a + b) \cdot m = a \cdot m + b \cdot m$, para todo $a, b \in A$ y $m \in M$.
4. $(ab) \cdot m = a \cdot (b \cdot m)$, para todo $a, b \in A$ y $m \in M$.

5. $1 \cdot m = m$, para todo $m \in M$.

Sea M un A-módulo. Cada elemento $a \in A$ define una aplicación

$$a\cdot\colon M \to M,\ m \mapsto a \cdot m.$$

El segundo punto expresa que $a\cdot$ es morfismo de grupos. En particular, $a \cdot 0 = 0$ y $a \cdot (-m) = -(a \cdot m)$.

Observemos que $0 \cdot m = 0$: $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m$, luego $0 \cdot m = 0$. Observemos que $(-a) \cdot m = -(a \cdot m)$, para todo $m \in M$: $0 = 0 \cdot m = (a + -a) \cdot m = a \cdot m + (-a) \cdot m$, despejando $(-a) \cdot m = -(a \cdot m)$.

2. Notación: Alguna vez, escribiremos am en vez de $a \cdot m$ por sencillez de escritura.

3. Ejemplos: 1. Todo anillo A es un A-módulo: con la suma definida en A y con el producto por los elementos de A definido en A.

2. Si A es un cuerpo, entonces los A-módulos son los A-espacios vectoriales.

3. Si G es un grupo abeliano, entonces es un $\mathbb{Z}$-módulo de modo natural: $n \cdot g := \overbrace{g + \stackrel{n}{\ldots} + g}$ si $n \in \mathbb{N}^+$, $n \cdot g := \overbrace{(-g) + \stackrel{-n}{\ldots} + (-g)}$ si $-n \in \mathbb{N}^+$, y definimos $0 \cdot g := 0$. Recíprocamente, si G es un $\mathbb{Z}$-módulo, en particular es un grupo abeliano.

4. Si $T\colon E \to E$ es un endomorfismo de k-espacios vectoriales entonces E tiene estructura natural de $k[x]$-módulo: $(\sum \lambda_i x^i) \cdot e := \sum \lambda_i T^i(e)$. Recíprocamente, dado un $k[x]$-módulo E, la aplicación $T\colon E \to E$ definida por $T(e) = x \cdot e$, es un endomorfismo de k-espacios vectoriales.

5. 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 subconjunto de $\prod_{i\in I} M_i$ formado por los elementos (m_i) que tienen todas sus componentes nulas salvo un número finito de ellas, y se llamará suma directa de los $\{M_i\}_{i\in I}$. Tanto $\prod_{i\in I} M_i$ como $\bigoplus_{i\in I} M_i$ son A-módulos con la siguiente suma y producto por elementos de A:

$$(m_i)_{i\in I} + (m'_i)_{i\in I} := (m_i + m'_i)_{i\in I}$$
$$a \cdot (m_i)_{i\in I} := (a \cdot m_i)_{i\in I}$$

4. Definición: Un subconjunto N de un A-módulo M, decimos que es un A-submódulo si con la operación $+$ de M y con la multiplicación $\cdot$ por elementos de A, N es un A-módulo.

Puede comprobarse que un subconjunto no vacío $X \subseteq M$ es un A-submódulo si y solo si para todo $x, x' \in X$ y $a \in A$ se cumple que $ax + x' \in X$.

La intersección de submódulos es submódulo.

5. Ejemplos: 1. Los K-subespacios vectoriales de un K-espacio vectorial E son justamente los K-submódulos de E.

2. Los ideales de un anillo A son justamente los A-submódulos de A.

3. Los subgrupos de un grupo abeliano G son justamente los $\mathbb{Z}$-submódulos de G.

4. Dado un endomorfismo k-lineal $T: E \to E$, los subespacios vectoriales $E' \subseteq E$ estables por T ($T(E') \subseteq E'$) son justamente los $k[x]$-submódulos de E.

5. $\underset{i\in I}{\oplus} M_i$ es un submódulo de $\prod_{i\in I} M_i$.

6. Dado un conjunto $\{M_i\}_{i\in I}$ de submódulos de M denotaremos

$$\sum_{i\in I} M_i = \{m \in M : m = \sum_{i\in I} m_i \text{ con } m_i \in M_i \text{ nulos para todo } i \in I \text{ salvo un número finito}\},$$

que es el menor submódulo de M que contiene a los submódulos M_i.

4.3. Morfismos de módulos

1. Definición: Una aplicación $f: M \to M'$ entre A-módulos M, M', diremos que es un morfismo de A-módulos (o una aplicación A-lineal) si cumple

1. $f(m+n) = f(m) + f(n)$, para todo $m, n \in M$.

2. $f(am) = af(m)$, para todo $a \in A$ y $m \in M$.

Cuando $f: M \to M'$ sea biyectiva diremos que f es un isomorfismo de A-módulos.

2. Ejemplos: 1. Sea M un A-módulo y $a \in A$. La aplicación $a \cdot M \to M$, $m \mapsto a \cdot m$ es un morfismo de A-módulos.

2. Sean G y G' dos grupos abelianos, es decir, dos $\mathbb{Z}$-módulos. Una aplicación $f: G \to G'$ es un morfismo de grupos si y solo si es un morfismo de $\mathbb{Z}$-módulos, y f es un isomorfismo de grupos si y solo si f es un isomorfismo de $\mathbb{Z}$-módulos.

3. Sean $T: E \to E$ y $T': E' \to E'$ dos endomorfismos k-lineales, es decir, E y E' son dos $k[x]$-módulos. Una aplicación lineal $\phi: E \to E'$ es un morfismo de $k[x]$-módulos si y solo si $\phi \circ T = T' \circ \phi$, es decir, el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ E' & \xrightarrow[T']{} & E' \end{array}$$

es conmutativo. En efecto, si ϕ es morfismo de $k[x]$-módulos

$$(\phi \circ T)(e) = \phi(T(e)) = \phi(x \cdot e) = x \cdot \phi(e) = T'(\phi(e)) = (T' \circ \phi)(e),$$

para todo $e \in E$. Recíprocamente„ si $\phi \circ T = T' \circ \phi$, entonces $\phi(x \cdot e) = \phi(T(e)) = T'(\phi(e)) = x \cdot \phi(e)$, para todo $e \in E$. Por tanto, $\phi(x^2 \cdot e) = x \cdot \phi(x \cdot e) = x^2 \cdot \phi(e)$, recurrentemente obtenemos que $\phi(x^n \cdot e) = x^n \cdot \phi(e)$ y por k-linealidad tenemos que $\phi(p(x) \cdot e) = p(x) \cdot \phi(e)$ para todo $p(x) \in k[x]$ y todo $e \in E$. Es decir, ϕ es un morfismo de $k[x]$-módulos.

Dado un isomorfismo k-lineal $\varphi: E \to V$, podemos definir un endomorfismo k-lineal (único) $S: V \to V$ tal que el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\varphi}\downarrow\wr & & \wr\downarrow{\scriptstyle\varphi} \\ V & \xrightarrow[S]{} & V \end{array}$$

es conmutativo. En efecto, $S := \varphi \circ T \circ \varphi^{-1}$. Diremos que T y S son equivalentes.

Por tanto, T y T' son equivalentes si y solo si existe un isomorfismo de $k[x]$-módulos $\phi: E \to E'$.

Veamos que T y T' son equivalentes si y solo si existen bases $\{e_i\}$ en E y $\{e'_j\}$ en E' de modo que la matriz de T en la base $\{e_i\}$ es igual a la matriz de T' en la base $\{e'_j\}$: Consideremos un isomorfismo k-lineal $\phi: E \to E'$, de modo que $\phi \circ T = T' \circ \phi$. Sea $\{e_i\}$ una base cualquiera de E. Entonces, $\{\phi(e_i)\}$ es una base de E' y la matriz de T en la base $\{e_i\}$ es igual a la matriz de T' en la base $\{\phi(e_i)\}$. Sea $\{e_i\}_{i\in I}$ una base de E y $\{e'_j\}_{j\in J}$ una base de E' de modo que la matriz de T en la base $\{e_i\}_{i\in I}$ es igual a la matriz de T' en la base $\{e'_j\}_{j\in J}$. Implícitamente se está suponiendo que $I = J$. Entonces, el endomorfismo$k$-lineal $\phi: E \to E'$ que cumple que $\phi(e_i) := e'_i$ es un isomorfismo k-lineal tal que $\phi \circ T = T' \circ \phi$.

4. **Submódulos en suma directa:** Diremos que dos submódulos M_1, M_2 de M están en suma directa si $M_1 \cap M_2 = 0$, que equivale a decir que si $m_1 + m_2 = m'_1 + m'_2$ (con $m_1, m'_1 \in M_1$ y $m_2, m'_2 \in M_2$) entonces $m_1 = m'_1$ y $m_2 = m'_2$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M_1 + M_2$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo.

En general, diremos que un conjunto $\{M_i\}_{i\in I}$ de submódulos de M están en suma directa si $M_i \cap \sum_{j\neq i} M_j = 0$ para todo i, que equivale a decir que si $\sum_{i\in I} m_i = \sum_{i\in I} m'_i$ (con $m_i, m'_i \in M_i$ para todo i, y todos son nulos salvo un número finito) entonces $m_i = m'_i$ para todo $i \in I$, que equivale a decir que el morfismo natural

$$\bigoplus_{i\in I} M_i \to \sum_{i\in I} M_i$$

es un isomorfismo. Se dice que M es la suma directa de los submódulos $\{M_i\}_{i\in I}$ si el morfismo $\bigoplus_{i\in I} M_i \to M$, $(m_i)_{i\in I} \mapsto \sum_{i\in I} m_i$ es un isomorfismo, que equivale a decir que todo $m \in M$ se escribe de modo único como $m = \sum_{i\in I} m_i$.

3. Definición: Sea $f: M \to M'$ un morfismo de A-módulos. El conjunto

$$\operatorname{Ker} f := \{m \in M : f(m) = 0\},$$

se denomina núcleo de f.

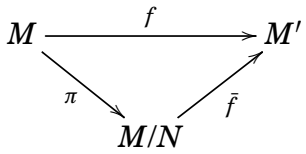
Se cumple que $\operatorname{Ker} f$ es un submódulo de M y que $f(m_1) = f(m_2)$ si y solo si $m_2 \in m_1 + \operatorname{Ker} f$, luego f es inyectiva si y solo si $\operatorname{Ker} f = 0$. El conjunto de los elementos de la imagen, $\operatorname{Im} f$, forman un submódulo de M'.

Si N es un submódulo de M entonces es un subgrupo conmutativo de M. Por tanto, podemos considerar el grupo cociente M/N, donde

$$M/N = \{\bar{m} \text{ (donde } \bar{m} =: m+N) \text{ ,} \forall\, m \in M\}$$

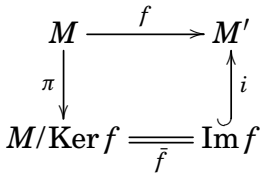
Recordemos que $\bar{m} = \bar{m'} \iff m - m' \in N$ y $\overline{m_1} + \overline{m_2} := \overline{m_1 + m_2}$. El producto $a \cdot \bar{m} := \overline{a \cdot m}$ dota a M/N de estructura de A-módulo (compruébese) y es la única estructura de A-módulo que podemos definir en M/N, de modo que el morfismo de paso al cociente $M \to M/N$, $m \mapsto \bar{m}$, sea un morfismo de módulos.

4. Teorema: *Sea $f : M \to M'$ un morfismo de A-módulos. Sea $N \subseteq \operatorname{Ker} f$ un A-submódulo. Existe un único morfismo $\bar{f} : M/N \to M'$ (que vendrá definido por $\bar{f}(\bar{m}) = f(m)$) de modo que el diagrama*



es conmutativo, siendo π el morfismo de paso al cociente.

5. Teorema de isomorfía: *Sea $f : M \to M'$ un morfismo de A-módulos. Se cumple que el diagrama*



donde $\pi(m) = \bar{m}$, $\bar{f}(\bar{m}) = f(m)$ (que está bien definida) e $i(m') = m'$, es conmutativo, $\bar{f}$ es un isomorfismo, π es epiyectiva e i inyectiva.

Demostración. Al lector. □

6. Ejemplo: Sean $N \subseteq M$ y $N' \subseteq M'$ dos A-submódulos. Consideramos la inclusión obvia $N \oplus N' \subseteq M \oplus M'$, $(n, n') \mapsto (n, n')$. Probemos que

$$(M \oplus M')/(N \oplus N') \simeq M/N \oplus M'/N'.$$

El morfismo $M \oplus M' \to M/N \oplus M'/N'$, $(m, m') \mapsto (\bar{m}, \bar{m'})$ es epiyectivo y el núcleo es $N \oplus N'$. Por el teorema de isomorfía se concluye.

4.4. Sistema de generadores. Módulos libres

1. Definición: Dado un subconjunto $X \subseteq M$, llamaremos submódulo generado por X y lo denotaremos $\langle X \rangle$, al mínimo submódulo de M que contiene a X.

Se cumple que

$$\langle X\rangle = \{\sum_{i=1}^{n} a_i m_i \in M, \forall\ a_i \in A, m_i \in X, n \in \mathbb{N}\}.$$

Por ejemplo, $\langle m\rangle = \{am \in M : \forall\, a \in A\} =: A \cdot m$.

2. Definición: Diremos que un conjunto de elementos de M, $\{m_i\}_{i\in I}$, es un sistema generador de M si $\langle m_i\rangle_{i\in I} = M$, es decir, para cada $m \in M$ existen $i_1,\dots,i_n \in I$ y $a_{i_1},\dots,a_{i_n} \in A$ de modo que $m = a_{i_1}m_{i_1} + \cdots + a_{i_n}m_{i_n}$.

Evidentemente, todo módulo tiene sistemas generadores, por ejemplo el formado por todos los elementos de M.

3. Definición: Diremos que un módulo M es finito generado si existe un sistema generador de M formado por un número finito de elementos. Diremos que un conjunto de elementos $\{m_i\}_{i\in I}$ es base de M, si es un sistema generador y los elementos son linealmente independientes, es decir, cumplen que siempre que $\sum_i a_i m_i = 0$, entonces $a_i = 0$, para todo i.

4. Ejemplo: Por ejemplo, $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ es un $\mathbb{Z}$-módulo finito generado, ya que $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} = \langle(1,0),(0,\bar{1})\rangle$.

5. Definición: Se dice que un módulo es libre si existe una base en el módulo.

En general los módulos no son libres, no tienen bases. Ésta es la gran diferencia de la teoría de módulos con la teoría de espacios vectoriales.

6. Ejemplo: $\mathbb{Z}/2\mathbb{Z}$ no es un $\mathbb{Z}$-módulo libre, porque si $\{\bar{n}_i\}_{i\in I}$ fuese una base, entonces $0 \neq 2\cdot\bar{n}_i = \overline{2\cdot n_i} = 0$, contradicción.

7. Ejercicio: Da una base del A-módulo libre $A[x]$.

8. Sea I un conjunto (de índices). Denotaremos $A^{(I)} = \bigoplus_{i\in I} A_i$, siendo $A_i = A$, para todo i. $A^{(I)}$ es un A-módulo libre de base la base estándar: Definamos $1_j := (a_i)_{i\in I}$, con $a_i = 0$ para todo $i \neq j$ y $a_j = 1$. Entonces, $\{1_i\}_{i\in I}$ es una base de $A^{(I)}$.

Sea $\{m_i\}_{i\in I}$ un conjunto de elementos de M, y definamos el morfismo

$$\phi\colon A^{(I)} \to M, (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i m_i$$

El morfismo ϕ es epiyectivo si y solo si $\{m_i\}_{i\in I}$ es un sistema generador de M. Como en todo módulo existen sistema generadores, todo módulo es isomorfo a un cociente de un libre.

El morfismo ϕ es inyectivo si y solo si los elementos $\{m_i\}_{i\in I}$ son linealmente independientes. Por tanto, ϕ es isomorfismo si y solo si $\{m_i\}_{i\in I}$ es una base de M.

Si $f : M \to N$ un isomorfismo de A-módulos y $\{m_i\}_{i\in I}$ es una base de M, entonces $\{f(m_i)\}_{i\in I}$ es una base de N. Por tanto, un módulo es libre si y solo si es isomorfo a un $A^{(I)}$.

9. Sea M un A-módulo e $J \subseteq A$ un ideal. Denotaremos $J \cdot M$ como el mínimo submódulo de M que contiene a $\{j \cdot m : \forall j \in J, \forall m \in M\}$. Es fácil comprobar que

$$J \cdot M := \{j_1 \cdot m_1 + \cdots + j_n \cdot m_n : \forall j_i \in J, \forall m_i \in M, \forall n > 0\}.$$

Observemos que $M/J \cdot M$ es de modo natural un A/J-módulo: $\bar{a} \cdot \bar{m} := \overline{a \cdot m} = \overline{a \cdot m}$, que está bien definida porque para todo $j \in J$ se cumple que $\overline{(a+j)} \cdot \bar{m} = \overline{(a+j) \cdot m} = \overline{a \cdot m + j \cdot m} = \overline{a \cdot m}$.

10. Proposición: *Si $A^n \simeq A^m$ entonces $n = m$ ($A \neq 0$).*

Demostración. Sea $\mathfrak{m} \subset A$ un ideal maximal. Entonces,

$$A^n/\mathfrak{m} \cdot A^n = (A \oplus \overset{n}{\cdots} \oplus A)/(\mathfrak{m} \oplus \overset{n}{\cdots} \oplus \mathfrak{m}) = A/\mathfrak{m} \oplus \overset{n}{\cdots} \oplus A/\mathfrak{m}.$$

Obviamente, $A^n/\mathfrak{m} \cdot A^n \simeq A^m/\mathfrak{m} \cdot A^m$. Por tanto,

$$n = \dim_{A/\mathfrak{m}} A^n/\mathfrak{m} \cdot A^n = \dim_{A/\mathfrak{m}} A^m/\mathfrak{m} \cdot A^m = m.$$

□

11. Definición: Si un A-módulo L es isomorfo a A^n (con $n \in \mathbb{N}$) se dice que L es un A-módulo libre de rango n.

12. Ejemplo: Los k-espacios vectoriales de dimensión n son k-módulos libres de rango n.

Con mayor generalidad si $L \simeq A^{(I)}$ se dice que el rango de L es el cardinal de I.

13. Definición: Sean L y L' dos A-módulos libres de bases $\{u_1, \ldots, u_n\}$ y $\{u'_1, \ldots, u'_m\}$, respectivamente. Sea $f : L \to L'$ un morfismo de A-módulos y sea

$$f(u_j) = \sum_{i=1}^{m} a_{ij} u'_i, \text{ para } a_{ij} \in A \text{ únicos.}$$

Diremos que $(a_{ij}) \in A^{m \times n}$ es la matriz asociada a f en las bases $\{u_j\}$ de L y $\{u'_i\}$ de L'.

Tenemos una correspondencia biunívoca entre el conjunto de los morfismos de módulos de L en L' y el conjunto de las matrices con coeficientes en A, $(a_{ij}) \in A^{m \times n}$.

Sean L, L' y L'' A-módulos libres de bases $\{u_1, \ldots, u_n\}$, $\{u'_1, \ldots, u'_m\}$ y $\{u''_1, \ldots, u''_r\}$. Sean $f : L \to L'$ y $g : L' \to L''$ morfismos de A-módulos, de matrices en las bases consideradas (a_{ij}) y (b_{rs}). Entonces la matriz de $g \circ f : L \to L''$ en las bases consideradas es igual al producto de matrices (usual)

$$(b_{rs}) \cdot (a_{ij}) = (c_{uv}),$$

con $c_{uv} = \sum_{l=1}^{m} b_{ul} \cdot a_{lv}$.

4.5. Teorema de descomposición

Sea M un A-módulo y $a \in A$. Denotaremos por $a\cdot$ el endomorfismo A-lineal

$$a\cdot\colon M \to M,\ m \mapsto a\cdot m.$$

1. Lema: *Sea M un A-módulo. Sean $p,q \in A$ tales que $(p,q)=A$. Entonces,*

$$\operatorname{Ker} pq\cdot = \operatorname{Ker} p\cdot \oplus \operatorname{Ker} q\cdot.$$

Demostración. Sean $\lambda,\mu \in A$ tales que

$$\lambda p + \mu q = 1.$$

Cada $m \in \operatorname{Ker} pq\cdot$ cumple $\lambda pm + \mu qm = 1\cdot m = m$, y $\lambda pm \in \operatorname{Ker} q\cdot$ y $\mu qm \in \operatorname{Ker} p\cdot$. Por tanto, $\operatorname{Ker} pq\cdot = \operatorname{Ker} p\cdot + \operatorname{Ker} q\cdot$.

$\operatorname{Ker} p\cdot \cap \operatorname{Ker} q\cdot = 0$: Si $m \in \operatorname{Ker} p\cdot \cap \operatorname{Ker} q\cdot$ entonces $m = \lambda pm + \mu qm = 0+0 = 0$.

□

Para los cálculos será conveniente conocer la siguiente proposición.

2. Proposición: *Sean $p,q \in A$ tales que $(p,q)=A$ y sea M un A-módulo anulado por $p\cdot q$. Se cumple que $\operatorname{Ker} p\cdot = q\cdot M$.*

Demostración. Obviamente $q\cdot M \subseteq \operatorname{Ker} p\cdot$. Sean $\lambda,\mu \in A$ tales que $\lambda p + \mu q = 1$. Dado $m \in \operatorname{Ker} p\cdot$ tenemos que $m = (\lambda p + \mu q)\cdot m = \mu q\cdot m \in q\cdot M$, luego $\operatorname{Ker} p\cdot \subseteq q\cdot M$ y $\operatorname{Ker} p\cdot = q\cdot M$. □

3. Teorema de descomposición: Sea M un A-módulo y $a_1,\dots,a_s \in A$, con $(a_i,a_j) = A$ para todo $i \neq j$. Entonces,

$$\operatorname{Ker}(a_1\cdots a_s)\cdot = \operatorname{Ker} a_1\cdot \oplus \cdots \oplus \operatorname{Ker} a_s\cdot.$$

Demostración. Primero observemos que si $(a,b)=A$ y $(a,c)=A$, entonces $(a,bc)=A$:

$$A = A\cdot A = (a,b)\cdot(a,c) = (a^2,ac,ab,bc) \subseteq (a,bc),$$

luego $(a,bc)=A$.

Recurrentemente, obtenemos que $(a_1,a_2\cdots a_s)=A$. Por el lema anterior,

$$\operatorname{Ker}(a_1\cdots a_s)\cdot = \operatorname{Ker} a_1\cdot \oplus \operatorname{Ker}(a_2\cdots a_s\cdot) = \cdots = \operatorname{Ker} a_1\cdot \oplus \cdots \oplus \operatorname{Ker} a_s\cdot$$

□

4. Corolario: *Sea $T\colon E \to E$ un endomorfismo k-lineal. Sea $p(x) = p_1(x)\cdots p_r(x) \in k[x]$, con $p_i(x)$ primo con $p_j(x)$, para todo $i \neq j$. Entonces,*

$$\operatorname{Ker} p(T) = \operatorname{Ker} p_1(T) \oplus \cdots \oplus \operatorname{Ker} p_r(T).$$

Demostración. E es un $k[x]$-módulo: $q(x)\cdot e = q(T)(e)$, para todo $q(x) \in k[x]$. Entonces,

$$\operatorname{Ker} p(T) = \operatorname{Ker} p(x)\cdot \overset{4.5.3}{=} \operatorname{Ker} p_1(x)\cdot \oplus \cdots \oplus \operatorname{Ker} p_r(x)\cdot = \operatorname{Ker} p_1(T) \oplus \cdots \oplus \operatorname{Ker} p_r(T).$$

□

4.5.1. Ecuaciones diferenciales lineales con coeficientes constantes

Sea F el $\mathbb{C}$-espacio vectorial de todas las funciones reales con valores complejos infinitamente diferenciables. Sea

$$D : F \to F,\ D(f(x)) = f'(x)$$

el "operador derivada". Es claro que D es un endomorfismo $\mathbb{C}$-lineal de F. Dado $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, entonces $P(D)\colon F \to F$ es el endomorfismo definido por

$$P(D)(f) = a_n D^n(f) + a_{n-1}D^{n-1}(f) + \cdots + a_0 \cdot f, \text{ donde } D^r(f) \text{ es la derivada } r\text{-ésima de } f.$$

5. Ejercicio: Calcula $(D^2 + D)(\cos x)$.

Queremos resolver ecuaciones diferenciales del tipo

$$a_n \cdot f^{n)} + \cdots + a_2 f'' + a_1 f' + a_o \cdot f = 0, \qquad \text{(donde los } a_i \text{ son constantes).}$$

Es decir, buscamos aquellas funciones $f \in F$. que cumplen que $P(D)(f) = 0$, donde $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Tenemos que calcular $\operatorname{Ker} P(D)$.

Veamos que

$$\operatorname{Ker} D^r = \{\text{Polinomios de grado estrictamente menor que } r\}.$$

En efecto,

$D(f) = 0 \iff f = cte$
$D^2(f) = 0 \iff D(D(f)) = 0 \iff D(f) = cte \iff f = cte \cdot x + cte'$
$D^3(f) = 0 \iff D^2(Df) = 0 \iff Df = cte \cdot x + cte' \iff f = \frac{cte}{2} \cdot x^2 + cte' \cdot x + cte''$
Etcétera.

6. Movimiento uniformemente acelerado: Supogamos que un objeto se mueve a lo largo de la recta (real) con una aceleración constante a. Digamos que $f(t)$ es la posición del móvil en el instante t. La velocidad del móvil es $f'(t)$ en cada instante t y la aceleración es $f''(t) = a$ en cada instante t. Por tanto, $f''' = 0$, es decir, $f(t) \in \operatorname{Ker} D^3$. Luego, $f(t) = \lambda + \mu t + \gamma t^2$. Observemos que $f(0) = \lambda$, $f'(0) = \mu$ y $f''(0) = 2 \cdot \gamma = a$. Por tanto,

$$f(t) = f(0) + f'(0) \cdot t + \frac{a}{2} \cdot t^2 \quad \text{y} \quad f'(t) = f'(0) + a \cdot t.$$

7. Fórmula de conmutación: *Sea $P(x) \in \mathbb{C}[x]$. Para toda $f \in F$ y $\alpha \in \mathbb{C}$, se cumple que*

$$P(D)(e^{\alpha x} \cdot f) = e^{\alpha x} \cdot P(D + \alpha \cdot \mathrm{Id})(f)$$

Demostración. $D(e^{\alpha x} \cdot f) = \alpha \cdot e^{\alpha x} \cdot f + e^{\alpha x} \cdot D(f) = e^{\alpha x} \cdot (D + \alpha \cdot \mathrm{Id})(f)$.

$D^2(e^{\alpha x} \cdot f) = D(D(e^{\alpha x} \cdot f)) = D(e^{\alpha x} \cdot (D + \alpha \cdot \mathrm{Id})(f)) = e^{\alpha x} \cdot (D + \alpha \cdot \mathrm{Id})((D + \alpha \cdot \mathrm{Id})(f)) = e^{\alpha x} \cdot (D + \alpha \cdot \mathrm{Id})^2(f)$.

Así sucesivamente, $D^n(e^{\alpha x}\cdot f) = e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})^n(f)$. Para $P(D)=\sum_i a_i D^i$ tendremos que

$$P(D)(e^{\alpha x}\cdot f) = \sum_i a_i D^i(e^{\alpha x}\cdot f) = \sum_i a_i\cdot e^{\alpha x}\cdot(D+\alpha\cdot \mathrm{Id})^i(f) = e^{\alpha x}\cdot P(D+\alpha\cdot \mathrm{Id})(f)$$

□

8. Teorema: *Se cumple que*

1. $\mathrm{Ker}(D-\alpha\cdot \mathrm{Id})^r = e^{\alpha x}\cdot\{$*Polinomios de grado estrictamente menor que* $r\}$.

2. *Si* $P(x)=(x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}$ *, entonces*

$$\begin{aligned}\mathrm{Ker}\,P(D) &= \mathrm{Ker}(D-\alpha_1\cdot \mathrm{Id})^{n_1}\oplus\cdots\oplus \mathrm{Ker}(D-\alpha_r\cdot \mathrm{Id})^{n_r}\\ &= e^{\alpha_1 x}\cdot\{\textit{Pol. de grado } < n_1\}\oplus\cdots\oplus e^{\alpha_r x}\cdot\{\textit{Pol. de grado } < n_r\}\end{aligned}$$

Demostración. 1. $(D-\alpha\cdot \mathrm{Id})^r f(x)=0 \iff 0=(D-\alpha\cdot \mathrm{Id})^r(e^{\alpha x}\cdot e^{-\alpha x}\cdot f(x)) = e^{\alpha x}\cdot D^r(e^{-\alpha x}\cdot f(x)) \iff 0=D^r(e^{-\alpha x}\cdot f(x)) \iff e^{-\alpha x}\cdot f(x)$ es un polinomio de grado menor que $r \iff f(x)$ es $e^{\alpha x}$ multiplicado por un polinomio de grado menor que r.

2. Es consecuencia de 1.

□

9. Nota: Supongamos $P(x)\in\mathbb{R}[x]$ y $\alpha=a+bi$ es una raíz compleja de $P(x)$, con $b\neq 0$. Entonces $\bar\alpha=a-bi$ también es una raíz compleja de $P(x)$. Más aún, la multiplicidad con la que aparece α es la misma con la aparece $\bar\alpha$, es decir, $P(x)=(x-\alpha)^n\cdot(x-\bar\alpha)^n\cdot Q(x)$, con $Q(\alpha),Q(\bar\alpha)\neq 0$. Probemos que

$$\left\{\begin{array}{l} f\in \mathrm{Ker}(D-\alpha\,\mathrm{Id})^n\oplus \mathrm{Ker}(D-\bar\alpha\,\mathrm{Id})^n \\ \text{tales que } f(x)\in\mathbb{R} \text{ para todo } x.\end{array}\right\} = e^{ax}\cdot\{q(x)\cdot\cos bx + r(x)\cdot \mathrm{sen}\, bx\}_{q(x),r(x)\in P_n}$$

donde P_n son todos los polinomios con coeficientes reales de grado $< n$: Por 4.5.8, tenemos que una base del $\mathbb{R}$-espacio vectorial $E=\mathrm{Ker}(D-\alpha\,\mathrm{Id})^n\oplus \mathrm{Ker}(D-\bar\alpha\,\mathrm{Id})^n$, es

$$\{e^{ax}\cdot e^{bix}\cdot x^r, ie^{ax}\cdot e^{bix}\cdot x^r, e^{ax}\cdot e^{-bix}\cdot x^r, ie^{ax}\cdot e^{-bix}\cdot x^r\}_{0\le r<n}.$$

Las funciones con valores en $\mathbb{R}$ de E, se obtienen sumando a cada función $f\in E$ su conjugada. Por tanto, una base de $\{f\in E:\ f(x)\in\mathbb{R},\ \forall x\in\mathbb{R}\}$ es

$$\{e^{ax}\cdot\cos bx\cdot x^r, e^{ax}\cdot \mathrm{sen}\, bx\cdot x^r,\}_{0\le r<n}.$$

10. Ley de desintegración radiactiva: Consideremos que tenemos una cierta cantidad $U(t)$ de gramos de uranio que permanece (sin desintegrar) en el tiempo t. Suponemos que la cantidad de uranio que se desintegra en un intervalo de tiempo (muy pequeño) t_1, $U(t)-U(t+t_1)$, es proporcional al tiempo t_1 transcurrrido y a la cantidad $U(t)$ de gramos que había en el instante t. Es decir, tenemos

$$U(t+t_1)-U(t) = -cte\cdot t_1\cdot U(t) \qquad (cte>0)$$

Por tanto,

$$\frac{U(t+t_1)-U(t)}{t_1} = -cte\cdot U(t)$$

Tomando límite $t_1 \to 0$, obtenemos

$$U'(t) = -cte\cdot U(t)$$

Es decir, $U(t)$ verifica la ecuación diferencial $U'+cte\cdot U=0$. Tenemos $(D+cte\cdot \mathrm{Id})(U)=0$, luego $U(t)=a\cdot e^{-cte\cdot t}$, para cierta constante a. Observemos que $U(0)=a\cdot e^0=a$. Luego,

$$\boxed{U(t)=U(0)\cdot e^{-cte\cdot t}}$$

Veamos cuál es la semivida del uranio, es decir, cuánto tiempo s ha de transcurrir para que se desintegre la mitad del uranio:

$$U(0)\cdot e^{-cte\cdot s} = U(s) = \frac{U(0)}{2}$$

Luego, $e^{-cte\cdot s}=\frac{-1}{2}$. Tomando logaritmo neperiano $-cte\cdot s=\ln 2^{-1}=-\ln 2$, luego

$$s=\frac{\ln 2}{cte} \quad \text{y} \quad U(t)=U(0)\cdot e^{-\frac{\ln 2}{s}\cdot t}=U(0)\cdot 2^{-\frac{t}{s}}.$$

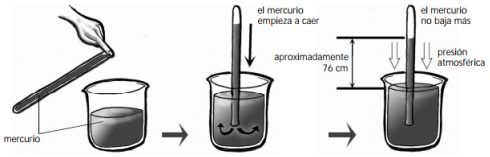
El carbono 14 que hay en la atmósfera aunque se desintegra en carbono no radiactivo (carbono 12 y 13), también se crea continuamente debido a las colisiones de los neutrones generados por los rayos cósmicos con el nitrógeno de la atmósfera superior y, resulta que la proporción de carbono 14 y carbono no radiactivo permanece en un nivel casi constante en la atmósfera a lo largo del tiempo. Las plantas adquieren el carbono atmosférico mediante la fotosíntesis, y los animales, mediante el consumo de plantas y de otros animales. Cuando un organismo muere el carbono 14 existente va desintegrándose. La proporción de carbono 14 y carbono no radiactivo cuando se examinan los restos del organismo proporciona una indicación del tiempo transcurrido desde su muerte.

11. Presión atmosférica: Sea $P(h)$ la presión atmosférica a una altura h del suelo. La diferencia de presión $P(h+t)-P(h)$ es proporcional a t y a la densidad del aire en h (que es proporcional a $P(h)$). Entonces,

$$\frac{P(h+t)-P(h)}{t} = -K\cdot P(h), \text{ luego } P'(h)=-K\cdot P(h)$$

Es decir, $(D + K \cdot \mathrm{Id})(P) = 0$ y $P(h) = a \cdot e^{-K \cdot h}$, donde $a = P(0)$. Puede medirse la altura en términos de la presión: $h = \frac{\ln P(0) - \ln P(h)}{K}$.

Problema: En 1643, Torricelli al realizar su experimento, al nivel del mar, obtuvo que la columna de mercurio medía 760 mm. (por encima del nivel de mercurio de la cubeta). Si a una altura de 100 metros sobre el nivel del mar la columna de mercurio mide 751 mm. ¿a qué altura sobre el nivel del mar estaríamos si la columna de mercurio mide 600 mm.?



Experimento de Torricelli

12. Interés compuesto continuo: Supongamos que tenemos un capital de 10^6 euros invertidos en un banco. El banco nos da por la inversión un interés del 2 por ciento anual y nos permite retirar el dinero en cualquier momento sin penalización y con el pago de los intereses del capital por el tiempo exacto transcurrido. Si retiramos el capital, con los intereses generados, al año y medio ¿cuánto dinero nos llevaremos?: Sea $f(t)$ el capital más los intereses generados que tenemos en el banco en el momento t. Observemos que $f(t+h) - f(t)$ es proporcional a $f(t)$ y al tiempo h transcurrido ("cuando h es muy pequeño"), es decir,

$$f(t+h) - f(t) = K \cdot h \cdot f(t), \quad \text{y} \quad \frac{f(t+h) - f(t)}{h} = K \cdot f(t)$$

Luego,

$$f'(t) = \lim_{h \to 0} \frac{f(t+h) - f(t)}{h} = K \cdot f(t)$$

Es decir, $(D - K \cdot \mathrm{Id})(f) = 0$, luego $f(t) = a \cdot e^{Kt}$. Sabemos que $f(0) = 10^6$, luego $a = 10^6$; y $10^6 \cdot e^K = f(1) = 10^6 \cdot (1 + 0'02)$, luego $e^K = 1'02$. Por tanto,

$$f(t) = 10^6 \cdot (1'02)^t$$

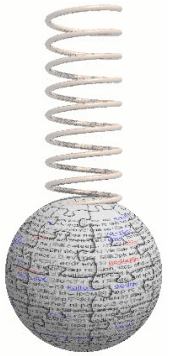
y $f(1'5) = 10^6 \cdot (1'02)^{1'5}$.

13. Ejemplo: Resolvamos la ecuación diferencial: $f'''' - 2f''' + 2f'' = 0$. Tenemos que resolver $(D^4 - 2D^3 + 2D^2)(f) = 0$, es decir, calcular $\mathrm{Ker}(D^4 - 2D^3 + 2D^2)$. Observemos que $x^4 - 2x^3 + 2x^2 = x^2(x^2 - 2x + 2) = x^2(x - (1+i))(x - (1-i))$. Luego,

$$\begin{aligned} \mathrm{Ker}(D^4 - 2D^3 + 2D^2) &= \mathrm{Ker}\, D^2 \oplus \mathrm{Ker}(D - (1+i) \cdot \mathrm{Id}) \oplus \mathrm{Ker}(D - (1-i) \cdot \mathrm{Id}) \\ &= \{a + bx + c \cdot e^{(1+i) \cdot x} + d \cdot e^{(1-i) \cdot x}\} \end{aligned}$$

Luego,

$$\left\{ \begin{array}{l} \text{Las funciones con valores en } \mathbb{R} \text{ solución de} \\ \text{la ecuación diferencial } f'''' - 2f''' + 2f'' = 0 \end{array} \right\} = \{a + bx + e^x \cdot (\lambda \cos x + \mu \,\mathrm{sen}\, x)\}$$



Wikipedia

14. Movimiento armónico simple: Consideremos un muelle cuyo extremo esté en el origen de la recta real. Denotemos por $f(t)$ la posición del extremo del muelle en el instante t. Si el extremo del muelle está en la posición $f(t)$ en el instante t, entonces el muelle ejerce una fuerza (luego aceleración) proporcional a $f(t)$ con sentido hacia el origen. Entonces,

$$f''(t) = -cte \cdot f(t), \qquad (cte > 0).$$

Es decir, $f(t)$ cumple la ecuación diferencial

$$(D^2 + cte)(f) = 0.$$

Como $x^2 + cte = (x - \sqrt{cte} \cdot i)(x + \sqrt{cte} \cdot i)$, tenemos que $f(t) = a\cos(cte \cdot t) + b\,\mathrm{sen}(cte \cdot t)$. Como $f(0) = 0$, entonces $a = 0$ y

$$f(t) = b \cdot \mathrm{sen}(cte \cdot t)$$

Observemos que b es la máxima elongación del muelle y $\frac{2\pi}{cte}$ el periodo del movimiento armónico.

15. Ejercicio: Resuelve la ecuación diferencial: $f'' + f = 0$.

Ecuaciones diferenciales lineales no homogéneas

Hasta ahora hemos resuelto ecuaciones diferenciales del tipo $P(D)(f) = 0$. Consideremos ahora una ecuación diferencial del tipo $P(D)(f) = g$, con $g \in F$. Sea f_0 una solución particular. Entonces, $f \in F$ cumple que $P(D)(f) = g$ si y sólo si

$$f = f_0 + f_1, \text{ con } f_1 \in \mathrm{Ker}\, P(D)$$

Dicho con palabras

$$\left[\begin{array}{l}\text{Todas las soluciones}\\ \text{de } P(D)(f) = g\end{array}\right] = \left[\begin{array}{l}\text{Una solución parti-}\\ \text{cular de } P(D)(f) = g\end{array}\right] + \left[\begin{array}{l}\text{Todas las soluciones de la}\\ \text{“homogénea” } P(D)(f) = 0\end{array}\right]$$

16. Ejemplo: Consideremos un objeto en caída libre. Supongamos que no hay más fuerza de rozamiento que la producida por el aire por causa de la velocidad del objeto. Supongamos que el rozamiento es proporcional a la velocidad. Planteemos la ecuación: Sea $V(t)$ la velocidad del objeto. La aceleración del objeto será igual a la gravedad g menos una constante por la velocidad (debido a la fuerza de rozamiento). Luego,

$$V'(t) = g - R \cdot V(t), \quad (R > 0).$$

Es decir, $(D + R \cdot \mathrm{Id})V = g$. Una solución particular de esta ecuación es $V_0 = \frac{g}{R}$. Luego, todas las soluciones son $V = \frac{g}{R} + a \cdot e^{-Rt}$. Si $V(0) = 0$, entonces $a = \frac{-g}{R}$ y

$$V(t) = \frac{g}{R}(1 - e^{-Rt}).$$

Denotemos $S(t)$ los metros recorridos en el tiempo t, entonces $V(t) = S'(t)$ e integrando $S(t) = \int \frac{g}{R}(1 - e^{-Rt}) = b + \frac{g}{R}(t + \frac{e^{-Rt}}{R})$. Como $S(0) = 0$, entonces $b = \frac{-g}{R^2}$ y

$$S(t) = \frac{g}{R}t + \frac{g}{R^2}(-1 + e^{-Rt}).$$

17. Sea $P(D)f = g$, con $g \in F$, una ecuación diferencial y supongamos que existe un polinomio $Q(x)$ tal que $Q(D)g = 0$. La aplicación lineal $P(D)\colon \operatorname{Ker} Q(D)P(D) \to \operatorname{Ker} Q(D)$ es epiyectiva (obsérvese que $\dim \operatorname{Ker} H(D) = \operatorname{gr}(H(x))$ y que el núcleo de esta aplicación lineal es $\operatorname{Ker} P(D)$). Sabemos calcular por Álgebra Lineal $f \in \operatorname{Ker} Q(D)P(D)$ tal que $P(D)(f) = g$.

Supongamos ahora además que $P(x)$ es primo $Q(x)$. Sean $\lambda(x)$ y $\mu(x)$ polinomios tales que $\lambda(x)\cdot P(x) + \mu(x)\cdot Q(x) = 1$. Por lo tanto, tenemos que $\lambda(D)\cdot P(D) + \mu(D)\cdot Q(D) = \mathrm{Id}$. Si aplicamos esta igualdad a g, obtenemos

$$g = \mathrm{Id}(g) = (\lambda(D)\cdot P(D) + \mu(D)\cdot Q(D))(g) = (\lambda(D)\cdot P(D))(g) = P(D)(\lambda(D)(g))$$

Por tanto, una solución particular es $f = \lambda(D)(g)$.

De otro modo: Sea $E = \langle g, g', g'', \ldots, g^{n)}, \ldots\rangle \subseteq \operatorname{Ker} Q(D)$ que es un espacio vectorial de dimensión finita y $g \in E$. $P(D)\colon E \to E$, $f \mapsto P(D)(f)$ es un isomorfismo (pues su inverso es $\lambda(D)$). Solo tenemos que calcular $f \in E$ tal que $P(D)(f) = g$.

18. Ejemplo: Resolvamos la ecuación diferencial $f''' - f = x^3$: Tenemos que resolver la ecuación $(D^3 - \mathrm{Id})(f) = x^3$. Observemos que $D^4(x^3) = 0$. Los polinomios $x^3 - 1$ y x^4 son primos entre sí. Tenemos

$$\begin{aligned} \underline{x^4} &= \underline{(x^3-1)}\cdot x + \underline{x} \\ \underline{x^3-1} &= \underline{x}\cdot x^2 - 1 \end{aligned}$$

Luego, $1 = \underline{x}\cdot x^2 - \underline{(x^3-1)} = (\underline{x^4} - \underline{(x^3-1)}\cdot x)\cdot x^2 - \underline{(x^3-1)} = x^2\cdot \underline{x^4} + (-x^3-1)\cdot \underline{(x^3-1)}$. Por lo tanto,

$$\begin{aligned} x^3 &= (D^2\cdot D^4 + (-D^3 - \mathrm{Id})\cdot(D^3 - \mathrm{Id}))(x^3) = ((-D^3 - \mathrm{Id})\cdot(D^3 - \mathrm{Id}))(x^3) \\ &= (D^3 - \mathrm{Id})((-D^3 - \mathrm{Id})(x^3)) = (D^3 - \mathrm{Id})(-6 - x^3). \end{aligned}$$

Luego una solución particular de la ecuación diferencial es $f_0 = -6 - x^3$. De otro modo: Sea $\operatorname{Ker} D^4 = \langle 1, x, x^2, x^3\rangle$. El endomorfismo lineal $D^3 - \mathrm{Id}\colon \operatorname{Ker} D^4 \to \operatorname{Ker} D^4$, $p(x) \mapsto (D^3 - \mathrm{Id})(p(x))$ es un isomorfismo lineal y es fácil calcular el polinomio $ax^3 + bx^2 + cx + d$ que cumple que $(D^3 - \mathrm{Id})(ax^3 + bx^2 + cx + d) = x^3$.

Todas las soluciones son

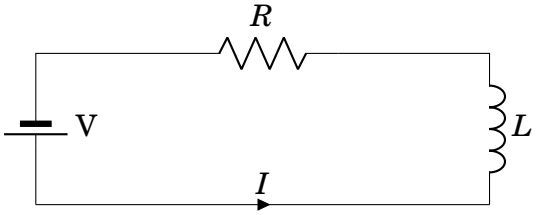
$$\begin{aligned} f_0 + \operatorname{Ker}(D^3 - \mathrm{Id}) &= f_0 + \operatorname{Ker}(D - \mathrm{Id}) + \operatorname{Ker}(D - \frac{-1-\sqrt{-3}}{2}\cdot \mathrm{Id}) + \operatorname{Ker}(D - \frac{-1+\sqrt{-3}}{2}\cdot \mathrm{Id}) \\ &= -6 - x^3 + a\cdot e^x + b\cdot e^{\frac{-1-\sqrt{-3}}{2}\cdot x} + c\cdot e^{\frac{-1+\sqrt{-3}}{2}\cdot x}. \end{aligned}$$

Todas las soluciones que son funciones con valores reales son

$$-6 - x^3 + a\cdot e^x + e^{\frac{-1}{2}x}\cdot(c\cdot \cos\frac{\sqrt{3}}{2}x + d\cdot \operatorname{sen}\frac{\sqrt{3}}{2}x).$$

19. Ejercicio : Resuelve la ecuación diferencial $f'' - f = senx$.

20. Circuito eléctrico Consideremos el circuito eléctrico que sigue:



La segunda ley de Kirchhoff afirma que la suma de las diferencias de potencial eléctrico en un circuito cerrado es igual a cero. La caída de potencial en una bobina es proporcional a la tasa de variación de la intensidad de corriente: $V_L = L \cdot \frac{dI}{dt}$, la caída de tensión en una resistencia es proporcional a la intensidad: $V_R = R \cdot I$ (ley de Ohm). Por tanto,

$$V = L \cdot \frac{dI}{dt} + R \cdot I.$$

Resolvamos la ecuación diferencial $LI' + RI = (LD + R\,\mathrm{Id})(I) = V$, cuando V es constante. Una solución particular es $I = V/R$ y la general es

$$I(t) = V/R + \mathrm{Ker}(LD + R\,\mathrm{Id}) = V/R + \mathrm{Ker}(D + \frac{R}{L}\,\mathrm{Id}) = V/R + \{\lambda \cdot e^{-\frac{Rt}{L}}\}.$$

Si suponemos que $I(0) = 0$, entonces $\lambda = -V/R$ y $I(t) = V/R \cdot (1 - e^{-\frac{Rt}{L}})$.

Supongamos ahora que $V = A\cos(wt)$. Tenemos que resolver la ecuación diferencial

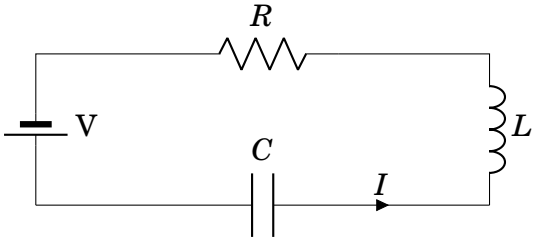
$$(LD + R\,\mathrm{Id})(I) = A \cdot \cos(wt).$$

Sea $E = \langle \cos(wt), \mathrm{sen}(wt) \rangle$. Buscamos una solución $\lambda \cdot \cos(wt) + \mu \cdot \mathrm{sen}(wt) \in E$:

$$\begin{aligned} A \cdot \cos(wt) &= (LD + R\,\mathrm{Id})(\lambda \cdot \cos(wt) + \mu \cdot \mathrm{sen}(wt)) \\ &= (R\mu - Lw\lambda)\,\mathrm{sen}(wt) + (R\lambda + Lw\mu)\cos(wt). \end{aligned}$$

Obtenemos $\lambda = \frac{AR}{L^2w^2+R^2}$ y $\mu = \frac{ALw}{L^2w^2+R^2}$. Por tanto, $I(t) = \frac{AR\cos(wt)}{L^2w^2+R^2} + \frac{ALw\,\mathrm{sen}(wt)}{L^2w^2+R^2} + \gamma \cdot e^{-\frac{Rt}{L}}$. Si suponemos que $I(0) = 0$, entonces

$$\begin{aligned} I(t) &= \frac{A}{L^2w^2 + R^2} \cdot (R \cdot (\cos(wt) - e^{-\frac{Rt}{L}}) + Lw \cdot \mathrm{sen}(wt)) \\ &\overset{t \gg 0}{\simeq} \frac{A}{L^2w^2 + R^2} \cdot (R \cdot \cos(wt) + Lw \cdot \mathrm{sen}(wt)). \end{aligned}$$



Añadamos un condensador. La diferencia de potencial causada por un condensador es proporcional a la carga, $V_C = \frac{Q}{C}$, luego derivando respecto del tiempo $V_C' = \frac{I}{C}$. Por tanto, $V = L \cdot \frac{dI}{dt} + R \cdot I + V_C$ y derivando

$$V' = LI'' + RI' + \frac{I}{C}.$$

Supongamos $V(t) = V_0 \cdot \cos(wt)$. Si $\tilde{V} := V_0 \cdot e^{iwt}$, entonces I es la parte real de las soluciones de la ecuación diferencial

$$\tilde{V}' = L\tilde{I}'' + R\tilde{I}' + \frac{\tilde{I}}{C}.$$

Busquemos una solución particular en $\langle e^{iwt} \rangle$, es decir, $\tilde{I} = Y \cdot e^{iwt}$, con $Y \in \mathbb{C}$. Tenemos que $iwV_0 \cdot e^{iwt} = (-Lw^2 + Rwi + \frac{1}{C}) \cdot Y \cdot e^{iwt}$, luego $\tilde{I} = \frac{iwV_0}{(-Lw^2+\frac{1}{C})+Rwi} \cdot e^{iwt}$. Por lo tanto,

$$\tilde{I} = \frac{\tilde{V}}{Z},$$

donde $Z = Z_0 \cdot e^{i\phi}$ (denominada impedancia), $\phi = \arctan \frac{Lw - \frac{1}{wc}}{R}$ (denominada desfase) y $Z_0 = \sqrt{(Lw - \frac{1}{wC})^2 + R^2}$. En conclusión„

$$\boxed{I(t) = \frac{V_0}{Z_0} \cdot \cos(wt - \phi)}\ [1]$$

Observemos que la amplitud del voltaje es V_0 y el de la intensidad $I_0 := \frac{V_0}{Z_0}$, luego

$$\boxed{V_0 = Z_0 \cdot I_0}$$

21. Resolvamos la ecuación diferencial $f''' - 2f'' + f = xe^x$ siguiendo otro método: Tenemos $(D^3 - 2D^2 + \mathrm{Id})(f) = xe^x$, luego una solución particular es

$$f = \frac{1}{D^3 - 2D^2 + \mathrm{Id}} xe^x = \frac{1}{(D^2 - D - \mathrm{Id})(D - \mathrm{Id})} xe^x = e^x \frac{1}{(D^2 + D - \mathrm{Id})D} x$$
$$\overset{*}{=} e^x(-\mathrm{Id} - D - 2D^2)\frac{1}{D}x = e^x(\frac{-x^2}{2} + cte - x - 2) = e^x(\frac{-x^2}{2} - x + a)$$

($*$ el desarrollo de Taylor de $\frac{1}{x^2+x-1}$ en $x = 0$ hasta orden tres es $-1 - x - 2x^2$).

22. Vamos a denotar $\int f = \frac{1}{D} f$ y en general $\int \overset{n}{\cdots} \int f = \frac{1}{D^n} f$.

Sea $P(x) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$. Existen polinomios $Q_1(x), \ldots, Q_r(x)$ tales que

$$\frac{1}{(x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}} = \frac{Q_1(x)}{(x - \alpha_1)^{n_1}} + \overset{r}{\cdots} + \frac{Q_r(x)}{(x - \alpha_r)^{n_r}}.$$

Resolvamos la ecuación diferencial $P(D)f = g$.

$$f = \frac{1}{P(D)} g = (\frac{Q_1(D)}{(D - \alpha_1 \mathrm{Id})^{n_1}} + \overset{r}{\cdots} + \frac{Q_r(D)}{(D - \alpha_r \mathrm{Id})^{n_r}})g = \sum_i \frac{Q_i(D)}{(D - \alpha_i \mathrm{Id})^{n_i}} g$$
$$\overset{4.5.7}{=} \sum e^{\alpha_i x} \cdot \frac{Q_i(D + \alpha_i \mathrm{Id})}{D^{n_i}} e^{-\alpha_i x} \cdot g = \sum e^{\alpha_i x} \cdot Q_i(D + \alpha_i \mathrm{Id}) \overset{n_i}{\int \cdots \int} e^{-\alpha_i x} \cdot g.$$

[1] Podemos decir que es la solución, porque si $R^2 \neq \frac{4L}{C}$ entonces

$$\mathrm{Ker}(LD^2 + RD + \frac{\mathrm{Id}}{C}) = \mathrm{Ker}(D - \frac{-R + \sqrt{R^2 - 4L/C}}{2L}) \oplus \mathrm{Ker}(D - \frac{-R - \sqrt{R^2 - 4L/C}}{2L})$$
$$= \{a \cdot e^{\frac{-R+\sqrt{R^2-4L/C}}{2L} t} + be^{\frac{-R-\sqrt{R^2-4L/C}}{2L} t} \overset{t \gg 0}{\simeq} 0\},$$

y si $R^2 = 4L/C$, $\mathrm{Ker}(D - \frac{-R-\sqrt{R^2-4L/C}}{2L}) = \{e^{\frac{-R}{2L} t} \cdot (a + bt) \overset{t \gg 0}{\simeq} 0\}$.

4.5.2. Ecuaciones en diferencias finitas

Sea $S = \{(a_n)_{n\in\mathbb{N}}\}$ el $\mathbb{C}$-espacio vectorial de las sucesiones de números complejos. La sucesión $(a_n)_{n\in\mathbb{N}}$ muchas veces la denotaremos simplemente (a_n). Consideremos el "operador siguiente" $\nabla\colon S \to S$ que es el endomorfismo $\mathbb{C}$-lineal definido por

$$\nabla(a_n) = (b_n), \text{ donde } b_n = a_{n+1}.$$

Diremos que $\Delta := \nabla - \mathrm{Id}$ es el "operador diferencia".

Como sabemos, dado un polinomio $P(x) = c_r x^r + c_{r-1}x^{r-1} + \cdots + c_0 \in \mathbb{C}[x]$, podemos considerar el endomorfismo lineal $P(\nabla)\colon S \to S$ definido por

$$\begin{aligned} P(\nabla)(a_n) &= (c_r\nabla^r + c_{r-1}\nabla^{r-1} + \cdots + c_0\,\mathrm{Id})(a_n) \\ &= (c_r a_{n+r} + c_{r-1}a_{n+r-1} + \cdots + c_0 a_n). \end{aligned}$$

Queremos resolver las ecuaciones en diferencias finitas (homogéneas)

$$c_r a_{n+r} + c_{r-1}a_{n+r-1} + \cdots + c_0 a_n = 0$$

Queremos calcular a_n, es decir, queremos calcular $\mathrm{Ker}\,P(\nabla)$.

23. Proposición: *Se cumple que* $\{(1),(n),\ldots,(n^{r-1})\}$ *es una base de* $\mathrm{Ker}\,\Delta^r$

Demostración. Obviamente, $\mathrm{Ker}\,\Delta = \langle(1)\rangle$. Si $p(n)$ es un polinomio de grado s, es fácil ver que $\Delta(p(n))$ es un polinomio de grado $s-1$. Por tanto, $\{(1),(n),\ldots,(n^{r-1})\} \subseteq \mathrm{Ker}\,\Delta^r$. Consideremos la aplicación lineal

$$\Delta\colon \mathrm{Ker}\,\Delta^s \to \mathrm{Ker}\,\Delta^{s-1},\ (a_n) \mapsto \Delta(a_n),$$

cuyo núcleo es $\mathrm{Ker}\,\Delta = \langle(1)\rangle$. Por tanto, $\dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^s \le \dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^{s-1} + 1$. Recurrentemente, obtenemos que $\dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^r \le r$. Por dimensiones $\langle(1),(n),\ldots,(n^{r-1})\rangle = \mathrm{Ker}\,\Delta^r$. □

24. Fórmula de conmutación: Sea $P(x) \in \mathbb{C}[x]$ y (a_n) una sucesión de números complejos. Entonces,

$$P(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot P(\alpha\nabla)(a_n).$$

Demostración. En efecto, $\nabla((\alpha^n)\cdot(a_n)) = \nabla(\alpha^n \cdot a_n) = (\alpha^{n+1}\cdot a_{n+1}) = (\alpha^n)\cdot(\alpha\cdot\nabla)(a_n)$. Por tanto, $\nabla^2((\alpha^n)\cdot(a_n)) = \nabla((\alpha^n)\cdot(\alpha\nabla)(a_n)) = (\alpha^n)\cdot(\alpha\cdot\nabla)^2(a_n)$. Recurrrentemente obtenemos $\nabla^r((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot(\alpha\nabla)^r(a_n)$ y $P(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot P(\alpha\nabla)(a_n)$. □

Por lo tanto,

$$\boxed{P(\nabla - \alpha)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot P(\alpha\cdot\Delta)(a_n)}$$

25. Teorema: *Se cumple que*

1. $\mathrm{Ker}(\nabla - \alpha\cdot\mathrm{Id})^r = (\alpha^n)\cdot\{$*pol.* $q(n)$ *de grado menor que* r*)*$\}$ *(suponemos* $\alpha \neq 0$*).*

2. *Si* $P(x) = (x-\alpha_1)^{r_1}\cdots(x-\alpha_s)^{r_s}$*, con* $\alpha_i \neq 0$ *para todo* i*, entonces*

$$\operatorname{Ker} P(\nabla) = (\alpha_1{}^n)\cdot\{(\textit{Pol. } q(n) \textit{ de grado} < r_1)\} \oplus \overset{r}{\cdots} \oplus (\alpha_s^n)\cdot\{\textit{Pol. } q(n) \textit{ de grado} < r_s\}.$$

Demostración. 1. $(s(n)) \in \operatorname{Ker}(\nabla-\alpha)^r \iff 0 = (\nabla-\alpha)^r(s(n)) \iff 0 = (\nabla-\alpha)^r((\alpha^n)\cdot(\alpha^{-n})\cdot(s(n))) = (\alpha^n)\cdot(\alpha\Delta)^r((\alpha^{-n})\cdot(s(n))) \iff 0 = \Delta^r((\alpha^{-n})\cdot(s(n))) \iff$ existe un polinomio $q(n)$ de grado menor que r tal que $\alpha^{-n}\cdot s(n) = q(n)$, es decir, $s(n) = \alpha^n \cdot q(n)$.

2. Es consecuencia de que $\operatorname{Ker} P(\nabla) = \operatorname{Ker}(\nabla - \alpha_1 \operatorname{Id})^{n_1} \oplus \cdots \oplus \operatorname{Ker}(\nabla - \alpha_r \operatorname{Id})^{n_r}$ y de 2. □

26. Nota: Supongamos $P(x) \in \mathbb{R}[x]$ y $\alpha = \rho\cdot(\cos\beta + i\cdot\operatorname{sen}\beta)$ es una raíz compleja de $P(x)$, con $\beta \neq 0, \pi$. Entonces, $P(x) = (x-\alpha)^r\cdot(x-\bar\alpha)^r\cdot Q(x)$, con $Q(\alpha), Q(\bar\alpha) \neq 0$. Es facil probar, a partir de 4.5.25, que

$$\left\{ \begin{array}{l} (s(n)) \in \operatorname{Ker}(\nabla^2 - 2\rho\cos(\beta\cdot n)\cdot\nabla + \rho^2)^r \\ \text{tales que } s(n) \in \mathbb{R} \text{ para todo } n. \end{array} \right\} = \left\{ \begin{array}{l} (s(n)) \in \operatorname{Ker}(\nabla - \alpha\operatorname{Id})^n \oplus \operatorname{Ker}(\nabla - \bar\alpha\operatorname{Id})^r \\ \text{tales que } s(n) \in \mathbb{R} \text{ para todo } n. \end{array} \right\}$$

$$= \left\{ \begin{array}{l} s(n) \in \langle \rho^n(\cos(\beta\cdot n) + i\operatorname{sen}(\beta\cdot n))\cdot x^s, \rho^n(\cos(\beta\cdot n) - i\operatorname{sen}(\beta\cdot n))\cdot x^s \mid 0 \le s < r\rangle_{\mathbb{C}}, \\ s(n) \in \mathbb{R},\ \forall n. \end{array} \right\}$$

$$= \left\{ \begin{array}{l} s(n) \in \langle \rho^n\cos(\beta\cdot n)\cdot x^s, \rho^n\operatorname{sen}(\beta\cdot n)\cdot x^s \mid 0 \le s < r\rangle_{\mathbb{C}}, \\ s(n) \in \mathbb{R},\ \forall n. \end{array} \right\}$$

$$= \rho^n\cdot\cos(\beta\cdot n)\cdot\left\{ \begin{array}{l} \text{Pol. } q(n) \text{ con coef.} \\ \text{reales de grado } < r \end{array} \right\} + \rho^n\cdot\operatorname{sen}(\beta\cdot n)\cdot\left\{ \begin{array}{l} \text{Pol. } q(n) \text{ con coef.} \\ \text{reales de grado } < r \end{array} \right\}.$$

27. Ejemplo: Resolvamos la ecuación $a_{n+2} = a_{n+1} + a_n$, con las condiciones iniciales $a_0 = 0, a_1 = 1$ (sucesión de Fibonacci). "Esta sucesión fue descrita por Leonardo de Pisa, matemático italiano del siglo XIII también conocido como Fibonacci. Tiene numerosas aplicaciones en ciencias de la computación, matemática y teoría de juegos. También aparece en configuraciones biológicas, como por ejemplo en las ramas de los árboles, en la disposición de las hojas en el tallo, en las flores de alcachofas y girasoles, en las inflorescencias del brécol romanesco, en la configuración de las piñas de las coníferas, en la reproducción de los conejos y en cómo el ADN codifica el crecimiento de formas orgánicas complejas. De igual manera, se encuentra en la estructura espiral del caparazón de algunos moluscos, como el nautilus." (Wikipedia). Tenemos que $a_{n+2} - a_{n+1} - a_n = 0$, luego

$$(\nabla^2 - \nabla - \operatorname{Id})(a_n) = (0).$$

Observemos que $x^2 - x - 1 = (x - \frac{1+\sqrt5}{2})\cdot(x - \frac{1-\sqrt5}{2})$, por tanto

$$(a_n) \in \operatorname{Ker}(\nabla^2 - \nabla - \operatorname{Id}) = \operatorname{Ker}(\nabla - \frac{1+\sqrt5}{2}\cdot\operatorname{Id}) \oplus (\nabla - \frac{1-\sqrt5}{2}\cdot\operatorname{Id}) = (a\cdot(\frac{1+\sqrt5}{2})^n + b\cdot(\frac{1-\sqrt5}{2})^n).$$

Recordemos que

$$0 = a_0 = a + b$$
$$1 = a_1 = a\cdot(\tfrac{1+\sqrt5}{2}) + b\cdot(\tfrac{1-\sqrt5}{2})$$

Resulta que $a = \frac{1}{\sqrt5}$ y $b = -\frac{1}{\sqrt5}$. Luego,

$$a_n = \frac{1}{\sqrt5}\cdot(\frac{1+\sqrt5}{2})^n - \frac{1}{\sqrt5}\cdot(\frac{1-\sqrt5}{2})^n.$$

28. Préstamos: Un banco nos presta un capital K, a devolver en N años, a un tipo de interés anual I. ¿Cuánto dinero D deberemos pagar al año, de modo que todos los años paguemos la misma cantidad y en los N años hayamos saldado nuestra deuda con el banco?

Resolución: Sea i_n el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n (por el capital K que nos han prestado). Entonces $D = a_n + i_n$. Además, $i_n = I \cdot (K - \sum_{r=1}^{n-1} a_r)$. Por tanto, $D = a_n + I \cdot (K - \sum_{r=1}^{n-1} a_r)$. Si aplicamos el operador diferencia Δ entonces

$$0 = \Delta(a_n) - I \cdot a_n = (\nabla - (1+I))(a_n).$$

Por tanto, $a_n = (1+I)^n \cdot \lambda$ y

$$D = a_1 + IK = (1+I) \cdot \lambda + IK. \qquad (*)$$

Tenemos que calcular λ. Nos falta decir que amortizamos el préstamo en N años, es decir, $K = \sum_{r=1}^{N} a_r$, que equivale a decir que $D = a_{N+1} = (1+I)^{N+1} \cdot \lambda$. Despejando λ y sustituyendo su valor en $(*)$ obtendremos que

$$D = \frac{IK}{1 - \frac{1}{(1+I)^N}}.$$

29. Ejercicio: Calcula cuántos números de longitud n se pueden escribir con ceros y unos, de modo que nunca aparezcan dos ceros seguidos (ejemplo: los números de longitud tres cumpliendo lo dicho son $010, 011, 101, 110, 111$, que son cinco distintos).

30. Ejercicio: Calcula $\operatorname{Ker} \nabla^r$.

Ecuaciones en diferencias finitas no homogéneas

Consideremos una ecuación en diferencias $P(\nabla)(s(n)) = z(n)$. Sea $(s_0(n))$ una solución particular. Entonces, $(s(n))$ es una solución de la ecuación en diferencias si y sólo si

$$s(n) = s_0(n) + t(n), \text{ con } t(n) \in \operatorname{Ker} P(\nabla)$$

Con palabras

$$\left[\begin{array}{l}\text{Todas las soluciones}\\ \text{de } P(\nabla)(s(n)) = (z(n))\end{array}\right] = \left[\begin{array}{l}\text{Solución particular}\\ \text{de } P(\nabla)(s(n)) = (z(n))\end{array}\right] + \left[\begin{array}{l}\text{Todas las soluciones de la}\\ \text{“homogénea” } P(\nabla)(s(n)) = 0\end{array}\right]$$

31. Resolvamos la ecuación $P(\nabla)(s(n)) = z(n)$, suponiendo que existe un polinomio $Q(x)$ primo con $P(x)$ de modo que $Q(\nabla)(z(n)) = 0$:

Por el algoritmo de Euclides podemos calcular polinomios $\lambda(x)$ y $\mu(x)$ tales que $\lambda(x) \cdot P(x) + \mu(x) \cdot Q(x) = 1$. Por tanto, $\lambda(\nabla) \cdot P(\nabla) + \mu(\nabla) \cdot Q(\nabla) = \mathrm{Id}$. Si aplicamos esta igualdad a $(z(n))$, obtenemos

$$(z(n)) = \lambda(\nabla) \cdot P(\nabla)(z(n)) = P(\nabla)(\lambda(\nabla)(z(n))).$$

Por tanto, una solución particular es $s_0(n) = \lambda(\nabla)(z(n))$.

32. Ejemplo: Resolvamos $a_{n+2}+2a_{n+1}-6a_n=2^n$: Tenemos que resolver

$$(\nabla^2+2\nabla-6\,\mathrm{Id})(a_n)=(2^n)$$

Calculemos una solución particular. Observemos que $(\nabla-2\,\mathrm{Id})(2^n)=(0)$ y que los polinomios x^2+2x-6 y $x-2$ son primos entre sí. Mediante el algoritmo de Euclides sabemos calcular $\lambda(x),\mu(x)$ de modo que $\lambda(x)\cdot(x^2+2x-6)+\mu(x)\cdot(x-2)=1$. En efecto,

$$x^2+2x-6=(x+4)(x-2)+2$$

Luego, $1=\frac{1}{2}\cdot(x^2+2x-6)-\frac{x+4}{2}(x-2)$. Luego,

$$\begin{aligned}(2^n)&=(\frac{1}{2}\cdot(\nabla^2+2\nabla-6\,\mathrm{Id})-\frac{\nabla+4\,\mathrm{Id}}{2}(\nabla-2\,\mathrm{Id}))(2^n)=\frac{1}{2}\cdot(\nabla^2+2\nabla-6\,\mathrm{Id})(2^n)\\&=(\nabla^2+2\nabla-6\,\mathrm{Id})(\frac{1}{2}2^n)\end{aligned}$$

Luego, (2^{n-1}) es una solución particular. Procedamos de otro modo:

$$(a_n)=\frac{1}{\nabla^2+2\nabla-6\,\mathrm{Id}}(2^n)=\frac{1}{2^2+2\cdot2-6}(2^n)=(2^{n-1})$$

($(\nabla-2\,\mathrm{Id})(2^n)=0$ y el desarrollo de Taylor de $\frac{1}{x^2+2x-6}$ de orden 0 en $x=2$ es $\frac{1}{2^2+2\cdot2-6}$).

Todas las soluciones son

$$\begin{aligned}a_n=2^{n-1}+\mathrm{Ker}(\nabla^2+2\nabla-6\,\mathrm{Id})&=2^{n-1}+\mathrm{Ker}(\nabla-(-1+\sqrt{7}))+\mathrm{Ker}(\nabla-(-1-\sqrt{7}))\\&=2^{n-1}+a\cdot(-1+\sqrt{7})^n+b\cdot(-1-\sqrt{7})^n\end{aligned}$$

33. Préstamos con gradiente lineal: Por la compra de un coche en un concesionario pagaremos cada año n un dinero d_n de modo que $d_n=A+G\cdot(n-1)$ (con $A=1000$ y $G=100$), durante $N=20$ años. Se supone que el tipo de interés anual es $I=5\%$. Determinar cuál es el valor K del coche (en la actualidad).

Resolución: Podemos decir que nos han prestado un capital K a un tipo de interés I a devolver en N años y que cada año n pagamos (por la amortización y los intereses) d_n. Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n=i_n+a_n$. Tenemos que $i_n=I\cdot(K-\sum_{r=1}^{n-1}a_r)$. Por tanto,

$$A+G\cdot(n-1)=d_n=a_n+I\cdot(K-\sum_{r=1}^{n-1}a_r).\qquad(*)$$

Para $n=1$, tenemos que

$$A=a_1+I\cdot K\qquad(**)$$

Tenemos que determinar a_1. Aplicando Δ en $(*)$ obtenemos

$$G=\Delta(a_n)-I\cdot(a_n)=(\Delta-I)(a_n)=(\nabla-(1+I))(a_n)$$

Una solución particular, es $a_n = \frac{-G}{I}$ y todas las soluciones son $a_n = \frac{-G}{I} + cte \cdot (1+I)^n$. Luego, $a_1 = \frac{-G}{I} + cte \cdot (1+I)$. Tenemos que calcular cte. Nos falta imponer que $\sum_{i=1}^{N} a_n = K$, es decir, $A + GN = d_{N+1} = a_{N+1} = -\frac{G}{I} + cte \cdot (1+I)^{N+1}$. Luego, $cte = \frac{A+GN+\frac{G}{I}}{(1+I)^{N+1}}$. En conclusión

$$a_1 = -\frac{G}{I} + \frac{A+GN+\frac{G}{I}}{(1+I)^{N+1}} \cdot (1+I) = -\frac{G}{I} + \frac{A+GN+\frac{G}{I}}{(1+I)^N}$$

Sustituyendo el valor de a_1 en $(**)$, puede comprobarse que

$$K = \frac{A}{I} \cdot \frac{(1+I)^N - 1}{(1+I)^N} + \frac{G}{I^2} \cdot \frac{(1+I)^N - 1 - IN}{(1+I)^N} = 22311'1.$$

Supongamos que voy a un banco que me ofrece un interés anual $I = 1\%$ por mi dinero. Tendría que depositar $K = 34592$ euros para que el banco me fuese dando cada año lo que el concesionario me pide (y al final el banco quedase en paz conmigo). En fin, un coche de 22311 euros me ha costado 34592 euros.

34. Préstamos de gradiente exponencial: Un préstamo de $K = 10^5$ euros se quiere devolver durante $N = 20$ años, pagando cada año n una anualidad d_n de modo que $d_n = I' d_{n-1}$ ($I' = 1 + 2\%$). Se supone que nos prestan el dinero a un tipo de interés anual $I = 5\%$. Calculemos d_1.

Resolución: Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n = i_n + a_n$. Tenemos que $i_n = I \cdot (K - \sum_{r=1}^{n-1} a_r)$. Por tanto,

$$d_n = a_n + I \cdot (K - \sum_{r=1}^{n-1} a_r).$$

Si aplicamos el operador diferencia Δ, entonces $\Delta(d_n) = \Delta(a_n) - I \cdot a_n = (\nabla - (1+I))(a_n)$. Por otra parte, $(\nabla - I')(d_n) = 0$ (luego $d_n = \lambda' I'^n$). Entonces, $(\nabla - I')(\Delta(d_n)) = 0$, es decir,

$$(\nabla - I')(\nabla - (1+I))(a_n) = 0$$

Por tanto, $a_n = \lambda I'^n + \mu(1+I)^n$. Sabemos que $d_{N+1} = a_{N+1}$, de lo que se deduce que $\lambda' = \lambda + \mu(\frac{1+I}{I'})^{N+1}$. De las ecuaciones

$$\lambda' I' = d_1 = a_1 + IK = \lambda I' + \mu(1+I) + IK$$
$$\lambda' I'^2 = d_2 = a_2 + I(K - a_1) = \lambda I'(I' - I) + \mu(1+I) + IK$$

se obtiene que $d_1 = \frac{K(1-I'+I)}{1-(\frac{I'}{1+I})^N}$.

Sumatorios

Dada una sucesión de números complejos (a_n), definamos la sucesión $s_n := \sum_{i=0}^{n-1} a_i$ (y $s_0 := 0$). Entonces, $\Delta(s_n) = (s_{n+1} - s_n) = (a_n)$. Denotaremos

$$\frac{1}{\Delta_0}(a_n) := (s_n) = (\sum_{i=0}^{n-1} a_i).$$

Como hemos dicho, $\Delta(\frac{1}{\Delta_0}(a_n)) = (a_n)$, luego $\Delta^{-1}(a_n) = \frac{1}{\Delta_0}(a_n) + \{(cte),\ \forall\, cte \in \mathbb{C}\}$.

35. Ejemplo: Calculemos $\sum_{i=0}^{n} i \cdot 2^i$: Recordemos que $(\nabla - 2\,\mathrm{Id})^2(n2^n) = 0$. Entonces,

$$\begin{aligned}\sum_{i=0}^{n-1} i \cdot 2^i = \frac{1}{\Delta_0}(n2^n) &= (\frac{1}{\nabla - \mathrm{Id}}(n2^n)) + (cte) \stackrel{*}{=} (\mathrm{Id} - (\nabla - 2\,\mathrm{Id}))(n2^n) + (cte) \\ &= (n2^n - n2^{n+1} + cte) = ((n-2)2^n + cte)\end{aligned}$$

($\stackrel{*}{=}$ el desarrollo de Taylor de $\frac{1}{x-1}$ de orden 2 en $x = 2$, es $1-(x-2)+h(x)(x-2)^2$). Haciendo $n = 1$, obtenemos que $cte = 2$. Luego,

$$\sum_{i=0}^{n} i \cdot 2^i = (n-1) \cdot 2^{n+1} + 2.$$

Se define $\binom{n}{i} := \frac{n \cdot (n-1) \cdots (n-i+1)}{i \cdot (i-1) \cdots 2 \cdot 1}$. Observemos que

$$\langle (1), (n), \ldots, (n^r) \rangle = \langle (\binom{n}{0}), (\binom{n}{1}), \ldots, (\binom{n}{r}) \rangle.$$

Además, $\Delta(\binom{n}{r}) = (\binom{n}{r-1})$. Por tanto, $\frac{1}{\Delta_0}(\binom{n}{r}) = \binom{n}{r+1}$.

Si escribimos $p(n) = \sum_{i=0}^{r} \lambda_i \binom{n}{i}$, tendremos que

$$\lambda_0 = p(0), \ldots, \lambda_i = p(i) - \binom{i}{i-1}\lambda_{i-1} - \cdots - \binom{i}{0}\lambda_0,$$

y $\sum_{i=0}^{n-1} p(i) = \frac{1}{\Delta_0}(p(n)) = \sum_{i=0}^{r} \lambda_i \binom{n}{i+1}$. Finalmente, $\sum_{i=0}^{n} p(i) = \sum_{i=0}^{r} \lambda_i \binom{n+1}{i+1}$

36. Ejercicio: Calcular $\sum_{i=0}^{n} (i^2 + i - 3)$.

4.6. Cuestionario

1. Sea M un A-módulo. Prueba que $0 \cdot m = 0$, $(-1) \cdot m = -m$, $a \cdot 0 = 0$ y $a \cdot (-m) = (-a) \cdot m$.

2. Dota a $A[x]$ de estructura de A-módulo.

3. Sea $\mathscr{C}(\mathbb{R}^2)$ el conjunto de todas las funciones continuas de $\mathbb{R}^2$ en $\mathbb{R}$. Dota a $\mathscr{C}(\mathbb{R}^2)$ de estructura de $\mathbb{R}$-espacio vectorial.

4. Sea M un A-módulo y $N \subseteq M$ un subconjunto. Prueba que N es un A-submódulo de M si y solo si $n + n' \in N$, para todo $n, n' \in N$ y $a \cdot n \in N$ para todo $a \in A$ y $n \in N$.

5. Prueba que los A-submódulos de A^3, $\langle (1,2,3), (1,0,0) \rangle$ y $\langle (0,2,3), (1,0,0) \rangle$ son iguales.

6. Prueba que $A[x]$ no es un A-módulo finito generado.

7. Dados un anillo A, $a \in A$ y un A-módulo M, denotaremos $a_M \colon M \to M$ el morfismo definido por $a_M(m) := a \cdot m$, para todo $m \in M$. Prueba que $\mathrm{Ker}\, a_{M_1 \oplus M_2} = \mathrm{Ker}\, a_{M_1} \oplus \mathrm{Ker}\, a_{M_2}$. Prueba que $\mathrm{Im}\, a_{M_1 \oplus M_2} = \mathrm{Im}\, a_{M_1} \oplus \mathrm{Im}\, a_{M_2}$.

8. Resuelve el problema 4.

9. Resuelve el problema 7.

10. Sea $E = \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x+1) \oplus \mathbb{Q}[x]/(x^2-5)$ y $e_1 = (\bar{1}, 0, 0)$, $e_2 = (0, \bar{1}, 0)$, $e_3 = (0, 0, \bar{1})$ y $e_4 = (0, 0, \bar{x})$ una base del $\mathbb{Q}$-espacio vectorial E. Calcular la matriz del endomorfismo $x\cdot \colon E \to E$, $e \mapsto x \cdot e$, en la base dada.

11. Resuelve la ecuación diferencial $y'' + y = 0$.

12. Resuelve la ecuación diferencial: $y'''' - 2y''' + 2y'' = 0$,

13. Resuelve $y'' - y = x^3$.

14. Resuelve $y'' - y = x + \operatorname{sen} x$.

15. Resuelve $y''' - 2y'' + y = xe^x$.

16. Calcula $\sum_{i=0}^{n} i^2$.

4.7. Biografía de Hermann Grassmann

Hermann Günther Grassmann (Stettin, 15 de abril de 1809 - ibíd., 26 de septiembre de 1877) fue un lingüista y matemático alemán. También ejerció de físico, humanista, erudito y editor, por lo que se le considera un claro ejemplo de polimatía.
Hermann Grassmann era el tercero de los doce hijos de Justus Günter Grassmann y Johanne Luise Friederike Medenwald. Su madre era hija de un pastor de Klein-Schönfeld. Su padre había sido también consagrado pastor, pero consiguió una plaza de profesor de matemáticas y física en el Instituto de Stettin, y fue un académico notable, autor de varios libros de texto escolar de Física y Matemáticas, además de llevar a cabo interesantes investigaciones en el campo de la cristalografía. Otro hermano de Hermann, Robert, también se dedicó a las matemáticas y ambos trabajaron conjuntamente en muchos proyectos.

Durante su juventud, Hermann fue educado por su madre, mujer de una vasta cultura. Luego asistió a una escuela privada, antes de ingresar en el Instituto de Stettin, en el que daba clases su padre. La mayoría de los matemáticos despuntan ante sus profesores desde muy jóvenes. Sin embargo, y a pesar de tener unas extraordinarias oportunidades al pertenecer a una familia proclive a la educación, Hermann no destacó de modo especial en sus años de estudios secundarios, hasta el punto de que su padre pensó que debía dedicarse a algún tipo de trabajo manual, como el de jardinero o artesano.

Hermann apreciaba la música y aprendió a tocar el piano, a la vez que proseguía sus estudios, en los que poco a poco iba mejorando, y en los exámenes finales de los estudios secundarios, con 18 años, terminó el segundo de su promoción. Tras demostrar al final de sus estudios su competencia académica, Hermann decidió estudiar Teología, y en 1827 se trasladó a Berlín junto a su hermano mayor para cursar estudios en la Universidad. Realizó estudios de Teología, lenguas clásicas, Filosofía y Literatura, y no parece que acudiera a ninguna clase de Matemáticas o Física.

A pesar de que parece evidente que Hermann no tuvo formación universitaria formal alguna en matemáticas, ésta era la materia que más le interesaba cuando regresó a Stettin, en otoño de 1830, tras haber completado sus estudios universitarios en Berlín. Evidentemente, la influencia de su padre en esta vía fue muy importante, y pudo haber llegado a ser profesor de matemáticas, pero ya se había decidido a llevar a cabo investigaciones matemáticas por su cuenta. Después de pasar un año investigando en matemáticas y preparando el examen para profesor de instituto, Hermann se fue a a Berlín en diciembre de 1831 para presentarse a dichos exámenes.

Parece ser que sus ejercicios escritos no debieron ser muy bien valorados, puesto que sus examinadores le dieron el título para enseñar solo en los primeros niveles de la secundaria. Se le dijo que, antes de poder enseñar en los niveles superiores, debería volver a examinarse y demostrar unos mayores conocimientos en los temas por los que había concursado. En la primavera de 1832 obtuvo una plaza de profesor ayudante en el Instituto de Stettin.

Fue sobre esta época cuando realizó sus dos primeros descubrimientos matemáticos significativos, que estaban destinados a llevarlo a las importantes ideas que desarrollaría años después. En la premisa de su Die Lineale Ausdehnungslehre, ein neuer Zweig der Mathematik (Teoría de la extensión lineal, una nueva rama de las matemáticas, 1844), Grassmann describe cómo había ido llegando a estas ideas ya alrededor del año 1832.

En 1834, Grassmann empezó a dar clases de matemáticas en la Gewerbeschule (Escuela de artes y oficios) de Berlín. Un año más tarde regresó a Stettin para dar clases de matemáticas, física, lengua alemana, latín y religión en un centro educativo nuevo, la Otto Schule. Esta gran variedad de materias a impartir es prueba de que aún estaba habilitado solamente para impartir clases en las escuelas en los niveles más bajos. En los cuatro años siguientes, Grassmann superó los exámenes que le permitieron dar clases de matemáticas, física, química y mineralogía en todos los niveles de los centros de educación secundaria.

Grassmann se sentía en parte frustrado por el hecho de tener que dar clases solo en niveles de secundaria, a pesar de ser capaz de elaborar una matemática innovadora. En 1847 pasa a ser “Oberlehre”. En 1852 se le asignó el puesto que anteriormente había desempeñado su padre en el Instituto de Stettin, y obtuvo de ese modo el título de profesor. En 1847 solicitó al ministro prusiano de Educación ser tenido en cuenta para el desempeño de un puesto de profesor universitario, y el ministro solicitó a Ernst Eduard Kummer su opinión acerca de Grassmann. Kummer contestó diciendo que el ensayo de Grassman, que había sido premiado en 1846, tenía “(...) buen material expresado de modo inadecuado”. Este informe de Kummer acabó con la esperanza de Grassmann de llegar a obtener una plaza de profesor universitario. Este episodio

confirma además el hecho de que las autoridades con las que Grassmann contactó nunca reconocieron la importancia real de sus ideas.

Durante los disturbios políticos que se desarrollan en Alemania en 1848-49, Hermann y Robert Grassmann editaron un periódico en Stettin para apoyar la unificación de Alemania en el marco de una monarquía constitucional. Después de escribir una serie de artículos sobre leyes constitucionales, Hermann, cada vez menos de acuerdo con la línea política del periódico, lo dejó.

Grassmann tuvo once hijos, de los que siete llegaron a adultos. Uno de sus hijos, Hermann Ernst Grassmann, llegó a profesor de matemáticas en la Universidad de Giessen.

Entre los muchos temas que abordó Grassmann está su ensayo sobre la teoría de las mareas. Lo elaboró en 1840, tomando como base la teoría de la Méchanique analytique de Lagrange y de la Méchanique céleste de Laplace, pero exponiendo esta teoría por métodos vectoriales, sobre los que trabajaba desde 1832. Este ensayo, publicado por primera en los Collected Works de 1894-1911, contiene el primer testimonio escrito de lo que hoy se conoce como Álgebra Lineal y la noción de espacio vectorial. Grassmann desarrolló estos métodos en Die Lineale Ausdehnungslehre, ein neuer Zweig der Mathematik y Die Ausdehnungslehre: Vollständig und in strenger Form bearbeitet.

En 1844, Grassmann publica su obra maestra, Die Lineale Ausdehnungslehre, ein neuer Zweig der Mathematik, más conocido como Ausdehnungslehre, que se puede traducir como "teoría de la extensión" o"teoría de las magnitudes extensiva". Después de proponer en Ausdehnungslehre nuevas bases para todas las matemáticas, el trabajo empieza con definiciones de naturaleza más bien filosófica. Grassmann demostró además que si la geometría se hubiese expresado en forma algebraica como él proponía, el número tres no hubiese desempeñado el papel privilegiado que tiene como número que expresa la dimensiones espaciales; de hecho, el número de posibles dimensiones de interés para la geometría es ilimitado.

Fearnley-Sander (1979) describe la creación del Álgebra Lineal de Grassmann de este modo:

"La definición de espacio lineal (...) se reconoce abiertamente alrededor de 1920, cuando Hermann Weyl y otros publicaron la definición formal. En realidad dicha definición había sido formulada unos treinta años antes por Peano, que había estudiado a fondo el trabajo matemático de Grassmann. Grassmann no formuló una definición formal - no existía entonces un lenguaje adecuado - pero no hay duda de que tuviera claro el concepto"

"Empezando con una colección de 'unidades' $e_1, e_2, e_3, \ldots$, él, efectivamente, definió el espacio lineal libre que generaban; en otros términos, considera la combinación lineal formal $a_1e_1 + a_2e_2 + a_3e_3 + \cdots$ donde a_j son números reales, define la suma y la multiplicación por números reales [en el modo que se usa actualmente] y demuestra formalmente las propiedades de espacio lineal de estas operaciones. (...) Desarrolla la teoría del la independencia lineal de modo extraordinariamente similar a la presentación que podemos encontrar en los textos modernos de álgebra lineal. Define la noción de subespacio, independencia, longitud, desdoblamiento, dimensión, suma e intersección de subespacios, y proyección de elementos en los subespacios"

"...pocos estuvieron tan cerca como Hermann Grassmann de crear, trabajando en

solitario, una nueva disciplina"

Desarrollando una idea de su padre, Grassmann definió también en Ausdehnungslehre el producto exterior, llamado también "producto combinatorio" (en alemán: äußeres Produkt o kombinatorisches Produkt), la operación clave en el álgebra que hoy se conoce como álgebra exterior. (Conviene no olvidar que en los tiempos de Grassmann la única teoría axiomática disponible era la Geometría euclidiana, y que la noción general de álgebra abstracta aún no había sido definida.) En 1878, William Kingdon Clifford unió el álgebra exterior con los cuaterniones de William Rowan Hamilton, sustituyendo la regla de Grassmann $e_p e_p = 0$ por $e_p e_p = 1$.

El Ausdehnungslehre fue un texto revolucionario, muy avanzado en su época como para poder ser apreciado. Grassmann lo expuso como tesis doctoral, pero Möbius no se consideró capaz de valoralrlo y se lo remitió a Ernst Kummer, que lo rechazó sin haber llevado a cabo una lectura atenta. En los 10 años siguientes, Grassmann escribió una serie de trabajos aplicando su teoría de la extensión, incluyendo una Neue Theorie der Elektrodynamik de 1845, y diversos trabajos sobre curvas y superficies alegbraicas, con la esperanza de que estas aplicaciones movieran a los demás a tomar más en serio su teoría.

En 1846, Möbius invitó a Grassmann a una competición para resolver un problema originalmente planteado por Leibniz: idear un cálculo geométrico privado de coordenadas y propiedades métricas. Geometrische Analyse geknüpft an die von Leibniz erfundene geometrische Charakteristik de Grassmann, fue la idea ganadora. Hay que decir sin embargo que el resultado de Grassmann fue el único presentado. De cualquier manera, Möbius, que era uno de los miembros del jurado, criticó el modo en que Grassmann introdujo la noción abstracta sin proporcionar al lector intuición alguna sobre la validez de estas nociones.

En 1853, Grassmann publicó una teoría sobre el modo en que se mezclan los colores; ésta y sus tres leyes de los colores siguen enseñándose hoy en día. El trabajo de Grassmann entraba en contradicción con el de Helmholtz. Grassmann escribió también sobre cristalografía, electromagnetismo, y mecánica.

En 1861 Grassmann expuso la primera formulación axiomática de la Aritmética, usando ampliamente el principio de inducción. Giuseppe Peano y sus seguidores citaron ampliamente este trabajo a partir de 1890.

En 1862, Grassman, tratando de conseguir el reconocimiento de su teoría de la extensión, publicó la segunda edición de la "Ausdehnungslehre", ampliamente reescrita, y con la exposición definitiva de su álgebra lineal. El resultado, Die Ausdehnungslehre: Vollständig und in strenger Form bearbeitet, que se conoce como"Enseñanza de la dilatació" no fue mejor considerada que la edición original, a pesar de que el método de exposición de esta segunda versión de "Ausdehnungslehre" se anticipara a lo que han sido los libros de texto en el Siglo XX. En esta obra desarrolla un cálculo operatorio directo para las diversas magnitudes geométricas, que se conoce como números de Grassmann.

El único matemático que valoró en su justa medida las ideas Grassmann en vida de éste fue Hermann Hankel. En su obra Theorie der complexen Zahlensysteme (1867) ayudó a que se conocieran mejor las ideas de Grassmann. Este trabajo:

"... desarrolló una parte del álgebra de Hermann Grassmann y de los cuaterniones

de Hamilton. Hankel fue el primero que reconoció la importancia de los textos de Grassmann, que habían sido menospreciados durante mucho tiempo..” (introducción de Hankel en el Dictionary of Scientific Biography. New York: 1970-1990)

Se tardó en adoptar los métodos matemáticos de Grassmann pero influyeron directamente en Felix Klein y Élie Cartan. La primera monografía de A. N. Whitehead, Universal Algebra de 1898, incluía la primera exposición sistemática en inglés de la teoría de la extensión y del álgebra exterior. La teoría de la extensión se aplicó al estudio de las formas diferenciales y en las aplicaciones de dichas formas al Análisis y a la Geometría. La Geometría Diferencial usa el Álgebra Exterior.

Contrariado por su incapacidad de conseguir que se le reconociera como matemático, Grassmann se dedicó a la lingüística histórica. Escribió libros de gramática alemana, elaboró catálogos de canciones populares y aprendió sánscrito. Su diccionario y su traducción del Ayurveda (que se sigue publicando hoy en día) tuvieron un gran reconocimiento entre los filólogos. Formuló una ley relativa a los fonemas de las lenguas indoeuropeas, que se conoce hoy como ley de Grassmann en su honor. También elaboró un Diccionario sobre el Rig-veda (1873-1875). Sus cualidades filológicas fueron reconocidas en vida; fue admitido en la American Oriental Society y en 1876 fue nombrado doctor honoris causa por la Universidad de Tubinga.

(Artículo tomado de wikipedia).

4.8. Problemas

1. Sea $(G,+)$ un grupo abeliano y consideremos en G su estructura natural de $\mathbb{Z}$-módulo. Prueba que lo subgrupos de G coinciden con los $\mathbb{Z}$-submódulos de G. Sea $(G',+)$ otro grupo abeliano y consideremos también su estructura natural de $\mathbb{Z}$-módulo. Prueba que los morfismos de grupos de G en G' coinciden con los morfismos de $\mathbb{Z}$-módulos de G en G'.

2. Sea E un K-espacio vectorial y $T: E \to E$ una aplicación K-lineal. Consideremos en E su estructura natural de $K[x]$-módulo. Prueba que los subespacios vectoriales de E, estables por el endomorfismo T, coinciden con los $K[x]$-submódulos de E. Sea $\phi: E \to E'$ un isomorfismo de $K[x]$-módulos. Prueba que la matriz de T en una base $\{e_i\}_{i\in I}$ de E es igual a la matriz del endomorfismo lineal $x\cdot: E' \to E'$ en la base $\{\phi(e_i)\}_{i\in I}$.

3. Sea $f: A \to B$ un morfismo de anillos y M un B-módulo. Dota a M de estructura de A-módulo.

4. Sea $I \subseteq A$ un ideal y M un A-módulo. Denotemos $I\cdot M$ como el mínimo submódulo de M que contiene a $\{i\cdot m\}_{i\in I, m\in M}$. Prueba que

$$I\cdot M = \{i_1\cdot m_1 + \cdots + i_n\cdot m_n \in M, \text{ variando los } i_j \in I, m_j \in M, \text{ y } n \in \mathbb{N}\}$$

5. Sea $I \subset A$ un ideal y M, M' A-módulos. Prueba que

$$I\cdot(M\oplus M') = I\cdot M \oplus I\cdot M'.$$

6. Sea $\pi\colon M \to N$ un morfismo de módulos. Si existe un morfismo de módulos $s\colon N \to M$ tal que $\pi \circ s = \mathrm{Id}$ prueba que $M \simeq \mathrm{Ker}\,\pi \oplus N$.

7. Sean $N_1, N_2 \subseteq M$ dos A-submódulos y sea $\bar{N}_2 = \{\bar{n}_2 \in M/N_1 : n_2 \in N_2\}$. Prueba que $(M/N_1)/\bar{N}_2 \simeq M/(N_1 + N_2)$.

8. Sean $N_1, N_2 \subseteq M$ dos A-submódulos. Prueba que $(N_1 + N_2)/N_1 = N_2/(N_1 \cap N_2)$.

9. Sea A un anillo y sean $a, b \in A$ tales que $(a, b) = A$. Prueba que el morfismo $b\cdot\colon A/aA \to A/aA$, $\bar{c} \mapsto \overline{bc}$ es un isomorfismo.

10. Sea A un anillo y $a_1, a_2 \in A$ tales que $(a_1, a_2) = A$. Prueba que el morfismo de A-módulos

$$A/a_1A \oplus A/a_2A \xrightarrow{\phi} A/a_1a_2A,\ (\bar{b}_1, \bar{b}_2) \mapsto \overline{a_2b_1 + a_1b_2},$$

es un isomorfismo. En general, sean $a_1, \ldots, a_n \in A$ tales que $(a_i, a_j) = A$, para todo $i \neq j$. Prueba que el morfismo de A-módulos

$$A/a_1A \oplus \cdots \oplus A/a_nA \xrightarrow{\phi} A/a_1 \cdots a_nA,\ (\bar{b}_1, \ldots, \bar{b}_n) \mapsto \overline{\sum_{i=1}^{n} c_i b_i},$$

donde $c_i := \prod_{j \neq i} a_j$, es un isomorfismo.

11. La ley del enfriamiento de Newton establece que la tasa de pérdida de calor de un cuerpo es proporcional a la diferencia de temperatura entre el cuerpo y sus alrededores. Un sólido a 20º centígrados es introducido en un lago de agua a temperatura de 5º. Si tarda dos minutos en enfriarse diez grados ¿Cuántos minutos tardará en enfriarse 14 grados?

12. Sea F el espacio vectorial formado por las funciones de $\mathbb{R}$ a $\mathbb{C}$ infinitamente derivables y $D\colon F \to F$ el operador derivada. Prueba que

    a) $D(e^f \cdot g) = e^f \cdot (D + f' \cdot \mathrm{Id})(g)$.

    b) Calcula las soluciones de la ecuación diferencial lineal $y' + fy = g$.

13. Sea F el espacio vectorial formado por las funciones de $\mathbb{R}^+$ a $\mathbb{C}$ infinitamente derivables y $\Theta\colon F \to F$ el operador $\mathbb{C}$-lineal definido por $\Theta(f) := xf'$.

    a) Prueba que $\mathrm{Ker}(\Theta - \alpha)^r = x^\alpha \cdot \{\sum_{i=0}^{r-1} \lambda_i (\ln x)^i : \ \forall\, \lambda_i \in \mathbb{C}\}$.

    b) Resuelve la ecuación de Euler-Cauchy

$$x^2y'' + bxy' + cy = 0,$$

    para $b, c \in \mathbb{C}$ y $x > 0$.

14. Resuelve la ecuación diferencial del movimiento armónico amortiguado

$$f'' + af' + bf = 0,\ (\text{con } a^2 - 4b < 0 \text{ y } a > 0).$$

15. Resuelve la ecuación diferencial del movimiento armónico forzado

$$f'' + af' + bf = c\cos(wx), \ \ (\text{con } a^2 - 4b < 0 \text{ y } a > 0).$$

16. Calcula $\int x^2 \cos^2 x \, dx$.

17. Sea $p(x) \in \mathbb{C}[x]$ y supongamos que $p(\alpha) \neq 0$, para cierto $\alpha \in \mathbb{C}$, sea $q_s(x) \in \mathbb{C}[x]$ un polinomio de grado s Prueba que una solución particular de la ecuación diferencial $(p(D)\cdot(D-\alpha)^m)(f) = e^{\alpha x}\cdot q_s(x)$ es de la forma $e^{\alpha x}\cdot x^m \cdot t(x)$ para cierto polinomio $t(x)$ de grado menor que s.

18. Prueba que $\Delta\binom{n}{i} = \binom{n}{i-1}$. Prueba que $\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{r}\}$ es una base de $\operatorname{Ker}\Delta^{r+1}$. Sea $p(n) = \sum_{i=0}^{r} \lambda_i \binom{n}{i}$, prueba que λ_i es el término 0 de la sucesión $\Delta^i(p(n))$, es decir,

$$\lambda_i = \sum_{j=0}^{i} \binom{i}{j} \cdot (-1)^j p(i-j).$$

Calcula $\sum_{i=0}^{n} i^2$.

19. Calcula cuántos números de longitud n se pueden escribir con ceros y unos, de modo que nunca aparezcan dos ceros seguidos (ejemplo: los números de longitud tres cumpliendo lo dicho son $010, 011, 101, 110, 111$, que son cinco distintos).

20. Resuelve la ecuación $a_{n+2} + 2a_{n+1} - 8a_n = 2^n$.

21. Calcula $\sum_{i=0}^{n} g^i$.

22. Un préstamo de $K = 10^5$ euros se quiere devolver durante $N = 20$ años, pagando cada año n una anualidad d_n de modo que $d_n = d_{n-1} + 10^3$. Se suponen que nos prestan el dinero a un tipo de interés anual del $I = 5\,\%$. Determinar d_1.

23. Sea $p(x) \in \mathbb{R}[x]$ un polinomio mónico de grado n. Sean $s_1(x), \ldots, s_n(x)$ soluciones, linealmente independientes, de la ecuación diferencial $p(D)y = 0$. Prueba que si las funciones $c_1(x), \ldots, c_n(x)$ cumplen las ecuaciones

$$\begin{array}{rcl} c_1(x)'s_1(x) + \ldots + c_n(x)'s_n(x) & = & 0 \\ \ldots & = & 0 \\ c_1(x)'s_1(x)^{n-2)} + \ldots + c_n(x)'s_n(x)^{n-2)} & = & 0 \\ c_1(x)'s_1(x)^{n-1)} + \ldots + c_n(x)'s_n(x)^{n-1)} & = & f(x) \end{array}$$

entonces $c_1(x)s_1(x) + \ldots + c_n(x)s_n(x)$ es una solución particular de $p(D)y = f(x)$.

24. Sea $p(x) \in \mathbb{R}[x]$ un polinomio mónico de grado r. Sean $s_1(n), \ldots, s_r(n)$ soluciones, linealmente independientes, de la ecuación en diferencias $p(\nabla)y = 0$. Prueba que si las sucesiones $c_1(n), \ldots, c_r(n)$ cumplen las ecuaciones

$$\begin{array}{rcl} \Delta(c_1)\nabla(s_1) + \ldots + \Delta(c_r)\nabla(s_r) & = & 0 \\ \ldots & = & 0 \\ \Delta(c_1)\nabla^{r-1}(s_1) + \ldots + \Delta(c_r)\nabla^{r-1}(s_r) & = & 0 \\ \Delta(c_1)\nabla^{r}(s_1) + \ldots + \Delta(c_r)\nabla^{r}(s_r) & = & f \end{array}$$

entonces $c_1 s_1 + \ldots + c_r s_r$ es una solución particular de $p(\nabla)y = f$.

25. Dado un morfismo de anillos $f: A \to B$ diremos que B es una A-álgebra y será usual que denotemos $f(a) = a$. Un morfismo de A-álgebras $g: B \to C$ es un morfismo de anillos tal que $g(a) = a$, para todo $a \in A$.

    a) Sea $\mathbb{R} \to K$ una extensión de cuerpos tal que $\dim_{\mathbb{R}} K < \infty$. Prueba que K es $\mathbb{R}$ o es isomorfo como $\mathbb{R}$-álgebra a $\mathbb{C}$.

    b) Sea $\mathbb{R} \to D$ una extensión de cuerpos tal que $\dim_{\mathbb{R}} D < \infty$. Pero supongamos que D no es conmutativo (si bien, $\lambda \cdot d = d \cdot \lambda$, para todo $\lambda \in \mathbb{R}$ y $d \in D$). Prueba que D es una $\mathbb{R}$-álgebra isomorfa a los cuaterniones de Hamilton $\mathbb{H} := \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k$ (donde $i^2 = j^2 = k^2 = ijk = -1$).

Capítulo 5

Módulos sobre dominios de ideales principales

5.1. Introducción

En este capítulo clasificamos los A-módulos finito generados, cuando A es un anillo euclídeo.

En particular clasificamos los grupos abelianos finito generados. Recordemos que los grupos abelianos son justamente los $\mathbb{Z}$-módulos. Veremos que todo grupo abeliano finito generado G es una suma directa finita de grupos cíclicos, es decir,

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \overset{r}{\cdots} \oplus \mathbb{Z}/n_r\mathbb{Z} \qquad (*)$$

Recordemos que si $n = p_1^{m_1} \cdots p_r^{m_r}$ es la descomposición de n en producto de potencias de primos, el teorema chino de los restos nos dice que $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{m_r}\mathbb{Z}$. Por tanto, en la descomposición $(*)$ podemos suponer que los n_i son potencias de primos (o son nulos). En esta situación, demostraremos que los enteros n_i clasifican G.

Clasificaremos también los endomorfismos de un espacio vectorial de dimensión finita. Recordemos que dar un endomorfismo de un k-espacio vectorial equivale a dotar al espacio vectorial de estructura de $k[x]$-módulo: dado un espacio vectorial E y un endomorfismo $T\colon E \to E$, definimos $x \cdot e = T(e)$, para todo $e \in E$, y en general $p(x) \cdot e = p(T)(e)$. Demostramos que existen unos polinomio mónicos irreducibles $p_1(x), \cdots, p_r(x)$ únicos, y un conjunto de números naturales n_{ij} únicos de modo que

$$E \simeq (k[x]/(p_1(x)^{n_{11}}) \oplus \cdots \oplus k[x]/(p_1(x)^{n_{1s_1}})) \oplus \cdots \oplus (k[x]/(p_r(x)^{n_{r1}}) \oplus \cdots \oplus k[x]/(p_r(x)^{n_{rsr}})).$$

como $k[x]$-módulos. Este isomorfismo nos permitirá, cuando $k = \mathbb{C}$, definir las bases de Jordan y expresar la matriz de T en una base de Jordan.

Aplicamos estos teoremas para resolver los sistemas de ecuaciones diofánticas y los sistemas de ecuaciones diferenciales lineales con coeficientes constantes.

Por último, probaremos que si A es un dominio de ideales principales y M es un A-módulo finito generado entonces existen, elementos irreducibles $p_i \in A$ (únicos salvo multiplicación por invertibles) y $n_{ij} > 0$, $n \in \mathbb{N}$ únicos de modo que

$$M \simeq A^n \oplus (A/(p_1^{n_{11}}) \oplus \cdots \oplus A/(p_1^{n_{1s_1}})) \oplus \cdots \oplus (A/(p_r^{n_{r1}}) \oplus \cdots \oplus A/(p_r^{n_{rsr}})).$$

5.2. Presentación de un módulo por módulos libres

Sea M un A-módulo cualquiera. Por desgracia, no podemos afirmar que sea libre. Solo podemos afirmar la existencia de sistemas de generadores $\{m_i\}_{i\in I}$, luego la existencia de epimorfismos $A^{(I)} \to M$, $(a_i)_{i\in I} \mapsto \sum_i a_i m_i$.

Consideremos un epimorfismo $\pi\colon A^{(I)} \to M$. Igualmente, podemos definir un epimorfismo $\pi'\colon A^{(J)} \to \operatorname{Ker}\pi$. Componiendo este último morfismo con la inclusión natural $\operatorname{Ker}\pi \overset{i}{\hookrightarrow} A^{(I)}$, tenemos un morfismo natural $f = i\circ\pi'\colon A^{(J)} \to A^{(I)}$. Consideremos la sucesión de morfismos

$$A^{(J)} \overset{f}{\to} A^{(I)} \overset{\pi}{\to} M.$$

En conclusión, $\operatorname{Im} f = \operatorname{Ker}\pi$ y $M \simeq A^{(I)}/\operatorname{Ker}\pi$. Luego,

$$\boxed{M \simeq A^{(I)}/\operatorname{Im} f}$$

Por tanto, el estudio de M se reduce al estudio de f, que es una aplicación A-lineal entre módulos libres. Si M es un A-módulo finito generado y A un dominio de de ideales principales demostremos que existen de conjuntos I y J finitos de modo que f es una aplicación A-lineal entre A-módulos libres finito generados.

1. Lema: *Sea M un A-módulo y $N \subseteq M$ un submódulo. Si N y M/N son A-módulos finito generados, entonces M es un A-módulo finito generado.*

Demostración. Escribamos, $N = \langle n_1,\dots,n_r\rangle$ y $M/N = \langle \bar{n}_{r+1},\dots,\bar{n}_s\rangle$. Veamos que $M = \langle n_1,\dots,n_s\rangle$: Dado $m \in M$, tenemos que $\bar{m} = \sum_{i=r+1}^{s} a_i\cdot\bar{n}_i$, para ciertos $a_i \in A$. Luego, $\bar{m} - \sum_{i=r+1}^{s} a_i\cdot\bar{n}_i = 0$ y $m - \sum_{i=r+1}^{s} a_i\cdot n_i \in N$. Por tanto, $m - \sum_{i=r+1}^{s} a_i n_i = \sum_{j=1}^{r} a_j n_j$ para ciertos $a_j \in A$, y por tanto

$$m = \sum_{k=1}^{s} a_k n_k.$$

□

2. Definición: Un anillo A se dice que es noetheriano si todos sus ideales son finito generados.

Los anillos de ideales principales son evidentemente anillos noetherianos. Si A es un anillo noetheriano e $I \subset A$ es un ideal entonces A/I es un anillo noetheriano. El teorema de la base de Hilbert afirma que si A es noetheriano entonces $A[x_1,\dots,x_n]$ es noetheriano.

3. Proposición: *Sea A un anillo noetheriano y M un A-módulo finito generado. Se cumple que todo submódulo $N \subseteq M$ es finito generado.*

Demostración. Supongamos $M = \langle m\rangle$. Consideremos el epimorfismo

$$\pi\colon A \to M, a \mapsto a\cdot m.$$

$\pi^{-1}(N)$ es un submódulo de A, luego es finito generado. Entonces, $N = \pi(\pi^{-1}(N))$ es finito generado.

$M = \langle m_1, \dots, m_r \rangle$ es finito generado. Demostremos la proposición por inducción sobre r. Si $r = 1$, la acabamos de demostrar. Supongamos que la proposición es cierta para $1, \dots, r-1$. Sea $\pi : M \to M/\langle m_r \rangle$ el morfismo de paso al cociente. $\pi(N)$ es un submódulo de $M/\langle m_r \rangle = \langle \bar{m}_1, \dots, \bar{m}_{r-1} \rangle$, luego por hipótesis de inducción $\pi(N)$ es finito generado. Consideremos el epimorfismo

$$\pi_{|N} : N \to \pi(N),\ n \mapsto \pi(n).$$

Obviamente,

$$\operatorname{Ker} \pi_{|N} = \operatorname{Ker} \pi \cap N \subseteq \operatorname{Ker} \pi = \langle m_r \rangle$$

Por tanto, $\operatorname{Ker} \pi_{|N}$ es finito generado. $N/\operatorname{Ker} \pi_{|N} \simeq \pi(N)$ es finito generado. Por el lema anterior N es finito generado.

□

4. Teorema: *Sea A un anillo noetheriano y M un A-módulo finito generado. Existe un morfismo de A-módulos $f : A^r \to A^s$ (con $r, s \in \mathbb{N}$) de modo que $A^s/\operatorname{Im} f \simeq M$, es decir, "existe una presentación de M por módulos libres finito generados".*

Demostración. Escribamos $M = \langle m_1, \dots, m_s \rangle$. Consideremos el epimorfismo de A-módulos $\pi : A^s \to M$, $(a_i) \mapsto \sum_i a_i \cdot m_i$. $\operatorname{Ker} \pi$ es un submódulo de A^s, luego es finito generado. Escribamos $\operatorname{Ker} \pi = \langle n_1, \dots, n_r \rangle$ y consideremos el epimorfismo $g : A^r \to \operatorname{Ker} \pi$, $(a_i) \mapsto \sum_i a_i n_i$ y sea $f : A^r \to A^s$ la composición de los morfismos $A^r \xrightarrow{g} \operatorname{Ker} \pi \hookrightarrow A^s$. Tenemos que $\operatorname{Im} f = \operatorname{Im} g = \operatorname{Ker} \pi$. Por tanto, $A^s/\operatorname{Im} f = A^s/\operatorname{Ker} \pi \simeq M$. □

Cuando A sea un anillo euclídeo, veremos cómo puede calcularse f y cómo encontrar bases donde f "diagonalice", y con ello clasificaremos los A-módulos finito generados.

5.3. Transformaciones elementales

Sea $\delta_{sr} \in M_m(A)$ una matriz cuyos coeficientes son todos nulos salvo el coeficiente sr que es 1.

Sean L y L' dos módulos libres de bases $B = \{u_1, \dots, u_m\}$ y $B' = \{u'_1, \dots, u'_n\}$, respectivamente. Sea $\phi : L \to L'$ una aplicación A-lineal de matriz en dichas bases (a_{ij}). Sea $\tilde{B} = \{u_1, \dots, u_r \overset{r}{+} a u_s, \dots, u_m\}$, que es otra base de L ($r \neq s$). La matriz de ϕ en las bases $\tilde{B}$ y B' es

$$(a'_{ij}) = (a_{ij}) \cdot (\mathrm{Id} + a \cdot \delta_{sr}),$$

que es igual a la matriz (a_{ij}) salvo que la columna r de (a'_{ij}) es igual a la columna r de (a_{ij}) más a-veces la columna s de (a_{ij}).

Observemos que $(\mathrm{Id} + a \cdot \delta_{sr})^{-1} = \mathrm{Id} - a \cdot \delta_{sr}$. Si $X_{rs} := (\mathrm{Id} + \delta_{sr})(\mathrm{Id} - \delta_{rs})(\mathrm{Id} + \delta_{sr})$, entonces $(a_{ij}) \cdot X_{sr}$ es igual a la matriz (a_{ij}) salvo que su columna r es la columna s de (a_{ij}) y su columna s es menos la columna r de (a_{ij}) .

Sea $\tilde{B}' = \{u'_1, \dots, u'_s \overset{s}{-} a u'_r, \dots, u'_n\}$, que es otra base de L'. La matriz de ϕ en las bases B y $\tilde{B}'$ es

$$(a'_{ij}) = (\mathrm{Id} + a \cdot \delta_{rs}) \cdot (a_{ij}),$$

que se obtiene cambiando la fila r, F_r, de la matriz (a_{ij}) por la fila $F_r + aF_s$.

Este tipo de transformaciones lineales $\mathrm{Id} + a \cdot \delta_{sr}$ $(r \neq s)$ las denominaremos transformaciones elementales especiales. Diremos que $\mathrm{Id} + a \cdot \delta_{rr}$ (con $1+a$ invertible) es una transformación elemental homotética.

1. Definición: Si A es un anillo y $\delta : A\setminus\{0\} \to \mathbb{N}$ es una aplicación que cumple que para cada $a, b \in A$ no nulos existen c, r tales que $a = bc + r$, con $r = 0$ ó $\delta(r) < \delta(b)$, diremos que (A, δ) es casieuclídeo.

Los dominios euclídeos son casieuclídeos.

Si A es un anillo $(p) \subset A$ es un ideal maximal, entonces $A/p^n A$ es casieuclídeo: Si a no es divisible por p, entonces $(a, p) = A$, luego $(\bar{a}) = A/p^n A$ y $\bar{a}$ es invertible. Entonces, todo $\bar{b} \in A/p^n A$, es $\bar{b} = \bar{p}^r \cdot inv$, con $r \leq n$, con r único. Definimos $\delta : A/p^n A\setminus\{0\} \to \mathbb{N}$, $\delta(\bar{b}) := r$, si $\bar{b} = p^r \cdot inv$ (y $r \leq n$). Es fácil es probar que $(A/p^n A, \delta)$ es casieuclídeo.

Los anillos casieuclídeos son anillos de ideales principales, porque todo ideal I no nulo está generado por un elemento no nulo $i \in I$, tal que $\delta(i)$ sea mínimo.

2. Proposición: *Sea (A, δ) un anillo casieuclídeo. Sea $\phi : L \to L'$ un morfismo de A-módulos, entre A-módulos libres finito generados. Existen bases $\{e_1, \ldots, e_m\}$ en L y $\{e'_1, \ldots, e'_n\}$ en L', de modo que $\phi(e_i) = \lambda_i e'_i$, para ciertos $\lambda_i \in A$, si $i \leq n$, y $\phi(e_i) = 0$ si $i > n$.*

Demostración. Vamos a probar que mediante transformaciones elementales especiales la matriz (a_{ij}) asociada a ϕ en unas bases, se transforma en una matriz "diagonal" (es decir, una matriz (c_{ij}) con $c_{ij} = 0$ para todo $i \neq j$).

Probemos que mediante transformaciones elementales obtenemos una matriz de la forma

$$\begin{pmatrix} c_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}.$$

Procedemos por inducción sobre $\delta(a_{11})$ (sigamos la convención $\delta(0) = +\infty$). Si $\delta(a_{11}) = 0$, entonces a_{11} es invertible y es fácil mediante transformaciones elementales conseguir que $a_{1j} = a_{j'1} = 0$, para todo $j, j' \neq 1$. Y hemos concluido. Supongamos que la afirmación hecha es cierta si $\delta(a_{11}) < n$. Sea $\delta(a_{11}) = n$. Si algún a_{i1} cumple $\delta(a_{i1}) < n$, permutando las filas 1 e i, obtenemos una nueva matriz cuyo coeficiente 11, a'_{11}, cumple que $\delta(a'_{11}) < n$ y concluimos por hipótesis de inducción. Podemos suponer que $\delta(a_{i1}) \geq \delta(a_{11})$ para todo i, e igualmente que $\delta(a_{1j}) \geq \delta(a_{11})$, para todo j. Si algún $a_{i1} \neq 0$ (con $i \neq 1$), entonces $a_{i1} = a_{11} \cdot c + a'_{i1}$, con $\delta(a'_{i1}) < \delta(a_{11}) = n$ ó $a'_{i1} = 0$. Cambiando la fila i, F_i, por $F_i - cF_1$, obtenemos una nueva matriz con la misma primera fila y primera columna, salvo que el coeficiente $i1$, que es a'_{i1} cumple que $a'_{i1} = 0$ ó $\delta(a'_{i1}) < n$ (en este último caso después de permutar la fila i con la primera podremos suponer que el coeficiente $\delta(a_{11}) < n$ y terminaríamos por inducción). Igual hacemos si algún coeficiente $a_{1i} \neq 0$ (con $i \neq 1$). En conclusión, por transformaciones elementales obtenemos una matriz de la forma

$$\begin{pmatrix} c_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}.$$

Procediendo del mismo modo reiteradamente, con la matriz (b_{ij}), "diagonalizaremos" ϕ.

□

5.4. Sistemas de ecuaciones lineales diofánticas

Resolvamos los sistemas de ecuaciones lineales diofánticos. Consideremos el sistema de ecuaciones

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

con $a_{ij}, b_k \in \mathbb{Z}$ para todo $i, j.k$, que escribimos abreviadamente $A \cdot x = b$. Mediante transformaciones elementales (en columnas y filas) diagonalizamos la matriz A. Es decir, sabemos calcular matrices cuadradas invertibles F y C de modo que $F \cdot A \cdot C = D$, donde $D = (d_{ij})$, con $d_{ij} = 0$ para todo $i \neq j$. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{A} & \mathbb{Z}^m \\ {\scriptstyle C}\uparrow & & \downarrow{\scriptstyle F} \\ \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m \end{array} \qquad \begin{array}{ccc} x & \xmapsto{A} & b \\ {\scriptstyle C}\uparrow & & \downarrow{\scriptstyle F} \\ x' & \xmapsto{D} & F \cdot b \end{array}$$

(con $x' := C^{-1}x$). Entonces, $D \cdot x' = F \cdot b$. Si calculamos x' (que es fácil), tenemos que $x = C \cdot x'$.

Escribamos los cálculos. Mediante transformaciones elementales de las n-primeras columnas y m-primeras filas de la matriz $\left(\begin{array}{c|c} A & b \\ \hline \mathrm{Id} & 0 \end{array}\right)$

$$\left(\begin{array}{c|c} F & 0 \\ \hline 0 & \mathrm{Id} \end{array}\right) \cdot \left(\begin{array}{c|c} A & b \\ \hline \mathrm{Id} & 0 \end{array}\right) \cdot \left(\begin{array}{c|c} C & 0 \\ \hline 0 & \mathrm{Id} \end{array}\right)$$

obtenemos la matriz

$$\left(\begin{array}{c|c} F \cdot A \cdot C & F \cdot b \\ \hline C & 0 \end{array}\right) = \left(\begin{array}{c|c} D & F \cdot b \\ \hline C & 0 \end{array}\right).$$

Finalmente, x' cumple $D \cdot x' = F \cdot b$ si y solo si $x = C \cdot x'$ cumple $A \cdot x = b$.

1. Ejemplo: Resolvamos la ecuación diofántica $2 \cdot x + 3 \cdot y = 5$:

$$\left(\begin{array}{cc|c} 2 & 3 & 5 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right) \overset{C_2 - C_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 2 & 1 & 5 \\ \hline 1 & -1 & 0 \\ 0 & 1 & 0 \end{array}\right) \overset{C_1 - 2C_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 0 & 1 & 5 \\ \hline 3 & -1 & 0 \\ -2 & 1 & 0 \end{array}\right).$$

Tenemos que $x' = x'$, $y' = 5$ son las soluciones del sistema $0 \cdot x' + 1 \cdot y' = 5$. Por tanto,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x' \\ 5 \end{pmatrix} = \begin{pmatrix} 3x' - 5 \\ -2x' + 5 \end{pmatrix}$$

son las soluciones de nuestra ecuación diofántica.

Con menos cálculos: Tenemos que $\binom{x}{y} = C \cdot \binom{x'}{5} = (\mathrm{Id} - \delta_{12}) \circ (\mathrm{Id} - 2\delta_{21}) \circ \binom{x'}{5}$. Luego,

$$\begin{pmatrix} x' \\ 5 \end{pmatrix} \overset{F_2 - 2F_1}{\rightsquigarrow} \begin{pmatrix} x' \\ 5 - 2x' \end{pmatrix} \overset{F_1 - F_2}{\rightsquigarrow} \begin{pmatrix} 3x' - 5 \\ 5 - 2x' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

2. Ejemplo: Resolvamos el sistema de ecuaciones diofánticas

$$\begin{aligned} 2x + 3y + z &= 6 \\ 4x + 2y + z &= 5 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 2 & 3 & 1 & 6 \\ 4 & 2 & 1 & 5 \end{array}\right) \overset{C_1 x C_3}{\rightsquigarrow} \left(\begin{array}{ccc|c} 1 & 3 & 2 & 6 \\ 1 & 2 & 4 & 5 \end{array}\right) \overset{F_2 - F_1}{\rightsquigarrow} \left(\begin{array}{ccc|c} 1 & 3 & 2 & 6 \\ 0 & -1 & 2 & -1 \end{array}\right) \overset{C_3 + 2C_2}{\rightsquigarrow} \left(\begin{array}{ccc|c} 1 & 3 & 8 & 6 \\ 0 & -1 & 0 & -1 \end{array}\right).$$

Las soluciones del sistema

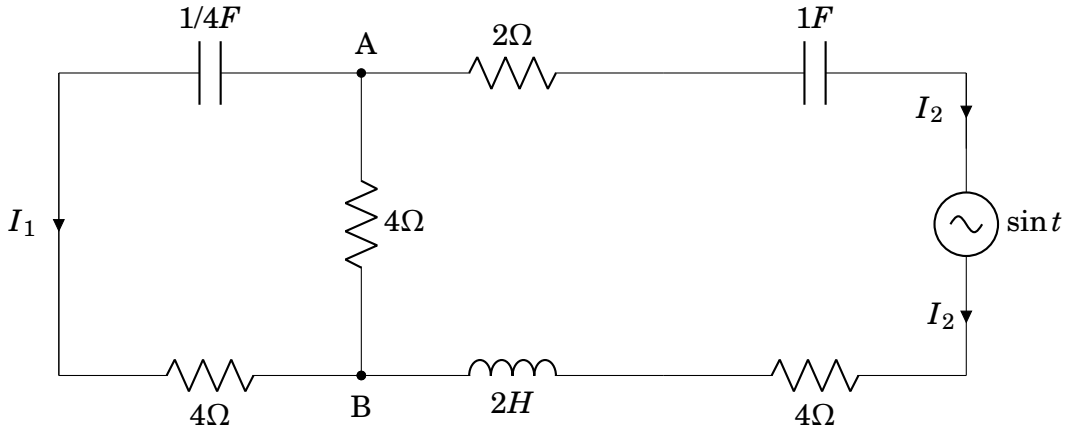
$$\begin{aligned} x' + 3y' + 8z' &= 6 \\ -y' &= -1 \end{aligned}$$

son $z' = z'$, $y' = 1$ y $x' = 3 - 8z'$. Luego las soluciones de nuestro sistema son

$$\begin{pmatrix} 3 - 8z' \\ 1 \\ z' \end{pmatrix} \overset{F_2 + 2F_3}{\rightsquigarrow} \begin{pmatrix} 3 - 8z' \\ 1 + 2z' \\ z' \end{pmatrix} \overset{F_1 x F_3}{\rightsquigarrow} \begin{pmatrix} z' \\ 1 + 2z' \\ 3 - 8z' \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Hemos resuelto sistemas de ecuaciones lineales con coeficientes enteros. De modo similar podemos resolver sistemas de ecuaciones lineales con coeficientes en un anillo euclídeo, por ejemplo, $\mathbb{C}[x]$.

3. Ejemplo: Calculemos las intensidades de corriente en los diferentes tramos del siguiente **circuito eléctrico.**



Las resistencias de R ohmios (Ω) producen una diferencial de potencial V entre sus extremos $V = I \cdot R$, las bobinas de inductancia L henrios (H) producen una diferencial de potencial V entre sus extremos $V = I' \cdot L$ y los condensadores de capacitancia C faradios (F) producen una diferencial de potencial V entre sus extremos que cumple $V' = I/C$. La suma de diferencia de potenciales en todo circuito cerrado, es nula. De B a A la corriente es de intensidad $I_1 + I_2$. Luego,

$$\begin{aligned} 4I_1' + 4(I_1' + I_2') + 4I_1 &= 0 \\ 4I_2' + 2I_2'' + 4(I_1' + I_2') + 2I_2' + I_2 &= \cos t \end{aligned}$$

Dividamos la primera ecuación por 4 y escribamos las ecuaciones matricialmente,

$$\begin{pmatrix} 2D+1 & D \\ 4D & 2D^2+10D+1 \end{pmatrix} \begin{pmatrix} I_1 \\ I_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \cos t \end{pmatrix}.$$

Resolvamos el sistema de ecuaciones mediante transformaciones elementales:

$$\left(\begin{array}{cc|c} 2D+1 & D & 0 \\ 4D & 2D^2+10D+1 & \cos t \end{array}\right) \overset{F_1 - \frac{1}{2}F_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & -D^2-4D-\frac{1}{2} & -\frac{1}{2}\cos t \\ 4D & 2D^2+10D+1 & \cos t \end{array}\right) \overset{F_2 - 4DF_1}{\rightsquigarrow}$$

$$\left(\begin{array}{cc|c} 1 & -D^2-4D-\frac{1}{2} & -\frac{1}{2}\cos t \\ 0 & 4D^3+18D^2+12D+1 & \cos t - 2\operatorname{sen} t \end{array}\right) \overset{C_2 + (D^2+4D+\frac{1}{2})C_1}{\rightsquigarrow}$$

$$\left(\begin{array}{cc|c} 1 & 0 & -\frac{1}{2}\cos t \\ 0 & 4D^3+18D^2+12D+1 & \cos t - 2\operatorname{sen} t \end{array}\right)$$

Tenemos que resolver el sistema de ecuaciones

$$\begin{aligned} J_1 &= -\tfrac{1}{2}\cos t \\ (4D^3+18D^2+12D+1)J_2 &= \cos t - 2\operatorname{sen} t \end{aligned}$$

Sus soluciones son

$$\begin{aligned} J_1 &= -\tfrac{\cos t}{2} \\ J_2 &= \tfrac{-\cos t}{353} + \tfrac{42\operatorname{sen} t}{353} + \lambda e^{-0'1t} + \mu e^{-0'7t} + \gamma e^{-3'7t} \end{aligned}$$

Luego,

$$\begin{pmatrix} J_1 \\ J_2 \end{pmatrix} = \begin{pmatrix} -\frac{\cos t}{2} \\ \frac{-\cos t}{353} + \frac{42\operatorname{sen} t}{353} + \lambda e^{-0'1t} + \mu e^{-0'7t} + \gamma e^{-3'7t} \end{pmatrix} \overset{F_1 + (D^2+4D+\frac{1}{2})F_2}{\rightsquigarrow}$$

$$\begin{pmatrix} \frac{-8\cos t - 17\operatorname{sen} t}{353} + 0'12\lambda e^{-0'1t} - 1'7\mu e^{-0'7t} - 0'58\gamma e^{-3'7t} \\ \frac{-\cos t + 42\operatorname{sen} t}{353} + \lambda e^{-0'1t} + \mu e^{-0'7t} + \gamma e^{-3'7t} \end{pmatrix} = \begin{pmatrix} I_1 \\ I_2 \end{pmatrix}.$$

Si $t >> 0$ entonces $(I_1, I_2) \simeq (\frac{-8\cos t - 17\operatorname{sen} t}{353}, \frac{-\cos t + 42\operatorname{sen} t}{353})$.

4. Ejemplo: Dividamos la población trabajadora en tres sectores: primario, secundario y terciario. Sea p_n la proporcion de trabajadores del sector primario después de n generaciones, sea s_n la proporción de trabajadores del sector secundario después de n generaciones y t_n la del terciario. Supongamos que la ocupación de los hijos depende de la ocupación de los padres y abuelos según el sistema de ecuaciones en diferencias finitas

$$\begin{pmatrix} p_{n+2} \\ s_{n+2} \\ t_{n+2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0'6 & 0'2 & 0'1 \\ 0'2 & 0'5 & 0'1 \\ 0'2 & 0'3 & 0'8 \end{pmatrix} \cdot \begin{pmatrix} p_{n+1} \\ s_{n+1} \\ t_{n+1} \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0'4 & 0'2 & 0'1 \\ 0'3 & 0'5 & 0'1 \\ 0'3 & 0'3 & 0'8 \end{pmatrix} \cdot \begin{pmatrix} p_n \\ s_n \\ t_n \end{pmatrix}$$

($p_n + s_n + t_n = 1$, para todo n). Resolvamos el sistema de ecuaciones y calculemos $\lim_{n\to\infty} p_n$.

Hagamos $t_n = 1 - p_n - s_n$, para todo n. Entonces, obtenemos

$$\begin{pmatrix} p_{n+2} \\ s_{n+2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0'5 & 0'1 \\ 0'1 & 0'4 \end{pmatrix} \cdot \begin{pmatrix} p_{n+1} \\ s_{n+1} \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0'3 & 0'1 \\ 0'2 & 0'4 \end{pmatrix} \cdot \begin{pmatrix} p_n \\ s_n \end{pmatrix} + \begin{pmatrix} 0'1 \\ 0'1 \end{pmatrix}.$$

Que escribimos

$$\begin{pmatrix} \nabla^2 - \frac{0'5}{2}\nabla - \frac{0'3}{2} & -\frac{0'1}{2}\nabla - \frac{0'1}{2} \\ -\frac{0'1}{2}\nabla - 0'1 & \nabla^2 - 0'2\nabla - 0'2 \end{pmatrix} \begin{pmatrix} p_n \\ s_n \end{pmatrix} = \begin{pmatrix} 0'1 \\ 0'1 \end{pmatrix}.$$

Que vamos a resolver por transformaciones elementales

$$\left(\begin{array}{cc|c} 20\nabla^2 - 5\nabla - 3 & -\nabla - 1 & 2 \\ -\nabla - 2 & 20\nabla^2 - 4\nabla - 4 & 2 \end{array}\right) \overset{F_1 + (20\nabla - 45)F_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 87 & 179 + 99\nabla - 980\nabla^2 + 400\nabla^3 & -48 \\ -\nabla - 2 & 20\nabla^2 - 4\nabla - 4 & 2 \end{array}\right)$$

$$\overset{F_2 + \frac{\nabla+2}{87}F_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 87 & 179 + 99\nabla - 980\nabla^2 + 400\nabla^3 & -48 \\ 0 & \frac{10 + 29\nabla - 121\nabla^2 - 180\nabla^3 + 400\nabla^4}{87} & \frac{10}{29} \end{array}\right) \overset{C_2 - \frac{179 + 99\nabla - 980\nabla^2 + 400\nabla^3}{87}C_1}{\rightsquigarrow}$$

$$\left(\begin{array}{cc|c} 87 & 0 & -48 \\ 0 & \frac{10 + 29\nabla - 121\nabla^2 - 180\nabla^3 + 400\nabla^4}{87} & \frac{10}{29} \end{array}\right)$$

Las soluciones de este último sistema

$$\begin{array}{rcl} 87 \cdot p'_n & = & -48 \\ \frac{10 + 29\nabla - 121\nabla^2 - 180\nabla^3 + 400\nabla^4}{87}(s'_n) & = & \frac{10}{29} \end{array}$$

son $p'_n = \frac{-16}{29}$, $s'_n = \frac{5}{23} + \lambda \cdot (-0'39)^n + \mu \cdot (-0'24)^n + \alpha \cdot (0'42)^n + \beta \cdot (0'65)^n$. Escribamos $P(\nabla) = \frac{179 + 99\nabla - 980\nabla^2 + 400\nabla^3}{87}$. Entonces,

$$\begin{pmatrix} p'_n \\ s'_n \end{pmatrix} \overset{F_1 - P(\nabla)F_2}{\rightsquigarrow} \begin{pmatrix} p'_n - P(\nabla)s'_n \\ s'_n \end{pmatrix} = \begin{pmatrix} p_n \\ s_n \end{pmatrix}.$$

$P(\nabla)(\gamma^n) = (P(\gamma) \cdot \gamma^n)$, por tanto,

$$\begin{array}{rcl} p_n & = & \frac{14}{69} + \lambda \cdot 0'32 \cdot (-0'39)^n - \mu \cdot 1'01 \cdot (-0'24)^n - \alpha \cdot 0'90 \cdot (0'42)^n + \beta \cdot 0'73 \cdot (0'65)^n \\ s_n & = & \frac{5}{23} + \lambda \cdot (-0'39)^n + \mu \cdot (-0'24)^n + \alpha \cdot (0'42)^n + \beta \cdot (0'65)^n \end{array}$$

Luego, $\lim_{n\to\infty}\begin{pmatrix}p_n\\ s_n\end{pmatrix}=\begin{pmatrix}\frac{14}{69}\\ \frac{5}{23}\end{pmatrix}$ y $\lim_{n\to\infty} t_n = 1-\frac{14}{69}-\frac{5}{23}=\frac{40}{69}$. Observemos, también, que el vector $w=\lim_{n\to\infty}(p_n,s_n,t_n)$ cumple que

$$w^t=\frac{1}{2}\begin{pmatrix}0'6 & 0'2 & 0'1\\ 0'2 & 0'5 & 0'1\\ 0'2 & 0'3 & 0'8\end{pmatrix}\cdot w^t+\frac{1}{2}\begin{pmatrix}0'4 & 0'2 & 0'1\\ 0'3 & 0'5 & 0'1\\ 0'3 & 0'3 & 0'8\end{pmatrix}\cdot w^t$$

es decir, es un autovector de autovalor 1 de $\frac{1}{2}\begin{pmatrix}0'6 & 0'2 & 0'1\\ 0'2 & 0'5 & 0'1\\ 0'2 & 0'3 & 0'8\end{pmatrix}+\frac{1}{2}\begin{pmatrix}0'4 & 0'2 & 0'1\\ 0'3 & 0'5 & 0'1\\ 0'3 & 0'3 & 0'8\end{pmatrix}$.

5.5. Clasificación de módulos sobre anillos euclídeos

1. Teorema: *Sea A un anillo casieuclídeo y M un A-módulo finito generado. Entonces, existen $a_1,\dots,a_n\in A$ de modo que*

$$M\simeq A/a_1A\oplus\cdots\oplus A/a_nA.$$

Demostración. Sea $L\xrightarrow{\phi}L'\xrightarrow{\pi}M$ una presentación de M por módulos libres finito generados. Sean $\{e_1,\dots,e_m\}$ y $\{e'_1,\dots,e'_n\}$ bases de L y L' de modo que $\phi(e_i)=\lambda_i e'_i$ si $1\le i\le n$ y $\phi(e_i)=0$ si $i>n$ (en el caso de que $m<n$, definimos $\lambda_i:=0$ para los $m<i\le n$). Entonces, $\operatorname{Im}\phi=\langle\lambda_1\cdot e'_1,\dots,\lambda_n\cdot e'_n\rangle$ y

$$M\simeq L'/\operatorname{Im}\phi=A\cdot e'_1\oplus\overset{n}{\cdots}\oplus A\cdot e'_n/(\lambda_1A\cdot e'_1\oplus\overset{n}{\cdots}\oplus\lambda_nA\cdot e'_n)\simeq A/\lambda_1A\oplus\overset{n}{\cdots}\oplus A/\lambda_nA.$$

□

Si $a\in A$ es nulo entonces $A/aA=A$. Si $a\in A$ es invertible entonces $A/aA=0$. Si $a\in A$ no es nulo ni invertible, entonces $a=p_1^{n_1}\cdots p_r^{n_r}$ con p_i irreducible, para todo i, y primo con p_j, para todo $j\neq i$. Además, por el teorema chino de los restos

$$A/aA\simeq A/p_1^{n_1}A\oplus\cdots\oplus A/p_r^{n_r}A.$$

Por tanto, tenemos demostrado el siguiente teorema.

2. Teorema de clasificación: *Sea A un anillo euclídeo y M un A-módulo finito generado. Entonces, existen elementos irreducibles $p_1,\dots,p_r\in A$ (con $(p_i)\neq(p_j)$ para todo $i\neq j$) y números naturales $n_{ij}\neq 0$ y n, de modo que*

$$M\simeq A^n\oplus(A/p_1^{n_{11}}A\oplus\cdots\oplus A/p_1^{n_{1s_1}}A)\oplus\cdots\oplus(A/p_r^{n_{r1}}A\oplus\cdots\oplus A/p_r^{n_{rs_r}}A).$$

5.5.1. Unicidad de los divisores elementales

Vamos a probar que n, los p_i (salvo multiplicación por invertibles) y los n_{ij} del teorema de clasificación son únicos (determinados por M).

3. Lema: *Sea A un anillo íntegro, $a \in A$ no nulo y $n > 0$. Consideremos el morfismo de A-módulos $a\cdot\colon A/a^nA \to A/a^nA$. Entonces,*

$$\operatorname{Ker} a\cdot \simeq A/aA$$
$$\operatorname{Im} a\cdot \simeq A/a^{n-1}A.$$

Demostración. $\operatorname{Ker} a\cdot = \{\bar{c} \in A/a^nA : \overline{ac} = 0\} = \{\bar{c} \in A/a^nA : ac \in a^nA\} = \langle \overline{a^{n-1}} \rangle$. El morfismo de A-módulos $A \to \langle \overline{a^{n-1}} \rangle$, $b \mapsto b \cdot \overline{a^{n-1}}$ es un epimorfismo y el núcleo es igual a aA, luego $\operatorname{Ker} a\cdot = \langle \overline{a^{n-1}} \rangle \simeq A/aA$. Por último, $\operatorname{Im} a\cdot = \langle \bar{a} \rangle$. El morfismo $A \to \langle \overline{a} \rangle$, $b \mapsto b\cdot\overline{a}$ es un epimorfismo y el núcleo es igual a $a^{n-1}A$, luego $\operatorname{Im} a\cdot = \langle \overline{a} \rangle \simeq A/a^{n-1}A$.

□

4. Lema: *Sea A un anillo íntegro y $a, b \in A$. Si b es primo y no divide a a, entonces el morfismo $b\cdot\colon A/aA \to A/aA$, $\bar{c} \mapsto \overline{bc}$ es inyectivo.*

Demostración. Si $\overline{bc} = 0$ entonces $bc = ad$ para cierto $d \in A$. Como b no divide a a, entonces b divide a d, es decir, $d = bd'$ luego $bc = abd'$ y $c = ad'$, luego $\bar{c} = 0$.

□

5. Teorema: *Sea A un anillo íntegro. Sean $\{p_1, \dots, p_r\}$ elementos primos de A, de modo que $(p_i) \neq (p_{i'})$, para todo $i \neq i'$. Sean $\{q_1, \dots, q_u\}$ elementos primos de A, de modo que $(q_j) \neq (q_{j'})$, para todo $j \neq j'$. Sean*

$$M = (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A)$$
$$N = (A/q_1^{m_{11}}A \oplus \cdots \oplus A/q_1^{m_{1t_1}}A) \oplus \cdots \oplus (A/q_u^{m_{u1}}A \oplus \cdots \oplus A/q_u^{m_{ut_u}}A)$$

donde $n_{ij}, m_{i'j'} > 0$ para todo ij e $i'j'$. Si $M \simeq N$ entonces, reordenando los sumandos, $(p_i) = (q_i)$ para todo i, y $n_{uv} = m_{uv}$, para todo uv.

Demostración. Dada un módulo E y $a \in A$, denotemos $a^E\colon E \to E$ el morfismo de A-módulos definido por $a^E(e) := a \cdot e$, para todo $e \in E$.

Por el lema 5.5.4, $\operatorname{Ker} p_1^{nM} = \overset{s_1}{\underset{i=1}{\oplus}} A/p_1^{n_{1i}}A$, para $n \gg 0$. Si $(p_1) \neq (q_i)$ para todo i, entonces $\operatorname{Ker} p_1^{nN} = 0$, lo cual es contradictorio porque $\operatorname{Ker} p_1^{nM} \simeq \operatorname{Ker} p_1^{nN}$. Reordenando, podemos suponer que $p_1 = q_1$ y en este caso $\operatorname{Ker} p_1^{nN} = \overset{t_1}{\underset{j=1}{\oplus}} A/p_1^{m_{1j}}A$. Reordenando podemos suponer que $n_{11} \geq n_{12} \geq \cdots \geq n_{1s_1} > 0$ y también podemos suponer que $m_{11} \geq m_{12} \geq \cdots \geq m_{1t_1} > 0$.

Denotemos $E := \operatorname{Ker} p_1^{nM}$ y $E' := \operatorname{Ker} p_1^{nN}$, que son isomorfos. Por el lema 5.5.3,

$$A/p_1A \oplus \overset{s_1}{\cdots} \oplus A/p_1A \simeq \operatorname{Ker} {p_1}^E \simeq \operatorname{Ker} {p_1}^{E'} \simeq A/p_1A \oplus \overset{t_1}{\cdots} \oplus A/p_1A$$

Luego, $s_1 = t_1$. Por el lema 5.5.3,

$$A/p_1^{n_{11}-1}A \oplus \cdots \oplus A/p_1^{n_{1s_1}-1}A \simeq \operatorname{Im} p_1{}^E \simeq \operatorname{Im} p_1{}^{E'} \simeq A/p_1^{m_{11}-1}A \oplus \cdots \oplus A/p_1^{m_{1t_1}-1}A.$$

Por inducción sobre la suma $\sum_i n_{1i}$, tenemos que $n_{1i}-1 = m_{1i}-1$, siempre que $n_{1i}-1 \neq 0$ y $m_{1i}-1 \neq 0$. Si s'_1 es el numero de los $n_{1i} \neq 1$ y t'_1 es el número de los $m_{1i} \neq 1$, entonces $s'_1 = t'_1$. Como $s_1 = t_1$, entonces $s_1 - s'_1 = t_1 - t'_1$, luego $n_{1i} = 1$ si y solo si $m_{1i} = 1$. Con todo junto, concluimos que $n_{1i} = m_{1i}$, para todo i.

□

6. Definición: Sea A un anillo íntegro y M un A-módulo. Llamaremos torsión de M, que denotaremos $T(M)$, a

$$T(M) := \{m \in M : \text{existe } a \in A \text{ no nulo tal que } am = 0\}.$$

7. Propiedades de la torsión de un módulo:

1. *$T(M)$ es un submódulo de M.*
2. *$T(T(M)) = T(M)$ y $T(M/T(M)) = 0$.*
3. *$T(M \oplus M') = T(M) \oplus T(M')$.*
4. *Si $\phi\colon M \to M'$ es un isomorfismo de módulos entonces $T(M) \to T(M')$, $m \mapsto \phi(m)$ es un isomorfismo de módulos, luego $M/T(M) \to M'/T(M')$, $\bar{m} \mapsto \overline{\phi(m)}$ es un isomorfismo de módulos.*

8. Teorema: *Sea A un anillo íntegro. Sean $\{p_1, \ldots, p_r\}$ elementos primos de A, de modo que $(p_i) \neq (p_{i'})$, para todo $i \neq i'$. Sean $\{q_1, \ldots, q_u\}$ elementos primos de A, de modo que $(q_j) \neq (q_{j'})$, para todo $j \neq j'$. Sean*

$$M = A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A)$$
$$N = A^m \oplus (A/q_1^{m_{11}}A \oplus \cdots \oplus A/q_1^{m_{1t_1}}A) \oplus \cdots \oplus (A/q_u^{m_{u1}}A \oplus \cdots \oplus A/q_u^{m_{ut_u}}A)$$

donde $n_{ij}, m_{i'j'} > 0$ para todo ij e $i'j'$. Si $M \simeq N$ entonces, $n = m$ y reordenando, $(p_i) = (q_i)$ para todo i, y $n_{uv} = m_{uv}$, para todo uv.

Demostración. $T(M) \simeq (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A)$, luego $M/T(M) \simeq A^n$. Por tanto, n está determinado por M (es el rango de $M/T(M)$). Tenemos que probar las unicidad de los $p_i^{n_{ij}}$. Esto es consecuencia del teorema 5.5.5. □

9. Teorema: *Sea A un anillo euclídeo y M un A-módulo finito generado. Entonces, existen elementos irreducibles $p_1, \ldots, p_r \in A$ ($(p_i) \neq (p_j)$, para todo $i \neq j$), únicos salvo multiplicación por invertibles, y $n \in \mathbb{N}$ y $0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que*

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A).$$

Se dirá que n es el rango de M y que los $p_i^{n_{ij}}$ son los divisores elementales de M.

10. Definición: Se dice que un A-módulo M es de torsión si $T(M) = M$. Se dice que M es un módulo sin torsión si $T(M) = 0$.

11. Corolario: *Sea A un anillo euclídeo y M un A-módulo finito generedo. M es libre si y solo si es un A-módulo sin torsión.*

5.5.2. Factores invariantes

12. Definición: Sea M un A-módulo. Se denomina ideal anulador de M, que denotaremos $\mathrm{Anul}_A(M)$, al ideal $\mathrm{Anul}_A(M) := \{a \in A : a \cdot m = 0, \text{ para todo } m \in M\}$.

13. Ejemplos: $\mathrm{Anul}_{\mathbb{Z}}(\mathbb{Z}) = 0$ y $\mathrm{Anul}_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = 6\mathbb{Z}$.

14. Ejemplo: Sea $m \in M$. El morfismo

$$A/\mathrm{Anul}(\langle m \rangle) \to \langle m \rangle, \bar{a} \mapsto a \cdot m$$

es un isomorfismo de A-módulos.

15. Proposición: *Si $\phi : M \to M'$ es un isomorfismo de A-módulos entonces* $\mathrm{Anul}(M) = \mathrm{Anul}(M')$.

16. Proposición: *Sean M y N dos A-módulos. Entonces,*

$$\mathrm{Anul}_A(M \oplus N) = \mathrm{Anul}_A(M) \cap \mathrm{Anul}_A(N).$$

Demostración. Es fácil de probar. □

17. Proposición: *Sea A un anillo euclídeo y M un A-módulo finito generado de torsión. El ideal anulador de M está generado por el mínimo común múltiplo de los divisores elementales asociados a M.*

Demostración. Por el teorema de clasificación sabemos que

$$M \simeq (A/p_1^{n_{11}}A \oplus \cdots A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_1^{n_{r1}}A \oplus \cdots A/p_r^{n_{rs_r}}A)$$

con p_i irreducibles, p_i primos con p_j para $i \neq j$. Podemos reordenar los sumandos $A/p_i^{n_{ij}}A$ de modo que $n_{11} \geq n_{12} \geq \cdots \geq n_{1s_1}$,..., $n_{r1} \geq n_{r2} \geq \cdots \geq n_{rs_r}$. Entonces,

$$\mathrm{Anul}_A(M) = p_1^{n_{11}} \cdot p_2^{n_{21}} \cdots p_r^{n_{r1}} = m.c.m.\{p_i^{n_{ij}}, \forall ij\}.$$

□

Sigamos con las hipótesis de la proposición anterior y con las notaciones de la demostración anterior. Definamos $\phi_1 = \mathrm{Anul}_A(M) = p_1^{n_{11}} \cdots p_r^{n_{r1}}$. Observemos que

$$M = (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_r^{n_{r1}}A) \oplus M_2 = A/\phi_1 A \oplus M_2$$

Argumentando igual con M_2, tenemos $\phi_2 \in A$ de modo que $\mathrm{Anul}_A(M_2) = \phi_2 A$ (ϕ_2 divide a ϕ_1, ya que $\mathrm{Anul}_A(M) \subseteq \mathrm{Anul}_A(M_2)$) y

$$M = A/\phi_1 A \oplus M_2 = A/\phi_1 A \oplus A/\phi_2 A \oplus M_3.$$

Recurrentemente, tenemos que

$$M = A/\phi_1 A \oplus A/\phi_2 A \oplus \cdots \oplus A/\phi_r A.$$

con $\phi_r | \phi_{r-1} | \cdots | \phi_1$, que se dice que son los factores invariantes de M.

5.6. Clasificación de los grupos abelianos

1. Teorema de clasificación: *Sea $(G,+)$ un grupo abeliano finito. Entonces, existen números primos $p_1,\ldots,p_r \in \mathbb{N}$ y números naturales no nulos $n_{ij} \in \mathbb{N}$ únicos de modo que*

$$\begin{aligned} G &\simeq (\mathbb{Z}/p_1^{n_{11}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_1^{n_{1s_1}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_r^{n_{r1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_{rs_r}}\mathbb{Z}) \\ &= \oplus_{ij} \mathbb{Z}/p_i^{n_{ij}}\mathbb{Z}. \end{aligned}$$

como grupo abeliano.

Demostración. Es consecuencia del teorema 5.5.9. □

2. Corolario : *Sea G un grupo abeliano finito. Entonces el orden de G es igual al producto de los divisores elementales asociados a G.*

3. Ejemplo : Clasifiquemos el $\mathbb{Z}$-módulo $M = \mathbb{Z}^3/\langle (2,4,2),(3,4,2),(2,2,2)\rangle$. Consideremos la aplicación lineal $\phi\colon \mathbb{Z}^3 \to \mathbb{Z}^3$, de matriz en las bases usuales

$$\phi \equiv \begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 2 \\ 2 & 2 & 2 \end{pmatrix}.$$

Tenemos que $M = \mathbb{Z}^3/\mathrm{Im}\,\phi$. Por transformaciones elementales obtenemos

$$\begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 2 \\ 2 & 2 & 2 \end{pmatrix} \overset{C_2-C_1}{\rightsquigarrow} \begin{pmatrix} 2 & 1 & 2 \\ 4 & 0 & 2 \\ 2 & 0 & 2 \end{pmatrix} \overset{C_1 x C_2}{\rightsquigarrow} \begin{pmatrix} 1 & 2 & 2 \\ 0 & 4 & 2 \\ 0 & 2 & 2 \end{pmatrix} \overset{\substack{C_2-2C_1 \\ C_3-2C_1}}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 2 \end{pmatrix} \overset{F_2 x F_3}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 4 & 2 \end{pmatrix}$$

$$\overset{F_3-2F_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -2 \end{pmatrix} \overset{C_3-C_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix} = D.$$

Tenemos el diagrama conmutativo

$$\begin{array}{ccccc} \mathbb{Z}^3 & \xrightarrow{\phi} & \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}^3/\mathrm{Im}\,\phi = M \\ \uparrow{\scriptstyle C} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle \bar{F}} \\ \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}^3/\mathrm{Im}\,D = \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \end{array}$$

Donde C viene dado por la composición de las transformaciones elementales de las columnas que hemos realizado, F por la composición de las transformaciones elementales de las filas que hemos realizado y D es la matriz diagonal de diagonal $1,2,-2$. Por tanto, $M \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ y tenemos clasificado M: los divisores elementales de M son $2,2$.

Calculemos F^{-1}. Tenemos que $F = (\mathrm{Id} - 2\delta_{32}) \cdot X_{23}$, luego $F^{-1} = X_{32} \cdot (\mathrm{Id} + 2\delta_{23})$. Multiplicando por la derecha por la matriz identidad obtenemos que

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{F_3+2F_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} \overset{F_2 \times F_3}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 0 \end{pmatrix} = F^{-1}.$$

Tenemos que $M = \langle \overline{(0,2,1)} \rangle \oplus \langle \overline{(0,1,0)} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

5.7. Clasificación de los endomorfismos lineales

1. Teorema de clasificación: *Sea E un k-espacio vectorial de dimensión finita y $T : E \to E$ un endomorfismo k-lineal. Entonces, existen polinomios irreducibles mónicos $p_1(x), \dots, p_r(x) \in k[x]$ y $0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que existe un isomorfismo de $k[x]$-módulos*

$$E \simeq (k[x]/(p_1(x)^{n_{11}}) \oplus \cdots \oplus k[x]/(p_1(x)^{n_{1s_1}})) \oplus \cdots \oplus (k[x]/(p_r(x)^{n_{r1}}) \oplus \cdots \oplus k[x]/(p_r(x)^{n_{rs_r}}))$$

(es decir, existe un isomorfismo k-lineal $\phi : E \simeq \oplus_{ij} k[x]/(p_i(x)^{n_{ij}})$, tal que $T = \phi^{-1} \circ x \cdot \circ \phi$).

Se dice que los $p_i(x)^{n_{ij}}$ son los divisores elementales asociados a T. Por tanto, los endomorfismos lineales están clasificados por sus divisores elementales.

Demostración. Es consecuencia del teorema 5.5.9. □

2. Corolario: *El polinomio anulador de T, $p_{\mathrm{Anul}(T)}(x)$, es el mínimo común múltiplo de los divisores elementales de T.*

Demostración. $\mathrm{Anul}(E) = (p_{\mathrm{Anul}(T)}(x))$, porque $p(x) \cdot e = 0$ para todo $e \in E$ si y solo si $p(T) = 0$. Por otra parte, por la proposición 5.5.17 $\mathrm{Anul}(E) = (m.c.m.\{p_i(x)^{n_{ij}}\})$. □

3. Corolario: *Sea k un cuerpo algebraicamente cerrado. Sea E un k-espacio vectorial de dimensión finita y $T : E \to E$ un endomorfismo k-lineal. Entonces, existen $\alpha_1, \dots, \alpha_r \in k$ y $0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que*

$$E \simeq \oplus_{ij} k[x]/((x - \alpha_i)^{n_{ij}}).$$

como $\mathbb{C}[x]$-módulos.

5.7.1. Matrices de Jordan

4. Lema: *Sea $\lambda \in k$. Entonces, $\{\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)}^{n-1}\}$ es una base del k-espacio vectorial $k[x]/((x-\lambda)^n)$.*

Demostración. Sabemos que las clases $\bar{1}, \bar{y}, \ldots, \bar{y}^{n-1}$ forman una base de $k[y]/(y^n)$. Haciendo el cambio $y = x - \lambda$ concluimos. □

Consideremos la aplicación lineal

$$x\cdot\colon k[x]/((x-\lambda)^n) \to k[x]/((x-\lambda)^n),\ \overline{p(x)} \mapsto \overline{x\cdot p(x)}.$$

Tomemos la base $\{e_j = \overline{(x-\lambda)}^j \mid 0 \le j \le n-1\}$. Se tiene

$$x\cdot e_j = x\cdot\overline{(x-\lambda)}^j = (x-\lambda)\cdot\overline{(x-\lambda)}^j + \lambda\overline{(x-\lambda)}^j = e_{j+1} + \lambda e_j.$$

Por lo tanto, la matriz de $x\cdot$ es igual a

$$\begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}.$$

5. Sea k un cuerpo algebraicamente cerrado y E un k-espacio vectorial de dimensión finita. Dado un endomorfismo k-lineal $T\colon E \to E$, sabemos que $E \simeq \bigoplus_{i,j} k[x]/((x-\lambda_i)^{n_{ij}})$. Tomando una base en cada sumando $k[x]/((x-\lambda_i)^{n_{ij}})$, como acabamos de hacer, obtendremos una base de E, llamada base de Jordan. La matriz de T en esta base es de la forma llamada de Jordan:

$$\begin{pmatrix} (B_{11}) & & & \\ & \ddots & & \\ & & (B_{ij}) & \\ & & & \ddots \end{pmatrix}$$

siendo (B_{ij}) la siguiente matriz cuadrada de orden n_{ij}

$$(B_{ij}) = \begin{pmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}.$$

6. Ejemplo: Sea $E = k[x]/((x-\lambda_1)^{n_1}\cdots(x-\lambda_r)^{n_r})$, con $\lambda_i \neq \lambda_j$ para todo $i \neq j$ y $n_i > 0$ para todo i. El morfismo

$$\begin{array}{rcl} k[x]/((x-\lambda_1)^{n_1}) \times \cdots \times k[x]/((x-\lambda_r)^{n_r}) & \to & k[x]/((x-\lambda_1)^{n_1}\cdots(x-\lambda_r)^{n_r}) \\ (\bar{p}_1, \ldots, \bar{p}_r) & \mapsto & \overline{c_1p_1 + \cdots + c_rp_r}, \end{array}$$

donde $c_i = \prod_{j\neq i}(x-\lambda_j)^{n_j}$ es un isomorfismo de $k[x]$-módulos por el problema 10 del tema 4. Si tomamos en cada sumando $k[x]/((x-\lambda_i)^{n_i}$ la base $\bar{1}, \overline{x-\lambda_i}, \ldots, \overline{(x-\lambda_i)^{n_i-1}}$, tendremos que $\left\{ e_{im_i} = \overline{(x-\lambda_1)^{n_1}\cdots(x-\lambda_i)^{m_i}\cdots(x-\lambda_r)^{n_r}} \right\}_{1\leq i\leq r, 0\leq m_i<n_i}$ es una base de E (ordenemos los vectores de la base según el siguiente orden $e_{im_i} < e_{jm_j}$ si $i<j$ ó $i=j$ y $m_i<m_j$) y la matriz de $x\cdot$ en esta base es

$$\left(\begin{array}{c|c|c} J_1 & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & J_r \end{array}\right), \quad \text{donde} \quad J_i = \overset{n_i}{\begin{pmatrix} \lambda_i & \cdots & \cdots & 0 \\ 1 & \lambda_i & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda_i \end{pmatrix}}.$$

7. Demos otro método para calcular una base de Jordan de T. Sigamos las notaciones de 5.7.5. Un número complejo λ es igual a alguno de los λ_i si y solo si $0 \neq \operatorname{Ker}(x-\lambda)\cdot \simeq \operatorname{Ker}(T-\lambda\cdot\mathrm{Id})$, es decir, $\det(T-\lambda\cdot\mathrm{Id})=0$ y λ es una raíz del polinomio característico de T (ver definición 5.7.11). Dado el morfismo de $k[x]$-módulos $x\cdot\colon k[x]/(x^n)\to k[x]/(x^n)$, $\overline{p(x)}\mapsto\overline{xp(x)}$ observemos que

$$\begin{array}{ccccccccccc} 0 & \hookrightarrow & \operatorname{Ker} x\cdot & \hookrightarrow & \operatorname{Ker} x^2\cdot & \hookrightarrow & \cdots & \hookrightarrow & \operatorname{Ker} x^{n-1}\cdot & \hookrightarrow & \operatorname{Ker} x^n\cdot = \operatorname{Ker} x^{n+1}\cdot \\ & & \| & & \| & & & & \| & & \| \\ & & (\overline{x}^{n-1}) & & (\overline{x}^{n-2}) & & & & (\overline{x}) & & k[x]/(x^n) \end{array}$$

Sea n_i el mínimo número natural tal que $\operatorname{Ker}(T-\lambda_i\cdot\mathrm{Id})^{n_i} = \operatorname{Ker}(T-\lambda_i\cdot\mathrm{Id})^{n_i+1}$. Puede comprobarse que el polinomio mínimo anulador de T es igual a $\prod_{i=1}^r (x-\lambda_i)^{n_i}$ y

$$E = \oplus_{i=1}^r \operatorname{Ker}(T-\lambda_i\cdot\mathrm{Id})^{n_i}.$$

Demos una base de Jordan en cada sumando directo $\operatorname{Ker}(T-\lambda_i\cdot\mathrm{Id})^{n_i}$. Para no ir arrastrando índices, escribamos $n=n_i$ y $S=T-\lambda_i\cdot\mathrm{Id}$. Consideremos la cadena de subespacios vectoriales

$$0 = \operatorname{Ker} S^0 \subset \operatorname{Ker} S^1 \subset \cdots \subset \operatorname{Ker} S^n.$$

Dado un subespacio vectorial $V_1 \subset V_2$ diremos que $\{e_i \in V_2\}_{i\in I}$ es una base suplementaria de V_1 en V_2 si $\{\bar{e}_i \in V_2/V_1\}_{i\in I}$ es una base de V_2/V_1 (es decir, $\{e_i\in V_2\}_{i\in I}$ son linealmente independientes y $\langle e_i\rangle_{i\in I}\oplus V_1 = V_2$). Observemos que la aplicación $\operatorname{Ker} S^i/\operatorname{Ker} S^{i-1} \to \operatorname{Ker} S^{i-1}/\operatorname{Ker} S^{i-2}$, $\bar{e}\mapsto\overline{S(e)}$ es inyectiva, para todo $i>1$. Procedamos:

1. Sea $\{e_1,\ldots,e_{r_1}\}$ una base suplementaria de $\operatorname{Ker} S^{n-1}$ en $\operatorname{Ker} S^n$.
2. Sea $\{S(e_1),\ldots,S(e_{r_1}),e_{r_1+1},\ldots,e_{r_2}\}$ una base suplem. de $\operatorname{Ker} S^{n-2}$ en $\operatorname{Ker} S^{n-1}$.
3. Sea $\{S^2(e_1),\ldots S^2(e_{r_1}),S(e_{r_1+1}),\ldots,S(e_{r_2}),e_{r_2+1},\ldots,e_{r_3}\}$ una base suplementaria de $\operatorname{Ker} S^{n-3}$ en $\operatorname{Ker} S^{n-2}$.
4. Procediendo así sucesivamente, $\{S^j e_i\}_{i.j}$ es una base de $\operatorname{Ker} S^n$. Ordenémosla por columnas como sigue

$\operatorname{Ker} S^n\downarrow$	e_1	$\cdots$	e_{r_1}							
$\operatorname{Ker} S^{n-1}\downarrow$	$S(e_1)$	$\cdots$	$S(e_{r_1})$	e_{r_1+1}	$\cdots$	e_{r_2}				
$\cup$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\cdots$			
$\operatorname{Ker} S$	$S^{n-1}(e_1)$	$\cdots$	$S^{n-1}(e_{r_1})$	$S^{n-2}(e_{r_1+1})$	$\cdots$	$S^{n-2}(e_{r_2})$	$\cdots$	$e_{r_{n-1}+1}$	$\cdots$	e_{r_n}

Observemos que cada columna i, $\{e_i, S(e_i), \ldots, S^{n-j}(e_i)\}$ (con $r_{j-1} < i \leq r_j$), es estable por S y la matriz de S sobre los vectores de esta columna es

$$N_j = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}_{n-j+1}.$$

En la base $\{S^j(e_i)\}$, ordenada como sigue: $S^r(e_i) < S^{r'}(e_{i'}) =$ si $i < i'$ ó $i = i'$ y $r < r'$, la matriz de S es

$$S \equiv \left(\begin{array}{c|c|c} M_1 & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & M_n \end{array}\right), \quad M_j = \left(\begin{array}{c|c|c} N_j & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & N_j \end{array}\right)_{r_j - r_{j-1}}, \quad N_j = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}_{n-j+1}.$$

Por último, recordemos que $T = S + \lambda_i \cdot \mathrm{Id}$. En la base escogida para S, la matriz de T es

$$T \equiv \left(\begin{array}{c|c|c} B_1 & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & B_n \end{array}\right), \quad B_j = \left(\begin{array}{c|c|c} J_j & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & J_j \end{array}\right)_{r_j - r_{j-1}}, \quad J_j = \begin{pmatrix} \lambda_i & \cdots & \cdots & 0 \\ 1 & \lambda_i & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda_i \end{pmatrix}_{n-i+1}.$$

5.7.2. Matriz característica

Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. Entonces, E es un $k[x]$-módulo y sabemos que $E \simeq \oplus_{ij} k[x]/(p_i(x)^{n_{ij}})$. Este isomorfismo lo obteníamos a partir de una presentación de E por $k[x]$-módulos libres. El objetivo de esta sección es obtener una presentación por $k[x]$-módulos libres de E y con ello explicitar el isomorfismo mencionado.

8. Definición-Notación: *Sean $v_1, \ldots, v_n$ elementos distintos de un conjunto. Llamaremos A-módulo libre de base $v_1, \ldots, v_n$ al A-módulo*

$$A * v_1 \oplus \cdots \oplus A * v_n := \{\textit{Sumas formales } a_1 * v_1 + \cdots + a_n * v_n, \forall\, a_1, \ldots, a_n \in A\},$$

donde definimos

$$\begin{aligned} (a_1 * v_1 + \cdots + a_n * v_n) + (a'_1 * v_1 + \cdots + a'_n * v_n) &:= (a_1 + a'_1) * v_1 + \cdots + (a_n + a'_n) * v_n \\ a \cdot (a_1 * v_1 + \cdots + a_n * v_n) &:= (aa_1) * v_1 + \cdots + (aa_n) * v_n. \end{aligned}$$

Denotemos $v_i = 0 * v_1 + \ldots + 1 * v_i + \ldots + 0 * v_n$, para cada i. Obviamente, $v_1, \ldots, v_n$ es una base del A-módulo $A * v_1 \oplus \cdots \oplus A * v_n$.

Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal, luego E es un $k[x]$-módulo. Demos una presentación de E por $k[x]$-módulos libres.

Sea $e_1,\dots,e_n$ una base del k-espacio vectorial E. Consideremos el $k[x]$-módulo libre $L = k[x]*e_1 \oplus \overset{n}{\cdots} \oplus k[x]*e_n$ de base $e_1,\dots,e_n$ y el morfismo de $k[x]$-módulos

$$\pi\colon L \to E,\ \pi(e_i) := e_i,$$

que es un epimorfismo. Consideremos los morfismos de $k[x]$-módulos $T\colon L \to L$, determinado por $T(e_i) := \sum_j a_{ij} * e_i$ y el morfismo de $k[x]$-módulos identidad $\mathrm{Id}\colon L \to L$, $l \mapsto l$. La sucesión de morfismos de $k[x]$-módulos

$$\boxed{L \xrightarrow{x\cdot \mathrm{Id} - T} L \xrightarrow{\pi} E}$$

es una presentación de E por $k[x]$-módulos libres:

Tenemos que probar que $\mathrm{Ker}\,\pi = \mathrm{Im}(x\cdot \mathrm{Id} - T)$. Dado $(x\cdot \mathrm{Id} - T)(e_i) \in \mathrm{Im}(x\cdot \mathrm{Id} - T)$, tenemos que

$$\pi((x\cdot \mathrm{Id} - T)(e_i)) = \pi(x * e_i - T(e_i)) = x\cdot e_i - T(e_i) = 0.$$

Luego, $\mathrm{Im}(x\cdot \mathrm{Id} - T) \subseteq \mathrm{Ker}\,\pi$. Sea ahora $\sum_i p_i(x) * e_i \in \mathrm{Ker}\,\pi$ (luego, $\sum_i p_i(T)(e_i) = 0$). En $L/\mathrm{Im}(x\cdot \mathrm{Id} - T)$ tenemos que $\overline{x\cdot m} = \overline{T(m)}$, para todo $m \in L$. Por tanto, $\overline{x^2\cdot m} = x\cdot\overline{x\cdot m} = x\cdot\overline{T(m)} = \overline{x\cdot T(m)} = \overline{T^2(m)}$. Recurrentemente, $\overline{x^n\cdot m} = \overline{T^n(m)}$ y $\overline{p(x)\cdot m} = \overline{p(T)(m)}$, para todo $p(x) \in k[x]$. Luego,

$$\overline{\sum_i p_i(x) * e_i} = \overline{\sum_i p_i(T)(e_i)} = \overline{0}.$$

Entonces, $\sum_i p_i(x) * e_i \in \mathrm{Im}(x\cdot \mathrm{Id} - T)$ y $\mathrm{Ker}\,\pi \subseteq \mathrm{Im}(x\cdot \mathrm{Id} - T)$.

9. Definición: Sea (a_{ij}) la matriz asociada a T en la base $\{e_1,\dots,e_n\}$. La matriz del endomorfismo de $k[x]$-módulos $x\cdot \mathrm{Id} - T\colon L \to L$ en la base $\{e_1,\dots,e_n\}$ del $k[x]$-módulo L es igual a

$$x\cdot \mathrm{Id} - (a_{ij}),$$

y se denomina la matriz característica asociada a T (en la base $\{e_1,\dots,e_n\}$) .

Mediante transformaciones elementales de la matriz $x\cdot \mathrm{Id} - (a_{ij})$ obtenemos una matriz diagonal D (cuyos coeficientes de la diagonal son ciertos polinomios $p_1(x),\dots,p_n(x)$ con coeficientes en k) y un diagrama conmutativo

$$\begin{array}{ccccc} L & \xrightarrow{x\cdot \mathrm{Id} - T} & L & \xrightarrow{\quad\pi\quad} & E \\ {\scriptstyle C}\uparrow\wr & & \wr\downarrow{\scriptstyle F} & & \wr\downarrow{\scriptstyle \bar{F}} \\ L & \xrightarrow[D]{} & L & \xrightarrow[\pi']{} & L/\mathrm{Im}\,D = k[x]/(p_1(x)) \oplus \cdots \oplus k[x]/(p_n(x)) \end{array}$$

donde π' es el morfismo de paso al cociente y $\bar{F}(\sum_i \lambda_i e_i) = \overline{F(\sum_i \lambda_i * e_i)}$.

Por último, si descomponemos en producto de potencias de irreducibles los polinomios $p_i(x) = \prod_j p_{ij}(x)^{n_{ij}}$, entonces $\{p_{ij}(x)^{n_{ij}}\}_{i,j}$ es el conjunto de los divisores elementales de T (en el caso de que $p_i(x)$ es constante, entonces $k[x]/(p_i(x)) = 0$ y lo desechamos).

10. Ejemplo: Clasifiquemos el endomorfismo $\mathbb{Q}$-lineal $T\colon \mathbb{Q}^4 \to \mathbb{Q}^4$ de matriz

$$\begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 0 & 2 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \end{pmatrix}$$

en la base estándar de $\mathbb{Q}^4$. Diagonalicemos la matriz característica

$$\begin{pmatrix} x-2 & 0 & 1 & 0 \\ 0 & x & -2 & 1 \\ -1 & 0 & x & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix} \overset{F_1 x F_3}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & x & 0 \\ 0 & x & -2 & 1 \\ x-2 & 0 & 1 & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix}$$

$$\overset{F_3+(-2+x)F_1}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & x & 0 \\ 0 & x & -2 & 1 \\ 0 & 0 & x^2-2x+1 & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix} \overset{C_3+xC_1}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x & -2 & 1 \\ 0 & 0 & x^2-2x+1 & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix}$$

$$\overset{F_2 x F_4}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & x+2 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & x & -2 & 1 \end{pmatrix} \overset{F_4+xF_2}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2+x \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & -2 & (x+1)^2 \end{pmatrix}$$

$$\overset{C_4+(x+2)C_2}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & -2 & (x+1)^2 \end{pmatrix} \overset{F_3 \times F_4}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & (x+1)^2 \\ 0 & 0 & (x-1)^2 & 0 \end{pmatrix}$$

$$\overset{F_4+\frac{(x-1)^2}{2}F_3}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & (x+1)^2 \\ 0 & 0 & 0 & \frac{(x-1)^2(x+1)^2}{2} \end{pmatrix} \overset{C_4+\frac{(x+1)^2}{2}C_3}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & \frac{(x-1)^2(x+1)^2}{2} \end{pmatrix}.$$

Por tanto, los divisores elementales asociados a T son $(x-1)^2, (x+1)^2$. El endomorfismo T es equivalente al endomorfismo

$$x\cdot\colon \mathbb{Q}[x]/((x-1)^2(x+1)^2) \to \mathbb{Q}[x]/((x-1)^2(x+1)^2).$$

Si en $\mathbb{Q}[x]/((x-1)^2(x+1)^2)$ tomamos la base

$$(*) \qquad \{\overline{(x+1)^2}, \overline{(x-1)(x+1)^2}, \overline{(x-1)^2}, \overline{(x+1)(x-1)^2}\},$$

la matriz de $x\cdot$ es

$$(**) \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Por último detallemos el isomorfismo $\bar{F}^{-1}\colon \mathbb{Q}[x]/((x-1)^2(x+1)^2) \simeq \mathbb{Q}^4$:

$$F^{-1} = X_{13}\circ(\mathrm{Id}+(2-x)\delta_{31})\circ X_{24}\circ(\mathrm{Id}-x\delta_{42})\circ X_{34}\circ(\mathrm{Id}-\frac{(x-1)^2}{2}\delta_{43}),$$

$\bar{F}^{-1}(\overline{1}) = \pi(F^{-1}(0,0,0,1))$ y

$$\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \overset{F_4-\frac{(x-1)^2}{2}F_3}{\rightsquigarrow} \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \overset{F_3\times F_4}{\rightsquigarrow} \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \overset{F_4-xF_2}{\rightsquigarrow} \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \overset{F_2\times F_4}{\rightsquigarrow} \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \overset{F_3+(2-x)F_1}{\rightsquigarrow} \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \overset{F_1\times F_3}{\rightsquigarrow} \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = F^{-1}\cdot\begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Luego, $\bar{F}^{-1}(\overline{1}) = (1,0,0,0)$. Vía $\bar{F}^{-1}$ la base correspondiente a la base $(*)$ es

$$\{(8,2,4,0),(4,6,4,2),(0,2,0,0),(0,2,0,2)\}.$$

La matriz asociada a T en esta base es la matriz $(**)$.

5.7.3. Polinomio característico. Teorema de Cayley-Hamilton

11. Definición: Sea E un k-espacio vectorial de dimensión finita y $T\colon E\to E$ un endomorfismo k-lineal. Se dice que $c_T(x) := \det(x\cdot\mathrm{Id}-T)\in k[x]$ es el polinomio característico de T.

12. Observación: Dada una base de E, y la matriz (a_{ij}) asociada a T en dicha base, se define $\det(x\cdot\mathrm{Id}-T) := \det(x\cdot\mathrm{Id}-(a_{ij}))$. Si consideramos otra base de E, entonces la matriz asociada a T en la nueva base es $(a'_{ij}) = (b_{ij})\cdot(a_{ij})\cdot(b_{ij})^{-1}$ (donde (b_{ij}) es la matriz de cambio de base. Observemos que

$$\begin{aligned}\det(x\cdot\mathrm{Id}-(a_{ij})) &= \det((b_{ij})\cdot(x\cdot\mathrm{Id}-(a_{ij}))\cdot(b_{ij})^{-1}) = \det(x\cdot\mathrm{Id}-(b_{ij})\cdot(a_{ij})\cdot(b_{ij})^{-1})\\ &= \det(x\cdot\mathrm{Id}-(a'_{ij})).\end{aligned}$$

13. Proposición: *Sea E un k-espacio vectorial de dimensión finita y $T\colon E\to E$ un endomorfismo k-lineal. El polinomio característico de T es igual al producto de los divisores elementales de T.*

Demostración. Sea $\{e_1,\dots,e_n\}$ una base de E, sea (a_{ij}) la matriz asociada a T en esta base, $L = \oplus_{i=1}^n k[x]*e_i$ y $\phi\colon L\to L$ el endomorfismo de $k[x]$-módulos de matriz en la base $\{e_i\}$, $x\,\mathrm{Id}-(a_{ij})$. Sabemos que $E\simeq L/\mathrm{Im}\,\phi$. Por transformaciones elementales especiales de los vectores de la base $\{e_i\}$ de L, que son cambios de base de determinante 1, sabemos que podemos obtener unas nuevas bases donde la matriz de ϕ es diagonal

$$\phi \equiv \begin{pmatrix} q_1(x) & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & q_n(x)\end{pmatrix}.$$

Por tanto,

$$c_T(x) = \det(\phi) = q_1(x)\cdots q_n(x).$$

Por otra parte, sabemos que $E \simeq k[x]/(q_1(x)) \oplus \cdots \oplus k[x]/(q_n(x))$. Descomponiendo cada polinomio $q_i(x)$ en producto de potencias de irreducibles obteníamos los divisores elementales de T (salvo multiplicación por invertibles de k). Luego, $q_1(x)\cdots q_n(x)$ es el producto de los divisores elementales de T (salvo multiplicación por invertibles de k). En conclusión, $c_T(x)$ (que es mónico) coincide con el producto de los divisores elementales (que son mónicos).

□

14. Teorema de Cayley-Hamilton: *Sea E un espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. Sea $c_T(x)$ el polinomio característico de T. El polinomio característico es múltiplo del polinomio mínimo anulador, es decir,*

$$c_T(T) = 0.$$

Además, los polinomios irreducibles que dividen al polinomio característico son los mismos que los que dividen al polinomio mínimo anulador.

Demostración. El polinomio característico es el producto de todos los divisores elementales y el polinomio mínimo anulador es el mínimo común múltiplo de ellos. Por lo tanto, el polinomio característico es múltiplo del anulador, es decir, $c_T(T) = 0$; y los polinomios irreducibles que dividen al polinomio característico son los mismos que los que dividen al polinomio mínimo anulador.

□

15. Definición: Se dice que un vector no nulo $e \in E$ es un vector propio de valor propio $\lambda \in k$ de T si $T(e) = \lambda e$.

16. Proposición: *Existe un vector propio $e \in E$ de valor propio $\lambda \in k$ si y solo si λ es una raíz de $c_T(x)$.*

Demostración. Existe un vector propio $e \in E$ de valor propio $\lambda \in k$ si y solo si $\operatorname{Ker}(\lambda \cdot \operatorname{Id} - T) \neq 0$, que equivale a que $\det(\lambda \cdot \operatorname{Id} - T) = 0$, que equivale a $c_T(\lambda) = 0$. □

17. Definición: Se dice que un endomorfismo k-lineal $T\colon E \to E$ diagonaliza si y solo si existe una base de E formada por vectores propios.

18. Proposición: *Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. T diagonaliza si y solo si el polinomio mínimo anulador de T tiene todas sus raíces en k y son de multiplicidad* 1.

Demostración. $\Rightarrow$) Sea $\{e_1,\ldots,e_n\}$ una base de E tal que $T(e_i) = \lambda_i e_i$. Sean $\lambda_{i_1},\ldots,\lambda_{i_r}$ distintos entre sí de modo que $\{\lambda_{i_1},\ldots,\lambda_{i_r}\} = \{\lambda_1,\ldots,\lambda_n\}$. Entonces, el polinomio anulador de T es $\prod_{j=1}^{r}(x - \lambda_{i_j})$

$\Leftarrow$) Sean $\lambda_1,\ldots,\lambda_r \in k$ distintos tal que el polinomio anulador de T sea $p(x) = \prod_{i=1}^{r}(x - \lambda_i)$, con $\lambda_i \neq \lambda j$ cuando $i \neq j$. Entonces,

$$E = \operatorname{Ker} p(x)\cdot = \operatorname{Ker}(x - \lambda_1)\cdot \oplus \cdots \oplus \operatorname{Ker}(x - \lambda_r)\cdot$$

Sea $\{e_{ij}\}_j$ una base de $\mathrm{Ker}(x-\lambda_i)\cdot = \mathrm{Ker}(T-\lambda_i\,\mathrm{Id})$. Entonces, $\{e_{ij}\}_{ij}$ es una base de E formada por vectores propios.

□

19. Corolario: *Sea E un k-espacio vectorial de dimensión finita y $T: E \to E$ un endomorfismo k-lineal. Si todas las raíces del polinomio característico de T están en k y son de multiplicidad* 1*, entonces T diagonaliza.*

Demostración. Si todas las raíces del polinomio característico son de multiplicidad 1 entonces el polinomio característico coincide con el polinomio anulador. Se concluye por la proposición 5.7.18. □

5.7.4. Sistemas de ecuaciones diferenciales lineales

20. Consideremos el sistema de ecuaciones diferenciales con coeficientes constantes

$$\begin{array}{rcl} \frac{dx_1}{dt} & = & a_{11}x_1+\cdots+a_{1n}x_n \\ \cdots & = & \cdots \\ \frac{dx_n}{dt} & = & a_{n1}x_1+\cdots+a_{nn}x_n \end{array}$$

donde $A=(a_{ij})$ es una matriz cuadrada de orden n, con coeficentes complejos. De modo conciso escribiremos el sistema anterior $X'=AX$. Por cambio lineal de coordenadas. $Y=BX$, tenemos $Y'=BX'=BAX=BAB^{-1}Y$ y para B conveniente podemos conseguir que $J=BAB^{-1}$ sea una matriz de Jordan (que es una matriz triangular). Ahora ya es fácil calcular Y y por tanto podemos calcular X.

Demos otro modo de calcular las soluciones: Se define $e^{At}:=\sum_{n=0}^{\infty}A^n\cdot\frac{t^n}{n!}$. Las soluciones del sistema $X'=AX$ son $\{X=e^{At}\cdot C\}$, siendo C una matriz columna de constantes cualesquiera. Para calcular e^{At}, recordemos que $A=B^{-1}JB$ y observemos que

$$e^{At}=e^{B^{-1}JBt}=B^{-1}e^{Jt}B.$$

Luego, $\{X=B^{-1}e^{Jt}\cdot C\}$. Sea D la matriz diagonal cuyos coeficientes en la diagonal son los de J. Escribamos $J=D+N$. Observemos que D y N conmutan y que $N^n=0$. Entonces,

$$e^{Jt}=e^{Dt}e^{Nt}=e^{Dt}\cdot(\mathrm{Id}+Nt+\frac{N^2t^2}{2!}+\cdots+\frac{N^{n-1}t^{n-1}}{(n-1)!}).$$

21. Sea $X'=AX+B(t)$ un sistema lineal de ecuaciones diferenciales. Tenemos que $(D-A)X=B(t)$, luego una solución particular es

$$X=\frac{1}{D-A}B(t)=\frac{1}{D-A}(e^{At}e^{-At}B(t))=e^{At}\frac{1}{D}(e^{-At}B(t)))=e^{At}\int e^{-At}B(t)dt.$$

22. Ejercicio: Resuélvanse los siguientes sistemas de ecuaciones diferenciales

$$\begin{array}{l} \frac{dx}{dt}=x-3y+3z \\ \frac{dy}{dt}=-2x-6y+13z \\ \frac{dz}{dt}=-x-4y+8z \end{array} \qquad \begin{array}{l} \frac{dx}{dt}=3x-y \\ \frac{dy}{dt}=x+y \\ \frac{dz}{dt}=3x+5z-3u \\ \frac{du}{dt}=4x-y+3z-u \end{array} \qquad \begin{array}{l} \frac{dx}{dt}=-11x-4y \\ \frac{dy}{dt}=15x+6y \end{array}$$

23. Sea $p(x)=\sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$ un polinomio de grado n. La ecuación diferencial

$$p(D)y = f(x)$$

es equivalente a al sistema de ecuaciones diferenciales lineales con coeficientes constantes de primer orden de n variables:

$$\begin{aligned} &x_1' = x_2\\ &\cdots\\ &x_{n-1}' = x_n\\ &x_n' = \tfrac{-1}{a_n}\cdot(\textstyle\sum_{i=0}^{n-1} a_i x_{i+1}) + f(x)\end{aligned}$$

24. Ejercicio: Sea $A=(p_{ij}(D))$ una matriz, con $p_{ij}(x)\in\mathbb{C}[x]$. Prueba que mediante las transformaciones elementales, el problema de resolver el sistema $AX(t)=Y(t)$, se reduce al problema de resolver ecuaciones $p(D)f(t)=h(t)$.

Resuelve el sistema de ecuaciones diferenciales

$$\begin{aligned} &x''-x+y' = e^t\\ &x''+2x'+x+y'' = e^t.\end{aligned}$$

5.8. Localización de módulos

Sea S un sistema multiplicativo de un anillo A y M un A-módulo. Podemos definir en el conjunto $M\times S$ la siguiente relación de equivalencia:

$$(m,s)\sim(m',s') \iff \text{existen } s_1,s_2\in S \text{ tales que } (s_1m,s_1s)=(s_2m',s_2s').$$

Denotaremos $\frac{m}{s}$ a la clase de equivalencia de (m,s).

1. Definición: Sea S un sistema multiplicativo de un anillo A y M un A-módulo, denotaremos por M_S:

$$M_S=\{\frac{m}{s},\ \forall\ m\in M, s\in S\}$$

y diremos que M_S es la localización de M por el sistema multiplicativo S.

Recordemos que que $\frac{m}{s}=\frac{m'}{s'}$ si y solo si existen $s_1,s_2\in S$ tales que $(s_1m,s_1s)=(s_2m',s_2s')$. Para definir una aplicación $M_S\to X$, tenemos que asignar a cada $\frac{m}{s}\in M_S$ un elemento $\phi(m,s)$, de modo que $\phi(tm,ts)=\phi(m,s)$, para todo $t\in S$. Igualmente, para definir una aplicación $M_S\times N_S\to X$, tenemos que asignar a cada $(\frac{m}{s},\frac{n}{s'})\in M_S\times N_S$ un elemento $\phi(m,s,n,s')$, de modo que $\phi(tm,ts,t'n,t's')=\phi(m,s,n,s')$, para todo $t,t'\in S$.

Con las operaciones (bien definidas)

$$\begin{aligned}\frac{m}{s}+\frac{m'}{s'} &:= \frac{s'm+sm'}{ss'}\\ \frac{a}{s}\cdot\frac{m}{s'} &:= \frac{am}{ss'}\end{aligned}$$

M_S tiene estructura de A_S-módulo. La aplicación canónica

$$M\to M_S,\ m\mapsto\frac{m}{1}$$

es un morfismo de A-módulos y diremos que es el morfismo de localización.

2. Ejercicio: Prueba que $\frac{m}{s} = 0$ si y solo sí existe un $t \in S$ de modo que $t \cdot m = 0$.

Todo morfismo $f : M \to N$ de A-módulos, induce la aplicación (bien definida)

$$f_S : M_S \to N_S, \frac{m}{s} \underset{\text{def}}{\mapsto} \frac{f(m)}{s},$$

que es morfismo de A_S-módulos.

3. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sean M y M' dos A-módulos. Entonces,*

$$(M \oplus M')_S = M_S \oplus M'_S$$

Demostración. Los morfismos de A_S-módulos $(M \oplus M')_S \to M_S \oplus M'_S$, $\frac{(m,m')}{s} \mapsto (\frac{m}{s}, \frac{m'}{s})$ y $M_S \oplus M'_S \to (M \oplus M')_S$, $(\frac{m}{s}, \frac{m'}{s'}) \mapsto \frac{(s'm, sm')}{ss'}$ son inversos entre sí. □

4. Ejemplo: Sea A un anillo íntegro y $\Sigma = A_{A\setminus\{0\}}$. Entonces,

$$(A^n)_{A\setminus\{0\}} = A_{A\setminus\{0\}} \oplus \overset{n}{\cdots} \oplus A_{A\setminus\{0\}} = \Sigma^n.$$

5. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sea M un A-módulo y $N \subseteq M$ un submódulo. Entonces, N_S es un submódulo de M_S (es decir, el morfismo $N_S \to M_S$ es inyectivo) y tenemos un isomorfismo natural*

$$M_S/N_S \simeq (M/N)_S.$$

Demostración. El morfismo $N_S \to M_S$ es inyectivo: Dado $\frac{n}{s} \in N_S$, si $\frac{n}{s} = 0$ en M_S, existe un elemento $s' \in S$ de modo que $s' \cdot n = 0$ en M (luego en N), por tanto $\frac{n}{s} = 0$ en N_S.

Consideremos el epimorfismo de paso al cociente $M \to M/N$. Localizando por S tenemos el morfismo $M_S \to (M/N)_S$, $m/s \mapsto \bar{m}/s$ que es claramente epiyectivo. Calculemos el núcleo: si $\bar{m}/s = 0$ entonces existe un elemento $s' \in S$ tal que $s' \cdot \bar{m} = 0$, es decir, $s' \cdot m \in N$, es decir, existe $n \in N$ de modo que $s' \cdot m = n$, luego $m/s = n/ss' \in N_S$. Recíprocamente, dado $n/s \in N_S$, entonces $\bar{n}/s = 0/s = 0$. □

6. Ejercicio: Sea $I \subseteq A$ un ideal y $S \subset A$ un sistema multiplicativo. Prueba que $I_S = I \cdot A_S$.

Sea A un anillo íntegro y M un A-módulo. Recordemos que definíamos la torsión $T(M)$ de M como $T(M) = \{m \in M : \text{existe } a \in A \text{ no nulo tal que } am = 0\}$.

Es fácil comprobar que $T(M)$ coincide con el núcleo del morfismo de localización $M \to M_{A-\{0\}}$, $m \mapsto \frac{m}{1}$. Además, $T(M)_{A-\{0\}} = 0$. Recordemos que $M/T(M)$ es un módulo sin torsión. Además,

$$(M/T(M))_{A-\{0\}} = M_{A-\{0\}}/T(M)_{A-\{0\}} = M_{A-\{0\}}.$$

7. Definición: Sea A un anillo íntegro, $\Sigma := A_{A-\{0\}}$ y M un A-módulo. Diremos que $\dim_\Sigma M_{A-\{0\}}$ es el rango de M.

8. Proposición: *Sea A un anillo íntegro. Si M es un A-módulo finito generado libre de torsión, entonces es un submódulo de un A-módulo libre del mismo rango.*

Demostración. Sea $\Sigma := A_{A\setminus\{0\}}$. Tenemos que $M = \langle m_1, \dots, m_n\rangle$ y el morfismo de localización $M \hookrightarrow M_{A\setminus\{0\}}$ es inyectivo. Evidentemente $\{\frac{m_1}{1}, \dots, \frac{m_n}{1}\}$ es un sistema generador del Σ-espacio vectorial $M_{A\setminus\{0\}}$. Sea $\{n_1, \dots, n_r\}$ una base del Σ-espacio vectorial $M_{A\setminus\{0\}}$. Para cada j tendremos $\frac{m_j}{1} = \sum_{s=1}^{r} \frac{a_{js}}{b_{js}} \cdot n_s$. Denotemos $b = \prod_{i,j} b_{ij}$. Con las notaciones obvias, tendremos el siguiente diagrama conmutativo de morfismos inyectivos

$$\begin{array}{ccc} M & \hookrightarrow & M_{A\setminus\{0\}} \\ & \searrow & \uparrow \\ & & A\frac{n_1}{b} \oplus \cdots \oplus A\frac{n_r}{b} \end{array}$$

□

5.9. Clasificación de los módulos sobre domios de ideales principales

El objetivo de esta sección es probar que el teorema de descomposición de un módulo finito generado M, sobre un anillo euclídeo, como suma directa de A-módulos A/a_iA, es igualmente cierto para módulos finito generados sobre dominios de ideales principales.

1. Proposición: *Sea A un dominio de ideales principales. Si M es un A-módulo finito generado libre de torsión, entonces es un A-módulo libre.*

Demostración. Por la proposición 5.8.8, basta probar que los submódulos de un A-módulo libre son libres. Procederemos por inducción sobre el rango del módulo libre, que denotaremos L.

Si el rango de L es cero es obvio. Si el rango de L es uno entonces $L \simeq A$. Por tanto, todo submódulo M de L es isomorfo a un ideal de A, luego $M \simeq aA$. Si $a \neq 0$ entonces $A \simeq aA$, $b \mapsto ab$, luego M es libre de rango 1. Si $a = 0$ entonces $M = 0$.

Supongamos que el rango de L es $n > 1$. Podemos suponer que $L = A^n$. Sea $L' \simeq A$ el submódulo de L, $L' := \{(a, 0, \dots, 0) \in L,\ \forall a \in A\}$. Obviamente $L'' := L/L'$, es un módulo libre de rango $n-1$. Sea $\pi\colon L \to L''$ el morfismo de paso al cociente. Dado $M \subseteq L$ consideremos el diagrama conmutativo

$$\begin{array}{ccccc} L' & \hookrightarrow & L & \xrightarrow{\pi} & L'' \\ \uparrow & & \uparrow & & \uparrow \\ L' \cap M = \operatorname{Ker}\pi_{|M} & \hookrightarrow & M & \xrightarrow{\pi_{|M}} & \pi(M) \end{array}$$

Por inducción $L' \cap M$ y $\pi(M)$ son libres de rango finito. Por tanto, como $\pi(M)$ es libre, el epimorfismo $M \to \pi(M)$ tiene sección y por el problema 6 del capítulo 4, tenemos un isomorfismo $M = (L' \cap M) \oplus \pi(M)$. En conclusión, M es libre. □

2. Primer teorema de descomposición: Sea A un dominio de ideales principales y M un A-módulo finito generado. Se cumple que

$$M \simeq T(M) \oplus (M/T(M)),$$

(observemos que $T(M)$ es un módulo finito generado de torsión y $M/T(M)$ es un módulo finito generado libre). Además, si $M \simeq M' \oplus L$, siendo M' un A-módulo de torsión y L libre, entonces $M' \simeq T(M)$ y $L \simeq (M/T(M))$.

Demostración. $M/T(M)$ es un módulo finito libre de torsión. Por la proposición anterior $M/T(M)$ es un módulo libre. El epimorfismo de paso al cociente $M \to M/T(M)$ tiene sección, porque $M/T(M)$ es libre, luego $M \simeq T(M) \oplus (M/T(M))$.

Si $M \simeq M' \oplus L$, entonces $T(M) \simeq T(M' \oplus L) = T(M') \oplus T(L) = M'$. Luego $(M/T(M)) \simeq (M' \oplus L)/M' = L$. Hemos concluido.

□

3. Observación: Observemos que $M_{A-\{0\}} = (M/T(M))_{A-\{0\}}$. Por tanto, el rango de $M/T(M)$ es el de M. Así pues, en el teorema anterior $M/T(M)$ es un módulo libre de rango el de M.

4. Si $M = \langle m_1, \ldots, m_r \rangle$ es un A-módulo de torsión y $(a_i) = \mathrm{Anul}(m_i)$, entonces

$$\mathrm{Anul}(M) = \mathrm{Anul}(m_1) \cap \ldots \cap \mathrm{Anul}(m_r) = (m.c.m.(a_1, \ldots, a_r)) = (a).$$

Si descomponemos a en potencias de irreducibles $a = p_1^{n_1} \cdots p_s^{n_s}$, por el teorema de descomposición 4.5.3, sabemos que

$$M = \mathrm{Ker}\, a\cdot = \mathrm{Ker}\, p_1^{n_1} \cdot \oplus \cdots \oplus \mathrm{Ker}\, p_s^{n_s} \cdot .$$

Hemos reducido el problema de la clasificación de los módulos finito generados sobre dominios de ideales principales, a la clasificación de los módulos finito generados de ideal anulador (p^n), con p irreducible.

5. Proposición: *Sea A DIP y $p \in A$ irreducible, M un A-módulo finito generado tal que $p^n \cdot M = 0$, para cierto $0 \neq n \in \mathbb{N}$. Entonces, existen números naturales $n_i \neq 0$ de modo que*

$$M \simeq \oplus_{n_i} A/p^{n_i} A.$$

Demostración. M es un $A/p^n A$-módulo finito generado y $A/p^n A$ es un anillo casieuclídeo. Dado $\bar{a} \in A/p^n A$, tenemos que

$$(A/p^n A)/(\bar{a}) = A/(p^n, a) = A/(m.c.d.(p^n, a)) = A/p^r A.$$

Concluimos por el teorema 5.5.1.

□

6. Teorema de clasificación: *Sea A un dominio de ideales principales y M un A-módulo finito generado. Entonces, existen elementos irreducibles $p_1,\dots,p_r \in A$ ($(p_i) \neq (p_j)$, para todo $i \neq j$), únicos salvo invertibles, y números naturales $n_{ij} \neq 0$ y n únicos, de modo que*

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A).$$

Demostración. La existencia de tal descomposición es consecuencia de 5.9.2, 4.5.3 y 5.9.5. La unicidad es consecuencia de 5.9.2 y 5.5.5. □

5.10. Cuestionario

1. Diagonaliza mediante transformaciones elementales la matriz con coeficientes enteros $\begin{pmatrix} 4 & 5 & 2 \\ 2 & 7 & 5 \\ 4 & 2 & 3 \end{pmatrix}$.

2. Resuelve el sistema de ecuaciones diofánticas

$$\begin{aligned} 2x + 3y + z &= 6 \\ 4x + 2y + z &= 5 \end{aligned}$$

3. Sean $M_1, M_2 \subseteq M$ dos A-submódulos. Prueba que

$$\mathrm{Anul}(M_1 + M_2) = \mathrm{Anul}(M_1) \cap \mathrm{Anul}(M_2).$$

4. Calcula el ideal anulador del $k[x]$-módulo $k[x]/((x+1)^2) \oplus k[x]/(x^2-1)$.

5. Clasifica los grupos abelianos de orden 36.

6. Calcula los divisores elementales asociados al $\mathbb{Z}$-módulo $\mathbb{Z}/84\mathbb{Z}$.

7. Clasifica el grupo abeliano $M = \mathbb{Z}^3/\langle (2,3,2),(3,4,2),(2,2,2)\rangle$.

8. ¿Son los grupos abelianos $\mathbb{Z}^2/\langle (4,2),(-2,2)\rangle$ y $\mathbb{Z}^2/\langle (7,4),(4,4)\rangle$ isomorfos?

9. Sea G un grupo abeliano finito ¿a qué es igual el producto de los divisores elementales de G?

10. Sea T un endomorfismo lineal de un espacio vectorial de dimensión finita ¿a qué es igual el producto de los divisores elementales de T?

11. Sea $p(x) \in k[x]$ un polinomio mónico ¿Calcula el polinomio característico del endomorfismo k-lineal $x\cdot\colon k[x]/(p(x)) \to k[x]/(p(x)), \overline{q(x)} \mapsto \overline{xq(x)}$?

12. Clasica todos los endomorfismos nihilpotentes de un espacio vectorial de dimensión 4.

13. Clasifíca el endomorfismo $\mathbb{R}$-lineal de matriz $\begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & -2 \\ 1 & 1 & 3 \end{pmatrix}$.

14. Calcula $(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z})_{\mathbb{Z}\setminus\{0\}}$.

15. Sea A un anillo íntegro y M un A-módulo. Prueba que el núcleo del morfismo de localización $M \to M_{A\setminus\{0\}}$, $m \mapsto \frac{m}{1}$ es igual a $T(M)$.

5.11. Biografía de Camile Jordan

Camille Jordan's father, Esprit-Alexandre Jordan (1800-1888), was an engineer who had been educated at the École Polytechnique. Camille's mother, Joséphine Puvis de Chavannes, was the sister of the famous painter Pierre Puvis de Chavannes who was the foremost French mural painter of the second half of the 19th century. Camille's father's family were also quite well known; a grand-uncle also called Ennemond-Camille Jordan (1771-1821) achieved a high political position while a cousin Alexis Jordan (1814-1897) was a famous botanist.

Jordan studied at the Lycée de Lyon and at the Collège d'Oullins. He entered the École Polytechnique to study mathematics in 1855. This establishment provided training to be an engineer and Jordan, like many other French mathematicians of his time, qualified as an engineer and took up that profession. Cauchy in particular had been one to take this route and, like Cauchy, Jordan was able to work as an engineer and still devote considerable time to mathematical research. Jordan's doctoral thesis was in two parts with the first part Sur le nombre des valeurs des fonctions being on algebra. The second part entitled Sur des periodes des fonctions inverses des intégrales des différentielles algebriques was on integrals of the form $\int u\,dz$ where u is a function satisfying an algebraic equation $f(u,z) = 0$. Jordan was examined on 14 January 1861 by Duhamel, Serret and Puiseux. In fact the topic of the second part of Jordan's thesis had been proposed by Puiseux and it was this second part which the examiners preferred. After the examination he continued to work as an engineer, first at Privas, then at Chalon-sur-Saône, and finally in Paris.

Jordan married Marie-Isabelle Munet, the daughter of the deputy mayor of Lyon, in 1862. They had eight children, two daughters and six sons.

From 1873 he was an examiner at the École Polytechnique where he became professor of analysis on 25 November 1876. He was also a professor at the Collège de France from 1883 although until 1885 he was at least theoretically still an engineer by profession. It is significant, however, that he found more time to undertake research when he was an engineer. Most of his original research dates from this period.

Jordan was a mathematician who worked in a wide variety of different areas essentially contributing to every mathematical topic which was studied at that time: on finite groups, on linear and multilinear algebra, on the theory of numbers, on the topology of polyhedra, differential equations, and mechanics.

Topology (called analysis situs at that time) played a major role in some of his first publications which were a combinatorial approach to symmetries. He introduced important topological concepts in 1866 built on his knowledge of Riemann's work in topology but not the work by Möbius for he was unaware of it. Jordan introduced the notion of homotopy of paths looking at the deformation of paths one into the other. He defined a homotopy group of a surface without explicitly using group terminology.

Jordan was particularly interested in the theory of finite groups. In fact this is not really an accurate statement, for it would be reasonable to argue that before Jordan began his research in this area there was no theory of finite groups. It was Jordan who was the first to develop a systematic approach to the topic. It was not until Liouville republished Galois's original work in 1846 that its significance was noticed at all. Serret, Bertrand and Hermite had attended Liouville's lectures on Galois theory and had begun to contribute to the topic but it was Jordan who was the first to formulate the direction the subject would take.

To Jordan a group was what we would call today a permutation group; the concept of an abstract group would only be studied later. To give an illustration of the way he tried to build up groups theory we will say a little about his contributions to finite soluble groups. The standard way to define such groups today would be to say that they are groups whose composition factors are abelian groups. Indeed Jordan introduced the concept of a composition series (a series of subgroups each normal in the preceding with the property that no further terms could be added to the series so that it retains that property). The composition factors of a group G are the groups obtained by computing the factor groups of adjacent groups in the composition series. Jordan proved the Jordan-Hölder theorem, namely that although groups can have different composition series, the set of composition factors is an invariant of the group.

Although the classification of finite abelian groups is straightforward, the classification of finite soluble groups is well beyond mathematicians today and for the foreseeable future. Jordan, however, clearly saw this as an aim of the subject, even if it was not one which might ever be solved. He made some remarkable contributions to how such a classification might proceed setting up a recursive method to determine all soluble groups of order n for a given n.

A second major piece of work on finite groups was the study of the general linear group over the field with p elements, p prime. He applied his work on classical groups to determine the structure of the Galois group of equations whose roots were chosen to be associated with certain geometrical configurations.

His work on group theory done between 1860 and 1870 was written up into a major text "Traité des substitutions et des équations algebraique" which he published in 1870. This treatise gave a comprehensive study of Galois theory as well as providing the first ever group theory book. For this work he was awarded the Poncelet Prize of the Académie des Sciences. The treatise contains the "Jordan normal form" theorem for matrices, not over the complex numbers but over a finite field. He appears not to have known of earlier results of this type by Weierstrass. His book brought permutation groups into a central role in mathematics and, until Burnside wrote his famous group theory text nearly 30 years later, this work provided the foundation on which the whole subject was built. It would also be fair to say that group theory was one of

the major areas of mathematical research for 100 years following Jordan's fundamental publication.

Jordan's use of the group concept in geometry in 1869 was motivated by studies of crystal structure. He considered the classification of groups of Euclidean motions. His work had gained him a wide international reputation and both Sophus Lie and Felix Klein visited him in Paris in 1870 to study with him. Jordan's interest in groups of Euclidean transformations in three dimensional space influenced Lie and Klein in their own theories of continuous and discontinuous groups.

The publication of Traité des substitutions et des équations algebraique did not mark the end of Jordan's contribution to group theory. He went on over the next decade to produce further results of fundamental importance. He studied primitive permutation groups and proved a finiteness theorem. He defined the class of a subgroup of the symmetric group to be $c > 1$ if c was the smallest number such that the subgroup had an element moving c points. His finiteness theorem showed that for a given c there are only finitely many primitive groups with class c other than the symmetric and alternating groups.

Generalising a result of Fuchs on linear differential equations, Jordan was led to study the finite subgroups of the general linear group of $n \times n$ matrices over the complex numbers. Although there are infinite families of such finite subgroups, Jordan found that they were of a very specific group theoretic structure which he was able to describe.

Another generalisation, this time of work by Hermite on quadratic forms with integral coefficients, led Jordan to consider the special linear group of $n \times n$ matrices of determinant 1 over the complex numbers acting on the vector space of complex polynomials in n indeterminates of degree m.

Jordan is best remembered today among analysts and topologists for his proof that a simply closed curve divides a plane into exactly two regions, now called the Jordan curve theorem. It was only his increased understanding of mathematical rigour which made him realise that a proof of such a result was necessary. He also originated the concept of functions of bounded variation and is known especially for his definition of the length of a curve. These concepts appears in his Cours d'analyse de l'École Polytechnique . Jordan was lecturing at the École Polytechnique and the book was written as a text for the students there. In some respects this is a little strange since it is a rigorous analysis text built on top of the attempts to put the topic on a firm foundation begun by Cauchy and given considerable impetus by Weierstrass. However, the courses at the École Polytechnique were supposed to train students to become civil and military engineers and this does not seem to be the approach which one would take trying to teach applications of the calculus to engineers. There had been a tradition of rigorous analysis at the École Polytechnique begun, of course, by Cauchy himself. Jordan was aware that his work was at a level that would be somewhat inappropriate for engineering students for he once said to Lebesgue that he called it "École Polytechnique analysis course"since:

"*... one puts that on the cover to please the publisher...*"

Among Jordan's many contributions to analysis we should also mention his generalisation of the criteria for the convergence of a Fourier series.

The Journal de Mathématiques Pure et Appliquées was a leading mathematical journal and played a very significant part in the development of mathematics throughout the 19th century. It was usually known as the Journal de Liouville since Liouville had founded the journal in 1836. Liouville died in 1882 and in 1885 Jordan became editor of the Journal, a role he kept for over 35 years until his death.

In 1912 Jordan retired from his positions. The final years of his life were saddened, however, because of World War I which began in 1914. Between 1914 and 1916 three of his six sons were killed in the war. Of his three remaining sons, Camille was a government minister, Édouard was a professor of history at the Sorbonne, and the third son was an engineer.

Among the honours given to Jordan was his election to the Académie des Sciences on 4 April 1881. On 12 July 1890 he became an officer of the Légion d'Honneur. He was the Honorary President of the International Congress of Mathematicians at Strasbourg in September 1920.

Finally we should note some rather confusing facts. Although given Jordan's work on matrices and the fact that the Jordan normal form is named after him, the Gauss-Jordan pivoting elimination method for solving the matrix equation $Ax = b$ is not. The Jordan of Gauss-Jordan is Wilhelm Jordan (1842 to 1899) who applied the method to finding squared errors to work on surveying.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

5.12. Problemas

1. Calcula las soluciones (en $\mathbb{Q}[x]$) del sistema de ecuaciones

$$\begin{array}{rcrcrcl} x^2\cdot Z_1 & + & x\cdot Z_2 & + & (x+1)\cdot Z_3 & = & x^2-x \\ x(x+1)\cdot Z_1 & + & (x+1)\cdot Z_2 & + & x\cdot Z_3 & = & x^2-1 \end{array}$$

   de variables Z_1, Z_2, Z_3.

2. Sean p y q números primos distintos. Calcula el número de grupos abelianos finitos desisomorfos de orden p^2q.

3. Prueba que un grupo abeliano finito que no sea cíclico contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, para un cierto entero primo p.

4. Sea G un grupo abeliano finito. Demuestra que G es cíclico si y solo si para cada n divisor del orden de G, existe un único subgrupo de G de orden n.

5. Sea G un subgrupo discreto del grupo aditivo de $\mathbb{R}^n$. Prueba que existe un número natural $r \leq n$, tal que G está generado como $\mathbb{Z}$-módulo por r vectores linealmente independientes sobre $\mathbb{R}$.

6. Clasifica el endomorfismo "multiplicar por x" sobre el espacio

$$E = k[x]/(x) \oplus k[x]/(x^3) \oplus k[x]/(x^5).$$

7. Clasifica los endomorfismos nilpotentes de un espacio vectorial de dimensión 3. Problema análogo para espacios de dimensión 4 y 5.

8. Clasifica los endomorfismos T de un espacio vectorial real E, que cumplan

   a) Anulador de $T = (x-1)^2$, $\dim E = 5$.

   b) Anulador de $T = (x^2+4)^2(x+8)^2$, $\dim E = 8$.

9. Sea E el espacio vectorial real de todos los polinomios con coeficientes reales de grado menor que 6, y sea D el operador derivada sobre E. Clasiica el endomorfismo $T = D^2$.

10. Sea $(G,+)$ un grupo finito abeliano. Prueba que G es cíclico si y solo si $n = |G|$ es el mínimo número natural (no nulo) tal que $n \cdot g = 0$ para todo $g \in G$.

11. Prueba que un grupo abeliano finito generado es cíclico si y solo si tiene un único factor invariante.

12. Sea $p(x) = \prod_{i=1}^{r}(x-\alpha_i)^{n_i} \in k[x]$, con $\alpha_i \neq \alpha_j$ para todo $i \neq j$. Consideremos el endomorfismo k-lineal

$$x\cdot\colon k[x]/(p(x)) \to k[x]/(p(x)),\ \overline{q(x)} \mapsto \overline{x\cdot q(x)}.$$

    Prueba que $\{\overline{(x-\alpha_1)^{n_1}\cdots(x-\alpha_j)^{m_j}\cdots(x-\alpha_r)^{n_r}}, \forall\, 0 \le m_j < n_j, \forall j\}$ es una base de Jordan de $x\cdot$.

13. Clasifica sobre el cuerpo racional los endomorfismos lineales

$$A = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & -1 \end{pmatrix}$$

    Da una base de Jordan, para B.

14. Mediante transformaciones elementales de la matriz característica, calcula los divisores elementales $p_i(x)^{n_{ij}}$ del endomorfismo de $\mathbb{R}^3$ de matriz

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & -2 \\ 1 & 1 & 3 \end{pmatrix}.$$

    Calcula $e_{ij} \in \mathbb{R}^3$ de modo que $\mathbb{R}^3 = \oplus_{ij}(k[x]/(p_i(x)^{n_{ij}})\cdot e_{ij}$.

15. Calcula una base de Jordan para cada uno de los endomorfismos lineales

$$A = \begin{pmatrix} -4 & 14 & 28 & -30 \\ -1 & 5 & 6 & -7 \\ -4 & 9 & 20 & -19 \\ -3 & 7 & 14 & -13 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 8 & 12 & -16 \\ 3 & -4 & -12 & 12 \\ -2 & 6 & 12 & -12 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

16. Sean $T, T' : E \to E$ dos endomorfismos lineales de un espacio vectorial de dimensión finita, de modo que en cierta base la matriz de T es la transpuesta de la de T'. Prueba que T y T' son endomorfismos equivalentes.

17. Sea A un anillo euclídeo y (a_{ij}) una matriz con coeficientes $a_{ij} \in A$. Sustituyendo de modo conveniente y sucesivo la fila F_i por la fila $F_i + b_j F_j$, $i \neq j$, $b_j \in A$ (arbitrario), demuestra que la matriz (a_{ij}) es "triangulable". Resuelve el sistema de ecuaciones diofánticas
$$7x + 5y = 1$$
$$5x + 3y = 3$$

18. Prueba que los grupos
$$(\mathbb{Z} \times \mathbb{Z})/\langle (7,5),(5,3)\rangle \text{ y } (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle (12,30,24),(4,8,6),(6,4,8)\rangle.$$
no son isomorfos.

19. Prueba que todo grupo abeliano de orden 12 está generado por dos elementos.

20. Prueba que si el polinomio característico de un endomorfismo lineal tiene todas sus raíces distintas entonces coincide con el polinomio anulador del endomorfismo.

21. Sea $T : E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Prueba que la condición necesaria y suficiente para que el endomorfismo $p(T)$ sea invertible es que $p(x)$ y $c_T(x)$ sean primos entre sí.

22. Sea $T : E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Sea $E' \subseteq E$ un subespacio estable por T. Denotemos $\bar{T} : E/E' \to E/E'$, $\bar{T}(\bar{e}) = \overline{T(e)}$, el endomorfismo inducido por T en E/E'. Prueba que
$$c_T(x) = c_{T_{|E'}}(x) \cdot c_{\bar{T}}(x).$$

23. Sea E un $\mathbb{C}$-espacio vectorial de dimensión n y T un endomorfismo de E. Sea $c_T(x) = \prod_{i=1}^{n} (x - \alpha_i)$ la descomposición en factores irreducibles del polinomio característico de T. Prueba que si $p(x)$ es un polinomio con coeficientes en $\mathbb{C}$, entonces
$$c_{p(T)}(x) = \prod_{i=1}^{n} (x - p(\alpha_i)).$$
En particular, se tiene que $\operatorname{tr}(p(T)) = \sum_{i=1}^{n} p(\alpha_i)$, $\det(p(T)) = \prod_{i=1}^{n} p(\alpha_i)$.

24. Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita. Sea $T : E \to E$ un endomorfismo $\mathbb{C}$-lineal de E. Demuestra que si $c_T(x)$ es el polinomio característico de T considerado como endomorfismo $\mathbb{C}$-lineal, entonces el polinomio característico de T considerado como endomorfismo $\mathbb{R}$-lineal es $c_T(x) \cdot \overline{c_T(x)}$ (donde $\overline{c_T(x)}$ es el conjugado de $c_T(x)$).

25. Sea $p(x) \in \mathbb{R}[x]$ un polinomio irreducible de grado 2 y $\alpha \in \mathbb{C}$ una de sus raíces. Dado $z = \lambda + \mu i$ sea $h_z = \begin{pmatrix} \lambda & -\mu \\ \mu & \lambda \end{pmatrix}$ que es la matriz de la homotecia $\mathbb{C} \to \mathbb{C}$, $z' \mapsto zz'$ en la base $\{1, i\}$. Prueba que existe una base de $\mathbb{R}[x]/(p(x)^n)$ en la que la matriz del endomorfismo $x\cdot$ es igual a

$$\begin{pmatrix} h_\alpha & h_0 & \cdots & h_0 \\ h_1 & h_\alpha & \cdots & h_0 \\ \vdots & \ddots & \ddots & \vdots \\ h_0 & \cdots & h_1 & h_\alpha \end{pmatrix}.$$

Si $\alpha = i$ y $n = 3$, calcula la matriz de $x^3\cdot$ y $e^{tx\cdot}$ en esta base.

26. Sea $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in k[x]$ un polinomio irreducible. Sea $h_{r(x)}$ la matriz del endomorfismo k-lineal $k[x]/(p(x)) \to k[x]/(p(x))$, $\overline{q(x)} \mapsto \overline{r(x)\cdot q(x)}$ en la base $\{\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}\}$. Calcula h_x. Demuestra que existe una base de $k[x]/(p(x)^m)$ en la que la matriz del endomorfismo $k[x]/(p(x)^m) \to k[x]/(p(x)^m)$, $\overline{q(x)} \mapsto \overline{x \cdot q(x)}$ es igual a

$$\begin{pmatrix} h_x & h_0 & \cdots & h_0 \\ h_1 & h_x & \cdots & h_0 \\ \vdots & \ddots & \ddots & \vdots \\ h_0 & \cdots & h_1 & h_x \end{pmatrix}.$$

27. Consideremos un sistema de ecuaciones

$$\begin{aligned} x_{n+1} &= a_{11}x_n + a_{12}y_n + a_{13}z_n \\ y_{n+1} &= a_{21}x_n + a_{22}y_n + a_{23}z_n \\ z_{n+1} &= a_{31}x_n + a_{32}y_n + a_{33}z_n \end{aligned}$$

con $a_{ij} \in \mathbb{C}$, para todo i, j. Plantéese la resolución de este sistema de ecuaciones.

Solución de los problemas

Solución de los problemas del capítulo primero

P1. a $\Rightarrow$ b. $\phi(gg') = (gg')^{-1} = g'^{-1}g^{-1} = g^{-1}g'^{-1} = \phi(g)\phi(g')$. b. $\Rightarrow$ a. Sabemos que $(gg')^{-1} = g^{-1}g'^{-1}$, luego tomando inversos, $gg' = g'g$.

a. $\Rightarrow$ c. $\phi(gg') = (gg')^2 = gg'gg' = g^2g'^2 = \phi(g)\phi(g')$. c. $\Rightarrow$ a. Como $gg'gg' = g^2g'^2$, multiplicando a la derecha por g^{-1} y por la izquierda por g'^{-1}, obtenemos $gg' = g'g$.

a. $\Rightarrow$ d. $\phi((g,g')\cdot(h,h')) = \phi(gh,g'h') = ghg'h' = gg'hh' = \phi(g,g')\cdot\phi(h,h')$. d. $\Rightarrow$ a. Como $ghg'h' = gg'hh'$ entonces $hg' = g'h$.

P2. Veamos que τ_a es un morfismo de grupos: $\tau_a(gg') = agg'a^{-1} = aga^{-1}ag'a^{-1} = \tau_a(g)\tau_a(g')$. Veamos que la aplicación inversa de τ_a es $\tau_{a^{-1}}$:

$$\tau_{a^{-1}}(\tau_a(g)) = \tau_{a^{-1}}(aga^{-1}) = a^{-1}aga^{-1}a = g,$$

e igualmente $\tau_a(\tau_{a^{-1}}(g)) = g$. Veamos que el morfismo $\tau : G \to \mathrm{Aut}(G)$, $\tau(a) := \tau_a$ es morfismo de grupos:

$$\tau(aa')(g) = \tau_{aa'}(g) = aa'g(aa')^{-1} = aa'ga'^{-1}a^{-1} = \tau_a(\tau_{a'}(g)) = \tau(a)(\tau(a')(g)),$$

luego $\tau(aa') = \tau(a)\circ\tau(a')$.

P3. Supongamos $x\cdot y \in H$, para todo $x,y \in H$. Entonces, dado $x \in H$, $x^2 \in H$, luego $x^3 \in H$, luego $x^n \in H$, para todo $n > 0$. Como H es finito, existen $n > m$ tales que $x^n = x^m$, luego $x^{n-m} = 1$ y tenemos que $1 \in H$ y $x^{-1} = x^{n-m-1} \in H$. Luego, H es subgrupo.

Si $G = \mathbb{Z}$ y $H = \mathbb{N}$, tenemos que s $x + y \in H$, para todo $x,y \in H$, pero H no es un subgrupo de G.

P4. Supongamos que $xH = H$, para todo $x \in H$. Entonces, dado $x \in H$, $x^2 \in H$, luego $x^3 \in H$, luego $x^n \in H$, para todo $n > 0$. Como H es finito, existen $n > m$ tales que $x^n = x^m$, luego $x^{n-m} = 1$ y tenemos que $1 \in H$ y $x^{-1} = x^{n-m-1} \in H$. Luego, H es subgrupo.

P5. a) $\langle 3,5\rangle = m.c.d.(3,5)\mathbb{Z} = \mathbb{Z}$.

b) $\langle(2,0),(0,5)\rangle 2\mathbb{Z}\times 5\mathbb{Z}$. $\langle(2,3),(4,5)\rangle = \langle(2,3),(0,-1)\rangle = \langle(2,0),(0,1)\rangle = 2\mathbb{Z}\times\mathbb{Z}$.

c) $(1,2,3) = (1,2)(2,3)$. En el grupo generado tenemos ya 4 elementos (contando Id), luego por el teorema de Lagrange, el grupo generado es S_3.

d) $\langle 1\rangle = \mathbb{Z}$. $\langle \frac{1}{2}\rangle = \mathbb{Z}\cdot\frac{1}{2} = \{\frac{n}{2},\ n\in\mathbb{Z}\}$. $\langle \frac{1}{6},\frac{1}{8}\rangle = \langle \frac{4}{24},\frac{3}{24}\rangle = \frac{1}{24}\cdot\langle 4,3\rangle = \frac{1}{24}\mathbb{Z}$.

P6. Por el teorema de Lagrange, el orden de todo subgrupo H de G es 1 o $p = |G|$. Por tanto, G no contiene más subrgupos que el trivial $\{1\}$ y el total. Por tanto, dado $g \neq 1$, tenemos que $\langle g\rangle = G$.

P7. Sea $g \in G$, $g \neq 1$. Tenemos que $\langle g\rangle = G$. Si $|G| = \infty$, entonces $G \simeq \mathbb{Z}$, que contiene muchos subgrupos y llegamos a contradicción. Luego, $G \simeq \mathbb{Z}/n\mathbb{Z}$. Si n no es primo, $n = mm'$, con $1 < m, m' < n$, entonces el subgrupo $\langle \bar{m}\rangle$ es de orden m' y tenemos un subgrupo que no es el trivial ni el total y llegamos a contradicción.

P8. Si $f : G \to G'$ es un isomorfismo de grupos, entonces $\mathrm{ord}(g) = \mathrm{ord}(f(g))$, para todo g. El morfismo $\tau_b : G \to G$, $\tau_b(a) = bab^{-1}$ es un isomorfismo de grupos, luego $\mathrm{ord}(a) = \mathrm{ord}(\tau(a))$. Sea $a' = ab$, entonces

$$\mathrm{ord}(ab) = \mathrm{ord}(a') = \mathrm{ord}(ba'b^{-1}) = \mathrm{ord}(ba).$$

P9. a) Dados $z, z' \in \mu_n$, entonces $zz' \in \mu_n$, porque $(zz')^n = z^n z'^n = 1\cdot 1 = 1$. También, $z^{-1} \in \mu_n$, porque $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$.

b) μ_n está generado por $e^{\frac{2\pi i}{n}}$, que tiene orden n.

P10. El morfismo $\phi\colon \mathrm{Ker}\,\pi \times G' \to G$, $\phi(k,g') := k\cdot s(g')$ es un isomorfismo. Si $(k,g') \in \mathrm{Ker}\,\phi$, entonces $\phi(k,g') = 1$, entonces $k\cdot s(g') = 1$, tomando π, $1 = \pi(k)\cdot\pi s(g') = 1\cdot g'$, luego $g' = 1$ y $k = 1$. Entonces, $(k,g') = 1$ y ϕ es inyectiva. Dado $g \in G$, entonces $(s\pi(g))^{-1} \in \mathrm{Ker}\,\pi$ y $\phi(g\cdot(s\pi(g))^{-1}, \pi(g)) = g$. Luego, ϕ es epiyectiva.

P11. Salvo notaciones es el mismo problema que el anterior.

P12. Sea $G = \mathbb{Z}/n\mathbb{Z}$. Todo subgrupo $H \subset G$ es cíclico. Luego, $H = \langle \bar{m}\rangle$ (donde $0 \leq m < n$). El orden d de H, que es el de $\bar{m}$, divide al orden de G, que es n. Sea $m' := \frac{n}{d} \in \mathbb{N}$. Entonces, $d\cdot\bar{m} = \bar{0}$, es decir, $d\cdot m = r\cdot n$, para cierto $r > 0$, y $m = r\cdot m'$. Por tanto, $H \subseteq \langle \bar{m'}\rangle$. Como el subgrupo de G generado por $\bar{m'}$ es de orden d, $H = \langle \bar{m'}\rangle$.

P13. Si $F((1,2)) = 1$, entonces $F((i,j)) = F(\tau\cdot(1,2)\cdot\tau^{-1}) = F(\tau)\cdot F((1,2))\cdot F(\tau)^{-1} = 1$ (donde τ es una permuatción que cumple que $\tau(1) = i$ y $\tau(2) = j$). Como toda permutación es producto de transposiciones, tendremos que $F(\sigma) = 1$, para toda σ).

Si $F((1,2)) = -1$, entonces $F((i,j)) = F(\tau\cdot(1,2)\cdot\tau^{-1}) = F(\tau)\cdot F((1,2))\cdot F(\tau)^{-1} = -1 = \mathrm{sign}(i,j)$ (donde τ es una permuatción que cumple que $\tau(1) = i$ y $\tau(2) = j$). Como toda permutación es producto de transposiciones, tendremos que $F(\sigma) = \mathrm{sign}(\sigma)$, para toda σ.

P14. Si τ es una transposición, entonces el orden de $F(\tau)$ divide a 2 y al orden de G, luego es 1, es decir, $F(\tau) = 1$. Como toda permutación $\sigma \in S_n$ es producto de transposiciones, entonces $F(\sigma) = 1$.

P15. Es claro que $\det(\tilde{(1,2)}) = -1 = \operatorname{sign}(1,2)$. Dado (i,j) y una permutación τ tal que $\tau(1) = i$ y $\tau(2) = j$, tenemos que $(i,j) = \tau\cdot(1,2)\cdot\tau^{-1}$ y $\tilde{(i,j)} = \tilde{\tau}\tilde{(1,2)}\tilde{\tau}^{-1}$. Por tanto, $\det(\tilde{(i,j)}) = \det(\tilde{(1,2)}) = \operatorname{sign}(1,2) = \operatorname{sign}(i,j)$. Como toda permutación es producto de transposiciones, tenemos que $\det(\tilde{\sigma}) = \operatorname{sign}(\sigma)$, para todo σ. De otro modo: utílicese el problema 13.

P16. Escribamos $\sigma \in A_n$ como producto de transposiciones $\sigma = t_1 \circ \cdots \circ t_n$. Como $1 = \operatorname{sign}(\sigma) = (-1)^n$ n es par. Basta ver que el producto de dos transposiciones (que es un elemento de A_n) es igual a un producto de tres ciclos. En efecto, $(a,b)(b,c) = (a,b,c)$ (a,b,c distintos) y $(a,b)(c,d) = (a,b)(b,c)(b,c)(c,d) = (a,b,c)(b,c,d)$, cuando a,b,c,d son distintos.

Solución de los problemas del capítulo segundo

P1. Sea $f\colon \mathbb{Z} \to \mathbb{Z}$ un morfismo de anillos. Tenemos que $f(1) = 1$, luego $f(2) = f(1+1) = f(1) + f(1) = 1 + 1 =: 2$,..., $f(n) = n$, para todo $n \in \mathbb{N}$ y por tanto $f(-n) = -n$ para todo $n \in \mathbb{N}$. Es decir, $f = \mathrm{Id}$.

Sea $f\colon \mathbb{Q} \to \mathbb{Q}$ un morfismo de anillos. $f_{|\mathbb{Z}} = \mathrm{Id}_{|\mathbb{Z}}$. Entonces, $f(\frac{n}{m}) = f(n\cdot m^{-1}) = n\cdot m^{-1} = \frac{n}{m}$ y $f = \mathrm{Id}$.

Sea $f\colon \mathbb{R} \to \mathbb{R}$ un morfismo de anillos. De nuevo, $f_{|\mathbb{Q}} = \mathrm{Id}_{|\mathbb{Q}}$. Dado $r > 0$, tenemos que $r = s^2$, para un $s > 0$. Entonces, $f(r) = f(s)^2 > 0$. Si $r > s$ entonces $r - s > 0$, luego $f(r) - f(s) = f(r-s) > 0$ y $f(r) > f(s)$. Dado $r \in \mathbb{R}$, sean $q_1, q_2 \in \mathbb{Q}$ tales que $q_1 < r < q_2$, entonces $q_1 = f(q_1) < f(r) < f(q_2) = q_2$. Por tanto, $f(r) = r$ y $f = \mathrm{Id}$.

P2. Observemos que dado $p(x) \in A[x]$ existen un polinomio único $q(x) \in A[x]$ y $b \in A$ tales que $p(x) = q(x)\cdot(x-a) + b$. Por tanto, $p(a) = 0$ si y solo si $b = 0$, es decir, $p(x) \in (x-a)$. Consideremos el epimorfismo $\pi\colon A[x] \to A$, $\pi(p(x)) := p(a)$. Tenemos que $\operatorname{Ker}\pi = (x-a)$, luego por el teorema de isomorfía, $A[x]/(x-a) \simeq A$.

P3. Por el teorema chino de los restos

$$\begin{aligned}\mathbb{R}[x]/((x^2+1)\cdot(x^2-1)) &= \mathbb{R}[x]/(x^2+1) \times \mathbb{R}[x]/(x^2-1)\\ &= \mathbb{R}[x]/(x^2+1) \times \mathbb{R}[x]/(x-1) \times \mathbb{R}[x]/(x+1) = \mathbb{C}\times\mathbb{R}\times\mathbb{R}.\end{aligned}$$

P4. a) Calculemos $t(x) = \sum_i^n b_i x^i$, tal que $1 = s(x)\cdot b(x) = \sum_i^{n=0} \sum_{i+j=n} a_i b_j x^n$. Luego, $b_0 = a_0^{-1}$ (luego a_0 ha de ser invertible. Además, $0 = \sum_{i+j=n} a_i b_j$, para $n > 0$,es decir, $b_n = -\frac{a_0}{\sum_{j=0}^{n-1} a_{n-j} b_j}$ y argumentando por recurrencia fácilmente concluimos.

b) El morfismo es claramente epiyectivo e inyectivo.

P5. Sabemos que $I \times J$ es un subgrupo de $A \times B$, con la operación $+$. Dado $(i,j) \in I \times J$ y $(a,b) \in A \times B$, entonces $(a,b)\cdot(i,j) = (ai, bj) \in I \times J$. El núcleo del epimorfismo $A \times B \to A/I \times B/J$, $(a,b) \mapsto (\bar{a}, \bar{b})$ es $I \times J$. Luego, $(A \times B)/I \times J = A/I \times B/J$.

P6. Trabajemos en $\mathbb{Z}/7\mathbb{Z}$. Entonces, el número n es divisible por 7 si y solo si $0=\bar{n}=\overline{n_r n_{r-1}\dots n_1\cdot 10+n_0}=\overline{n_r n_{r-1}\dots n_1}\cdot\bar{3}+\bar{n}_0$. Observemos que $\bar{3}^{-1}=-\bar{2}$. Luego,

$$0=\overline{n_r n_{r-1}\dots n_1}\cdot\bar{3}+\bar{n}_0 \iff 0=(-\bar{2})\cdot(\overline{n_r n_{r-1}\dots n_1}\cdot\bar{3}+\bar{n}_0)=\overline{n_r n_{r-1}\dots n_1}-\bar{2}\cdot\bar{n}_0$$
$$=\overline{n_r n_{r-1}\dots n_1-2\cdot n_0}$$

Es decir, n es divisible por 7 si y solo si $n_r n_{r-1}\dots n_1-2\cdot n_0$ es divisible por 7.

P7. Trabajemos en $\mathbb{Z}/13\mathbb{Z}$. Entonces, el número n es divisible por 13 si y solo si $0=\bar{n}=\overline{n_r n_{r-1}\dots n_1\cdot 10+n_0}=\overline{n_r n_{r-1}\dots n_1}\cdot(-\bar{3})+\bar{n}_0$. Observemos que $-\bar{3}\cdot\bar{4}=\bar{1}$. Luego,

$$0=\overline{n_r n_{r-1}\dots n_1}\cdot(-\bar{3})+\bar{n}_0 \overset{\bar{4}\cdot}{\iff} 0=\overline{n_r n_{r-1}\dots n_1}+\bar{4}\cdot\bar{n}_0$$
$$=\overline{n_r n_{r-1}\dots n_1+4\cdot n_0}$$

Es decir, n es divisible por 13 si y solo si $n_r n_{r-1}\dots n_1+4\cdot n_0$ es divisible por 13.

P8. Observemos que $x^3-1=(x-1)(x^2+x+1)$. Luego las raíces de x^2+x+1 son $e^{\frac{2\pi i}{3}}$ y $e^{\frac{4\pi i}{3}}$. Sea

$$\delta\colon \mathbb{Z}[e^{\frac{2\pi i}{3}}]\to\mathbb{N},\ \delta(a+be^{\frac{2\pi i}{3}}):=(a+be^{\frac{2\pi i}{3}})\cdot(a+be^{\frac{4\pi i}{3}})=a^2+b^2-ab.$$

Para probar que $(\mathbb{Z}[e^{\frac{2\pi i}{3}}],\delta)$ es un anillo euclídeo se procede del mismo modo con el que hemos probado que el anillo de los enteros de Gauss es euclídeo.

P9. Tenemos que $a=bc$. Por tanto, $\delta(a)\geq\delta(b)$. Si c es invertible (es decir, $(a)=(b)$) entonces $b=a\cdot c^{-1}$ y $\delta(b)\geq\delta(a)$, luego $\delta(a)=\delta(b)$. Si $\delta(a)=\delta(b)$, entonces $b=a\cdot d+r$, con $r=0$ ó $\delta(r)<\delta(a)=\delta(b)$. Entonces, $b=b\cdot c\cdot d+r$ y $r=b\cdot(1-c\cdot d)$. Por tanto, $r=0$ porque si no $\delta(r)\geq\delta(b)$. En conclusión, $1-c\cdot d=0$, luego c es invertible (es decir, $(a)=(b)$).

P10. Si $a=bc$, con b y c propios, entonces $\delta(b)<\delta(a)$ y llegamos a contradicción.

P11. Tenemos que $\delta(ab)=\min\{\delta'(abc),c\in A\setminus\{0\}\}\geq\min\{\delta'(ad),d\in A\setminus\{0\}\}=\delta(a)$. Sean $a,b\in A$, y sea s tal que $\delta(b)=\delta'(bs)$. Sean c',r' tales que $as=c'bs+r'$, con $\delta'(r')<\delta'(bs)$ ó $r'=0$. Sea r tal que $r'=rs$. Tenemos que $a=c'b+r$ y $\delta(r)\leq\delta'(r')<\delta'(bs)=\delta(b)$ ó $r=0$.

P12. Son comprobaciones sencillas.

P13. La primera afirmación ha sido probada en la demostración del teorema 2.4.3.

Dado $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n$ sea $|\alpha|=\alpha_1+\dots+\alpha_n$ y dado $p(x)=\sum_\alpha\lambda_\alpha x^\alpha\in k[x_1,\dots,x_n]$ sea $\mathrm{gr}(p(x))=\max\{|\alpha|:\lambda_\alpha\neq 0\}$. Toda cadena ascendente de ideales $(p_1(x))\subset(p_2(x))\subset\dots\subset(p_n(x))\subset\dots$ estabiliza porque $\mathrm{gr}(p_1(x))\geq\mathrm{gr}(p_2(x))\geq\dots\geq\mathrm{gr}(p_n(x))$ y $\mathrm{gr}(p_i(x))=\mathrm{gr}(p_{i+1}(x))$ si y solo si $(p_i(x))=(p_{i+1}(x))$. Para $s(x)=\sum_\alpha\lambda_\alpha x^\alpha\in k[[x_1,\dots,x_n]]$ define $\mathrm{gr}(s(x))=\min\{|\alpha|:\lambda_\alpha\neq 0\}$ y demuestra que toda cadena ascendente de ideales $(s_1(x))\subset(s_2(x))\subset\dots\subset(s_n(x))\subset\dots$ de $k[[x_1,\dots,x_n]]$ estabiliza.

P14. Dado $p(x) \in k[x_1,\dots,x_n,\dots] =: A$ sea $n \in \mathbb{N}$, tal que $p(x) \in k[x_1,\dots,x_n] = B$. Si $p(x)$ es reducible en A, entonces es reducible en B (al lector). Por el lema de Gauss, B es DFU, luego A también. A no es noetheriano, porque el ideal $(x_1,\dots,x_n,\dots)$ no es finito generado, como el lector puede comprobar.

P15. 1. Probemos que si A no es íntegro entonces $A = A_1 \times A_2$, donde A_1 es DIP ó $A_1 = B/(p^n)$, con $(p) \subset B$ maximal: a) Si existe una inclusión de ideales primos $(p) \subsetneq (q)$, entonces $p = qa = qpb$ y $p(1-qb) = 0$. Denotemos $\mathrm{Anul}(p) := \{a \in A : ap = 0\}$, entonces $1-qb \in \mathrm{Anul}(p)$ y $1-qb \notin (q)$. Por tanto, $(p, \mathrm{Anul}(p)) = A$ y por el teorema chino de los restos $A = A/(p) \times A/\mathrm{Anul}(p)$. b) Podemos suponer que todo ideal primo (p) es maximal. Sea p primo divisor de cero. Como nuestro anillo es noetheriano, la cadena $\mathrm{Anul}(p) \subseteq \mathrm{Anul}(p^2) \subseteq \cdots \subseteq \mathrm{Anul}(p^n) \subseteq \cdots$ estabiliza. Sea n, tal que $(a_n) := \mathrm{Anul}(p^n) = \mathrm{Anul}(p^{n+1}) =: (a_{n+1})$. Si $\mathrm{Anul}(p^n) \not\subseteq (p)$. entonces $(p^n, \mathrm{Anul}(p^n)) = A$ y por el teorema chino de los restos $A = A/(p^n) \times A/\mathrm{Anul}(p^n)$. Si $\mathrm{Anul}(p^n) \subseteq (p)$, entonces $a_n = pb$, entonces $(b) \subset (a_{n+1})$, luego $(a_n) = (p)(b) \subseteq (p)(a_{n+1}) \subseteq (a_n)$. Por tanto, $(a_n) = (p)(a_{n+1}) = (p)(a_n)$ y

$$(a_n) = (p)(a_n) = \cdots = (p^n)(a_n) = (0)$$

Lo cual es absurdo porque p es divisor de cero, luego $a_n \neq 0$.

2. Si A es íntegro hemos terminado. Si A no es íntegro entonces $A = A_1 \times A_2$, con A_1 DIP ó $A_1 = B_1/(p^n)$ ($(p) \subset B$ maximal). Si A_2 no es cero y no es íntegro, entonces $A_2 = A_{21} \times A_{22}$ con con A_2 DIP ó $A_2 = B_2/(q^n)$ ($(q) \subset B_2$ maximal) y $A = A_1 \times A_{21} \times A_{22}$. Este proceso ha de terminar en un número finito de pasos (y así demostramos lo que nos piden). Si no termina tenemos la cadena infinita de inclusiones de ideales de A,

$$A_1 \times \{0\} \subsetneq A_1 \times A_{21} \times \{0\} \subsetneq A_1 \times A_{21} \times A_{31} \times \{0\} \subsetneq \cdots$$

Imposible, porque A es noetheriano.

P16. Sea $\frac{a}{b} \in \mathbb{Q}$, que podemos suponer irreducible (es decir, a y b primos entre sí), tal que $(\frac{a}{b})^2 = 2$, entonces $a^2 = 2b^2$. Entonces 2 divide á a, $a = 2a'$ y $2a' = b$, luego divide también a b, hemos llegado a contradicción. No existe $\frac{a}{b}$ tal que $(\frac{a}{b})^2 = 2$.

P17. Por el algoritmo de Euclides, obtenemos que x^2+1 es el máximo común divisor de ambos polinomios. Tenemos $x^4+x^3+x-1 = (x^2+1)\cdot(x^2+x-1)$. Luego, el mínimo común múltiplo es $(x^2+x-1)\cdot(x^4+x^3+2x^2+x+1)$.

P18. Lo calculamos por el algoritmo de Euclides. Tenemos que $\frac{6}{-1+3i} = \frac{6\cdot(-1-3i)}{(-1+3i)\cdot(-1-3i)} = \frac{-6}{10} - \frac{18}{10}\cdot i$ y $-1-2i$ es el entero de Gauss más cercano. Tenemos que

$$6 = (-1+3i)\cdot(-1-2i) + (-1+i).$$

Tenemos que $\frac{-1+3i}{-1+i} = \frac{(-1+3i)(-1-i)}{(-1+i)(-1-i)} = \frac{4-2i}{2} = 2-i$, luego $-1+i$ es el másximo común divisor buscado.

P19. Tenemos

$$\begin{matrix} 2x+4y+3z=6 \\ 4x+6y+3z=4 \end{matrix} \equiv \begin{matrix} 4x+8y+6z=12 \\ 4x+6y+3z=4 \end{matrix} \equiv \begin{matrix} 4x+8y+6z=12 \\ -2y-3z=-8 \end{matrix}$$

Las soluciones de $-2y-3z=-8$ son $y=-8+3n$ y $z=8-2n$. Entonces,

$$12=4x+8y+6z\equiv 6=2x+4y+3z=2x+4(-8+3n)+3(8-2n)=2x+6n-8$$

y las soluciones de $6=2x+6n-8$, son las de $14=2x+6n$, que son $x=7-3m$ y $n=m$. En conclusión, $x=7-3m$, $y=-8+3m$ y $z=8-2m$.

P20. $N(z\cdot z')=N(z)\cdot N(z')$ porque el conjugado de un producto de números complejos es igual al producto de los conjugados. Si $N(a+b\sqrt{-5})=a^2+5b^2=1$ entonces $a=\pm 1$ y $b=0$. Si $2=z\cdot z'$ y z y z' no son invertibles, entonces $4=N(2)=N(z)\cdot N(z')$ y por tanto $N(z)=N(z')=2$ lo cual es imposible, como es fácil de comprobar. El resto del problema al lector.

P21. Observemos que c es un isomorfismo de anillos porque es la composición de los isomorfismos $\mathbb{C}[z,1/z]\to\mathbb{C}[z,1/z]$, $\sum_i a_i z^i \mapsto \sum_i \bar{a}_i z^i$, $\sum_i a_i z^{-i}$.

a) Es claro que $\mathbb{C}[z,1/z]^c=\{a_0z^n+a_1z^{n-1}+\cdots+a_{n-1}z+a_n+\bar{a}_{n+1}z^{-1}+\cdots+\bar{a}_{2n}z^{-n}$, con $a_n\in\mathbb{R}\}$. Dejamos que el lector pruebe que los polinomios con coeficientes complejos que cumplen que si α es una raíz de multiplicidad r, entonces $1/\bar{\alpha}$ es raíz de multiplicidad r, son los polinomios de la forma $a_0z^{2n}+a_1z^{2n-1}+\cdots+a_{n-1}zn-1+a_nz^n+\bar{a}_{n-1}z^{n-1}+\cdots+\bar{a}_{2n}$, con $a_n\in\mathbb{R}$, multiplicados por una constante.

b) Por cada raíz $\alpha\in\mathbb{C}$, con $\alpha\neq 1/\bar{\alpha}$ (es decir, $|\alpha|^2=\alpha\cdot\bar{\alpha}\neq 1$) de $p(z)$, tenemos que $p(z)=\frac{1}{\alpha+1/\bar{\alpha}}\cdot\frac{(z-\alpha)\cdot(z-1/\bar{\alpha})}{z}\cdot\frac{q(z)}{z^{n-1}}$, con $q(z)/z^{n-1}\in\mathbb{C}[z,1/z]^c$. Por cada raíz α con $\alpha=\bar{1}/\bar{\alpha}$ (es decir, $|\alpha|=1$) de $p(z)$ ha de existir otra raíz β de $p(z)$ tal que $\beta=1/\bar{\beta}$ (porque el grado de $p(z)$ es par) y $p(z)=\frac{1}{\alpha+\beta}\cdot\frac{(z-\alpha)\cdot(z-\beta)}{z}\cdot\frac{q(z)}{z^{n-1}}$, con $q(z)/z^{n-1}\in\mathbb{C}[z,1/z]^c$. Observemos que $(\frac{(z-\alpha)\cdot(z-\beta)}{z})\cdot(\frac{(z-\alpha)\cdot(z-\beta}{z})=(\frac{(z-\alpha)\cdot(z-\alpha)}{z})\cdot(\frac{(z-\beta)\cdot(z-\beta)}{z})$. Con todo es fácil concluir.

c) Vía la igualdad $\mathbb{C}[z,1/z]=\mathbb{C}[x,y]/(x^2+y^2-1)$, c en $\mathbb{C}[x,y]/(x^2+y^2-1)$ es igual a $c(\overline{a_{nm}x^ny^m})=\bar{a}_{nm}x^ny^m$, luego

$$\begin{aligned}\mathbb{C}[z,1/z]^c&=(\mathbb{C}[x,y]/(x^2+y^2-1))^c=(\mathbb{R}[x,y]/(x^2+y^2-1)\oplus\mathbb{R}[x,y]/(x^2+y^2-1)\cdot i)^c\\&=\mathbb{R}[x,y]/(x^2+y^2-1).\end{aligned}$$

Dado $\alpha=a+bi$ el irreducible $\frac{1}{\alpha+1/\bar{\alpha}}\cdot\frac{(z-\alpha)\cdot(z-1/\bar{\alpha})}{z}$ es igual a $\frac{2}{1+a^2+b^2}(ax+by)-1$ (la recta $ax+by-\frac{1+a^2+b^2}{2}=0$ no corta con $x^2+y^2-1=0$ si $a^2+b^2\neq 1$, y corta tangentemente a la circunferencia en (a,b) si $a^2+b^2=1$). Sean $\alpha=a+bi$ y $\beta=a'+b'i$ de módulo 1. El irreducible $\frac{1}{\alpha+\beta}\frac{(z-\alpha)\cdot(z-\beta)}{z}$ es igual al irreducible $\lambda^{-1}\cdot(\frac{x-a}{a'-a}-\frac{y-b}{b'-b})$ (con $\lambda=\frac{a}{a'-a}-\frac{b}{b'-b}$).

P22. Buscamos $\bar{\lambda}$ tal que $\bar{\lambda}\cdot\bar{7}=\bar{1}$, es decir, λ del modo que exista μ tal que $\lambda\cdot 7=1+\mu\cdot 982$. Es decir, $\lambda\cdot 7+(-\mu)\cdot 982=1$. Efectivamente, 7 y 982 son primos entre sí y λ y $-\mu$ se calculan con el algoritmo de Euclídes...$\lambda=421$.

P23. Tenemos que $1+x+x^2$ y x^3-2 son primos entre sí. Con el algoritmo de Euclídes obtenemos que

$$(x-1)(x^2+x+1)-(x^3-2)=1.$$

Luego, $\overline{1+x+x^2}^{-1}=\overline{x-1}$. Consideremos el epimorfismo $\mathbb{Q}[x]/(x^3-2)\to\mathbb{Q}[\sqrt[3]{2}]$, $\overline{p(x)}\mapsto p(\sqrt[3]{2})$ (de hecho es un isomorfismo). Por un morfismo de anillos los inversos se aplican en inversos. Luego, como $\overline{1+x+x^2}^{-1}=\overline{x-1}$, entonces $(1+\sqrt[3]{2}+(\sqrt[3]{2})^2)^{-1}=\sqrt[3]{2}-1$.

P24. Tenemos que resolver el sistema de ecuaciones $p(x,y)=x^2+y^2-1=0$, $q(x,y)=x^3+y^3-1=0$. Consideremos estos polinomios como polinomios en la variable y con coeficientes en $\mathbb{C}(x)$. Calculemos primero mediante el algoritmo de Euclides, polinomios $a(y),b(y)\in\mathbb{C}(x)[y]$ tales que $a(y)\cdot p(x,y)+b(y)\cdot q(x,y)=1$ (con $\operatorname{gr}a(y)<3$ y $\operatorname{gr}b(y)<2$). Después calculemos el polinomio de grado mínimo $h(x)\in\mathbb{C}[x]$ tal que $a'(x,y)=h(x)\cdot a(y), b'(x,y)=h(x)\cdot b(y)\in\mathbb{C}[x,y]$. Tendremos que $a'(x,y)\cdot p(x,y)+b'(x,y)\cdot q(x,y)=h(x)$. Si (α,β) es una solución del sistema, entonces $h(\alpha)=0$. Recíprocamente, si $h(\alpha)=0$ entonces $a'(\alpha,y)p(\alpha,y)+b'(\alpha,y)q(\alpha,y)=0$. Por la minimalidad de $h(x)$, podemos suponer que $a'(\alpha,y)\neq 0$ (o que $b'(\alpha,y)\neq 0$). Entonces, los polinomios $p(\alpha,y)$ y $q(\alpha,y)$ de grados dos y tres, tienen raíces comunes, y las raíces β del $m.c.d.(p(\alpha,y),q(\alpha,y)$ cumplen que $p(\alpha,\beta)=q(\alpha,\beta)=0$.

P25. Sea $\tau\in\operatorname{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z})$ y denotemos $\bar{m}=\tau(\bar{1})$. Se cumple que

$$\tau(\bar{i})=\tau(\bar{1}+\overset{i}{\cdots}+\bar{1})=\tau(\bar{1})+\overset{i}{\cdots}+\tau(\bar{1})=i\cdot\bar{m}=h_{\bar{m}}(\bar{i}),$$

es decir, $\tau=h_{\bar{m}}$ es una homotecia. Luego, $\mathbb{Z}/n\mathbb{Z}=\operatorname{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z})$, $\bar{m}\mapsto h_{\bar{m}}$.

Como $h_{\bar{m}\cdot\bar{m}'}=h_{\bar{m}}\circ h_{\bar{m}'}$, los invertibles (con el producto) de $\mathbb{Z}/n\mathbb{Z}$ se identifican con los invertibles de $\operatorname{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z})$ con la composición.

P26. Observemos que $A[x,y]=A[x][y]$. Dado $p(x,y)\in A[x,y]$ considerémoslo como un polinomio en y con coeficientes en $A[x]$. Dividamos por $y-x$, entonces $p(x,y)=(y-x)\cdot c(x,y)+r(x)$. Por tanto, si $p(x,x)=0$ entonces $r(x)=0$ y $p(x,y)\in(y-x)$.

El núcleo del epimorfismo $A[x,y]\to A[x]$, $p(x,y)\mapsto p(x,x)$, es el ideal $(y-x)$. Por el teorema de isomorfía $A[x,y]/(y-x)=A[x]$.

P27. Denotemos el determinante por $p(x_1,\dots,x_n)$. Observemos que

$$p(x_1,\dots,\underset{j}{x_i},\dots,\underset{i}{x_i},\dots,x_n)=0,$$

para $i>j$. Por lo tanto, $p(x_1,\dots,x_n)=(x_n-x_{n-1})\cdot q(x_1,\dots,x_n)$. Observemos que $q(x_1,\dots,x_n,x_{n-1},x_n)=0$, luego $p(x_1,\dots,x_n)=(x_n-x_{n-1})(x_n-x_{n-2})\cdot h(x_1,\dots,x_n)$. Recurrentemente, $p(x_1,\dots,x_n)$ es múltiplo de $\prod_{i>j}(x_i-x_j)$. Ambos son polinomios homogéneos de grado $\frac{n\cdot(n-1)}{2}$. Luego, son iguales salvo multiplicación por un número racional. El coeficiente que acompaña al monomio $x_n^{n-1}x_{n-1}^{n-2}\cdots x_2$ es el 1 en ambos polinomios, luego son iguales.

P28. Observemos que $504 = 7\cdot 8\cdot 9$. Basta probar que $n^3(n^3-1)(n^3+1) = n^3(n^6-1)$ es divisible por 7,9 y 8. Por el teorema de Fermat, sabemos que si n no es divisible por 7 entonces n^6-1 es divisible por 7. Por la congruencia de Euler sabemos que si n no es divisible por 3 entonces $n^6-1 = n^{\phi(9)}-1$ es divisible por 9. Si n es divisible por 3, n^3 es divisible por 9. Por último, si n es par, entonces n^3 es divisible por 8, si n es impar, entonces $n^3-1 = 2\cdot m$ es par y $n^3+1 = 2\cdot m+2$, luego $(n^3-1)\cdot(n^3+1) = (2\cdot m)\cdot(2\cdot m+2) = 4\cdot m\cdot(m+1)$ que es múltiplo de 8.

P29. Observemos que $\phi(1147) = \phi(31)\cdot\phi(37) = 30\cdot 36$ es primo con 73. Por tanto, existen λ y μ, que sabemos calcular por el algoritmo de Euclides, de modo que $\lambda\cdot 73+\mu\cdot\phi(1147) = 1$. Luego, $n^{\lambda\cdot 73} = n \mod 1147$. Por tanto, $\mathbb{Z}/1147\mathbb{Z} \to \mathbb{Z}/1147$, $\bar{n}\mapsto \bar{n}^{\lambda}$ es la aplicación inversa buscada.

P30. $17^{2023} = 0 \mod 17^2$ y $17^{2023} = 17^{6\cdot 337+1} = 17 \mod 7 = 3 \mod 7$. Por el algoritmo de Euclides obtenemos $1 = 124\cdot 7 - 3\cdot 17^2$. El morfismo $\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/17^2\mathbb{Z}\to\mathbb{Z}/7\cdot 17^2\mathbb{Z}$, $(\bar{n},\bar{m})\mapsto -3\cdot 17^2\cdot n+124\cdot 7\cdot m$ es inverso del morfismo $\mathbb{Z}/7\cdot 17^2\mathbb{Z}\to\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/17^2\mathbb{Z}$, $\bar{r}\mapsto(\bar{r},\bar{r})$, Luego, $17^{2023} = 124\cdot 7\cdot 3 \mod 2023 = 581 \mod 2023$.

P31. Sea $\mathbb{F}_p^{*2} = \{c^2, c\in\mathbb{F}_p^*\}$, $(p\neq 2)$. El núcleo del epimorfismo $\mathbb{F}_p^*\to\mathbb{F}_p^{*2}$, $c\mapsto c^2$ es $\{\pm 1\}$. Por tanto, $|\mathbb{F}_p^{*2}| = (p-1)/2$. Luego, $\mathbb{F}_p^{*2}$ es un subgrupo de $\mathbb{F}_p^*$ de índice 2 y coincide con el núcleo del epimorfismo $\mathbb{F}_p^*\to\{\pm 1\}$, $c\mapsto c^{\frac{p-1}{2}}$ (para probar que es un epimorfismo úsese que $x^{\frac{p-1}{2}}-1\in\mathbb{F}_p[x]$ tiene a lo más $\frac{p-1}{2}$ raíces en $\mathbb{F}_p$).

P32. Si $p = a^2+b^2$ entonces $p = (a+bi)\cdot(a-bi)$ y p no es irreducible en $\mathbb{Z}[i]$. Recíprocamente, si $p = z\cdot z'$, con $z,z'\in\mathbb{Z}[i]$ y no invertibles, entonces $p^2 = \delta(p) = \delta(z)\cdot\delta(z')$, luego $p = \delta(z) = \delta(z')$ (si $\delta(z) = 1$, entonces z sería uno de los invertibles $\pm 1,\pm i$), luego $p = a^2+b^2$ (donde $z = a+bi$).

Veamos cuándo el número primo p es irreducible en $\mathbb{Z}[i]$. Que p sea irreducible equivale a que $\mathbb{Z}[i]/(p)$ sea cuerpo. Denotemos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ y observemos que $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$. Entonces, $\mathbb{Z}[i]/(p) = \mathbb{F}_p[x]/(x^2+1)$ es cuerpo si y solo si x^2+1 no tiene raíces en $\mathbb{F}_p$, es decir, -1 no es un resto cuadrático módulo p.

Por el problema 31, $-1\in\mathbb{F}_p^{*2}$ si y solo si $(-1)^{\frac{p-1}{2}} = 1$ (o $p=2$), que equivale a que $\frac{p-1}{2}$ sea par, que equivale a que $p\equiv 1 \mod 4$. Con todo, p es irreducible en $\mathbb{Z}[i]$ si y solo si $p\equiv 3 \mod 4$.

En conclusión, un número primo $p\in\mathbb{Z}$ descompone en suma de dos cuadrados perfectos si y solo si $p\equiv 1 \mod 4$ ó $p = 2$.

P33. $\Rightarrow$) Podemos suponer $m>0$. Tenemos que $(b-1)\cdot(b+1) = b^2-1$ es múltiplo de a^m. Si $b-1$ y $b+1$ no son múltiplos de a^m, entonces $b-1$ y $b+1$ son múltiplos de a y su suma $2b$ es múltiplo de a, luego b es múltiplo de a y es imposible porque $b^2 = 1 \mod a^m$. En conclusión, $b-1$ o $b+1$ es múltiplo de a^m.

P34. Tenemos que calcular los enteros de Gauss $a+bi\in\mathbb{Z}[i]$, tales que $\delta(a+bi) = (a+bi)(a-bi) = a^2+b^2 = 2178 = 2\cdot 3^2\cdot 11^2$. Observemos que $3,11 = 3 \mod 4$,

luego son primos en $\mathbb{Z}[i]$ y han de dividir a $a+bi$, es decir, $a+bi = 3\cdot 11\cdot(a'+b'i)$ y $\delta(a'+b'i)=2$. Por tanto, $\{(a',b') = (1,1),(-1,-1),(-1,1),(1,-1)\}$ y

$$\{(a,b) = (33,33),(-33,-33),(-33,33),(33,-33)\}.$$

P35. La aplicación $A_S \times A_S \to A_S$, $(\frac{a}{s},\frac{a'}{s'}) \mapsto \frac{s'a+sa'}{ss'}$ esta bien definida porque la aplicación $\varphi\colon A\times S\times A\times S \to A_S$, $\varphi(a,s,a',s') := \frac{s'a+sa'}{ss'}$ cumple que

$$\varphi(ta,ts,t'a',t's') = \frac{t's'ta+tst'a'}{tst's'} = \frac{s'a+sa'}{ss'} = \varphi(a,s,a',t').$$

P36. $\Rightarrow$) Definamos $g(\frac{a}{s}) := f(a)\cdot f(s)^{-1}$. $\Leftarrow$) $f(s)^{-1} = g(\frac{s}{1})^{-1} = g(\frac{1}{s})$.

P37. Consideremos el morfismo $i\colon A_S \to A_{S\cdot S'}$, $i(\frac{a}{s}) := \frac{a}{s}$. El inverso de $i(s') = \frac{s'}{1}$ es $\frac{1}{s'}$, tenemos pues el morfismo $(A_S)_{S'} \to A_{S\cdot S'}$, $\frac{\frac{a}{s}}{s'} \mapsto \frac{a}{s}\cdot\frac{1}{s'} = \frac{a}{s\cdot s'}$.

El morfismo $A_{S\cdot S'} \to (A_S)_{S'}$, $\frac{a}{s\cdot s'} \mapsto \frac{\frac{a}{s}}{s'}$ es el inverso del anterior.

P38. 1. En efecto, $\frac{a}{1}\cdot\frac{b}{s} = \frac{1}{1}$.

2. $\frac{p}{1}$ no es invertible, porque si $\frac{p}{1}\cdot\frac{a}{s} = \frac{1}{1}$, entonces $pa = s$. Si $\frac{a_1}{s_1}.\frac{a_2}{s_2} = \frac{p}{1}.\frac{a_0}{s_0}$, entonces $a_1a_2s_0 = ps_1s_2$. Luego, $a_1 = p\cdot a_1'$ (ó $a_2 = p\cdot a_2'$). Luego, $\frac{a_1}{s_1} = \frac{p}{1}\cdot\frac{a_1'}{s_1}$ (ó $\frac{a_2}{s_2} = \frac{p}{1}\cdot\frac{a_2'}{s_2}$).

3. Sea $\frac{a}{s}\in A_S$ y escribamos $a = p_1\cdots p_r\cdots p_{r+1}\cdots p_n$ como producto de primos, donde p_i divide a algún elemento de S si y solo si $i>r$. Entonces, $\frac{a}{s} = \frac{p_1}{1}\cdots\frac{p_r}{1}\cdot inv$ es producto de primo. En conclusión, los irreducibles de A_S son primos y todo elemento es producto de irreducibles, luego A_S es DFU.

P39. $\Rightarrow$) Sea $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$ una cadena creciente de ideales de A. Consideremos el ideal $I = \underset{i}{\cup} I_i$. Tenemos que $I = (i_1,\ldots,i_n)$. Sea $r\in\mathbb{N}$ tal que I_r contiene a $i_1,\ldots,i_n$. Entonces, $I = I_r$ y $I_r = I_{r+1} = I_{r+2} = \cdots$.

$\Leftarrow$) Sea $I\subset A$ un ideal. Sea $i_1\in I$, si $I\neq(i_1)$ sea $i_2\in I\backslash(i_1)$. Si $I\neq(i_1,i_2)$ sea $i_3\in I\backslash(i_1,i_2)$. Si $I\neq(i_1,i_2,i_3)$ sea $i_4\in I\backslash(i_1,i_2,i_3)$. Este proceso ha de terminar porque

$$(i_1)\underset{\neq}{\subset}(i_1,i_2)\underset{\neq}{\subset}(i_1,i_2,i_3)\underset{\neq}{\subset}(i_1,i_2,i_3,i_4)\underset{\neq}{\subset}\cdots$$

y si termina I es finito generado.

P40. Veamos el recíproco. Sea $a\in A$ un elemento irreducible. El ideal (a) está incluido en algún ideal maximal $\mathfrak{m} = (b)$. Por tanto, $a = bc$, para algún $c\in A$. Como a es irreducible, c ha de ser invertible, luego $(a) = (b) = \mathfrak{m}$. Por el teorema 2.4.3, A es un dominio de factorización única. Sea (a_1,a_2) un ideal de A y $b = m.c.d(a_1,a_2)$. Entonces, $a_1 = bc_1$ y $a_2 = bc_2$, de modo que no existe ningún elemento propio que divida a c_1 y c_2 a la vez. Por tanto, el ideal (c_1,c_2) no está incluido en ningún maximal, luego $(c_1,c_2) = A$ y $(a_1,a_2) = b\cdot(c_1,c_2) = b\cdot A$. Ahora es fácil concluir que todo ideal (que es finito generado) es principal.

P41. Observemos que $x^4+2x^2+1=(x+i)^2\cdot(x-i)^2$. Por el algoritmo de Euclides obtenemos que $1=(\frac{x}{4i}-\frac{1}{2})(x+i)^2+(\frac{-x}{4i}-\frac{1}{2})(x-i)^2$. Por tanto,

$$\int \frac{x^5}{x^4+2x^2+1}dx=\int x+\frac{\frac{-x^4}{2i}+x^3-\frac{x^2}{4i}+\frac{x}{2}}{(x-i)^2}+\frac{\frac{x^4}{2i}+x^3+\frac{x^2}{4i}+\frac{x}{2}}{(x+i)^2}dx$$

Tenemos que

$$\frac{-x^4}{2i}+x^3-\frac{x^2}{4i}+\frac{x}{2}=(x-i)^2\cdot(\frac{-x^2}{2i}-\frac{3}{4i})-\frac{x}{2}-\frac{3}{4i}=(x-i)^2\cdot(\frac{-x^2}{2i}-\frac{3}{4i})-\frac{1}{2}(x-i)-\frac{5}{4i}.$$

$$\frac{x^4}{2i}+x^3+\frac{x^2}{4i}+\frac{x}{2}=(x+i)^2\cdot(\frac{x^2}{2i}+\frac{3}{4i})-\frac{x}{2}+\frac{3}{4i}=(x+i)^2\cdot(\frac{x^2}{2i}+\frac{3}{4i})-\frac{1}{2}(x+i)+\frac{5}{4i}.$$

Luego, $\int \frac{x^5}{x^4+2x^2+1}dx=\frac{x^2}{2}-\frac{\ln(x-i)}{2}+\frac{5}{4(x-i)}-\frac{\ln(x+i)}{2}-\frac{5}{4(x+i)}=\frac{x^2}{2}-\frac{\ln(x^2+1)}{2}+\frac{5}{2(x^2+1)}$.

P42. Tenemos que $dt=ie^{ix}dx$, luego $dx=\frac{dt}{it}$, $cos(x)=\frac{e^{ix}+e^{-ix}}{2}=\frac{t+t^{-1}}{2}$, $\sin(x)=\frac{e^{ix}-e^{-ix}}{2i}=\frac{t-t^{-1}}{2i}$ y $\cos(3x)=\frac{e^{3ix}+e^{-3ix}}{2}=\frac{t^3+t^{-3}}{2}$.

Solución de los problemas del capítulo tercero

P1. Procedamos por inducción sobre $n=\operatorname{gr}p(x)$. El caso $n=0$ es evidente. Caso $n>0$: $(p(x)-\sum_{i=0}^{n}\frac{p^{i)}(0)}{i!}\cdot x^i)'=p'(x)-\sum_{i=1}^{n}\frac{p^{i)}(0)}{(i-1)!}\cdot x^{i-1}=0$ por la hipótesis de inducción, luego $p(x)-\sum_{i=0}^{n}\frac{p^{i)}(0)}{i!}\cdot x^i=cte$, y $cte=0$ como se comprueba tomando $x=0$.

P2. *a*) $1=\sum_{i=1}^{n}\frac{1}{p'(\alpha_i)}\cdot\frac{p(x)}{x-\alpha_i}$, porque coinciden tomando valores en los α_i y son polinomios de grado menor o igual que $n-1$.

b) Trabajemos en $k[[\frac{1}{x}]]$. Tenemos que $\frac{1}{p(x)}=x^{-n}+\mu_1\cdot x^{-n-1}+\cdots+\mu_m\cdot x^{-n-m}+\cdots$ y $\sum_{i=1}^{n}\frac{1}{p'(\alpha_i)}\cdot\frac{1}{x-\alpha_i}=\sum_{r=0}^{\infty}(\sum_i\frac{\alpha_i^r}{p'(\alpha_i)})\cdot x^{-r-1}$.

P3. Consideremos un epimorfismo $\pi\colon k[x_i]_{i\in I}\to K'$. Sea $\{e_j\}_{j\in J}$ una base del k-espacio vectorial $\operatorname{Ker}\pi$ y $\{e_j,e_{j'}\}_{j\in J,j'\in J'}$ una base del k-espacio vectorial $k[x_i]_{i\in I}$. Se cumple que $\{e_j,e_{j'}\}_{j\in J,j'\in J'}$ es una base del K-espacio vectorial $K[x_i]_{i\in I}$. Además, $\langle e_j|j\in J\rangle_K$ es un ideal de $K[x_i]_{i\in I}$. Por tanto, tenemos las inyecciones

$$K'=k[x_i]_{i\in I}/\langle e_j|j\in J\rangle_k\hookrightarrow K[x_i]_{i\in I}/\langle e_j|j\in J\rangle_K=:B$$
$$K\hookrightarrow K[x_i]_{i\in I}/\langle e_j|j\in J\rangle_K=:B.$$

Si $\mathfrak{m}\subset B$ es un ideal maximal, $L=B/\mathfrak{m}$ es la extensión de cuerpos buscada.

P4. Supongamos que $\operatorname{gr}(p(x))>1$. Entonces, $p(x)$ no tiene raíces reales. Sea $a+bi\in\mathbb{C}$ $(b\neq 0)$ una raíz de $p(x)$, entonces $a-bi\in\mathbb{C}$ también es raíz de $p(x)$. El polinomio irreducible $q(x)=(x-a-bi)(x-a+bi)\in\mathbb{R}[x]$ divide a $p(x)$, luego $p(x)=\lambda\cdot q(x)$, con $\lambda\in\mathbb{R}$ y $\operatorname{gr}(p(x)=2$.

P5. Escribamos $p(x)=a_0(x-\alpha_1)\cdots(x-\alpha_n)$. Entonces,

$$\begin{aligned} p(x)\cdot p(-x) &= a_0(x-\alpha_1)\cdots(x-\alpha_n)\cdot a_0(-x-\alpha_1)\cdots(-x-\alpha_n) \\ &= a_0^2(-x^2+\alpha_1^2)\cdots(-x^2+\alpha_n) = q(x^2). \end{aligned}$$

y $q(x)\in k[x]$ porque $q(x^2)\in k[x]$. Si calculamos $p(x)\cdot p(-x)$ e igualamos coeficientes con $q(x^2)=b_0x^{2n}+b_1x^{2(n-1)}+\cdots+b_n$, obtenemos que

$$b_r=\sum_{i+j=2r}(-1)^{r-i}a_ia_j=a_r^2-2a_{r-1}a_{r+1}+2a_{r-2}a_{r+2}+\cdots.$$

Comentario: Si $|\alpha_1|>|\alpha_2|,\ldots,|\alpha_n|$, entonces $|\alpha_1^{2^m}|>>|\alpha_2^{2^m}|,\ldots,|\alpha_n^{2^m}|$ y si $h(x)=a_0^{2^m}x^n+c_1x^{n-1}+\cdots+c_n$ es el polinomio de raíces $\{\alpha_i^{2^m}\}$ entonces $\alpha_1\simeq\frac{\sqrt[2^m]{-c_1}}{a_0}$.

P6. $\Delta=f(\alpha_1,\alpha_2)=(\alpha_1-\alpha_2)^2$. Entonces, $f(\alpha_1,0)=\alpha_1^2=\bar{a}_1^2$ y

$$f(\alpha_1,\alpha_2)-a_1^2=(\alpha_1-\alpha_2)^2-(\alpha_1+\alpha_2)^2=\alpha_1\alpha_2\cdot(-4)$$

Luego, $\Delta=a_1^2-4a_2$.

P7. $\Delta=f(\alpha_1,\alpha_2,\alpha_3)=(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$. Entonces,

$$f(\alpha_1,\alpha_2,0)=(\alpha_1-\alpha_2)^2\alpha_1^2\alpha_2^2=(\bar{a}_1^2-4\bar{a}_2)\bar{a}_2^2$$

y

$$\frac{f(\alpha_1,\alpha_2,\alpha_3)-(a_1^2-4a_2)a_2^2}{a_3}=\cdots=-4a_1^3+18a_1a_2-27a_3$$

Luego, $\Delta=a_3(-4a_1^3+18a_1a_2-27a_3)+(a_1^2-4a_2)a_2^2$.

Otro modo: Sea $x'=x+\frac{a_1}{3}$, entonces $p(x)=x'^3+a_2'x'+a_3'=:q(x')$, con $a_2'=\frac{-a_1^2}{3}+a_2$ y $a_3'=\frac{2a_1^3}{27}-\frac{a_2a_1}{3}+a_3$. El polinomio $q(x')$ tiene el mismo discriminante que $p(x)$. Tenemos que $(\alpha_1'-\alpha_2')^2(\alpha_1'-\alpha_3')^2(\alpha_2'-\alpha_3')^2=\lambda\cdot a'^3_2+\mu\cdot a'^2_3$. Si tomamos como raíces $0,1,-1$ y raíces $2,-1,-1$ obtenemos que

$$4=\lambda\cdot(-1)^3 \text{ y } 0=\lambda\cdot(-3)^3+\mu\cdot 2^2.$$

Luego, $\lambda=-4$ y $\mu=-27$.

P8. Sabemos que $\frac{p'(x)}{p(x)}=\sum_i\frac{1}{x-\alpha_i}$ y que $\frac{1}{x-\alpha}=\frac{1}{x}+\frac{\alpha}{x^2}+\cdots+\frac{\alpha^n}{x^{n+1}}+\cdots$, luego

$$\frac{p'(x)}{p(x)}=\sum_i\frac{1}{x-\alpha_i}=\sum_i(\frac{1}{x}+\frac{\alpha_i}{x^2}+\cdots+\frac{\alpha_i^n}{x^{n+1}}+\cdots)=\frac{\sigma_0}{x}+\frac{\sigma_1}{x^2}+\cdots+\frac{\sigma_n}{x^{n+1}}+\cdots$$

Multiplicando por $p(x)$ en esta igualdad obtenemos

$$\sum_{i=0}^{n-1}(n-i)\cdot a_i\cdot x^{n-i-1}=(\sum_{i=0}^{n}a_ix^{n-i})\cdot\sum_{i=0}^{\infty}\frac{\sigma_i}{x^{i+1}}.$$

Igualando el coeficiente de x^r en ambos lados de la igualdad obtenemos las fórmulas de Newton.

P9. a) $x^4+x^2+1=(x^2+x+1)^2$ en $\mathbb{Z}/2\mathbb{Z}[x]$.

b) $x^4+x^3-x=x\cdot(x^3+x^2-1)$ en $\mathbb{Z}/3\mathbb{Z}[x]$.

c) Si $x^4+4x^3+3x^2+2x+3=p(x)\cdot q(x)$ en $\mathbb{Z}[x]$, entonces $p(x)$ y $q(x)$ son de grados dos, porque al hacer módulo 2 el polinomio descompone en producto de dos polinomios irreducibles de grado 2. Pero por otra parte uno ha de ser de grado 3 y el otro de grado 1, porque así sucede al hacer cociente por 3. Contradicción, luego $p(x)$ es irreducible. Como es primitivo también es irreducible en $\mathbb{Q}[x]$.

P10. El morfismo que asigna a cada polinomio su recíproco,

$$\mathbb{Q}[x]\setminus\{0\}\to\mathbb{Q}[x]\setminus\{0\},\ p(x)\mapsto p(1/x)\cdot x^{\mathrm{gr}(p(x))},$$

es una biyección que respeta el producto. Por tanto, un polinomio es irreducible si y solo si lo es su recíproco. El criterio de Nietsnesie es consecuencia del criterio de Eisenstein.

P11. Por el lema de Gauss, basta demostrar que $p(x)=x^p-px+1$ es irreducible en $\mathbb{Z}[x]$. El polinomio $q(y)=p(y-1)$ es irreducible por el criterio de Eisenstein (considerando el primo p).

P12. No tiene raíces racionales, luego si no es irreducible descompone en producto de un polinomio con coeficientes enteros irreducible de grado 2 por otro de grado 3, $x^5-2x^4+x+1=(ax^2+bx+c)\cdot(a'x^3+b'x^2+c'x+d')$. Entonces, $1=p(0)q(0)$, $1=p(1)q(1)$ y $-3=p(-1)q(-1)$. Puedo suponer $p(0)=1$, $p(1)=\pm1$, y $p(-1)=\pm3\pm1$. Entonces,

$p(0)=$	1	1	1	1	1	1	1	1
$p(1)=$	1	1	1	1	-1	-1	-1	-1
$p(-1)=$	1	-1	3	-3	1	-1	3	-3
$p(x)=$	1	$-x^2+x+1$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

y $x^5-2x^4+x+1=(-x^2+x+1)\cdot(-x^3+x^2+1)$.

P13. Consideremos el morfismo $f:\mathbb{Q}[x]\to\mathbb{C}$, $f(q(x))=q(\sqrt{2})$. $\mathrm{Ker}\,f=(x^2-2)$. Luego, $p(\sqrt{2})=0$ si y solo si $p(x)\in\mathrm{Ker}\,f=(x^2-2)$.

Consideremos el morfismo $f:\mathbb{Q}[x]\to\mathbb{C}$, $f(q(x))=q(\sqrt[3]{2})$. $\mathrm{Ker}\,f=(x^3-2)$, porque x^3-2 es irreducible por el criterio de Eisenstein y porque $x^3-2\in\mathrm{Ker}\,f$. Luego, $p(\sqrt[3]{2})=0$ si y solo si $p(x)\in\mathrm{Ker}\,f=(x^3-2)$.

P14. Sea $\mu_n:=\{z\in\mathbb{C}:z^n=1\}$ y X_d el conjunto de las ráices d-ésimas primitivas de la unidad. Como $\mu_n=\coprod_{d|n}X_d$, tenemos que

$$n=|\mu_n|=\sum_{d|n}|X_d|=\sum_{d|n}\phi(d)$$

P15. El directo es el problema 12 del primer capítulo.

Recíproco: sea G verificando la hipótesis. Sea $G = \coprod_{d|n} G_d$, siendo $G_d \subset G$ los elementos de orden d. Si existe un elemento de orden d, entonces el grupo generado H es el único de dicho orden, luego G_d es el conjunto de generadores de H y, por tanto, $|G_d| = \phi(d)$. Por tanto, $|G_d| = 0, \phi(d)$. Pero como $\sum_{d|n} \phi(d) = n = |G| = \sum_{d|n} |G_d|$, se concluye que para cada d divisor de n es $|G_d| = \phi(d) \neq 0$. En particular, $G_n \neq \emptyset$, es decir, G admite un generador y por tanto es cíclico.

P16. La cota superior de Lagrange de $x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3$ es

$$L = 1 + \sqrt{7}.$$

Una cota inferior I, es el opuesto de una cota superior de Lagrange del polinomio $-(-x^5 + 2x^4 + 5x^3 + 8x^2 + 7x - 3) = x^5 - 2x^4 - 5x^3 - 8x^2 - 7x + 3$, es decir,

$$I = -(1 + 8) = -9.$$

Los demás polinomios al lector.

P17. El sistema de Sturm son los polinomios $f(x) = x^3 + 3x^2 - 1$, $f_1(x) = 3x^2 + 6x$, $f_2(x) = 2x + 1$, $f_3(x) = 1$. El número de raíces reales son

$$V_{-\infty}^{\infty}(f(x), f_1(x), f_2(x), f_3(x)) = V(-,+,-,+) - V(+,+,+,+) = 3.$$

Una cota superior es $x = 1$ y una cota inferior es $x = -3$. El número de raíces entre 0 y 1 son $V_0^1(f(x), f_1(x), f_2(x), f_3(x)) = V(-1,0,1,1) - V(3,9,,3,1) = 1.$, entre $-1,0$ son $V_{-1}^0(f(x), f_1(x), f_2(x), f_3(x)) = V(1,-3,-1,1) - V(-1,0,1,1) = 1.$ y entre $-2,-3$ son $V_{-3}^{-2}(f(x), f_1(x), f_2(x), f_3(x)) = V(-,+,-,+) - V(+,0,-,+) = 1$.

Aproximemos la raíz entre 0 y 1: $f(0{,}5) = -0{,}125$, $f(0{,}7) = 0{,}813$, $f(0{,}6) = 0{,}296$. Luego, 0,55 es una raíz, con un error de 0,05. Aproximemos la raíz entre -1 y 0: $f(-0{,}5) = -0{,}375$, $f(-0{,}7) = 0{,}127$, $f(-0{,}6) = -0{,}136$. Luego, $-0{,}65$ es una raíz, con un error de 0,05. Aproximemos la raíz entre -2 y -3: $f(-2{,}5) = 2{,}125$, $f(-2{,}7) = 1{,}187$, $f(-2{,}8) = 0{,}568$, $f(-2{,}9) = -0{,}59$. Luego, $-2{,}85$ es una raíz, con un error de 0,05.

P18. Calculemos una cota inferior de las raíces positivas del polinomio

$$f(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3.$$

Sea $h(x) = -x^5 \cdot f(\frac{1}{x}) = 3x^5 + 7x^4 - 8x^3 + 5x^2 - 2x - 1$. Consideremos el polinomio y sus derivadas sucesivas (salvo multiplicación por $\lambda > 0$): $3x^5 + 7x^4 - 8x^3 + 5x^2 - 2x - 1$, $15x^4 + 28x^3 - 24x^2 + 10x - 2$, $30x^3 + 42x^2 - 24x + 5$, $15x^2 + 14x - 4$, $15x + 7$, 1, que son positivos en $x = 1$ y es una cota superior de las raíces reales de $h(x)$. Por tanto, una cota inferior de las raíces positivas de $f(x)$ es $\frac{1}{1} = 1$. Por el teorema de Budan-Fourier el número de raíces positivas de $f(x)$ es 1.

P19. Los polinomios de Sturm son

$$-4x^5 + 26x^4 - 33x^2 + 98x + 5,\ 2x^4 - 13x^3 + 10x - 49,\ -5 + 13x^2,\ 8231/169 - 5x,\ -$$

Entonces,

$$E_{-\infty}^{-3} = V_{-\infty}^{-3} = V(+,+,+,-) - V(+,+,+,+,-) = 0$$
$$E_{-3}^{0} = V_{-3}^{0} = V(+,+,+,-) - V(+,-,-,+,-) = -2$$
$$E_{0}^{3} = V_{0}^{3} = V(+,-,-,+,-) - V(+,-,+,+,-) = 0$$
$$E_{3}^{\infty} = V_{3}^{\infty} = V(+,-,+,+,-) - V(-,+,+,-,-) = 1.$$

P20. Tenemos que calcular $\frac{1}{2}\cdot E_{-1}^{1}(\frac{t^4+2t^3+5t^2-2t-1}{t^2}) = 0$, porque $t=0$ es un polo de multiplicidad par.

P21. Traslademos el punto $(1,1)$ al origen. Tenemos que calcular el número de vueltas de la curva $\bar{x} = \frac{-2}{t^4+1}$, $\bar{y} = \frac{-1}{t^2+1}$ alrededor del origen: $\frac{1}{2}E_{-1}^{1}\frac{2(t^4+1)}{t^2+1} = \frac{1}{2}E_{-1}^{1}\frac{2}{t^2+1} = 0$, porque no existen polos.

P22. La curva viene parametrizada por $(\frac{t^2-1}{t^2+1} - \frac{2ti}{t^2+1})^5 + (\frac{t^2-1}{t^2+1} - \frac{2ti}{t^2+1}) + 1$, para $t \in (-\infty,\infty)$. Luego el número de vueltas alrededor del origen es igual a

$$\frac{1}{2}E_{-\infty}^{\infty}\frac{4t(3t^8-28t^6+66t^4-28t^2+3)}{3t^{10}-37t^8+222t^6-202t^4+47t^2-1} = E_{0}^{\infty}\frac{3x^4-28x^3+66x^2-28x+3}{3x^5-37x^4+222x^3-202x^2+47x-1}$$

Apliquemos el teorema 3.5.11. Obtenemos los restos de Sturm: $-9x^3-3x^2+5x+1$, $-87x^2+50x-7$, $-3x+1$. Luego el número de vueltas es

$$V(-,+,+,-,+) - V(+,+,-,-,-) = 3-1 = 2.$$

P23. a) Podemos suponer $a_0 > 0$. Por la proposición 3.5.38, podemos suponer que $a_1, a_2 > 0$. Por el criterio de Hurwitz concluimos.

b) Podemos suponer $a_0 > 0$. Por la proposición 3.5.38, podemos suponer que $a_1, a_2, a_3 > 0$. Por el criterio de Hurwitz concluimos.

c) Podemos suponer $a_0 > 0$. Por la proposición 3.5.38, podemos suponer que $a_1, a_2, a_3, a_4 > 0$. Por el criterio de Hurwitz, el polinomio es de Hurwitz si y solo si $a_1a_2a_3 - a_3^2a_0 - a_1^2a_4 > 0$ y $a_1a_2 - a_3a_0 > 0$. Ahora bien, $a_1a_2a_3 - a_3^2a_0 - a_1^2a_4 = a_3(a_1a_2 - a_3a_0) - a_4a_1^2$, luego el polinomio es de Hurwitz si y solo si $a_1a_2a_3 - a_3^2a_0 - a_1^2a_4 > 0$.

P24. Sea $y = x + \frac{1}{x} = \frac{x^2+1}{x}$, es decir, $x^2 - yx + 1 = 0$. Consideremos el sistema

$$\left.\begin{aligned} P(x) &= 0 \\ Q(x) = x^2 - yx + 1 &= 0 \end{aligned}\right\}$$

Las soluciones del sistema son $x = \alpha_i$, $y = \alpha_i + \frac{1}{\alpha_i}$. Luego las raíces de $R(y) := R(P,Q)$ son $y = \alpha_i + \frac{1}{\alpha_i}$. Las raíces de $Q(x)$ son $x, 1/x$ (con $y = x + 1/x$). Luego

$$\boxed{R(y) = P(x)\cdot P(\frac{1}{x})}$$

haciendo el cambio $x + \frac{1}{x} = y$ (o sustituyendo $x = \frac{y+\sqrt{y^2-4}}{2}$ y $\frac{1}{x} = \frac{y-\sqrt{y^2-4}}{2}$).

P25. La ecuación $x^5-1=0$ tiene por soluciones las raíces quintas de 1:

$$\varepsilon^k = cos\,\frac{2k\pi}{5} + sen\,\frac{2k\pi}{5}$$

con lo que

$$cos\,\frac{2k\pi}{5} = \frac{1}{2}(\varepsilon^k + \overline{\varepsilon}^k) = \frac{1}{2}(\varepsilon^k + \frac{1}{\varepsilon^k})$$

así que el sistema es

$$\left.\begin{array}{l} x^5-1=0 \\ y = \frac{1}{2}(x+\frac{1}{x}) \end{array}\right\}$$

Siguiendo el problema 24, la resultante queda:

$$R(y) = (x^5-1)(\frac{1}{x^5}-1) = -(x^5+\frac{1}{x^5})+2$$

haciendo el cambio $2y = x+x^{-1}$. Elevando $x+x^{-1}$ a 5 y a 3 y después de un pequeño cálculo se obtiene:

$$R(y) = 16y^5 - 20y^3 + 5y - 1$$

Igualmente sabríamos calcular el polinomio de raíces $sen\,\frac{2k\pi}{5}$, con $k=1,\ldots,5$, ya que $sen\,\frac{2k\pi}{5} = \frac{1}{2i}(\varepsilon^k - \varepsilon^{-k})$ y se aplica el método del problema 25.

P26. Es el polinomio $R(y) = P(x)\cdot P(-\frac{1}{x})$, haciendo el cambio $y = x - \frac{1}{x}$ (es decir sustituyendo $x = \frac{y+\sqrt{y^2+4}}{2}$ y $-\frac{1}{x} = \frac{y-\sqrt{y^2+4}}{2}$).

P27. Si x es solución de la ecuación $y = ax+\frac{b}{x}$, entonces $\frac{b}{ax}$ también y se concluye como en los en los problemas 24 y 26, que el polinomio buscado es $R(y) = P(x)\cdot P(\frac{b}{ax})$ haciendo $ax+\frac{b}{x} = y$ (es decir sustituyendo $x = \frac{y+\sqrt{y^2-4ab}}{2a}$ y $\frac{b}{ax} = \frac{y-\sqrt{y^2-4ab}}{2a}$).

P28. Sea $R(y) := R(P(x),F(x,y))$ considerados $P(x)$ y $F(x,y)$ como polinomios en x (con coeficientes en $k[y]$). Igual que en los ejemplos anteriores β es raíz de $R(y)$ y de $P(x)$, por tanto, $x-\beta$ es factor común del m.c.d.$(P(x),R(x))$. (Si la relación se verifica únicamente para las raíces α_1,α_2, entonces β es la única raíz común de $P(x),R(x)$ y, por tanto, el m.c.d.$(P,R) = (x-\beta)$. Entonces β se calcula y α será una raíz común de $P(x)$ y $F(x,\beta)$ y, por tanto, de $m.c.d.(P(x),F(x,\beta))$.

Conocidas $\alpha=\alpha_1$ y $\beta=\alpha_2$ se divide $P(x)$ por $(x-\alpha_1)(x-\alpha_2)$. El cociente $P_1(x)$ es de grado $n-2$. (¡el grado de dificultad ha bajado en 2 unidades!).

P29. $R_0(x) = x^2+ax+b$, $R_1(x) = P'(x) = 2x+a$, $R_2(x) = P(-\frac{a}{2}) = -\frac{a^2}{4}+b$, luego $g_0 = 2, g_1 = 1, g_2 = 0$ y $d_0 = 1, d_1 = 2, d_2 = -\frac{a^2}{4}+b$:

$$\Delta = (-1)^{\binom{2}{2}}\cdot R(P,P') = (-1)^{2\cdot 1+1\cdot 0}\cdot 2^{2-0}(-\frac{a^2}{4}+b)^{1-0} = a^2-4b.$$

P30. $R_0(x) = x^3 + px + q$, $R_1(x) = P'(x) = 3x^2 + p$, $R_2(x) = \frac{2}{3}px + q$ y por último $R_3(x) = R_2(-\frac{3}{2}\frac{q}{p}) = \frac{3^3}{2^2}\frac{q^2}{p^2} + p$, luego $g_0 = 3, g_1 = 2, g_2 = 1, g_3 = 0$ y $d_0 = 1, d_1 = 3, d_2 = \frac{2}{3}p, d_3 = \frac{3^3}{2^2}\frac{q^2}{p^2} + p$:

$$\Delta = (-1)^{\binom{3}{2}} \cdot R(P,P') = -(-1)^{3\cdot 2+2\cdot 1+1\cdot 0} \cdot 3^{3-1}(\frac{2}{3}p)^{2-0}(\frac{3^3}{2^2}\frac{q^2}{p^2} + p) = -(4p^3 + 27q^2).$$

Solución de los problemas del capítulo cuarto

P1. Sea $G' \subseteq G$ un subgrupo. Sea $g \in G'$. Dado $n \in \mathbb{N}$, tenemos que $ng = g + \overset{n}{\cdots} + g \in G'$ y $-n \cdot g = (-g) + \overset{n}{\cdots} + (-g) \in G'$. En conclusión, G' es un $\mathbb{Z}$-submódulo de G. Sea $H \subseteq G$ un submódulo, en particular es un subgrupo. Sea $f : G \to G'$ un morfismo de grupos. Dado $n \in \mathbb{N}$, tenemos que $f(n\cdot g) = f(g + \overset{n}{\cdots} + g) = f(g) + \overset{n}{\cdots} + f(g) = n \cdot f(g)$ y $f(-n\cdot g) = f(-g + \overset{n}{\cdots} + (-g)) = f(-g) + \overset{n}{\cdots} + f(-g) = n \cdot f(-g) = n(\cdot - f(g)) = -n \cdot f(g)$. Luego, f es un morfismo de $\mathbb{Z}$-módulos. Recírpocamente si f es un morfismo de $\mathbb{Z}$-módulos en particular es un morfismo de grupos.

P2. Sea $E' \subseteq E$ estable por T, es decir, tenemos el endomorfismo $T_{|E'} : E' \to E'$, $T_{|E'}(e') = T(e')$. Por tanto, E' es un $K[x]$-módulo y la estructura de $K[x]$-módulo es la inducida por E, porque $p(T_{|E'})(e') = p(T)(e')$, para todo $p(x) \in K[x]$ y $e' \in E'$. Luego, E' es un $K[x]$-submódulo de E. Recíprocamente. si E' es un $K[x]$-submódulo de E, dado $e' \in E'$, tenemos que $= T(e') = x \cdot e' \in E'$, luego E' es estable por T.

Sea (a_{ij}) la matriz de T en la base $\{e_i\}$, es decir, $T(e_i) = \sum_j a_{ij}e_j$. Tenemos que $x \cdot \phi(e_i) = \phi(x \cdot e_i) = \phi(T(e_i)) = \phi(\sum_j a_{ij}e_j) = \sum_j a_{ij}\phi(e_i)$. Luego la matriz asociada a $x\cdot$ en la base $\{\phi(e_i)\}$ es (a_{ij}).

P3. Dado $a \in A$ y $m \in M$, definimos $a \cdot m := f(a) \cdot m$.

P4. El subconjunto $N := \{i_1 \cdot m_1 + \cdots + i_n \cdot m_n \in M$, variando los $i_j \in I, m_j \in M$, y $r \in \mathbb{N}\}$ es un submódulo de M y es el mínimo que contiene a $\{i \cdot m\}_{i\in I, m\in M}$.

P5. El conjunto $\{i \cdot (m,m'), \forall i \in I, (m.m') \in M \oplus M'\}$ está incluido en $IM \oplus IM'$, luego $I \cdot (M \oplus M') \subseteq IM \oplus IM'$. Los conjuntos $\{im, \forall i \in I, m \in M\}$, $\{im', \forall i \in I, m' \in M'\}$ están incluidos en $I \cdot (M \oplus M')$, luego $IM, IM' \subseteq I \cdot (M \oplus M')$, luego $IM \oplus IM' \subseteq I \cdot (M \oplus M')$.

P6. El morfismo $f : \operatorname{Ker}\pi \oplus N \to M$, $f(k,n) = k + s(n)$ es inyectivo: si $f(k,n) = 0$, es decir, $k + s(n) = 0$, entonces tomando π obtenemos que $0 + n = 0$, luego $n = 0$ y $k = 0$ y $(k,n) = 0$. Por último, f es epiyectivo: dado m, tenemos que $m - s(\pi(n)) \in \operatorname{Ker}\pi$ y $f(m - s(\pi(n)), \pi(n)) = m$.

P7. El morfismo $\pi : M \to (M/N_1)/\bar{N}_2$, $\pi(m) := \overline{\bar{m}}$ es epiyectivo. Como

$$\operatorname{Ker}\pi = \{m \in M : \overline{\bar{m}} = 0\} = \{m \in M : \bar{m} \in \bar{N}_2\} = \{m \in M : \exists n_2 \in N_2 \text{ tal que } \bar{m} = \bar{n}_2\}$$
$$= \{m \in M : \bar{m} \in \bar{N}_2\} = \{m \in M : \exists n_2 \in N_2, n_1 \in N_1 \text{ tales que } m = n_1 + n_2\} = N_1 + N_2$$

terminamos por el teorema de isomorfía.

P8. El morfismo $N_2 \to (N_1+N_2)/N_1$, $n \mapsto \bar{n}$, es epiyectivo de núcleo $N_1 \cap N_2$. Por el teorema de isomorfía concluimos.

P9. Sean $\lambda, \mu \in A$ tales que $\lambda a + \mu b = 1$. Entonces, $\overline{\mu b} = \overline{\lambda a + \mu b} = \bar{1}$ en A/aA, luego $\mu\cdot$ es el morfismo inverso de $b\cdot$.

P10. El morfismo $\pi\colon A/a_1a_A \to A/a_1A \oplus A/a_2A$, $\pi(\bar{t}) = (\bar{t},\bar{t})$ es un isomorfismo por el teorema chino de los restos. La composición $\pi \circ \phi$ es un isomorfismo por el problema 9 . Por tanto, ϕ es un isomorfismo.

En el caso general se argumenta igual. Probemos solo que $(a_i, c_i) = A$. Para ello léase la demostración del teorema 4.5.3.

P11. Sea $T(t)$ la temperatura del sólido en el instante t. Por la ley de enfriamento de Newton $\frac{dT}{dt} = K\cdot(5-T)$, es decir, $T' + KT = 5K$, que escribimos

$$(D + K\,\mathrm{Id})(T) = 5K.$$

Una solución particular T_0 de esta escuación diferencial es $T_0 = 5$. Todas las soluciones son $5 + \mathrm{Ker}(D + K\,\mathrm{Id}) = 5 + e^{-Kt}\cdot\mu$. Tenemos que $T(t) = 5 + e^{-Kt}\cdot\mu$, $T(0) = 20$ y $T(2) = 10$. Luego $\mu = 15$ y $K = \ln\sqrt{3}$.

P12. El apartado a) es una comprobación inmediata. Resolvamos b). Tenemos

$$g = y' + fy = (D + f\,\mathrm{Id})(y) = (D + f\,\mathrm{Id})(e^{-\int f}e^{\int f}y) = e^{-\int f}D(e^{\int f}y).$$

Luego, $D(e^{\int f}y) = e^{\int f}g$. Entonces, $e^{\int f}y = cte + \int e^{\int f}g$ e $y = e^{-\int f}(cte + \int e^{\int f}g)$.

P13. a) Consideremos el cambio de variable $x = e^t$ (o $t = \ln x$). Tenemos que $\frac{\partial}{\partial t} = \Theta$, por la regla de la cadena:

$$\frac{\partial f(x)}{\partial t} = \frac{\partial f(x)}{\partial x}\cdot\frac{\partial x}{\partial t} = \frac{\partial f(x)}{\partial x}\cdot x = \Theta(f(x))$$

Por tanto,

$$\mathrm{Ker}(\Theta - \alpha\,\mathrm{Id})^r = \mathrm{Ker}(\frac{\partial}{\partial t} - \alpha\,\mathrm{Id})^r = e^{\alpha t}\cdot\{\sum_{i=0}^{r-1}\lambda_i t^i\} = x^\alpha\cdot\{\sum_{i=0}^{r-1}\lambda_i(\ln x)^i\}.$$

b) $\Theta^2 = x^2\frac{\partial^2}{\partial x^2} + x\frac{\partial}{\partial x}$. Por tanto,

$$0 = x^2y'' + bxy' + cy = (\Theta^2 + (b-1)\Theta + c\,\mathrm{Id})(y).$$

Entonces, $y \in \mathrm{Ker}(\Theta^2 + (b-1)\Theta + c\,\mathrm{Id})$. Sean $\alpha, \beta = \frac{-b+1\pm\sqrt{(b-1)^2-4c}}{2}$. Entonces,

$$y = \begin{cases} \lambda x^\alpha + \mu x^\beta, & \text{si } \alpha \neq \beta \\ x^\alpha(\lambda + \mu\ln x), & \text{si } \alpha = \beta \end{cases}$$

P14. Tenemos $(D^2+aD+b\,\mathrm{Id})(f)=0$. Las raíces de x^2+ax+b son $\frac{-a\pm\sqrt{a^2-4b}}{2}$. Luego,

$$f\in\mathrm{Ker}(D^2+aD+b\,\mathrm{Id})=e^{\frac{-ax}{2}}\cdot(\lambda\cos(\frac{\sqrt{-a^2+4b}}{2}x)+\mu\,\mathrm{sen}(\frac{\sqrt{-a^2+4b}}{2}x)).$$

P15. Calculemos una solución particular. Sea $E=\langle\cos wt,\mathrm{sen}\,wt\rangle$. Busquemos en E una solución particular. Resolvamos $(D^2+aD+b\,\mathrm{Id})(\lambda\cos wt+\mu\,\mathrm{sen}\,wt)=c\cos wt$, es decir,

$$\begin{aligned}(b-w^2)\cdot\lambda+aw\cdot\mu&=c\\ -aw\cdot\lambda+(b-w^2)\cdot\mu&=0\end{aligned}$$

Luego, $\lambda=\frac{c(b-w^2)}{(b-w^2)^2+a^2w^2}$ y $\mu=\frac{acw}{(b-w^2)^2+a^2w^2}$.

P16. $\int x^2\cos^2x\,dx=\frac{1}{D}(x^2(\frac{e^{xi}+e^{-xi}}{2})^2)=\frac{1}{D}(x^2\frac{e^{2xi}+e^{-2xi}+2}{4})$

$$\begin{aligned}&=\frac{x^3}{6}+\frac{e^{2xi}}{4}\frac{1}{D+2i\,\mathrm{Id}}(x^2)+\frac{e^{-2xi}}{4}\frac{1}{D-2i\,\mathrm{Id}}(x^2)\\&=cte+\frac{x^3}{6}+\frac{e^{2xi}}{4}(\frac{-i}{2}+\frac{1}{4}D+\frac{i}{8}D^2)(x^2)+\frac{e^{-2xi}}{4}(\frac{i}{2}+\frac{1}{4}D+\frac{-i}{8}D^2)(x^2)\\&=cte+\frac{x^3}{6}+\frac{(2x^2+1)\,\mathrm{sen}(2x)}{8}+\frac{x\cos(2x)}{4}.\end{aligned}$$

P17. El endomorfismo $p(D)\colon\mathrm{Ker}(D-\alpha)^{s+1}\to\mathrm{Ker}(D-\alpha)^{s+1}$ es un isomorfismo porque $p(x)$ es primo con $(x-\alpha)^m$. Luego, $(D-\alpha)^mf=p(D)^{-1}(e^{\alpha x}\cdot q_s(x))=e^{\alpha x}\cdot q_s'(x)\in\mathrm{Ker}(D-\alpha)^{s+1}$. El morfismo $(D-\alpha)^m\colon\mathrm{Ker}(D-\alpha)^{s+m+1}\to\mathrm{Ker}(D-\alpha)^{s+1}$ es epiyectivo, luego existe $f=e^{\alpha x}\cdot(\sum_{i=0}^{m+r}a_ix^i)$ tal que $(D-\alpha)^mf=e^{\alpha x}\cdot q_s'(x)$. Es decir,

$$e^{\alpha x}\cdot q_s'(x)=(D-\alpha)^m(e^{\alpha x}\cdot\sum_{i=0}^{m+r}a_ix^i)=e^{\alpha x}\cdot D^m(\sum_{i=0}^{m+r}a_ix^i)$$

y podemos suponer que $a_i=0$ para $i<m$.

P18. Tenemos que $\Delta\binom{n}{j}=(\binom{n+1}{j}-\binom{n}{j})=(\binom{n}{j-1})$. $\{\binom{n}{0},\binom{n}{1},\dots,\binom{n}{r}\}$ son linealmente independientes: Si $p(n)=\sum_{j=0}^r\lambda_j\binom{n}{j}$, entonces $\Delta^i(p(n))=\sum_{j=i}^r\lambda_i\binom{n}{j-i}$ y el término 0 es λ_i. Por tanto, si $p(n)=0$, entonces $\lambda_j=0$ para todo j. Por dimensiones, tenemos que $\{\binom{n}{0},\binom{n}{1},\dots,\binom{n}{r}\}$ es una base de $\mathrm{Ker}\,\Delta^{r+1}$.

Por último, observemos que $\Delta^i=(\nabla-1)^i=\sum_{j=0}^i(-1)^j\nabla^{i-j}$.

$p(n)=\sum_{i=0}^n i^2=\lambda_0+\lambda_1\binom{n}{1}+\lambda_2\binom{n}{2}+\lambda_3\binom{n}{3}$. Con

$$\lambda_0=\binom{0}{0}(-1)^0p(0)=0,\quad\lambda_1=\binom{1}{0}(-1)^0p(1)+\binom{1}{1}(-1)^1p(0)=1,$$
$$\lambda_2=\binom{2}{0}(-1)^0p(2)+\binom{2}{1}(-1)^1p(1)+\binom{2}{2}(-1)^2p(0)=5-2=3,$$
$$\lambda_3=\binom{3}{0}(-1)^0p(3)+\binom{3}{1}(-1)^1p(2)+\binom{3}{2}(-1)^2p(1)=14-3\cdot5+3\cdot1=2.$$

P19. Sea a_n los números de longitud n con las condiciones exigidas. Sea b_n los números de longitud n con las condiciones exigidas y que acaben en 1, sea c_n los números de longitud n con las condiciones exigidas y que acaben en 0. Tenemos que $b_n = a_{n-1}$, $a_n = b_n + c_n$ y $a_n = 2b_{n-1} + c_{n-1}$. Por tanto,

$$a_n = 2b_{n-1} + c_{n-1} = 2b_{n-1} + (a_{n-1} - b_{n-1}) = a_{n-2} + a_{n-1}.$$

Luego, $(\nabla^2 - \nabla - 1)(a_n) = 0$ y además $a_1 = 2$ y $a_2 = 3$. Que sabemos resolver.

P20. La ecuación es $(\nabla^2 + 2\nabla - 8)(a_n) = (2^n)$. Observemos que $\nabla^2 + 2\nabla - 8 = (\nabla - 2)(\nabla + 4)$ y que $(\nabla - 2)(2^n) = 0$. Por lo tanto, $(\nabla - 2)^2(\nabla + 4)(a_n) = 0$. Luego, $a_n = 2^n(an + b) + (-4)^n c$. Si aplicamos $(\nabla - 2)(\nabla + 4)$ a a_n, obtenemos

$$2^n = (\nabla + 4)(\nabla - 2)(2^n(an + b)) = (\nabla + 4)(2^n(2\Delta)(an + b)) = (\nabla + 4)(2^{n+1}a) = 2^n(4 + 8)a,$$

luego $a = \frac{1}{12}$.

P21. Sea $a_n := \sum_{i=0}^{n-1} g^i$. Entonces, $(a_n) = \frac{1}{\Delta}(g^n)$. Observemos que $(\nabla - g)(g^n) = 0$. Entonces, una solución particular es

$$(a_n) = \frac{1}{\Delta}(g^n) = \frac{1}{\nabla - 1}(g^n) = (\frac{1}{g-1} + s(\nabla)(\nabla - g))(g^n) = \frac{1}{g-1}(g^n)$$

Todas las soluciones son $(a_n) = (\frac{g^n}{g-1}) + \operatorname{Ker}\Delta = (\frac{g^n}{g-1}) + (\mu)$ Ahora bien, $1 = a_1 = \frac{g}{g-1} + \mu$. Luego $\mu = 1 - \frac{g}{g-1} = \frac{-1}{g-1}$. En conclusión,

$$\sum_{i=0}^{n} g^i = \frac{g^{n+1}}{g-1} + \frac{-1}{g-1} = \frac{g^{n+1} - 1}{g-1}$$

P22. Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n = i_n + a_n$. Tenemos que $i_n = I \cdot (K - \sum_{r=1}^{n-1} a_r)$. Por tanto,

$$d_n = a_n + I \cdot (K - \sum_{r=1}^{n-1} a_r).$$

Si aplicamos el operador diferencia Δ, entonces $10^3 = \Delta(a_n) - I \cdot a_n = (\nabla - (1 + I))(a_n)$. Por tanto, $a_n = (1 + I)^n \cdot \lambda + \frac{-10^3}{I}$. Tenemos que calcular λ. Nos falta decir que amortizamos la hipoteca en N años, es decir,

$$K = \sum_{r=1}^{N} a_r$$

Tenemos que $b_n := \sum_{r=1}^{n-1} a_r = \frac{(1+I)^n \lambda}{I} - \frac{10^3 \cdot (n-1)}{I} + \mu$. Como $b_1 = 0$, tenemos que $\mu = \frac{-(1+I)\lambda}{I}$. Luego $K = b_{N+1} = \frac{(1+I)^{N+1}\lambda}{I} - \frac{10^3 \cdot N}{I} - \frac{\lambda(1+I)}{I}$ y despejando obtenemos que $\lambda = \frac{IK + 10^3 N}{(1+I)^{N+1} - (1+I)}$ Entonces,

$$d_1 = a_1 + IK = (1 + I)\lambda + \frac{-10^3}{I} + IK = \frac{IK + \frac{10^3 N}{(1+I)^N}}{1 - \frac{1}{(1+I)^N}} - \frac{10^3}{I}$$

P23. Observemos que $D^i(\sum_i c_i(x)s_i(x)) = \sum_i c_i(x)D^i s_i(x)$, para $i < n$. Entonces,

$$D^n(\sum_i c_i(x)s_i(x)) = D(\sum_i c_i(x)D^{n-1}s_i(x)) = \sum_i c_i(x)D^n s_i(x) + \sum_i c_i(x)'D^{n-1}s_i(x).$$

Luego, $p(D)(\sum_i c_i(x)s_i(x)) = \sum_i c_i(x)p(D)(s_i(x)) + \sum_i c_i(x)'s_i(x)^{n-1)} = 0 + f(x)$.

P24. Observemos que

$$\nabla(gh) = g\nabla(h) + \Delta(g)\nabla(h)$$

Por tanto, por esta fórmula y la primera ecuación del sistema de ecuaciones

$$\nabla(\sum_i c_i s_i) = \sum_i c_i \nabla(g_i) + \sum_i \Delta(c_i)\nabla(s_i) = \sum_i c_i \nabla(g_i)$$

Luego, por la fórmula y la segunda ecuación del sistema de ecuaciones

$$\nabla^2(\sum_i c_i s_i) = \nabla(\sum_i c_i \nabla(g_i)) = \sum_i c_i \nabla^2(g_i)$$

y recurrentemente

$$\nabla^{r-1}(\sum_i c_i s_i) = \nabla(\sum_i c_i \nabla^{r-2}(g_i)) = \sum_i c_i \nabla^{r-1}(g_i)$$

Escribamos $p(\nabla) = \nabla^r + q(\nabla)$. Entonces,

$$\begin{aligned} p(\nabla)(\sum_i c_i s_i) &= \nabla^r(\sum_i c_i) + \sum_i c_i q(\nabla)s_i = \nabla(\sum_i c_i \nabla^{r-1}s_i) + \sum_i c_i q(\nabla)s_i \\ &= (\sum_i \Delta(c_i)\nabla^r s_i) + (\sum_i c_i \nabla^r s_i) + \sum_i c_i q(\nabla)s_i \\ &= (\sum_i \Delta(c_i)\nabla^r s_i) + \sum_i c_i p(\nabla)s_i = f + 0 = f \end{aligned}$$

P25. a) Supongamos que $\mathbb{R} \neq K$ y sea $\alpha \in K \setminus \mathbb{R}$. Evidentemente, α es $\mathbb{R}$-algebraico porque el morfismo $\mathbb{R}[x] \to K$, $p(x) \mapsto p(\alpha)$ no pueder ser inyectivo, pues $\dim_{\mathbb{R}} \mathbb{R}[x] = \infty$. $\mathbb{R}[\alpha] = \mathbb{R}[x]/(p(x))$, donde $p(x)$ es el polinomio mónico de grado mínimo que anula a α, que es irreducible (porque D es íntegro). Las raíces de $p(x)$ están en $\mathbb{C}$, luego $\mathbb{R}[\alpha] \subset \mathbb{C}$ y son iguales.

b) Supongamos que $\mathbb{R} \neq D$. Dado $\alpha \in D \setminus \mathbb{R}$, tenemos que $\mathbb{R}[\alpha]$ es un cuerpo conmutativo: es isomorfo a $\mathbb{R}[x]/(p(x))$, donde $p(x)$ es el polinomio mónico de grado mínimo que anula a α, luego es irreducible y $\mathbb{R}[x]/(p(x))$ es un cuerpo. Por el apartado anterior $\mathbb{R}[\alpha] \simeq \mathbb{C}$. Consideremos un morfismo inyectivo $\mathbb{C} \hookrightarrow D$ (que lo pensaremos como una inclusión) y consideremos el endomorfismo $\mathbb{C}$-lineal $D \xrightarrow{\cdot i} D$, $d \mapsto d \cdot i$. Obviamente, $(\cdot i)^2 = -\mathrm{Id}$, luego $x^2 + 1$ anula al endomorfismo $\cdot i$. Sea $D^+ = \mathrm{Ker}(\cdot i - i)$ y $D^- = \mathrm{Ker}(\cdot i + i)$. Sabemos que $D = D^+ \oplus D^-$. $D^+ = \mathbb{C}$, porque si existe $\alpha \in D^+ \setminus \mathbb{C}$, tendríamos que $\mathbb{C}[\alpha] \subseteq D^+$ es un cuerpo cuya dimensión como $\mathbb{R}$-espacio vectorial sería mayor que 2. Observemos que dados $\alpha, \alpha' \in D^+$ y $\beta, \beta' \in D^-$, tenemos que $\alpha\alpha', \beta\beta' \in D^+$ y $\alpha\beta \in D^-$. Por tanto, como el morfismo inyectivo $D^+ \to D^-$, $d \mapsto d \cdot \beta$ compuesto con el morfismo inyectivo $D^- \to D^+$,

$d \mapsto d\cdot\beta$ es un isomorfismo, tenemos que $D = D^+ \oplus D^+\cdot\beta = \mathbb{C}\oplus\mathbb{C}\cdot\beta$, para todo $\beta \in D^-$ no nulo. Además, $\beta^2 \in \mathbb{R}$ porque $\beta^2 \in \mathbb{C}\cap\mathbb{R}[\beta]$ que es igual a $\mathbb{R}$ porque $\mathbb{R}[\beta]$ tiene dimensión 2. Es más, $\beta^2 < 0$, porque si $\beta^2 > 0$ entonces el polinomio $x^2 - \beta^2$ tiene dos raíces reales y la raíz no real β (que pertenecen al cuerpo $\mathbb{R}[\beta] \simeq \mathbb{C}$), lo que es contradictorio. Sea $\lambda = \sqrt{-\beta^2} \in \mathbb{R}^+$ y $j := \frac{\beta}{\lambda} \in D^-$, entonces $j^2 = -1$. Tenemos que $D = \mathbb{C}\oplus\mathbb{C}\cdot j = \mathbb{R}\oplus\mathbb{R}\cdot i\oplus\mathbb{R}\cdot j\oplus\mathbb{R}\cdot ij$. Como $ij = -ji$, si definimos $k = ij$, tenemos que $i^2 = j^2 = k^2 = ijk = -1$. Si existe D, hemos probado que existen $1, i, j, k$ cumpliendo $i^2 = j^2 = k^2 = ijk = -1$ y formando una base de D. Veamos que existe un cuerpo no conmutativo de dimensión finita. Sea

$$D = \{\begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix},\ \forall z_1, z_2 \in \mathbb{C}\}^1$$

es una extensión de cuerpos (no conmutativa) de $\mathbb{R}$ de dimensión 4.

Solución de los problemas del capítulo quinto

P1. Escribamos el sistema matricialmente

$$\left(\begin{array}{ccc|c} x^2 & x & x+1 & x^2-x \\ x(x+1) & x+1 & x & x^2-1 \end{array}\right) \overset{C_2-C_3}{\rightsquigarrow} \left(\begin{array}{ccc|c} x^2 & -1 & x+1 & x^2-x \\ x(x+1) & 1 & x & x^2-1 \end{array}\right)$$

$$\overset{F_1+F_2}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2x^2+x & 0 & 2x+1 & 2x^2-x-1 \\ x(x+1) & 1 & x & x^2-1 \end{array}\right) \overset{\substack{C_3-xC_2 \\ C_1-x(x+1)C_2}}{\rightsquigarrow} \left(\begin{array}{ccc|c} 2x^2+x & 0 & 2x+1 & 2x^2-x-1 \\ 0 & 1 & 0 & x^2-1 \end{array}\right)$$

$$\overset{C_1-xC_3}{\rightsquigarrow} \left(\begin{array}{ccc|c} 0 & 0 & 2x+1 & 2x^2-x-1 \\ 0 & 1 & 0 & x^2-1 \end{array}\right)$$

Cuyas soluciones son $Z_2' = x^2-1$, $Z_3' = x-1$, $Z_1' = p(x)$ (cualquiera). Entonces,

$$\begin{pmatrix} p(x) \\ x^2-1 \\ x-1 \end{pmatrix} \overset{F_3-xF_1}{\rightsquigarrow} \begin{pmatrix} p(x) \\ x^2-1 \\ x-1-xp(x) \end{pmatrix} \overset{\substack{F_2-xF_3 \\ F_2-x(x+1)F_1}}{\rightsquigarrow} \begin{pmatrix} p(x) \\ x-1-xp(x) \\ x-1-xp(x) \end{pmatrix} \overset{F_3-F_2}{\rightsquigarrow} \begin{pmatrix} p(x) \\ x-1-xp(x) \\ 0 \end{pmatrix} = \begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \end{pmatrix}$$

P2. Los grupos abelianos desisomorfos de orden p^2q son

$$\mathbb{Z}/p^2\mathbb{Z}\oplus\mathbb{Z}/q\mathbb{Z},\ \mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/q\mathbb{Z}.$$

P3. Sea G un grupo abeliano de orden finito. Entonces, $G \simeq \underset{ij}{\oplus}\mathbb{Z}/p_i^{n_{ij}}\mathbb{Z}$, para ciertos primos p_i (p_i primo con p_j, para $i \neq j$) y ciertos n_{ij}. Si no existe un i, con dos n_{ij}, entonces por el teorema chino de los restos G sería cíclico. Tenemos pues un subgrupo $G' = \mathbb{Z}/p_i^{n_{i1}}\mathbb{Z}\oplus\mathbb{Z}/p_i^{n_{i2}}\mathbb{Z}$ de G. El subgrupo de G' definido por $G'' = \overline{\langle p_i^{n_{i1}-1}\rangle}\times\overline{\langle p_i^{n_{i2}-1}\rangle}$ es el subgrupo buscado.

[1] Observemos que $\det\begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix} = |z_1|^2 + |z_2|^2$, luego si $\begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}$ es no nula, entonces es invertible.

P4. Por el problema anterior, si G no es cíclico contiene un subgrupo G' isomorfo a $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$, que contiene al menos dos subgrupos isomorfos a $\mathbb{Z}/p\mathbb{Z}$.

Si $G\simeq\mathbb{Z}/n\mathbb{Z}$ y $d|n$, sea $m=n/d$. Entonces, $\langle\bar{m}\rangle$ es un subgrupo de orden d. Si H es un subgrupo de orden d, entonces $H\subseteq\operatorname{Ker} d\cdot=\langle\bar{m}\rangle$, luego $H=\langle\bar{m}\rangle$.

P5. Que G sea un subgrupo discreto equivale a decir que si una sucesión $\{g_n\}_{n\in\mathbb{N}}$ de elementos de G es converge a un punto $g\in\mathbb{R}^n$, entonces $g_n=g$, para todo $n\geq m$, para cierto m. Esto es equivalente a decir, que si una sucesión $\{g_n\}_{n\in\mathbb{N}}$ de elementos de G es converge a 0, entonces $g_n=0$, para todo $n\geq m$, para cierto m.

Procedamos por inducción sobre n.

Supongamos que $n=1$. Dados $g_1,g_2\in G$ no nulos, tenemos que $\langle g_1,g_2\rangle$ es un grupo abeliano finito generado sin torsión, luego es libre. Veamos que es de rango 1. Consideremos , el epimorfismo $\pi\colon\mathbb{Z}^2\to\langle g_1,g_2\rangle$, $\pi(n,m)=ng_1+mg_2$. Tenemos que $\mathbb{Z}^2=\langle g_1,g_2\rangle\oplus\operatorname{Ker}\pi$. Por tanto, el rango o es 1 (y hemos terminado), ó es 2 y en este caso $\operatorname{Ker}\pi=0$, es decir, g_1 y g_2 son $\mathbb{Z}$-linealmente independientes. Ahora bien, dados dos números reales ($g_1\neq g_2$) existen $\lambda_n,\mu_n\in\mathbb{Z}$, no nulos, de modo que $|\lambda_ng_1+\mu_ng_2|<1/n$. Entonces, la sucesión $\{\lambda_ng_1+\mu_ng_2\}$ converge a cero y llegamos a contradicción. Sea $g_1\in G$ no nulo, si $\langle g_1\rangle\subsetneq G$, sea $g_1'\in G\setminus\langle g_1\rangle$, tenemos $\langle g_1\rangle\subsetneq\langle g_1,g_1'\rangle=\langle g_2\rangle$. Si $\langle g_2\rangle\subsetneq G$, sea $g_2'\in G\setminus\langle g_2\rangle$, tenemos $\langle g_2\rangle\subsetneq\langle g_2,g_2'\rangle=\langle g_3\rangle$. Así sucesivamente vamos obteniendo una cadena

$$\langle g_1\rangle\subsetneq\langle g_2\rangle\subsetneq\cdots\subsetneq\langle g_n\rangle\subsetneq\cdots$$

que ha de estabilizar, porque si no la sucesión de números reales no nulos $\{g_n\}$ sería convergente a cero. Por tanto, $G=\langle g_n\rangle$, para un $n>>0$, y es libre de rango 1.

Supongamos $G\subset\mathbb{R}^n$, con $n>1$. Sea $\pi\colon\mathbb{R}^n\to\mathbb{R}^{n-1}$, $\pi(x_1,\ldots,x_n)=(x_2,\ldots,x_n)$. Veamos que $\pi(G)$ es un subgrupo discreto de $\mathbb{R}^{n-1}$: Sea $\{\pi(g_n)\}$, con $g_n\in G$ y $\pi(g_n)\neq 0$ para todo n, una sucesión convergente a 0. Podemos suponer que $||\pi(g_n)||<1$ para todo n. El núcleo del morfismo $\pi_{|G}\colon G\to\pi(G)$, es igual a $G\cap\mathbb{R}\times 0\overset{n-1}{\cdots}\times 0=\langle g\rangle$, por el caso $n=1$. Tomando $g_n+m\cdot g$, con $m\in\mathbb{Z}$ conveniente, en vez de g_n, podemos suponer que la primera coordenada es de módulo menor que $||g||$. Por tanto, $||g_n||\leq||\pi(g_n)||+||g||\leq 1+||g||$. Por tanto, $\{g_n\}$ es una sucesión de puntos que yacen en un compacto de $\mathbb{R}^n$. Luego, contiene una subsucesión convergente y llegamos a contradicción. Por hipótesis de inducción, $\pi(G)$ es un grupo abeliano libre de rango menor o igual que $n-1$. Por tanto, el epimorfismo $\pi_{|G}\colon G\to\pi(G)$ tiene sección y $G\simeq\pi(G)\oplus\operatorname{Ker}\pi_{|G}$ y como $\operatorname{Ker}\pi_{|G}$ es libre de rango menor o igual que 1, hemos concluido.

P6. Los divisores elementales de $x\cdot$ son x,x^3,x^5.

P7. El polinomio anulador divide a x^n, para $n>>0$. Luego los divisores elementales son potencias de x. Por tanto, solo hay tres casos $\{x^3\}$, $\{x^2,x\}$, $\{x,x,x\}$.

En dimensión 4, $\{x^4\},\{x^3,x\}$, $\{x^2,x^2\}$, $\{x^2,x,x\}$, $\{x,x,x,x\}$.

En dimensión 5, $\{x^5\},\{x^4,x\},\{x^3,x^2\}$, $\{x^3,x,x\}$, $\{x^2,x^2,x\}$, $\{x^2,x,x,x\}$, $\{x,x,x,x,x\}$.

P8. a) Los divisores elementales pueden ser $\{(x-1)^2,(x-1)^2,x-1\}$ o bien pueden ser $\{(x-1)^2,x-1,x-1,x-1\}$.

b) Los divisores elementales pueden ser $\{(x^2+4)^2,x^2+4,(x+8)^2\}$ o pueden ser $\{(x^2+4)^2,(x+8)^2,(x+8)^2\}$ o $\{(x^2+4)^2,(x+8)^2,x+8,x+8\}$.

P9. El polinomio anulador de T es x^3, $\dim_{\mathbb{R}}\operatorname{Ker}x\cdot=\dim_{\mathbb{R}}\operatorname{Ker}D^2=2$. Luego, solo hay dos divisores elementales que han de ser $\{x^3,x^3\}$.

P10. Escribamos

$$G\simeq(\mathbb{Z}/p_1^{n_{11}}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_1^{n_{1s_1}}\mathbb{Z})\oplus\cdots\oplus(\mathbb{Z}/p_r^{n_{r1}}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_r^{n_{rs_r}}\mathbb{Z}),$$

con $p_{11}\geq p_{12}\geq\cdots$, …, $p_{r1}\geq p_{r2}\geq\cdots$. El mínimo número natural n no nulo tal que $n\cdot g=0$ para todo $g\in G$ es $n=p_1^{n_{11}}\cdots p_r^{n_{r1}}$ y $|G|=\prod_{ij}p_i^{n_{ij}}$. G es cíclico si y solo si $s_1=\cdots=s_r=1$, que equivale a que $n=|G|$.

P11. Obvio.

P12. Es una sencilla comprobación.

P13. El polinomio característico de A es x^4-7x+5 que no tiene raíces múltiples. Luego, A solo tiene un factor invariante x^4-7x+5.

El polinomio característico de B es $x^2(2+x)^2$. La dimensión de $\operatorname{Ker}B$ es 1 y la dimensión de $\operatorname{Ker}(B+2)$ es 1. Luego, los divisores elementales son $x^2,(2+x)^2$.

El ideal anulador de $e=(1,0,0,0)$ es $x^2(2+x)^2$. Entonces una base de Jordan es $\{(2+x)^2\cdot e,x\cdot(2+x)^2\cdot e,x^2\cdot e,(2+x)\cdot x^2\cdot e\}$, es decir,

$$\{(2,4,2,4),(0,4,0,4),(2,-4,-2,4),(0,4,0,-4)\}.$$

En esta base la matriz asociada a B es

$$\begin{pmatrix}0&0&0&0\\1&0&0&0\\0&0&-2&0\\0&0&1&-2\end{pmatrix}.$$

P14.

$$\begin{pmatrix}x&1&0\\0&x-1&2\\-1&-1&x-3\end{pmatrix}\overset{F_1xF_3}{\rightsquigarrow}\begin{pmatrix}-1&-1&x-3\\0&x-1&2\\x&1&0\end{pmatrix}\overset{F_3+xF_1}{\rightsquigarrow}\begin{pmatrix}-1&-1&x-3\\0&x-1&2\\0&1-x&x(x-3)\end{pmatrix}$$
$$\overset{C_2-C_1}{\underset{C_3+(x-3)C_1}{\rightsquigarrow}}\begin{pmatrix}-1&0&0\\0&x-1&2\\0&1-x&x(x-3)\end{pmatrix}\overset{C_2xC_3}{\rightsquigarrow}\begin{pmatrix}-1&0&0\\0&2&x-1\\0&x(x-3)&1-x\end{pmatrix}\overset{F_3+\frac{x(3-x)}{2}F_2}{\rightsquigarrow}$$
$$\begin{pmatrix}-1&0&0\\0&2&x-1\\0&0&\frac{(x-1)^2(x-2)}{2}\end{pmatrix}\overset{C_3+\frac{1-x}{2}C_2}{\rightsquigarrow}\begin{pmatrix}-1&0&0\\0&2&0\\0&0&\frac{(x-1)^2(2-x)}{2}\end{pmatrix}.$$

Por tanto, $\mathbb{R}^3 \simeq \mathbb{R}[x]/((x-1)^2(2-x)) = \mathbb{R}[x]/(x-2) \oplus \mathbb{R}[x]/((x-1)^2)$ y los divisores elementales son $(x-2)$ y $(x-1)^2$.

Sea $e = (1,0,0)$ entonces una base de Jordan de T, es

$$\{(x-1)^2 e = (1,-2,1), (x-2)e = (-2,0,1), (x-1)(x-2)e = (2,-2,0)\}.$$

$\mathbb{R}^3 = [\mathbb{R}[x]/(x-2)] \cdot (1-2,1) \oplus [\mathbb{R}[x]/((x-1)^2)] \cdot (-2,0,1)$.

P15. $c_A(x) = (x-2)^4$, $\mathrm{Ker}(A-2\mathrm{Id}) = \langle((2,3,0,1),(0,-2,1,0)\rangle$ y $\mathrm{Ker}(A-2\mathrm{Id})^2 = \mathbb{C}^4$. Los vectores $(1,0,0,0)$ y $(0,1,0,0)$ son una base suplementaria de $\mathrm{Ker}(A-2\mathrm{Id})$ dentro de $\mathrm{Ker}(A-2\mathrm{Id})^2$. Entonces,

$$\{(1,0,0,0),(A-2\mathrm{Id})\cdot(1,0,0,0),(0,1,0,0),(A-2\mathrm{Id})\cdot(0,1,0,0)\}.$$

es una base de Jordan de A.

Tenemos que $c_B(x) = (x-2)^4$. $\mathrm{Ker}(B-2\mathrm{Id}) = \langle(0,2,0,1),(2,-1,1,0)\rangle$ que está estrictamente incluido en $\mathrm{Ker}(B-2\mathrm{Id})^2 = \langle(-4,0,0,1),(4,01,0),(2,1,0,0)\rangle$ que está estrictamente incluido en $\mathrm{Ker}(B-2\mathrm{Id})^3 = \mathbb{C}^4$. Una base suplementaria de $\mathrm{Ker}(B-2\mathrm{Id})^2$ dentro de $\mathrm{Ker}(B-2\mathrm{Id})^3 = \mathbb{C}^4$ es $(1,0,0,0)$. Tenemos la primera parte de nuestra base de Jordan: $\{(1,0,0,0),(B-2\mathrm{Id})\cdot(1,0,0,0),(B-2\mathrm{Id})^2\cdot(1,0,0,0)\}$, es decir,

$$\{(1,0,0,0),(-2,3,-2,0),(4,0,2,1)\}.$$

Por dimensiones $(-2,3,-2,0)$ es una base suplementaria de $\mathrm{Ker}(B-2\mathrm{Id})$ dentro de $\mathrm{Ker}(B-2\mathrm{Id})^2$. Por último como $(4,0,2,1),(0,2,0,1)$ es una base suplementaria de 0 dentro de $\mathrm{Ker}(B-2\mathrm{Id})$, la base de Jordan es

$$\{(1,0,0,0),(-2,3,-2,0),(4,0,2,1),(0,2,0,1)\}.$$

P16. Dado un $k[x]$-módulo M, entonces $M^* = \mathrm{Hom}_k(M,k)$ es un $k[x]$-módulo de modo natural: Dados $p(x) \in k[x]$ y $w \in M^*$, se define $(p(x)\cdot w)(m) := w(p(x)\cdot m)$.

El ideal anulador de M es igual al ideal anulador de M^*: Si $p(x)\cdot M = 0$, entonces $p(x)\cdot M^* = 0$. Por tanto, $\mathrm{Anul}(M) \subseteq \mathrm{Anul}(M^*)$. Si $p(x)\cdot M \neq 0$, existe $m \in M$ tal que $p(x)\cdot m \neq 0$. Sea $w \in M^*$ tal que $w(p(x)\cdot m) \neq 0$, entonces $p(x)\cdot w \neq 0$, ya que $(p(x)\cdot w)(m) = w(p(x)\cdot m) \neq 0$. Con todo, $\mathrm{Anul}(M) = \mathrm{Anul}(M^*)$.

Si $\dim_k M = n < \infty$, entonces $\dim_k M^* = n$. Si $M = k[x]/(p(x))$ entonces $M^* \simeq k[x]/(p(x))$, porque $\mathrm{Anul}(M^*) = \mathrm{Anul}(M) = (p(x))$, y $M^* \simeq k[x]/(p(x))$ por dimensiones. Si $M = M_1 \oplus M_2$, entonces $M^* = M_1^* \oplus M_2^*$ como $k[x]$-módulos. Por último si $M = \oplus_i k[x]/(p_i(x))$ entonces $M^* = \oplus_i k[x]/(p_i(x))^* = \oplus_i k[x]/(p_i(x))$.

Por último, si la matriz asociada a $x\cdot\colon M \to M$ en una base es (a_{ij}), entonces la matriz asociada a $x\cdot\colon M^* \to M^*$ en la base dual es la transpuesta de (a_{ij}).

P17. Por transformaciones elementales obtenemos

$$\left(\begin{array}{cc|c} 7 & 5 & 1 \\ 5 & 3 & 3 \end{array}\right) \overset{F_1-F_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 2 & 2 & -2 \\ 5 & 3 & 3 \end{array}\right) \overset{F_2-2F_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 2 & 2 & -2 \\ 1 & -1 & 7 \end{array}\right) \overset{F_1xF_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & -1 & 7 \\ 2 & 2 & -2 \end{array}\right)$$
$$\overset{F_2-2F_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & -1 & 7 \\ 0 & 4 & -16 \end{array}\right).$$

Luego, $y = -4$ y $x = 3$.

P18. Por transformaciones elementales obtenemos

$$\begin{pmatrix} 7 & 5 \\ 5 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 12 & 4 & 6 \\ 30 & 8 & 4 \\ 24 & 6 & 8 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -42 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

Luego el primer grupo es isomorfo a $\mathbb{Z}/4\mathbb{Z}$ y el segundo a $\mathbb{Z}/2ZZ \oplus \mathbb{Z}/42\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; y no pueden ser isomorfos por que tienen divisores elementales distintos $\{2^2\} \neq \{2,2,3,7,2\}$.

P19. Los divisores elementales son $\{2,2,3\}$ en tal caso el grupo es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, o son $\{2^2,3\}$ en tal caso el grupo es isomorfo a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. En ambos casos existen sistemas generadores formados por dos elementos.

P20. Es consecuencia inmediata del teorema de Cayley-Hamilton.

P21. El polinomio característico $c_T(x)$ y el polinomio anulador $p_{anul}(x)$ tienen las mismas raíces, por tanto, un polinomio es primo con $c_T(x)$ si y solo si es primo con $p_{anul}(x)$. Si $p(x)$ es primo con $p_{anul}(x)$ existen $\lambda(x)$ y $\mu(x)$ tales que $\lambda(x)p(x) + \mu(x)p_{anul}(x) = 1$. Por tanto, $\lambda(T) \circ p(T) + 0 = \mathrm{Id}$ y el inverso de $p(T)$ es $\lambda(T)$. Si $p(x)$ y $p_{anul}(x)$ no son primos entre sí, sea $q(x)$ el máximo común divisor. Observemos que si $q(T)$ es inyectivo, entonces el polinomio anulador sería $p_{anul}(x)/q(x)$, y esto es contradictorio. Como $\operatorname{Ker} q(T) \subseteq \operatorname{Ker} p(T)$. tenemos que $p(T)$ no es inyectivo, luego no es invertible.

P22. Sea $\{e_1,\dots,e_r\}$ una base de E' y (a_{ij}) la matriz de $T_{|E'}$. Sea $\{e_1,\dots,e_n\}$ una base de E, luego $\{\bar{e}_{r+1},\dots,\bar{e}_n\}$ es una base de E/E'. Sea (b_{kl}) la matriz de $\bar{T}$ en la base $\{\bar{e}_{r+1},\dots,\bar{e}_n\}$. La matriz de T en la base $\{e_1,\dots,e_n\}$ es de la forma

$$\left(\begin{array}{c|c} (a_{ij}) & (c_{rs}) \\ \hline 0 & (b_{kl}) \end{array}\right)$$

y el polinomio característico es

$$c_T(x) = \left|\begin{array}{c|c} (a_{ij}) - x\,\mathrm{Id} & (c_{rs}) \\ \hline 0 & (b_{kl}) - x\,\mathrm{Id} \end{array}\right| = c_{T_{|E'}}(x) \cdot c_{\bar{T}}(x).$$

P23. Sea $\{e_1,\dots,e_n\}$ una base de Jordan de T. La matriz de T es la base de Jordan es triangular, de diagonal $\alpha_1,\dots,\alpha_n$. Es fácil comprobar que la matriz de $p(T)$ en la base $\{e_1,\dots,e_n\}$ es triangular de diagonal $p(\alpha_1),\dots,p(\alpha_n)$. Luego el polinomio característico de $p(T)$ es $\prod_{i=1}^{n}(x - p(\alpha_i))$.

P24. Si $\alpha \in \mathbb{R}$, $E = \mathbb{C}[x]/(x-\alpha)^n$ y $T = x\cdot$, entonces tenemos el isomorfismo de $\mathbb{R}[x]$-módulos

$$\mathbb{C}[x]/((x-\alpha)^n) = \langle \bar{1}\rangle \oplus \langle \bar{i}\rangle \simeq \mathbb{R}[x]/((x-\alpha)^n) \oplus \mathbb{R}[x]/((x-\alpha)^n).$$

Si $\alpha \in \mathbb{C}\setminus\mathbb{R}$, $E = \mathbb{C}[x]/(x-\alpha)^n$ y $T = x\cdot$, entonces tenemos el isomorfismo de $\mathbb{R}[x]$-módulos

$$\mathbb{C}[x]/((x-\alpha)^n) = \langle \bar{1}\rangle \simeq \mathbb{R}[x]/(((x-\alpha)\cdot(x-\overline{\alpha}))^n).$$

En ambos casos, el polinomio característico de T como endomorfismo $\mathbb{R}$-lineal es $c_T(x)\cdot\overline{c_T(x)}$.

El caso general se deduce de que $E \simeq \oplus_{n_{\alpha,i}} \mathbb{C}[x]/((x-\alpha)^{n_{\alpha,i}})$.

P25. El núcleo del morfismo $\mathbb{R}[x] \to \mathbb{C}[x]/((x-\alpha)^n)$, $q(x) \mapsto \overline{q(x)}$ es igual a $(p(x)^n)$, porque $\overline{q(x)} = 0$ si y solo si α es una raíz de $q(x)$ de multiplicidad mayor o igual que n. Por tanto, $\mathbb{R}[x]/(p(x)^n) \simeq \mathbb{C}[x]/((x-\alpha)^n)$ (como $\mathbb{R}[x]$-módulos) porque es inyectivo y la dimensión de ambos es $2n$. En la base $\{1, \overline{x-\alpha}, \dots, \overline{x-\alpha}^{n-1}\}$ de $\mathbb{C}[x]/((x-\alpha)^n)$ como $\mathbb{C}$-espacio vectorial, la matriz de $x\cdot$ es la matriz de Jordan conocida. La base $\{1, i, \overline{x-\alpha}, i\overline{x-\alpha}, \dots, \overline{x-\alpha}^{n-1}, i\overline{x-\alpha}^{n-1}\}$ de $\mathbb{C}[x]/((x-\alpha)^n)$ como $\mathbb{R}$-espacio vectorial, es la base del problema buscada. Si $\alpha = i$, entonces $h_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y

$$x^3\cdot = \begin{pmatrix} h_i & h_0 & h_0 \\ h_1 & h_i & h_0 \\ h_0 & h_1 & h_i \end{pmatrix}^3 = [\begin{pmatrix} h_i & h_0 & h_0 \\ h_0 & h_i & h_0 \\ h_0 & h_0 & h_i \end{pmatrix} + \begin{pmatrix} h_0 & h_0 & h_0 \\ h_1 & h_0 & h_0 \\ h_0 & h_1 & h_0 \end{pmatrix}]^3 =$$

$$= \begin{pmatrix} -h_i & h_0 & h_0 \\ h_0 & -h_i & h_0 \\ h_0 & h_0 & -h_i \end{pmatrix} + \begin{pmatrix} h_0 & h_0 & h_0 \\ -3h_1 & h_0 & h_0 \\ h_0 & -3h_1 & h_0 \end{pmatrix} + \begin{pmatrix} h_0 & h_0 & h_0 \\ h_0 & h_0 & h_0 \\ 3h_i & h_0 & h_0 \end{pmatrix}$$

$$= \begin{pmatrix} -h_i & h_0 & h_0 \\ -3h_1 & -h_i & h_0 \\ 3h_i & -3h_1 & -h_i \end{pmatrix}.$$

$$e^{tx\cdot} = e^{\begin{pmatrix} th_i & h_0 & h_0 \\ h_0 & th_i & h_0 \\ h_0 & h_0 & th_i \end{pmatrix} + \begin{pmatrix} h_0 & h_0 & h_0 \\ th_1 & h_0 & h_0 \\ h_0 & th_1 & h_0 \end{pmatrix}} = e^{\begin{pmatrix} th_i & h_0 & h_0 \\ h_0 & th_i & h_0 \\ h_0 & h_0 & th_i \end{pmatrix}} \cdot e^{\begin{pmatrix} h_0 & h_0 & h_0 \\ th_1 & h_0 & h_0 \\ h_0 & th_1 & h_0 \end{pmatrix}}$$

$$= \begin{pmatrix} h_{e^{ti}} & h_0 & h_0 \\ h_0 & h_{e^{ti}} & h_0 \\ h_0 & h_0 & h_{e^{ti}} \end{pmatrix} \cdot \begin{pmatrix} h_1 & h_0 & h_0 \\ th_1 & h_1 & h_0 \\ \frac{t^2}{2}h_1 & th_1 & h_1 \end{pmatrix} = \begin{pmatrix} h_{e^{ti}} & h_0 & h_0 \\ th_{e^{ti}} & h_{e^{ti}} & h_0 \\ \frac{t^2}{2}h_{e^{ti}} & th_{e^{ti}} & h_{e^{ti}} \end{pmatrix}$$

con $h_{e^{ti}} = \begin{pmatrix} \cos t & -\operatorname{sen} t \\ \operatorname{sen} t & \cos t \end{pmatrix}$.

P26. Comprueba que $h_x = \begin{pmatrix} 0 & 0 & \cdots & -a_n \\ 1 & 0 & \cdots & -a_{n-1} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & -a_1 \end{pmatrix}$. Sea $K = k[y]/(p(y))$ y $\alpha = \bar{y}$. El morfismo $\phi\colon k[x]/(p(x)^m) \to K[x]/((x-\alpha)^m)$, $\phi(\overline{q(x)}) = \overline{q(x)}$ es un isomorfismo de $k[x]$-

módulos. La matriz del endomorfimo K-lineal $K[x]/((x-\alpha)^m) \to K[x]/((x-\alpha)^m)$, $\overline{q(x)} \mapsto \overline{xq(x)}$, en la base $\{\bar{1}, \bar{x}-\alpha, \ldots, \overline{(x-\alpha)^{m-1}}\}$ es la matriz de Jordan conocida. Via ϕ, la base requerida es igual a

$$\{1, \alpha, \ldots, \alpha^{n-1}; ; \ldots; (\bar{x}-\alpha)^{m-1}, (\bar{x}-\alpha)^{m-1}\alpha, \ldots, (\bar{x}-\alpha)^{m-1}\alpha^{n-1}\}.$$

P27. Escribamos el sistema de ecuaciones $\nabla(X_n) = A \cdot X_n$, con

$$X_n := \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix}, \quad \nabla(X_n) := X_{n+1} = \begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix}, \quad A := (a_{ij}).$$

Entonces, las soluciones serán $X_n = A^n \cdot C$, siendo C una matriz de una columna y tres filas con coeficientes constantes cualesquiera. Para calcular A^n para todo n, recordemos que $A = B \cdot J \cdot B^{-1}$, siendo J la matriz de Jordan asociada y que $A^n = B \cdot J^n \cdot B^{-1}$.

Bibliografía

[1] ATIYAH, M.F., MACDONALD, I.G.: *Introducción al Álgebra Conmutativa*, Ed. Reverté, 1973.

[2] BOURBAKI, N.: *Elements of Mathematics. Commutative Algebra*, Ed. Hermann - Adissson-Wesley, 1972.

[3] JACOBSON, N.: *Basic Algebra I*, W. H. Freeman and Company, San Francisco, 1974.

[4] KOSTRIKIN, A.I.: *Introducción al Álgebra*, McGraw-Hill, Madrid, 1992.

[5] LANG, S.: *Álgebra*, Ed. Aguilar, Madrid, 1971.

[6] NAVARRO, J.A.: *Álgebra Conmutativa Básica*, Manuales UEX 19, 1996.

[7] VAN DER WAERDEN, B.L.: *Modern Algebra*, Vol I. Frederick Ungar, New York, 1964.

Índice alfabético

198

UNIVERSIDAD DE EXTREMADURA

111