Teoría de Números Algebraica

Grado en Matemáticas

Colección manuales uex - 99

Pedro
Sancho de Salas

99

TEORÍA DE NÚMEROS ALGEBRAICA

GRADO EN MATEMÁTICAS

MANUALES UEX

99

PEDRO SANCHO DE SALAS

TEORÍA DE NÚMEROS ALGEBRAICA

GRADO EN MATEMÁTICAS

UNIVERSIDAD DE EXTREMADURA

2022

UNIVERSIDAD DE EXTREMADURA

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 1135-870-X
ISBN de méritos 978-84-606-9499-1

Índice general

Introducción

El presente texto está concebido por el autor como el manual de la asignatura cuatrimestral Teoría de Números, del cuarto curso del Grado de Matemáticas de la UEX. Este curso es una introducción a la Teoría de Números y hacemos un especial énfasis en la relación de esta teoría con la Teoría de Curvas Algebraicas. Suponemos que los alumnos han cursado antes un curso de Teoría de Galois (Álgebra I) y un curso de Variedades Algebraicas (Álgebra II).

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).

Describamos brevemente el contenido de la asignatura.

La Teoría de Números, "the Queen of Mathematics", es la rama de las Matemáticas más antigua y que modernamente usa conceptos y herramientas de las más diversas ramas de las Matemáticas, como el Álgebra, la Geometría, el Análisis, la Variable Compleja, etc. La Teoría de Números es la rama de las matemáticas que estudia los números naturales y las soluciones de los sistemas de ecuaciones diofánticas (sistemas de ecuaciones con coeficientes números enteros). El estudiante conoce ya tópicos de la Teoría de Números: El teorema fundamental de la Aritmética (o teorema de factorización única), la teoría de congruencias, etc.

Para la resolución de múltiples problemas enunciados sólo en términos de números naturales y para la resolución de los sistemas de ecuaciones diofánticas, es necesario considerar los anillos de números, que son los anillos generados por raíces de un polinomio con coeficientes enteros. Por ejemplo, en el problema de qué números primos son suma de dos cuadrados perfectos conviene considerar el anillo de enteros de Gauss $\mathbb{Z}[i]$. Este anillo es un anillo euclídeo, por lo tanto es un dominio de factorización única.

Por desgracia, en general los anillos de números no son dominios de factorización única. Dado un anillo de números, A, existe un número finito de fracciones $\frac{a_i}{b_i}$ (donde $a_i, b_i \in A$ y $\frac{a_i}{b_i}$ son raíces de polinomios mónicos con coeficientes en $\mathbb{Z}$) de modo que $B := A[\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}]$ ya es casi un dominio de factorización única: todo ideal de B es igual a un producto de ideales primos de modo único. Estos anillos, B, son anillos localmente de ideales principales (como lo es $\mathbb{Z}$). Para todo ello estudiaremos la dependencia entera y la desingularización. Estamos hablando, pues, de los dominios de factorización única y cómo resolver el problema de que un anillo de números no sea dominio de factorización

única.

Para el estudio de un anillo de números A (como para el estudio de las ecuaciones diofánticas), conviene estudiar A/pA para todo primo p, es decir, conviene hacer congruencias módulo p. Así el grupo de Galois de un polinomio $P(x)$ con coeficientes en $\mathbb{Z}$ (o con coeficientes en un anillo de números A) , queda determinado por el grupo de Galois de las reducciones de $P(x)$ módulo p (variando los primos p), que es el grupo de Galois de un cuerpo finito, que es un grupo cíclico generado por el automorfismo de Fröbenius. Obtendremos múltiples aplicaciones de este hecho, entre ellas el cálculo del grupo de Galois de diversos polinomios, la Ley de reciprocidad cuadrática de Gauss, etc.

Para el estudio de un anillo de números A (y la clasificación de estos anillos) se introducen el discriminante de A, el grupo $\mathrm{Pic}(A)$ y el grupo de los invertibles de A. El teorema de Hermite afirma que solo existe un número finito de cuerpos de números de discriminante fijo dado. El grupo $\mathrm{Pic}(A)$ es el grupo de los ideales de A, módulo isomorfismos. Mide la obstrucción a que el anillo A no sea un dominio de factorización única. Probamos que es un grupo finito y como consecuencia se obtiene que existe una extensión finita de anillos B de A, tal que todo ideal de A extendido a B es principal. Probamos que el grupo de los invertibles de A, que son los elementos de norma ± 1, es un grupo finito generado, cuya parte de torsión es el grupo de las raíces de la unidad que están en A.

Por último introducimos la función zeta de Riemann, que es de gran importancia en la Teoría de números en el estudio de la distribución de los números primos. Aplicamos la función zeta para determinar cuándo dos extensiones de Galois son isomorfas y para demostrar que un sistema de ecuaciones diofánticas tiene soluciones complejas si y solo módulo p admite soluciones enteras, para infinitos p.

La Teoría de Curvas Algebraicas y la Teoría de Números están estrecha y sorprendentemente relacionadas. $\mathbb{Z}$ y $k[x]$ son anillos euclídeos y ambos son dominios de factorización única. Los anillos de funciones algebraicas de las curvas algebraicas son $k[x]$-álgebras finitas (geométricamente: toda curva se proyecta vía un morfismo finito en la recta afín). Los anillos de números, como veremos, son $\mathbb{Z}$-álgebras finitas ($\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$ son ejemplos). Estamos hablando en ambos casos de anillos noetherianos de dimensión de Krull 1. Entre estos anillos, en ambas teorías, destacarán los anillos que son localmente anillos de ideales principales: los anillos de Dedekind. En la teoría de Galois se han estudiado anillos de dimensión de Krull cero, ahora estudiamos los de dimensión de Krull 1.

Finalmente, quiero agradecer al profesor Juan Antonio Navarro González el haber puesto a mi disposición sus notas sobre la Teoría de Números, en las que me he basado para escribir este curso. También agradezco al profesor Juan Bautista Sancho de Salas sus notas sobre valoraciones y valores absolutos que he seguido para escribir el capítulo quinto.

Capítulo 1

Dominios de factorización única

1.1. Introducción

Todo número natural se escribe de modo único como producto de números primos. En este capítulo vamos a estudiar los anillos donde se cumple esta propiedad, es decir, aquellos anillos donde todo elemento (no nulo, ni invertible) es producto de elementos irreducibles de modo único (salvo orden de los factores y multiplicación por invertibles).

1.2. Anillos euclídeos

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

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

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 $\delta(r)<\delta(b)$.

2. Ejercicio: Sea (A,δ) un anillo euclídeo. Pruébese que $a\in A\setminus\{0\}$ es invertible si y solo si $\delta(a)=\delta(1)$. Pruébese que si $a\in A\setminus\{0\}$ no es invertible entonces $\delta(a)>\delta(1)$. Sea $\delta'\colon A\setminus\{0\}\to\mathbb{N}$, $\delta'(a):=\delta(a)-\delta(1)$. Pruébese que (A,δ') es un anillo euclídeo y que $a\in A\setminus\{0\}$ es invertible si y solo si $\delta'(a)=0$.

3. Ejemplos de anillos euclídeos:

El anillo de los números enteros: Definimos $\delta\colon\mathbb{Z}\setminus\{0\}\to\mathbb{N}$, $\delta(n):=|n|$, donde $|n|=n$ si n es positivo y $|n|=-n$ si n es negativo. Es fácil de probar que $(\mathbb{Z},\delta)$ es un anillo euclídeo.

Los anillos de polinomios: Dado $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$, con $a_n \neq 0$, diremos que es de grado n y denotaremos $gr(p(x)) = n$. Seguiremos la convención: $gr(0) = -\infty$.

Si A es un anillo íntegro, entonces el grado de polinomios es aditivo, es decir, se cumple la fórmula

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

para cada par de polinomios $p(x), q(x) \in A[x]$. Por tanto, si $p(x)$ 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. $gr(r(x)) < gr(q(x))$.

Demostración. Existencia: Si $\mathrm{gr}\, q(x) > \mathrm{gr}\, p(x)$ entonces $c(x) = 0$ y $r(x) = p(x)$. Supongamos $\mathrm{gr}\, q(x) = m \leq n = \mathrm{gr}\, p(x)$ y escribamos $p(x) = a_0 x^n + \ldots + a_n$ y $q(x) = b_0 x^m + \cdots + b_m$. Procedemos por inducción sobre $\mathrm{gr}\, p(x)$. Si $\mathrm{gr}\, p(x) = 0$, entonces $\mathrm{gr}\, q(x) = 0$ y $c(x) = \frac{a_0}{b_0}$ y $r(x) = 0$. Sea, pues, $\mathrm{gr}(p(x)) > 0$. 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, $(k[x], \mathrm{gr})$ es un anillo euclídeo.

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. Veamos que es un anillo euclídeo. Consideremos la aplicación

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

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 $\delta(r) < \delta(z')$. En conclusión, $(\mathbb{Z}[i], \delta)$ es un anillo euclídeo.

1.3. Dominios de ideales principales

1. Definición: Sea A un anillo. Diremos que un ideal $I \subset A$ 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.

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

Demostración. Sea (A,δ) un anillo euclídeo. Sea $I \subset A$ 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 $I = i \cdot A$: Sea $j \in I$ no nulo y $c, r \in A$ de modo que $j = c \cdot i + r$ y $r = 0$ ó $\delta(r) < \delta(j)$. Observemos que $r \in I$, luego no es posible que $\delta(r) < \delta(j)$. 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 $n > 1$).

3. Definición: Los elementos de un anillo íntegro que no son nulos ni invertibles se los denomina elementos propios del anillo.

4. Definiciones: Un elemento propio de un anillo íntegro se dice que es irreducible si no descompone en producto de dos elementos propios. Un elemento propio a de un anillo íntegro se dice que es primo si (a) es un ideal primo. Se dice que dos elementos propios son primos entre sí, si carecen de divisores propios comunes.

5. Nota: Según la definición $-5 \in \mathbb{Z}$ es primo, si bien cuando hablemos de un *número primo* nos referiremos a un número natural primo (en $\mathbb{Z}$).

6. Proposición: *Sea A un anillo íntegro. Los elementos primos de A son irreducibles.*.

Demostración. Sea $a \in A$ primo. 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. □

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

1. *p es un irreducible de A.*
2. *p es un primo de A.*

3. pA es un ideal maximal de A.

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

2. $\Rightarrow$ 1. Es consecuencia de 1.3.6.

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

□

Si A es d.i.p. entonces no existen más ideales primos que (0) y que los maximales: Si tenemos $(0) \underset{\neq}{\subset} \mathfrak{p} = (t') \subseteq \mathfrak{m} = (t)$, siendo $\mathfrak{p}$ un ideal primo y $\mathfrak{m}$ maximal, entonces $t' = t \cdot t''$, para cierto $t'' \in A$. Como (t') es primo, entonces t' es irreducible, luego t'' es invertible y $\mathfrak{p} = \mathfrak{m}$. En conclusión, A es un cuerpo o A es un anillo de dimensión de Krull 1.

1.4. 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. El acrónimo d.f.u. significará dominio de factorización única.

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.

□

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 $I_m = I_{m+1} = I_{m+2} = \cdots$.

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 de A es primo.*

Demostración. $\Rightarrow$) Si $a = p_1^{n_1} \cdots p_r^{n_r}$ y $aA \underset{\neq}{\subset} bA$ entonces $b = p_1^{m_1} \cdots p_r^{m_r} \cdot inv$, donde los $m_i \leq n_i$ para todo i, y para algún i, $m_i < n_i$. 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 $(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \dots$ que ha de ser finita por noetherianidad y terminará cuando a_n sea irreducible.

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 $(a) \underset{\neq}{\subset} (b_1) \underset{\neq}{\subset} (b_2) \underset{\neq}{\subset} \dots$ 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). Pongamos $p_1 = q_1$ (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. Proposición: *Si A es un dominio de ideales principales entonces toda cadena ascendente de ideales (principales) es estable.*

Demostración. 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 $I = I_m = I_{m+1} = \cdots$.

□

5. Teorema: *Los dominios de ideales principales son dominios de factorización única. En particular, los anillos euclídeos son dominos de factorización única.*

Demostración. Es consecuencia inmediata de la proposición 1.3.7 y el teorema 1.4.3.

□

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 $p_1, \dots, p_r$ 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:

$$m.c.d.(a,b) = p_1^{\min(n_1,m_1)} \cdots p_r^{\min(n_r,m_r)}$$
$$m.c.m.(a,b) = p_1^{\max(n_1,m_1)} \cdots p_r^{\max(n_r,m_r)}$$

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.

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 $aA \cap bA$. Por tanto, el máximo común divisor y el mínimo común múltiplo de dos elementos de un dominio de ideales principales A siempre existen y están bien definidos salvo factores invertibles.

6. 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*

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

7. 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} 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.

8. Dados dos números enteros $n,m \in \mathbb{Z}$, 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.

9. 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. $2000=7\cdot266+138$. b. $266=1\cdot138+128$. c. $138=1\cdot128+10$. d. $128=12\cdot10+8$ e. $10=1\cdot8+2$. Luego, $m.c.d(2000,266)=2$. Lo cual era evidente, pero ahora sabremos calcular n y m: $2=10-1\cdot8=10-1\cdot(128-12\cdot10)=-128+13\cdot10=-128+13(138-128)=13\cdot138-14\cdot128=13\cdot138-14(266-138)=-14\cdot266+27\cdot138=-14\cdot266+27(2000-7\cdot266)=27\cdot2000-203\cdot266$.

Por tanto, una solución particular de nuestro sistema de ecuaciones diofánticas es $x_0=-2\cdot27=-54$, $y_0=-2\cdot203=-406$. Las soluciones de la ecuación homogénea $2000x-266y=0$ son las soluciones de $1000x-133y=0$, que son $x=n\cdot133$, $y=n\cdot1000$. Todas las soluciones de nuestro sistema de ecuaciones diofánticas son

$$\begin{cases} x=-54+n\cdot133\\ y=-406+n\cdot1000\end{cases}$$

1.5. $K[x_1,\ldots,x_n]$ es d.f.u.

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 $\Sigma=A_{A\setminus0}$. 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. Sea $p(x)\in A[x]$ un polinomio no constante 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 $A[x]$ (luego es primitivo). 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 1.5.2 1., $p_1(x)\cdot p_2(x)$ es primitivo. Por el lema 1.5.2 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

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

la descomposición en irreducibles en $\Sigma[x]$. Por el lema 1.5.2 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 1.5.2 1., $q_1(x) \cdots q_r(x)$ es primitivo. Por el lema 1.5.2 2., v es un invertible de A.

• Cada $q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por 1.5.3.

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

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

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 1.5.3. $\Sigma[x]$ es d.f.u. , 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.*

1.6. Anillos noetherianos

1. Definición : Se dice que un A-módulo M es noetheriano si todo submódulo de M es finito generado. Se dice que un anillo A es noetheriano si es un A-módulo noetheriano, es decir, si todo ideal es finito generado.

2. Ejemplos : Si k es un cuerpo entonces es un anillo noetheriano y los k-módulos noetherianos son los k-espacios vectoriales de dimensión finita.

$\mathbb{Z}$ y $k[x]$ son anillos noetherianos.

Los dominios de ideales principales son noetherianos.

3. Proposición : *Un módulo M es noetheriano si y solo si toda cadena creciente de submódulos de M, $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ estabiliza, es decir, para $n >> 0$, $M_n = M_m$, para todo $m \geq n$.*

Demostración. Si M es noetheriano y $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ una cadena creciente de submódulos de M, consideremos el submódulo $N := \cup_i M_i = \langle m_1, \ldots, m_r \rangle$. Para $n >> 0$, $m_1, \ldots, m_r \in M_n$, luego $M_n \subseteq N \subseteq M_n$, es decir, $N = M_n$ y $M_n = M_m$, para todo $m \geq n$.

Veamos el recíproco. Sea N un submódulo, si $N \neq 0$ sea $0 \neq m_1 \in N$ y $M_1 := \langle m_1 \rangle$. Si $M_1 \neq N$, sea $m_2 \in N \setminus M_1$ y $M_2 := \langle m_1, m_2 \rangle$. Así sucesivamente vamos construyendo una cadena $0 \underset{\neq}{\subset} M_1 \underset{\neq}{\subset} M_2 \underset{\neq}{\subset} M_3 \underset{\neq}{\subset} \cdots$ que por la propiedad exigida a M ha de ser finita. Luego, para $n >> 0$, $N = M_n = \langle m_1, \ldots, m_n \rangle$.

□

4. Teorema: *Sea A un anillo noetheriano íntegro. A es un dominio de factorización única si y solo si todo elemento irreducible de A genera un ideal primo.*

Demostración. Es consecuencia inmediata del teorema 1.4.3. □

5. Teorema: *Sea A un anillo noetheriano íntegro. A es d.i.p. si y solo si todo ideal maximal es principal.*

Demostración. $\Leftarrow$) Sea $I = (i_1, \ldots, i_n)$ un ideal no nulo de A. Podemos suponer que $i_1 \neq 0$. Si $I \underset{\neq}{\subset} A$ entonces está incluido en un ideal maximal, $I \subseteq \mathfrak{m}_1 = (t_1)$. Por tanto, $i_j = t_1 \cdot i'_j$ para ciertos $i'_j \in A$, para todo j, además $(i_1) \underset{\neq}{\subset} (i'_1)$. Tenemos que $I = t_1 \cdot (i'_1, \ldots, i'_n)$. Sea $I_2 = (i'_1, \ldots, i'_n)$. Si $I_2 \underset{\neq}{\subset} A$ entonces está incluido en un ideal maximal, $I_2 \subseteq \mathfrak{m}_2 = (t_2)$. Por tanto, $i'_j = t_2 \cdot i''_j$ para ciertos $i''_j \in A$, además $(i'_1) \underset{\neq}{\subset} (i''_1)$. Tenemos que $I = t_1 \cdot t_2 \cdot (i''_1, \ldots, i''_n)$. Este proceso por noetherianidad ha de terminar en un número finito n de pasos y terminará cuando $I = t_1 \cdots t_n \cdot I_n$ con $I_n = A$. Es decir, $I = (t_1 \cdots t_n)$.

□

6. Proposición: *Sea A un anillo noetheriano íntegro de dimensión de Krull 1. A es d.i.p. si y solo si es d.f.u.*

Demostración. $\Leftarrow$) Sea $\mathfrak{p}$ un ideal primo no nulo. Consideremos un elemento de $\mathfrak{p}$ no nulo, que será producto de irreducibles, luego existe $t \in \mathfrak{p}$ irreducible. Como A es de dimensión de Krull 1, $\mathfrak{p} = (t)$. Por el teorema anterior, A es d.i.p. □

7. Proposición: *Sea M un A-módulo y $N \subseteq M$ un submódulo. M es noetheriano $\iff$ N y M/N son noetherianos.*

Demostración. La implicación directa es obvia.

Veamos la inversa: Dado un submódulo $N' \subset M$, tenemos que $N' \cap N = \langle n_1, \ldots, n_r \rangle$ es un módulo finito generado. La imagen del morfismo $N' \to M/N$, $n' \mapsto \bar{n'}$ es isomorfa a $N'/(N' \cap N)$, que como es un submódulo de M/N, es un módulo finito generado. Por tanto, $N'/(N' \cap N) = \langle \bar{m}_1, \ldots, \bar{m}_s \rangle$. Luego, $N' = \langle n_1, \ldots, n_r, m_1, \ldots, m_s \rangle$. □

8. Corolario : *$M = M' \oplus M''$ es un A-módulo noetheriano si y solo si M' y M'' son A-módulos noetherianos.*

Demostración. Podemos considerar M' como submódulo de M: $M' \hookrightarrow M$, $m' \mapsto (m', 0)$. Como $M/M' \simeq M''$, $\overline{(m', m'')} \mapsto m''$, concluimos por la proposición anterior. □

9. Teorema : *Si A es un anillo noetheriano todo A-módulo finito generado es noetheriano.*

Demostración. Si $M = A^n$ entonces es noetheriano por el corolario anterior. Si $M = \langle m_1, \dots, m_n \rangle$, entonces es isomorfo a un cociente de A^n: $A^n \to M$, $(a_i) \mapsto \sum_i a_i m_i$. Por tanto, M es noetheriano. □

10. Ejemplo : $\mathbb{Z}[\sqrt[3]{2}] \simeq \mathbb{Z}[x]/(x^3 - 2)$ es un $\mathbb{Z}$-módulo generado por $\bar{1}, \bar{x}, \bar{x}^2$ (de hecho es una base). Por tanto, $\mathbb{Z}[\sqrt[3]{2}]$ es un $\mathbb{Z}$-módulo noetheriano. Luego, $\mathbb{Z}[\sqrt[3]{2}]$ es un anillo noetheriano.

11. Teorema de la base de Hilbert : *Si A es un anillo noetheriano entonces $A[x]$ es un anillo noetheriano.*

Demostración. Sea $I \subset A[x]$ un ideal. Tenemos que ver que es finito generado:

Sea $J \subseteq A$ el conjunto formado por los coeficientes de máximo grado de los $p(x) \in I$. Es fácil ver que J es un ideal de A. Observemos para ello, que si $p(x) = a_0 x^n + \cdots + a_n, q(x) = b_0 x^m + \cdots + b_m \in I$, entonces $x^m p(x) + x^n q(x) = (a_0 + b_0) x^{n+m} + \cdots \in I$, luego si $a_0, b_0 \in J$ entonces $a_0 + b_0 \in J$.

Por ser A noetheriano, $J = (b_1, \dots, b_r)$ es finito generado. Así, existen $p_1, \dots, p_r \in I$ cuyos coeficientes de grado máximo son $b_1, \dots, b_r$, respectivamente. Además, multiplicando cada p_i por una potencia conveniente de x, podemos suponer que $\operatorname{gr} p_1 = \cdots = \operatorname{gr} p_r$. Escribamos $\operatorname{gr} p_i = m$.

Dado $p(x) = a_0 x^n + \cdots + a_n \in I$. Supongamos que $n \geq m$. Escribamos $a_0 = \lambda_1 b_1 + \cdots + \lambda_r b_r$, con $\lambda_i \in A$ para todo i. Tenemos que $p(x) - \sum_i \lambda_i x^{n-m} p_i \in I$ y $\operatorname{gr}(p(x) - \sum_i \lambda_i x^{n-m} p_i) < \operatorname{gr} p(x)$.

Recurrentemente obtendré que

$$I = (p_1, \dots, p_r)_{A[x]} + I \cap \{A + Ax + \cdots + Ax^{m-1}\}$$

Ahora bien, $I \cap \{A + Ax + \cdots + Ax^{m-1}\}$ es un A-módulo finito generado ya que es submódulo de $\{A + Ax + \cdots + Ax^{m-1}\}$, que es un A-módulo noetheriano. En conclusión, si escribimos $I \cap \{A + Ax + \cdots + Ax^{m-1}\} = \langle q_1, \dots, q_s \rangle_A$, tenemos que $I = (p_1, \dots, p_r, q_1, \dots, q_s)$. □

12. Corolario : *Si A es un anillo noetheriano entonces $A[x_1, \dots, x_n]/I$ es un anillo noetheriano.*

Demostración. $A[x_1,\dots,x_n] = A[x_1,\dots,x_{n-1}][x_n]$ es noetheriano por el teorema de la base de Hilbert y por inducción sobre n. Por tanto, el cociente $A[x_1,\dots,x_n]/I$ es un anillo noetheriano. □

1.7. Ejemplos

Veamos algunos ejemplos y problemas clásicos de la teoría de números.

1. Sabemos resolver los sistemas de ecuaciones lineales diofánticos. Consideremos el sistema de ecuaciones

$$\begin{gathered} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{gathered}$$

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), sabemos calcular matrices cuadradas invertibles F y C de modo que $F \cdot A \cdot C = (d_{ij})$, con $d_{ij} = 0$ para todo $i \neq j$. Entonces, si denotamos $x' := C^{-1} \cdot x$ y $b' := B \cdot b$,

$$(d_{ij}) \cdot x' = F \cdot (a_{ij}) \cdot C \cdot x' = F \cdot A \cdot x = F \cdot b = b'$$

Sistema que es sencillo de resolver, y acabamos porque $x = C \cdot x'$.

2. El anillo de los enteros de Gauss, $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, es euclídeo. Veamos que *un número primo $p \in \mathbb{Z}$ descompone en suma de dos cuadrados perfectos si y solo si p no es irreducible en $\mathbb{Z}[i]$*: 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.

Sea $\mathbb{F}_p^{*2} = \{a^2, a \in \mathbb{F}_p^*\}$, con $p \neq 2$. El núcleo del epimorfismo $\mathbb{F}_p^* \to \mathbb{F}_p^{*2}$, $a \mapsto a^2$ 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 $\mathbb{F}_p^* \to \{\pm 1\}$, $a \mapsto a^{\frac{p-1}{2}}$ (el polinomio $x^{\frac{p-1}{2}} - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene a lo más $\frac{p-1}{2}$ raíces en $\mathbb{Z}/p\mathbb{Z}$).

Por tanto, $-1 \in \mathbb{F}_p^{*2}$ 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 $p = 2$.

Sea $n \in \mathbb{Z}$ suma de dos cuadrados perfectos, $n = a^2 + b^2 = (a+bi)\cdot(a-bi)$. Sea $p \in \mathbb{Z}$ un número primo, irreducible en $\mathbb{Z}[i]$, que divida a n. Por ser p irreducible en $\mathbb{Z}[i]$, p divide a $a+bi$ (ó a $a-bi$). Luego p divide á a y b. Tenemos que $n = p^2 \cdot n'$ con $n' = (\frac{a}{p} + \frac{b}{p}\cdot i)\cdot(\frac{a}{p} - \frac{b}{p}\cdot i)$. Si n es producto de números enteros que son suma de cuadrados perfectos entonces n es suma de cuadrados perfectos. Por tanto, *la condición necesaria y suficiente para que un número natural sea suma de dos cuadrados perfectos es que en la descomposición como producto de potencias de primos los exponentes de los primos congruentes con* 3 mód 4 *sean pares.*

3. Resolvamos la ecuación diofántica

$$a^2 + b^2 = 2178$$

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

$$\{(a,b) = (33,33),(-33,-33),(-33,33),(33,-33)\}.$$

Calculemos las soluciones racionales de la ecuación anterior: Dados $z, z' \in \mathbb{Q}[i]$, $\delta(z) = \delta(z')$ si y solo existe $z'' \in \mathbb{Q}[i]$ tal que $z = z'z''$ y $\delta(z'') = 1$. El teorema 90 de Hilbert afirma que $\delta(z'') = 1$ si y solo si $z'' = (c+di)/(c-di) = \frac{c^2-d^2}{c^2+d^2} + \frac{2cd}{c^2+d^2}i$. Por tanto, $\delta(a+bi) = 2178$ si y solo

$$a+bi \in (33+33i)\cdot\{\frac{c^2-d^2}{c^2+d^2} + \frac{2cd}{c^2+d^2}i : c,d \in \mathbb{Z}\} = \{\frac{33(c-d)^2}{c^2+d^2} + 33\frac{c^2-d^2+2cd}{c^2+d^2}i : c,d \in \mathbb{Z}\}$$

4. El anillo de números de Eisenstein, $\mathbb{Z}[e^{2\pi i/3}]$, es un anillo euclídeo: Se puede argumentar igual que como hemos hecho con el anillo de números de Gauss.

5. La ecuación de Fermat $x_1^3 + x_2^3 = x_3^3$ no tiene soluciones enteras $x_1x_2x_3 \neq 0$:

Si x_1, x_2, x_3 son una solución y x_1, x_2, x_3 son múltiplos de n entonces $x_1/n, x_2/n, x_3/n$ son una solución. Podemos suponer que $(x_1, x_2, x_3) = (1)$. Si dos de x_1, x_2, x_3 son múltiplos de n, entonces el tercero lo es, luego $(x_1, x_2) = (x_1, x_3) = (x_2, x_3) = (1)$. Reordenando las variables x_1, x_2, x_3 y cambiando alguna de signo si es necesario, podemos suponer que x_1 y x_2 no son múltiplos de 3. Si x_3 no es múltiplo de 3, llegamos a contradicción porque es imposible que $x_1^3 + x_2^3 = x_3^3 \mod 9$, ya que $x_i^3 = \pm 1 \mod 9$, para todo i. Por tanto, x_3 es múltiplo de 3.

Sea $\xi = e^{\frac{2\pi}{3}}$ y trabajemos en el anillo de Eisenstein $\mathbb{Z}[\xi] \simeq \mathbb{Z}[x]/(x^2+x+1)$, que es un anillo euclídeo. Los elementos invertibles de $\mathbb{Z}[\xi]$ son $\{\pm 1, \pm\xi, \pm\xi^2\}$, porque $a+b\xi$ es invertible si y solo si $1 = |a+b\xi|^2 = (a+b\xi)\cdot(a+b\xi^2) = a^2+b^2-ab$. El elemento $\sqrt{-3} = (1-\xi)\cdot\xi$ es irreducible porque $\mathbb{Z}[\xi]/(1-\xi) = \mathbb{Z}[x]/(x^2+x+1, 1-x) = \mathbb{Z}/(3)$ es íntegro.

Basta demostrar que no existen $x_1, x_2, x_3 \in \mathbb{Z}[\xi]$, primos dos a dos y con x_3 múltiplo de $\xi - 1$, que sean solución de la ecuación de Fermat. Sea x_1, x_2, x_3 una solución con $|x_1 x_2 x_3|$ mínimo. Escribamos $x_1 = a + b \cdot (\xi - 1) \in \mathbb{Z}[\xi] = \mathbb{Z}[\xi - 1]$, con $a, b \in \mathbb{Z}$. Tenemos que $\bar{a} = \bar{x}_1 \neq 0$ en $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}[\xi]/(\xi - 1)$. Además, módulo (3), $\xi \cdot x_1 = (1 + (\xi - 1)) \cdot x_1 = a + (a + b)(\xi - 1)$ y $\xi^2 \cdot x_1 = a + (2a + b)(\xi - 1)$. Como b ó $a + b$ ó $2a + b$ es múltiplo de 3, cambiando x_1 por $\xi \cdot x_1$ ó $\xi^2 \cdot x_1$, si es necesario, podemos suponer que b es múltiplo de 3. Igualmente, si $x_2 = a' + b'(\xi - 1)$ podemos suponer que b' es múltiplo de 3. En $\mathbb{Z}[\xi]/(\xi - 1) = \mathbb{Z}/3\mathbb{Z}$, tenemos que $a + a' = x_1 + x_2 = x_1^3 + x_2^3 = x_3^3 = 0$, luego $a + a'$ es múltiplo de 3 y $x_1 + x_2$ es múltiplo de 3.

Sean $s_1 = x_1 + \xi x_2$, $s_2 = x_1 + \xi^2 x_2$ y $s_3 = x_1 + x_2$, entonces, $s_1 \cdot s_2 \cdot s_3 = x_3^3$. Observemos que $x_1 + x_2$ es primo con x_2 porque x_1 es primo con x_2. Entonces,

$$(x_1 + x_2, x_1 + \xi x_2) = (x_1 + x_2, (\xi - 1)x_2) = (x_1 + x_2, \xi - 1) = (\xi - 1).$$
$$(x_1 + x_2, x_1 + \xi^2 x_2) = (x_1 + x_2, (\xi^2 - 1)x_2) = (x_1 + x_2, \xi - 1) = (\xi - 1).$$
$$(x_1 + \xi x_2, x_1 + \xi^2 x_2) = (x_1 + \xi x_2, (\xi^2 - \xi)x_2) = (x_1 + \xi x_2, \xi - 1) = (\xi - 1).$$

Por lo tanto, $(s_i, s_j) = (\xi - 1)$ para todo $i \neq j$. Entonces,

$$s_1' = \frac{s_1}{\xi - 1} = \frac{x_1 + \xi x_2}{\xi - 1} = \frac{x_1 + x_2}{\xi - 1} + x_2$$
$$s_2' = \frac{\xi \cdot s_2}{\xi - 1} = \frac{\xi x_1 + x_2}{\xi - 1} = \frac{x_1 + x_2}{\xi - 1} + x_1$$
$$s_3' = \frac{\xi^2 s_3}{\xi - 1} = \frac{\xi^2 (x_1 + x_2)}{\xi - 1}$$

son primos dos a dos, y

$$s_1' \cdot s_2' \cdot s_3' = (x_3/(\xi - 1))^3 \quad \text{y} \quad s_1' + s_2' = -s_3'.$$

Por lo tanto, s_1', s_2' y s_3' son cubos salvo multiplicación por invertibles. Además, $\frac{x_1 + x_2}{\xi - 1}$ (o equivalentemente s_3'), que es múltiplo de $\xi - 1$, es múltiplo de $(\xi - 1)^{3m}$, luego es múltiplo de 3.

Veamos cómo es un cubo de $\mathbb{Z}[\xi] = \mathbb{Z}[\xi - 1]$, módulo (3):

$$\overline{c + d(\xi - 1)}^3 = \bar{c}^3 = \bar{c} \in \mathbb{Z}/3\mathbb{Z} \subset \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cdot (\xi - 1).$$

Como $s_1' = \bar{x}_2 = \bar{a}'$, $\xi \cdot s_1' = \bar{a}' + \bar{a}' \cdot (\xi - 1)$ y $\xi^2 \cdot s_1' = (-1 - \xi) \cdot \bar{a}' = -2\bar{a}' - \bar{a}' \cdot (\xi - 1)$ entonces, $s_1' = y_1^3$, igualmente $s_2' = y_2^3$, y por tanto $-s_3' = y_3^3$. Luego,

$$y_1^3 + y_2^3 = y_3^3.$$

Observemos que y_1, y_2, y_3 son primos dos a dos porque s_1', s_2', s_3' son primos dos a dos. Además, y_3 es múltiplo de $\xi - 1$, porque lo es s_3'. Por último,

$$|y_1 y_2 y_3| = \sqrt[3]{|s_1' s_2' s_3'|} = \left|\frac{x_3}{\xi - 1}\right| < |x_1 x_2 x_3|$$

y hemos llegado a contradicción.

6. Kummer, para probar el teorema de Fermat, es decir, para demostrar que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras ($xyz \neq 0$) hizo la descomposición

$$x^n = z^n - y^n = (z - \xi^1 y)\cdots(z - \xi^n y),$$

siendo $\xi = e^{\frac{2\pi i}{n}}$ y trabajó con los números $\sum a_i \xi^i$, $a_i \in \mathbb{Z}$. Es decir, trabajó en el anillo (concepto general introducido más tarde por Dedekind) $\mathbb{Z}[\xi]$. Argumentando sobre la factorización única, probó que la descomposición anterior no es posible, con $x, y, z \in \mathbb{Z}$ no nulos. Dirichlet le hizo observar a Kummer el error (cometido también por Cauchy y Lamé) de suponer que todos los anillos considerados eran dominios de factorización única. Consideremos por sencillez el anillo de Kummer $\mathbb{Z}[\sqrt{-5}]$, tenemos dos descomposiciones en factores irreducibles $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$. Para restaurar la factorización única, Kummer introdujo los números ideales (no dio una definición general). Si bien $1+\sqrt{-5}$ y 2 son irreducibles observemos que $(1+\sqrt{-5})^2$ es múltiplo de 2. Es como si hubiese un m.c.d. "ideal" de 2 y $1+\sqrt{-5}$. En la extensión $\mathbb{Z}[\sqrt{-5}] \hookrightarrow \mathbb{Z}[(1+\sqrt{-5})/\sqrt{2}, \sqrt{2}]$ tenemos la factorización única por irreducibles $6 = \sqrt{2}^2 \cdot ((1+\sqrt{-5})/\sqrt{2}) \cdot (1-\sqrt{-5})/\sqrt{2}$ (si bien ya estamos en anillos de enteros que no son los de partida). Dedekind observó que lo que estaba definiendo Kummer era el concepto de ideal (recordemos que en los dominios de ideales principales $(a_1,\ldots,a_n) = (m.c.d.(a_1,\ldots,a_n))$, el concepto de ideal primo y que había probado que en tales anillos (dominios de Dedekind) todo ideal es producto de ideales primos. Hilbert (con las "torres de Hilbert") probó que todo anillo de enteros se mete en otro anillo mayor donde sus ideales se hacen principales.

7. Sea $x^n + c_1 x^{n-1} + \cdots + c_n \in \mathbb{Z}[x]$ un polinomio irreducible y sean $\alpha_1,\ldots,\alpha_n$ sus raíces. Consideremos $\mathbb{Z}[\alpha_1] \subset \mathbb{C}$ y la norma $N\colon \mathbb{Z}[\alpha_1] \to \mathbb{N}$, donde dado $z \in \mathbb{Q}[\alpha_1]$, $N(z)$ es el determinante de la homotecia de factor z en $\mathbb{Q}[\alpha_1]$. Si $z = a + b\alpha_1$, entonces $N(z) = \prod_i (a + b\alpha_i)$.

Resolver la ecuación diofántica $a^n + c_1 a^{n-1} b + \cdots + c_n b^n = c$, equivale a encontrar los $z = a - b\alpha_1 \in \mathbb{Z}[\alpha_1]$, tales que $N(z) = c$. Advirtamos, que en general, $\mathbb{Z}[\alpha_1]$ no es un dominio de factorización única, ni sus invertibles son simplemente las raíces de la unidad incluidas en $\mathbb{Z}[\alpha_1]$.

Por desgracia los anillos de la Teoría de Números y los anillos de funciones algebraicas de las curvas algebraicas no son dominios de factorización única. Tampoco son anillos localmente de ideales principales, si lo fuesen serían localmente dominios de factorización única, pero pueden incluirse en anillos "un poco más" grandes que sí lo son.

1.8. Apéndice: Localización

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. Ejemplo: $\mathbb{Z}\setminus\{0\}$ es un sistema multiplicativo de $\mathbb{Z}$.

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

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

Observemos que $\frac{a}{s} = \frac{a'}{s'}$ si y solo si existen $s_1, s_2 \in S$ tales que $(as_1, ss_1) = (a's_2, s's_2)$. Además, $\frac{a}{s} = \frac{s_1 a}{s_1 s}$, para todo $s_1 \in S$.

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

Con la suma y producto ordinarios de fracciones

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

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

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

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

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

6. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Entonces,*

1. $\frac{a}{s} = 0 \in A_S$ *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 $\frac{a}{s} = \frac{a'}{s'}$.

□

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

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

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

10. Ejercicio: Pruébese 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 $a_0, \ldots, a_n \in A$, con $a_i = 0$ ó $\mathrm{gr}(a_i) < \mathrm{gr}(p)$, 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 $a_0 = c_n$ concluimos que $\frac{a}{p^n} = \sum_{i=0}^{n} \frac{a_i}{p^i}$.

□

12. Proposición: *Sea $i: A \to A_S$ el morfismo de localización y $i^*: \operatorname{Spec} A_S \to \operatorname{Spec} A$, $i^*(\mathfrak{q}) := i^{-1}(\mathfrak{q})$ el morfismo inducido en los espectros primos. Se cumple que que las asignaciones*

$$\operatorname{Spec} A_S \longleftrightarrow \{x \in \operatorname{Spec} A : \mathfrak{p}_x \cap S = \emptyset\} \subseteq \operatorname{Spec} A$$

$$\mathfrak{q} \longmapsto i^*(\mathfrak{q}) := i^{-1}(\mathfrak{q})$$

$$\mathfrak{p} \cdot A_S \longleftarrow \mathfrak{p}$$

están bien definidas y son inversas entre sí.

Demostración. Sea $\mathfrak{q} \subset A_S$ un ideal primo. Si $s \in i^{-1}(\mathfrak{q}) \cap S$ entonces $\frac{s}{1} \in \mathfrak{q}$, luego $1 \in \mathfrak{q}$ y $\mathfrak{q} \in A$, lo cual es contradictorio.

Si $\mathfrak{p} \subset A$ es un ideal primo tal que $\mathfrak{p} \cap S = 0$, entonces $\mathfrak{p} \cdot A_S$ es un ideal primo: Si $\frac{a}{s} \cdot \frac{a'}{s'} \in \mathfrak{p} \cdot A_S$, entonces $\frac{aa'}{ss'} = \frac{p}{s''}$, para cierto $p \in \mathfrak{p}$. Luego, existen $t, t' \in S$ tales que $taa' = t'p$ (y $tss' = t's''$). Luego, $taa' \in \mathfrak{p}$ y a ó a' pertenece a $\mathfrak{p}$. Por tanto, $\frac{a}{s}$ o $\frac{a'}{s'}$ pertenece a $\mathfrak{p} \cdot A_S$. Se cumple, además, $i^{-1}(\mathfrak{p} \cdot A_S) = \mathfrak{p}$: Claramente, $\mathfrak{p} \subseteq i^{-1}(\mathfrak{p} \cdot A_S)$. Si $p \in i^{-1}(\mathfrak{p} \cdot A_S)$, entonces $\frac{p}{1} \in \mathfrak{p} \cdot A_S$ y de nuevo $p \in \mathfrak{p}$.

Dejamos que el lector compruebe que $\mathfrak{q} = i^{-1}(\mathfrak{q}) \cdot A_S$.

□

13. Ejemplo: Sea $x \in \operatorname{Spec} A$. Por la proposición anterior $\operatorname{Spec} A_x = \{\mathfrak{p}_y \cdot A_x$, para todo $y \in \operatorname{Spec} A$ tal que $\mathfrak{p}_y \subseteq \mathfrak{p}_x\}$. En particular, A_x es un anillo local de ideal maximal $\mathfrak{p}_x \cdot A_x$.

1.8.1. 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:

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

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

14. Definición: Sea S un sistema multiplicativo de un anillo A y M un A-módulo, denotaremos por M_S:

$$M_S = \{\frac{m}{s},\ \forall\ m \in M, \forall\ s \in S\}$$

y diremos que M_S es la localización de M por el sistema multiplicativo S.

Observemos que $\frac{m}{s} = \frac{m'}{s'}$ si y solo si existen $s_1, s_2 \in S$ tales que $(s_1 m, s_1 s) = (s_2 m', s_2 s')$. Para definir una aplicación $M_S \to X$, tenemos que asignar a cada $\frac{m}{s} \in M_S$ un elemento $\phi(m,s) \in X$, de modo que $\phi(tm, ts) = \phi(m,s)$, para todo $t \in S$.

Podemos definir (bien) las operaciones

$$\frac{m}{s}+\frac{m'}{s'}:=\frac{s'm+sm'}{ss'}$$
$$\frac{a}{s}\cdot\frac{m}{s'}:=\frac{am}{ss'}$$

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.

15. Proposición: *Sea A un anillo, $S\subset A$ un sistema multiplicativo y M un A-módulo. Entonces,*

1. *$\frac{m}{s}=0\in M_S$ si y solo si existe $s'\in S$ tal que $s'\cdot m=0$ (en M).*
2. *$\frac{m}{s}=\frac{m'}{s'}$ si y solo si existe un $t\in S$ de modo que $t\cdot(s'm-sm')=0$ (en M).*

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

$\Leftarrow$) $\frac{m}{s}=\frac{s'm}{s's}=\frac{0}{s's}=\frac{0}{1}=0$.

2. $\frac{m}{s}=\frac{m'}{s'}$ si y solo si $0=\frac{m}{s}-\frac{m'}{s'}=\frac{s'm-sm'}{ss'}$, por 1., si y solo si existe un $t\in S$ de modo que $t\cdot(s'm-sm')=0$.

□

16. Proposición: *Sea $S\subseteq A$ un sistema multiplicativo y M un A-módulo. Si el morfismo $s\cdot\colon M\to M,\ m\mapsto s\cdot m$ es un isomorfismo de A-módulos para todo $s\in S$, entonces $M=M_S$.*

Demostración. Probemos que el morfismo de localización $M\to M_S$, $m\mapsto\frac{m}{1}$ es isomorfismo. Es inyectivo: si $\frac{m}{1}=0$, entonces existe $s\in S$ tal que $s\cdot m=0$, luego $m=0$. Es epiyectivo: dado $\frac{m}{s}$ sea $m'\in M$ tal que $sm'=m$, entonces $m'\mapsto\frac{m'}{1}=\frac{sm'}{s}=\frac{m}{s}$. □

Todo morfismo $f\colon M\to N$ de A-módulos, induce la aplicación (bien definida)

$$f_S\colon M_S\to N_S,\ \frac{m}{s}\underset{\text{def}}{\mapsto}\frac{f(m)}{s},$$

que es morfismo de A_S-módulos.

17. 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. □

18. Ejemplo: Sea A un anillo íntegro y $\Sigma = A_{A\setminus\{0\}}$. Entonces,

$$(A^n)_{A\setminus\{0\}} = A_{A\setminus\{0\}} \oplus \overset{n}{\cdots} \oplus A_{A\setminus\{0\}} = \Sigma^n.$$

19. Proposición: *Sea $f : A \to B$ un morfismo de anillos, $S \subseteq A$ un sistema multiplicativo y M un B-módulo (en particular, es un A-módulo: $a \cdot m := f(a) \cdot m$, para todo $a \in A$ y $m \in M$). Se cumple que*

$$M_S = M_{f(S)}$$

Demostración. El morfismo $M_S \to M_{f(S)}$, $\frac{m}{s} \mapsto \frac{m}{f(s)}$ está bien definido y es un isomorfismo. □

20. Lema: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sea $f : M \to N$ un morfismo de A-módulos. Entonces,*

1. $(\operatorname{Ker} f)_S = \operatorname{Ker} f_S$. *En particular, si f es inyectivo f_S es inyectivo.*
2. $(\operatorname{Im} f)_S = \operatorname{Im} f_S$. *Luego, si f es epiyectivo f_S es epiyectivo.*

Demostración. 1. El morfismo $(\operatorname{Ker} f)_S \to \operatorname{Ker} f_S$, $\frac{m}{s} \mapsto \frac{m}{s}$ es un isomorfismo: Si $\frac{m}{s} = 0 \in M_S$, entonces existe $t \in S$ tal que $t \cdot m = 0 \in M$, por tanto $\frac{m}{s} = 0 \in (\operatorname{Ker} f)_S$. Dado $\frac{m}{s} \in \operatorname{Ker} f_S$, $\frac{f(m)}{s} = 0$ en N_S, luego existe $t \in S$ de modo que $tf(m) = 0$, entonces $f(tm) = 0$ y $tm \in \operatorname{Ker} f$. Por tanto, $\frac{tm}{ts} \mapsto \frac{tm}{ts} = \frac{m}{s}$.

2. $\operatorname{Im} f$ está incluido en N, luego $(\operatorname{Im} f)_S$ está incluido en N_S, por 1. El morfismo inyectivo $(\operatorname{Im} f)_S \to \operatorname{Im} f_S$, $\frac{f(m)}{s} \mapsto \frac{f(m)}{s} = f_S(\frac{m}{s})$ es isomorfismo, porque es claramente epiyectivo. □

Sea M un A-módulo y $N \subseteq M$ un A-submódulo. Consideremos el morfismo epiyectivo de paso al cociente $M \to M/N$. Por la proposición anterior, el núcleo del epimorfismo $M_S \to (M/N)_S$ es N_S, luego

$$M_S/N_S \simeq (M/N)_S.$$

Dado un morfismo de A-módulos $f : M \to N$ se define $\operatorname{Coker} f := M/\operatorname{Im} f$, entonces

$$(\operatorname{Coker} f)_S = (M/\operatorname{Im} f)_S = M_S/(\operatorname{Im} f)_S = M_S/\operatorname{Im} f_S = \operatorname{Coker} f_S.$$

21. Ejercicio: Sea $I \subseteq A$ un ideal y $S \subset A$ un sistema multiplicativo. Prueba que $I_S = I \cdot A_S$.

22. Notación: Dado $x \in \operatorname{Spec} A$, cuando lo pensemos como ideal incluido en A lo denotaremos $\mathfrak{p}_x$. Dado un A-módulo M, denotaremos $M_x = M_{A\setminus\mathfrak{p}_x}$.

23. Proposición: *1. Sea M un A-módulo. Si $M_x = 0$ para todo $x \in \operatorname{Spec} A$, entonces $M = 0$.*

2. Sea $f : M \to M'$ un morfismo de A-módulos. Si $f_x : M_x \to M'_x$, $f_x(m/s) := f(m)/s$ es un isomorfismo para todo $x \in \operatorname{Spec} A$, entonces f es un isomorfismo.

3. Sean $N, N' \subseteq M$ dos A-submódulos. $N = N' \iff N_x = N'_x$ para todo $x \in \operatorname{Spec} A$.

Demostración. 1. Dado $m \in M$, $I := \{a \in A : a \cdot m = 0\}$ es un ideal de A. Tenemos que $m = 0$ si y solo si $I = A$. Si $I \neq A$, sea $\mathfrak{m}_x$ un ideal maximal que contenga a I. Por hipótesis, $m/1 = 0 \in M_x$, luego existe $a \in A \setminus \mathfrak{m}_x$ tal que $a \cdot m = 0$, lo cual contradice que $I \subseteq \mathfrak{m}_x$.

2. Si f_x es un isomorfismo para todo x, entonces $\operatorname{Ker} f_x = 0$ y $\operatorname{Coker} f_x = 0$, para todo x. Por el lema anterior, $(\operatorname{Ker} f)_x = \operatorname{Ker} f_x$ y que $(\operatorname{Coker} f)_x = \operatorname{Coker} f_x$. Por el punto 1., $\operatorname{Ker} f = 0$ y $\operatorname{Coker} f = 0$, es decir, f es un isomorfismo.

3. $N = N' \iff N = N + N'$ y $N' = N + N' \iff N_x = (N + N')_x = N_x + N'_x$ y $N'_x = (N + N')_x = N_x + N'_x$, para todo $x \in \operatorname{Spec} A \iff N_x = N'_x$, para todo $x \in \operatorname{Spec} A$. □

24. Proposición: *Sea A un anillo tal que $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$ y los ideales primos $\mathfrak{p}_{x_i}$ son maximales. Entonces, el morfismo*

$$A \to A_{x_1} \times \overset{n}{\cdots} \times A_{x_n}, a \mapsto (a/1, \ldots, a/1)$$

es un isomorfismo.

Demostración. Si $x_i \neq x_j$, $(A_{x_i})_{x_j} = 0$, porque $\operatorname{Spec}(A_{x_i})_{x_j} = \emptyset$, pues es igual al conjunto de los ideales primos de A contenidos en $\mathfrak{p}_{x_i}$ y $\mathfrak{p}_{x_j}$. Obviamente, $(A_{x_i})_{x_i} = A_{x_i}$. Por tanto, el morfismo $A \to A_{x_1} \times \overset{n}{\cdots} \times A_{x_n}$ es un isomorfismo porque al localizar en todos los puntos de $\operatorname{Spec} A$ es un isomorfismo. □

25. Corolario: *Sea A un anillo tal que $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$ y los ideales primos $\mathfrak{p}_{x_i}$ son maximales y sea M un A-módulo. Entonces,*

$$M \to M_{x_1} \times \overset{n}{\cdots} \times M_{x_n}, m \mapsto (m/1, \ldots, m/1)$$

es un isomorfismo.

Demostración. En efecto, $M = M \otimes_A A = M \otimes_A \prod_i A_{x_i} = \prod_i M_{x_i}$.

□

26. Proposición: *Sea M un A-módulo finito generado. Entonces,*

$$\operatorname{Sop}(M) := \{x \in \operatorname{Spec} A : M_x \neq 0\}$$

es un cerrado de $\operatorname{Spec} A$.

Demostración. Tenemos que probar que si $M_x = 0$ entonces existe un entorno abierto U de x, tal que $M_y = 0$ para todo $y \in U$. Escribamos $M = \langle m_1, \ldots, m_n \rangle$. Como $\frac{m_i}{1} = 0$ porque $M_x = 0$, existen $s_i \in A \setminus \mathfrak{p}_x$ tales que $s_i \cdot m_i = 0$. Por tanto, si $s := \prod_i s_i$, tenemos que $s \cdot m_i = 0$ para todo i. Luego, $M_y = 0$ para todo $y \in U := \operatorname{Spec} A - (s)_0$. □

1.9. Cuestionario

1. Sea $(A, \delta : A\setminus\{0\} \to \mathbb{N})$ un anillo euclídeo. Probar

   a) Si $I \subseteq A$ es un ideal, entonces $c \in I$ genera el ideal I si y solo si $\delta(c) \leq \delta(i)$, para todo $i \in I$.

   b) $a \in A$ es invertible si y solo si $\delta(a) \leq \delta(b)$ para todo $b \in A$.

   c) Sea $n := \min\{\delta(a) : a \in A\}$ y $\delta' : A\setminus\{0\} \to \mathbb{N}$, $\delta'(a) := \delta(a) - n$. Entonces, (A, δ') es un anillo euclídeo y $a \in A$ es invertible si y solo si $\delta'(a) = 0$.

2. Sea A un anillo íntegro y $a, b \in A$. Entonces, $(a) = (b)$ si y solo si existe $i \in A$ invertible tal que $a = b \cdot i$.

3. Sea k un cuerpo y $p(x) \in k[x]$ un polinomio de grado dos o tres. Prueba que $p(x)$ es irreducible si y solo si no tiene ninguna raíz en k.

4. Sea $p(x) = a_0 x^n + \cdots + a_n \in \mathbb{Z}[x]$ y $p \in \mathbb{Z}$ un número primo. Prueba que si a_0 no es múltiplo de p y $\overline{p(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ es irreducible, entonces $p(x)$ es irreducible en $\mathbb{Q}[x]$.

5. ¿Es $k[x, y]$ un dominio de factorización única?¿Es un dominio de ideales principales?

6. ¿Es $\mathbb{Z}[x]$ DFU? ¿Es $\mathbb{Z}[x]$ dip?

7. Sea k un cuerpo. Prueba que $k[[x]]$ es un dominio de ideales principales y es local.

8. Sea A un dominio de ideales principales ¿Es A un dominio de factorización única?

9. Prueba que $C(\mathbb{R}^2, \mathbb{R})$ no es un anillo noetheriano.

10. Sea $C(\mathbb{R}^2)$ el anillo de funciones continuas reales de $\mathbb{R}^2$ y $f \in C(\mathbb{R}^2)$ no invertible. Prueba que existen funciones continuas f_1, f_2 no invertibles tales que $f = f_1 \cdot f_2$ ¿Existen elementos irreducibles en $C(\mathbb{R}^2)$?

1.10. Biografía de Emmy Noether

NOETHER BIOGRAPHY

Emmy Noether's father, Max Noether, was a distinguished mathematician and a professor at Erlangen but he came from a family of wholesale hardware dealers. Her mother was Ida Amalia Kaufmann (1852-1915), from a wealthy Cologne family. Both Emmy's parents were of Jewish origin and the reader may be surprised at this since Noether is not a Jewish name. We should explain, therefore, how this came about and, at the same time, give some information on Emmy Noether's ancestors. Max Noether's paternal grandfather was Elias Samuel, the founder of a business in Bruchsal. Elias had nine children, one being a son Hertz Samuel. In 1809 the State of Baden made the Tolerance Edict which required Jews to adopt Germanic names. Elias Samuel chose the surname Nöther, becoming Elias Nöther, but also changed the given names of his children, giving Hertz the name Hermann. When he was eighteen years old, Hermann Nöther left his home town of Bruchsal and studied theology at the University of Mannheim. Then in 1837, together with his brother Joseph, he set up a wholesale business in iron hardware. Hermann Nöther and his wife Amalia had five children, the third of which was Max. The two children older than Max were Sarah (born 6 November 1839) and Emil. It is worth noting at this point that the Nöther iron-wholesaling business remained a family firm for exactly one hundred years, until the Nazis removed Jewish families from their own businesses in 1937. One other comment is necessary at this point. Although the family name was chosen to be Nöther by Max's grandfather, Max and his family always used the form Noether (except on Max's wedding certificate where the form Nöther appears).

Emmy was the eldest of her parents' four children, the three younger children being boys. Alfred Noether (1883-1918) studied chemistry and was awarded a doctorate from Erlangen in 1909. However, his career was short since he died nine years later. Fritz Noether (1884-1941) became an applied mathematician. However, as a Jew he was unable to work and left Germany in 1937. He was appointed as a professor at the University of Tomsk in the Soviet Union but accused of anti-Soviet acts he was sentenced to death and shot. He was found not guilty by the Supreme Court of the Soviet Union in 1988. Gustav Robert Noether (1889-1928) had bad health all his life. He was mentally handicapped, spent most of his life in an institution and died young. The first school that Emmy attended was on Fahrstrasse. Auguste Dick wrote:

Emmy did not appear exceptional as a child. Playing among her peers in the schoolyard on Fahrstrasse she probably was not especially noticeable - a near-sighted, plain-looking little girl, though not without charm. Her teachers and classmates knew Emmy as a clever, friendly, and likeable child. She had a slight lisp and was one of the few who attended classes in the Jewish religion.

After elementary school, Emmy Noether attended the Städtische Höhere Töchter

Schule on Friedrichstrasse in Erlangen from 1889 until 1897. She had been born in the family home at Hauptstrasse 23 and lived there until, in the middle of her time at high school, in 1892, the family moved to a larger apartment at Nürnberger Strasse 32. At the high school she studied German, English, French, arithmetic and was given piano lessons. She loved dancing and looked forward to parties with children of her father's university colleagues. At this stage her aim was to become a language teacher and after further study of English and French she took the examinations of the State of Bavaria and, in 1900, became a certificated teacher of English and French in Bavarian girls schools. She was awarded the grade of "very good" in the examinations, the weakest part being her classroom teaching.

However Noether never became a language teacher. Instead she decided to take the difficult route for a woman of that time and study mathematics at university. Women were allowed to study at German universities unofficially and each professor had to give permission for his course. Noether obtained permission to sit in on courses at the University of Erlangen during 1900 to 1902. She was one of only two female students sitting in on courses at Erlangen and, in addition to mathematics courses, she continued her interest in languages being taught by the professor of Roman Studies and by an historian. At the same time she was preparing to take the examinations which allowed a student to enter any university. Having taken and passed this matriculation examination in Nürnberg on 14 July 1903, she went to the University of Göttingen. During 1903-04 she attended lectures by Karl Schwarzschild, Otto Blumenthal, David Hilbert, Felix Klein and Hermann Minkowski. Again she was not allowed to be a properly matriculated student but was only allowed to sit in on lectures. After one semester at Göttingen she returned to Erlangen.

At this point the rules were changed and women students were allowed to matriculate on an equal basis to the men. On 24 October 1904 Noether matriculated at Erlangen where she now studied only mathematics. In 1907 she was granted a doctorate after working under Paul Gordan. The oral examination took place on Friday 13 December and she was awarded the degree 'summa cum laude'. Hilbert's basis theorem of 1888 had given an existence result for finiteness of invariants in n variables. Gordan, however, took a constructive approach and looked at constructive methods to arrive at the same results. Noether's doctoral thesis followed this constructive approach of Gordan and listed systems of 331 covariant forms. Colin McLarty wrote that:

... her dissertation of 1908 with Gordan pursued a huge calculation that had stumped Gordan forty years before and which Noether could not complete either. So far as I know no one has ever completed it or even checked it as far as she went. It was old-fashioned at the time, a witness to the pleasant isolation of Erlangen, and made no use of Gordan's own work building on Hilbert's ideas.

Having completed her doctorate the normal progression to an academic post would have been the habilitation. However this route was not open to women so Noether remained at Erlangen, helping her father who, particularly because of his own disabilities, was grateful for his daughter's help. Noether also worked on her own research,

in particular she was influenced by Ernst Fischer who had succeeded Gordan to the chair of mathematics when he retired in 1911. Noether wrote about Fischer's influence:

Above all I am indebted to Mr E Fischer from whom I received the decisive impulse to study abstract algebra from an arithmetical viewpoint, and this remained the governing idea for all my later work.

Fischer's influence took Noether towards Hilbert's abstract approach to the subject and away from the constructive approach of Gordan. Now this was very important to her development as a mathematician for Gordan, despite his remarkable achievements, had his limitations. Noether's father, Max Noether, said of Gordan:

Gordan was never able to do justice to the development of fundamental concepts; even in his lectures he completely avoided all basic definitions of a conceptual nature, even that of the limit.

Noether's reputation grew quickly as her publications appeared. In 1908 she was elected to the Circolo Matematico di Palermo, then in 1909 she was invited to become a member of the Deutsche Mathematiker-Vereinigung and in the same year she was invited to address the annual meeting of the Society in Salzburg. She gave the lecture Zur Invariantentheorie der Formen von n Variabeln (On the theory of invariants for the forms of n variables). In 1913 she lectured in Vienna, again to a meeting of the Deutsche Mathematiker-Vereinigung. Her lecture on this occasion was Über rationale Funktionenkörper (On fields of rational functions). While in Vienna she visited Franz Mertens and discussed mathematics with him. One of Merten's grandsons remembered Noether's visit:

... although a woman, [she] seemed to me like a Catholic chaplain from a rural parish - dressed in a black, almost ankle-length and rather nondescript, coat, a man's hat on her short hair ... and with a shoulder bag carried crosswise like those of the railway conductors of the imperial period, she was rather an odd figure.

During these years in Erlangen she advised two doctoral students who were both officially supervised by her father. These were Hans Falckenberg (doctorate 1911) and Fritz Seidelmann (doctorate 1916).

In 1915 Hilbert and Klein invited Noether to return to Göttingen. The reason for this was that Hilbert was working on physics, in particular on ideas on the theory of relativity close to those of Albert Einstein. He decided that he needed the help of an expert on invariant theory and, after discussions with Klein, they issued the invitation. Van der Waerden wrote:

She came and at once solved two important problems. First: How can one obtain all differential covariants of any vector or tensor field in a Riemannian space? ... The second problem Emmy investigated was a problem from special relativity. She proved: To every infinitesimal transformation of the Lorentz group there corresponds a Conservation Theorem.

This result in theoretical physics is sometimes referred to as Noether's Theorem, and proves a relationship between symmetries in physics and conservation principles.

This basic result in the theory of relativity was praised by Einstein in a letter to Hilbert when he referred to Noether's penetrating mathematical thinking. Of course, she arrived in Göttingen during World War I. This was a time of extreme difficulty and she lived in poverty during these years and politically she became a radical socialist. However, they were extraordinarily rich years for her mathematically. Hermann Weyl, in wrote about Noether's political views:

During the wild times after the Revolution of 1918, she did not keep aloof from the political excitement, she sided more or less with the Social Democrats; without being actually in party life she participated intensely in the discussion of the political and social problems of the day. ... In later years Emmy Noether took no part in matters political. She always remained, however, a convinced pacifist, a stand which she held very important and serious.

Hilbert and Klein persuaded her to remain at Göttingen while they fought a battle to have her officially on the Faculty. In a long battle with the university authorities to allow Noether to obtain her habilitation there were many setbacks and it was not until 1919 that permission was granted and she was given the position of Privatdozent. During this time Hilbert had allowed Noether to lecture by advertising her courses under his own name. For example a course given in the winter semester of 1916-17 appears in the catalogue as:

Mathematical Physics Seminar: Professor Hilbert, with the assistance of Dr E Noether, Mondays from 4-6, no tuition.

At Göttingen, after 1919, Noether moved away from invariant theory to work on ideal theory, producing an abstract theory which helped develop ring theory into a major mathematical topic. Idealtheorie in Ringbereichen (1921) was of fundamental importance in the development of modern algebra. In this paper she gave the decomposition of ideals into intersections of primary ideals in any commutative ring with ascending chain condition. Emanuel Lasker (who became the world chess champion) had already proved this result for a polynomial ring over a field. Noether published Abstrakter Aufbau der Idealtheorie in algebraischen Zahlkorpern in 1924. In this paper she gave five conditions on a ring which allowed her to deduce that in such commutative rings every ideal is the unique product of prime ideals.

In the same year of 1924 B.L. van der Waerden came to Göttingen and spent a year studying with Noether. After returning to Amsterdam van der Waerden wrote his book Moderne Algebra in two volumes. The major part of the second volume consists of Noether's work. From 1927 onwards Noether collaborated with Helmut Hasse and Richard Brauer in work on non-commutative algebras. They wrote a beautiful paper joint paper Beweis eines Hauptsatzes in der Theorie der Algebren which was published in 1932. In addition to teaching and research, Noether helped edit Mathematische Annalen. Much of her work appears in papers written by colleagues and students, rather than under her own name.

Further recognition of her outstanding mathematical contributions came with invitations to address the International Congress of Mathematicians at Bologna in Sep-

tember 1928 and again at Zurich in September 1932. Her address to the 1932 Congress was entitled Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und zur Zahlentheorie. In 1932 she also received, jointly with Emil Artin, the Alfred Ackermann-Teubner Memorial Prize for the Advancement of Mathematical Knowledge. In April 1933 her mathematical achievements counted for nothing when the Nazis caused her dismissal from the University of Göttingen because she was Jewish. She received no pension or any other form of compensation but, nevertheless, she considered herself more fortunate than others. She wrote to Helmut Hasse on 10 May 1933:

Many thanks for your dear compassionate letter! I must say, though, that this thing is much less terrible for me than it is for many others. At least I have a small inheritance (I was never entitled to a pension anyway) which allows me to sit back for a while and see.

Weyl spoke about Noether's reaction to the dire events that were taking place around her in the address he gave at her funeral:

You did not believe in evil, indeed it never occurred to you that it could play a role in the affairs of man. This was never brought home to me more clearly than in the last summer we spent together in Göttingen, the stormy summer of 1933. In the midst of the terrible struggle, destruction and upheaval that was going on around us in all factions, in a sea of hate and violence, of fear and desperation and dejection - you went your own way, pondering the challenges of mathematics with the same industriousness as before. When you were not allowed to use the institute's lecture halls you gathered your students in your own home. Even those in their brown shirts were welcome; never for a second did you doubt their integrity. Without regard for your own fate, openhearted and without fear, always conciliatory, you went your own way. Many of us believed that an enmity had been unleashed in which there could be no pardon; but you remained untouched by it all.

She accepted a one-year visiting professorship at Bryn Mawr College in the USA and in October 1933 sailed to the United States on the ship Bremen to take up the appointment. She had hoped to delay accepting the invitation since she would have liked to have gone to Oxford in England but it soon became clear that she had to leave quickly. At Bryn Mawr she was made very welcome by Anna Johnson Pell Wheeler who was head of mathematics. Noether ran a seminar during the winter semester of 1933-34 for three students and one member of staff. They worked through the first volume of van der Waerden's Moderne Algebra. In February 1934 she began giving weekly lectures at the Institute for Advanced Study, Princeton. In a letter to Hasse, dated 6 March 1934, she wrote:

I have started with representation modules, groups with operators ...; Princeton will receive its first algebraic treatment this winter, and a thorough one at that. My audience consists mostly of research fellows, besides Albert and Vandiver, but I'm beginning to realise that I must be careful; after all, they are essentially used to explicit computation and I have already driven a few of them away with my approach.

Noether returned to Germany in the summer of 1934. There see saw her brother Fritz for what would be the last time, and visited Artin in Hamburg before going on to Göttingen. In 1980 Artin's wife recalled Noether's visit:

Now the one thing I remember most vividly is the trip on the Hamburg Untergrund, which is the subway in Hamburg. We picked up Emmy at the Institute, and she and Artin immediately started talking mathematics. At that time it was Idealtheorie, and they started talking about Ideal, Führer, and Gruppe, and Untergruppe, and the whole car suddenly started pricking up their ears. [Each of the German nouns has both mathematical and political meanings.] And I was frightened to death - I thought, my goodness, next thing's going to happen, somebody's going to arrest us. Of course, that was in 1934, and all. But Emmy was completely oblivious, and she talked very loudly and very excitedly, and got louder and louder, and all the time the "Führer" came out, and the "Ideal". She was very full of life, and she constantly talked very fast and very loud.

She returned to the United States where her visiting professorship at Bryn Mawr had been extended for a further year. She continued her weekly lectures at Princeton where Richard Brauer had now arrived. After her lectures she enjoyed talking about mathematics with Weyl, Veblen and Brauer.

Noether's death was sudden and unexpected. In April 1935 doctors discovered that she had a tumour. Two days later they operated, finding further tumours which they believed to be benign and did not remove. The operation seemed a success and for three days her condition improved. However, on the fourth day she suddenly collapsed and developed a very high temperature. She died later that day.

Weyl in his Memorial Address said:

Her significance for algebra cannot be read entirely from her own papers, she had great stimulating power and many of her suggestions took shape only in the works of her pupils and co-workers.

Van der Waerden wrote:

For Emmy Noether, relationships among numbers, functions, and operations became transparent, amenable to generalisation, and productive only after they have been dissociated from any particular objects and have been reduced to general conceptual relationships.

Although she received little recognition in her lifetime considering the remarkable advances that she made, she has been honoured in many ways following her death. A crater on the moon is named for her. A street in her hometown is named for her and the school she attended is now named the Emmy Noether School. Various organisations name scholarships and lectures after Emmy Noether.

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

1.11. Problemas

1. Prueba que el número de números primos es infinito.

   Resolución: Supongamos que es finito y sean $\{p_1,\dots,p_n\}$ todos los primos. Entonces, $p_1\cdots p_n+1$ sería un nuevo número primo y llegamos a contradicción.

2. Prueba que el número de números primos de la forma $4n+1$ para algún n es infinito.

   Resolución: Un primo $p\in\mathbb{Z}$ no es primo en $\mathbb{Z}[i]$ si y solo si $p=4n+1$ ó $p=2$. Supongamos que el conjunto C de los números primos de $\mathbb{Z}$ que no son primos en $\mathbb{Z}[i]$ es un conjunto finito. Escribamos $C=\{p_1=2,p_2,\dots,p_n\}$. Tenemos que $p_i=z_i\cdot\bar{z}_i$, donde $z_i,\bar{z}_i$ son irreducibles de $\mathbb{Z}[i]$. Sea $D=\{q_i\}$ el conjunto de todos los primos de $\mathbb{Z}$ que son primos en $\mathbb{Z}[i]$. El conjunto de todos los irreducibles de $\mathbb{Z}[i]$, salvo multiplicación por unidades, son $\{q_i,z_j,\bar{z}_j\}_{i,j}$. Entonces $z=p_1\cdots p_n+i$ no es divisible por ninguno de los irreducibles de $\mathbb{Z}[i]$. Hemos llegado a contradicción.

3. Prueba que el número de polinomios mónicos irreducibles es infinito.

   Resolución: Si $\{p_1(x),\dots,p_n(x)\}$ es el conjunto de todos los polinomios mónicos irreducibles, entonces $p_1(x)\cdots p_r(x)+1$ es un polinomio mónico irreducible más.

4. Prueba que $z=a+bi\in\mathbb{Z}[i]$ es irreducible si y solo si z, salvo multiplicación por invertibles, es un número primo p, con $p=3 \mod 4$ ó $\delta(z):=z\cdot\bar{z}=p$, con p primo. Descompón $35\in\mathbb{Z}[i]$ en producto de irreducibles.

   Resolución: Si $\delta(z)=p$ es primo entonces z es irreducible, porque si $z=z_1\cdot z_2$ entonces $p=\delta(z)=\delta(z_1)\cdot\delta(z_2)$ y $\delta(z_1)=1$, luego z_1 es invertible (ó $\delta(z_2)=1$, luego z_2 es invertible). Si z es un número primo p, con $p=3 \mod 4$ sabemos que es irreducible. Veamos el recíproco. Supongamos que z es irreducible, luego $\bar{z}$ es irreducible. Si $\delta(z)=z\cdot\bar{z}$ no es un número primo, ha de ser el producto de dos números primos irreducibles en $\mathbb{Z}[i]$ y z ha de ser (salvo multiplicación por un invertible) un número primo irreducible en $\mathbb{Z}[i]$.

   $35=7\cdot5$. $7=3 \mod 4$, luego es irreducible y $5=(1+2i)\cdot(1-2i)$. Luego,

   $$35=7\cdot(1+2i)\cdot(1-2i).$$

5. Sea A un anillo íntegro y $\delta:A\setminus\{0\}\to\mathbb{N}$ una aplicación que satisface: "Si $a,b\in A$ y $b\neq0$, entonces existen $q,r\in A$ de modo que $a=bq+r$ y o bien $r=0$ o $\delta(r)<\delta(b)$". Sea $\delta':A\setminus\{0\}\to\mathbb{N}$ definida por $\delta'(a):=\min\{\delta(ba)\}_{b\in A\setminus\{0\}}$. Prueba que (A,δ') es un anillo euclídeo.

   Resolución: Obviamente $\delta'(e)=\min\{\delta(be)\}_{b\in A\setminus\{0\}}\leq\min\{\delta(bfe)\}_{b\in A\setminus\{0\}}=\delta'(fe)$.

   Dados $a,b\in A$ y b no nulo, sea $i\in A\setminus\{0\}$, de modo que $\delta'(b)=\delta(ib)$. Existen $q,r\in A$ de modo que $a=qib+r$, con $r=0$ o $\delta(r)<\delta(ib)$, luego si definimos $q'=qi$ tenemos que $a=q'b+r$, con $r=0$ o $\delta'(r)\leq\delta(r)<\delta'(b)$.

6. Sea (A,δ) un anillo euclídeo y sean $a,b,c \in A$ propios. Si $a = bc$ prueba que $\delta(b) < \delta(a)$ (y $\delta(c) < \delta(a)$).

   Resolución: Sabemos que $\delta(b) \leq \delta(a)$. Si $\delta(b) = \delta(a)$, entonces existe $d,r \in A$ tales que $b = ad + r$ con $\delta(r) < \delta(b)$ ó $r = 0$. Ahora bien, $r = b - ad = b(1 - cd)$. Si $r \neq 0$ tenemos que $\delta(r) \geq \delta(b)$, llegando a contradicción. Si $r = 0$, entonces $b = ad = bcd$, luego $cd = 1$ y c es invertible, lo cual es contradictorio.

7. **Ternas pitagóricas:** Calcula todas las soluciones de la ecuación diofántica

$$a^2 + b^2 = c^2$$

   (se dice que $(a,b,c) \in \mathbb{Z}^3$ es una terna pitagórica si $a^2 + b^2 = c^2$ y $abc \neq 0$).

   Resolución: Si (na,nb,c) es una terna pitagórica, entonces n divide a c y $(a,b,c/n)$ es una terna pitagórica. Calculemos las ternas pitagóricas (a,b,c) con a y b primos entre sí. Tenemos que calcular todos los enteros de Gauss $z = a + bi \in \mathbb{Z}[i]$ tales que $N(z) := z \cdot \bar{z} = c^2$, para algún $c \in \mathbb{Z}$ (con a y b primos entre sí). Veamos que $N(z) = c^2$ (para algún $c \in \mathbb{Z}$) si y solo si existe $u \in \mathbb{Z}[i]$ de modo que $z = u^2$ (o $z = iu^2$): Obviamente si $z = u^2$, entonces $N(z) = u^2 \cdot \bar{u}^2 = (u \cdot \bar{u})^2$, donde $u \cdot \bar{u} \in \mathbb{Z}$. Veamos el recíproco. Sea z_1 un entero de Gauss irreducible que divida a z (en particular z_1 no puede ser un número entero). Sea n el número natural mayor tal que z_1^n divida a z. Luego, $z = z_1^n \cdot u$ y u es primo con z_1 y también con $\bar{z}_1$. Además, $\bar{z} = \bar{z}_1^n \cdot \bar{u}$ y $\bar{u}$ es primo con z_1 y $\bar{z}_1$. Luego, n es el mayor número natural tal que $(z_1 \cdot \bar{z}_1)^n$ divide a $z \cdot \bar{z} = c^2$. Observemos que $z_1 \cdot \bar{z}_1$ es un número primo. Luego, n es un número par. Por tanto, z es un cuadrado (salvo multiplicación por un invertible).

   Si escribimos $u = x + yi$, entonces $z = u^2 = (x^2 - y^2) + 2xyi$ y que $c = \pm u \cdot \bar{u} = \pm(x^2 + y^2)$. En conclusión, las ternas pitagóricas son de la forma

$$(a,b,c) = n \cdot (x^2 - y^2, 2xy, \pm(x^2 + y^2))$$

   (o bien $z = iu^2$ y $(a,b,c) = n \cdot (2xy, y^2 - x^2, \pm(x^2 + y^2))$).

En una tablilla cuneiforme babilónica aproximadamente del año 1.800 a.C. se ha encontrado una enumeración de ternas pitagóricas, entre las cuales se encontraba $(4961, 6480, 8161)$. Se obtiene con $x = 81$ y $y = 40$.

8. Prueba que la ecuación $x^4 + y^4 = z^2$ no tiene soluciones enteras $xyz \neq 0$.

Resolución: Si (x,y,z) es un solución y n divide a x e y, entonces $(x/n, y/n, z/n^2)$ es otra solución. Consideremos una solución con $z > 0$ mínimo, x e y han de ser primos entre sí. Observemos que (x^2, y^2, z) es una terna pitagórica. Por el problema anterior existe a, b de modo que $x^2 = a^2 - b^2$, $y^2 = 2ab$ (permutando x por y si es necesario) y $z^2 = a^2 + b^2$. Si probamos que $a = c^2$ es un cuadrado y c verifica una ecuación como la de z llegamos a contradicción, porque $c < a < z$. Tenemos que $x^2 + b^2 = a^2$ (como x e y son primos entre sí, entonces a y b son primos entre sí, además y es par, x impar). Entonces, $a = u^2 + v^2$, $x = u^2 - v^2$ y $b = 2uv$ (u y v primos entre sí). Además, $y^2 = 2ab = 4 \cdot (u^2 + v^2)uv$, como u, v y $u^2 + v^2$ son primos entre sí y su producto es un cuadrado resulta que han de ser cuadrados. En conclusión, a cumple lo buscado porque $a = u^2 + v^2$ y a, u y v son cuadrados.

9. Prueba que $x^4 + y^4 = z^4$ no tiene soluciones enteras $xyz \neq 0$.

   Resolución: Es consecuencia inmediata del problema anterior.

10. Prueba que la ecuación diofántica $y^2 - x^3 + 1 = 0$ tiene una única solución $(x,y) = (0,1)$.

    Resolución: Sea (x,y) una solución. Observemos que x no es par, porque si lo fuese tendríamos que $y^2 + 1 = 0 \mod 8$ y esto es imposible. Trabajemos en $\mathbb{Z}[i]$. Tenemos que $(y+i)\cdot(y-i) = x^3$. Observemos que $y+i$ y $y-i$ son primos con 2, porque x es primo con 2. Entonces, Entonces, $y+i$ e $y-i$ son primos entre sí, porque $(y+i, y-i) = (y+i, 2i) = (y+i, 2) = (1)$. Por tanto, salvo multiplicación por invertibles, $y+i$ e s un cubo. Como los invertibles de $\mathbb{Z}[i]$ son $\pm 1, \pm i$, que son cubos, entonces $y+i$ es un cubo. Luego,

$$y + i = (a + b \cdot i)^3 = (a^3 - 3ab^2) + (3a^2b - b^3) \cdot i$$

    tenemos que $1 = 3a^2b - b^3 = b(3a^2 - b^2)$, luego $b = -1$, $a = 0$, $y = 0$ y $x = 1$.

11. Prueba que $\mathbb{R}[x.y]/(x^2 + y^2 + 1)$ es un dominio de ideales principales y que no es un anillo euclídeo.

    Resolución: $A := \mathbb{R}[x,y]/(x^2+y^2+1)$ es un anillo íntegro noetheriano. Para ver que es d.i.p. basta ver que los ideales maximales $\mathfrak{m}$ son principales. Ahora bien, $A/\mathfrak{m}$ es una $\mathbb{R}$-extensión finita de $\mathbb{R}$ (teorema de los ceros de Hilbert) y no puede ser $\mathbb{R}$ (pues $x^2 + y^2 + 1 = 0$ no tiene soluciones reales), luego $A/\mathfrak{m} = \mathbb{C}$. Por tanto, $\bar{1}, \bar{x}, \bar{y}$ son linealmente dependientes en $A/\mathfrak{m}$, luego existen $a, b, c \in \mathbb{R}$ (no todos nulos simultáneamente) tales que $a + bx + cy \in \mathfrak{m}$, es fácil ver que $\dim_{\mathbb{R}} A/(a + bx + cy) = 2$, luego $\mathfrak{m} = (a + bx + cy)$.

    Veamos que A no es euclídeo:

    a. $\mathbb{R} - \{0\}$ son los invertibles de A: Sea $\tau : A \to A$ el automorfismo de $\mathbb{R}$-álgebras definido por $\tau(\bar{x}) = \bar{x}$ y $\tau(\bar{y}) = -\bar{y}$. $A = \mathbb{R}[x] \oplus \mathbb{R}[x] \cdot \bar{y}$ y $A^{\langle \tau \rangle} = \mathbb{R}[x]$. Dado $a \in A$

definimos $N\colon A \to \mathbb{R}[x]$, $N(a) := a \cdot \tau(a) \in A^{\langle\tau\rangle} = \mathbb{R}[x]$, que cumple que $N(ab) = N(a)N(b)$. Si a es invertible en A entonces $N(a)$ es invertible en $\mathbb{R}[x]$. Sea $p(x) + q(x)\cdot\bar{y} \in A$ invertible, tenemos que $N(p(x)+q(x)\cdot\bar{y}) = p(x)^2 - q(x)^2\bar{y}^2 = p(x)^2 + q(x)^2(1+x^2)$ es invertible, luego es un polinomio de grado cero. Esto solo es cierto si $p(x) \in \mathbb{R}$ y $q(x) = 0$.

b. Supongamos que (A,δ) es euclídeo y sea $c \in A - \mathbb{R}$ un elemento de $\delta(c)$ mínimo.

c. Todo elemento de A módulo (c) es igual a un elemento de $\mathbb{R}$, es decir, el morfismo $\mathbb{R} \to A/(c)$, $\lambda \mapsto \bar{\lambda}$ es epiyectivo, es decir, $\mathbb{R} = A/(c)$ lo cual es imposible.

12. Sea $n = p_1^{n_1}\cdots p_r^{n_r}$ la descomposición en potencias de primos de $n \in \mathbb{N}$. Prueba que $\mathbb{Z}[e^{2\pi i/n}] = \mathbb{Z}[e^{\frac{2\pi i}{p_1^{n_1}}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[e^{\frac{2\pi i}{p_r^{n_r}}}]$.

Resolución: El morfismo natural $\mathbb{Z}[e^{\frac{2\pi i}{p_1^{n_1}}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[e^{\frac{2\pi i}{p_r^{n_r}}}] \to \mathbb{Z}[e^{2\pi i/n}]$ es epiyectivo y es un morfismo entre $\mathbb{Z}$-módulos libres del mismo rango, luego es isomorfismo.

13. Sea $\mathcal{O}$ un anillo local noetheriano de dimensión de Krull mayor que cero y sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$. Prueba que $\mathfrak{m}$ es un ideal principal si y solo si $\mathcal{O}$ es un dominio de ideales principales.

Resolución: Veamos la implicación directa. Escribamos $\mathfrak{m} = (t)$. Dado $a \in \mathcal{O}$ no nulo, si a no es invertible entonces $a = t\cdot a_1$. Si a_1 no es invertible, entonces $(a) \underset{\neq}{\subset} (a_1)$, porque si son iguales $a_1 = b\cdot a$ y $a = tba$, luego $(1-tb)a = 0$ y como $1-tb$ es invertible $a = 0$ y llegamos a contradicción. Si a_1 no es invertible de nuevo $a_1 = t\cdot a_2$ y $a = t^2\cdot a_2$. Si a_2 no es invertible, de nuevo, $(a_1) \underset{\neq}{\subset} (a_2)$, y seguimos el proceso. Por noetherianidad, este proceso termina y tendremos que $a = t^n \cdot c$ con c invertible.

Dado un ideal $I = (f_1,\ldots,f_r)$, tenemos que $f_i = t^{n_i}\cdot g_i$, con g_i invertible, luego $I = (t^{n_1},\ldots,t^{n_r}) = (t^n)$, donde n es el mínimo de los $\{n_i\}$.

Observemos que t no es nilpotente, porque si no $\operatorname{Spec}\mathcal{O} = \operatorname{Spec}\mathcal{O}/(t) = \{\mathfrak{m}\}$. Ahora es fácil probar que $\mathcal{O}$ es íntegro.

14. Sea $\mathcal{O}$ un anillo local noetheriano de dimensión de Krull mayor que cero y sea $\mathfrak{m}$ su ideal maximal. Prueba que $\mathcal{O}$ es un dominio de ideales principales si y solo si $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Resolución: Si $\mathfrak{m}/\mathfrak{m}^2 = 0$ entonces $\mathfrak{m} = 0$, por el lema de Nakayama; luego $\mathcal{O}$ sería un cuerpo lo cual es contradictorio con las hipótesis. Por tanto, $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$ si y solo si $\mathfrak{m}$ es principal, por el lema de Nakayama. Por el problema 13 concluimos.

15. Sean $x_1,\ldots,x_n \in \operatorname{Spec}A$ y $S = A \setminus \bigcup_{i=1}^{n} \mathfrak{p}_{x_i}$. Prueba que $\operatorname{Spec}A_S = \bigcup_{i=1}^{n} \operatorname{Spec}A_{x_i}$.

Resolución: Probemos que si un ideal $I \subseteq \bigcup_i \mathfrak{p}_{x_i}$ entonces $I \subseteq \mathfrak{p}_{x_j}$ para algún j. Sea m el número natural mínimo tal que I esté incluido en la unión de m de los

ideales primos $\mathfrak{p}_{x_1},\dots,\mathfrak{p}_{x_n}$. Tenemos que probar que $m=1$. Podemos suponer que $I\subseteq \bigcup_{i=1}^{m}\mathfrak{p}_{x_i}$ y que $n=m$. Sea $s_i\in I$ tal que $s_i\notin \bigcup_{j\neq i}^{n}\mathfrak{p}_{x_j}$, es decir, $s_i(x_j)\neq 0$ para todo $j\neq i$ (y $s_i(x_i)=0$). Sea $t_i=\prod_{j\neq i} s_j\in I$, entonces $t_i(x_i)\neq 0$ y $t_i(x_j)=0$ para todo $j\neq i$.

Sea $t=t_1+\cdots+t_n\in I$ entonces $t(x_j)=0$, para todo j, es decir, $t\notin \bigcup_{i=1}^{n}\mathfrak{p}_{x_i}$ y hemos llegado a contradicción.

Por tanto,

$$\operatorname{Spec}A_S=\{y\in\operatorname{Spec}A:\ \mathfrak{p}_y\cap S=\emptyset\}=\{y\in\operatorname{Spec}A:\ \mathfrak{p}_y\subseteq\bigcup_{i=1}^{n}\mathfrak{p}_{x_i}\}$$
$$=\bigcup_{i=1}^{n}\{y\in\operatorname{Spec}A:\ \mathfrak{p}_y\subseteq\mathfrak{p}_{x_i}\}=\bigcup_{i=1}^{n}\operatorname{Spec}A_{x_i}.$$

16. Sea $\mathfrak{m}_x\subset A$ un ideal maximal y M un $A/\mathfrak{m}_x^n$-módulo ($n>0$). Prueba que el morfismo de localización $M\to M_x$ es un isomorfismo.

Resolución: Dado $s\in A\setminus\mathfrak{m}_x$, se cumple que $\bar{s}\in A/\mathfrak{m}_x^n$ es invertible porque $\operatorname{Spec}A=\{\bar{\mathfrak{m}}_x\}$ y $\bar{s}\notin\bar{\mathfrak{m}}_x$. Sea $\bar{t}=\bar{s}^{-1}$. El inverso del morfismo $s\cdot\colon M\to M$ es $t\cdot$, pues el inverso de $\bar{s}\cdot$ es $\bar{t}\cdot$. Hemos concluido por la proposición 1.8.16.

17. Sean $S,S'\subset A$ dos sistemas multiplicativos. Prueba que $\operatorname{Spec}A_S=\operatorname{Spec}A_{S'}$ si y solo si los morfismos $A_S\to A_{SS'}$, $A_{S'}\to A_{SS'}$ son isomorfismos (luego $A_S=A_{S'}$). Sea $\mathfrak{p}_x\subset A$ un ideal primo tal que $\mathfrak{p}_x\cap S=\emptyset$ y denotemos $\mathfrak{p}_{x'}=\mathfrak{p}_x\cdot A_S$. Prueba que $A_x=(A_S)_{x'}$.

Resolución: $\Rightarrow$) Los elementos $s'=\frac{s'}{1}$ (con $s'\in S'$) no se anulan en ningún punto de $\operatorname{Spec}A_S=\operatorname{Spec}A_{S'}$, luego son invertibles en A_S. Luego, $A_S=(A_S)_{S'}=A_{SS'}$. $A_x=(A_S)_{x'}$ porque

$$\operatorname{Spec}(A_S)_{x'}=\{y\in\operatorname{Spec}A:\ \mathfrak{p}_y\cap S=\emptyset\text{ y }\mathfrak{p}_y\cdot A_S\subseteq\mathfrak{p}_{x'}\}$$
$$=\{y\in\operatorname{Spec}A:\ \mathfrak{p}_y\cap S=\emptyset\text{ y }\mathfrak{p}_y\subseteq\mathfrak{p}_x\}=\{y\in\operatorname{Spec}A:\ \mathfrak{p}_y\subseteq\mathfrak{p}_x\}=\operatorname{Spec}A_x.$$

.

18. Sea A un dominio de factorización única y $S\subseteq A$ un sistema multiplicativo. Prueba que A_S es un dominio de factorización única.

Resolución: Dado $a\in A$ irreducible, veamos que $\frac{a}{1}\in A_S$ es irreducible o invertible. Si $\frac{a}{s}=\frac{a_1}{s_1}\cdot\frac{a_2}{s_2}$, entonces $as_1s_2=a_1a_2s$, luego $a_1=a\cdot b$, ó $a_2=a\cdot b$, ó $s=a\cdot b$ (luego $\frac{a}{s}$ es invertible). En el primer caso, $\frac{a}{s}=\frac{a}{s}\cdot\frac{bs}{s_1}\cdot\frac{a_2}{s_2}$, luego $\frac{bs}{s_1}\cdot\frac{a_2}{s_2}=1$ y $\frac{a_2}{s_2}$ es invertible, lo que muestra que $\frac{a}{s}$ es irreducible.

Si $\frac{c}{s}\in A_S$ es irreducible, entonces salvo multiplicación por invertibles resulta que $\frac{c}{s}=\frac{c'}{s'}$ con $c'\in A$ irreducible: sea $c=c_1\cdots c_n$ la descomposición en producto de irreducibles de a, entonces $\frac{c}{s}=\frac{c_1}{s}\cdot\frac{c_2}{1}\cdots\frac{c_n}{1}$ y todos los factores son invertibles salvo uno que es irreducible.

Dado $\frac{b}{s} \in A_S$, sea $b = b_1 \cdots b_n$ la descomposición en producto de irreducibles de a. Entonces, $\frac{b}{s} = \frac{b_1}{s} \cdot \frac{b_2}{1} \cdots \frac{b_n}{1}$ es una descomposición en producto de irreducibles (e invertibles).

Veamos la unicidad de la factorización. Si $\frac{a}{s} = \frac{a_1}{s_1} \cdots \frac{a_n}{s_n} = \frac{a'_1}{s'_1} \cdots \frac{a'_m}{s'_m}$ son descomposiciones en producto de factores irreducibles (donde podemos suponer que los a_i y los a'_j son irreducibles), entonces $a_1 \cdots a_n \cdot s'_1 \cdots s'_m = a'_1 \cdots a'_m \cdot s_1 \cdots s_n$. Como a_1 no divide a ningún $t \in S$ (pues $\frac{a_1}{s_1}$ no es invertible) tenemos salvo orden e invertibles que $a_1 = a'_1$, y por recurrencia es fácil concluir.

19. Sea A un dominio de ideales principales y $S \subseteq A$ un sistema multiplicativo. Pruébese que A_S es un dominio de ideales principales.

Resolución: Sea $J \subset A_S$ un ideal. Sea $I := \{a \in A : \frac{a}{1} \in J\}$. Entonces, $J = I \cdot A_S$. Como I es principal, J lo es.

Capítulo 2

Dominios de Dedekind

2.1. Introducción

Los anillos que necesitamos para la Teoría de Números y para un curso de Curvas Algebraicas son los dominios localmente principales. Estos anillos se denominan anillos de Dedekind y estos anillos están caracterizados por que todo ideal se escribe de modo único (salvo orden) como producto de ideales primos.

2.2. Dominios de Dedekind

1. Definición: Diremos que un anillo A íntegro noetheriano es un dominio de Dedekind si y solo si A_x es un dominio de ideales principales para todo punto cerrado $x \in \operatorname{Spec} A$.

Observemos que los dominios de Dedekind, que no sean cuerpos, son anillos de dimensión de Krull 1.

2. Ejemplos: Los cuerpos son dominios de Dedekind.

Los dominios de ideales principales son dominios de Dedekind.

Los anillos euclídeos son anillos de ideales principales, luego son dominios de Dedekind.

3. Teorema: *Si A es un dominio de Dedekind e $I \subset A$ un ideal propio, entonces I se escribe de modo único como producto de ideales primos (salvo ordenación de los factores).*

Demostración. Sean $\{x_1, \ldots, x_m\} = (I)_0$. Sabemos que A_{x_i} es un anillo de ideales principales. Por tanto, $I_{x_i} = \mathfrak{p}_{x_i}^{n_i} A_{x_i}$, para cierto $n_i \in \mathbb{N}$ único. El ideal

$$\mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_m}^{n_m}$$

es igual localmente a I, luego son iguales globalmente. Evidentemente los exponentes n_i están determinados porque lo están al localizar. □

4. Teorema: *Sea A un dominio de integridad. Si todo ideal propio de A se escribe de modo único como producto de ideales primos (salvo ordenación de los factores) entonces A es un dominio de Dedekind.*

Demostración. Sea $\mathfrak{m}_x \subset A$ un ideal maximal. Por la unicidad $\mathfrak{m}_x^2 \neq \mathfrak{m}_x$. Sea $a \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$, es decir, $0 \neq \bar{a} \in \mathfrak{m}_x/\mathfrak{m}_x^2$. Observemos que $(\mathfrak{m}_x/\mathfrak{m}_x^2)_x = \mathfrak{m}_x/\mathfrak{m}_x^2$, porque dado $s \in A \setminus \mathfrak{m}_x$, $\bar{s}$ es invertible en $A/\mathfrak{m}_x$ y el morfismo $s\cdot\colon \mathfrak{m}_x/\mathfrak{m}_x^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$, $\bar{m} \mapsto s \cdot \bar{m} = \overline{sm} = \bar{s} \cdot \bar{m}$ es isomorfismo. Por tanto, $0 \neq \bar{a} \in \mathfrak{m}_x/\mathfrak{m}_x^2 = (\mathfrak{m}_x/\mathfrak{m}_x^2)_x = \mathfrak{m}_x A_x/\mathfrak{m}_x^2 A_x$. Escribamos $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ como producto de ideales primos. Reordenando podemos suponer que $\mathfrak{p}_i \subseteq \mathfrak{m}_x$ si y solo si $i \leq r$ (para cierto $r \leq n$). Localizando en x, tenemos que $a \cdot A_x = \mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot A_x \subseteq \mathfrak{m}_x^r A_x$, pero $a \notin \mathfrak{m}_x^2 A_x$, luego $r = 1$ y $a \cdot A_x = \mathfrak{p}_1 \cdot A_x$. Sea $b \in \mathfrak{m}_x$ tal que $b \notin aA_x$. Escribamos $(a,b) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ como producto de ideales primos. Reordenando podemos suponer que $\mathfrak{q}_i \subseteq \mathfrak{m}_x$ si y solo si $i \leq s$ (para cierto $s \leq n$). Localizando en x, tenemos que $(a,b) \cdot A_x = \mathfrak{q}_1 \cdots \mathfrak{q}_s \cdot A_x \subseteq \mathfrak{m}_x^s A_x$, pero $a \notin \mathfrak{m}_x^2 A_x$, luego $s = 1$ y $(a,b) \cdot A_x = \mathfrak{q}_1 \cdot A_x$ que es un ideal primo. Igualmente, $(a, b^2)A_x$ es un ideal primo y ha de coincidir con $(a,b)A_x$. Entonces, $(\bar{b}) = (\bar{b}^2)$ en el anillo íntegro A_x/aA_x, luego $\bar{b}$ es invertible, lo cual es contradictorio porque $A_x/(a,b)A_x$ es no nulo. En conclusión, $\mathfrak{m}_x A_x = aA_x$.

Dado un ideal primo $0 \neq \mathfrak{p} \underset{\neq}{\subset} \mathfrak{m}_x$, tenemos que todos los elementos de $\mathfrak{p}A_x$ son multiplos de a y es fácil ver que $\mathfrak{p}A_x = a \cdot \mathfrak{p}A_x = \mathfrak{m}_x \mathfrak{p} A_x$, luego $\mathfrak{p} = \mathfrak{m}_x \mathfrak{p}$ (porque localmente son iguales) y llegamos a contradicción. Luego todos los ideales primos de A, no nulos, son maximales.

Sólo nos falta probar que A es noetheriano. Basta ver que $\mathfrak{m}_x$ es finito generado. Tenemos $(a) = \mathfrak{m}_x \cdot \mathfrak{m}_{x_2}^{n_2} \cdots \mathfrak{m}_{x_r}^{n_r}$ Sea $b \in A$ tal que su clase en $A/\mathfrak{m}_x \times A/\mathfrak{m}_{x_2} \times \cdots \times A/\mathfrak{m}_{x_r}$ sea igual a $(\bar{0}, \bar{1}, \ldots, \bar{1})$, entonces $\mathfrak{m}_x = (a,b)$, como se comprueba localmente.

□

Los anillos de Dedekind no son dominios de factorización única en general, aunque estos teoremas estén muy cerca de afirmarlo. Por la proposición 1.6.6, un dominio de Dedekind es d.f.u. si y solo si es d.i.p. Se tiene las siguiente inclusiones estrictas (ver el problema 11 del capítulo 1. y el problema 14 de este capítulo).

{Anillos euclídeos} $\subset$ {Dominios de ideales principales} $\subset$ {Dominios de Dedekind}

2.2.1. Ideales fraccionarios

Sea A un anillo íntegro de cuerpo de fracciones K.

Dados dos A-submódulos $I_1, I_2 \subseteq K$, se define

$$I_1 \cdot I_2 := \langle i_1 \cdot i_2, \forall i_1 \in I_1, \forall i_2 \in I_2 \rangle$$
$$[I_1 : I_2] := \{f \in K : f \cdot I_2 \subseteq I_1\}$$

que son A-submódulos de K. Observemos que

$$[I_1 : I_2 + I_3] = [I_1 : I_2] \cap [I_1 : I_3].$$

y si $I_2 \subseteq I_3$ entonces $[I_1 : I_2] \supseteq [I_1 : I_3]$.

5. Proposición : *Sean I, J dos A-submódulos de K y supongamos que J es un A-módulo finito generado. Sea $S \subset A$ un sistema multiplicativo, entonces*

$$[I : J]_S = [I_S : J_S].$$

Demostración. Escribamos $J = f_1 A + \cdots + f_r A_r$, con $f_i \in K$. Entonces,

$$[I : J]_S = (\cap_{i=1}^r [I : f_i A])_S = (\cap_{i=1}^r f_i^{-1} I)_S = \cap_{i=1}^r f_i^{-1} I_S = \cap_{i=1}^r [I_S : f_i A_S] = [I_S : J_S].$$

□

6. Definición : Llamemos ideal fraccionario de K a los A-submódulos no nulos finito generados de K. [1]

Supongamos que A es noetheriano, que I es un ideal fraccionario de K y que J es un A-submódulo no nulo de K. Dado $f \in J$ no nulo, observemos que $[I : J] \subset [I : fA] = f^{-1} I$ que es un A-módulo finito generado, luego $[I : J]$ es finito generado. En conclusión, la suma, producto y división de ideales fraccionarios es ideal fraccionario.

7. Ejemplo : Calculemos los ideales fraccionarios de $\mathbb{Q}$. Sea $I = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$ un ideal fraccionario de $\mathbb{Q}$. Sea $b = b_1 \cdots b_n$ entonces

$$I = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle = \langle \frac{a_1'}{b}, \ldots, \frac{a_n'}{b} \rangle = \frac{1}{b} \cdot \langle a_1', \ldots, a_n' \rangle = \frac{1}{b} \cdot m.c.d.(a_1', \ldots, a_n') \cdot \mathbb{Z} = \frac{a}{b} \cdot \mathbb{Z}.$$

8. Proposición : *Dos ideales fraccionarios I, I' son isomorfos (como A-módulos) si y solo si existe $f \in K$ tal que $I' = f \cdot I$.*

Demostración. $\Rightarrow$) Dado un isomorfismo $I \simeq I'$, localizando por $A \setminus \{0\}$, obtenemos un isomorfismo de K-espacios vectoriales $K \simeq K$, que es multiplicar por una $f \in K$, luego $I' = f \cdot I$.

□

Por tanto, si $I_1 \simeq I_1'$ e $I_2 \simeq I_2'$ entonces $I_1 \cdot I_2 \simeq I_1' \cdot I_2'$.

[1] Advertencia: los ideales fraccionarios de K no son ideales de K.

9. Proposición: *La aplicación*

$$\{\textit{Ideales finito generados de } A\}/\simeq \longrightarrow \{\textit{Ideales fraccionarios de } K\}/\simeq,\ [\mathfrak{a}]\mapsto[\mathfrak{a}]$$

es un isomorfismo de semigrupos.

Demostración. Evidentemente la aplicación es inyectiva. Dado un ideal fraccionario I, existe $a\in A$ tal que $a\cdot I$ es un ideal de A, por tanto $[I]=[aI]$ y la aplicación es epiyectiva. □

10. Nota: A partir de ahora en esta subsección supondremos que A es un dominio de Dedekind y que K es el cuerpo de fracciones de A.

11. Proposición: *Sea A un domino de Dedekind de cuerpo de fracciones K y $I\subset K$ un ideal fraccionario. Entonces, $I\cdot[A:I]=A$ y por tanto el conjunto de ideales fraccionarios de K es un grupo.*

Demostración. Basta probar que $I_x\cdot[A_x:I_x]=A_x$ para todo $x\in \mathrm{Spec}_{max}A$. Podemos suponer que A es un dominio de ideales principales local y tenemos que probar que $I\cdot[A:I]=A$. A es un anillo euclídeo, e I es un A-módulo finito generado sin torsión de rango 1 (porque $I_{A\setminus\{0\}}=K$), luego es libre de rango 1, es decir $I=f\cdot A$. Entonces, $I\cdot[A:I]=fA\cdot f^{-1}A=A$. □

Dado un ideal fraccionario I, denotemos $I^{-1}=[A:I]$, que es el inverso de I. Obviamente, $I^{-n}:=I^{-1}\overset{n}{\cdots}I^{-1}$ es igual a $[A:I^n]$, para todo $n>0$, pues ambos son el inverso de I^n. Observemos que

$$(\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_m}^{n_m})\cdot(\mathfrak{m}_{x_1}^{n'_1}\cdots\mathfrak{m}_{x_m}^{n'_m})=\mathfrak{m}_{x_1}^{n_1+n'_1}\cdots\mathfrak{m}_{x_m}^{n_m+n'_m},\ \text{para todo } n_i,n'_i\in\mathbb{Z}.$$

12. Proposición: *Sea I un ideal fraccionario de K. Existen ciertos $x_1,\dots,x_m\in\mathrm{Spec}\,A$ distintos (y únicos) y ciertos $n_1,\dots,n_m\in\mathbb{Z}$ no nulos (únicos), de modo que*

$$I=\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_m}^{n_m}.$$

Demostración. Sea $a\in A$ tal que $a\cdot I$ sea un ideal de A. Por el teorema 2.2.3, $(a)=\mathfrak{m}_{x_1}^{r_1}\cdots\mathfrak{m}_{x_m}^{r_m}$ y $a\cdot I=\mathfrak{m}_{x_1}^{s_1}\cdots\mathfrak{m}_{x_m}^{s_m}$, con $r_i,s_i\geq 0$. Por tanto,

$$I=(a)^{-1}\cdot aI=\mathfrak{m}_{x_1}^{-r_1}\cdots\mathfrak{m}_{x_m}^{-r_m}\cdot\mathfrak{m}_{x_1}^{s_1}\cdots\mathfrak{m}_{x_m}^{s_m}=\mathfrak{m}_{x_1}^{s_1-r_1}\cdots\mathfrak{m}_{x_m}^{s_m-r_m}.$$

Supongamos $\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_m}^{n_m}=\mathfrak{m}_{x_1}^{n'_1}\cdots\mathfrak{m}_{x_m}^{n'_m}$, con $n_i,n'_i\in\mathbb{Z}$. Reordenando, podemos suponer que $n_i\geq n'_i$ si y solo si $1\leq i<s$. Entonces, $\mathfrak{m}_{x_1}^{n_1-n'_1}\cdots\mathfrak{m}_{x_{s-1}}^{n_{s-1}-n'_{s-1}}=\mathfrak{m}_{x_s}^{n'_s-n_s}\cdots\mathfrak{m}_{x_m}^{n'_m-n_m}$, y por el teorema 2.2.3, $n_j-n'_j=0$ para todo j.

□

13. Definición: El grupo de Picard de A, que denotaremos $\mathrm{Pic}\,A$, es el grupo de las clases de isomorfía de los ideales no nulos de A.

14. Proposición: $\mathrm{Pic}\,A = \{1\}$ *si y solo si* A *es un dominio de ideales principales.*

Demostración. $\Rightarrow$) Dado un ideal no nulo $I \subseteq A$, tenemos que $[I] = [A]$, es decir, I es isomorfo a A, luego existe $f \in K$ tal que $I = f\cdot$, luego I es principal.

$\Leftarrow$) Si todo ideal es principal, entonces todo ideal es isomorfo a A, luego $\mathrm{Pic}\,A = \{1\}$.

□

2.3. Puntos singulares. Criterios diferenciales

1. Proposición: *Sea* A *un anillo íntegro noetheriano.* A *es un dominio de Dedekind si y solo si* A *es un cuerpo o para todo ideal primo maximal* $\mathfrak{m}$*, se cumple que* $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Demostración. Si A es un dominio de Dedekind entonces es un cuerpo o tiene dimensión de Krull 1. En este segundo caso, para todo ideal maximal $\mathfrak{m}_x$, por el teorema 1.6.5, $\mathfrak{m}_x A_x = (t)$, luego $(\bar{t}) = \mathfrak{m}_x A_x/\mathfrak{m}_x^2 A_x = (\mathfrak{m}_x/\mathfrak{m}_x^2)_x = \mathfrak{m}_x/\mathfrak{m}_x^2$ y $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = 1$. Recíprocamente, si $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = 1$ entonces $\mathfrak{m}_x A_x/\mathfrak{m}_x^2 A_x = (\bar{t})$ y por el lema de Nakayama $\mathfrak{m}_x A_x = (t)$. Por el teorema 1.6.5 A_x es d.i.p., y A es un dominio de Dedekind.

□

2. Definición: Sea A un anillo íntegro de dimensión de Krull 1. Diremos que un punto cerrado $x \in \mathrm{Spec}\,A$ es no singular si A_x es un anillo de ideales principales (es decir, $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 = 1$). Diremos que x es singular si A_x no es un anillo de ideales principales (es decir, $\dim_{A/\mathfrak{m}_x} \mathfrak{m}_x/\mathfrak{m}_x^2 > 1$).

Por tanto, los dominios de Dedekind son los dominios noetherianos de dimensión de Krull 1 sin puntos singulares.

3. Definición: Dado un ideal maximal $\mathfrak{m}_x \subset A$ y $f \in \mathfrak{m}_x$, denotaremos $d_x f := \bar{f} \in \mathfrak{m}_x/\mathfrak{m}_x^2$. Si A es una k-álgebra y $A/\mathfrak{m}_x = k$, denotaremos $f(x) := \bar{f} \in A/\mathfrak{m}_x = k$ y $d_x f := \overline{f - f(x)} \in \mathfrak{m}_x/\mathfrak{m}_x^2$.

4. Ejemplo: Sea $\mathfrak{m}_\alpha := (x_1 - \alpha_1, \ldots, x_n - \alpha_n) \subset k[x_1, \ldots, x_n]$ y $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Entonces, $p(x_1, \ldots, x_n) = p(\alpha) + \sum_i \frac{\partial p}{\partial x_i}(\alpha)(x_i - \alpha_i) + \sum_{ij}(x_i - \alpha_i)(x - \alpha_j)\cdot h_{ij}(x)$. Por tanto,

$$d_\alpha p(x_1, \ldots, x_n) = \frac{\partial p}{\partial x_1}(\alpha) d_\alpha x_1 + \cdots + \frac{\partial p}{\partial x_n}(\alpha) d_\alpha x_n$$

y $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$ es un k-espacio vectorial de base $\{d_\alpha x_i = \overline{x_i - \alpha_i}\}$.

5. Proposición: *Sea $\mathfrak{m}_x \subset A$ un ideal maximal. Sea $I = (f_1, \ldots, f_n) \subset A$ un ideal incluido en $\mathfrak{m}_x$ y sea $\bar{m}_x \subset A/I$ el ideal de las clases de $\mathfrak{m}_x$. Se cumple que*

$$\bar{m}_x/\bar{m}_x^2 = (\mathfrak{m}_x/\mathfrak{m}_x^2)/\langle d_x f_1, \ldots, d_x f_n\rangle.$$

Demostración. Observemos que $\bar{m}_x = \mathfrak{m}_x/I$. Por tanto,

$$\bar{m}_x/\bar{m}_x^2 = \mathfrak{m}_x/(I + \mathfrak{m}_x^2) = (\mathfrak{m}_x/\mathfrak{m}_x^2)/\bar{I} = (\mathfrak{m}_x/\mathfrak{m}_x^2)/\langle d_x f_1, \ldots, d_x f_n\rangle.$$

□

6. Ejemplo: Sea $p(x,y) \in \mathbb{C}[x,y]$ y $(\alpha,\beta) \in \mathbb{C}^2$ tal que $p(\alpha,\beta) = 0$, entonces $(\alpha,\beta) \in \mathrm{Spec}_{max}\, \mathbb{C}[x,y]/(p(x,y))$.

Denotemos la imagen de $\mathfrak{m}_{(\alpha,\beta)}$ en $\mathbb{C}[x,y]/(p(x,y))$, $\bar{\mathfrak{m}}_{(\alpha,\beta)}$. Como

$$\bar{\mathfrak{m}}_{(\alpha,\beta)}/\bar{\mathfrak{m}}_{(\alpha,\beta)}^2 = (\mathfrak{m}_{(\alpha,\beta)}/\mathfrak{m}_{(\alpha,\beta)}^2)/(d_{(\alpha,\beta)}p(x,y)),$$

$\dim \bar{\mathfrak{m}}_{(\alpha,\beta)}/\bar{\mathfrak{m}}_{(\alpha,\beta)}^2 = 1$ si y solo si $d_{(\alpha,\beta)}p(x,y) \neq 0$.

Luego, $\mathcal{O} = (\mathbb{C}[x,y]/(p(x,y)))_{(\alpha,\beta)}$ es un dominio de ideales principales si y solo si $d_{(\alpha,\beta)}p(x,y) \neq 0$. Por ejemplo, si $\frac{\partial p}{\partial y}(\alpha,\beta) \neq 0$, entonces $\bar{\mathfrak{m}}_{(\alpha,\beta)}/\bar{\mathfrak{m}}_{(\alpha,\beta)}^2 = (d_{(\alpha,\beta)}x)$, luego $\bar{\mathfrak{m}}_{(\alpha,\beta)} \cdot \mathcal{O} = (x - \alpha)$.

7. Ejemplo: $\mathrm{Spec}\, \mathbb{C}[x,y]/(y^2 - x^3)$ tiene un único punto singular: el origen. En efecto, $0 = d_{(\alpha,\beta)}(y^2 - x^3) = -3\alpha^2 d_{(\alpha,\beta)}x + 2\beta d_{(\alpha,\beta)}y$ si y solo si $(\alpha,\beta) = (0,0)$.

8. Definición: Sea $A \to B$ un morfismo finito y $\pi\colon \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ el morfismo inducido. Sea $y \in \mathrm{Spec}_{max} B$ y $x := \pi(y)$. Se dice que x es un punto rama de π si $B/\mathfrak{m}_x B$ no es una $A/\mathfrak{m}_x$-álgebra separable. Se dice que π ramifica en y (o que y es un punto de ramificación de π) si $B_y/\mathfrak{m}_x B_y$ no es una $A/\mathfrak{m}_x$-álgebra separable.

$B/\mathfrak{m}_x B$ es una $A/\mathfrak{m}_x$-álgebra finita, luego

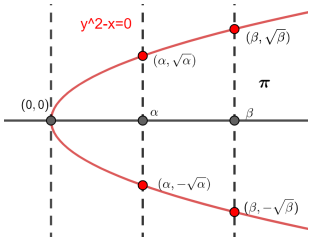
$$B/\mathfrak{m}_x B = \prod_{y \in \mathrm{Spec}\, B/\mathfrak{m}_x B} (B/\mathfrak{m}_x B)_y = \prod_{y \in \pi^{-1}(x)} B_y/\mathfrak{m}_x B_y$$

y no es separable si y solo si alguno de los $B_y/\mathfrak{m}_x B_y$ no es separable. Por tanto,

$$\pi(\{\text{Puntos de ramificación de } \pi\}) = \{\text{Puntos rama de } \pi\}.$$

9. Ejemplo: Consideremos el morfismo finito e inyectivo

$$\mathbb{C}[x] \to \mathbb{C}[x,y]/(y^2 - x), \;\; p(x) \mapsto \overline{p(x)}.$$



Sea $\pi\colon \operatorname{Spec}\mathbb{C}[x,y]/(y^2-x) \to \operatorname{Spec}\mathbb{C}[x]$, $(\alpha,\beta)\mapsto\alpha$ el morfismo inducido. Calculemos los puntos rama y los puntos de ramificación de π. Dado $\alpha\in\operatorname{Spec}_{max}\mathbb{C}[x]$, tenemos que $\pi^{-1}(\alpha)=\operatorname{Spec}\mathbb{C}[x,y]/(x-\alpha,y^2-x)=\operatorname{Spec}\mathbb{C}[y]/(y^2-\alpha)$ y $\mathbb{C}[y]/(y^2-\alpha)$ es una $\mathbb{C}$-álgebra finita separable si y solo si $\alpha\neq 0$. Por tanto, α es un punto rama si y solo si $\alpha\neq 0$. Observemos que $\pi^{-1}(0)=\{(0,0)\}$ y que $(\mathbb{C}[y]/(y^2))_{(0,0)}=\mathbb{C}[y]/(y^2)$ no es una $\mathbb{C}$-álgebra finita separable. Por tanto, $(0,0)$ es el único punto de ramificación de π.

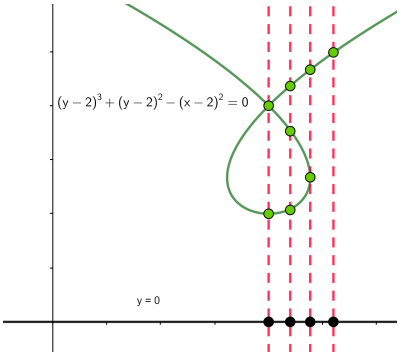
10. Ejercicio: Consideremos el morfismo

$$\begin{array}{ccc}\mathbb{C}[x] & \to & \mathbb{C}[x,y]/((y-2)^3+(y-2)^2-(x-2)^2)\\ p(x) & \mapsto & \overline{p(x)}\end{array}$$

y el morfismo inducido

$$\begin{array}{ccc}\operatorname{Spec}\mathbb{C}[x,y]/((y-2)^3+(y-2)^2-(x-2)^2) & \xrightarrow{\pi} & \operatorname{Spec}\mathbb{C}[x]\\ (\alpha,\beta) & \mapsto & \alpha\end{array}$$

Calcula los puntos rama y de ramificación de π.



11. Proposición: *Sea A un anillo íntegro de cuerpo de fracciones Σ. Sea $p(x)\in A[x]$ un polinomio mónico separable y sea $0\neq\Delta\in A$ el discriminante de $p(x)$. Consideremos el morfismo finito $A\hookrightarrow A[x]/(p(x))$ y el morfismo inducido $\pi\colon \operatorname{Spec}A[x]/(p(x))\to\operatorname{Spec}A$. Entonces,*

$$\{\textit{Puntos rama de } \pi\}=(\Delta)_0\cap\operatorname{Spec}_{max}A.$$

Demostración. El punto z es un punto rama si y solo $(A[x]/(p(x)))/\mathfrak{p}_z=A/\mathfrak{p}_z[x]/(\overline{p(x)})$ no es una $A/\mathfrak{p}_z$-álgebra separable, es decir, $\overline{p(x)}\in A/\mathfrak{p}_z[x]$ no es separable, que equivale a decir que el discriminante de $\overline{p(x)}$ es nulo, o equivalentemente $\bar{\Delta}=0$ en $A/\mathfrak{p}_z$, es decir, $z\in(\Delta)_0$. □

12. Proposición: *Sea $i\colon A\to B$ un morfismo de anillos finito y $i^*\colon \operatorname{Spec}B\to\operatorname{Spec}A$ el morfismo inducido en espectros. Sea $y\in\operatorname{Spec}B$ un punto cerrado y $x=i^*(y)$. Si $(B/\mathfrak{m}_xB)_y$ es un cuerpo, entonces $\mathfrak{m}_x\cdot B_y=\mathfrak{m}_y\cdot B_y$.*

Consecuencia: "Si y no es un punto de ramificación, entonces $\mathfrak{m}_x\cdot B_y=\mathfrak{m}_y\cdot B_y$ y si además $\mathfrak{m}_xA_x$ es principal, entonces $\mathfrak{m}_yB_y$ es principal."

Demostración. Si $(B/\mathfrak{m}_xB)_y=B_y/\mathfrak{m}_xB_y$ es un cuerpo, entonces $\mathfrak{m}_x\cdot B_y$ es igual al ideal maximal de B_y, es decir, $\mathfrak{m}_y\cdot B_y$.

Si y no es de ramificación entonces $(B/\mathfrak{m}_xB)_y=B_y/\mathfrak{m}_x\cdot B_y$ es una $A/\mathfrak{m}_x$-álgebra finita separable local, luego un cuerpo, por tanto $\mathfrak{m}_x\cdot B_y=\mathfrak{m}_y\cdot B_y$. □

13. Corolario: *Sea $A \hookrightarrow B$ un morfismo de anillos finito entre anillos íntegros y sea $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido en espectros. Si A es un dominio de Dedekind, entonces*

$$\{\textit{Ptos. singulares de } \operatorname{Spec} B\} \subseteq \{\textit{Ptos. de ramificación de } \pi\} \subseteq \pi^{-1}(\{\textit{Ptos. rama de } \pi\}).$$

14. Ejemplo: Consideremos el morfismo $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$. Podemos calcular $\operatorname{Spec}\mathbb{Z}[x]$ por la fórmula de la fibra. Tenemos que los ideales maximales de $\mathbb{Z}[x]$ son de la forma $\mathfrak{m}_y = (p, q(x))$, con p primo y $q(x)$ irreducible módulo p; los ideales primos no maximales son de la forma $(q(x))$ con $q(x) \in \mathbb{Z}[x]$ irreducible, y el ideal minimal es (0).

Consideremos el ideal maximal $\mathfrak{m}_y = (p, q(x)) \subset \mathbb{Z}[x]$ y sea $k(y) := \mathbb{Z}[x]/\mathfrak{m}_y$. Entonces, $\mathfrak{m}_y/\mathfrak{m}_y^2$ es un $k(y)$-espacio vectorial de base $\{\bar{p}, \overline{q(x)}\}$, porque si $\mathfrak{m}_y/\mathfrak{m}_y^2$ tuviese dimensión 1, ello implicaría que $\mathbb{Z}[x]_y$ sería de dimensión de Krull pero esto es imposible porque tenemos la cadena de ideales primos $(0) \subset (p) \subset (p, q(x))$. Sea $f(x) \in \mathfrak{m}_y$ y sea $\bar{\mathfrak{m}}_y$ las clases de $\mathfrak{m}_y$ en $\mathbb{Z}[x]/(f(x))$. Entonces, $\bar{\mathfrak{m}}_y/\bar{\mathfrak{m}}_y^2 = (\mathfrak{m}_y/\mathfrak{m}_y^2)/(d_y f(x))$. Por tanto,

$$\dim_{k(y)}(\bar{\mathfrak{m}}_y/\bar{\mathfrak{m}}_y^2) = 1, \text{ si y solo si } d_y f(x) \neq 0.$$

Calculemos los puntos singulares de $\operatorname{Spec}\mathbb{Z}[\sqrt{2}]$ y de $\operatorname{Spec}\mathbb{Z}[\sqrt{5}]$: Consideremos el morfismo finito $\mathbb{Z} \to \mathbb{Z}[\sqrt{2}]$. El conjunto de los puntos singulares de $\mathbb{Z}[\sqrt{2}]$ es un subconjunto del conjunto de los puntos de ramificación, por la proposición anterior. $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2-2)$ y x^2-2 es separable módulo p, para todo p salvo $p=2$. Observemos que $\operatorname{Spec}\mathbb{Z}[x]/(2, x^2-2) = \operatorname{Spec}\mathbb{Z}[x]/(2, x^2) = \{(\bar{2}, \bar{x})\}$. Por tanto, $y \in \operatorname{Spec}\mathbb{Z}[\sqrt{2}]$ es no singular, para todo y, salvo quizá cuando $\bar{\mathfrak{m}}_y = (2, \sqrt{2})$. Ahora bien, para $\mathfrak{m}_y = (2, x)$, tenemos que $d_y(x^2-2) = d_y 2 \neq 0$, luego y es no singular. Efectivamente, $\bar{\mathfrak{m}}_y = (\sqrt{2})$. En conclusión, $\mathbb{Z}[\sqrt{2}]$ es dominio de Dedekind.

$\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ y x^2-5 es separable módulo p, para todo primo p salvo $p = 2$ y $p = 5$. Observemos que $\operatorname{Spec}\mathbb{Z}[x]/(2, x^2-5) = \operatorname{Spec}\mathbb{Z}[x]/(2, (x+1)^2) = \{(\bar{2}, \overline{x+1})\}$ y $\operatorname{Spec}\mathbb{Z}[x]/(5, x^2-5) = \operatorname{Spec}\mathbb{Z}[x]/(5, x^2) = \{(\bar{5}, \bar{x})\}$. Para $\mathfrak{m}_y = (2, x+1)$, tenemos que

$$d_y(x^2-5) = d_y((x+1)^2 - 2(x+1) - 2^2) = 0,$$

luego y es singular. Para $\mathfrak{m}_y = (5, x)$, tenemos que $d_y(x^2-5) = -d_y(5) \neq 0$, luego y es no singular. En conclusión, $y \in \operatorname{Spec}\mathbb{Z}[\sqrt{5}]$, con $\mathfrak{m}_y = (2, \sqrt{5}+1)$, es el único punto singular.

15. Lema: *Sean $i_1\colon A \to B_1$ y $i_2\colon A \to B_2$ morfismos finitos. Sea $y \in \operatorname{Spec}(B_1 \otimes_A B_2)$ un punto cerrado. Consideremos los diagramas conmutativos obvios*

$$\begin{array}{ccc} B_1 & \xrightarrow{\pi_2} & B_1 \otimes_A B_2 \\ {\scriptstyle i_1}\uparrow & \overset{i}{\nearrow} & \uparrow{\scriptstyle \pi_1} \\ A & \xrightarrow[i_2]{} & B_2 \end{array} \qquad \begin{array}{ccc} \operatorname{Spec} B_1 & \xleftarrow{\pi_2^*} & \operatorname{Spec}(B_1 \otimes_A B_2) \\ {\scriptstyle i_1^*}\downarrow & \overset{i^*}{\swarrow} & \downarrow{\scriptstyle \pi_1^*} \\ \operatorname{Spec} A & \xleftarrow[i_2^*]{} & \operatorname{Spec} B_2 \end{array} \qquad \begin{array}{ccc} y_1 & \xleftarrow{\pi_2^*} & y \\ {\scriptstyle i_1^*}\downarrow & \overset{i^*}{\swarrow} & \downarrow{\scriptstyle \pi_1^*} \\ x & \xleftarrow[i_2^*]{} & y_2 \end{array}$$

Entonces,

1. $i_2^{*-1}(\{\textit{Puntos rama de } i_1^*\}) = \{\textit{Puntos rama de } \pi_1^*\}$.

2. *Supongamos que B_1 y B_2 son dominios de Dedekind. Entonces,*

$\{y \in \mathrm{Spec}_{max} B_1 \otimes_A B_2 : \dim \mathfrak{m}_y/\mathfrak{m}_y^2 > 1\} \subseteq \pi^{*-1}(\{\textit{Ptos. rama de } i_1^*\} \cap \{\textit{Ptos. rama de } i_2^*\})$.

3. $\{\textit{Puntos rama de } i^*\} = \{\textit{Puntos rama de } i_1^*\} \cup \{\textit{Puntos rama de } i_2^*\}$.

Demostración. 1. Observemos que

$$(B_1 \otimes_A B_2)/(\mathfrak{m}_{y_2}) = (B_1 \otimes_A B_2) \otimes_{B_2} B_2/\mathfrak{m}_{y_2} = B_1 \otimes_A (B_2/\mathfrak{m}_{y_2}) = B_1/\mathfrak{m}_x B_1 \otimes_{A/\mathfrak{m}_x} B_2/\mathfrak{m}_{y_2}$$

que es una $B/\mathfrak{m}_{y_2}$-álgebra separable si y solo si $B_1/\mathfrak{m}_x B_1$ es una $A/\mathfrak{m}_x$-álgebra separable. Luego, y_2 es un punto rama de π_1^* si y solo si x es un punto rama de i_1^*.

2. Si

$$y \notin \pi^{*-1}\{\text{Ptos. rama de } i_1^*\} = \pi_1^{*-1}(i_2^{*-1}\{\text{Ptos. rama de } i_1^*\}) \overset{1.}{=} \pi_1^{*-1}\{\text{Puntos rama de } \pi_1^*\}$$

entonces y_1 no es un punto rama, luego $\mathfrak{m}_y \cdot (B_1 \otimes B_2)_y = \mathfrak{m}_{y_1} \cdot (B_1 \otimes B_2)_y$ es principal, luego $\dim \mathfrak{m}_y/\mathfrak{m}_y^2 = 1$.

3. Observemos que

$$(B_1 \otimes_A B_2)/(\mathfrak{m}_x) = (B_1 \otimes_A B_2) \otimes_A A/\mathfrak{m}_x = (B_1/\mathfrak{m}_x B_1) \otimes_{A/\mathfrak{m}_x} (B_2/\mathfrak{m}_x B_2)$$

y recordemos que dos k-álgebras finitas C_1, C_2 son separables si y solo si $C_1 \otimes_k C_2$ es separable. Luego, x es un punto rama de i^* si y solo si no es rama para i_1^* o i_2^*.

□

16. Proposición: *$\mathbb{Z}[e^{\frac{2\pi i}{m}}]$ es un dominio de Dedekind.*

Demostración. Escribamos $\xi_m = e^{2\pi i/m} \in \mathbb{C}$. Veamos que $\mathbb{Z}[\xi_m]$ es un dominio de Dedekind. Supongamos $m = p^n$, con p primo. El polinomio mínimo anulador de ξ_{p^n}, $\Phi_{p^n}(x)$, que divide a $x^{p^n} - 1$, es separable módulo todo primo $q \neq p$. Por tanto, si $\mathfrak{m}_y \subset \mathbb{Z}[\xi_m]$, cumple que $\mathfrak{m}_y \cap \mathbb{Z} = (q)$, tenemos que $\mathfrak{m}_y \cdot \mathbb{Z}[\xi_{p^n}]_y = (q)$, para $q \neq p$. El único punto singular posible de $\mathrm{Spec}\,\mathbb{Z}[\xi_{p^n}] = \mathrm{Spec}\,\mathbb{Z}[x]/(\Phi_{p^n}(x))$, es $\mathfrak{m}_y = (p, \bar{x} - 1)$. Observemos que

$$\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}}) = (x^{p^{n-1}})^{p-1} + \cdots + x^{p^{n-1}} + 1$$

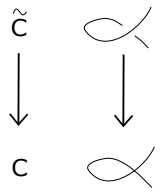
Por tanto, $\mathbb{Z}[x]/(\Phi_{p^n}(x), x-1) = \mathbb{Z}/(p)$ y $(p, \bar{x}-1) = (\bar{x}-1)$. Luego, y es no singular. Luego, $\mathbb{Z}[\xi_m]$ es un dominio de Dedekind.

Escribamos ahora, $m = p_1^{n_1} \cdots p_r^{n_r}$ como producto de potencias de número primos. Por el lema anterior, $\mathbb{Z}[\xi_{p_1^{n_1}}] \otimes \cdots \otimes \mathbb{Z}[\xi_{p_r^{n_r}}]$ es anillo localmente de ideales principales.

Observemos que $\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_{p_1^{n_1}}, \ldots, \xi_{p_r^{n_r}}]$ y es igual a un cociente (de hecho es igual) de $\mathbb{Z}[\xi_{p_1^{n_1}}] \otimes \cdots \otimes \mathbb{Z}[\xi_{p_r^{n_r}}]$. Luego, es localmente d.i.p., luego es un dominio de Dedekind.

□

2.4. Anillos normales de dimensión de Krull 1



Consideremos el nodo $C \equiv y^2 - x^2 + x^3 = 0$ y la curva $\tilde{C}$ que se obtiene de "despegar las dos ramas" de C. El morfismo natural $\tilde{C} \to C$, "pegar las dos ramas", es un morfismo finito que es isomorfismo fuera del nodo de C, luego es birracional (es decir, quitando un número finito conveniente de puntos en $\tilde{C}$ y en C es un isomorfismo). Parece claro intuitivamente que entre curvas no singulares en todo punto, no existen más morfismos finitos birracionales que los isomorfismos. En este sección vamos a ver la relación que hay entre los anillos de Dedekind y los anillos de noetherianos de dimensión de Krull 1 íntegramente cerrados en su cuerpo de fracciones.

1. Definiciones: Diremos que un anillo íntegro A es íntegramente cerrado en su cuerpo de fracciones Σ, si todo elemento de Σ entero sobre A pertenece a A. También se dice que A es un anillo normal.

Se dice que un morfismo de anillos $A \to B$ es entero si todo elemento de B es entero sobre A, es decir, si B es unión de A-subálgebras finitas.

Sea $A \to B$ un morfismo inyectivo de anillos. Llamaremos cierre entero de A en B al subanillo de B formado por todos los elementos de B enteros sobre A.

2. Proposición: *Los dominios de factorización única son anillos normales.*

Demostración. Sea A un dominio de factorización única y Σ su cuerpo de fracciones. Sea $\frac{a}{b} \in \Sigma$ una fracción de modo que b no sea invertible y sea primo con a. Si $\frac{a}{b}$ es entero sobre A, verifica una relación

$$(\frac{a}{b})^n + a_1(\frac{a}{b})^{n-1} + \ldots + a_n = 0$$

Multiplicando por b^n tendremos que a^n es múltiplo de b, lo que contradice que b es primo con a. En conclusión, los únicos elementos de Σ enteros sobre A son los de A.

□

3. Teorema: *Sea $\mathcal{O}$ un anillo íntegro local noetheriano de dimensión de Krull* 1. *Las siguientes condiciones son equivalentes:*

1. *$\mathcal{O}$ es dominio de ideales principales.*
2. *$\mathcal{O}$ es normal.*

Demostración. 1. $\Rightarrow$ 2. $\mathcal{O}$ es un dominio de ideales principales, luego dominio de factorización única y es normal.

2. $\Rightarrow$ 1. Sea f un elemento no nulo del ideal maximal $\mathfrak{m}$ de $\mathcal{O}$. $\mathcal{O}/f\mathcal{O}$ es un anillo local de dimensión cero. Por tanto, el ideal maximal $\mathfrak{m}$ en $\mathcal{O}/f\mathcal{O}$ es nilpotente. Es decir, existe

un $n \in \mathbb{N}$ de modo que $\mathfrak{m}^n \subseteq f\mathcal{O}$. Sea $n \in \mathbb{N}$ mínimo verificando $\mathfrak{m}^n \subseteq f\mathcal{O}$. Sea $g \in \mathfrak{m}^{n-1}$ de modo que $g \notin f\mathcal{O}$. Basta probar que $\mathfrak{m} = \frac{f}{g} \cdot \mathcal{O}$, pues tendríamos que $\mathfrak{m}$ es un $\mathcal{O}$-módulo principal y $\mathcal{O}$ un dominio de ideales principales. Se verifica que $\frac{g}{f} \cdot \mathfrak{m} \subseteq \frac{1}{f} \cdot \mathfrak{m}^n \subseteq \mathcal{O}$. Si $\frac{g}{f} \cdot \mathfrak{m} \neq \mathcal{O}$, tendremos que $\frac{g}{f} \cdot \mathfrak{m} \subseteq \mathfrak{m}$. Por tanto, $\frac{g}{f} \cdot$ es un endomorfismo de $\mathfrak{m}$, que ha de satisfacer el correspondiente polinomio característico. Luego $\frac{g}{f}$ es entero sobre $\mathcal{O}$, así pues $\frac{g}{f} \in \mathcal{O}$. Contradicción porque $g \notin f\mathcal{O}$.

□

4. Lema : *El cierre entero conmuta con localizaciones: Sea $A \to B$ un morfismo de anillos y $S \subset A$ un sistema multiplicativo. Sea $\bar{A}$ el cierre entero de A en B y $\overline{A_S}$ el cierre entero de A_S en B_S. Entonces,*

$$\overline{A_S} = (\bar{A})_S$$

En particular, si A es normal, entonces A_S también.

Un anillo íntegro es normal en su cuerpo de fracciones si y solo si es localmente normal.

Demostración. $A_S \to (\bar{A})_S$ es un morfismo entero, luego $(\bar{A})_S \subseteq \overline{A_S}$. Sea $f \in \overline{A_S}$. Existe una relación entera

$$f^n + a_1/s_1 \cdot f^{n-1} + \cdots + a_n/s_n = 0 \qquad \text{con} a_i \in A \text{ y } s_i \in S$$

Sea $s = s_1 \cdots s_n$ (luego $s \in S$). Multiplicando la relación anterior por $t^n s^n$ (para cierto $t \in S$) obtenemos una relación entera de tsf con coeficientes en A, luego $tsf \in \bar{A}$ y $f \in (\bar{A})_S$. Luego, $(\bar{A})_S = \overline{A_S}$.

Por último, $A = \bar{A} \iff A_x = (\bar{A})_x = \overline{A_x}$ para todo $x \in \operatorname{Spec} A$.

□

5. Teorema: *Un anillo noetheriano íntegro A de dimensión de Krull 1 es un dominio de Dedekind si y solo si A es normal.*

Demostración. $A = \bar{A}$ si y solo si $A_x = (\bar{A})_x = \overline{A_x}$ para todo punto cerrado $x \in \operatorname{Spec} A$. Por otra parte, $A_x = \overline{A_x}$ si y solo si A_x es un domino de ideales principales, por el teorema 2.4.3. □

6. Corolario: *Sea A un anillo noetheriano íntegro de dimensión de Krull 1. A es un dominio de ideales principales si y sólo si es un dominio de factorización única.*

Demostración. $\Leftarrow$) A es de Dedekind porque es normal, al ser dominio de factorización única. Dado un ideal primo $\mathfrak{p} \subset A$ no nula, sea $a \in \mathfrak{p}$ irreducible. Como (a) es un ideal primo entonces $\mathfrak{p} = (a)$, es decir, es principal. Entonces, todo ideal es principal por el teorema 2.2.3.

□

7. Corolario: *Sea A un anillo noetheriano de dimensión de Krull 1, íntegro de cuerpo de fracciones Σ, y sea $\bar{A}$ el cierre entero de A en Σ. Se cumple que $y \in \operatorname{Spec} A$ es no singular si y solo si $A_y = (\bar{A})_y$.*

Demostración. El punto $y \in \operatorname{Spec} A$ es no singular si y solo si A_y es d.i.p., y esto ocurre si y solo si $A_y = \overline{(A_y)} = (\bar{A})_y$. □

Sea A un anillo noetheriano íntegro de dimensión de Krull 1 y $\bar{A}$ el cierre entero de A en su cuerpo de fracciones. Si el morfismo $A \hookrightarrow \bar{A}$ es finito, por ejemplo cuando A sea un anillo de números o el anillo de funciones algebraicas de una curva íntegra, entonces $\bar{A}$ es un anillo noetheriano, luego es un dominio de Dedekind.

8. Definición: Sea A un anillo noetheriano íntegro de dimensión de Krull 1. Se dice que $\operatorname{Spec} \bar{A}$ es la desingularización de $\operatorname{Spec} A$ y que $\operatorname{Spec} \bar{A} \to \operatorname{Spec} A$ es el morfismo de desingularización.

2.5. Anillo de números y anillo de funciones algebraicas de una curva

1. Definiciones: Diremos que un anillo íntegro A es un anillo de números si el morfismo $\mathbb{Z} \hookrightarrow A$ es inyectivo y finito. Dada una extensión finita de cuerpos $\mathbb{Q} \hookrightarrow \Sigma$ diremos que Σ es un cuerpo de números y que el cierre entero de $\mathbb{Z}$ en Σ es el anillo de números de Σ. [2]

En el capítulo 3 probaremos que el anillo de números de Σ es un anillo de números.

2. Observación: Si es A un anillo de números entonces $\dim A = \dim \mathbb{Z} = 1$. Además, $A_{\mathbb{Z}\setminus\{0\}}$ es una $\mathbb{Q}$-álgebra finita íntegra, luego es un cuerpo (de números) que ha de coincidir con el cuerpo de fracciones de A.

3. Ejemplos: $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/3}]$, $\mathbb{Z}[\sqrt{-5}]$ y $\mathbb{Z}[\sqrt{2}, i]$ son anillos de números.

4. Ejemplo: El anillo de números $\mathbb{Z}[\sqrt{5}]$ no es localmente principal en el punto y, donde $\mathfrak{m}_y = (2, \sqrt{5}+1)$. El cierre entero de $\mathbb{Z}[\sqrt{5}]$ en $\mathbb{Q}[\sqrt{5}]$ es igual a $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, que es el anillo de números de $\mathbb{Q}[\sqrt{5}]$.

5. Proposición: *Sea K un cuerpo de números. Un elemento $a \in K$ es entero (sobre $\mathbb{Z}$) si y solo si el polinomio característico del endomorfismo lineal $a\cdot\colon K \to K$, $b \mapsto a \cdot b$ es un polinomio con coeficientes enteros*

[2] En la bibliografía se dice que A es un *orden* (del cuerpo de fracciones de A) y al anillo de números de Σ se le denomina anillo de enteros de Σ.

Demostración. $\Leftarrow$) Es evidente.

$\Rightarrow$) Sea $\{a_1,\dots,a_n\}$ una base del $\mathbb{Q}$-espacio vectorial K, con $a = a_1$. Multiplicando cada a_i, para $i \geq 2$, por ciertos números enteros podemos suponer que los polinomios característicos de los a_i son polinomios con coeficientes enteros, luego podemos suponer que la base está formada por elementos enteros. $A = \mathbb{Z}[a_1,\dots,a_n]$ es un anillo de números de K y es un $\mathbb{Z}$-módulo libre de rango n. Consideremos una base del $\mathbb{Z}$-módulo A (que es una base del $\mathbb{Q}$-espacio vectorial K). En esta base la matriz del endomorfismo $a\cdot\colon K \to K$ es una matriz con coeficientes enteros, luego el polinomio característico de $a\cdot$ es un polinomio con coeficientes enteros.

□

6. Ejemplo: Probemos que $\mathbb{Z}[\sqrt{-5}]$ es un anillo de Dedekind. Calculemos los elementos $a + b\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ enteros sobre $\mathbb{Z}$. La matriz de $(a + b\sqrt{-5})\cdot\colon \mathbb{Q}[\sqrt{-5}] \to \mathbb{Q}[\sqrt{-5}]$ en la base $\{1, \sqrt{-5}\}$ es igual a

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}$$

y su polinomio característico es igual a $x^2 - 2ax + (5b^2 + a^2)$, luego $2a, 5b^2 + a^2 \in \mathbb{Z}$. Si a es entero, entonces b es es entero. Si a no es entero, entonces $a = \frac{n}{2}$ con n impar, luego $b = \frac{m}{2}$ con m impar y $5m^2 + n^2 = \dot{4}$, luego $0 = \overline{5m^2 + n^2} = \overline{1 \cdot 1 + 1} = \bar{2}$ en $\mathbb{Z}/4\mathbb{Z}$, y hemos llegado a contradicción. En conclusión, $\mathbb{Z}[\sqrt{-5}] = \overline{\mathbb{Z}[\sqrt{-5}]}$ y es de Dedekind.

7. Definición: Diremos que $\operatorname{Spec} A$ es una curva íntegra afín si A es una k-álgebra de tipo finito íntegra y de dimensión de Krull 1. Diremos que A es el anillo de funciones algebraicas de $\operatorname{Spec} A$.

8. Ejemplos:

1. La recta afín $\mathbb{A}^1 = \operatorname{Spec} k[x]$.
2. La circunferencia $S^1 = \operatorname{Spec} k[x,y]/(x^2 + y^2 - 1)$.
3. El nodo $\operatorname{Spec} k[x,y]/(y^2 - x^2 + x^3)$.
4. La cúspide $\operatorname{Spec} k[x,y]/(y^2 - x^3)$.
5. La cuártica espacial $\operatorname{Spec} \mathbb{C}[x,y,z]/(1 + x^2 + y^2 + z^2, 2 + x^2 - y^2)$.

En el capítulo 3, probaremos que el morfismo de desingularización $A \hookrightarrow \bar{A}$ es un morfismo finito, luego $\operatorname{Spec} \bar{A}$ es una curva algebraica (sin puntos singulares).

Sea $\operatorname{Spec} A$ es una curva íntegra y $\Sigma = A_{A\setminus\{0\}}$ el cuerpo de fracciones de A. Consideremos un morfismo $k[x] \hookrightarrow A$ finito inyectivo. $A_{k[x]\setminus\{0\}}$ es una $k(x)$-álgebra finita íntegra, luego es un cuerpo que ha de coincidir con el cuerpo de fracciones Σ de A. Luego, $k(x) \hookrightarrow \Sigma$ es una extensión de cuerpos finita.[3]

[3] Se dice que Σ es una k-extensión de cuerpos de tipo finito de grado de trascendencia 1. Si $y \in \Sigma$ es un elemento k-trascendente, existe un polinomio $p(x_1,x_2) \in k[x_1,x_2]$, tal que $p(x,y) = 0$. Luego el morfismo, $k(y) \to k(x,y)$ es finito y por tanto la composición de morfismos $k(y) \hookrightarrow k(x,y) \hookrightarrow \Sigma$ es un morfismo finito.

9. Sea A un anillo de números o el anillo de funciones algebraicas de una curva algebraica íntegra. Por la proposición 1.8.26,

$$\{\text{Puntos singulares de Spec}\,A\} \overset{2.4.7}{=} \{x \in \operatorname{Spec} A : (\bar{A}/A)_x = 0\} = \operatorname{Sop}(\bar{A}/A)$$

es un cerrado de $\operatorname{Spec} A$, que no es $\operatorname{Spec} A$ porque $(\bar{A}/A)_g = 0$, donde $\mathfrak{p}_g = (0)$. Por tanto, el número de puntos singulares de $\operatorname{Spec} A$ es finito.

2.6. Valoraciones

1. Definición: Sea Σ un cuerpo y $\Sigma^* = \Sigma \setminus \{0\}$. Una valoración real de Σ es una aplicación $v : \Sigma^* \to \mathbb{R}$ que cumple

1. $v(fg) = v(f) + v(g)$, para todo $f, g \in \Sigma^*$.
2. $v(f+g) \geq \min\{v(f), v(g)\}$, para todo $f, g \in \Sigma^*$.

Si $\operatorname{Im} v = \{0\}$ se dice que v es trivial. Si $\operatorname{Im} v = \mathbb{Z}$, se dice que v es una valoración discreta. Seguiremos la convención $v(0) = \infty$.

Observemos que $v(1) = v(1 \cdot 1) = v(1) + v(1)$, luego $v(1) = 0$. Por tanto, $0 = v(1) = v(f \cdot f^{-1}) = v(f) + v(f^{-1})$, luego $v(f^{-1}) = -v(f)$.

2. Ejercicio: Sea A un anillo íntegro y $v : A \setminus \{0\} \to \mathbb{R}$ una aplicación que cumple 1. y 2., y sea $\Sigma = A_{A \setminus \{0\}}$. Prueba que la aplicación $\Sigma^* \to \mathbb{R}$, $\frac{a}{b} \mapsto v(a) - v(b)$, está bien definida y es una valoración real de Σ.

3. Valoración $\mathfrak{p}$-ádica: Sea A un anillo íntegro de cuerpo de fracciones Σ y $\mathfrak{p} \subset A$ un ideal. Supongamos que $\cap_n \mathfrak{p}^n = 0$ y que para toda $f, g \in A$ se cumple que si $f \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$ y $g \in \mathfrak{p}^m \setminus \mathfrak{p}^{m+1}$ entonces $f \cdot g \in \mathfrak{p}^{n+m} \setminus \mathfrak{p}^{n+m+1}$. Para cada $f \in A$ no nula, denotemos $v_{\mathfrak{p}}(f)$ al máximo número natural n tal que $f \in \mathfrak{p}^n$. Es fácil ver que la aplicación

$$\begin{aligned} v_{\mathfrak{p}} : \Sigma^* &\to \mathbb{Z} \\ f/g &\mapsto v_{\mathfrak{p}}(f/g) = v_{\mathfrak{p}}(f) - v_{\mathfrak{p}}(g) \end{aligned}$$

está bien definida y es una valoración discreta de Σ.

Se dice que $v_{\mathfrak{p}}$ es la valoración $\mathfrak{p}$-ádica. Si denotamos $\mathfrak{p} = \mathfrak{p}_x$ denotaremos $v_{\mathfrak{p}} = v_x$.

Sea $\mathcal{O}$ un anillo local noetheriano íntegro de ideal maximal $\mathfrak{m} = (t)$, $t \neq 0$. Entonces, dada $f \in \mathcal{O}$ tendremos que $f = t^n \cdot u$, con u invertible y $v_{\mathfrak{m}}(f) = n$ y es inmediato comprobar que $\mathcal{O} = \{f \in \Sigma \mid v_{\mathfrak{m}}(f) \geq 0\}$.

Supongamos que A es un anillo de Dedekind, sea $f \in A$ no nula y $(f)_0 = \{x_1, \ldots, x_r\}$, entonces

$$(f) = \mathfrak{p}_{x_1}^{v_{x_1}(f)} \cdots \mathfrak{p}_{x_r}^{v_{x_r}(f)}.$$

En efecto, $(f) = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}$ y $f \cdot A_{x_i} = \mathfrak{p}_{x_i}^{n_i} \cdot A_{x_i}$, luego $f \in \mathfrak{p}_{x_i}^{n_i} \setminus \mathfrak{p}_{x_i}^{n_i+1}$ y $v_{x_i}(f) = n_i$.

4. Ejercicio: Sea $\mathfrak{m}_5 = 5\cdot\mathbb{Z} \subset \mathbb{Z}$ y $v_5 : \mathbb{Q} \to \mathbb{Z}$ la valoración $\mathfrak{m}_5$-ádica. Calcula $v_5(120/25)$.

5. Ejercicio: Sea $\mathfrak{m}_{(0,0)} = (x,y) \subset k[x,y]$ y $v_{(0,0)} : k(x,y) \to \mathbb{Z}$ la valoración $\mathfrak{m}_{(0,0)}$-ádica. Calcula $v_{(0,0)}(\frac{y-x^2}{y^2-x^2+x^3})$.

6. Proposición: *Sea Σ un cuerpo y $v : \Sigma^* \to \mathbb{R}$ una valoración real. Entonces,*

$$\mathcal{O}_v := \{f \in \Sigma : v(f) \geq 0\}.$$

es un anillo local de ideal maximal $\mathfrak{p}_v := \{f \in \Sigma : v(f) > 0\}$, cuyo conjunto de invertibles es $\mathcal{O}_v^* := \{f \in K : v(f) = 0\}$ y de cuerpo de fracciones Σ.

Demostración. Es fácil comprobar que $\mathcal{O}_v$ es un anillo y que $\mathfrak{p}_v \subset \mathcal{O}_v$ es un ideal.

Para toda $f \in \Sigma$, o bien $f \in \mathcal{O}_v$ o bien $f^{-1} \in \mathcal{O}_v$ (pues $v(f) \geq 0$ ó $v(f^{-1}) = -v(f) \geq 0$). Por tanto, el cuerpo de fracciones de $\mathcal{O}_v$ es Σ.

Un elemento $f \in \Sigma$ es un invertible de $\mathcal{O}_v$ si y solo si $v(f) = 0$: $f \in \mathcal{O}_v$ es invertible $\iff f, f^{-1} \in \mathcal{O}_v \iff v(f), -v(f) = v(f^{-1}) \geq 0 \iff v(f) = 0$.

Como $\mathcal{O}_v = \mathcal{O}_v^* \coprod \mathfrak{p}_v$, entonces $\mathfrak{p}_v$ es el único ideal maximal de $\mathcal{O}_v$.

□

2.6.1. Anillos de valoración

7. Definición: Dada una valoración $v : \Sigma^* \to \mathbb{R}$ diremos que $\mathcal{O}_v$ es un anillo de valoración de Σ y que $\mathfrak{p}_v$ es el ideal de la valoración v. Si v es discreta diremos que $\mathcal{O}_v$ es un anillo de valoración discreta de Σ.

$\mathcal{O}_v = \Sigma$ si y solo si v es trivial. Se dice que Σ es el anillo de valoración trivial.

8. Proposición: *Sea $\mathcal{O}$ un anillo local íntegro (y supongamos que no es cuerpo). Entonces,*

1. *$\mathcal{O}$ es de valoración discreta si y solo si $\mathcal{O}$ es d.i.p.*
2. *$\mathcal{O}$ es de valoración discreta si y solo si es de valoración y es noetheriano.*

Demostración. Supongamos que $\mathcal{O}_v$ es un anillo de valoración discreta. Sea $t \in \mathcal{O}_v$ tal que $v(t) = 1$. Dado $f \in \mathcal{O}_v$, sea $n = v(f) \geq 0$. Entonces, $v(f/t^n) = 0$ y $f/t^n = i$ invertible, luego $f = t^n \cdot i$. Dado un ideal $I \subset \mathcal{O}_v$, se cumple que $I = (t^m)$, donde $m = \text{mín}\{v(f)$, para toda $f \in I\}$. Por tanto, $\mathcal{O}_v$ es d.i.p., luego noetheriano.

Si $\mathcal{O}$ es d.i.p. de ideal maximal $\mathfrak{m}$, entonces $\mathcal{O} = \mathcal{O}_{v_\mathfrak{m}}$, que es de valoración discreta.

Si $\mathcal{O}_v$ es noetheriano entonces todo ideal $I \subset \mathcal{O}_v$ es principal: El ideal $I = (f_1, \ldots, f_n)$ es finito generado. Sea f_i tal que $v(f_i) \leq v(f_j)$ para todo j. Observemos que $v(\frac{f_j}{f_i}) = v(f_j) - v(f_i) \geq 0$, luego $\frac{f_j}{f_i} \in \mathcal{O}_v$, $f_j = f_i \cdot \frac{f_j}{f_i}$ y $I = (f_i)$.

□

9. Teorema: *Tenemos la biyección de conjuntos:*

$$\{\textit{Valoraciones discretas de } \Sigma\} = \{\textit{Anillos de valoración discreta de } \Sigma\}$$

$$v \longmapsto \mathcal{O}_v$$

$$v_{\mathfrak{p}_v} \longmapsfrom \mathcal{O}_v$$

Demostración. Solo tenemos que ver si v es discreta entonces $v = v_{\mathfrak{p}_v}$: Sea $t \in \mathcal{O}_v$ tal que $v(t) = 1$. Dado $f \in \mathcal{O}_v$, tenemos que $v(f) = n \geq 0$ y $v(\frac{f}{t^n}) = 0$, luego $u = \frac{f}{t^n} \in \mathcal{O}_v$ es invertible y $f = t^n \cdot u$. Por tanto, $\mathfrak{p}_v = (t)$ y $f \in \mathfrak{p}_v^n \setminus \mathfrak{p}_v^{n+1}$, luego $v_{\mathfrak{p}_v}(f) = n = v(f)$. □

10. Definición: Diremos que dos valoraciones $v, v' \colon \Sigma \setminus \{0\} \to \mathbb{R}$ son equivalentes si existe $\alpha > 0$ de modo que $v' = \alpha \cdot v$.

11. Proposición: *Sea Σ un cuerpo y $v, v' \colon \Sigma^* \to \mathbb{R}$ dos valoraciones reales. Entonces, $\mathcal{O}_v = \mathcal{O}_{v'}$ si y solo si v y v' son equivalentes.*

Demostración. Obviamente, si $v' = \alpha \cdot v$, entonces $\mathcal{O}_v = \mathcal{O}_{v'}$.

Supongamos que $\mathcal{O}_v = \mathcal{O}_{v'}$. Fijemos $f \in \mathfrak{p}_v = \mathfrak{p}_{v'}$ no nulo (el caso $\mathfrak{p}_v = 0$, es decir, $\mathcal{O}_v = \Sigma$ implica $v = 0 = v'$). Podemos suponer, multiplicando v por un α, que $v(f) = v'(f)$. Ahora, dado $f' \in \Sigma^*$, sea $C := \{\frac{n}{m} \in \mathbb{Q} \colon v(f') - \frac{n}{m} v(f) \geq 0\}$. Entonces,

$$C = \{\frac{n}{m} \in \mathbb{Q} \colon mv(f') - nv(f) \geq 0\} = \{\frac{n}{m} \in \mathbb{Q} \colon v(f'^m/f^n) \geq 0\} = \{\frac{n}{m} \in \mathbb{Q} \colon f'^m/f^n \in \mathcal{O}_v\}.$$

Sea $C' := \{\frac{n}{m} \in \mathbb{Q} \colon v'(f') - \frac{n}{m} v'(f) \geq 0\}$, igualmente $C' = \{\frac{n}{m} \in \mathbb{Q} \colon f'^m/f^n \in \mathcal{O}_{v'}\}$. Luego, $C = C'$. Por tanto,

$$v(f') = (\text{Supremo de } C) \cdot v(f) = (\text{Supremo de } C') \cdot v'(f) = v'(f'),$$

luego $v = v'$. □

2.6.2. Anillos de valoración y cierre entero

12. Proposición: *Los anillos de valoración son normales.*

Demostración. Sea $\mathcal{O}_v$ un anillo de valoración de Σ y $a \in \Sigma$ entero sobre $\mathcal{O}_v$. Existen $c_i \in \mathcal{O}_v$ tales que $a^n + c_1 a^{n-1} + \cdots + c_n = 0$. Entonces $a^n = -(c_1 a^{n-1} + \cdots + c_n)$, luego $nv(a) = v(a^n) \geq \text{ínf}\{v(c_1 a^{n-1}), \ldots, v(c_n)\} \geq \text{ínf}\{(n-1)v(a), \ldots, 0\}$, luego $v(a) \geq 0$ y $a \in \mathcal{O}_v$. □

13. Lema: *Sea A un anillo íntegro (luego A está incluido en su cuerpo de fracciones Σ y al localizar por un sistema multiplicativo también). Entonces,*

$$A = \bigcap_{x \in \mathrm{Spec}_{max} A} A_x.$$

Demostración. Sea $\frac{a}{b} \in \bigcap_{x \in \mathrm{Spec}_{max} A} A_x$, con $a, b \in A$. Entonces, $aA \subseteq bA$, porque así sucede al localizar en todo punto cerrado de $\mathrm{Spec}\, A$. Por tanto, $\frac{a}{b} \in A$. □

14. Lema: *Sea $\mathcal{O}_v$ un anillo de valoración de Σ y sea $\mathcal{O}$ un subanillo local de Σ, cuyo ideal maximal denotamos $\mathfrak{m}$. Si $\mathcal{O}_v \subseteq \mathcal{O}$ y $\mathfrak{m} \cap \mathcal{O}_v = \mathfrak{p}_v$, es decir, "$\mathcal{O}$ domina a $\mathcal{O}_v$", entonces $\mathcal{O} = \mathcal{O}_v$.*

Demostración. Sea $f \in \mathcal{O} \setminus \mathcal{O}_v$, entonces $v(f) < 0$. Por tanto, $v(f^{-1}) > 0$, luego $f^{-1} \in \mathfrak{p}_v$. Por tanto, $f^{-1} \in \mathfrak{m}$ y $f \in \mathcal{O}$, lo cual es contradictorio. □

15. Teorema: *Sea K un cuerpo de números y A el anillo de números de K. Se cumple que*

1. *Todos los anillos de valoración de K son discretos (salvo el trivial).*
2. $\mathrm{Spec}\, A \setminus \{(0)\} = \{$*Valoraciones discretas de K*$\}$
   $$x \mapsto v_x$$
3. *A es igual a la intersección de todos los anillos de valoración de K, es decir,*
   $$A = \bigcap_{\{v \,:\, K^* \to \mathbb{Z}\}} \mathcal{O}_v$$

Demostración. Sea $\mathcal{O}_v$ un anillo de valoración de K. Todo elemento de A es entero sobre $\mathbb{Z}$, luego entero sobre $\mathcal{O}_v$, luego pertenece a $\mathcal{O}_v$ por la proposición 2.6.12. Por tanto, $A \subseteq \mathcal{O}_v$. Sea $\mathfrak{p}_x := \mathfrak{p}_v \cap A$. Entonces, $A_x \subseteq \mathcal{O}_v$, A_x es de valoración y $\mathcal{O}_v$ domina a A_x, luego $\mathcal{O}_v = A_x$ por el lema 2.6.14. Por tanto, $\mathcal{O}_v$ es un anillo de valoración discreta y además si v es discreta entonces $v = v_x$.

Por último, por el lema 2.6.13, $A = \cap_{x \in \mathrm{Spec}\, A} A_x = \bigcap_{\{v \,:\, K^* \to \mathbb{Z}\}} \mathcal{O}_v$.

□

16. Ejemplo: $\mathrm{Spec}\, \mathbb{Z} = \{$Conjunto de anillos de valoración de $\mathbb{Q}\}$.

17. Ejercicio: Calcula todas las valoraciones reales de $\mathbb{Q}(\sqrt{5})$.

18. Teorema: *Sea A el anillo de una k-curva íntegra y Σ el cuerpo de fracciones de A y $\bar{A}$ el cierre entero de A en Σ. Entonces se cumple*

1. *Todos los anillos de valoración de Σ, que contienen a k, son discretos (salvo el trivial).*

2. $\operatorname{Spec}\bar{A}\setminus\{(0)\} = \{$*Valoraciones discretas* $v\colon \Sigma \to \mathbb{Z}$ *tales que* $v(A)\subseteq\mathbb{N}\}$, $x \mapsto v_x$.

3. $\bar{A}$ *es igual a la intersección de todos los anillos de valoración de* Σ *que contienen a* A*, es decir,*

$$\bar{A} = \bigcap_{\left\{v\colon \Sigma^*\to\mathbb{Z} \atop v(A)\subseteq\mathbb{N}\right\}} \mathcal{O}_v$$

Demostración. 2. Sea $\mathcal{O}_v$ un anillo de valoración de Σ que contenga a A. $\mathcal{O}_v$ es normal. Todo elemento de Σ entero sobre A, es entero sobre $\mathcal{O}_v$, luego pertenece a $\mathcal{O}_v$. Por tanto, $\bar{A}\subseteq\mathcal{O}_v$. Sea $\mathfrak{p}_x = \mathfrak{p}_v\cap\bar{A}$. Entonces, $\bar{A}_x\subseteq\mathcal{O}_v$. $\bar{A}_x$ es un anillo de valoración discreta. Por el lema anterior $\bar{A}_x = \mathcal{O}_v$. Por tanto, $\mathcal{O}_v$ es un anillo de valoración discreta y si v es discreta $v = v_x$.

3. $\bar{A} = \bigcap_{x\in\operatorname{Spec}\bar{A}} \bar{A}_x = \bigcap_{\left\{v\colon \bar{\Sigma}^*\to\mathbb{Z} \atop v(A)\subseteq\mathbb{N}\right\}} \mathcal{O}_v$.

1. Sea $\mathcal{O}_v$ un anillo de valoración. Sea $x\in\Sigma$ trascendente. Tomando x^{-1} en vez de x, si es necesario, podemos suponer que $x\in\mathcal{O}_v$. Por tanto, $\mathcal{O}_v$ contiene a $k[x]$, luego contiene al cierre entero, B, de $k[x]$. Por el punto 2., $\mathcal{O}_v = B_y$, para cierto punto cerrado $y\in\operatorname{Spec}B$, y concluimos que $\mathcal{O}_v$ es un anillo de valoración discreta.

□

19. Corolario: *Sea* A *el anillo de una curva íntegra y* Σ *el cuerpo de fracciones de* A*. Sea* $\Sigma\hookrightarrow\Sigma'$ *una extensión finita de cuerpos y* A' *el cierre entero de* A *en* Σ'*. Entonces se cumple*

1. $\operatorname{Spec}A'\setminus\{(0)\} = \{$*Valoraciones discretas* $v\colon \Sigma' \to \mathbb{Z}$ *tales* $v(A)\subseteq\mathbb{N}\}$, $x\mapsto v_x$.

2. A' *es igual a la intersección de todos los anillos de valoración de* Σ' *que contienen a* A*, es decir,*

$$A' = \bigcap_{\left\{v\colon \bar{\Sigma}^*\to\mathbb{Z} \atop v(A)\subseteq\mathbb{N}\right\}} \mathcal{O}_v$$

Demostración. Observemos solo que un anillo de valoración de Σ' contiene a A' si y solo si contiene a A, y que el cierre entero de A' en Σ' es A'. □

2.6.3. Variedad de Riemann

Sea K una k-extensión de cuerpos de tipo finito de grado de trascendencia 1, es decir, K es una $k(x)$-extensión finita de cuerpos. Supongamos por sencillez que k es un cuerpo de característica cero.

20. Definición: Diremos que el conjunto C de todos los anillos de valoración de K, triviales sobre k (es decir, que contienen a k) es la variedad de Riemann asociada a K.

21. Dotemos a C de estructura de espacio topológico: sus cerrados propios son los conjuntos finitos de anillos de valoración, distintos del anillo de valoración trivial.

Sea $U = \{v \in C : v(x) \geq 0\}$ y $U' = \{v \in C : v(\frac{1}{x}) \geq 0\}$. Obviamente, $C = U \cup U'$. Sea A el cierre entero de $k[x]$ en K. Por el teorema 2.6.19, tenemos la igualdad $\operatorname{Spec} A = U$, $y \mapsto A_y$. Igualmente, si A' es el cierre entero de $k[1/x]$ en K, se cumple que $\operatorname{Spec} A' = U'$. U' es un abierto de C, ya que

$$C \setminus U' = \{v \in C : v(1/x) < 0\} = \{v \in C : v(x) > 0\} = \operatorname{Spec} A/(x)$$

que es un número finito de puntos. Igualmente, U es un abierto de C. Además,

$$U \cap U' = \{v \in U : v(x) = 0\} = \operatorname{Spec} A \setminus (x)_0 = \operatorname{Spec} A_x = \operatorname{Spec} A'_{1/x}$$

En conclusión, C se recubre por dos abiertos U, U', cada uno de ellos es una curva afín íntegra no singular[4], y $C \setminus U$ y $C \setminus U'$ son conjuntos finitos.

22. Ejemplo: La variedad de Riemann asociada a $k(x)$ se denota $\mathbb{P}^1$. Observemos que $\mathbb{P}^1 = \operatorname{Spec} k[x] \cup \operatorname{Spec} k[\frac{1}{x}]$. Sea $\infty \in \operatorname{Spec} k[\frac{1}{x}]$ el ideal primo $\mathfrak{m}_\infty = (\frac{1}{x}) \subset k[\frac{1}{x}]$, entonces es fácil de probar que

$$\mathbb{P}^1 = \operatorname{Spec} k[x] \coprod \{\infty\}.$$

23. Ejercicio: Sea $\Sigma = \mathbb{Q}(x)$ y $\mathfrak{p}_0 := (x) \subset \mathbb{Q}[x]$, $\mathfrak{p}_i := (x^2 + 1) \subset \mathbb{Q}[x]$ y $\mathfrak{p}_\infty := (1/x) \subset \mathbb{Q}[1/x]$ y consideremos las respectivas valoraciones ádicas $v = v_0$, v_i y v_∞. Calcula $v(\frac{x^2+1}{x})$ en los tres casos.

24. Todo morfismo $K \to L$ de k-extensiones, entre extensiones de tipo finito de grado de trascendencia 1, induce el morfismo entre las variedades de Riemann asociadas, definido por

$$\pi : C_L \to C_K,\ \mathcal{O}_w \mapsto \mathcal{O}_w \cap K.$$

Dado $x \in K$ trascendente, sean A y B el cierre entero de $k[x]$ en K y L respectivamente, y $U := \operatorname{Spec} A$ y $V := \operatorname{Spec} B$. Entonces, $\pi^{-1}(U) = V$ y el morfismo $\pi : V \to U$ es el morfismo inducido por el morfismo de anillos $A \to B$, que es un morfismo finito.

Dado $f \in K$ trascendente, consideremos la inclusión $k(x) \hookrightarrow K$, $x \mapsto f$. Entonces, tenemos un morfismo entre las variedades de Riemann

$$\tilde{f} : C_K \to \mathbb{P}^1.$$

Sea A el cierre entero de $k[f]$, tenemos el morfismo $k[x] \to A$, $x \mapsto f$ y $\tilde{f}^{-1}(\operatorname{Spec} k[x]) = \operatorname{Spec} A$. Sea $p \in \operatorname{Spec} A$ y consideremos la composición $k[x] \to A \to A/\mathfrak{m}_p$, $x \mapsto f \mapsto f(p)$. El núcleo de la composición es $\mathfrak{m}_{\tilde{f}(p)} = (x - f(p)) = \mathfrak{m}_{f(p)}$, por tanto $\tilde{f}(p) = f(p)$.

[4] Por el teorema 3.2.7.

25. Variedad proyectiva: Consideremos el espacio proyectivo topológico

$$\mathbb{P}^n(\mathbb{R}) = \mathbb{R}^{n+1}\setminus\{0\}/\sim \qquad (e \sim e' \iff e = \lambda\cdot e').$$

Dado un polinomio homogéneo $p(x_0,\dots,x_n)\in\mathbb{R}[x_0,\dots,x_n]$, denotaremos

$$(p(x_0,\dots,x_n))_0^h = \{[(\alpha_0,\dots,\alpha_n)]\in\mathbb{P}^n(\mathbb{R})\colon p(\alpha_0,\dots,\alpha_n)=0\}$$

que es un cerrado de $\mathbb{P}^n(\mathbb{R})$, y sea $U^h_{p(x_0,\dots,x_n)} := \mathbb{P}^n(\mathbb{R}) - (p(x_0,\dots,x_n))_0^h$ que es un abierto de $\mathbb{P}^n(\mathbb{R})$. Obviamente, $\mathbb{P}^n(\mathbb{R}) = \cup_{i=0}^n U^h_{x_i}$ y

$$\begin{array}{rcl} U^h_{x_i} & = & \mathbb{R}^n \\ [(\alpha_0,\dots,\alpha_n)] & \longmapsto & (\frac{\alpha_0}{\alpha_i},\dots,\widehat{\frac{\alpha_i}{\alpha_i}},\dots\frac{\alpha_n}{\alpha_i}) \\ [(\lambda_1,\dots,\lambda_i,1,\lambda_{i+1},\dots,\lambda_n)] & \longmapsfrom & (\lambda_1,\dots,\lambda_n) \end{array}$$

Vía esta identificación, es fácil ver que

$$(p(x_0,\dots,x_n))_0^h \cap U^h_{x_i} = (p(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}))_0.$$

En Geometría Algebraica[5] se define

$$\mathbb{P}^n(k) := \bigcup_{i=0}^n \operatorname{Spec} k[\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}].^{6}$$

Dado un ideal $I = (p_1(x_0,\dots,x_n),\dots,p_r(x_0,\dots,x_n)) \subseteq k[x_0,\dots,x_n]$ generado por polinomios homogéneos, se define $(I)_0^h$ como sigue

$$\begin{aligned}(I)_0^h \cap U^h_{x_i} &:= (p_1(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}),\dots,p_r(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}))_0 \\ &= \operatorname{Spec}\ k[\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}]\Big/(p_1(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}),\dots,p_r(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}))\end{aligned}$$

Se dice que $X = (I)_0^h$ es una variedad proyectiva. Se dice que X es íntegra si es un espacio topológico irreducible y $X\cap U^h_{x_i}$ es una variedad afín íntegra para todo i. Se llama dimensión de X al máximo de las dimensiones de $X\cap U^h_{x_i}$. Se dice que X es una curva proyectiva si es de dimensión 1.

Si denotamos $\xi_i = \bar{x}_i \in k[x_0,\dots,x_n]/I$, entonces $k[x_0,\dots,x_n]/I = k[\xi_0,\dots,\xi_n]$ y

$$U^h_{\xi_i} := X\cap U^h_{x_i} = \operatorname{Spec} k[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}].$$

[5] Véase también la sección 3.4.

[6] Definimos $\operatorname{Spec} k[\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}]\cap\operatorname{Spec} k[\frac{x_0}{x_j},\dots,\frac{x_n}{x_j}] := \operatorname{Spec} k[\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}]_{\frac{x_j}{x_i}} = \operatorname{Spec} k[\frac{x_0}{x_j},\dots,\frac{x_n}{x_j}]_{\frac{x_i}{x_j}}$.

26. Sea X una variedad proyectiva íntegra. Se dice que $\Sigma := k(\xi_1/\xi_0, \ldots, \xi_n/\xi_0)$ es"el cuerpo de funciones de X" (que no depende de la ordenación de los ξ_i). Dado un punto $x \in U^h_{\xi_i} = \operatorname{Spec} k[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$, denotaremos $\mathcal{O}_{X,x} := k[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]_x \subseteq \Sigma$ (que no depende del abierto $U^h_{\xi_i}$ que contiene a x, considerado). Dados $x \in U^h_{\xi_i}$, $x' \in U^h_{\xi_j}$ distintos, se cumple que x y x' están ambos a la vez en uno de los abiertos afines $U^h_{\xi_i}, U^h_{\xi_j}, U^h_{\xi_i+\xi_j}$, luego $\mathcal{O}_{X,x} \neq \mathcal{O}_{X,x'}$.

Dado un anillo de valoración $\mathcal{O}_v$ de Σ, trivial sobre k, existe un único punto $x \in X$, tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{X,x}$: Sea ξ_j/ξ_i tal que $v(\xi_j/\xi_i)$ sea máximo entre todos los i, j. Observemos que $v(\xi_k/\xi_i) \geq 0$, porque si $v(\xi_k/\xi_i) < 0$, entonces $v(\xi_j/\xi_k) = v(\xi_i/\xi_k \cdot \xi_j/\xi_i) = v(\xi_i/\xi_k) + v(\xi_i/\xi_j) > v(\xi_i/\xi_j)$, lo cual es contradictorio. Por tanto, $k[\xi_0/\xi_i, \ldots, \xi_n/\xi_i] \subset \mathcal{O}_v$. Si $\mathfrak{p}_x := \mathfrak{p}_v \cap k[\xi_0/\xi_i, \ldots, \xi_n/\xi_i]$, tenemos que $\mathcal{O}_v$ domina a $\mathcal{O}_{X,x}$. Sea otro $x' \in X$ tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{X,x'}$. Podemos suponer, por cambio de coordenadas, que $x, x' \in U^h_{\xi_0}$. Entonces, $\mathfrak{p}_{x'} := \mathfrak{p}_v \cap k[\xi_1/\xi_0, \ldots, \xi_n/\xi_0] = \mathfrak{p}_x$ y $x' = x$.

27. Desingularización de una curva proyectiva: Supongamos ahora además que X es una curva. Sea V la variedad de Riemann de Σ. Consideremos el morfismo natural $\pi\colon V \to X$, donde $\pi(v)$ es tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{C,\pi(v)}$. Consideramos el abierto

$$U^h_{\xi_0} = \operatorname{Spec} k[\xi_1/\xi_0, \ldots, \xi_n/\xi_0]$$

y un morfismo finito $k[x] \hookrightarrow k[\xi_1/\xi_0, \ldots, \xi_n/\xi_0]$. Sea A el cierre entero de $k[x]$ en Σ (que es el cierre entero de $k[\xi_1/\xi_0, \ldots, \xi_n/\xi_0]$ en Σ) y $U = \operatorname{Spec} A$. Entonces, $\pi^{-1}(U^h_{\xi_0}) = U$ y el morfismo inducido por la inclusión $k[\xi_1/\xi_0, \ldots, \xi_n/\xi_0] \hookrightarrow A$ es el morfismo $\pi\colon U \to U^h_{\xi_0}$.

Se dice que V es la desingularización de X.

28. Teorema: *Si C es una curva proyectiva íntegra no singular en todo punto, entonces la variedad de Riemann del cuerpo de funciones de C es isomorfa a C*

Se puede probar el recíproco: "las variedades de Riemann son curvas proyectivas no singulares en todo punto."

29. Ejemplo: La variedad de Riemann asociada al cuerpo de fracciones del anillo $\mathbb{C}[x, y]/(y^2 - x(x-1)(x-2))$ es igual a la curva proyectiva plana de ecuaciones afines $y^2 - x(x-1)(x-2) = 0$.

2.7. Apéndice: Morfismos finitos

Sean A y B anillos. Dado un morfismo de anillos $A \to B$ se dice que B es una A-álgebra. Usualmente seguiremos la notación $A \to B$, $a \mapsto a$.

1. Ejemplo: Todo anillo es una $\mathbb{Z}$-álgebra de modo único.

2. Ejemplo: $\mathbb{R}[x, y]$ es una $\mathbb{R}$-álgebra de modo natural.

3. Definición: Un morfismo de anillos $f: A \to B$ se dice que es finito si B es un A-módulo finito generado, con la estructura natural de A-módulo que define f en B ($a \cdot b := f(a) \cdot b$). En este caso, también se dice que B es una A-álgebra finita. Si $A \to B$ es un morfismo finito, diremos que el morfismo inducido $\operatorname{Spec} B \to \operatorname{Spec} A$ es finito.

4. Ejemplo: El morfismo $A \to A[x]/(x^n + a_1 x^{n-1} + \cdots + a_n)$ es un morfismo finito, porque $\{\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}\}$ es una base del A-módulo $A[x]/(x^n + a_1 x^{n-1} + \cdots + a_n)$.

5. Ejemplo: El morfismo $\operatorname{Spec} k[x,y]/(y^2 - x^2 + x^3) \to \operatorname{Spec} k[x]$ definido por $(\alpha, \beta) \mapsto \alpha$ es un morfismo finito.

6. Ejemplo: Si α es una raíz de un polinomio con coeficientes en $\mathbb{Q}$, entonces $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ es un morfismo finito.

7. Definición: Sea $A \to B$ un morfismo de anillos. Se dice que $b \in B$ es entero sobre A si verifica una relación del tipo

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0, \qquad \text{con} \, a_i \in A$$

El teorema de Hamilton-Cayley que conocemos para los endomorfismos de espacios vectoriales, también es cierto para los endomorfismos de módulos. Con precisión, sea $M = \langle m_1, \ldots, m_r \rangle$, $f: M \to M$, $f(m_i) = \sum_j a_{ij} m_j$ un endomorfismo de A-módulos; si $p_c(x)$ es el polinomio característico de la matriz (a_{ij}), entonces $p_c(f) = 0$. En efecto, consideremos la matriz $B = (x_{ij})$ de coeficientes variables y el polinomio característico $p_c(x)$ de esta matriz. $p_c(x)$ es un polinomio con coeficientes en $\mathbb{Z}[x_{ij}] \subset \mathbb{Q}(x_{ij})$. Por el teorema de Hamilton-Cayley $p_c(B) = 0$. Por tanto, especializando a $x_{ij} = a_{ij}$, tendremos que $p_c(f) = 0$.

8. Proposición: *Sean $f: A \to B$ un morfismo de anillos y $b \in B$. Denotemos $A[b] = \{p(b) \in B, \text{para } p(x) \in A[x]\}$. El morfismo $A \to A[b]$ es finito $\Leftrightarrow$ b es entero sobre A.*

Demostración. $\Rightarrow$) Consideremos el endomorfismo de A-módulos

$$\begin{array}{ccc} A[b] & \xrightarrow{\cdot b} & A[b] \\ p(b) & \longmapsto & p(b) \cdot b \end{array}$$

Si (a_{ij}) es una matriz asociada a $\cdot b$ en un sistema generador de $A[b]$, entonces el polinomio característico de (a_{ij}), $p_c(x)$ anula a $\cdot b$, luego $0 = p_c(b\cdot)(1) = p_c(b)$ y b es entero sobre A.

$\Leftarrow$) Sea $p(x)$ un polinomio mónico con coeficientes en A que anula a b. Entonces $A[b]$ es un cociente de $A[x]/(p(x))$. Como $A[x]/(p(x))$ es un A-módulo finito generado se concluye. □

9. Observación: Para la demostración de $\Rightarrow$) solo es necesario suponer que $A[b]$ está incluido en una A-álgebra finita.

10. Proposición: *La composición de morfismos finitos es finito.*

Demostración. Sean $A \overset{\text{finito}}{\longrightarrow} B \overset{\text{finito}}{\longrightarrow} C$. Es decir, $B = Ab_1 + \cdots + Ab_n$ y $C = Bc_1 + \cdots + Bc_m$. Luego,

$$C = (Ab_1 + \cdots + Ab_n)c_1 + \cdots + (Ab_1 + \cdots + Ab_n)c_m = \sum_{i=1,j=1}^{n,m} Ab_i c_j$$

En conclusión, $A \to C$ es un morfismo finito.

□

11. Ejemplo: $\mathbb{Z} \to \mathbb{Z}[\sqrt{2}, i]$ es un morfismo finito.

12. Proposición: *Sea $f : A \to B$ un morfismo de anillos. El conjunto de elementos de B enteros sobre A forman una A-subálgebra de B.*

Demostración. Sean $b_1, b_2 \in B$ enteros sobre A. Tenemos que $A \to A[b_1]$ es un morfismo finito, y $A[b_1] \to A[b_1, b_2]$ es un morfismo finito porque si b_2 verifica una relación entera con coeficientes en A, en particular la verifica con coeficientes en $A[b_1]$. Por tanto, por la proposición 2.7.10, $A \to A[b_1, b_2]$ es un morfismo finito. Luego, por la observación anterior, todo elemento $p(b_1, b_2) \in A[b_1, b_2] \subseteq B$, con $p(x, y) \in A[x, y]$, es entero sobre A.

□

13. Proposición: *Si $A \to B$ es un morfismo finito y $A \to C$ un morfismo de anillos, entonces $C = A \otimes_A C \to B \otimes_A C$ es un morfismo finito. "Los morfismos finitos son estables por cambio de base".*

Demostración. Es inmediata. □

14. Corolario: *Si $A \to B$ es un morfismo finito, entonces $A_S \to B_S$ y $A/I \to B/I \cdot B$ son morfismos finitos*

15. Proposición: *La composición de dos morfismos enteros es entero.*

Demostración. Sean $A \to B$ y $B \to C$ dos morfismos enteros. Dado $c \in C$, existe un polinomio $p(x) = \sum_i b_i x^i \in B[x]$ tal que $p(c) = 0$. Sea $B' := A[b_i]_i$. Los morfismos $A \to B'$ y $B' \to B'[c]$ son finitos. Por tanto, $A \to B'[c]$ es finito y c es entero sobre A. En conclusión, $A \to C$ es un morfismo entero. □

Dejamos que el lector pruebe que el cierre entero de un anillo íntegro en su cuerpo de fracciones es un anillo normal.

16. Ejercicio: Demuestra que $\mathbb{Z}$ es un anillo íntegramente cerrado en $\mathbb{Q}$.

17. Proposición: *Si $f : A \hookrightarrow B$ es un morfismo entero e inyectivo, entonces el morfismo inducido $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo*

Demostración. Supongamos que f es un morfismo finito. Dado $x \in \operatorname{Spec} A$, el morfismo $A_x \to B_x$ es finito e inyectivo. Por Nakayama, $\mathfrak{p}_x B_x \neq B_x$, luego $\operatorname{Spec} B_x/\mathfrak{p}_x B_x \neq \emptyset$. Es decir, la fibra de x es no vacía, luego f^* es epiyectivo.

Ahora ya, si B es entero sobre A, entonces $B_x/\mathfrak{p}_x B_x \neq 0$ porque si $B_x/\mathfrak{p}_x B_x = 0$, es decir, $1 \in \mathfrak{p}_x B_x$, para alguna subálgebra finita B_i se verificará que $1 \in \mathfrak{p}_x B_i$, es decir, $(B_i)_x/\mathfrak{p}_x(B_i)_x = 0$ y llegaremos a contradicción con el párrafo anterior. De nuevo, tenemos que la fibra de x es no vacía y f^* es epiyectivo. □

18. Definición: Llamaremos dimensión de Krull de un anillo A, que denotaremos $\dim A$, al supremo de las longitudes de las cadena de ideales primos de A, o equivalentemente, al supremo de las longitudes de las cadenas de cerrados irreducibles de $\operatorname{Spec} A$. Llamaremos dimensión de $\operatorname{Spec} A$, que denotaremos $\dim \operatorname{Spec} A$, a la dimensión de Krull de A.

19. Ejercicio: Probar que el supremo de las longitudes de las cadenas de cerrados irreducibles de $\operatorname{Spec} A$ es igual a $\dim \operatorname{Spec} A$.

20. Ejercicio: Demuestra que la dimensión de Krull de $\mathbb{Z}$ y $k[x]$ es uno y la de $\mathbb{C}[x, y]$ dos.

21. Lema: *Sea k un cuerpo. Si A es una k-álgebra finita íntegra entonces A es un cuerpo.*

Demostración. Sea $a \in A$ no nulo. El morfismo $A \xrightarrow{a\cdot} A$, $b \mapsto a \cdot b$ es una aplicación k-lineal inyectiva porque A es íntegro. Por dimensiones ha de ser epiyectiva. Es decir, $a\cdot$ es un isomorfismo lineal, luego a es invertible y A es cuerpo.

□

22. Lema: *Sea k un cuerpo y A una k-álgebra finita. Entonces, todo ideal primo de A es maximal y $|\operatorname{Spec} A| < \infty$.*

Demostración. Sea $\mathfrak{p} \subset A$, un ideal primo. $A/\mathfrak{p}$ es una k-álgebra finita íntegra, luego es cuerpo y $\mathfrak{p}$ es un ideal maximal.

Sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ ideales maximales. Las inclusiones $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subset \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \subset \cdots \subset \mathfrak{m}_1 \cdot \mathfrak{m}_2 \subset \mathfrak{m}_1 \subset A$ son estrictas porque $(\mathfrak{m}_1 \cdots \mathfrak{m}_i)_0 = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_i\}$. Observemos que si la dimensión del k-espacio vectorial A es m, entonces en A no pueden existir cadenas de inclusiones estrictas de más de $m+1$ subespacios vectoriales . Entonces $n \leq m$. Luego $|\operatorname{Spec} A| \leq \dim_k A$. □

23. Teorema: *Sea $f : A \to B$ es un morfismo de anillos entero. El morfismo inducido $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ es una aplicación cerrada de fibras de dimensión cero (y finitas si f es finito).*

Demostración. Sea $C = (J)_0$ un cerrado de $\operatorname{Spec} B$. Debemos demostrar que $f^*(C)$ es un cerrado de $\operatorname{Spec} A$. Consideremos los diagramas

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A/(J\cap A) & \longrightarrow & B/J \end{array} \qquad \begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow & & \uparrow \\ (J\cap A)_0 = \operatorname{Spec} A/(J\cap A) & \xleftarrow[f^*{}_{|C}]{} & \operatorname{Spec} B/J = C \end{array}$$

Como $A/J\cap A \hookrightarrow B/J$ es un morfismo entero inyectivo, por 2.7.17 $f^*{}_{|C}$ es epiyectiva y $f^*(C) = (J\cap A)_0$.

La fibra de un punto $x \in \operatorname{Spec} A$ es $f^{*-1}(x) = \operatorname{Spec} B_x/\mathfrak{p}_x B_x$. Supongamos que f es un morfismo finito. Observemos que si $f^{*-1}(x) \neq \emptyset$ entonces $B_x/\mathfrak{p}_x B_x$ es una $A_x/\mathfrak{p}_x$-álgebra finita. Por el lema anterior, concluimos que f^* es de fibras de dimensión cero y finitas. Si f entero es sencillo deducir que las fibras son de dimensión cero una vez que se sabe esto para los morfismos finitos. □

24. Ejercicio: Probar que la inclusión natural $k[x] \hookrightarrow k[x,y]/(xy-1)$ no es un morfismo finito.

Una A-álgebra B se dice que es de tipo finito si existen $\xi_1,\dots,\xi_n \in B$ que generen A-algebraicamente B, es decir, el morfismo

$$\pi\colon A[x_1,\dots,x_n] \to B,\ p(x_1,\dots,x_n) \mapsto p(\xi_1,\dots,\xi_n)$$

es epiyectivo. Escribiremos $B = A[\xi_1,\dots,\xi_n]$. $\operatorname{Ker}\pi \subset A[x_1,\dots,x_n]$ es un ideal, que estará generado por ciertos polinomios $p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n)$. Por tanto,

$$B \simeq A[x_1,\dots,x_n]/(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))$$

25. Lema de normalización de Noether: *Sea $A = k[\xi_1,\dots,\xi_n]$ una k-álgebra de tipo finito. Supongamos que k tiene un número infinito de elementos*[7]*. Existe un morfismo finito e inyectivo*

$$k[x_1,\dots,x_r] \hookrightarrow A$$

"Toda variedad algebraica afín se proyecta con fibras finitas en un espacio afín".

Demostración. Vamos a hacerlo por inducción sobre n. Para $n = 0$, no hay nada que decir. Supongamos que el teorema es cierto hasta $n-1$.

Si los $\{\xi_i\}$ son algebraicamente independientes entre sí, entonces $k[\xi_1,\dots,\xi_n] = k[x_1,\dots,x_n]$ y hemos concluido. Podemos suponer que existe $p(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$, no nulo, tal que $p(\xi_1,\dots,\xi_n) = 0$.

[7] Esta hipótesis no es necesaria, solo la imponemos porque la demostración del lema es algo más sencilla.

Escribamos $p(x_1,\ldots,x_n)=p_s(x_1,\ldots,x_n)+p_{s-1}(x_1,\ldots,x_n)+\ldots+p_0(x_1,\ldots,x_n)$ como suma de polinomios homogéneos $p_r(x_1,\ldots,x_n)$ de grado r. Sean $x_i =: x_i' + \lambda_i x_n$, para $i < n$. Entonces,

$$p(x_1'+\lambda_1 x_n,\ldots,x_{n-1}'+\lambda_{n-1}x_n,x_n) = p_s(\lambda_1,\ldots,\lambda_{n-1},1)x_n^s + \text{polinomio en } x_1',\ldots,x_{n-1}',x_n \text{ de grado en } x_n \text{ menor que } s$$

Así pues, si elegimos $\lambda_1,\ldots,\lambda_{n-1}\in k$ de modo que $p_s(\lambda_1,\ldots,\lambda_{n-1},1)\neq 0$, tendremos que ξ_n es entero sobre $k[\xi_1',\ldots,\xi_{n-1}']$, con $\xi_i' = \xi_i - \lambda_i\xi_n$. Por tanto, la composición

$$k[x_1,\ldots,x_r] \underset{\text{Hip.ind.}}{\overset{\text{finito}}{\hookrightarrow}} k[\xi_1',\ldots,\xi_{n-1}'] \overset{\text{finito}}{\hookrightarrow} k[\xi_1',\ldots,\xi_{n-1}',\xi_n]=k[\xi_1,\ldots,\xi_{n-1},\xi_n]$$

es un morfismo finito. □

26. Teorema de los ceros de Hilbert: *Sea A una k-álgebra de tipo finito y $\mathfrak{m}$ un ideal maximal. Entonces $A/\mathfrak{m}$ es una extensión finita de k.*

Demostración. Obviamente $A/\mathfrak{m}$ es una k-álgebra de tipo finito sobre k. Por el lema de normalización de Noether, existe un morfismo finito inyectivo

$$k[x_1,\ldots,x_r]\hookrightarrow A/\mathfrak{m}$$

Por tanto, $k[x_1,\ldots,x_r]$ ha de tener dimensión de Krull cero, luego $r=0$ y concluimos. □

27. Teorema: *Sea $B=\mathbb{C}[x_1,\ldots,x_n]/(p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$. La aplicación*

$$\{(\alpha_1,\ldots,\alpha_n)\in\mathbb{C}^n : p_1(\alpha_1,\ldots,\alpha_n)=\cdots=p_r(\alpha_1,\ldots,\alpha_n)=0\} \to \operatorname{Spec}_{max}B$$
$$(\alpha_1,\ldots,\alpha_n)\mapsto(\bar{x}_1-\alpha_1,\ldots,\bar{x}_n-\alpha_n)$$

es biyectiva

Demostración. Sea $(\alpha_1,\ldots,\alpha_n)\in\mathbb{C}^n$ tal que $p_1(\alpha_1,\ldots,\alpha_n)=\cdots=p_r(\alpha_1,\ldots,\alpha_n)=0$. Entonces,

$$B/(\bar{x}_1-\alpha_1,\ldots,\bar{x}_n-\alpha_n) = \mathbb{C}[x_1,\ldots,x_n]/(x_1-\alpha_1,\ldots,x_n-\alpha_n,p_1(x_1,\ldots,x_n),\ldots,p_r(x_1,\ldots,x_n))$$
$$= \mathbb{C}/(p_1(\alpha_1,\ldots,\alpha_n),\cdots,p_r(\alpha_1,\ldots,\alpha_n)=\mathbb{C},$$

luego $(\bar{x}_1-\alpha_1,\ldots,\bar{x}_n-\alpha_n)$ es un ideal maximal de B.

Sea $\mathfrak{m}\subset B$ un ideal maximal. $B/\mathfrak{m}=\mathbb{C}$ por el teorema de los ceros de Hilbert. Tenemos que $\bar{x}_i\in B/\mathfrak{m}$ es igual a cierto número complejo α_i y $p_i(\alpha_1,\ldots,\alpha_n)=\overline{p_i(x_1,\ldots,x_n)}=0\in B/\mathfrak{m}=\mathbb{C}$, para todo i. Luego $\bar{x}_i-\alpha_i=0\in B/\mathfrak{m}$ y $(\bar{x}_1-\alpha_1,\ldots,\bar{x}_n-\alpha_n)\subseteq\mathfrak{m}$ y han de coincidir.

□

2.8. Cuestionario

1. Calcula los puntos singulares de $\operatorname{Spec}\mathbb{C}[x,y]/(y^2-x^3)$.
2. Calcula los puntos singulares de $\operatorname{Spec}\mathbb{C}[x,y]/(y^2-x^2+x^3)$.
3. Calcula los puntos singulares de $\operatorname{Spec}\mathbb{C}[x,y,z]/(1+x^2+y^2+z^2, 2+x^2-y^2)$.
4. ¿Es $\mathbb{Z}[\sqrt{5}]$ un anillo de Dedekind?
5. ¿Es $(5)\subset\mathbb{Z}[e^{2\pi i/5}]$ un ideal primo? Descompón (5) como potencia de ideales primos.
6. ¿Es $2\in\mathbb{Z}[\sqrt{-5}]$ irreducible? ¿Es (2) un ideal primo? ¿Es $\mathbb{Z}[\sqrt{-5}]$ un anillo de Dedekind?¿Es $\mathbb{Z}[\sqrt{-5}]$ un dominio de factorización única?¿Es dip?
7. Prueba que $2\cdot 3=(1+\sqrt{-5})\cdot(1-\sqrt{-5})$ son dos factorizaciones de 6 como producto de irreducibles de $\mathbb{Z}[\sqrt{-5}]$. Descompón los ideales (2), (3), $(1+\sqrt{-5})$ y $(1-\sqrt{-5})$ como producto de ideales primos de $\mathbb{Z}[\sqrt{-5}]$. Descompón el ideal $(6)\subset\mathbb{Z}[\sqrt{-5}]$ como producto de ideales primos.
8. ¿Es $\operatorname{Spec}\mathbb{C}[x,y]$ una curva algebraica íntegra?
9. ¿Es $\operatorname{Spec}\mathbb{C}(x)[y]$ una curva $\mathbb{C}(x)$-algebraica íntegra?
10. ¿Es $\mathbb{Z}[x]$ un anillo de números?
11. ¿Es $\mathbb{Z}[1/2]$ un anillo de números?
12. ¿Es $\mathbb{Z}[i\sqrt{3}+\sqrt{5},\sqrt[7]{3}]$ un anillo de números?
13. Sea $\mathfrak{p}_5:=(5)\subset\mathbb{Z}$. Calcula $v_5(125/40)$.
14. Resuelve el ejercicio 2.6.17.
15. Sea V la variedad de Riemann de K. Dado $f\in k$ y $v\in V$ ¿Es $v(f)=0$?
16. Sea $\mathbb{P}^1$ la variedad de Riemann de $k(x)$ y $f\in k(x)$. Si $v(f)=0$, para toda $v\in\mathbb{P}^1$ ¿entonces, $f\in k$?
17. Sea V la variedad de Riemann de un cuerpo K de tipo finito de grado de trascendencia 1. Si $f\in K$ es algebraico sobre k, prueba que $v(f)=0$, para toda $v\in V$. Si $f\in K$ es trascendente sobre k, prueba que existen $v,v'\in V$ tales que $v(f)>0$ y $v'(f)<0$.
18. ¿Es una variedad de Riemann recubrible por dos abiertos que sean curvas algebraicas afines no singulares? ¿Y por uno solo?

2.9. Biografía de Dedekind

DEDEKIND BIOGRAPHY

Richard Dedekind's father was a professor at the Collegium Carolinum in Brunswick. His mother was the daughter of a professor who also worked at the Collegium Carolinum. Richard was the youngest of four children and never married. He was to live with one of his sisters, who also remained unmarried, for most of his adult life.

He attended school in Brunswick from the age of seven and at this stage mathematics was not his main interest. The school, Martino-Catharineum, was a good one and Dedekind studied science, in particular physics and chemistry. However, physics became less than satisfactory to Dedekind with what he considered an imprecise logical structure and his attention turned towards mathematics.

The Collegium Carolinum was an educational institution between a high school and a university and he entered it in 1848 at the age of 16. There he was to receive a good understanding of basic mathematics studying differential and integral calculus, analytic geometry and the foundations of analysis. He entered the University of Göttingen in the spring of 1850 with a solid grounding in mathematics.

Göttingen was a rather disappointing place to study mathematics at this time, and it had not yet become the vigorous research centre that it turned into soon afterwards. Mathematics was directed by M.A. Stern and G. Ulrich. Gauss also taught courses in mathematics, but mostly at an elementary level. The physics department was directed by Listing and Wilhelm Weber. The two departments combined to initiate a seminar which Dedekind joined from its beginning. There he learnt number theory which was the most advanced material he studied. His other courses covered material such as the differential and integral calculus, of which he already had a good understanding. The first course to really make Dedekind enthusiastic was, rather surprisingly, a course on experimental physics taught by Weber. More likely it was Weber who inspired Dedekind rather than the topic of the course.

In the autumn term of 1850, Dedekind attended his first course given by Gauss. It was a course on least squares:

... fifty years later Dedekind remembered the lectures as the most beautiful he had ever heard, writing that he had followed Gauss with constantly increasing interest and that he could not forget the experience.

Dedekind did his doctoral work in four semesters under Gauss's supervision and submitted a thesis on the theory of Eulerian integrals. He received his doctorate from Göttingen in 1852 and he was to be the last pupil of Gauss. However he was not well trained in advanced mathematics and fully realised the deficiencies in his mathematical education.

At this time Berlin was the place where courses were given on the latest mathematical developments but Dedekind had not been able to learn such material at Göttingen. By this time Riemann was also at Göttingen and he too found that the mathematical education was aimed at students who were intending to become secondary school teachers, not those with the very top abilities who would go on to research careers. Dedekind therefore spent the two years following the award of his doctorate learning the latest mathematical developments and working for his habilitation.

In 1854 both Riemann and Dedekind were awarded their habilitation degrees within a few weeks of each other. Dedekind was then qualified as a university teacher and he began teaching at Göttingen giving courses on probability and geometry.

Gauss died in 1855 and Dirichlet was appointed to fill the vacant chair at Göttingen. This was an extremely important event for Dedekind who found working with Dirichlet extremely profitable. He attended courses by Dirichlet on the theory of numbers, on potential theory, on definite integrals, and on partial differential equations. Dedekind and Dirichlet soon became close friends and the relationship was in many ways the making of Dedekind, whose mathematical interests took a new lease of life with the discussions between the two. Bachmann, who was a student in Göttingen at this time wrote:

... recalled in later years that he only knew Dedekind by sight because Dedekind always arrived and left with Dirichlet and was completely eclipsed by him.

Dedekind wrote in a letter in July 1856:

What is most useful to me is the almost daily association with Dirichlet, with whom I am for the first time beginning to learn properly; he is always completely amiable towards me, and he tells me without beating about the bush what gaps I need to fill and at the same time he gives me the instructions and the means to do it. I thank him already for infinitely many things, and no doubt there will be many more.

Dedekind certainly still continued to learn mathematics at this time as a student would by attending courses, such as those by Riemann on abelian functions and elliptic functions. Around this time Dedekind studied the work of Galois and he was the first to lecture on Galois theory when he taught a course on the topic at Göttingen during this period.

While at Göttingen, Dedekind applied for J L Raabe's chair at the Polytechnikum in Zürich. Dirichlet supported his application writing that Dedekind was 'an exceptional pedagogue'. In the spring of 1858 the Swiss councillor who made appointments came to Göttingen and Dedekind was quickly chosen for the post. Dedekind was appointed to the Polytechnikum in Zürich and began teaching there in the autumn of 1858.

In fact it was while he was thinking how to teach differential and integral calculus, the first time that he had taught the topic, that the idea of a Dedekind cut came to him. He recounts that the idea came to him on 24 November 1858. His idea was that every real number r divides the rational numbers into two subsets, namely those greater than r and those less than r. Dedekind's brilliant idea was to represent the

real numbers by such divisions of the rationals.

Dedekind and Riemann travelled together to Berlin in September 1859 on the occasion of Riemann's election to the Berlin Academy of Sciences. In Berlin, Dedekind met Weierstrass, Kummer, Borchardt and Kronecker.

The Collegium Carolinum in Brunswick had been upgraded to the Brunswick Polytechnikum by the 1860s, and Dedekind was appointed to the Polytechnikum in 1862. With this appointment he returned to his home town and even to his old educational establishment where his father had been one of the senior administrators for many years. Dedekind remained there for the rest of his life, retiring on 1 April 1894. He lived his life as a professor in Brunswick:

... in close association with his brother and sister, ignoring all possibilities of change or attainment of a higher sphere of activity. The small, familiar world in which he lived completely satisfied his demands: in it his relatives completely replaced a wife and children of his own and there he found sufficient leisure and freedom for scientific work in basic mathematical research. He did not feel pressed to have a more marked effect in the outside world: such confirmation of himself was unnecessary.

After he retired, Dedekind continued to teach the occasional course and remained in good health in his long retirement. The only spell of bad health which Dedekind had experienced was 10 years after he was appointed to the Brunswick Polytechnikum when he had a serious illness, shortly after the death of his father. However he completely recovered and, as we mentioned, remained in good health.

Dedekind made a number of highly significant contributions to mathematics and his work would change the style of mathematics into what is familiar to us today. One remarkable piece of work was his redefinition of irrational numbers in terms of Dedekind cuts which, as we mentioned above, first came to him as early as 1858. He published this in Stetigkeit und Irrationale Zahlen in 1872. In it he wrote:

Now, in each case when there is a cut (A_1, A_2) *which is not produced by any rational number, then we create a new, irrational number* a*, which we regard as completely defined by this cut; we will say that this number* a *corresponds to this cut, or that it produces this cut.*

As well as his analysis of the nature of number, his work on mathematical induction, including the definition of finite and infinite sets, and his work in number theory, particularly in algebraic number fields, is of major importance.

Dedekind loved to take his holidays in Switzerland, the Austrian Tyrol or the Black Forest in southern Germany. On one such holiday in 1874 he met Cantor while staying in the beautiful city of Interlaken and the two discussed set theory. Dedekind was sympathetic to Cantor's set theory as is illustrated by this quote from Was sind und was sollen die Zahlen (1888) regarding determining whether a given element belongs to a given set:

In what way the determination comes about, or whether we know a way to decide it, is a matter of no consequence in what follows. The general laws that are to be developed do not depend on this at all.

In this quote Dedekind is arguing against Kronecker's objections to the infinite and, therefore, is agreeing with Cantor's views.

Among Dedekind's other notable contributions to mathematics were his editions of the collected works of Peter Dirichlet, Carl Gauss, and Georg Riemann. Dedekind's study of Dirichlet's work did, in fact, lead to his own study of algebraic number fields, as well as to his introduction of ideals. Dedekind edited Dirichlet's lectures on number theory and published these as Vorlesungen über Zahlentheorie in 1863. It is noted that:

Although the book is assuredly based on Dirichlet's lectures, and although Dedekind himself referred to the book throughout his life as Dirichlet's, the book itself was entirely written by Dedekind, for the most part after Dirichlet's death.

It was in the third and fourth editions of Vorlesungen über Zahlentheorie, published in 1879 and 1894, that Dedekind wrote supplements in which he introduced the notion of an ideal which is fundamental to ring theory. Dedekind formulated his theory in the ring of integers of an algebraic number field. The general term 'ring' does not appear, it was introduced later by Hilbert.

Dedekind, in a joint paper with Heinrich Weber published in 1882, applies his theory of ideals to the theory of Riemann surfaces. This gave powerful results such as a purely algebraic proof of the Riemann-Roch theorem.

Dedekind's work was quickly accepted, partly because of the clarity with which he presented his ideas and partly since Heinrich Weber lectured to Hilbert on these topics at the University of Königsberg. Dedekind's notion of ideal was taken up and extended by Hilbert and then later by Emmy Noether. This led to the unique factorisation of integers into powers of primes to be generalised to ideals in other rings.

In 1879 Dedekind published Über die Theorie der ganzen algebraischen Zahlen which was again to have a large influence on the foundations of mathematics. In the book Dedekind:

... presented a logical theory of number and of complete induction, presented his principal conception of the essence of arithmetic, and dealt with the role of the complete system of real numbers in geometry in the problem of the continuity of space. Among other things, he provides a definition independent of the concept of number for the infiniteness or finiteness of a set by using the concept of mapping and treating the recursive definition, which is so important to the theory of ordinal numbers.

Dedekind's brilliance consisted not only of the theorems and concepts that he studied but, because of his ability to formulate and express his ideas so clearly, he introduced a new style of mathematics that been a major influence on mathematicians ever since. As Edwards writes:

Dedekind's legacy ... consisted not only of important theorems, examples, and concepts, but a whole style of mathematics that has been an inspiration to each succeeding generation.

Many honours were given to Dedekind for his outstanding work, although he always remained extraordinarily modest regarding his own abilities and achievements.

He was elected to the Göttingen Academy (1862), the Berlin Academy (1880), the Academy of Rome, the Leopoldino-Carolina Naturae Curiosorum Academia, and the Académie des Sciences in Paris (1900). Honorary doctorates were awarded to him by the universities of Kristiania (Oslo), Zurich and Brunswick.

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

2.10. Problemas

1. Prueba que todo anillo de Dedekind que tenga solo un número finito de ideales primos es un anillo de ideales principales.

   Resolución: Sea $\mathrm{Spec}_{max} A = \{x_1, \dots, x_n\}$. Consideremos el epimorfismo de paso al cociente
   $$\pi\colon A \to A/\mathfrak{p}_{x_1}^2\,\mathfrak{p}_{x_2}\cdots\mathfrak{p}_{x_n} = A/\mathfrak{p}_{x_1}^2 \times A/\mathfrak{p}_{x_2} \times \cdots \times A/\mathfrak{p}_{x_n}$$
   Sea $f_1 \in \mathfrak{p}_{x_1} \setminus \mathfrak{p}_{x_1}^2$ y $f \in A$ tal que $\pi(f) = (\bar{f_1}, \bar{1}, \dots, \bar{1})$. Se cumple que $(f) = \mathfrak{p}_{x_1}$ porque así es localmente en cada punto x_i. Luego todos los ideales primos del anillo de Dedekind son principales luego A es d.i.p.

2. Prueba que todo anillo de Dedekind que tenga solo un número finito de ideales primos es un anillo euclídeo.

   Resolución: Sea $\mathrm{Spec}_{max} A = \{x_1, \dots, x_r\}$. Definamos $\mathrm{gr}\colon A\setminus\{0\} \to \mathbb{N}$ como sigue: dado $a \in A$ no nula tenemos que $(a) = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}$. Definimos $\mathrm{gr}(a) = n_1 + \cdots + n_r$. Obviamente, $\mathrm{gr}(ab) = \mathrm{gr}(a) + \mathrm{gr}(b) \geq \mathrm{gr}(a)$. Dados $a, b \in A$ no nulos, escribamos $(a) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ y $(b) = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$. Si $n_i \geq m_i$ para todo i, entonces a es múltiplo de b y existe $q \in A$ tal que $a = bq$. Supongamos que $n_1 < m_1, \dots, n_s < m_s$ y $n_{s+1} \geq m_{s+1}, \dots, n_r \geq m_r$. Sea $r \in A$, tal que $r = a \mod \mathfrak{p}_i^{m_i}$, para $i \leq s$ y $r = b \mod \mathfrak{p}_j^{m_j+1}$, para $j \geq s$. Entonces, $a - r = 0 \mod (b)$ y $\mathrm{gr}\, r < \mathrm{gr}\, b$. Existe $q \in A$, de modo que $a - r = bq$, es decir, $a = bq + r$ con $\mathrm{gr}\, r < \mathrm{gr}\, b$.

3. Sea A un dominio de Dedekind e $0 \neq I \subset A$ un ideal. Prueba que A/I es un anillo de ideales principales.

   Resolución: $\mathrm{Spec}(A/I) = (I)_0 = \{x_1, \dots, x_r\}$ y
   $$A/I = \prod_i (A/I)_{x_i} = \prod_i A_{x_i}/I \cdot A_{x_i}$$
   Dado un ideal $J \subset A/I$ se tiene que $J_{x_i} = (t_{x_i})$ es principal porque es un ideal de $(A/I)_{x_i} = A_{x_i}/I_{x_i}$ que es de ideales principales. Además, $J = \prod_i J_{x_i}$, porque así es localmente. Vía esta igualdad $J = \langle (t_{x_i})_i \rangle$ porque así es localmente.

4. Prueba que en un anillo de Dedekind todos los ideales están generados por dos elementos.

Resolución: Sea $I \subset A$ un ideal y $f \in I$ no nulo. $A/(f)$ es un anillo de ideales principales, luego $\bar{I} = (\bar{g})$. Por tanto, $I = (f, g)$.

5. Sean I, J, K ideales de un dominio de Dedekind. Prueba que si $I \cdot J = I \cdot K$ entonces $J = K$.

   Resolución: Es consecuencia inmediata del teorema 2.2.3.

6. Prueba que $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ es un dominio de Dedekind.

   Resolución: $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y) = \mathbb{C}[x,y]_S$, con $S = \{p(x) \cdot q(y) \in \mathbb{C}[x,y], \text{ no nulos}\}$. Por tanto, $\operatorname{Spec} \mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y) = \{z \in \operatorname{Spec} C[x,y] \colon \mathfrak{p}_z = (p(x,y)) \colon p(x,y)$ es un polinomio irreducible que depende de las variables x e y; ó $p(x,y) = 0\}$. Por tanto, el anillo $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ es un dominio de ideales primcipales.

7. Prueba que si un anillo es íntegro noetheriano y todos sus ideales maximales son principales, entonces es d.i.p.

   Resolución: Es dominio de Dedekind. Todo ideal es producto de ideales maximales, luego todo ideal es principal.

8. Sea A un dominio de Dedekind e $I \subset A$ un ideal no nulo. Prueba que existe un ideal J tal que $I \cdot J$ es un ideal principal.

   Resolución: $I^{-1} \cdot I = A$ y existe $a \in A$ tal que $a \cdot I^{-1} \subset A$. Por tanto, $(a \cdot I^{-1}) \cdot I = aA$.

9. Sea A un anillo noetheriano íntegro de cuerpo de fracciones K e $I \subset K$ un ideal fraccionario. Se dice que I es invertible si existe otro ideal fraccionario $J \subset K$ tal que $I \cdot J = A$. Prueba que I es invertible si y solo si I_x es un A_x-módulo monógeno para todo $x \in \operatorname{Spec} A$. Si A es de dimensión de Krull 1 y $x \in \operatorname{Spec}_{max} A$, prueba que x es no singular si y solo si $\mathfrak{p}_x$ es invertible.

   Resolución: Observemos que I es invertible si y solo si $I \cdot [A \colon I] = A$, lo cual es una cuestión local. Podemos suponer que A es un anillo local de ideal maximal $\mathfrak{m}_x$. Evidentemente, si I es monógeno entonces es invertible. Supongamos que I es invertible, es decir, existe un ideal fraccionario tal que $I \cdot J = A$. Si $i \cdot j \in \mathfrak{m}_x$ para todo $i \in I$ y $j \in J$, entonces $I \cdot J \subset \mathfrak{m}_x \neq A$. Luego existen $i \in I$ y $j \in J$ de modo que $u = i \cdot j \notin \mathfrak{m}_x$, es decir, u es un invertible de A. Por tanto, $I \cdot j = A$, luego $I = j^{-1} \cdot A$ que es monógeno.

   Por último, $\mathfrak{p}_x$ es invertible si y solo si $\mathfrak{p}_x$ es localmente de ideales principales, que equivale a decir que x es no singular.

10. Sea A un dominio de Dedekind de cuerpo de fracciones K. Sean I_1, I_2 dos ideales fraccionarios de K. Prueba que $I_2 \cdot [I_1 \colon I_2] = I_1$.

    Resolución: El conjunto de los ideales fraccionarios de K es un grupo abeliano con la multiplicación. $I_2 \cdot [I_1 \colon I_2] \subseteq I_1$ y $[I_1 \colon I_2]$ es el ideal fraccionario más grande

cumpliendo esta inclusión, como $J = I_1 \cdot I_2^{-1}$ cumple que $I_2 \cdot J = I_1$ tenemos que $[I_1 : I_2]$ también cumple que $I_2 \cdot [I_1 : I_2] = I_1$.

11. Descompón $33 + 11\sqrt{-7}$ en producto de elementos irreducibles de $\mathbb{Z}[\sqrt{-7}]$.

Resolución: $\mathbb{Z}[\sqrt{-7}] = \mathbb{Z}[x]/(x^2+7)$ y vía esta igualdad $33 + 11\sqrt{-7} = 33 + 11x$. Obviamente, $33 + 11x = 11(3 + x)$. Por una parte, $(11)_0 = \{(11, x-2), (11, x+2)\}$ y $11 = -(x-2)(x+2)$, y resulta que $(x-2)$ y $(x+2)$ son primos. Por otra, $N(3+x) = 9+7 = 16$. Si $3+x$ no es irreducible $3+x = (a+bx)\cdot(c+dx)$ con $N(a+bx) = a^2+7b^2 = 4$ y $N(c+dx) = c^2+7d^2 = 4$, luego $a = \pm 2$, $b = 0$ y $c = \mp 2$, $d = 0$ y llegamos a contradicción. Luego, $33 + 11x = (2-x)(x+2)(3+x)$.

12. ¿Es $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ entero sobre $\mathbb{Z}$?

Resolución: $\frac{3+2\sqrt{6}}{1-\sqrt{6}} = \frac{(3+2\sqrt{6})(1+\sqrt{6})}{-5} = \frac{(3+2\cdot 6)+(3+2)\sqrt{6}}{-5} = -3-\sqrt{6}$ que es entero sobre $\mathbb{Z}$.

13. Sea $A = \mathbb{C}[x_1, \ldots, x_n]/(p_1, \ldots, p_{n-1})$ y $\alpha \in \operatorname{Spec}_{max} A$. Prueba que A_α es un dominio de ideales principales si y solo si $(\frac{\partial p_i}{\partial x_j}(\alpha))_{ij}$ es una matriz de rango $n-1$.

Resolución: $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 = \langle d_\alpha x_1, \ldots, d_\alpha x_n\rangle / \langle d_\alpha p_1, \ldots, d_\alpha p_{n-1}\rangle$. Luego, $\dim_{\mathbb{C}} \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 = 1$ si y solo si $(\frac{\partial p_i}{\partial x_j}(\alpha))_{ij}$ es una matriz de rango $n-1$. Además, la dimensión de Krull de A_α es mayor o igual que 1. Con todo, se concluye por el problema 13 del capítulo 1.

14. Prueba que $\mathbb{Z}[\sqrt{-5}]$ es un anillo de Dedekind. Sea $\mathfrak{m} = (2, 1+\sqrt{-5})$. Prueba que 2 es irreducible y que (2) no es un ideal primo (por tanto $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única). Prueba que $\mathfrak{m}^2 = (2)$ pero que $\mathfrak{m}$ no es principal.

Resolución: Consideremos el morfismo $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-5}]$. Los ideales primos (p) tales que la $\mathbb{Z}/p\mathbb{Z}$-álgebra $\mathbb{Z}[\sqrt{-5}]/(p) = \mathbb{Z}/p\mathbb{Z}[x]/(x^2+5)$ no es separable son $p = 2, 5$. Tenemos que $(2)_0 = \{(2, x+1) = \mathfrak{p}_y\}$ y $(5)_0 = \{(5, x) = (x)\}$. Así pues, el único punto singular posible es $y \in \operatorname{Spec} \mathbb{Z}[x]/(x^2+5) \subset \operatorname{Spec} \mathbb{Z}[x]$. Ahora bien, $d_y(x^2+5) = d_{y_1}((x+1)^2 - 2(x+1) + 6) = 3d_y 2 \neq 0$, luego $\mathfrak{p}_y/\mathfrak{p}_y^2 = \langle d_y(x+1)\rangle$ e y es no singular. Además, $\mathfrak{p}_y^2 = (2^2, (x+1)^2, 2(x+1)) = (4, 2(x+1) - 6, 2(x+1)) = (2)$.

Dado un número complejo z, sea $N(z) = z \cdot \bar{z}$, Entonces, $N(a+bx) = a^2 + 5b^2$. Si $2 = (a+bx)\cdot(c+dx)$, entonces $4 = N(2) = (a^2+5b^2)\cdot(c^2+5d^2)$, luego $b = d = 0$, y $a = \pm 2$ y $c = \mp 1$ (ó $c = \pm 2$ y $a = \mp 1$). En conclusión, 2 es irreducible. El ideal $\mathfrak{m}$ no puede ser principal porque 2 es irreducible.

15. Prueba que $2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$ son dos factorizaciones de 6 como producto de irreducibles de $\mathbb{Z}[\sqrt{-5}]$. Descompón los ideales (2), (3), $(1+\sqrt{-5})$ y $(1-\sqrt{-5})$ en $\mathbb{Z}[\sqrt{-5}]$ como producto de ideales primos. Descompón como producto de ideales primos el ideal (6).

Resolución: Dado $a+b\sqrt{-5}$ definimos $N(a+b\sqrt{-5})=(a+b\sqrt{-5})\cdot(a-b\sqrt{-5})=a^2+5b^2$. $N(2)=4$, si $2=z_1\cdot z_2$, con z_1 y z_2 propios entonces $N(z_1)=N(z_2)=2$, lo cual es imposible. Luego, 2 es irreducible. Igualmente, $3,1+\sqrt{-5}),1-\sqrt{-5}$ son irreducibles.

$(2)=\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_r}^{n_r}$. $(2)_0=\{x_1,\ldots,x_r\}$. Por otra parte,

$$\begin{aligned}(2)_0&=\operatorname{Spec}\mathbb{Z}[\sqrt{-5}]/2\cdot\mathbb{Z}[\sqrt{-5}]=\operatorname{Spec}\mathbb{Z}/2\mathbb{Z}[x]/(x^2+5)\\&=\operatorname{Spec}\mathbb{Z}/2\mathbb{Z}[x]/(x^2+1)=\operatorname{Spec}\mathbb{Z}/2\mathbb{Z}[x]/((x+1)^2)=\{(\overline{x+1})\}.\end{aligned}$$

Es decir, $(2)_0=\{(2,1+\sqrt{-5})=\mathfrak{m}_y\}$. Tendremos, $(2)=\mathfrak{m}_y^n$. Tenemos que calcular n. Observemos,

$$d_y(x^2+5)=d_y((x+1-1)^2+5)=d_y6=3d_y2$$

Luego, $\mathfrak{m}_y/\mathfrak{m}_y^2=\langle d_y(x+1)\rangle$ y $\mathfrak{m}_y=(1+\sqrt{-5})\cdot\mathbb{Z}[\sqrt{-5}]$. Luego,

$$2\cdot\mathbb{Z}[\sqrt{-5}]_y=\mathfrak{m}_y^n\cdot\mathbb{Z}[\sqrt{-5}]_y=(1+\sqrt{-5})^n\cdot\mathbb{Z}[\sqrt{-5}]_y$$

si y solo si $\overline{(1+\sqrt{-5})^n}=0$ y $\overline{(1+\sqrt{-5})^{n-1}}\neq 0$ en $\mathbb{Z}[\sqrt{-5}]_y/2\cdot\mathbb{Z}[\sqrt{-5}]_y$. Por otra parte,

$$\mathbb{Z}[\sqrt{-5}]_y/2\cdot\mathbb{Z}[\sqrt{-5}]_y=\mathbb{Z}/2\mathbb{Z}[x]/((x+1)^2)$$

luego $n=2$. Por tanto,

$$(2)=(2,1+\sqrt{-5})^2$$

$(3)=\mathfrak{m}_{x_1}^{n_1}\cdots\mathfrak{m}_{x_r}^{n_r}$. $(3)_0=\{x_1,\ldots,x_r\}$. Por otra parte,

$$\begin{aligned}(3)_0&=\operatorname{Spec}\mathbb{Z}[\sqrt{-5}]/3\cdot\mathbb{Z}[\sqrt{-5}]=\operatorname{Spec}\mathbb{Z}/3\mathbb{Z}[x]/(x^2+5)\\&=\operatorname{Spec}\mathbb{Z}/3\mathbb{Z}[x]/(x^2-1)=\operatorname{Spec}\mathbb{Z}/3\mathbb{Z}[x]/((x+1)(x-1))=\{(\overline{x+1}),(\overline{x-1})\}.\end{aligned}$$

Es decir, $(3)_0=\{(3,1+\sqrt{-5})=\mathfrak{m}_y,(3,1-\sqrt{-5})=\mathfrak{m}_z\}$. Tenemos que $(3)=\mathfrak{m}_y^n\cdot\mathfrak{m}_z^m$. Tenemos que calcular n y m. Observemos que

$$d_y(x^2+5)=d_y((x+1-1)^2+5)=2d_y(x+1)+2d_y3,$$

Luego $\mathfrak{m}_y/\mathfrak{m}_y^2=\langle d_y3\rangle$ y $\mathfrak{m}_y\cdot\mathbb{Z}[\sqrt{-5}]_y=(3)\cdot\mathbb{Z}[\sqrt{-5}]_y$. Luego, $n=1$. Del mismo modo, $m=1$. Luego,

$$(3)=(3,1+\sqrt{-5})\cdot(3,1-\sqrt{-5}).$$

El lector puede comprobar que

$$(1+\sqrt{-5})=(2,1+\sqrt{-5})\cdot(3,1+\sqrt{-5})\text{ y }(1-\sqrt{-5})=(2,1-\sqrt{-5})\cdot(3,1-\sqrt{-5}).$$

16. Sea A un dominio de Dedekind y sean $I_1, I_2 \subseteq A$ dos ideales no nulos. Escribamos sus descomposiciones como producto de ideales primos $I_1 = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}$ y $I_2 = \mathfrak{p}_{x_1}^{m_1} \cdots \mathfrak{p}_{x_r}^{m_r}$, con $n_i \geq 0$, $m_i \geq 0$, $\mathfrak{p}_{x_i}$ ideal primo y $\mathfrak{p}_{x_i} \neq \mathfrak{p}_{x_j}$, para todo $i \neq j$. Prueba que

$$\begin{aligned} I_1 \cap I_2 &= \mathfrak{p}_{x_1}^{\text{máx}(n_1,m_1)} \cdots \mathfrak{p}_{x_r}^{\text{máx}(n_r,m_r)} \\ I_1 + I_2 &= \mathfrak{p}_{x_1}^{\text{mín}(n_1,m_1)} \cdots \mathfrak{p}_{x_r}^{\text{mín}(n_r,m_r)} \end{aligned}$$

Resolución: Pruébese las igualdades localizando en todo punto cerrado de $\operatorname{Spec} A$.

17. Prueba que $\mathbb{Z}[\sqrt{2}, i]$ no es un dominio de Dedekind. Demuestra que $\mathbb{Z}[\sqrt{2}, \frac{i+1}{\sqrt{2}}]$ es el anillo de números de $\mathbb{Q}[\sqrt{2}, i]$.

Resolución: $A = \mathbb{Z}[\sqrt{2}]$ es un dominio de Dedekind. Estudiemos los puntos rama del morfismo $A = \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}, i]$. $A = \mathbb{Z}[\sqrt{2}]$ es un $\mathbb{Z}$-módulo libre de rango 2 y $\mathbb{Z}[\sqrt{2}, i]$ es un $\mathbb{Z}$-módulo libre de rango 4, $A[x]/(x^2+1)$ es un $\mathbb{Z}$-módulo libre de rango 4. Por tanto, el epimorfismo $A[x]/(x^2+1) \to \mathbb{Z}[\sqrt{2}, i]$ es un isomorfismo. El polinomio $x^2 + 1 \in A/\mathfrak{m}[x]$ no es separable si y solo si $x^2 + 1$ y $2x$ tienen raíces comunes, es decir, $2 = 0$ en $A/\mathfrak{m}$. Por tanto, los puntos rama son $(2)_0 = \{(\sqrt{2})\}$. Los puntos singulares de $A[x]/(x^2+1)$ están incluidos en $(\sqrt{2})_0 = \{(\sqrt{2}, \overline{x+1})\}$. Sea $\mathfrak{m}_z = (\sqrt{2}, x+1) \subset A[x]$. Consideremos el morfismo de paso al cociente $A[x] \to A[x]/(x^2+1)$ y $\bar{\mathfrak{m}}_z = (\sqrt{2}, \overline{x+1})$. Entonces,

$$\bar{\mathfrak{m}}_z/\bar{\mathfrak{m}}_z^2 = (\mathfrak{m}_z/\mathfrak{m}_z^2)/\langle \overline{x^2+1} \rangle = (\mathfrak{m}_z/\mathfrak{m}_z^2)/\langle \overline{(x+1)^2 - 2(x+1) + 2} \rangle = \mathfrak{m}_z/\mathfrak{m}_z^2$$

que tiene dimensión 2, luego $\bar{\mathfrak{m}}_z$ es singular.

Denotemos $x = i$. Observemos que $0 = \frac{1}{2} \cdot (x^2+1) = \frac{1}{2} \cdot ((x+1)^2 - 2(x+1) + 2) = (\frac{x+1}{\sqrt{2}})^2 - \sqrt{2} \cdot \frac{x+1}{\sqrt{2}} + 1$. Por tanto, $\frac{i+1}{\sqrt{2}} \in \mathbb{Q}[\sqrt{2}, i]$ es entero sobre $\mathbb{Z}[\sqrt{2}]$ y

$$\mathbb{Z}[\sqrt{2}, i] \subseteq \mathbb{Z}[\sqrt{2}, \frac{i+1}{\sqrt{2}}] \subseteq \overline{\mathbb{Z}[\sqrt{2}, i]}.$$

Los puntos singulares de $B := \mathbb{Z}[\sqrt{2}, \frac{i+1}{\sqrt{2}}]$ están incluidos en $(\sqrt{2})_0$. Observemos que $B = A[y]/(y^2 - \sqrt{2}y + 1)$, luego $(\sqrt{2})_0 = \{(\sqrt{2}, y+1) =: \mathfrak{m}_t\}$. Por último, $\mathfrak{m}_t \cdot B_t = (y+1) \cdot B_t$, luego B es de Dedekind y ha de coincidir con $\overline{\mathbb{Z}[\sqrt{2}, i]}$.

18. **Teorema de Kummer-Dedekind:** Sea α raíz de un polinomio $p(x) \in \mathbb{Z}[x]$ mónico irreducible. Sea p un número primo y sea

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

la factorización de $\overline{p(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ en producto de potencias de irreducibles (primos entre sí, y podemos suponer que los polinomios $p_i(x) \in \mathbb{Z}[x]$ son mónicos y $\operatorname{grad}(p(x)) = \sum_i n_i \operatorname{grad}(p_i(x))$). Entonces,

a) $(p)_0 = \{y_1, \dots, y_n\} \subset \operatorname{Spec} \mathbb{Z}[\alpha]$, con $\mathfrak{p}_{y_i} = (p, p_i(\alpha))$.

b) El punto y_i es singular si y solo si $n_i > 1$ y $r_i(x) \in p^2 \cdot \mathbb{Z}[x]$, donde

$$p(x) = q_i(x) \cdot p_i(x) + r_i(x), \text{ con } \operatorname{grad}(r_i(x)) < \operatorname{grad}(p_i(x)).$$

c) $(p) = \mathfrak{p}_{y_1}^{n_1} \cdots \mathfrak{p}_{y_r}^{n_r}$ si y solo si $y_1, \dots, y_r$ son no singulares.

d) Si y_i es singular, entonces $\frac{q_i(\alpha)}{p} \in \overline{\mathbb{Z}[\alpha]} \setminus \mathbb{Z}[\alpha]$.

Resolución: a) Obsérvese que

$$\begin{aligned}(p)_0 &= \operatorname{Spec} \mathbb{Z}[\alpha]/(p) = \operatorname{Spec} \mathbb{Z}[x]/(p, p(x)) = \operatorname{Spec} \mathbb{F}_p[x]/(\overline{p_1(x)}^{n_1} \cdots \overline{p_r(x)}^{n_r}) \\ &= (\overline{p_1(x)}^{n_1} \cdots \overline{p_r(x)}^{n_r})_0 = \cup_i (\overline{p_i(x)})_0 = \{(\overline{p_1(x)}), \dots, (\overline{p_i(x)})\} \subset \operatorname{Spec} \mathbb{F}_p[x]\end{aligned}$$

b) El punto y_i es singular si y solo si $d_{y_i} p(x) = 0$. Observemos que, módulo (p), $q_i(x) = p_i(x)^{n_i - 1}$ y $r_i(x) = 0$. Entonces, $d_{y_i} p(x) = q_i(x)(y_i) d_{y_i} p_i(x) + \frac{r_i(x)}{p}(y_i) d_{y_i} p$ y $d_{y_i} p(x) = 0$ si y solo si $q_i(x)(y_i) = 0$ y $\frac{r_i(x)}{p}(y_i) = 0$. Tenemos que $q_i(x)(y_i)$ es la clase de $\bar{q}_i(x) = \bar{p}_i(x)^{n_i - 1} \in \mathbb{F}_p[x]/(\overline{p(x)})$ en $\mathbb{F}_p[x]/(\overline{p_i(x)})$, que es nula si $n_i - 1 > 0$; y $\frac{r_i(x)}{p}(y_i)$ es la clase de $\overline{\frac{r_i(x)}{p}} \in \mathbb{Z}[x]/(p_i(x))$ en $\mathbb{F}_p[x]/(\overline{p_i(x)})$, que es nula si el polinomio $\frac{r_i(x)}{p}$ es múltiplo de p (recordemos que $\operatorname{grad}(r_i(x)) < \operatorname{grad}(p_i(x))$).

(*c*) Si $(p) = \mathfrak{p}_{y_1}^{n_1} \cdots \mathfrak{p}_{y_r}^{n_r}$ entonces $\mathfrak{p}_{y_i}$ es un ideal fraccionario invertible, luego y_i es no singular. Supongamos que $y_1, \dots, y_n$ son no singulares. Para probar la igualdad basta probarla localmente. Basta ver que $(p)_{y_i} = \mathfrak{p}_{y_i}^{n_i} \cdot \mathbb{Z}[\alpha]_{y_i}$. Tenemos que ver que n_i es el menor número natural tal que $\mathfrak{p}_{y_i}^{n_i} \subseteq (p)_{y_i}$ y $\mathfrak{p}_{y_i}^{n_i - 1} \not\subseteq (p)_{y_i}$. Haciendo módulo (p), buscamos el mínimo número natural m tal que $\overline{\mathfrak{p}_{y_i}^m} = (\overline{p_i(x)}^m)$ es cero en $\mathbb{Z}[\alpha]_{y_i}/(p) = \mathbb{F}_p[x]/(p_i(x)^{n_i})$, que es claramente $m = n_i$.

(*d*) Observemos que $0 = p(\alpha) = q_i(\alpha) \cdot p_i(\alpha) + r_i(\alpha)$ y como y_i es singular recordemos que $q_i(x)$ es múltiplo de $p_i(x)$ y $r_i(x) \in p^2 \cdot \mathbb{Z}[x]$. Entonces, $\frac{q_i(\alpha)}{p} \cdot p = q_i(\alpha) \in \mathfrak{p}_{y_i}$ y $\frac{q_i(\alpha)}{p} \cdot p_i(\alpha) = -\frac{r_i(\alpha)}{p} \in \mathfrak{p}_{y_i}$. Por tanto, tenemos el endomorfismo de $\mathbb{Z}[\alpha]$-módulos $\frac{q_i(\alpha)}{p} \cdot : \mathfrak{p}_{y_i} \to \mathfrak{p}_{y_i}$, que está anulado por el teorema de Hamilton-Cayley por el polinomio característico. Por lo tanto, $\frac{q_i(\alpha)}{p}$ es entero sobre $\mathbb{Z}[\alpha]$.

19. Pruébese que el anillo local de $k[x, y]$ en el origen es normal pero no es un anillo de valoración.

Resolución: Sea $\mathcal{O}$ el anillo local de $k[x, y]$ en el origen. $k[x, y]$ es un dominio de factorización única, luego es normal y $\mathcal{O}$ también. El ideal (x, y) es finito generado y $\dim_k (x, y)/(x, y)^2 = 2$. Luego, $(x, y) \cdot \mathcal{O}$ no es principal y no es un anillo de valoración.

Capítulo 3

Discriminante. Desingularización

3.1. Introducción

El anillo $\mathbb{C}[x,y]/(y^2-x^3)$ de funciones algebraicas de la curva $y^2-x^3=0$ no es localmente principal en el origen. Los anillos de funciones de las curvas y los de la Teoría de Números no son locamente principales. En este capítulo trataremos de determinar en qué puntos no son localmente principales y cómo construir un anillo "un poco más amplio" que ya es localmente de ideales principales (es decir, de Dedekind), utilizando como herramienta el discriminante.

3.2. Traza y métrica de la traza

Sea B una k-álgebra finita. Dado $a \in B$, consideremos el endomorfismo k-lineal

$$h_a : B \to B,\ h_a(b) := a \cdot b.$$

1. Definición: Sea $\mathrm{tr}: B \to k$, la aplicación definida por $\mathrm{tr}(a) := \mathrm{tr}(h_a)$. Diremos que $\mathrm{tr}(a)$ es la traza de a. Observemos que tr es una aplicación k-lineal.

2. Definición: Sea $\mathrm{Tr}: B \times B \to k$ la aplicación definida por $\mathrm{Tr}(a,a') := \mathrm{tr}(h_{aa'})$, que es una aplicación k-bilineal simétrica. Diremos que Tr es la métrica de la traza.

Si $\{e_1,\ldots,e_n\}$ es una base del k-espacio vectorial B, se dice, que $(\mathrm{Tr}(e_i,e_j))_{ij}$ es la matriz asociada a Tr en la base $\{e_1,\ldots,e_n\}$.

3. Ejemplo: Consideremos la $\mathbb{Q}$-álgebra trivial $\mathbb{Q}^3$. Calculemos la matriz asociada a la métrica de la traza en la base estándar $\{e_1=(1,0,0), e_2=(0,1,0), e_3=(0,0,1)\}$: En primer lugar calculemos la matriz asociada a las aplicaciones $\mathbb{Q}$-lineales $h_{(1,0,0)}, h_{(0,1,0)}$

83

y $h_{(0,0,1)}$. Es fácil ver que

$$h_{(1,0,0)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; h_{(0,1,0)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; h_{(0,0,1)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Por tanto, $\mathrm{Tr}(e_i, e_j) = \begin{cases} \mathrm{tr}(0) = 0 \text{ si } i \neq j. \\ \mathrm{tr}(e_i) = \mathrm{tr}(h_{e_i}) = 1 \text{ si } i = j. \end{cases}$ Por lo tanto, $\mathrm{Tr} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

4. Ejercicio: Calcula la matriz de la métrica de la traza de la $\mathbb{Q}$-álgebra finita $\mathbb{Q}[\sqrt{2}]$ en la base $\{1, \sqrt{2}\}$.

5. Supongamos que B es una k-álgebra finita separable. Existe una k-extensión Σ que la trivializa, es decir,

$$B \otimes_k \Sigma = \Sigma \times \overset{n}{\cdots} \times \Sigma.$$

Si escribimos $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{k-alg}(B, \Sigma)$, es fácil deducir de las siguientes igualdades $\mathrm{Hom}_{k-alg}(B, \Sigma) = \mathrm{Hom}_{\Sigma-alg}(B \otimes_k \Sigma, \Sigma) = \mathrm{Hom}_{\Sigma-alg}(\Sigma^n, \Sigma)$ que el morfismo

$$B \otimes_k \Sigma \to \Sigma \times \overset{n}{\cdots} \times \Sigma, \; a \otimes \lambda \mapsto (\sigma_1(a) \cdot \lambda, \overset{n}{\ldots}, \sigma_n(a) \cdot \lambda)$$

es un isomorfismo de Σ-álgebras. Por cambio, de cuerpo base $k \hookrightarrow \Sigma$, tenemos el endomorfismo Σ-lineal

$$h_a \otimes 1 \colon B \otimes_k \Sigma \to B \otimes_k \Sigma, \; b \otimes \lambda \mapsto ab \otimes \lambda.$$

Si la matriz de h_a en una k-base $\{e_i\}$ es (a_{ij}) la matriz de $h_a \otimes 1$ en la Σ-base $\{e_i \otimes 1\}$ es (a_{ij}). Por lo tanto, $\mathrm{tr}(h_a) = \mathrm{tr}(h_a \otimes 1)$. Por otra parte, recordemos que vía el isomorfismo $B \otimes_k \Sigma = \Sigma \times \overset{n}{\cdots} \times \Sigma$, $a \otimes 1$ se aplica en $(\sigma_1(a), \ldots, \sigma_n(a))$, luego la matriz de $h_a \otimes 1 = h_{a \otimes 1}$ en la base estándar de $\Sigma \times \overset{n}{\cdots} \times \Sigma$ es la matriz diagonal de coeficientes $\sigma_i(a)$. Por tanto,

$$\mathrm{tr}(a) = \sum_i \sigma_i(a) \text{ y } \mathrm{Tr}(a, b) = \sum_i \sigma_i(ab).$$

Si $\{e_1, \ldots, e_n\}$ es una k-base de B entonces

$$\boxed{\mathrm{Tr} \equiv (\mathrm{tr}(e_i e_j)) = (\sigma_j(e_i))^t \cdot (\sigma_j(e_i)).}$$

6. Sea B una k-álgebra finita y sea $T \colon B \to B^\vee = \mathrm{Hom}_k(B, k)$ la polaridad definida por la métrica de la traza, es decir, $T(b)(b') := \mathrm{Tr}(b, b')$. La matriz asociada a T en una base $\{e_1, \ldots, e_n\}$ y su dual es igual a la matriz asociada a Tr. Sea $\mathrm{rad}\,\mathrm{Tr} := \mathrm{Ker}\, T = \{b \in B \colon T_2(b, b') = 0, \; \forall \; b' \in B\}$. Observemos que $\mathrm{rad}\,\mathrm{Tr}$ es un ideal de B, porque $\mathrm{Tr}(bb_1, b_2) = \mathrm{Tr}(b, b_1 b_2)$ y que $\mathrm{rad}\, B \subseteq \mathrm{rad}\,\mathrm{Tr}$ porque la traza de los endomorfismos lineales nilpotentes es nula. El concepto de traza, métrica de la traza, polaridad y radical de la métrica de la traza son estables por cambios de cuerpo base. Si el determinante de la matriz asociada a Tr es no nulo, entonces $\mathrm{rad}\, B = 0$ y lo sigue siendo por cambio de cuerpo base, luego B es una k-álgebra separable. Recíprocamente, si B es separable por cambio de cuerpo base B es trivial y el determinante de Tr es no nulo.

7. Teorema: *Sea A un anillo noetheriano íntegro e íntegramente cerrado en su cuerpo de fracciones Σ. Sea $\Sigma \hookrightarrow \bar{\Sigma}$ una extensión finita separable de cuerpos y $\bar{A}$ el cierre entero de A en $\bar{\Sigma}$. Entonces, el morfismo $A \hookrightarrow \bar{A}$, es finito y el cuerpo de fracciones de $\bar{A}$ es $\bar{\Sigma}$.*

Demostración. $\bar{\Sigma}$ es el cuerpo de fracciones de $\bar{A}$, porque el cierre entero conmuta con localizaciones por 2.4.4, luego $\bar{A}_{A-0} = \overline{A_{A-0}} = \bar{\Sigma}$.

Como A es noetheriano, basta probar que $\bar{A}$ es un submódulo de un A-módulo libre finito generado.

Sea T_2 la métrica de la traza en $\bar{\Sigma}$, $T_2(f,g) = \mathrm{tr}(f \cdot g)$, y sea $T : \bar{\Sigma} \to \bar{\Sigma}^\vee$ su polaridad asociada, que es un isomorfismo por ser $\bar{\Sigma}$ una Σ-álgebra separable. Sea $\bar{a}_1, \ldots, \bar{a}_n \in \bar{A}$ una base de $\bar{\Sigma}$ como Σ-espacio vectorial y $w_1, \ldots, w_n \in \bar{\Sigma}^*$ su base dual. Si probamos que $T(\bar{A}) \subseteq Aw_1 + \cdots + Aw_n$ concluimos.

Como ya sabemos, $\mathrm{tr}(a') = \sum_{g \in G} g(a')$, siendo $G = \mathrm{Hom}_{\Sigma - alg}(\bar{\Sigma}, \bar{\bar{\Sigma}})$ y $\bar{\bar{\Sigma}}$ la envolvente de Galois de la extensión $\Sigma \to \bar{\Sigma}$. Dado $a' \in \bar{A}$, escribamos $T(a') = \lambda_1 w_1 + \cdots + \lambda_n w_n$, con $\lambda_i \in \Sigma$. Tenemos que ver que $\lambda_i \in A$. Se tiene que

$$\lambda_i = T(a')(\bar{a}_i) = \mathrm{tr}(a' \cdot \bar{a}_i) = \sum_{g \in G} g(a' \cdot \bar{a}_i)$$

Ahora bien, $a' \cdot \bar{a}_i \in \bar{A}$, luego $g(a' \cdot \bar{a}_i)$ es entero sobre A y λ_i es entero sobre A. Como A es íntegramente cerrado en su cuerpo de fracciones entonces $\lambda_i \in A$.

□

8. Corolario: *Sea K un cuerpo de números. El anillo de números de K (es decir, el cierre entero de $\mathbb{Z}$ en K) es un anillo de números (es decir, una $\mathbb{Z}$-álgebra finita íntegra).*

Demostración. $\mathbb{Z}$ es íntegramente cerrado en $\mathbb{Q}$ y tenemos el morfismo finito $\mathbb{Q} \hookrightarrow K$. Concluimos, Concluimos por el teorema 3.2.7. □

9. Corolario: *Supongamos por sencillez que k es un cuerpo de característica cero. Sea A el anillo de funciones algebraicas de una curva íntegra, Σ su cuerpo de fracciones y $\bar{A}$ el cierre entero de A en Σ. Entonces, el morfismo $A \hookrightarrow \bar{A}$ es finito.*

Demostración. Recordemos que existe un morfismo finito $k[x] \hookrightarrow A$. Ahora se procede como en teoría de números cambiando $\mathbb{Z}$ por $k[x]$ y $\mathbb{Q}$ por $k(x)$. □

3.3. Discriminante

Sea K un cuerpo de números, es decir, una extensión finita de cuerpos de $\mathbb{Q}$ y sea $A \subset K$ el anillo de números de K. K es una $\mathbb{Q}$-álgebra finita separable, consideremos la traza $tr : K \to \mathbb{Q}$. Si $a \in A$, existe un polinomio mónico $p(x) \in \mathbb{Z}[x]$ tal que $p(a) = 0$, entonces para todo $\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$ se cumple que $\sigma(a)$ es entero sobre $\mathbb{Z}$ (por que

$p(\sigma(a)) = \sigma(p(a)) = \sigma(0) = 0$). Por tanto, $\mathrm{tr}(a)$ es entero sobre $\mathbb{Z}$ y pertenece a $\mathbb{Q}$, luego $\mathrm{tr}(a) \in \mathbb{Z}$. Tenemos, pues, el diagrama conmutativo

$$\begin{array}{ccc} K & \xrightarrow{\mathrm{tr}} & \mathbb{Q} \\ \uparrow & & \uparrow \\ A & \xrightarrow{\mathrm{tr}} & \mathbb{Z} \end{array}$$

y la aplicación $\mathbb{Z}$-bilineal simétrica $\mathrm{Tr}\colon A \times A \to \mathbb{Z}$, $\mathrm{Tr}(a,b) = \mathrm{tr}(ab)$.

Sea A un anillo de números de un cuerpo de números K. Observemos que $A_{\mathbb{Z}\setminus\{0\}}$ es una $\mathbb{Q}$-álgebra finita íntegra, luego es un cuerpo y ha de coincidir con K. A es un $\mathbb{Z}$-módulo libre de rango $\dim_{\mathbb{Q}} K$: como es un $\mathbb{Z}$-módulo finito generado sin torsión es libre $A \simeq \mathbb{Z}^n$ y localizando por el sistema multiplicativo $A\setminus\{0\}$, obtenemos que $K \simeq A_{A\setminus\{0\}} \simeq \mathbb{Q}^n$, luego $n = \dim_{\mathbb{Q}} K$.

Si consideramos una base del $\mathbb{Z}$-módulo libre A, ésta es una base del $\mathbb{Q}$-espacio vectorial K.

1. Definición: Sea $a_1,\dots,a_n$ una base del $\mathbb{Z}$-módulo libre A. Llamaremos discriminante de A, que denotaremos Δ_A, al determinante de la matriz de la métrica de la traza en la base $a_1,\dots,a_n$. Es decir,

$$\boxed{\Delta_A = \det(\mathrm{tr}(a_i a_j)).}$$

Sea $\mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = \{\sigma_1,\dots,\sigma_n\}$. Entonces, $\boxed{\Delta_A = \det(\sigma_j(a_i))^2.}$

Si consideramos otra base $b_1,\dots,b_n$ de A y (b_{ij}) es la matriz de cambio de base (es decir, $b_i = \sum_j b_{ij} a_j$) entonces $(\mathrm{tr}(b_i b_j)) = (b_{ij})^t \cdot (\mathrm{tr}(a_i a_j)) \cdot (b_{ij})$ y

$$\det(\mathrm{tr}(b_i b_j)) = \det((b_{ij}))^2 \cdot \det(\mathrm{tr}(a_i a_j)) = \det(\mathrm{tr}(a_i a_j)).$$

porque $\det((b_{ij})) = \pm 1$, ya que $(b_{ij}) \in M_n(\mathbb{Z})^*$ luego $\det((b_{ij})) \in \mathbb{Z}^* = \{\pm 1\}$.

2. Ejercicio: Calcula el discriminante de $\mathbb{Z}[i]$.

3. Ejercicio: Sea A un anillo de números de cuerpo de fracciones K, supongamos que $i \notin K$ y sea n el rango del $\mathbb{Z}$-módulo A. Demuestra que $\Delta_{A[i]} = (-4)^n \cdot \Delta_A^2$.

4. Ejemplo: Sea $\alpha \in \mathbb{C}$ entero sobre $\mathbb{Z}$ y sea $p(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Z}[x]$ el polinomio mínimo anulador. Sea $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(p(x))$ y $\mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = \{\sigma_i\}$. Las raíces de $p(x)$ son $\{\alpha_i := \sigma_i(\alpha)\}_i$.

Una $\mathbb{Z}$-base de $\mathbb{Z}[\alpha]$ es $\{1,\alpha,\dots,\alpha^{d-1}\}$. Recordemos que el valor del determinante de Vandermonde es $\det(x_i^j) = \prod_{i<j}(x_i - x_j)$. Entonces,

$$\Delta_{\mathbb{Z}[\alpha]} = \det((\sigma_i(\alpha^j)))^2 = \det((\alpha_i^j))^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \Delta(p(x)).$$

$\Delta(p(x))$ es igual[1] al determinante de la homotecia

$$h_{p(x)'}\colon \mathbb{Q}[x]/(p(x)) \to \mathbb{Q}[x]/(p(x)),$$

multiplicado por $(-1)^{\frac{d(d-1)}{2}}$.

Calculemos el discriminante de $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$, con p primo distinto de 2. Hemos probado que $\Delta_{\mathbb{Z}[e^{\frac{2\pi i}{p}}]} = \Delta(\Phi_p(x))$. Observemos que $x^p - 1 = (x-1)\cdot\Phi_p(x)$, entonces

$$\Delta(x^p-1) = \Phi_p(1)^2 \cdot \Delta(\Phi_p(x)) = p^2 \cdot \Delta(\Phi_p(x)),$$

$\Delta(x^p-1)$ es igual al determinante de $h_{p\cdot x^{p-1}}\colon \mathbb{Q}[x]/(x^p-1) \to \mathbb{Q}[x]/(x^p-1)$, que es p^p, multiplicado por $(-1)^{\frac{p\cdot(p-1)}{2}} = (-1)^{\frac{(p-1)}{2}}$. Luego,

$$\Delta_{\mathbb{Z}[e^{\frac{2\pi i}{p}}]} = \Delta(\Phi_p(x)) = (-1)^{\frac{(p-1)}{2}} \cdot p^{p-2}.$$

3.3.1. Desingularización vía el discriminante

5. Proposición: *Sea A un anillo de números, consideremos el morfismo finito $\mathbb{Z} \to A$ y el morfismo inducido en espectros $\pi\colon \operatorname{Spec} A \to \operatorname{Spec}\mathbb{Z}$. Entonces,*

$$\{\textit{Puntos rama de } \pi\} = (\Delta_A)_0.$$

Demostración. Sea $\mathfrak{m}_x = (p)$. Por definición, x es un punto rama si y solo si A/pA no es una $\mathbb{Z}/p\mathbb{Z}$-álgebra separable, es decir, $\Delta_{A/pA} = \overline{\Delta_A} \in \mathbb{Z}/p\mathbb{Z}$ es nulo, es decir, $x \in (\Delta_A)_0$. □

6. Corolario: *Sea A un anillo de números. Sigamos las notaciones de la proposición anterior. Entonces,*

$$\{\textit{Puntos singulares de } \operatorname{Spec} A\} \subseteq \pi^{-1}(\{\textit{Puntos rama de } \pi\}) = (\Delta_A)_0.$$

Dado un $\mathbb{Z}$-módulo libre Γ, una métrica simétrica T_2 en Γ (una aplicación $\mathbb{Z}$-bilineal simétrica) y una base $e_1,\dots,e_n$ de Γ, se define el discriminante de Γ, que denotamos Δ_Γ como

$$\Delta_\Gamma := \det(T_2(e_i, e_j))$$

y no depende de la base escogida.

Sea $\Gamma' \subset \Gamma$ un submódulo de rango n. Existen bases en $\{e'_1,\dots,e'_n\}$, $\{e_1,\dots,e_n\}$ en Γ' y Γ de modo que $e'_i = \lambda_i \cdot e_i$, para ciertos $\lambda_i \in \mathbb{Z}$. Observemos, $\Delta_{\Gamma'} = (\lambda_1\cdots\lambda_n)^2 \cdot \Delta_\Gamma$. Además, $(\Delta_{\Gamma'}) = (\Delta_\Gamma)$ si y solo si $\Gamma = \Gamma'$.

Observemos que $\Gamma/\Gamma' \simeq \mathbb{Z}/\lambda_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\lambda_n\mathbb{Z}$, luego $|\Gamma/\Gamma'| = |\lambda_1\cdots\lambda_n|$ y

$$\boxed{\Delta_{\Gamma'} = |\Gamma/\Gamma'|^2 \cdot \Delta_\Gamma}$$

Podemos demostrar de nuevo el siguiente teorema.

[1] La demostración se basa en que se puede suponer por cambio de cuerpo base que todas las raíces están en el cuerpo base y el teorema chino de los restos.

7. Teorema : *Sea K un cuerpo de números. El anillo de números de K (es decir, el cierre entero de $\mathbb{Z}$ en K) es un anillo de números (es decir, una $\mathbb{Z}$-álgebra finita íntegra).*

Demostración. Podemos escribir $K = \mathbb{Q}(\xi_1,\dots,\xi_n)$, con $\xi_1,\dots,\xi_n$ enteros sobre $\mathbb{Z}$. Sea $A := \mathbb{Z}[\xi_1,\dots,\xi_n]$, cuyo cuerpo de fracciones es K y sea Δ_A su discriminante. Sea $a_1 \in K$ un elemento entero, que no pertenece a A y sea $A_1 = A[a_1]$. Tenemos el morfismo finito $A \hookrightarrow A_1$ y $(\Delta_A) \underset{\neq}{\subset} (\Delta_{A_1})$. Igualmente, sea $a_2 \in K$ un elemento entero, que no pertenece a A_1 y sea $A_2 = A_1[a_2]$. Tenemos el morfismo finito $A_1 \hookrightarrow A_2$ y $(\Delta_{A_1}) \underset{\neq}{\subset} (\Delta_{A_2})$ Obviamente este proceso ha de terminar en un número finito m de pasos y lo hará cuando A_m sea el anillo de números de K. Observemos que A_m es un anillo de números.

□

8. Definición : Sea K un cuerpo de números. Se define el discriminante de K, que denotamos por Δ_K, como el discriminante del anillo de números de K.

9. Corolario : *Sea $K \hookrightarrow K'$ una extensión finita de cuerpos de números y A y A' los anillos de números de K y K', respectivamente. Entonces, el morfismo $A \hookrightarrow A'$ es finito.*

Demostración. A' es un $\mathbb{Z}$-módulo finito generado, luego es un A-módulo finito generado.

□

10. Corolario : *Sea A un anillo de números. Se cumple que*

$$\{\textit{Puntos singulares de } \operatorname{Spec} A\} \subseteq \bigcup_{p^2 \mid \Delta_A} (p)_0.$$

Demostración. Sea $\bar{A}$ el anillo de números de $K = A_{A\setminus\{0\}}$. $\bar{A}/A$ es un grupo abeliano finito, luego isomorfo a $\oplus_{ij}\mathbb{Z}/p_i^{n_{ij}}\mathbb{Z}$, con p_i primos. Sea $y \in \operatorname{Spec}_{max} A$ un punto singular singular y $\mathfrak{m}_y \cap \mathbb{Z} = (p) =: \mathfrak{m}_x$, entonces $(\bar{A}/A)_y \neq 0$, luego $(\bar{A}/A)_x \neq 0$ y p divide a $|\bar{A}/A|$. Recordemos que $\Delta_A = |\bar{A}/A|^2 \cdot \Delta_{\bar{A}}$, luego p^2 divide a Δ_A. □

11. Ejemplo : Sea $\alpha \in \mathbb{C}$ raíz de un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 2, y $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(p(x))$. Calculemos el anillo de números A de K.

$K = \mathbb{Q}[\sqrt{m}]$, con $m \in \mathbb{Q}$. Podemos escribir $m = r^2 \cdot n$, donde n es un número entero sin factores cuadráticos (no existe ningún número primo p tal que p^2 divida a n). Entonces, $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{n}]$. El discriminante de $x^2 - n$ es $4n$, luego $\Delta_{\mathbb{Z}[\sqrt{n}]} = 4 \cdot n$. Tenemos que $\mathbb{Z}[\sqrt{n}] \subseteq A$ y

$$\Delta_{\mathbb{Z}[\sqrt{n}]} = |A/\mathbb{Z}[\sqrt{n}]|^2 \cdot \Delta_A.$$

Si $\mathbb{Z}[\sqrt{n}] \neq A$, entonces $\Delta_A = n$ y $|A/\mathbb{Z}[\sqrt{n}]| = 2$. Por el Corolario 3.3.10, los únicos puntos singulares de $\mathbb{Z}[\sqrt{n}]$ posibles están en $(2)_0$. Ahora bien,

$$(2)_0 = \operatorname{Spec} \mathbb{Z}[\sqrt{n}]/(2) = \operatorname{Spec} \mathbb{Z}/2\mathbb{Z}[x]/(x^2 - n) = \begin{cases} (\bar{x}) \text{ si } n \text{ es par} \\ (\bar{x}+1) \text{ si } n \text{ es impar} \end{cases}$$

Es decir, $(2)_0$ es $\{(2, \sqrt{n})\}$ si n es par ó $\{(2, \sqrt{n}+1)\}$ si n es impar.

Sea $\mathfrak{m}_y = (2,x) \subset \mathbb{Z}[x]$. Si n es par, entonces $d_y(x^2-n) = d_y 2 \neq 0$, luego $(\bar{2},\bar{x}) \subset \mathbb{Z}[x]/(x^2-n)$ es no singular. Es decir, $(2, \sqrt{n}) \subset \mathbb{Z}[\sqrt{n}]$ es no singular. Si n es impar, sea $\mathfrak{m}_y = (2, x+1) \subset \mathbb{Z}[x]$, entonces

$$d_y(x^2-n) = d_y((x+1-1)^2-n) = d_y((x+1)^2-2(x+1)+1-n) = d_y(1-n) = 0$$

si y solo si $1-n$ es múltiplo de 4. Es decir, $(2, \sqrt{n}+1) \subset \mathbb{Z}[\sqrt{n}]$ es singular si y solo si $1-n$ es múltiplo de 4. En este caso, observemos que $\frac{\sqrt{n}+1}{2}$ es entero porque

$$0 = \frac{(\sqrt{n}+1)^2 - 2(\sqrt{n}+1)+1-n}{4} = (\frac{\sqrt{n}+1}{2})^2 - \frac{\sqrt{n}+1}{2} + \frac{1-n}{4}$$

Por tanto, $A = \mathbb{Z}[\frac{\sqrt{n}+1}{2}]$.

Demostremos de nuevo que el anillo de números de un cuerpo de números es un anillo de números precisando en qué $\mathbb{Z}$-módulo finito generado está incluido.

12. Teorema: *Sea K un cuerpo de números y A su anillo de números. Sea $\alpha_1,\dots,\alpha_n \in A$ una $\mathbb{Q}$-base de K y escribamos $\Delta_{\mathbb{Z}\cdot\alpha_1+\cdots+\mathbb{Z}\cdot\alpha_n} = r^2 \cdot s$ de modo que ningún primo al cuadrado divida a s. Entonces,*

$$A \subseteq \frac{\mathbb{Z}\cdot\alpha_1+\cdots+\mathbb{Z}\cdot\alpha_n}{r}.$$

Demostración. Denotemos $M = \mathbb{Z}\cdot\alpha_1+\cdots+\mathbb{Z}\cdot\alpha_n$ y consideremos la inclusión $M \hookrightarrow A$. Existe una $\mathbb{Z}$-base $v_1,\dots,v_n$ de M, de modo que $\frac{1}{d_1}\cdot v_1,\dots,\frac{1}{d_n}\cdot v_n$ es una $\mathbb{Z}$-base de A, para ciertos números naturales $d_1,\dots,d_n$. Observemos que $|A/M| = d_1\cdots d_n$, luego $\Delta_M = |A/M|^2\cdot\Delta_A = d_1^2\cdots d_n^2\cdot\Delta_A$ y por tanto $d_1\cdots d_n$ divide a r. Entonces,

$$A = \mathbb{Z}\cdot\frac{1}{d_1}\cdot v_1+\cdots+\mathbb{Z}\cdot\frac{1}{d_n}\cdot v_n \subseteq \mathbb{Z}\cdot\frac{1}{r}\cdot v_1+\cdots+\mathbb{Z}\cdot\frac{1}{r}\cdot v_n = \frac{1}{r}\cdot M.$$

□

Demos un algoritmo para el cálculo del anillo de números de un cuerpo de números.

13. Teorema: *Sea K un cuerpo de números y $\{a_1,\dots,a_n\}$ una $\mathbb{Q}$-base de K, formada por elementos enteros. Sea M el $\mathbb{Z}$-módulo generado por la base. Si M no es igual al anillo de números de K, existe un primo p tal que p^2 divide a Δ_M y números naturales $0 \leq r_1,\dots,r_s < p$, para un $s < n$ de modo que $a = \frac{1}{p}\cdot(r_1a_1+\cdots+r_sa_s+a_{s+1})$ es entero. Si M' es el $\mathbb{Z}$-módulo generado por $\{a_1,\dots,a_s,a,a_{s+2},\dots,a_n\}$ entonces $\Delta_{M'} = \frac{\Delta_M}{p^2}$.*

Demostración. Sea A el anillo de números de K. Escribamos $\Delta_M = u^2\cdot v$, con $u,v \in \mathbb{N}$ y de modo que ningún primo al cuadrado divida a v. Sabemos que $M \subseteq A \subseteq \frac{M}{u}$. Si p es un primo que no divide a u (es decir, p^2 no divide a Δ_M) y denotamos $\mathfrak{m}_x = (p)$,

entonces $M_x = (\frac{M}{u})_x$ y $M_x = A_x$. Sea $\mathfrak{m}_x = (p)$, tal que $M_x \neq A_x$, luego p^2 divide Δ_M o equivalentemente p divide a u. Tenemos, $M_x \subsetneq A_x \subseteq (\frac{M}{u})_x = \frac{1}{p^n} \cdot M_x$ (con $n = v_x(u)$). Entonces, existe $b = \sum_i \frac{m_i}{p^n} \cdot a_i \in A \setminus M$, con $m = \min\{v_x(\frac{m_i}{p^n})\} < 0$. Entonces, $c = p^{-m-1} \cdot b \in A \cap \frac{1}{p} \cdot M$ y $c \notin M$. Escribamos $c = \sum_i \frac{n_i}{p} \cdot a_i$. Sea $s+1$ máximo tal que $n_{s+1} \notin (p)$. Sea $t \in \mathbb{N}$ tal que $t \cdot n_{s+1} = 1 \mod p$. Existe $d \in M$ tal que $a = t \cdot c - d = \frac{1}{p} \cdot (r_1 a_1 + \cdots + r_s a_s + a_{s+1})$ es el entero buscado.

Por último, consideremos las inclusiones

$$M = \mathbb{Z} \cdot a_1 + \cdots + \mathbb{Z} \cdot a_n = \mathbb{Z} \cdot a_1 + \cdots + \underset{s+1}{\mathbb{Z} \cdot pa} + \cdots + \mathbb{Z} \cdot a_n \hookrightarrow \mathbb{Z} \cdot a_1 + \cdots + \underset{s+1}{\mathbb{Z} \cdot a} + \cdots + \mathbb{Z} \cdot a_n = M'$$

Entonces, $\Delta_M = |M'/M|^2 \cdot \Delta_{M'} = p^2 \cdot \Delta_{M'}$.

□

En el teorema hemos pasado de un $\mathbb{Z}$-módulo M de elementos enteros de discriminante Δ_M a otro, M', de discriminante $\Delta_{M'} = \frac{1}{p^2} \cdot \Delta_M$. Si repetimos este proceso con M' y así sucesivamente este proceso ha de terminar y lo hará cuando M_n sea el anillo de números de K. Sólo un número finito de primos p cumplen que p^2 divide a Δ_M y solo un número finito de elementos $a \in K$ son de la forma escrita en el teorema. El proceso termina cuando para todo primo p tal que p^2 divide a Δ_{M_n}, todos los a de la forma escrita no son elementos enteros de K.

14. Ejemplo: Consideremos el ejemplo de Dedekind: calculemos el anillo de números de $K := \mathbb{Q}[x]/(x^3 + x^2 - 2x + 8)$. Sea $A' := \mathbb{Z}[x]/(x^3 + x^2 - 2x + 8)$. Se puede comprobar que $\Delta_{A'} = 2^2 \cdot 503$. El primo considerado en el teorema anterior, con $M := A'$, solo puede ser $p = 2$. El ideal primo $\mathfrak{m}_y = (2, x)$ es singular, entonces A' no es el anillo de números de K. Si tenemos un $\mathbb{Z}$-submódulo $M' \subset K$ formado por elementos enteros tal que $A' \subsetneq M'$, como $\Delta_{M'} = |M'/A|^2 \cdot \Delta_{A'}$, entonces $\Delta_{M'} = 503$, luego M' es el anillo de números de K.

Consideremos la $\mathbb{Z}$-base $\{1, x, x^2\}$ de A'. Por el teorema anterior, uno de lo siguientes elementos de K

$$1/2, (1+x)/2, x/2, (1+x+x^2)/2, (1+x^2)/2, (x+x^2)/2, x^2/2$$

es entero. Dividiendo $x^3 + x^2 - 2x + 8 = 0$ por 4, tenemos que

$$0 = (x/2)^2 x + (x/2)^2 - (x/2) + 2 = (x/2) = (x/2)^2 (x+1) - (x/2) + 2.$$

Multiplicando por $x+1$, $(\frac{x^2+x}{2})^2 - \frac{x^2+x}{2} + 2(x+1) = 0$, luego $\frac{x^2+x}{2}$ es entero sobre A' y por tanto entero sobre $\mathbb{Z}$, es decir, es un elemento entero de K. Por tanto,

$$\mathbb{Z} \oplus \mathbb{Z} \cdot x \oplus \mathbb{Z} \cdot \frac{x^2 + x}{2}$$

es el anillo de números de K.

3.3.2. Discriminante y volumen

15. Definición: Sea E un $\mathbb{R}$-espacio vectorial de dimensión n y $\{e_1,\dots,e_n\}$ una base. Se dice que $\Gamma := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ es una red de E y que E/Γ es el paralelepípedo asociado a la red Γ.

Observemos que $E/\Gamma = \{\sum_i \lambda_i \cdot \bar{e}_i : 0 \le \lambda_i < 1\}$.

Para definir el volumen de los paralelepípedos de un $\mathbb{R}$-espacio vectorial solo se necesita fijar una unidad de medida. Si tenemos una métrica, la unidad de medida que se fija es aquella en la que el volumen de un "cubo" de lados de módulo 1 es 1. Precisemos la definición.

16. Definición: Sea $\Gamma = \mathbb{Z}\cdot e_1 \oplus \cdots \oplus \mathbb{Z}\cdot e_n$ una red de un $\mathbb{R}$-espacio vectorial E y T_2 una métrica simétrica no singular de E. Se define el volumen del paralelepípedo E/Γ, como el número real positivo $Vol_{T_2}(E/\Gamma)$ siguiente

$$Vol_{T_2}(E/\Gamma) := \sqrt{|\det(T_2(e_i,e_j)|} = \sqrt{|\Delta_\Gamma|}.$$

17. Observaciones: 1. Sea $\Gamma' = \mathbb{Z}\cdot e'_1 \oplus \cdots \oplus \mathbb{Z}\cdot e'_n$ otro retículo y sea (λ_{ij}) la matriz de cambio de base, es decir, $e'_j = \sum_i \lambda_{ij} e_i$, entonces

$$Vol_{T_2}(E/\Gamma') = \sqrt{|\det(T_2(e'_i,e'_j))|} = \sqrt{|\det(T_2(e_i,e_j))|\cdot \det(\lambda_{ij})^2} = Vol_{T_2}(E/\Gamma)\cdot|\det(\lambda_{ij})|.$$

2. Sea T'_2 otra métrica semétrica no singular de E, si $Vol_{T'_2}(E/\Gamma) = \lambda \cdot Vol_{T_2}(E/\Gamma)$, entonces $Vol_{T'_2}(E/\Gamma') = \lambda \cdot Vol_{T_2}(E/\Gamma')$.

Sea K un cuerpo de números. $K \otimes_{\mathbb{Q}} \mathbb{R}$ es una $\mathbb{R}$-álgebra finita separable, luego es reducida, luego es producto de extensiones finitas de $\mathbb{R}$. Es decir, $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$, con $r + 2s = n$. Observemos que

$$\mathrm{Hom}_{\mathbb{R}-alg}(K \otimes_{\mathbb{Q}} \mathbb{R}, \mathbb{C}) = \mathrm{Hom}_{\mathbb{R}-alg}(\mathbb{R}^r \times \mathbb{C}^s, \mathbb{C}) = \{\pi_1,\dots,\pi_{r+s}, c\circ\pi_{r+1},\dots,c\circ\pi_{r+s}\},$$

donde π_i es la proyección en el factor i-ésimo y c es conjugar. Por otra parte,

$$\mathrm{Hom}_{\mathbb{R}-alg}(K \otimes_{\mathbb{Q}} \mathbb{R}, \mathbb{C}) = \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) = \{\sigma_1,\dots,\sigma_n\}.$$

Reordenando, podemos suponer que los $\pi_1,\dots,\pi_{r+s}$ se corresponden con $\sigma_1,\dots,\sigma_{r+s}$. Ahora ya, puede probarse que el morfismo

$$K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s, \quad a \otimes 1 \mapsto (\sigma_1(a),\dots,\sigma_{r+s}(a))$$

es isomorfismo. Sea A un anillo de números de K (o en general un ideal fraccionario) y consideremos la identificación obvia $\mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$ y denotemos σ a la composición

$$A \hookrightarrow A \otimes_{\mathbb{Z}} \mathbb{R} = A \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{R} = K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n,\ a \mapsto (\sigma_1(a),\dots,\sigma_{r+s}(a)) = \sigma(a).$$

Vía σ, A es el retículo de $\sigma(A) \subset \mathbb{R}^n$. Si $\{a_1 \dots a_n\}$ es una $\mathbb{Z}$-base de A, entonces $\sigma(A)$ es el retículo $\mathbb{Z}\cdot\sigma(a_1) \oplus \cdots \oplus \mathbb{Z}\cdot\sigma(a_n) \subset \mathbb{R}^n$.

La matriz de la métrica de la traza de la $\mathbb{R}$-álgebra $\mathbb{C}$ en la base $\{1, i\}$ de $\mathbb{C}$ es

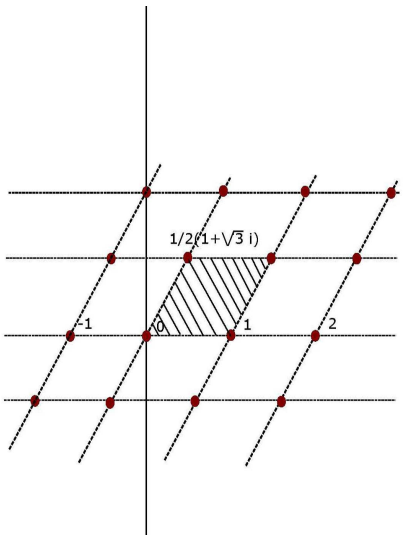
$$\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

Por tanto, el determinante de la matriz de la métrica de la traza en la base obvia del $\mathbb{R}$-espacio vectorial $\mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$ es igual a $(-4)^s$. El determinante de la métrica estándar T_2 de $\mathbb{R}^n$ en la base estándar de $\mathbb{R}^n = \mathbb{R}^r \times \mathbb{C}^s$ es 1. Por tanto,

$$\begin{array}{rcl} \Delta_A & = & (-4)^s \cdot \Delta_A^{T_2} = (-4)^s \det(\sigma(a_1); \dots; \sigma(a_n))^2 = (-4)^s \cdot Vol(\mathbb{R}^n/A)^2 \\ \sqrt{|\Delta_A|} & = & 2^s \cdot Vol(\mathbb{R}^n/A) \end{array}$$

(hemos denotado $Vol = Vol_{T_2}$ el volumen estándar).

18. Ejemplo: Consideremos el anillo de números $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$.



Vamos a considerar como red $\Gamma = A$. Una base del $\mathbb{Z}$-módulo A es $\{1, 1/2(1+\sqrt{-3})\}$. Tenemos que el cuerpo de números es $K = \mathbb{Q}[\sqrt{-3}]$, $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{C} = \mathbb{R}^2$ y $\mathrm{Hom}_{anillos}(K, \mathbb{C}) = \{I, c \circ I\}$, donde I es la inclusión obvia y c es la conjugación de $\mathbb{C}$. Por tanto,

$$\Delta_A = (-4)^1 \begin{vmatrix} 1 & 1/2 \\ 0 & 1/2\sqrt{3} \end{vmatrix}^2 = -3.$$

y

$$Vol(\mathbb{R}^2/A) = 2^1 \begin{vmatrix} 1 & 1/2 \\ 0 & 1/2\sqrt{3} \end{vmatrix} = \sqrt{3}.$$

Por otra parte, también

$$\Delta_A = \begin{vmatrix} 1 & 1/2 + 1/2\sqrt{-3} \\ 1 & 1/2 - 1/2\sqrt{-3} \end{vmatrix}^2 = -3.$$

3.3.3. Norma en anillos de números

19. Definición: Sea A una k-álgebra finita. Diremos que la aplicación $N\colon A \to k$ definida por $N(a) := \det(h_a)$ (donde $h_a\colon A \to A$, es la aplicación k-lineal definida por $h_a(a') = aa'$) es la aplicación norma.

Observemos que $N(ab) = \det(h_{ab}) = \det(h_a \circ h_b) = \det(h_a)\cdot\det(h_b) = N(a)N(b)$, para todo $a, b \in A$.

Si A es una k-álgebra finita separable, $k \hookrightarrow \Sigma$ es una k-extensión trivializante de A y $\{\sigma_1,\dots,\sigma_n\} = \mathrm{Hom}_{k-alg}(K,\Sigma)$, con argumentos similares a los dados con la traza tr, tenemos que

$$N(a) = \prod_{i=1}^{n} \sigma_i(a).$$

Sea K un cuerpo de números. K es una $\mathbb{Q}$-álgebra finita separable. Si $a \in K$ es entero sobre $\mathbb{Z}$, entonces para todo $\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})$ se cumple que $\sigma(a)$ es entero sobre $\mathbb{Z}$, porque si $p(x) \in \mathbb{Z}[x]$ es un polinomio mónico tal que $p(a) = 0$, entonces $p(\sigma(a)) = \sigma(p(a)) = \sigma(0) = 0$. Por tanto, $N(a) = \prod_{i=1}^{n} \sigma_i(a)$ es entero sobre $\mathbb{Z}$ y pertenece a $\mathbb{Q}$, luego $N(a) \in \mathbb{Z}$.

20. Teorema: *Sea A un anillo de números de cuerpo de fracciones K. Dada $a \in A \subset K$, se cumple que*

$$|N(a)| = |A/aA|.$$

Demostración. Sea $T\colon \mathbb{Z}^n \to \mathbb{Z}^n$ un isomorfismo $\mathbb{Z}$-lineal, entonces $\det(T)$ y $\det(T^{-1})$ son números enteros. Como $1 = \det(T)\cdot\det(T^{-1})$, entonces $\det(T) = \pm 1$.

Existen sendas bases $\mathscr{B}$ y $\mathscr{B}'$ de los $\mathbb{Z}$-módulos A y A en las que la matriz (d_{ij}) del endomorfismo $a\cdot\colon A \to A$ es diagonal. El determinante de (d_{ij}) es igual salvo signos a $|A/aA|$. Sea (a_{ij}) la matriz de cambio de base, de la base $\mathscr{B}'$ a la base $\mathscr{B}$, entonces $\det(a_{ij}) = \pm 1$. La matriz del endomorfismo lineal $a\cdot$ en la base $\mathscr{B}$ es igual a $(a_{ij})\cdot(d_{ij})$. Por tanto, salvo signos, el determinante del endomorfismo $a\cdot$ es igual a $|A/aA|$. □

Denotemos los invertibles del anillo de números A, A^*.

21. Proposición: *Sea A un anillo de números de cuerpo de fracciones K. Se cumple que*

$$A^* = \{a \in A : N(a) = \pm 1\}.$$

Demostración. Sea $a \in A$. $|N(a)| = |A/(a)| = 1$ si y solo si $a \in A^*$. □

22. Observación: Dado $a \in A$ sea $p_c(x) = \sum_{i=0}^{n} a_i x^{n-i}$ el polinomio característico de la homotecia $a\cdot\colon A \to A$. Sabemos que $N(a) = (-1)^n a_n$ y por otra parte $0 = p(a) = b\cdot a + a_n$, con $b \in A$. En conclusión, $N(a) = a\cdot c$, con $c = (-1)^{n+1} b \in A$.

A partir de ahora, en esta sección, K será un cuerpo de números y A el anillo de números de K.

23. Proposición: *Sea $a \in A$ no nulo y escribamos $(a)_0 = \{x_1,\dots,x_r\}$. Entonces,*

$$|N(a)| = \prod_i |A/\mathfrak{m}_{x_i}|^{v_{x_i}(a)}.$$

Demostración. Veamos primero que $|A/\mathfrak{m}_x^n| = |A/\mathfrak{m}_x|^n$: Sabemos que $\mathfrak{m}_x/\mathfrak{m}_x^2 = (\bar{t})$, luego $\mathfrak{m}_x^{n-1}/\mathfrak{m}_x^n = (\bar{t}^{n-1})$. Por tanto, $\mathfrak{m}_x^{n-1}/\mathfrak{m}_x^n \simeq A/\mathfrak{m}_x$. De la sucesión exacta

$$0 \to \mathfrak{m}_x^{n-1}/\mathfrak{m}_x^n \to A/\mathfrak{m}_x^n \to A/\mathfrak{m}_x^{n-1} \to 0$$

concluimos que

$$|A/\mathfrak{m}_x^n| = |A/\mathfrak{m}_x^{n-1}| \cdot |\mathfrak{m}_x^{n-1}/\mathfrak{m}_x^n| = |A/\mathfrak{m}_x^{n-1}| \cdot |A/\mathfrak{m}_x| = |A/\mathfrak{m}_x^{n-2}| \cdot |A/\mathfrak{m}_x| \cdot |A/\mathfrak{m}_x|$$
$$= \cdots = |A/\mathfrak{m}_x| \cdot \overset{n}{\cdots} \cdot |A/\mathfrak{m}_x| = |A/\mathfrak{m}_x|^n.$$

Por otra parte, $(a) = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, con $n_i = v_{x_i}(a)$ y $A/(a) = A/\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r} = \prod_i A/\mathfrak{m}_x^{n_i}$, por el teorema chino de los restos. Por tanto,

$$|N(a)| = |A/(a)| = |\prod_i A/\mathfrak{m}_{x_i}^{n_i}| = \prod_i |A/\mathfrak{m}_{x_i}|^{n_i}.$$

□

Veamos que la noción de norma de un elemento $f \in K$ se puede extender a la noción de norma de un ideal fraccionario.

24. Definición: Dado un ideal fraccionario $I = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$ de K definimos la norma de I, que denotamos $N(I)$, como el número racional positivo

$$N(I) := \prod_i |A/\mathfrak{m}_{x_i}|^{n_i}.$$

Evidentemente, N: {Ideales fraccionarios de K} $\to \mathbb{Q}^*$ es un morfismo de grupos.

25. Proposición: *Dado un ideal $\mathfrak{a} \subset A$ no nulo, se cumple que $N(\mathfrak{a}) = |A/\mathfrak{a}|$.*

Demostración. Escribamos $\mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, entonces $A/\mathfrak{a} = \prod_i A/\mathfrak{m}_{x_i}^{n_i}$ y

$$|A/\mathfrak{a}| = \prod_i |A/\mathfrak{m}_{x_i}^{n_i}| = \prod_i |A/\mathfrak{m}_{x_i}|^{n_i} = N(\mathfrak{a}).$$

□

26. Proposición: *Dado $0 \neq f \in K$, se cumple que $N(fA) = |N(f)|$.*

Demostración. Dado $a \in A$, $|N(a)| \overset{3.3.20}{=} |A/aA| = N(aA)$. Escribamos $f = a/b$, $a, b \in A$. Entonces, $(f) \cdot (b) = (a)$ y

$$N((f)) = N((a))/N((b)) = |N(a)/N(b)| = |N(f)|.$$

□

27. Proposición: *Dados dos ideales fraccionarios $I' \subseteq I$, se cumple que*

$$N(I') = N(I) \cdot |I/I'|.$$

Demostración. Escribamos $I = \prod_i \mathfrak{m}_{x_i}^{n_i}$ e $I' = \prod_i \mathfrak{m}_{x_i}^{n_i'}$, donde $n_i' \geq n_i$ para todo i. Sea $\mathfrak{a} := \prod_i \mathfrak{m}_{x_i}^{n_i'-n_i} \subset A$. Entonces, $I' = I \cdot \mathfrak{a}$. Además, $I/I' \simeq A/\mathfrak{a}$ porque son $A/\mathfrak{a}$-módulos, $\operatorname{Spec} A/\mathfrak{a} = \{x_i\}$ y coinciden localmente, pues $(I/I')_{x_i} = (\mathfrak{m}_{x_i}^{n_i}/\mathfrak{m}_{x_i}^{n_i'})_{x_i} \simeq (A/\mathfrak{m}_{x_i}^{n_i'-n_i})_{x_i} = (A/\mathfrak{a})_{x_i}$. Entonces,

$$|I/I'| = |A/\mathfrak{a}| = N(\mathfrak{a}) = N(I')/N(I).$$

□

Si I es un ideal fraccionario de K, entonces es una red de $K \otimes_{\mathbb{Q}} \mathbb{R}$: I es un A-módulo finito generado sin torsión, entonces es un $\mathbb{Z}$-módulo finito generado sin torsión, luego $\mathbb{Z}$-libre. Sea $\{f_1, \ldots, f_n\}$ una $\mathbb{Z}$-base del $\mathbb{Z}$-módulo finito generado I, entonces $\{\frac{f_1}{1}, \ldots, \frac{f_n}{1}\}$ es una $\mathbb{Q}$-base de $I_{\mathbb{Z}\setminus\{0\}}$. Recordemos que $A_{\mathbb{Z}\setminus\{0\}} = K$ porque es una $\mathbb{Q}$-álgebra finita íntegra, luego es un cuerpo que contiene a A, por tanto es K. Entonces, $I_{\mathbb{Z}\setminus\{0\}}$ es un K-submódulo de K, por tanto es igual a K. En conclusión, $\{f_1, \ldots, f_n\}$ es una $\mathbb{Q}$-base de K, luego $\{f_1 \otimes 1, \ldots, f_n \otimes 1\}$ es una $\mathbb{R}$-base de $K \otimes_{\mathbb{Q}} \mathbb{R}$ y

$$I = \mathbb{Z} \cdot f_1 \oplus \cdots \oplus \mathbb{Z} \cdot f_n = \mathbb{Z} \cdot (f_1 \otimes 1) \oplus \cdots \oplus \mathbb{Z} \cdot (f_n \otimes 1) \subset \mathbb{R} \cdot (f_1 \otimes 1) \oplus \cdots \oplus \mathbb{R} \cdot (f_n \otimes 1) = K \otimes_{\mathbb{Q}} \mathbb{R}$$

Recordemos que $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$ y que $\sqrt{|\Delta_I|} = 2^s \cdot Vol(\mathbb{R}^n/I)$.

28. Proposición: *Si I es un ideal fraccionario, entonces*

$$\boxed{N(I) = \frac{\sqrt{|\Delta_I|}}{\sqrt{|\Delta_A|}} = \frac{Vol(\mathbb{R}^n/I)}{Vol(\mathbb{R}^n/A)}}$$

Demostración. Si tenemos una inclusión de ideales fracccionarios $I' \subseteq I$, recordemos que $N(I') = |I/I'| \cdot N(I)$ y que $\sqrt{|\Delta_{I'}|} = |I/I'| \cdot \sqrt{|\Delta_I|}$. Por tanto,

$$\frac{N(I')}{\sqrt{|\Delta_{I'}|}} = \frac{|I/I'| \cdot N(I)}{|I/I'| \cdot \sqrt{|\Delta_I|}} = \frac{N(I)}{\sqrt{|\Delta_I|}}.$$

Sean $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideales tales que $I = \mathfrak{a} \cdot \mathfrak{b}^{-1}$ (luego, $\mathfrak{a} \subseteq I$ y $\mathfrak{a} \subseteq A$). Entonces,

$$\frac{N(I)}{\sqrt{|\Delta_I|}} = \frac{N(\mathfrak{a})}{\sqrt{|\Delta_{\mathfrak{a}|}}} = \frac{N(A)}{\sqrt{|\Delta_A|}} = \frac{1}{\sqrt{|\Delta_A|}}.$$

□

3.4. Apéndice: Variedades proyectivas

1. Definición: Sea R un anillo y supongamos que como grupo, con la operación $+$, es suma directa de subgrupos R_i, con $i \in \mathbb{Z}$. Diremos que el anillo $R = \bigoplus_{n \in \mathbb{Z}} R_n$ es un álgebra graduada, si para cada $r_i \in R_i$ y $r_j \in R_j$, entonces $r_i \cdot r_j \in R_{i+j}$. Diremos que $r_i \in R_i$ es un elemento homogéneo de grado i.

Observemos que R_0 es un subanillo de R.

2. Definición: Sea $R = \underset{n\in\mathbb{Z}}{\oplus} R_n$ un álgebra graduada. Diremos que un ideal $I \subset R$ de un álgebra graduada es homogéneo, si está generado por elementos homogéneos.

3. Ejercicio: Prueba que un ideal $I \subseteq R$ es homogéneo si y solo si $I = \underset{n}{\oplus} I_n$, siendo $I_n = I \cap R_n$. Es decir, I es homogéneo si cumple que $f = f_n + f_{n+1} + \cdots + f_m \in I$ (con $f_i \in R_i$, para todo i) si y solo si $f_i \in I$ para todo i.

4. Ejercicio: Prueba que un ideal homogéneo $\mathfrak{p} \subseteq R$ es primo si y solo si cumple que si el producto de dos elementos homogéneos pertenece a $\mathfrak{p}$ entonces uno de los dos pertenece a $\mathfrak{p}$.

5. Definición: Llamaremos ideal irrelevante de R al ideal $(\underset{n\neq 0}{\oplus} R_n) \subseteq R$.

6. Definición: Llamaremos espectro proyectivo de R, y lo denotaremos $\mathrm{Proj}R$, al conjunto de ideales primos homogéneos de R que no contienen al ideal irrelevante.

Evidentemente $\mathrm{Proj}R \subset \mathrm{Spec}R$. Consideraremos $\mathrm{Proj}R$ como espacio topológico con la topología inicial heredada de la topología de Zariski de $\mathrm{Spec}R$. Si denotamos $(f)_0^h = \{x \in \mathrm{Proj}R, f \in \mathfrak{p}_x\}$ y escribimos $f = f_n + f_{n+1} \cdots + f_m$, es obvio que $(f)_0^h = (f_n, \ldots, f_m)_0^h = (f_n)_0^h \cap \cdots \cap (f_m)_0^h$. Por tanto, una base de cerrados de la topología de $\mathrm{Proj}R$ son los cerrados $(f)_0^h$, con $f \in R$ homogéneo, y una base de abiertos de la topología de $\mathrm{Proj}R$ son los abiertos

$$U_f^h = \{x \in \mathrm{Proj}R, f \notin \mathfrak{p}_x\}, \ \ (f \text{ homogéneo}).$$

7. Definición: Llamaremos espacio proyectivo de dimensión n (sobre k) a

$$\mathbb{P}_k^n = \mathrm{Proj}\, k[x_0, \ldots, x_n]$$

.

8. Definición: Diremos que un morfismo de álgebras $\phi\colon R \to R'$ graduadas es un morfismo graduado (de grado r) si transforma funciones homogéneas de grado n en funciones homogéneas de grado nr, para todo $n \in \mathbb{Z}$.

Si $\phi\colon R \to R'$ es un morfismo graduado entonces el morfismo inducido $\phi^*\colon \mathrm{Spec}R' \to \mathrm{Spec}R$, aplica ideales primos homogéneos en ideales primos homogéneos. Si suponemos que la imagen del ideal irrelevante de R por ϕ, no está contenido en más ideal primo homogéneo que los que contengan al irrelevante de R', tenemos definido un morfismo

$$\phi^*\colon \mathrm{Proj}R' \to \mathrm{Proj}R, x \mapsto \phi^*(x), \text{ donde } \mathfrak{p}_{\phi*(x)} = \phi^{-1}(\mathfrak{p}_x).$$

9. Ejemplo : Sea $\phi\colon k[x_0,x_1,x_2]\to k[x_0,x_1,x_2]$, $\phi(x_i)=\sum_j \lambda_{ij}x_j$, de modo que $\det(\lambda_{ij})\neq 0$. Entonces ϕ es un isomorfismo graduado, que induce un isomorfismo $\phi^*\colon \mathbb{P}^2\to\mathbb{P}^2$. Diremos que ϕ es un cambio de coordenadas homogéneo.

10. Proposición : *Si I es un ideal homogéneo de R entonces R/I es un álgebra, de modo que el morfismo $R\to R/I$ es un morfismo graduado que induce un isomorfismo*

$$\operatorname{Proj}(R/I)=(I)_0^h.$$

Si $f_m\in R$ es un elemento homogéneo de grado m, entonces R_{f_m} es una álgebra graduada, diciendo que el grado de $\frac{g_n}{f_m^r}$ es $n-mr$, para cada $g_n\in R_n$. Dejamos que el lector demuestre la siguiente proposición.

11. Proposición: *El morfismo de localización $R\to R_f$ (f homogénea) es un morfismo graduado que induce un isomorfismo*

$$\operatorname{Proj}R_f=U_f^h.$$

12. Proposición : *Sea R un álgebra graduada y $f\in R$ un elemento homogéneo de grado* 1. *Entonces,*

$$U_f^h=\operatorname{Proj}R_f=\operatorname{Spec}[R_f]_0.$$

Demostración. Veamos que la composición de los morfismos naturales

$$\operatorname{Proj}R_f\hookrightarrow\operatorname{Spec}R_f\to\operatorname{Spec}[R_f]_0,$$

que asigna a cada ideal primo homogéneo $\mathfrak{p}\subset R_f$ el ideal primo $[\mathfrak{p}]_0:=\mathfrak{p}\cap[R_f]_0$, es el homeomorfismo buscado. Observemos que el ideal primo $\mathfrak{p}\subset R_f$ está determinado por sus elementos homogéneos de grado cero: un elemento homogéneo $g\in R_f$ de grado m pertenece a $\mathfrak{p}$ si y solo si g/f^m pertenece a $[\mathfrak{p}]_0$. Por tanto, $\operatorname{Proj}R_f\to\operatorname{Spec}[R_f]_0$ es inyectivo. Observemos que $R_f=\oplus_{n\in\mathbb{Z}}[R_f]_0\cdot f^n$. Si $\mathfrak{q}\subset[R_f]_0$ es un ideal primo, entonces el ideal homogéneo $\mathfrak{p}:=\oplus_{n\in\mathbb{Z}}\mathfrak{q}\cdot f^n\subset R_f$ es un ideal primo homogéneo: Si $g,g'\in R_f$ son dos elementos homogéneos de grados m y m' respectivamente, tales que $g\cdot g'\in\mathfrak{p}$, entonces $(g/f^m)\cdot(g'/f^{m'})=(gg')/f^{m+m'}\in\mathfrak{q}$, luego g/f^m ó $g'/f^{m'}$ pertenece a $\mathfrak{q}$, y por tanto g ó g' pertenece a $\mathfrak{p}$. Observemos $\mathfrak{p}\cap[R_f]_0=\mathfrak{q}$. En conclusión, $\operatorname{Proj}R_f\to\operatorname{Spec}[R_f]_0$ es biyectivo. Finalmente, si $g\in R$ es homogénea de grado m, la biyección anterior transforma $(g)_0^h=(g/f^m)_0^h$ en $(g/f^m)_0$. Luego la biyección continua dada es un homeomorfismo. □

Por sencillez, supondremos a partir de ahora que $R=R_0[\xi_0,\ldots,\xi_n]$, donde cada ξ_i es de grado 1. Con esta hipótesis, $[R_0[\xi_0,\ldots,\xi_n]_{\xi_i}]_0=R_0[\xi_0/\xi_i,\ldots,\xi_n/\xi_i]$, donde entendemos por $R_0[\xi_0/\xi_i,\ldots,\xi_n/\xi_i]$ la R_0-subálgebra de $R_0[\xi_0,\ldots,\xi_n]_{\xi_i}$ generada por $\xi_0/\xi_i,\ldots,\xi_n/\xi_i$.

13. Teorema: *Sea* $R = R_0[\xi_0,\dots,\xi_n]$. *Sean* $U_i := \mathrm{Proj}R\setminus(\xi_i)_0^h$. *Entonces,*

1. $\mathrm{Proj}R = \bigcup_{i=0}^{n} U_i$.
2. U_i *es homeomorfo a* $\mathrm{Spec}R_0[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$.

Diremos que U_i *es un abierto afín de* $\mathrm{Proj}R$. *Por tanto, el espectro proyectivo admite un recubrimiento por abiertos afines.*

Demostración. 1. $\mathrm{Proj}R = \bigcup_{i=0}^{n} U_i$, ya que $\bigcap_{i=0}^{n}(\xi_i)_0^h = (\xi_0,\dots,\xi_n)_0^h = \emptyset$, pues $(\xi_0,\dots,\xi_n)$ es el ideal irrelevante.

2. Es consecuencia de la proposición 3.4.12.

□

14. Definición: Llamaremos variedad proyectiva (sobre k) al espectro proyectivo de un álgebra graduada del tipo $k[\xi_0,\dots,\xi_n] = k[x_0,\dots,x_n]/I$, siendo I un ideal homogéneo. Es decir, una variedad proyectiva es un cerrado del espacio proyectivo $\mathbb{P}^n$. Si además es de dimensión 1, diremos que es una curva proyectiva.

15. Ejercicio: 1. Demuestra que el epimorfismo $\mathbb{C}[x_0,x_1,x_2] \to \mathbb{C}[x_0,x_1,x_2]/(x_0^2+x_1^2+x_2^2)$ define una inmersión cerrada $\mathrm{Proj}\,\mathbb{C}[x_0,x_1,x_2]/(x_0^2+x_1^2+x_2^2) \hookrightarrow \mathbb{P}^2$

2. Escribe las ecuaciones de la curva proyectiva plana

$$\mathrm{Proj}\,\mathbb{C}[x_0,x_1,x_2]/(x_0^2+x_1^2+x_2^2)$$

en cada uno de los abiertos "afines", complementario del cerrado $(x_i)_0^h$ ("deshomogeneiza $x_0^2+x_1^2+x_2^2$ por cada variable x_i").

3. Define una curva proyectiva plana que en uno de los abiertos afines sea la curva plana "afín" $y+x^2=0$. ¿Corta la recta $x=0$, a la curva $y+x^2=0$, en algún punto del "infinito"?

3.4.1. Espacio tangente en un punto

El espacio tangente a una variedad diferenciable en un punto es un concepto intrínseco, que no depende de la inmersión de la variedad diferenciable en un $\mathbb{R}^n$. El espacio tangente a una variedad en un punto se define en términos de su anillo de funciones diferenciables. Ya sabemos que la diferencial de una función en un punto y los módulos de diferenciales de Kähler son conceptos algebraicos. En esta sección, dado un anillo local, definiremos el espacio tangente en el punto cerrado.

Comencemos con un ejemplo sencillo. Consideremos el nodo, es decir, la curva plana $y^2-x^2+x^3=0$. El espacio tangente en el origen del nodo es aquella variedad homogénea que mejor se aproxima al nodo. El nodo "infinitesimalmente" en el origen es

equivalente a $y^2 - x^2 = 0$. Así pues, diremos que el cono tangente a $y^2 - x^2 + x^3 = 0$ en el origen es $y^2 - x^2 = 0$. En general, si una subvariedad $X \subset \mathbb{A}_n$, viene definida por los ceros de un ideal $I \subset k[x_1, \ldots, x_n]$, entonces el cono tangente C_0X en el origen es la variedad definida por el ideal $I_h = (f_r)_{f \in I}$, donde f_r es la parte homogénea de grado más pequeño de f. Es decir, si pensamos que X es la intersección de las variedades $f = 0$, con $f \in I$, entonces el cono tangente es la intersección de las variedades homogéneas $f_r = 0$.[2]

Veamos cómo construir I_h. Sea $\mathfrak{m}_0 = (x_1, \ldots, x_n) \subset k[x_1, \ldots, x_n]$ y $\bar{\mathfrak{m}}_0 \subset k[x_1, \ldots, x_n]/I$ el ideal maximal de las funciones de X que se anulan en el origen. Se tiene la sucesión exacta $I \cap \mathfrak{m}_0^r \to \mathfrak{m}_0^r \to \bar{\mathfrak{m}}_0^r \to 0$ y por tanto la sucesión exacta

$$I \cap \mathfrak{m}_0^r \to \mathfrak{m}_0^r/\mathfrak{m}_0^{r+1} \to \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1} \to 0$$

En conclusión,

$$\bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1} = \{\text{Polinomios } p(x_1, \ldots, x_n) \text{ homogéneos de grado } r\}/\{f_r\}_{f = f_r + \ldots + f_n \in I}$$

Por tanto, $\oplus_r \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1} = k[x_1, \ldots, x_n]/I_h$. Entonces, $\operatorname{Spec}(\bigoplus_{r=0}^{\infty} \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1})$ es el cono tangente de X en el origen y $\operatorname{Proj}(\bigoplus_{r=0}^{\infty} \bar{\mathfrak{m}}_0^r/\bar{\mathfrak{m}}_0^{r+1})$ es el espacio tangente de X en el origen.

Demos ahora las definiciones con toda precisión y mayor generalidad.

16. Definición: Sea $X = \operatorname{Spec} A$ y $x \in X$ un punto cerrado de ideal $\mathfrak{m}$. Llamaremos cono tangente de X en x a

$$C_xX = \operatorname{Spec} G_{\mathfrak{m}}A := \operatorname{Spec} \bigoplus_{i=0}^{\infty} \mathfrak{m}^i/\mathfrak{m}^{i+1}.$$

Llamaremos vértice del cono al punto de C_xX definido por el ideal (maximal) irrelevante $\bigoplus_{r>0} \mathfrak{m}^r/\mathfrak{m}^{r+1}$. Llamaremos espacio tangente de X en x a

$$T_xX := \operatorname{Proj} G_{\mathfrak{m}}A.$$

17. Ejemplo: El cono tangente de un espacio afín en el origen es isomorfo al espacio afín. Es decir, si $A = k[x_1, \ldots, x_n]$ y $\mathfrak{m} = (x_1, \ldots, x_n)$, entonces $G_{\mathfrak{m}}A \simeq A$.

18. Proposición: *Sea $I \subset A$ un ideal y $f \in I^r \setminus I^{r+1}$. Denotemos f_r la clase de f en $I^r/I^{r+1} \subset G_IA$. Si f_r es no divisor de cero en G_IA, entonces*

1. $(f) \cap I^n = f \cdot I^{n-r}$, *para* $n \geq r$.

[2] Advertamos que debemos tomar todas las $f \in I$ y que no basta con tomar cualquier sistema generador.

2. $G_{\bar{I}}(A/(f)) = (G_I A)/(f_r)$*, donde* $\bar{I}$ *es el ideal* I *en* $A/(f)$*.*

Demostración. 1. Es claro que $f \cdot I^{n-r} \subseteq (f) \cap I^n$. Probemos la inclusión inversa. Si $h \in (f) \cap I^n$, entonces $h = f \cdot g$, con $g \in A$. Sea $s \geq 0$ el máximo tal que $g \in I^s$. Tenemos que ver que $s \geq n - r$. Escribamos $0 \neq g_s = \bar{g} \in I^s/I^{s+1}$. Por hipótesis, $0 \neq f_r \cdot g_s \in I^{r+s}/I^{r+s+1}$, luego $h = f \cdot g \notin I^{r+s+1}$. Por tanto, $n < r + s + 1$, es decir, $s \geq n - r$.

2. El núcleo del epimorfismo $I^n/I^{n+1} \to \bar{I}^n/\bar{I}^{n+1}$ es

$$(I^n \cap (I^{n+1} + (f))/I^{n+1} = (I^{n+1} + I^n \cap (f))/I^{n+1} \overset{1.}{=} (I^{n+1} + f \cdot I^{n-r})/I^{n+1}.$$

Luego la sucesión

$$0 \to I^{n-r}/I^{n-r+1} \xrightarrow{f\cdot = f_r \cdot} I^n/I^{n+1} \to \bar{I}^n/\bar{I}^{n+1} \to 0$$

es exacta, y $G_{\bar{I}}(A/(f)) = (G_I A)/(f_r)$.

□

19. Ejercicio: Escribamos el polinomio $p(x,y) = p_n(x,y) + p_{n+1}(x,y) + \ldots + p_m(x,y)$ como suma de polinomios homogéneos. Sea $\mathcal{O} = (k[x,y]/p(x,y))_{x_0}$, con $\mathfrak{m}_{x_0} = (x,y)$. Demuestra que $G_{\mathfrak{m}_{x_0}}\mathcal{O} = k[x,y]/(p_n(x,y))$.

20. Ejercicio: Prueba que el espacio tangente de la intersección de dos hipersuperficies transversales es la intersección de los espacios tangentes. Es decir, considérese el espacio afín $\mathbb{A}_3 = \operatorname{Spec} k[x_1,x_2,x_3]$ y las superficies $f_1(x_1,x_2,x_3) = 0$, $f_2(x_1,x_2,x_3) = 0$. Sea $\mathfrak{m} = (x_1,x_2,x_3)$, y $f_{1,n}$, $f_{2,m}$ las componentes homogéneas de grado mínimo de f_1, f_2. Supongamos que no existen polinomios irreducibles que dividan a $f_{1,n}$ y $f_{2,m}$ (es decir, $f_{2,m}$ no es divisor de cero en $G_{\mathfrak{m}}(k[x_1,x_2,x_3]/(f_1)) = k[x_1,x_2,x_3]/(f_{1,n})$). Prueba que

$$G_{\mathfrak{m}}(k[x_1,x_2,x_3]/(f_1,f_2)) \simeq k[x_1,x_2,x_3]/(f_{1,n},f_{2,m})$$

21. Definición: Sea A un anillo, $X = \operatorname{Spec} A$ y $x \in X$ un punto cerrado. Diremos que $\tilde{X} := \operatorname{Proj}(A \oplus \mathfrak{m}_x \oplus \mathfrak{m}_x^2 \oplus \cdots)$ es la explosión de X en x y el morfismo natural

$$\tilde{X} = \operatorname{Proj}(A \oplus \mathfrak{m}_x \oplus \mathfrak{m}_x^2 \oplus \cdots) \to X$$

el morfismo de explosión en x.

22. Proposición: *Sea* $X = \operatorname{Spec} A$ *y* $\pi\colon \tilde{X} \to X$ *el morfismo de explosión en un punto cerrado* x*. Se cumple que*

1. $\pi^{-1}(X \setminus x) \overset{\pi}{=} X \setminus x$*.*

2. $\pi^{-1}(x) = T_x X$*. "La fibra de* x *es igual al espacio tangente de* X *en* x*".*

Demostración. 1. Sea $\mathfrak{m}_x$ el maximal correspondiente a x. Consideremos el morfismo $A \to (A \oplus \mathfrak{m}_x \oplus \mathfrak{m}_x^2 \oplus \cdots)$. Dado $\xi \in \mathfrak{m}_x$, tenemos que

$$\begin{aligned}\pi^{-1}(U_\xi) &= \operatorname{Proj}(A \oplus \mathfrak{m} \oplus \cdots)_\xi = \operatorname{Proj}(A_\xi \oplus \mathfrak{m}_\xi \oplus \cdots) \\ &= \operatorname{Proj}(A_\xi \oplus A_\xi \oplus \cdots) = \operatorname{Proj} A_\xi[t] = \operatorname{Spec} A_\xi = U_\xi.\end{aligned}$$

Recubriendo $X \backslash x$ por abiertos del tipo U_ξ obtenemos el punto 1.

2. Por ser x cerrado

$$\pi^{-1}(x) = \operatorname{Proj}\left[(A \oplus \mathfrak{m}_x \oplus \mathfrak{m}_x^2 \oplus \cdots) \otimes_A A/\mathfrak{m}_x\right] = \operatorname{Proj} G_{\mathfrak{m}_x} A = T_x X.$$

□

3.4.2. Desingularización por explosiones

Sea A un anillo de números o el anillo de funciones algebraicas de una curva algebraica íntegra. Sea $x \in \operatorname{Spec} A$ un punto cerrado, denotemos $\mathcal{O} = A_x$, $\bar{\mathcal{O}} = \bar{A}_x$ y $\mathfrak{m} = \mathfrak{m}_x \mathcal{O}$.

Consideremos la inclusión $i\colon \mathcal{O} \hookrightarrow \bar{\mathcal{O}}$ y el morfismo inducido $i^*\colon \operatorname{Spec}\bar{\mathcal{O}} \to \operatorname{Spec}\mathcal{O}$. Escribamos $\operatorname{Spec}_{\max}\bar{\mathcal{O}} = \{\mathfrak{m}_{x_1}, \ldots, \mathfrak{m}_{x_r}\} = i^{*-1}(\mathfrak{m})$. $\bar{\mathcal{O}}$ es un dominio de ideales principales, porque es un dominio de Dedekind con solo un número finito de ideales primos. Entonces $\mathfrak{m} \cdot \bar{\mathcal{O}} = (f)$. Supongamos que $f \in \mathfrak{m}$.

Escribamos $\mathfrak{m} = (\xi_1, \ldots, \xi_n)$. Como $\mathfrak{m} \cdot \bar{\mathcal{O}} = f \cdot \bar{\mathcal{O}}$, tenemos que $\xi_i/f \in \bar{\mathcal{O}}$. Consideremos el anillo

$$\mathcal{O}_1 := \mathcal{O}[\xi_1/f, \ldots, \xi_n/f] \subseteq \bar{\mathcal{O}}.$$

Tenemos que $\mathcal{O}_1$ contiene a $\mathcal{O}$ y $\mathfrak{m} \cdot \mathcal{O}_1 = f \cdot \mathcal{O}_1$. Por tanto, si x es no singular entonces $\mathcal{O}_1$ contiene estrictamente a $\mathcal{O}$. Si $f' \in \mathfrak{m}$ cumple también que $\mathfrak{m} \cdot \bar{\mathcal{O}} = f'\bar{\mathcal{O}}$, entonces $\mathcal{O}[\xi_1/f, \ldots, \xi_n/f] = \mathcal{O}[\xi_1/f', \ldots, \xi_n/f']$: f'/f es un invertible de $\bar{\mathcal{O}}$, porque $f\bar{\mathcal{O}} = f'\bar{\mathcal{O}}$, luego f'/f es invertible en $\mathcal{O}[\xi_1/f, \ldots, \xi_n/f]$ porque si perteneciese a algún ideal primo así sucedería también en $\bar{\mathcal{O}}$. Luego,

$$\mathcal{O}[\xi_1/f, \ldots, \xi_n/f] = \mathcal{O}[\xi_1/f, \ldots, \xi_n/f]_{f'/f} = \mathcal{O}[\xi_1/f', \ldots, \xi_n/f']_{f/f'} = \mathcal{O}[\xi_1/f', \ldots, \xi_n/f'].$$

23. Definición: Si $f \in \mathfrak{m}_x$ cumple que $\mathfrak{m} \cdot \bar{\mathcal{O}} = (f)$ diremos que f es un parámetro transversal a $\operatorname{Spec}\mathcal{O}$ en x. Diremos que $\mathcal{O}_1 = \mathcal{O}[\xi_1/f, \ldots, \xi_n/f]$ es el anillo de la explosión de $\operatorname{Spec}\mathcal{O}$ en x.

24. Proposición: *Supongamos x singular y sea $f \in \mathfrak{m}_x$ un parámetro transversal a* $\operatorname{Spec}\mathcal{O}$ *en x. Entonces,*

$$\mathcal{O}_1 = \mathcal{O}[\xi_1/f, \ldots, \xi_n/f],$$

contiene estrictamente a $\mathcal{O}$ y está incluido en $\bar{\mathcal{O}}$.

Por sucesivas explosiones en puntos singulares podemos obtener la desingularización.[3]

Veamos qué es $\operatorname{Spec}\mathscr{O}_1$ geométricamente. Consideremos el anillo graduado

$$\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots.$$

Dado $\xi\in\mathfrak{m}$ considerado como elemento de grado uno de este anillo lo denotaremos $\tilde{\xi}$. Tenemos que $\mathscr{O}[\xi_1/f,\dots,\xi_n/f]=\left[(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)_{\tilde{f}}\right]_0$, $\xi_i/f\mapsto\tilde{\xi}_i/\tilde{f}$ es un isomorfismo. Veamos que $(\tilde{f})_0^h=\emptyset$: El morfismo $\mathscr{O}[\tilde{\xi}_1,\dots,\tilde{\xi}_n]=\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots\to\bar{\mathscr{O}}\oplus\mathfrak{m}\cdot\bar{\mathscr{O}}\oplus\mathfrak{m}^2\cdot\bar{\mathscr{O}}\oplus\cdots=\bar{\mathscr{O}}[\tilde{\xi}_1,\dots,\tilde{\xi}_n]$ es finito. Por tanto, el morfismo

$$\operatorname{Spec}\bar{\mathscr{O}}=\operatorname{Proj}(\bar{\mathscr{O}}\oplus\mathfrak{m}\cdot\bar{\mathscr{O}}\oplus\mathfrak{m}^2\cdot\bar{\mathscr{O}}\oplus\cdots)\to\operatorname{Proj}(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)$$

es epiyectivo, de fibras finitas (de dimensión cero). Luego, dado $f'\in\mathfrak{m}$, se cumple que $(\tilde{f}')_0^h=\emptyset$ en $\operatorname{Proj}(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)$ si y solo si $(\tilde{f}')_0^h=\emptyset$ en $\operatorname{Proj}(\bar{\mathscr{O}}\oplus\mathfrak{m}\cdot\bar{\mathscr{O}}\oplus\mathfrak{m}^2\cdot\bar{\mathscr{O}}\oplus\cdots)$. El ideal $(\tilde{f})$ es el irrelevante, luego $(\tilde{f})_0^h=\emptyset$. Por tanto,

$$\operatorname{Proj}(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)=\operatorname{Proj}(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)-(\tilde{f})_0^h=\operatorname{Spec}\left[(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)_{\tilde{f}}\right]_0=\operatorname{Spec}\mathscr{O}_1$$

Es decir, $\operatorname{Spec}\mathscr{O}_1$ es la explosión de $\operatorname{Spec}\mathscr{O}$ en x.

Dado $f'\in\mathfrak{m}\cdot\bar{\mathscr{O}}$, se cumple que $(f')=\mathfrak{m}\cdot\bar{\mathscr{O}}$ si y solo si $(\tilde{f}')_0^h=\emptyset$: si escribimos $f'=f\cdot g$, tenemos que $\tilde{f}'=\tilde{f}\cdot g$ y $(\tilde{f}')_0^h=(\tilde{f}\cdot g)_0^h=(g)_0^h$ que será vacío si y solo si g es invertible, es decir, si y solo si $(f')=\mathfrak{m}\cdot\bar{\mathscr{O}}$.

Por la proposición 3.4.22, $\operatorname{Proj}(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)$ es la unión disjunta del punto genérico y $\operatorname{Proj}G_{\mathfrak{m}}\mathscr{O}$. Luego, $f'\in\mathfrak{m}$ cumple que $(\tilde{f}')_0^h=\emptyset$ en $\operatorname{Proj}(\mathscr{O}\oplus\mathfrak{m}\oplus\mathfrak{m}^2\oplus\cdots)$ si y solo si $(\overline{\tilde{f}'})_0^h=\emptyset$ en $\operatorname{Proj}G_{\mathfrak{m}}\mathscr{O}$.

Con todo, hemos demostrado que f es transversal a $\operatorname{Spec}\mathscr{O}$ en x si y solo si $(\overline{\tilde{f}})_0^h=\emptyset$ en $\operatorname{Proj}G_{\mathfrak{m}}\mathscr{O}$.

Escribamos $\operatorname{Proj}G_{\mathfrak{m}_x}\mathscr{O}=\{y_1,\dots,y_r\}$ y $\mathfrak{p}_{y_i}=\mathfrak{p}_{y_i,0}\oplus\mathfrak{p}_{y_i,1}\oplus\cdots\subset\mathscr{O}/\mathfrak{m}_x\oplus\mathfrak{m}_x/\mathfrak{m}_x^2\oplus\cdots$. Tenemos que $\mathfrak{p}_{y_i,1}\subsetneq\mathfrak{m}_x/\mathfrak{m}_x^2$, porque $\mathfrak{p}_{y_i}$ no contiene al ideal irrelevante. Supongamos que $|\mathscr{O}/\mathfrak{m}_x|=\infty$. Entonces, existe $\bar{f}\in\mathfrak{m}/\mathfrak{m}^2$ que no pertenece a ninguno de los $\mathfrak{p}_{y_i,1}$, por tanto, $\emptyset=(\overline{\tilde{f}})_0^h\subset\operatorname{Proj}G_{\mathfrak{m}}\mathscr{O}$. [4]

25. Ejemplo: Sea $p(x,y)=0$ una curva íntegra tal que el origen es un punto singular de multiplicidad k (es decir, $p(x,y)\in(x,y)^k\setminus(x,y)^{k+1}$). Supongamos que $p(0,y)=y^k\cdot q(y)$, con $q(0)\neq0$ (es decir, $x=0$ corta transversalmente a la curva en el origen). Tenemos que y/x es entero sobre el anillo $(\mathbb{C}[x,y]/(p(x,y)))_{q(y)}$, y que

$$(\mathbb{C}[x,y]/(p(x,y)))[y/x]=\mathbb{C}[x,y/x]/(r(x,y/x)),$$

[3] Podríamos haber partido de un anillo $\mathscr{O}$ con varios ideales maximales, es decir, $\operatorname{Spec}_{max}\mathscr{O}=\{x,z_1,\dots,z_n\}$, entonces definimos $\mathscr{O}_1=\mathscr{O}[\xi_1/f,\dots,\xi_n/f]$, donde f es transversal a $\operatorname{Spec}\mathscr{O}_x$ en x y $f(z_i)\neq0$ (es decir, $f\notin\mathfrak{m}_{z_i}$), para todo i.

[4] Si $|\mathscr{O}/\mathfrak{m}|<\infty$, se puede demostrar que existe $m>0$ y $\bar{f}\in\mathfrak{m}^m/\mathfrak{m}^{m+1}$, tal que $\emptyset=(\overline{\tilde{f}})_0^h\subset\operatorname{Proj}G_{\mathfrak{m}}\mathscr{O}$. En este caso, puede demostrarse que $\mathscr{O}_1=\mathscr{O}[\xi^\alpha/f]_{|\alpha|=m}$.

donde $x^k \cdot r(x, y/x) = p(x, y)$.

En efecto, escribamos $p(x,y) = p_k(x,y) + \cdots + p_n(x,y)$, con $p_r(x,y)$ homogéneo de grado r, para todo r. Entonces,

$$p(x,y)/x^k = p_k(1,y/x) + \cdots + p_n(1,y/x)x^{n-k} =: r(x,y/x)$$

Luego, $(\mathbb{C}[x,y]/(p(x,y)))[y/x] = \mathbb{C}[x,y/x]/(r(x,y/x))$. Además, si escribimos $p(x,y) = y^k q(y) + xp'(x,y)$, podemos escribir $p'(x,y)/x^{k-1}$ como un polinomio en y/x de grado menor o igual que $k-1$ con coeficientes polinomios en x e y. Por tanto, como $0 = r(x,y/x) = (y/x)^k q(y) + p'(x,y)/x^{k-1}$, tenemos que y/x es entero sobre $(\mathbb{C}[x,y]/(p(x,y)))_{q(y)}$.

26. Ejemplo: $\mathrm{Spec}\,\mathbb{C}[x,y]/(y^2 - x^3)$ es no singular en todo punto, salvo en el origen. Observemos que $x = 0$ es transversal a la curva en el origen y

$$(y/x)^2 - x = 0.$$

Por tanto, y/x es entero sobre $\mathbb{C}[x,y]/(y^2 - x^3)$. Luego,

$$(\mathbb{C}[x,y]/(y^2 - x^3))[y/x] = \mathbb{C}[x,y/x]/((y/x)^2 - x)$$

está incluido en el cierre entero de $\mathbb{C}[x,y]/(y^2 - x^3)$. Ahora bien, $\mathbb{C}[x,y/x]/((y/x)^2 - x)$ es no singular en todo punto, luego es el cierre entero de $\mathbb{C}[x,y]/(y^2 - x^3)$.

27. Ejemplo: Calculemos la desingularización de $\mathbb{Z}[\sqrt{n}]$. Si $n = m^2 \cdot n'$, entonces $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}[m\sqrt{n'}] \subseteq \mathbb{Z}[\sqrt{n'}]$ y la desingularización de $\mathbb{Z}[\sqrt{n}]$ coincide con la de $\mathbb{Z}[\sqrt{n'}]$. Así pues, podemos suponer que n carece de factores cuadráticos. $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}[x]/(x^2 - n)$ y $x^2 - n$ es separable módulo p, salvo para $p = 2$ y p divisor de n. Por tanto, los únicos puntos singulares posibles son $\mathfrak{m}_y = (p,x)$, con p divisor de n, y $\mathfrak{m}_y = (2, x+1)$ cuando n es impar. Observemos, en el primer caso, que que $(\mathbb{Z}[x]/(x^2 - n, x)_y = \mathbb{Z}/p\mathbb{Z}$, luego $\mathfrak{m}_y \cdot (\mathbb{Z}[x]/(x^2 - n, x))_y = (x)$ e y es no singular. Veamos qué sucede cuando $\mathfrak{m}_y = (2, x+1)$. Observemos que

$$d_y(x^2 - n) = d_y((x+1)^2 - 2\cdot(x+1) - 2\cdot\frac{n-1}{2}) = -(\frac{n-1}{2})d_y 2 = 0$$

si y solo si $\frac{n-1}{2}$ es par, es decir, $n = 1 \mod 4$. Por tanto, y es singular, si $n = 1 \mod 4$. Supongamos que ésta es la situación. Observemos que

$$(\frac{x+1}{2})^2 - \frac{x+1}{2} - \frac{n-1}{4} = 0.$$

Por tanto, $\frac{\sqrt{n}+1}{2}$ es entero sobre $\mathbb{Z}$, luego sobre $\mathbb{Z}[\sqrt{n}]$. Si A es el cierre entero de $\mathbb{Z}[\sqrt{n}]$, entonces A contiene a $\mathbb{Z}[\sqrt{n}, \frac{\sqrt{n}+1}{2}] = \mathbb{Z}[\frac{\sqrt{n}+1}{2}]$. Los únicos puntos singulares de $\mathbb{Z}[\frac{\sqrt{n}+1}{2}]$, están sobre la fibra de (2). Ahora bien, el polinomio $y^2 - y - \frac{n-1}{4}$, que anula a $\frac{\sqrt{n}+1}{2}$, es separable módulo 2. En conclusión, $\mathbb{Z}[\frac{\sqrt{n}+1}{2}]$ es no singular en todo punto y es igual al cierre entero de $\mathbb{Z}[\sqrt{n}]$.

28. Ejercicio: Sea $n \in \mathbb{Z}$, con $n \neq 0,1$ y sin factores cuadráticos. Demuestra que el discriminante de $K = \mathbb{Q}[\sqrt{n}]$ es n si $n \equiv 1 \mod 4$, y es $4n$ si $n \equiv 2,3 \mod 4$.

29. Ejercicio: Sea $n \in \mathbb{Z}$, con $n \neq 0,1$ y sin factores cuadráticos. Sea Δ el discriminante de $\mathbb{Q}[\sqrt{n}]$. Prueba que el anillo de números de $\mathbb{Q}[\sqrt{n}]$ es igual a $\mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$.

3.5. Cuestionario

1. Calcula en $\mathbb{Q}[i]$ la traza, norma y métrica de la traza.
2. Resuelve el ejercicio 3.3.3.
3. Calcula el discriminante, los puntos singulares y la desingularización de $\mathbb{Z}[\sqrt[3]{10}]$.
4. Consideremos $\mathbb{R}^3$ con el producto escalar estándar. Calcula el volumen del paralelepípedo definido por los vectores $(1,3,2),(1,2,1)$ y $(0,1,-1)$.
5. Sea $A = \mathbb{Z}[i] \subset \mathbb{C}$ y consideremos en la $\mathbb{R}$-álgebra $\mathbb{C}$ la métrica de la traza. Calcula $Vol(\mathbb{C}/A)$.
6. Sean I e I' ideales fraccionarios de un cuerpo de números. Prueba que
$$Vol(\mathbb{R}^r \times \mathbb{C}^s/II') = \frac{Vol(\mathbb{R}^r \times \mathbb{C}^s/I) \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/I')}{\sqrt{|\Delta_K|}}.$$
7. Resuelve el ejercicio 3.4.28.
8. Resuelve el ejercicio 3.4.29.
9. Calcula la desingularización de $\mathbb{C}[x,y]/(y^2 - x^2 + x^3)$.

3.6. Biografía de Heisuke Hironaka

HIRONAKA BIOGRAPHY:

Heisuke Hironaka's father ran a textile factory. This was not an occupation he wanted but he was forced into the family business when his father (Heisuke's paternal grandfather) died while he was still a schoolboy. Heisuke's mother was his father's third wife. After his first wife died, he remarried and had four children. However, his second wife then died and he married for the third time, to a younger sister of his second wife who, by this time, was widowed with one child. These five children comprised three boys and two girls. Heisuke's parents then had ten child-

ren of their own (six boys and four girls), so Heisuke grew up in a family of fifteen children. Of his parents' ten children, Heisuke was the second eldest having one older sister.

Two of Heisuke's half-brothers were killed, one fighting against the Americans and one fighting against the Chinese. Heisuke's father was devastated and as a consequence sold his textile factory and gave up work. Heisuke attended elementary school and then middle school where he began to develop a liking for mathematics. The town of Yamaguchi is about 80 km from Hiroshima and on Monday, 6 August 1945, at 8.15 in the morning, Heisuke's father witnessed the dropping of the atomic bomb on Hiroshima. They were fortunate that their area was not affected by the radiation. After middle school, Heisuke attended the boys' junior high school in Yanai. This meant that he had to take a 30 minute train journey to school every day. He started to learn to play the piano and became very keen but was advised by his teachers not to think of becoming a professional musician. After a mathematics professor from Hiroshima University gave a lecture at the junior high school, Heisuke became enthusiastic and applied to study mathematics at Hiroshima University. However he did not study for the entrance examination and failed. In the following year he applied to study physics at Kyoto University and was accepted. He was able to live with one of his sisters who had married and was living in Kyoto.

Kyoto University was founded in 1897 to train small numbers of selected students as academics. By the time Hironaka entered Kyoto University in 1949, it had been integrated into a mass higher education system but had maintained its prestige. In his first year Hironaka studied physics, chemistry and biology. In his second year, however, he began to realise that he was best suited to mathematics. By his third year as an undergraduate he had moved completely to courses in mathematics. Yasuo Akizuki, a pioneer of modern algebra in Japan, was a major influence on Hironaka during his time at Kyoto. He received his Bachelor of Science in 1954 and his Master of Science in 1956, both from Kyoto University. An important event happened in 1956 when Oscar Zariski visited Kyoto University:

When Zariski visited, I tried to tell him what I was doing. I have never been good in English! But my colleagues and teachers helped me to explain to him what I was doing. At some point Zariski said, "Maybe you can come to Harvard and study" And I said,"Okay."

Hironaka went to the United States in the summer of 1957 where he continued his studies at Harvard. He undertook research for his doctorate, with Oscar Zariski as his thesis advisor. While at Harvard, Hironaka became friends with Alexander Grothendieck who spent the academic year 1958-59 there. He invited Hironaka to the Institut des Hautes Etudes Scientifique in Paris in 1959-60 where he found himself the only visiting fellow. He was awarded a Ph.D. from Harvard in 1960 for his thesis On the Theory of Birational Blowing-up. He had already published three papers before submitting his thesis, On the arithmetic genera and the effective genera of algebraic curves (1957), A note on algebraic geometry over ground rings. The invariance of Hil-

bert characteristic functions under the specialization process (1958), and A generalized theorem of Krull-Seidenberg on parameterized algebras of finite type (1960). After completing his studies at Harvard, Hironaka was appointed to the staff at Brandeis University. Also in 1960 he married Wakako who was a Wien International Scholar at Brandeis University during 1958-60. She obtained an M.A. in Anthropology from Brandeis University Graduate School in 1964. Heisuke and Wakako Hironaka had one son Jo and one daughter Eriko. Wakako wrote several books, essays, translations, and critiques on education, culture, society, and women's issues. She entered Japanese politics being first elected to the House of Councillors in 1986. She has held high positions in the Democratic Party of Japan and in the Hosokawa Cabinet.

After being on the faculty at Brandeis University, Hironaka was appointed to Colombia University, and then to Harvard in 1968. In 1970 he had the distinction of being awarded a Fields Medal at the International Congress at Nice. This was for his work on algebraic varieties which we describe below.

Two algebraic varieties are said to be equivalent if there is a one-to-one correspondence between them with both the map and its inverse regular. Two varieties U and V are said to be birationally equivalent if they contain open sets U' and V' that are in biregular correspondence. Classical algebraic geometry studies properties of varieties which are invariant under birational transformations. Difficulties that arise as a result of the presence of singularities are avoided by using birational correspondences instead of biregular ones. The main problem in this area is to find a nonsingular algebraic variety U, that is birationally equivalent to an irreducible algebraic variety V, such that the mapping $f : U \to V$ is regular but not biregular.

Hironaka gave a general solution of this problem in any dimension in 1964 in Resolution of singularities of an algebraic variety over a field of characteristic zero. His work generalised that of Zariski who had proved the theorem concerning the resolution of singularities on an algebraic variety for dimension not exceeding 3. Jackson writes:

Taking a strikingly original approach, Hironaka created new algebraic tools and adapted existing ones suited to the problem. These tools have proved useful for attacking many other problems quite far removed from the resolution of singularities.

Hironaka talked about his solution in his lecture On resolution of singularities (characteristic zero) to the International Congress of Mathematicians in Stockholm in 1962.

In 1975 Hironaka returned to Japan where he was appointed a professor in the Research Institute for Mathematical Sciences of Kyoto University. He gave a course on the theory of several complex variables in 1977 and his lecture notes were written up and published in the book Introduction to analytic spaces (Japanese). Ikuo Kimura writes:

Some fundamental theorems in the theory of several complex variables and of the geometry of complex manifolds are proved in a simple but rigorous form. ... Throughout this book one recognizes again the importance of the preparation theorem,

and one finds good introductions to the study of the advanced theory of Stein spaces, the works of A Douady, and the theory of the resolution of singularities, to which Hironaka has contributed deeply.

Hironaka was Director of the Research Institute in Kyoto from 1983 to 1985, retiring in 1991 when he was made Professor Emeritus. However, in1996 he became president of Yamaguchi University, being inaugurated on 16 May. He held this position until 2002. He then became Academic Director of the University of Creation, a private university in Takasaki, Gunma, Japan.

We should also mention two educational projects which Hironaka has established. Jackson writes:

Hironaka has contributed much time and effort to encouraging young people interested in mathematics. In 1980, he started a summer seminar for Japanese high school students and later added one for Japanese and American college students; the seminars ran for more than two decades under his direction and continue to this day. To support the seminars he established a philanthropic foundation in 1984 called the Japan Association for Mathematical Sciences. The association also provides fellowships for Japanese students to pursue doctoral studies abroad.

Among the many honours he has received, in addition to the Fields Medal, we mention the Japan Academy Award in 1970 and the Order of Culture from Japan in 1975. He has been elected to the Japan Academy, the American Academy of Arts and Sciences and academies in France, Russia, Korea and Spain.

On 4-5 May 2009 the Clay Mathematics Institute held its 2009 Clay Research Conference in Harvard Science Center. Hironaka was invited to give one of the featured lectures on recent research advances and he spoke on Resolution of Singularities in Algebraic Geometry. The abstract for his talk reads:

I will present my way of proving resolution of singularities of an algebraic variety of any dimension over a field of any characteristic. There are some points of general interest, I hope, technically and conceptually more than just the end result. The resolution problem for all arithmetic varieties (meaning algebraic schemes of finite type over the ring of integers) is reduced to the question of how to extend the result from modulo p^m to modulo p^{m+1} after a resolution of singularities over $\mathbb{Q}$. I want to discuss certain problems which arise in this approach.

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

3.7. Problemas

1. Demuestra que $\Delta_{\mathbb{Z}[e^{\frac{2\pi i}{p^n}}]} = \pm p^{p^{n-1}\cdot(pn-n-1)}$, con p primo.

Resolución: Observemos que $x^{p^n}-1=(x^{p^{n-1}}-1)\cdot\phi_{p^n}(x)$. Entonces,

$$\Delta(x^{p^n}-1)=\prod_{\epsilon|\epsilon^{p^{n-1}}=1}\Phi_{p^n}(\epsilon)^2\cdot\Delta(x^{p^{n-1}}-1)\cdot\Delta(\Phi_{p^n}(x)).$$

$\Delta(x^{p^n}-1)=(-1)^{\binom{p^n}{2}}\cdot p^{n\cdot p^n}$ y $\Phi_{p^n}(x)=\Phi_p(x^{p^{n-1}})$ luego $\Phi_{p^n}(\epsilon)=\Phi_p(1)=p$.

2. *a*) Sean $T\colon E\to E$ y $S\colon E'\to E'$ dos endomorfismos k-lineales y sean $n=\dim_k E$, $m=\dim_k E'$. Prueba que $\det(T\otimes S)=\det(T)^m\cdot\det(S)^n$.

   b) Sean Γ y Γ' dos $\mathbb{Z}$-módulos libres de rangos n y m respectivamente. Sean T_2 y T_2' dos aplicaciones $\mathbb{Z}$-bilineales simétricas de Γ y Γ', respectivamente y sea $T_2\otimes T_2'$ la aplicación $\mathbb{Z}$-bilineal de $\Gamma\otimes_{\mathbb{Z}}\Gamma'$ definida por

   $$T_2\otimes T_2'(a\otimes a',b\otimes b'):=T_2(a,b)\cdot T_2'(a',b').$$

   Prueba que $\Delta_{\Gamma\otimes\Gamma'}=\Delta_\Gamma^m\cdot\Delta_{\Gamma'}^n$.

   c) Sean B y B' k-álgebras finitas separables y Tr_B y $\mathrm{Tr}_{B'}$ sus respectivas métricas de la traza. Prueba que $\mathrm{Tr}_B\otimes\mathrm{Tr}_{B'}$ es la métrica de la traza $\mathrm{Tr}_{B\otimes B'}$ de $B\otimes_k B'$.

   d) Sean K y K' dos cuerpos de números tales que $K\otimes_{\mathbb{Q}}K'=K''$ es un cuerpo. Sean A, A' y A'' los anillos de números de K,K' y K''. Si Δ_K y $\Delta_{K'}$ son primos entre sí, prueba que $A''=A\otimes_{\mathbb{Z}}A'$ y que $\Delta_{K''}=\Delta_K^{\dim_k K'}\cdot\Delta_{K'}^{\dim_k K}$.

   e) Prueba que $\Delta_{\mathbb{Q}[e^{2\pi i/pq}]}=p^{(p-2)(q-1)}\cdot q^{(q-2)(p-1)}$, con 2, p,q primos distintos.

   Resolución: a) $T\otimes S=(T\otimes\mathrm{Id})\circ(Id\otimes S)$ y es fácil comprobar que $\det(T\otimes\mathrm{Id})=\det(T)^m$ y $\det(\mathrm{Id}\otimes S)=\det(S)^n$.

   b) Sea $\{a_i\}$ una base de Γ y $\{b_r\}$ una base de Γ', luego una base de $\Gamma\otimes\Gamma'$ es $\{a_i\otimes b_r\}$. Si (a_{ij}) es la matriz asociada a T_2 y (b_{rs}) es la matriz asociada a T_2', entonces la matriz asociada a $T_2\otimes T_2'$ es $(a_{ij}\cdot b_{rs})$. Por *a*), $\Delta_{\Gamma\otimes\Gamma'}=\Delta_\Gamma^m\cdot\Delta_{\Gamma'}^n$.

   c) Sea $\bar{k}'$ el cierre algebraico de k, $\mathrm{Hom}_{k-alg}(B,\bar{k})=\{\sigma_i\}$ y $\mathrm{Hom}_{k-alg}(B',\bar{k})=\{\tau_r\}$, entonces $\mathrm{Hom}_{k-alg}(B\otimes_k B',\bar{k})=\{\sigma_i\otimes\tau_r\}$, luego

   $$\mathrm{tr}_{B\otimes B'}(b\otimes b')=\sum_{i,r}\sigma_i(b)\cdot\tau_r(b')=(\sum_i\sigma_i(b))\cdot(\sum_r\tau_r(b')=\mathrm{tr}_B(b)\cdot\mathrm{tr}_{B'}(b').$$

   Por tanto,

   $$\mathrm{Tr}_{B\otimes B'}(b\otimes b',c\otimes c')=\mathrm{tr}_{B\otimes B'}(bc\otimes b'c')=\mathrm{tr}_B(bc)\cdot\mathrm{tr}_{B'}(b'c')=\mathrm{Tr}_B(b,c)\cdot\mathrm{Tr}_{B'}(b'c').$$

   y $\mathrm{Tr}_{B\otimes B'}=\mathrm{Tr}_B\otimes\mathrm{Tr}_{B'}$.

   d) Si $A\to B$ es un morfismo de anillos finito y B es un A-módulo libre puede hablarse igualmente de $\mathrm{tr}\colon B\to A$, $\mathrm{Tr}\colon B\times B\to A$ y de $\Delta_{B/A}\in A$. Resulta que

el conjunto de los puntos rama del morfismo $A \to B$ es igual $(\Delta_{B/A})_0$. Si A es de Dedekind, se cumple igualmente que $\{\text{Puntos singulares de Spec}B\} \subset (\Delta_{B/A})_0$. En el caso que nos ocupa se cumple:

$$\{\text{Puntos singulares de Spec}A \otimes A'\} \subseteq (\Delta_{A\otimes A'/A})_0 \cap (\Delta_{A\otimes A'/A'})_0 = (\Delta_{A'})_0 \cap (\Delta_A)_0 = \emptyset.$$

Por último,

$$\begin{aligned}\Delta_{K''} = \Delta_{A\otimes A'} &= \det(\mathrm{Tr}_{A\otimes A'}) = \det(\mathrm{Tr}_A \otimes \mathrm{Tr}_{A'}) = \det(\mathrm{Tr}_A)^{\dim_k K'} \cdot \det(\mathrm{Tr}_{A'})^{\dim_k K} \\ &= \Delta_K^{\dim_k K'} \cdot \Delta_{K'}^{\dim_k K}.\end{aligned}$$

e) Recordemos que $\Delta_{\mathbb{Z}[e^{2\pi i/p}]} = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$ y aplíquese *d*).

3. Sean K y K' dos cuerpos de números y supongamos que $K'' = K \otimes_{\mathbb{Q}} K'$ es cuerpo. Sean A, A' y A'' los anillos de números de K, K' y K''. Sea $g = m.c.d.(\Delta_A, \Delta_{A'})$. Prueba que $A'' \subseteq \frac{1}{g} \cdot (A \otimes_{\mathbb{Z}} A')$.

   Resolución: Probemos que $A'' \subseteq \frac{1}{\Delta_A} \cdot (A \otimes_{\mathbb{Z}} A')$. Es un problema local en A'. Localizando, podemos suponer que A' es d.i.p. Entonces, $A'' \subseteq \frac{1}{\Delta_{A\otimes A'/A'}} \cdot (A \otimes_{\mathbb{Z}} A') = \frac{1}{\Delta_A} \cdot (A \otimes_{\mathbb{Z}} A')$. Por tanto,

$$A'' \subseteq \frac{1}{\Delta_A} \cdot (A \otimes_{\mathbb{Z}} A') \bigcap \frac{1}{\Delta_{A'}} \cdot (A \otimes_{\mathbb{Z}} A') = \frac{1}{g} \cdot (A \otimes_{\mathbb{Z}} A').$$

4. Prueba que si K es una $\mathbb{Q}$-extensión de Galois, entonces $\sqrt{\Delta_K} \in K$.

   Resolución: $\sqrt{\Delta_K} = \pm \cdot \det((\sigma_i(a_j))) \in K$.

5. Prueba que el discriminante de todo cuerpo de números es congruente con $0, 1$ mód 4.

   Pista: El determinante $\det((\sigma_i(a_j)))$, como todo determinante, es una suma de términos, cada uno afectado de un signo positivo o negativo. Sea P (resp. N) la suma de los términos afectados por el signo positivo (resp. la suma de los términos afectados por el signo negativo), entonces $\Delta = (P - N)^2 = (P+N)^2 - 4PN$ y $P + N, PN \in \mathbb{Z}$.

6. **Teorema de Brill:** Sea A un anillo de números de un cuerpo de números K y escribamos $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$. Se cumple que $\mathrm{sign}(\Delta_A) = (-1)^s$.

   Resolución: $\Delta_A = (-4)^s \cdot Vol(\mathbb{R}^{r+2s}/A)^2$.

7. Calcula el anillo de números de $\mathbb{Q}[\sqrt[3]{m}]$, donde $m \in \mathbb{Q}$.

   Resolución: Como $\mathbb{Q}[n\sqrt[3]{m}] = \mathbb{Q}[\sqrt[3]{m}]$ para todo $n \in \mathbb{Z}$, podemos suponer que $m \in \mathbb{Z}$. Podemos suponer además que m no es divisible por el cubo de ningún número

primo. Podemos suponer que $m = ab^2$, donde a y b son primos entre sí, y ninguno de los dos es divisible por el cuadrado de un primo.

Calculemos los puntos singulares de $A = \mathbb{Z}[x]/(x^3 - ab^2)$. Los números primos para los que $x^3 - ab^2$ y su derivada $3x^2$ tienen raíces comunes son 3 y los que dividen a ab^2. Además, $\Delta_A = 27ab^2$. Supongamos que el primo p divide a ab^2. Tenemos que comprobar si el ideal primo $\mathfrak{p}_y = (p, x)$ es singular y resulta que lo es si y solo si divide a b. En este caso, si dividimos por x^2, obtenemos

$$x - a(b/x)^2 = 0.$$

Luego, $ax - (ab/x)^2 = 0$ y tenemos que $x' := ab/x = x^2/b = \sqrt[3]{a^2 b}$ es entero. Efectivamente, verifica la ecuación $x'^3 - a^2 b = 0$ y $\mathbb{Z}[x']/(x'^3 - a^2 b)$ es no singular en (p, x'). Tenemos que $\mathbb{Z}[x, x'] \subset \mathbb{Q}[\sqrt[3]{m}]$ es no singular en todos los puntos que contengan a (p).

Supongamos que $p = 3$ y no divide a a ni a b. Cambiando a por $-a$, si es necesario, podemos suponer que $ab^2 = 1 \mod 3$. Cambiando b por $-b$, si es necesario, podemos suponer que $b = 1 \mod 3$ (luego $a = 1 \mod 3$). Tenemos que ver si $\mathfrak{p}_z = (3, x - 1)$ es un punto singular de $\mathbb{Z}[x]/(x^3 - ab^2)$. Observemos que

$$x^3 - ab^2 = (x-1)^3 + 3(x-1)^2 + 3(x-1) + 1 - ab^2 = 0.$$

Luego z es un punto singular si y solo si $1 - ab^2 = 0 \mod 9$ y esto ocurre si y solo si $a = b \mod 9$ (como puede comprobarse). Si $a \neq b \mod 9$, $\mathbb{Z} + \mathbb{Z}x + \mathbb{Z}x'$ es el anillo de números. Supongamos $a = b \mod 9$. Si dividimos por $(x-1)^2$, obtenemos

$$(x-1) + \frac{3}{x-1} \cdot x + (\frac{3}{x-1})^2 \cdot \frac{(1 - ab^2)}{9} = 0.$$

Luego, multiplicando por $\frac{(1-ab^2)}{9}$, obtenemos que $\frac{(1-ab^2)}{9} \cdot \frac{3}{x-1} = \frac{1-ab^2}{3(x-1)} = \frac{1-x^3}{3(x-1)} = \frac{1+x+x^2}{-3}$ es entero. Luego, $\mathbb{Z} + \mathbb{Z}x + \mathbb{Z}x' + \mathbb{Z}\frac{1+x+x^2}{3} = \mathbb{Z} + \mathbb{Z}x + \mathbb{Z}\frac{1+x+x'}{3}$ es el anillo de números.

8. Sea $K = \mathbb{Q}[\sqrt{-d}]$, donde d es un número natural, no divisible por ningún primo al cuadrado. Sea A el anillo de números de K. Prueba que A es un anillo euclídeo si y solo si $d = 1, 2, 3, 7, 11$.

Resolución: Si $d = 5, 6, 10$, el anillo de números de K es $\mathbb{Z}[\sqrt{-d}]$ y resulta que el ideal (2) no es un ideal primo. Pero 2 es irreducible porque $N(2) = 4$ y si $2 = (a + b\sqrt{-d})(c + e\sqrt{-d})$ tendríamos que $4 = (a^2 + db^2)(c^2 + de^2)$, lo que implica que $b = e = 0$ y a ó c igual a ± 1. En conclusión, A no es un dominio euclídeo.

Supongamos $d > 11$. $A \subseteq \mathbb{Z} \cdot 1/2 \oplus \mathbb{Z}\sqrt{-d}/2$. Sea $c = \frac{a+b\sqrt{-d}}{2} \in A$, tal que $N(c) = \frac{a^2+db^2}{4} \leq 3$. Entonces, $|a| \leq 3$ y $b = 0$. Luego, $c = \{0, 1, -1\}$. En particular, $A^* = \{1, -1\}$. Si (A, δ) fuese euclídeo, sea $f \in A \setminus \{0, 1, -1\}$ con $\delta(f)$ mínimo. Dado $a \in A$,

tendremos que $a = qf + r$, con $r = 0, 1, -1$. Es decir, $A/(f) = \{\bar{0}, \bar{1}, -\bar{1}\}$, luego $N(f) = |A/(f)| \leq 3$ y $f \in \{0, 1, -1\}$. Hemos llegado a contradicción.

Para $d = 1, 3, 7, 11$, el anillo de números de $\mathbb{Q}[\sqrt{-d}]$ es igual a $\mathbb{Z}[\frac{1-\sqrt{-d}}{2}]$, que es euclídeo con norma euclídea δ el valor absoluto de la norma, porque todo punto del paralelogramos definido por los vectores $\{1, \frac{1-\sqrt{-d}}{2}\}$ dista de alguno de los vértices menos de 1, y se puede argumentar como hacíamos con los enteros de Gauss.

El anillo de números de $\mathbb{Q}[\sqrt{-2}]$ es $\mathbb{Z}[\sqrt{-2}]$, que es euclídeo con norma euclídea el valor absoluto de la norma, porque todo punto del paralelogramos definido por los vectores $\{1, \sqrt{-2}\}$ dista de alguno de los vértices menos de 1, y se puede argumentar como hacíamos con los enteros de Gauss.

9. Sea $c \in \mathbb{N}$, $d = \dim_{\mathbb{Q}} K$ y A el anillo de números de K. Consideremos la acción natural por multiplicación de A^* en $\{f \in A : |N(f)| = c\}$. Prueba que

$$|\{f \in A : |N(f)| = c\}/A^*| \leq c^d.$$

"El número de $f \in A$, salvo multiplicación por invertibles, tales que $|N(f)| = c$ es menor o igual que c^d."

Resolución: Si $|N(f)| = |A/fA| = c$, entonces $c \cdot (A/fA) = 0$, es decir, $c \in fA$. Supongamos $|N(f)| = |N(f')| = c$. Si $\overline{f'} = \bar{f}$ en A/cA, entonces $f' = f + ce$, para cierto $e \in A$, luego $f' \in (f)$ e igualmente $f \in (f')$, es decir, $f' \in f \cdot A^*$. Por tanto, tenemos el morfismo inyectivo

$$\{f \in A : |N(f)| = c\}/A^* \hookrightarrow (A/cA), \bar{f} \mapsto \bar{f}.$$

Por último, A es un $\mathbb{Z}$-módulo libre de rango d, luego A/cA es un $\mathbb{Z}/c\mathbb{Z}$-módulo libre de rango d y $|A/cA| = c^d$.

10. Sea $c \in \mathbb{N}$ y A el anillo de números de un cuerpo de números. Pruébese que existe un número finito de ideales de A de norma c dada.

Solución: Sea $\mathfrak{a} \subset A$ tal que $N(\mathfrak{a}) = c$. Si $\mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, entonces $c = N(\mathfrak{a}) = \prod_i |A/\mathfrak{m}_{x_i}|^{n_i}$. Obviamente, $|A/\mathfrak{m}_{x_i}|, n_i \leq c$. Si considereramos el morfismo

$$\pi : \operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z},$$

inducido por el morfismo finito $\mathbb{Z} \to A$ y denotamos $\mathfrak{m}_{\pi(x_i)} = (p_i)$. Tenemos que $\mathbb{Z}/(p_i) \hookrightarrow A/\mathfrak{m}_{x_i}$, luego $p_i \leq c$. Es decir, los x_i están en la fibra de los ideales primos de $\mathbb{Z}$ generados por números primos menores que c.

11. Prueba que si un cuerpo de números K contiene alguna raíz imaginaria de la unidad, entonces $N(\alpha) > 0$, para todo $\alpha \in K^*$.

Resolución: Sea ξ la raíz imaginaria. Dado $\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})$ se cumple que $\sigma(K) \not\subseteq \mathbb{R}$, porque $\sigma(\xi) \notin \mathbb{R}$. Por tanto, si $c\colon \mathbb{C} \to \mathbb{C}$ es la conjugación de números complejos, se cumple que $\sigma \neq c \circ \sigma$. Luego, $\mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = \{\sigma_1,\dots,\sigma_n, c\circ\sigma_1,\dots,c\circ\sigma_n\}$ con $\#\mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = 2n$ y

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)\cdot c(\sigma_i(\alpha)) > 0.$$

12. Sea A un anillo de números de cuerpo de fracciones K. Prueba que (A,δ) es un anillo euclídeo, donde δ es el valor absoluto de la norma, si y solo si para cada elemento $f \in K$ existe $g \in A$ de modo que $|N(f-g)| < 1$.

    Resolución: Veamos el directo. Obviamente, dados $a,b \in A$, $|N(ab)| = |N(a)||N(b)| \geq |N(a)|$.

    Sean $a,b \in A$, b no nula. Sea $q \in A$ tal que $|N(a/b-q)| < 1$. Sea $r := a - bq$, entonces $a = bq + r$ y $|N(r)| = |N(a-bq)| < |N(b)|\cdot|N(a/b-q)| < |N(b)|$.

    El recíproco es similar.

13. Desingulariza la curva $y^2 - y^3 + x^4 = 0$ en un entorno del origen.

    Resolución: $0 = (y^2-y^3+x^4)/x^2 = (y/x)^2 - (y/x)^3 x + x^2$ que es una curva de coordenadas y/x y x, singular en el origen. Tenemos el morfismo finito

    $$\mathbb{C}[x,y]/(y^2-y^3+x^4) \hookrightarrow \mathbb{C}[x,y/x]/((y/x)^2-(y/x)^3x+x^2).$$

    De nuevo, $0 = ((y/x)^2-(y/x)^3x+x^2)/x^2 = (y/x^2)^2 - (y/x^2)^3x^2 + 1 = z^2 + z^3x^2 + 1$ que es una curva ya sin puntos singulares. Así pues, la desingularización del anillo $\mathbb{C}[x,y]/(y^2-y^3+x^4)$ es $\mathbb{C}[x,z]/(z^2+z^3x^2+1)$ con $z = y/x^2$.

Capítulo 4

Fibras de un morfismo finito

4.1. Introducción

Si $C = \operatorname{Spec} A$ es una curva, por el lema de normalización de Noether, existe un morfismo finito $C \to \mathbb{A}_1$. Equivalentemente, si A es un anillo de números, el morfismo $\mathbb{Z} \hookrightarrow A$ es un morfismo finito, o geométricamente, $\operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z}$ es un morfismo finito. Para el estudio de las curvas y anillos de números, conviene estudiar las fibras de los morfismo finitos, dónde éstos ramifican, cuáles son las multiplicidades con los que aparecen los puntos en las fibras, etc.

Sea $p(x) \in \mathbb{Z}[x]$ mónico y consideremos el morfismo finito

$$\pi\colon \operatorname{Spec} \mathbb{Z}[x]/(p(x)) \to \operatorname{Spec} \mathbb{Z}.$$

El estudio de la fibra del punto genérico g de $\operatorname{Spec} \mathbb{Z}$ ($\mathfrak{p}_g = (0)$) es el estudio de $\mathbb{Q}[x]/(p(x))$ (que equivale al estudio de $p(x) \in \mathbb{Q}[x]$). El estudio de la fibra del punto cerrado p de $\operatorname{Spec} \mathbb{Z}$ ($\mathfrak{m}_p = (p)$) es el estudio de $\mathbb{F}_p[x]/(\overline{p(x)})$ (que equivale al es estudio de $\overline{p(x)} \in \mathbb{F}_p[x]$). Veremos que hay una estrecha relación entre el grupo de Galois de $p(x)$ y los grupos de Galois de $\overline{p(x)} \in \mathbb{F}_p[x]$, para cada primo p. El grupo de Galois de $\overline{p(x)} \in \mathbb{F}_p[x]$ es un grupo elemental, pues es un grupo cíclico generado por el automorfismo de Fröbenius F, donde $F(a) := a^p$, para todo a. Como aplicaciones calcularemos el grupo de Galois de la extensiones de cuerpos ciclotómicas y demostraremos la ley de reciprocidad cuadrática de Gauss.

4.2. Longitud de un módulo

Usualmente, se define la dimensión de un espacio vectorial, como el número de vectores de sus bases. El concepto de base de un espacio vectorial es elaborado, si bien es muy práctico. Si intuimos que $\mathbb{R}^3$ es de dimensión 3 es porque observamos la cadena de inclusiones irrefinable: punto, recta, plano, espacio. Puede definirse la dimensión de un espacio vectorial, como la longitud de las cadenas irrefinables de subespacios

vectoriales. En los A-módulos pueden no existir bases, pero si podemos hablar de la longitud de las cadenas irrefinables de submódulos de un módulo.

1. Definición: Diremos que un A-módulo $M \neq 0$ es simple cuando sus únicos submódulos son los triviales: 0 y M.

Si M es un A-módulo simple entonces $M = \langle m \rangle$, luego $M \simeq A/\text{Anul}\langle m \rangle$. Ahora bien, los submódulos de $A/\text{Anul}\langle m \rangle$ se corresponden con los ideales de A que contienen a $\text{Anul}\langle m \rangle$. Por tanto, $M = \langle m \rangle$ es simple si y solo si $\text{Anul}\langle m \rangle$ es un ideal maximal, es decir, M es simple si y solo si $M \simeq A/\mathfrak{m}$, donde $\mathfrak{m}$ es un ideal maximal de A.

2. Definición: Diremos que una cadena finita de submódulos

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

es una serie de composición en M, si los cocientes sucesivos M_i/M_{i-1} son A-módulos simples. Diremos que la longitud de esta serie de composición es n.

Como los submódulos de M_i/M_{i-1} se corresponden biyectivamente con los submódulos de M_i que contienen a M_{i-1}, el que M_i/M_{i-1} sea simple equivale a que no existe una cadena $M_{i-1} \subsetneq N \subsetneq M_i$. Por tanto, que una cadena de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ sea una serie de composición equivale a decir que no podemos añadirle más "eslabones".

3. Definición: Llamaremos longitud de M a la mínima longitud de todas sus series de composición. Si no existe ninguna serie de composición diremos que la longitud de M es infinita. Denotaremos a la longitud de un módulo M por $l(M)$.

4. Proposición: *Todas las series de composición de un módulo tienen la misma longitud.*

Demostración. Si $l(M) = \infty$ la proposición es obvia. Supongamos que $l(M) = n < \infty$.

Dado un submódulo propio $N \subset M$ se cumple que $l(N) < l(M)$: Sea

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

una serie de composición de longitud mínima de M. Si en $0 = M_0 \cap N \subseteq M_1 \cap N \subseteq \cdots \subseteq M_n \cap N = N$ quitamos los términos repetidos obtenemos una serie de composición en N, porque $M_i \cap N/M_{i-1} \cap N \hookrightarrow M_i/M_{i-1}$, luego $M_i \cap N/M_{i-1} \cap N = M_i/M_{i-1}$ pues M_i/M_{i-1} es simple. Por tanto, $l(N) \leq l(M)$. Si $l(N) = l(M)$ entonces $M_i \cap N/M_{i-1} \cap N \neq 0$ para todo i. Entonces, $M_1 \cap N$ contiene estrictamente a $M_0 \cap N = 0$ y está incluido en M_1, luego $M_1 \cap N = M_1$. Sigamos, $M_2 \cap N$ contiene estrictamente a $M_1 \cap N = M_1$ y está incluido en M_2 luego $M_2 \cap N = M_2$ Recurrentemente, $N = M_n \cap N = M_n = M$, lo que es contradictorio.

Así pues, dada una serie de composición $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_m = M$, tenemos que $l(M) > l(M'_{m-1}) > \cdots > l(M'_1)$, luego $l(M) \geq m$. Como $m \geq n = l(M)$, tenemos que $m = n$.

□

5. Ejercicio: Sea E un k-espacio vectorial. Prueba que si E es un k-espacio vectorial simple entonces $\dim_k E = 1$. En general, prueba que $\dim_k E = l(E)$.

Consideremos $\mathbb{Z}$ como $\mathbb{Z}$-módulo. Prueba que $l(\mathbb{Z}) = \infty$ y que sin embargo $\mathbb{Z}$ es un $\mathbb{Z}$-módulo de rango 1.

Observemos que hemos demostrado que si un módulo es de longitud finita todo submódulo suyo es de longitud finita. Si un módulo es de longitud finita todo cociente suyo también lo es, pues toda serie de composición define por paso al cociente una serie de composición (eliminando las igualdades que aparezcan en la serie, en el cociente).

6. Proposición: *Sea $N \subseteq M$ un submódulo. Entonces, $l(M) = l(N) + l(M/N)$.*

Demostración. Las cadenas de submódulos de M que contienen a N se corresponden biunívocamente con las cadenas de submódulos de M/N. Sea $l(N) = n$ y $l(M/N) = m$, entonces existe una cadena irrefinable de submódulos de 0 a N de longitud n y existe una cadena irrefinable de submódulos de N a M de longitud m, es decir, tenemos una cadena irrefinable de submódulos de 0 a M de longitud $n+m$. □

7. Proposición: *Se cumple que $l(M \oplus N) = l(M) + l(N)$.*

Demostración. Es consecuencia de la proposición anterior, considerando la inclusión $M \hookrightarrow M \oplus N$, $m \mapsto (m,0)$ y el cociente $(M \oplus N)/M \simeq N$, $\overline{(m,n)} \mapsto n$. □

8. Corolario: *Sea $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$ una cadena de A-submódulos de un A-módulo M. Se cumple que*

$$l(M) = \sum_{i=1}^{n} l(M_i/M_{i-1}).$$

Demostración. Procedemos por inducción sobre n. El caso $n = 1$ es obvio. Para $n > 1$, $l(M) = l(M_{n-1}) + l(M/M_{n-1}) = \sum_{i=1}^{n-1} l(M_i/M_{i-1}) + l(M/M_{n-1}) = \sum_{i=1}^{n} l(M_i/M_{i-1})$. □

9. Proposición: *Sea $\mathcal{O}$ una k-álgebra local de ideal maximal $\mathfrak{m}$ y M un $\mathcal{O}$-módulo. Entonces,*

$$\dim_k M = l(M) \cdot \dim_k \mathcal{O}/\mathfrak{m}.$$

Demostración. Sea $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ una serie de composición. Por tanto, $n = l(M)$ y $M_i/M_{i-1} \simeq \mathcal{O}/\mathfrak{m}$. Entonces,

$$\dim_k M = \sum_{i=1}^{n} \dim_k M_i/M_{i-1} = n \cdot \dim_k \mathcal{O}/\mathfrak{m} = l(M) \cdot \dim_k \mathcal{O}/\mathfrak{m}$$

□

10. Lema: *Sea A un anillo íntegro y $f, g \in A$ no nulos. Se cumple que*

$$l(A/(fg)) = l(A/(f)) + l(A/(g)).$$

Demostración. El morfismo $A/(g) \xrightarrow{f\cdot} A/(fg)$ es inyectivo: Si $\overline{fa} = 0$ en $A/(fg)$, entonces fa es múltiplo de fg, entonces como A es íntegro, a es múltiplo de g, es decir, $\bar{a} = 0$ en $A/(g)$.

$\operatorname{Im} f\cdot = (\bar{f}) \subseteq A/(fg)$, luego $A/(g) \simeq (\bar{f})$ y $(A/(fg))/(\bar{f}) = A/(fg, f) = A/(f)$. Por tanto,

$$l(A/(fg)) = l((\bar{f})) + l((A/(fg))/(\bar{f})) = l(A/(g)) + l(A/(f)).$$

□

11. Lema: *Sea A un dominio de ideales principales y $a \in A$ no nulo. Si $a = u \cdot p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición en potencias de factores irreducibles (donde u es invertible) de a, entonces $l_A(A/(a)) = n_1 + \cdots + n_r$.*

Demostración. $l_A(A/(a)) = \sum_i n_i l_A(A/(p_i)) = \sum_i n_i$. □

12. Proposición: *Sea A un dominio de Dedekind y sea $I \subseteq A$ un ideal no nulo. Si $I = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}$ es la descomposición en producto de ideales primos, entonces*

$$l_A(A/I) = n_1 + \cdots + n_r.$$

Demostración. Por el teorema chino de los restos, $A/I = A/\mathfrak{p}_{x_1}^{n_1} \times \cdots \times A/\mathfrak{p}_{x_r}^{n_r}$. Por tanto, $l_A(A/I) = \sum_i l_A(A/\mathfrak{p}_{x_i}^{n_i})$. Observemos que

$$l_A(A/\mathfrak{p}_{x_i}^{n_i}) = l_{A/\mathfrak{p}_{x_i}^{n_i}}(A/\mathfrak{p}_{x_i}^{n_i}) = l_{A_{x_i}/\mathfrak{p}_{x_i}^{n_i}A_{x_i}}(A_{x_i}/\mathfrak{p}_{x_i}^{n_i}A_{x_i}) = l_{A_{x_i}}(A_{x_i}/\mathfrak{p}_{x_i}^{n_i}A_{x_i}) = n_i,$$

porque A_{x_i} es d.i.p. y $\mathfrak{p}_{x_i}A_{x_i} = t_iA_{x_i}$, con t_i irreducible. Luego, $l_A(A/I) = \sum_i n_i$. □

13. Ejercicio: Sea v una valoración discreta y sea $f \in \mathcal{O}_v$. Prueba que $v(f) = l(\mathcal{O}_v/(f))$.

14. Ejercicio: Sea $A = \mathbb{C}[x,y]/(y^2 - x)$, Σ el cuerpo de fracciones de A y $\mathfrak{p}_{(0,0)} := (x,y) \subset A$ ¿Calcular $v_{(0,0)}(\frac{\bar{x}+\bar{y}}{\bar{x}^2})$?.

4.3. Multiplicidad y grado de un punto

1. Definición: Sea A una k-álgebra finita, sea $Y = \operatorname{Spec} A$, que es un número finito de puntos cerrados, y sea $y \in Y$.

1. Llamaremos número de puntos de Y contando grados y multiplicidades a $\dim_k A$.
2. Llamaremos multiplicidad con la que aparece y en Y a $m_y(Y) := l_A(A_y)$.

3. Llamaremos grado de y a $\operatorname{gr} y := \dim_k A/\mathfrak{m}_y$.

2. Proposición: *Se cumple que*

$$\textit{Número de puntos de } Y \textit{ contando grados y multiplicidades} = \sum_{y\in Y} m_y(Y)\cdot \operatorname{gr} y.$$

Demostración. $A = \prod_{y\in Y} A_y$, luego $\dim_k A = \sum_{y\in Y} \dim_k A_y = \sum_{y\in Y} \dim_k(A/\mathfrak{m}_y)\cdot l_A(A_y)$ y hemos concluido. □

3. Ejemplo: Consideremos la ecuación

$$x^2\cdot(x-1)^3\cdot(x^2+1)=0.$$

Las soluciones reales de esta ecuación son $x = 0, 1$. Tiene además una solución compleja $x = i$ y su conjugada $x = -i$. Intuitivamente podríamos decir que $x = 0$ aparece dos veces, $x = 1$ tres veces y $x = \pm i$ una vez. También podríamos decir que la ecuación tiene 7 soluciones: dos veces $x = 0$, tres $x = 1$ y una vez $x = \pm i$. Consideremos la $\mathbb{R}$-álgebra finita $A = \mathbb{R}[x]/(x^2\cdot(x-1)^3\cdot(x^2+1))$ y

$$\operatorname{Spec} A = \{\mathfrak{m}_0 = (\bar{x}),\ \mathfrak{m}_1 = (\overline{x-1}) \text{ y } \mathfrak{m}_{\pm i} = (\overline{x^2+1})\}.$$

La multiplicidad con la que aparece el punto 0 en $\operatorname{Spec} A$ es 2, con la que aparece 1 es tres y con la que aparece $\pm i$ es 1. El número de puntos de $\operatorname{Spec} A$ contando multiplicidades y grados es $\dim_{\mathbb{R}} A = 7$. Por tanto,

$$\begin{aligned}\text{Nº de ptos de } \operatorname{Spec} A, \text{ contando mult. y grd.} &= \dim_{\mathbb{R}} A = 7 = 2\cdot 1 + 3\cdot 1 + 1\cdot 2\\ &= m_0(\operatorname{Spec} A)\cdot \operatorname{gr} 0 + m_1(\operatorname{Spec} A)\cdot \operatorname{gr} 1 + m_{\pm i}(\operatorname{Spec} A)\cdot \operatorname{gr} \pm i.\end{aligned}$$

4. Definición: Sea $A \hookrightarrow B$ un morfismo finito inyectivo y

$$\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$$

el morfismo inducido. Dado $x \in \operatorname{Spec} A$, $\pi^{-1}(x) = \operatorname{Spec} B/\mathfrak{m}_x B$ y $B/\mathfrak{m}_x B$ es una $A/\mathfrak{m}_x$-álgebra finita. Llamaremos número de puntos de $\pi^{-1}(x)$, contando muktiplicidades y grados a $\dim_{A/\mathfrak{m}_x} B/\mathfrak{m}_x B$, multiplicidad con la que aparece $y \in \pi^{-1}(x)$ en $\pi^{-1}(x)$ a $m_y := l_B((B/\mathfrak{m}_x B)_y)$, y grado de y sobre x a $\operatorname{gr}_x y := \dim_{A/\mathfrak{m}_x} B/\mathfrak{m}_y$.

Por tanto,

$$\text{Nº de puntos de } \pi^{-1}(x), \text{ contando grados y multiplicidades} = \sum_{y\in\pi^{-1}(x)} m_y\cdot \operatorname{gr}_x y$$

5. Ejercicio: Consideremos el morfismo finito e inyectivo

$$\mathbb{R}[x] \to \mathbb{R}[x,y]/(y^2-x),\ \ x \mapsto \bar{x}.$$

Sea

$$\pi\colon \operatorname{Spec}\mathbb{R}[x,y]/(y^2-x) \to \operatorname{Spec}\mathbb{R}[x], (\alpha,\beta) \mapsto \alpha$$

el morfismo inducido. Dado un punto racional $\alpha \in \operatorname{Spec}\mathbb{R}[x]$, calcula el número de puntos de las fibras, las multiplicidades y grados de los puntos de las fibras de π.

6. Proposición: *Sea $A \hookrightarrow B$ un morfismo finito inyectivo, A un dominio de Dedekind y B íntegro. Sea*

$$\pi\colon \operatorname{Spec}B \to \operatorname{Spec}A$$

el morfismo inducido en los espectros. Se cumple que "el número de puntos de las fibras de π, contando multiplicidades y grados es constante", y es igual a $\dim_{\Sigma_A}\Sigma_B$.

Demostración. Sea $x \in \operatorname{Spec}A$ un punto cerrado. A_x es un dominio de ideales principales y B_x es un A_x-módulo finito generado sin torsión. Luego, $B_x = A_x^{n_x}$. Observemos que $B_{A\setminus\{0\}}$ es una Σ_A-álgebra finita íntegra, luego es un cuerpo y $B_{A\setminus\{0\}} = \Sigma_B$. Si localizamos los términos de la igualdad $B_x = A_x^{n_x}$ por $A\setminus\{0\}$, obtenemos

$$\Sigma_B = \Sigma_A^{n_x}$$

Por tanto, $n_x = \dim_{\Sigma_A}\Sigma_B$. Si tensamos los términos de la igualdad $B_x = A_x^{n_x}$ por $\otimes_A A/\mathfrak{m}_x$, obtenemos

$$B/\mathfrak{m}_x B = (A/\mathfrak{m}_x)^{n_x}$$

Por tanto, el número de puntos de la fibra de x, contando grados y multiplicidades, es igual a $n_x = \dim_{\Sigma_A}\Sigma_B$.

□

7. Definición: Sea $\phi\colon A \to B$ un morfismo finito entre dominios de Dedekind. Sea $\mathfrak{m}_y$ un ideal maximal de B y $\mathfrak{m}_x := \mathfrak{m}_y \cap B$. Entonces $\mathfrak{m}_x B_y = \mathfrak{m}_y^{e_y} B_y$, para cierto $e_y \in \mathbb{N}$, que llamaremos índice de ramificación de y.

8. Proposición: *Sea $\phi\colon A \to B$ un morfismo finito entre dominios de Dedekind. Sea $x \in \operatorname{Spec}A$ un ideal maximal e y un punto en la fibra de x. La multiplicidad con la que aparece y en la fibra de x es igual al índice de ramificación de y.*

Demostración. $l_B((B/\mathfrak{m}_x B)_y) = l_B(B_y/\mathfrak{m}_y^{e_y} B_y) = e_y$.

□

Se cumple que π no ramifica en y si y solo si $B_y/\mathfrak{m}_x B_y = B/\mathfrak{m}_y$ y $B/\mathfrak{m}_y B$ es una $A/\mathfrak{m}_x$-extensión separable, es decir, si y solo si la multiplicidad de y en la fibra de x es 1, y $B/\mathfrak{m}_y B$ es una $A/\mathfrak{m}_x$-extensión separable.

Observemos que si π no ramifica en y, entonces $\mathfrak{m}_x B_y = \mathfrak{m}_y B_y$, luego si $\mathfrak{m}_x A_x$ es principal entonces $\mathfrak{m}_y B_y$ también lo es.

9. Ejemplo: Consideremos el morfismo finito $\mathbb{Z} \to \mathbb{Z}[i]$. Calculemos las fibras del morfismo inducido $\pi\colon \operatorname{Spec}\mathbb{Z}[i] \to \operatorname{Spec}\mathbb{Z}$ y los grados y multiplicidades con los que aparecen los puntos en las fibras. Como $\dim_{\mathbb{Q}} \mathbb{Q}[i] = 2$, el número de puntos de las fibras, contando grados y multiplicidades es 2. Dado $\mathfrak{m}_p = (p) \in \operatorname{Spec}\mathbb{Z}$,

$$\pi^{-1}(p) = \operatorname{Spec}\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1) = \begin{cases} (\bar{0}) & \text{si } x^2+1 \text{ es irreducible en } \mathbb{Z}/p\mathbb{Z}[x]. \\ (\overline{x+1}) & \text{si } p = 2. \\ (\overline{x-n}), (\overline{x-m}) & \text{cuando } p \neq 2 \text{ y } n^2, m^2 = -1 \mod p. \end{cases}$$

Si $p = 3 \mod 4$ entonces $\pi^{-1}(p) = \{(p)\}$ y éste es un punto de grado dos y aparece con multiplicidad 1 en la fibra. Si $p = 2$, $\pi^{-1}(2) = \{(i+1)\}$ y éste es un punto de grado 1 y aparece con multiplicidad 2 en la fibra. Por último, si $p = 1 \mod 4$ entonces $\pi^{-1}(p) = \{(i-n), (i-m)\colon\ n^2, m^2 = -1 \mod p\}$ y son puntos de grado 1 y aparecen con multiplicidad 1 en la fibra.

4.3.1. Ceros y polos de una función

10. Proposición: *Sea A un dominio de Dedekind y $f \in A$ no nulo. Entonces,*

$$\sum_{x \in \operatorname{Spec}_{\max} A} v_x(f) = l(A/(f)).$$

Demostración. Escribamos $(f) = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}$.

Si $x \notin \{x_1, \ldots, x_r\}$, entonces $f \cdot A_x = A_x$ y $l(A_x/f \cdot A_x) = 0 = v_x(f)$. Por otra parte, $f \cdot A_{x_i} = \mathfrak{p}_{x_i}^{n_i} \cdot A_{x_i}$ y $l(A_{x_i}/f \cdot A_{x_i}) = l(A_{x_i}/\mathfrak{p}_{x_i}^{n_i} \cdot A_{x_i}) = n_i = v_{x_i}(f)$.

Por último,

$$l(A/(f)) = l(A/\mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}) = \sum_i n_i = \sum_i v_{x_i}(f) = \sum_{x \in \operatorname{Spec}_{\max} A} v_x(f).$$

□

Sea V la variedad de Riemann asociada a K y $f \in K$ trascendente. Consideremos la inclusión $k(x) \hookrightarrow K, x \mapsto f$ y el morfismo inducido entre las variedades de Riemann

$$\tilde{f}\colon V \to \mathbb{P}^1.$$

Sea A el cierre entero de $k[f]$ y A' el cierre entero de $k[1/f]$. Tenemos los morfismos $k[x] \to A$, $x \mapsto f$ y $k[1/x] \to A'$, $1/x \mapsto 1/f$, que inducen en espectros los morfismos $U =$

$\operatorname{Spec} A \to \operatorname{Spec} k[x]$ y $U' = \operatorname{Spec} A' \to \operatorname{Spec} k[1/x]$, que coinciden sobre las intersecciones y define el morfismo $\tilde{f}\colon V \to \mathbb{P}^1$ de partida. Sea $p \in U$ y consideremos la composición $k[x] \to A \to A/\mathfrak{m}_p$, $x \mapsto f \mapsto f(p)$. El núcleo de la composición es $\mathfrak{m}_{\tilde{f}(p)} = (x - f(p)) = \mathfrak{m}_{f(p)}$, por tanto $\tilde{f}(p) = f(p)$.

Recordemos que el número de puntos de las fibras (contando grados y multiplicidades) es constante. Veamos el número de puntos de la fibra del $0 \in \operatorname{Spec} k[x] \subset \mathbb{P}^1$ ($\mathfrak{p}_0 = (x)$): La x en A es f, $(f) = \mathfrak{m}_{x_1}^{e_1} \cdots \mathfrak{m}_{x_n}^{e_n}$, donde $\{x_1, \ldots, x_n\}$ son los puntos de la fibra de 0 y $e_i = v_{x_i}(f)$ (y $v_x(f) = 0$, para todo $x \in U$ distinto de los x_i). Por tanto,

$$\text{Nº de puntos de la fibra del } 0 = \dim_k A/(f) = \sum_{x \in C, v_x(f) \geq 0} v_x(f) \operatorname{gr}_k x,$$

número que se denomina *número de ceros de* f. Igualmente, el número de puntos de la fibra del $\infty \in \operatorname{Spec} k[1/x] \subset \mathbb{P}^1$ ($\mathfrak{p}_\infty = (1/x)$) es

$$\text{Nº de puntos de la fibra del } \infty = \dim_k A'/(1/f) = \sum_{x \in C, v_x(1/f) \geq 0} v_x(1/f) \operatorname{gr}_k x$$

número que se denomina *número de polos de* f. Por tanto,

$$0 = \text{Nº de puntos de la fibra del } 0 \; - \; \text{Nº de puntos de la fibra del } \infty = \sum_{x \in C} v_x(f) \operatorname{gr}_k x$$

11. Teorema: *Sea K una extensión de tipo finito de k de grado de trascendencia 1, V la variedad de Riemann asociada a K y $f \in K$. Entonces,*

$$\boxed{\textstyle\sum_{x \in V} v_x(f) \operatorname{gr}_k x = 0},$$

es decir, el número de ceros de f es igual a su número de polos.

Teorema de Bezout

Sea $p_n(x_0, x_1, x_2)$ un polinomio homogéneo de grado n. Diremos que la curva proyectiva plana $C = \operatorname{Proj} k[x_0, x_1, x_0]/(p_n(x_0, x_1, x_2))$ es de grado n. Sea $q_m(x_0, x_1, x_m)$ un polinomio homogéneo de grado m y $C' = \operatorname{Proj} k[x_0, x_1, x_0]/(q_m(x_0, x_1, x_2))$. Supongamos que C y C' no tienen componentes comunes. Entonces,

$$C \cap C' = \operatorname{Proj} k[x_0, x_1, x_0]/(p_n(x_0, x_1, x_2), q_m(x_0, x_1, x_2))$$

es igual a un número finito de puntos. Por cambio de coordenadas, podemos suponer que $C \cap C'$ no tiene puntos en el infinito, $x_0 = 0$ (supongamos si es necesario que $\#k = \infty$). Por tanto, $C \cap C' = (C \cap U_{x_0}^h) \cap (C' \cap U_{x_0}^h)$ y podemos trabajar en el abierto afín $U_{x_0}^h$. Si $p(x, y) = p_m/x_0^n$ y $q(x, y) = q_m/x_0^m$ son las deshomogeneizaciones por x_0, tenemos que

$$C \cap C' = \operatorname{Proj} k[x_0, x_1, x_0]/(p_n(x_0, x_1, x_2), q_m(x_0, x_1, x_2)) = \operatorname{Spec} k[x, y]((p(x, y), q(x, y))$$

El anillo $k[x, y]((p(x, y), q(x, y))$ no depende del abierto afín $U_{x_0}^h$ considerado. Diremos que $(C \cap C') := \dim_k k[x, y]((p(x, y), q(x, y))$ es el número de puntos de corte de C con C', contando multiplicidades de corte y grados de los puntos de corte.

12. Teorema de Bézout: *El número de puntos de corte de dos curvas planas proyectivas de grados n y m, sin componentes comunes, contando multiplicidades de corte y grados de los puntos de corte, es igual a $n \cdot m$.*

Demostración. Sigamos las notaciones previas. Podemos suponer que k es algebraicamente cerrado. Demostremos el teorema solo en el caso de que C es no singular (si no habría que desingularizarla...). Podemos suponer que $C \cap C'$, $C \cap \{x_0 = 0\}$ y $C \cap \{x_1 = 0\}$ son disjuntos dos a dos. Sea K el cuerpo de fracciones de $k[x,y]/((p(x,y))$ y consideremos $q(x,y) = \frac{q_m(x_0,x_1,x_2)}{x_0^m} \in K$. El número de ceros de $q(x,y)$ en C, contando grados y multiplicidades, es igual a $\dim_k k[x,y]/((p(x,y),q(x,y))$; y el número de polos de $q(x,y)$ en C, contando grados y multiplicidades, es igual al número de ceros de $(x_0/x_1)^m$, que son m veces el número de puntos de corte de C con la recta $\{x_0 = 0\}$. Por tanto,

$$(C \cap C') = m \cdot (C \cap \{x_0 = 0\}) = m \cdot n$$

□

4.3.2. Apéndice: Multiplicidad del anillo local

Sea A un anillo de números o el anillo de funciones algebraicas de una curva algebraica íntegra. Sea $x \in \mathrm{Spec} A$ un punto cerrado, denotemos $\mathscr{O} = A_x$, $\bar{\mathscr{O}} = \bar{A}_x$ y $\mathfrak{m} = \mathfrak{m}_x \mathscr{O}$.

Como $\bar{\mathscr{O}}$ es un domino de Dedekind, tendremos que $\mathfrak{m}_x \cdot \bar{\mathscr{O}} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$, donde $x_1, \ldots, x_r$ son los puntos de la fibra de x en el morfismo de desingularización. Observemos que el número de puntos de la fibra de x, contando multiplicidades y grados es

$$l_{\mathscr{O}}(\bar{\mathscr{O}}/\mathfrak{m}_x\bar{\mathscr{O}}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}) = \sum_i n_i \cdot \mathrm{gr}_x(x_i), \quad (\mathrm{gr}_x(x_i) = \dim_{\mathscr{O}/\mathfrak{m}_x} \bar{\mathscr{O}}/\mathfrak{m}_{x_i}).$$

Sea $f \in \mathscr{O}$. Observemos que $l_{\mathscr{O}}(\mathscr{O}/f\mathscr{O}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/f\bar{\mathscr{O}})$, pues del diagrama conmutativo

$$\begin{array}{ccc} \mathscr{O} & \longrightarrow & \bar{\mathscr{O}} \\ \downarrow{\scriptstyle f\cdot} & & \downarrow{\scriptstyle f\cdot} \\ \mathscr{O} & \longrightarrow & \bar{\mathscr{O}} \end{array}$$

se deduce que $l_{\mathscr{O}}(\bar{\mathscr{O}}/\mathscr{O}) + l_{\mathscr{O}}(\mathscr{O}/f \cdot \mathscr{O}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/f \cdot \mathscr{O}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/f \cdot \bar{\mathscr{O}}) + l_{\mathscr{O}}(\bar{\mathscr{O}}/\mathscr{O})$, y concluimos.

Sea ahora $f \in \mathfrak{m}_x$ un parámetro transversal a x, entonces

$$mult_x(\mathscr{O}) := l_{\mathscr{O}}(\mathscr{O}/f \cdot \mathscr{O}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/f \cdot \bar{\mathscr{O}}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/\mathfrak{m}_x \cdot \bar{\mathscr{O}}) = \sum_i n_i \cdot \mathrm{gr}_x(x_i)$$

y este número se dice que es la multiplicidad de $\mathrm{Spec}\mathscr{O}$ en x. Dado $f' \in \mathfrak{m}_x$, entonces

$$l_{\mathscr{O}}(\mathscr{O}/f'\mathscr{O}) = l_{\mathscr{O}}(\bar{\mathscr{O}}/f'\bar{\mathscr{O}}) \geq l_{\mathscr{O}}(\bar{\mathscr{O}}/\mathfrak{m}_x\bar{\mathscr{O}}) = mult_x(\mathscr{O}).$$

Si $\mathcal{O}_1$ es el anillo de la explosión de $\mathrm{Spec}\mathcal{O}$ en x, y $f' \in \mathfrak{m}_x^n$, entonces

$$l_{\mathcal{O}}(\mathcal{O}/f'\mathcal{O}) = l_{\mathcal{O}}(\mathcal{O}_1/f'\mathcal{O}_1) = l_{\mathcal{O}}(\mathcal{O}_1/f^n \cdot \frac{f'}{f^n} \cdot \mathcal{O}_1) = l_{\mathcal{O}}(\mathcal{O}_1/f^n\mathcal{O}_1) + l_{\mathcal{O}}(\mathcal{O}_1/\frac{f'}{f^n} \cdot \mathcal{O}_1)$$
$$= mult_x(\mathcal{O}) \cdot n + l_{\mathcal{O}}(\mathcal{O}_1/\frac{f'}{f^n} \cdot \mathcal{O}_1).$$

13. Ejemplo: Sea $C = \mathrm{Spec}\,\mathbb{C}[x,y]/(p(x,y))$ una curva plana que pasa por el origen. Escribamos $p(x,y) = p_m(x,y) + p_{m+1}(x,y) + \cdots + p_n(x,y)$ como suma de polinomios homogéneos. Sabemos que $T_{(0,0)}C = \mathrm{Proj}\,\mathbb{C}[x,y]/(p_m(x,y))$. Sea $x + \lambda y$ cualquier recta transversal a C en $(0,0)$ (es decir, $x+\lambda y$ no divide a $p_m(x,y)$). Denotemos $\mathcal{O} = (\mathbb{C}[x,y]/(p(x,y)))_{(0,0)}$. Tenemos que la multiplicidad de C en $(0,0)$ es igual a

$$l_{\mathcal{O}}(\mathcal{O}/(x+\lambda y)) = \dim_{\mathbb{C}}(\mathbb{C}[y]/(y^m)) = m.$$

Supongamos que $p(x,y) = y^2 - x^2 + x^3$ y consideremos la curva plana $y - x + x^2 = 0$. Calculemos la multiplicidad de corte de ambas curvas en el punto $(0,0)$, que es igual a $l((\mathbb{C}[x,y]/(y^2 - x^2 + x^3, y - x + x^2)_{(0,0)} = l(\mathcal{O}/(y - x + x^2))$. Observemos que $\mathcal{O}_1$ es la localización de $(\mathbb{C}[x,y/x]/((y/x)^2 - 1 + x)$ en los puntos $(x,y)_0 = (x)_0 = \{(x, y/x - 1), (x, y/x + 1)\}$. Entonces,

$$l_{\mathcal{O}}(\mathcal{O}/(y - x + x^2)) = 2 + l_{\mathcal{O}}(\mathcal{O}_1/(y/x - 1 + x)) = 2 + l(((\mathbb{C}[x,y/x]/((y/x)^2 - 1 + x, y/x - 1 + x)_{(0,1)})$$
$$= 2 + 1 = 3,$$

porque $y/x - 1 + x$ es transversal a $(y/x)^2 - 1 + x = 0$ en el punto $(0,1)$.

4.4. Espectro primo del anillo de invariantes

Sea G un grupo finito de automorfismos de un anillo B. Dado $g \in G$, el automorfismo $g\colon B \to B$, induce el automorfismo $g^*\colon \mathrm{Spec}B \to \mathrm{Spec}B$. G opera sobre $\mathrm{Spec}B$ de modo natural: dado $g \in G$ y $y \in \mathrm{Spec}B$, $gy := g^{*-1}(y)$, es decir, $\mathfrak{p}_{gy} := g(\mathfrak{p}_y)$.

1. Teorema: *Sea G un grupo finito de automorfismos de un anillo B. Denotemos por $B^G := \{b \in B\colon g(b) = b \text{ para todo } g \in G\}$ y por $(\mathrm{Spec}B)/G := \{\bar{y}, \text{ con } y \in \mathrm{Spec}B, \text{ donde decimos que } \bar{y} = \bar{z} \text{ si y solo si existe } g \in G \text{ tal que } z = gy\}$. Se cumple que*

$$\mathrm{Spec}(B^G) = (\mathrm{Spec}B)/G.$$

Demostración. Empecemos observando que dada $f \in B$, el polinomio $\prod_{g \in G}(x - g(f))$ es un polinomio mónico con coeficientes en B^G que anula a f, luego f es entero sobre B^G. Por tanto, $B^G \hookrightarrow B$ es un morfismo entero, luego induce en espectros un morfismo epiyectivo de fibras de dimensión cero.

Tenemos que ver que las fibras del morfismo $\mathrm{Spec}B \to \mathrm{Spec}B^G$ son órbitas por la acción de G.

Dado un ideal primo $\mathfrak{p}_y \subset B$, $g(\mathfrak{p}_y)$ corta a B^G en el mismo ideal primo que $\mathfrak{p}_y$. Sea $\mathfrak{p}_z$ es un ideal primo de B distinto de $g(\mathfrak{p}_y) = \mathfrak{p}_{g(y)}$ para todo $g \in G$, tal que z e y tienen la misma imagen por el morfismo $\mathrm{Spec}B \to \mathrm{Spec}B^G$, digamos x. Por ser el morfismo $B^G \hookrightarrow B$ entero sabemos que $\mathfrak{p}_z \nsubseteq \mathfrak{p}_{g(y)}$, para todo $g \in G$, luego existe una $f \in B$ que se anula en z y no se anula en ninguno de los $g(y)$. Entonces $N(f) := \prod_{g\in G} g(f) \in B^G$ se anula en z y no se anula en ninguno de los $g(y)$. Llegamos a contradicción, porque por un lado $N(f)$ ha de anularse en x y por el otro no.

□

2. Ejercicio: Sea $\tau\colon \mathbb{C}[x,y]/(y^2-x) \to \mathbb{C}[x,y]/(y^2-x)$ el automorfismo de $\mathbb{C}$-álgebras definido por $\tau(y) = -y$ y $\tau(x) = x$ y sea $G = \{\mathrm{Id}, \tau\}$. Explicitar la operación de G sobre $X = \mathrm{Spec}\,\mathbb{C}[x,y]/(y^2-x)$. Calcula X/G.

3. Ejercicio: Sea $\tau\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ el automorfismo de anillos definido por $\tau(\sqrt{2}) = -\sqrt{2}$ y sea $G = \{\mathrm{Id}, \tau\}$. Sea $X = \mathrm{Spec}\,\mathbb{Z}[\sqrt{2}]$. Calcula X/G.

Si $B = R[\xi_1, \ldots, \xi_n]$ es una R-álgebra de tipo finito y G es un grupo finito de automorfismos de R-álgebras de B, entonces el morfismo $B^G \to B$ es un morfismo finito, porque $B = B^G[\xi_1, \ldots, \xi_n]$ y los ξ_i son enteros sobre B^G. Consideremos el morfismo

$$\pi\colon \mathrm{Spec}B \to \mathrm{Spec}B^G$$

y un punto cerrado $x \in \mathrm{Spec}B^G$. Dados $y_1, y_2 \in \mathrm{Spec}B$ tales que $\pi(y_1) = \pi(y_2) = x$, tenemos que existe $g \in G$, tal que $g(y_1) = y_2$. Por tanto, tenemos $B/\mathfrak{m}_{y_1} \simeq B/\mathfrak{m}_{y_2}$, luego $\mathrm{gr}_x y_1 = \mathrm{gr}_x y_2$. Igualmente tenemos que $l_{B_{y_1}}((B_{y_1}/\mathfrak{m}_x B_{y_1})) = l_{B_{y_2}}((B_{y_2}/\mathfrak{m}_x B_{y_2}))$, luego la multiplicidad con la que aparece y_1 en la fibra de x es igual a multiplicidad con la que aparece y_2 en la fibra de x. Sea $D = \{g \in G\colon g(y_1) = y_1\}$ el subgrupo de descomposición de y_1. Entonces, $\pi^{-1}(x) = G \cdot y_1 = G/D$ y tenemos que

$$\text{Número de puntos de } \pi^{-1}(x) \text{ contando grados y multiplicidades} = |G/D| \cdot m_{y_1} \cdot \mathrm{gr}_x y_1.$$

Si y_1 no es un punto de ramificación entonces ninguno de los puntos de la fibra de x es de ramificación y tenemos que

$$\text{Número de puntos de } \pi^{-1}(x) \text{ contando grados y multiplicidades} = |G/D| \cdot \mathrm{gr}_x y_1.$$

Recordemos que dado un ideal primo $\mathfrak{p}_y \subset B$, denotamos el cuerpo residual de y, $(B_y/\mathfrak{p}_y B_y) =: k(y)$ y dado $b \in B$ denotamos $b(y) := \bar{b} \in k(y)$.

Sea $g\colon B \to B$ un automorfismo e $y \in \mathrm{Spec}B$. Tenemos el isomorfismo

$$\bar{g}\colon k(y) \to k(gy),\ \ \bar{g}(\bar{b}) = \overline{g(b)}$$

(es decir, $\bar{g}(b(y)) := (gb)(gy)$).

4. Teorema: *Sea B una R-álgebra de tipo finito y G un grupo finito de automorfismos de R-álgebras de B. Consideremos el morfismo finito*

$$\pi\colon \operatorname{Spec} B \to \operatorname{Spec} B^G.$$

Sea $y \in \operatorname{Spec} B$, $x := \pi(y)$ y $D := \{g \in G\colon g(y) = y\}$ el "grupo de descomposición" de y. Si $k(x) \hookrightarrow k(y)$ es separable, entonces $k(y)$ es una $k(x)$-extensión de Galois y el morfismo natural

$$G \supseteq D \to \operatorname{Aut}_{k(x)-alg}(k(y)),\ g \mapsto \bar{g}$$

es epiyectivo.

Demostración. Localizando en x, podemos suponer que y e x son puntos cerrados. Observemos que $\pi^{-1}(x) = \operatorname{Spec} B/\mathfrak{m}_x B = \{y_1, \ldots, y_n\} = G \cdot y$. Por el teorema del elemento primitivo, $k(y) = k(x)[\theta]$. Sea $b \in B$ tal que $b(y) = \theta$ y $b(y_i) = 0$ para todo $y_i \neq y$. Tenemos que $P(X) := \prod_{g \in G}(X - g(b)) \in B^G[X] \subset B[X]$ y módulo $\mathfrak{m}_y$, tenemos que $\overline{P(X)} = \prod_{g \in D}(X - \bar{g}(\theta)) \cdot X^{|G|-|D|} \in k(x)[X] \subset k(y)[X]$ es un polinomio que anula a θ y todas sus raíces están en $k(y)$. Por tanto, $k(y)$ es una $k(x)$-extensión de Galois de grupo un cociente de D.

□

5. Corolario: *Si además suponemos en el teorema anterior que B es un anillo íntegro de dimensión de Krull 1 y que x es un punto no singular no rama, entonces $D \simeq \operatorname{Aut}_{k(x)-alg}(k(y))$.*

Demostración. Sean Σ_{B^G} y Σ_B los cuerpos de fracciones de B^G y B. Observemos que $(\Sigma_B)^G = \Sigma_{B^G}$: dado $b_1/b_2 \in (\Sigma_B)^G$, tenemos que $N(b_2) \cdot (b_1/b_2) \in B^G$, luego $b_1/b_2 \in \Sigma_{B^G}$. Por tanto, Σ_B es una Σ_{B^G}-extensión de Galois de grupo G. Tenemos que

$$\begin{aligned} |G| &= \dim_{\Sigma_{B^G}} \Sigma_B = \text{Número de puntos de } \pi^{-1}(x) \text{ contando grados y multiplicidades} \\ &= |G/D| \cdot \operatorname{gr}_x y \end{aligned}$$

Luego, $k(y)$ es una $k(x)$-extensión de Galois de orden $|D|$ y el epimorfismo

$$D \to \operatorname{Aut}_{k(x)-alg}(k(y))$$

es isomorfismo.

□

4.5. Automorfismo de Fröbenius

Sea $\mathbb{Z} \hookrightarrow A$ un morfismo finito, $\mathfrak{m} \subset A$ un ideal maximal y $(p) = \mathfrak{m} \cap \mathbb{Z}$. Observemos que $A/\mathfrak{m}$ es una extensión finita de cuerpos de $\mathbb{Z}/p\mathbb{Z}$, luego $A/\mathfrak{m} \simeq \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}$ es un cuerpo con un número finito de elementos.

1. Cuerpos finitos: Sea K es un cuerpo finito y $p > 0$ la característica de K. Supongamos que $\dim_{\mathbb{F}_p} K = n$. Entonces $|K| = p^n$ y los elementos de $K\setminus\{0\}$ son las raíces de $x^{p^n-1} - 1$ (que es separable). En conclusión, existe un único cuerpo (salvo isomorfismos) de orden p^n, que coincide con el conjunto de todas las raíces de $x^{p^n} - x$ y es un $\mathbb{F}_p$-extensión de Galois de grado n, que denotaremos $\mathbb{F}_{p^n}$. Observemos que $p^n - 1 = |\mathbb{F}_{p^n}^*|$ es el anulador del grupo abeliano $\mathbb{F}_{p^n}^*$ (es decir, $p^n - 1$ es el mínimo número natural m tal que $\alpha^m = 1$, para todo $\alpha \in \mathbb{F}_{p^n}^*$). Por tanto, $\mathbb{F}_{p^n}^*$ es cíclico y existe $\alpha \in \mathbb{F}_{p^n}^*$, tal que $\mathbb{F}_{p^n}^* = \{\alpha^r\}_{r<p^n}$.

El automorfismo de Fröbenius $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(a) := a^p$ es un automorfismo de orden n, luego $\mathrm{Aut}_{\mathbb{F}_p - alg}\, \mathbb{F}_{p^n} = \langle F\rangle$. Sea $\langle F^m\rangle \subset \langle F\rangle$ un subgrupo (podemos suponer que m divide a n). Entonces, $\mathbb{F}_{p^n}^{\langle F^m\rangle} = \mathbb{F}_{p^m}$ y $\mathbb{F}_{p^n}$ es una $\mathbb{F}_{p^m}$-extensión de Galois de grupo de Galois $\langle F^m\rangle$.

2. Teorema: *Sea $\mathbb{Q} \hookrightarrow \Sigma$ una extensión de Galois de grupo G y A un anillo de números de Σ, estable por G. Consideremos el morfismo natural*

$$\pi\colon \mathrm{Spec}\, A \to \mathrm{Spec}\, \mathbb{Z}.$$

Sea $y \in \mathrm{Spec}_{\max} A$, $\pi(y) \in \mathrm{Spec}\, \mathbb{Z}$ y escribamos $\mathfrak{m}_{\pi(y)} = (p)$. El automorfismo de Fröbenius, F, de $A/\mathfrak{m}_y$ está inducido por algún automorfismo $F_p \in G$ de A. Además, F_p es único cuando π no ramifica en y, en este caso se dice que F_p es el automorfismo de Fröbenius de Σ_A en el primo p.

3. Observaciones:

1. $F_p\colon \Sigma_A \to \Sigma_A$, es el automorfismo de A que deja estable $\mathfrak{m}_y$, determinado por la condición $F_p(a) = a^p \mod \mathfrak{m}_y$, para todo $a \in A$.

2. En el teorema, en la fibra de (p), si en vez de tomar y consideramos otro punto y', entonces como G opera transitivamente en las fibras, existe $g \in G$ de modo que $y' = gy$. Por tanto, el grupo de descomposición de y' es gDg^{-1} y el automorfismo que asociaríamos a F sería gF_pg^{-1}.

3. Si y no es de ramificación, entonces $\mathfrak{m}_y \cdot A_y = p \cdot A_y$. Es decir, todos los puntos de la fibra del ideal primo (p) son no singulares. Si $\bar{A}$ es el cierre entero de A en Σ_A, entonces $A_{y_i} = \bar{A}_{y_i}$, $A/pA = \bar{A}/p\bar{A}$ y el automorfismo de Fröbenius de Σ_A en p no depende del anillo A considerado.

4. Sea $\Sigma' \subset \Sigma_A$ una $\mathbb{Q}$-subextensión de Galois, A' el anillo de números de Σ' y $\bar{A}$ el anillo de números de Σ_A. Si $\mathbb{Z} \to \bar{A}$ no ramifica en p, entonces $\mathbb{Z} \to A'$ tampoco, porque si $pA' = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_r^{e_r}$, con $e_1 > 1$ entonces la descomposición de $p\bar{A}$ también

tendrá algún factor repetido. Además, el automorfismo de Fröbenius, F_p de Σ_A en p, induce en Σ' un automorfismo, que sobre $A'/\mathfrak{m}_1 \subseteq A/\mathfrak{m}_{y_1}$ es el automorfismo de Fröbenius. Por tanto, el automorfismo de Fröbenius de Σ' en p es igual a $F_{p_{|\Sigma'}}$.

Sea $q(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in \mathbb{Z}[x]$ un polinomio separable. Supongamos que $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ es separable. El polinomio $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ es separable precisamente en los primos p que no dividan al discriminante $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$. Consideremos el anillo de números $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Dado un ideal $\mathfrak{m} \subset A$ en la fibra de p, $A/\mathfrak{m} = \mathbb{Z}/p\mathbb{Z}[\bar{\alpha}_1, \ldots, \bar{\alpha}_n]$ es el cuerpo de descomposición de $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$. Como A es un cociente de $\mathbb{Z}[x]/(q(x))^{\otimes n}$, tenemos que A/pA es una $\mathbb{Z}/p\mathbb{Z}$-álgebra separable.

4. Definición: Sea $q(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in \mathbb{Z}[x]$ un polinomio separable. Dado un primo $p \in \mathbb{Z}$, tal que $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ es separable, llamaremos automorfismo de Fröbenius en p de $q(x)$ al automorfismo de Fröbenius, F_p del cuerpo de descomposición de $q(x)$. Es decir, F_p es la permutación de $\alpha_1, \ldots, \alpha_n$ tal que la correspodiente permutación de $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ coincida con el morfismo elevar a p.

4.5.1. Aplicaciones

1. *Existen polinomios con coeficientes enteros irreducibles que no lo son módulo cualquier número primo:* cualquier cuártica cuyo grupo de Galois sea el grupo de Klein es irreducible, aunque no lo sea módulo cualquier primo p, pues el grupo generado por el automorfismo de Fröbenius en p no opera transitivamente sobre las raíces.

2. *Existen polinomios con coeficientes enteros sin raíces racionales pero que módulo cualquier número primo p tiene raíces en $\mathbb{Z}/p\mathbb{Z}$:* Si todo automorfismo $g \in G$ deja fija alguna raíz de $q(x)$, entonces $F(\bar{\alpha}_i) = \bar{\alpha}_i$, para algún i. Por tanto, $\overline{q(x)}$ tiene alguna raíz en $\mathbb{Z}/p\mathbb{Z}$.

   Considerando $\Sigma = \mathbb{Q}[i, \sqrt{2}]$, vemos que el polinomio $(x^2+1)(x^2-2)(x^2+2)$ tiene raíz modular en todo primo p, aunque carece de raíces racionales.

3. *El grupo de Galois, G, de la extensión ciclotómica n-ésima, $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ es $(\mathbb{Z}/n\mathbb{Z})^*$:* $x^n - 1$ es separable módulo p, cuando p no divide a n. $F(\overline{e^{\frac{2\pi i}{n}}}) = \overline{e^{\frac{2p\pi i}{n}}}$, luego $F_p(e^{\frac{2\pi i}{n}}) = e^{\frac{2p\pi i}{n}}$. Es decir, vía la inclusión $G \subseteq (\mathbb{Z}/n\mathbb{Z})^*$, $F_p = \bar{p}$. Concluimos porque $((\mathbb{Z}/n\mathbb{Z})^*, \cdot) = \langle p \rangle_{\{p<n, \text{ primo y no divide a } n\}}$.

4. *Para cada número natural n, existe un polinomio $p(x) \in \mathbb{Q}[x]$ de grado n cuyo grupo de Galois es S_n:* Sea $q_2(x)$ un polinomio irreducible de grado n separable con coeficientes en $\mathbb{Z}/2\mathbb{Z}$, sea $q_3(x)$ un polinomio de grado n separable con coeficientes en $\mathbb{Z}/3\mathbb{Z}$ que contenga una raíz en $\mathbb{Z}/3\mathbb{Z}$ y un factor irreducible de grado $n-1$, y sea $q_5(x)$ un polinomio separable de grado n con coeficientes en $\mathbb{Z}/5\mathbb{Z}$ que admita $n-2$ raíces y tenga un factor irreducible de grado dos. Por el

teorema chino de los restos existe un polinomio $q(x)$ de grado n con coeficientes en $\mathbb{Z}$ cuyas reducciones módulo 2, 3 y 5 son $q_2(x)$, $q_3(x)$ y $q_5(x)$, respectivamente. Entonces, F_2 opera transitivamente sobre las raíces de $q(x)$, es decir, es un n-ciclo, F_3 es un $n-1$-ciclo y F_5 es un 2-ciclo. Dejamos que el lector pruebe que $\langle F_2, F_3, F_5\rangle = S_n$.

5. **Ley de reciprocidad cuadrática de Gauss.** Dado un polinomio $p(x) \in \mathbb{Z}[x]$ de grado 2 queremos saber para qué primos $q \neq 2$ el polinomio $\overline{p(x)} \in \mathbb{F}_q[x]$ tiene raíces modulares. Este problema se reduce a estudiar el caso $p(x) = x^2 - n$, con $n \in \mathbb{Z}$. Escribiremos (el símbolo de Legendre)

$$(\frac{n}{q}) := \begin{cases} 1, & \text{si } n \text{ es un resto cuadrático módulo } q \ (\bar{n} = a^2, \text{ para cierto } a \in \mathbb{F}_q) \\ -1, & \text{en otro caso} \end{cases}$$

Recordemos que $\bar{n} \in \mathbb{F}_q^{*2}$ si y solo $\bar{n}^{(q-1)/2} = 1 \in \mathbb{F}_q^*$. Así pues, $(\frac{n}{q}) = \bar{n}^{\frac{q-1}{2}} = \pm 1 \in \mathbb{F}_q^*$ ($n \neq 0 \mod q$). Observemos que si $n' = n \mod q$, entonces $(\frac{n'}{q}) = (\frac{n}{q})$, luego podemos suponer $0 < n < q$. Además, si $n = r \cdot s$, $(\frac{n}{q}) = (\frac{r}{q}) \cdot (\frac{s}{q})$.

Descomponiendo n en producto de primos podemos suponer que $n = p$ es primo, distinto de q. Tenemos que ver qué primos q cumplen que $\bar{p} \in \mathbb{F}_q^{*2}$.

El grupo de Galois G de $\mathbb{Q}[e^{2\pi i/q}]$ es isomorfo a $\mathbb{F}_q^*$, que es cíclico. El polinomio $x^q - 1$ es separable módulo todo primo $p \neq q$. Observemos que vía el isomorfismo $G \simeq \mathbb{F}_q^*$, F_p se aplica en $\bar{p}$. Tenemos que ver cuándo $\bar{p} \in \mathbb{F}_q^{*2}$, es decir, cuándo F_p es la identidad sobre $\mathbb{Q}[e^{2\pi i/q}]^{\mathbb{F}_q^{*2}}$. $\mathbb{F}_q^*$ es un grupo cíclico, luego para cada número r que divida a $q-1$ solo existe un subgrupo de $\mathbb{F}_q^*$ de orden r. $\mathbb{F}_q^{*2}$ es el único subgrupo de índice 2 de $\mathbb{F}_q^*$. La única subextensión de grado dos de $\mathbb{Q}[e^{2\pi i/q}]$, es $K := \mathbb{Q}[e^{2\pi i/q}]^{\mathbb{F}_q^{*2}} = \mathbb{Q}[\sqrt{\Delta}] = \mathbb{Q}[\sqrt{\tilde{q}}]$, donde $\tilde{q} = (-1)^{\frac{q-1}{2}} \cdot q$. Luego, $\bar{p} \in \mathbb{F}_q^{*2}$ si y solo si F_p es la identidad sobre K.

Supongamos que $p \neq 2$, entonces $x^2 - \tilde{q}$ módulo p es separable. El automorfismo de Fröbenius de K en p, que es F_p restringido a K, es igual a la identidad cuando $\tilde{q} \in \mathbb{F}_p^{*2}$. Por tanto,

$$(\frac{p}{q}) = (\frac{\tilde{q}}{p}) = (\frac{-1}{p})^{\frac{q-1}{2}} \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot (\frac{q}{p}).$$

Supongamos $p = 2$. Como $q = 1, 3 \mod 4$ entonces $\tilde{q} = 1 \mod 4$. El cierre entero de $\mathbb{Z}[\sqrt{\tilde{q}}]$ es $\mathbb{Z}[\frac{\sqrt{\tilde{q}}+1}{2}]$. El polinomio anulador de $\frac{\sqrt{\tilde{q}}+1}{2}$ es $x^2 - x - \frac{\tilde{q}-1}{4} \in \mathbb{Z}[x]$, que es separable módulo 2. El automorfismo de Fröbenius F_2 de K en 2 es la identidad cuando las raíces de $x^2 - x - \overline{\frac{\tilde{q}-1}{4}} \in \mathbb{Z}/2\mathbb{Z}[x]$ estén en $\mathbb{Z}/2\mathbb{Z}$, es decir $\frac{\tilde{q}-1}{4}$ sea múltiplo de 2. Por tanto, observando que $\frac{\tilde{q}+1}{2}$ es impar, tenemos que

$$(\frac{2}{q}) = (-1)^{\frac{\tilde{q}-1}{4}} = (-1)^{\frac{\tilde{q}+1}{2}\cdot\frac{\tilde{q}-1}{4}} = (-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{q^2-1}{8}}.$$

4.6. Cuestionario

1. Calcula $l_{\mathbb{Z}}(\mathbb{Z}/4\mathbb{Z})$ y $l_{\mathbb{Z}}(\mathbb{Z}/12\mathbb{Z})$.
2. Calcula $l_{k[x]}(k[x]/(x^2))$, $l_{k[x]}(k[x]/(x^2\cdot(x-1)^3)$.
3. Explica detalladamente el ejemplo 4.3.3.
4. Resuelve el ejercicio 4.3.5.
5. Resuelve el ejercicio 2.6.23.
6. Resuelve el ejercicio 4.2.14.
7. Resuelve el ejercicio 4.4.2
8. Sea $\tau\colon \mathbb{R}[x,y]/(y^2-x)\to\mathbb{R}[x,y]/(y^2-x)$ el automorfismo de $\mathbb{R}$-álgebras definido por $\tau(y)=-y$ y $\tau(x)=x$ y sea $G=\{\mathrm{Id},\tau\}$. Consideremos el morfismo

$$\pi\colon \operatorname{Spec}\mathbb{R}[x,y]/(y^2-x)\to\operatorname{Spec}(\mathbb{R}[x,y]/(y^2-x))^G=\operatorname{Spec}\mathbb{R}[x]$$

   Calcula los puntos de ramificación de π. Para todo $y\in\operatorname{Spec}_{max}\mathbb{R}[x,y]/(y^2-x)$ calcula la multiplicidad con la que aparece en la fibra de $x=\pi(y)$, su grado y su grupo descomposición.
9. Resuelve el ejercicio 4.4.3
10. Consideremos el morfismo finito $\mathbb{Z}\to\mathbb{Z}[\sqrt{3}]$. Calcula el número de puntos, contando grados y multiplicidades, de las fibras de este morfismo, los puntos de ramificación e índices de ramificación.
11. Calcula el automorfismo de Fröbenius de $\mathbb{Q}[\sqrt{2}]$ en 3.
12. Resuelve el problema 9.
13. Resuelve el problema 10.
14. Calcula $(\frac{14}{23})$.
15. Sean $p<q$ números primos y supongamos $p\neq 2$. Prueba que $(\frac{p}{q})=-(\frac{q}{p})$ si y solo sí $(q-1)/2$ y $(p-1)/2$ son impares.
16. Sea $q>2$ primo. Prueba que $(\frac{2}{q})=1$ si y solo si $q+1$ ó $q-1$ es divisible por 8.
17. Sea Σ el cuerpo de fracciones de $\mathbb{C}[x,y]/(y^2-x)$ y V la variedad de Riemann de Σ. Calcula los ceros y polos de $f=\frac{y+1}{x}$ ¿Se cumple que $\sum_{v\in V}v(f)=0$?

4.7. Biografía de 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 qua-

lity 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 repre-

sentations 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/).

4.8. Problemas

1. Sea $A = k[x,y]$ y $\mathfrak{m} = (x,y)$. Calcula $l_A(A/\mathfrak{m}^3)$.

   Resolución: $l_A(A/\mathfrak{m}^3) = l_{A/\mathfrak{m}^3}(A/\mathfrak{m}^3) = \frac{\dim_k A/\mathfrak{m}^3}{\dim_k A/\mathfrak{m}} = 6$, pues una base de $A/\mathfrak{m}^3$ es $\{\bar{1}, \bar{x}, \bar{y}, \bar{x}^2, \bar{x}\bar{y}, \bar{y}^2\}$.

2. Sea $A = k[x,y]$ y $\mathfrak{m} = (x,y)$. Calcula $l_A(A/\mathfrak{m}^n)$.

   Resolución: $l_A(A/\mathfrak{m}^n) = l_{A/\mathfrak{m}^n}(A/\mathfrak{m}^n) = \frac{\dim_k A/\mathfrak{m}^n}{\dim_k A/\mathfrak{m}} = \binom{n+1}{2}$, pues el conjunto de los polinomios en dos variables de grado menor que n es un espacio vectorial de dimensión $\binom{n+1}{2}$.

3. Sea $A = \mathbb{Z}[\sqrt{-5}]$. Calcula $l_A(A/(6))$. Descompón $(6) \subset \mathbb{Z}[\sqrt{-5}]$ como producto de ideales primos.

   Resolución: $l_A(A/(6)) = l_A(A/(2)) + l_A(A/(3))$. $A/(2) = \mathbb{F}_2[x]/((x+1)^2)$, luego $l_A(A/(2)) = l_{A/(2)}(A/(2)) = l_{\mathbb{F}_2[x]}(\mathbb{F}_2[x]/((x+1)^2)) = 2$. $A/(3) = \mathbb{F}_3[x]/(x^2+2) = \mathbb{F}_3[x]/((x+1)(x+2))$, luego $l_A(A/(3)) = l_{\mathbb{F}_3[x]}(\mathbb{F}_3[x]/((x+1)(x+2))) = 2$. En conclusión, $l_A(A/(6)) = 4$.

   $(6)_0 = (2)_0 \cup (3)_0 = \{\mathfrak{m}_{x_1} = (2, \sqrt{-5}+1), \mathfrak{m}_{x_2} = (3, \sqrt{-5}+1), \mathfrak{m}_{x_3} = (3, \sqrt{-5}+2)\}$ y

   $$(6) = \mathfrak{m}_{x_1}^2 \cdot \mathfrak{m}_{x_2} \cdot \mathfrak{m}_{x_3}.$$

4. Calcula el número de puntos de corte de la curva $\mathbb{Q}$-algebraica $y^2 - x^2 - x^3 = 0$ con la recta $y - x = 0$, contando grados y multiplicidades. Calcula el grado de los puntos de corte y la multiplicidad con la que aparecen.

   Resolución: $\dim_{\mathbb{Q}} \mathbb{Q}[x,y]/(y^2 - x^2 - x^3, y - x) = \dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^3) = 3$ es el número de puntos de corte de las curvas. $Y = \operatorname{Spec} \mathbb{Q}[x,y]/(y^2 - x^2 - x^3, y - x) = \operatorname{Spec} \mathbb{Q}[x]/(x^3) = \{(x,y) = \mathfrak{m}_z\}$. La multiplicidad con la que aparece z en Y es

   $$m_z(Y) := l_{\mathbb{Q}[x]/(x^3)}(\mathbb{Q}[x]/(x^3)) = 3.$$

   El grado de z es

   $$\operatorname{gr}_{\mathbb{Q}} z = \dim_{\mathbb{Q}}(\mathbb{Q}[x]/(x^3))/\mathfrak{m}_z = \dim_{\mathbb{Q}} \mathbb{Q} = 1.$$

5. Consideremos la inclusión $\mathbb{C}[x] \hookrightarrow \mathbb{C}[[x]]$ y pasando a los cuerpos de fracciones la inclusión $\mathbb{C}(x) \hookrightarrow \mathbb{C}((x))$. Prueba que $\operatorname{sen} x \in \mathbb{C}((x)) \setminus \mathbb{C}(x)$.

   Resolución: $\operatorname{sen} x$ no tiene polos en $\operatorname{Spec} \mathbb{C}[x]$ y no es un polinomio.

6. Consideremos el morfismo $\mathbb{C}[x,y] \to \mathbb{C}[[\theta]]$, $x \mapsto \theta, y \mapsto sen\theta$. Demuestra que $\mathcal{O}_v = \mathbb{C}(x,y) \cap \mathbb{C}[[\theta]]$ es un anillo de valoración discreta, tal que $\mathcal{O}_v/\mathfrak{p}_v = \mathbb{C}$. Explicar la frase "$v(p(x,y))$ es igual a la multiplicidad de intersección de $p(x,y) = 0$ con $y = senx$, en el origen".

   Resolución: Sea $v' \colon \mathbb{C}[[\theta]] \to \mathbb{Z}$, $v'(s(\theta)) = n$ si $s(\theta) = a_n\theta^n + a_{n+1}\theta^{n+1} + \cdots$, con $a_n \neq 0$. Obviamente v' es una valoración discreta, que extiende a $\mathbb{C}((\theta))$ y cuyo anillo de valoración es $\mathbb{C}[[\theta]]$. Tenemos la composición $\mathbb{C}(x,y) \to \mathbb{C}((\theta)) \xrightarrow{v'} \mathbb{Z}$ es una valoración discreta, que denotamos v y $\mathcal{O}_v = \mathbb{C}(x,y) \cap \mathbb{C}[[\theta]]$. El núcleo del epimorfismo $\mathbb{C}[[x,y]] \to \mathbb{C}[[\theta]]$, $x \mapsto \theta, y \mapsto sen\theta$ es el ideal $(y - \operatorname{sen} x)$, luego $\mathbb{C}[[x,y]]/(y - \operatorname{sen} x) = \mathbb{C}[[\theta]]$ y

$$v(p(x,y)) = v'(p(\theta, \operatorname{sen}\theta)) = l(\mathbb{C}[[\theta]]/(p(\theta, \operatorname{sen}\theta)) = l(\mathbb{C}[[x,y]]/(y - \operatorname{sen} x, p(x,y)))$$

7. Sea p un número primo y $m > 0$ un número natural no divisible por p. Sea $K = \mathbb{F}_p[w]$, donde w es una raíz m-ésima primitiva de la unidad. Demuestra que $\dim_{\mathbb{F}_p} K$ es igual al orden de p en $(\mathbb{Z}/m\mathbb{Z})^*$.

   Resolución: El automorfismo de Fröbrenius en p de $\mathbb{Q}[e^{2\pi i/m}]$ es $F_p = \bar{p} \in (\mathbb{Z}/m\mathbb{Z})^*$. El grupo de Galois de K es isomorfo a $\langle \bar{p} \rangle$. El orden de $\langle \bar{p} \rangle$, que es igual al orden de p en $(\mathbb{Z}/m\mathbb{Z})^*$, es igual a $\dim_{\mathbb{F}_p} K$.

8. Sea $A = \mathbb{Z}[e^{2\pi i/m}]$, donde $m = p^n \cdot m'$, m' no divisible por p. Sea f el orden de p en $(\mathbb{Z}/m\mathbb{Z})^*$. Demuestra que la factorización en producto de ideales primos de (p) es

$$(p) = (\mathfrak{m}_1 \cdots \mathfrak{m}_r)^e$$

   con $r = \phi(m')/f$ y $e = \phi(p^n)$.

   Resolución: A es el anillo de números de $\mathbb{Q}[e^{2\pi i/m}]$, que es una $\mathbb{Q}$-extensión de Galois. Por tanto, $(p) = (\mathfrak{m}_1 \cdots \mathfrak{m}_r)^e$, con $\phi(p^n m') = re \cdot \dim_{\mathbb{F}_p} A/\mathfrak{m}_1$.

   Sea $B = \mathbb{Z}[e^{2\pi i/m'}]$ y $C = \mathbb{Z}[e^{2\pi i/p^n}]$. Tenemos que $A = B \otimes_{\mathbb{Z}} C$ y por tanto

$$A/pA = A \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = (B/pB) \otimes_{\mathbb{Z}/p\mathbb{Z}} (C/pC)$$

   Por el ejemplo 2.3.16, sabemos que la descomposición de (p) en B, es $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, y $\dim_{\mathbb{F}_p} B/\mathfrak{p}_i = f$ por el problema anterior. Por tanto, $s = \phi(m')/f$. Por el ejemplo 2.3.16, sabemos que la descomposición de (p) en C, es $(p) = \mathfrak{p}^u$ y $C/\mathfrak{p} = \mathbb{F}_p$.

   Por tanto, $B/pB \simeq (B/\mathfrak{p}_1)^s$ y $B/\mathfrak{p}_1 \otimes_{\mathbb{Z}/p\mathbb{Z}} C/\mathfrak{p}^e$ es una $\mathbb{F}_p$-álgebra local de cuerpo residual $B/\mathfrak{p}_1$. En conclusión, A/pA es producto de s álgebras locales de cuerpos residuales $B/\mathfrak{p}_1$. Luego, $(p) = (\mathfrak{m}_1 \cdots \mathfrak{m}_r)^e$, con $r = s = \phi(m')/f$ y $\dim_{\mathbb{F}_p}(A/\mathfrak{m}_i) = \dim_{\mathbb{F}_p} B/\mathfrak{m}_1 = f$, luego como $\phi(p^n m') = (\phi(m')/f)fe$ tendremos que $e = \phi(p^n)$.

9. Prueba que el grupo de Galois de x^3+2x^2+4x+1 es igual a S_3, argumentando con los morfismos de Fröbenius en 2 y 3.

   Resolución: Módulo 2, $x^3+2x^2+4x+1 = x^3+1 = (x+1)(x^2+x+1)$. Por tanto, F deja fija una raíz y permuta dos. Luego, F_2 es un dos ciclo. Módulo 3, $x^3+2x^2+4x+1 = x^3-x^2+x+1$ y es irreducible, luego $\langle F\rangle$ opera transitivamente y F ha de ser un tres ciclo. Luego, F_3 es un tres ciclo. Como $\langle F_2, F_3\rangle = S_3$ concluimos que el grupo de Galois es S_3.

10. Si un polinomio con coeficientes enteros mónico es irreducible módulo un número primo, entonces, ¿es irreducible? ¿Es x^4+2x^2+x+1 irreducible módulo 2? ¿Es $x^4+2x^2+x+1 \in \mathbb{Q}[x]$ irreducible? Prueba que el grupo de Galois de x^4+2x^2+x+1 es igual a S_4, argumentando con los morfismos de Fröbenius en 2 y 5.

    Resolución: Recordemos que un polinomio mónico es irreducible en $\mathbb{Z}[x]$ si y solo si lo es en $\mathbb{Q}[x]$. Obviamente, si un polinomio mónico descompone en producto de dos polinomios su reduccción módulo un primo también.

    El polinomio x^4+2x^2+x+1 no tiene raices en $\mathbb{F}_2$ y el único polinomio irreducible de grado dos (salvo producto por un escalar) es x^2+x+1. Como $x^4+2x^2+x+1 \neq (x^2+x+1)^2 = x^4+x^2+1$, tenemos que x^4+2x^2+x+1 es irreducible en $\mathbb{F}_2[x]$. Luego x^4+2x^2+x+1 es irreducible en $\mathbb{Q}[x]$. Tenemos que F_2 es un 4-ciclo porque $\langle F_2\rangle$ opera transitivamente en las raíces. Módulo 5, $x^4+2x^2+x+1 = (x-1)(x^3+x^2+3x-1)$ y x^3+x^2+3x-1 es irreducible. Luego, F_5 es un tres ciclo. Como $\langle F_2, F_5\rangle = S_4$ concluimos que el grupo de Galois es S_4.

11. Prueba que un número primo p es primo en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ si y solo si $p = 2 \mod 3$.

    Resolución: p es primo en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ si y solo si $\mathbb{Z}[e^{\frac{2\pi i}{3}}]/(p) = \mathbb{F}_p[x]/(x^2+x+1)$ es íntegro. Si $p=2$ entonces es íntegro, si $p=3$ no es íntegro. Supongamos $p \neq 2,3$. Tenemos que ver cuándo $x^2+x+1 \in \mathbb{F}_p[x]$ es irreducible, que equivale a decir que $\sqrt{-3} \notin \mathbb{F}_p$, osea $(\frac{-3}{p}) \neq 1$. Por la ley de reciprocidad cuadrática de Gauss

$$(\frac{-3}{p}) = (-1)^{\frac{p-1}{2}} \cdot (\frac{3}{p}) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{3-1}{2}} \cdot (\frac{p}{3}) = (\frac{p}{3}) = p \mod 3$$

    que es distinto de $\bar{1}$ si y solo si $p = 2 \mod 3$.

12. Prueba que la condición necesaria y suficiente para que un número entero sea de la forma a^2+b^2-ab es que en la descomposición como producto de potencias de primos los exponentes de los primos congruentes con $2 \mod 3$ sean pares. Resuelve la ecuación diofántica

$$x^2+y^2-xy = 1452$$

    Resolución El anillo de Eisenstein con la aplicación

$$N\colon \mathbb{Z}[e^{\frac{2\pi i}{3}}] \to \mathbb{N},\ N(a+be^{\frac{2\pi i}{3}}) = (a+be^{\frac{2\pi i}{3}})\cdot(a+be^{\frac{-2\pi i}{3}}) = a^2+b^2-ab$$

es euclídeo. Si p es un número primo y $p \neq 2 \mod 3$, entonces no es primo en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ y si $a+be^{\frac{2\pi i}{3}}$ es un irreducible que lo divide, entonces $p = N(a+be^{\frac{2\pi i}{3}}) = a^2+b^2-ab$. Si $n = N(z)$ y $n' = N(z')$ entonces $n \cdot n' = N(z) \cdot N(z') = N(z \cdot z')$. Si un número primo p, que es primo en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ (es decir, $p = 2 \mod 3$), divide a $n = a^2+b^2-ab = (a+be^{\frac{2\pi i}{3}}) \cdot (a+be^{\frac{-2\pi i}{3}})$ entonces p ha de dividir a $a+be^{\frac{2\pi i}{3}}$ (ó a $a+be^{\frac{-2\pi i}{3}}$), luego divide a a y b, por tanto, p^2 divide a n. Con todo es fácil concluir la afirmación del enunciado.

Resolvamos $x^2+y^2-xy = 1452$. Tenemos que $1452 = 2^2 \cdot 3 \cdot 11^2$, que 2 y 11 son primos en $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ y que $3 = (1-e^{\frac{2\pi i}{3}})(1-e^{\frac{4\pi i}{3}})$ (y $1-e^{\frac{4\pi i}{3}} = -(1-e^{\frac{2\pi i}{3}}) \cdot e^{\frac{4\pi i}{3}}$). Luego,

$$x+ye^{\frac{2\pi i}{3}} = 2 \cdot 11 \cdot (1-e^{\frac{2\pi i}{3}}) \cdot \{\pm 1, \pm e^{\frac{2\pi i}{3}}, \pm e^{\frac{-2\pi i}{3}}\}$$

y el conjunto de las soluciones son $\{\pm(22,-22), \pm(22,44), \pm(44,22)\}$.

13. Sea $K = \mathbb{Q}[e^{\frac{2\pi i}{3}}, e^{\frac{2\pi i}{p}}]$, con p primo congruente con 1 módulo 3. Sea $z \in \mathbb{Z}[e^{\frac{2\pi i}{3}}]$ no divisible por $e^{\frac{2\pi i}{3}} - 1$. Prueba que

    a) Si z es un cubo de K entonces $z \in \pm 1 + 3 \cdot \mathbb{Z}[e^{\frac{2\pi i}{3}}]$.

    b) Uno y solo uno de los elementos $\{\pm z, \pm e^{\frac{2\pi i}{3}} \cdot z, \pm e^{\frac{4\pi i}{3}} \cdot z\}$ es igual a $1 \mod (3)$.

    c) La única $\mathbb{Q}[e^{\frac{2\pi i}{3}}]$-subextensión de grado 3 de K es $\mathbb{Q}[e^{\frac{2\pi i}{3}}][\sqrt[3]{p\alpha}]$ donde $N(\alpha) = p$ y $\alpha = 1 \mod (3)$.

Resolución: Denotemos $w = e^{\frac{2\pi i}{3}}$.

a) Escribamos $z = c^3$, con $c \in K$, observemos que c es entero (sobre $\mathbb{Z}$) porque lo es sobre $\mathbb{Z}[w]$. El anillo de números de K es $A = \mathbb{Z}[w] \otimes_{\mathbb{Z}} \mathbb{Z}[e^{\frac{2\pi i}{p}}]$. Entonces, $c = \sum_{j=0}^{p-1} z_j \cdot e^{\frac{2j\pi i}{p}}$, con $z_j \in \mathbb{Z}[w]$. Entonces, $z = c^3 = \sum_{j=0}^{p-1} z_j^3 \cdot e^{\frac{6j\pi i}{p}} \mod 3$, luego $z = z_0^3 \mod 3 \cdot \mathbb{Z}[w]$. Escribamos $z_0 = a+b(\frac{2\pi i}{3}-1)$. Entonces, $z_0^3 = a^3 \mod 3 \cdot \mathbb{Z}[w]$. Por tanto, $z = a^3 \mod 3 \cdot \mathbb{Z}[w]$. Además, si hacemos cociente por $(1-w)$ tenemos que $\pm 1 = \bar{z} = \overline{a^3} \in \mathbb{Z}/3\mathbb{Z}$.

b) Escribamos $z = a+b(w-1)$. Módulo $(1-w)$, tenemos que $0 \neq \bar{z} = \bar{a} \in \mathbb{Z}/3\mathbb{Z}$. Además, $w \cdot z = (w-1+1) \cdot z = a+(a+b)(w-1) \mod (3)$ y $w^2 \cdot z = a+(2a+b)(w-1) \mod (3)$. Uno y solo uno de $b, a+b, 2a+b$ es múltiplo de 3.

c) El grupo de Galois de $\mathbb{Q}[w] \hookrightarrow K$ es igual al grupo cíclico $\mathbb{F}_p^*$ y $|\mathbb{F}_p^*| = p-1 = \dot{3}$. Por tanto, solo hay una $\mathbb{Q}[w]$-subextensión K' de grado 3 y ésta será extender por una raíz cúbica. Ahora es fácil concluir que $K' = \mathbb{Q}[w][\sqrt[3]{ab^2}]$, donde $ab^2 \in \mathbb{Z}[w]$, ningún primo de $\mathbb{Z}[w]$ al cuadrado divide a a o b y a y b son primos entre sí. Observemos que $\mathbb{Q}[w][\sqrt[3]{ab^2}] = \mathbb{Q}[w][\sqrt[3]{a^2b}]$.

Sea $\alpha \in \mathbb{Z}[w]$ un primo que divide a a y sea $\mathfrak{m}_y = (\sqrt[3]{ab^2}, \alpha) \subset \mathbb{Z}[w][\sqrt[3]{ab^2}]$. Entonces, y es un punto no singular y es un punto de ramificación del morfismo

$\mathbb{Z}[w] \to \mathbb{Z}[w][\sqrt[3]{ab^2}]$, luego (α) es un punto de rama del morfismo $\mathbb{Z}[w] \to A$, luego α divide a p. Si α divide a b, equivalentemente tendremos que divide a p.

Escribamos $p = \alpha \cdot \bar{\alpha}$, de modo que $\alpha = 1 \mod(3)$. Observemos que $\sqrt[3]{p} \notin K$, porque $\mathbb{Q}[\sqrt[3]{p}]$ no es una extensión de Galois. Por a) y b), p por cualquier invertible no es un cubo de $\mathbb{Z}[w]$. Igualmente, p^2 por cualquier invertible no es un cubo de $\mathbb{Z}[w]$. Si $\sqrt[3]{\alpha} \in K$, entonces $\sqrt[3]{\bar{\alpha}} \in K$, luego $\sqrt[3]{p} \in K$ y llegamos a contradicción. Por a) y b), α por cualquier invertible no es un cubo de $\mathbb{Z}[w]$. Igualmente, α^2 por cualquier invertible no es un cubo de $\mathbb{Z}[w]$.

14. Sean p, q dos números primos distintos, congruentes con $1 \mod 3$ y sea $\alpha, \beta \in \mathbb{Z}[e^{\frac{2\pi i}{3}}]$ tal que $N(\alpha) = p$, $N(\beta) = q$ y $\alpha, \beta = 1 \mod(3)$. Prueba que $\sqrt[3]{q} \in \mathbb{Z}/p\mathbb{Z} \iff \sqrt[3]{p\alpha} \in \mathbb{Z}/q\mathbb{Z} = \mathbb{Z}[e^{\frac{2\pi i}{3}}]/(\beta)$.

Resolución: Denotemos $w = e^{\frac{2\pi i}{3}}$ El grupo de Galois de la extensión de cuerpos $\mathbb{Q}[w] \to \mathbb{Q}[w][e^{\frac{2\pi i}{p}}]$ es $\mathbb{F}_p^*$ y el morfismo de Fröbenius en (α) es $F_q = \bar{q}$. Por tanto, $\bar{q} \in \mathbb{F}_p^{*3}$ si y solo si F_q es la identidad sobre $K = \mathbb{Q}[w][e^{\frac{2\pi i}{p}}]^{\mathbb{F}_p^{*3}} = \mathbb{Q}[w][\sqrt[3]{p\alpha}]$. Ahora bien, F_q es el morfismo de Fröbenius en (β) de K y es la identidad si y solo si $\sqrt[3]{p\alpha} \in \mathbb{Z}[w]/(\beta) = \mathbb{Z}/q\mathbb{Z}$.

15. Sea $C = \operatorname{Proj} \mathbb{C}[x_0, x_1, x_2]/(-x_0^2 + x_1^2 + x_2^2)$ la circunferencia compleja proyectiva. Calcula las asíntotas de C, en coordenadas afines $x = x_1/x_0$ e $y = x_2/x_0$ ¿En cuántos, puntos se cortan dos circunferencias reales proyectivas, y con qué multiplicidad de corte?

Resolución: Los puntos de corte de $x_0 = 0$ con $-x_0^2 + x_1^2 + x_2^2 = 0$, son los puntos $\{(0,1,i),(0,1,-i)\}$, que en coordenadas afines ($\bar{x} = x_0/x_1$ y $\bar{y} = x_2/x_1$ en $U_{x_1}^h$, son los puntos $\{(0,i),(0,-i)\}$ de la curva $-\bar{x}^2 + \bar{y}^2 + 1 = 0$. Las tangentes en estos puntos son las rectas $\bar{y} + i = 0$ y $\bar{y} - i = 0$, que proyectivamente son las rectas $x_2 + ix_1 = 0$ y $x_2 - ix_1 = 0$. Entonces, las asíntotas de C, en coordenadas afines $x = x_1/x_0$ e $y = x_2/x_0$, son las rectas $y + ix = 0$ e $y - ix = 0$.

Las circunferencias complejas cortan todas a la recta del infinito en dos puntos: $\{(0,1,i),(0,1,-i)\}$. Por tanto, las circunferencias reales cortan todas a la recta del infinito en un único punto (de grado 2). Por el teorema de Bézout dos circunferencias se cortan en cuatro puntos contando multiplicidades de corte y grado. Si las dos circunferencias reales no se cortan en ningún punto afín, han de cortarse en el punto del infinito (de grado 2) con multiplicidad de corte 2. Las que se cortan en dos puntos afines, éstos han de ser de grado 1 y han de cortarse en éstos transversalmente, y en el punto del infinito también se cortan transversalmente. Por último, si se cortan en un solo punto afín, éste ha de ser real (si no se cortarían también en el conjugado y sería también de grado 2 y llegaríamos por el teorema de Bézout a contradicción) y han de cortase en este punto con multiplicidad 2 (y transversalmente en el punto del infinito).

16. Calcula la variedad de Riemann asociada al cuerpo de funciones de la curva $y^2 - x^2 + x^3 = 0$.

Resolución: La variedad de de Riemann asociada al cuerpo de funciones de la curva $y^2 - x^2 + x^3 = 0$ es igual a la desingulariación de la curva proyectiva de ecuaciones afines $y^2 - x^2 + x^3 = 0$. Puede comprobarse que esta curva proyectiva no tiene más punto singular que el origen. La multiplicidad de esta curva (nodo) en el origen es 2 y $x = 0$ es transversal en el origen al nodo. Dividiendo por x^2, tenemos que

$$(y/x)^2 - 1 + x = 0$$

que resulta ser una curva afín no singular en todo punto. Si denotamos $z = y/x$, tenemos que $z^2 - 1 + x = 0$ son las ecuaciones afines de una curva proyectiva no singular. En conclusión, $\mathrm{Proj}\,\mathbb{R}[x_0, x_1, x_2]/(x_2^2 - x_0^2 + x_1 x_0)$ es la variedad de Riemann asociada a al cuerpo de funciones de la curva $y^2 - x^2 + x^3 = 0$ (donde $x = x_1/x_0$ y $y = zx = x_2 x_1/x_0^2$).

Capítulo 5

Teoremas fundamentales de la Teoría de Números

5.1. Introducción

Para el estudio y clasificación de los anillos de números, A, se introducen el discriminante de A, el grupo $\mathrm{Pic}(A)$ y el grupo de los invertibles de A. Dado un cuerpo de números, K tenemos la inmersión canónica $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$ y resulta que el anillo de números de K, A, es una red de $\mathbb{R}^d$. Dada $a \in A$, hay una relación fundamental entre los valores de a en las valoraciones discretas definidas por los puntos cerrados de $\mathrm{Spec}A$ y los valores absolutos de las coordenadas de $a \in \mathbb{R}^r \times \mathbb{C}^s$. La aritmética de A está ligada con cuestiones topológico-analíticas de A en su inmersión en $\mathbb{R}^d$. El discriminante de A, que es el determinante de la métrica de la traza, es igual $\pm 2^s \cdot Vol(\mathbb{R}^d/A)^2$. El teorema de Hermite afirma que solo existe un número finito de cuerpos de números de discriminante fijo dado. El grupo de los ideales de A módulo isomorfismos, $\mathrm{Pic}A$, es un grupo finito. Como consecuencia se obtiene que existe una extensión finita de K, L, tal que todo ideal de A extendido al anillo de números de L es principal. El grupo de los invertibles de A, que son los elementos de norma ± 1, es un grupo finito generado de rango $r+s-1$ y torsión el grupo de las raíces de la unidad que están en K.

Introducimos la función zeta de Riemann, que es de gran importancia en la Teoría de números en el cálculo de la distribución de los números primos. Aplicamos la función zeta de Riemann para determinar cuándo dos extensiones de Galois son isomorfas y para demostrar que un sistema de ecuaciones diofánticas tiene soluciones complejas si y solo módulo p admite soluciones enteras, para infinitos primos p.

5.2. Valores absolutos

1. Definición: Un valor absoluto sobre un anillo A es una aplicación $||: A \to \mathbb{R}$ que cumple la siguientes condiciones para todo $a, b \in A$,

1. $|a| \geq 0$; y $|a| = 0$ si y solo si $a = 0$.
2. *Desigualdad triangular:* $|a + b| \leq |a| + |b|$.
3. $|ab| = |a||b|$.

Es inmediato comprobar que todo valor absoluto cumple: $|1| = 1$ y $|-a| = |a|$. También $|n| \leq n$ para todo $n \in \mathbb{N}$. Todo anillo que posea un valor absoluto es necesariamente íntegro, y el valor absoluto extiende de modo único al cuerpo de fracciones.

La aplicación $||: A \to \mathbb{R}$ tal que $|a| := 1$ para todo $a \in A \setminus \{0\}$ y que cumple que $|0| := 0$ se denomina valor absoluto trivial.

2. Ejemplo: $||: \mathbb{Q} \to \mathbb{R}$, $|a| := a$ si $a > 0$ y $|a| := -a$ si $a < 0$ es un valor absoluto.

3. Ejercicio: Sea $p \in \mathbb{N}$ primo y $v_p : \mathbb{Q} \to \mathbb{Z}$ la valoración discreta definida por el ideal primo $(p) \subset \mathbb{Z}$. Probad que la aplicación $||_p : \mathbb{Q} \to \mathbb{R}$, $|a|_p := e^{-v_p(a)}$ es un valor absoluto.

Todo anillo A con un valor absoluto $||$ es un espacio métrico, es decir, un espacio con una distancia (o "métrica"): Se define la distancia $d(a, a') := |a - a'|$, para todo $a, a' \in A$. Por tanto, $(A, ||)$ es un espacio topológico.

4. Definición: Dos valores absolutos $||_1$ y $||_2$ sobre un cuerpo K se dicen equivalentes si existe un número real $r > 0$ tal que $|a|_1 = |a|_2^r$, para todo $a \in K$.

5. Proposición: *Dos valores absolutos sobre un cuerpo K son equivalentes si y solo si definen en K la misma topología.*

Demostración. Evidentemente, si dos valores absolutos son equivalentes definen la misma topología. Veamos el recíproco.

Dejemos al lector la consideración de los valores absolutos triviales (que se caracterizan por inducir la topología trivial). La topología determina la bola abierta unidad $B(0,1)$ de un valor absoluto:

$$|x| < 1 \iff \lim_{n\to\infty} x^n = 0.$$

Luego, si dos valores absolutos definen la misma topología sus respectivas bolas unidad son iguales.

Fijemos un punto x con $|x| > 1$, es decir, $1/x \in B(0,1)$. Dado y, tendremos que $|y| = |x|^\alpha$, para cierto número real α. Observemos que

$$\frac{n}{m} < \alpha \iff |x|^{\frac{n}{m}} < |x|^\alpha = |y| \iff \frac{|x|^{\frac{n}{m}}}{|y|} < 1 \iff \left|\frac{x^n}{y^m}\right| < 1 \iff \frac{x^n}{y^m} \in B(0,1).$$

Por tanto, si $||'$ define la misma topología que $||$, tenemos que $|y|' = |x|'^\alpha$. Si definimos $r := \log_{|x|} |x|'$, entonces $|y|' = |x|'^\alpha = (|x|^r)^\alpha = |y|^r$, para todo y. □

5.2.1. Valores absolutos no arquimedianos

6. Definición: Se dice que un valor absoluto $||: A \to \mathbb{R}$ es ultramétrico si cumple que $|a+b| \leq \max\{|a|,|b|\}$, para todo $a,b \in A$.

7. Proposición: *Dada una valoración real $v: K\backslash\{0\} \to \mathbb{R}$, la aplicación $||_v: K \to \mathbb{R}$, $|a|_v := e^{-v(a)}$ es un valor absoluto ultramétrico. Recíprocamente, dado un valor absoluto ultramétrico $||: K \to \mathbb{R}$, la aplicación $v_{||}: K\backslash\{0\} \to \mathbb{R}$, $v_{||}(a) := -\ln|a|$ es una valoración real. Por tanto,*

$$\{\textit{Valores absolutos ultramétricos de } K\}/\sim = \{\textit{Valoraciones reales de } K\}/\sim$$

8. Definición: Un valor absoluto $||: A \to \mathbb{R}$ se dice arquimediano si la imagen de la aplicación natural $\mathbb{N} \to \mathbb{R}$, $n \mapsto |n|$ no está acotada, es decir, para cada constante $C > 0$ existe un número natural n tal que $|n| > C$.

Evidentemente, todo cuerpo K dotado de un valor absoluto arquimediano debe ser de característica cero (se dice que K es de característica cero si $n := 1 + \overset{n}{\cdots} + 1 \neq 0$ en K, para todo número natural $n > 0$).

9. Ejemplo: El valor absoluto usual de $\mathbb{Q}$ es un valor absoluto arquimediano.

10. Proposición: *Un valor absoluto $||: A \to \mathbb{R}$ es no arquimediano si y solo si es ultramétrico.*

Demostración. $\Rightarrow$) Para todo natural n se cumple $|n| \leq 1$, pues si para algún natural fuera $|n| > 1$ entonces variando m, $\{|n^m| = |n|^m\}$ no sería acotado. Dados $a,b \in A$ con $|a| \leq |b|$, se tiene

$$\begin{aligned} |a+b|^n = |(a+b)^n| &\leq |a|^n + |n||a|^{n-1}|b| + \cdots + |n||a||b|^{n-1} + |b|^n \\ &\leq |a|^n + |a|^{n-1}|b| + \cdots + |a||b|^{n-1} + |b|^n \leq (1+n)|b|^n, \end{aligned}$$

de donde

$$|a+b| \leq (1+n)^{1/n}|b|,$$

y tomando límite para $n \to \infty$ se concluye que

$$|a+b| \leq 1 \cdot |b| = \max\{|a|,|b|\}.$$

$\Leftarrow$) De la desigualdad ultramétrica, resulta por inducción que $|n| \leq 1$ para todo $n \in \mathbb{N}$. □

11. Corolario: *Sea K un cuerpo de números y A el anillo de números de K. Entonces,*

$$\left\{ \begin{array}{l} \textit{Valores absolutos de } K \\ \textit{no arquimedianos, mód. equiv.} \end{array} \right\} = \left\{ \begin{array}{l} \textit{Valoraciones reales de } K, \\ \textit{mód equiv.} \end{array} \right\} = \operatorname{Spec} A$$

Por tanto, dado un valor absoluto no arquimediano $|\,|: K \to \mathbb{R}$ existe un número real $\alpha > 0$ y un punto cerrado $x \in \operatorname{Spec} A$, de modo que $|a| = e^{-\alpha \cdot v_x(a)}$, para todo $a \in K \setminus \{0\}$.

12. Corolario: *Sea K una $k(x)$-extensión finita de cuerpos y V la variedad de Riemann de K. Como los valores absolutos de K triviales sobre k son no arquimedianos, tenemos*

$$\left\{ \begin{array}{l} \textit{Valores absolutos de } K, \\ \textit{triviales sobre } k, \textit{ mód. equiv.} \end{array} \right\} = \left\{ \begin{array}{l} \textit{Valoraciones reales de } K, \\ \textit{triviales sobre } k, \textit{ mód equiv.} \end{array} \right\} =: V$$

5.2.2. Valores absolutos arquimedianos

13. Lema: *Sea $|\,|: \mathbb{N} \to \mathbb{R}$ un valor absoluto. Si $|\,|$ es arquimediano, entonces $|d| > 1$ para todo $d > 1$. Si $|\,|$ no es arquimediano, entonces $|d| \leq 1$ para todo $d \in \mathbb{N}$.*

Demostración. Supongamos que $|d| \leq 1$, para algún $d > 1$. Desarrollemos cualquier natural n en base d,

$$n = a_0 + a_1 d + \ldots + a_k d^k, \qquad \text{con } 0 \leq a_i < d,\ a_k \neq 0.$$

De donde

$$|n| \underset{|a_i| \leq d}{\leq} d + d|d| + \ldots + d|d|^k \underset{|d| \leq 1}{\leq} d(1+k) \leq d(1 + \log_d n).$$

Por tanto,

$$|n^k| \leq d(1 + \log_d n^k) = d(1 + k \log_d n).$$

Por otra parte, $|n^k| = |n|^k$. Entonces,

$$1 = \frac{|n^k|}{|n^k|} \leq \lim_{k \to \infty} \frac{d(1 + k \log_d n)}{|n|^k} = 0$$

si $|n| > 1$. Por tanto, $|n| \leq 1$, para todo n.

Supongamos $|d| > 1$, para un $d > 1$. Entonces, $|d^m| = |d|^m >> 0$, para $m >> 0$ y $|\,|$ es arquimediano.

□

14. Primer teorema de Ostrowski, 1917: *Todo valor absoluto arquimediano sobre $\mathbb{Q}$ es equivalente al valor absoluto usual.*

Demostración. Consideremos un número natural $d > 1$. Por el lema sabemos que $|d| > 1$, así que $|d| = d^\alpha$ para cierto $\alpha > 0$. Sustituyendo d por una potencia suya podemos suponer que $|d| > 2$. Basta probar que $|n| = n^\alpha$, para todo $n \in \mathbb{N}$. Desarrollemos cualquier número natural n en base d,

$$n = a_0 + a_1 d + \cdots + a_k d^k, \;\; 0 \leq a_i < d,$$

de donde

$$|n| \leq d + d|d| + \cdots + d|d|^k = d(1 + |d| + \cdots + |d|^k) = d \cdot \frac{|d|^{k+1} - 1}{|d| - 1}$$
$$\underset{|d|>2}{\leq} d|d|^{k+1} \leq d \cdot d^{\alpha\cdot(k+1)} = d^{\alpha+1} \cdot d^{k\cdot\alpha} \leq d^{\alpha+1} n^\alpha.$$

Sustituyendo en esta desigualdad n por n^k, sacando raíz k-ésima y tomado límite para $k \to \infty$, resulta $|n| \leq n^\alpha$. Si esta desigualdad fuera estricta para algún natural m, digamos $|m| = m^\beta$ con $\beta < \alpha$, entonces sustituyendo d por m en el argumento de arriba obtendriamos la desigualdad $|n| \leq n^\beta$ para todo $n \in \mathbb{N}$, lo que contradice $|d| = d^\alpha$.

□

Vamos ahora a determinar los valores absolutos arquimedianos sobre un cuerpo de números K (extensión finita de $\mathbb{Q}$).

15. Definición: Sea K un cuerpo dotado de un valor absoluto $||$. Una norma sobre un K-espacio vectorial E es una aplicación $|||| : E \to \mathbb{R}$ que cumple las siguientes propiedades:

1. $||e|| \geq 0$ para todo $e \in E$; y $||e|| = 0$ si y solo si $e = 0$.
2. Desigualdad triangular; $||e_1 + e_2|| \leq ||e_1|| + ||e_2||$, para todo $e_1, e_2 \in E$.
3. $||\lambda e|| = |\lambda| \cdot ||e||$, para todo $\lambda \in K$ y $e \in E$.

$E, ||||$ es un espacio métrico, con la distancia $d(e, e') := ||e - e'||$. Diremos que una norma $||||$ es más fina que otra $||||'$ si la topología definida por $||||$ es más fina que la definida por $||||'$. El lector puede comprobar que $||||$ es más fina que $||||'$ si y solo si existe una constante $C > 0$ de modo que $|||| \geq C \cdot ||||'$.

16. Ejemplo: Consideremos el K-espacio vectorial K^n. Se define la *norma infinita* $||||_\infty$ en K^n como sigue:

$$||(\lambda_1, \ldots \lambda_n)||_\infty := \text{máx}\{|\lambda_1|, \ldots, |\lambda_n|\}.$$

La topología definida en K^n por la norma infinita coincide con la topología producto. Toda aplicación K-lineal $K^n \to K^m$ es continua.

Si E es un K-espacio vectorial con una base $\{e_1, \ldots, e_n\}$, podemos identificar E con K^n, $E \to K^n$ $\sum_i \lambda_i e_i \mapsto (\lambda_1, \ldots, \lambda_n)$. Vía esta identificación la norma infinita de K^n define

una norma en E, que seguimos denominando norma infinita. La norma infinita es la más fina sobre E: En efecto, si $||\,||'$ es otra norma, consideremos la constante $C := \text{máx}\{||e_1||', \ldots, ||e_n)||'\}$; entonces se cumple

$$||e||' = ||\sum_i \lambda_i e_i||' \leq \sum_i |\lambda_i| ||e_i||' \leq \sum_i |\lambda_i| C \leq C \cdot n \cdot ||e||_\infty.$$

17. Proposición: *Si F es un subespacio vectorial cerrado de un espacio vectorial normado $(E, ||\,||)$, entonces*

$$||\bar{e}|| := \text{ínf}\{||e'|| : e' \in e + F\}$$

es una norma sobre E/F, y la proyección natural $E \to E/F$ es continua.

18. Proposición: *Sean $(K, |\,|)$ un cuerpo completo y E un K-espacio vectorial de dimensión finita. Todas las normas sobre E son topológicamente equivalentes y completas.*

Demostración. Es rutinario comprobar que E es completo para la norma infinita $||\,||$, y por tanto también es completo para cualquier otra norma topológicamente equivalente a la norma infinita.

Ya sabemos que cualquier norma $||\,||'$ sobre E es menos fina que la norma infinita. Para la afirmación inversa procedamos por inducción sobre $n = \dim_K E$. El caso $n = 1$ es evidente. Por hipótesis de inducción, todo subespacio de E de dimensión menor que n es completo para la norma $||\,||'$ luego también es cerrado. Por tanto, si $\{e_1, \ldots, e_n\}$ es una base de E, las proyecciones $\pi_j : E \to Ke_j$, $\pi_j(\sum_i \lambda_i e_i) := \lambda_j e_j$, son continuas tomando en E la norma $||\,||'$ y en Ke_j la norma cociente (que equivale, como todas, a la norma infinita). Por tanto, la aplicación identidad

$$(E, ||\,||') \xrightarrow{\oplus_j \pi_j} (\oplus_j Ke_j = E, ||\,||)$$

es continua. Luego la topología definida por $||\,||$ es menos fina que la de $||\,||'$. □

19. Teorema: *Sea K un cuerpo de números. Dado un valor absoluto arquimediano $|\,|$ sobre K, existe un morfismo de cuerpos $K \to \mathbb{C}$, único salvo conjugación compleja, tal que $|\,|$ es equivalente a la restricción a K del valor absoluto usual de $\mathbb{C}$. Por tanto,*

$$\left\{ \begin{array}{l} \textit{valores absolutos arquimedianos} \\ \textit{sobre } K\textit{, módulo equivalencia} \end{array} \right\} = \left\{ \begin{array}{l} \textit{morfismos } K \to \mathbb{C} \\ \textit{mód. conjugación} \end{array} \right\}$$

$$|\,|_{[\sigma]} \longleftarrow\!\shortmid [\sigma], \quad (\sigma : K \to \mathbb{C})$$

$$|f|_{[\sigma]} := |\sigma(f)|.$$

Demostración. Vamos a ver que el completado $\hat{K}$ de K se indentifica con $\mathbb{R}$ o con $\mathbb{C}$, de modo único salvo conjugación, como cuerpos y espacios topológicos. En tal caso, si denotamos por σ la composición $K \hookrightarrow \hat{K} \subset \mathbb{C}$, tenemos que la topología definida en K por $||$ es igual a la inicial por el morfismo σ, es decir, $||$ y $||_{[\sigma]}$ definen la misma topología, luego son equivalentes.

Sea $\hat{\mathbb{Q}} \to \hat{K}$ la compleción de la extensión $\mathbb{Q} \to K$ respecto del valor absoluto $||$. Como la restricción de $||$ a $\mathbb{Q}$ es equivalente al valor absoluto usual (por 5.2.14), se tiene $\hat{\mathbb{Q}} = \mathbb{R}$, dotado $\mathbb{R}$ de un valor absoluto $||$ equivalente al usual. Escribamos $K = \mathbb{Q}(a_1, ...a_n)$. El subcuerpo $\mathbb{R}(a_1, ..., a_n) \subseteq \hat{K}$ es una extensión finita de $\mathbb{R}$, así que es completo respecto $||$ por 5.2.18, luego es un cerrado de $\hat{K}$. Como este cerrado es denso en $\hat{K}$ (por contener a K), se concluye que $\mathbb{R}(a_1, ..., a_n) = \hat{K}$, es decir, $\hat{K}$ es una extensión finita de $\mathbb{R}$. Por tanto, $\hat{K} = \mathbb{R}$ ó $\hat{K} = \mathbb{C}$. Si $\hat{K} = \mathbb{R} = \hat{\mathbb{Q}}$ entonces, como hemos dicho ya, la topología definida por $||_{\hat{K}}$ en $\mathbb{R}$ es la usual. En el segundo caso, la topología definida por $||_{\hat{K}}$ sobre $\hat{K} = \mathbb{C}$ es igual a la usual de $\mathbb{C}$, porque $||_{\hat{K}}$ es una norma del $\mathbb{R}$-espacio vectorial $\hat{K} = \mathbb{C}$, y todas las normas de $\mathbb{C} = \mathbb{R}^2$ definen la misma topología (la usual). En conclusión, tenemos $K \hookrightarrow \mathbb{C}$ y la topología definida por el valor absoluto de $\mathbb{C}$ en K es igual a la topología definida definida por $||$. En cuanto a la unicidad: Supongamos que tenemos dos morfismos $\sigma_1, \sigma_2 \colon K \hookrightarrow \mathbb{C}$ de modo que la topología inicial de K es la definida por $||$. Si $\hat{K} = \mathbb{R}$ entonces $\sigma_1 = \sigma_2$. Si $\hat{\sigma}_1, \hat{\sigma}_2 \colon \hat{K} \to \mathbb{C}$ son isomorfismos de $\mathbb{R}$-álgebras, entonces $\hat{\sigma}_1 = \hat{\sigma}_2$ ó $\hat{\sigma}_1 = c \circ \hat{\sigma}_2$ (donde c es el morfismo conjugación), luego $\sigma_1 = \sigma_2$ ó $\sigma_1 = c \circ \sigma_2$. □

20. Corolario: *Sea K un un cuerpo de números y A el anillo de números de K. Entonces,*

$$\left\{ \begin{array}{l} \textit{Val. abs. de } K, \\ \textit{módulo equiv.} \end{array} \right\} = \left\{ \begin{array}{l} \textit{Val. abs. no arquimedianos} \\ \textit{de } K, \textit{ módulo equivalencia} \end{array} \right\} \coprod \left\{ \begin{array}{l} \textit{Val. abs. arquimedianos} \\ \textit{de } K, \textit{ módulo equivalencia} \end{array} \right\}$$
$$= \left\{ \begin{array}{l} \textit{Valoraciones reales de } K, \\ \textit{módulo equivalencia} \end{array} \right\} \coprod \left\{ \begin{array}{l} \textit{morfismos } K \to \mathbb{C} \\ \textit{mód. conjugación} \end{array} \right\}.$$

21. Ejercicio: Sea $||_\infty$ el valor absoluto usual de $\mathbb{Q}$. Explicitar la igualdad

$$\left\{ \begin{array}{l} \text{valores absolutos sobre } \mathbb{Q}, \\ \text{módulo equivalencia} \end{array} \right\} = \operatorname{Spec} \mathbb{Z} \coprod \{|\,|_\infty\}.$$

5.2.3. Producto de los valores absolutos de una función

A partir de ahora, en esta sección, supondremos que K es un cuerpo de números y A el anillo de números de K. En $\operatorname{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$ establezcamos la siguiente relación de equivalencia diremos que σ es equivalente a sí misma y a σ compuesta con la conjugación, que denotamos $\bar{\sigma}$.

Sea $X = \operatorname{Spec}_{\max} A$, $X_\infty = \operatorname{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})/\sim$ y $\bar{X} = X \coprod X_\infty$. Recordemos que $\bar{X}$ se identifica con los valores absolutos de K, módulo equivalencia.

22. Definición: Dado $x \in X$ definimos $\operatorname{gr} x := \ln|A/\mathfrak{m}_x|$. Dado $\sigma \in X_\infty$, diremos que $\operatorname{gr}[\sigma] = 1$, si $\sigma = \bar{\sigma}$; y $\operatorname{gr}[\sigma] = 2$, si $\sigma \neq \bar{\sigma}$.

23. Teorema: *Para toda $f \in K$, se cumple que*[1]

$$\boxed{\prod_{x \in \bar{X}} |f|_x^{\operatorname{gr} x} = 1,}$$

($|f|_x := e^{-v_x(f)}$ para cada $x \in \operatorname{Spec}_{max} A$).

Demostración. Como $f = a_1/a_2$, con $a_1, a_2 \in A$, basta probar el teorema para $f = a \in A$. Observemos que

$$|N(a)| = |\prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})} \sigma(a)| = \prod_{[\sigma] \in X_\infty} |a|_\sigma^{\operatorname{gr}[\sigma]}.$$

Por otra parte, como $(a) = \prod_{x \in X} \mathfrak{m}_x^{v_x(a)}$ entonces

$$|N(a)| = |A/aA| = |A/\prod_{x \in X} \mathfrak{m}_x^{v_x(a)}| = \prod_{x \in X} |A/\mathfrak{m}_x|^{v_x(a)} = \prod_{x \in X} e^{\operatorname{gr} x \cdot v_x(a)} = \prod_{x \in X} |a|_x^{-\operatorname{gr} x}.$$

Luego, $1 = N(a) \cdot N(a)^{-1} = \prod_{x \in \bar{X}} |f|_x^{\operatorname{gr} x}$. □

24. Definición: Dado $[\sigma] \in X_\infty$, sea $v_{[\sigma]} \colon K \setminus \{0\} \to \mathbb{R}$, $v_{[\sigma]}(f) := -\ln|\sigma(f)|$ que diremos que es una "valoración real" del infinito (que cumple que $v_{[\sigma]}(f \cdot g) = v_{[\sigma]}(f) + v_{[\sigma]}(g)$).

25. Tomando $-\ln$ en el teorema 5.2.23, obtenemos

$$\boxed{\sum_{y \in \bar{X}} v_y(f) \cdot \operatorname{gr} y = 0.}$$

Fórmula equivalente a la que se tiene en curvas algebraicas (véase teorema 4.3.11).

26. Ejercicio: Comprueba la fórmula del teorema 5.2.23, para $K = \mathbb{Q}[i]$ y $f = i + 1$.

5.3. Divisores afines y divisores completos

Sea A un dominio de Dedekind de cuerpo de fracciones K.

[1] Ver también el problema 3.

1. Definición: Llamaremos grupo de divisores afines de K, que denotaremos $\mathrm{Div}(A)$, al grupo abeliano libre de base los puntos cerrados de $\mathrm{Spec}\, A$,

$$\mathrm{Div}(A) = \oplus_{x\in \mathrm{Spec}_{max} A}\mathbb{Z}\cdot x$$

Cada $D = \sum_i n_i \cdot x_i \in \mathrm{Div}(A)$ diremos que es un divisor afín. Dado un divisor $D = \sum_{x\in \mathrm{Spec}_{max} A} n_x \cdot x$, diremos que el conjunto $\mathrm{Sop}(D) = \{x \in \mathrm{Spec}_{max} A, n_x \neq 0\}$ es el soporte de D.

2. Definición: Diremos $D = \sum_x n_x x \geq D' = \sum_x n'_x x$ si $n_x \geq n'_x$, para todo x. Diremos que $D = \sum_x n_x x$ es efectivo si $D \geq 0$.

Dado un ideal fraccionario de K, $I = \prod_i \mathfrak{m}_{x_i}^{n_i}$ denotemos $D(\prod_i \mathfrak{m}_{x_i}^{n_i}) := \sum_i n_i x_i$. Dado un divisor afín $\sum_i n_i x_i$ denotemos $I_{\sum_i n_i x_i} := \prod_i \mathfrak{m}_{x_i}^{n_i}$.

3. Proposición: *Tenemos los isomorfismos de grupos*

$$\begin{array}{rcl} \mathrm{Div}\, A & = & \{\textit{Ideales fraccionarios de } K\} \\ \{\textit{Divisores afines efectivos de } A\} & = & \{\textit{Ideales no nulos de } A\} \\ \sum_i n_i x_i & \underset{D}{\overset{I_-}{\rightleftarrows}} & \prod_i \mathfrak{m}_{x_i}^{n_i} \end{array}$$

4. Definición: Cada $f \in K$, no nula, define un divisor afín, llamado divisor afín principal, que denotamos $D(f)$:

$$D(f) = \sum_{x\in \mathrm{Spec}_{max} A} v_x(f)\cdot x$$

Se dice que dos divisores afines D, D' son afínmente equivalentes si existe $f \in K$ tal que $D = D' + D(f)$.

Si dos ideales fraccionarios no nulos $I, I' \subset K$ son isomorfos $I \simeq I'$, localizando en el punto genérico obtenemos un isomorfismo de K-módulos de K, que es multiplicar por una $f \in K$, luego $I' = f \cdot I$.

5. Proposición: *Tenemos los isomorfismos*

$$\begin{array}{rcccl} \mathrm{Pic}\, A & = & \{\textit{Ideales fraccionarios de } K\}/\simeq & = & \mathrm{Div}\, A/\sim \\ & = & \{\textit{Ideales no nulos de } A\}/\simeq & = & \{\textit{Divisores efectivos de } A\}/\sim \\ & & \left[\prod_i \mathfrak{m}_{x_i}^{n_i}\right] & \longleftrightarrow & \left[\sum_i n_i x_i\right] \end{array}$$

Demostración. Observemos que $D(f\cdot I) = D(f) + D(I)$ porque $f\cdot I = (f)\cdot I$ y $D((f)) = D(f)$. Ahora ya, es consecuencia inmediata de las proposiciones 5.3.3 y 2.2.9. □

Supongamos que K es un cuerpo de números.

6. Definición: Se define grado de un divisor afín $D = \sum_x n_x \cdot x$, que lo denotamos por $\mathrm{gr}\, D$, como

$$\mathrm{gr}\, D = \sum_x n_x \cdot \mathrm{gr}\, x.$$

7. Proposición: *Dado un ideal fraccionario $I \subseteq K$ se cumple que*

$$N(I) = e^{\mathrm{gr}(D(I))}$$

Es decir, el diagrama

$$\begin{array}{ccc} \mathrm{Div}(A) & = & \{\textit{Ideales fraccionarios}\} \\ \downarrow{\scriptstyle \mathrm{gr}} & & \downarrow{\scriptstyle N} \\ \mathbb{R} & \xrightarrow{\quad e^x \quad} & \mathbb{R}^+ \end{array}$$

es conmutativo.

Demostración. Las aplicaciones $\mathrm{Div}(A) \to \mathbb{R}^+$, $D \mapsto e^{\mathrm{gr}(D)}, N(I_D)$ son morfismos de grupos. Para ver que son iguales basta comprobar que coinciden sobre los puntos $x \in \mathrm{Spec}_{max} A$. Efectivamente, $e^{\mathrm{gr}(x)} = |A/\mathfrak{m}_x| = N(\mathfrak{m}_x) = N(I_x)$. □

La aplicación $\mathrm{gr}\colon \mathrm{Div}\, A \to \mathbb{R}$ no factoriza vía $\mathrm{Pic}\, A$, es decir, el grado de los divisores afines principales no es cero. Para solventar esta dificultad deberemos completar los divisores afines con los puntos del infinito.

8. Notación: Sea A el anillo de números de un cuerpo de números K. Sea $X = \mathrm{Spec}_{max} A$, $X_\infty = \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})/\sim$ y $\bar{X} = X \coprod X_\infty$.

9. Definición: Llamaremos grupo de los divisores completos de $\bar{X}$, que denotaremos $\mathrm{Div}(\bar{X})$, al grupo

$$\mathrm{Div}(\bar{X}) = (\bigoplus_{x \in X} \mathbb{Z} \cdot x) \oplus (\bigoplus_{[\sigma] \in X_\infty} \mathbb{R} \cdot [\sigma])$$

y diremos que $\bar{D} = \sum_{x \in X} n_x x + \sum_{[\sigma] \in X_\infty} \lambda_{[\sigma]} [\sigma]$ es un divisor completo. Diremos que $\bar{D}_{|X} := \sum_{x \in X} n_x x$ es la parte afín de $\bar{D}$ y que $\bar{D}_\infty := \sum_{[\sigma] \in X_\infty} \lambda_{[\sigma]} [\sigma]$ es la parte del infinito de $\bar{D}$.

Dado $\bar{D}' = \sum_{x \in X} n'_x x + \sum_{[\sigma] \in X_\infty} \lambda'_{[\sigma]} [\sigma]$, diremos que $\bar{D}' \geq \bar{D}$ si $n'_x \geq n_x$ y $\lambda'_{[\sigma]} \geq \lambda_{[\sigma]}$, para todo x y $[\sigma]$.

10. Definiciones: Dado $[\sigma] \in X_\infty$ y $f \in K$, denotemos $v_{[\sigma]}(f) := -\ln |\sigma(f)|$. Diremos que

$$\bar{D}(f) = \sum_{x \in \bar{X}} v_x(f) \cdot x$$

es el divisor principal completo asociado a f. El conjunto de los divisores completos principales es un subgrupo de $\mathrm{Div}(\bar{X})$. Se dice que dos divisores completos son linealmente equivalentes si difieren es un divisor completo principal, El cociente de $\mathrm{Div}(\bar{X})$ por el subgrupo de los divisores principales completos se denota $\mathrm{Pic}(\bar{X})$ y se denomina grupo de Picard completo.

11. Definición: Dado un divisor completo $\bar{D} = \sum_{x\in X} n_x \cdot x + \sum_{y\in X_\infty} \lambda_y \cdot y$ llamaremos grado de $\bar{D}$, que denotamos $\operatorname{gr}\bar{D}$, a

$$\operatorname{gr}(\bar{D}) := \sum_{x\in X} n_x \cdot \operatorname{gr} x + \sum_{y\in X_\infty} \lambda_y \cdot \operatorname{gr} y$$

Observemos que $\operatorname{gr}\colon \operatorname{Div}(\bar{X}) \to \mathbb{R}$ es un morfismo de grupos.

12. Teorema: *Para toda $f \in K$, se cumple que*

$$\operatorname{gr}(\bar{D}(f)) = 0$$

Demostración. Es consecuencia de 5.2.25 □

13. Ejercicio: Sea $\bar{X}$ el conjunto de valores absolutos de $\mathbb{Q}$, módulo equivalencia. Prueba que $\operatorname{Pic}\bar{X} = \mathbb{R}$.

5.4. Teorema de Riemann-Roch débil

1. Notación: Sea $\operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = \{\sigma_1,\dots,\sigma_r,\sigma_{r+1},\dots\sigma_{r+s},\sigma_{r+s+1} = \bar{\sigma}_{r+1},\dots,\sigma_{r+2s} = \bar{\sigma}_{r+s}\}$ (donde $\sigma_i(K) \subset \mathbb{R}$ si y solo si $i \le r$ y $\bar{\sigma}_{r+i}$ es igual a la composición de σ_{r+i} con el morfismo de conjugación). Consideremos la inmersión canónica

$$K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s,\ \ f \mapsto (\sigma_1(f),\dots,\sigma_{r+s}(f).)$$

2. Definición: Sea D' un divisor completo, definimos $\bar{I}_{D'} := \{f \in K : \bar{D}(f) \ge D'\}$.

Si $D' = n_1x_1 + \cdots + n_mx_m + \lambda_1y_1 + \cdots + \lambda_{r+s}y_{r+s}$, entonces

$$\begin{aligned}\bar{I}_{D'} &= \left\{ \begin{array}{r} f \in K : v_{x_i}(f) \ge n_i,\ \forall i \\ v_x(f) \ge 0,\ \forall x \ne x_i \end{array} \right\} \cap \left\{ f \in K : v_{y_i}(f) \ge \lambda_i,\ \forall y_i \right\} \\ &= \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m} \bigcap \{(\mu_i) \in \mathbb{R}^r \times \mathbb{C}^s : |\mu_i| \le e^{-\lambda_i},\ \forall i\}.\end{aligned}$$

3. Propiedades:

1. *Si $D' = D'' + \bar{D}(g)$, entonces $\bar{I}_{D'} = g \cdot \bar{I}_{D''} \simeq \bar{I}_{D''}$.*
2. *El conjunto $\bar{I}_{D'}$ es finito porque es la intersección de la red $\mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m}$ con el compacto $\{(\mu_j) \in \mathbb{R}^r \times \mathbb{C}^s : |\mu_j| \le e^{-\lambda_j},\ \forall j\}$, que es finito.*
3. *En el caso $D' = 0$, entonces $\bar{I}_{\{0\}} \setminus \{0\} = \{f \in K^* : \bar{D}(f) \ge 0\} = \{f \in K^* : \bar{D}(f) = 0\}$ forma un subgrupo multiplicativo de K^* que, al ser finito, ha de coincidir con las raíces n-ésimas de la unidad contenidas en K, que denotaremos μ_K.*
4. *$\bar{I}_{-D'} \setminus \{0\}/\mu_K = \{$Div. efectivos completos linealmente equiv. a $D'\}$, $[f] \mapsto D' + \bar{D}f$.*

5. *Si* $\mathrm{gr}(D')<0$ *entonces* $\bar{I}_{-D'}=\{0\}$.

6. *Si* $\mathrm{gr}(D')=0$ *y* $\bar{I}_{-D'}\neq\{0\}$*, entonces existe* f *tal que* $D'=\bar{D}(f)$.

4. Teorema del punto de la red de Minkowski: *Sea* E *un* $\mathbb{R}$*-espacio vectorial de dimensión* d*. Sea* Γ *una red de* E *y* C *un compacto de* E *convexo y simétrico respecto del origen. Si* $Vol(C)\geq 2^d Vol(E/\Gamma)$[2]*, entonces* C *contiene algún vector no nulo de la red* Γ.

Demostración. Como $Vol(\frac{1}{2}\cdot C)\geq Vol(E/\Gamma)$, la composición $\frac{1}{2}\cdot C\hookrightarrow E\to E/\Gamma$ no puede ser inyectiva (pues definiría un homeomorfismo $\frac{1}{2}\cdot C=E/\Gamma$, y por tanto una sección continua de $E\to E/\Gamma$). Por tanto, existen $x,y\in C$ distintos tales que $\frac{y-x}{2}\in\Gamma$. Como C es convexo y simétrico $\frac{y-x}{2}\in C$. □

5. Teorema de Riemann-Roch débil: *Sea* D' *un divisor completo. Si*

$$\mathrm{gr}\,D'\geq \ln\sqrt{|\Delta_K|}-s\cdot\ln(\pi/2)$$

entonces D' *es linealmente equivalente a un divisor completo efectivo.*

Demostración. Tenemos que probar que $\bar{I}_{-D'}-\{0\}\neq\emptyset$. $-D'=D(I)+D_\infty$, para cierto ideal fraccionario I y cierto divisor $D_\infty=\sum_i\lambda_i y_i$. Sea $C=\{(\mu_1,\dots,\mu_{r+s})\in\mathbb{R}^r\times\mathbb{C}^s:\ |\mu_i|\leq e^{-\lambda_i},\ \forall i\}$, entonces $\bar{I}_{-D'}=I\cap C$ y

$$Vol(\mathbb{R}^r\times\mathbb{C}^s/I)\overset{3.3.28}{=}N(I)\cdot Vol(\mathbb{R}^r\times\mathbb{C}^s/A)=N(I)\cdot 2^{-s}\sqrt{|\Delta_K|}\overset{5.3.7}{=}2^{-s}e^{\mathrm{gr}(D(I))}\cdot\sqrt{|\Delta_K|},$$
$$Vol(C)=2^r e^{-(\lambda_1+\cdots+\lambda_r)}\cdot\pi^s e^{-2(\lambda_{r+1}+\cdots+\lambda_{r+s})}=2^r(\frac{\pi}{2})^s e^{-\mathrm{gr}(D_\infty)}.$$

El teorema del punto de la red de Minkowski asegura que $\bar{I}_{-D'}\neq\{0\}$ cuando

$$2^r(\frac{\pi}{2})^s e^{-\mathrm{gr}(D_\infty)}=Vol(C)\geq 2^d Vol(\mathbb{R}^r\times\mathbb{C}^s/I)=2^r e^{\mathrm{gr}\,D(I)}\sqrt{|\Delta_K|}$$

es decir, cuando $(\frac{\pi}{2})^s e^{\mathrm{gr}\,D'}\geq\sqrt{|\Delta_K|}$. Tomando ln concluimos.

□

5.5. Finitud del grupo de Picard

1. Proposición: *Todo divisor afín* D *es afínmente equivalente a un divisor afín efectivo de grado menor o igual que* $\ln\sqrt{|\Delta_K|}$.

[2] La proporción entre volúmenes no depende del paralelepípedo de volumen 1 prefijado.

Demostración. Sea D_∞ un divisor en el infinito tal que $\mathrm{gr}(D+D_\infty) = \ln\sqrt{|\Delta_K|}$. Por el teorema de Riemann-Roch débil, existe $f \in K$ tal que $D+D_\infty+\bar{D}f$ es un divisor efectivo, de grado $\ln\sqrt{|\Delta_K|}$. Como $D+D_\infty+\bar{D}f = D+D(f)+\bar{D}(f)_\infty+D_\infty$ entonces D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que $\ln\sqrt{|\Delta_K|}$. □

2. Proposición: *Todo ideal fraccionario $I \subset K$ es isomorfo a un ideal (de A) de norma menor o igual que $\sqrt{|\Delta_K|}$.*

Demostración. Es consecuencia de la proposición anterior y 5.3.7. □

3. Teorema: $\mathrm{Pic}\,A$ *es un grupo finito.*

Demostración. El número de divisores afines efectivos de grado menor o igual que cierto número es finito. Dado $[D] \in \mathrm{Pic}\,A$, D es afínmente equivalente a un divisor afín efectivo de grado menor o igual que $\ln\sqrt{|\Delta_K|}$. □

4. Ejercicio: Sea K un cuerpo de números y A el anillo de números de K. Prueba que si todo ideal primo $\mathfrak{p}_x \subset A$, tal que $|A/\mathfrak{p}_x| \leq \sqrt{|\Delta_K|}$, es principal, entonces A es un dominio de ideales principales.

Es conocido que el anillo de números de $\mathbb{Q}[\sqrt{-r}]$, con $r > 0$ y no divisible por ningún primo al cuadrado, es de ideales principales si y solo si $r = 1,2,3,7,11,19,43,67,163$.

5. Corolario: *Sea K un cuerpo de números y A el anillo de números de K. Existe un número natural $n > 0$, de modo que todo ideal $\mathfrak{a} \subset A$ cumple que $\mathfrak{a}^n$ es principal.*

Demostración. Sea $n = |\mathrm{Pic}\,A|$. Entonces, $[\mathfrak{a}]^n = [A]$, para todo $[\mathfrak{a}] \in \mathrm{Pic}\,A$, es decir, $\mathfrak{a}^n$ es un ideal principal, para todo ideal $\mathfrak{a} \subseteq A$. □

6. Corolario: *Sea K un cuerpo de números y A el anillo de números de K. Existe una extensión finita L de K, de modo que todos los ideales de A extendidos al anillo de números de L son principales.*

Demostración. Sea $\mathfrak{a} \subset A$ un ideal y $n > 0$ tal que $\mathfrak{a}^n = (c)$ es principal. Si K' es una extensión finita de cuerpos de K que contiene a $\sqrt[n]{c}$ y B es el anillo de números de K', entonces $\mathfrak{a}\cdot B = (\sqrt[n]{c})$. En efecto, $(\mathfrak{a}\cdot B)^n = c\cdot B = (\sqrt[n]{c})^n$, luego las descomposiciones en producto de ideales primos de $\mathfrak{a}\cdot B$ y la $(\sqrt[n]{c})$ han de ser la misma, luego son iguales. Si $\mathrm{Pic}\,A = \{[\mathfrak{a}_1],\ldots,[\mathfrak{a}_n]\}$ y $\mathfrak{a}_i^n = (c_i)$, entonces $L = K[\sqrt[n]{c_1},\ldots,\sqrt[n]{c_n}]$ es la extensión de cuerpos buscada.

□

5.6. El discriminante: invariante fundamental

Veamos que el discriminante de un cuerpo de números es un invariante asociado fundamental para su clasificación.

1. Teorema de Minkowski: *Sea K un cuerpo de números. $|\Delta_K| = 1$ si y solo si $K = \mathbb{Q}$.*

Demostración. Si $\Delta_K = \pm 1$, por el teorema de Riemann-Roch 5.4.5, todo divisor completo de grado cero es principal, lo cual es imposible porque hay un número no numerable de divisores completos de grado cero y solo un número numerable de $f \in K$; salvo $|X_\infty| = 1$, es decir, salvo los casos $r = 1$ y $s = 0$ (luego $K = \mathbb{Q}$) y $r = 0$ y $s = 1$ (luego $d = 2$ y $K = \mathbb{Q}[\sqrt{n}]$ que tiene discriminante n, si $n \equiv 1 \mod 4$, o $4n$, si $n \equiv 2,3 \mod 4$).

□

2. Teorema de Hermite: *Solo hay un número finito de extensiones de $\mathbb{Q}$ de grado y discriminantes dados.*

Demostración. Sea K una extensión de discriminante Δ y grado d.

Supongamos que $i \in K$ (luego $r = 0$). Consideremos en el infinito el divisor

$$D' := (d + \ln \sqrt{|\Delta_K|}) \cdot [\sigma_1] - [\sigma_2] - \ldots - [\sigma_s]$$

El teorema de Riemann-Roch débil afirma que $\bar{I}_{-D'} \neq 0$, es decir, existe $f \in A$ no nula tal que $|\sigma_i(f)| \leq e^{-1} < 1$, para todo $i > 1$ (y $|\sigma_1(f)| \leq e^d \cdot \sqrt{|\Delta_K|}$) . Podemos pensar $\sigma_1 \colon K \hookrightarrow \mathbb{C}$ como una inclusión. Como $N(f)$ es un número entero, se sigue $|\sigma_1(f)| = |f| > 1$. Tomando $i \cdot f$ en vez de f, si es necesario, puedo suponer que f no es un número real. Sea $H = \{\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) \colon \sigma(f) = f\}$, tendremos que $|\sigma(f)| = |f| > 1$, para todo $\sigma \in H$. Por tanto, $H = \{\sigma_1\}$. Por la Teoría de Galois sabemos que $K = \mathbb{Q}[f]$ y $\mathbb{Q}[f] = \mathbb{Q}[x]/(q(x))$, con $q(x) = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})}(x - \sigma(f))$. Los coeficientes de $q(x)$ están acotados, pues sus raíces $\sigma_i(f)$ lo están, y como son números enteros solo hay un número finito de tales polinomios. Por tanto, salvo isomorfismos solo hay un número finito de extensiones K posibles.

Si $i \notin K$, entonces $|\Delta_{K[i]}| \leq |\Delta_{A[i]}| = 4^d |\Delta_A|^2 = 4^d |\Delta_K|^2$. El número de cuerpos cuyo valor absoluto del discriminante es menor que $4^d |\Delta^2|$ y grado $2d$, que contienen a i, es finito. Cada uno de estos cuerpos contiene un número finito de subextensiones. En conclusión, el número de cuerpos de discriminante Δ y grado d es finito.

□

3. La cota de Minkowski: *Sea K un cuerpo de números y $d = \dim_{\mathbb{Q}} K$. Dado un ideal fraccionario $I \subset K$, existe $f \in I$ no nula, de modo que*

$$|N(f)| \leq c|N(I)|, \text{ con } c = d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|}$$

Tomando $I = A$, obtenemos que $d < \sqrt{|\Delta_K|}$ ó $d < 3$.

Demostración. Consideremos el compacto

$$C = \{(\lambda_1, \dots, \lambda_r, \dots, \lambda_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i \le r} |\lambda_i| + \sum_{j > r} 2|\lambda_j| \le t\}.$$

Se cumple[3] que $Vol(C) = 2^r(\frac{\pi}{2})^s t^d/d!$. Sea t, de modo que $Vol(C) = 2^d Vol(\mathbb{R}^r \times \mathbb{C}^s/I)$. Entonces, por el teorema del punto de la red de Minkowski existe $f \in I$ no nula, de modo que $\sum_i |\sigma_i(f)| \le t$. Como la media geométrica está acotada por la media aritmética,

$$|N(f)| = \prod_i |\sigma_i(f)| \le (\sum_i |\sigma_i(f)|/d)^d \le t^d/d^d = d! d^{-d} (8/\pi)^s \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/I)$$
$$= d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|} \cdot |N(I)|$$

Consideremos $I = A$, entonces existe $f \in A$ de modo que $|N(f)| \le c$, luego $c \ge 1$. Para todo número natural $m \ge 3$, se cumple que $m! m^{-m} (4/\pi)^{Ent[\frac{m}{2}]} \cdot m < 1$. Se sigue que si $d \ge 3$ entonces $\sqrt{|\Delta_K|} > d$. Luego, $d < 3$ ó $d < \sqrt{|\Delta_K|}$.

□

4. Ejercicio: Sea K un cuerpo de números de discriminante -4. Prueba que $\dim_{\mathbb{Q}} K = 2$. Prueba que $K = \mathbb{Q}[i]$.

5. Ejercicio: Prueba que $K = \mathbb{Q}[\sqrt{-3}]$ es el único cuerpo de números tal que $\dim_{\mathbb{Q}} K > \sqrt{|\Delta_K|}$ y que $K = \mathbb{Q}$ es el único cuerpo de números tal que $\dim_{\mathbb{Q}} K = \sqrt{|\Delta_K|}$.

6. Corolario: *Sea A el anillo de números de un cuerpo de números K. Sea $I \subseteq A$ un ideal. Existe un ideal $I' \subset A$ isomorfo a I, de modo que $N(I') \le d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|}$.*

Demostración. Existe $f \in I^{-1}$ tal que $|N(f)| \le d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|} \cdot N(I^{-1})$, por 5.6.3. $I' := f \cdot I \subset A$ es un ideal isomorfo a I. Tomando normas, obtenemos que

$$N(I') = |N(f)| \cdot N(I) \le d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|}.$$

□

5.7. Invertibles. Elementos de norma 1

Queremos estudiar el grupo de invertibles de un anillo de números A, que coincide con el grupo de los enteros de K de norma ± 1.

Sea $\mathrm{Div}_\infty = \oplus_{y \in X_\infty} \mathbb{R} \cdot y = \mathbb{R}^{r+s}$ el espacio vectorial de los divisores completos con soporte en el infinito. El espacio vectorial Div^0_∞ de los divisores completos con soporte en el infinito de grado 0 es un hiperplano de Div_∞.

Sea A^* el conjunto de todos los invertibles de A y $\mathrm{Pic}^0_\infty := \mathrm{Div}^0_\infty / \sim = \mathrm{Div}^0_\infty / \bar{D}(A^*)$. Consideremos la sucesión exacta

$$1 \to \mu_K \to A^* \xrightarrow{\bar{D}} \mathrm{Div}^0_\infty \to \mathrm{Pic}^0_\infty \to 0$$

[3] Véase el problema 19.

1. Proposición: Pic^0_∞ *es compacto.*

Demostración. Fijemos un divisor de grado $c := \ln\sqrt{|\Delta_K|}$, $D'_\infty = \frac{c}{\mathrm{gr}\, y_1}\cdot y_1 \in \mathrm{Div}_\infty$. Sea Div^c_∞ el conjunto de los divisores con soporte en el infinito de grado c. Obviamente, $\mathrm{Div}^0_\infty = \mathrm{Div}^c_\infty$, $\bar{D} \mapsto \bar{D} + D'_\infty$, $\mathrm{Pic}^0_\infty = \mathrm{Div}^0_\infty/\bar{D}(A^*) = \mathrm{Div}^c_\infty/\bar{D}(A^*) =: \mathrm{Pic}^c_\infty$ y basta demostrar que Pic^c_∞ es compacto.

Dado $\bar{D} \in \mathrm{Div}^c_\infty$, por el teorema de Riemann-Roch débil existe $f \in K$ tal que

$$\bar{D} + \bar{D}(f) \geq 0$$

La parte afín de $\bar{D} + \bar{D}(f)$ es igual a $D(f) \geq 0$ y sea $c' = \mathrm{gr}(D(f))$. La parte del infinito de $\bar{D} + \bar{D}(f)$ es $\bar{D} + \bar{D}(f)_\infty \geq 0$, que tiene grado $c - c'$ y está en el compacto

$$C_{c-c'} := \{D'' \in \mathrm{Div}^{c-c'}_\infty : D'' \geq 0\} \subset \mathrm{Div}^{c-c'}_\infty .$$

Es decir, $\bar{D}$ pertenece al compacto $C_f := C_{c-c'} - \bar{D}(f)_\infty \subset \mathrm{Div}^c_\infty$. Observemos que $f \in A$, porque $D(f) \geq 0$ y que $\mathrm{gr}(D(f)) = c' \leq c$. El conjunto de los divisores $D(f)$, con $f \in A$, tales que $\mathrm{gr}\, D(f) \leq c$ es finito, digamos que es $\{D(f_1), \ldots, D(f_n)\}$. Entonces,

$$\mathrm{Div}^c_\infty = \bigcup_{g \in \bigcup_{i=1}^n f_i \cdot A^*} C_g \text{ y por tanto } \mathrm{Pic}^c_\infty = \cup_i \overline{C_{f_i}},$$

que es unión de un número finito de compactos, luego compacto.

□

2. Lema: *Sea* Γ *un subgrupo discreto de* $\mathbb{R}^d$. *Entonces, existen* $r \leq d$ *vectores linealmente independientes* $e_1, \ldots, e_r \in \mathbb{R}^d$ *de modo que* $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r$.

Demostración. Γ es un cerrado de $\mathbb{R}^d$: Si una sucesión $\{v_n \in \Gamma\}$ converge a $v \in \mathbb{R}^d$, entonces $v_n - v_m \to 0$, para $n, m >> 0$. Como Γ es discreto $v_n - v_m = 0$ para todo $n, m >> 0$. Luego, $v_n = v_m$ para todo $n, m >> 0$ y $v = v_n \in \Gamma$, para $n >> 0$.

Sustituyendo $\mathbb{R}^d$ por el subespacio vectorial que genera Γ, podemos suponer que Γ contiene una base de $\mathbb{R}^d$. Podemos suponer que Γ contiene la base estándar de $\mathbb{R}^d$, es decir, que $\mathbb{Z}^d \subseteq \Gamma$. Consideremos la proyección $\pi\colon \mathbb{R}^d \to \mathbb{R}^d/\mathbb{Z}^d = S^d_1$, que es abierta luego la topología de S^d_1 coincide con la topología final de π. $\pi(\Gamma)$ es un cerrado, porque $\pi^{-1}(\pi(\Gamma)) = \Gamma + \mathbb{Z}^d = \Gamma$ es un cerrado, luego es compacto. Además, $\pi(\Gamma)$ es discreto: sea U un abierto tal que $U \cap \Gamma = \mathbb{Z}^d$, entonces $\pi(U) \cap \pi(\Gamma) = \bar{0}$ es un abierto de $\pi(\Gamma)$. Por tanto, $\pi(\Gamma)$ es finito y obtenemos que Γ es finito generado. Como carece de torsión, pues está incluido en $\mathbb{R}^d$, es un grupo libre de rango d. Existen, $e_1, \ldots, e_d \in \Gamma$ tales que $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_d$ y como $e_1, \ldots, e_d$ generan $\mathbb{R}^d$, han de ser linealmente independientes en $\mathbb{R}^d$. □

3. Teorema de Dirichlet: Pic^0_∞ *es un toro de dimensión* $r+s-1$ *y los invertibles* A^* *es un grupo finito generado de rango* $r+s-1$ *y de torsión el grupo de las raíces de la unidad contenidas en* K.

Demostración. A es un subconjunto discreto de $K\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}^r\times\mathbb{C}^s$, luego A^* es un subgrupo discreto de $(\mathbb{R}^r\times\mathbb{C}^s)^*$. Consideremos el epimorfismo de grupos (que tiene sección)

$$(\mathbb{R}^r\oplus\mathbb{C}^s)^*\xrightarrow{\ln||}\mathrm{Div}_\infty,\ (\lambda_i)\mapsto\sum_i-(\ln|\lambda_i|)\cdot y_i,$$

que es una aplicación abierta de núcleo un campacto que denotamos C. La imagen de A^* es $\bar{D}(A^*)$. El núcleo del epimorfismo $A^*\to\bar{D}(A^*)$, $f\mapsto\bar{D}(f)$ es el conjunto de las raíces de la unidad contenidas en K, μ_K.

$\bar{D}(A^*)\subset\mathrm{Div}_\infty$ es discreto: sea U un abierto de $(\mathbb{R}^r\times\mathbb{C}^s)^*$ que contenga a C y tal que $U\cap A^*=\mu_K$ y W un abierto de $(\mathbb{R}^r\times\mathbb{C}^s)^*$ que contenga a 1 y tal que $C\cdot W\subseteq U$, entonces $\ln|W|\cap\bar{D}(A^*)=\{0\}$.

Por el lema anterior $\bar{D}(A^*)\subset\mathrm{Div}^0_\infty\simeq\mathbb{R}^{r+s-1}$ es un grupo libre de rango $\le r+s-1$. La compacidad de Pic^0_∞ implica que el rango de $\bar{D}(A^*)$ es $r+s-1$ y que Pic^0_∞ es un toro de dimensión $r+s-1$. Por tanto,

$$A^*\simeq\mu_K\oplus\mathbb{Z}^{r+s-1}.$$

□

4. Ejercicio: Prueba que existen $\xi_1,\dots,\xi_{r+s-1}\in A^*$, de modo que $a\in A^*$ si y solo si

$$a=\mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1}\in\mathbb{Z}$ (únicos) y una raíz n-ésima de la unidad $\mu\in\mu_K$ (única).

5. Proposición: *El subgrupo de enteros de* K *de norma* 1, $\{a\in A: N(a)=1\}$, *es un grupo abeliano libre de rango* $r+s-1$ *si* $\dim_{\mathbb{Q}}K$ *es impar, y es un grupo abeliano finito generado de rango* $r+s-1$ *y torsión* μ_K *si* $\dim_{\mathbb{Q}}K$ *es par.*

Demostración. Como $G:=\{a\in A: N(a)=1\}$ es un subgrupo de índice finito de A^* (1 ó 2) concluimos que es un grupo abeliano finito generado de rango $r+s-1$.

Si $\dim_{\mathbb{Q}}K$ es impar, entonces $r>0$, luego $K\subset\mathbb{R}$ y $\mu_K=\{\pm1\}$. Obviamente $N(-1)=-1$, por tanto la parte de torsión de G es igual a $\mu_K\cap G=\{1\}$. Si $\dim_{\mathbb{Q}}K$ es par, entonces $N(\xi)=1$ para todo $\xi\in\mu_K$: Obviamente $N(\pm1)=1$. Si $\xi\in\mu_K$ es imaginaria entonces $r=0$. Entonces, $N(a)=\prod_{i=1}^s\sigma_i(a)\bar{\sigma}_i(a)>0$, para todo $a\in A\setminus\{0\}$. Por tanto la parte de torsión de G es igual a $\mu_K\cap G=\mu_K$.

□

6. Ejercicio: Prueba que existen $\xi_1,\dots,\xi_{r+s-1}\in A$ de norma 1, de modo que $a\in A$ es de norma 1, si y solo

$$a=\begin{cases}\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_k K \text{ impar.}\\ \mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu\in\mu_K, \text{ si } \dim_k K \text{ es par.}\end{cases}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1}\in\mathbb{Z}$ (únicos). Prueba que existen además $\mu_1,\dots,\mu_i\in A$ de norma $c\in\mathbb{Z}$, de modo que $N(a)=c\in\mathbb{Z}$ si y solo

$$a=\begin{cases}\mu_i\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_k K \text{ impar.}\\ \mu_i\cdot\mu\cdot\xi_1^{n_1}\cdots\xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu\in\mu_K, \text{ si } \dim_k K \text{ es par.}\end{cases}$$

para ciertos números enteros $n_1,\dots,n_{r+s-1}\in\mathbb{Z}$ (únicos), para un i (único) (recordar el ejercicio 10).

7. Ejemplo: Sea $n>1$ un entero sin factores cuadráticos y $K=\mathbb{Q}[\sqrt{n}]$, $A=\mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$ el anillo de números de K. A^* es un grupo abeliano de rango 1 y parte de torsión ±1. Obviamente $A^*\subseteq\{\frac{a+b\sqrt{\Delta}}{2}: a,b\in\mathbb{Z}\}$ y si $N(\frac{a+b\sqrt{\Delta}}{2})=\pm1$ entonces $\frac{a+b\sqrt{\Delta}}{2}\in A^*$, porque su polinomio anulador sería $x^2-ax\pm1$. Por tanto,

$$A^*=\{\frac{a+b\sqrt{\Delta}}{2}, a,b\in\mathbb{Z}: a^2-b^2\Delta=\pm4\}=\{\pm\xi^n, \forall n\in\mathbb{Z}\}.$$

Para calcular $\xi=\frac{a+b\sqrt{\Delta}}{2}$, que es único salvo toma de inverso y multiplicación por -1, podemos suponer que $a,b>0$ y ha de ser aquel que cumpla además que a y b son mínimos.

8. Ejercicio: Calcula los invertibles de los anillos de enteros de $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ y $\mathbb{Q}[\sqrt{6}]$.

9. Sea $\mathrm{Div}^0(\bar{X})$ el conjunto de los divisores completos de grado cero. Consideremos el morfismo natural $\mathrm{Div}(\bar{X})\to\mathrm{Div}(X)$, $\bar{D}\mapsto\bar{D}_{|X}$ y la sucesión exacta,

$$0\to\mathrm{Div}^0_\infty\to\mathrm{Div}^0(\bar{X})\to\mathrm{Div}(X)\to0$$

Sea $\mathrm{Pic}^0(\bar{X})$ el grupo de las clases de equivalencia de los divisores completos de grado 0. La sucesión exacta

$$0\to\mathrm{Pic}^0_\infty\to\mathrm{Pic}^0(\bar{X})\to\mathrm{Pic}(X)\to0$$

relaciona el grupo de Picard completo (de divisores de grado cero) con el grupo de Picard de A y Pic^0_∞.

5.8. Número de ideales de norma acotada

1. Teorema: *Sea $S(n)$ el número de ideales de A de norma $\leq n$. Existe una constante no nula v tal que*

$$S(n) = vn + O(n^{1-1/d})$$

(donde entendemos que $\lim_{x\to\infty} \frac{O(x)}{x} = cte$).

Demostración. En virtud de la finitud de $\mathrm{Pic}A$, basta probar el teorema para el número $T(n)$ de ideales de norma $\leq n$ en una clase de isomorfismos dada. El conjunto de ideales de A está en correspondencia biunívoca con el conjunto de divisores afines efectivos y recordemos que si I es un ideal de norma n, entonces $D(I)$ es un divisor de grado $\ln n$. Por tanto, $T(n)$ es el número de divisores afines efectivos, D', de grado $\leq \ln n$, afínmente equivalentes a un divisor afín efectivo dado (que es equivalente a un divisor $-D(\mathfrak{a})$, para cierto ideal $\mathfrak{a} \subset A$). Sea $m = \mathrm{gr}D(\mathfrak{a})$. La condición $D' = D(f) - D(\mathfrak{a}) \geq 0$ significa que $f \in \mathfrak{a}$, y la condición $\mathrm{gr}(D(f) - D(\mathfrak{a})) = \mathrm{gr}(D(f)) - \mathrm{gr}D(\mathfrak{a}) \leq \ln n$ significa $-\mathrm{gr}(\bar{D}(f)_\infty) = \mathrm{gr}(D(f)) \leq \ln n + m$. Es decir,

$$T(n) = \text{Nº de conjuntos } fA^* \text{ tales que } fA^* \subset \mathfrak{a} \text{ y } -\mathrm{gr}(\bar{D}(f)_\infty) \leq \ln n + m.$$

(observemos que $-\mathrm{gr}(\bar{D}(g)_\infty) = \mathrm{gr}(D(g)) = \mathrm{gr}(D(f))$ para toda $g \in f \cdot A^*$).

Consideremos los morfismos

$$\begin{array}{ccccc} (\mathbb{R}^r \oplus \mathbb{C}^s)^* & \overset{\bar{D}_\infty}{\to} & \mathrm{Div}_\infty & \overset{-\mathrm{gr}}{\to} & \mathbb{R} \\ (\lambda_1, \ldots, \lambda_{r+s}) & \mapsto & -\sum_i (\ln|\lambda_i|) \cdot y_i & & \end{array}$$

Observemos que $\mathrm{Ker}\bar{D}_{\infty|A} = \{a \in A : \bar{D}(a)_\infty = 0\} = \{a \in A : \bar{D}(a) = 0\} = \mu_K$. Por lo tanto, $fA^* \subset \mathfrak{a}$ si y solo si $\bar{D}_\infty(fA^*) \subset \bar{D}_\infty(\mathfrak{a})$.
Consideremos el divisor de grado 1 con soporte en el infinito, $D'_\infty = \frac{1}{d} \cdot (y_1 + \cdots + y_{r+s})$, entonces $\mathrm{Div}_\infty = \mathrm{Div}^0_\infty \oplus \mathbb{R} \cdot D'_\infty$. Sea $P \subset \mathrm{Div}^0_\infty$ un paralelepípedo fundamental de la red $\bar{D}(A^*) = \bar{D}_\infty(A^*)$ en Div^0_∞, luego $\mathrm{Div}^0_\infty = \bar{D}_\infty(A^*) \oplus P$ y

$$\mathrm{Div}_\infty = \bar{D}_\infty(A^*) \oplus P \oplus \mathbb{R} \cdot D'_\infty.$$

Dado $f \cdot A^*$, entonces existe un único $p \in P$ de modo que $\bar{D}_\infty(fA^*) = \bar{D}_\infty(A^*) + p + \lambda \cdot D'_\infty$ (donde $\lambda = \mathrm{gr}(\bar{D}_\infty(f))$). Luego, $\bar{D}_\infty(fA^*) \cap \bar{D}_\infty(\mathfrak{a}) \neq \emptyset$ si y solo si $(P \oplus \mathbb{R} \cdot D'_\infty) \cap \bar{D}_\infty(\mathfrak{a}) = \{p + \lambda \cdot D'_\infty\}$. Por tanto, $T(n) = |(P \oplus [-\ln n - m, \infty) \cdot D'_\infty) \cap \bar{D}_\infty(\mathfrak{a})|$. Luego,

$$T(n) = \frac{|\bar{D}_\infty^{-1}(P \oplus [-\ln n - m, \infty) \cdot D'_\infty) \cap \mathfrak{a}|}{|\mu_K|} = \frac{|(n^{\frac{1}{d}} \cdot \bar{D}_\infty^{-1}(P \oplus [-m, \infty) \cdot D'_\infty) \cap \mathfrak{a}|}{|\mu_K|}.$$

Por el lema[4] 5.8.2, hemos concluido.

□

[4] Donde $E = \mathbb{R}^r \times \mathbb{C}^s$, $\Gamma = \mathfrak{a}$ y $U = \bar{D}_\infty^{-1}(P \oplus [-m, \infty) \cdot D'_\infty) \coprod \{0\} = (0, e^m] \cdot \bar{D}_\infty^{-1}(P) \coprod \{0\}$.

2. Lema: *Sea U un recinto acotado y limitado por un número finito de hipersuperficies diferenciables en un espacio vectorial real E de dimensión d y sea $\Gamma \subset E$ una red. Si $P(\lambda)$ denota el número de puntos de $\lambda \cdot U \cap \Gamma$, existe una constante no nula v tal que*

$$P(\lambda) = v\lambda^d + O(\lambda^{d-1}).$$

Demostración. Podemos suponer que $E = \mathbb{R}^d$ y $\Gamma = \mathbb{Z}^d$. Observemos que el número de puntos de $\lambda U \cap \Gamma$ es el mismo que el de $U \cap \lambda^{-1}\Gamma$. Sea $C = \{x \in \mathbb{R}^d : 0 \le x_i \le \lambda^{-1}, \forall i\}$. Considerando la unión $\bigcup_{p \in U \cap \lambda^{-1}\Gamma} p + C$, obtenemos una figura que casi coincide con U, pues le faltan algunos puntos de U y le sobran otros, pero tales puntos están en el compacto C_ϵ de los puntos que distan $\le \epsilon = \sqrt{d}/\lambda$ del borde de U. Luego,

$$Vol(U) - Vol(C_\epsilon) \le P(\lambda) Vol(C) \le Vol(U) + Vol(C_\epsilon).$$

Como $Vol(C) = \lambda^{-d}$ y $Vol(C_\epsilon) = O(\epsilon) = O(\lambda^{-1})$ se concluye que

$$P(\lambda) = \lambda^d \cdot Vol(U) + \lambda^d O(\lambda^{-1}) = \lambda^d \cdot Vol(U) + O(\lambda^{d-1}).$$

□

5.9. La función zeta

Veamos la demostración de Euler de que el número de números primos es infinito: Dado un número finito de primos distintos $\{p_1, \dots, p_r\}$ observemos que

$$(1 - \frac{1}{p_1})^{-1} \cdots (1 - \frac{1}{p_r})^{-1} = (1 + p_1^{-1} + p_1^{-2} + \cdots) \cdots (1 + p_r^{-1} + p_r^{-2} + \cdots) = \sum_{n \in P} \frac{1}{n}$$

donde P es el conjunto de números naturales que se pueden expresar como producto de potencias de $p_1, \dots, p_r$. Denotemos $S = \sum_{n=1}^{\infty} \frac{1}{n}$. Tenemos que $S - 1 \le \int_1^\infty \frac{1}{t} dt \le S$. Como $\int_1^\infty \frac{1}{t} dt = \ln t]_1^\infty = \infty$ tenemos que $S = \infty$. Si existiese un número finito de números primos, $\{p_1, \dots, p_r\}$, entonces

$$(1 - \frac{1}{p_1})^{-1} \cdot \cdots \cdot (1 - \frac{1}{p_r})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

y hemos llegado a contradicción.

Para cada $x > 1$ consideremos la serie $S(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$. Tenemos las desigualdades $S(x) - 1 \le \int_1^\infty \frac{1}{t^x} dt \le S(x)$. Como $\int_1^\infty \frac{1}{t^x} dt = \frac{t^{1-x}}{1-x}]_1^\infty = \frac{1}{x-1}$, la serie $S(x)$ converge. Es más, como los sumandos n^{-x} son funciones continuas en x decrecientes, la serie de funciones $S(x)$ es uniformemente convergente (en los intervalos $[a, \infty)$) y converge a una función continua. Además, $\lim_{x \to 1} (x-1) \cdot S(x) = 1$. Observemos que

$$(1 - \frac{1}{p_1^x})^{-1} \cdots (1 - \frac{1}{p_r^x})^{-1} = (1 + p_1^{-x} + p_1^{-2x} + \cdots) \cdots (1 + p_r^{-x} + p_r^{-2x} + \cdots) = \sum_{n \in P} \frac{1}{n^x}.$$

Por tanto[5], $S(x) = \prod_{p \text{ primo}} (1 - \frac{1}{p^x})^{-1}$.

1. Teorema: *La serie* $\zeta(x) := \sum_{n=1}^{\infty} n^{-x}$ *es una función continua en* $(1,\infty)$ *tal que*

$$\lim_{x\to 1}(x-1)\cdot\zeta(x) = 1 \quad y \quad \zeta(x) = \prod_{p\ primo}(1-\frac{1}{p^x})^{-1}.$$

Tratemos de generalizar todas estas definiciones y resultados a los anillos de números.

2. Definición: Sea K un cuerpo de números y A el anillo de números de K. Se dice que

$$\zeta_K(x) := \sum_{0\neq \mathfrak{a}\subseteq A} N(\mathfrak{a})^{-x}$$

es la función zeta (de Dedekind) de K.

3. Ejercicio: Prueba que $\zeta(x) = \zeta_{\mathbb{Q}}(x)$.

4. Teorema: *La función* $\zeta_K(x)$ *es continua en la semirecta* $x > 1$,

$$\lim_{x\to 1}(x-1)\cdot\zeta_K(x) = v \quad y \quad \zeta_K(x) = \prod_{\mathfrak{p}}(1-\frac{1}{N(\mathfrak{p})^x})^{-1}.$$

Demostración. Por el teorema 5.8.1 el número de ideales de norma n es $v + a_n$, donde $b_n := a_1 + \cdots + a_n = O(n^{1-\frac{1}{d}})$. Por tanto, $\zeta_K(x) = v\cdot\zeta(x) + \sum_n a_n n^{-x}$ y el siguiente lema permite concluir que $\sum_n a_n n^{-x}$ es una función continua en $x > 1 - \frac{1}{d}$. Luego, $\zeta_K(x)$ lo es en $x > 1$ y

$$\lim_{x\to 1}(x-1)\cdot\zeta_K(x) = v\cdot\lim_{x\to 1}(x-1)\cdot\zeta(x) = v.$$

La igualdad $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-x} = \prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-x})^{-1}$ expresa la unicidad de la descomposición de cada ideal no nulo de A en producto de ideales primos. □

5. Lema: *Sea* (a_n) *una sucesión de números reales y sea* $b_n := a_1+\cdots+a_n$. *Si* $b_n = O(n^{\epsilon})$ *entonces la serie* $\sum_n a_n n^{-x}$ *converge uniformemente en los compactos de la semirrecta* (ϵ,∞).

Demostración. Para cada pareja de números naturales $m < r$,

$$\sum_{n=m}^{r} a_n\cdot n^{-x} = \sum_{n=m}^{r}(b_n - b_{n-1})\cdot n^{-x} = b_r r^{-x} - b_{m-1}m^{-x} + \sum_{n=m}^{r-1} b_n\cdot(n^{-x} - (n+1)^{-x}).$$

Por hipótesis existe una constante $c > 0$ tal que $|b_n| < cn^{\epsilon}$, para todo n. Luego,

$$|b_r r^{-x} - b_{m-1}m^{-x}| \le |b_r r^{-x}| + |b_{m-1}m^{-x}| \le cr^{-x+\epsilon} + c(m-1)^{\epsilon}\cdot m^{-x} \le 2cm^{-x+\epsilon}$$
$$|b_n\cdot(n^{-x} - (n+1)^{-x})| \le cn^{\epsilon}\cdot x\int_n^{n+1} t^{-x-1}dt \le c\cdot x\int_n^{n+1} t^{-x-1+\epsilon}dt.$$

[5] Recuerde el lector que toda serie de números complejos absolutamente convergente es incodicionalmente convergente.

Por tanto,

$$|\sum_{n=m}^{r} a_n \cdot n^{-x}| \leq 2cm^{-x+\epsilon} + c \cdot x \int_m^{\infty} t^{-x-1+\epsilon} dt \leq (2 + \frac{x}{-x+\epsilon}) \cdot cm^{-x+\epsilon},$$

que tiende a cero para $m >> 0$ (fijado el compacto de la semirrecta (ϵ, ∞)). □

5.10. Raíces modulares y la función zeta

1. Definición: Sea A un anillo de números, $\mathfrak{p}_x \subset A$ un ideal maximal y $\mathfrak{m}_p = (p) := \mathfrak{p}_x \cap \mathbb{Z}$. Llamaremos grado de x sobre $\mathbb{Z}$, que denotaremos $\mathrm{gr}_{\mathbb{Z}} x$, a

$$\mathrm{gr}_{\mathbb{Z}} x := l_{\mathbb{Z}}(A/\mathfrak{p}_x) = \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{p}_x = \mathrm{gr}_p x.$$

2. Ejemplo: Sea $A = \mathbb{Z}[x]/(q(x))$. Los primos de A de grado 1 sobre $\mathbb{Z}$ se corresponden con las raíces de $\overline{q(x)}$ en $\mathbb{Z}/p\mathbb{Z}$, variando p (llamadas raíces modulares de $q(x)$): Dada $y \in \mathrm{Spec}\, A$, con $\mathrm{gr}_{\mathbb{Z}} y = 1$ tenemos que $A/\mathfrak{p}_y = \mathbb{Z}/p\mathbb{Z}$ y si $\bar{x} \mapsto \bar{n}$ entonces $0 = \overline{q(x)} \mapsto q(\bar{n}) = 0$, es decir, $\bar{n}$ es una raíz modular de $q(x)$. Recíprocamente, si $\bar{n} \in \mathbb{Z}/p\mathbb{Z}$ es una raíz de $\overline{q(x)}$, entonces el núcleo del morfismo $A \to \mathbb{Z}/p\mathbb{Z}$, $\overline{p(x)} \mapsto p(\bar{n})$ es un ideal primo de A de grado 1 sobre $\mathbb{Z}$.

3. Recordemos (proposición 4.3.6) que si $\mathrm{Spec}\, A/pA = \{x_1, \ldots, x_r\}$ entonces

$$d = \mathrm{gr}_{\mathbb{Z}} x_1 \cdot m_{x_1} + \cdots + \mathrm{gr}_{\mathbb{Z}} x_r \cdot m_{x_r} \geq \mathrm{gr}_{\mathbb{Z}} x_1 + \cdots + \mathrm{gr}_{\mathbb{Z}} x_r.$$

Por tanto, $\mathrm{gr}_{\mathbb{Z}} x_i \leq d$ y el número de puntos x_i de grado m es menor o igual que d/m.

4. Notación: Dadas dos funciones continuas $f(x)$ y $g(x)$ en la semirrecta $x > 1$, escribiremos $f(x) \sim g(x)$ cuando $\lim_{x \to 1} \frac{f(x)}{g(x)}$ existe, es finito y no nulo.

Tenemos que $\zeta_K(x) \sim \frac{1}{x-1}$.

5. Lema: *Sea $m \geq 2$ un número natural y P cualquier conjunto de números primos. El producto $\prod_{p \in P}(1 - \frac{1}{p^{mx}})^{-1}$ define una función continua en la semirrecta $x > 1/2$.*

Demostración. La serie $\zeta(mx) = \sum_n (n^m)^{-x}$ es uniformemente convergente en los compactos de la semirrecta $x > 1/m$, por tanto la subserie formada por los términos correspondientes a los números n con todos sus factores primos en P es uniformemente convergente en los compactos de la semirrecta $x > 1/m$ y coincide con el productorio considerado. □

6. Teorema: *Se cumple que*

$$\zeta_K(x) \sim \prod_{\mathrm{gr}_{\mathbb{Z}} y = 1} (1 - \frac{1}{N(\mathfrak{p}_y)^x})^{-1}.$$

Demostración. Sea $P_{m,r} := \{\text{primos } p \in \mathbb{Z}, \text{ tales que el número de ideales primos de } A \text{ de grado } m \text{ sobre } \mathbb{Z} \text{ en la fibra de } (p) \text{ es } r\}$. Observemos que si $P_{m,r} \neq \emptyset$ entonces $m \cdot r \leq d$. Para cada $p \in P_{m,r}$ existen r ideales primos $\mathfrak{p}_y \subset A$ en la fibra de (p) de grado m sobre $\mathbb{Z}$ (observemos que $N(\mathfrak{p}_y) = |A/\mathfrak{p}_y| = p^m$).

Como

$$\begin{aligned}\zeta_K(x) &= \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} \cdot \prod_{\mathrm{gr}_{\mathbb{Z}}\, y>1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} \\ &= \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} \cdot \prod_{m>1, mr\leq d} \prod_{p\in P_{m,r}} (1-\frac{1}{(p^m)^x})^{-r}\end{aligned}$$

y $\prod_{p\in P_{m,r}} (1-\frac{1}{(p^m)^x})^{-r}$ definen funciones continuas en la semirrecta $x > 1/2$ según 5.10.5, hemos concluido.

□

7. Notación: Sea K un cuerpo de números y A el anillo de números de K. Con abuso de notación, diremos que un ideal primo $\mathfrak{p} \subset A$ es un ideal primo de K.

8. Teorema: *Todo cuerpo de números tiene infinitos ideales primos de grado* 1 *sobre* $\mathbb{Z}$.

Demostración. Sigamos el argumento de Euler. Si K solo tuviera un número finito de primos de grado 1, entonces

$$\frac{1}{x-1} \sim \zeta_K(x) \sim \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1}$$

y $\lim_{x\to 1} \frac{\prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1}}{1/(x-1)} = \lim_{x\to 1} (x-1) \cdot \prod_{\mathrm{gr}_{\mathbb{Z}}\, y=1} (1-\frac{1}{N(\mathfrak{p}_y)^x})^{-1} = 0$, lo que es contradictorio.

□

9. Nota Todo anillo de números A tiene un número infinito de ideales primos de grado 1 sobre $\mathbb{Z}$. Si $a \in A$ es no nulo, entonces A_a tiene un número infinito de ideales primos de grado 1 sobre $\mathbb{Z}$.

5.10.1. Aplicaciones

10. Corolario: *Todo polinomio no constante con coeficientes enteros* $q(x)$ *tiene infinitas raíces modulares. Más aún, hay infinitos números primos* p *en los que* $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ *tiene todas sus raíces en* $\mathbb{Z}/p\mathbb{Z}$.

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $q(x)$. La existencia de infinitos primos en $\mathbb{Q}[\alpha_1]$ de grado 1 sobre $\mathbb{Z}$, muestra que $q(x)$ tiene infinitas raíces raíces modulares. La existencia de infinitos primos en $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ de grado 1 sobre $\mathbb{Z}$, muestra que hay infinitos primos p en los que la reducción $\overline{q(x)}$ tiene todas sus raíces en $\mathbb{Z}/p\mathbb{Z}$. □

11. Corolario: *Dado* $0 \neq n \in \mathbb{N}$*, en la lista* $\{1+mn, m \in \mathbb{N}\}$ *existen infinitos números primos.*

Demostración. Tenemos que probar que existen infinitos primos p (podemos suponer que no dividen a n), tales que $p = 1 \in (\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}$. Ahora bien, $p = 1 \mod n$ si y solo si el automorfismo de Fröbenius en p, F_p, de $\mathbb{Q}[e^{2\pi i/n}]$ es igual al morfismo Id, es decir, $\overline{x^n - 1} \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene todas sus raíces en $\mathbb{Z}/p\mathbb{Z}$ (y son distintas). □

12. Corolario: *Sea* G *un grupo abeliano finito. Existe una extensión de Galois* $\mathbb{Q} \hookrightarrow K$ *de grupo de Galois* G*.*

Demostración. Como G es un grupo finito abeliano entonces $G \simeq \overset{r}{\underset{i=1}{\oplus}} \mathbb{Z}/n_i\mathbb{Z}$. Por el corolario 5.10.11, existen números primos distintos $p_1, \ldots, p_r$ tales que $p_i = 1 \mod n_i$, para todo i, luego $p_i - 1 = m_i \cdot n_i$. Sea $n = p_1 \cdots p_r$. El grupo de Galois de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^* = \prod_i (\mathbb{Z}/p_i\mathbb{Z})^*$. Recordemos que $(\mathbb{Z}/p_i\mathbb{Z})^*$ es un grupo cíclico (ver 4.5.1). Sea $H_i = \langle \bar{n}_i \rangle \subset \mathbb{Z}/(p_i - 1)\mathbb{Z} \simeq (\mathbb{Z}/p_i\mathbb{Z})^*$ y $H = \prod_i H_i \subset (\mathbb{Z}/n\mathbb{Z})^*$. Entonces,

$$(\mathbb{Z}/n\mathbb{Z})^*/H = \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})^*/H_i = \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \simeq G$$

y por la teoría de Galois, el grupo de Galois de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]^H$ es $(\mathbb{Z}/n\mathbb{Z})^*/H \simeq G$.

□

El teorema de Kronecker-Weber afirma que toda extensión finita de Galois de $\mathbb{Q}$ de grupo de Galois conmutativo es una subextensión de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$, para cierto n.

13. Lema: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0 &= q_1(x_1, \ldots, x_n) \\ &\cdots\cdots \\ 0 &= q_r(x_1, \ldots, x_n) \end{aligned}$$

tenga alguna solución compleja es que admita soluciones $\mathbb{Q}$*-algebraicas*

Demostración. Las soluciones complejas del sistema de ecuaciones diofánticas se corresponden biunívocamente, por el teorema de los ceros de Hilbert, con los ideales maximales de $\mathbb{C}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$. El sistema no tiene soluciones complejas si y solo si $0 = \mathbb{C}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$.

Igualmente, por el teorema de los ceros de Hilbert, el sistema no tiene soluciones algebraicas si y solo si $\mathbb{Q}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$ no tiene ideales maximales, es decir, $0 = \mathbb{Q}[x_1, \ldots, x_n]/(q_1, \ldots, q_r)$.

Concluimos porque $\mathbb{C}[x_1, \ldots, x_n]/(q_1, \ldots, q_r) = 0$ si y solo si $\mathbb{Q}[x_1, \ldots, x_n]/(q_1, \ldots, q_r) = 0$, ya que $\mathbb{C}[x_1, \ldots, x_n]/(q_1, \ldots, q_r) = \mathbb{Q}[x_1, \ldots, x_n]/(q_1, \ldots, q_r) \otimes_{\mathbb{Q}} \mathbb{C}$.

□

14. Proposición: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0 &= q_1(x_1,\dots,x_n)\\ &\cdots\cdots\\ 0 &= q_r(x_1,\dots,x_n)\end{aligned}$$

tenga alguna solución compleja es que admita soluciones modulares en infinitos primos

Demostración. Si el sistema de ecuaciones diofánticas no tiene soluciones complejas, entonces $\mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r)=0$, luego $\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)=0$. Es decir, existen polinomios $h_1,\dots,h_r\in\mathbb{Q}[x_1,\dots,x_n]$ tales que $\sum_i h_i q_i = 1$. Multiplicando por $N\in\mathbb{N}$ conveniente tenemos que $\sum_i h'_i q_i = N$, con $h'_1,\dots,h'_r\in\mathbb{Z}[x_1,\dots,x_n]$. Ahora es evidente que, salvo en los primos que dividan a N, la reducción $\bar{q}_1=0,\dots,\bar{q}_r=0$ módulo p del sistema dado carece de soluciones en $\mathbb{Z}/p\mathbb{Z}$.

Recíprocamente, si el sistema considerado tiene alguna raíz compleja, entonces el sistema admite alguna solución en una extensión finita K de $\mathbb{Q}$. Sea A el anillo de números de K. Como $K=A\otimes_{\mathbb{Z}}\mathbb{Q}$, tal solución será

$$x_1=\frac{a_1}{m_1},\dots,x_n=\frac{a_n}{m_n}$$

con $a_i\in A$ y $m_i\in\mathbb{Z}$. Sea $m=\prod_i m_i$, entonces $x_i=\frac{a_i}{m_i}\in A_m$, para todo i. Como el teorema 5.10.8 afirma la existencia de infinitos primos $\mathfrak{p}$ de grado 1 en A_m, se concluye la existencia de infinitos primos p, tales que el sistema considerado tiene solución en $\mathbb{Z}/p\mathbb{Z}=A/\mathfrak{p}$.

□

15. Definición: Sea K un cuerpo de números y A el anillo de números de K. Diremos que un ideal $\mathfrak{a}$ descompone totalmente en A (o con abuso de notación, en K) si $\mathfrak{a}=\mathfrak{p}_{x_1}\cdots\mathfrak{p}_{x_n}$ con $\mathrm{gr}_{\mathbb{Z}}\,x_i=1$, para todo i.

Observemos que $\mathfrak{a}$ descompone totalmente en A si y solo si todos los puntos de $(\mathfrak{a})_0$ son de grado 1. Sea $p(x)\in\mathbb{Z}[x]$ un polinomio, $K=\mathbb{Q}[x]/(p(x))$, p un número primo y supongamos que $\overline{p(x)}\in\mathbb{F}_p[x]$ no tiene raíces múltiples. Si A es el anillo de números de K, se cumple que $A/(p)=\mathbb{F}_p[x]/(\overline{p(x)})$. Entonces, (p) descompone totalmente en K si y solo si todas las raíces de $\overline{p(x)}\in\mathbb{F}_p[x]$ pertenecen a $\mathbb{F}_p$.

16. Teorema: *Sea K un cuerpo de números y $K\hookrightarrow L$ una extensión finita. Si casi todo primo de grado 1 sobre $\mathbb{Z}$ de K descompone totalmente en L, entonces $K=L$.*

Demostración. Sea $d=\dim_K L$. Por hipótesis, la fibra de casi todos los primos de grado 1 sobre $\mathbb{Z}$ de K está formada por d primos de L, de grado 1 sobre $\mathbb{Z}$. Además, cada primo de L de grado 1 sobre $\mathbb{Z}$, está sobre un primo de K de grado 1 sobre $\mathbb{Z}$. Luego,

$$\frac{1}{x-1}\sim\zeta_L(x)\sim\zeta_K(x)^d\sim(\frac{1}{x-1})^d$$

y $d=1$. □

17. Corolario: *Si la reducción de $q(x) \in \mathbb{Z}[x]$ módulo p descompone totalmente en casi todo p, entonces $q(x)$ descompone totalmente en $\mathbb{Q}[x]$.*

Demostración. Podemos suponer que $q(x)$ es irreducible. Sea $K = \mathbb{Q}[x]/(q(x))$ y $A = \mathbb{Z}[x]/(q(x))$. Observemos que un primo $p \in \mathbb{Z}$ descompone totalmente en A si y solo si $\overline{q(x)}$ descompone totalmente en $\mathbb{Z}/p\mathbb{Z}[x]$. Por hipótesis, casi todo primo $p \in \mathbb{Z}$ descompone totalmente en K, luego por el teorema anterior, $\mathbb{Q} = K$ y $q(x) = \lambda \cdot (x - \alpha)$ en $\mathbb{Q}[x]$. □

18. Corolario: *Si un número entero es resto cuadrático módulo casi todo primo, entonces es un cuadrado perfecto.*

Demostración. Considérese en el corolario anterior $q(x) = x^2 - n$. □

19. Corolario: *Sea K un cuerpo de números y $K \to L, L'$ dos K-extensiones de Galois. Si casi todos los primos de K de grado 1 sobre $\mathbb{Z}$ que descomponen totalmente en L también descomponen totalmente en L', entonces $L' \subseteq L$. Si $q(x), q'(x) \in \mathbb{Z}[x]$, la condición necesaria y suficiente para que todas las raíces de $q'(x)$ sean expresiones racionales de las raíces de $q(x)$ es que en casi todos los primos p en los que el automorfismo de Fröbenius de $q(x)$ sea trivial lo sea el automorfismo de Fröbenius de $q'(x)$.*

Demostración. Dado un cuerpo de números Σ denotemos A_Σ el anillo de números de Σ.

Sea $\mathfrak{q} \subset A_L$ un ideal primo, que no sea de ramificación sobre A_K, que sea de grado 1 sobre $\mathbb{Z}$. Entonces, $\mathfrak{p} = \mathfrak{q} \cap A_K$ es de grado 1 sobre $\mathbb{Z}$. Al ser $K \to L$ de Galois, tenemos que $\mathfrak{p}$ descompone totalmente es L; luego también en L' (casi siempre) por hipótesis. Es decir, $A_L/\mathfrak{p}A_L$ y $A_{L'}/\mathfrak{p}A_{L'}$ son $A_K/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$-álgebras triviales.

El morfismo natural $A_L \otimes_{A_K} A_{L'} \to A_{LL'}$ es epiyectivo en casi todo punto, porque al localizar en el punto genérico de A_K, tenemos el epimorfismo $L \otimes_K L' \to LL'$. Por tanto, (casi siempre) $A_{LL'}/\mathfrak{p}A_{LL'}$ es una $\mathbb{Z}/p\mathbb{Z}$-álgebra trivial porque tenemos el epimorfismo

$$(A_L/\mathfrak{p}A_L) \otimes_{A_K/\mathfrak{p}} (A_{L'}/\mathfrak{p}A_{L'}) \to A_{LL'}/\mathfrak{p}A_{LL'}$$

Por tanto, $\mathfrak{q}$ descompone totalmente en LL', y el corolario anterior permite concluir que $L = LL'$, es decir, $L' \subseteq L$.

□

5.11. Cuestionario

1. Sea $|\,|' \colon \mathbb{N} \to \mathbb{R}$ un valor absoluto y supongamos que $|5|' = 3$. Prueba que $|\,|'$ es arquimediano y calcula $|7|'$.

2. Calcula los valores absolutos arquimedianos de $\mathbb{Q}(e^{2\pi i/5})$ y $\mathbb{Q}(\sqrt[3]{2})$.

3. Resuelve el ejercicio 5.2.26.

4. Demuestra que $\operatorname{Pic} A = \{0\}$ si y solo si A es d.i.p.

5. Consideremos $\mathbb{Q}(i)$. Calcula $D(i+1)$ y $D(i+3)$.

6. Dados dos divisores afines $D_1 = \sum_{i=1}^{r} n_i x_i$ y $D_2 = \sum_{i=1}^{r} m_i x_i$, definimos

$$\text{ínf}\{D_1, D_2\} := \sum_{i=1}^{r} \text{ínf}\{n_i, m_i\} \cdot x_i.$$

   Sean $I_1, I_2 \subset K$ dos ideales fraccionarios. Prueba que

$$D(I_1 + I_2) = \text{ínf}\{D(I_1), D(I_2)\}.$$

7. Consideremos $\mathbb{Q}(i)$. Calcula $\bar{D}(i+1)$ y $\bar{D}(i+3)$.

8. Resuelve el ejercicio 5.3.13.

9. Denotemos $\mathfrak{p}_{x_i} := (i) \subset \mathbb{Z}$. Sea $\bar{X}$ el conjunto de valores absolutos de $\mathbb{Q}$, módulo equivalencia. Consideremos el divisor completo $\bar{D} = 2x_3 + 2x_5 \in \operatorname{Div} \bar{X}$. Calcula $\bar{I}_{-\bar{D}}$.

10. Prueba que $\mathbb{Z}[i]$ es un dominio de ideales principales.

11. Prueba que $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ es un dominio de ideales principales.

12. Prueba el ejercicio 5.6.4.

13. Calcula $\mathbb{Z}[i]^*$, $\mathbb{Z}[e^{2\pi i/3}]^*$.

14. Sea A el anillo de números de un cuerpo de números y $S(n)$ el número de $f \in A$, salvo multiplicación por invertibles, tales que $|N(f)| \leq n$. Prueba que existe una constante $v > 0$, de modo que $S(n) = v \cdot n + O(n^{1-\frac{1}{d}})$.

15. Prueba que $\zeta(x) = \zeta_{\mathbb{Q}}(x)$.

16. Sea $\mathfrak{p}_x = (7) \subset \mathbb{Z}[i]$. Calcula $\operatorname{gr}_{\mathbb{Z}} x$.

17. ¿Existen infinitos primos $p \in \mathbb{Z}$ para los que $\sqrt[7]{3} \in \mathbb{Z}/p\mathbb{Z}$?

18. ¿Existen infinitos primos $p \in \mathbb{Z}$ para los que $\sqrt{3} \notin \mathbb{Z}/p\mathbb{Z}$?

5.12. Biografía de Dirichlet

DIRICHLET BIOGRAPHY

Lejeune Dirichlet's family came from the Belgium town of Richelet where Dirichlet's grandfather lived. This explains the origin of his name which comes from "Le jeune de Richele" meaning "Young from Richelet". Dirichlets came from the neighbourhood of Liège in Belgium and not, as many had claimed, from France. His father was the postmaster of Düren, the town of his birth situated about halfway between Aachen and Cologne. Even before he entered the Gymnasium in Bonn in 1817, at the age of 12, he had developed a passion for mathematics and spent his pocket-money on buying mathematics books. At the Gymnasium he was a model pupil being:

... an unusually attentive and well-behaved pupil who was particularly interested in history as well as mathematics.

After two years at the Gymnasium in Bonn his parents decided that they would rather have him attend the Jesuit College in Cologne and there he had the good fortune to be taught by Ohm. By the age of 16 Dirichlet had completed his school qualifications and was ready to enter university. However, the standards in German universities were not high at this time so Dirichlet decided to study in Paris. It is interesting to note that some years later the standards in German universities would become the best in the world and Dirichlet himself would play a hand in the transformation.

Dirichlet set off for France carrying with him Gauss's Disquisitiones arithmeticae a work he treasured and kept constantly with him as others might do with the Bible. In Paris by May 1822, Dirichlet soon contracted smallpox. It did not keep him away from his lectures in the Collège de France and the Faculté des Sciences for long and soon he could return to lectures. He had some of the leading mathematicians as teachers and he was able to profit greatly from the experience of coming in contact with Biot, Fourier, Francoeur, Hachette, Laplace, Lacroix, Legendre, and Poisson.

From the summer of 1823 Dirichlet was employed by General Maximilien Sébastien Foy, living in his house in Paris. General Foy had been a major figure in the army during the Napoleonic Wars, retiring after Napoleon's defeat at Waterloo. In 1819 he was elected to the Chamber of Deputies where he was leader of the liberal opposition until his death. Dirichlet was very well treated by General Foy, he was well paid yet treated like a member of the family. In return Dirichlet taught German to General Foy's wife and children.

Dirichlet's first paper was to bring him instant fame since it concerned the famous Fermat's Last Theorem. The theorem claimed that for $n > 2$ there are no non-zero integers x, y, z such that $x^n + y^n = z^n$. The cases $n = 3$ and $n = 4$ had been proved by Euler and Fermat, and Dirichlet attacked the theorem for $n = 5$. If $n = 5$ then one of x, y, z is even and one is divisible by 5. There are two cases: case 1 is when the number

divisible by 5 is even, while case 2 is when the even number and the one divisible by 5 are distinct. Dirichlet proved case 1 and presented his paper to the Paris Academy in July 1825. Legendre was appointed one of the referees and he was able to prove case 2 thus completing the proof for $n = 5$. The complete proof was published in September 1825. In fact Dirichlet was able to complete his own proof of the $n = 5$ case with an argument for case 2 which was an extension of his own argument for case 1. It is worth noting that Dirichlet made a later contribution proving the $n = 14$ case (a near miss for the $n = 7$ case!).

On 28 November 1825 General Foy died and Dirichlet decided to return to Germany. He was encouraged in this by Alexander von Humboldt who made recommendations on his behalf. There was a problem for Dirichlet since in order to teach in a German university he needed an habilitation. Although Dirichlet could easily submit an habilitation thesis, this was not allowed since he did not hold a doctorate, nor could he speak Latin, a requirement in the early nineteenth century. The problem was nicely solved by the University of Cologne giving Dirichlet an honorary doctorate, thus allowing him to submit his habilitation thesis on polynomials with a special class of prime divisors to the University of Breslau. There was, however, much controversy over Dirichlet's appointment.

From 1827 Dirichlet taught at Breslau but Dirichlet encountered the same problem which made him choose Paris for his own education, namely that the standards at the university were low. Again with von Humboldt's help, he moved to the Berlin in 1828 where he was appointed at the Military College. The Military College was not the attraction, of course, rather it was that Dirichlet had an agreement that he would be able to teach at the University of Berlin. Soon after this he was appointed a professor at the University of Berlin where he remained from 1828 to 1855. He retained his position in the Military College which made his teaching and other administrative duties rather heavier than he would have liked.

Dirichlet was appointed to the Berlin Academy in 1831 and an improving salary from the university put him in a position to marry, and he married Rebecca Mendelssohn, one of the composer Felix Mendelssohn's two sisters. Dirichlet had a lifelong friend in Jacobi, who taught at Königsberg, and the two exerted considerable influence on each other in their researches in number theory.

In the 1843 Jacobi became unwell and diabetes was diagnosed. He was advised by his doctor to spend time in Italy where the climate would help him recover. However, Jacobi was not a wealthy man and Dirichlet, after visiting Jacobi and discovering his plight, wrote to Alexander von Humboldt asking him to help obtain some financial assistance for Jacobi from Friedrich Wilhelm IV. Dirichlet then made a request for assistance from Friedrich Wilhelm IV, supported strongly by Alexander von Humboldt, which was successful. Dirichlet obtained leave of absence from Berlin for eighteen months and in the autumn of 1843 set off for Italy with Jacobi and Borchardt. After stopping in several towns and attending a mathematical meeting in Lucca, they arrived in Rome on 16 November 1843. Schläfli and Steiner were also with them, Schläfli's

main task being to act as their interpreter but he studied mathematics with Dirichlet as his tutor.

Dirichlet did not remain in Rome for the whole period, but visited Sicily and then spent the winter of 1844/45 in Florence before returning to Berlin in the spring of 1845. Dirichlet had a high teaching load at the University of Berlin, being also required to teach in the Military College and in 1853 he complained in a letter to his pupil Kronecker that he had thirteen lectures a week to give in addition to many other duties. It was therefore something of a relief when, on Gauss's death in 1855, he was offered his chair at Göttingen.

Dirichlet did not accept the offer from Göttingen immediately but used it to try to obtain better conditions in Berlin. He requested of the Prussian Ministry of Culture that he be allowed to end lecturing at the Military College. However he received no quick reply to his modest request so he wrote to Göttingen accepting the offer of Gauss's chair. After he had accepted the Göttingen offer the Prussian Ministry of Culture did try to offer him improved conditions and salary but this came too late.

The quieter life in Göttingen seemed to suit Dirichlet. He had more time for research and some outstanding research students. However, sadly he was not to enjoy the new life for long. In the summer of 1858 he lectured at a conference in Montreux but while in the Swiss town he suffered a heart attack. He returned to Göttingen, with the greatest difficulty, and while gravely ill had the added sadness that his wife died of a stroke.

We should now look at Dirichlet's remarkable contributions to mathematics. We have already commented on his contributions to Fermat's Last Theorem made in 1825. Around this time he also published a paper inspired by Gauss's work on the law of biquadratic reciprocity.

He proved in 1837 that in any arithmetic progression with first term coprime to the difference there are infinitely many primes. This had been conjectured by Gauss. Davenport wrote in 1980:

Analytic number theory may be said to begin with the work of Dirichlet, and in particular with Dirichlet's memoir of 1837 on the existence of primes in a given arithmetic progression.

Shortly after publishing this paper Dirichlet published two further papers on analytic number theory, one in 1838 with the next in the following year. These papers introduce Dirichlet series and determine, among other things, the formula for the class number for quadratic forms.

His work on units in algebraic number theory Vorlesungen über Zahlentheorie (published 1863) contains important work on ideals. He also proposed in 1837 the modern definition of a function:

If a variable y is so related to a variable x that whenever a numerical value is assigned to x, there is a rule according to which a unique value of y is determined, then y is said to be a function of the independent variable x.

In mechanics he investigated the equilibrium of systems and potential theory. The-

se investigations began in 1839 with papers which gave methods to evaluate multiple integrals and he applied this to the problem of the gravitational attraction of an ellipsoid on points both inside and outside. He turned to Laplace's problem of proving the stability of the solar system and produced an analysis which avoided the problem of using series expansion with quadratic and higher terms disregarded. This work led him to the Dirichlet problem concerning harmonic functions with given boundary conditions. Some work on mechanics later in his career is of quite outstanding importance. In 1852 he studied the problem of a sphere placed in an incompressible fluid, in the course of this investigation becoming the first person to integrate the hydrodynamic equations exactly.

Dirichlet is also well known for his papers on conditions for the convergence of trigonometric series and the use of the series to represent arbitrary functions. These series had been used previously by Fourier in solving differential equations. Dirichlet's work is published in Crelle's Journal in 1828. Earlier work by Poisson on the convergence of Fourier series was shown to be non-rigorous by Cauchy. Cauchy's work itself was shown to be in error by Dirichlet who wrote of Cauchy's paper:

The author of this work himself admits that his proof is defective for certain functions for which the convergence is, however, incontestable.

Because of this work Dirichlet is considered the founder of the theory of Fourier series. Riemann, who was a student of Dirichlet, wrote in the introduction to his habilitation thesis on Fourier series that it was Dirichlet

... who wrote the first profound paper about the subject.

Dirichlet's character and teaching qualities are summed up as follows:

He was an excellent teacher, always expressing himself with great clarity. His manner was modest; in his later years he was shy and at times reserved. He seldom spoke at meetings and was reluctant to make public appearances.

At age 45 Dirichlet was described by Thomas Hirst as follows

He is a rather tall, lanky-looking man, with moustache and beard about to turn grey with a somewhat harsh voice and rather deaf. He was unwashed, with his cup of coffee and cigar. One of his failings is forgetting time, he pulls his watch out, finds it past three, and runs out without even finishing the sentence.

Koch sums up Dirichlet's contribution writing that

... important parts of mathematics were influenced by Dirichlet. His proofs characteristically started with surprisingly simple observations, followed by extremely sharp analysis of the remaining problem. With Dirichlet began the golden age of mathematics in Berlin.

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

5.13. Problemas

1. Sea $v: K \to \mathbb{Z}$ una valoración discreta y $|\,| = e^{-v(\,)}$ el valor absoluto asociado. Probar:

   a) Todos los triángulos en K son isósceles.

   b) Todos los puntos de una bola de radio r son centros de la bola de radio r.

   Resolución: a) Consideremos el triángulo definido por tres puntos $a, b, c \in K$. Podemos suponer $a = 0$. Si el lado ab tiene longitud mayor que el lado ac, entonces $v(b) < v(c)$, entonces $v(b-c) = v(b)$ y el lado bc mide igual que el ab.

   b) Precisando más en *a*), si consideremos los dos lados de igual longitud de un triángulo, resulta que el tercer lado es de longitud igual o menor. Con esto es fácil concluir *b*).

2. Calcula módulo equivalencias todos los valores absolutos que pueden definirse en $\mathbb{Z}[i]$.

   Resolución: Los valores absolutos arquimedianos que pueden definirse en $\mathbb{Z}[i]$, módulo equivalencias, se corresponden biunívocamente con los morfismos de $\mathbb{Q}[i]$, módulo conjugación, en $\mathbb{C}$. Luego tenemos un único valor absoluto arquimediano, módulo equivalencia: $|a+bi| = a^2 + b^2$.

   Los valores absolutos no arquimedianos que pueden definirse en $\mathbb{Z}[i]$, módulo equivalencias, se corresponden biunívocamente con $\operatorname{Spec}\mathbb{Z}[i]$. Precisemos más. Sea $p \in \mathbb{Z}$ un número primo tal que $p = 3 \mod 4$, es decir, $\mathfrak{p}_p := (p) \subset \mathbb{Z}[i]$ es un ideal primo. Entonces, tenemos el correspondiente valor absoluto $|a+bi|_p := p^{-2n}$, donde $a+bi \in \mathbb{Z}[i]$ es dividible por p^n y no por p^{n+1}. Sea $p = 2$ y consideremos el ideal primo $\mathfrak{p}_2 = (2, i+1)$. Entonces, tenemos el correspondiente valor absoluto $|a+bi|_2 := 2^{-n}$, donde a^2+b^2 es divisible por 2^n y no por 2^{n+1}. Sea $p \in \mathbb{Z}$ un número primo tal que $p = 1 \mod 4$, luego los dos ideales primos que contienen a p son $\mathfrak{p}_p = (p, i+c)$ y $\mathfrak{p}_{\tilde{p}} = (p, i-c)$, donde $0 < c < p$ y $c^2 = -1 \mod p$. Tenemos los correspondientes valores absolutos: Escribamos $a+bi = p^n \cdot (a'+b'i)$, con $a'+b'i$ no divisible por p y supongamos que $a'^2+b'^2$ es divisible por $p^{n'}$ y no por $p^{n'+1}$. Entonces, $|a+bi|_p = p^{-n-n'}$ y $|a+bi|_{\tilde{p}} = p^{-n}$ si $a'-b'c = 0 \mod p$; y $|a+bi|_p = p^{-n}$ y $|a+bi|_{\tilde{p}} = p^{-n-n'}$ si $a'-b'c \neq 0 \mod p$.

3. Sea K un cuerpo de números de anillo de números A. Dado $x \in \operatorname{Spec}_{max} A$ y $(p) = \mathfrak{m}_x \cap \mathbb{Z}$ definamos[6] ahora $|f|_x := p^{-v_x(f)}$ y $\operatorname{gr}_{\mathbb{Z}} x := \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{m}_x = \log_p |A/\mathfrak{m}_x|$. Prueba que

$$\prod_{x \in \bar{X}} |f|_x^{\operatorname{gr}_{\mathbb{Z}} x} = 1.$$

[6] Las definiciones que siguen son las usuales en los textos de Teoría de Números.

Resolución: Podemos suponer que $f \in A$. Entonces,

$$|N(f)| = |A/fA| = |\prod_{x\in \mathrm{Spec}\, A} A_x/fA_x| = \prod_{x\in \mathrm{Spec}\, A} |A_x/fA_x| = \prod_{x\in \mathrm{Spec}\, A} |A_x/\mathfrak{m}_x^{v_x(f)}A_x|$$
$$= \prod_{x\in \mathrm{Spec}\, A} |A_x/\mathfrak{m}_x A_x|^{v_x(f)} = \prod_{x\in \mathrm{Spec}\, A} (p^{\mathrm{gr}_{\mathbb{Z}}\, x})^{v_x(f)} = \prod_{x\in \mathrm{Spec}\, A} |f|_x^{-\mathrm{gr}_{\mathbb{Z}}\, x}.$$

Por otra parte, $|N(f)| = \prod_{[\sigma]\in X_\infty} |f|_{[\sigma]}^{\mathrm{gr}[\sigma]}$.

4. Prueba que $K \subset K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ es un conjunto denso.

   Resolución: $K = \mathbb{Q} \oplus \overset{d}{\cdots} \oplus \mathbb{Q}$ y $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R} \oplus \overset{d}{\cdots} \oplus \mathbb{R}$.

5. Prueba que si $\dim_{\mathbb{Q}} K = d$ es impar, entonces $\mu_K = \{\pm 1\}$.

   Resolución: $\dim_{\mathbb{Q}} K = r + 2s$, entonces $r > 0$ y existe algún morfismo $K \hookrightarrow \mathbb{R}$, luego $\mu_K = \{\pm 1\}$.

6. Sea $\{e_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{R}^n\}_{i=1,\ldots,n}$ una base y $c_1, \ldots, c_n$ números reales positivos tales que $c_1 \cdots c_n > |\det((a_{ij}))|$. Prueba que existe $(m_1 \ldots, m_n) \in \mathbb{Z}^n \setminus \{0\}$ tal que

$$|\sum_j a_{ij} m_j| < c_i, \ \forall i.$$

   Resolución: Sea $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n \subset \mathbb{R}^n$. $Vol(\mathbb{R}^n/\Gamma) = |\det((a_{ij}))|$. Consideremos el compacto $C := \{(\lambda_1, \cdots, \lambda_n) \in \mathbb{R}^n : |\lambda_i| \leq c_i, \text{ para todo } i\}$. $Vol(C) = 2^n \cdot c_1 \cdots c_n$. Por el teorema del punto de la red de Minkowski, existe $x = \sum_i m_i e_i \in \Gamma \cap C$ no nulo.

7. Sea K un cuerpo de números y $d = \dim_{\mathbb{Q}} K$. Prueba que para todo ideal fraccionario I de K, existe $f \in I$ tal que $|\sigma(f)| < (N(I) \cdot \sqrt{|\Delta_K|} \cdot (\frac{2}{\pi})^s)^{1/d}$, para toda $\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$.

   Resolución: Consideremos la red $I \subset RR^r \times \mathbb{C}^s$. Recordemos que $Vol(\mathbb{R}^r \times \mathbb{C}^s/I) = N(I) \cdot \sqrt{|\Delta_K|}$. Sea $C = \{(\lambda_1, \ldots, \lambda_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : |\lambda_i| \leq c\}$. $Vol(C) = 2^s((2c)^r(\pi c^2)^s) = 2^{r+s}\pi^s c^d$. Para $c = (N(I) \cdot \sqrt{|\Delta_K|} \cdot (\frac{2}{\pi})^s)^{1/d}$, se cumple que $Vol(C) \geq 2^d \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/I)$. Por el teorema del punto de red de Minkowski existe $f \in I \cap C$, es decir, lo que nos piden probar.

8. Sea K un cuerpo de números de anillo e $I \subset K$ un ideal fraccionario. Sean $c_y > 0$, con $y \in X_\infty$ tales que

$$\prod_{y\in X_\infty} c_y^{\mathrm{gr}\, y} > (\frac{2}{\pi})^s \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/I).$$

   Prueba que existe $0 \neq f \in I$, tal que $|f|_y < c_y$ para todo $y \in X_\infty$.

Resolución: Consideremos la red $I \subset \mathbb{R}^r \times \mathbb{C}^s$. Recordemos que $Vol(\mathbb{R}^r \times \mathbb{C}^s/I) = N(I)\cdot\sqrt{|\Delta_K|}$. Sea $C = \{(\lambda_1,\dots,\lambda_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : |\lambda_i| \leq c_i\}$. $Vol(C) = 2^s 2^r \pi^s \prod_{y\in X_\infty} c_y^{\mathrm{gr}\, y}$. Se cumple que $Vol(C) \geq 2^d \cdot Vol(\mathbb{R}^r \times \mathbb{C}^s/I)$. Por el teorema del punto de red de Minkowski existe $f \in I \cap C$, es decir, lo que nos piden probar.

9. Sea K un cuerpo de números de anillo de números A. Prueba que existe un ideal $\mathfrak{a} \subseteq A$ tal que $N(\mathfrak{a}) \leq \frac{d!}{d^d}\cdot(\frac{4}{\pi})^s \cdot \sqrt{|\Delta_K|}$.

   Resolución: Consideremos el ideal fraccionario $I = A$. Por la proposición 5.6.3, existe $a \in A$ tal que $N(aA) = |N(a)| \leq \frac{d!}{d^d}\cdot(\frac{4}{\pi})^s \cdot \sqrt{|\Delta_K|}$.

10. Prueba que el anillo de números de $\mathbb{Q}[\sqrt{n}]$ es un anillo de ideales principales, para $n = 5, 8, 11, -3, -4, -7, -8, -11$.

    Consideremos $K = \mathbb{Q}[\sqrt{5}]$. $\Delta_K = 5$. El anillo de números de K es $A = \mathbb{Z}[\frac{5+\sqrt{5}}{2}] = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathbb{Z}[x]/(x^2 - x - 1)$. Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z| \leq \sqrt{5} < 3$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z| = 2$. $(2)_0 = \{(2)\}$, y en este caso $\mathfrak{p}_z = (2)$.

    Consideremos $K = \mathbb{Q}[\sqrt{8}] = \mathbb{Q}[\sqrt{2}]$. $\Delta_K = 8$ y el anillo de números de K es $A = \mathbb{Z}[\frac{8+\sqrt{8}}{2}] = \mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2 - 2)$. Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z| \leq \sqrt{8} < 3$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z| = 2$. $(2)_0 = \{(2,x)\}$, luego $\mathfrak{p}_z = (x)$.

    Consideremos $K = \mathbb{Q}[\sqrt{11}]$. $\Delta_K = 44$. El anillo de números de K es

    $$A = \mathbb{Z}[\frac{44+\sqrt{44}}{2}] = \mathbb{Z}[\sqrt{11}] = \mathbb{Z}[x]/(x^2 - 11).$$

    Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z| \leq \sqrt{44} < 7$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z| = 2,3,4,5$. $(2)_0 = \{(2,x-1)\}$ y $(2,x-1) = (x-3)$. $(3)_0 = \{(3,x^2-2) = (3)\}$. $(5)_0 = \{(5,x+1) = (x-4),(5,x-1) = (x+4)\}$.

    Consideremos $K = \mathbb{Q}[\sqrt{-3}]$. $\Delta_K = -3$. El anillo de números de K es

    $$A = \mathbb{Z}[\frac{-3+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[x]/(x^2 - x + 1).$$

    Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z| \leq \sqrt{3} < 2$ son principales.

    Consideremos $K = \mathbb{Q}[\sqrt{-4}] = \mathbb{Q}[\sqrt{-1}]$. $\Delta_K = -4$. El anillo de números de K es $A = \mathbb{Z}[\frac{-4+\sqrt{-4}}{2}] = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[x]/(x^2+1)$. Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z| \leq \sqrt{4} = 2$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z| = 2$. $(2)_0 = \{(2,x+1) = (x+1)\}$.

Consideremos $K=\mathbb{Q}[\sqrt{-7}]$. $\Delta_K=-7$. El anillo de números de K es

$$A=\mathbb{Z}[\frac{-7+\sqrt{-7}}{2}]=\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]=\mathbb{Z}[x]/(x^2-x+2).$$

Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z|\leq\sqrt{7}<3$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z|=2,3$. $(2)_0=\{(2,x)=(x),(2,x-1)=(x-1)\}$ y $(3)_0=\{(3)\}$.

Consideremos $K=\mathbb{Q}[\sqrt{-8}]=\mathbb{Q}[\sqrt{-2}]$. $\Delta_K=-8$. El anillo de números de K es $A=\mathbb{Z}[\frac{-8+\sqrt{-8}}{2}]=\mathbb{Z}[\sqrt{-2}]=\mathbb{Z}[x]/(x^2+2)$. Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z|\leq\sqrt{8}<3$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z|=2$. $(2)_0=\{(2,x)=(x)\}$.

Sea $K=\mathbb{Q}[\sqrt{-11}]$. $\Delta_K=-11$. El anillo de números de K es $A=\mathbb{Z}[\frac{-11+\sqrt{-11}}{2}]=\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]=\mathbb{Z}[x]/(x^2-x+3)$. Tenemos que probar que los ideales primos $\mathfrak{p}_z$ tal que $|A/\mathfrak{p}_z|\leq\sqrt{11}<4$ son principales. Luego, solo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z|=2,3,4$. $(2)_0=\{(2)\}$ y $(3)_0=\{(3,x)=(x),(3,x-1)=(x-1)\}$.

11. Prueba que la ecuación $x_1^5+x_2^5=x_3^5$ no tiene soluciones enteras, que cumplan $x_1x_2x_3\neq 0$.

Resolución: Podemos suponer que $(x_1,x_2)=(x_1,x_3)=(x_2,x_3)=(1)$ y que x_1 y x_2 son primos con 5. Entonces, x_3 es divisible por 5, porque $x_1^5+x_2^5=x_3^5 \mod 25$, lo cual es imposible ya que $x_i^5=\pm1,\pm7$ para todo i.

Sea $\xi=e^{\frac{2\pi i}{5}}$ que es raíz del polinomio $x^4+x^3+x^2+x+1$. Si dividimos por x^2 y tomamos $y=x+\frac{1}{x}$, obtenemos el polinomio y^2+y-1, cuyas raíces son $\alpha=\xi+\frac{1}{\xi}=\frac{-1+\sqrt{5}}{2}$ y $\alpha'=\xi^2+\frac{1}{\xi^2}=\frac{-1-\sqrt{5}}{2}$. El anillo $\mathbb{Z}[\alpha]$ es de Dedekind, es el anillo de enteros de $\mathbb{Q}[\sqrt{5}]$, y por el problema 10 es un d.i.p. Además, $\mathbb{Z}[\alpha]/(\alpha-2)=\mathbb{Z}[x]/(x^2+x-1,x-2)=\mathbb{Z}/(5)$, luego $\alpha-2$ es irreducible. Por último tenemos el automorfismo de anillos de orden 2, $\tau\colon\mathbb{Z}[\alpha]\to\mathbb{Z}[\alpha]$, $\tau(\alpha)=\alpha'$ y $\mathbb{Z}[\alpha]^{\langle\tau\rangle}=\mathbb{Z}$. Observemos que $(\alpha-2)=(\alpha'-2)=(\sqrt{5})$.

Trabajemos en $\mathbb{Z}[\alpha]$. Probemos que no existen $x_1,x_2,x_3\in\mathbb{Z}[\alpha]$, de modo que sean primos dos a dos, x_3 es divisible por 5 y $x_1^2+x_2^2,x_1\cdot x_2\in\mathbb{Z}$. Consideremos una solución con $|x_1x_2x_3|$ mínimo

Tenemos que

$$(x_1+x_2)\cdot(x_1+\xi x_2)\cdot(x_1+\xi^2x_2)\cdot(x_1+\xi^3x_2)\cdot(x_1+\xi^4x_2)=x_3^5.$$

Sean

$$\begin{aligned}
s_1&=(x_1+\xi x_2)\cdot(x_1+\xi^4x_2)=x_1^2+x_2^2+\alpha\cdot x_1x_2=(x_1+x_2)^2+(\alpha-2)\cdot x_1x_2\\
s_2&=(x_1+\xi^2x_2)\cdot(x_1+\xi^3x_2)=x_1^2+x_2^2+\alpha'\cdot x_1x_2=(x_1+x_2)^2+(\alpha'-2)\cdot x_1x_2\\
s_3&=x_1+x_2
\end{aligned}$$

Entonces, $s_1 \cdot s_2 \cdot s_3 = -x_3^5$. Observemos que $x_1 + x_2$ y s_1 son primos con x_1 y x_2. Tenemos que

$$(x_1 + x_2, s_1) = (x_1 + x_2, (2-\alpha)x_1^2) = (x_1 + x_2, 2-\alpha) = (\alpha - 2)$$
$$(x_1 + x_2, s_2) = (x_1 + x_2, (2-\alpha')x_1^2) = (x_1 + x_2, 2-\alpha') = (2-\alpha') = (\alpha - 2)$$
$$(s_1, s_2) = (s_1, s_1 - s_2) = (s_1, \sqrt{5} \cdot x_1 x_2) = (\sqrt{5}) = (\alpha - 2)$$

Por tanto, $\frac{s_1}{\alpha-2}, \frac{s_2}{\alpha'-2}, \sqrt{5}$ son dos a dos primos entre sí y 5^4 divide a s_3, porque $s_1 s_2 s_3$ es múltiplo de 5^5. Además, $s_1' = \frac{s_1}{\alpha-2}, s_2' = \frac{s_2}{\alpha'-2}, s_3$ son dos a dos primos entre sí. Como $s_1' \cdot s_2' \cdot \frac{s_3}{5^4} = (\frac{x_3}{5})^5$ entonces salvo multiplicación por invertibles, $s_1' = c^5$ (con $c \in \mathbb{Z}[\alpha]$). Observemos que $(a + b\alpha)^5 = a^5 + b^5\alpha^5 \mod 5 = a^5 + b^5 \cdot (\frac{-1+\sqrt{5}}{2})^5 = a + 2b \mod 5$, por lo tanto $(a + b\alpha)^5 \in \mathbb{Z} + (5)$. Por el ejemplo 5.7.7, los invertibles de $\mathbb{Z}[\alpha]$ son $\{\pm(\frac{1+\sqrt{5}}{2})^n,\ n \in \mathbb{Z}\} = \{\pm\alpha^n,\ n \in \mathbb{Z}\}$. Por tanto, solo uno de $\alpha^i \cdot s_1'$, para $0 \le i < 5$ es igual a c^5. Tenemos que

$$s_1' = x_1 x_2 + \frac{(x_1 + x_2)^2}{\alpha - 2} \in \mathbb{Z} + (5)$$

Probemos que

$$\overline{\alpha^i \cdot s_1'} \notin \mathbb{Z}/5\mathbb{Z} \subset \mathbb{Z}[\alpha]/(5) = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \cdot \alpha,$$

para $0 < i < 5$: En efecto, $\bar{s}_1' = \overline{x_1 x_2}$ y $\alpha^2 = -\alpha + 1$, $\alpha^3 = 2\alpha - 1$ y $\alpha^4 = -3\alpha + 2$.

Entonces, $s_1' = y_1^5$ (con $y_1 \in \mathbb{Z}[\alpha]$), $s_2' = -y_2^5$ (con $y_2 = -\tau(y_1)$) y

$$y_1^5 + y_2^5 = -\frac{(x_1 + x_2)^2}{\sqrt{5}} = -\sqrt{5}^{15} \cdot (\frac{x_1 + x_2}{5^4})^2 = y_3^5$$

con $y_3 = -\sqrt{5}^3 \cdot \sqrt[5]{(\frac{x_1+x_2}{5^4})^2}$. Observemos que y_1, y_2, y_3 son dos a dos primos entre sí, porque lo son s_1', s_2', s_3, igualmente $y_1, y_2, \sqrt{5}$ son dos a dos primos entre sí. Además, $y_1^2 + y_2^2, y_1 y_2 \in \mathbb{Z}[\alpha]^{\langle\tau\rangle} = \mathbb{Z}$. Por último, $|y_1 y_2 y_3| < |x_1 x_2 x_3|$ y hemos llegado a contradicción.

12. Prueba que las únicas soluciones enteras de la ecuación

$$y^2 + 2 = x^3$$

son $y = \pm 5, x = 3$.

Resolución: $A = \mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[x]/(x^2 + 2)$ es un anillo de Dedekind. Veamos que es de ideales principales (luego dominio de factorización única). $\Delta_A = -8$. Tenemos que probar que todo ideal primo $\mathfrak{p}_y \subset A$ tal que $|A/\mathfrak{p}_y| \le \sqrt{|\Delta_A|} < 3$ es principal. Tenemos que $y \in (2)_0 = \{(2, x) = (x)\}$.

Si $y^2+2=x^3$, entonces $(y-\sqrt{-2})(y+\sqrt{-2})=x^3$. Observemos que

$$(y-\sqrt{-2}, y+\sqrt{-2})_0 = (y-\sqrt{-2}, 2\sqrt{-2})_0 = (y-\sqrt{-2}, \sqrt{-2})_0$$
$$= (y, \sqrt{-2})_0 = \begin{cases} \emptyset, & \text{si } y \neq \dot{2} \\ (\sqrt{-2}), & \text{si } y = \dot{2} \end{cases}$$

Ahora bien, si $y=\dot{2}$, entonces y^2+2 no es múltiplo de 4, pero $x^3=y^2+2$ es múltiplo de 8 (porque x ha de ser múltiplo de 2), contradicción. En conclusión, $y-\sqrt{-2}$ y $y+\sqrt{-2}$ son primos entre sí. Como su producto es un cubo, entonces $y-\sqrt{-2}$ es un cubo, es decir, $y-\sqrt{2}=(a+b\sqrt{-2})^3=(a^3-6ab^2)+(3a^2b-2b^3)\sqrt{-2}$. Luego, $b(3a^2-2b^2)=-1$, luego $b=1$ y $a=\pm 1$, de donde $y=\pm 5$ y por tanto $x=3$.

13. **La batalla de Hastings** (14 de octubre de 1066). "Los hombres de Harold permanecían bien juntos, como solían hacer, y formaban 13 escuadrones, con el mismo número de hombres en cada escuadrón, y hostigaban a los esforzados normandos que se aventuraban entrar en sus reductos; porque un único golpe de un hacha de guerra sajona podía romper sus lanzas y cortar sus mayas... Cuando Harold se lanzó él mismo al ataque, los sajones formaban un poderoso escuadrón de hombres, gritando exclamaciones de guerra..." ¿Cuántos sajones había en la batalla de Hastings?

Resolución: Sea x el número de sajones que hay en cada lado de los 13 escuadrones primeros e y el número de sajones que hay en cada lado del escuadrón último considerado. Entonces,

$$13\cdot x^2+1=y^2.$$

Tenemos que resolver esta ecuación diofántica, es decir, tenemos que resolver la ecuación $y^2-13x^2=1$. Consideremos $K=\mathbb{Q}[\sqrt{13}]$, entonces $N(y+x\sqrt{13})=y^2-13x^2$. Sea A el anillo de números de K. Entonces, por el ejemplo 5.7.7,

$$A^*=\{\frac{a+b\sqrt{13}}{2}, a,b\in\mathbb{Z}: a^2-13b^2=\pm 4\}.$$

Entonces, A^* está generado por $\xi=\frac{3+1\sqrt{13}}{2}$ (y por $-\xi$). El mínimo $n>0$ tal que $\xi^n\in\mathbb{Z}[\sqrt{13}]$, es $n=3$ y $\xi^3=18+5\sqrt{13}$. Luego,

$$\{a+b\sqrt{13}, a,b\in\mathbb{Z}: N(a+b\sqrt{13})=\pm 1\}=A^*\cap\mathbb{Z}[\sqrt{13}]=\langle 18+5\sqrt{13}\rangle$$

Ahora bien, $N(18+5\sqrt{13})=-1$. Luego, $\{a+b\sqrt{13}, a,b\in\mathbb{Z}: N(a+b\sqrt{13})=1\}=\langle(18+5\sqrt{13})^2\rangle=\langle 649+180\sqrt{13}\rangle$. En conclusión,

$$\{a+b\sqrt{13}, a,b\in\mathbb{N}: N(a+b\sqrt{13})=1\}=\{(649+180\sqrt{13})^n, \text{ con } n>0\}$$

La solución razonable de la ecuación diofántica $y^2-13x^2=1$ es $x=180$ e $y=649$. Luego el número de sajones era 649^2.

14. Prueba que si $\dim_{\mathbb{Q}} K >> 0$ entonces $|\Delta_K| >> 0$.

    Resolución: Por la proposición 5.6.3 (con $I = A$ y $d = \dim_{\mathbb{Q}} K$), $c = d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|} > 1$. Luego, si $d >> 0$ entonces $|\Delta_K| >> 0$.

15. Sea K un cuerpo de números y $P \subset \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$ un subconjunto propio, tal que si $\sigma \in P$, y c es el automorfismo conjugar de $\mathbb{C}$, entonces $c \circ \sigma \in P$. Prueba que existe un invertible ϵ en el anillo de números de K, tal que $|\sigma(\epsilon)| < 1$, para todo $\sigma \in P$ y $|\sigma(\epsilon)| > 1$, para todo $\sigma \notin P$.

    Resolución: Sea el cuadrante $C = \{\sum_{\sigma \in X_\infty} \lambda_\sigma \cdot \sigma \in \mathrm{Div}_\infty : \lambda_\sigma > 0 \text{ si } \sigma \in P, \text{ y } \lambda_\sigma < 0 \text{ si } \sigma \notin P\}$. Div^0_∞ es un hiperplano de Div_∞ que corta al cuadrante C.

    Sea A el anillo de números de K. $\bar{D}(A^*)$ es una red de Div^0_∞, luego $\bar{D}(A^*) \cap C \neq \emptyset$. Sea $\bar{D}(\epsilon) \in \bar{D}(A^*) \cap C$. Entonces, $\epsilon \in A^*$ cumple que $|\sigma(\epsilon)| < 1$, para todo $\sigma \in P$ y $|\sigma(\epsilon)| > 1$, para todo $\sigma \notin P$.

16. Prueba que $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ es d.i.p. pero no es un anillo euclídeo.

    Resolución: $A = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ es el anillo de números de $K = \mathbb{Q}[\sqrt{-19}]$. Tenemos que comprobar que los ideales $\mathfrak{p}_x \subset A$ tales que $|A/\mathfrak{p}_x| \leq \sqrt{|\Delta_K|} = \sqrt{19}$ son principales. Sea $\mathfrak{p}_x$ tal que $\mathfrak{p}_x \cap \mathbb{Z} = (2)$. Como $A = \mathbb{Z}[x]/(x^2 + x + 5)$, entonces $\mathfrak{p}_x = (2)$ porque $A/(2) = \mathbb{F}_2[x]/(x^2 + x + 1)$ es un cuerpo. Sea $\mathfrak{p}_x$ tal que $\mathfrak{p}_x \cap \mathbb{Z} = (3)$. Se cumple que $\mathfrak{p}_x = (3)$, porque $A/(3) = \mathbb{F}_3[x]/(x^2 + x + 2)$ es un cuerpo. Con todo A es d.i.p.

    Supongamos que A es euclídeo. Por el teorema de Dirichlet, los invertibles, A^*, es el conjunto de las raíces de la unidad incluidas en $\mathbb{Q}[\sqrt{-19}]$, es decir, $\{\pm 1\}$. Sea $c \in A \setminus \{0, 1, -1\}$ de grado mínimo. Dado $z \in A \setminus \{0, 1, -1\}$ tenemos que $z = z' \cdot c + r$, con $r = 0$ ó $\mathrm{gr}\, r < \mathrm{gr}\, c$, luego $r = \pm 1$. Luego, $A/(c) = \{\bar{0}, \bar{1}, -\bar{1}\}$, es decir, $A/(c) = \mathbb{F}_2$ ó $A = \mathbb{F}_3$. Por tanto, $A/(c)$ es un cociente de $A/(2)$ ó $A/(3)$, pero éstos son cuerpos de orden 4 y 9, luego es imposible.

17. En el lema 5.8.2, sea $E = \mathbb{R}^d$ con la métrica estándar. Prueba que

$$v = \frac{Vol(U)}{Vol(E/\Gamma)}.$$

    Resolución: En la demostración del lema, mediante una transformación lineal transformamos Γ en $\mathbb{Z}^d$. Esta transformación transforma cuerpos de volumen x en cuerpos de volumen $x/Vol(E/\Gamma)$. Una vez hecha esta transformación (manteniendo notaciones), probamos que $v = Vol(U)$.

18. Prueba que $v = \pi/4$ en el teorema 5.8.1 para $A = \mathbb{Z}[i]$.

    Resolución: $r = 0$, $s = 1$, $\mu_{\mathbb{Q}[i]} = \{\pm 1, \pm i\}$ luego $|\mu_{\mathbb{Q}[i]}| = 4$. Siguiendo las notaciones de la demostración del teorema 5.8.1, $\mathfrak{a} = \mathbb{Z}[i]$, $m = 0$, $P = \{0\}$ $\bar{D}^{-1}_\infty(P) = S^1$ y U es el disco de radio 1. Luego,

$$v = \frac{Vol(U)}{|\mu_{\mathbb{Q}[i]}| \cdot Vol(\mathbb{C}/\mathbb{Z}[i])} = \pi/4.$$

19. Sea $C = \{(\lambda_i) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i\le r} |\lambda_i| + \sum_{j>r} 2|\lambda_j| \le t\}$. Prueba que

$$Vol(C) = 2^r \cdot (\frac{\pi}{2})^s \cdot \frac{t^{r+2s}}{(r+2s)!}.$$

Resolución: $Vol(C) = \int_C dx_1 \cdots dx_r \cdot dy_1 \cdot dz_1 \cdots dy_s \cdot dz_s$.. Cambiando a coordenadas polares $y_i = u_i \cdot \cos\theta_i, z_i = u_i \operatorname{sen}\theta_i$, tenemos

$$Vol(C) = \int_D u_1 \cdots u_s dx_1 \cdots dx_r \cdot du_1 \cdots du_s \cdot d\theta_1 \cdots d\theta_s,$$

Donde $D = \{(x,u,\theta) \in \mathbb{R}^{r+2s} : 0 \le \theta_i \le 2\pi, u_i \ge 0, |x_1| + \cdots + |x_r| + 2u_1 + \cdots + 2u_s \le t\}$. Hagamos el cambio de coordenadas $2u_i = w_i$. Entonces, $Vol(C) = 2^r 4^{-s} (2\pi)^s I_{r,s}(t)$, donde

$$I_{r,s}(t) = \int_E w_1 \cdots w_s dx_1 \cdots dx_r \cdot dw_1 \cdots dw_s,$$

donde $E = \{(x,w) \in \mathbb{R}^{r+s} : x_i, w_i \ge 0,\ x_1 + \cdots + x_r + w_1 + \cdots + w_s \le t\}$.. Tenemos que $I_{r,s}(t) = t^{r+2s} I_{r,s}(1)$. Reescribiendo el dominio como $x_2 + \cdots + x_r + w_1 + \cdots + w_s \le t - x_1$, tenemos por el teorema de Fubini

$$I_{r,s}(1) = \int_0^1 I_{r-1,s}(1-x_1)dx_1 = \int_0^1 (1-x_1)^{r+2s-1} dx_1 \cdot I_{r-1,s}(1) = \frac{1}{r+2s} I_{r-1,s}(1),$$

y entonces por inducción $I_{r,s}(1) = \frac{1}{(r+2s)\cdots(2s+1)} \cdot I_{0,s}(1)$. De la misma manera

$$I_{0,s}(1) = \int_0^1 w_1 (1-w_1)^{2s-2} dw_1 \cdot I_{0,s-1}(1) = \frac{1}{2s \cdot (2s-1)} \cdot I_{0,s-1}(1),$$

de donde por inducción $I_{0,s}(1) = \frac{|}{(2s)!} I_{0,0}(1) = \frac{1}{(2s)!}$ y $I_{r,s}(1) = \frac{1}{(r+2s)!}$. Por tanto,

$$Vol(C) = 2^r \cdot (\frac{\pi}{2})^s \cdot \frac{t^{r+2s}}{(r+2s)!}.$$

Bibliografía

[1] ANDREWS, G.E.: *Number Theory*, Dover, 1994.

[2] ANGLIN, W.S.: *The queen of mathematics. An introduction to number theory*, Kluwer A.P./Texts in the Math. Sc., vol. 8 1995.

[3] BAKER, A.: *Breve introducción a la teoría de números*, Alianza Editorial/472 AU Ciencias, 1986.

[4] BOREVICH, Z.I. AND SHAFAREVICH, I.R.: *Number Theory*, Academic Press, Inc. 1966.

[5] EVEREST, W.: *An introduction to number theory*, Springer-Verlag/Graduate Texts in Math., vol. 232 Versión digital en http://lope.unex.es.

[6] FROHLICH, A.: *Algebraic number theory*, Cambridge U.P./Cambr. Stud. Adv. Math., vol. 27, 1991.

[7] HASSE, H.: *Number theory*, Springer-Verlag/Grundl. Math. Wissensch., vol. 229, 1969.

[8] IBORRA, C.: *Teoría de números*, www.uv.es/ivorra/Libros/Numeros.pdf

[9] IRELAND, K.; ROSEN, M.: *A classical introduction to modern number theory*, Springer-Verlag/Graduate Texts in Math., vol. 84, 1982.

[10] LANG, S.: *Algebraic number theory*, Springer-Verlag/Graduate Texts in Math., vol. 110, 1994.

[11] LI, W.C.: *Number theory with applications*, World Scientific, 1996.

[12] MILLER, S.J.; TAKLOO-BIGHASH, R.: *An invitation to modern number theory*, Princeton University Press, 2006.

[13] NATHANSON, M.B.: *Elementary methods in number theory*, Springer-Verlag/Graduate Texts in Math., vol. 195, 2000.

[14] NEUKIRCH, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg 1999.

[15] ORE, O.:*Number theory and its history.*, McGraw-Hill Book Company, Inc., 1948.

[16] PARSHIN, A.N.; SHAFAREVICH, I.R.: *Number theory I. Fundamental problems, ideas and theories.*, Springer-V./Encyclopaedia of Math. Sc., vol. 49, 1995.

[17] ROSE, H.E.:*A course in number theory*, Oxford University Press Inc., 2007.

[18] ELEMENTARY NUMBER THEORY: , International Thomson Publ. PWS Publ.CO, 1994.

[19] TATTERSAL, J.J.: *Elementary number theory in nine chapters*, Cambridge University Press, 1999

[20] WEIL, A.:*Number theory for beginners*, Springer-Verlag, 1979.

[21] WEIL, A.:*Basic number theory*, . Springer-Verlag/Grundl. Math. Wissensch., vol. 144, 1974.

Índice alfabético

UNIVERSIDAD DE EXTREMADURA

99