Teoría de Números

Grado en Matemáticas

Colección manuales uex - 99

Pedro
Sancho de Salas

99

TEORÍA DE NÚMEROS

GRADO EN MATEMÁTICAS

MANUALES UEX

99

PEDRO SANCHO DE SALAS

TEORÍA DE NÚMEROS

GRADO EN MATEMÁTICAS

UNIVERSIDAD DE EXTREMADURA

2015

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 cuatro 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 enteros, 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 enteros no son dominios de factorización única. Dado un anillo de números enteros, A, existe un número finito de fracciones a_n/b_n (raíces de polinomios mónicos con coeficientes en $\mathbb{Z}$) de modo que $B := A[a_1/b_1, \ldots, a_n/b_n]$ ya es casi un dominio de factorización única: todo ideal de B (principal o no) 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 enteros no sea dominio de factorización única.

Para el estudio de un anillo de números enteros 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 enteros 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 enteros 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 sólo 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 anillos de A, B, 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 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 sólo 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 enteros, 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 tercero.

Capítulo 1

Anillos de enteros y anillos de curvas algebraicas

1.1. Introducción

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

En el segundo curso del Grado en Matemáticas hemos probado que $\mathbb{Z}$ y $k[x]$ son anillos euclídeos. Hemos demostrado que todo entero descompone en producto de números primos, el algoritmo de Euclides, etc.

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

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

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

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

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

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

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

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

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

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

Veamos otros ejemplos de anillos (de números enteros) euclídeos.

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

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

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

3. El anillo de los enteros de Gauss, $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, es euclídeo: Sea $\delta : \mathbb{C} \to \mathbb{N}$ definido por $\delta(z) = z \cdot \bar{z} = a^2 + b^2$ (con $z = a + bi$). Como $\delta(zz') = \delta(z)\delta(z')$, entonces $\delta(z) \leq \delta(zz')$, para todo $z, z' \in \mathbb{Z}[i]$, no nulos. Dados $z, z' \in \mathbb{Z}[i]$, $z' \neq 0$, sea c un entero de Gauss tal que $\delta(z/z' - c) < 1$ (luego $\delta(z - z'c) < \delta(z')$). Entonces, $z = z'c + r$, con $r = z - z'c$ y $\delta(r) < \delta(z')$.

Veamos que *un número primo $p \in \mathbb{Z}$ descompone en suma de dos cuadrados perfectos si y sólo 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 sólo 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 $\mathbb{F}_p^* \to \{\pm 1\}$, $a \mapsto a^{\frac{p-1}{2}}$.

Por tanto, $-1 \in \mathbb{F}_p^{*2}$ si y sólo 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 sólo si $p \equiv 3$ mód 4.

En conclusión, un número primo $p \in \mathbb{Z}$ descompone en suma de dos cuadrados perfectos si y sólo 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 $\mathbb{Z}[i]$. Obviamente, p^r divide a $a + bi$ si y sólo si divide a $a - bi$. Por tanto, $n = p^{2s} \cdot n'$, con n' no divisible por p y suma de dos cuadrados perfectos. Si n es producto de números enteros que son suma de cuadrados perfectos entonces 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.*

4. 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 sólo 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 sólo 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 sólo

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

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

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

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

siendo ξ una raíz primitiva n-ésima de la unidad 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) de enteros $\mathbb{Z}[\xi]$. 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 de enteros eran dominios de factorización única. Consideremos por sencillez el anillo $\mathbb{Z}[\sqrt{-5}]$, 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.

6. Sea $x^n + c_1x^{n-1} + \cdots + c_n \in \mathbb{Z}[x]$ 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 b en $\mathbb{Q}[\alpha_1]$. Si $z = a + b\alpha_1$, entonces $N(b) = \prod_i (a + b\alpha_i)$.

Resolver la ecuación diofántica $a^n + c_1a^{n-1}b + \cdots + c_nb^n = c$, 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. Este capítulo trata de los problemas de la factorización única en estos anillos y cómo resolverlos.

1.2. 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.

3. 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, $N'/(N' \cap N) = \langle \bar{m}_1, \ldots, \bar{m}_s \rangle$. Por tanto, $N' = \langle n_1, \ldots, n_r, m_1, \ldots, m_s \rangle$. □

4. Corolario: *$M = M' \oplus M''$ es un A-módulo noetheriano si y sólo 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. □

5. 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 $M = \langle m_1, \ldots, m_n \rangle$, 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. □

6. 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.

7. 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 $p(x) = a_0x^n + \cdots + a_n, q(x) = b_0x^m + \cdots + b_m \in I$, 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, $J = (b_1, \ldots, b_r)$ es finito generado. Así, existen $p_1, \ldots, p_r \in I$ cuyos coeficientes de grado máximo son $b_1, \ldots, b_r$, 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 $p(x) = a_0x^n + \cdots + a_n \in I$. 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

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

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 $I \cap \{A + Ax + \cdots + Ax^{m-1}\} = \langle q_1, \ldots, q_s \rangle_A$, tenemos que $I = (p_1, \ldots, p_r, q_1, \ldots, q_s)$. □

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

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

□

9. Definición: Sea A un anillo íntegro. Un elemento propio (no nulo ni invertible) de A se dice que es irreducible si no descompone en producto de dos elementos propios.

10. Ejercicio: Sea A un anillo íntegro y $a \in A$. Si $(a) \subset A$ es un ideal primo, probar que a es irreducible.

11. Proposición: *Un módulo M es noetheriano si y sólo 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 $n >> 0$, $N = M_n = \langle m_1, \ldots, m_n \rangle$.

□

12. Teorema de descomposición en factores irreducibles: *Todo elemento propio $a \in A$, de un anillo noetheriano íntegro, descompone en producto de factores irreducibles $a = p_1 \cdots p_n$.*

Demostración. 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 $(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \ldots$ 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 $(a) \underset{\neq}{\subset} (b_1) \underset{\neq}{\subset} (b_2) \underset{\neq}{\subset} \ldots$ que ha de ser finita y terminará cuando b_n sea irreducible. En tal caso $a = a_1 \cdots a_{n-1} \cdot b_n$ es producto de irreducibles. □

1.3. Dominios de factorización única

1. Definición: Se dice que un anillo íntegro, A, es un dominio de factorización única si todo elemento propio de A es igual a un producto de irreducibles de modo único, salvo factores por invertibles y orden.

$\mathbb{Z}$, $k[x]$ y en general los anillos euclídeos son dominios de factorización única.

2. Lema de Euclides: *Sea A d.f.u. y $a \in A$ no nula. Entonces, a es irreducible $\iff$ $(a) \subset A$ es un ideal primo.*

Demostración. $\Rightarrow$) Sea $b \cdot c \in (a)$. Existe $d \in A$ tal que $b \cdot c = a \cdot d$. Si consideramos las descomposición en factores irreducibles de b, c y d, y recordamos que A es d.f.u. , tenemos que a aparece (salvo multiplicación por un invertible) en la descomposición en producto de factores irreducibles de b o c. Luego, a divide a b o c. En conclusión, $(a) \subset A$ es un ideal primo.

□

3. 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.

4. Lema: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Sean $P(x), Q(x) \in A[x]$ dos polinomios primitivos. Entonces,*

1. *$P(x) \cdot Q(x)$ es primitivo.*

2. *Si existen $a,b \in A$ tales que $a \cdot P(x) = b \cdot Q(x)$, entonces $b = a \cdot u$, para cierto invertible $u \in A$. Por tanto, si $P(x) = \frac{b}{a} \cdot Q(x)$ en $\Sigma[x]$, entonces $\frac{b}{a} = u \in A$ es un invertible de A.*

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. Haciendo cociente en $A[X]$ por $p \cdot A[x]$, tenemos que

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

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

2. Sea p un elemento irreducible que divida a a. Haciendo cociente en $A[X]$ por $p \cdot A[x]$, tenemos que $0 = \bar{b} \cdot \overline{Q(x)}$, luego $\bar{b} = 0$ y p divide a b. Dividiendo a a y b a la vez por p y repitiendo sucesivamente este proceso obtendremos que a divide a b, y por simetría que b divide a a. Luego, $b = a \cdot u$, para cierto invertible $u \in A$. □

5. Teorema : *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Un polinomio no constante primitivo, $P(x) \in A[x]$, es irreducible en $A[x]$ si y sólo si es irreducible en $\Sigma[x]$.*

Demostración. Supongamos que $P(x)$ es irreducible en $\Sigma[x]$. Si $P(x) = P_1(x) \cdot P_2(x)$, con $P_1(x), P_2(x) \in A[x]$, entonces como $P(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $P_1(x)$ o $P_2(x)$ ha de ser de grado cero, digamos $P_1(x) = a$. Como $P(x)$ es primitivo $P_1(x) = a \in A$ es invertible. En conclusión, $P(x)$, es irreducible en $A[x]$.

Supongamos que $P(x)$ es irreducible en $A[X]$. Supongamos que $P(x) = \tilde{P}_1(x) \cdot \tilde{P}_2(x)$, siendo $\tilde{P}_1(x), \tilde{P}_2(x) \in \Sigma[x]$. Eliminando denominadores podemos suponer que

$$P(x) = \frac{a}{b} P_1(x) \cdot P_2(x)$$

con $P_1(x), P_2(x) \in A[x]$, primitivos. Por el lema 1.3.4, $\frac{a}{b} = u \in A$, luego $P(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

6. Teorema (Gauss): *Si A es un dominio de factorización única, entonces $A[x]$ también lo es.*

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

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

la descomposición en irreducibles en $\Sigma[x]$. Eliminando denominadores y sacando el máximo común divisor en los numeradores, es claro que se puede escribir:

$$Q(x) = \frac{b}{c} \cdot Q_1(x) \cdots Q_r(x) \qquad (*)$$

con $Q_i(x) = \frac{a_i}{b_i} \widetilde{Q}_i(x) \in A[x]$ primitivos.

• Por el lema 1.3.4, $\frac{b}{c} = u \in A$ es un invertible de A.

• Cada $Q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por el teorema 1.3.5.

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

$$P(x) = a \cdot Q(x) = u \cdot p_1 \cdots p_s Q_1(x) \cdots Q_r(x)$$

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 el teorema 1.3.5. Por tanto, los polinomios $P_i(x)$ (una vez reordenados) difieren de los $Q_i(x)$ en invertibles de A. Tachando los términos polinómicos comunes se obtiene, salvo invertibles de A, la igualdad $q_1 \cdots q_l = p_1 \cdots p_s$, de donde salvo permutación de los factores es $q_i = p_i$ (salvo invertibles de A).

□

Por el teorema de Gauss, $\mathbb{Z}[x_1, \ldots, x_n]$ y $k[x_1, \ldots, x_n]$ son dominios de factorización única.

1.4. Dominios de ideales principales

1. Definición: Se dice que un anillo es un dominio de ideales principales si es un anillo íntegro y todos sus ideales son principales (es decir, generados por un elemento).

Evidentemente, los dominios de ideales principales son noetherianos.

2. Ejemplo: Los anillos euclídeos son d.i.p. Así pues, $\mathbb{Z}$ y $k[x]$ son d.i.p.

3. Ejercicio: Probar que $k[x, y]$ no es d.i.p.

4. Lema de Euclides: *Si $a \in A$ es un elemento irreducible de un dominio de ideales principales, entonces $(a) \subset A$ es un ideal primo.*

Demostración. Si a es irreducible y divide a bc, entonces si a no divide a b implica que $(a, b) = (1)$. Por tanto, existen $\alpha, \beta \in A$ tales que $\alpha a + \beta b = 1$. Luego $\alpha a c + \beta b c = c$. De esta igualdad obtenemos que a divide a c. □

5. Teorema: *Si A es d.i.p. entonces es d.f.u.*

Demostración. Por ser A noetheriano todo elemento propio del anillo es producto de irreducibles. Veamos ahora la unicidad. Sean $a = p_1 \cdots p_n = q_1 \cdots q_m$ dos descomposiciones en factores irreducibles. Por el Lema de Euclides, q_1 divide algún factor p_i, luego coincide con él (salvo un factor invertible). Reordenando, podemos decir que $p_1 = q_1$ (salvo invertibles). Simplificando la igualdad original tenemos $p_2 \cdots p_n = q_2 \cdots q_m$ (salvo invertibles). 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 multiplicación por invertibles). □

6. Teorema: *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión de Krull mayor que cero y sea $\mathfrak{m}$ el ideal maximal de $\mathcal{O}$. Entonces, $\mathfrak{m} = (t)$ es un ideal principal si y sólo si $\mathcal{O}$ es un dominio de ideales principales.*

Demostración. Veamos la implicación directa. 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 $(a) \underset{\neq}{\subseteq} (a_1)$, 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, $(a_1) \underset{\neq}{\subseteq} (a_2)$, y seguimos el proceso. Por noetherianidad, este proceso termina y tendremos que $a = t^n \cdot c$ con c invertible.

Dado un ideal $I = (f_1, \dots, f_r)$, tenemos que $f_i = t^{n_i} \cdot g_i$, con g_i invertible, luego $I = (t^{n_1}, \dots, t^{n_r}) = (t^n)$, 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.

□

7. Corolario: *Sea $\mathcal{O}$ un anillo local noetheriano de dimensión de Krull mayor que cero y sea $\mathfrak{m}$ su ideal maximal. Entonces, $\mathcal{O}$ es un dominio de ideales principales si y sólo si* $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Demostración. 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 sólo si $\mathfrak{m}$ es principal, por el lema de Nakayama. Por el teorema anterior concluimos. □

1.5. Dominios de Dedekind

1. Definición: Diremos que un anillo A íntegro noetheriano (que no sea cuerpo) es un dominio de Dedekind si y sólo si A_x es un dominio de ideales principales para todo punto cerrado $x \in \operatorname{Spec} A$.

Observemos que los dominios de Dedekind son anillos de dimensión de Krull 1.

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

3. Lema: *Sea $S \subseteq A$ un sistema multiplicativo. Si*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} M' \to 0$$

es una sucesión exacta de A-módulos, entonces

$$0 \to N_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M'_S \to 0$$

es una sucesión exacta de A_S-módulos.

4. 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 sólo 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 $x \in \operatorname{Spec} A$. □

5. Teorema: *Si A es un dominio de Dedekind e $I \subseteq A$ un ideal no nulo, 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

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

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

Los anillos de Dedekind no son dominios de factorización única en general, aunque esta proposición esté muy cerca de afirmarlo. Se tiene las siguiente inclusiones estrictas (ver problemas 3 y 15)

$$\{\text{Anillos euclídeos}\} \subset \{\text{D.I.P.}\} \subset \{\text{Dominios de Dedekind}\}$$

6. Teorema: *Un anillo es un dominio de ideales principales si y sólo si es un dominio de Dedekind y de factorización única.*

Demostración. $\Leftarrow$) Dado un ideal primo $\mathfrak{p}$ no nulo, sea $a \in \mathfrak{p}$ irreducible. Entonces, (a) es un ideal primo incluido en $\mathfrak{p}$, luego $\mathfrak{p} = (a)$. Por tanto, por el teorema 1.5.5, todo ideal es principal.

□

7. Definición: Sea A un anillo íntegro de dimensión de Krull 1. Diremos que un punto cerrado $x \in \operatorname{Spec} A$ es no singular si A_x es un anillo de ideales principales. Diremos que x es singular si A_x no es un anillo de ideales principales.

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

8. 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 $d_x f := \overline{f - f(x)} \in \mathfrak{m}_x/\mathfrak{m}_x^2$.

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

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

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

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

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

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

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

□

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

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 sólo 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 sólo 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 $\bar{\mathfrak{m}}_{(\alpha,\beta)}\cdot\mathcal{O} = (x-\alpha)$.

12. Ejemplo: $\operatorname{Spec}\mathbb{C}[x,y]/(y^2-x^3)$ 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 sólo si $(\alpha,\beta)=(0,0)$.

13. Proposición: *Sea $i\colon A \hookrightarrow B$ un morfismo finito, $x \in \operatorname{Spec}A$ un punto cerrado y $i^{*-1}(x) = \operatorname{Spec}(B/\mathfrak{m}_x B) = \{y_1,\dots,y_r\}$. Si $B/\mathfrak{m}_x B$ es un anillo reducido (por ejemplo, cuando sea una $A/\mathfrak{m}_x$-álgebra separable), entonces $\mathfrak{m}_x\cdot B_{y_i} = \mathfrak{m}_{y_i}\cdot B_{y_i}$, para todo i; si además $\mathfrak{m}_x A_x$ es principal, entonces $\mathfrak{m}_{y_i}B_{y_i}$ es principal.*

Demostración. Como $B/\mathfrak{m}_x B$ es reducida, $\bar{\mathfrak{m}}_{y_1}\cdots\bar{\mathfrak{m}}_{y_r} = 0$. Por tanto, $\mathfrak{m}_{y_1}\cdots\mathfrak{m}_{y_r} \subseteq \mathfrak{m}_x B$ y

$$\mathfrak{m}_{y_i}B_{y_i} = \mathfrak{m}_{y_1}\cdots\mathfrak{m}_{y_r}B_{y_i} \subseteq \mathfrak{m}_x B_{y_i}$$

Como $\mathfrak{m}_x\cdot B \subseteq \mathfrak{m}_{y_i}$, entonces $\mathfrak{m}_x\cdot B_{y_i} = \mathfrak{m}_{y_i}\cdot B_{y_i}$. □

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; y los ideales primos no maximales son de la forma $(q(x))$ con $q(x) \in \mathbb{Z}[x]$ irreducible y el ideal minimal (0).

Consideremos el odeal maximal $\mathfrak{m}_y = (p, q(x))$ 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 $\{\bar{p}, \overline{q(x)}\}$. Sea $f(x) \in \mathfrak{m}_y$ y denotemos las clases de $\mathfrak{m}_y$ en $\mathbb{Z}[x]/(f(x))$, $\bar{\mathfrak{m}}_y$. Entonces, $\bar{\mathfrak{m}}_y/\bar{\mathfrak{m}}_y^2 = (\mathfrak{m}_y/\mathfrak{m}_y^2)/(d_y f(x))$. Por tanto,

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

Calculemos los puntos singulares de $\operatorname{Spec}\mathbb{Z}[\sqrt{2}]$ y de $\operatorname{Spec}\mathbb{Z}[\sqrt{5}]$:

$\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2-2)$ 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 domino 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. Ejemplo: Sea $\xi_m = e^{2\pi i/m} \in \mathbb{C}$ una raíz primitiva m-ésima de la unidad. 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 $\operatorname{Spec}\mathbb{Z}[\xi_{p^n}] = \operatorname{Spec}\mathbb{Z}[x]/(\Phi_{p^n}(x))$, 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.

Escribamos ahora, $m = p^n \cdot m'$, con m' primo con p. Por inducción, podemos suponer que $\mathbb{Z}[\xi_{m'}]$ es no singular al localizar en todo punto. Observemos que $\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_{m'}, \xi_{p^n}]$. Observemos que ξ_{p^n} es separable en fibras sobre $\mathbb{Z}[\xi_{m'}]$, salvo quizás en los puntos $y \in \operatorname{Spec}\mathbb{Z}[\xi_{m'}]$ tales que $\mathfrak{m}_y \cap \mathbb{Z} = (p)$. Luego, los únicos puntos singulares posibles de $\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_{m'}, \xi_{p^n}]$ son de la forma $\mathfrak{m}_{y'} = (\mathfrak{m}_y, \xi_{p^n} - 1)$ (donde $\mathfrak{m}_y \cap \mathbb{Z} = (p)$). Ahora bien, $\mathfrak{m}_y \mathbb{Z}[\xi_{m'}]_y = (p)$. Luego, $\mathfrak{m}_{y'} \cdot \mathbb{Z}[\xi_m]_{y'} = (p, \xi_{p^n} - 1) = (\xi_{p^n} - 1)$, e y' es no singular.

1.6. Anillos de curvas y anillos de enteros

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 (abusiva) $A \to B$, $a \mapsto a$.

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.

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,

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

Sea $B = \mathbb{C}[x_1,\dots,x_n]/(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))$. Por los teoremas de los ceros de Hilbert sabemos que

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

3. 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.

4. 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 $\operatorname{Spec}\mathbb{C}[x,y,z]/(1+x^2+y^2+z^2, 2+x^2-y^2)$.

Si B es una A-álgebra, entonces B es de modo natural un A-módulo. Una A-álgebra B se dice que es una A-álgebra finita si B es un A-módulo finito generado. Ejemplo: $B := A[x]/(x^n + a_1x^{n-1} + \cdots + a_n)$ es una A-álgebra finita porque $\{\bar{1},\bar{x},\dots,\bar{x}^{n-1}\}$ es un sistema generador del A-módulo B (es más, es una base). Se dice, también, que $A \to B$ es un morfismo finito si B es una A-álgebra finita (es decir, si B es un A-módulo finito generado). La composición de morfismos finitos es finito. $A \to A[\xi_1,\dots,\xi_n]$ es un morfismo finito si y sólo si $\xi_1,\dots,\xi_n$ son enteros sobre A (es decir, existen polinomios mónicos con coeficientes en A, $p_i(x)$, tales que $p_i(\xi_i) = 0$).

Si $\operatorname{Spec} A$ es una curva íntegra afín por el lema de normalización de Noether existe un morfismo finito inyectivo $k[x] \hookrightarrow A$. Recíprocamente, si A es un anillo íntegro y existe un morfismo inyectivo finito $k[x] \hookrightarrow A$ entonces A es una k-álgebra de tipo finito íntegra y de dimensión de Krull 1.

5. Definición: Diremos que un anillo íntegro A es un anillo de números enteros si el morfismo $\mathbb{Z} \hookrightarrow A$ es inyectivo y finito.

6. 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 enteros.

Si $f\colon A \hookrightarrow B$ es un morfismo finito inyectivo, entonces el morfismo en los espectros $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectivo y las fibras son finitas y de dimensión cero (es decir, si $f^*(x) = f^*(x')$ y $x \neq x'$, entonces $\mathfrak{p}_x \not\subset \mathfrak{p}_{x'}$). Además, la dimensión de Krull de A coincide con la de B. Por tanto, los anillos de números son anillos noetherianos íntegros de dimensión de Krull 1.

1.7. Desingularización

Se dice que un morfismo de anillos $A \to B$ es entero si y sólo si todos los elementos de B son enteros sobre A. Dado un morfismo de anillos $A \to B$, el conjunto de elementos de B enteros sobre A, es una A-subálgebra de B, entera sobre A, y se dice que es el cierre entero de A en B. Un anillo íntegro A se dice que es íntegramente cerrado en su cuerpo de fracciones, $\Sigma_A = A_{A\setminus 0}$, si el cierre entero de A en Σ_A es A.

1. Proposición: *Los dominios de factorización única son íntegramente cerrados en su cuerpo de fracciones.*

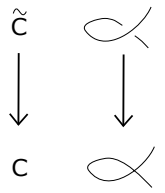
Demostración. Sea A un dominio de factorización única y Σ su cuerpo de fracciones. Sea $\frac{a}{b} \in \Sigma$ una fracción de modo que b no sea invertible y sea primo con a. Si $\frac{a}{b}$ es entero sobre A, verifica una relación

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

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.

□

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.



2. 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 íntegramente cerrado en su cuerpo de fracciones Σ.*

Demostración. 1. $\Rightarrow$ 2. $\mathcal{O}$ es un dominio de ideales principales, luego dominio de factorización única y es íntegramente cerrado en su cuerpo de fracciones.

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 $g \notin f\mathcal{O}$.

□

3. 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 íntegramente cerrado, entonces A_S también.

Un anillo íntegro es íntegramente cerrado en su cuerpo de fracciones si y sólo si es localmente íntegramente cerrado.

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 $x \in \operatorname{Spec} A$.

□

4. Teorema: *Un anillo noetheriano íntegro A de dimensión de Krull 1 es un dominio de Dedekind si y sólo si A es íntegramente cerrado en su cuerpo de fracciones.*

Demostración. $A = \bar{A}$ si y sólo 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 sólo si A_x es un domino de ideales principales, por el teorema 1.7.2. □

Sea A un anillo noetheriano íntegro de dimensión de Krull 1. Si el cierre entero de A en su cuerpo de fracciones, $\bar{A}$, es un anillo noetheriano entonces $\bar{A}$ es un dominio de Dedekind y 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.

1.8. Finitud del morfismo de desingularización

1. Lema: *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. $\bar{A}_{A\setminus 0} = \overline{A_{A\setminus 0}} = \bar{\Sigma}$, porque el cierre entero conmuta con localizaciones por 1.7.3. En particular, $\bar{\Sigma}$ es el cuerpo de fracciones de $\bar{A}$.

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 $\bar{\Sigma}$, $T_2(f,g) := \operatorname{tr}(f \cdot g)$, y sea $iT_2 \colon \bar{\Sigma} \to \bar{\Sigma}^*$ su polaridad asociada, que es un isomorfismo por ser $\bar{\Sigma}$ 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 $iT_2(\bar{A}) \subseteq Aw_1 + \cdots + Aw_n$ 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 $iT_2(a') = \lambda_1 w_1 + \cdots + \lambda_n w_n$, con $\lambda_i \in \Sigma$. Tenemos que ver que $\lambda_i \in A$. Se tiene que

$$\lambda_i = iT_2(a')(\bar{a}_i) = \mathrm{tr}(a' \cdot \bar{a}_i) = \sum_{g\in G} g(a' \cdot \bar{a}_i)$$

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 $\lambda_i \in A$.

□

2. Teorema: *Sea A un anillo de números enteros de cuerpo de fracciones Σ y $\bar{\Sigma}$ una extensión finita de cuerpos de Σ. Entonces, el cierre entero de A en $\bar{\Sigma}$, $\bar{A}$, es un anillo de números enteros de cuerpo de fracciones $\bar{\Sigma}$ y el morfismo $A \to \bar{A}$ es finito.*

Demostración. El morfismo $\mathbb{Z} \hookrightarrow A$ es finito, localizando en $S := \mathbb{Z}\backslash 0$, tenemos que A_S es una $\mathbb{Q}$-álgebra finita íntegra, luego es cuerpo. Por tanto, $A_S = \Sigma$ y $\mathbb{Q} \hookrightarrow \Sigma$ es un morfismo finito. Además, el cierre entero de A en $\bar{\Sigma}$ coincide con el cierre entero de $\mathbb{Z}$ en $\bar{\Sigma}$. Por el lema anterior, $\bar{A}$ es una $\mathbb{Z}$-álgebra finita (luego un anillo de números y una A-álgebra finita) de cuerpo de fracciones $\bar{\Sigma}$. □

3. Teorema: *Sea A una k-álgebra de tipo finito íntegra de cuerpo de fracciones Σ. Sea $\Sigma \hookrightarrow \bar{\Sigma}$ una extensión finita de cuerpos y $\bar{A}$ el cierre entero de A en $\bar{\Sigma}$. Entonces, $A \hookrightarrow \bar{A}$ es un morfismo finito, y $\bar{\Sigma}$ es el cuerpo de fracciones $\bar{A}$.*

Demostración. Por el lema de normalización de Noether existe un morfismo

$$k[x_1, \ldots, x_n] \hookrightarrow A$$

finito e inyectivo. El cierre entero de A en $\bar{\Sigma}$ coincide con el cierre entero de $k[x_1, \ldots, x_n]$ en $\bar{\Sigma}$, luego podemos suponer que $A = k[x_1, \ldots, x_n]$.

Sea Ω la envolvente normal de $\bar{\Sigma}$. El cierre entero de A en Ω contiene a $\bar{A}$, luego si demostramos que el cierre entero de A en Ω es un A-módulo finito generado tendremos que $\bar{A}$ también lo es. Así pues, podemos suponer que $\bar{\Sigma}$ es una extensión normal de Σ.

Sea G el grupo de Galois de $\bar{\Sigma}$. Sea $\bar{\Sigma}^G$ los elementos de $\bar{\Sigma}$ invariantes por G y denotemos A' al cierre entero de A en $\bar{\Sigma}^G$. A' es un A-módulo finito generado: Observemos que $\Sigma \hookrightarrow \bar{\Sigma}^G$ es una extensión puramente inseparable. Sea $\mathrm{car}\, k = p > 0$ y escribamos $\bar{\Sigma}^G = \Sigma[\xi_1, \ldots, \xi_r]$. Existe $m >> 0$ de modo que $\xi_i^{p^m} \in \Sigma = k(x_1, \ldots, x_n)$, para todo i. Escribamos $\xi_i^{p^m} = p_i/q_i$, con $p_i = \sum_j \lambda_{ij} x^j \in k[x_1, \ldots, x_n]$ y $q_i = \sum_j \mu_{ij} x^j \in k[x_1, \ldots, x_n]$. Sea $k' := k(\sqrt[p^m]{\lambda_{ij}}, \sqrt[p^m]{\mu_{ij}})_{ij}$ y $\Sigma' := k'(\sqrt[p^m]{x_1}, \ldots, \sqrt[p^m]{x_n})$. Se verifica que $\xi_i = \sqrt[p^m]{p_i/q_i} \in \Sigma'$, luego $\bar{\Sigma}^G \subseteq \Sigma'$. Podemos suponer que $\bar{\Sigma}^G = \Sigma'$. Ahora bien, el cierre entero $k[x_1, \ldots, x_n]$ en Σ' es $k'[\sqrt[p^m]{x_1}, \ldots, \sqrt[p^m]{x_n}]$, pues $k'[\sqrt[p^m]{x_1}, \ldots, \sqrt[p^m]{x_n}]$ es un $k[x_1, \ldots, x_n]$-módulo finito generado y es íntegramente cerrado (porque es un anillo de polinomios). Hemos concluido.

$\bar{A}$ coincide con el cierre entero de A' en $\bar{\Sigma}$, luego $\bar{A}$ es un A'-módulo finito generado por el lema anterior, pues $\bar{\Sigma}^G \hookrightarrow \bar{\Sigma}$ es una extensión separable (de Galois). Por tanto, $\bar{A}$ es un A-módulo finito generado.

□

4. Definición: Una extensión finita de $\mathbb{Q}$, K, se dice que es un cuerpo de números. El cierre entero de $\mathbb{Z}$ en un cuerpo de números K se dice que es el anillo de enteros de K.

5. Teorema: *Sea A el anillo de una curva afín íntegra (resp. un anillo de números enteros). Sea Σ el cuerpo de fracciones de A, $\Sigma \hookrightarrow \bar{\Sigma}$ una extensión finita de cuerpos y $\bar{A}$ el cierre entero de A en $\bar{\Sigma}$. Entonces,*

1. *$\bar{A}$, es el anillo de una curva afín íntegra (resp. un anillo de números enteros) no singular de cuerpo de fracciones $\bar{\Sigma}$ y el morfismo $A \to \bar{A}$ es finito.*

2. *Si $\bar{\Sigma} = \Sigma$, dado $x \in \operatorname{Spec} A$, el morfismo $A_x \to \bar{A}_x$ es isomorfismo si y sólo si x es no singular. Además, el conjunto de puntos singulares de A es un conjunto finito de puntos cerrados de* $\operatorname{Spec} A$. *"Diremos que $A \to \bar{A}$ es el morfismo de desingularización y que $\bar{A}$ es la desingularización de A".*

Demostración. 1. Es consecuencia de 1.8.2 y 1.8.3.

2. Si x es un punto no singular, entonces A_x es dominio de ideales principales luego íntegramente cerrado. Por tanto, $A_x = \overline{A_x} = \bar{A}_x$. Recíprocamente, si $A_x = \bar{A}_x$, entonces A_x es íntegramente cerrado, pues lo es $\bar{A}$ y por tanto $\bar{A}_x$ (por 1.7.3).

$\bar{A}$ es un A-módulo finito generado. Además, $\bar{A}_{A\setminus 0} = \overline{A_{A\setminus 0}} = \bar{\Sigma} = \Sigma$. Luego $(\bar{A}/A)_{A\setminus 0} = 0$ y existe $f \in A\setminus 0$ tal que $(\bar{A}/A)_f = 0$. Por tanto, $(\bar{A}/A)_x = 0$ para todo $x \notin (f)_0$. Luego, $A_x = \bar{A}_x$ para todo $x \notin (f)_0$. Como $(f)_0$ es un número finito de puntos cerrados, entonces el número de puntos singulares de $\operatorname{Spec} A$ es finito.

□

6. Ejemplo: $\operatorname{Spec}\mathbb{C}[x,y]/(y^2 - x^3)$ es no singular en todo punto, salvo en el origen. Observemos que

$$(y/x)^2 - x = 0$$

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 $\mathbb{C}[x,y]/(y^2 - x^3)$.

7. 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 $(\mathbb{Z}[x]/(x^2 - n, x)_y = \mathbb{Z}/2\mathbb{Z}$, luego $\mathfrak{m}_y \cdot (\mathbb{Z}[x]/(x^2 - n, x))_y = (x)$ e y es no singular. Veamos que 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 sólo 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 esta 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 $\mathbb{Z}[\sqrt{n}]$.

1.9. Apéndice: Métrica de la traza

Sea K una k-extensión finita de cuerpos. Dado $a \in K$, consideremos el endomorfismo k-lineal

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

Definamos en K la métrica (simétrica) de la traza:

$$T_2 : K \times K \to K,\ T_2(a,a') := \mathrm{tr}(h_{aa'})$$

Tenemos por tanto la polaridad asociada a T_2:

$$iT_2 : K \to K^* := \mathrm{Hom}_k(K,k),\ a \mapsto iT_2(a),\ \text{donde } iT_2(a)(a') := T_2(a,a')$$

Si $\{e_1,\dots,e_n\}$ es una base del k-espacio vectorial K, se dice, que $(T_2(e_i,e_j))_{ij}$ es la matriz asociada a T_2 en la base $\{e_1,\dots,e_n\}$. Si $\{w_1,\dots,w_n\}$ es la base dual de $\{e_1,\dots,e_n\}$, resulta que la matriz asociada a la polaridad iT_2 es precisamente $(T_2(e_i,e_j))_{ij}$.

Supongamos, a partir de ahora, que K es una k-extensión finita separable.

Existe una k-extensión Σ que la trivializa, es decir,

$$K \otimes_k \Sigma = \Sigma \times \overset{n}{\cdots} \times \Sigma$$

Explícitamente, si $\{g_1,\dots,g_n\} = \mathrm{Hom}_{k-alg}(K,\Sigma)$ tenemos que

$$K \otimes_k \Sigma \to \Sigma \times \overset{n}{\cdots} \times \Sigma,\ a \otimes \lambda \mapsto (g_1(a)\cdot\lambda, \overset{n}{\dots}, g_n(a)\cdot\lambda)$$

es un isomorfismo de Σ-álgebras.

Por cambio, de cuerpo base $k \hookrightarrow \Sigma$, tenemos el endomorfismo Σ-lineal

$$h_a \otimes 1 : K \otimes_k \Sigma \to K \otimes_k \Sigma,\ (h_a \otimes 1)(b \otimes \lambda) := a \cdot b \otimes \lambda = h_{a\otimes 1}(b \otimes \lambda)$$

Si la matriz de h_a en una base $\{e_i\}$ es (a_{ij}) la matriz de $h_a \otimes 1$ es (a_{ij}). Por lo tanto, $\mathrm{tr}(h_a) = \mathrm{tr}(h_a \otimes 1)$. Ahora bien, recordemos que vía el isomorfismo $K \otimes_k \Sigma = \Sigma \times \overset{n}{\cdots} \times \Sigma$, $a \otimes 1 = (g_1(a),\dots,g_n(a))$, 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 $g_i(a)$. Por tanto,

$$tr(h_a) = \sum_i g_i(a)$$

Resulta que T_2 es no singular, es decir, el determinante de la matriz a T_2 es no nulo: Basta verlo por cambio de cuerpo base $k \hookrightarrow \Sigma$, para la Σ-álgebra trivial Σ^n. Si consideramos la base estándar de Σ^n, la matriz asociada a T_2 es igual a la matriz Id, que tiene obviamente determinante no nulo.

1.10. Cuestionario

1. Sea X un espacio topológico y $f \in C(X,\mathbb{R})$ no invertible. Probar que existen funciones continuas f_1, f_2 no invertibles tales que $f = f_1 \cdot f_2$ ¿Existen elementos irreducibles en $C(X,\mathbb{R})$?
2. Probar que $C(\mathbb{R}^n,\mathbb{R})$ no es un anillo noetheriano.
3. ¿Es $\mathbb{Z}[x]$ DFU? ¿Es $\mathbb{Z}[x]$ DIP?
4. Sea A DFU y $p(x) = a_0x^n + \cdots + a_n \in A[x]$. Sean $b_1, b_2 \in A$ que no tengan divisores irreducibles comunes. Probar que si $p(b_1/b_2) = 0$ entonces b_1 divide a a_n y b_2 divide a a_0.
5. ¿Es $\operatorname{Spec}\mathbb{C}[x,y]$ una curva algebraica íntegra?
6. ¿Es $\operatorname{Spec}\mathbb{C}(x)[y]$ una curva $\mathbb{C}(x)$-algebraica íntegra?
7. ¿Es $\mathbb{Z}[x]$ un anillo de números enteros?
8. ¿Es $\mathbb{Z}[1/2]$ un anillo de números enteros?
9. ¿Es $\mathbb{Z}[i\sqrt{3} + \sqrt{5}, \sqrt[7]{3}]$ un anillo de números enteros?
10. Sea A un dominio de ideales principales ¿Es A un dominio de factorización única?
11. Calcular los puntos singulares de $\operatorname{Spec}\mathbb{C}[x,y]/(y^2 - x^3)$.
12. Calcular los puntos singulares de $\operatorname{Spec}\mathbb{C}[x,y]/(y^2 - x^2 + x^3)$.
13. Calcular los puntos singulares de $\operatorname{Spec}\mathbb{C}[x,y,z]/(1 + x^2 + y^2 + z^2, 2 + x^2 - y^2)$.
14. ¿Es $\mathbb{Z}[\sqrt{5}]$ un anillo de Dedekind?
15. ¿Es $(5) \subset \mathbb{Z}[e^{2\pi i/5}]$ un ideal primo? Descomponer (5) como potencia de ideales primos.
16. ¿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 d.i.p.?
17. Probar que $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ son dos factorizaciones de 6 como producto de irreducibles de $\mathbb{Z}[\sqrt{-5}]$. Descomponer en $\mathbb{Z}[\sqrt{-5}]$ como producto de ideales primos los ideales (2), (3), $(1 + \sqrt{-5})$ y $(1 - \sqrt{-5})$. Descomponer como producto de ideales primos el ideal (6).
18. Calcular la desingularización de $\mathbb{C}[x,y]/(y^2 - x^2 + x^3)$.

1.11. 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 Dede-

kind 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/).

1.12. Problemas

1. Probar 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. Probar 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 sólo 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. Probar 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 de dimensión de Krull 1. 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 $\tau\colon A\to A$ 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 sólo es cierto si $p(x)\in\mathbb{R}$ y $q(x)=0$.

   b. Supongamos que A es euclídeo y sea $c\in A-\mathbb{R}$ un elemento de grado mínimo. Podemos suponer que c es irreducible.

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

4. **Ternas pitagóricas:** Calcular 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 sólo 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 $u \cdot \bar{u} \in \mathbb{Z}$. Recíprocamente, sea $p \in \mathbb{Z}$ que divida a c. Si p es primo en $\mathbb{Z}[i]$ entonces divide a z (contradicción) o a $\bar{z}$, luego también a z (contradicción). Así pues, $p = z_1 \cdot \bar{z}_1$, con z_1 (y $\bar{z}_1$) irreducible. Podemos decir que z_1 divide a z (y $\bar{z}_1$ no divide a z, porque $z_1 \cdot \bar{z}_1$ no divide a z) y que $\bar{z}_1$ divide a $\bar{z}$ (y z_1 no divide a $\bar{z}$). Por tanto, z_1^2 que divide a c^2 ha de dividir a z. Tenemos $N(z/z_1^2) = (c/p)^2$. Por recurrencia concluimos.

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

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

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

En una tablilla cuneiforme aproximadamente del año 1.500 a.C. se ha encontrado una enumeración de ternas pitagóricas, entre las cuales se encontraba $(4961, 6480, 8161)$. Se obtiene con $x = 81$ y $y = 40$.

5. Probar 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.

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

   Resolución: Es consecuencia inmediata del problema anterior.

7. Sea A un dominio de factorización única y $S \subseteq A$ un sistema multiplicativo. Probar 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 $\frac{a}{s} \in A_S$ es irreducible, entonces salvo multiplicación por invertibles resulta que $\frac{a}{s} = \frac{a'}{s'}$ con $a' \in A$ irreducible: sea $a = a_1 \cdots a_n$ la descomposición en producto de irreducibles de a, entonces $\frac{a}{s} = \frac{a_1}{s} \cdot \frac{a_2}{1} \cdots \frac{a_n}{1}$ y todos los factores son invertibles salvo uno que es irreducible.

Dado $\frac{a}{s} \in A_S$, sea $a = a_1 \cdots a_n$ la descomposición en producto de irreducibles de a. Entonces, $\frac{a}{s} = \frac{a_1}{s} \cdot \frac{a_2}{1} \cdots \frac{a_n}{1}$ es una descomposición 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 dividen a ningún $t \in S$ (pues $\frac{a_1}{s_1}$ no es invertible) tenemos salvo orden e invertibles que $a_1 = b_1$, y por recurrencia es fácil concluir.

8. Sea $n = p_1^{n_1} \cdots p_r^{n_r}$ la descomposición en potencias de primos de $n \in \mathbb{N}$. Probar 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.

9. Probar que todo anillo de Dedekind que tenga sólo un número finito de ideales primos es un anillo de ideales principales.

   Resolución: Sea $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$. 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 $\pi(f) = (\bar{f_1}, \bar{1}, \ldots, \bar{1})$. 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.

10. Probar que todo anillo de Dedekind que tenga sólo un número finito de ideales primos es un anillo euclídeo.

    Resolución: Sea $\operatorname{Spec} A = \{x_1, \ldots, x_r\}$. Definamos $\operatorname{gr} \colon A \setminus \{0\} \to \mathbb{N}$ 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 $\operatorname{gr}(a) = n_1 + \cdots + n_r$. Obviamente, $\operatorname{gr}(ab) = \operatorname{gr}(a) + \operatorname{gr}(b) \geq \operatorname{gr}(a)$. 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 $n_1 < m_1, \ldots, n_s < m_s$ y $n_{s+1} \geq m_{s+1}, \ldots, n_r \geq m_r$. 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 $\operatorname{gr} r < \operatorname{gr} b$. Existe $q \in A$, de modo que $a - r = bq$, es decir, $a = bq + r$ con $\operatorname{gr} r < \operatorname{gr} b$.

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

    Resolución: Sea $(I)_0 = \{x_1, \ldots, x_r\}$ y sea $S = \{s \in A \colon s(x_1) \neq 0, \ldots, s(x_r) \neq 0\}$. Se cumple que $\operatorname{Spec} A_S = \{(0), \mathfrak{p}_{x_1}, \ldots, \mathfrak{p}_{x_r}\}$. Luego, A_S es d.i.p. Además, $A/I = (A/I)_S = A_S/I_S$, como se comprueba localmente, y es d.i.p. porque es un cociente de un d.i.p.

12. Probar 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 d.i.p., luego $\bar{I} = (\bar{g})$. Por tanto, $I = (f, g)$.

13. Sea $A = \mathbb{C}[x_1, \ldots, x_n]/(p_1, \ldots, p_{n-1})$ y $\alpha \in \operatorname{Spec}_{max} A$. probar que A_α es un dominio de ideales principales si y sólo 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 sólo 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 1.4.7.

14. Probar 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, $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ es un dominio de ideales primcipales.

15. Probar que $\mathbb{Z}[\sqrt{-5}]$ es un anillo de Dedekind. Sea $\mathfrak{m} = (2, 1 + \sqrt{-5})$. Probar 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). Probar 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 en tal caso $\mathbb{Z}[\sqrt{-5}]$ sería un dominio de ideales principales, luego un dominio de factorización única.

16. Descomponer $33 + 11\sqrt{-7}$ 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, $33 + 11x = (2 - x)(x + 2)(3 + x)$.

17. ¿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 $\mathbb{Z}$.

18. 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 $q(0) \neq 0$ (es decir, $x = 0$ corta transversalmente a la curva en el origen). Probar que y/x es entero sobre el anillo $(\mathbb{C}[x,y]/(p(x,y)))_{q(y)}$, y que

$$(\mathbb{C}[x,y]/(p(x,y)))[y/x] = \mathbb{C}[x,y/x]/(r(x,y/x)),$$

donde $x^k \cdot r(x,y/x) = p(x,y)$.

Resolución: 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 $(\mathbb{C}[x,y]/(p(x,y)))_{q(y)}$.

19. Desingularizar 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 $\mathbb{C}[x,y]/(y^2 - y^3 + x^4) \hookrightarrow \mathbb{C}[x,y/x]/((y/x)^2 - (y/x)^3 x + x^2)$. De nuevo, $0 = ((y/x)^2 - (y/x)^3 x + x^2)/x^2 = (y/x^2)^2 - (y/x^2)^3 x^2 + 1 = z^2 + z^3 x^2 + 1$ que es una curva ya sin puntos singulares. Así pues, la desingularización de $\mathbb{C}[x,y]/(y^2 - y^3 + x^4)$ es $\mathbb{C}[x,z]/(z^2 + z^3 x^2 + 1)$ con $z = y/x^2$.

Capítulo 2

Fibras de los morfismos finitos

2.1. 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.

2.2. 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. En los A-módulos libres se define el rango del A-módulo libre como el número de elementos de sus bases.

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. En términos de éstas definiremos la longitud del módulo, concepto que no coincide con el de rango, en general.

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 es simple si y sólo si $\text{Anul}\langle m \rangle$ es un ideal maximal, es decir, M es simple si y sólo 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 $M_{i-1} \underset{\neq}{\subset} N \underset{\neq}{\subset} M_i$. 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 $l(M)$.

Sobre espacios vectoriales el concepto de longitud coincide con el de dimensión.

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 $m = n$.

□

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).

5. 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 $n+m$. □

6. Proposición: *Se cumple que* $l(M \oplus N) = l(M) + l(N)$.

Demostración. Tenemos la inclusión $M \hookrightarrow M \oplus N$, $m \mapsto (m,0)$ y $(M \oplus N)/M \simeq N$, $\overline{(m,n)} \mapsto n$. Concluimos por la proposición previa. □

7. Corolario: *Sea* $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$ *una cadena de* A*-submódulos de* 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 $n > 1$, $l(M) = l(M_{n-1}) + l(M/M_{n-1}) = \sum_{i=1}^{n-1} l(M_i/M_{i-1}) + l(M/M_{n-1}) = \sum_{i=1}^{n} l(M_i/M_{i-1})$. □

8. Proposición: *Sea* $\mathcal{O}$ *una* k*-álgebra local de ideal maximal* $\mathfrak{m}$*. Probar que si* M *es un* $\mathcal{O}$*-módulo de longitud finita 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,

$$\dim_k M = \sum_{i=1}^{n} \dim_k M_i/M_{i-1} = n \cdot \dim_k \mathcal{O}/\mathfrak{m} = l(M) \cdot \dim_k \mathcal{O}/\mathfrak{m}$$

□

2.3. Multiplicidades y grados en dimensión cero

1. Proposición: *Sea* A *un anillo tal que* $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$ *y los ideales primos* $\mathfrak{m}_{x_i}$ *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 contenido en $\mathfrak{m}_{x_i}$ y $\mathfrak{m}_{x_j}$. 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. □

2. 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 $\operatorname{gr} y := \dim_k A/\mathfrak{m}_y$.

3. 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. En efecto, $A = \prod_{y\in Y} A_y$, luego $\dim_k A = \sum_{y\in Y} \dim_k A_y = \dim_k(A/\mathfrak{m}_y)\cdot l_A(A_y)$. Con todo, se concluye. □

4. Ejercicio: Sea la $\mathbb{R}$-álgebra finita $A = \mathbb{R}[x]/(x^4-2x^3+2x^2-2x+1)$ y sea $Y = \operatorname{Spec} A$. Calcular el número de puntos de Y, contando grados y multiplicidades. Calcular la multiplicidad y grado de cada punto de Y.

2.4. Fibras de un morfismo finito

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 $\pi^{-1}(x)$ 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,

$$\text{Número de puntos de } \pi^{-1}(x) \text{ contando grados y multiplicidades} = \sum_{y\in\pi^{-1}(x)} m_y \cdot \operatorname{gr}_x y$$

1. 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 $\alpha \in \operatorname{Spec}\mathbb{R}[x]$, calcular el número de puntos de las fibras, las multiplicidades y grados de los puntos de las fibras de π.

2. 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 anillos. 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 $n_x = \dim_{\Sigma_A} \Sigma_B$.

□

3. 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. Probemos primero que $(\bar{f}) \subset A/(fg)$ es un A-módulo isomorfo a $A/(g)$. 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 $A/(g)$. La imagen del morfismo es $(\bar{f}) \subset A/(fg)$, luego $A/(g) \simeq (\bar{f})$.

Observemos que $(A/(fg))/(\bar{f}) = A/(fg, f) = A/(f)$. Luego,

$$l(A/(fg)) = l((\bar{f})) + l((A/(fg))/(\bar{f})) = l(A/(g)) + l(A/(f))$$

□

4. 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.

5. 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. Escribamos $\mathfrak{m}_y B_y = (t)$. Entonces,

$$l_B(B/\mathfrak{m}_x B)_y = l_B(B_y/\mathfrak{m}_y^{e_y} B_y) = l_B(B_y/(t^{e_y})) = e_y \cdot l_B(B_y/(t)) = e_y,$$

□

Sea $A \hookrightarrow B$ un morfismo finito inyectivo y $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ el morfismo inducido.

6. Definición: Se dice que π no ramifica en y si $B_y/\mathfrak{m}_x B_y$ es una $A/\mathfrak{m}_x$-álgebra separable. Si π ramifica en y se dice que y es un punto de ramificación de π y que $\pi(y)$ es un punto rama de π.

Se cumple que π no ramifica en y si y sólo 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 sólo 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.

7. Proposición: *Sea A un anillo íntegro de cuerpo de fracciones Σ. Sea $p(x) \in A[x]$ un polinomio mónico irreducible en $\Sigma[x]$ y separable, y $0 \neq \Delta \in A$ 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, $z \in \operatorname{Spec}_{\text{máx}} A$ es un punto de rama de π si y sólo si $z \in (\Delta)_0$.*

Demostración. El punto z es un punto rama si y sólo $(A[x]/(p(x)))/\mathfrak{p}_z = A/\mathfrak{p}_z[x]/(\overline{p(x)})$ 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, $z \in (\Delta)_0$. □

8. Teorema: *Sea $A \hookrightarrow B$ un morfismo finito inyectivo entre anillos noetherianos íntegros de dimensión de Krull* 1. *Sean Σ_A y Σ_B los cuerpos de fracciones de A y B respectivamente. Supongamos que $\Sigma_A \hookrightarrow \Sigma_B$ es una extensión separable de cuerpos. Entonces, el morfismo* $\mathrm{Spec}B \to \mathrm{Spec}A$ *ramifica en un número finito de puntos.*

Demostración. Escribamos $B = A[\alpha_1, \ldots, \alpha_n]$, donde los α_i son enteros y separables sobre A. Los puntos rama del morfismo $A \to A[\alpha_i]$ son un número finito. Luego los puntos rama del morfismo $A \to A[\alpha_1] \otimes_A \cdots \otimes_A A[\alpha_n]$ son un número finito. Como B es un cociente de $A[\alpha_1] \otimes_A \cdots \otimes_A A[\alpha_n]$, los puntos rama de $A \to B$ son un número finito. Luego $\mathrm{Spec}B \to \mathrm{Spec}A$ ramifica en un número finito de puntos. □

9. Ejercicio: Consideremos el morfismo finito $\mathbb{Z} \to \mathbb{Z}[\sqrt{3}]$. Calcular el número de puntos, contando grados y multiplicidades, de las fibras de este morfismo, los puntos de ramificación e índices de ramificación.

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, $\mathfrak{p}_{gy} := g(\mathfrak{p}_y)$.

10. Teorema: *Sea G un grupo finito de automorfismos de un anillo B. Denotemos por $B^G := \{b \in B\colon g(b) = b$ para todo $g \in G\}$ y por $(\mathrm{Spec}B)/G := \{\bar{y}$, con $y \in \mathrm{Spec}B$, donde decimos que $\bar{y} = \bar{z}$ si y sólo si existe $g \in G$ tal que $z = gy\}$. Se cumple que*

$$\mathrm{Spec}(B^G) = (\mathrm{Spec}B)/G$$

donde $B^G = \{b \in B\colon g(b) = b$, para todo $g \in G\}$.

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, 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 $\mathfrak{p}_z \not\subseteq \mathfrak{p}_{g(y)}$, 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.

□

11. 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 $X = \mathrm{Spec}\,\mathbb{C}[x,y]/(y^2-x)$. Calcular X/G.

12. 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 $X = \mathrm{Spec}\,\mathbb{Z}[\sqrt{2}]$. Calcular X/G.

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, $y \in \mathrm{Spec}B$. Entonces tenemos el automorfismo $\bar{g}\colon k(y) \to k(gy)$, $\bar{g}(\bar{b}) = \overline{g(b)}$ (es decir, $\bar{g}(b(y)) := (gb)(gy)$).

13. 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 $\pi\colon \mathrm{Spec}B \to \mathrm{Spec}B^G$. Sea $y \in \mathrm{Spec}B$, $x := \pi(y)$ y denotemos $k(x)$, $k(y)$ los cuerpos residuales de x e y. Sea $D := \{g \in G\colon g(y) = y\}$ el "grupo de descomposición" de y. Si $k(y)$ es una $k(x)$-álgebra separable, entonces $k(y)$ es una $k(x)$-extensión de Galois y el morfismo natural $D \to \mathrm{Aut}_{k(x)-alg}(k(y))$, $g \mapsto \bar{g}$ es epiyectivo.*

Demostración. Localizando en x, podemos suponer que y e x son puntos cerrados. Observemos que $\pi^{-1}(x) = \mathrm{Spec}B/\mathfrak{m}_x B = \{y_1, \dots, y_n\} = G \cdot y$. 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 $\overline{P(X)} = \prod_{g\in D}(X - \bar{g}(\theta)) \cdot X^{|G|-|D|} \in k(x)[X]$ 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.

□

14. Ejercicio: Calcular el grupo de descomposición de $x \in X$, cuando X es el definido en el ejercicio 2.4.11 o 2.4.12.

2.5. Automorfismo de Fröbenius

Si K es un cuerpo finito, $p > 0$ la característica de K y $\dim_{\mathbb{F}_p} K = n$, entonces $|K| = p^n$. Los elementos de $K\backslash\{0\}$ 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 $\mathbb{F}_{p^n}$. 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 $\mathrm{Aut}_{\mathbb{F}_p-alg}\mathbb{F}_{p^n} = \langle F\rangle$. Es más, si $m \leq n$, $\mathbb{F}_{p^n}$ es una $\mathbb{F}_{p^m}$-extensión de Galois de grupo de Galois $\langle F^m\rangle$.

1. Teorema: *Sea A un anillo de enteros tal que su cuerpo de fracciones Σ_A sea una $\mathbb{Q}$-extensión de Galois de grupo G y tal que $G \cdot A = A$. Sea $\mathfrak{m}_y \subset A$ un ideal maximal y sea $(p) = \mathfrak{m}_y \cap \mathbb{Z}$. El automorfismo de Fröbenius, F, de $A/\mathfrak{m}_y$ está inducido por algún automorfismo $F_p \in G$ de A, y éste es único cuando A/pA es reducida (es decir, el morfismo $\mathrm{Spec}A \to \mathrm{Spec}\,\mathbb{Z}$ no ramifica en y), en este caso se dice que F_p es el automorfismo de Fröbenius de Σ_A en el primo p.*

Demostración. Observemos que $A^G = \mathbb{Z}$ porque está incluido en $\mathbb{Q}$ y es finito sobre $\mathbb{Z}$. Observemos que $A/\mathfrak{m}_y$ es una $\mathbb{Z}/p\mathbb{Z}$-extensión de Galois. Sea $D := \{g \in G : g(y) = y\}$, por el teorema 2.4.13, el morfismo $D \to \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}-alg} A/\mathfrak{m}_y = \langle F \rangle$ es epiyectivo, luego F está inducido por algún automorfismo $F_p \in D$. La fibra de p es igual a $G \cdot y$, luego todos los puntos de la fibra de p (que son $|G/D|$) tienen la misma multiplicidad y grado. Recordemos que el número de puntos de las fibras del morfismo $\mathbb{Z} \hookrightarrow A$ es constante, e igual a $\dim_{\mathbb{Q}} \Sigma_A = |G|$. Supongamos además que y no es un punto de ramificación. Entonces,

$$|G| = \text{Nº de puntos de la fibra de } p\text{, cont. grad. y mult.} = |G/D| \cdot \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{m}_y$$

Luego, $\dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{m}_y = |D|$, $D = \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}-alg} A/\mathfrak{m}_y = \langle F \rangle$ y F_p es único. □

2. Observaciones: 1. $F_p : \Sigma_A \to \Sigma_A$, 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 A/pA es reducida y $y_i \in \mathrm{Spec}(A/pA)$, entonces $(A/pA)_{y_i} = A/\mathfrak{m}_{y_i}$. Por tanto, $\mathfrak{m}_{y_i} \cdot A_{y_i} = p \cdot A_{y_i}$. 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 enteros de Σ' y $\bar{A}$ el anillo de enteros 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 enteros $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. 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.

3. 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.

2.6. 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 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 número primo $q \neq 2$ y un entero $n \in \mathbb{Z}$, queremos saber cuándo $x^2 - n \in \mathbb{F}_q[x]$ tiene raíces modulares. Escribiremos (el símbolo de Legendre)

$$\left(\frac{n}{q}\right) := \begin{cases} 1, & \text{si } n \text{ es un resto cuadrático módulo } q \ (\bar{n} = a^2, \text{ para cierto } a \in \mathbb{F}_q) \\ -1, & \text{en otro caso} \end{cases}$$

   Recordemos que $\bar{n} \in \mathbb{F}_q^{*2}$ si y sólo $\bar{n}^{(q-1)/2} = 1 \in \mathbb{F}_q^*$. 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 $n = r \cdot s$, $(\frac{n}{q}) = (\frac{r}{q}) \cdot (\frac{s}{q})$.

   Demos un algoritmo para un cálculo rápido de $(\frac{n}{q})$. Descomponiendo n en producto de primos podemos suponer que $n = p$ es primo. Tenemos que ver cuándo $\bar{p} \in \mathbb{F}_q^{*2}$.

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 $\mathbb{Q}[e^{2\pi i/q}]^{\mathbb{F}_q^{*2}}$. $\mathbb{F}_q^{*2}$ 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 sólo 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 es 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 $p=2$. Desgraciadamente $\mathbb{Z}\hookrightarrow\mathbb{Z}[\sqrt{\tilde{q}}]$ ramifica en (2), lo cual ya implica que el ideal primo de la fibra, $(2,\sqrt{\tilde{q}}+1)$ es singular (véase 2.5.2 4.) y que $\tilde{q}=1 \mod 4$. Pero si consideramos el cierre entero de $\mathbb{Z}[\sqrt{\tilde{q}}]$, que es $\mathbb{Z}[\frac{\sqrt{\tilde{q}}+1}{2}]$ ya no ramifica en (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 $\frac{\tilde{q}-1}{4}$ sea múltiplo de 2. Por tanto,

$$(\frac{2}{q})=(-1)^{\frac{\tilde{q}-1}{4}}=(-1)^{\frac{\tilde{q}+1}{2}\cdot\frac{\tilde{q}-1}{4}}=(-1)^{\frac{\tilde{q}^2-1}{8}}=(-1)^{\frac{q^2-1}{8}}$$

2.7. Cuestionario

1. Calcular $l_{\mathbb{Z}}(\mathbb{Z}/4\mathbb{Z})$ y $l_{\mathbb{Z}}(\mathbb{Z}/12\mathbb{Z})$.
2. Calcular $l_{k[x]}(k[x]/(x^2))$, $l_{k[x]}(k[x]/(x^2\cdot(x-1)^3)$.
3. Resolver el ejercicio 2.3.4.
4. Resolver el ejercicio 2.4.1.
5. Resolver el ejercicio 2.4.11
6. Sea $\tau:\mathbb{R}[x,y]/(y^2-x)\to\mathbb{R}[x,y]/(y^2-x)$ el automorfismo de $\mathbb{R}$-álgebras definido por $\tau(y)=-y$ y $\tau(x)=x$ y sea $G=\{\mathrm{Id},\tau\}$. Consideremos el morfismo

$$\pi:\ \mathrm{Spec}\,\mathbb{R}[x,y]/(y^2-x)\to\mathrm{Spec}(\mathbb{R}[x,y]/(y^2-x))^G=\mathrm{Spec}\,\mathbb{R}[x]$$

   Calcular los puntos de ramificación de π. Para todo $y\in\mathrm{Spec}_{max}\,\mathbb{R}[x,y]/(y^2-x)$ calcular la multiplicidad con la que aparece en la fibra de $x=\pi(y)$, su grado y su grupo descomposición.
7. Resolver el ejercicio 2.4.12
8. Resolver el ejercicio 2.4.9.

9. Calcular el automorfismo de Fröbenius de $\mathbb{Q}[\sqrt{2}]$ en 3.
10. Resolver el problema 7.
11. Resolver el problema 8.
12. Calcular $(\frac{14}{23})$.
13. Sean $p < q$ primos y supongamos $p \neq 2$. Probar que $(\frac{p}{q}) = -(\frac{q}{p})$ si y sólo sí $(q-1)/2$ y $(p-1)/2$ son impares.
14. Sea $q > 2$ primo. Probar que $(\frac{2}{q}) = 1$ si y sólo si $q+1$ ó $q-1$ es divisible por 8.

2.8. 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 quality of Fröbenius's work in his Zürich years. Weierstrass and Fuchs listed 15 topics on which Fröbenius had made major contributions:

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

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

-The theory of linear differential equations.

-On Pfaff's problem.

-Linear forms with integer coefficients.

-On linear substitutions and bilinear forms...

-On adjoint linear differential operators...

-The theory of elliptic and Jacobi functions...

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

-On Sylow's theorem.

-On double cosets arising from two finite groups.

-On Jacobi's covariants...

-On Jacobi functions in three variables.

-The theory of biquadratic forms.

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

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

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

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

This paper on group characters was presented to the Berlin Academy on July 16 1896 and it contains work which Fröbenius had undertaken in the preceding few

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

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

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

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

Fröbenius had a number of doctoral students who made important contributions to mathematics. These included Edmund Landau who was awarded his doctorate in 1899, Issai Schur who was awarded his doctorate in 1901, and Robert Remak who was awarded his doctorate in 1910. Fröbenius collaborated with Schur in representation theory of groups and character theory of groups. It is certainly to Fröbenius's credit that he so quickly spotted the genius of his student Schur. Fröbenius's representation theory for finite groups was later to find important applications in quantum mechanics and theoretical physics which may not have entirely pleased the man who had such "pure"views about mathematics.

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

Haubrich gave the following overview of Fröbenius's work:

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

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

2.9. Problemas

1. Sea $A = k[x,y]$ y $\mathfrak{m} = (x,y)$. Calcular $l_A(A/\mathfrak{m}^3)$.

   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 $\mathfrak{m} = (x,y)$. Calcular $l_A(A/\mathfrak{m}^n)$.

   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 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 factores irreducibles (u invertible), entonces $l_A(A/(a)) = n_1 + \cdots + n_r$.

   Resolución: $l_A(A/(a)) = \sum_i n_i l_A(A/(p_i)) = \sum_i n_i$.

4. Sea A un dominio de Dedekind e $I \subseteq A$ 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 $l_A(A/I) = n_1 + \cdots + n_r$.

   Resolución: $l_A(A/I) = \sum_i l_A(A/\mathfrak{p}_{x_i}^{n_i}) = \sum_i l_{A_{x_i}}(A_{x_i}/\mathfrak{p}_{x_i}^{n_i} A_{x_i}) = \sum_i n_i$, pues $\mathfrak{p}_{x_i} A_{x_i} = t_i A_{x_i}$, t_{x_i} irreducible.

5. Sea $A = \mathbb{Z}[\sqrt{-5}]$. Calcular $l_A(A/(6))$.

   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. Calcular 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. Calcular 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

$$\mathrm{gr}_{\mathbb{Q}}\, z = \dim_{\mathbb{Q}}(\mathbb{Q}[x]/(x^3))/\mathfrak{m}_z = \dim_{\mathbb{Q}} \mathbb{Q} = 1.$$

7. Probar 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 permita 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.

8. 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? Probar 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 sólo 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.

Capítulo 3

Valoraciones y valores absolutos

3.1. Introducción

Hablemos sin excesiva precisión.

Sea $C = \operatorname{Spec} A$ una k-curva afín no singular, sea K el cuerpo de fracciones de A. En Geometría Algebraica se prueba que C es un abierto de una curva proyectiva no singular $\bar{C}$, denominada la variedad de Riemann de K. $\bar{C} = C \coprod \bar{C}_\infty$, donde $\bar{C}_\infty$ es un conjunto finito. Se cumple $\bar{C}$ es biyectivo con el conjunto de valores absolutos de K, $|-|$ tales que $|\lambda| = 1$ para todo $\lambda \in k$. Precisemos la correspondencia: dado un punto $x \in C$ y $a \in A$ se define el valor absoluto $|a|_x := e^{-v_x(a)}$, donde se dice que $v_x(a) = n$ si $a \in \mathfrak{m}_x^n \setminus \mathfrak{m}_x^{n+1}$. Probaremos que el producto de todos los valores absolutos de toda $f \in K$ no nula es igual a 1. O dicho de otro modo: el número de ceros de una función (meromorfa) es igual al número de polos. Una consecuencia inmediata es el teorema de Bézout, que dice que 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 $n \cdot m$.

Sea A el anillo de enteros de un cuerpo de números K. Sea $\bar{C}$ el conjunto de todos los valores absolutos de K. Se cumple que $\bar{C}$ se corresponde biyectivamente con $\operatorname{Spec} A \coprod \bar{C}_\infty$, donde $\bar{C}_\infty = \operatorname{Hom}_{anillos}(K, \mathbb{C})$. Dado $x \in \operatorname{Spec} A$ se le asigna el valor absoluto $|a|_x := e^{-v_x(a)}$, dado $\sigma \in \bar{C}_\infty$ se le asigna el valor absoluto $|a|_\sigma := |\sigma(a)|$. Ahora ya, la Teoría de Números puede ser guiada por la Geometría Algebraica. Por ejemplo, probaremos que el producto de todos los valores absolutos de una $f \in K$ es igual a 1.

3.2. Valoraciones. Anillos de valoración

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 verifica

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 $v(f^{-1}) = -v(f)$.

Sea $\mathcal{O}$ un anillo local de ideal maximal $\mathfrak{m}$ y cuerpo de fracciones Σ. Supongamos que $\mathcal{O}$ cumple que si $f \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$ y $g \in \mathfrak{m}^m \setminus \mathfrak{m}^{m+1}$ entonces $f \cdot g \in \mathfrak{m}^{n+m} \setminus \mathfrak{m}^{n+m+1}$. Para cada $f \in \mathcal{O}$ no nula, denotemos $v_{\mathfrak{m}}(f)$ al máximo número natural n tal que $f \in \mathfrak{m}^n$. Es fácil ver que la aplicación

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

está bien definida y es una valoración discreta de Σ. Esta valoración se denomina valoración $\mathfrak{m}$-ádica.

Si $\mathcal{O}$ es de ideales principales, es inmediato ver que $\mathcal{O} = \{f \in \Sigma \mid v_{\mathfrak{m}}(f) \geq 0\}$. Veamos el recíproco.

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

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

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

Si v es discreta entonces $\mathcal{O}_v$ es un dominio de ideales principales de dimensión de Krull 1, y $v = v_{\mathfrak{p}_v}$.

Demostración. 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. $\mathcal{O}_v$ es un anillo local porque los invertibles son precisamente $\{f \in \Sigma : v(f) = 0\}$ y el ideal maximal es $\mathfrak{p}_v := \{f \in \Sigma : v(f) > 0\}$.

Si v es discreta, $\mathfrak{p}_v = (t)$, para cualquier t tal que $v(t) = 1$: Dado $f \in \mathfrak{p}_v$, entonces $v(f) = n > 0$ y $v(f/t^n) = 0$, luego f/t^n es un invertible de $\mathcal{O}_v$ y $f = (f/t^n) \cdot t^n$. Por tanto, $\mathcal{O}_v$ es un dominio de ideales principales. Para concluir, veamos que $v = v_{\mathfrak{p}_v}$. Sea t un parámetro que genere $\mathfrak{p}_v$, luego $v(t) = 1$. Si $f \in \mathcal{O}_v$, entonces $f = ut^n$, con u invertible, luego $v(f) = n = v_{\mathfrak{p}_v}(f)$ y $v = v_{\mathfrak{p}_v}$. □

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

$$\begin{aligned} \{\textit{Valoraciones discretas de } \Sigma\} &= \left\{ \begin{array}{l} \textit{Subanillos propios de } \Sigma\textit{, de cuerpo de frac-} \\ \textit{ciones } \Sigma\textit{, locales, de ideales principales} \end{array} \right\} \\ v &\mapsto \mathcal{O}_v \end{aligned}$$

4. Ejercicio: Sea v una valoración discreta y sea $f \in \mathcal{O}_v$. Probar que $v(f) = l(\mathcal{O}_v/(f))$.

5. Definición: Dada una valoración $v : \Sigma^* \to \mathbb{R}$ diremos que $\mathcal{O}_v$ es un anillo de valoración de Σ. Si v es discreta diremos que $\mathcal{O}_v$ es un anillo de valoración discreta de Σ.

Por el teorema anterior, un anillo es un anillo de valoración discreta de Σ si y sólo si es un subanillo propio local de ideales principales de Σ, de cuerpo de fracciones Σ.

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

6. 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 sólo si existe $\alpha > 0$ tal que $v' = \alpha \cdot v$.*

Demostración. Obviamente, si $v' = \alpha \cdot v$, entonces $\mathcal{O}_v = \mathcal{O}_{v'}$. Supongamos que $\mathcal{O}_v = \mathcal{O}_{v'}$. Sea $f \in \mathfrak{p}_v = \mathfrak{p}_{v'}$ no nulo (caso $\mathcal{O}_v = \Sigma$ implica $v = 0 = v'$). Podemos suponer 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,

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

Luego, si definimos $C' = \{\frac{n}{m} \in \mathbb{Q} \colon v'(f') - \frac{n}{m} v'(f) \geq 0\}$, tendremos que $C = C'$ y esto implica que $v(f') = v'(f')$, luego $v = v'$. □

3.3. Anillos de valoración y cierre entero

1. Proposición: *Los anillos de valoración son íntegramente cerrados en su cuerpo de fracciones.*

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 $a \in \mathcal{O}_v$. □

2. 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,*

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

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

3. 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. □

4. 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 son discretos (salvo el trivial).*
2. $\operatorname{Spec} \bar{A} = \{$*Anillos de valoración de Σ que contienen a A*$\}$, $x \mapsto \bar{A}_x$.

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

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

Demostración. 2. Sea $\mathcal{O}_v$ un anillo de valoración de Σ que contenga a A. $\mathcal{O}_v$ es íntegramente cerrado en su cuerpo de fracciones. 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 $\bar{A}_x = \mathcal{O}_v$.

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.

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

□

5. 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. $\operatorname{Spec} A' = \{$*Anillos de valoración de Σ' que contienen a A*$\}$, $x \mapsto A'_x$.
2. *A' es igual a la intersección de todos los anillos de valoración de Σ' que contienen a A, es decir,*

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

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

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

1. *Todos los anillos de valoración de K son discretos (salvo el trivial).*
2. $\operatorname{Spec} A = \{$*Anillos de valoración de K*$\}$, $x \mapsto A_x$.
3. *A es igual a la intersección de todos los anillos de valoración de K, es decir,*

$$A = \bigcap_{v\colon K^* \to \mathbb{Z}} \mathcal{O}_v$$

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 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 tanto, $\operatorname{Spec} A = \{$Conjunto de anillos de valoración de $K\}$, $x \mapsto A_x$ y todos los anillos de valoración de K son discretos (salvo el trivial). Como $A = \cap_{x\in\operatorname{Spec} A} A_x$ concluimos 3.

□

7. Ejemplo: $\operatorname{Spec}\mathbb{Z} = \{\text{Conjunto de anillos de valoración de } \mathbb{Q}\}$.

8. Ejemplo: $\mathbb{P}^1(\mathbb{C}) = \{\text{Conjunto de anillos de valoración de } \mathbb{C}(x), \text{ triviales sobre } \mathbb{C}\}$.

9. 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_∞. Calcular $v(\frac{x^2+1}{x})$ en los tres casos.

10. 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 $v_{(0,0)}(\frac{\bar{x}+\bar{y}}{\bar{x}^2})$?.

11. Ejercicio: Calcular todas las valoraciones discretas de $\mathbb{Q}(\sqrt{5})$.

12. Ejercicio: Sea $A = \mathbb{C}[x,y]/(y^2 - x)$, Σ el cuerpo de fracciones de A. Sea v una valoración discreta de Σ, trivial sobre $\mathbb{C}$. Supongamos que $v(\bar{x}) \geq v(\bar{y})$. Si $v(\bar{y}) \geq 0$, probar que existe $z \in \operatorname{Spec} A$, tal que $v = v_z$. Si $v(\bar{y}) \leq 0$ y definamos $B := \mathbb{C}[\bar{x}/\bar{y}, 1/\bar{y}] \subset \Sigma$ (observemos que $1/\bar{y} - (\bar{x}/\bar{y})(1/\bar{y})^2 = 0$). Probar que existe $z \in \operatorname{Spec} B$ tal que $v = v_z$.

3.3.1. 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. Sea C el conjunto de todos los anillos de valoración de K, triviales sobre k (es decir, que contienen a k). Dotemos a C de la siguiente 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 3.3.5, 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, y $C \setminus U$ y $C \setminus U'$ son conjuntos finitos.

13. Definición: Se dice que C es la variedad de Riemann asociada a K.

Todo morfismo $K \to L$ de k-extensiones, entre extensiones de tipo finito de grado de trascendencia 1, induce un morfismo $\pi : C_L \to C_K$ entre las variedades de Riemann asociadas, definido por $\mathcal{O}_w \mapsto \mathcal{O}_w \cap K$. 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, el morfismo $\pi : V \to U$ es el morfismo inducido por el morfismo de anillos natural $A \to B$, que es un morfismo finito.

14. Variedad de Riemann y curvas proyectivas: Sea $C' = \operatorname{Proj} k[\xi_0, \ldots, \xi_n]$ ($\operatorname{gr} \xi_i = 1$, para todo i) una curva proyectiva y supongamos que $k[\xi_0, \ldots, \xi_n]$ es un anillo íntegro. Sea $\Sigma := k(\xi_1/\xi_0, \ldots, \xi_n/\xi_0)$, "el cuerpo de funciones de C'" (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

$\mathcal{O}_{C',x} := k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]_x \subseteq \Sigma$ (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 $\mathcal{O}_{C',x} \neq \mathcal{O}_{C',x'}$.

Dado un anillo de valoración $\mathcal{O}_v$ de Σ, trivial sobre k, existe un único punto $x \in C'$, tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',x}$: 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, $k[\xi_0/\xi_i,\dots,\xi_n/\xi_i] \subset \mathcal{O}_v$. Si $\mathfrak{p}_x := \mathfrak{p}_v \cap k[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, tenemos que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',x}$. Sea otro $x' \in C'$ tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',x'}$. Podemos suponer, por cambio de coordenadas, que $x, x' \in U^h_{\xi_0}$. Entonces, $\mathfrak{p}_{x'} := \mathfrak{p}_v \cap k[\xi_1/\xi_0,\dots,\xi_n/\xi_0] = \mathfrak{p}_x$ y $x' = x$.

Sea C la variedad de Riemann de Σ. Consideremos el morfismo natural $\pi\colon C \to C'$, donde $\pi(v)$ es tal que $\mathcal{O}_v$ domina a $\mathcal{O}_{C',\pi(v)}$. Consideramos el abierto

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

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

Se dice que C es la desingularización de C'.

15. 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.

16. Ejemplos: La variedad de Riemann asociada a $k(x)$ es la recta proyectiva $\mathbb{P}^1$.

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

3.3.2. Ceros y polos de una función

Sea C la variedad de Riemann asociada a K y $f \in K$ trascendente. Consideremos la inclusión $k(f) \hookrightarrow K$ y el morfismo inducido entre las variedades de Riemann

$$\tilde{f}\colon C \to \mathbb{P}^1.$$

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 $\tilde{f}\colon C \to \mathbb{P}^1$ 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 $\{x_1,\dots,x_n\}$ 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,

$$0 = \text{Nº de puntos de la fibra del } 0 \; - \; \text{Nº de puntos de la fibra del } \infty = \sum_{x \in C} v_x(f) \operatorname{gr}_k x$$

17. Teorema: *Sea K una extensión de tipo finito de k de grado de trascendencia 1, C la variedad de Riemann asociada a K y $f \in K$. Entonces,*

$$\boxed{\textstyle\sum_{x \in C} v_x(f) \operatorname{gr}_k x = 0},$$

es decir, el número de ceros de f es igual a su número de polos.

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, $C \cap C' = (C \cap U^h_{x_0}) \cap (C' \cap U^h_{x_0})$ y podemos trabajar en el abierto afín $U^h_{x_0}$. 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 $U^h_{x_0}$ 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.

18. 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 sólo 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 $q(x, y) \in K$. 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,

$$(C \cap C') = m \cdot (C \cap \{x_0 = 0\}) = m \cdot n$$

□

3.4. 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 sólo 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. Ejemplos: $||: \mathbb{Q} \to \mathbb{R}$, $|a| := a$ si $a > 0$ y $|a| := -a$ si $a < 0$ es un valor absoluto.

Sea $p \in \mathbb{N}$ primo. La aplicación $||_p : \mathbb{Q} : \mathbb{R}$, $|a|_p := e^{-v_p(a)}$ 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.

3. 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 $a \in K$.

4. Proposición: *Dos valores absolutos sobre un cuerpo K son equivalentes si y sólo si inducen 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 triviales (que se caracterizan por inducir la topología discreta). 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. Observemos que

$$\frac{n}{m} < \alpha \iff \frac{|x|^{\frac{n}{m}}}{|y|} < 1 \iff \left|\frac{x^n}{y^m}\right| < 1 \iff \frac{x^n}{y^m} \in B(0, 1)$$

Por tanto, si $||'$ es equivalente a $||$, tenemos que $|y|' = |x|'^\alpha$. Si definimos $r := \log_{|x|} |x|'$, $|y|' = |x|'^\alpha = (|x|^r)^\alpha = |y|^r$, para todo y. □

3.4.1. Valores absolutos arquimedianos

5. 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 toda constante $C > 0$ existe un número natural n tal que $|n| > C$.

Evidentemente, todo cuerpo dotado de un valor absoluto arquimediano debe ser de característica cero.

6. 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,

$$n = a_0 + a_1 d + \ldots + a_k d^k, \qquad \text{con } 0 \leq a_i < d$$

De donde

$$|n| \leq d + d|d| + \ldots + d|d|^k \leq d(1+k) \leq d(1 + \log_d n)$$

Por tanto,

$$|n^k| \leq d(1 + k \log_d n)$$

Por otra parte,

$$|n^k| = |n|^k$$

Entonces,

$$1 \leq \lim_{k \to \infty} \frac{d(1 + k \log_d n)}{|n|^k} = 0$$

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.

□

7. Primer teorema de Ostrowski, 1917: *Todo valor absoluto arquimediano sobre* $\mathbb{Q}$ *es equivalente al valor absoluto usual.*

Demostración. Por el lema $|2| > 1$. Sustituyendo $||$ por $||^r$, con $r > 0$ conveniente, podemos suponer que $|2| = 2$. Entonces, $|3| \leq |2| + |1| = 3$ y $4 = |2| \cdot |2| = |4| \leq |3| + 1$, luego $|3| = 3$. Entonces, $|5| \leq |4| + |1| = 5$ y $6 = |2| \cdot |3| = |6| \leq |5| + 1$, luego $|5| = 5$. Así sucesivamente, obtenemos que $||$ es el valor absoluto usual sobre $\mathbb{N}$, luego lo es sobre $\mathbb{Q}$. □

Vamos ahora a determinar los valores absolutos arquimedianos sobre un cuerpo de números K (extensión finita de $\mathbb{Q}$).

8. 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 sólo 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 sólo si existe una constante $C > 0$ de modo que $||| \geq C \cdot |||'$.

9. Ejemplo: Si E es un K-espacio vectorial con una base finita $\{e_1, \ldots, e_n\}$, se define la *norma infinita* como sigue:

$$||\sum_i \lambda_i e_i|| := \text{máx}\{|\lambda_1|, \ldots, |\lambda_n|\}.$$

La norma infinita define en E la topología producto respecto de la identificación $E = K^n$, $\sum_i \lambda_i e_i \mapsto (\lambda_1, \ldots, \lambda_n)$. Toda aplicación K-lineal $E \to E$ es continua para la 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

$$||e||' = ||\sum_i \lambda_i e_i||' \leq \sum_i |\lambda_i| ||e_i||' \leq \sum_i |\lambda_i| C = C \cdot n \cdot ||e||.$$

10. 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.

11. 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 $n = \dim_K E$. Por hipótesis de inducción, todo subespacio de E de dimensión menor que n es completo para la norma $|||'$ luego también es cerrado. Por tanto, 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 $|||'$. □

12. 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,*

$$\left\{ \begin{array}{l} \textit{valores absolutos arquimedianos} \\ \textit{sobre K, módulo equivalencia} \end{array} \right\} = \left\{ \begin{array}{l} \textit{morfismos } K \to \mathbb{C} \\ \textit{mód. conjugación} \end{array} \right\}$$

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.

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 3.4.7), 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 3.4.11, 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 $\hat{K} = \mathbb{C}$ (este último isomorfismo está unívocamente determinado salvo conjugación). En el segundo caso, el valor absoluto $||$ sobre $\hat{K} = \mathbb{C}$ es equivalente al usual porque es una norma sobre el cuerpo $(\mathbb{R}, ||)$, y tales normas son todas equivalentes a la norma infinita, la cual define la topología producto usual en $\mathbb{R}^2 = \mathbb{C}$. □

Observemos que

$$\mathrm{Hom}_{anillos}(K, \mathbb{C}) = \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) = \mathrm{Hom}_{\mathbb{R}-alg}(K \otimes_{\mathbb{Q}} \mathbb{R}, \mathbb{C})$$

Como $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ y $\mathrm{Hom}_{\mathbb{R}-alg}(\mathbb{R}^r \times \mathbb{C}^s, \mathbb{C})/\mathrm{conj} = \mathrm{Spec}(\mathbb{R}^r \times \mathbb{C}^s)$, $[\phi] \mapsto \mathrm{Ker}\,\phi$, tenemos que

$$\mathrm{Hom}_{anillos}(K, \mathbb{C})/\mathrm{conj} = \mathrm{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$$

Explícitamente, dado $x \in \mathrm{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$ tenemos la composición de morfismos

$$K \to K \otimes_{\mathbb{Q}} \mathbb{R} \to (K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{m}_x \hookrightarrow \mathbb{C}.$$

En conclusión,

$$\left\{ \begin{array}{l} \text{valores absolutos arquimedianos} \\ \text{sobre } K\text{, módulo equivalencia} \end{array} \right\} = \left\{ \begin{array}{c} \text{morfismos } K \to \mathbb{C} \\ \text{mód. conjugación} \end{array} \right\} = \mathrm{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$$

3.4.2. Valores absolutos no arquimedianos

13. Definición : Se dice que un valor absoluto $|| : A \to \mathbb{R}$ es ultramétrico si cumple que $|a + b| \leq \mathrm{máx}\{|a|, |b|\}$, para todo $a, b \in A$.

14. Proposición : *Un valor absoluto* $|| : A \to \mathbb{R}$ *es no arquimediano si y sólo si es ultramétrico.*

Demostración. $\Rightarrow$) Para todo natural n se cumple $|n| \leq 1$, pues si para algún natural fuera $|n| > 1$ entonces $|n^m| = |n|^m$ no sería acotado. Dados $a, b \in A$ con $|a| \leq |b|$, se tiene

$$|a + b|^n = |(a + b)^n| \leq |a|^n + |n||a|^{n-1}|b| + \cdots + |n||a||b|^{n-1} + |b|^n \leq (1 + n)|b|^n,$$

de donde

$$|a + b| \leq (1 + n)^{1/n}|b|,$$

y tomando límite para $n \to \infty$ se concluye que

$$|a + b| \leq 1 \cdot |b| = \mathrm{máx}\{|a|, |b|\}.$$

$\Leftarrow$) De la desigualdad ultramétrica, resulta por inducción que $|n| \leq 1$ para todo $n \in \mathbb{N}$. □

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

16. Proposición: *Dada una valoración $v : K\backslash\{0\} \to \mathbb{R}$, la aplicación $|\,|_v : K \to \mathbb{R}$, $|a|_v := e^{-v(f)}$ 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. Por tanto,*

$$\{\textit{Valores absolutos no arquimedianos de } K\}/\sim = \{\textit{Valoraciones reales de } K\}/\sim$$

17. Corolario: *Sea K un un cuerpo de números y A el anillo de enteros de K. Entonces,*

$$\left\{\begin{array}{l}\textit{Val. abs. de } K,\\ \textit{módulo equiv.}\end{array}\right\} = \left\{\begin{array}{l}\textit{Val. abs. no arquimedianos}\\ \textit{de } K\textit{, módulo equivalencia}\end{array}\right\} \coprod \left\{\begin{array}{l}\textit{Val. abs. arquimedianos}\\ \textit{de } K\textit{, módulo equivalencia}\end{array}\right\}$$
$$= \left\{\begin{array}{l}\textit{Valoraciones reales de } K,\\ \textit{módulo equivalencia}\end{array}\right\} \coprod \operatorname{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$$
$$\overset{3.3.6}{=} \operatorname{Spec} A \coprod \operatorname{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$$

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 $a \in K\backslash\{0\}$.

18. Ejercicio: Sea $|\,|_\infty$ el valor absoluto usual de $\mathbb{Q}$. Explicitar la igualdad

$$\left\{\begin{array}{l}\text{valores absolutos sobre } \mathbb{Q},\\ \text{módulo equivalencia}\end{array}\right\} = \operatorname{Spec}\mathbb{Z} \coprod \{|\,|_\infty\}$$

19. Corolario: *Sea K una $k(x)$-extensión finita de cuerpos y C la variedad de Riemann de K. Como los valores absolutos de K triviales sobre k son no arquimedianos, tenemos*

$$\left\{\begin{array}{l}\textit{Valores absolutos de } K,\\ \textit{triviales sobre } k\textit{, mód. equiv.}\end{array}\right\} = \left\{\begin{array}{l}\textit{Valoraciones reales de } K,\\ \textit{triviales sobre } k\textit{, mód equiv.}\end{array}\right\} \overset{3.3.4}{=} C$$

3.5. Producto de valores absolutos de una función

Sea C una variedad de Riemann de cuerpo de funciones K. Dado $x \in C$, sea $|\,|_x$ el valor absoluto asociado a x definido por $|f|_x = e^{-v_x(f)}$, para cada $f \in K$. Entonces, se cumple que

$$\boxed{\prod_{x \in C} |f|_x^{\operatorname{gr}_k x} = e^{-\sum_{x \in C} \operatorname{gr}_k x \cdot v_x(f)} \overset{3.3.17}{=} e^0 = 1}$$

Vamos a probar que en Teoría de Números tenemos la misma fórmula.

1. Definición: Dado un anillo A y un ideal maximal $\mathfrak{m}_x \subset A$, tal que $A/\mathfrak{m}_x$ sea un cuerpo finito, notaremos $\operatorname{gr} x := \ln|A/\mathfrak{m}_x|$.

Sea K un cuerpo de números y A el anillo de enteros de K. Denotemos $X = \operatorname{Spec} A$ el conjunto de valores absolutos no arquimedianos de K (módulo equivalencia), $X_\infty :=$

$\mathrm{Spec}(K\otimes_{\mathbb{Q}}\mathbb{R})$ el conjunto de valores absolutos arquimedianos de K (módulo equivalencia), y $\bar{X}=X\coprod X_\infty$ el conjunto de valores absolutos de K (módulo equivalencia).

Dado $x\in X=\mathrm{Spec}\,A$, sea $|\,|_x$ el valor absoluto no arquimediano asociado a x definido por $|a|_x:=e^{-v_x(a)}$. Observemos que $|a|_x^{-\mathrm{gr}\,x}=|A/\mathfrak{m}_x|^{v_x(a)}$.

En el caso de $K=\mathbb{Q}$, la fórmula anterior es de comprobación inmediata:

2. Proposición: *Digamos que* $\mathrm{gr}\,\infty=1$. *Entonces, dada* $0\neq f\in\mathbb{Q}$

$$\prod_{x\in\mathrm{Spec}\,\mathbb{Z}\coprod\{\infty\}}|f|_x^{\mathrm{gr}\,x}=1$$

3. Definición: Sea B una k-álgebra finita separable. Dada $b\in B$ consideremos el k-endomorfismo lineal $b\cdot\colon B\to B$, $b'\mapsto bb'$. Se define la norma de b, que denotamos $N(b)$, como $N(b):=\det(b\cdot)$.

Obviamente, $N(1)=1$ y $N(bb')=N(b)\cdot N(b')$. Sea Σ una k-extensión que trivialice a B y $\{\sigma_1,\dots,\sigma_n\}=\mathrm{Hom}_{k-alg}(B,\Sigma)$. Entonces, argumentando como hacíamos con la traza,

$$\boxed{N(b)=\textstyle\prod_i\sigma_i(b)}$$

Si K es un cuerpo de números, entonces es una $\mathbb{Q}$-álgebra finita separable y tenemos la norma $N\colon K\to\mathbb{Q}$.

4. Proposición: *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. Existen sendas bases de los $\mathbb{Z}$-módulos A y A en las que el endomorfismo $a\cdot\colon A\to A$ diagonaliza. El determinante de la matriz de $a\cdot$ en estas bases es igual salvo signos a $|A/aA|$, y es igual, salvo signos al determinante del endomorfismo $a\cdot$, con lo que concluimos. □

Sea $|\,|$ el valor absoluto usual de $\mathbb{C}$. Dado $y\in X_\infty$, sea $|\,|_y$ el valor absoluto arquimediano de K asociado a y definido por $|f|_y=|f(y)|$, donde $f(y)$ es igual a la clase de f en $(K\otimes_{\mathbb{Q}}\mathbb{R})/\mathfrak{p}_y$. Dicho de otro modo, si y se corresponde con $\sigma\colon K\to\mathbb{C}$, entonces $f(y)=\sigma(f)$ y $|f|_y=|\sigma(f)|$. Dado $y\in X_\infty$, denotemos $\mathrm{gr}\,y:=\dim_{\mathbb{R}}(K\otimes_{\mathbb{Q}}\mathbb{R})/\mathfrak{m}_y$.

5. Teorema: *Sea K un cuerpo de números. Para toda $f\in K$, se cumple que*

$$\boxed{\textstyle\prod_{x\in\bar{X}}|f|_x^{\mathrm{gr}\,x}=1}$$

Demostración. Sea A el anillo de enteros de K. Tenemos que $f=a_1/a_2$, con $a_1,a_2\in A$. Basta probar el teorema para $f=a\in A$. Como $(a)=\prod_{x\in X}\mathfrak{m}_x^{v_x(a)}$,

$$|N(a)|=|A/aA|=|A/\prod_{x\in X}\mathfrak{m}_x^{v_x(a)}|=\prod_{x\in X}|A/\mathfrak{m}_x|^{v_x(a)}=\prod_{x\in X}|a|_x^{-\mathrm{gr}\,x}.$$

Por otra parte, $|N(a)|=\prod_{\sigma\in\mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})}|\sigma(a)|=\prod_{y\in X_\infty}|a|_y^{\mathrm{gr}\,y}$.

Luego, $\prod_{x\in\bar{X}}|a|_x^{\mathrm{gr}\,x}=1$.

□

6. Ejercicio: Comprobar la fórmula del teorema 3.5.5, para $K=\mathbb{Q}[i]$ y $f=i+1$.

Denotemos los invertibles de A, A^*.

7. Proposición: $A^* = \{a \in A : N(a) = \pm 1\}$.

Demostración. Sea $a \in A$. $|N(a)| = |A/(a)| = 1$ si y sólo si $a \in A^*$. □

8. Observación: Dado $a \in A$ sea $p_c(x) = \sum_{i=0}^{n} a_i x^{n-i}$ el polinomio característico de la homotecia $a\cdot : A \to A$. 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 $c \in A$.

9. Proposición: *Sea $c \in \mathbb{N}$ y $d = \dim_{\mathbb{Q}} K$. Consideremos la acción natural por multiplicación de A^* en $\{f \in A : |N(f)| = c\}$, entonces*

$$|\{f \in A : |N(f)| = c\}/A^*| \leq c^d$$

"El número de $f \in A$, salvo multiplicación por invertibles, tales que $|N(f)| = c$ es menor o igual que c^d."

Demostración. Si $|N(f)| = |A/fA| = c$, entonces $c \cdot (A/fA) = 0$, es decir, $c \in fA$. Supongamos $|N(f)| = |N(f')| = c$. Si $\overline{f'} = d\bar{f}$ en A/cA, con $d \in A^*$, entonces $f' = df + ce$, para cierto $e \in A$, luego $f' \in (f)$ e igualmente $f \in (f')$, es decir, $f' \in f \cdot A^*$. Por tanto, tenemos que

$$\{f \in A : |N(f)| = c\}/A^* \subseteq (A/cA)/A^*, \bar{f} \mapsto \overline{\bar{f}}$$

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 $|A/cA| = c^d$.

□

3.6. 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 $R = \bigoplus_{n\in\mathbb{Z}} R_n$ un álgebra graduada. Diremos que un ideal $I \subset R$ de un álgebra graduada es homogéneo, si está generado por elementos homogéneos.

3. Ejercicio: Probar que un ideal $I \subseteq R$ es homogéneo si y sólo si $I = \bigoplus_n I_n$, 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 sólo si $f_i \in I$ para todo i.

4. Ejercicio: Probar que un ideal homogéneo $\mathfrak{p} \subseteq R$ es primo si y sólo 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 $(\bigoplus_{n\neq 0} R_n) \subseteq R$.

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*

$$\mathrm{Proj}(R/I) = (I)_0^h$$

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*

$$\mathrm{Proj}R_f = U_f^h$$

12. Proposición: *Sea R un álgebra graduada y $f \in R$ un elemento homogéneo de grado* 1. *Entonces,*

$$U_f^h = \mathrm{Proj}R_f = \mathrm{Spec}[R_f]_0$$

Demostración. Veamos que la composición de los morfismos naturales

$$\mathrm{Proj}R_f \hookrightarrow \mathrm{Spec}R_f \to \mathrm{Spec}[R_f]_0,$$

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 sólo 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 $R = R_0[\xi_0,\dots,\xi_n]$, donde cada ξ_i es de grado 1. Con esta hipótesis, $[R_0[\xi_0,\dots,\xi_n]_{\xi_i}]_0 = R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$, donde entendemos por $R_0[\xi_0/\xi_i,\dots,\xi_n/\xi_i]$ la R_0-subálgebra de $R_0[\xi_0,\dots,\xi_n]_{\xi_i}$ generada por $\xi_0/\xi_i,\dots,\xi_n/\xi_i$.

13. Teorema: *Sea* $R = R_0[\xi_0,\dots,\xi_n]$. *Sean* $U_i := \operatorname{Proj} R \setminus (\xi_i)_0^h$. *Entonces,*

1. $\operatorname{Proj} R = \bigcup_{i=0}^{n} U_i$.
2. U_i *es homeomorfo a* $\operatorname{Spec} R_0[\frac{\xi_0}{\xi_i},\dots,\frac{\xi_n}{\xi_i}]$.

Diremos que U_i *es un abierto afín de* $\operatorname{Proj} R$. *Por tanto, el espectro proyectivo admite un recubrimiento por abiertos afines.*

Demostración. 1. $\operatorname{Proj} R = \bigcup_{i=0}^{n} U_i$, 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 3.6.12.

□

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. Demostrar 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 $\operatorname{Proj}\mathbb{C}[x_0,x_1,x_2]/(x_0^2+x_1^2+x_2^2) \hookrightarrow \mathbb{P}^2$

2. Escribir las ecuaciones de la curva proyectiva plana

$$\operatorname{Proj}\mathbb{C}[x_0,x_1,x_2]/(x_0^2+x_1^2+x_2^2)$$

en cada uno de los abiertos "afines", complementario del cerrado $(x_i)_0^h$ ("deshomogeneizar $x_0^2+x_1^2+x_2^2$ por cada variable x_i").

3. Definir 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"?

3.7. Cuestionario

1. Sea $\mathfrak{p}_5 := (5) \subset \mathbb{Z}$. Calcular $v_5(125/40)$.
2. Resolver el ejercicio 3.3.9.
3. Resolver el ejercicio 3.3.10.
4. Resolver el ejercicio 3.3.11.
5. Resolver el ejercicio 3.3.12.
6. Sea C la variedad de Riemann de K. Dado $f \in k$ y $v \in C$ ¿Es $v(f) = 0$?
7. 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, $f \in k$?
8. Sea C la variedad de Riemann de un cuerpo K de tipo finito de grado de trascendencia 1. Si $f \in K$ es algebraico sobre k, probar que $v(f) = 0$, para toda $v \in C$. Si $f \in K$ es trascendente sobre k, probar que existen $v, v' \in C$ tales que $v(f) > 0$ y $v'(f) < 0$.
9. ¿Es una variedad de Riemann recubrible por dos abiertos que sean curvas algebraicas afines no singulares? ¿Y por uno sólo?
10. Sea Σ el cuerpo de fracciones de $\mathbb{C}[x,y]/(y^2 - x)$ y C la variedad de Riemann de Σ. Calcular los ceros y polos de $f = \frac{y+1}{x}$ ¿Se cumple que $\sum_{v \in C} v(f) = 0$?
11. Sea $|\,|: \mathbb{N} \to \mathbb{R}$ un valor absoluto y supongamos que $|2| = 3$. Probar que $|\,|$ es arquimediano y calcular $|7|$.
12. Calcular los valores absolutos arquimedianos de $\mathbb{Q}(e^{2\pi i/5})$ y $\mathbb{Q}(\sqrt[3]{2})$.
13. Resolver el ejercicio 3.5.6.

3.8. Biografía de Riemann

RIEMANN BIOGRAPHY

Bernhard Riemann's father, Friedrich Bernhard Riemann, was a Lutheran minister. Friedrich Riemann married Charlotte Ebell when he was in his middle age. Bernhard was the second of their six children, two boys and four girls. Friedrich Riemann acted as teacher to his children and he taught Bernhard until he was ten years old. At this time a teacher from a local school named Schulz assisted in Bernhard's education.
In 1840 Bernhard entered directly into the third class at the Lyceum in Hannover. While at the Lyceum he lived with his grandmother but, in 1842, his grandmother died and Bernhard moved to the Johanneum Gymnasium in Lüneburg.

Bernhard seems to have been a good, but not outstanding, pupil who worked hard at the classical subjects such as Hebrew and theology. He showed a particular interest in mathematics and the director of the Gymnasium allowed Bernhard to study mathematics texts from his own library. On one occasion he lent Bernhard Legendre's book on the theory of numbers and Bernhard read the 900 page book in six days.

In the spring of 1846 Riemann enrolled at the University of Göttingen. His father had encouraged him to study theology and so he entered the theology faculty. However he attended some mathematics lectures and asked his father if he could transfer to the faculty of philosophy so that he could study mathematics. Riemann was always very close to his family and he would never have changed courses without his father's permission. This was granted, however, and Riemann then took courses in mathematics from Moritz Stern and Gauss.

It may be thought that Riemann was in just the right place to study mathematics at Göttingen, but at this time the University of Göttingen was a rather poor place for mathematics. Gauss did lecture to Riemann but he was only giving elementary courses and there is no evidence that at this time he recognised Riemann's genius. Stern, however, certainly did realise that he had a remarkable student and later described Riemann at this time saying that he: *"... already sang like a canary."*

Riemann moved from Göttingen to Berlin University in the spring of 1847 to study under Steiner, Jacobi, Dirichlet and Eisenstein. This was an important time for Riemann. He learnt much from Eisenstein and discussed using complex variables in elliptic function theory. The main person to influence Riemann at this time, however, was Dirichlet. Klein writes:

Riemann was bound to Dirichlet by the strong inner sympathy of a like mode of thought. Dirichlet loved to make things clear to himself in an intuitive substrate; along with this he would give acute, logical analyses of foundational questions and would avoid long computations as much as possible. His manner suited Riemann, who adopted it and worked according to Dirichlet's methods.

Riemann's work always was based on intuitive reasoning which fell a little below the rigour required to make the conclusions watertight. However, the brilliant ideas which his works contain are so much clearer because his work is not overly filled with lengthy computations. It was during his time at the University of Berlin that Riemann worked out his general theory of complex variables that formed the basis of some of his most important work.

In 1849 he returned to Göttingen and his Ph.D. thesis, supervised by Gauss, was submitted in 1851. However it was not only Gauss who strongly influenced Riemann at this time. Weber had returned to a chair of physics at Göttingen from Leipzig during the time that Riemann was in Berlin, and Riemann was his assistant for 18 months. Also Listing had been appointed as a professor of physics in Göttingen in 1849. Through Weber and Listing, Riemann gained a strong background in theoretical physics and, from Listing, important ideas in topology which were to influence his ground breaking research.

Riemann's thesis studied the theory of complex variables and, in particular, what we now call Riemann surfaces. It therefore introduced topological methods into complex function theory. The work builds on Cauchy's foundations of the theory of complex

variables built up over many years and also on Puiseux's ideas of branch points. However, Riemann's thesis is a strikingly original piece of work which examined geometric properties of analytic functions, conformal mappings and the connectivity of surfaces.

In proving some of the results in his thesis Riemann used a variational principle which he was later to call the Dirichlet Principle since he had learnt it from Dirichlet's lectures in Berlin. The Dirichlet Principle did not originate with Dirichlet, however, as Gauss, Green and Thomson had all made use of it. Riemann's thesis, one of the most remarkable pieces of original work to appear in a doctoral thesis, was examined on 16 December 1851. In his report on the thesis Gauss described Riemann as having:

... a gloriously fertile originality.

On Gauss's recommendation Riemann was appointed to a post in Göttingen and he worked for his Habilitation, the degree which would allow him to become a lecturer. He spent thirty months working on his Habilitation dissertation which was on the representability of functions by trigonometric series. He gave the conditions of a function to have an integral, what we now call the condition of Riemann integrability. In the second part of the dissertation he examined the problem which he described in these words:

While preceding papers have shown that if a function possesses such and such a property, then it can be represented by a Fourier series, we pose the reverse question: if a function can be represented by a trigonometric series, what can one say about its behaviour.

To complete his Habilitation Riemann had to give a lecture. He prepared three lectures, two on electricity and one on geometry. Gauss had to choose one of the three for Riemann to deliver and, against Riemann's expectations, Gauss chose the lecture on geometry. Riemann's lecture Über die Hypothesen welche der Geometrie zu Grunde liegen (On the hypotheses that lie at the foundations of geometry), delivered on 10 June 1854, became a classic of mathematics.

There were two parts to Riemann's lecture. In the first part he posed the problem of how to define an n-dimensional space and ended up giving a definition of what today we call a Riemannian space. Freudenthal wrote:

It possesses shortest lines, now called geodesics, which resemble ordinary straight lines. In fact, at first approximation in a geodesic coordinate system such a metric is flat Euclidean, in the same way that a curved surface up to higher-order terms looks like its tangent plane. Beings living on the surface may discover the curvature of their world and compute it at any point as a consequence of observed deviations from Pythagoras' theorem.

In fact the main point of this part of Riemann's lecture was the definition of the curvature tensor. The second part of Riemann's lecture posed deep questions about the relationship of geometry to the world we live in. He asked what the dimension of real space was and what geometry described real space. The lecture was too far ahead of its time to be appreciated by most scientists of that time. Monastyrsky wrote:

Among Riemann's audience, only Gauss was able to appreciate the depth of Riemann's thoughts. ... The lecture exceeded all his expectations and greatly surprised him. Returning to the faculty meeting, he spoke with the greatest praise and rare enthusiasm to Wilhelm Weber about the depth of the thoughts that Riemann had pre-

sented.

It was not fully understood until sixty years later. Freudenthal writes:

The general theory of relativity splendidly justified his work. In the mathematical apparatus developed from Riemann's address, Einstein found the frame to fit his physical ideas, his cosmology, and cosmogony: and the spirit of Riemann's address was just what physics needed: the metric structure determined by data.

So this brilliant work entitled Riemann to begin to lecture. However,

Not long before, in September, he read a report "On the Laws of the Distribution of Static Electricit" at a session of the Göttingen Society of Scientific researchers and Physicians. In a letter to his father, Riemann recalled, among other things, "the fact that I spoke at a scientific meeting was useful for my lectures". In October he set to work on his lectures on partial differential equations. Riemann's letters to his dearly-loved father were full of recollections about the difficulties he encountered. Although only eight students attended the lectures, Riemann was completely happy. Gradually he overcame his natural shyness and established a rapport with his audience.

Gauss's chair at Göttingen was filled by Dirichlet in 1855. At this time there was an attempt to get Riemann a personal chair but this failed. Two years later, however, he was appointed as professor and in the same year, 1857, another of his masterpieces was published. The paper Theory of abelian functions was the result of work carried out over several years and contained in a lecture course he gave to three people in 1855-56. One of the three was Dedekind who was able to make the beauty of Riemann's lectures available by publishing the material after Riemann's early death.

The abelian functions paper continued where his doctoral dissertation had left off and developed further the idea of Riemann surfaces and their topological properties. He examined multi-valued functions as single valued over a special Riemann surface and solved general inversion problems which had been solved for elliptic integrals by Abel and Jacobi. However Riemann was not the only mathematician working on such ideas. Klein writes:

... when Weierstrass submitted a first treatment of general abelian functions to the Berlin Academy in 1857, Riemann's paper on the same theme appeared in Crelle's Journal, Volume 54. It contained so many unexpected, new concepts that Weierstrass withdrew his paper and in fact published no more.

The Dirichlet Principle which Riemann had used in his doctoral thesis was used by him again for the results of this 1857 paper. Weierstrass, however, showed that there was a problem with the Dirichlet Principle. Klein writes:

The majority of mathematicians turned away from Riemann ... Riemann had quite a different opinion. He fully recognised the justice and correctness of Weierstrass's critique, but he said, as Weierstrass once told me, that he appealed to Dirichlet's Principle only as a convenient tool that was right at hand, and that his existence theorems are still correct.

We return at the end of this article to indicate how the problem of the use of Dirichlet's Principle in Riemann's work was sorted out.

In 1858 Betti, Casorati and Brioschi visited Göttingen and Riemann discussed with them his ideas in topology. This gave Riemann particular pleasure and perhaps Betti in particular profited from his contacts with Riemann. These contacts were renewed

when Riemann visited Betti in Italy in 1863.

In 1859 Dirichlet died and Riemann was appointed to the chair of mathematics at Göttingen on 30 July. A few days later he was elected to the Berlin Academy of Sciences. He had been proposed by three of the Berlin mathematicians, Kummer, Borchardt and Weierstrass. Their proposal read:

Prior to the appearance of his most recent work [Theory of abelian functions], Riemann was almost unknown to mathematicians. This circumstance excuses somewhat the necessity of a more detailed examination of his works as a basis of our presentation. We considered it our duty to turn the attention of the Academy to our colleague whom we recommend not as a young talent which gives great hope, but rather as a fully mature and independent investigator in our area of science, whose progress he in significant measure has promoted.

A newly elected member of the Berlin Academy of Sciences had to report on their most recent research and Riemann sent a report on "On the number of primes less than a given magnitude" another of his great masterpieces which were to change the direction of mathematical research in a most significant way. In it Riemann examined the zeta function

$$\zeta(s) = \sum_n (1/n^s) = \prod_p (1 - p^{-s})^{-1}$$

which had already been considered by Euler. Here the sum is over all natural numbers n while the product is over all prime numbers. Riemann considered a very different question to the one Euler had considered, for he looked at the zeta function as a complex function rather than a real one. Except for a few trivial exceptions, the roots of $\zeta(s)$ all lie between 0 and 1. In the paper he stated that the zeta function had infinitely many nontrivial roots and that it seemed probable that they all have real part 1/2. This is the famous Riemann hypothesis which remains today one of the most important of the unsolved problems of mathematics.

Riemann studied the convergence of the series representation of the zeta function and found a functional equation for the zeta function. The main purpose of the paper was to give estimates for the number of primes less than a given number. Many of the results which Riemann obtained were later proved by Hadamard and de la Vallée Poussin.

In June 1862 Riemann married Elise Koch who was a friend of his sister. They had one daughter. In the autumn of the year of his marriage Riemann caught a heavy cold which turned to tuberculosis. He had never had good health all his life and in fact his serious health problems probably go back much further than this cold he caught. In fact his mother had died when Riemann was 20 while his brother and three sisters all died young. Riemann tried to fight the illness by going to the warmer climate of Italy.

The winter of 1862-63 was spent in Sicily and he then travelled through Italy, spending time with Betti and other Italian mathematicians who had visited Göttingen. He returned to Göttingen in June 1863 but his health soon deteriorated and once again he returned to Italy. Having spent from August 1864 to October 1865 in northern Italy, Riemann returned to Göttingen for the winter of 1865-66, then returned to Selasca on the shores of Lake Maggiore on 16 June 1866. Dedekind wrote:

His strength declined rapidly, and he himself felt that his end was near. But still, the day before his death, resting under a fig tree, his soul filled with joy at the glorious landscape, he worked on his final work which unfortunately, was left unfinished.

Finally let us return to Weierstrass's criticism of Riemann's use of the Dirichlet's Principle. Weierstrass had shown that a minimising function was not guaranteed by the Dirichlet Principle. This had the effect of making people doubt Riemann's methods. Freudenthal writes:

All used Riemann's material but his method was entirely neglected. ... During the rest of the century Riemann's results exerted a tremendous influence: his way of thinking but little.

Weierstrass firmly believed Riemann's results, despite his own discovery of the problem with the Dirichlet Principle. He asked his student Hermann Schwarz to try to find other proofs of Riemann's existence theorems which did not use the Dirichlet Principle. He managed to do this during 1869-70. Klein, however, was fascinated by Riemann's geometric approach and he wrote a book in 1892 giving his version of Riemann's work yet written very much in the spirit of Riemann. Freudenthal writes:

It is a beautiful book, and it would be interesting to know how it was received. Probably many took offence at its lack of rigour: Klein was too much in Riemann's image to be convincing to people who would not believe the latter.

In 1901 Hilbert mended Riemann's approach by giving the correct form of Dirichlet's Principle needed to make Riemann's proofs rigorous. The search for a rigorous proof had not been a waste of time, however, since many important algebraic ideas were discovered by Clebsch, Gordan, Brill and Max Noether while they tried to prove Riemann's results. Monastyrsky writes:

It is difficult to recall another example in the history of nineteenth-century mathematics when a struggle for a rigorous proof led to such productive results.

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

3.9. 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. Pruébese que el anillo local de $k[x,y]$ en el origen es íntegramente cerrado 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 íntegramente cerrado en su cuerpo de fracciones 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.

3. Consideremos la inclusión $\mathbb{C}[x] \hookrightarrow \mathbb{C}[[x]]$ y pasando a los cuerpos de fracciones la inclusión $\mathbb{C}(x) \hookrightarrow \mathbb{C}((x))$. Probar que $\operatorname{sen} x \in \mathbb{C}((x))\backslash\mathbb{C}(x)$.

   Resolución: $\operatorname{sen} x$ no tiene polos en $\operatorname{Spec}\mathbb{C}[x]$ y no es un polinomio.

4. Consideremos el morfismo $\mathbb{C}[x,y] \to \mathbb{C}[[\theta]]$, $x \mapsto \theta, y \mapsto sen\theta$. Demostrar 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

   $$v(p(x,y)) = v'(p(\theta, \operatorname{sen}\theta)) = l(\mathbb{C}[[\theta]]/(p(\theta, \operatorname{sen}\theta)) = l(\mathbb{C}[[x,y]]/(y - \operatorname{sen} x, p(x,y)))$$

5. Probar 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 $\sigma \in \operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})$ 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, $\operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = \{\sigma_1, \ldots, \sigma_n, c \circ \sigma_1, \ldots, c \circ \sigma_n\}$ con $\#\operatorname{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C}) = 2n$ y

   $$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \cdot c(\sigma_i(\alpha)) > 0$$

6. 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. Calcular 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 la $-x_0^2 + x_1^2 + x_2^2 = 0$, 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 $U^h_{x_1}$, 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 sólo 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).

7. Calcular 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, $\mathrm{Proj}\,\mathbb{R}[x_0,x_1,x_2]/(x_2^2 - x_0^2 + x_1x_0)$ 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 $y = zx = x_2x_1/x_0^2$).

8. Calcular 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 $\mathrm{Spec}\,\mathbb{Z}[i]$. 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 $a'-b'c\neq 0 \mod p$.

9. Sea K un cuerpo de números de anillo de enteros A. Sea $\bar{X}$ el conjunto de valores absolutos de K, módulo equivalencia. $\bar{X} = \mathrm{Spec}\, A \coprod X_\infty$. Dado $y \in X_\infty$ definamos $v_y(f) = -\ln |f|_y$, para cada $f \in K$. Probar que

$$\sum_{x\in\bar{X}} \mathrm{gr}\, x \cdot v_x(f) = 0$$

Resolución: Sabemos que $\prod_{x\in\bar{X}} |f|_x^{\mathrm{gr}\, x} = 1$. Tomando ln en esta ecuación concluimos.

Capítulo 4

Teoremas fundamentales de la Teoría de Números

4.1. Introducción

Para el estudio y clasificación de los anillos de números enteros, 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 enteros 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 sólo 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 enteros 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 sólo módulo p admite soluciones enteras, para infinitos primos p.

1. Notación: Sea K una $\mathbb{Q}$-extensión finita de cuerpos de grado d, A el anillo de enteros de K y sean

$$\{\sigma_1,\ldots,\sigma_r,\sigma_{r+1},\ldots\sigma_{r+s},\sigma_{r+s+1}=\bar{\sigma}_{r+1},\ldots,\sigma_{r+2s}=\bar{\sigma}_{r+s}\}=\mathrm{Hom}_{\mathbb{Q}-alg}(K,\mathbb{C})$$

(donde $\sigma_i(K) \subset \mathbb{R}$ si y sólo si $i \leq r$ y $\bar{\sigma}_{r+i}$ es igual a la composición de σ_{r+i} con el morfismo de conjugación).

4.2. Divisores afines

Sea K una $\mathbb{Q}$-extensión finita de cuerpos de grado d y A el anillo de enteros de K.

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. 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 $D = \sum_x n_x x$, diremos que $\mathrm{gr}(D) = \sum_x n_x \cdot \mathrm{gr}\, x$ es el grado de D. Dado un divisor $D = \sum_{x \in \mathrm{Spec}\, A} n_x \cdot x$, diremos que el conjunto $\mathrm{Sop}(D) = \{x \in \mathrm{Spec}\, A, n_x \neq 0\}$ es el soporte de D.

2. 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 $D = D' + D(f)$. El conjunto de los divisores afines principales de $\mathrm{Div}\, A$, es un subgrupo y el cociente de $\mathrm{Div}\, A$ por el subgrupo de los divisores afines principales se denota $\mathrm{Pic}\, A = \mathrm{Div}\, A / \sim$ y se llama grupo de clases de ideales de A o grupo de Picard de A.

3. Ejercicio: Probar que $\mathrm{Pic}\, \mathbb{Z} = \{0\}$.

4. Ejercicio: Probar que $\mathrm{Pic}\, A = \{0\}$ si y sólo si A es un dominio de ideales principales.

Si dos ideales no nulos $\mathfrak{a}, \mathfrak{a}' \subset A$ son isomorfos, localizando en el punto genérico obtenemos un isomorfismo de K-módulos de K, que es multiplicar por una $f \in K$, luego $\mathfrak{a}' = f \cdot \mathfrak{a}$.

5. Proposición: *Se cumplen las igualdades*

$$\begin{array}{ccc} \textit{Conj. de ideales no nulos de } A & = & \textit{Conj. de divisores afines efectivos} \\ \mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r} & \mapsto & D(\mathfrak{a}) := \sum_i n_i x_i \end{array}$$

$$\textit{Conjunto de ideales no nulos de } A\textit{, módulo isomorfismos} = \mathrm{Pic}\, A,\ [\mathfrak{a}] \mapsto [D(\mathfrak{a})]$$

Demostración. Veamos la segunda igualdad. La asignación es epiyectiva: Dado un divisor afín D, sea $f \in A$, tal que $D + Df = \sum_{i=1}^r n_i x_i$ sea un divisor afín efectivo. Sea $\mathfrak{a} = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$. Entonces, $D(\mathfrak{a}) = D + Df$.

La asignación es inyectiva: Si $D(\mathfrak{a}) = D(\mathfrak{a}') + Df$, entonces $\mathfrak{a} = f \cdot \mathfrak{a}'$ y $\mathfrak{a}$ es isomorfo a $\mathfrak{a}'$. □

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

Los ideales fraccionarios son A-módulos localmente principales, porque son A-módulos finito generados de rango 1 sin torsión.

En el conjunto de ideales fraccionarios tenemos la operación multiplicación de ideales.

7. Definición: Sea $x \in \operatorname{Spec} A$ un punto cerrado y $n \in \mathbb{Z}$. Denotamos

$$\mathfrak{m}_x^n := \{h \in K : D(h) \geq nx\}.$$

Si $n > 0$, entonces $\mathfrak{m}_x^n \subseteq A$ es el ideal ya conocido.

Supongamos $n < 0$. Dado un punto cerrado $x \in \operatorname{Spec} A$, sea $t_x \in K$ tal que $v_x(t_x) = 1$. Sean $y_1, \ldots, y_r$ los puntos de $\operatorname{Spec} A$, distintos de x, donde $n_i := v_{y_i}(t_x) < 0$. Existe $g \in A$ tal que $v_x(g) = 0$ y tal que $v_{y_i}(g) \geq n \cdot n_i$, para todo i. Sea $J = A + \cdot g t_x^n A$. Observemos que $J_y = A_y$, para $y \neq x$ y que $J_x = t_x^n A_x$. Observemos que $J = \mathfrak{m}_x^n$, porque $J \subseteq \mathfrak{m}_x^n$ y $\mathfrak{m}_x^n \subseteq J$ localmente. Por tanto, $\mathfrak{m}_x^n$ es un ideal fraccionario. Además, $(\mathfrak{m}_x^n)_y = A_y$, para todo $y \neq x$ y $(\mathfrak{m}_x^n)_x = t_x^n A_x$.

8. Proposición: *Sea I un ideal fraccionarios de K. Existen ciertos $x_1, \ldots, x_m \in \operatorname{Spec} A$ distintos (y únicos) y ciertos $n_1, \ldots, n_m \in \mathbb{Z}$ (únicos), de modo que*

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

Demostración. Sea $I = f_1 A + \cdots + f_n A$ un ideal fraccionario de K. Dado $x \in \operatorname{Spec} A$, sea $t_x \in K$ tal que $v_x(t_x) = 1$. Entonces, $I_x = f_1 A_x + \cdots + f_n A_x = t_x^{v_x(f_1)} A_x + \cdots + t_x^{v_x(f_n)} A_x$. Luego, si $n_x := \text{ínf}\{v_x(f) : f \in I\} = \text{ínf}\{v_x(f_1), \ldots, v_x(f_n)\}$, entonces $I_x = t_x^{n_x} \cdot A_x$. Observemos que $n_x = 0$ para todo x salvo un número finito. En conclusión,

$$I = \prod_{x \in \operatorname{Spec} A} \mathfrak{m}_x^{n_x}$$

porque ambos son ideales fraccionarios de K, que coinciden localmente.

□

Observemos que $\prod_{x \in \operatorname{Spec}_{max} A} \mathfrak{m}_x^{n_x} \cdot \prod_{x \in \operatorname{Spec}_{max} A} \mathfrak{m}_x^{n'_x} = \prod_{x \in \operatorname{Spec}_{max} A} \mathfrak{m}_x^{n_x + n'_x}$.

Si dos ideales fraccionarios no nulos $I, I' \subset K$ son isomorfos, localizando en el punto genérico obtenemos un isomorfismo de K-módulos de K, que es multiplicar por una $f \in K$, luego $I' = f \cdot I$.

9. Proposición: *Las asignaciones*

$$\begin{array}{rcl} \operatorname{Div} A & \longrightarrow & \{\textit{Ideales fraccionarios de } K\} \\ D = \sum_i n_i x_i & \longmapsto & I_D := \{f \in K : D(f) \geq D\} = \prod_i \mathfrak{m}_{x_i}^{n_i} \\ D(I) := \sum_x \text{ínf}\{v_x(f) : f \in I\} \cdot x & \longleftarrow & I \end{array}$$

son inversas entre sí. Por tanto,

$$\operatorname{Pic} A = \textit{Conjunto de ideales fraccionarios de } K\textit{, módulo isomorfismos}$$

Demostración. Si $I = \prod_x \mathfrak{m}_x^{n_x}$ entonces $D(I) = \sum_x n_x x$. Dado $D = \sum_x n_x x$ se cumple que

$$I_D = \{f \in K : D(f) \geq \sum_x n_x x\} = \cap_x \mathfrak{m}_x^{n_x} = \prod_x \mathfrak{m}_x^{n_x}.$$

□

10. 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.

11. Proposición: *Dado un ideal fraccionario $I \subseteq K$ se cumple que*

$$N(I) = e^{\mathrm{gr}(D(I))}$$

Es decir, el diagrama

$$\begin{array}{ccc} \mathrm{Div}(A) & = & \{\textit{Ideales fraccionarios}\} \\ \downarrow{\scriptstyle \mathrm{gr}} & & \downarrow{\scriptstyle N} \\ \mathbb{R} & \xrightarrow{e^x} & \mathbb{R}^+ \end{array}$$

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, $e^{\mathrm{gr}(x))} = |A/\mathfrak{m}_x| = N(\mathfrak{m}_x) = N(I_x)$. □

12. Proposición: *Dado un ideal $\mathfrak{a} \subset A$, entonces $N(\mathfrak{a}) = |A/\mathfrak{a}|$. Dados dos ideales fraccionarios $I' \subseteq I$, se cumple que $N(I')/N(I) = |I/I'|$.*

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

$$|A/\mathfrak{a}| = \prod_i |A/\mathfrak{m}_{x_i}^{n_i}| = \prod_i |A/\mathfrak{m}_{x_i}|^{n_i} = N(\mathfrak{a})$$

Existe un ideal $\mathfrak{a} \subseteq A$ tal que $I' = I \cdot \mathfrak{a}$. Además, $I/I' \simeq A/\mathfrak{a}$ porque son A-módulos de torsión y localmente coinciden. Entonces,

$$|I/I'| = |A/\mathfrak{a}| = N(\mathfrak{a}) = N(I')/N(I)$$

□

13. Proposición: *Dado $0 \neq f \in K$, entonces $N(fA) = |N(f)|$.*

Demostración. Dado $a \in A$, $|N(a)| \overset{3.5.4}{=} |A/aA| = N(aA)$. Escribamos $f = a/b$, $a, b \in A$. Entonces, $(f) \cdot (b) = (a)$ y

$$N((f)) = N((a))/N((b)) = |N(a)/N(b)| = |N(f)|$$

□

14. Proposición: *Sea $c \in \mathbb{Z}$. Salvo multiplicación por invertibles existe un número finito de $a \in A$ tal que $N(a) = c$.*

Demostración. $|N(a)| = |A/aA| = |c|$ si y sólo si $\mathrm{gr}\, D(a) = \ln|c|$. Ahora bien, divisores afines efectivos de grado dado sólo existen un número finito. Por tanto, existen $a_1, \ldots, a_m$ de modo que: $\mathrm{gr}\, D(a_i) = \ln|c|$ y si $\mathrm{gr}\, D(a) = \ln|c|$, entonces $Da = Da_i$. Luego a es igual salvo multiplicación por invertibles a alguno de los a_i.

□

15. Ejercicio: Consideremos la aplicación

$$\{\text{Ideales fraccionarios de } K\} \to \{\text{Ideales fraccionarios de } \mathbb{Q}\},\ I \mapsto N(I)\cdot\mathbb{Z}$$

Probar que $N(I)\cdot\mathbb{Z} = \langle N(f)\rangle_{f\in I}$.

Solución: Basta ver que localmente como $\mathbb{Z}$-módulos son iguales. Sea $S \subseteq \mathbb{Z}$ un sistema multiplicativo. Podemos definir igualmente $\mathrm{Div}(A_S)$, los ideales A_S-fraccionarios de K y su norma. Observemos que $N(I)\cdot\mathbb{Z}_S = N(I_S)$ y $\langle N(f)\rangle_{f\in I}\cdot\mathbb{Z}_S = \langle N(f)\rangle_{f\in I_S}$. Sea $S = \mathbb{Z}\backslash(p)$, entonces A_S es un dominio de ideales principales y como I_S es principal se concluye por la proposición 4.2.13.

16. Ejercicio: Sea K una $\mathbb{Q}$-extensión de Galois de grupo G. Dado un ideal fraccionario I de K, probar que

$$N(I)\cdot A = \prod_{\sigma\in G} \sigma(I).$$

Solución: Procédase como en el ejercicio anterior.

4.3. Divisores completos

1. Notación: Sea $X = \mathrm{Spec}_{max}\, A$, $X_\infty = \mathrm{Spec}(K\otimes_{\mathbb{Q}}\mathbb{R})$ y $\bar{X} = X \coprod X_\infty$.

2. Definición: Llamaremos grupo de los divisores completos de $\bar{X}$, que denotaremos $\mathrm{Div}(\bar{X})$, al grupo

$$\mathrm{Div}(\bar{X}) = (\oplus_{x\in X}\mathbb{Z}\cdot x)\oplus(\oplus_{y\in X_\infty}\mathbb{R}\cdot y)$$

y diremos que $\bar{D} = \sum_{x\in X} n_x x + \sum_{y\in X_\infty}\lambda_y y$ 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 $\bar{D}_\infty := \sum_{y\in X_\infty}\lambda_y y$ es la parte del infinito de $\bar{D}$.

Dado $\bar{D}' = \sum_{x\in X} n'_x x + \sum_{y\in X_\infty}\lambda'_y y$, diremos que $\bar{D}' \geq \bar{D}$ si $n'_x \geq n_x$ y $\lambda'_y \geq \lambda_y$, para todo x e y.

3. Definición: Dado $y \in X_\infty$ y $f \in K$, denotemos $v_y(f) := -\ln|f|_y$. 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 $\mathrm{Div}(\bar{X})$. 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.

4. 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 $\mathrm{gr}\,\bar{D}$, a

$$\mathrm{gr}(\bar{D}) := \sum_{x\in X} n_x\cdot \mathrm{gr}\, x + \sum_{y\in X_\infty}\lambda_y\cdot \mathrm{gr}\, y$$

Observemos que $\mathrm{gr}\colon \mathrm{Div}(\bar{X}) \to \mathbb{R}$ es un morfismo de grupos.

5. Teorema: *Para toda $f \in K$, se cumple que*

$$\mathrm{gr}(\bar{D}(f)) = 0$$

Demostración. Es consecuencia de la proposición 3.5.5 □

6. Ejercicio: Sea $\bar{X}$ el conjunto de valores absolutos de $\mathbb{Q}$, módulo equivalencia. Probar que $\mathrm{Pic}\,\bar{X} = \mathbb{R}$.

4.4. Volumen de un paralelepípedo. Discriminante

1. Definición: Sea E un $\mathbb{R}$-espacio vectorial de dimensión n. Diremos que un subgrupo aditivo Γ de E es una red si está generado por alguna base $\{e_1,\dots,e_n\}$ del espacio vectorial, es decir, $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ y $E = \Gamma \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}e_1 \oplus \cdots \oplus \mathbb{R}e_n$.

Se dice que E/Γ es el paralelepípedo generado por $e_1,\dots,e_n$.

Sea $T_2\colon E \times E \to \mathbb{R}$ una métrica simétrica sobre un $\mathbb{R}$-espacio vectorial E de dimensión n. T_2 extiende a $\Lambda^n_{\mathbb{R}} E$:

$$\begin{aligned} T_2(e_1 \wedge \cdots \wedge e_n, e'_1 \wedge \cdots \wedge e'_n) &:= (i_{e_1}T_2 \wedge \cdots \wedge i_{e_n}T_2)(e'_1,\cdots,e'_n) \\ &= \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \cdot T_2(e_1, e'_{\sigma(1)}) \cdots T_2(e_n, e'_{\sigma(n)}) \end{aligned}$$

Se cumple que $T_2(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n) = \det((T_2(e_i,e_j)))$. Si $e_1,\dots,e_n$ es una base ortonormal entonces $T_2(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n) = 1$. En general si $e'_1,\dots,e'_n$ es una base ortogonal obtenida por Gram Schmidt a partir de $e_1,\dots,e_n$, tenemos que $e_1 \wedge \cdots \wedge e_n = e'_1 \wedge \cdots \wedge e'_n$ y $T_2(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n) = T_2(e'_1,e'_1)\cdots T_2(e'_n,e'_n)$, que como definiremos más abajo es salvo signo el cuadrado del volumen formado por el paralelepípedo formado por $e_1,\dots,e_n$

Se define el discriminante de $\Gamma = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$, Δ_Γ, por

$$\boxed{\Delta_\Gamma := \det((T_2(e_i,e_j)))}$$

Sean $e'_1,\dots,e'_n \in E$, con $e'_i = \sum_j \lambda_{ij} e_j$, entonces $e'_1 \wedge \cdots \wedge e'_n = \det(\lambda_{ij}) \cdot e_1 \wedge \cdots \wedge e_n$, y

$$\begin{aligned} \det((T_2(e'_i,e'_j))) &= T_2(e'_1 \wedge \cdots \wedge e'_n, e'_1 \wedge \cdots \wedge e'_n) = \det(\lambda_{ij})^2 \cdot T_2(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n) \\ &= \det(\lambda_{ij})^2 \cdot \det((T_2(e_i,e_j))). \end{aligned}$$

Si $e'_1,\dots,e'_n$ es otra base del $\mathbb{Z}$-módulo Γ, entonces $\det(\lambda_{ij}) = \pm 1$. Por tanto, Δ_Γ no depende de la base de Γ escogida.

Se define el volumen del paralelepípedo generado por $e_1,\dots,e_n$, por

$$\boxed{Vol(E/\Gamma) := \sqrt{|\Delta_\Gamma|} = \sqrt{|\det(T_2(e_i,e_j))|}}$$

2. Ejemplo: Sea K un cuerpo de números, de grado d sobre $\mathbb{Q}$. Sea $\Gamma \subset K$ un $\mathbb{Z}$-módulo libre de rango d. Consideremos la inclusión canónica

$$\Gamma \hookrightarrow \Gamma \otimes_{\mathbb{Z}} \mathbb{R} = K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \oplus \mathbb{C}^s =: \mathcal{O}_\infty,\ a \mapsto (\sigma_1(a), \ldots, \sigma_r(a), \sigma_{r+1}(a), \ldots, \sigma_{r+s}(a))$$

Γ es una red de $\mathcal{O}_\infty$. *Todo anillo de enteros, como todo ideal fraccionario son redes de* $\mathcal{O}_\infty$.

En $\mathcal{O}_\infty$ tenemos la métrica de la traza T_2. Sea $\{a_1, \ldots, a_d\}$ una base de $\Gamma \subset K$.

3. Si $\Gamma \cdot \Gamma \subseteq \Gamma$, entonces $T_2(a_i \cdot a_j)$ es igual a la traza del endomorfismo de $\mathbb{Z}$-módulos $(a_i a_j)\cdot : \Gamma \to \Gamma$, luego es un número entero y Δ_Γ es un número entero.

4. En $\mathcal{O}_\infty = \mathbb{R}^d$ tenemos también la métrica euclídea estándar S_2. Se cumple que $\det(T_2) = (-4)^s \cdot \det(S_2)$ y por tanto el volumen de los paralelepípedos con la métrica de la traza es 2^s-veces el volumen de los paralelepípedos con la métrica euclídea estándar.

Luego Δ_Γ es igual a $(-4)^s$ por el determinante de S_2 en la base $\{(\sigma_1(a_j), \ldots, \sigma_{r+s}(a_j)) \in \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d\}_j$, es decir

$$\boxed{\Delta_\Gamma = (-4)^s \det((\sigma_i(a_j)))^2}$$

(donde $(\sigma_i(a_j))$ es una matriz cuadrada de números reales de orden d) y

$$\boxed{Vol(\mathcal{O}_\infty/\Gamma) = \sqrt{|\Delta_\Gamma|} = 2^s |\det((\sigma_i(a_j)))|}$$

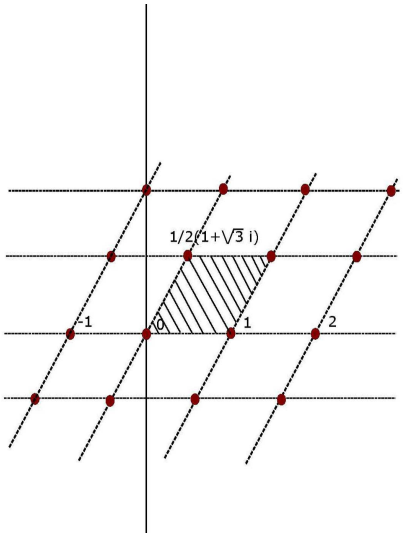
5. $K \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}^d$, $a \otimes 1 \mapsto (\sigma_1(a), \cdots, \sigma_d(a))$. Y la métrica de la traza de $\mathbb{C}^d$ coincide con la métrica estándar. Entonces,

$$\boxed{\Delta_\Gamma = \det((\sigma_i(a_j)))^2}$$

(donde $(\sigma_i(a_j))$ es una matriz cuadrada de números complejos de orden d) y

$$\boxed{Vol(\mathcal{O}_\infty/\Gamma) = \sqrt{|\Delta_\Gamma|} = |\det((\sigma_i(a_j)))|}$$

6. 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

$$\Delta_A = \begin{vmatrix} 1 & 1/2 + 1/2\sqrt{-3} \\ 1 & 1/2 - 1/2\sqrt{-3} \end{vmatrix}^2 = -3$$

7. Ejercicio: Sea A un anillo de enteros y supongamos que $i \notin A$. Demostrar que $\Delta_{A[i]} = (-4)^d \cdot \Delta_A^2$.

Si tenemos dos redes $\Gamma' \subseteq \Gamma$, entonces existen bases en Γ' y Γ donde la matriz de la inclusión es diagonal y es claro que

$$\Delta_{\Gamma'} = |\Gamma/\Gamma'|^2 \cdot \Delta_\Gamma$$
$$Vol(\mathcal{O}_\infty/\Gamma') = |\Gamma/\Gamma'| \cdot Vol(\mathcal{O}_\infty/\Gamma)$$

Recordemos que si $I' \subseteq I$ son ideales fraccionarios, $|I/I'| = N(I')/N(I)$.

8. Proposición: *Si I es un ideal fraccionario, entonces*

$$\boxed{Vol(\mathcal{O}_\infty/I) = N(I) \cdot \sqrt{|\Delta_A|}}$$

Demostración. Sean $\mathfrak{a}$, $\mathfrak{b} \subseteq A$ ideales tales que $I = \mathfrak{a} \cdot \mathfrak{b}^{-1}$ (luego, $I \subseteq \mathfrak{b}^{-1}$ y $A \subseteq \mathfrak{b}^{-1}$). Entonces,

$$Vol(\mathcal{O}_\infty/I) = \frac{N(I)}{N(\mathfrak{b}^{-1})} \cdot Vol(\mathcal{O}_\infty/\mathfrak{b}^{-1}) = \frac{N(I)}{N(\mathfrak{b}^{-1})} \cdot N(\mathfrak{b}^{-1}) \cdot Vol(\mathcal{O}_\infty/A) = N(I) \cdot \sqrt{|\Delta_A|}$$

□

9. Ejemplo: Sea α raíz de un polinomio irreducible $p(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Z}[x]$ y sea $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(p(x))$. Sea $\{\sigma_i\} = \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C})$, entonces las raíces de $p(x)$ son $\{\sigma_i(\alpha)\}_i$.

Una base de $\mathbb{Z}[\alpha]$ es $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Por tanto,

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

Sea A el anillo de enteros de K. Entonces,

$$\Delta(p(x)) = \Delta_{\mathbb{Z}[\alpha]} = |A/\mathbb{Z}[\alpha]|^2 \cdot \Delta_A$$

Por ejemplo, el discriminante de $x^2 - n$ es $4n$. Si n no tiene factores cuadráticos y $\mathbb{Z}[\sqrt{n}]$ no es normal, entonces $|A/\mathbb{Z}[\alpha]| = 2$. Como $\frac{\sqrt{n}+1}{2}$ es entero, $A = \mathbb{Z}[\frac{\sqrt{n}+1}{2}]$ (y $\Delta_A = n$).

10. Ejercicio: Sea $n \in \mathbb{Z}$, con $n \neq 0, 1$ y sin factores cuadráticos. Demostrar que el discriminante de $K = \mathbb{Q}[\sqrt{n}]$ es n si $n \equiv 1 \mod 4$, y es $4n$ si $n \equiv 2, 3 \mod 4$.

11. Ejercicio: Sea $n \in \mathbb{Z}$, con $n \neq 0, 1$ y sin factores cuadráticos. Sea Δ el discriminante de $\mathbb{Q}[\sqrt{n}]$. Probar que el anillo de enteros de $\mathbb{Q}[\sqrt{n}]$ es igual a $\mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$.

4.5. Teorema de Riemann-Roch débil

1. Definición: Sea $\bar{D}$ un divisor completo, definimos $\bar{I}_{\bar{D}} := \{f \in K : \bar{D}(f) \geq \bar{D}\}$.

Si $\bar{D} = n_1x_1 + \cdots + n_mx_m + \lambda_1y_1 + \cdots + \lambda_{r+s}y_{r+s}$, entonces

$$\bar{I}_{\bar{D}} = \left\{ \begin{array}{c} f \in K : v_{x_i}(f) \geq n_i, \forall i \\ v_x(f) \geq 0, \forall x \neq x_i \end{array} \right\} \cap \{f \in K : v_{y_i}(f) \geq \lambda_i, \forall y_i\}$$
$$= \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_m}^{n_m} \bigcap \{(\mu_i) \in \mathbb{R}^r \times \mathbb{C}^s = \mathcal{O}_\infty : |\mu_i| \leq e^{-\lambda_i}, \forall i\}$$

2. Propiedades: *1. Si $D' = \bar{D} + \bar{D}(f)$, entonces $f\cdot : \bar{I}_{\bar{D}} \simeq \bar{I}_{D'}$ es una biyección.*

2. *El conjunto $\bar{I}_{\bar{D}}$ 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 $\{(\mu_j) \in \mathbb{R}^r \times \mathbb{C}^s = \mathcal{O}_\infty : |\mu_j| \leq e^{-\lambda_j}, \forall j\}$, que es finito.*

3. *En el caso $\bar{D} = 0$, denotamos $\bar{I}_{\bar{D}} = \mathcal{O}_{\bar{X}}(\bar{X})$. Entonces, $\mathcal{O}_{\bar{X}}(\bar{X})\backslash\{0\} = \{f \in K^* : \bar{D}(f) = 0\}$ 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. *Si $\mathrm{gr}(\bar{D}) > 0$ entonces $\bar{I}_{\bar{D}} = \{0\}$.*

5. *Si $\mathrm{gr}(\bar{D}) = 0$ y $\bar{I}_{\bar{D}} \neq \{0\}$, entonces existe f tal que $\bar{D} = \bar{D}(f)$: Sea $f \in \bar{I}_{\bar{D}}$ no nula, entonces $-\bar{D} + \bar{D}(f) \geq 0$, luego $-\bar{D} + \bar{D}(f) = 0$ y $\bar{D} = \bar{D}(f)$.*

3. Teorema del punto de la red de Minkowski: *Sea E un espacio vectorial real de dimensión d, con una métrica T_2 no singular. Sea Γ una red de E y C un compacto de E, convexo y simétrico respecto del origen. Si $Vol(C) \geq 2^d Vol(E/\Gamma)$, 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 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 $\frac{y-x}{2} \in C$. □

4. Notación: Sea A el anillo de enteros del cuerpo de números K. Por abuso de notación, escribiremos $\Delta_K := \Delta_A$.

5. Teorema de Riemann-Roch débil: *Sea $\bar{D}$ un divisor completo. Entonces, $\bar{I}_{-\bar{D}} \neq \{0\}$ cuando*

$$\mathrm{gr}\,\bar{D} \geq \ln \sqrt{|\Delta_K|} - s \cdot \ln(\pi/2)$$

Demostración. $-\bar{D} = D(I) + D_\infty$, para cierto ideal fraccionario I y cierto divisor $D_\infty = \sum_i \lambda_i y_i$. Sea $C = \{(\mu_1, \ldots, \mu_{r+s}) \in \mathcal{O}_\infty : |\mu_i| \leq e^{-\lambda_i}, \forall i\}$, entonces $\bar{I}_{-\bar{D}} = I \cap C$.

$$Vol(\mathcal{O}_\infty/I) = N(I) \cdot \sqrt{|\Delta_K|} = e^{\mathrm{gr}(D(I))} \cdot \sqrt{|\Delta_K|}$$
$$Vol(C) = 2^s \cdot (2^r e^{-(\lambda_1 + \cdots + \lambda_r)} \cdot \pi^s e^{-2(\lambda_{r+1} + \cdots + \lambda_{r+s})}) = 2^d (\frac{\pi}{2})^s e^{-\mathrm{gr}(D_\infty)}$$

El teorema del punto de la red de Minkowski asegura que $\bar{I}_{-\bar{D}} \neq \{0\}$ cuando

$$2^d (\frac{\pi}{2})^s e^{-\mathrm{gr}(D_\infty)} = Vol(C) \geq 2^d Vol(\mathcal{O}_\infty/I) = 2^d e^{\mathrm{gr}\,D(I)} \sqrt{|\Delta_K|}$$

es decir, cuando $(\frac{\pi}{2})^s e^{\mathrm{gr}\,\bar{D}} \geq \sqrt{|\Delta_K|}$. Tomando ln concluimos.

□

6. Corolario: *Si $\bar{D}$ es un divisor completo y $\operatorname{gr}\bar{D} \geq \ln \sqrt{|\Delta_K|}$, entonces $\bar{D}$ es linealmente equivalente a un divisor completo efectivo.*

4.6. 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* $\ln \sqrt{|\Delta_K|}$.

Demostración. Sea D_∞ un divisor en el infinito tal que $\operatorname{gr}(D + D_\infty) = \ln \sqrt{|\Delta_K|}$. 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 $\ln \sqrt{|\Delta_K|}$. Por tanto, 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 4.2.11. □

3. Teorema: $\operatorname{Pic} A$ *es un grupo finito.*

Demostración. El número de divisores afines efectivos de grado menor o igual que cierto número es finito. Dado $[D] \in \operatorname{Pic} A$, 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 enteros de K. Probar que si todo ideal primo $\mathfrak{p}_x \subset A$ es principal si $|A/\mathfrak{p}_x| \leq \sqrt{|\Delta_K|}$, entonces A es un dominio de ideales principales.

Es conocido que el anillo de enteros de $\mathbb{Q}[\sqrt{-r}]$, con $r > 0$ y no divisible por ningún primo al cuadrado, es de ideales principales si si sólo si $r = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

5. Corolario: *Sea K un cuerpo de números y A el anillo de enteros 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 $n = |\operatorname{Pic} A|$. Entonces, $[\mathfrak{a}]^n = [A]$, para todo $[\mathfrak{a}] \in \operatorname{Pic} A$, 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 enteros de K. Existe una extensión finita L de K, de modo que todos los ideales de A extendidos al anillo de enteros de L son principales.*

Demostración. Sea $\mathfrak{a} \subset A$ un ideal y $n > 0$ tal que $\mathfrak{a}^n = (c)$ es principal. Si B es el anillo de enteros de $K[\sqrt[n]{c}]$, 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 $\operatorname{Pic} A = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_n]\}$ 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.

□

4.7. 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 sólo si $K = \mathbb{Q}$.*

Demostración. Si $\Delta_K = \pm 1$, por el corolario 4.5.6, 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 sólo 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: *Sólo 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.

Podemos suponer que $i \in K$: si $i \notin K$, entonces $|\Delta_{K[i]}| \leq |\Delta_{A[i]}| = 4^d |\Delta_A|^2 = 4^d |\Delta_K|^2$, y como probaremos, 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 y cada uno de éstos contiene un número finito de subextensiones. En conclusión, el número de cuerpos de discriminante Δ y grado d es finito.

Suponemos, pues, que $i \in K$ (luego $r = 0$). Consideremos en el infinito el divisor

$$(d + \ln \sqrt{|\Delta_K|}) \cdot y_1 - y_2 - \ldots - y_s$$

El teorema de Riemann-Roch débil afirma la existencia de una $f \in A$ tal que $|\sigma_i(f)| \leq e^{-1} < 1$, para todo $i > 1$. Como $N(f)$ es un número entero, se sigue $|\sigma_1(f)| = |f| > 1$. Sea $H = \{\sigma \in \mathrm{Hom}_{\mathbb{Q}-alg}(K, \mathbb{C}) \colon \sigma(f) = f\}$, tendremos que $|\sigma(f)| > 1$, para todo $\sigma \in H$. Por tanto, $H = \{\sigma_1\}$ y $K = \mathbb{Q}[f]$ (o bien, $H = \{\sigma_1, \bar{\sigma}_1\}$, en este caso $K = \mathbb{Q}[if]$ y tomaríamos if en vez de f). Observemos, además, que $|\sigma_1(f)| \leq e^d \cdot \sqrt{|\Delta_K|}$. Por tanto, los coeficientes del polinomio anulador de f están acotados, pues sus raíces $\sigma_i(f)$ lo están, y como son números enteros sólo hay un número finito de tales polinomios.

□

3. Proposición: *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*

$$|N(f)| \leq c|N(I)|, \text{ con } c = d! d^{-d} (4/\pi)^s \cdot \sqrt{|\Delta_K|}$$

Fijado el discriminante del cuerpo de números, el grado está acotado.

Demostración. Consideremos el compacto

$$C = \{(\lambda_1, \ldots, \lambda_r, \ldots, \lambda_{r+s}) \in \mathcal{O}_\infty = \mathbb{R}^r \times \mathbb{C}^s \colon \sum_{i \leq r} |\lambda_i| + \sum_{j > r} 2|\lambda_j| \leq t\}$$

que tiene volumen $2^r\pi^s t^d/d!$. Sea t, de modo que $Vol(C) = 2^d Vol(\mathcal{O}_\infty/I)$. Entonces, por el teorema del punto de la red de Minkowski existe $f \in I$ no nula, de modo que $\sum_i |\sigma_i(f)| \leq t$. Como la media geométrica está acotada por la media aritmética,

$$|N(f)| = \prod_i |\sigma_i(f)| \leq (\sum_i |\sigma_i(f)|/d)^d \leq t^d/d^d = d!d^{-d}(4/\pi)^s \cdot Vol(\mathcal{O}_\infty/I)$$
$$= d!d^{-d}(4/\pi)^s \cdot \sqrt{|\Delta_K|} \cdot |N(I)|$$

Consideremos $I = A$, entonces existe $f \in A$ de modo que $|N(f)| \leq c$, luego $c \geq 1$. Para todo número natural $m \geq u, 4$ ($u \geq 0$), se cumple que $m!m^{-m}(4/\pi)^{\frac{m}{2}} \cdot u < 1$. Se sigue que si $d > 4$ entonces $d < \sqrt{|\Delta_K|}$.

□

4. Ejercicio: Sea K un cuerpo de números de discriminante -4. Probar que $\dim_{\mathbb{Q}} K = 2$. Probar que $K = \mathbb{Q}[i]$.

4.8. Invertibles. Elementos de norma 1

Queremos estudiar el grupo de invertibles de un anillo de enteros A, que coincide con el grupo de los enteros de K de norma ± 1.

Sea $\mathrm{Div}^0(\bar{X})$ el conjunto de los divisores completos de grado cero. Sea $\mathrm{Div}_\infty = \oplus_{y \in X_\infty} \mathbb{R} \cdot y = \mathbb{R}^{r+s}$ el grupo de los divisores completos de soporte en el infinito y Div^0_∞ el grupo de los divisores completos de soporte en el infinito de grado 0. Consideremos el morfismo natural $\mathrm{Div}(\bar{X}) \to \mathrm{Div}(X)$, $\bar{D} \mapsto \bar{D}_{|X}$ y la sucesión exacta,

$$0 \to \mathrm{Div}^0_\infty \to \mathrm{Div}^0(\bar{X}) \to \mathrm{Div}(X) \to 0$$

Sea $\mathrm{Pic}^0(\bar{X})$ el grupo de las clases de equivalencia de los divisores completos de grado 0. Sea A^* el conjunto de todos los invertibles de A y $\mathrm{Pic}^0_\infty := \mathrm{Div}^0_\infty/\bar{D}(A^*)$. Las sucesiones

$$0 \to \mathrm{Pic}^0_\infty \to \mathrm{Pic}^0(\bar{X}) \to \mathrm{Pic}(X) \to 0$$
$$1 \to \mu_K \to A^* \xrightarrow{\bar{D}} \mathrm{Div}^0_\infty \to \mathrm{Pic}^0_\infty \to 0$$

son exactas. Sabemos que $\mathrm{Pic}(X)$ es un grupo finito.

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

$$\bar{D} + \bar{D}(f) \geq 0$$

Como $D(f) \geq 0$, entonces $f \in A$ y $c' := \mathrm{gr} D(f) \geq 0$. $\bar{D} + \bar{D}_\infty(f)$ está en el compacto

$$C := \{D'' \in \mathrm{Div}^{c-c'}_\infty : D'' \geq 0\}$$

Es decir, $\bar{D}$ pertenece al compacto $C_f := C - \bar{D}_\infty(f) \subset \mathrm{Div}^c_\infty$. Observemos que $c' \leq c$. El número de $f \in A$, salvo multiplicación por invertibles, tales que $\mathrm{gr}D(f) \leq c$ es finito. Por tanto, existe un número finito de funciones $f_i \in A$ de modo que para cada $\bar{D} \in \mathrm{Div}^c_\infty$, existe i tal que $\bar{D} \in C_{f_i} \mod \bar{D}(A^*)$. 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 $\mathbb{R}^d$, y que $\mathbb{Z}^d \subseteq \Gamma$. Consideremos la proyección $\pi : \mathbb{R}^d \to \mathbb{R}^d/\mathbb{Z}^d = S^d_1$. Observemos que 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. 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 $\Gamma = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r$ 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 las raíces de la unidad contenidas en K.*

Demostración. A es un subconjunto discreto de $\mathcal{O}_\infty$, luego A^* es un subgrupo discreto de $\mathcal{O}^*_\infty$. Consideremos el epimorfismo de grupos (que tiene sección)

$$\bar{D}_\infty : \mathcal{O}^*_\infty = (\mathbb{R}^r \oplus \mathbb{C}^s)^* \to \mathrm{Div}_\infty, \ (\lambda_i) \mapsto \sum_i -(\ln|\lambda_i|) \cdot y_i$$

La imagen de A^* es $\bar{D}(A^*)$, luego $\bar{D}(A^*)$ es discreto en $\mathrm{Div}^0_\infty = \mathbb{R}^{r+s-1}$. Por el lema anterior $\bar{D}(A^*)$ es un grupo libre de rango $\leq r + s - 1$. 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 $r + s - 1$. El núcleo del epimorfismo $A^* \to \bar{D}(A^*)$, $f \mapsto \bar{D}(f)$ es $\mathcal{O}_{\bar{X}}(\bar{X}) =: \mu_K$, que son las raíces de la unidad contenidas en K. Por tanto,

$$A^* \simeq \mu_K \oplus \mathbb{Z}^{r+s-1}$$

□

4. Ejercicio : Probar que existen $\xi_1, \ldots, \xi_{r+s-1} \in A^*$, de modo que $a \in A^*$ si y sólo si

$$a = \mu \cdot \xi_1^{n_1} \cdots \xi_{r+s-1}^{n_{r+s-1}}$$

para ciertos números enteros $n_1, \ldots, n_{r+s-1} \in \mathbb{Z}$ (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. Si $\dim_{\mathbb{Q}} K$ es impar, entonces $r > 0$, luego $K \subset \mathbb{R}$ y $\mu_K = \{\pm 1\}$. Además, $N(-1) = -1$, luego $\{a \in A : N(a) = 1\}$ es un subgrupo de índice dos de A^* y $\mu_K \cap \{a \in A : N(a) = 1\} = \{1\}$. Por tanto, $\{a \in A : N(a) = 1\}$ es un grupo de rango $r+s-1$ sin torsión, luego libre.

Si $\dim_{\mathbb{Q}} K$ es par, entonces $N(\xi) = 1$ para todo $\xi \in \mu_K$: Obviamente $N(\pm 1) = 1$. 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 $a \in A \setminus \{0\}$.

Como $\{a \in A : N(a) = 1\}$ es un subgrupo de índice finito de A^* (1 ó 2) y $\mu_K \subset \{a \in A : N(a) = 1\}$, concluimos que es un grupo abeliano finito generado de rango $r+s-1$ y torsión μ_K.

□

6. Ejercicio: Probar que existen $\xi_1, \ldots, \xi_{r+s-1} \in A$ de norma 1, de modo que $a \in A$ es de norma 1, si y sólo

$$a = \begin{cases} \xi_1^{n_1} \cdots \xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_k K \text{ impar.} \\ \mu \cdot \xi_1^{n_1} \cdots \xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu \in \mu_K, \text{ si } \dim_k K \text{ es par.} \end{cases}$$

para ciertos números enteros $n_1, \ldots, n_{r+s-1} \in \mathbb{Z}$ (únicos). Probar que existen además $\mu_1, \ldots, \mu_i \in A$ de norma $c \in \mathbb{Z}$, de modo que $N(a) = c \in \mathbb{Z}$ si y sólo

$$a = \begin{cases} \mu_i \cdot \xi_1^{n_1} \cdots \xi_{r+s-1}^{n_{r+s-1}} & \text{si } \dim_k K \text{ impar.} \\ \mu_i \cdot \mu \cdot \xi_1^{n_1} \cdots \xi_{r+s-1}^{n_{r+s-1}} & \text{para un (único) } \mu \in \mu_K, \text{ si } \dim_k K \text{ es par.} \end{cases}$$

para ciertos números enteros $n_1, \ldots, n_{r+s-1} \in \mathbb{Z}$ (únicos), para un i (único) (recordar la proposición 4.2.14).

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 enteros 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 $N(\frac{a+b\sqrt{\Delta}}{2}) = \pm 1$ entonces $\frac{a+b\sqrt{\Delta}}{2} \in A^*$, porque su polinomio anulador sería $x^2 - ax \pm 1$. Por tanto,

$$A^* = \{\frac{a+b\sqrt{\Delta}}{2}, a, b \in \mathbb{Z} : a^2 - b^2\Delta = \pm 4\}$$

Para calcular el generador de A^*, que es único salvo toma de inverso y multiplicación por -1, observemos podemos suponer que $a, b > 0$ y ha de ser aquel que cumpla además que a y b son mínimos.

8. Ejercicio: Calcular los invertibles de los anillos de enteros de $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ y $\mathbb{Q}[\sqrt{6}]$.

4.9. 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 $\lim_{x\to\infty} \frac{O(x)}{x} = k \neq 0$)

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 $\mathrm{gr}(D(f)) \leq \ln n + m$. Es decir, $T(n)$ es el número de conjuntos fA^* tales que $f \in \mathfrak{a}$ y tales que $\mathrm{gr}(D(f)) \leq \ln n + m$.

Consideremos los morfismos

$$\begin{array}{ccccc} (\mathbb{R}^r \oplus \mathbb{C}^s)^* = \mathscr{O}_\infty^* & \overset{\bar{D}_\infty}{\to} & \mathrm{Div}_\infty & \overset{-\mathrm{gr}}{\to} & \mathbb{R} \\ (\lambda_1, \ldots, \lambda_{r+s}) & \mapsto & -\sum_i (\ln|\lambda_i|) \cdot y_i & & \end{array}$$

Observemos que $-\mathrm{gr}(\bar{D}_\infty(f)) = \mathrm{gr}(D(f))$, ya que $\mathrm{gr}\bar{D}(f) = 0$. Sea G el núcleo del morfismo de grupos $\bar{D}_\infty$ y $\mathrm{Div}_\infty \to \mathscr{O}_\infty^*$, $\sum_i \mu_i y_i \mapsto (e^{-\mu_1}, \ldots, e^{-\mu_{r+s}})$ una sección de $\bar{D}_\infty$, luego $\mathscr{O}_\infty^* = G \times \mathrm{Div}_\infty$. Sea $\mathbb{R} \to \mathrm{Div}_\infty$, $t \mapsto \frac{-t}{d} \cdot (y_1 + \cdots + y_{r+s})$ una sección de $-\mathrm{gr}$. Luego $\mathrm{Div}_\infty = \mathrm{Div}_\infty^0 \times \mathbb{R}$ y

$$\mathscr{O}_\infty^* = G \times \mathrm{Div}_\infty^0 \times \mathbb{R}$$

y la homotecia por $\lambda \in \mathbb{R}$ en $\mathscr{O}_\infty^*$ se corresponde con la traslación por $\ln \lambda^d$ en el tercer factor de $G \times \mathrm{Div}_\infty^0 \times \mathbb{R}$. Sea $P \subset \mathrm{Div}_\infty^0$ el paralelepípedo fundamental de la red $\bar{D}(A^*)$ en Div_∞^0. Para cada conjunto fA^*, existe $fu \in fA^*$ tal que $\bar{D}_\infty(fu) \in P \times \mathbb{R} \subset \mathrm{Div}_\infty$ y todos los que cumplen esta condición son $f \cdot u \cdot \mu_K$ (observemos además que $\mathrm{gr}(D(fv)) = \mathrm{gr}D(f)$, para todo $v \in A^*$). Luego, si $w = |\mu_K|$, entonces $w \cdot T(n)$ es el número de elementos de la red $\mathfrak{a}$ en el conjunto

$$U_n := G \times P \times (-\infty, \ln n + m] = n^{1/d} U_1$$

Por el lema[1] 4.9.2, $w \cdot T(n) = v \cdot n + O(n^{\frac{d-1}{d}})$.

□

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*

$$P(\lambda) = v\lambda^d + O(\lambda^{d-1})$$

[1] Donde $E = \mathscr{O}_\infty$, $\Gamma = \mathfrak{a}$ y $U = U_1 \coprod \{0\}$. $U_1 = G \times P \times (\infty, m]$ es acotado porque si denotamos por ϕ la igualdad $G \times \mathrm{Div}_\infty^0 \times \mathbb{R} = \mathscr{O}_\infty^*$, entonces $\phi(G \times P \times (-\infty, m]) = (0, e^{m/d}] \cdot \phi(G \times P \times \{0\})$. Observemos además que el cierre de $G \times P \times (-\infty, m]$ en $\mathscr{O}_\infty$ es igual a este conjunto unión $0 \in \mathscr{O}_\infty$

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 $\cup_{p \in U \cap \lambda^{-1}\Gamma} p + C$, 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

$$P(\lambda) = \lambda^d \cdot Vol(U) + \lambda^d O(\lambda^{-1}) = \lambda^d \cdot Vol(U) + O(\lambda^{d-1})$$

□

4.10. La función zeta

El número de números primos es infinito. Veamos la demostración de Euler de este hecho. 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 $p_1, \dots, p_r$. 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.

En el siguiente teorema vemos que la serie $\sum_{n=1}^{\infty} \frac{1}{n^x}$ es convergente para todo $x > 1$, que $\sum_{n=1}^{\infty} \frac{1}{n^x} = \prod_{p \text{ primo}} (1 - \frac{1}{p^x})^{-1}$ y qué sucede cuando $x \to 1$.

1. Teorema: *La serie $\zeta(x) = \sum_{n=1}^{\infty} n^{-x}$ es una función continua en $(1, \infty)$ tal que*

$$\lim_{x \to 1} (x-1) \cdot \zeta(x) = 1 \quad y \quad \zeta(x) = \prod_{p \text{ primo}} (1 - \frac{1}{p^x})^{-1}$$

Demostración. La serie $\sum_{n=1}^{\infty} n^{-x}$ es una serie de términos positivos y tenemos

$$\frac{1}{x-1} = \int_1^{\infty} t^{-x} dt < \sum_{n \ge 1} n^{-x} < 1 + \int_1^{\infty} t^{-x} dt = 1 + \frac{1}{x-1}$$

luego es convergente, para cada $x \in (1, \infty)$. Además, los sumandos n^{-x} son funciones continuas en x decrecientes, por lo que la serie $\zeta(x)$ es uniformemente convergente (en los intervalos $[a, \infty)$) y converge a una función continua.

Por último, la igualdad[2] $\sum_{n=1}^{\infty} n^{-x} = \prod_p (1 + p^{-x} + p^{-2x} + \cdots) = \prod (1 - p^{-x})^{-1}$ expresa la unicidad de la descomposición de n en producto de números primos. □

[2] Recuerde el lector que toda serie de números complejos absolutamente convergente es incodicionalmente convergente.

2. Corolario: *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 $\zeta(mx) = \sum_n (n^m)^{-x}$ define una función continua en la semirrecta $x > 1/m$ y la subserie formada por los términos correspondientes a los números n con todos sus factores primos en P coincide con el producto considerado. □

Tratemos de generalizar todas estas definiciones y resultados a los anillos de números.

3. Definición: Sea K un cuerpo de números y A el anillo de enteros de K. Se dice que

$$\zeta_K(x) := \sum_{0\neq \mathfrak{a}\subset A} N(\mathfrak{a})^{-x}$$

es la función zeta de K.

4. Ejercicio: Probar que $\zeta(x) = \zeta_{\mathbb{Q}}(x)$.

5. 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 4.9.1 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. □

6. 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. Por hipótesis existe una constante $c > 0$ tal que $|b_n| < cn^\epsilon$, para todo n. Ahora, para cada pareja de números naturales $m < r$,

$$\sum_{n=m}^{r} a_n\cdot n^{-x} = \sum_{n=m}^{r}(b_n - b_{n-1})\cdot n^{-x} = b_r r^{-x} - b_{m-1}(m-1)^{-x} + \sum_{n=m}^{r-1} b_n\cdot(n^{-x} - (n+1)^{-x})$$

Como $|b_n\cdot(n^{-x}-(n+1)^{-x})| \leq cn^\epsilon\cdot x\int_n^{n+1} t^{-x-1}dt \leq c\cdot x\int_n^{n+1} t^{-x-1+\epsilon}dt$,

$$|\sum_{n=m}^{r} a_n\cdot n^{-x}| \leq 2cm^{-x+\epsilon} + c\cdot x\int_m^\infty t^{-x-1+\epsilon}dt = (2c + \frac{cx}{-x+\epsilon})\cdot m^{-x+\epsilon},$$

que tiende a cero para $m >> 0$ (fijado el compacto de la semirrecta (ϵ,∞)). □

7. Definición: Sea A un anillo de números enteros, $\mathfrak{p}_x \subset A$ 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

$$\mathrm{gr}_{\mathbb{Z}}\, x := l_{\mathbb{Z}}(A/\mathfrak{p}_x) = \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{p}_x = \mathrm{gr}_p\, x$$

Recordemos que si $\mathrm{Spec}\, A/pA = \{x_1, \ldots, x_r\}$ entonces $d = \mathrm{gr}_{\mathbb{Z}}\, x_1 \cdot m_{x_1} + \cdots + \mathrm{gr}_{\mathbb{Z}}\, x_r \cdot m_{x_r}$. 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.

Por ejemplo, dado un polinomio mónico $q(x) \in \mathbb{Z}[x]$ sea $A = \mathbb{Z}[x]/(q(x))$. Los primos de A de grado sobre $\mathbb{Z}$ igual a 1 se corresponden con las raíces racionales de $q(x)$ en $\mathbb{Z}/p\mathbb{Z}$ (variando p).

8. 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.

9. 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 $P_{m,r} := \{\text{primos } p \in \mathbb{Z}, \text{ tales que el número de ideales primos de grado } m \text{ sobre } \mathbb{Z} \text{ en la fibra de } p \text{ es } r\}$. Observemos que si $P_{m,r} \neq \emptyset$ entonces $m \cdot r \leq d$. Para cada $p \in P_{m,r}$ existen r primos $\mathfrak{p}_y \in A$ 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 4.10.2, hemos concluido.

□

Sea K un cuerpo de números y A el anillo de enteros de K. Con abuso de notación, diremos que un ideal primo $\mathfrak{p} \subset A$ es un ideal primo de K.

10. Teorema: *Todo cuerpo de números tiene infinitos ideales primos de grado* 1 *sobre* $\mathbb{Z}$.

Demostración. Si K sólo tuviera un número finito de primos de grado 1, entonces existe $c \neq 0$ tal que

$$\lim_{x\to 1} \zeta(x) = c \cdot \lim_{x\to 1} \prod_{\mathrm{gr}_{\mathbb{Z}}\, y = 1} (1 - \frac{1}{N(\mathfrak{p}_y)^x})^{-1} < \infty$$

y $\lim_{x\to 1} (x-1) \cdot \zeta(x) = 0$ y llegamos a contradicción.

□

4.10.1. Aplicaciones

11. Lema: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0 &= q(x_1,\dots,x_n)\\ &\dots\dots\\ 0 &= q_r(x_1,\dots,x_n) \end{aligned}$$

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 $\mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r)$. El sistema no tiene soluciones complejas si y sólo si $0=\mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r)$.

Igualmente, por el teorema de los ceros de Hilbert, el sistema no tiene soluciones algebraicas si y sólo si $\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)$ no tiene ideales maximales, es decir, $0=\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)$.

Concluimos porque $\mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r)=0$ si y sólo si $\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)=0$, ya que $\mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r)=\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)\otimes_{\mathbb{Q}}\mathbb{C}$.

□

12. Proposición: *La condición necesaria y suficiente para que un sistema de ecuaciones diofánticas*

$$\begin{aligned} 0 &= q(x_1,\dots,x_n)\\ &\dots\dots\\ 0 &= q_r(x_1,\dots,x_n) \end{aligned}$$

tenga alguna solución compleja es que admita soluciones modulares en infinitos primos

Demostración. Si el sistema no tiene soluciones complejas, entonces

$$0=\mathbb{C}[x_1,\dots,x_n]/(q_1,\dots,q_r)=\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)\otimes_{\mathbb{Q}}\mathbb{C},$$

por tanto $\mathbb{Q}[x_1,\dots,x_n]/(q_1,\dots,q_r)=0$. Luego 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 enteros 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 4.10.10 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 $\mathbb{Z}/p\mathbb{Z}=A/\mathfrak{p}$.

□

13. Corolario: *Todo polinomio no constante con coeficientes enteros $q(x)$ tiene infinitas raíces modulares. Más aún, hay infinitos números primos p en los que $\overline{q(x)} \in \mathbb{Z}/p\mathbb{Z}$ 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 $\mathbb{Z}/p\mathbb{Z}$. □

14. 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 sólo si el automorfismo de Fröbenius en p, F_p de $\mathbb{Q}[e^{2\pi/i}]$ 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). □

15. Definición: Sea K un cuerpo de números y A el anillo de enteros 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 sólo 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 enteros de K, se cumple que $A/(p) = \mathbb{F}_p[x]/(\overline{p(x)})$. Entonces, (p) descompone totalmente en K si y sólo 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, que necesariamente han de tener 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,

$$\zeta_L(x) \sim \zeta_K(x)^d$$

Si $d > 1$, existe una constante $c > 0$, de modo que

$$\lim_{x\to 1}(x-1)\cdot\zeta_L(x) = c \cdot \lim_{x\to 1}(x-1)\cdot\zeta_K(x)\cdot\lim_{x\to 1}\zeta_K(x)^{d-1} = \infty,$$

lo cual es contradictorio.

□

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 sólo 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 F denotemos A_F el anillo de enteros de F.

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, $L' \subseteq L$.

□

4.11. Cuestionario

1. Demostrar que $\operatorname{Pic} A = \{0\}$ si y sólo si A es d.i.p..
2. Consideremos $\mathbb{Q}(i)$. Calcular $D(i+1)$ y $D(i+3)$.
3. 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. Probar que
$$D(I_1 + I_2) = \text{ínf}\{D(I_1), D(I_2)\}.$$
4. Consideremos $\mathbb{Q}(i)$. Calcular $\bar{D}(i+1)$ y $\bar{D}(i+3)$.
5. Resolver el ejercicio 4.3.6.

6. Consideremos $\mathbb{R}^3$ con el producto escalar estándar. Calcular el volumen del paralelepípedo definido por los vectores $(1,3,2),(1,2,1)$ y $(0,1,-1)$.
7. Sea $A=\mathbb{Z}[i]\subset\mathbb{C}$ y consideremos en la $\mathbb{R}$-álgebra $\mathbb{C}$ la métrica de la traza. Calcular $Vol(\mathbb{C}/A)$.
8. Resolver el ejercicio 4.4.7.
9. Sean I,I' ideales fraccionarios de un cuerpo de números. Probar que
$$Vol(\mathcal{O}_\infty/II')=\frac{Vol(\mathcal{O}_\infty/I)\cdot Vol(\mathcal{O}_\infty/I')}{\sqrt{|\Delta_K|}}$$
10. 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 $\bar{D}=2x_3+2x_5\in \mathrm{Div}\,\bar{X}$. Calcular $\bar{I}_{-\bar{D}}$.
11. Probar que $\mathbb{Z}[i]$ es un dominio de ideales principales.
12. Probar que $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ es un dominio de ideales principales.
13. Probar el ejercicio 4.7.4.
14. Calcular $\mathbb{Z}[i]^*$, $\mathbb{Z}[e^{2\pi i/3}]^*$.
15. Sea A el anillo de enteros de un cuerpo de números y $S(n)$ el número de $f\in A$, salvo multiplicación por invertibles, tales que $|N(f)|\leq n$. Probar que existe una constante $v>0$, de modo que $S(n)=v\cdot n+O(n^{1-\frac{1}{d}})$.
16. Probar que $\zeta(x)=\zeta_{\mathbb{Q}}(x)$.
17. Sea $\mathfrak{p}_x=(7)\subset\mathbb{Z}[i]$. Calcular $\mathrm{gr}_{\mathbb{Z}}\,x$.
18. ¿Existen infinitos primos $p\in\mathbb{Z}$ para los que $\sqrt[7]{3}\in\mathbb{Z}/p\mathbb{Z}$?
19. ¿Existen infinitos primos $p\in\mathbb{Z}$ para los que $\sqrt{3}\notin\mathbb{Z}/p\mathbb{Z}$?

4.12. 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. These 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/).

4.13. Problemas

1. Probar que $K \subset \mathcal{O}_\infty$ es un conjunto denso.

   Resolución: $K = \mathbb{Q} \oplus \overset{d}{\cdots} \oplus \mathbb{Q}$ y $\mathcal{O}_\infty := K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R} \oplus \overset{d}{\cdots} \oplus \mathbb{R}$.

2. Probar 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 $\mu_K = \{\pm 1\}$.

3. Probar que si K es una $\mathbb{Q}$-extensión de Galois, entonces $\sqrt{\Delta_K} \in K$.

   Resolución: $\sqrt{\Delta_K} = \pm \cdot \det((\sigma_i(a_j))) \in K$

4. Probar que el discriminante de todo cuerpo de números es congruente con $0, 1$ mód 4.

   Pista: El determinante $\det(T_2(a_i, a_j))$, 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 positivos (resp. la suma de los términos negativos), entonces $\Delta = (P-N)^2 = (P+N)^2 - 4PN$.

5. 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 $c_1 \cdots c_n > |\det((a_{ij}))|$. Probar 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.

6. Sea K un cuerpo de números y $d = \dim_{\mathbb{Q}} K$. Probar 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 $I \subset \mathcal{O}_\infty = \mathbb{R}^r \times \mathbb{C}^s$. Recordemos que $Vol(\mathcal{O}_\infty/I) = N(I)\cdot\sqrt{|\Delta_K|}$. Sea $C = \{(\lambda_1,\dots,\lambda_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : |\lambda_i| \le c\}$. $Vol(C) = 2^s((2c)^r(\pi c^2)^s) = 2^{r+s}\pi^s c^d$. Para $c = (N(I)\cdot\sqrt{|\Delta_K|}\cdot(\frac{2}{\pi})^s)^{1/d}$, se cumple que $Vol(C) \ge 2^d \cdot Vol(\mathcal{O}_\infty/I)$. Por el teorema del punto de red de Minkowski existe $f \in I \cap C$, es decir, lo que nos piden probar.

7. 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

$$\prod_{y\in X_\infty} c_y^{\mathrm{gr}\, y} > (\frac{2}{\pi})^s \cdot Vol(\mathcal{O}_\infty/I)$$

   Probar que existe $0 \ne f \in I$, tal que $|f|_y < c_y$ para todo $y \in X_\infty$.

   Resolución: Consideremos la red $I \subset \mathcal{O}_\infty = \mathbb{R}^r \times \mathbb{C}^s$. Recordemos que $Vol(\mathcal{O}_\infty/I) = N(I)\cdot\sqrt{|\Delta_K|}$. Sea $C = \{(\lambda_1,\dots,\lambda_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : |\lambda_i| \le c_i\}$. $Vol(C) = 2^s 2^r \pi^s \prod_{y\in X_\infty} c_y^{\mathrm{gr}\, y}$. Se cumple que $Vol(C) \ge 2^d \cdot Vol(\mathcal{O}_\infty/I)$. 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 de enteros A. Probar que existe un ideal $\mathfrak{a} \subseteq A$ tal que $N(\mathfrak{a}) \le \frac{d!}{d^d}\cdot(\frac{4}{\pi})^s \cdot \sqrt{|\Delta_K|}$.

   Resolución: Consideremos el ideal fraccionario $I = A$. Por la proposición 4.7.3, existe $a \in A$ tal que $N(aA) = |N(a)| \le \frac{d!}{d^d}\cdot(\frac{4}{\pi})^s \cdot \sqrt{|\Delta_K|}$.

9. Probar que el anillo de enteros 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 enteros 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 $|A/\mathfrak{p}_z| \le \sqrt{5} < 3$ son principales. Luego, sólo 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 enteros 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 $|A/\mathfrak{p}_z| \le \sqrt{8} < 3$ son principales. Luego, sólo 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 enteros 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 $|A/\mathfrak{p}_z| \le \sqrt{44} < 7$ son principales. Luego, sólo 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 enteros 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 $|A/\mathfrak{p}_z| \le \sqrt{3} < 2$ son principales.

Consideremos $K=\mathbb{Q}[\sqrt{-4}]=\mathbb{Q}[\sqrt{-1}]$. $\Delta_K=-4$. El anillo de enteros 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, sólo 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 enteros 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, sólo 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 enteros 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, sólo 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 enteros 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, sólo tenemos que comprobarlos para los ideales tales que $|A/\mathfrak{p}_z|=2,3,4$. $(2)_0=\{(2)\}$ y $(3)_0=\{(3,x)=(x),(3,x-1)=(x-1)\}$.

10. Probar que las únicas soluciones enteras de la ecuación

$$y^2+2=x^3$$

son $y=\pm5$,$x=3$.

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 $|A/\mathfrak{p}_y|\leq\sqrt{|\Delta_A|}<3$ 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

$$\begin{aligned}(y-\sqrt{-2},y+\sqrt{-2})_0&=(y-\sqrt{-2},2\sqrt{-2})_0=(y-\sqrt{-2},\sqrt{-2})_0\\&=(y,\sqrt{-2})_0=\begin{cases}\emptyset, & \text{si } y\neq\dot{2}\\ (\sqrt{-2}), & \text{si } y\neq\dot{2}\end{cases}\end{aligned}$$

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 $a=\pm1$, de donde $y=\pm5$ y por tanto $x=3$.

11. **La batalla de Hastings** (14 de octubre de 1066). "Los hombres de Harold permanecían bien juntos, como solían hacer, y formaban 13 escuadrones (i.e. cuadrados), 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 4.8.7,

$$A^* = \{\frac{a + b\sqrt{13}}{2}, a, b \in \mathbb{Z} : a^2 - 13b^2 = \pm 4\}$$

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.

12. Probar que si $\dim_{\mathbb{Q}} K >> 0$ entonces $|\Delta_K| >> 0$.

Resolución: Por la proposición 4.7.3 (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 $|\Delta_K| >> 0$.

13. 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 $c \circ \sigma \in P$. Probar que existe un invertible ϵ en el anillo de enteros 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 enteros 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 $\sigma \notin P$.

14. Probar 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 enteros 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. Podemos suponer que c es irreducible. Dado $z \in A \setminus \{0, 1, -1\}$ tenemos que $z = z' \cdot c + r$, con $r = 0$ ó $\operatorname{gr} r < \operatorname{gr} c$, 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.

15. En el lema 4.9.2, sea $E = \mathbb{R}^d$ con la métrica estándar. Probar 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 $v = Vol(U)$.

16. Probar que $v = \pi/4$ en el teorema 4.9.1 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 4.9.1, $\mathfrak{a} = \mathbb{Z}[i]$ y $m = 0$, $G = S^1$, $P = \{0\}$ y $U_1 = G \times (-\infty, 0]$ y resulta ser el círculo unidad. Luego,

$$v = \frac{Vol(U_1)}{|\mu_{\mathbb{Q}[i]}| \cdot Vol(\mathbb{C}/\mathbb{Z}[i])} = \pi/4$$

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