Teoría de números algebraica

Pierre Samuel

Traducido por: NICOLÁS OJEDA BÄR

Pierre Samuel, doctor en ciencias, profesor de la universidad Paris XI, nació en 1921. Sus trabajos conciernen principalmente el álgebra conmutativa y la geometría algebraica.

Índice general

Introducción

La Teoría de Números, o Aritmética, a veces es llamada la "Reina de la Matemática". La simplicidad del objeto de estudio (los números enteros y sus generalizaciones), la elegancia, la diversidad de los métodos y los numeros problemas irresueltos ejercen una poderosa atracción sobre los matemáticos, ya sean principiantes, teóricos de números profesionales o especialistas en otras ramas de la matemática. Es por eso que no debe sorprender al lector que el autor de este libro es un geómetra algebraico, que no tiene ninguna publicación original dentro del dominio de la Aritmética propiamente dicho.

De hecho, este libro no se distingue ni por su profundidad ni por su alcance. Más aún, sólo presenta uno de los posibles puntos de vista con los cuales se puede abordar la teoría de números, a saber, el punto de vista algebraico. Salvo un resultado elemental de Minkowski sobre reticulados en $\mathbf{R}^n$, no se tocan en ningún momento los bellos, y fértiles, métodos analíticos.

La preponderancia otorgada al punto de vista algebraico me parece justificada por diversas razones. En primer lugar, permite ponerse rápidamente en el marco donde los problemas de la aritmética se enuncian en su forma más natural, incluso cuando sólo involucran los números enteros usuales. Veremos, por ejemplo, que la búsqueda de soluciones en enteros de la ecuación de Pell-Fermat $x^2 - dy^2 = \pm 1$ (d: un entero dado libre de cuadrados) es un problema que esencialmente concierne al cuerpo cuadrático $\mathbf{Q}(\sqrt{d})$. Para la "gran" ecuación de Fermat $x^n + y^n = z^n$, es el cuerpo de raíces n-ésimas de la unidad que juega el papel decisivo. Para escribir un entero como suma de dos (respectivamente, cuatro) cuadrados, veremos que es muy ventajoso trabajar con el anillo $\mathbf{Z}[i]$ de los enteros de Gauss (respectivamente, con un anillo de cuaterniones conveniente). La ley de reciprocidad cuadrática hace intervenir al mismo tiempo los cuerpos cuadráticos y las raíces de la unidad. A lo largo de todo esto, aparecen cuerpos más generales que $\mathbf{Q}$, anillos más generales que $\mathbf{Z}$, como también sus cuerpos y anillos cocientes, es decir, cuerpos finitos y álgebras sobre éstos.

Así, si bien no agota la Teoría de Números, el método algebraico permite obtener rapidamente resultados substanciales. De hecho, de continuar en esta misma dirección, arrivaríamos a teoremas más profundos, como aquellos de la teoría de cuerpos de clases.

Por otra parte, aún aquellos que prefieren los métodos analíticos no ignoran que éstos sólo adquieren su máxima expresión cuando se los aplica a cuerpos de números algebraicos y no sólamente a $\mathbf{Q}$. Por ejemplo, no vale la pena estudiar sólamente la función $\zeta(s)$ sin tratar al mismo tiempo la función $\zeta_{\mathrm{K}}(s)$ de un cuerpo de números K, ni otras numerosas "series L."

Finalmente, el desarollo del método algebraico tiene la ventaja de presentar al estudiante con numerosos ejemplos ilustrativos de las nociones introducidas en el curso de álgebra: grupos, anillos, cuerpos, ideales, anillos y cuerpos cociente, homomorfismos e isomorfismos, módulos y espacios vectoriales. Al mismo tiempo se introducen numerosas nociones algebraicas que son fundamentales en otras ramas de la matemática, como la Geometría Algebraica. Por ejemplo, los elementos enteros sobre un anillo, las extensiones de cuerpos, la teoría de Galois, los módulos sobre dominios de ideales principales, los anillos y módulos noetherianos, los anillos de Dedekind y los anillos de fracciones.

Lo anterior describe implicitamente lo que el lector encontrará en este libro y aquello que le será imposible encontrar aquí. He asumido que él conoce el álgebra de un primer curso de licenciatura: nociones básicas sobre los grupos, anillos, cuerpos, polinomios, espacios vectoriales—el manejo de los subobjetos, objetos cociente y objetos producto—el mecanismo del paso al cociente por un ideal o un submodulo—las diversas nociones de homomorfismo e isomorfismo. Todo lo necesario sobre estas cuestiones puede encontrarse en un libro básico de álgebra "moderna," por ejemplo el excelente "Cours d'Algèbre" de R. Godement o el "Algebra" de S. Lang[1]. Por eso, utilisaré este lenguaje y resultados sin mencionarlo y espero poder mostrarle al lector que son muy eficaces a la hora de obtener rapidamente teoremas substanciales de la aritmética. Por otra parte, pensé que, si bien estos temas se cubren en la orientación de "algebra" de la Licenciatura, sería más cómodo para el lector poder encontrar aquí todo lo necesario sobre elementos enteros de un anillo, extensiones algebraicas de cuerpos, teoría de Galois, modulos y anillos noetherianos y anillos de fracciones. He intenatado presentar estos temas sin ninguna laguna (??), pero al mismo tiempo evitando cualquiera sofisticacion inutil.

[1]Desde ya, estas dos obras tienen un alcance mucho mayor.

Este libro debe su existencia a un curso de "Matemática avanzada" dictado en la Universidad de Paris en 1965 y de nuevo en 1966. Notas fotocopiadas de Alfred Vidal-Madjar, alumno del École Normale Supérieure, al cual le agradezco vivamente, sirvieron como una primera versión. Algunos pasajes provienen de cursos dicatdos en el École Normale Supérieure de Jeunes Filles y en la Universidad de Clermont-sur-Tiretaine. Por último, me fueron muy importantes el consejo y la influencia de numerosos matemáticos. Entre estos, quiero agradecer especialmente al maestro de mi generación, N. Bourbaki, que tuvo la amabilidad de mostrarme algunos de sus manuscritos que todavía no han sido publicados. También les agradezo a mis amigos Emil Grosswald, Georges Poitou, Jean-Pierre Serre y John Tate.

Prefacio a la segunda edición

Mis sinceros agradecimientos a numerosos lectores de la primera edición, entre ellos Germaine Revuz, Alain Bouvier y Pierre Cartier, que envíaron listas de correcciones sumamente útiles. Las observaciones del traductor de la edición inglesa, Alan Silberger, también han sido muy valiosas.

julio 1971

À NICOLE
qui a su créer autour de moi
une atmosphère favorable à ce livre.

Repaso de notaciones, definiciones y resultados

Utilizamos las notaciones usuales de la teoría de conjuntos: $\in$, $\subset$, $\cup$, $\cap$. El complemento de un subconjunto B de un conjunto A se nota $A - B$. El cardinal (o potencia o número de elementos) de un conjunto A lo notaremos card(A); si A es un grupo también hablamos del orden de A.

Suponemos que el lector está familiarizado con las nociones de grupo, anillo, cuerpo y espacio vectorial, como así también la teoría básica de los espacios vectoriales (llamada también "algebra lineal"). En este libro, salvo en el capítulo V, §7, "anillo" (resp. "cuerpo") quiere decir anillo (resp. cuerpo) **conmutativo y con unidad.**

Dado un grupo finito G y un subgrupo H de G, recordamos que card(H) divide a card(G); el cociente $\mathrm{card(G)}/\mathrm{card(H)}$ se llama el índice de H en G y se nota $(G : H)$.

Dados dos subconjuntos A y B de un grupo G (escrito aditivamente), $A + B$ denota el conjunto de sumas $a + b$ con $a \in A$ y $b \in B$.

Dado un anillo A, denotamos por A[X] o A[Y] (letras mayúsculas) el anillo de polinomios (formales) en una variable sobre A; escribimos $A[X_1, \ldots, X_n]$ para el anillo de polinomios en n variables y A[[X]] para las series formales.

Por convención, un subanillo A de un anillo B contiene el elemento unidad de B. Dado un anillo B, un subanillo A de B y un elemento $x \in B$, denotamos por $A[x]$ el subanillo de B generado por A y x, es decir, la intersección de todos los subanillos de B que contienen A y x; es el conjunto de sumas de la forma $a_0 + a_1 x + \cdots + a_n x^n$ ($a_i \in A$); Escribimos $A[x_1, \ldots, x_n]$ para el subanillo de B generado por A y una colección finita $(x_1, \ldots, x_n)$ de elementos de B.

Un anillo se dice **dominio íntegro** (o sin divisores de cero) si el producto de dos elementos no nulos es no nulo y si A tiene más de un elemento.

Un ideal $\mathfrak{b}$ de un anillo A es un subgrupo aditivo tal que $x \in \mathfrak{b}$ y $a \in A$ implican $ax \in \mathfrak{b}$. El anillo completo y el conjunto que consiste del único elemento 0 (escrito $\{0\}$) son ideales, algunas veces llamados "triviales". Un cuerpo no posee ningún otro ideal, y esta propiedad caracteriza a los cuerpos entre todos los anillos. Dada una familia (b_i) de elementos de un anillo A, la

intersección de los ideales de A que contienen a los b_i es un ideal de A, llamado el ideal generado por los b_i; es el conjunto de sumas finitas $\sum_i a_i b_i$ con $a_i \in \mathrm{A}$. Un ideal generado por un elemento b se dice principal y lo escribimos Ab ó (b).

Dado un anillo A y un ideal $\mathfrak{b}$ de A, las clases de equivalencia $a+\mathfrak{b}$ ($a \in \mathrm{A}$) forman un anillo, llamado anillo cociente de A por $\mathfrak{b}$ y notado $\mathrm{A}/\mathfrak{b}$. Los ideales de $\mathrm{A}/\mathfrak{b}$ son de la forma $\mathfrak{b}'/\mathfrak{b}$, donde $\mathfrak{b}'$ recorre el conjunto de ideales de A que contienen a $\mathfrak{b}$. para que $\mathrm{A}/\mathfrak{b}$ sea un cuerpo es necesario y suficiente que $\mathfrak{b}$ sea maximal entre los ideales de A distintos a A; en este caso decimos que $\mathfrak{b}$ es maximal. Un ideal $\mathfrak{p}$ se dice primo si $\mathrm{A}/\mathfrak{p}$ es un dominio íntegro.

Dados dos anillos A, A$'$ con elementos neutros e y e', un homomorfismo $f : \mathrm{A} \to \mathrm{A}'$ es una función f de A en A$'$ tal que:

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(e) = e'.$$

Dado un anillo A, una **A-álgebra** es un anillo B equipado con un homomorfismo $\varphi : \mathrm{A} \to \mathrm{B}$. Si A es un cuerpo φ es injectivo, y en este caso generalmente identificamos A con su imagen $\varphi(\mathrm{A})$ (que es un subanillo de B).

Dado un cuerpo L y un subcuerpo K de L, decimos que L es una extension de K.

El elemento neutro de un anillo A sera escrito casi siempre como 1.

La noción de **módulo** sobre un anillo A (o de A-módulo) es una generalización directa del concepto de espacio vectorial sobre un cuerpo. Un A-modulo M es un grupo abeliano (escrito aditivamente) junto con una aplicación $\mathrm{A} \times \mathrm{M} \to \mathrm{M}$ (escrita multiplicativamente) tal que $a(x+y) = ax + ay$, $(a+b)x = ax + bx$, $a(bx) = (ab)x$ y $1x = x$ (a,$b \in$ A, x,$y \in$ M). Se tienen las nociones de submódulo y módulo cociente. Dados dos A-módulos M y M$'$, un homomorfismo (o aplicación A-lineal) de M en M$'$ es una función $f : \mathrm{M} \to \mathrm{M}'$ tal que

$$f(x+y) = f(x) + f(y), \quad f(ax) = af(x) \quad (a \in \mathrm{A}, x,y \in \mathrm{M}).$$

Dado un homomorfismo $f : \mathrm{X} \to \mathrm{X}'$ (de grupos, anillos o módulos), llamamos **núcleo** de f, y lo escribimos $\ker(f)$, a la imagen recíproca por f del elemento neutro de X$'$. Es un subgrupo normal (o un ideal, o un submódulo) de X; para que f sea inyectiva es necesario y suficiente que $\ker(f)$ consista únicamente del elemento neutro de X. Llamamos **imagen** de f al subconjunto $f(\mathrm{X})$ de X$'$; es un subgrupo (o un subanillo, o un submódulo) de X$'$.

Dados dos conjuntos X, X$'$, una función f de X en X$'$ generalmente se nota $f : \mathrm{X} \to \mathrm{X}'$. Cuando una función $f : \mathrm{X} \to \mathrm{X}'$ se describe dando el valor que le asigna a un elemento arbitrario x de X, utilizamos la notación

$x \mapsto f(x)$. Por ejemplo, la función seno, $\sin : \mathbf{R} \to \mathbf{R}$ puede definirse por

$$x \mapsto \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}.$$

Utilizamos las notaciones usuales para los siguientes objetos matemáticos:

N: conjunto de los enteros naturales (0,1,2,...,n,...) (N por "números").

Z: anillo de los enteros racionales (enteros naturales o sus opuestos) (Z por "Zahlen").

Q: cuerpo de números racionales (cocientes de elementos de **Z**) (Q por "quotients").

R: cuerpo de los números reales (R por "reales").

C: cuerpo de los números complejos (C por "complejos").

$\mathbf{F}_q$: cuerpo finito de q elementos (F por "finito" o "field").

CAPÍTULO I

Dominios de ideales principales

1. Divisibilidad en dominios de ideales principales

Sea A un dominio íntegro, K su cuerpo de fracciones, x e y dos elementos de K. Decimos que x **divide a** y si existe $a \in \mathrm{A}$ tal que $y = ax$. También utilizamos las expresiones "x es un divisor de y", "y es un múltiplo de x" y lo notamos $x \mid y$. Esta relación entre elementos de K depende de forma esencial del anillo A. Si es necesario precisarlo, decimos que se trata de divisibilidad en K **respecto a** A**.**

Dado $x \in \mathrm{K}$, el conjunto de multiplos de x es, utilizando la notación clásica, Ax. Así, $x \mid y$ se puede escribir también $y \in \mathrm{A}x$ o incluso $\mathrm{A}y \subset \mathrm{A}x$. El conjunto A$x$ se llama **ideal fraccionario principal** de K respecto a A. Si $x \in \mathrm{A}$, Ax el el ideal principal (usual) de A generado por x. Como la relación de divisibilidad $x \mid y$ equivale a la relación de **orden** $\mathrm{A}y \subset \mathrm{A}x$, se tienen las dos propiedades siguientes que poseen todas las relaciones de orden.

(1) $$x \mid x; \quad \text{si } x \mid y \text{ y } y \mid z \text{ entonces } x \mid z.$$

Por otra parte, si $x \mid y$ y $y \mid x$, no podemos concluir en general que $x = y$; sólamente se tiene que Ax = Ay, lo que quiere decir (si $y \neq 0$) que el cociente xy^{-1} es un elemento **inversible** de A. Tales pares de elementos se dicen **asociados;** son indistinguibles desde el punto de vista de la divisibilidad.

Ejemplo. Los elementos de K asociados a 1 son los elementos inversibles de A. Usualmente se llaman **unidades** de A y forman un grupo con la multiplicación, que notaremos $\mathrm{A}^\times$. El cálculo de las unidades de un anillo A es un problema interesante y nosotros lo trataremos cuando A es el anillo de enteros de un cuerpo de números (ver cápitulo IV). Los siguientes son algunos ejemplos fáciles:

a) Si A es un cuerpo, $\mathrm{A}^\times$ es el conjunto de elementos no nulos de A;
b) Si A = $\mathbf{Z}$, $\mathrm{A}^\times$ consiste de $+1$ y -1.
c) Las unidades del anillo de polinomios $\mathrm{B} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ son, si A es un dominio íntegro, las constantes inversibles. Es decir, $\mathrm{B}^\times = \mathrm{A}^\times$.

d) Las unidades del anillo de series formales $A[[X_1, \ldots, X_n]]$ son las series formales cuyo término constante es inversible.

Definición 1. *Un anillo* A *se dice un dominio de ideales principales si es un dominio íntegro y si todo ideal es principal.*

En el curso de álgebra básica se demuestra que el anillo **Z** es un dominio de ideales principales (Recordemos que todo ideal $\mathfrak{a} \neq (0)$ de **Z** contiene un entero $b > 0$ mínimo; utilizando división euclidea de $x \in \mathfrak{a}$ por b, vemos que x es un múltiplo de b). Si k es un cuerpo, sabemos igualmente que el anillo $k[X]$ de polinomios en **una** variable es un dominio de ideales principales (mismo método: tomamos un polinomio no nulo $b(X)$ de grado mínimo en el ideal dado $\mathfrak{a}$ y utilizamos división euclidea por $b(X)$). Este método se generaliza a los anillos que se conocen como "euclideos" ([**13**], capítulo VIII, §1, ejercicio; o [**21**], capítulo I). Si k es un cuerpo, es fácil ver que todo ideal no nulo del anillo de series formales $A = k[[X]]$ es de la forma AX^n con $n \geq 0$, de manera que $A = k[[X]]$ es un dominio de ideales principales.

La divisibilidad en el cuerpo de fracciones K de un **dominio de ideales principales** A es particularmente simple. Como es una generalización inmediata del caso de los enteros usuales, hacemos una revisión breve.

I. Dos elementos cualesquiera u, v de K tienen un **máximo común divisor** (m.c.d), es decir un element d tal que las relaciones

$$\text{"}x \mid y \text{ y } x \mid v\text{"} \text{ y } \text{"}x \mid d\text{"} \tag{1}$$

son equivalentes. Equivalentemente, Au y Av tienen un **supremo**[1] en el conjunto ordenado de los ideales fraccionarios principales; por ejemplo, el ideal $Au + Av$, que es un ideal fraccionario principal pues el anillo A es un dominio de ideales principales (la afirmación es clara si $u, v \in A$; nos reducimos a este caso multiplicando u y v por un denominador común). De hecho, obtenemos un poco más ("**la identidad de Bezout**"): existen elementos a, b de A tal que el m.c.d. d de u y v se escribe

$$d = au + bc. \tag{2}$$

El m.c.d. de u y v está determinado de forma única a menos de un elemento inversible de A.

II. Dos elementos cualesquiera u, v de K tienen un **mínimo común múltiplo** (m.c.m.), es decir un elemento m tal que las relaciones

$$\text{"}u \mid x \text{ y } v \mid x\text{"} \text{ y } \text{"}m \mid x\text{"} \tag{3}$$

[1]N. del T.: cota superior minimal.

son equivalentes. Esto se puede ver observando que pasar al inverso $t \mapsto t^{-1}$ invierte las relaciones de divisibilidad, lo que nos reduce al caso del m.c.d.; de esto se sigue que

$$\text{mcm}(u,v) = \text{mcd}(u^{-1},v^{-1})^{-1} \quad (\text{si } u,v \neq 0), \tag{4}$$

de donde deducimos la fórmula usual

$$\text{mcm}(u,v) \cdot \text{mcd}(u,v) = uv. \tag{5}$$

También podríamos haber procedido como en I) y observar que la existencia del m.c.m. de u y v equivale a la existencia de un **ínfimo**[2] para $\mathrm{A}u$ y $\mathrm{A}v$ en el conjunto ordenado de los ideales fraccionarios principales; esta no es otra que $\mathrm{A}u \cap \mathrm{A}v$.

III. Dos elementos a, b de A se dicen **coprimos** si 1 es uno de sus m.c.d. Recordemos el fundamental **Lema de Euclides.** Sean a, b, c elementos de un dominio de ideales principales A; si a divide a bc y es coprimo con b, entonces a divide a c.

> *Demostración breve: por Bezout* (2)*, existen* a' *y* $b' \in \mathrm{A}$ *tales que* $1 = a'a + b'b$*, de donde* $c = a'ac + b'bc$*. Como* a *divide a cada uno de los términos de la derecha, también divide a* c*.*

IV. Por último, tenemos la importante "descomposición en factores primos:"

Teorema. *Sea* A *un dominio de ideales principales con cuerpo de fracciones* K*. Existe un subconjunto* P *de* A *tal que todo* $x \in \mathrm{K}$ *se escribe de forma única*

$$x = u \prod_{p \in \mathrm{P}} p^{v_p(x)} \tag{6}$$

donde u *es un elemento inversible de* A *y los exponentes* $v_p(x)$ *son elementos de* $\mathbf{Z}$*, todos nulos salvo un número finito.*

> *Para una presentación más sistemática de estas cuestiones, enviamos al lector a* [**13**]*, Algèbre, capítulo VI, §1 y capítulo VII, §1. Una parte de la teoría (más precisamente, todo aquello que no depende de la identidad de Bezout) se extiende a anillos más generales que los dominios de ideales principales, a saber los* **dominios de factorización única;** *ver* [**19**]*, o* [**14**] *Algèbre commutative, capítulo VII, §3.*

[2]N. del T.: cota inferior maximal.

2. Un ejemplo: las ecuaciones $x^2+y^2=z^2$ y $x^4+y^4=z^4$

Una de las partes más atractivas de la Teoría de Números es el estudio de las **ecuaciones diofánticas.** Se consideran ecuaciones polinomiales $P(x_1,\ldots,x_n)=0$ con coefficientes en $\mathbf{Z}$ (resp. en $\mathbf{Q}$) de las cuales se buscan soluciones (x_i) enteras (resp. racionales). Podemos reemplazar $\mathbf{Z}$ (resp. $\mathbf{Q}$) por anillos A (resp. cuerpos K) más generales. Veremos un ejemplo de esto más tarde (§6).

Estudiaremos aquí dos casos particulares de la famosa **ecuación de Fermat:**

$$x^n+y^n=z^n. \tag{1}$$

Fermat afirmó haber demostrado que, si $n\geq 3$, esta ecuación no tiene soluciones (x,y,z) con x,y,z números enteros no nulos; su demostración nunca se encontró. Numerosos matemáticos trabajaron intensamente desde entonces en este problema y mostraron que la afirmación de Fermat es verdadera para un gran número de valores del exponente n. Sin embargo, todavía no se ha encontrado una demostración general (i.e. válida para todo n).

> *La opinión actual más usual es que, en su "demostración", Fermat había cometido un error, pero un error digno de un matemático de primer orden. Por ejemplo, tal vez tuvo le idea (genial para su época) de trabajar en el anillo de enteros del cuerpo de raíces n-ésimas de la unidad y creyó que este anillo era siempre un dominio de ideales principales. Efectivamente, se sabe demostrar la afirmación de Fermat para todo exponente n tal que este anillos es un dominio de ideales principales. Pero no lo es para todo n; de hecho, si n es primo, este anillo sólo es un dominio de ideales principales para un número finito de valores de n*[1].

Si $n=2$, la ecuación (1) tiene soluciones enteras, por ejemplo (3,4,5). Podemos describir completamente todas las soluciones:

Teorema 1. *Si x, y, z son enteros ≥ 1 tales que $x^2+y^2=z^2$, existe un entero d y enteros coprimos u, v tales que (salvo una permutación de x e y) se tiene:*

$$x=d(u^2-v^2)\quad y=2duv\quad z=d(u^2+v^2) \tag{2}$$

[1]Ver C.L. Siegel — "Gesamelte Weke", t. III, p. 436–442.

Un cálculo fácil muestra que las fórmulas (2) dan soluciones de $x^2+y^2=z^2$. Recíprocamente, sean x, y, z enteros ≥ 1 tales que $x^2+y^2=z^2$. Dividiendo x, y, z por su m.c.d. podemos suponer que son coprimos entre sí. En este caso también son coprimos dos a dos. En efecto, si, por ejemplo, x y z tiene un factor común p, entonces p divide a $y^2=z^2-x^2$ y por lo tanto divide a y. En particular, dos de los números x, y, z son impares y el tercero es necesariamente par. Los números x e y no pueden ser ambos impares, pues sino se tendría $x^2\equiv 1 \pmod 4$, $y^2\equiv 1 \pmod 4$ de donde $z^2\equiv 2 \pmod 4$, lo que contradice el hecho de que z^2 es un cuadrado. Por lo tanto se tiene, eventualmente intercambiando x e y, que

$$x \text{ es impar, } y \text{ es par, } z \text{ es impar.} \tag{3}$$

Escribamos la ecuación de la siguiente forma

$$y^2=z^2-x^2=(z-x)(z+x). \tag{4}$$

Como el m.c.d. de $2x$ y $2z$ es 2, y $2x=(z+x)-(z-x)$ y $2z=(z+x)+(z-x)$, el m.c.d. de $z-x$ y $z+x$ no puede ser otro que 2. Sea $y=2y'$, $z+x=2x'$, $z-x=2z'$, donde y', x', z' son enteros, pues y, $z+x$ y $z-x$ son pares por (3). Se tiene luego que $y'^2=x'z'$. Como x' y z' son coprimos, la descomposición en factores primos de y'^2 muestra que x' y z' son **cuadrados** u^2 y v^2: en efecto, todo factor primo de y'^2 aparece completamente, con su exponente par, o bien en x' o bien en z'. Se tiene por lo tanto que $z+x=2u^2$, $z-x=2v^2$, $y^2=2u^2\cdot 2v^2$, de donde $x=u^2-v^2$, $y=2uv$, $z=u^2+v^2$. Aquí, u y v son coprimos, pues sino x, y, z tendrían un factor primo en común. Las fórmulas (2) se deducen multiplicando de nuevo el m.c.d. por d.

Teorema 2. *La ecuación $x^4+y^4=z^2$ no tiene soluciones en números enteros $x,y,z\geq 1$.*

Razonemos por el absurdo. Se tiene entonces una solución (x,y,z) donde z es **minimal.** En este caso, x, y y z son coprimos dos a dos. En efecto, si, por ejemplo, x e y tuvieran un factor primo en común p, entonces p^4 dividiría a z^2, por lo que p^2 dividiría a z, y $\left(\frac{x}{p},\frac{y}{p},\frac{z}{p^2}\right)$ sería otra solución, contradiciendo la minimalidad de z. Los otros dos casos son análogos e incluso más fáciles.

Como nuestra ecuación se puede escribir $(x^2)^2+(y^2)^2=z^2$, podemos aplicar el teorema 1: después de, eventualmente, permutar x e y, existen enteros $u,v\geq 1$ coprimos tales que

$$x^2=u^2-v^2, \quad y^2=2uv, \quad z=u^2+v^2. \tag{5}$$

Como $4 \mid y^2$, la relación $y^2=2uv$ muestra que uno de los números u y v es par; el otro es necesariamente impar. La condición "u par, v impar" implica

$u^2 \equiv 0 \pmod 4$, $v^2 \equiv 1 \pmod 4$, de donde $x^2 = u^2 - v^2 \equiv -1 \pmod 4$, lo que es absurdo. Luego, u es impar y $v = 2v'$. La relación $y^2 = 4uv'$ y el hecho de que u y v' son coprimos muestran que u y v' son dos cuadrados a^2 y b^2. Apliquemos de nuevo el teorema 1, esta vez a la ecuación $x^2 + v^2 = u^2$ (cf. (5)); como x y u son impares, v par, y x, v, u coprimos dos a dos, existen enteros coprimos c,$d \geq 1$ tales que

$$x = c^2 + d^2, \quad v = 2cd, \quad u = c^2 = d^2. \tag{6}$$

Luego, de $v = 2v' = 2b^2$, deducimos $cd = b^2$, de manera que c y d son nuevamente cuadrados x'^2 e y'^2, pues son coprimos. Como $u = a^2$, la última ecuación de (6) se escribe

$$a^2 = x'^4 + y'^4 \tag{7}$$

que tiene **la misma forma** que la ecuación original. Por otra parte, se tiene, por (5), $z = u^2 + v^2 = a^4 + 4b^4 > a^4$, de donde $z > a$, lo que contradice el caracter minimal de z. El teorema está demostrado.

> *Una ligera variante de nuestra demostración muestra como, dada una solución* (x,y,z) *en enteros* ≥ 1 *de* $x^4 + y^4 = z^2$*, construir una sucesión* (x_n,y_n,z_n) *infinita de tales soluciones, donde la sucesión* z_n *es estrictamente decreciente, lo que es un absurdo. Este es el método de* **descenso infinito** *de Fermat.*

Corolario. *La ecuación* $x^4+y^4 = z^4$ *no admite soluciones enteras* $x,y,z \geq 1$.

En efecto, esta ecuación puede escribirse $x^4+y^4 = (z^2)^2$ y podemos aplicar el teorema 2.

3. Algunos lemas sobre ideales; la función φ de Euler

Sea $n \geq 1$ un entero natural. Llamamos **función de Euler** de n, y notamos $\varphi(n)$, al número de enteros q, coprimos con n, tales que $0 \leq q \leq n$ (equivalentemente, $1 \leq q \leq n-1$, pues 0 y n no son coprimos con n). Si p es un número primo, es claro que

$$\varphi(p) = p - 1. \tag{1}$$

Si $n = p^s$, una potencia de un número primo, los enteros coprimos a p^s son aquellos que no son múltiplos de p. Como hay p^{s-1} múltiples de p entre 1 y p^s, se tiene

$$\varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1). \tag{2}$$

Nos proponemos ahora calcular $\varphi(n)$ utilizando la descomposición de n en factores primos. Para ello, nos hace falta una caracterización de $\varphi(n)$ y algunos lemas sobre los ideales que también nos serán útiles más adelante.

Proposición 1. *Sea $n \geq 1$ un entero natural. El valor de la función de Euler $\varphi(n)$ es igual al número de generadores de $\mathbf{Z}/n\mathbf{Z}$ y también igual al número de elementos inversibles del anillo $\mathbf{Z}/n\mathbf{Z}$.*

Recordemos que cada clase de congruencia mod $n\mathbf{Z}$ contiene un único entero q tal que $0 \leq q \leq n-1$. Para un tal entero q, notemos $\overline{q}$ su clase mod $n\mathbf{Z}$. Razonando "en círculo", basta demostrar las implicaciones: q coprimo con $n \Rightarrow \overline{q}$ inversible $\Rightarrow \overline{q}$ genera $\mathbf{Z}/n\mathbf{Z} \Rightarrow q$ coprimo con n.

Si q es coprimo con n, la identidad de Bezout (§1, (2)) muestra que existen enteros x e y tales que $qx + ny = 1$, de donde $\overline{q} \cdot \overline{x} = \overline{1}$ y $\overline{q}$ es inversible.

Si $\overline{q}$ es inversible, notemos x a un entero tal que $\overline{q} \cdot \overline{x} = 1$. Si $\overline{a}$ es un elemento cualquier de $\mathbf{Z}/n\mathbf{Z}$ y si a es un representante de $\overline{a}$, tenemos $\overline{a} = \overline{ax}\overline{q}$ (en el anillo $\mathbf{Z}/n\mathbf{Z}$), de donde $\overline{a} = (ax) \cdot \overline{q}$ (en el grupo aditivo $\mathbf{Z}/n\mathbf{Z}$). Por lo tanto $\overline{q}$ genera el grupo $\mathbf{Z}/n\mathbf{Z}$.

Finalmente, si $\overline{q}$ genera $\mathbf{Z}/n\mathbf{Z}$, existe un entero x tal que $x \cdot \overline{q} = \overline{1}$. Luego, tal que $xq \equiv 1 \pmod{n}$. Es decir, existe un entero y tal que $xq - 1 = yn$, de donde $1 = xq - yn$. Esta es una identidad de Bezout que muestra que q es coprimo con n.

Lema 1. *Sean* A *un anillo,* $\mathfrak{a}$ *y* $\mathfrak{b}$ *dos ideal de* A *tales que* $\mathfrak{a} + \mathfrak{b} = \mathrm{A}$. *Luego,* $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ *y el homomorfismo canónico* $\varphi : \mathrm{A} \to \mathrm{A}/\mathfrak{a} \times \mathrm{A}/\mathfrak{b}$ *define un isomorfismo* $\theta : \mathrm{A}/\mathfrak{ab} \to \mathrm{A}/\mathfrak{a} \times \mathrm{A}/\mathfrak{b}$.

> *Recordemos que el homomorfismo φ le hace corresponder a cada $x \in \mathrm{A}$ el par formado por la clase de x* mod $\mathfrak{a}$ *y la clase de y* mod $\mathfrak{b}$.

En general, se tiene que $\mathfrak{ab} \subset \mathfrak{a}$ y $\mathfrak{ab} \subset \mathfrak{b}$, de donde $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Sea ahora $x \in \mathfrak{a} \cap \mathfrak{b}$. Como $\mathfrak{a} + \mathfrak{b} = \mathrm{A}$, existen elementos $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ tales que $a + b = 1$. Luego, $x = ax + xb$ es suma de dos elementos de $\mathfrak{ab}$, de donde $x \in \mathfrak{ab}$ y $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$. Luego, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.

Está claro que el núcleo de φ es $\mathfrak{a} \cap \mathfrak{b}$. Como $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, φ es constante en cada clase de equivalencia mod $\mathfrak{ab}$, por lo que se tiene la función $\theta : \mathrm{A}/\mathfrak{ab} \to \mathrm{A}/\mathfrak{a} \times \mathrm{A}/\mathfrak{b}$. Esta función es evidentemente un homomorfismo. Como $\varphi^{-1}(0) = \mathfrak{ab}$, tenemos que $\theta^{-1}(0) = (0)$ y luego θ es inyectiva. Falta mostrar que θ es sobreyectiva.

Hemos explicado con detalle este argumento de "pasaje al cociente" a modo de ilustración. En lo que sigue, seremos bastante más breves al realizar razonamientos análogos.

Para mostrar la sobreyectividad de θ (o, lo que es lo mismo, de φ) debemos construir un elemento x de A tal que su clase módulo $\mathfrak{a}$ y su clase módulo $\mathfrak{b}$ puedan elegirse arbitrariamente. Sean y y z dos representantes de tales clases. Existen elementos $x \in \mathfrak{a}$ y $b \in \mathfrak{b}$ tales que $a + b = 1$. Definimos $x = az + by$. Modulo $\mathfrak{a}$, se tiene $x \equiv by \equiv (1 - a)y \equiv y - ay \equiv y$; intercambiando x e y, deducimos que $x \equiv z \bmod \mathfrak{b}$. LQQD.

Lema 2. *Sean* A *un anillo y* $(\mathfrak{a}_i)_{1 \leq i \leq r}$ *una colección finita de ideales de* A *tal que* $\mathfrak{a}_i + \mathfrak{a}_j = \mathrm{A}$ *si* $i \neq j$. *Se tiene entonces un isomorfismo canónico de* $\mathrm{A}/\mathfrak{a}_1 \cdots \mathfrak{a}_r$ *sobre* $\prod_{i=1}^{r} \mathrm{A}/\mathfrak{a}_i$.

El lema 1 es el caso $r = 2$ del lema 2. Procedemos por indución en r a partir de este caso. Sea $\mathfrak{b} = \mathfrak{a}_2 \cdots \mathfrak{a}_r$ y mostremos que $\mathfrak{a}_1 + \mathfrak{b} = \mathrm{A}$. En efecto, si $i \geq 2$, tenemos $\mathfrak{a}_1 + \mathfrak{a}_i = \mathrm{A}$ por lo que existen elementos $c_i \in \mathfrak{a}_1$ y $a_i \in \mathfrak{a}_i$ tales que $c_i + a_i = 1$. Multiplicando miembro a miembro, se tiene que $c + a_2 \ldots a_n = 1$, donde c es una suma de términos donde cada término contiene al menos un c_i como factor. Luego, $c \in \mathfrak{a}_1$. Como $a_2 \cdots a_r \in \mathfrak{b}$, obtenemos que $\mathfrak{a}_1 + \mathfrak{b} = \mathrm{A}$.

Por el lema 1, se tiene un isomorfismo $\mathrm{A}/\mathfrak{a}_1\mathfrak{b} \sim \mathrm{A}/\mathfrak{a}_1 \times \mathrm{A}/\mathfrak{b}$. Por la hipótesis inductiva, se tiene un isomorfismo

$$\mathrm{A}/\mathfrak{b} = \mathrm{A}/\mathfrak{a}_2 \cdots \mathfrak{a}_r \sim (\mathrm{A}/\mathfrak{a}_2) \times \cdots \times (\mathrm{A}/\mathfrak{a}_r).$$

Componiendo estos isomorfismos se obtiene el resultado. LQQD.

Ahora aplicamos estos resultados al anillo $\mathbf{Z}$:

Proposición 2. *Sean* n *y* n' *dos enteros coprimos. Entonces el anillo* $\mathbf{Z}/nn'\mathbf{Z}$ *es isomorfo al anillo producto* $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n'\mathbf{Z}$.

Este es un caso particular del lema 2, ya que la hipótesis $n\mathbf{Z} + n'\mathbf{Z} = \mathbf{Z}$ no es otra cosa que la identidad de Bezout.

Corolario 1. *Si* n *y* n' *son dos enteros* ≥ 1 *coprimos, se tiene que* $\varphi(nn') = \varphi(n)\varphi(n')$.

En efecto, $\varphi(nn')$ es el número de elementos inversibles del anillo $\mathbf{Z}/nn'\mathbf{Z}$ (proposición 1), que es isomorfo a $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n'\mathbf{Z}$. Ahora bien, un elemento (α,β) de un anillo producto es inversible si y sólo si cada uno de sus componentes α y β es inversible. Aplicando la proposición 1 se obtiene el resultado.

Corolario 2. *Sea n un entero ≥ 1 y $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ su descomposición en factores primos. Entonces $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$.*

Por el corolario 1, se tiene $\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$. Por (2), se tiene $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$. Multiplicando obtenemos la fórmula deseada.

4. Algunos preliminares sobre módulos

Para poder estudiar los módulo sobre un dominio de ideales principales, nos harán falta algunos preliminares.

Dado un anillo A y un conjunto I notamos $\mathrm{A}^{(\mathrm{I})}$ el conjunto de las familias $(a_i)_{i\in \mathrm{I}}$, indexadas por I, de elementos de A **tales que** $a_i = 0$ salvo un número **finito** de índices $i \in \mathrm{I}$. De manera que $\mathrm{A}^{(\mathrm{I})}$ es un subconjunto del conjunto producto A^{I}, y un submódulo de A^{I} si dotamos a A^{I} de la estructura de A-módulo inducida por sus factores.

Si I is finito, se tiene $\mathrm{A}^{(\mathrm{I})} = \mathrm{A}^{\mathrm{I}}$.

Para $j \in \mathrm{I}$, la familia $(\delta_{ji})_{i\in \mathrm{I}}$ definida por $\delta_{jj} = 1$ y $\delta_{ji} = 0$ si $i \neq j$, es un elemento e_j de $\mathrm{A}^{(\mathrm{I})}$. Todo elemento $(a_j)_{j\in \mathrm{I}}$ de $\mathrm{A}^{(\mathrm{I})}$ se escribe de una forma única como combinación lineal (finita) de los e_j. Más precisamente:

$$(a_j)_{j\in \mathrm{I}} = \sum_{j\in \mathrm{I}} a_j e_j \tag{1}$$

(observemos que, en la suma de la derecha, casi todos los términos son cero salvo un número finito, de manera que la suma tiene sentido). Decimos que $(e_j)_{j\in \mathrm{I}}$ es la **base canónica** de $\mathrm{A}^{(\mathrm{I})}$.

Sea A un anillo, M un A-módulo y $(x_i)_{i\in \mathrm{I}}$ una familia de elementos de M. A todo elemento $(a_i)_{i\in \mathrm{I}}$ de $\mathrm{A}^{(\mathrm{I})}$ le hacemos corresponder el elemento $\sum_i a_i x_i$ de M (como antes, la suma tiene sentido). De esta manera hemos definido una aplicación $\varphi : \mathrm{A}^{(\mathrm{I})} \to \mathrm{M}$ que es evidentemente **lineal.** Si $(e_i)_{i\in \mathrm{I}}$ es la base canónica de $\mathrm{A}^{(\mathrm{I})}$, se tiene $\varphi(e_i) = x_i$ para todo $i \in \mathrm{I}$.

Las equivalencias siguientes son inmediatas:

(2) los x_i son linealmente equivalentes $\iff$ φ es inyectiva.

(3) $(x_i)_{i\in \mathrm{I}}$ son un sistema de generadores $\iff$ φ es sobreyectiva.

Si φ es **biyectiva**, decimos que $(x_i)_{i\in \mathrm{I}}$ es una **base** de M. Esto quiere decir que todo elemento x de M se escribe, **de manera única,** como combinación lineal de los x_i. Un módulo M que admite una base se llama un **módulo libre.**

Contrariamente a lo que ocurre con los espacios vectoriales sobre un cuerpo, un módulo sobre un anillo no admite necesariamente una base. Por ejemplo, el $\mathbf{Z}$*-módulo* $\mathbf{Z}/n\mathbf{Z}$ *con* $n \neq 0{,}1$ *no es libre. En lo que sigue demostraremos que ciertos módulos son libres; un resultado de este tipo es raramente trivial.*

Un módulo se dirá **de tipo finito** si admite un sistema finito de generadores. El siguiente teorema es básico para el estudio de los anillos y módulos noetherianos, que estudiaremos más a fondo en el capítulo III.

Teorema 1. *Sea* A *un anillo,* M *un* A*-módulo. Las siguientes condiciones son equivalentes:*

1. *Toda familia no vacía de submódulos de* M *posee un elemento maximal (para la relación de inclusión);*
2. *Toda sucesión creciente* $(\mathrm{M}_n)_{n\geq 0}$ *(para la relación de inclusión) de submódulos de* M *se estaciona (es decir, existe* n_0 *tal que* $\mathrm{M}_n = \mathrm{M}_{n_0}$ *para todo* $n \geq n_0$*);*
3. *Todo submódulo de* M *es de tipo finito.*

Mostremos que a) implica c). Sea E un submódulo de M y sea Φ la familia de submódulos de tipo finito de E. Φ no es vacía pues $\{0\} \in \Phi$. Por a), Φ admite un elemento maximal F. Si $x \in \mathrm{E}$, $\mathrm{F} + \mathrm{A}x$ es un submódulo de tipo finito de E (generado por la unión de $\{x\}$ y un sistema finito de generadores de F). Luego tenemos $\mathrm{F} + \mathrm{A}x = \mathrm{F}$ pues $\mathrm{F} + \mathrm{A}x \supset \mathrm{F}$ y F es maximal. Por lo tanto, $x \in \mathrm{F}$, $\mathrm{E} \subset \mathrm{F}$, $\mathrm{E} = \mathrm{F}$ y E es de tipo finito.

Probemos ahora que c) implica b). Sea $(\mathrm{M}_n)_{n\geq 0}$ una sucesión creciente de submódulos de M. Luego $\mathrm{E} = \bigcup_{n\geq 0} \mathrm{M}_n$ es un submódulo de M. Por c), E admite un sistema finito de generadores $(x_1, \ldots, x_q)$. Para todo i, hay un índice $n(i)$ tal que $x_i \in \mathrm{M}_{n(i)}$. Sea n_0 el más grande de los $n(i)$. Tenemos $x_i \in \mathrm{M}_{n_0}$ para todo i, de donde $\mathrm{E} \subset \mathrm{E}_{n_0}$ y $\mathrm{E} = \mathrm{M}_{n_0}$. Para $n \geq n_0$, las inclusiones $\mathrm{M}_{n_0} \subset \mathrm{M}_n \subset \mathrm{E}$ y la igualdad $\mathrm{M}_{n_0} = \mathrm{E}$ muestran que $\mathrm{M}_{n_0} = \mathrm{M}_n$. Luego la sucesión (M_n) se estaciona a partir de n_0.

Falta demostrar que b) implica a). La equivalencia de a) y b) es un caso particular del siguiente lema sobre los conjuntos ordenados:

Lema 1. *Sea* T *un conjunto ordenado. Las siguientes condiciones son equivalentes:*

a) *Toda familia no vacía de elementos de* T *admite un elemento maximal;*
b) *Toda sucesión creciente* $(t_n)_{n\geq 0}$ *de elementos de* T *se estaciona.*

a) $\Rightarrow$ *b*): Sea t_q un elemento maximal de la sucesión creciente (t_n). Si $n \geq q$ tenemos $t_n \geq t_q$ (la sucesión es creciente), luego $t_n = t_q$ (el elemento t_q es maximal).

b) $\Rightarrow$ *a*). Supongamos que S es un subconjunto no vacío de T sin ningún elemento maximal. Luego, si $x \in$ S, el conjunto de elementos de S estrictamente superiores a x es no vacío. Por el axioma de elección, existe una aplicación $f : \mathrm{S} \to \mathrm{S}$ tal que $f(x) > x$ para todo $x \in$ S. Como S es no vacío, podemos elegir $t_0 \in$ S y definir por recurrencia la sucesión $(t_n)_{n\geq 0}$ por $t_{n+1} = f(t_n)$. Esta sucesión es estrictamente creciente, luego no se estaciona. De esta manera, hemos demostrado la implicación b) $\Rightarrow$ a) por el contrapositivo. LQQD.

Corolario del teorema 1. *En un dominio de ideales principales* A *toda familia no vacía de ideales admite un elemento maximal.*

En efecto, si consideramos a A como un módulo sobre si mismo, sus submódulos son precisamente sus ideales. Como estos son todos principales, son A-módulos generados por un sólo elemento, luego son de tipo finito. Podemos aplicar entonces la implicación c) $\Rightarrow$ a) del teorema 1.

5. Módulos sobre dominios de ideales principales

Sea A un dominio íntegro y K su cuerpo de fracciones. Un A-módulo libre, en particular isomorfo a un $\mathrm{A}^{(\mathrm{I})}$, puede incluirse en un espacio vectorial sobre K ($\mathrm{K}^{(\mathrm{I})}$ en el caso de $\mathrm{A}^{(\mathrm{I})}$). Por lo tanto lo mismo es cierto para todo submódulo M de un A-módulo libre. La dimensión del subespacio generado por M se llama el **rango** de M. Es el número máximo de elementos linealmente independientes de M. Si el propio M es libre y admite una base con n elementos, entonces el rango de M es igual a n.

Teorema 1. *Sea* A *un dominio de ideales principales,* M *un* A*-módulo libre de rango finito* n *y* M' *un submódulo de* M*. Entonces:*

1. M' *es libre, de rango* $\leq n$*;*
2. *Existe una base* $(e_1, \ldots, e_n)$ *de* M*, un entero* $q \leq n$ *y elementos no nulos* $a_1, \ldots, a_q$ *de* A *tales que* $(a_1 e_1, \ldots, a_q e_q)$ *es una base de* M' *y tal que* a_i *divide a* a_{i+1} *para todo* $1 \leq i \leq q-1$*.*

Como el teorema es trivial si $\mathrm{M}' = \{0\}$, podemos suponer que $\mathrm{M}' \neq \{0\}$. Sea L(M,A) el conjunto de formas lineales de M. Si $u \in$ L(M,A), $u(\mathrm{M}')$ es un sub-A-módulo de A, es decir un ideal de A. Podemos escribir $u(\mathrm{M}') = \mathrm{A}a_u$ para algún $a_u \in$ A pues todos los ideales son principales. Sea $u \in$ L(M,A) tal que $\mathrm{A}a_u$ es **maximal** entre los $\mathrm{A}a_v$ ($v \in$ L(M,A)) (§4, corolario del teorema 1). Tomemos una base $(x_1, \ldots, x_n)$ de M de manera de identificar M con A^n. Sea

$\mathrm{pr}_i : \mathrm{M} \to \mathrm{A}$ la i-ésima proyección coordenada, definida por $\mathrm{pr}_i(x_j) = \delta_{ij}$. Como $\mathrm{M}' \neq \{0\}$, alguno de los $\mathrm{pr}_i(\mathrm{M}')$ es $\neq \{0\}$. Por lo tanto $a_u \neq 0$. Por construcción, existe $e' \in \mathrm{M}'$ tal que $u(e') = a_u$. Mostremos que, **para todo** $v \in \mathrm{L(M,A)}$, a_u **divide a** $v(e')$. En efecto, si d es el m.c.d. de a_u y $v(e')$, se tiene $d = ba_u + cv(e')$ para algunos b,$c \in \mathrm{A}$, de donde $d = (bu + cv)(e')$. Como $bu + cv$ es una forma lineal w en M, se sigue que $\mathrm{A}a_u \subset \mathrm{A}d \subset w(\mathrm{M}')$. La maximalidad de $\mathrm{A}a_u$ implica que $\mathrm{A}d = \mathrm{A}a_u$ de manera que a_u divide a $v(e')$.

En particular, a_u divide a todos los $\mathrm{pr}_i(e')$ y podemos escribir $\mathrm{pr}(e') = a_u b_i$ para algún $b_i \in \mathrm{A}$. Sea $c = \sum_{i=1}^{n} b_i x_i$. Se tiene $e' = a_u e$. Como $u(e') = a_u = a_u \cdot u(e)$, se sigue que $u(e) = 1$ (recordar que $a_u \neq 0$). *Mostremos ahora que*

$$\mathrm{M} = \mathrm{A}e + \mathrm{Ker}(u) \tag{1}$$

$$\mathrm{M}' = \mathrm{A}e' + (\mathrm{M}' \cap \mathrm{Ker}(u)) \quad (\textit{donde } e' = a_u e) \tag{2}$$

donde las sumas son directas. En efecto, todo $x \in \mathrm{M}$ se escribe $x = u(x)e + (x - u(x)e)$ y se tiene $u(x - u(x)e) = u(x) - u(x)u(e) = 0$, lo que demuestra (1). Si $y \in \mathrm{M}'$, se tiene $u(y) = ba_u$ para algún $b \in \mathrm{A}$, y por lo tanto

$$y = ba_u e + (y - u(y)e) = be' + (y - u(y)e).$$

Además, $y - u(y)e \in \mathrm{Ker}(u)$ y también $y - u(y)e = y - be' \in \mathrm{M}'$, lo que demuestra (2). Finalmente, para mostrar que las sumas son directas, basta ver que $\mathrm{A}e \cap \mathrm{Ker}(u) = \{0\}$. Pero, si $x = ce$ es un elemento de $\mathrm{A}e$ ($c \in \mathrm{A}$) y si además $u(x) = 0$, se tiene $c = cu(e) = u(ce) = u(x) = 0$, de donde $x = 0$.

Ahora demostraremos a) haciendo inducción en el rango q de M'. Si $q = 0$, se tiene $\mathrm{M}' = \{0\}$ y todo es trivial. Si $q > 0$, $\mathrm{M}' \cap \mathrm{Ker}(u)$ es de rango $q - 1$ por (2), y por lo tanto es libre por la hipótesis inductiva. Como en (2) la suma es directa, obtenemos una base de M' agregando e' a una base de $\mathrm{M}' \cap \mathrm{Ker}(u)$. Por lo tanto M' es libre y vale a).

A continuación, demostraremos b) haciendo inducción en el rango n de M. Todo es trivial si $n = 0$. Por a), $\mathrm{Ker}(u)$ es libre y de rango $n - 1$ pues, en (1), la suma es directa. Apliquemos la hipótesis inductiva al módulo libre $\mathrm{Ker}(u)$ y a su submódulo $\mathrm{M}' \cap \mathrm{Ker}(u)$: existe $q \leq n$, una base $(e_2, \ldots, e_n)$ de $\mathrm{Ker}(u)$ y elementos no nulos $a_2, \ldots, a_q$ de A tales que $(a_2 e_2, \ldots, a_q e_q)$ es una base de $\mathrm{M}' \cap \mathrm{Ker}(u)$ y a_i divide a a_{i+1} para $2 \leq i \leq q - 1$. Utilizando la notación anterior, ponemos $a_1 = a_u$ y $e_1 = e$. Luego $(e_1, e_2, \ldots, e_n)$ es una base de M por (1) y $(a_1 e_1, \ldots, a_q e_q)$ es una base de M' (por (2) y porque $e' = a_1 e_1$). Sólo resta mostrar la divisibilidad $a_1 \mid a_2$. Sea v la forma lineal en M definida por $v(e_1) = v(e_2) = 1$, $v(e_i) = 0$ para $i \geq 3$. Se tiene $a_1 = a_u = v(a_u e_1) = v(e') \in v(\mathrm{M}')$, de donde $\mathrm{A}a_u \subset v(\mathrm{M}')$. Por la maximalidad de $\mathrm{A}a_u$ se deduce

que $v(\mathrm{M}') = \mathrm{A}a_u = \mathrm{A}a_1$; como $a_2 = v(a_2e_2) \in v(\mathrm{M}')$, se tiene que $a_2 \in \mathrm{A}a_1$, es decir, $a_1 \mid a_2$. LQQD.

Los ideales $\mathrm{A}a_i$ *del Teorema 1 se llaman* **factores invariantes** *de* M' *en* M. *Puede demostrarse que están unívocamente determinados por* M *y* M' *(*[**13**]*, Capítulo VII, §3).*

Corolario 1. *Sea* A *un dominio de ideales principales y* E *un* A*-módulo de tipo finito. Entonces* E *es isomorfo a un producto* $(\mathrm{A}/\mathfrak{a}_1) \times (\mathrm{A}/\mathfrak{a}_2) \times \cdots \times (\mathrm{A}/\mathfrak{a}_n)$*, donde los* $\mathfrak{a}_i$ *son ideales de* A *tales que* $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n$.

Sea, en efecto, $(x_1, \ldots, x_n)$ un sistema de generadores de E. Por lo visto al comienzo de §4, se tiene un homomorfismo sobreyectivo $\varphi : \mathrm{A}^n \to \mathrm{E}$, de manera que E es isomorfo a $\mathrm{A}^n/\operatorname{Ker}(\varphi)$. Por el teorema 1, existe una base $(e_1, \ldots, e_n)$ de A^n, un entero $q \leq n$, y elementos no nulos $a_1, \ldots, a_q$ de A tales que $(a_1e_1, \ldots, a_qe_q)$ es una base de $\operatorname{Ker}(\varphi)$ y a_i divide a a_{i+1} para todo $1 \leq i \leq q-1$. Definimos $a_p = 0$ si $q+1 \leq p \leq n$. Luego $\mathrm{A}^n/\operatorname{Ker}(\varphi)$ es isomorfo al producto de los $\mathrm{A}e_i/\mathrm{A}a_ie_i$ $(1 \leq i \leq n)$ y $\mathrm{A}e_i/\mathrm{A}a_ie_i$ es isomorfo a $\mathrm{A}/\mathrm{A}a_i$. Poniendo $\mathfrak{a}_i = \mathrm{A}a_i$, se obtiene el resultado. LQQD.

Diremos que un módulo E sobre un dominio íntegro A es **libre de torsión** si la relación $ax = 0$ $(a \in \mathrm{A},\ x \in \mathrm{E})$ implica $a = 0$ o $x = 0$.

Corolario 2. *Todo módulo* E *libre de torsion y de tipo finito sobre un dominio de ideales principales es libre.*

Aplicamos el corolario 1: $\mathrm{E} \sim (\mathrm{A}/\mathfrak{a}_1) \times \cdots \times (\mathrm{A}/\mathfrak{a}_n)$. Suprimiendo los factores nulos, podemos suponer que $\mathfrak{a}_i \neq \mathrm{A}$ para todo i. Si $\mathfrak{a}_1 \neq (0)$, a es un elemento no nulo de $\mathfrak{a}_1$, x_1 es un elemento no nulo de $\mathrm{A}/\mathfrak{a}_1$ y $x = (x_1, 0, \ldots, 0)$, se sigue que $ax = 0$, lo que contradice el hecho de que E es libre de torsión. Luego, $\mathfrak{a}_1 = (0)$, $\mathfrak{a}_i = (0)$ para todo i (pues $\mathfrak{a}_i \subset \mathfrak{a}_1$) y E es isomorfo a A^n.

La hipótesis de que E *es de tipo finito es imprescindible: por ejemplo,* $\mathbf{Q}$ *es un* $\mathbf{Z}$*-módulo libre de torsion que no es libre.*

Corolario 3. *Sobre un dominio de ideales principales, todo módulo* E *de tipo finito es isomorfo a un producto finito de módulos* M_i*, donde cada* M_i *es igual a* A *o a un cociente* $\mathrm{A}/\mathrm{A}p^s$ *con* p *primo.*

Utilizamos el corolario 1, y descomponemos cada factor $\mathrm{A}/\mathrm{A}a$ con $a \neq 0$ mediante §3, lema 2: si $a = up_1^{s_1} \ldots p_r^{s_r}$ es la descomposición en factores primos de a, $\mathrm{A}/\mathrm{A}a$ es isomorfo al producto de los $\mathrm{A}/\mathrm{A}p_i^{s_i}$.

Corolario 4. *Sea* G *un grupo conmutative finito. Existe* $x \in \mathrm{G}$ *tal que su orden el el m.c.m. de los órdenes de los elementos de* G.

Un grupo conmutativo es un $\mathbf{Z}$-módulo (si lo escribimos aditivamente). Por el corolario 1, tenemos $\mathrm{G} \simeq \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$ con $a_1 \mid a_2 \mid \cdots \mid a_n$. Ninguno de los a_i es nulo, pues sino G sería infinito. Notemos y la clase de 1 en $\mathbf{Z}/a_n\mathbf{Z}$ y pongamos $x = (0,\ldots,0,y)$. El orden de x es evidentemente a_n. Si $z = (z_1,\ldots,z_n) \in \mathrm{G}$, tenemos $a_n z = 0$ pues a_i divide a_n para todo i. Luego, a_n es un múltiplo del orden de z. Por lo tanto, el elemento buscado es x.

6. Raíces de la unidad en un cuerpo

Teorema 1. *Sea* K *un cuerpo. Todo subgrupo finito* G *del grupo multiplicativo* $\mathrm{K}^\times$ *consiste de raíces de la unidad y es cíclico.*

En efecto, por el corolario 4 al teorema 1 de la §5, existe $z \in \mathrm{G}$ cuyo orden n es tal que $y^n = 1$ para todo $y \in \mathrm{G}$. Como un polinomio de grado n sobre un cuerpo (por ejemplo $\mathrm{X}^n - 1$) tiene a lo sumo n raíces en el cuerpo, el número de elementos de G es a lo sumo n. Pero, como z es de orden n, G contiene los n elementos $z, z^2, \ldots, z^n = 1$, que son todos distintos. Luego, G consiste de estos elementos y es cíclico.

Si un cuerpo K contiene n raíces n-ésimas de la unidad, éstas forman un grupo cíclico de orden n (isomorfo a $\mathbf{Z}/n\mathbf{Z}$). Un generador de este grupo se llama una **raiz primitiva n-ésima de la unidad;** toda raiz n-ésima de la unidad es por lo tanto una potencia de una tal raiz primitiva. De la proposición 1 de la §3, el número de estas raíces es $\varphi(n)$.

7. Cuerpos finitos

Sea K un cuerpo. Existe un único homomorfismo de anillos $\varphi : \mathbf{Z} \to \mathrm{K}$ (definido por $\varphi(n) = 1 + 1 + \cdots + 1$, n veces, si $n \geq 0$ y $\varphi(-n) = -\varphi(n)$).

- Si φ es inyectiva, $\mathbf{Z}$ se identifica con un subanillo de K. Luego K contiene el cuerpo de fracciones $\mathbf{Q}$ de $\mathbf{Z}$; decimos que K es **de característica** 0**.**
- Si φ no es inyectiva, su núcleo es un ideal $p\mathbf{Z}$ con $p > 0$. Luego $\mathbf{Z}/p\mathbf{Z}$ se identifica con un subanillo de K, necesariamente un dominio íntegro, por lo que p es un **número primo.** Decimos que K es **de característica** p**.** En este caso $\mathbf{Z}/p\mathbf{Z}$ es un cuerpo, que notamos $\mathbf{F}_p$.

  El subcuerpo, $\mathbf{Q}$ *o* $\mathbf{F}_p$*, es el subcuerpo más pequeño de* K*. Lo llamamos el* **subcuerpo primo** *de* K*.*

Para todo número primo p existen cuerpos de caractéristica p, por ejemplo $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Proposición 1. *Si* K *es un cuerpo de característica $p \neq 0$, se tiene $px = 0$ para todo $x \in \mathrm{K}$ y $(x+y)^p = x^p + y^p$ para todo $x, y \in \mathrm{K}$.*

Si $x \in \mathrm{K}$, se tiene $p \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0$. Por otra parte, de la fórmula del binomio, se tiene $(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}$; el coeficiente binomial $\binom{p}{j}$ es el entero $\frac{p!}{j!(p-j)!}$. Como el número primo p aparece como factor en el numerador y no aparece en el denominador, $\binom{p}{j}$ es múltiplo de p para $1 \leq j \leq p-1$. Luego el término correspondiente es nulo.

Por inducción en n se tiene $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ para todo $n \geq 0$.

Teorema 1. *Sea* K *un cuerpo finito. Sea $q = \mathrm{card}(\mathrm{K})$. Entonces:*

a) *La característica de* K *es un número primo p,* K *es un espacio vectorial de dimensión finita s sobre $\mathbf{F}_p$ y se tiene $q = p^s$.*
b) *El grupo multiplicativo* K^* *es cíclico de orden $q-1$.*
c) *Se tiene $x^{q-1} = 1$ para todo $x \in \mathrm{K}^*$ y $x^q = x$ para todo $x \in \mathrm{K}$.*

Efectivamente, como $\mathbf{Z}$ es infinito, K no puede ser de característica 0. Por lo tanto, K contiene $\mathbf{F}_p$ para algún primo p. Por lo tanto K es un espacio vectorial sobre $\mathbf{F}_p$. Su dimensión s es finita pues sino K sería infinito. Como espacio vectorial, K es isomorfo a $(\mathbf{F}_p)^s$, luego tiene p^s elementos. La parte b) se sigue del teorema 1 de la §6. La parte c) es inmediata.

Ejemplo. Apliquemos b) a $\mathbf{F}_p$, donde p es primo: existe un entero $x \in \mathbf{Z}$ tal que $0 \leq x \leq p-1$ y tal que todo entero y que no es múltiplo de p es congruente a una potencia de x módulo p. Decimos que x es **una raíz primitiva módulo p.** La determinación de raíces primitivas módulo p no es un asunto completamente trivial. Por ejemplo, hay $\varphi(6) = 2$ raíces primitivas módulo 7: el 3 y el 5 (en efecto, se tiene $1^2 \equiv 6^2 \equiv 1 \pmod 7$ y $2^3 \equiv 4^3 \equiv 1 \pmod 7$ y las únicas posibilidades restantes son el 3 y el 5).

Observación. Se sigue de c) que un cuerpo finito K de q elementos es el conjunto de raíces del polinomio $\mathrm{X}^q - \mathrm{X}$ (que tiene exactamente q raíces). Se puede demostrar que dos cuerpo finitos de q elementos son isomorfos. A menudo se nota $\mathbf{F}_q$ el cuerpo finito de q elementos.

A manera de ejercicio y de intermedio, ahora demostraremos un elegante teorema concerniente a las ecuaciones diofánticas sobre un cuerpo finito:

Teorema 2 (Chevalley)**.** *Sea* K *un cuerpo finito y* $\mathrm{F}(\mathrm{X}_1,\ldots,\mathrm{X}_n)$ *un polinomio homogéneo de grado* d *sobre* K*. Si* $d < n$*, existe un punto* $(x_1,\ldots,x_n) \in \mathrm{K}^n$ *distinto al origen* $(0,\ldots,0)$ *tal que* $\mathrm{F}(x_1,\ldots,x_n) = 0$*.*

> *Dado un cuerpo* K *y un entero* j*, se dice que* K *es un* **cuerpo** C_j *si todo polinomio homogéneo sobre* K *de grado* d *en* n *variables* **tal que** $n > d^j$*, admite un cero no trivial (i.e. distinto al origen) en* K^n*. Los cuerpos* C_0 *son exactamente los cuerpos algebraicamente cerrados. El teorema de Chevalley dice que los cuerpos finitos son* C_1 *(también llamados cuerpos "quasi-algebraicamente cerrados"). Se puede demostrar que, si* K *es un cuerpo* C_j*, el cuerpo* $\mathrm{K}(\mathrm{T})$ *de funciones racionales en una variable sobre* K *y el cuerpo* $\mathrm{K}((\mathrm{T}))$ *de series formales en una variable sobre* K *son cuerpos* C_{j+1} *(*[**17**]*). Por mucho tiempo se ignoraba si los cuerpos p-ádicos eran* C_2*, pero recientemente se demostró que esto no es así (*[**20**]*).*

Demostremos el teorema 2. Sea q el cardinal de K y p su característica (de forma que $q = p^s$). Sea $\mathrm{V} \subset \mathrm{K}^n$ el conjunto de ceros de F, i.e. los puntos $(x_1,\ldots,x_n) \in \mathrm{K}^n$ tales que $\mathrm{F}(x) = 0$ (de ahora en más, utilizamos la notación vectorial en la cual x denota un punto $(x_1,\ldots,x_n)$ de K^n). Por el teorema 1, c), se tiene $\mathrm{F}(x)^{q-1} = 0$ si $x \in \mathrm{V}$, y $\mathrm{F}(x)^{q-1} = 1$ si $x \in \mathrm{K}^n - \mathrm{V}$. Es decir, el polinomio $\mathrm{G}(x) = \mathrm{F}(x)^{q-1}$ es la **función característica** de $\mathrm{K}^n - \mathrm{V}$, con valores in $\mathbf{F}_p$. El número, módulo p, de puntos de $\mathrm{K}^n - \mathrm{V}$ puede escribirse como la suma $\sum_{x\in\mathrm{K}^n} \mathrm{G}(x)$. Nosotros calcularemos esta suma y mostraremos que es **cero.** Luego $\mathrm{card}(\mathrm{K}^n - \mathrm{V})$ será un múltiplo de p; como $\mathrm{card}(\mathrm{K}^n) = q^n = p^{ns}$ también es un múltiplo de p, $\mathrm{card}(\mathrm{V})$ será un múltiplo de p. Como V contiene al origen, deberá conteger necesariamente otros puntos, pues $p \geq 2$ y de esta manera habremos demostrado el teorema 2.

Calculemos entonces $\sum_{x\in\mathrm{K}^n} \mathrm{G}(x)$. El polinomio G es combinación lineal de monomios $\mathrm{M}_\alpha(\mathrm{X}) = \mathrm{X}_1^{\alpha_1}\cdots\mathrm{X}_n^{\alpha_n}$; por lo que basta calcular $\sum_{x\in\mathrm{K}^n} \mathrm{M}_\alpha(x) = \sum_{x\in\mathrm{K}^n} x_1^{\alpha_1}\cdots x_n^{\alpha_n} = \left(\sum_{x_1\in\mathrm{K}} x_1^{\alpha_1}\right)\cdots\left(\sum_{x_n\in\mathrm{K}} x_n^{\alpha_n}\right)$. Se trata entonces de calcular sumas de la forma $\sum_{z\in\mathrm{K}} z^\beta$ $(\beta \in \mathbf{N})$.

(a) Si $\beta = 0$, se tiene $z^\beta = 1$ para todo $z \in \mathrm{K}$, y la suma vale $q = 0$;
(b) Si $\beta > 0$, el término 0^β es cero y la suma se reduce a $\sum_{z\in\mathrm{K}^*} z^\beta$. Recordemos que K^* es un grupo cíclico de orden $q-1$ (teorema 1, b)); sea ω un generador. Luego, $\sum_{z\in\mathrm{K}^*} z^\beta = \sum_{j=0}^{q-2} \omega^{\beta j}$, que es una serie geométrica. Por lo tanto:

(b') Si la razón ω^β es $\neq 1$, es decir, si β no es múltiplo de $q-1$, se tiene $\sum_{j=0}^{q-2} \omega^{\beta j} = \frac{\omega^{\beta(q-1)}-1}{\omega^\beta - 1} = 0$ (pues $\omega^{q-1} = 1$).

(b") Si $\omega^\beta = 1$, es decir si β es un múltiplo de $q-1$, se tiene

$$\sum_{j=0}^{q-2} \omega^{\beta j} = q - 1.$$

Resulta de (a), (b') y (b") que $\sum_{x \in \mathrm{K}^n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ se anula **salvo si** todos los α_i son > 0 y divisibles por $q-1$. El grado $\alpha_1 + \cdots + \alpha_n$ del es, en ese caso, $\geq (q-1)n$. Pero, como $\mathrm{G} = \mathrm{F}^{q-1}$, G tiene grado $(q-1)d$, y se tiene $(q-1)d < (q-1)n$ por hipótesis. Por lo tanto, se tiene que $\sum_{x \in \mathrm{K}^n} \mathrm{M}_\alpha(x) = 0$ para todo monomio que figura en G con un coeficiente no nulo. Sumando, resulta que $\sum_{x \in \mathrm{K}^n} \mathrm{G}(x) = 0$. Ya vimos que esta relación implica la conclusión deseada.

> *Observemos que en vez de suponer que* F *es homogéneo, es suficiente suponer que* F *no tiene término constante. Por otra parte, la desigualdad* **estricta** $d < n$ *entre el grado y el número de variables es esencial. Por ejemplo, la* **norma** *de* $\mathbf{F}_{q^n}$ *en* $\mathbf{F}_q$ *(cf. capítulo II, §6) es un polinomio homogéneo de grado n en n variables sobre* $\mathbf{F}_q$ *que sólo se anula en el origen.*

Ejemplo. Un ejemplo. Una forma cuadrática en 3 variables sobre un cuerpo **finito** K "representa al 0" (i.e. tiene un cero no trivial). Pasando de K^3 al plano proyectivo $\mathrm{P}_2(\mathrm{K})$, esto quiere decir que una **cónica** sobre K admite un punto racional sobre K (i.e. tal que sus coordenadas homogéneas pueden elegirse en K). El ejemplo de la cónica $x^2 + y^2 + z^2 = 0$ sobre $\mathbf{R}$ (resp. $x^2 + y^2 - 3y^2 = 0$ sobre $\mathbf{Q}$: para verificar que $x^2 + y^2 - 3z^2 = 0$ no admite soluciones no triviales en $\mathbf{Q}$ se reduce al caso donde x, y, z son enteros coprimos entre sí, y luego se reduce módulo 4) muestra que el teorema no es verdad para todo los cuerpos.

CAPÍTULO II

Elementos enteros sobre un anillo; elementos algebraicos sobre un cuerpo

Entre todos los números complejos, en este libro nos ocuparemos de los números **algebraicos,** es decir, aquellos que satisfacen una ecuación de la forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

donde los a_i son números racionales. Cuando los a_i son enteros ($a_i \in \mathbf{Z}$), el número algebraico x se dice **entero algebraico.** Por ejemplo, $\sqrt{2}$, $\sqrt{3}$, i y $e^{2i\pi/5}$ son enteros algebraicos. No es evidente a priori que sumas y productos de números algebraicos (resp. enteros algebraicos) son de nuevo números algebraicos (resp. enteros algebraicos). Consideremos, por ejemplo, $x = \sqrt{2} + \sqrt{3}$. Elevando al cuadrado, se tiene $x^2 = 2 + 3 + 2\sqrt{6}$. Separando la raíz cuadrada de los demás términos se obtiene la igualdad $x^2 - 6 = 2\sqrt{6}$ y elevando al cuadrado nuevamente se obtiene finalmente $(x^2 - 5)^2 = 24$, lo que muestra que x es un entero algebraico. El lector tendrá que esforzarse para hacer lo mismo con $\sqrt[3]{5} + \sqrt[5]{7}$ y se convencerá que la serie de trucos utilizandos en la demostración de que este número es algebraico no se pueden generalizar fácilmente.

Para superar esta dificultad, los algebristas del último siglo, Dedekind en particular, tuvieron la idea de "linearizar" el problema, es decir, de introducir la noción de módulo. Esto es lo que haremos nosotros también. Reemplazar $\mathbf{Z}$ (o $\mathbf{Q}$) por un anillo conmutativo cualquiera no require más esfuerzo y nos será muy útil en lo que sige. Comenzaremos estudiando el caso general de elementos enteros sobre un anillo y después estudiaremos el caso particular de elementos algebraicos sobre un cuerpo.

1. Elementos enteros sobre un anillo

Teorema 1. *Sea* R *un anillo,* A *un subanillo de* R *y* x *un elemento de* R*. Las siguientes propiedades son equivalentes:*

1. *Existen* $a_0, \ldots, a_{n-1} \in \mathrm{A}$ *tales que*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1}$$

(es decir, x es raíz de un polinomio mónico sobre A*)*

2. *El anillo* $\mathrm{A}[x]$ *es un* A*-módulo de tipo finito.*
3. *Existe un subanillo* B *de* R *que contiene a* A *y a x y que es un* A*-módulo de tipo finito.*

Mostremos que *a*) implica *b*). Sea M el sub-A-módulo de R generado por $1, x, \ldots, x^{n-1}$. Por *a*) se tiene $x^n \in \mathrm{M}$. Mostremos que $x^{n+j} \in \mathrm{M}$ haciendo inducción en j. En efecto, multiplicando (1) por x^j se obtiene $x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j$. Como $\mathrm{A}[x]$ es el A-módulo generado por los x^k $(k \geq 0)$, se deduce que $\mathrm{A}[x] = \mathrm{M}$, lo que demuestra *b*).

La implicación *b*) $\Rightarrow$ *c*) es trivial. Mostremos que *c*) implica *a*). Sea $(y_1, \ldots, y_n)$ un sistema finito de generadores del A-módulo B. Es decir, $\mathrm{B} = \mathrm{A}y_1 + \cdots + \mathrm{A}y_n$. Como $x \in \mathrm{B}$, $y_i \in \mathrm{B}$ y B es un subanillo de R, se sigue que $xy_i \in \mathrm{B}$ de manera que existen elementos a_{ij} de A tales que $xy_i = \sum_{j=1}^n a_{ij}y_j$. Esto se puede reescribir

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})y_j = 0 \quad (i = 1, \ldots, n)$$

Se obtiene así un sistema de n ecuaciones lineales homogéneas en $(y_1, \ldots, y_n)$.

Si d es el determinante $\det(\delta_{ij}x - a_{ij})$, la fórmula de Cramer muestra que $dy_i = 0$ para todo i. Como $\mathrm{B} = \sum_i \mathrm{A}y_i$, se deduce que $d\mathrm{B} = 0$, de donde $d = d \cdot 1 = 0$ pues B posee un elemento neutro. Ahora bien, si desarollamos el determinante

$$d = \det(\delta_{ij}x - a_{ij}),$$

obtenemos una ecuación de la forma $\mathrm{P}(x) = 0$ con P un polinomio de grado n sobre A. Este polinomio es mónico pues el coeficiente de x^n proviene únicamente del producto $\prod_{i=1}^n (x - a_{ii})$ de los elementos de la diagonal principal. Por lo tanto *a*) es verdad.

Definición 1. *Sea* R *un anillo y* A *un subanillo de* R*. Un elemento x de* R *se dice entero sobre* A *si satisface las condiciones equivalentes a, b), c) del teorema 1. Sea* $\mathrm{P} \in \mathrm{A[X]}$ *un polinomio mónico tal que* $\mathrm{P}(x) = 0$ *(la existencia de este polinomio se sigue de a)); la relación* $\mathrm{P}(x) = 0$ *se llama una ecuación de dependencia integral de x sobre* A*.*

Ejemplo. El elemento $x = \sqrt{2}$ de $\mathbf{R}$ es entero sobre $\mathbf{Z}$; una ecuación de dependencia integral está dada por $x^2 - 2 = 0$.

Proposición 1. *Sea* R *un anillo,* A *un subanillo de* R *y* $(x_i)_{1\leq i\leq n}$ *una colección finita de elementos de* R. *Si, para todo* i, x_i *es entero sobre* $\mathrm{A}[x_1,\ldots,x_{i-1}]$ *(en particular, si todos los* x_i *son enteros sobre* A*), entonces* $\mathrm{A}[x_1,\ldots,x_n]$ *es un* A*-módulo de tipo finito.*

Razonemos por inducción en n. Si $n=1$, se trata de la afirmación b) del teorema 1. Supongamos que la proposición es verdad para $n-1$. Entonces $\mathrm{B}=\mathrm{A}[x_1,\ldots,x_{n-1}]$ es un A-módulo de tipo finito y podemos escribir $\mathrm{B}=\sum_{j=1}^{p}\mathrm{A}b_j$. Aplicando el caso $n=1$ se sigue que $\mathrm{A}[x_1,\ldots,x_n]=\mathrm{B}[x_n]$ es un B-módulo de tipo finito, que lo podemos escribir $\sum_{k=1}^{q}\mathrm{B}c_k$. Luego se tiene

$$\mathrm{A}[x_1,\ldots,x_n]=\sum_{k=1}^{q}\mathrm{B}c_k=\sum_{k=1}^{q}\left(\sum_{j=1}^{p}\mathrm{A}b_j\right)c_k=\sum_{j,k}\mathrm{A}b_jc_k,$$

de manera que (b_jc_k) es un sistema finito de generadores del A-módulo $\mathrm{A}[x_1,\ldots,x_n]$.

Corolario 1. *Sea* R *un anillo,* A *un subanillo de* R*,* x *e* y *dos elementos de* R *enteros sobre* A*. Entonces* $x+y$, $x-y$ *y* xy *son enteros sobre* A*.*

En efecto, se tiene que $x+y, x-y, xy\in\mathrm{A}[x,y]$. Por la proposición 1, $\mathrm{A}[x,y]$ es un A-módulo de tipo finito; luego, por la parte c) del teorema 1, $x+y$, $x-y$ y xy son enteros sobre A.

Corolario 2. *Sea* R *un anillo y* A *un subanillo de* R*. El conjunto* A′ *de elementos de* R *enteros sobre* A *es un subanillo de* R *que contiene a* A*.*

Efectivamente, A′ es un subanillo de R por el corolario 1; contiene a A pues todo $a\in\mathrm{A}$ es raíz del polinomio mónico $\mathrm{X}-a$ y por lo tanto es entero.

Definición 2. *Sea* R *un anillo,* A *un subanillo de* R*. El anillo* A′ *de los elementos de* R *enteros sobre* A *se llama la* **clausura íntegra** *de* A *en* R*. Sea* A *un dominio íntegro y* K *su cuerpo de fracciones. La clausura íntegra de* A *en* K *se llama la clausura íntegra de* A*. Sea* B *un anillo y* A *un subanillo de* B*. Decimos que* B *es* **entero** *sobre* A *si todo elemento de* B *es entero sobre* A *(es decir, si la clausura entera de* A *en* B *es todo* B*).*

Proposición 2 (de transitividad)**.** *Sea* C *un anillo,* B *un subanillo de* C *y* A *un subanillo de* B*. Si* B *es entero sobre* A *y* C *es entero sobre* B*, entonces* C *es entero sobre* A*.*

En efecto, sea $x\in\mathrm{C}$; x es entero sobre B y por lo tanto se tiene una ecuación de dependencia entera $x^n+b_{n-1}x^{n-1}+\cdots+b_0=0$ con $b_i\in\mathrm{B}$. Sea $\mathrm{B}'=\mathrm{A}[b_0,\ldots,b_{n-1}]$, de manera que x también es entero sobre B′. Como B es entero sobre A, los b_i son enteros sobre A. Por lo tanto, por la proposición 1,

$B'[x] = A[b_0, \ldots, b_{n-1}, x]$ es un A-módulo de tipo finito. Por la parte *c*) del teorema 1 concluimos que x es entero sobre A. Por lo tanto C es entero sobre A.

Proposición 3. *Sea* B *un dominio íntegro y* A *un subanillo de* B *tal que* B *es entero sobre* A. *Para que* B *sea un cuerpo es necesario y suficiente que* A *lo sea.*

Supongamos que A es un cuerpo y sea $b \in B$, $b \neq 0$. Luego $A[b]$ es un espacio vectorial de dimension **finita** sobre A (teorema 1, *b*)). Por otra parte, $y \mapsto by$ es una aplicación A-lineal de $A[b]$ en si mismo, que es inyectiva pues $A[b]$ es un dominio íntegro y $b \neq 0$. Por lo tanto, también es sobreyectiva y existe $b' \in A[b]$ tal que $bb' = 1$. Luego b es inversible en B y B es un cuerpo[1].

Reciprocamente, supongamos que B es un cuerpo y sea $a \in A$, $a \neq 0$. Luego a admite una inversa $a^{-1} \in B$ que satisface une ecuación de dependencia entera

$$a^{-n} + a_{n-1}a^{-n+1} + \cdots + a_1 a^{-1} + a_0 = 0 \quad (a_i \in A)$$

Multiplicando por a^{n-1}, obtenemos $a^{-1} = -(a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1})$, de donde $a^{-1} \in A$, de manera que A es un cuerpo.

2. Anillos íntegramente cerrados

Definición. *Decimos que un anillo* A *es íntegramente cerrado si es un dominio íntegro y su clausura íntegra es el mismo* A.

En otras palabras, si todo elemento x del cuerpo de fracciones K de A que es entero sobre A es un elemento de A.

Ejemplo 1. Sea A un dominio íntegro y K su cuerpo de fracciones. Entonces la **clausura íntegra** A' de A (es decir, la clausura íntegra de A en K) es un anillo íntegramente cerrado. En efecto, la clausura íntegra de A' es entera sobre A', y por lo tanto sobre A (§1, proposición 2). Luego coincide con A'.

Ejemplo 2. *Todo dominio de ideales principales es íntegramente cerrado.* Un dominio de ideales principales A es un dominio íntegro por definición. Sea x un elemento entero sobre A de su cuerpo de fracciones. Se tiene una ecuación de dependencia entera

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in A) \tag{1}$$

[1]El mismo tipo de razonamiento, utilizando la homotecia $y \mapsto by$, muestra que todo dominio íntegro **finito** es un cuerpo.

Ahora bien, podemos escribir $x = a/b$ con a,$b \in$ A **coprimos.** Multiplicando (1) por b^n obtenemos

$$a^n + b(a_{n-1}a^{n-1} + \cdots + a_1 ab^{n-2} + a_0 b^{n-1}) = 0.$$

Por lo tanto b divide a a^n. Como es coprimo con a, la aplicación repetida del lema de Euclides muestra que b divide a a. Luego $x = a/b \in$ A y A es íntegramente cerrado.

> *Observemos que solamente utilizamos las propiedades multiplicativas de los dominios de ideales principales (elementos coprimos, lema de Euclides). El mismo razonamiento muestra que todo anillo de* **factorización única** *es íntegramente cerrado.*

3. Elementos algebraicos sobre un cuerpo. Extensiones algebraicas

Definición. *Sea* R *un anillo y* K *un subcuerpo de* R*. Decimos que un elemento* x *de* R *es* **algebraico sobre** K *si existen elementos* $a_0, \ldots, a_n$ *de* K*, no todos nulos, tales que* $a_n x^n + \cdots + a_1 x + a_0 = 0$*.*

En otras palabras, los **monomios** $(x^j)_{j \in \mathbf{N}}$ son linealmente dependientes sobre K. Un elemento que no es algebraico sobre K se dice **trascendente** sobre K; equivalentemente, los monomios $(x^j)_{j \in \mathbf{N}}$ son linealmente independientes sobre K.

En la condición de la definición 1, podemos suponer que a_n es no nulo; luego, admite un inverso a_n^{-1} pues K es un cuerpo. Multiplicando por a_n^{-1} se obtiene una ecuación de dependencia entera. Por lo tanto:

(1) *Sobre un cuerpo, algebraico = entero.*

Por lo tanto podemos aplicar la teoría de los elementos enteros; por ejemplo, si K $\subset$ R y $x \in$ R, el teorema 1, *b*) de la §1 implica:

(2) x *algebraico sobre* K $\iff$ [K[x] : K] *es finito.*

Decimos que un anillo R que contiene un cuerpo K es **algebraico** sobre K si todo elemento de R es algebraico sobre K. Cuando el mismo R es un cuerpo, decimos que R es una **extensión algebraica** de K.

Dado un cuerpo L y un subcuerpo K de L, la dimensión [L : K] se llama **grado** de L sobre K. El teorema 1, *c*) de la §1 muestra entonces:

(3) *Si el grado de* L *sobre* K *es finito,* L *es una extensión algebraica de* K*.*

Llamamos **cuerpo de números algebraicos** (o **cuerpo de números**) a toda extensión de **Q** de grado finito.

Proposición 1. *Sea* K *un cuerpo,* L *una extensión algebraica de* K *y* M *una extensión algebraica de* L. *Entonces* M *es una extensión algebraica de* L. *Más aún,* $[M : K] = [M : L][L : K]$ *("multiplicatividad del grado").*

La primera afirmación es un caso particular de la proposición 2 de la §1. Más aún, si $(x_i)_{i\in I}$ es una base de L sobre K y $(y_j)_{j\in J}$ es una base de M sobre L, entonces $(x_i y_j)_{(i,j)\in I\times J}$ es una **base** de M sobre K: en efecto, es un sistema de generadores, tal como se vió en la proposición 1 de la §1. Por otra parte, una relación $\sum_{i,j} a_{ij}x_i y_j = 0$ con $a_{ij} \in K$ implica $\sum_j \left(\sum_i a_{ij}x_i\right) y_j = 0$, de donde se sigue que $\sum_i a_{ij}x_i = 0$ para todo j (pues $\sum a_{ij}x_i \in L$) y en consecuencia que $a_{ij} = 0$ para todo i, j. Esto demuestra la fórmula de la multiplicatividad del grado.

Proposición 2. *Sea* R *un anillo y* K *un subcuerpo de* R. *Entonces*

a) *El conjunto* K′ *de los elementos de* R *algebraicos sobre* K *es un subanillo de* R *que contiene a* K;
b) *Si* R *es un dominio íntegro,* K′ *es un subcuerpo de* R.

En efecto, *a*) es un caso particular del corolario 2 de la proposición 1, §1 y *b*) resulta de la proposición 3 de §1.

Ahora estudiaremos más de cerca los elementos algebraicos sobre un cuerpo. Sea R un anillo, K un subcuerpo de R y x un elemento de R. Existe un único homomorfismo φ del anillo de polinomios K[X] en R tal que $\varphi(X) = x$ y tal que $\varphi(a) = a$ para todo $a \in K$. La imagen de φ es $K[x]$. La definición de elemento algebraico se traduce en:

(4) $$x \text{ es algebraico sobre } K \iff \mathrm{Ker}(\varphi) \neq (0).$$

Si x es algebraico sobre K, el ideal $\mathrm{Ker}(\varphi)$ es un ideal **principal** $(F(X))$ (pues K[X] es un dominio de ideales principales) generado por un polinomio no nulo F(X) que podemos suponer **mónico** pues K es un cuerpo. Este polinomio mónico está determinado de forma única por K y x y se llama el **polinomio minimal** de x sobre K. Traduciendo la definición, obtenemos:

(5) *Sea* F(X) *el polinomio minimal de* x *sobre* K *y sea* $G(X) \in K[X]$. *Para que* $G(x) = 0$ *es necesario y suficiente que* F(X) *divida a* G(X) *en* K[X].

Más aún, pasando al cociente, obtenemos un **isomorfismo canónico**

(6) $$K[X]/(F(X)) \xrightarrow{\sim} K[x].$$

Con la misma notación de antes, supongamos ahora que x es algebraico sobre K y sea $F(X)$ su polinomio minimal. Aplicando (5) y la proposición 3 de la §1, se obtienen las siguientes equivalencias:

$$(7) \qquad K[X] \text{ es un cuerpo} \iff K[x] \text{ es un dominio íntegro} \iff F(X) \text{ es irreducible.}$$

Reciprocamente, sea K un cuerpo y $F(X) \in K[X]$ un polinomio irreducible. Luego $K[X]/(F(X))$ es un cuerpo que contiene a K y tal que, si notamos x la clase de X en este cuerpo, se tiene $F(x) = 0$, de manera que $F(X)$ es divisible por $X - x$ en el cuerpo $K[x]$. Más generalmente:

Proposición 3. *Sea* K *un cuerpo y* $P(X) \in K[X]$ *un polinomio no constante. Existe una extension algebraica* K' *de* K *de grado finito tal que* $P(X)$ *se descompone en factores lineales en* $K'[X]$.

Razonamos por inducción sobre el grado d de $P(X)$. El resultado es evidente si $d = 1$. Supongamos que el enunciado está demostrado para grados no mayores a $d - 1$.

Sea $F(X)$ un factor irreducible de $P(X)$. Acabamos de ver que existe una extensión K'' de K de grado finito (concretamente, $K[X]/(F(X))$) y un elemento $x \in K''$ tal que $F(X)$ es multiplo de $X - x$ en $K''[X]$. Se tiene entonces que $P(X) = (X - x)P_1(X)$ con $P_1(X) \in K''[X]$. De la hipótesis inductiva se sigue que $P_1(X)$ se descompone en factores lineales en una extensión K' de K'' de grado finito. Luego K' es una extensión de grado finito de K (proposición 1) y $P(X)$ se descompone en factores lineales en $K'[X]$.

Observación (cuerpos algebraicamente cerrados). Decimos que K es **algebraicamente cerrado** si **todo** polinomio no constante $P(X) \in K[X]$ se descompone en factores lineales en $K[X]$. Para verificar esta propieadad basta, por inducción en el grado, que todo polinomio no constante $P(X) \in K[X]$ admita una raíz $x \in K$. Aplicando una versión "transfinita" de la proposición 3 (es decir, combinando la proposición 3 con el teorema de Zorn; cf. [**13**], capítulo V y [**21**], capítulo II), se demuestra que todo cuerpo es un subcuerpo de un cuerpo algebraicamanete cerrado.

Utilizando las técnicas del Análisis puede demostrarse, de varias maneras[1], que el cuerpo **C** de los **números complejos** es algebraicamente cerrado. Esto es todo lo que nosotros necesitaremos.

4. Elementos conjugados, cuerpos conjugados

Dados dos cuerpos L y L′ conteniendo un cuerpo K, llamamos **K-isomorfismo** de L en L′ a todo isomorfismo $\varphi : L \to L'$ tal que $\varphi(a) = a$ para todo $a \in K$. En este caso, decimos que L y L′ son **K-isomorfos,** o (si L y L′ son algebraicos sobre K) que son **cuerpos conjugados sobre** K**.**

Dadas dos extensiones L y L′ de K, decimos que dos elementos $x \in L$ y $x' \in L'$ son **conjugados** sobre K si existe un K-isomorfismo $\varphi : K(x) \to K(x')$ tal que $\varphi(x) = x'$. En tal caso, φ es única. Esto quiere decir que o bien x y x' son ambos trascendentes sobre K, o bien x y x' son ambos algebraicos sobre K y tienen el mismo polinomio minimal (cf. (5), §3).

Ejemplo. Sea F(X) un polinomio **irreducible** de grado n sobre K y sean $x_1, \ldots, x_n$ sus raíces en una extensión K′ de K (§3, proposición 3). Luego los x_i son conjugados dos a dos sobre K (§3, (6)) y los cuerpos $K[x_i]$ también son conjugados dos a dos sobre K.

Lema. *Sea* K *un cuerpo de característica cero o un cuerpo finito,* $F(X) \in K[x]$ *un polinomio mónico irreducible y* $F(X) = \prod_{i=1}^{n}(X - x_i)$ *su descomposicón en factores lineales en una extensión* K′ *de* K *(§3, proposición 3). Entonces las* n *raíces* $x_1, \ldots, x_n$ *de* F(X) *son todas distintas.*

Razonemos por el absurdo. En el caso contrario, F(X) admite una raíz **múltiple** x, que tendría que ser entonces también raíz del polinomio derivado F′(X), en cuyo caso F(X) dividiría a F′(X) ((4), §3). Como $d^\circ F' < d^\circ F$, esto implica que F′(X) es el polinomio nulo. Ahora bien, si

$$F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad (a_i \in K)$$

se tiene

$$F'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1.$$

Deducimos que $n \cdot 1 = 0$ y $j \cdot a_j = 0$ para $j = 1, \ldots, n-1$. Esto es imposible en característica cero.

[1]Para una demostración que utiliza las propiedades de las funciones continuas sobre un espacio compacto, ver [**16**]. Para una demostración que utiliza las propiedades de las funciones holomorfas de una variable compleja, ver [**15**]. Nostoros presentaremos en el apéndice a este capítulo una demostración más algebraica, que sólo utilizará las propiedades más simples de los números reales.

En característica $p \neq 0$, la implicación es que p divide a n y que $a_j = 0$ si j no es un múltiplo de p (recordemos que p es un número primo). Luego, $\mathrm{F(X)}$ es de la forma

$$\mathrm{F(X)} = \mathrm{X}^{qp} + b_{q-1}\mathrm{X}^{(q-1)p} + \cdots + b_1\mathrm{X}^p + b_0 \quad (b_i \in \mathrm{K}).$$

Si cada uno de los b_i es una **potencia p-ésima,** es decir $b_i = c_i^p$ para algún $c_i \in \mathrm{K}$, se sigue que $\mathrm{F(X)} = (\mathrm{X}^q + c_{q-1}\mathrm{X}^{q-1} + \cdots + c_0)^p$ (capítulo I, §7, proposición 1) y $\mathrm{F(X)}$ no es irreducible. Por otra parte, si K es un cuerpo finito de característica p ($\neq 0$), la aplicación $x \mapsto x^p$ de K en K es inyectiva (pues $x^p = y^p$ implica $x^p - y^p = (x-y)^p = 0$ y $x - y = 0$). Por lo tanto también es sobreyectiva pues K es finito. Hemos obtenido una una contradicción.

> *Los cuerpos* K *de característica* $p \neq 0$ *tales que* $x \mapsto x^p$ *es sobreyectiva (i.e. tales que todo elemento de* K *es una potencia* p*-ésima) se llaman cuerpos* **perfectos.** *Acabamos de demostrar que todo cuerpo finito es perfecto. Por convención, un cuerpo de característica cero es perfecto. De hecho, hemos demostrado que la conclusión del teorema vale bajo la hipótesis de que* K *sea un cuerpo perfecto. El cuerpo* $\mathbf{F}_p(\mathrm{T})$ *de las funciones racionales en une variable sobre* $\mathbf{F}_p$ *no es perfecto, pues la variable* T *no es una potencia* p*-ésima en* $\mathbf{F}_p(\mathrm{T})$.

Teorema 1. *Sea* K *un cuerpo de característica cero o finito,* K′ *una extensión de* K *de grado finito* n *y* C *un cuerpo algebraicamente cerrado que contiene a* K. *Entonces existen* n K*-isomorfismos distintos de* K′ *en* C.

El resultado es cierto para una extensión **unigenerada** K′, es decir de la forma $\mathrm{K}' = \mathrm{K}[x]$ ($x \in \mathrm{K}$). En este caso el polinomio minimal $\mathrm{F(X)}$ de x sobre K tiene grado n y admite n raíces $x_1, \ldots, x_n$ en C que son distinas por el lema anterior. Para cada $i = 1, \ldots, n$ se tiene entonces un K-isomorfismo $\sigma_i : \mathrm{K}' \to \mathrm{C}$ tal que $\sigma_i(x) = x_i$.

En el caso general, procedemos por inducción en el grado n de K′. Sea $x \in \mathrm{K}'$; consideremos los cuerpos intermedios $\mathrm{K} \subset \mathrm{K}[x] \subset \mathrm{K}'$ y sea $q = [\mathrm{K}[x] : \mathrm{K}]$. Podemos suponer que $q > 1$. Por el caso unigenerado, se tienen q K-isomorfismos distintos $\sigma_1, \ldots, \sigma_q$ de $\mathrm{K}[x]$ en C. Como $\mathrm{K}[\sigma_i(x)]$ y $\mathrm{K}[x]$ son isomorfos, podemos construir una extension K_i' de $\mathrm{K}[\sigma_i(x)]$ y un isomorfismo $\tau_i : \mathrm{K}' \to \mathrm{K}_i'$ que prolonga a σ_i. Ahora bien, $\mathrm{K}[\sigma_i(x)]$ es un cuerpo de característica cero o finito. Como

$$[\mathrm{K}_i' : \mathrm{K}[\sigma_i(x)]] = [\mathrm{K}' : \mathrm{K}[x]] = \frac{n}{q} < n,$$

la hipótesis inductiva implica que se tienen $\frac{n}{q}$ $\mathrm{K}[\sigma_i(x)]$-isomorfismos distintos θ_{ij} de K'_i en C. Luego las n composiciones $\theta_{ij} \circ \tau_i$ son los $q \cdot \frac{n}{q} = n$ K-isomorfismos deseados de K′ en C. Son distintos pues $\theta_{ij} \circ \tau_i$ y $\theta_{i'j'} \circ \tau_{i'}$ son distintos cuando se los restringe a $\mathrm{K}[x]$ si $i \neq i'$ y si $j \neq j'$ entonces θ_{ij} y $\theta_{i'j'}$ son distintos cuando se los restringe a K'_i. LQQD.

El teorema 1 se extiende a un cuerpo perfecto K*: puede demostrarse que toda extension algebraica de un cuerpo perfecto (en particular,* $\mathrm{K}[\sigma_i(x)]$*) es un cuerpo perfecto; el resto de la demostración es igual.*

Corolario ("teorema del elemento primitivo")**.** *Sea* K *un cuerpo finito o de característica cero y sea* K′ *una extension de* K *de grado finito n. Existe entonces un elemento x en* K′ *(llamado "primitivo") tal que* $\mathrm{K}' = \mathrm{K}[x]$.

Si K es finito, K′ es finito y su grupo multiplicativo K'^* consiste en las potencias de un mismo elemento x (capítulo I, §7, teorema 1, *b*)). Entonces se tiene $\mathrm{K}' = \mathrm{K}[x]$.

Supongamos ahora que K es de característica cero, en particular infinito. Por el teorema 1, existen n K-isomorfismos σ_i de K′ en un cuerpo algebraicamente cerrado C que contiene a K. Si $i \neq j$, la ecuación $\sigma_i(y) = \sigma_j(y)$ $(y \in \mathrm{K}')$ define un subconjunto V_{ij} de K′ que es evidentemente un sub-K-espacio vectorial de K′ y que es distinto de K′ pues $\sigma_i \neq \sigma_j$. Como K es infinito, el álgebra lineal muestra que la unión de los V_{ij} no es todo K′.

Sea x en el complemento de dicha unión. Los $\sigma_i(x)$ son entonces distintos dos a dos, de manera que el polinomio minimal $\mathrm{F(X)}$ de x sobre K tiene al menos n raíces distintas (los $\sigma_i(x)$) en C. Tenemos por lo tanto que $d^\circ \mathrm{F} \geq n$, es decir que $[\mathrm{K}[x] : \mathrm{K}] \geq n$. Como $\mathrm{K}[x] \subset \mathrm{K}'$ y $[\mathrm{K}' : \mathrm{K}] = n$ deducimos que $\mathrm{K}' = \mathrm{K}[x]$. LQQD.

5. Enteros de un cuerpo cuadrático

Interrumpimos ahora la teoría general para dar un ejemplo.

Definición. *Llamamos cuerpo cuadrático a toda extensión de grado* 2 *del cuerpo* $\mathbf{Q}$ *de los números racionales.*

Si K es un cuerpo cuadrático, cualquier elemento x de $\mathrm{K} - \mathbf{Q}$ es de grado 2 sobre $\mathbf{Q}$ por lo que es un elemento primitivo de K (i.e. $\mathrm{K} = \mathbf{Q}[x]$ y $(1,x)$ es una base de K sobre $\mathbf{Q}$). Sea $\mathrm{F(X)} = \mathrm{X}^2 + b\mathrm{X} + c$ $(b,c \in \mathbf{Q})$ el polinomio minimal de un tal elemento $x \in \mathrm{K}$. La resolución de la ecuación de segundo grado

$x^2+bx+c=0$ muestra que $2x=-b\pm\sqrt{b^2-4c}$, por lo que $\mathrm{K}=\mathbf{Q}(\sqrt{b^2-4c})$[1]. Como b^2-4ac es un número racional $\frac{u}{v}=\frac{uv}{v^2}$ con $u,v\in\mathbf{Z}$, se sigue que $\mathrm{K}=\mathbf{Q}(\sqrt{uv})$ con $uv\in\mathbf{Z}$. Análogamente vemos que se tiene $\mathrm{K}=\mathbf{Q}(\sqrt{d})$ donde d es un entero **sin factores cuadrados** en su descomposición factores primos. Así hemos probado:

Proposición 1. *Todo cuerpo cuadrático es de la forma* $\mathbf{Q}(\sqrt{d})$*, donde* d *es un entero libre de cuadrados.*

El elemento $\sqrt{d}$ es una raíz del polinomio irreducible X^2-d. Esta raíz admite un **conjugado** en K, concretamente $-\sqrt{d}$. Por lo tanto existe un automorfismo σ de K que envía $\sqrt{d}$ en $-\sqrt{d}$ (§4). Un elemento general de K se escribe de la forma $a+b\sqrt{d}$ con $a,b\in\mathbf{Q}$ y por lo tanto se tiene

$$\sigma(a+b\sqrt{d})=a-b\sqrt{d} \tag{1}$$

Nos proponemos estudiar ahora el anillo A de **enteros** de K, es decir, el conjunto de los $x\in\mathrm{K}$ que son enteros sobre $\mathbf{Z}$ (§1, corolario 2 de la proposición 2). Si $x\in\mathrm{A}$, $\sigma(x)$ es raíz de la misma ecuación de dependencia entera que x, por lo que $\sigma(x)\in\mathrm{A}$. Luego, se tiene $x+\sigma(x)\in\mathrm{A}$ y $x\cdot\sigma(x)\in\mathrm{A}$. Ahora bien, si $x=a+b\sqrt{d}$ con $a,b\in\mathbf{Q}$, se sigue de (1) que

$$x+\sigma(x)=2a\in\mathbf{Q},\quad x\sigma(x)=a^2-db^2\in\mathbf{Q}. \tag{2}$$

Como $\mathbf{Z}$ es un dominio de ideales principales, y por lo tanto íntegramente cerrado (§2, ex. 2), se concluye que

$$2a\in\mathbf{Z},\quad a^2-db^2\in\mathbf{Z}. \tag{3}$$

Estas condiciones (3) son necesarias para que $x=a+b\sqrt{d}$ sea entero sobre $\mathbf{Z}$. Pero también son suficientes pues en caso de valer, x es raíz de

$$x^2-2ax+a^2-db^2=0.$$

De (3) se deduce que $(2a)^2-d(2b)^2\in\mathbf{Z}$. Como $2a\in\mathbf{Z}$, se sigue que $d(2b)^2\in\mathbf{Z}$. Recordemos que d es libre de cuadrados. Si $2b$ no fuera entero, su denominador contendría un factor primo p. Este factor aparecería como p^2 en $(2b)^2$ y la multiplicación por d no podría producir un entero. Por lo tanto, $2b\in\mathbf{Z}$.

En resúmen, podemos escribir $a=\frac{u}{2}$, $b=\frac{v}{2}$ con $u,v\in\mathbf{Z}$. La condición (3) se traduce en:

$$u^2-dv^2\in 4\mathbf{Z}. \tag{4}$$

[1]Por $\sqrt{b^2-4c}$ se entiende uno de los dos elementos de K cuyo cuadrado es b^2-4ac.

Si v es par, (4) muestra que u también lo es y por lo tanto a,$b \in \mathbf{Z}$. Si v es impar, necesariamente $v^2 \equiv 1 \bmod 4$. Recordemos que la clase de $u^2 \bmod 4$ es 0 ó 1 (escribir la tabla de los cuadrados mod 4). Como d es libre de cuadrados, no es un múltiplo de 4 y por lo tanto necesariamente se tiene que $u^2 \equiv 1 \bmod 4$ y $d \equiv 1 \bmod 4$. Hemos demostrado el siguiente teorema:

Teorema 1. *Sea* $\mathrm{K} = \mathbf{Q}(\sqrt{d})$ *un cuerpo cuadrático con* $d \in \mathbf{Z}$ *libre de cuadrados (y por lo tanto* $\not\equiv 0 \bmod 4$*).*

a) *Si* $d \equiv 2$ *ó* $d \equiv 3 \bmod 4$*, el anillo* A *de enteros de* K *es el conjunto de los elementos* $a + b\sqrt{d}$ *con* a,$b \in \mathbf{Z}$*.*
b) *Si* $d \equiv 1 \bmod 4$*,* A *es el conjunto de los* $\frac{1}{2}(u + v\sqrt{d})$ *con* u,$v \in \mathbf{Z}$ *de la misma paridad.*

En el caso $d \equiv 2$ ó $3 \bmod 4$, una base del $\mathbf{Z}$-módulo A es evidentemente $(1,\sqrt{d})$. En el caso $d \equiv 1 \bmod 4$, una base del $\mathbf{Z}$-módulo A es $\left(1,\frac{1}{2}(1+\sqrt{d})\right)$. En efecto, por b), los elementos 1 y $\frac{1}{2}(1+\sqrt{d})$ pertenecen a A. Recíprocamente, para mostrar que $\frac{1}{2}(u + v\sqrt{d})$ (con u,$v \in \mathbf{Z}$ de la misma paridad) es combinación $\mathbf{Z}$-linear de 1 y $\frac{1}{2}(1+\sqrt{d})$, podemos suponer, restando de ser necesario $\sqrt{1}2(1+\sqrt{d})$, que u y v son pares, en cuyo caso $\frac{1}{2}(u + v\sqrt{d}) = \left(\frac{u}{2} - \frac{v}{2}\right) \cdot 1 + v \cdot \frac{1}{2}(1+\sqrt{d})$.

Para terminar, un poco de **terminología.** Si $d > 0$, decimos que $\mathbf{Q}(\sqrt{d})$ es un **cuerpo cuadrático real** (pues existe un subcuerpo de $\mathbf{R}$ conjugado a $\mathbf{Q}(\sqrt{d})$ sobre $\mathbf{Q}$). Si $d < 0$, decimos que $\mathbf{Q}(\sqrt{d})$ es un **cuerpo cuadrático imaginario.**

6. Norma y traza

a) Repaso de álgebra lineal. Sea A un anillo, E un A-módulo **libre** de rango finito y u un endomorfismo de E. En álgebra lineal se define la **traza,** el **determinante** y el **polinomio característico** de u. Si se elige una base (e_i) de E y si (a_{ij}) es la matriz de u en esta base, estas cantidades están dadas, respectivamente, por las expresiones

$$\text{(1)} \qquad \operatorname{Tr} u = \sum_{i=1}^{n} a_{ii}, \quad \det(u) = \det(a_{ij}), \quad \text{y} \quad \det(\mathrm{X} \cdot \mathrm{I_E} - u)$$

NB. Estas cantidades son independientes de la base elegida.

Las fórmulas (1) muestran que valen las siguientes propiedades:

$$\begin{aligned} \operatorname{Tr}(u+u') &= \operatorname{Tr}(u)+\operatorname{Tr}(u') \\ \det(uu') &= \det(u)\det(u') \\ \det(\mathrm{X}\cdot \mathrm{I}_{\mathrm{E}} - u) &= \mathrm{X}^n - (\operatorname{Tr} u)\cdot \mathrm{X}^{n-1} + \cdots + (-1)^n \det u. \end{aligned} \tag{2}$$

b) Norma y traza de una extensión. Sea B un anillo y A un subanillo de B tal que B es un A-módulo libre de rango finito n (por ejemplo, A puede ser un cuerpo y B una extensión de A de grado n). Si $x \in \mathrm{B}$, la multiplicación m_x por x (es decir, $y \mapsto xy$) es un endomorfismo del A-módulo B.

Definición 1. *Llamamos traza (resp. norma, polinomio característico) de* $x \in \mathrm{B}$ *relativa a* B *y* A *a la traza (resp. determinante, polinomio característico) del endomorfismo* m_x *de multiplicación por* x.

La traza (resp. norma) de x se nota $\operatorname{Tr}_{\mathrm{A/B}}(x)$ (resp. $\mathrm{N}_{\mathrm{A/B}}(x)$), o bien $\operatorname{Tr}(x)$ (resp. $\mathrm{N}(x)$) si no hay riesgo de confusión. Es un elemento de A. El polinomio característico de x es un polinomio mónico con coeficientes en A.

Si $x, x' \in \mathrm{B}$ y $a \in \mathrm{A}$, es evidente que $m_x + m_{x'} = m_{x+x'}$, $m_x \circ m_{x'} = m_{xx'}$ y $m_{ax} = a m_x$. Por otra parte, la matriz de m_a en cualquier base de B sobre A es una matriz diagonal con todos sus elementos diagonales iguales a a. Se sigue entonces de las fórmulas (1) y (2) que:

$$\begin{aligned} &\operatorname{Tr}(x+x') = \operatorname{Tr}(x)+\operatorname{Tr}(x'), \quad \operatorname{Tr}(ax) = a\operatorname{Tr}(x), \quad \operatorname{Tr}(a) = n\cdot a \\ &\mathrm{N}(xx') = \mathrm{N}(x)\mathrm{N}(x'), \qquad \mathrm{N}(a) = a^n, \qquad \mathrm{N}(ax) = a^n \mathrm{N}(x). \end{aligned} \tag{3}$$

Proposición 1. *Sea* K *un cuerpo de característica cero o finito,* L *una extensión algebraica de* K *de grado* n, x *un elemento de* L *y* $x_1, \ldots, x_n$ *las raíces del polinomio minimal de* x *sobre* K *(en una extensión conveniente de* K*; cf. §3, proposición 3), cada una repetida* $[\mathrm{L} : \mathrm{K}[x]]$ *veces. Entonces* $\operatorname{Tr}_{\mathrm{L/K}}(x) = x_1 + \cdots + x_n$, $\mathrm{N}_{\mathrm{L/K}}(x) = x_1 \cdots x_n$ *y el polinomio característico de* x *relativo a* L *y* K *es* $(\mathrm{X} - x_1)\cdots(\mathrm{X} - x_n)$.

En particular, el polinomio característico es la potencia $[\mathrm{L} : \mathrm{K}[x]]$-*ésima del polinomio minimal de* x *sobre* K.

Tratemos primero el caso cuando x es un **elemento primitivo** de L sobre K (cf. §4, corolario del teorema 1). Sea $\mathrm{F}(\mathrm{X})$ el polinomio minimal de x sobre K. Entonces L es K-isomorfo a $\mathrm{K}[\mathrm{X}]/(\mathrm{F}(\mathrm{X}))$ (§3, fórmula (5)) y $(1, x, \ldots, x^{n-1})$ es una base de L sobre K. Si $\mathrm{F}(\mathrm{X}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_1\mathrm{X} + a_0$, la

matriz del endomorfismo m_x en esta base es:

$$\begin{vmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{vmatrix}$$

El determinante de $\mathrm{X} \cdot 1_{\mathrm{L}} - m_x$ es por lo tanto

$$\begin{vmatrix} \mathrm{X} & 0 & \cdots & 0 & a_0 \\ -1 & \mathrm{X} & & 0 & a_1 \\ 0 & -1 & & 0 & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & \mathrm{X} & a_{n-2} \\ 0 & 0 & & -1 & \mathrm{X} + a_{n-1} \end{vmatrix}$$

Desarollando este determinante se obtiene el polinomio característico de x, que es por lo tanto igual al polinomio minimal $\mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$. Por (2), se deduce que $\mathrm{Tr}(x) = -a_{n-1}$ y $\mathrm{N}(x) = (-1)^n a_0$. Como x es primitivo, se tiene además que $\mathrm{F}(\mathrm{X}) = (\mathrm{X} - x_1) \cdots (\mathrm{X} - x_n)$, de donde, comparando coeficientes, se deduce que

$$\mathrm{Tr}(x) = x_1 + \cdots + x_n \quad \text{y} \quad \mathrm{N}(x) = x_1 \cdots x_n.$$

Pasemos ahora el **caso general,** y sea $r = [\mathrm{L} : \mathrm{K}[x]]$. Basta demostrar que el polinomio característico $\mathrm{P}(\mathrm{X})$ de x relativo a L y K es igual a la potencia r-ésima del polinomio minimal de x sobre K.

Sea $(y_i)_{i=1,\ldots,q}$ una base de $\mathrm{K}[x]$ sobre K y $(z_j)_{j=1,\ldots,r}$ una base de L sobre $\mathrm{K}[x]$. Luego $(y_i z_j)$ es una base de L sobre K y se tiene $n = qr$ (§3, proposición 1). Sea $\mathrm{M} = (a_{ih})$ la matriz de la multiplicación por x en $\mathrm{K}[x]$ respecto a la base (y_i): es decir, se tiene que $xy_i = \sum_h a_{ih} y_h$. Se sigue que $x(y_i z_j) = (\sum_h a_{ih} y_h)\, z_j = \sum_h a_{ih}(y_h z_j)$. Ordenando la base $(y_i z_j)$ de L sobre K de forma lexicográfica, vemos que la matriz M' de la multiplicación por x

en L respecto a esta base es una matriz diagonal por bloques:

$$\mathrm{M}_1 = \begin{vmatrix} \mathrm{M} & 0 & \cdots & 0 \\ 0 & \mathrm{M} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{M} \end{vmatrix}$$

Como la matriz $\mathrm{X} \cdot \mathrm{I} - \mathrm{M}_1$ es una matriz diagonal por bloques de la forma $\mathrm{X} \cdot \mathrm{I}_q - \mathrm{M}$, se sigue que $\det(\mathrm{X} \cdot \mathrm{I}_n - \mathrm{M}_1) = (\det(\mathrm{X} \cdot \mathrm{I}_q - \mathrm{M}))^r$. Como el miembro de la izquierda es $\mathrm{P}(\mathrm{X})$ y $\det(\mathrm{X} \cdot \mathrm{I}_q - \mathrm{M})$ es el polinomio minimal de x sobre K por lo demostrado en la primera parte, la proposición queda demostrada. LQQD.

Para terminar, veamos un resultado sobre la traza y la norma de elementos enteros.

Proposición 2. *Sea* A *un dominio íntegro,* K *su cuerpo de fracciones,* L *una extensión de* K *de grado finito y* x *un elemento de* L *entero sobre* A. *Supongamos que* K *es de característica cero. Entonces los coeficientes del polinomio característico* $\mathrm{P}(\mathrm{X})$ *de* x *respecto a* L *y* K *(en particular,* $\mathrm{Tr}_{\mathrm{L/K}}(x)$ *y* $\mathrm{N}_{\mathrm{L/K}}(x)$*), son enteros sobre* A.

Utilizamos la proposición 1: se tiene $\mathrm{P}(\mathrm{X}) = (\mathrm{X} - x_1) \cdots (\mathrm{X} - x_n)$. Los coeficientes de $\mathrm{P}(\mathrm{X})$ son, salvo el signo, sumas de productos de los x_i. Basta demostrar que los x_i son enteros sobre A (§1, corolario 1 de la proposición 1). Como cada x_i es conjugado con x sobre K (§4), se tienen K-isomorfismos $\sigma_i : \mathrm{K}[x] \to \mathrm{K}[x_i]$ tales que $\sigma_i(x) = x_i$. Aplicando σ_i a una ecuación de dependencia entera de x sobre A, se obtiene una ecuación de dependencia entera de x_i sobre A.

Corolario. *Supongamos además que* A *es íntegramente cerrado. Entonces los coeficientes del polinomio característico de* x *(en particular* $\mathrm{Tr}_{\mathrm{L/K}}(x)$ *y* $\mathrm{N}_{\mathrm{L/K}}(x)$*) pertenecen a* A.

En efecto, los coeficientes son elementos de K por definición y son enteros sobre A por la proposición 2.

> *Observemos que las cantidades* $x + \sigma(x)$ *y* $x \cdot \sigma(x)$ *que utilizamos en el estudio de los cuerpos cuadráticos (§5) son la traza y la norma de* x. *De hecho, probamos allí (§5,* (3)*) un caso particular del corolario anterior.*

7. Discriminante

Definición 1. *Sea* B *un anillo y* A *un subanillo de* B *tal que* B *es un* A*-módulo libre de rango finito* n*. Si* $(x_1,\dots,x_n)\in \mathrm{B}^n$*, llamamos discriminante del sistema* $(x_1,\dots,x_n)$ *al elemento de* A *definido por*

$$\mathrm{D}(x_1,\dots,x_n)=\det(\mathrm{Tr}_{\mathrm{B/A}}(x_ix_j)). \tag{1}$$

Proposición 1. *Si* $(y_1,\dots,y_n)\in \mathrm{B}^n$ *es otro sistema de elementos de* B *tal que* $y_i=\sum_{j=1}^n a_{ij}x_j$ *con* $a_{ij}\in \mathrm{A}$*, se tiene*

$$\mathrm{D}(y_1,\dots,y_n)=\det(a_{ij})^2\mathrm{D}(x_1,\dots,x_n). \tag{2}$$

En efecto, se tiene $\mathrm{Tr}(y_py_q)=\mathrm{Tr}\left(\sum_{i,j}a_{pi}a_{qj}x_ix_j\right)=\sum_{i,j}a_{pi}a_{qj}\,\mathrm{Tr}(x_iy_j)$, de donde se sigue la igualdad de matrices $(\mathrm{Tr}(y_py_q))=(a_{pi})\cdot(\mathrm{Tr}(x_ix_j))\cdot{}^t(a_{qj})$ (donde ${}^t\mathrm{M}$ denota le transpuesta de la matriz M). Para terminar basta tomar determinantes en esta igualdad. LQQD.

Se sigue de la proposición 1 que los discriminantes de dos bases cualesquiera de B sobre A son **asociados** en A: en efecto, la matriz de cambio de base (a_{ij}) es inversible por lo que su determinante es inveresible. Por lo tanto, podemos hacer la

Definición 2. *Bajo las hipótesis de la definición 1, llamamos discriminante de* B *sobre* A*, y lo notamos* $\mathfrak{D}_{\mathrm{B/A}}$*, al ideal principal de* A *generado por el discriminante de una base cualquiera de* B *sobre* A*.*

Proposición 2. *Supongamos que* $\mathfrak{D}_{\mathrm{B/A}}$ *contiene un elemento que no es divisor de cero. Entonces, para que un sistema* $(x_1,\dots,x_n)\in \mathrm{B}^n$ *sea una base de* B *sobre* A *es necesario y sufciente que* $\mathfrak{D}_{\mathrm{B/A}}$ *esté generado por* $\mathrm{D}(x_1,\dots,x_n)$*.*

La necesidad fue demostrada más arriba. Supongamos que $d=\mathrm{D}(x_1,\dots,x_n)$ genera $\mathfrak{D}_{\mathrm{B/A}}$. Sea $(e_1,\dots,e_n)$ une base cualquiera de B sobre A. Escribamos $d'=\mathrm{D}(e_1,\dots,e_n)$ y $x_i=\sum_{j=1}^n a_{ij}e_j$ con $a_{ij}\in \mathrm{A}$. Se tiene $d=\det(a_{ij})^2d'$. Por hipótesis se tiene $\mathrm{A}d=\mathfrak{D}_{\mathrm{B/A}}=\mathrm{A}d'$. Luego, existe $b\in \mathrm{A}$ tal que $d'=bd$, de donde $d(1-b\det(a_{ij})^2)=0$. Se sigue que d no puede ser un divisor de cero, pues sino todo los elementos de $\mathrm{A}d=\mathfrak{D}_{\mathrm{B/A}}$ serían divisores de cero. Por lo tanto, deducimos que $1-b\det(a_{ij})^2=0$, lo que muestra que $\det(a_{ij})$ es inversible y por lo tanto también lo es la matriz (a_{ij}). En consecuencia, $(x_1,\dots,x_n)$ es una base de B sobre A.

Proposición 3. *Sea* K *un cuerpo finito o de característica cero,* L *une extensión de* K *de grado finito* n *y* $\sigma_1,\dots,\sigma_n$ *los* n K*-isomorfismos distintos de*

L *en un cuerpo algebraicamente cerrado* C *que contiene a* K *(§4, teorema 1). Entonces si* $(x_1,\dots,x_n)$ *es una base de* L *sobre* K, *se tiene*

$$\mathrm{D}(x_1,\dots,x_n) = \det(\sigma_i(x_j))^2 \neq 0. \tag{3}$$

La primera igualdad resulta de un cálculo fácil:

$$\mathrm{D}(x_1,\dots,x_n) = \det(\mathrm{Tr}(x_i x_j)) = \det\left(\sum_k \sigma_k(x_i y_j)\right) = \det\left(\sum_k \sigma_k(x_i)\sigma_k(x_j)\right)$$
$$= \det(\sigma_k(x_i)) \cdot \det(\sigma_k(x_j)) = \det(\sigma_i(x_j))^2.$$

Sólo resta demostrar que $\det(\sigma_i(x_j)) \neq 0$. Razonemos por el absurdo. Si $\det(\sigma_i(x_j)) = 0$, existen $u_1,\dots,u_n \in \mathrm{C}$, no todos nulos, tales que $\sum_{i=1}^n u_i\sigma_i(x_j) = 0$ para todo j. Por linealidad, se deduce $\sum_{i=1}^n u_i\sigma_i(x) = 0$ para todo $x \in \mathrm{L}$. Esto contradice el siguiente resultado:

Lema de Dedekind. *Sea* G *un grupo,* C *un cuerpo y* $\sigma_1,\dots,\sigma_n$ *homomorfismos distintos de* G *en el grupo multiplicativo* C^*. *Entonces los* σ_i *son linealmente independientes sobre* C *(i.e.* $\sum_i u_i\sigma_i(g) = 0$ *para todo* $g \in \mathrm{G}$ *implica que todos los* u_i *son nulos*).

Supongamos que los σ_i son linealmente dependientes y consideremos una relación no trivial $\sum_i u_i\sigma_i = 0$ ($u_i \in \mathrm{C}$) tal que el número q de los u_i no nulos sea *mínimo.* Renumerando si es necesario, podemos suponer que

$$u_1\sigma_1(g) + \cdots + u_q\sigma_q(g) = 0 \quad \text{para todo } g \in \mathrm{G}. \tag{4}$$

Necesariamente $q \geq 2$ pues los σ_i no son todos nulos. Si g y h son dos elementos cualesquiera de G, se tiene

$$u_1\sigma_1(hg) + \cdots + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0.$$

Multiplicando (4) por $\sigma_1(h)$ y restando de la última ecuación, obtenemos

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_1(g) + \cdots + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

Como esta ecuación vale para todo $g \in \mathrm{G}$ y q se eligió mínimo, se sigue que $u_2(\sigma_1(h) - \sigma_2(h)) = 0$, de donde $\sigma_1(h) = \sigma_2(h)$ pues $u_2 \neq 0$. Esto contradice la hipótesis de que σ_i son distintos. LQQD.

Observación. En las condiciones de la proposición 3, la relación $\mathrm{D}(x_1,\dots,x_n) \neq 0$ significa que la forma bilineal $(x,y) \mapsto \mathrm{Tr}_{\mathrm{L/K}}(xy)$ es **no degenerada,** es decir que $\mathrm{Tr}_{\mathrm{L/K}}(xy) = 0$ para todo $y \in \mathrm{L}$ implica que $x = 0$. De esta manera, la aplicación K-lineal que a cada $x \in \mathrm{L}$ le hace corresponder la forma K-lineal $s_x : y \mapsto \mathrm{Tr}_{\mathrm{L/K}}(xy)$ es una inyección de L en su dual $\mathrm{Hom_K}$(L,K) (con la estructura natural de espacio vectorial sobre K). Como L y $\mathrm{Hom_K}$(L,K) tienen

la misma dimensión finita n sobre K se sigue que $x \mapsto s_x$ es un isomorfismo. La existencia de **"bases duales"** en un espacios vectorial y su dual muestra entonces que, para toda base $(x_1, \ldots, x_n)$ de L sobre K, existe otra base $(y_1, \ldots, y_n)$ tal que

$$\mathrm{Tr}_{\mathrm{L/K}}(x_y y_j) = \delta_{ij} \quad (1 \leq i, j \leq n). \tag{5}$$

Esta observación nos será útil en lo que sigue.

Teorema 1. *Sea* A *un anillo íntegramente cerrado,* K *su cuerpo de fracciones,* L *una extensión de* K *de grado finito* n *y* A′ *la clausura íntegra de* A *en* L. *Supongamos que* K *es de característica cero. Entonces* A′ *es un sub-*A*-módulo de un* A*-módulo libre de rango* n.

Sea $(x_1, \ldots, x_n)$ una base de L sobre K. Cada x_i es algebraico sobre K, por lo que se tiene $a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_0$ con $a_j \in \mathrm{A}$ para $j = 0, \ldots, n$. Multiplicando por una potencia de x_i podemos suponer que $a_n \neq 0$. Multiplicando por a_n^{n-1} vemos que $a_n x_i$ es entero sobre A. Sea $x_i' = a_n x_i$. Entonces $(x_1', \ldots, x_n')$ es una base de L sobre K contenida en A′.

Por la observación de más arriba, existe otra base $(y_1, \ldots, y_n)$ de L sobre K tal que $\mathrm{Tr}(x_i' y_j) = \delta_{ij}$ (5). Sea $z \in \mathrm{A}'$. Como $(y_1, \ldots, y_n)$ es una base de L sobre K, podemos escribir $z = \sum_{j=1}^n b_j y_j$ con $b_j \in \mathrm{K}$. Para todo i se tiene $x_i' z \in \mathrm{A}'$ (pues $x_i' \in \mathrm{A}'$), de donde $\mathrm{Tr}(x_i' z) \in \mathrm{A}$ (§6, corolario de la proposición 2). Como

$$\mathrm{Tr}(x_i' z) = \mathrm{Tr}\left(\sum_j b_j x_i' y_j\right) = \sum_j b_j \,\mathrm{Tr}(x_i' y_j) = \sum b_j \delta_{ij} = b_i$$

se sigue que $b_i \in \mathrm{A}$ para todo i. Por lo tanto A′ está contenido en el A-módulo libre $\sum_{j=1}^n \mathrm{A} y_j$. LQQD.

Corolario. *Bajo las hipótesis del teorema 1, supongamos además que* A *es un dominio de ideales principales. Entonces* A′ *es un* A*-módulo libre de rango* n.

En efecto, en este caso un submódulo de un A-módulo libre es de nuevo libre (capítulo I, §5, teorema 1, *b*)) y de rango $\leq n$. Por otra parte, vimos en la demostración del teorema 1 que A′ contiene una base de L sobre K y por lo tanto es de rango n.

A modo de ejercicio, el lector que no esté familiarizado con el contenido de la observación que precede al teorema 1 puede tratar de encontrar una demostración más calculadora ??? del siguiente teorema:

con la notación de arriba, sea $d = \mathrm{D}(x'_1,\ldots,x'_n)$ *y supongamos que* $z = \sum_i c_i x'_i$ *(*$c_i \in \mathrm{K}$*) es entero sobre* A. *Entonces* $dc_i \in \mathrm{A}$ *(calcular* $\mathrm{Tr}(zx'_j)$ *y utilizar la fórmula de Cramer).*

Un ejemplo de cálculo de discriminante. Sea K un cuerpo finito o de característica cero, $\mathrm{L} = \mathrm{K}[x]$ una extension de K de grado finito n y F(X) el polinomio minimal de x sobre K. Entonces

$$\mathrm{D}(1,x,\ldots,x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{\mathrm{L/K}}(\mathrm{F}'(x)) \tag{6}$$

(donde F′(X) denote el polinomio derivado de F(X)). En efecto, sean $x_1,\ldots,x_n$ las raíces de F(X) en una extensión de K. Estos son los conjugados de x (§3, proposición 3 y §4). Se tiene

$$\begin{aligned}
\mathrm{D}(1,x,\ldots,x^{n-1}) &= \det(\sigma_i(x^j))^2 \text{ (proposición 3)} = \det(x_i^j)^2 \\
(-1)^{\frac{n(n-1)}{2}} \det(x_i^j)^2 &= \prod_{i\neq j}(x_i - x_j) \text{ (Vandermonde)} = \prod_i \left(\prod_{j\neq i}(x_i - x_j) \right) \\
&= \prod_i \mathrm{F}'(x_i) = \mathrm{N}_{\mathrm{L/K}}(\mathrm{F}'(x))
\end{aligned}$$

(pues los $\mathrm{F}'(x_i)$ son los conjugados de $\mathrm{F}'(x)$).

En particular, apliquemos (6) al caso donde F(X) es un **trinomio** $\mathrm{X}^n + a\mathrm{X} + b$ ($a,b \in \mathrm{K}$). Sea $y = \mathrm{F}'(x)$. Se tiene

$$y = nx^{n-1} + x = -(n-1)a - nbx^{-1}$$

(pues $x^n + ax + b = 0$, de donde $nx^{n-1} = -na - nbx^{-1}$). Se deduce que $x = -nb(y+(n-1)a)^{-1}$. El polinomio minimal de y sobre K es el numerador de $\mathrm{F}(-nb(\mathrm{Y} + (n-1)a)^{-1})$. Haciendo las cuentas, calculamos que es $(\mathrm{Y} + (n-1)a)^n - na(\mathrm{Y} + (n-1)a)^{n-1} + (-1)^n b^{n-1}$. La norma de y es el producto de $(-1)^n$ y el término constante de este polinomio, es decir,

$$n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

Se sigue que

$$\mathrm{D}(1,x,\ldots,x^{n-1}) = \left[n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n\right](-1)^{\frac{n(n-1)}{2}}. \tag{7}$$

Si $n = 2$ (resp. 3), recobramos la conocida fórmula $4b - a^2$ (resp. $-4a^3 - 27b^2$).

8. Terminología de los cuerpos de números

Llamamos **cuerpo de números algebraicos** (o **cuerpo de números**) a toda extensión de $\mathbf{Q}$ de grado finito (y por lo tanto algebraica). Dado un cuerpo de números K, el grado $[K : \mathbf{Q}]$ se llama **grado** de K. Un cuerpo de números de grado 2 (resp. 3) se llama **cuerpo cuadrático** (cf. §5) (resp. **cuerpo cúbico**). Un cuerpo de números tiene característica cero.

Dado un cuerpo de números K, los elementos de K que son enteros sobre $\mathbf{Z}$ se llaman **enteros** de K. Forman un **subanillo** A de K (§1, corolario 2 de la proposición 1) que es un $\mathbf{Z}$-módulo **libre** de rango $[K : \mathbf{Q}]$ (§7, corolario del teorema 1). Los discriminantes de las diferentes bases del $\mathbf{Z}$-módulo A difieren en un elementos inversible de $\mathbf{Z}$ (§7, definición 2), que además es un cuadrado (§7, proposición 1). Luego este elemento es necesariamente $+1$, de manera que los discriminantes de dos bases cualesquiera del $\mathbf{Z}$-módulo A son **iguales;** su valor en común se llama **discriminante absoluto,** o **discriminante,** de K.

Como un cuerpo de números K determina de forma unívoca al anillo A de los enteros de K, a veces haremos un abuso del lenguaje y le atribuiremos a K propiedades de A. Así, cuando hablemos de ideales (o de unidades) de K, se trata de ideales (o unidades) de A.

9. Cuerpos ciclotómicos

Llamamos **cuerpo ciclotómico** a todo cuerpo generado sobre $\mathbf{Q}$ por raíces de la unidad. Dado un número primo p, denotamos z una raíz primitiva p-ésima de la unidad (como elemento de $\mathbf{C}$ por ejemplo). Ahora estudiaremos el cuerpo ciclotómico $\mathbf{Q}[z]$. El número z es raíz del polinomio $X^p - 1$. Como z es $\neq 1$, también es raíz del polinomio $\frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1$, llamado **polinomio ciclotómico.** No es inmediatamente evidente el hecho de que este polinomio es irreducible sobre $\mathbf{Q}$ (equivalentemente, $\mathbf{Q}[z]$ tiene grado $p-1$). Para demostrarlo nos hará falta el

Criterio de Eisenstein. *Sea* A *un anillo principal,* $p \in A$ *un elemento primo de* A *y* $F(X) = X^n + a_{n-1}x^{n-1} + \cdots + a_1X + a_0$ *un elemento de* $A[X]$ *tal que* p *divide a todos los* a_i *(*$0 \leq i \leq n-1$*), pero tal que* p^2 *no divide a* a_0*. Entonces* $F(X)$ *es irreducible sobre el cuerpo de fracciones* K *de* A*.*

Supongamos en efecto que se tiene $F = G \cdot H$ con $G, H \in K[X]$, G y H **mónicos.** Las raíces de F son **enteras** sobre A. Como todas las raíces de G (resp. H) son raíces de F, éstas son todas enteras sobre A (§1, corolario 1 de la proposición 1). Como A es un dominio de ideales principales, y por lo tanto íntegramente cerrado (§2, ex. 2), se tiene que $G \in A[X]$ y $H \in A[X]$.

Sean ahora $\overline{\mathrm{F}}$, $\overline{\mathrm{G}}$, $\overline{\mathrm{H}}$ las imágenes de F, G, H en $(\mathrm{A}/\mathrm{A}p)[\mathrm{X}]$, de manera que $\overline{\mathrm{F}} = \overline{\mathrm{G}} \cdot \overline{\mathrm{H}}$. Por la hipótesis en los a_i, se tiene $\overline{\mathrm{F}} = \mathrm{X}^n$. Como $\mathrm{A}/\mathrm{A}p$ es un **dominio íntegro,** la descomposición $\mathrm{X}^n = \overline{\mathrm{G}} \cdot \overline{\mathrm{H}}$ es necesariamente de la forma $\mathrm{X}^n = \mathrm{X}^q \cdot \mathrm{X}^{n-q}$ (pues $\overline{\mathrm{G}}$ y $\overline{\mathrm{H}}$ son mónicos), de donde $\overline{\mathrm{G}} = \mathrm{X}^q$ y $\overline{\mathrm{H}} = \mathrm{X}^{n-q}$. Si G y H son ambos no constantes, se sigue que p divide los términos constantes de G y H y por lo tanto p^2 divide al término constante a_0 de F, lo que contradice la hipótesis. Por lo tanto, o bien G o bien H es constante y por lo tanto F es irreducible. LQQD.

Ejemplo. El polinomio $\mathrm{X}^3 - 2\mathrm{X} + 6$ es irreducible sobre $\mathbf{Q}$ (tomar $p = 2$, $\mathrm{A} = \mathbf{Z}$).

Teorema 1. *Para todo número primo p, el polinomio ciclotómico* $\mathrm{X}^{p-1} + \mathrm{X}^{p-2} + \cdots + \mathrm{X} + 1$ *es irreducible en* $\mathbf{Q}[\mathrm{X}]$.

En efecto, pongamos $\mathrm{X} = \mathrm{Y} + 1$. Se tiene

$$\mathrm{X}^{p-1} + \cdots + 1 = \frac{\mathrm{X}^p - 1}{\mathrm{X} - 1} = \frac{(\mathrm{Y}+1)^p - 1}{\mathrm{Y}}$$
$$= \mathrm{Y}^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} \mathrm{Y}^{j-1} = \mathrm{F}_1(\mathrm{Y}).$$

Como p divide a todos los coeficientes binomiales $\binom{p}{j}$ pero p^2 no divide al término constante $\binom{p}{1} = p$, $\mathrm{F}_1(\mathrm{Y})$ es irreducible por el criterio de Eisenstein y por lo tanto también lo es el polinomio ciclotómico. LQQD.

Seguimos denotando por z una raíz p-ésima primitiva de la unidad. Resulta del teorema 1 que el cuerpo $\mathbf{Q}[z]$ tiene grado $p-1$ y $(1, z, \ldots, z^{p-2})$ es una base de $\mathbf{Q}[z]$ sobre $\mathbf{Q}$. Ahora investigaremos el anillo de enteros de $\mathbf{Q}[z]$ y demostraremos que es $\mathbf{Z}[z]$.

Para ello, nos hará falta calcular algunas **trazas y normas** (escribiremos $\mathrm{Tr}(x)$ y $\mathrm{N}(x)$ en vez de $\mathrm{Tr}_{\mathbf{Q}[z]/\mathbf{Q}}(x)$ y $\mathrm{N}_{\mathbf{Q}(z)/\mathbf{Q}}(x)$). Observemos que los conjugados de z sobre $\mathbf{Q}$ son los z^j, $(j = 1, \ldots, p-1)$ (teorema 1).

La irreducibilidad del polinomio ciclotómica implica:

$$\mathrm{Tr}(z) = -1, \quad \mathrm{Tr}(1) = p - 1, \tag{1}$$

de donde se sigue $\mathrm{Tr}(z^j) = -1$ para $j = 1, \ldots, p-1$ y por lo tanto

$$\mathrm{Tr}(1 - z) = \mathrm{Tr}(1 - z^2) = \cdots = \mathrm{Tr}(1 - z^{p-1}) = p. \tag{2}$$

Por otra parte el cálculo hecho en la demostración del teorema 1 muestra que $\mathrm{N}(z-1) = (-1)^{p-1}p$, de donde $\mathrm{N}(1-z) = p$. Como la norma de $1 - z$ es el

producto de todos los conjugados de $1-z$, obtenemos

$$p = (1-z)(1-z^2)\dots(1-z^{p-1}). \tag{3}$$

Notemos A al anillo de enteros de $\mathbf{Q}[z]$. Evidentemente A contiene a z y a sus potencias. Ahora demostraremos que

$$\mathrm{A}(1-z) \cap \mathbf{Z} = p\mathbf{Z}. \tag{4}$$

En efecto se tiene $p \in \mathrm{Z}(1-z)$ por (3), de donde $\mathrm{A}(1-z)\cap\mathbf{Z} \supset p\mathbf{Z}$. Como $p\mathbf{Z}$ es un ideal maximal de $\mathbf{Z}$, la relación $\mathrm{A}(1-z)\cap\mathbf{Z} \neq p\mathbf{Z}$ implicaría $\mathrm{A}(1-z)\cap\mathbf{Z} = \mathbf{Z}$ y $1-z$ sería inversible en A. Entonces sus conjugados también lo serían y por lo tanto p sería inversible por (4). Es decir, $\frac{1}{p}$ sería entero sobre $\mathbf{Z}$, lo que es absurdo (§2, ex. 2).

Mostremos por último que, para todo $y \in \mathrm{A}$, se tiene

$$\mathrm{Tr}(y(1-z)) \in p\mathbf{Z}. \tag{5}$$

En efecto cada conjugado $y_j(1-z^j)$ de $y(1-z)$ es múltiplo (en A) de $1-z^j$, que es a su vez múltiplo de $1-z$ pues

$$1-z^j = (1-z)(1+z+\dots+z^{j-1}).$$

Como la traza es la suma de los conjugados se sigue que

$$\mathrm{Tr}(y(1-z)) \in \mathrm{A}(1-z),$$

de donde se sigue (5) utilizando (4) y el hecho de que la traza de un entero pertenece a $\mathbf{Z}$ (§6, corolario de la proposición 2).

Ahora estamos listos para determinar el anillo de enteros de $\mathbf{Q}[z]$.

Teorema 2. *Sea p un número primo y z una raíz primitiva p-ésima de la unidad (en $\mathbf{C}$). Entonces el anillo* A *de enteros del cuerpo ciclotómico* $\mathbf{Q}[z]$ *es* $\mathbf{Z}[z]$ *y* $(1,z,\dots,z^{p-2})$ *es una base del* $\mathbf{Z}$*-módulo* A.

En efecto, sea $x = a_0 + a_1 z + \dots + a_{p-2}z^{p-2}$ ($a_i \in \mathbf{Q}$) un elemento de A. Entonces se tiene

$$x(1-z) = a_0(1-z) + a_1(z-z^2) + \dots + a_{p-2}(x^{p-2} - z^{p-1})$$

Tomando trazas en ambos lados de la igualdad, resulta de (1) y (2) que

$$\mathrm{Tr}(x(1-z)) = a_0\,\mathrm{Tr}(1-z) = a_0 p,$$

de donde, utilizando (5), $pa_0 \in p\mathbf{Z}$ y por lo tanto $a_0 \in \mathbf{Z}$. Como $z^{-1} = z^{p-1}$ se sigue que $z^{-1} \in \mathrm{A}$, de donde $(x-a_0)z^{-1} = a_1 + a_2 z + \dots + a_{p-2}z^{p-3} \in \mathrm{A}$. Aplicando la primer parte del argumento a este elemento deducimos que $a_1 \in \mathbf{Z}$. Aplicando sucesivamente este procedimiento, vemos que todos los $a_i \in \mathbf{Z}$. LQQD.

Observación. Lo que hicimios en esta § se extiende sin dificultad a cuerpos ciclotómicos $\mathbf{Q}[t]$ donde t es una raíz primitiva p^r-ésima de la unidad (p primo). Un tal cuerpo tiene grado $p^{r-1}(p-1)$ y su anillo de enteros es $\mathbf{Z}[t]$. El polinomio minimal de t sobre $\mathbf{Q}$ es

$$\mathrm{X}^{p^{r-1}(p-1)} + \mathrm{X}^{p^{r-1}(p-2)} + \cdots + \mathrm{X}^{p^{r-1}} + 1 = \frac{\mathrm{X}^{p^r} - 1}{\mathrm{X}^{p^{r-1}} - 1}.$$

Apéndice. El cuerpo de los números complejos es algebraicamente cerrado

Dado un cuerpo K, consideremos las siguientes propiedades:

(a) Todo polinomio de grado > 0 sobre K es un producto de polinomios lineales.
(b) Todo polinomio de grado > 0 sobre K admite una raíz en K.

Es claro que *a*) implica *b*). Reciprocamente, si *b*) es verdad, P(X) es un polinomio de grado $d \geq 1$ sobre K y $a \in \mathrm{K}$ es una raíz de P(X), entonces P(X) es un múltiplo de $\mathrm{X} - a$, y una inducción en el grado d muestra que *a*) es verdad. Un cuerpo K que satisface las condiciones equivalentes *a*) y *b*) se dice **algebraicamente cerrado.**

Mostraremos ahora que $\mathbf{C}$ ($= \mathbf{R}[i]$, $i^2 = -1$) es algebraicamente cerrado utilizando un método que se debe esencialmente a Lagrange. De los números reales sólamente utilizaremos las siguientes propiedades:

1. Todo polinomio de grado impar sobre $\mathbf{R}$ admite una raíz en $\mathbf{R}$; este es un caso fácil del teorema del valor intermedio.
2. Todo polinomio de grado dos sobre $\mathbf{C}$ tiene sus raíces en $\mathbf{C}$. Un cálculo fácil con "$ax^2 + bx + c = 0$" muestra que es suficiente demostrar que todo $z = a + bi \in \mathbf{C}$ (a,$b \in \mathbf{R}$) posee una raíz cuadrado en $\mathbf{C}$. Como $(x + iy)^2 = a + ib$ (x,$y \in \mathbf{R}$) es equivalente a $x^2 - y^2 = a$, $2xy = b$, se debe tener que $a^2 + b^2 = (x^2 + y^2)^2$ o $x^2 + y^2 = \sqrt{a^2 + b^2}$. Deducimos los valores de x^2 e y^2, de donde obtenemos aquellos de x e y.
3. Dado un polinomio no constante $\mathrm{P(X)} \in \mathrm{K[X]}$, existe una extensión K' de K tal que P(X) se descompone en factores lineales en $\mathrm{K}'[\mathrm{X}]$. Esto fue demostrado de manera sencilla en la proposición 3 de §3 (aquella demostración es casi completamente independiente del material que la precede, basta saber que, si F(X) es irreducible, $\mathrm{K[X]/(F(X))}$ es un cuerpo y hacer un demostración por inducción).
4. Las relaciones entre los coeficientes y las raíces de un polinomio.

5. El hecho de que un polinomio simétrico $G(X_1,\dots,X_n) \in K[X_1,\dots,X_n]$ es un polinomio en las funciones simétricas elementales $\sum X_i$, $\sum X_iX_j$, ..., $X_1\cdots X_n$ de las X_i.

Finalmente, tenemos el

Teorema. *El cuerpo de los números complejos es algebraicamente cerrado.*

Demostraremos la parte (b), que todo polinomio no constante $P(X) \in \mathbf{C}[X]$ admite una raíz en $\mathbf{C}$. Considerando $F(X) = P(X)\overline{P}(X)$ ($\overline{P}$: el polinomio cuyos coeficientes son los conjugados complejos de los coeficientes correspondientes de P) podemos suponer que $P(X)$ tiene coeficientes reales: en efecto, si $a \in \mathbf{C}$ es una raíz de $F(X)$, entonces o bien a es raíz de $P(X)$ o bien a es raíz de $\overline{P}(X)$ y en este caso $\overline{a}$ es raíz de $P(X)$. Ahora escribimos el grado de $F(X)$ ($\in \mathbf{R}[X]$) en la manera $d = 2^n q$, donde q es impar. Razonaremos por inducción en el **exponente** n de 2.

Si $n = 0$, d es impar y $F(X)$ posee una raíz en $\mathbf{R}$. (cf. 1)). Supongamos que $n \geq 1$. Por 3) existe una extensión K' de $\mathbf{C}$ y elementos $x_1,\dots,x_d \in K'$ tales que $F(X) = \prod_{i=1}^{d}(X - x_i)$ (suponiendo que $F(X)$ es mónico, lo que está permitido). Sea c un elemento arbitrario de $\mathbf{R}$; consideremos los elementos $y_{ij} = x_i + x_j + cx_ix_j$ de K' ($i \leq j$). Hay $\frac{1}{2}d(d+1) = 2^{n-1}q(d+1)$ de estos números y $q(d+1)$ es **impar.** El polinomio $G(X) = \prod_{i\leq j}(X - y_{ij})$ tiene coeficientes que son polinomios simétricos el los x_i con coeficientes reales. Por 5) son entonces necesariamente polinomios con coeficientes reales en las funciones simétricas elementales de los x_i y por lo tanto los coeficientes de $G(X)$ son reales por 4). Como el grado es de la forma $2^{n-1} \times$ (impar), le hipótesis inductiva muestar que $G(X)$ admite una raíz $z_c \in \mathbf{C}$. Luego, alguno de los y_{ij}, por ejemplo $y_{i(c),j(c)} = x_{i(c)} + y_{j(c)} + cx_{i(c)}x_{j(c)}$ es igual a z_c.

Como $\mathbf{R}$ es **infinito** y el conjunto de los pares (i,j) ($i \leq j$) es finito, existen dos números reales distintos c, c' tales que $i(c) = i(c')$ y $j(c) = j(c')$. Sean r, s estos índices. Luego $x_r + x_s + cx_rx_s = z_c \in \mathbf{C}$ y

$$x_r + x_s + c'x_rx_s = z_{c'} \in \mathbf{C}.$$

Restando esta ecuación de la análoga con c se deduce que $x_r + x_s \in \mathbf{C}$ y $x_rx_s \in \mathbf{C}$. Luego, por 4), x_r y x_s son raíces de una ecuación de segundo grado con coeficientes en $\mathbf{C}$. Como $\mathbf{C} \subset K'$, se tiene que $x_r, x_s \in \mathbf{C}$ por 2). Así, hemos demostrado que $F(X)$ posee una raíz en $\mathbf{C}$ y el teorema está demostrado.

La demostración dada parece apropiada para un curso opcional o de primer ciclo, y también en una lección...

CAPÍTULO III

Anillos noetherianos y anillos de Dedekind

El lector que quiere saber porqué introducimos los anillos de Dedekind puede dirigirse a §4 y leer el ejemplo y la discusión que siguen al teorema 1. Los anillos noetherianos, de los cuales estudiaremos un mínimo de propiedades, son más generales que los anillos de Dedekind. Los introducimos para poder enunciar estas propiedades en su nivel natural de generalidad y también porque juegan un rol fundamental en otras aplicaciones del álgebra, por ejemplo en en Geometría Algebraica. Por último, el pasaje de los anillos noetherianos a los módulos del mismo nombre es otro caso de "linearización", una técnica cuya eficacia el lector ya a podido comprobar.

1. Módulos y anillos noetherianos

En el capítulo I, §4, teorema 1 demostramos el siguiente resultado:

Teorema 1. *Sea* A *un anillo y* M *un* A*-módulo. Las siguientes condiciones son equivalentes:*

a) *Toda familia no vacía de submódulos de* M *posee un elemento maximal.*
b) *Toda sucesión creciete de submódulos de* M *se estaciona.*
c) *Todo submódulo de* M *es de tipo finito.*

Definición 1. *Un* A*-módulo* M *se dice noetheriano si satisface las condiciones equivalentes del teorema 1. Un anillo* A *se dice noetheriano si, considerado como un* A*-módulo, es un módulo noetheriano.*

Vimos (capítulo I, §4, corolario del teorema 1) que un dominio de ideales principales es noetheriano.

Proposición 1. *Sea* A *un anillo,* E *un* A*-módulo y* E′ *un submódulo de* E*. Para que* E *sea noetheriano es necesario y suficiente que* E′ *y* E/E′ *sean noetherianos.*

Demostremos la necesidad. Supongamos que E es noetheriano. El conjunto ordenado de los submódulos de E′ (resp. E/E′) es isomorfo al conjunto ordenado de los submódulos de E contenidos en E′ (resp. conteniendo E′). Por lo tanto, E′ y E/E′ son noetherianos por *a*) o *b*).

Reciprocamente, supongamos que E′ y E/E′ son noetherianos. Sea $(F_n)_{n\geq 0}$ una sucesión creciente de submódulos de E. Como E′ es noetheriano, existe un entero n_0 tal que $F_n \cap E' = F_{n+1} \cap E'$ para todo $n \geq n_0$. Como E/E′ es noetheriano, existe un entero n_1 tal que

$$(F_n + E')/E' = (F_{n+1} + E')/E' \text{ para todo } n \geq n_1.$$

Por lo tanto se tiene $F_n + E' = F_{n+1} + E'$. Tomemos $n \geq \sup(n_0,n_1)$ y mostremos que se tiene $F_n = F_{n+1}$. Bata ver que $F_{n+1} \subset F_n$. Sea $x \in F_{n+1}$. Como $F_{n+1}+E' = F_n+E'$, existen $y \in F_n$ y $z',z'' \in E'$ tales que $x+z' = y+z''$. Luego, $x - y = z'' - z' \in F_{n+1} \cap E'$. Como $F_{n+1} \cap E' = F_n \cap E'$, se tiene $x - y \in F_n$, de donde $x \in F_n$ pues $y \in F_n$. Así $F_{n+1} = F_n$ para todo $n \geq \sup(n_0,n_1)$ y E es noetheriano por *b*).

Corolario 1. *Sea* A *un anillo,* $E_1,\ldots,E_n$ A*-módulos noetherianos. Entonces el* A*-módulo producto* $\prod_{i=1}^{n} E_i$ *es noetheriano.*

Si $n = 2$, E_1 se identifica con el submódulo $E_1 \times (0)$ de $E_1 \times E_2$ y el cociente correspondiente es isomorfo a E_2, por lo que el resultado se sigue en este caso de la proposición 1. El caso general se deduce haciendo inducción en n.

Corolario 2. *Sea* A *un anillo noetheriano y* E *un* A*-módulo de tipo finito. Entonces* E *es un* A*-módulo noetheriano* (*y por lo tanto todo submódulo es de tipo finito*).

En efecto (capítulo I, §4), E es isomorfo a un módulo cociente A^n/R (donde n es el cardinal de un sistema finito de generadores de E). Como A^n es noetheriano por el corolario 1, A^n/R también lo es por la proposición 1.

2. Aplicación a los elementos enteros

Proposición 1. *Sea* A *un anillo noetheriano íntegramente cerrado,* K *su cuerpo de fracciones,* L *una extensión de* K *de grado finito n y* A′ *la clausura íntegra de* A *en* L. *Supongamos que* K *es de característica cero. Entonce* A′ *es un* A*-módulo de tipo finito y un anillo noetheriano.*

En efecto, sabemos que A′ es un submódulo de un A-módulo libre de rango n (capítulo II, §7, teorema 1). Por lo tanto, A′ es un A-módulo de tipo finito (§1, corolario 2 de la proposición 1) y por lo tanto noetheriano (ibid).

Por otra parte los ideales de A' son casos particulares de sub-A-módulos de A'. Por lo tanto satisfacen la condición de maximalidad (§1, teorema 1, *a*) de manera que A' es un anillo noetheriano.

Ejemplo. El anillo de los enteros de un cuerpo de números L es **noetheriano** (poner $A = \mathbf{Z}$, $K = \mathbf{Q}$).

3. Algunos preliminares sobre ideales

Un ideal $\mathfrak{p}$ de un anillo A se dice **primo** si el anillo cociente $A/\mathfrak{p}$ es un **dominio íntegro.** Equivalentemente, las condiciones $x \in A - \mathfrak{p}$, $y \in A - \mathfrak{p}$ implican $xy \in A - \mathfrak{p}$ o, en otras palabras, que el complemento $A - \mathfrak{p}$ de $\mathfrak{p}$ es estable por multiplicación.

Para que un ideal $\mathfrak{m}$ de A sea **maximal** (es decir, maximal entre los ideales de A distintos a A), es necesario y suficiente que $A/\mathfrak{m}$ no tenga otros ideales que él mismo y (0). Es decir que $A/\mathfrak{m}$ sea un **cuerpo.** En particular, **todo ideal maximal es primo.** La recíproca es falsa, por ejemplo el ideal (0) de $\mathbf{Z}$ es primo pero no maximal.

Lema 1. *Sea* A *un anillo,* $\mathfrak{p}$ *un ideal primo de* A *y* A' *un subanillo de* A. *Entonces* $p \cap A'$ *es un ideal primo de* A'.

En efecto, $\mathfrak{p} \cap A'$ es el núcleo del homomorfismo compuesto $A' \to A \to A/\mathfrak{p}$, de manera que se tiene un homomorfismo inyectivo $A'/\mathfrak{p} \cap A' \to A/\mathfrak{p}$. Como un subanillo de un dominio íntegro es un dominio íntegro, el resultado está demostrado.

Dados dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ de un anillo A, llamamos **producto** de $\mathfrak{a}$ y $\mathfrak{b}$, y lo notamos $\mathfrak{ab}$, no sólamente al conjunto de los productos ab, donde $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ (conjunto que en general no es un ideal), pero al conjunto de **sumas finitas** $\sum a_i b_i$ de tales productos. Es fácil ver que $\mathfrak{ab}$ es un **ideal** de A y que se tiene

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}.$$

> *En general no hay una igualdad: en un dominio de ideales principales el miembro de la izquierda corresponde al producto, y el de la derecha a su m.c.m.*

El producto de ideales es asociativo y conmutativo y A funciona como elemento neutro.

> *Dados un* A*-módulo* E, *un submódulo* F *y un ideal* $\mathfrak{a}$ *de* A, *definimos de la misma manera el producto* $\mathfrak{a}$F*; es un submódulo de* E.

Lema 2. *Si un ideal primo* $\mathfrak{p}$ *de un anillo* A *contiene un producto de ideales* $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n$*, entonces* $\mathfrak{p}$ *contiene uno de ellos.*

En efecto, si $\mathfrak{a}_i \not\subset \mathfrak{p}$ para todo i, existe $a_i \in \mathfrak{a}_i$ tal que $a_i \notin \mathfrak{p}$. Se tiene entonces que $a_1\cdots a_n \notin \mathfrak{p}$ pues $\mathfrak{p}$ es primo. Pero también $a_1\cdots a_n \in \mathfrak{a}_1\cdots\mathfrak{a}_n$. Contradicción.

Lema 3. *En un anillo noetheriano, todo ideal contiene un producto de ideales primos. En un dominio íntegro noetheriano* A*, todo ideal no nulo contiene un producto de ideales primos no nulos.*

Utilizaremos un argumento típico de la teoría de anillos noetherianos. Demostremos la segunda afirmación (la demostración de la primera es análoga: simplemente hay que borrar tres veces "no nulos"). Razonemos por el absurdo. Entonces la familia Φ de ideales no nulos de A que no contienen ningún producto de ideales primos no nulos es **no vacía.** Como A es noetheriano, Φ admite un elemento **maximal** $\mathfrak{b}$ (§1, teorema 1, *a*)). El ideal $\mathfrak{b}$ no es primo pues sino contendría el producto consistente en sí mismo. Luego, existen $x, y \in \mathrm{A} - \mathfrak{b}$ tal que $xy \in \mathfrak{b}$. Los ideales $\mathfrak{b} + \mathrm{A}x$ y $\mathfrak{b} + \mathrm{A}y$ contienen estrictamente a $\mathfrak{b}$, por lo que no pertenecen a Φ pues $\mathfrak{b}$ es maximal en Φ. Por lo tanto contienen productos de ideales primos no nulos:

$$\mathfrak{b} + \mathrm{A}x \supset \mathfrak{p}_1\cdots\mathfrak{p}_n, \quad \mathfrak{b} + \mathrm{A}y \supset \mathfrak{q}_1\cdots\mathfrak{q}_r$$

Como $xy \in \mathfrak{b}$, se tiene que

$$(\mathfrak{b} + \mathrm{A}x)(\mathfrak{b} + \mathrm{A}y) \subset \mathfrak{b}\,; \quad \text{de donde} \quad \mathfrak{p}_1\cdots\mathfrak{p}_n\mathfrak{q}_1\cdots\mathfrak{q}_r \subset \mathfrak{b},$$

lo que es una contradicción.

Sea ahora A un **dominio íntegro** y K su cuerpo de fracciones. Llamamos **ideal fraccionario** de A (o de K respecto a A) a todo sub-A-módulo I de K tal que existe $d \in \mathrm{A}$, $d \neq 0$ que satisface $\mathrm{I} \subset d^{-1}\mathrm{A}$. Esto quiere decir que los elementos de I tienen un "denominador común" $d \in \mathrm{A}$. Los ideales ordinarios de A son ideales fraccionarios (con $d = 1$). Los llamamos **ideales enteros** si hay riezgo de confusión. Todo sub-A-módulo **de tipo finito** I de K es un ideal fraccionario. En efecto, si $(x_1, \ldots, x_n)$ es un sistema finito de generadores de I, los x_i tienen un denominador común d (por ejemplo el producto de los denominadores d_i, donde $x_i = a_i d_i^{-1}$ con $a_i, d_i \in \mathrm{A}$) y d sirve de denominador común de I. Recíprocamente, si A es **noetheriano,** todo ideal fraccionario I es un A-módulo de **tipo finito:** en efecto, se tiene $\mathrm{I} \subset d^{-1}\mathrm{A}$ y $d^{-1}\mathrm{A}$ es un A-módulo isomorfo a A, luego noetheriano.

Definimos el **producto** II' de dos ideales fraccionario I, I′ como el conjunto de sumas finitas $\sum x_i y_i$ donde $x_i \in \mathrm{I}$ y $y_i \in \mathrm{I}'$. Si I e I′ son ideales fraccionarios

con denominadores comunes d y d', entonces los conjuntos

$$\mathrm{I} \cap \mathrm{I}', \quad \mathrm{I} + \mathrm{I}', \quad \mathrm{II}'$$

son **ideales fraccionarios.** En efecto, es claro que son sub-A-módulos de K y admiten como denominador común, respectivamente, a d (o d'), dd' y dd'. Los ideales fraccionarios no nulos de A forman un **monoide** conmutativo con la multiplicación.

4. Anillos de Dedekind

Definición 1. *Un anillo* A *se llama* **anillo de Dedekind** *si es noetheriano e íntegramente cerrado (en particular, un dominio íntegro) y si todo ideal primo no nulo de* A *es maximal.*

El anillo **Z** y, más generalmente, todo dominio de ideales principales es un anillo de Dedekind. El anillo de enteros de un cuerpo de números es un anillo de Dedekind como consecuencia del teorema siguiente:

Teorema 1. *Sea* A *un anillo de Dedekind,* K *su cuerpo de fracciones,* L *una extensión de* K *de grado finito y* A′ *la clausura íntegra de* A *en* L. *Supongamos que* K *tiene característica cero. Luego,* A′ *es un anillo de Dedekind y un* A*-módulo de tipo finito.*

En efecto, A′ es íntegramente cerrado por construcción, noetheriano y A-módulo de tipo finito por la proposición de §2. Resta demostrar que todo idel primo $\mathfrak{p}' \neq (0)$ de A′ es maximal. Tomemos un elemento $x \neq 0$ de $\mathfrak{p}'$ y consideremos una ecuación de dependencia entera de x sobre A de grado mínimo:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in \mathrm{A}) \tag{1}$$

Necesariamente $a_0 \neq 0$, pues sino podríamos dividir por x y obtendríamos una ecuación de dependencia íntegral de grado $n-1$. Por (1), se tiene que $a_0 \in \mathrm{A}'x \cap \mathrm{A} \subset \mathfrak{p}' \cap \mathrm{A}$. Por lo tanto, $\mathfrak{p}' \cap \mathrm{A} \neq (0)$. Como $\mathfrak{p}' \cap \mathrm{A}$ es un ideal primo de A (§3, lema 1), $\mathfrak{p}' \cap \mathrm{A}$ es un ideal maximal de A, y $\mathrm{A}/\mathfrak{p}' \cap \mathrm{A}$ es un cuerpo. Pero $\mathrm{A}/\mathfrak{p}' \cap \mathrm{A}$ se identifica con un subanillo de $\mathrm{A}'/\mathfrak{p}'$ y $\mathrm{A}'/\mathfrak{p}'$ es **entero** sobre $\mathrm{A}/\mathfrak{p}' \cap \mathrm{A}$ pues A′ es entero sobre A. Luego, $\mathrm{A}'/\mathfrak{p}'$ es un cuerpo (capítulo II, §1, proposición 3), de manera que $\mathfrak{p}'$ es maximal. LQQD.

El interes en los anillos de Dedekind proviene de que el anillo de enteros de un cuerpo de números es un anillo de Dedekind pero no siempre un dominio de ideales principales.

Ejemplo. Consideremos el anillos de enteros $\mathrm{A} = \mathbf{Z}[\sqrt{-5}]$ de $\mathbf{Q}[\sqrt{-5}]$ (capítulo II, §5, teorema 1). Se tiene

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

Las normas de los cuatro factores son, respectivamente, 6, 6, 4 y 9. Luego $1 + \sqrt{-5}$ no puede tener un divisor no trivial en A, pues la norma de un tal divisor sería un divisor no trivial de 6, pero las ecuaciones

$$a^2 + 5b^2 = 2 \quad \text{y} \quad a^2 + 5b^2 = 3$$

no tienen soluciones en $\mathbf{Z}$. Si A es un dominio de ideales principales, el elemento $1 + \sqrt{-5}$ que divide al producto $2 \cdot 3$ por (2) (BOOK IS WRONG?), debería dividir a alguno de los factores, pero entonces, tomando normas, 6 dividiría a 4 o a 9, lo que es imposible.

Históricamente, el teórico de números Kummer (1810–1893) se dió cuenta de que ciertos anillos de enteros de cuerpos de números (de hecho, de cuerpos ciclotómicos, relacionados con sus trabajos sobre la ecuación de Fermat; cf. I, §2) no eran dominios de ideales principales. Para superar, al menos en parte, estos inconvenientes, Kummer y Dedekind (1831–1916) introdujeron la noción de **ideal,** y Dedekind estudió los anillos que hoy llevan su nombre. El principal interés de los dominios de ideales principales es la existencia de descomposición única en factores primos. En los anillos de Dedekind, esto se generaliza felizmente a una descomposición única en **ideales primos,** que es útil en muchos sentidos y que describiremos a continuación:

Teorema 2. *Sea* A *un anillo de Dedekind que no es un cuerpo. Todo ideal maximal de* A *es inversible en el monoide de ideales fraccionarios de* A.

Sea $\mathfrak{m}$ un ideal maximal de A. Se tiene $\mathfrak{m} \neq (0)$ pues A no es un cuerpo. Sea

$$\mathfrak{m}' = \{x \in \mathrm{K} \mid x\mathfrak{m} \subset \mathrm{A}\} \tag{3}$$

Es claro que $\mathfrak{m}'$ es un sub-A-módulo de K y que admite como denominador común cualquier elemento no nulo de $\mathfrak{m}$. Por lo tanto, $\mathfrak{m}'$ es un ideal fraccionario de A. Basta demostrar que $\mathfrak{m}'\mathfrak{m} = \mathrm{A}$. Como $\mathfrak{m}'\mathfrak{m} \subset \mathrm{A}$ por (3) y es claro que $\mathrm{A} \subset \mathfrak{m}'$ (pues $\mathfrak{m}$ es un ideal) se sigue que $\mathfrak{m} = \mathrm{A}\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$. Como $\mathfrak{m}$ es maximal y $\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset \mathrm{A}$ se deduce que, o bien $\mathfrak{m}'\mathfrak{m} = \mathrm{A}$, o bien $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. Solo queda probar que $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ es imposible.

Si $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ y $x \in \mathfrak{m}'$ se tiene $x\mathfrak{m} \subset \mathfrak{m}$ de donde $x^2\mathfrak{m} \subset x\mathfrak{m} \subset \mathfrak{m}$ y, por inducción, $x^n\mathfrak{m} \subset \mathfrak{m}$ para todo $n \in \mathbf{N}$. Luego, cualquier elemento no nulo d de $\mathfrak{m}$ sirve de denominador común para todos los x^n, de manera que $\mathrm{A}[x]$ es un ideal fraccionario de A. Como A es noetheriano, $\mathrm{A}[x]$ es un A-módulo de tipo

finito (§3, al final), por lo que x es **entero** sobre A (capítulo II, §1, teorema 1). Como A es íntegramente cerrado, se tiene $x \in \mathrm{A}$. Hemos demostrado que $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ implica $\mathfrak{m}' = \mathrm{A}$. Resta ver que $\mathfrak{m}' = \mathrm{A}$ es imposible.

En efecto, tomemos un elemento no nulo $a \in \mathfrak{m}$. El ideal $\mathrm{A}a$ contiene un producto $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$ de ideales primos no nulos (§3, lema 3). Podemos suponer que n es mínimo. Se tiene $\mathfrak{m} \supset \mathrm{A}a \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$ por lo que $\mathfrak{m}$ debe contener algun $\mathfrak{p}_i$ (§3, lema 2), por ejemplo $\mathfrak{p}_1$. Como $\mathfrak{p}_1$ es maximal por hipótesis, se sigue que $\mathfrak{m} = \mathfrak{p}_1$. Sea $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, de manera que $\mathrm{A}a \supset \mathfrak{m}\mathfrak{b}$, pero $\mathrm{A}a \not\supset \mathfrak{b}$ pues n es minimal. Existe entonces un elemento $b \in \mathfrak{b}$ tal que $b \notin \mathrm{A}a$. Como $\mathfrak{m}\mathfrak{b} \subset \mathrm{A}a$, se tiene $\mathfrak{m}b \subset \mathrm{A}a$, de donde $\mathfrak{m}ba^{-1} \subset \mathrm{A}$. La definición (3) de $\mathfrak{m}'$ implica que $ba^{-1} \in \mathfrak{m}'$. Pero como $b \notin \mathrm{A}a$, se sigue que $ba^{-1} \notin \mathrm{A}$ y por lo tanto $\mathfrak{m}' \neq \mathrm{A}$. LQQD.

Teorema 3. *Sea* A *un anillo de Dedekind,* P *el conjunto de ideales primos no nulos de* A.

1. *Todo ideal fraccionario no nulo* $\mathfrak{b}$ *de* A *se escribe de una única manera de la forma*

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathrm{P}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})} \tag{4}$$

   donde los $n_{\mathfrak{p}}(\mathfrak{b})$ *son números enteros, casi todos nulos.*
2. *El monoide de ideales fraccionarios no nulos de* A *es un grupos.*

Demostremos primero la afirmación de **existencia** de *a*), es decir que todo ideal fraccionario $\mathfrak{b}$ es producto de potencias (≥ 0 o ≤ 0) de ideles primos. Sabemos que existe un elemento no nulo de A tal que $d\mathfrak{b} \subset \mathrm{A}$, i.e. tal que $d\mathfrak{b}$ es un ideal entero de A. Como $\mathfrak{b} = (d\mathfrak{b}) \cdot (\mathrm{A}d)^{-1}$, podemos suponer que $\mathfrak{b}$ es un ideal entero. Ahora argumentamos como en el lema 3 de la §3 y consideramos la familia Φ de los ideales $\neq (0)$ de A que no son productos de ideales primos. Supongamos, por el absurdo, que Φ es no vacía. Entonces admite un elemento maximal $\mathfrak{a}$ pues A es noetheriano. Se tiene $\mathfrak{a} \neq \mathrm{A}$ pues A es el producto de la familia vacía de ideales primos. Luego $\mathfrak{a}$ está contenido en un ideal maximal $\mathfrak{p}$, a saber un elemento maximal de la familia de los ideales no triviales de A que contienen a $\mathfrak{a}$. Sea $\mathfrak{p}'$ el ideal (fraccionario) inverso a $\mathfrak{p}$ Como $\mathfrak{a} \subset \mathfrak{p}$ se deduce que $\mathfrak{a}\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = \mathrm{A}$. Como $\mathfrak{p}' \supset \mathrm{A}$, se tiene $\mathfrak{a}\mathfrak{p}' \supset \mathfrak{a}$, e incluso $\mathfrak{a}\mathfrak{p}' \neq \mathfrak{a}$: en efecto, si $\mathfrak{a}\mathfrak{p}' = \mathfrak{a}$ y $x \in \mathfrak{p}'$, se tiene $x\mathfrak{a} \subset \mathfrak{a}$, $x^n\mathfrak{a} \subset \mathfrak{a}$ para todo n, x es entero sobre A y luego $x \in \mathrm{A}$ (como en el teorema 2). Pero esto es imposible pues $\mathfrak{p}' \neq \mathrm{A}$ (sino $\mathfrak{p}' = \mathrm{A}$ y $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$). Como $\mathfrak{a}$ es maximal en Φ, se sigue que $\mathfrak{a}\mathfrak{p}' \in \Phi$ y por lo tanto $\mathfrak{a}\mathfrak{p}'$ debe ser un producto $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ de ideales primos. Multiplicando por $\mathfrak{p}$, vemos que $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Es decir, todo ideal entero de A es un producto de ideales primos.

Pasemos ahora a la afirmación de **unicidad** de *a*). Supongamos que se tiene $\prod_{p\in \mathrm{P}} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p}\in \mathrm{P}} \mathfrak{p}^{m(\mathfrak{p})}$, es decir $\prod_{\mathfrak{p}\in \mathrm{A}} \mathfrak{p}^{n(\mathfrak{p})-m(\mathfrak{p})} = \mathrm{A}$. Si los $n(\mathfrak{p})-m(\mathfrak{p})$ no son todos nulos, podemos separar los exponentes en positivos y negativos y obtener:

$$\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s} \tag{5}$$

con $\mathfrak{p}_i,\mathfrak{q}_j \in \mathrm{P}$, $\alpha_i > 0$, $\beta_j > 0$, $\mathfrak{p}_i \neq \mathfrak{q}_j$ para todo i,j. Como $\mathfrak{p}_1$ contiene a $\mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s}$, contiene a unos de los $\mathfrak{q}_j$ (§3, lema 2), supongamos $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Como $\mathfrak{p}_1$ y $\mathfrak{q}_1$ son ambos maximales, esto implica que $\mathfrak{p}_1 = \mathfrak{q}_1$, lo que es una contradicción.

Por último, (4) muestra que $\prod_{\mathfrak{p}\in \mathrm{P}} \mathfrak{p}^{-n_{\mathfrak{p}}(\mathfrak{b})}$ es el inverso de $\mathfrak{b}$, lo que demuestra *b*).

Observación. Acabamos de ver que el monoide I(A) de ideales fraccionarios no nulos de un anillo de Dedekind A es un grupo. Los ideales fraccionarios **principales** (es decir, los de la forma $\mathrm{A}x$, $x \in \mathrm{K}^*$) forman un subgrupo F(A) de I(A) (pues $(\mathrm{A}x)\cdot(\mathrm{A}y)^{-1} = \mathrm{A}xy^{-1}$). El grupo cociente $\mathrm{C(A)} = \mathrm{I(A)/F(A)}$ se llama el **grupo de clases de ideales** de A. Para que A sea un dominio de ideales principales es necesario y suficiente que C(A) consista únicamente del elemento neutro.

Terminemos con un **formulario,** en el cual $n_{\mathfrak{p}}(\mathfrak{b})$ denote el exponente de $\mathfrak{p}$ en la descomposición de $\mathfrak{b}$ como producto de ideales primos (cf. (4)).

$$n_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b}) \quad \text{(trivial)} \tag{6}$$

$$\mathfrak{b} \subset \mathrm{A} \iff n_{\mathfrak{p}}(\mathfrak{b}) \geq 0 \text{ para todo } \mathfrak{p} \in \mathrm{P} \tag{7}$$

($\Longrightarrow$ se sigue de la demostración del teorema 3; $\Leftarrow$ es trivial)

$$\mathfrak{a} \subset \mathfrak{b} \iff n_{\mathfrak{p}}(\mathfrak{a}) \geq n_{\mathfrak{p}}(\mathfrak{b}) \text{ para todo } \mathfrak{p} \in \mathrm{P}. \tag{8}$$

(en efecto, $\mathfrak{a} \subset \mathfrak{b}$ equivale a $\mathfrak{a}\mathfrak{b}^{-1} \subset \mathrm{A}$; aplicamos (6) y (7))

$$n_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) = \inf(n_{\mathfrak{p}}(\mathfrak{a}),n_{\mathfrak{p}}(\mathfrak{b})) \tag{9}$$

(pues $\mathfrak{a}+\mathfrak{b}$ es el supremo de $\mathfrak{a}$ y $\mathfrak{b}$ para la inclusión de ideales; para terminar aplicar (8))

$$n_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b}) = \sup(n_{\mathfrak{p}}(\mathfrak{a}),n_{\mathfrak{p}}(\mathfrak{b})) \tag{10}$$

(razón análoga, las desigualdades se invierten en (8))

5. Norma de un ideal

En toda esta §, K *denota un cuerpo de números, n su grado y* A *el anillo de enteros de* K. Escribimos $\mathrm{N}(x)$ en lugar de $\mathrm{N}_{\mathrm{K}/\mathbf{Q}}(x)$.

Proposición 1. *Si x es un elemento no nulo de* A*, se tiene* $|\mathrm{N}(x)| = \mathrm{card}(\mathrm{A}/\mathrm{A}x)$.

> *Notemos que, como $x \in \mathrm{A}$, se tiene $\mathrm{N}(x) \in \mathbf{Z}$ (capítulo II, §6, corolario de la proposición 2), de manera que la fórmula anterior tiene sentido.*

Sabemos que A es un $\mathbf{Z}$-módulo libre de rango n (capítulo II, §8) y $\mathrm{A}x$ es un sub-$\mathbf{Z}$-módulo de A. También es de rango n pues la multiplicación por x es un isomorfismo $\mathrm{A} \to \mathrm{A}x$. Por lo visto en el capítulo I, §5, teorema 1, existe una base $(e_1, \ldots, e_n)$ del $\mathbf{Z}$-módulo A y elementos c_i de $\mathbf{N}$ tales que $(c_1e_1, \ldots, c_ne_n)$ es una base de $\mathrm{A}x$. Luego $\mathrm{A}/\mathrm{A}x$ es isomorfo a $\prod_{i=1}^{n} \mathbf{Z}/c_i\mathbf{Z}$ y su cardinal es $c_1c_2 \cdots c_n$. Sea u la aplicación $\mathbf{Z}$-lineal de A sobre $\mathrm{A}x$ definida por $u(e_i) = c_ie_i$ para $i = 1, \ldots, n$. Se tiene $\det(u) = c_1 \cdots c_n$.

Por otra parte, $(xe_1, \ldots, xe_n)$ es otra base de $\mathrm{A}x$. Por lo tanto tenemos un automorfismo v del $\mathbf{Z}$-módulo $\mathrm{A}x$ tal que $v(c_ie_i) = xe_i$. Como $\det(v)$ es inversible en $\mathbf{Z}$, se tiene que $\det(v) = \pm 1$. Pero entonces $v \circ u$ no es otra cosa que multiplicación por x y su determinante es, por definición, $\mathrm{N}(x)$ (capítulo II, §6, definición 1). Como $\det(v \circ u) = \det(v) \cdot \det(u)$, deducimos que $\mathrm{N}(x) = \pm c_1c_2 \cdots c_n = \pm\,\mathrm{card}(\mathrm{A}/\mathrm{A}x)$.

Definición 1. *Dado un ideal entero no nulo $\mathfrak{a}$ de* A*, llamamos norma de $\mathfrak{a}$, y notamos* $\mathrm{N}(\mathfrak{a})$*, al número* $\mathrm{card}(\mathrm{A}/\mathfrak{a})$.

Observemos que $\mathrm{N}(\mathfrak{a})$ es **finito.** En efecto, si a es un elemento no nulo de $\mathfrak{a}$, se tiene $\mathrm{A}a \subset \mathfrak{a}$ y $\mathrm{A}/\mathfrak{a}$ se identifica con un cociente de $\mathrm{A}/\mathrm{A}a$. De esto que $\mathrm{card}(\mathrm{A}/\mathfrak{a}) \leq \mathrm{card}(\mathrm{A}/\mathrm{A}a)$, que es finito por la proposición 1. Al mismo tiempo, esto demuestra que para un ideal principal $\mathrm{A}b$ se tiene $\mathrm{N}(\mathrm{A}b) = |\mathrm{N}(b)|$.

Proposición 2. *Si $\mathfrak{a}$ y $\mathfrak{b}$ son dos ideales enteros no nulos de* A*, se tiene* $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.

Descomponiendo $\mathfrak{b}$ en un producto de ideales maximales (§4, teorema 3), vemos que basta demostrar que se tiene $\mathrm{N}(\mathfrak{a}\mathfrak{m}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{m})$ para $\mathfrak{m}$ maximal. Como $\mathfrak{a}\mathfrak{m} \subset \mathfrak{a}$, tenemos $\mathrm{card}(\mathrm{A}/\mathfrak{a}\mathfrak{m}) = \mathrm{card}(\mathrm{A}/\mathfrak{a})\,\mathrm{card}(\mathfrak{a}/\mathfrak{a}\mathfrak{m})$. Luego, basta probar que $\mathrm{card}(\mathfrak{a}/\mathfrak{a}\mathfrak{m}) = \mathrm{card}(\mathrm{A}/\mathfrak{m})$. Ahora bien, $\mathfrak{a}/\mathfrak{a}\mathfrak{m}$ es un A-módulo anulado por $\mathfrak{m}$, y por lo tanto, un espacio vectorial sobre $\mathrm{A}/\mathfrak{m}$. Sus subespacios vectoriales son sub-A-módulos y por lo tanto son de la forma $\mathfrak{q}/\mathfrak{a}\mathfrak{m}$, donde $\mathfrak{q}$ es un ideal tal que $\mathfrak{a}\mathfrak{m} \subset \mathfrak{q} \subset \mathfrak{a}$. Pero la fórmula (8) de §4 muestra que

no hay ningún ideal contenido estrictamente entre $\mathfrak{am}$ y $\mathfrak{a}$. Luego el espacio vectorial $\mathfrak{a}/\mathfrak{am}$ es de dimensión uno sobre $\mathrm{A}/\mathfrak{m}$ y se tiene en consecuencia que $\mathrm{card}(\mathfrak{a}/\mathfrak{am}) = \mathrm{card}(\mathrm{A}/\mathfrak{m})$. LQQD.

CAPÍTULO IV

Clases de ideales y el teorema de las unidades

El presente capítulo está consagrado a dos teorema importantes de finitud. Nos serán útiles algunas herramientas del Análisis (tomadas prestadas de la Topología y la integración en $\mathbf{R}^n$).

1. Preliminares sobre subgrupos discretos de $\mathbf{R}^n$

Un subgrupo aditivo H de $\mathbf{R}^n$ es discreto si y sólo si para todo compacto K de $\mathbf{R}^n$, la intersección $\mathrm{H} \cap \mathrm{K}$ es finita. Un ejemplo típico de subgrupo discreto de $\mathbf{R}^n$ es $\mathbf{Z}^n$. Ahora demostraremos que este es esencialmente el único:

Teorema 1. *Sea* H *un subgrupo discreto de* $\mathbf{R}^n$. *Entonces* H *está generado (como* $\mathbf{Z}$*-módulo) por* r *vectores linealmente independientes sobre* $\mathbf{R}$ *(en particular,* $r \leq n$*).*

Elijamos, en efecto, un sistema $(e_1, \ldots, e_r)$ de elementos de H que sean linealmente independientes sobre $\mathbf{R}$ y tal que r sea máximo. Sea

$$\mathrm{P} = \left\{ \sum_{i=1}^{r} \alpha_i e_i \mid 0 \leq \alpha_i \leq 1 \right\} \subset \mathbf{R}^n \tag{1}$$

el paralelotopo ???? construido con estos vectores. Es claro que P es compacto y por lo tanto $\mathrm{P} \cap \mathrm{H}$ es finito. Sea $x \in \mathrm{H}$. Como r es maximal, x se escribe $x = \sum_{i=1}^{r} \lambda_i e_i$ con $\lambda_i \in \mathbf{R}$. Consideremos entonces, para $j \in \mathbf{Z}$, el elemento

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \tag{2}$$

(donde $[\mu]$ denota la parte entera de $\mu \in \mathbf{R}$). Se tiene que

$$x_j = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i,$$

de donde $x_j \in \mathrm{P}$ y $x_j \in \mathrm{P} \cap \mathrm{H}$ por (2). Si observamos que $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$, vemos que el $\mathbf{Z}$-módulo H está generado por $\mathrm{P} \cap \mathrm{H}$, y por lo tanto es de **tipo finito.**

Por otra parte, como $\mathrm{P} \cap \mathrm{H}$ es finito y $\mathbf{Z}$ es infinito, existen dos enteros distintos j y k tales que $x_j = x_k$. Se sigue entonces de (2) que, para estos enteros, se tiene $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$, lo que muestra que los λ_i son **racionales.** Así el $\mathbf{Z}$-módulo H está generado por un número **finito** de elementos, todos ellos combinaciones lineales de los (e_i) con coeficientes racionales. Sea d un denominador común ($d \in \mathbf{Z}$, $d \neq 0$) de estos coeficientes. Se tiene entonces que $d\mathrm{H} \subset \sum_{i=1}^{r} \mathbf{Z} e_i$. Por lo tanto existe una base (f_i) del $\mathbf{Z}$-módulo $\sum_{i=1}^{r} \mathbf{Z} e_i$ y elementos $\alpha_i \in \mathbf{Z}$ tales que $(\alpha_1 f_1, \ldots, \alpha_r f_r)$ generan $d\mathrm{H}$ (capítulo I, §5, teorema 1). Como el $\mathbf{Z}$-módulo tiene el mismo rango que H y $\mathrm{H} \supset \sum_{i=1}^{r} \mathbf{Z} e_i$, el rango de $d\mathrm{H}$ es $\geq r$ y por lo tanto es igual a r y los α_i son todos no nulos. Como los (f_i) son, al igual que los (e_i), linealmente independientes sobre $\mathbf{R}$, vemos que $d\mathrm{H}$, y por lo tanto también H, está generado (sobre $\mathbf{Z}$) por r elementos linealmente independientes sobre $\mathbf{R}$.

Observación (Ejemplo de aplicación). Sea $t = (\theta_1, \ldots, \theta_n) \in \mathbf{R}^n$ tal que alguno de los θ_i es **irracional.** Sea $(e_1, \ldots, e_n)$ la base canónica de $\mathbf{R}^n$ y H el subgrupo de $\mathbf{R}^n$ generado sobre $\mathbf{Z}$ por $(e_1, \ldots, e_n, t)$. H no es discreto pues sino, aplicando el teorema 1, t sería combinación lineal racional de los e_i. Por lo tanto, dado $\varepsilon > 0$, existen un elemento no nulo de H a distancia menor que ε del 0. Por lo tanto existen enteros $p_i \in \mathbf{Z}$, $q \in \mathbf{N}$, $q \neq 0$, tales que $|q\theta_i - p_i| \leq \varepsilon$, es decir $\left|\theta_i - \frac{p_1}{q}\right| \leq \frac{\varepsilon}{q}$. Observemos que la estimación simplista de θ_i entre dos múltiplos consecutivos de $\frac{1}{q}$ sólo produce la aproximación $\left|\theta_i - \frac{n_i}{q}\right| \leq \frac{1}{2q}$ ($n_i \in \mathbf{Z}$). Este resultado en uno de los primeros resultados de la rica teoría de aproximación de números irracionales por números racionales. Para más detalles sobre esta teoría, ver Koksma, "Diophantische Approximationen", Berlin (Springer), 1936.

Definición 1. *Un subgrupo discreto de rango n de $\mathbf{R}^n$ se llama un reticulado de $\mathbf{R}^n$.*

Por el teorema 1, un reticulado está generado sobre $\mathbf{Z}$ por una base de $\mathbf{R}^n$ que es entonces una $\mathbf{Z}$-base del mismo. Para cada $\mathbf{Z}$-base $e = (e_1, \ldots, e_n)$ de un reticulado H, denotamos por P_e el paralepípedo semi-abierto $\mathrm{P}_e = \{\sum_{i=1}^{n} \alpha_i e_i \mid 0 \leq \alpha_i < 1\}$; Así todo punto de $\mathbf{R}^n$ es congruente módulo H a un único punto de P_e (decimos en este caso que P_e es un **dominio fundamental** para H). Escribiremos μ para la **medida de Lebesgue** en $\mathbf{R}^n$, de forma

que, para todo subconjunto medible S de $\mathbf{R}^n$, $\mu(\mathrm{S})$ denotará su medida (que nosotros llamaremos también su volúmen).

Lema 1. *El volúmen $\mu(\mathrm{P}_e)$ es independiente de la base e elegida.*

En efecto, sea $(f_1,\ldots,f_n)$ otra base de H. Se tiene $f_i = \sum_{j=1}^n \alpha_{ij} e_j$ para algunos $\alpha_{ij} \in \mathbf{Z}$. Es bien sabido el efecto de una transformación lineal en el volúmen y se tiene $\mu(\mathrm{P}_f) = |\det(\alpha_{ij})|\,\mu(\mathrm{P}_e)$. Pero, como es un determinante de un cambio de base, $\det(\alpha_{ij})$ es inversible en $\mathbf{Z}$, por lo tanto igual a ± 1. Se concluye que $\mu(\mathrm{P}_f) = \mu(\mathrm{P}_e)$.

El volúmen de uno cualquiera de los P_e se llama el **volúmen del reticulado** H y se nota $v(\mathrm{H})$ (la palabra "volúmen" aquí es un abuso del lenguaje, pues $\mu(\mathrm{H}) = 0$. ¿Tal vez sería mejor decir "malla" del reticulado H?).

Teorema 2 (Minkowski)**.** *Sea* H *un reticulado de* $\mathbf{R}^n$ *y* S *un subconjunto medible de* $\mathbf{R}^n$ *tal que* $\mu(\mathrm{S}) > v(\mathrm{H})$*. Entonces existen dos elementos distintos x, y de* S *tales que* $x - y \in \mathrm{H}$.

En efecto, sea $e = (e_1,\ldots,e_n)$ una $\mathbf{Z}$-base de H y P_e el paralepípedo semiabierto construido con e. Como P_e es un dominio fundamental para H, S es la unión disjunta de los $\mathrm{S} \cap (h + \mathrm{P}_e)$ $(h \in \mathrm{H})$. Se sigue que

$$\mu(\mathrm{S}) = \sum_{h\in\mathrm{H}} \mu(\mathrm{S} \cap (h + \mathrm{P}_e)) \tag{3}$$

Como μ es invariante por translaciones, se tiene

$$\mu(\mathrm{S} \cap (h + \mathrm{P}_e)) = \mu((-h + \mathrm{S}) \cap \mathrm{P}_e)$$

Por otra parte, los conjuntos $(-h + \mathrm{S}) \cap \mathrm{P}_e$ $(h \in \mathrm{H})$ no pueden ser disjuntos dos a dos, pues de ser así, $\mu(\mathrm{P}_e) \geq \sum_{h\in\mathrm{H}} \mu((-h+\mathrm{S})\cap\mathrm{P}_e)$, que contradice (3) y la hipótesis $\mu(\mathrm{P}_e) = v(\mathrm{H}) < \mu(\mathrm{S})$. Luego existen dos elementos distintos h, h' de H tales que $\mathrm{P}_e \cap (-h + \mathrm{S}) \cap (-h' + \mathrm{S}) \neq \emptyset$. Por lo tanto se tienen dos elementos x, y de S tales que $-h + x = -h' + y$, de donde $x - y = h - h' \in \mathrm{H}$ y $x \neq y$ pues $h \neq h'$. LQQD.

Corolario. *Sea* H *un reticulado de* $\mathbf{R}^n$*,* S *un subconjunto medible, simétrico respecto a* 0 *y convexo en* $\mathbf{R}^n$*. Supongamos que una de las siguientes condiciones es verdad:*

a) *se tiene* $\mu(\mathrm{S}) > 2^n v(\mathrm{H})$
b) *se tiene* $\mu(\mathrm{S}) \geq 2^n v(\mathrm{H})$ *y* S *es compacto.*

Entonces $\mathrm{S} \cap \mathrm{H}$ *contiene un punto distinto a* 0.

En el caso a), aplicamos el teorema 1 a

$$S' = \frac{1}{2}S \quad \left(\text{pues } \mu(S') = \frac{1}{2^n}\mu(S) > v(H)\right);$$

luego existen dos puntos distintos z, y de S′ tales que $y - z \in H$. Entonces $x = y - z = \frac{1}{2}(2y + (-2z))$ es un punto de S (pues S es simétrico y convexo), que satisface la conclusión. En el caso b), aplicamos el caso a) a $(1 + \varepsilon)S$) ($\varepsilon > 0$). Poniendo $H' = H - \{0\}$, vemos que $H' \cap (1 + \varepsilon)S$ es no vacío, y es finito pues es compacto y discreto. Entonces $\bigcap_{\varepsilon>0} H' \cap (1 + \varepsilon)S$ es no vacío. Un elemento de esta intersección pertenece a $\bigcap_{\varepsilon>0}(1 + \varepsilon)S$, conjunto que es igual a S pues S es compact. LQQD.

La hipótesis de compacidad es necesaria en b), como lo muestra el paralepípedo abierto $\{\sum_{i=1}^{n} \lambda_i e_i \mid -1 < \lambda_i < +1\}$ *y el reticulado de base* (e_i).

2. La inmersión canónica de un cuerpo de números

Sea K un cuerpo de números y n su grado. Vimos (capítulo II, §4, teorema 1) que se tienen n isomorfismos distintos $\sigma_i : K \to \mathbf{C}$. Tenemos exactamente n pues el polinomio minimal de un elemento primitovo de K sobre $\mathbf{Q}$ (**ibid.**, corolario del teorema 1) tiene n raíces en $\mathbf{C}$. Sea $\alpha : \mathbf{C} \to \mathbf{C}$ la conjugación compleja. Entonces, para todo i, $\alpha \circ \sigma_i$ es uno de los σ_j y es igual a σ_i si y sólo si $\sigma_i(K) \subset \mathbf{R}$. Sea r_1 el número de aquellos i tales que $\sigma_i(K) \subset K$. Los restantes son un número par $2r_2$ y se tiene

$$r_1 + 2r_2 = n. \tag{1}$$

Numeraremos los σ_i de manera que $\sigma_i(K) \subset \mathbf{R}$ si $1 \leq i \leq r_1$ y $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ si $r_1 + 1 \leq j \leq r_1 + r_2$. Así, los $r_1 + r_2$ primeros σ_i determinan los r_2 restantes. Si $x \in K$, escribimos

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \tag{2}$$

Llamaremos a σ la **inclusión canónica** de K en $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. Es un homomorfismo inyectivo para las correspondientes estructuras de anillos. Generalmente identificaremos $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ con $\mathbf{R}^n$ (cf. (1)). Las notaciones σ, K, n, r_1, r_2 serán utlizadas en el resto de esta §.

Proposición 1. *Si* M *es un sub-*$\mathbf{Z}$*-módulo libre de rango* n *de* K *y si* $(x_i)_{1\leq i\leq n}$ *es una* $\mathbf{Z}$*-base de* M*, luego* $\sigma(M)$ *es un reticulado de* $\mathbf{R}^n$*, cuyo volúmen está*

dado por

$$v(\sigma(\mathrm{M})) = 2^{-r_2} \left| \det_{1\le i,j\le n} (\sigma_i(x_j)) \right| \tag{3}$$

En efecto, para i fijo, las coordenadas de $\sigma(x_i)$ respecto a la base canónica de $\mathbf{R}^n$ están dadas por

$$\sigma_1(x_i), \ldots, \sigma_{r_1}(x_i), \mathrm{R}(\sigma_{r_1+1}(x_i)), \mathrm{I}(\sigma_{r_1+1}(x_i)), \ldots, \mathrm{R}(\sigma_{r_1+r_2}(x_i)), \mathrm{I}(\sigma_{r_1+r_2}(x_i)) \tag{4}$$

donde R e I denotan la parte real y la parte imaginaria. Calculemos el determinante D cuyo i-ésima columna está dada por (4). Utilizando las fórmulas $\mathrm{R}(z) = \frac{1}{2}(z+\overline{z})$ y $\mathrm{I}(z) = \frac{1}{2i}(z-\overline{z})$ $(z \in \mathbf{C})$ y la linearidad respcto a las filas, obtenemos $\mathrm{D} = \pm(2i)^{-r_2} \det(\sigma_j(x_i))$. Como los x_i forman una base de K sobre $\mathbf{Q}$ se tiene $\det(\sigma_j(x_i)) \neq 0$ (capítulo II, §7, proposición 3) y por lo tanto $\mathrm{D} \neq 0$. Por lo tanto los vectores $\sigma(x_i)$ son linealmente independientes en $\mathbf{R}^n$, de manera que el $\mathbf{Z}$-módulo que general (es decir, $\sigma(\mathrm{M})$) es un reticulado de $\mathbf{R}^n$. El cálculo de D que acabamos de hacer muestra que su volúmen está dado por (3).

Proposición 2. *Sea d el discriminante absoluto de* K, A *su anillo de enteros y $\mathfrak{a}$ un ideal entero no nulo de* A. *Entonces $\sigma(\mathrm{A})$ y $\sigma(\mathfrak{a})$ son reticulados y se tiene*

$$v(\sigma(\mathrm{A})) = 2^{-r_2} |d|^{1/2} \qquad v(\sigma(\mathfrak{a})) = 2^{-r_2} |d|^{1/2} \mathrm{N}(\mathfrak{a}). \tag{5}$$

En efecto, sabemos que A y $\mathfrak{a}$ son $\mathbf{Z}$-módulos libres de rango n, de manera que podemos aplicar la proposición 1. Por otra parte, si (x_i) es una $\mathbf{Z}$-base de A, se tiene $d = \det(\sigma_i(x_j))^2$ (capítulo II, §7, proposición 3). De esto se sigue la primer fórmula (5). La segunda se deduce observando que $\sigma(\mathfrak{a})$ es un subgrupo de $\sigma(\mathrm{A})$ de índice $\mathrm{N}(\mathfrak{a})$ (capítulo III, §5, definición 1) y que por lo tanto un dominio fundamental para $\sigma(\mathfrak{a})$ se obtiene como unión disjunta de $\mathrm{N}(\mathfrak{a})$ copias de un dominio fundamental de $\sigma(\mathrm{A})$.

3. Finitud del grupo de clases de ideales

Proposición 1. *Sea* K *un cuerpo de números, n su grado, r_1 y r_2 los enteros definidos al comienzo de §2, d su discriminante absoluto y $\mathfrak{a}$ un ideal entero no nulo de* K. *Entonces $\mathfrak{a}$ contiene un elemento no nulo x tal que*

$$\left|\mathrm{N}_{\mathrm{K}/\mathbf{Q}}(x)\right| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2} \mathrm{N}(\mathfrak{a}). \tag{1}$$

En efecto, sea σ la inmersión canónica de K en $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ (§2). Sea t un número real > 0 y B_t el conjunto de aquellos

$$(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

tales que

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t. \tag{2}$$

Entonces B_t es un conjunto compact, convexo, simétrico respecto al origen y veremos en el apéndice que su volúmen es

$$\mu(\mathrm{B}_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_r} \frac{t^n}{n!}. \tag{3}$$

Elijamos t tal que $\mu(\mathrm{B}_t) = 2^n v(\sigma(\mathfrak{a}))$, es decir tal que

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} \, |d|^{1/2} \, \mathrm{N}(\mathfrak{a})$$

(§2, proposición 2) o, equivalentemente, $t^n = 2^{n-r_1} \pi^{-r_2} n! \, |d|^{1/2} \, \mathrm{N}(\mathfrak{a})$. Por el corolario del teorema 2, §1, existe un elemento x de $\mathfrak{a}$ no nulo tal que $\sigma(x) \in \mathrm{B}_t$. Ahora estimemos la norma $|\mathrm{N}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2$. La desigualdad de la media geométrica muestra que se tiene

$$|\mathrm{N}(x)| \leq \left[\frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right]^n \leq \frac{t^n}{n^n} \quad \text{(por (2))}$$

de donde $|\mathrm{N}(x)| \leq \frac{1}{n^n} 2^{n-r_1} \pi^{-r_2} n! \, |d|^{1/2} \, \mathrm{N}(\mathfrak{a})$, lo que es equivalente a (1) ya que $r_1 + 2r_2 = n$. LQQD.

Corolario 1. *Con la misma notación que antes, toda clase de ideales de* K *(capítulo III, §4) contiene un ideal entero* $\mathfrak{b}$ *tal que*

$$\mathrm{N}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \, |d|^{1/2} \, . \tag{4}$$

En efecto, sea $\mathfrak{a}'$ un ideal perteneciente a la clase dada. Multiplicando por un escalar, podemos suponer que $\mathfrak{a} = \mathfrak{a}'^{-1}$ es un ideal entero. Tomemos un elemento x no nulo de $\mathfrak{a}$ tal que (1) sea verdad. Entonces $\mathfrak{b} = x\mathfrak{a}^{-1}$ es un ideal entero perteneciente a la clase dada cuya norma satisface (4) utilizando la multiplicatividad de las normas (capítulo III, §5, proposición 2).

Corolario 2. *Sea* K *un cuerpo de números, n su grado y d su discriminante absoluto. Entonces si* $n \geq 2$, *se tiene* $|d| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$ *y* $\frac{n}{\log |d|}$ *está acotado por una constante independiente de* K.

En efecto, como $\mathrm{N}(\mathfrak{b}) \geq 1$, se tiene $|d|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}$. Como $\frac{\pi}{4} < 1$ y $2r_2 \leq n$, se tiene $|d| \geq a_n$, donde $a_n = \left(\frac{\pi}{4}\right)^{r_2} \frac{n^{2n}}{(n!)^2}$. Ahora bien, se tiene $a_2 = \frac{\pi^2}{4}$ y $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} = \frac{\pi}{4}$(1+2+términos positivos) (por la fórmula del binomio) $\geq \frac{3\pi}{4}$. De donde $n \geq 2$, $|d| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$, o que implica la desigualdad deseada. La estimación uniforme de $\frac{n}{\log|d|}$ se sigue tomando logaritmos.

Teorema 1 (Hermite-Minkowski)**.** *Para todo cuerpo de números* $\mathrm{K} \neq \mathbf{Q}$*, el discriminante absoluto* d *de* K *es* $\neq \pm 1$*.*

En efecto, por el corolario 2, se tiene $|d| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$ y $\frac{\pi}{3} > 1$, $\frac{3\pi}{4} > 1$ de donde se sigue que $|d| > 1$.

Teorema 2 (Dirichlet)**.** *Para todo cuerpo de números* K*, el grupo de clases de ideales de* K *es finito (capítulo III, §4).*

En virtud del corolario 1 de la proposición 1, basta demostrar que el conjunto de ideales enteros $\mathfrak{b}$ de K, cuya norma es un entero dado q, es finito. Como para un tal ideal $\mathfrak{b}$ se tiene que $\mathrm{card}(\mathrm{A}/\mathfrak{b}) = q$ (capítulo III, §5), se sigue que $q \in \mathfrak{b}$ pues en un grupo el orden de un elemento divide al orden del grupo. Por lo tanto los ideales $\mathfrak{b}$ considerados son algunos de aquellos que contienen a Aq, y hay un número finito de estos últimos (capítulo III, §4, fórmula (8), o bien por la finitud de $\mathrm{A}/\mathrm{A}q$).

Teorema 3 (Hermite)**.** *En* $\mathbf{C}$ *hay sólo un número finito de cuerpos de números de discriminante* d *dado.*

En efecto, por el corolario 2 de la proposición 1, el grado de un tal cuerpo está acotado. Luego podemos suponer que n, y r_1 y r_2 están fijos.

En $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ consideramos el siguiente conjunto B:

1. Si $r_1 > 0$, B es el conjunto de los $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ tales que

$$|y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2}, \quad |y_i| \leq \frac{1}{2} \text{ para } i = 2, \ldots, r_1, \quad |z_j| \leq \frac{1}{2} \text{ para } j = 1, \ldots, r_2. \tag{5}$$

2. Si $r_1 = 0$, B es el conjunto de los $(z_1, \ldots, z_{r_2}) \in \mathbf{C}^{r_2}$ tales que

$$|z_1 - \overline{z}_1| \leq 2^n \frac{8}{\pi} \left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2}, \quad |z_1 + \overline{z}_1| \leq \frac{1}{2}, \quad |z_j| \leq \frac{1}{2} \text{ para } j = 2, \ldots, r_2. \tag{6}$$

Entonces B es un conjunto compacto, convexo y simétrico respecto al origen, cuyo volúmen es exactamente $2^n 2^{-r_2} |d|^{1/2}$ [1]. Si σ es la inmersión canónica de K (§2), la proposición 2 de la §2 y el cor. del teorema 2 de la §1 muestran que existe un entero $x \neq 0$ de K tal que $\sigma(x) \in$ B.

Mostremos que x es un elemento **primitivo** de K sobre **Q**. En efecto, en el caso a), (5) muestra que se tiene $|\sigma_i(x)| \leq \frac{1}{2}$ si $i \neq 1$. Como

$$|\mathrm{N}(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$$

es un entero $\neq 0$ (capítulo II, §6, corolario de la proposición 2), deducimos que $|\sigma_1(x)| \geq 1$, de donde $\sigma_1(x) \neq \sigma_i(x)$ para todo $i \neq 1$. Pero si x no fuera primitivo, $\sigma_1(x)$ coincidiría con alguno de los $\sigma_i(x)$ con $i \neq 1$ (capítulo II, §6, proposición 1), lo que termina la demostración en este caso. ???? En el caso b), se tiene de la misma manera que $|\sigma_1(x)| = \overline{|\sigma_1(x)|} \geq 1$, de donde $\sigma_1(x) \neq \sigma_j(x)$ cuando σ_j es distinto de σ_1 y $\overline{\sigma}_1$. Por otra parte, (6) muestra que la parte real $|\mathrm{R}(\sigma_1(x))|$ es $\leq \frac{1}{4}$, de manera que $\sigma_1(x)$ no es real y $\sigma(x) \neq \overline{\sigma_1(x)}$. Como en el caso a), concluimos que x no es primitivo.

Ahora las fórmulas (5) y (6) muestran que los conjugados $\sigma_i(x)$ de x son **acotados,** y por lo tanto también lo son las funciones simétricas elementales en los $\sigma_i(x)$, es decir, los coeficientes del polinomio minimal de x. Como estos también son elementos de **Z** (capítulo II, §6, corolario de la proposición 2), sólo pueden tomar en este caso un número finito de valores. Por lo tanto, sólo hay un número finito de posibles polinomios minimales de x y en consecuencia solamente un número finito de valores posibles para x en **C**. Como x genera K, el teorema 3 queda demostrado LQQD.

4. El teorema de las unidades

Por abuso del lenguaje, llamamos **unidades** de un cuerpo de números K a los elementos inversibles del anillo de enteros A de K. Estás unidades forman un grupo multiplicativo notado A^*. El siguiente resultado nos será útil.

Proposición 1. *Sea* K *un cuerpo de números y* $x \in$ K. *Para que* x *sea una unidad de* K *es necesario y suficiente que* x *sea un entero de* K *de norma* ± 1.

En efecto, si x es una unidad de K, $\mathrm{N}(x)$ y $\mathrm{N}(x^{-1})$ son elementos de **Z** cuyo producto es $\mathrm{N}(1) = 1$. Luego, $\mathrm{N}(x) = \pm 1$. Recíprocamente, sea x un entero de K de norma ± 1. Su polinomio característico se escribe $x^n + a_{n-1}x^{n-1} + \cdots +$

[1] Este volúmen se calcula, de manera fácil, observando que B es un producto de intervalos, discos y un rectángulo en el caso b).

$a_1 x \pm 1 = 0$ para algunos $a_0 \in \mathbf{Z}$ (capítulo II, §6). Luego $\pm(x^{n-1} + \cdots + a_1)$ es el inverso de x y es un entero de K, por lo que x es una unidad de K.

Teorema 1 (Dirichlet)**.** *Sea* K *un cuerpo de números, n su grado,* r_1 *y* r_2 *los enteros definidos en §2 y* $r = r_1 + r_2 - 1$. *El grupo* A^* *de las unidades de* K *es isomorfo a* $\mathbf{Z}^r \times G$, *donde* G *es un grupo cíclico finito, formado por las raíces de la unidad contenidas en* K.

Probaremos primero que nada que A^* es un grupo conmutativo de tipo finito y calcularemos su rango. Consdireemos la inmersión canónica (§2) $x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x))$ de K en $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ y la aplicación

$$x \mapsto L(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|) \tag{1}$$

de K^* en $\mathbf{R}^{r_1+r_2}$. Es un homomorfismo (i.e. $L(xy) = L(x) + L(y)$), que llamaremos **inmersión logarítmica** de K^*. Sea B un subespacio compacto de $\mathbf{R}^{r_1+r_2}$ y mostremos que el conjunto B' de las unidades $x \in A^*$ tales que $L(x) \in B$ es **finito.** En efecto, como B está acotado, existe un número real $\alpha > 1$ tal que, para todo $x \in B'$, se tiene

$$\frac{1}{\alpha} \leq |\sigma_i(x)| \leq \alpha \quad (i = 1, \ldots, n).$$

Entonces, las funciones simétricas elementales en los $\sigma_i(x)$ están acotadas en valor absoluto y, como toman valores en $\mathbf{Z}$ (pues $x \in A$), sólo pueden tomar un número finito de valores. Luego sólo hay un número finito de polinomio característicos posibles para x y por lo tanto sólo un número finito de valores posibles para x. La finitud de B' tiene entonces las siguientes consecuencias:

1. El núcleo G de la restricción de L a A^* es un grupo finito. Luego consiste en raíces de la unidad y es **cíclico** (capítulo I, §6, teorema 1). Toda **raíz de la unidad** en K pertenece a este núcleo, ya que son enteros de K y $|\sigma_i(x)|^q = |\sigma_i(x^q)| = |1| = 1$ implica $|\sigma_i(x)| = 1$.
2. La imagen $L(A^*)$ es un subgrupo discreto de $\mathbf{R}^{r_1+r_2}$ (§1) y por lo tanto un $\mathbf{Z}$-módulo libre de rango $s \leq r_1 + r_2$ (§1, teorema 1). Como $L(A^*)$ es libre, A^* es isomorfo a $G \times L(A^*) = G \times \mathbf{Z}^s$. Sólo nos resta demostrar que el rango s de $L(A^*)$ es igual a $r_1 + r_2 - 1$.

La desigualdad $s \leq r_1 + r_2 - 1$ es fácil. En efecto, si $x \in A^*$, la igualdad $\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)}$ (proposición 1) implica que el vector $L(x) = (y_1, \ldots, y_{r_1+r_2})$ pertenece al hiperplano W de ecuación

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0, \tag{2}$$

y por lo tanto $\mathrm{L}(\mathrm{A}^*)$ es un subgrupo discreto de W, de donde $s \leq r_1 + r_2 - 1$.

Sólo queda demostrar que $\mathrm{L}(\mathrm{A}^*)$ contiene $r = r_1 + r_2 - 1$ vectores linealmente independientes, lo que es más delicado. Se trata de mostrar que, para toda forma lineal $f \neq 0$ en W, existe una unidad u tal que $f(\mathrm{L}(u)) \neq 0$. Como la proyección de W sobre $\mathbf{R}^r$ es un isomorfismo (por (2)), podemos escribir, para todo $y = (y_1, \ldots, y_{r+1}) \in \mathrm{W} \subset \mathbf{R}^{r+1}$,

$$f(y) = c_1 y_1 + \cdots + c_r y_r \quad \text{con} \quad c_i \in \mathbf{R} \tag{3}$$

Fijemos un número real α suficientemente grande, más precisamente tal que

$$\alpha \geq 2^n \left(\frac{1}{2\pi}\right)^{r_2} |d|^{1/2}.$$

Para todo sistema $\lambda = (\lambda_1, \ldots, \lambda_r)$ de r números reales > 0, sea λ_{r+1} el número real > 0 tal que $\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$. En $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, el conjunto B de los $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2})$ ($y_i \in \mathbf{R}$, $z_j \in \mathbf{C}$) tales que $|y_i| \leq \lambda_i$ y $|z_j| \leq \lambda_j$ es compacto, convexo, simétrico respecto al origen y su volúmen es $\prod_{i=1}^{r_1} 2\lambda_i \prod_{r=r_1+1}^{r_2} \pi\lambda_j^2 = 2^r \pi^{r_2} \alpha \geq 2^n 2^{-r_2} |d|^{1/2}$. Luego, por la proposición 2 de la §2 y el corolario del teorema 2 de §1, existe un **entero** x_λ **de** K tal que $\sigma(x_\lambda) \in \mathrm{B}$; dicho de otra menra, se tiene $|\sigma_i(x_\lambda)| \leq \lambda_i$ para todo $i = 1, \ldots, n$ (poniendo $\lambda_{j+r_2} = \lambda_j$ para $j = r_1 + 1, \ldots, r_1 + r_2$). Como x_λ es un entero, se tiene

$$1 \leq |\mathrm{N}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

Por otra parte, para todo i, se tiene

$$|\sigma_i(x_\lambda)| = |\mathrm{N}(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} \lambda_j^{-1} = \lambda_i \alpha^{-1}$$

De donde $\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$ para todo i, de manera que se tiene

$$0 \leq \log \lambda_i - \log |\sigma_i(x_\lambda)| \leq \log \alpha. \tag{4}$$

Entonces por (3), se tiene también

$$\left| f(\mathrm{L}(x_\lambda)) - \sum_{i=1}^{r} c_i \log \lambda_i \right| \leq \left(\sum_{i=1}^{r} |c_i| \right) \log \alpha \tag{5}$$

Sea β una constante estrictamente mayor al miembro de la derecha de (5) y, para todo entero $h > 0$, elijamos r números reales $\lambda_{i,h} > 0$ ($i = 1, \ldots, r$) tales que $\sum_{i=1}^{r} c_i \log \lambda_{i,h} = 2\beta h$. Sea

$$\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r,h}),$$

y sea x_h el entero $x_{\lambda(h)}$ correspondiente. Por ???? se tiene

$$|f(\mathrm{L}(x_h)) - 2\beta h| < \beta,$$

de donde

$$(2h-1)\beta < f(\mathrm{L}(x_h)) < (2h+1)\beta. \tag{6}$$

Resulta de (6) que los números $f(\mathrm{L}(x_h))$ $(h \geq 0)$ son todos **disintos.** Por otra parte, como $|\mathrm{N}(x_h)| \leq \alpha$, hay un número finito de los ideales $\mathrm{A}x_h$ (cf. §3, demostración del teorema 2). Luego existen dos índices h y k distintos tales que $\mathrm{A}x_h = \mathrm{A}x_k$ y por lo tanto exite una **unidad** u de A tal que $x_k = ux_h$. Por lo tanto (como f es lineal) se tiene que $f(\mathrm{L}(u)) = f(\mathrm{L}(x_k)) - f(\mathrm{L}(x_h)) \neq 0$, y u es la unidad buscada. LQQD.

Observación. El teorema 1 (llamado "teorema de las unidades") muestra que existen r $(= r_1 + r_2 - 1)$ y unidades (u_i) de K tal que toda unidad u de K se escribe, de manera única, en la forma

$$u = zu_1^{n_1} \cdots u_r^{n_r} \tag{7}$$

donde los $n_i \in \mathbf{Z}$ y z es una raíz de la unidad. Entones (u_i) se llama un **sitema de unidades fundamentales** de K.

Ejemplo (Ejemplo de los cuerpos ciclotómicos). Sea p un número primo $\neq 2$, z una raíz primitiva p-ésima de la unidad en $\mathbf{C}$ y K el cuerpo ciclotómico $\mathbf{Q}[z]$ (cf. capítulo II, §9). Se tiene $[\mathrm{K} : \mathbf{Q}] = p - 1$ (*ibid.*, teorema 1). Como ningún conjugado de z en $\mathbf{C}$ es real, se tiene $r_1 = 0$, $2r_1 = p - 1$, de donde $r = \frac{p-3}{2}$.

5. Las unidades de un cuerpo cuadrático imaginario

Sea K un cuerpo cuadrático imaginario (capítulo II, §5). Entonces tenemos $r_1 = 0$, $2r_2 = 2$, $r_2 = 1$ y $r_1 + r_2 - 1 = 0$. Así, las únicas unidades de K son las raíces de la unidad contenidas en K (§4, teorema 1). Estas forman un grupo **finito cíclico.** Redemostraremos este resultado con un sencillo cálculo que además nos dará un poco más de precisión.

Sea $\mathrm{K} = \mathbf{Q}[\sqrt{-m}]$, donde m es un entero > 0 libre de cuadrados. Recordemos que las unidades de K son los enteros de norma ± 1 de K (§4, proposición 1).

1) Si $m \equiv 2$ ó $2 \pmod 4$, el anillo de enteros de K es $\mathbf{Z} + \mathbf{Z}\sqrt{-m}$ (capítulo II, §5, teorema 1). Si $x = a + b\sqrt{-m}$ $(a,b \in \mathbf{Z})$, tenemos

$$\mathrm{N}(x) = a^2 + mb^2 \geq 0.$$

Por lo tanto, para que x sea una unidad es necesario y suficiente que $a^2 + mb^2 = 1$. Si $m \geq 2$, esto implica que $b = 0$ y $a = \pm 1$, de donde $x = \pm 1$. Si $m = 1$,

además de las soluciones $x = \pm 1$ están las soluciones $a = 0$, $b = \pm 1$, $x = \pm i$ ($i^2 = -1$).

2) Si $m \equiv 3 \pmod 4$, el anillo de enteros de K es $\mathbf{Z}+\mathbf{Z}\frac{1+\sqrt{-m}}{2}$ (capítulo II, §5, teorema 1). Si $x = a+\frac{b}{2}(1+\sqrt{-m})$ (a,$b \in \mathbf{Z}$), tenemos $\mathrm{N}(x) = \left(a+\frac{b}{2}\right)^2 + \frac{mb^2}{4}$. Por lo tanto, para que x sea una unidad es necesario y suficiente que $(2a+b)^2 + mb^2 = 4$. Si $m \geq 7$, esto implica que $b = 0$, de donde $(2a)^2 = 4$, $a = \pm 1$, y $x = \pm 1$. Si $m = 3$, también obtenemos las soluciones $b = \pm 1$, de donde $(2a \pm 1)^2 = \pm 1$, es decir

$$x = \frac{1}{2}(\pm 1 \pm \sqrt{-3})$$

(los signos ± 1 son independientes).

En resúmen, hemos obtenido el siguiente resultado:

Proposición 1. *Si* K *es un cuerpo cuadrático imaginario, el grupo* G *de las unidades de* K *está formado por* $+1$ *y* -1*, excepto en los dos casos siguientes:*

1) *si* $\mathrm{K} = \mathbf{Q}[i]$ *(*$i^2 = -1$*),* G *está formado de las raíces cuartas de la unidad* i, -1, $-i$, 1.
2) *Si* $\mathrm{K} = \mathbf{Q}[\sqrt{-3}]$, G *está formado de las raíces sextas de la unidad* $\left(\frac{1+\sqrt{-3}}{2}\right)^j$, $j = 0,1,\ldots,5$.

6. Las unidades de un cuerpo cuadrático real

Este § será decididamente más divertido que el anterior. Sea K un cuerpo cuadrático real. Con la notación habitual, se tiene $r_1 = 2$, $r_2 = 0$, de donde $r = r_1 + r_2 - 1 = 1$. El teorema de las unidades (§4, teorema 1) muestra que el grupo de las unidades de K es isomorfo al producto de $\mathbf{Z}$ por el grupo de las raíces de la unidad contenidas en K. Como K admite una inmersión en $\mathbf{R}$, estás son 1 y -1. Por lo tanto, suponiendo que K está inmerso en $\mathbf{R}$, tenemos:

Proposición 1. *Las unidades positivas de un cuerpo cuadrático real* $\mathrm{K} \subset \mathbf{R}$ *forman un grupo (multiplicativo) isomorfo a* $\mathbf{Z}$.

Este grupo admite un sólo generador > 1. Lo llamamos **la unidad fundamental de** K**.**

Sea $\mathrm{K} = \mathbf{Q}[\sqrt{d}]$ donde d es un entero ≥ 2 libre de cuadrados y sea $x = a+b\sqrt{d}$ (a,$b \in \mathbf{Q}$) una unidad de K. Los números x, x^{-1}, $-x$, $-x^{-1}$ son todas unidades de K y, como $\mathrm{N}(x) = (a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$ (§4, proposición 1), estos cuatro números son precisamente $\pm a \pm b\sqrt{d}$. Si $x \neq \pm 1$, exactamente uno de los cuatro números x, x^{-1}, $-x$, $-x^{-1}$ es > 1 y es el más grande de

los cuatro. Por lo tanto **las unidades** > 1 **de** K **son las unidades de la forma** $a + b\sqrt{d}$ **con** $a,b > 0$**.**

a) Supongamos primero que $d \equiv 2$ ó $3 \pmod 4$. Entonces el anillo de enteros de K es $\mathbf{Z} + \mathbf{Z}\sqrt{d}$ (capítulo II, §5, teorema 1). Como las unidades de K son los enteros de norma ± 1 (§4, proposición 1), las unidades > 1 de K son los números $a + b\sqrt{d}$ con $a,b \in \mathbf{Z}$, $a,b > 0$ tales que

$$a^2 - db^2 = \pm 1. \tag{1}$$

Vemos entonces que las soluciones "en números enteros naturales" (a,b) de la ecuación (1) (llamada **"ecuación de Pell-Fermat"**) se obtienen de la siguiente manera: tomamos la unidad fundamental $a_1 + b_1\sqrt{d}$ de K y ponemos

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n \quad (n \geq 1). \tag{2}$$

La sucesión (a_n,b_n) provee ???? entonces **todas las soluciones** de (1).

Observación (Observaciones). 1) Resulta de (2) que $b_{n+1} = a_1b_n + b_1a_n$. Como $a_1, b_1, a_n, b_n > 0$, la sucesión (b_n) es estrictamente creciente. Así, para **calcular** explícitamente la unidad fundamental $a_1 + b_1\sqrt{d}$, podemos comenzar escribiendo la sucesión de los db^2 ($b \in \mathbf{N}$, $b \geq 1$) y detenernos en el primer término db_1^2 de esta sucesión que difiera de un cuadrado a_1^2 por ± 1. Entonces $a_1 + b_1\sqrt{d}$ es la unidad fundamental de K. Por ejemplo, si $d = 7$, la sucesión de los db^2 es $7, 28, 63 = 64 - 1 = 8^2 - 1$. Por lo tanto tenemos $b_1 = 3$, $a_1 = 8$ y la unidad fundamental de $\mathbf{Q}[\sqrt{7}]$ es $8 + 3\sqrt{7}$. Vemos de la misma manera que las unidades fundamentales de $\mathbf{Q}[\sqrt{2}$, $\mathbf{Q}[\sqrt{3}]$ y $\mathbf{Q}[\sqrt{6}]$ son $1 + \sqrt{2}$, $2 + \sqrt{3}$, $5 + 2\sqrt{6}$. Hay otras maneras de calcularlas, más eficaces, relacionadas con la teoría de fracciones continuas.

2) Si la unidad fundamental es de norma 1, los (a_n,b_n) son todos soluciones de (1') $a^2 - db^2 = 1$. Entonces (1") $a^2 - db^2 = -1$ no posee soluciones. Si la unidad fundamental es de norma -1, las soluciones de (1') son los (a_{2n},b_{2n}) y las de (1") son los (a_{2n+1},b_{2n+1}). El primer caso ocurre por ejemplo si $d = 3$, $d = 6$ y $d = 7$ y el segundo si $d = 2$ y $d = 10$.

b) Supongamos ahora que $d \equiv 1 \pmod 4$. Los enteros de $\mathrm{K} = \mathbf{Q}[\sqrt{d}]$ son entonces los números $\frac{1}{2}(a + b\sqrt{d})$ con $a,b \in \mathbf{Z}$ de la misma paridad (capítulo II, §5, teorema 1). Por lo tanto, si $\frac{1}{2}(a + b\sqrt{d})$ es una unidad de K, se tiene (§4, proposición 1)

$$a^2 - db^2 = \pm 4. \tag{3}$$

Reciprocamente para todo solución (a,b) en números enteros de (3), $\frac{1}{2}(a + b\sqrt{d})$ es un entero de K (pues su traza es a y su norma es ± 1 por (3)) y por lo tanto

una unidad de K. Como en *a*) vemos que, si $\frac{1}{2}(a_1 + b_1\sqrt{d})$ denota la unidad fundamental de K, las soluciones (a,b) de (3) en números enteros > 0 forman una sucesión (a_n,b_n) $(n \geq 1)$ definida por

$$a_n + b_n\sqrt{d} = 2^{1-n}(a_1 + b_1\sqrt{d})^n. \tag{4}$$

El cálculo de $a_1 + b_1\sqrt{d}$ puede efectuarse como en *a*); las unidades fundamentales de $\mathbf{Q}[\sqrt{5}]$, $\mathbf{Q}[\sqrt{13}]$ y $\mathbf{Q}[\sqrt{17}]$ son $\frac{1}{2}(1+\sqrt{5})$, $\frac{1}{2}(3+\sqrt{13})$, $4+\sqrt{17}$. Estas tres unidades son de norma -1. Para la elección de signo $\pm$ en (3) se tienen los mismos resultados que en el caso *a*).

Observación. En el caso $d \equiv 1 \pmod 4$, las soluciones de la ecuación de Pell-Fermat propiamente dichas

$$a^2 - db^2 = \pm 1 \tag{5}$$

corresponden a las unidades $a + b\sqrt{d}$ $(a,b > 0)$ del anillo $\mathrm{B} = \mathbf{Z}[\sqrt{d}]$, que es un subanillo del anillo A de enteros de K. Ahora bien, las unidades > 0 de B forman un subgrupo G del grupo de unidades positivas de A. Sea $u = \frac{1}{2}(a + b\sqrt{d})$ la unidad fundamental de K. Si a y b son ambos **pares,** se sigue que $u \in \mathrm{B}$, de manera que G **está formado de las potencias de** u (este es le caso si $d = 17$). Si a y b son ambos **impares, se sigue que** $u^3 \in \mathrm{B}$**:** en efecto se tiene $8u^3 = a(a^2 + 3b^2d) + b(3a^2 + b^2d)\sqrt{d}$. Como $a^2 - db^2 = \pm 4$, tenemos $a^2 + 3b^2d = 4(b^2d \pm 1)$, que es un múltiplo de 8 pues b y d son impares. En este caso G **está formado de las potencias de** u^3 (en efecto, necesariamente $u^2 \notin \mathrm{B}$ pues sino $u = u^3/u^2 \in \mathrm{B}$). Este es el caso si $d = 5$ (resp. $d = 13$), en cuyo caso $u^3 = 2 + \sqrt{5}$ (resp. $u^3 = 18 + 5\sqrt{13}$).

7. Una generalización del teorema de las unidades

Proposición 1. *Sea* A *un anillo que es un* $\mathbf{Z}$*-módulo de tipo finito. Entonces el grupo multiplicativo* A^* *de los elementos inversibles de* A *es un grupo multiplicativo de tipo finito.*

Para un grupo conmutativo G, "de tipo finito" quiere decir "de tipo finito para la estructura de **Z-módulo** de G". Un subgrupo de un grupo conmutativo de tipo finito es de tipo finito (capítulo III, §1, corolario 2 del teorema 1). Observemos primero que nada que A es un anillo **noetheriano** y que los ideales de A son los sub-$\mathbf{Z}$-módulos de A.

Primero trataremos el caso donde A es un **dominio íntegro.** Si su cuerpo de fracciones K es de característica cero, es un $\mathbf{Q}$-espacio vectorial de tipo finito, luego un cuerpo de números. Por otra parte A es entero sobre $\mathbf{Z}$ (pues es un $\mathbf{Z}$-módulo de tipo finito, cf. capítulo II, §1, teorema 1) y por lo tanto

es un subanillo del anillo B de enteros de K. Luego, $A^* \subset B^*$ y B^* es de tipo finito por el teorema de las unidades (§4, teorema 1). Si K es de característica $p \neq 0$, K es una extensión finita de $\mathbf{F}_p$, en particular un cuerpo finito, en cuyo caso A^* es finito.

Pasemos ahora al caso cuando A es **reducido** (lo que significa, por definición, que 0 es el único elemento nilpotente de A). Nos hará falta el siguiente lema.

Lema. *En un anillo noetheriano reducido* A*, el ideal* (0) *es intersección finita de ideales primos.*

En efecto, sabemos que en un anillo noetheriano, todo ideal contiene un producto de ideales primos (capítulo III, §3, lema 3). Como (0) es el ideal más pequeño, debe **ser** un producto de ideales primos: $(0) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q}$. Sea $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$. Se tiene $x^{n_1+\cdots+n_q} \in \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q} = (0)$, de manera que $x^{n_1+\cdots+n_q} = 0$, de donde $x = 0$ pues A es reducido. Por lo tanto, $(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$.

En resúmen, $(0) = \mathfrak{p}_1 \cap \ldots \mathfrak{p}_1$ con los $\mathfrak{p}_i$ ideales primos. Deducimos que el homomorfismo canónico $\varphi : A \to \prod_{i=1}^{q} A/\mathfrak{p}_i$ es inyectivo. Como un elemento de un anillo producto es inversible si y sólo si todas sus componentes son inversibles, se sigue que $(\prod_i A/\mathfrak{p}_i)^* = \prod_i (A/\mathfrak{p}_i)^*$. Por el caso de un dominio íntegro, cada $(A/\mathfrak{p}_i)^*$ es de tipo finito y por lo tanto también lo es $\prod (A/\mathfrak{p}_i)^*$ y por lo tanto también $\varphi(A^*)$ (recordemos que $\mathbf{Z}$ es noetheriano). Es decir, A^* es de tipo finito ya que φ es inyectiva.

Pasemos finalmente al caso **general.** Observemos que el conjunto $\mathfrak{n}$ de elementos nilpotentes de A es un **ideal,** pues $x^p = 0$, $y^p = 0$ y $a \in A$ implica que $(x + y)^{p+q-1} = 0$ y $(ax)^p = 0$. Por otra parte, existe un entero s tal que $\mathfrak{n}^s = (0)$: en efecto, como A es noetheriano, $\mathfrak{n}$ admite un sistema finito de generadores $(x_1, \ldots, x_r)$ con $x_i^{q_i} = 0$ para todo i. Entonces, si $s = q_1 + \cdots + q_r$, todo monomio en los x_i de grado s es nulo, de manera que $\mathfrak{n}^s = (0)$. Procederemos por inducción en s. El caso $s = 1$ es precisamente el caso de A reducido, que ya tratamos. Supongamos por lo tanto que $s > 1$ y notemos φ el homomorfismo canónico $\varphi : A \to A/\mathfrak{n}^{s-1}$. Se tiene $\varphi(A^*) \subset (A/\mathfrak{n}^{s-1})^*$, de manera que $\varphi(A^*)$ es un grupo de tipo finito. Por otra parte el núcleo de la restricción de φ a A^* está contenido en $1 + \mathfrak{n}^{s-1}$ y por lo tanto es **igual** a $1 + \mathfrak{n}^{s-1}$, pues como $s > 1$, se tiene $(\mathfrak{n}^{s-1})^2 \subset \mathfrak{n}^s = (0)$, y todo elemento $1 + x$ de $1 + \mathfrak{n}^{s-1}$ es inversible en virtud de $(1 + x)(1 - x) = 1 - x^2 = 1$. Sólo resta demostrar que el grupo multiplicativo $1 + \mathfrak{n}^{s-1}$ es de tipo finito. Como $(\mathfrak{n}^{s-1})^2 = (0)$ se tiene $(1 + x)(1 + y) = 1 + x + y$ para $x,y \in \mathfrak{n}^{s-1}$, de manera que $x \mapsto 1 + x$ es un isomorfismo del grupo aditivo $\mathfrak{n}^{s-1}$ sobre el

grupo multiplicativo $1 + \mathfrak{n}^{s-1}$. Pero, como A es un $\mathbf{Z}$-módulo de tipo finito, también lo es $\mathfrak{n}^{s-1}$. LQQD.

Utilizando métodos pertenecientes a la Geometría Algebraica puede demostrarse que para todo anillo **reducido** B *de la forma* $\mathrm{B} = \mathbf{Z}[x_1,\ldots,x_n]$ *(es decir, generado como anillo sobre* $\mathbf{Z}$ *por un número finito de elementos), el grupo* B^* *de los elementos inversibles es de tipo finito (*[**18**]*).*

Apéndice. Un cálculo de volúmen

Proposición. *Sean* $r_1,r_2 \in \mathbf{N}$, $n = r_1 + 2r_2$, $t \in \mathbf{R}$ *y* B_t *el conjunto de aquellos* $(y_1,\ldots,y_{r_1},z_1,\ldots,z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ *tales que*

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t. \tag{1}$$

Entonces para la medidad de Lebesgue μ *se tiene* $\mu(\mathrm{B}_t) = 0$ *si* $t < 0$ *y*

$$\mu(\mathrm{B}_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} \quad \textit{si} \quad t \geq 0. \tag{2}$$

Podemos suponer que estamos en el caso $t \geq 0$ pues si $t < 0$ tenemos $\mathrm{B}_t = \emptyset$ y $\mu(\mathrm{B}_t) = 0$. Escribimos $\mu(\mathrm{B}_t) = \mathrm{V}(r_1,r_2,t)$ y hacemos inducción doble en r_1 y r_2. Se tiene $\mathrm{V}(1,0,t) = 2t$ (segmento $[-t,+t]$) y

$$\mathrm{V}(0,1,t) = \frac{\pi t^2}{4}$$

(disco de radio $\frac{t}{2}$), lo que coincide con (2).

Pasemos de r_1 a $r_1 + 1$. El conjunto $\mathrm{B}_t \subset \mathbf{R} \times \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ correspondiente a $r_1 + 1$ y r_2 está definido por

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t \quad (y \in \mathbf{R})$$

La fórmula de integración "por partes" nos da ????

$$\mathrm{V}(r_1+1,r_2,t) = \int_{\mathbf{R}} \mathrm{V}(r_1,r_2,t-|y|)\,dy = \int_{-t}^{+t} \mathrm{V}(r_1,r_2,t-|y|)\,dy.$$

Por la hipótesis inductiva, esto coincide con ????

$$\mathrm{V}(r_1+1,r_2,t) = 2\int_0^t 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-y)^n}{n!}dy = 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^{n+1}}{(n+1)!},$$

lo que de nuevo coincide con (2).

Pasemos finalmente de r_2 a r_2+1. El conjunto $\mathrm{B}_t \subset \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \times \mathbf{C}$ correspondiente a r_1 y r_2+1 está definido por

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| + 2\,|z| \leq t \quad (z \in \mathbf{C})$$

La fórmula de integración "por partes" nos da aquí ??????

$$\mathrm{V}(r_1,r_2+1,t) = \int_{\mathbf{C}} \mathrm{V}(r_1,r_2,t-2\,|z|)\,d\mu(z) = \int_{|z|\leq \frac{t}{2}} \mathrm{V}(r_1,r_2,t-2\,|z|)\,d\mu(z)$$

donde $d\mu(z)$ denota la medida de Lebesgue sobre $\mathbf{C}$. Poniendo

$$z = \rho e^{i\theta}\ (\rho \in \mathbf{R}_+,\ 0 \leq \theta \leq 2\pi) \text{ se tiene } d\mu(z) = \rho\,d\rho\,d\theta$$

Utilizando la hipótesis inductiva, podemos reescribir esto ????

$$\mathrm{V}(r_1,r_2+1,t) = \int_0^{t/2}\int_0^{2\pi} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{(t-2\rho)^n}{n!}\rho\,d\rho\,d\theta$$

$$= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{2\pi}{n!}\int_0^{t/2}(t-2\rho)^n\rho\,d\rho$$

Para calcular $\int_0^{t/2}(t-2\rho)^n\rho\,d\rho$ ponemos $2\rho = x$ e integramos por partes. Encontramos que esta integral vale $\frac{t^{n+2}}{4(n+1)(n+2)}$, de donde $\mathrm{V}(r_1,r_2+1,t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{t^{n+2}}{(n+2)!}$, lo que coincide con (2) pues $r_1+2(r_2+1) = n+2$.

CAPÍTULO V

Descomposición de ideales primos en extensiones

Sea K un cuerpo de números, A el anillo de enteros de K, L una extensión finita de K y B la clausura íntegra de A en L (que no es otra cosa que el anillo de enteros de L). Dado un ideal primo $\mathfrak{p} \neq (0)$ de A, el ideal $B\mathfrak{p}$ que genera en B no es en general primo; pero se descompone en producto de ideales primos (capítulo III, §4, teorema 3): $B\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i}$. En este capítulo nos proponemos estudiar esta descomposición. El caso donde B es un A-módulo **libre** (p.ej. cuando A es un dominio de ideales principales; cf. capítulo II, §7, corolario del teorema 1) es particularmente simple. Expondremos en §1 una técnica que nos permite situarnos en este caso.

1. Preliminares sobre anillos de fracciones

Definición 1. *Sea* A *un dominio íntegro,* K *su cuerpo de fracciones y* S *un subconjunto de* A *stable por multiplicación que no cotiene* 0 *y contiene* 1. *Llamamos anillo de fracciones de* A *respecto a* S, *y lo notamos* $S^{-1}A$, *al conjunto de elementos* $\frac{a}{s} \in K$ *con* $a \in A$ *y* $s \in S$.

Es un anillo conmutativo (pues $\frac{a}{s} + \frac{a'}{s'} = \frac{s'a+sa'}{ss'}$ y $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$) y contiene a A (pues $1 \in S$). Si S consiste únicamente del 1, o si consiste únicamente de elementos inversibles de A, se tiene $S^{-1}A = A$.

Proposición 1. *Sea* A *un dominio íntegro,* S *un subconjunto múltiplicativamente estable de* A *que contiene al* 1 *y que no contiene al* 0 *y sea* $A' = S^{-1}A$.

1. *Para todo ideal* $\mathfrak{b}'$ *de* A', *se tiene* $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$ *de manera que* $\mathfrak{b}' \mapsto \mathfrak{b}' \cap A$ *es una inyección creciente (para la inclusión) del conjunto de ideales de* A' *en el conjunto de ideales de* A.
2. *La aplicación* $\mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ *es un isomorfismo del conjunto ordenado (para la inclusión) del conjunto de ideales primos de* A' *sobre el conjunto de ideales primos* $\mathfrak{p}$ *de* A *tales que* $\mathfrak{p} \cap S = \emptyset$. *La aplicación inversa es* $\mathfrak{p} \mapsto \mathfrak{p}A'$.

Demostremos 1). Si $\mathfrak{b}'$ es un ideal de A', se tiene $\mathfrak{b}' \cap A \subset \mathfrak{b}'$, de donde $(\mathfrak{b}' \cap A)A' \subset \mathfrak{b}'$ pues $\mathfrak{b}'$ es un ideal. Para demostrar la inclusión inversa, sea $x \in \mathfrak{b}'$; se tiene $x = \frac{a}{s}$ con $a \in A$ y $s \in S$. Luego $xs \in \mathfrak{b}'$ pues $A \subset A'$ y $\mathfrak{b}'$ es un ideal, de donde $a \in \mathfrak{b}'$ y $a \in \mathfrak{b}' \cap A$. Entonces $x = \frac{1}{s} \cdot a \in A'(\mathfrak{b}' \cap A)$, de donde $\mathfrak{b}' \subset A'(\mathfrak{b}' \cap A)$ y $\mathfrak{b}' = A'(\mathfrak{b}' \cap A)$. Esta fórmula asegura la inyectividad de la aplicación $\varphi : \mathfrak{b}' \mapsto \mathfrak{b}' \cap A$ pues se tiene una aplicación $\theta : \mathfrak{b} \mapsto A'\mathfrak{b}$ tal que $\theta \circ \varphi =$ identidad. Que φ es creciente es evidente. Esto demuestra 1).

Pasemos a 2). Si $\mathfrak{p}'$ es un ideal primo de A', entonces $\mathfrak{p} = \mathfrak{p}' \cap A$ es un ideal primo de A (capítulo III, §3, lema 1). Además se tiene $\mathfrak{p} \cap S = \emptyset$ pues, si $s \in \mathfrak{p} \cap S$, se tiene que $s \in \mathfrak{p}'$ y $1 = \frac{1}{s} \cdot s \in A'\mathfrak{p}' = \mathfrak{p}'$, lo que es absurdo.

Reciprocamete, sea $\mathfrak{p}$ un ideal primo de A tal que $\mathfrak{p} \cap S = \emptyset$. Mostraremos que $\mathfrak{p}A'$ es un ideal primo de A' y que se tiene $\mathfrak{p}A' \cap A = \mathfrak{p}$.

Observemos primero que nada que $\mathfrak{p}A'$ **es el conjunto de los** $\frac{p}{s}$ **con** $p \in \mathfrak{p}$ **y** $s \in S$**:** en efecto todo elemento x de $\mathfrak{p}A'$ se escribe $x = \sum_{i=1}^{n} \frac{a_i}{s_i} p_i$ ($a_i \in A$, $s_i \in S$, $p_i \in \mathfrak{p}$), por lo tanto $x = \sum_i \frac{b_i}{s} p_i$ utilizando un denominador en común ($b_i \in S$, $s \in S$) y por lo tanto $x = \frac{p}{s}$ con $p = \sum b_i p_i \in \mathfrak{p}$. Deducimos que $1 \notin \mathfrak{p}A'$ pues $\mathfrak{p} \cap S = \emptyset$ y por lo tanto no podemos tener $1 = \frac{p}{s}$ con $p \in \mathfrak{p}$ y $s \in S$. Mostremos que el ideal $\mathfrak{p}A'$ es primo: sean $\frac{a}{s} \in A'$ y $\frac{b}{t} \in A'$ tales que $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{p}A'$; entonces tenemos $\frac{a}{s} \cdot \frac{b}{t} = \frac{p}{u}$ con $p \in \mathfrak{p}$ y $u \in S$, de donde $abu = pst \in \mathfrak{p}$. Como $\mathfrak{p} \cap S = \emptyset$, se tiene $u \notin \mathfrak{p}$, de donde $ab \in \mathfrak{p}$ (pues $\mathfrak{p}$ es primo). Así, a o b pertenecen a $\mathfrak{p}$, de manera que $\frac{a}{s}$ o $\frac{b}{t}$ pertenecen a $\mathfrak{p}A'$. Mostremos por último que $\mathfrak{p} = \mathfrak{p}A' \cap A$. La inclusión $\mathfrak{p} \subset \mathfrak{p}A' \cap A$. Reciprocamente, si $x \in \mathfrak{p}A' \cap A$, se tiene $x = \frac{p}{s}$ ($p \in \mathfrak{p}$, $s \in S$) pues $x \in \mathfrak{p}A'$, de donde $sx = p \in \mathfrak{p}$. Como $s \notin \mathfrak{p}$ (se tiene $\mathfrak{p} \cap S = \emptyset$) y $\mathfrak{p}$ es primo, deducimos que $x \in \mathfrak{p}$.

Ahora bien, las fórmulas $\mathfrak{p} = \mathfrak{p}A' \cap A$ y $\mathfrak{p}' = A'(\mathfrak{p} \cap A)$ muestran que las aplicaciones $\varphi : \mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ y $\theta : \mathfrak{p} \mapsto \mathfrak{p}A$ (MAL EN EL LIBRO?) (restrictas a los ideales primos descritos en el enunciado) son dos biyecciones inversas la una de la otra, pues sus composiciones en los dos sentidos son la aplicación identidad. Que son crecientes es evidente. LQQD.

Corolario. *Si* A *es un dominio íntegro noetheriano, todo anillo de fracciones* $S^{-1}A$ *es noetheriano.*

En efecto, el conjunto de ideales de $S^{-1}A$ se aplica, de manera inyectiva y creciente, en aquel de los ideales de A (proposición 1, 1). Por lo tanto satisface también la condición de maximalidad.

Proposición 2. *Sea* R *un dominio íntegro,* A *un subanillo de* R*,* S *una subconjunto multiplicativamente estable de* A *con* $1 \in S$ *y* $0 \notin S$ *y* B *la clausura íntegra de* A *en* R*. Entonces la clausura íntegra de* $S^{-1}A$ *en* $S^{-1}R$ *es* $S^{-1}B$.

En efecto, todo elemento de $S^{-1}B$ se escribe en la forma $\frac{b}{s}$ con $b \in B$ y $s \in S$. Se tiene una ecuación de dependencia entera $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ con $a_0 = 0$. Dividiendo por s^n se obtiene $\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s} = 0$, lo que muestra que $\frac{b}{s}$ es entero sobre $S^{-1}A$. Reciprocamente, sea $\frac{x}{s}$ ($x \in R$, $s \in S$) un elemento de $S^{-1}R$ entero sobre $S^{-1}A$. Se tiene una ecuación de dependencia entera $\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_0}{t_0} = 0$ ($a_i \in A$, $t_i \in S$); multiplicando por $(t_0 t_1 \cdots t_{n-1})^n$ vemos que $x t_0 \cdots t_{n-1}/s$ es entero sobre A y por lo tanto un elemento de B. Así, $\frac{x}{s} = \frac{a}{t_0 \cdots t_{n-1}} \cdot \frac{x t_0 \cdots t_{n-1}}{s}$ es un elemento de $S^{-1}B$.

Corolario. *Si* A *es un anillo íntegramente cerrado, todo anillo de fracciones* $S^{-1}A$ *también es íntegramente cerrado.*

En efecto tomamos R el cuerpo de fraccione de A en la proposición anterior.

Proposición 3. *Si* A *es un anillo de Dedekind, todo anillo de fracciones* $S^{-1}A$ *es un anillo de Dedekind.*

En efecto, $S^{-1}A$ es noetheriano (corolario de la proposición 1) e íntegramente cerrado (corolario de la proposición 2). Además, como "perdemos" ideales primos al pasar de A a $S^{-1}A$ (proposiciones 1, 2), todo ideal primo no nulo de $S^{-1}A$ es maximal.

Proposición 4. *Sea* A *un anillo de Dedekind,* $\mathfrak{p}$ *un ideal primo no nulo de* A *y sea* $S = A - \mathfrak{p}$. *Entonces* $S^{-1}A$ *es un dominio de ideales principales y existe un elemento primo* p *de* $S^{-1}A$ *tal que los únicos ideales no nulos de* $S^{-1}A$ *son los* $(p^n)_{n \geq 0}$.

En efecto, como $\mathfrak{p}$ es el único ideal primo $\neq (0)$ de A contenido en $\mathfrak{p}$, es decir, disjunto con S, el único ideal primo no nulo de $S^{-1}A$ es $\mathfrak{P} = \mathfrak{p}S^{-1}A$ (proposición 1, 2). Como $S^{-1}A$ es un anillo de Dedekind (proposición 3), sus únicos ideales no nulos son los $\mathfrak{P}^n$ ($n \geq 0$). Tomamos entonces $p \in \mathfrak{P} - \mathfrak{P}^2$; el ideal (p) que genera está contenido en $\mathfrak{P}$ y no contiene a $\mathfrak{P}^2$, por lo que necesariamente $(p) = \mathfrak{P}$. Los únicos ideales no nulos de $S^{-1}A$ son así los (p^n) y por lo tanto $S^{-1}A$ es un dominio de ideales principales.

Proposición 5. *Sea* A *un dominio íntegro,* S *un subconjunto multiplicativamente cerrado de* A ($1 \in S$, $0 \notin S$) *y* $\mathfrak{m}$ *un ideal maximal tal que* $\mathfrak{m} \cap S = \emptyset$. *Entonces*

$$S^{-1}A/\mathfrak{m}S^{-1}A \simeq A/\mathfrak{m}.$$

Más precisamente el homomorfismo compuesto $A \to S^{-1}A \to S^{-1}A/\mathfrak{m}S^{-1}A$ tiene núcleo $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$ (proposición 1, 2)), de donde una inyección $\varphi : A/\mathfrak{m} \to S^{-1}A/\mathfrak{m}S^{-1}A$. Sólo resta mostrar que φ es sobreyectivo. Sea $x = \frac{a}{s} \in S^{-1}A$ ($a \in A$, $s \in S$). Como $s \notin \mathfrak{m}$ (se tiene $\mathfrak{m} \cap S = \emptyset$) y como $\mathfrak{m}$ es maximal, s es inversible mod $\mathfrak{m}$ y existe b tal que $bs \equiv 1 \pmod{}m$. Entonces $\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{m}S^{-1}A$, de manera que la imagen por φ de la clase de ab es igual a la clase de $\frac{a}{s} = x$. LQQD.

2. Descomposición de un ideal primo en una extensión

En este §, denotamos por A *un anillo de Dedekind de característica cero, por* K *su cuerpo de fracciones, por* L *una extensión de* K *de grado finito n y por* B *la clausura íntegra de* A *en* L. *Recordemos que* B *es un anillo de Dedekind (capítulo III, §4, teorema 1).*

Sea $\mathfrak{p}$ un ideal primo no nulo de A. Entonces $B\mathfrak{p}$ es un ideal de B que tiene una descomposición

$$B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}, \tag{1}$$

donde los $\mathfrak{P}_i$ son ideales primos de B, dos a dos distintos, y donde los e_i son enteros ≥ 1.

Proposición 1. *Los* $\mathfrak{P}_i$ *son exactamente los ideales primos* $\mathfrak{Q}$ *de* B *tales que* $\mathfrak{Q} \cap A = \mathfrak{p}$.

En efecto, para un ideal primo $\mathfrak{Q}$ de B, la relación $\mathfrak{Q} \cap A = \mathfrak{p}$ equivale a $\mathfrak{Q} \supset \mathfrak{p}B$ ($\Rightarrow$ es evidente; $\Leftarrow$ pues $\mathfrak{Q} \cap A$ es un ideal primo de A y $\mathfrak{p}$ es maximal). La proposición 1 resulta entonces del formulario de los anillos de Dedekind (capítulo III, §4).

Así $A/\mathfrak{p}$ se identifica a un submódulo de $B/\mathfrak{P}_i$. Estos dos anillos son cuerpos. Como B es un A-módulo de tipo finito (capítulo III, §4, teorema 1), $B/\mathfrak{P}_i$ es un espacio vectorial de dimensión finita sobre $A/\mathfrak{p}$. Notaremos esta dimensión por f_i y la llamaremos el **grado residual** de $\mathfrak{P}_i$ sobre A. El exponente e_i en (1) se llama el **índice de ramificación de** $\mathfrak{P}_i$ sobre A. Por último observemos que se tiene $B\mathfrak{p} \cap A = \mathfrak{p}$ ($\supset$ evidente; $\subset$ resulta de que $\mathfrak{P}_i \cap A = \mathfrak{p}$), de manera que $B/B\mathfrak{p}$ es un espacio vectorial sobre $A/\mathfrak{p}$, de dimensión finita sobre este??.

Teorema 1. *Con la notación de arriba, se tiene*

$$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n. \tag{2}$$

La primera igualdad es fácil. Consideremos la sucesión de ideales

$$\mathrm{B} \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supset \cdots \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \supset \cdots \supset \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_q^{e_q} = \mathrm{B}\mathfrak{p}.$$

Dos términos consecutivos son de la forma $\mathfrak{B}$ y $\mathfrak{B}\mathfrak{P}_i$; pero como no hay ideales estrictamente contenidos entre $\mathfrak{B}$ y $\mathfrak{B}\mathfrak{P}_i$, $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ es un espacio vectorial de dimensión 1 sobre $\mathrm{B}/\mathfrak{P}_i$ (cf. demostración de la proposición 2, §5, capítulo III). Por lo tanto es un espacio vectorial de dimensión f_i sobre $\mathrm{A}/\mathfrak{p}$. Ahora bien, en la sucesión de arriba, hay e_i cocientes consecutivos de la forma $\mathfrak{B}/\mathfrak{P}_i$ con i dado. La dimensión total $[\mathrm{B} : \mathrm{B}\mathfrak{p} : \mathrm{A}/\mathfrak{p}]$ es igual a la suma de las dimensiones de estos cocientes, es decir a $\sum_{i=1}^{q} e_i f_i$.

La segunda igualdad es fácil también en el caso en el cual B es un A-módulo libre, en particular cuando A es un **dominio de ideales principales** (capítulo II, §7, corolario del teorema 1): en efecto una base $(x_1, \ldots, x_n)$ del A-módulo B da, por reducción mod $\mathrm{B}\mathfrak{p}$, una base de $\mathrm{B}/\mathrm{B}\mathfrak{p}$ sobre $\mathrm{A}/\mathfrak{p}$. Nos reduciremos a este case considerando el subconjunto multiplicativo $\mathrm{S} = \mathrm{A} - \mathfrak{p}$ de A y los anillos de fracciones $\mathrm{A}' = \mathrm{S}^{-1}\mathrm{A}$ y $\mathrm{B}' = \mathrm{S}^{-1}\mathrm{B}$. Sabemos que A' es un dominio de ideales principales en el cual $\mathfrak{p}\mathrm{A}'$ es el único ideal maximal (§1, proposición 4) y que B' es la clausura íntegra de A' en L (§1, proposición 2). Por el caso de dominios de ideales principales, se tiene $[\mathrm{B}'/\mathfrak{p}\mathrm{B}' : \mathrm{A}'/\mathfrak{p}\mathrm{A}'] = n$. Consideremos entonces ls descomposición del ideal $\mathfrak{p}\mathrm{B}'$ en el anillo de Dedekind B': de $\prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$, deducimos que $\mathfrak{p}\mathrm{B}' = \prod_{i=1}^{q} (\mathrm{B}'\mathfrak{P}_i)^{e_i}$. Como $\mathfrak{P}_i \cap \mathrm{A} = \mathfrak{p}$, (proposición 1), se tiene $\mathfrak{P}_i \cap \mathrm{S} = \emptyset$ y $\mathrm{B}'\mathfrak{P}_i$ es un ideal primo no nulo de B' (§1, proposiciones 1, 2). La primer parte de la demostración nos da ?????!!!! por lo tanto

$$[\mathrm{B}'/\mathfrak{p}\mathrm{B}' : \mathrm{A}'/\mathfrak{p}\mathrm{A}'] = \sum_{i=1}^{q} e_i [\mathrm{B}'/\mathrm{B}'\mathfrak{P}_i : \mathrm{A}'/\mathfrak{p}\mathrm{A}'].$$

Ahora bien, se tiene $\mathrm{A}'/\mathfrak{p}\mathrm{A}' \simeq \mathrm{A}/\mathfrak{p}$ y $\mathrm{B}'/\mathrm{B}'\mathfrak{P}_i \simeq \mathrm{B}/\mathfrak{P}_i$ (§1, proposición 5), de donde, combinando las igualdades, $n = [\mathrm{B}'/\mathfrak{p}\mathrm{B}' : \mathrm{A}'/\mathfrak{p}\mathrm{A}'] = \sum_{i=1}^{q} e_i f_i$, lo que demuestra (2).

Proposición 2. *Con la misma notación que antes, el anillo* $\mathrm{B}/\mathrm{B}\mathfrak{p}$ *es isomorfo a* $\prod_{i=1}^{q} \mathrm{B}/\mathfrak{P}_i^{e_i}$.

En efecto, como $\mathfrak{P}_i$ es el único ideal maximal de B que contiene a $\mathfrak{P}_i^{e_i}$, se tiene $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = \mathrm{B}$ si $i \neq j$. Aplicamos entonces (1) y el lema de §3, capítulo I.

Ejemplo de los cuerpos ciclotómicos. Sea p un número primo y $z \in \mathbf{C}$ una raíz primitiva p-ésima de la unidad. Las raíces p^r-ésimas de la unidad, en $\mathbf{C}$, son entonces los z^j $(j = 1, \ldots, p^r)$. Entre ellas, las raíces primitivas son los z^j

tales que j no es un múltiplo de p y por lo tanto su número es

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

(cf. capítulo I, §6). Estas racíces primitivas p^r-ésimas de la unidad son las raíces del polinomio ciclotómico

$$\text{(3)} \qquad \mathrm{F(X)} = \frac{\mathrm{X}^{p^r} - 1}{\mathrm{X}^{p^{r-1}} - 1} = \mathrm{X}^{p^{r-1}(p-1)} + \mathrm{X}^{p^{r-1}(p-2)} + \cdots + \mathrm{X}^{p^{r-1}} + 1.$$

Nos proponemos ahora demostrar aquí que se tiene $[\mathbf{Q}[z] : \mathbf{Q}] = p^{r-1}(p-1)$, es decir que F(X) es irreducible (cf. capítulo II, §9). Pongamos $e = p^{r-1}(p-1)$ y sean $z_1, \ldots, x_e$ las raíces primitivas p^r-ésimas de la unidad. Como el término constante de $\mathrm{F(X+1)}$ es p, se tiene

$$\prod_{j=1}^{e}(z_j - 1) = \pm p.$$

Sea B el anillo de enteros de $\mathbf{Q}[z]$; evidentemente se tiene $z_j \in \mathrm{B}$, y también $z_j - 1 \in \mathrm{B}(z_k - 1)$ para todo j, k pues z_j es una potencia z_k^q de z_k y se tiene $z_k^q - 1 = (z_k - 1)(z_k^{q-1} + \cdots + z_k + 1)$. Así todos los ideales $\mathrm{B}(z_k - 1)$ son iguales. Tenemos por lo tanto $\mathrm{B}p = \mathrm{B}(z_1 - 1)^e$.

Escribimos $\mathrm{B}p = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$ donde los $\mathfrak{P}_i$ son ideales primos de B. Los e_i son por lo tanto todos múltiplos de e. Pero como $e \geq [\mathbf{Q}[z] : \mathbf{Q}]$ (por (3)), se sigue que $e \geq \sum_{i=1}^{q} e_i f_i$ (teorema 1). De estas desigualdades opuestas ????? deducimos que $q = 1$, $e = e_1$, $f_1 = 1$, $[\mathbf{Q}[z] : \mathbf{Q}] = e$. En resúmen:

1. $[\mathbf{Q}[z] : \mathbf{Q}] = e = p^{r-1}(p-1)$
2. $\mathrm{B}(z_1 - 1)$ es un ideal primo de B de grado residual 1.
3. $\mathrm{B}p = \mathrm{B}(z_1 - 1)^e$.

3. Discriminante y ramificación

Con la notación de §2 (sea $\mathrm{B}\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$, decimos que un ideal primo $\mathfrak{p}$ de A **ramifica** en B (o en L) si alguno de los índices de ramificación e_i es ≥ 2. Por medio de la teoría del discriminante (capítulo II, §7) ahora determinaremos los ideales primos de A que ramifican en B, y veremos en particular que sólo hay **un número finito.** Algunos lemas sobre los discriminantes nos serán útiles.

Lema 1. *Sea* A *un anillo,* $\mathrm{B}_1, \ldots, \mathrm{B}_q$ *anillos que contienen a* A *y que son* A*-módulos libres de rango finito y* $\mathrm{B} = \prod_{i=1}^{q} \mathrm{B}_i$ *el anillo producto. Entonces* $\mathfrak{D}_{\mathrm{B/A}} = \prod_{i=1}^{q} \mathfrak{D}_{\mathrm{B}_i/\mathrm{A}}$ *(cf. capítulo II, §7, definición 2).*

En efecto una inducción sobre q nos permite suponer que $q = 2$. Sean entonces $(x_1, \ldots, x_m)$, $(y_1, \ldots, y_n)$ dos bases de B_1 y B_2 sobre A. Con la identificación clásica de B_1 y B_2 con $B_1 \times (0)$ y $(0) \times B_2$, $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ es una base de $B = B_1 \times B_2$ sobre A. Se tiene $x_i y_j = 0$ por definición de la estructura de anillo producto, de donde $\mathrm{Tr}(x_i y_j) = 0$. Así, el determinante $D(x_1, \ldots, x_m, y_1, \ldots, y_n)$ se escribe:

$$\begin{vmatrix} \mathrm{Tr}(x_i x_{i'}) & 0 \\ 0 & \mathrm{Tr}(y_j y_{j'}) \end{vmatrix}$$

Por lo tanto tiene el valor ????

$$\det(\mathrm{Tr}(x_i x_{i'})) \cdot \det(\mathrm{Tr}(y_j y_{j'})),$$

de donde

$$D(x_1, \ldots, x_m, y_1, \ldots, y_n) = D(x_1, \ldots, x_m) D(y_1, \ldots, y_n).$$

Lema 2. *Sea* A *un anillo,* B *un anillo que contiene a* A *y que admite una base finita* $(x_1, \ldots, x_n)$ *y* $\mathfrak{a}$ *un ideal de* A. *Si* $x \in B$, *notamos* $\overline{x}$ *la clase de* x *en* $B/\mathfrak{a}B$. *Entonces* $(\overline{x}_1, \ldots, \overline{x}_n)$ *es una base de* $B/\mathfrak{a}B$ *sobre* $A/\mathfrak{a}$ *y se tiene*

$$D(\overline{x}_1, \ldots, \overline{x}_n) = \overline{D(x_1, \ldots, x_n)}. \tag{1}$$

En efecto, sea $x \in B$. Si la matriz de la multiplicación por x, en la base (x_i) es (a_{ij}) $(a_{ij} \in A)$, la matriz de la multiplicación por $\overline{x}$ en la base $(\overline{x}_i)$ es la matriz $(\overline{a}_{ij})$. Por lo tanto se tiene $\mathrm{Tr}(\overline{x}) = \overline{\mathrm{Tr}(x)}$, de donde

$$\mathrm{Tr}(\overline{x}_i \cdot \overline{x}_j) = \overline{\mathrm{Tr}(x_i x_j)},$$

y por lo tanto se obtiene (1) tomando determinantes.

Lema 3. *Sea* K *un cuerpo finito o de característica cero y* L *una* K*-álgebra de dimensión finita sobre* K. *Para que* L *sea reducido es necesario y suficiente que* $\mathfrak{D}_{L/K} \neq (0)$.

Supongamos primero que L no es reducida y sea $x \in L$ un elemento nilpotente no nulo. Ponemos $x_1 = x$ y completamos este elemento de base en una base $(x_1, \ldots, x_n)$ de L sobre K. Entonces $x_1 x_j$ es nilpotente y por lo tanto la multiplicación por $x_1 x_j$ es un endomorfismo nilpotente; por lo tanto todos sus autovalores son nulos, de donde $\mathrm{Tr}(x_1 x_j) = 0$. La matriz $(\mathrm{Tr}(x_i x_j))$ tiene por lo tanto una fila nula, de manera que su determinante $D(x_1, \ldots, x_n)$ es nulo, de donde $\mathfrak{D}_{L/K} = (0)$.

Reciprocamente, supongamos que L es reducido. Entonces el ideal (0) de L es una intersección finita de ideales primos, $(0) = \bigcap_{i=1}^{q} \mathfrak{P}_i$ (capítulo IV, §6, lema). Como $L/\mathfrak{P}_i$ es un dominio íntegro de dimensión finita sobre K,

es un cuerpo (capítulo II, §1, proposición 3). Por lo tanto $\mathfrak{P}_i$ es un ideal maximal de L, de manera que $\mathfrak{P}_i + \mathfrak{P}_j = \mathrm{L}$ si $i \neq j$. Así L es isomorfo al producto $\prod_{i=1}^{q} \mathrm{L}/\mathfrak{P}_i$ (capítulo I, §3, lema 1). Tenemos por lo tanto $\mathfrak{D}_{\mathrm{L/K}} = \prod_{i=1}^{q} \mathfrak{D}_{(\mathrm{L}/\mathfrak{P}_i)/\mathrm{K}}$ (lema 1). Ahora bien, $\mathfrak{D}_{(\mathrm{L}/\mathfrak{P}_i)/\mathrm{K}} \neq (0)$ pues K es finito o de característica cero (capítulo II, §7, proposición 3), de donde $\mathfrak{D}_{\mathrm{L/K}} \neq (0)$. LQQD.

Definición 1. *Sean* K *y* L *dos cuerpos de números con* $\mathrm{K} \subset \mathrm{L}$, A *y* B *los anillos de enteros de* K *y* L. *Llamamos ideal discriminante de* B *sobre* A *(o de* L *sobre* K*), y lo notamos* $\mathfrak{D}_{\mathrm{B/A}}$ *o* $\mathfrak{D}_{\mathrm{L/K}}$*, al ideal de* A *generado por los discriminantes de las bases de* L *sobre* K *contenidas en* B.

Observación 1. Si $(x_1, \ldots, x_n)$ es una base de L sobre K contenida en B, se tiene $\mathrm{Tr}_{\mathrm{L/K}}(x_i x_j) \in \mathrm{A}$ (capítulo II, §6, corolario de la proposición 2), de donde $\mathrm{D}(x_1, \ldots, x_n) \in \mathrm{A}$. Así $\mathfrak{D}_{\mathrm{B/A}}$ es un ideal **entero** de A. Es **no nulo** por el capítulo II, §7, proposición 3.

Observación 2. Cuando B es un A-módulo **libre** (por ejemplo si A es principal) ya habíamos definido el ideal discriminante $\mathfrak{D}_{\mathrm{B/A}}$ como aquel generado por $\mathrm{D}(e_1, \ldots, e_n)$, donde $(e_1, \ldots, e_n)$ es una base de B sobre A (capítulo II, §7, definición 2). Coincide con el definido arriba pues, para toda base (x_i) de L sobre K contenida en B, se tiene $x_i = \sum_i a_{ij} e_j$ con $a_{ij} \in \mathrm{A}$, de donde $\mathrm{D}(x_1, \ldots, x_n) = \det(a_{ij})^2 \mathrm{D}(e_1, \ldots, e_n)$ (capítulo II, §7, proposición 1).

Teorema 1. *Con la notación de la def., para que un ideal primo* $\mathfrak{p}$ *de* A *ramifique en* B *es necesario y suficiente que contena al ideal discriminante* $\mathfrak{D}_{\mathrm{B/A}}$. *Sólo hay un número finito de ideales primos de* A *que ramifican en* B.

La segunda afirmación resulta de la primera pues vimos que $\mathfrak{D}_{\mathrm{B/A}} \neq (0)$.

Demostremos la primera. Como $\mathrm{B}/\mathfrak{p}\mathrm{B} \simeq \prod_{i=1}^{q} \mathrm{B}/\mathfrak{P}_i^{e_i}$ (§2, proposición 2), "$\mathfrak{p}$ ramifica" es equivalente a "$\mathrm{B}/\mathfrak{p}\mathrm{B}$ no reducido", es decir a "$\mathfrak{D}_{(\mathrm{B}/\mathfrak{p}\mathrm{B})/(\mathrm{A}/\mathfrak{p})} = (0)$" (CHEQUEAR LIBRO) pues $\mathrm{A}/\mathfrak{p}$ es un cuerpo finito (lema 3). Ahora bien, si ponemos $\mathrm{S} = \mathrm{A} - \mathfrak{p}$, $\mathrm{A}' = \mathrm{S}^{-1}\mathrm{A}$, $\mathrm{B}' = \mathrm{S}^{-1}\mathrm{B}$ y $\mathfrak{p}' = \mathfrak{p}\mathrm{A}'$, entonces A′ es un dominio de ideales principales (§1, proposición 4), B′ es un A′-módulo libre y se tiene $\mathrm{A}/\mathfrak{p} \simeq \mathrm{A}'/\mathfrak{p}'$ y $\mathrm{B}/\mathfrak{p}\mathrm{B} \simeq \mathrm{B}'/\mathfrak{p}'\mathrm{B}'$ (§1, proposición 5). Por lo tanto, si denotamos por $(e_1, \ldots, e_n)$ una base de B′ sobre A′, la relación $\mathfrak{D}_{(\mathrm{B}/\mathfrak{p}\mathrm{B})/(\mathrm{A}/\mathfrak{p})} = (0)$ es equivalente a $\mathrm{D}(e_1, \ldots, e_n) \in \mathfrak{p}'$ (lema 2). Por lo tanto, si $\mathrm{D}(e_1, \ldots, e_n) \in \mathfrak{p}'$ y $(x_1, \ldots, x_n)$ es una base de L sobre K contenida en B, se tiene $x_i = \sum a'_{ij} e_j$ con $a'_{ij} \in \mathrm{A}'$ (pues $\mathrm{B} \subset \mathrm{B}'$), de donde $\mathrm{D}(x_1, \ldots, x_n) = \det(a'_{ij})^2 \mathrm{D}(e_1, \ldots, e_n) \in \mathfrak{p}'$. Como $\mathfrak{p}' \cap \mathrm{A} = \mathfrak{p}$ (§1, proposiciones 1, 2), deducimos que $\mathrm{D}(x_1, \ldots, x_n) \in \mathfrak{p}$ y $\mathfrak{D}_{\mathrm{B/A}} \subset \mathfrak{p}$. Reciprocamente, si $\mathfrak{D}_{\mathrm{B/A}} \subset \mathfrak{p}$, se tiene $\mathrm{D}(e_1, \ldots, e_n) \in \mathfrak{p}'$ pues

podemos escribir $e_i = \frac{y_i}{s}$ con $y_i \in \mathrm{B}$ y $s \in \mathrm{S}$ para $1 \leq i \leq n$. Así,

$$\mathrm{D}(e_1, \ldots, e_n) = s^{-2n}\mathrm{D}(x_1, \ldots, x_n) \in \mathrm{A}'\mathfrak{D}_{\mathrm{B/A}} \subset \mathrm{A}'\mathfrak{p} = \mathfrak{p}'.$$

Ejemplo de los cuerpos cuadráticos. Tomemos $\mathrm{K} = \mathbf{Q}$ y $\mathrm{L} = \mathbf{Q}[\sqrt{d}]$, donde d es un entero libre de cuadrados (capítulo II, §5).

a) Si $d \equiv 2$ ó $3 \pmod 4$, $(1, \sqrt{d})$ es una base del anillo de enteros de L. Como $\mathrm{Tr}(1) = 2$, $\mathrm{Tr}(\sqrt{d}) = 0$ y $\mathrm{Tr}(d) = 2d$, se tiene $\mathrm{D}(1, \sqrt{d}) = 4d$. Los números primos que ramifican en L son por lo tanto 2 y los divisores primos de d.

b) Si $d \equiv 1 \pmod 4$, $\left(1, \frac{1+\sqrt{d}}{2}\right)$ es una base del anillo de enteros de L. Se tiene

$$\mathrm{Tr}(1) = 2, \quad \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1$$

y

$$\mathrm{Tr}\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) = \mathrm{Tr}\left(\frac{d+1}{4} + \frac{1}{2}\sqrt{d}\right) = \frac{d+1}{2}.$$

De donde se obtiene $\mathrm{D}\left(1, \frac{1+\sqrt{d}}{2}\right) = 2 \cdot \frac{d+1}{2} - 1 = d$. Los números primos que ramifican en L son por lo tanto los divisores de d.

Observamos que un cuerpo cuadrático $\mathbf{Q}[\sqrt{d}]$ está unívocamente determinado por su discriminante D; en efecto $4d = \mathrm{D}$ si $d \equiv 2$ ó $3 \pmod 4$ y $\mathrm{D} \equiv 1 \pmod 4$ es imposible. También observamos que el discriminante de un cuerpo cuadrático no es un entero arbitrario.

Ejemplo de los cuerpos ciclotómicos. Sea p un número primo, $z \in \mathbf{C}$ una raíz primitiva p-ésima de la unidad y $\mathrm{L} = \mathbf{Q}[z]$ el cuerpo ciclotómico correspondiente. Sabemos que el anillo B de enteros de L admite $(1, z, \ldots, z^{p-2})$ como base sobre $\mathbf{Z}$ (capítulo II, §9, teorema 2) y que el polinomio minimal $\mathrm{F}(\mathrm{X})$ de z sobre $\mathbf{Q}$ satisface $(\mathrm{X}-1)\mathrm{F}(\mathrm{X}) = \mathrm{X}^p - 1$ (**ibid;** teorema 1). Ahora calcularemos el discriminante $\mathfrak{D}_{\mathrm{B}/\mathbf{Z}}$ utilizando la fórmula $\mathrm{D}(1, z, \ldots, z^{p-2}) = \mathrm{N}(\mathrm{F}'(z))$ (capítulo II, §7, fórmula (6)). Derivando $(\mathrm{X}-1)\mathrm{F}(\mathrm{X}) = \mathrm{X}^p - 1$, obtenemos $(z-1)\mathrm{F}'(z) = pz^{p-1}$ (pues $\mathrm{F}(z) = 0$). Como $\mathrm{N}(p) = p^{p-1}$, $\mathrm{N}(z) = \pm 1$, $\mathrm{N}(z-1) = \pm p$ (capítulo II, §9), tenemos por lo tanto

$$\mathrm{D}(1, z, \ldots, z^{p-2}) = \pm p^{p-2}. \tag{2}$$

Se sigue que p es el **único** número primo que ramifica en $\mathbf{Q}[z]$.

El siguiente resultado es a veces útil para determinar el anillo de enteros de un cuerpo de números:

Proposición 1. *Sea* L *un cuerpo de números de grado* n *sobre* $\mathbf{Q}$ *y* $(x_1,\ldots,x_n)$ *enteros de* L *que forman una base de* L *sobre* $\mathbf{Q}$. *Si el discriminante* $\mathrm{D}(x_1,\ldots,x_n)$ *es libre de cuadrados entonces* $(x_1,\ldots,x_n)$ *es una base sobre* $\mathbf{Z}$ *del anillo* B *de enteros de* L.

En efecto, si $(e_1,\ldots,e_n)$ es una base de B sobre $\mathbf{Z}$, se tiene $x_1 = \sum_{j=1}^{n} a_{ij}e_j$ con $a_{ij} \in \mathbf{Z}$. De donde se sigue que $\mathrm{D}(x_1,\ldots,x_n) = \det(a_{ij})^2\mathrm{D}(e_1,\ldots,e_n)$. Como $\mathrm{D}(x_1,\ldots,x_n)$ es libre de cuadrados, deducimos que $\det(a_{ij}) = \pm 1$, lo que implica que $(x_1,\ldots,x_n)$ también es una base de B sobre $\mathbf{Z}$.

> *El ejemplo de los cuerpos ciclotómicos (para* $p \geq 5$*), o de los cuerpos cuadráticos, muestra que la condición suficiente anterior no es necesaria.*

Ejemplo. El polinomio $\mathrm{X}^3-\mathrm{X}-1$ (resp. $\mathrm{X}^3+\mathrm{X}+1$, $\mathrm{X}^3+10\mathrm{X}+1$) es **irreducible** sobre $\mathbf{Q}$. Sino, en efecto, tendría un factor lineal, y por lo tanto una raíz $x \in \mathbf{Q}$ y se tendría entonces que $x \in \mathbf{Z}$ pues el polinomio es mónico. Como el término constante es 1, tendríamos que $x = \pm 1$ (pues todo factor de x divide al término constante). Pero esto no es verdad. Por lo tanto, si denotamos por $x \in \mathbf{C}$ una raíz de este polinomio, el cuerpo $\mathrm{L} = \mathbf{Q}[x]$ es un **cuerpo cúbico** (i.e. de grado 3). Así $(1,x,x^3)$ es una base de L sobre $\mathbf{Q}$ y x es evidentemente un entero de L. Como, utilizando la fórmula (7) del §7, capítulo II, se tiene que $\mathrm{D}(1,x,x^2) = -4 + 27 = 23$ (resp. 31, 4027), que es un número primo. Por lo tanto $(1,x,x^2)$ es una base sobre $\mathbf{Z}$ del anillo de enteros de L.

4. Descomposición de un número primo en un cuerpo cuadrático

Sea $d \in \mathbf{Z}$ un entero libre de cuadrados, L el cuerpo cuadrático $\mathrm{L} = \mathbf{Q}[\sqrt{d}]$, B el anillo de enteros de L y p un número primo. Estudiaremos la descomposición en ideales primos del ideal $p\mathrm{B}$.

La fórmula $\sum_{i=1}^{q} e_i f_i = 2$ (§2, teorema 1) muestra que se tiene $q \leq 2$ y que sólo puede producirse tres casos:

1. $q = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$. Decimos entonces que p **se descompone totalmente** en L;
2. $q = 1$, $e_1 = 1$, $f_1 = 2$; decimos entonces que p es **inerte** en L;
3. $q = 1$, $e_1 = 2$, $f_1 = 1$; esto quiere decir que p **ramifica** en L.

Examinemos primero el **caso cuando** p **es impar.** Sabemos (capítulo II, §5) que $\mathrm{B} = \mathbf{Z} + \mathbf{Z}\sqrt{d}$ o $\mathrm{B} = \mathbf{Z} + \mathbf{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ según el valor de d. Pero, si tomamos las clase de B módulo $\mathrm{B}p$, vemos, en el segundo caso, que $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ (con

b impar) es congruente a $a+(b+p)\left(\frac{1+\sqrt{d}}{2}\right)$, que es un elemento de $\mathbf{Z}+\mathbf{Z}\sqrt{d}$. Por lo tanto, en todos los casos, se tiene

$$\mathrm{B}/\mathrm{B}p \simeq (\mathbf{Z}+\mathbf{Z}\sqrt{d})/(p).$$

Ahora bien, $\mathbf{Z}+\mathbf{Z}\sqrt{d} \simeq \mathbf{Z}[\mathrm{X}]/(\mathrm{X}^2-d)$, de donde se sigue

$$\mathrm{B}/\mathrm{B}p \simeq \mathbf{Z}[\mathrm{X}]/(p,\mathrm{X}^2-d) \simeq (\mathbf{Z}[\mathrm{X}]/(p))/(\mathrm{X}^2-d) \simeq \mathbf{F}_p[\mathrm{X}]/(\mathrm{X}^2-\overline{d}),$$

donde $\overline{d}$ denota la clase de d módulo p. Ahora bien, la afirmación de que p se descompone totalmente (resp. es inerte, ramifica) en B significa que $\mathrm{B}/\mathrm{B}p$ es un producto de dos cuerpos (resp. es un cuerpo, tiene elementos nilpotentes) (cf. §2, proposición 2), esto significa por lo tnto que, en $\mathbf{F}_p[\mathrm{X}]$, el polinomio X^2-d es producto de dos factores distintos de grado uno (resp. es irreducible, es un cuadrado). Y esto ocurre si $\overline{d}$ es un cuadrado no nulo en $\mathbf{F}_p$ (resp. no es un cuadrado en $\mathbf{F}_p$, es nulo en $\mathbf{F}_p$). Cuando $\overline{d}$ es un cuadrado no nulo en $\mathbf{F}_p$ (resp. no es un cuadrado en $\mathbf{F}_p$) decimos que d es un **residue cuadrático** (resp. un **no residue cuadrático**) módulo p.

Tratemos ahora **el caso** $p=2$. Si $d \equiv 2,3 \pmod 4$, se tiene $\mathrm{B}=\mathbf{Z}+\mathbf{Z}\sqrt{d}$, de donde, como más arriba $\mathrm{B}/2\mathrm{B} \simeq \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^2-\overline{d})$. Ahora bien, $\mathrm{X}^2-\overline{d}$ vale X^2 o $\mathrm{X}^2+1=(\mathrm{X}+1)^2$ y es por lo tanto un cuadrado. Así 2 ramifica en B. Si $d \equiv 1 \pmod 4$, $\frac{1+\sqrt{d}}{2}$ admite $\mathrm{X}^2-\mathrm{X}-\frac{d-1}{4}$ como polinomio minimal, de donde, como más arriba, $\mathrm{B}/2\mathrm{B} \simeq \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^2-\mathrm{X}-\delta)$ donde δ es la clase mod 2 de $\frac{d-1}{4}$. Si $d \equiv 1 \pmod 8$ se tiene $\delta=0$ y $\mathrm{X}^2-\mathrm{X}-\delta=\mathrm{X}(\mathrm{X}-1)$, de manera que 2 se descompone totalmente. Si $d \equiv 5 \pmod 8$, se tiene $\delta=1$ y $\mathrm{X}^2-\mathrm{X}-\delta=\mathrm{X}^2+\mathrm{X}+1$ es irreducible en $\mathbf{F}_2[\mathrm{X}]$, de manera que 2 es inerte.

En resúmen, hemos demostrado los siguientes resultados:

Proposición 1. *Sea* $\mathrm{L}=\mathbf{Q}[\sqrt{d}]$ *un cuerpo cuadrático, donde* $d \in \mathbf{Z}$ *es libre de cuadrados.*

1. *Se descomponent totalmente en* L*: los números primos impares* p *tales que* d *es un residuo cuadrático mód* p *y* 2 *y* $d \equiv 1 \pmod 8$*;*
2. *Son inertes en* L*: los números primos impares* p *tales que* d *no es un residue cuadrático mod* p *y* 2 *si* $d \equiv 5 \pmod 8$*;*
3. *Ramifican en* L*: los divisores primos impares de* d *y* 2 *si* $d \equiv 2$ *ó* $3 \pmod 4$.

La afirmación c) ya había sido demostrada en un ejemplo del §3.

5. La ley de reciprocidad cuadrática

Dados un número primo **impar** p y un entero d coprimo con p, hemos introducido en el §4 la frase "d es **un residue cuadrático** mod p" (resp. "d **no es un residue cuadrático** mod p") como queriendo decir que la clase de d mod p es un cuadrado (resp. no es un cuadrado) en $\mathbf{F}_p^*$. Ahora introducimos aquí el **símbolo de Legendre** $\left(\frac{d}{p}\right)$ definido así:

$$(1) \qquad \begin{cases} \left(\frac{d}{p}\right) = +1 & \text{si } d \text{ es un residuo cuadrático mod } p. \\ \left(\frac{d}{p}\right) = -1 & \text{si } d \text{ no es un residuo cuadrático mod } p. \end{cases}$$

Por supuesto ???? $\left(\frac{d}{p}\right)$ sólo está definido para d coprimo con p, es decir para $d \in \mathbf{Z} - p\mathbf{Z}$. Como el grupo multiplicativo $\mathbf{F}_p^*$ es cíclico de orden par $p-1$ (capítulo I, §7, teorema 1), los cuadrados forman un subgrupo $\mathbf{F}_p^{*2}$ de índice 2 y $\mathbf{F}_p^*/\mathbf{F}_p^{*2}$ es isomorfo a $\{+1, -1\}$. Así el símbolo de Legendre se obtiene componiendo los homomorfismo

$$\mathbf{Z} - p\mathbf{Z} \to \mathbf{F}_p^* \to \mathbf{F}_p^*/\mathbf{F}_p^{*2} \xrightarrow{\sim} \{+1, -1\}.$$

Por lo tanto se tiene la fórmula de multiplicatividad

$$(2) \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proposición 1 (Criterio de Euler)**.** *Si p es un número primo impar y si $a \in \mathbf{Z} - p\mathbf{Z}$, se tiene $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

En efecto sea w una raíz primitiva mod p (capítulo I, §7). Se tiene $a \equiv w^j \pmod{p}$ para algún $0 \leq j \leq p-2$ pues la clase $\overline{w}$ de w es un generador de $\mathbf{F}_p^*$. Es claro que "a residue cuadrático" equivale a "j par". Por lo tanto se tiene $\left(\frac{a}{p}\right) = (-1)^j$. Por otra parte, $\mathbf{F}_p^*$ tiene un sólo elemento de orden 2, a saber $\overline{w}^{\frac{p-1}{2}}$ y necesariamente debe ser igual a -1 pues su cuadrado es 1. Por lo tanto, en $\mathbf{Z}$, se tiene $-1 \equiv w^{\frac{p-1}{2}} \pmod{p}$. Así,

$$\left(\frac{a}{p}\right) = (-1)^j \equiv w^{j \cdot \frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Ahora demostraremos un resultado celebre, que muestra que las propiedades de congruencias módulo dos números primos impares distintos no son independientes.

Teorema 1 ("Ley de reciprocidad cuadrática de Legendre-Gauss"). *Si p y q son dos números primos impares distintos, se tiene*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

En efecto, consideremos, en una extensión conveniente de $\mathbf{F}_q$, una raíz primitiva p-ésima de la unidad w. Como $w^p = 1$, la notación w^x tiene sentido para $x \in \mathbf{F}_p$. También escribiremos el símbolo de Legendre $\left(\frac{x}{p}\right)$ para $x \in \mathbf{F}_p^*$ pues $\left(\frac{d}{p}\right)$ sólo depende evidentemente de la clase de d mod p. Si $x \in \mathbf{F}_p^*$, consideremos la **"suma de Gauss"**.

$$\tau(a) = \sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right) w^{ax}. \tag{3}$$

Es un elemento de una extensión de $\mathbf{F}_q$. Poniendo $ax = y$, se tiene

$$\tau(a) = \sum_{y \in \mathbf{F}_p^*} \left(\frac{ya^{-1}}{p}\right) w^y = \left(\frac{a^{-1}}{p}\right) \sum_{y \in \mathbf{F}_p^*} \left(\frac{y}{p}\right) w^y$$

(por (2)), de donde

$$\tau(a) = \left(\frac{a}{p}\right) \tau(1). \tag{4}$$

Por otra parte, como estamos calculando en característica q y $\left(\frac{x}{p}\right) \in \mathbf{F}_q$, se tiene $\tau(1)^q = \sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right)^q w^{qx}$, de donde, identificando q con su clase mod p,

$$\tau(1)^q = \tau(q). \tag{5}$$

Calculemos ahora $\tau(1)^2$. Se tiene

$$\tau(1)^2 = \sum_{x,y \in \mathbf{F}_p^*} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) w^{x+y}.$$

Poniendo $y = tx$, esto se vuelve ????

$$\tau(1)^2 = \sum_{x,t \in \mathbf{F}_p^*} \left(\frac{x}{p}\right)^2 \left(\frac{t}{p}\right) w^{x(1+t)} = \sum_{x,t} \left(\frac{t}{p}\right) w^{x(1+t)} = \sum_{t \in \mathbf{F}_p^*} \left[\left(\frac{t}{p}\right) \sum_{x \in \mathbf{F}_p^*} w^{x(1+t)}\right].$$

Si $w^{1+t} \neq 1$, se tiene $\sum_{j=0}^{p-1} (w^{1+t})^j = 0$ por la fórmula de la sucesión geométrica, pues $(w^{1+t})^p = 1$, de donde $\sum_{x \in \mathbf{F}_p^*} w^{x(1+t)} = -1$. Si $w^{1+t} = 1$, se tiene

$\sum_{x\in\mathbf{F}_p^*} w^{x(1+t)} = p-1$. Esto último ocurre unicamente cuando $t=-1$, pues w es una raíz primitiva p-ésima de la unidad. Tenemos por lo tanto

$$\tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\in\mathbf{F}_p^*, t\neq -1}\left(\frac{t}{p}\right).$$

Como hay tantos cuadrados como no cuadrados en $\mathbf{F}_p^*$, se tiene

$$\sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right) = 0, \quad \text{de donde} \quad \tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)p.$$

Por el criterio de Euler (proposición 1), tenemos por lo tanto,

$$\tau(1)^2 = (-1)^{\frac{p-1}{2}}p. \tag{6}$$

Por último, por (4) y (5), tenemos $\tau(1)^q = \tau(q) = \left(\frac{q}{p}\right)\tau(1)$. Como $\tau(1)$ es no nulo por (6), podemos simplificar: $\tau(1)^{q-1} = \left(\frac{q}{p}\right)$. Por (6) de nuevo tenemos

$$\left(\frac{q}{p}\right) = (\tau(1)^2)^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}}p^{\frac{q-1}{2}}.$$

Como $p^{\frac{q-1}{2}} = \left(\frac{q}{p}\right)$ (proposición 1) y $\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)^{-1}$, la ley de reciprocidad cuadrática queda demostrada.

Proposición 2 ("fórmulas complementarias")**.** *Si p es un número primo impar se tiene*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. *CHECK THIS.*

En efecto *a*) es un caso particular del criterio de Euler (proposición 1). Demostremos por lo tanto *b*). Observemos primero que nada que, como los cuadrados de $1,3,5,7$ mod 8 son 1,1,1,1, se tiene $p^2\equiv 1 \pmod 8$ y la fórmula escrita tiene sentido. Obeservemos a continuación que, en el grupo $\mathrm{H} = \{1,3,5,7\}$ de elementos inversibles de $\mathbf{Z}/8\mathbf{Z}$, $\{1,7\}$ es un subgrupo H' de índice 2. Pongamos $\theta(x) = 1$ si $x\in\mathrm{H}'$ y $\theta(x) = -1$ si $x\in\mathrm{H}-\mathrm{H}'$, de manera que $\theta(xy) = \theta(x)\theta(y)$ para $x,y\in\mathrm{H}$. Sea entonces w una raíz primitiva 8-ésima de la unidad en una extensión de $\mathbf{F}_p$. Como en el teorema 1, consderemos, para $a\in\mathrm{H}$, la **"suma de Guass"**.

$$\tau(a) = \sum_{x\in\mathrm{H}}\theta(x)w^{ax}. \tag{7}$$

Como en el teorema 1, se tiene $\tau(a) = \theta(a)\tau(1)$ y $\tau(1)^p = \tau(p)$ (identificando p con su clase mod 8). Por la definición de $\theta(x)$, se tiene

$$\begin{aligned}\tau(1) &= w - w^3 - w^5 + w^7 = (1 - w^2)(w - w^5)\\ &= w(1 - w^2)(1 - w^4) = 2w(1 - w^2)\end{aligned}$$

(pues $w^8 = 1$ y $w^4 = -1$), de donde

$$\tau(1)^2 = 4w^2(1 - 2w^2 + w^4) = -8w^4 = 8.$$

Como en el teorema 1, deducimos que $\tau(1)^p = \tau(p) = \theta(p)\tau(1)$, de donde, simplificando, $\theta(p) = (\tau(1)^2)^{\frac{p-1}{2}} = 8^{\frac{p-1}{2}} = \left(\frac{8}{p}\right)$ (proposición 1) $= \left(\frac{2}{p}\right)^2 = \left(\frac{2}{p}\right)$. Tenemos por lo tanto que $\left(\frac{2}{p}\right) = \theta(p)$. Pero como podemos constatar con un cálculo directo, si $x = 1,3,5,7$ (o, más eficazmente, si $x = 1,3,-3,-1$), se tiene $\theta(x) = (-1)^{\frac{x^2-1}{2}}$ y $\frac{x^2-1}{2}$ sólo depende de la clase de x mod 8. LQQD.

Ejemplo. La ley de reciprocidad cuadrática y las fŕomulas complementarias permiten calcular el símbolo de Legendre por reducción sucesiva. Calculemos así $\left(\frac{23}{59}\right)$, sin escribir la larga table de los cuadrados módulo 49. Se tiene

$$\begin{aligned}\left(\frac{23}{59}\right) &= (-1)^{11\cdot 29}\left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = -(-1)^{6\cdot 11}\left(\frac{23}{13}\right) = -\left(\frac{10}{13}\right)\\ &= -\left(\frac{-3}{13}\right) = -\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) = -(-1)^6\left(\frac{3}{13}\right)\\ &= -(-1)^{6\cdot 1}\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

Por lo tanto 23 no es un cuadrado módulo 59.

6. Teorema de los dos cuadrados

Ahora aplicaremos la proposición 1 del §4 al cuerpo $\mathbf{Q}[i]$ donde $i^2 = -1$. Como $-1 \equiv 3 \pmod 4$, el anillo B de enteros de L es $\mathbf{Z} + \mathbf{Z}i$. Se llama **el anillo de enteros de Gauss.** Su discriminante es -4 (§3, ejemplo). Si p es un número primo impar y si u es un generador del grupo cíclico $\mathbf{F}_p^*$, se tiene $-1 = u^{\frac{p-1}{2}}$. Por lo tanto -1 es un cuadrado en $\mathbf{F}_p$ si y sólo si $\frac{p-1}{2}$ es par. De esto se sigue la clasificación:

- 2 ramifica en $\mathbf{Q}[i]$;
- los números primos de la forma $4k + 1$ se descomponen totalmente;
- los números primos de la forma $4k + 3$ quedan intertes.

El siguiente resultado nos será muy útil:

Proposición 1. *El anillo* $\mathrm{B} = \mathbf{Z} + \mathbf{Z}i$ *de los enteros de Gauss es un dominio de ideales principales.*

Aplastemos, en efecto, esta mosca con un "gros pave" ???? Con la notación del capítulo IV, §3, tenemos $n = 2$, $r_1 = 0$, $r_2 = 1$, $d = -4$. Por lo tanto (capítulo IV, §3, corolario de la proposición 1), toda clase de ideales de B contiene un ideal entero de norma $\leq \frac{4}{\pi} \cdot \frac{2}{4} |4|^{1/2} = \frac{4}{\pi}$, por lo tanto contiene al ideal unidad B (que es el único ideal entero de norma 1) pues $\frac{4}{\pi} < 2$. Así todo ideal de B es equivalente al ideal principal B, y es por lo tanto principal. LQQD.

> **Sketch???** *de una demostración elemental: como los puntos de* B *forman un retículo de* $\mathbf{C}$*, un poco de geometría muestra que, para todo* $x \in \mathbf{Q}[i]$*, existe* $z \in \mathrm{B}$ *tal que* $\mathrm{N}(x - z) = |x - z|^2 \leq \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} < 1$*; entonces, si* $\mathfrak{a}$ *es un ideal no nulo de* B*, elegimos en* $\mathfrak{a}$ *un elemento no nulo* u *de norma minimal (NB: esta norma es un entero* > 0*); para* $v \in \mathfrak{a}$ *aproximamos* $\frac{v}{u}$ *por un* $z \in \mathrm{B}$ *tal que* $\mathrm{N}\left(\frac{v}{u} - z\right) < 1$*. Entonces*
>
> $$\mathrm{N}(v - zu) < \mathrm{N}(u), \quad \textit{de donde} \quad v - zu = 0$$
>
> *pues* $v - zu \in \mathfrak{a}$*. En consecuencia* $v \in \mathrm{B}u$ *y* $\mathfrak{a} = \mathrm{B}u$*. Observemos la analogía con el proceso de división euclidea en* $\mathbf{Z}$*.*

Proposición 2 (Fermat)**.** *Todo número primo* $p \equiv 1 \pmod 4$ *es suma de dos cuadrados (i.e. es de la forma* $p = a^2 + b^2$ *con* $a,b \in \mathbf{N}$*).*

En efecto Bp se descompone en un producto $\mathfrak{p}_1\mathfrak{p}_2$ de ideales primos distintos. De esto se sigue que $p^2 = \mathrm{N}(\mathrm{B}p) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2)$ (capítulo III, §5, proposición 2). Como las normas de $\mathfrak{p}_1$ y de $\mathfrak{p}_2$ son distintas de 1, necesariamente se tiene

$$\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p.$$

Pero como $\mathfrak{p}_1$ es un ideal principal $\mathrm{B}(a+bi)$ $(a,b \in \mathbf{Z})$ (proposición 1), se sigue que, tomando normas, $p = \mathrm{N}(a + bi) = a^2 + b^2$. LQQD.

Teorema 1. *Sea* x *un entero natural y* $x = \prod_p p^{v_p(x)}$ *su descomposición en factores primos. Para que* x *sea suma de dos cuadrados es necesario y suficiente que, para todo* $p \equiv 3 \pmod 4$*, el exponente* $v_p(x)$ *sea par.*

Para demostrar la suficiencia, observemos que una suma de dos cuadrados $a^2 + b^2$ es la norma $\mathrm{N}(a+bi)$ de un elemento de B; por la multiplicatividad de las normas, el conjunto S de sumas de dos cuadrados es por lo tanto estable por

multiplicación. Como $2 = 1^2 + 1^2 \in \mathrm{S}$ y como todo cuadrado es elemento de S ($x^2 = x^2 + 0^2$), se sigue entonces de la proposición 2, que nuestra condición es suficiente.

Reciprocamente, sean $x = a^2 + b^2$ una suma de dos cuadrados (a,$b \in \mathbf{N}$) y p un número primo $\equiv 3 \pmod 4$. Vimos que el ideal Bp de B es primo. Por otra parte, se tiene $x = a^2 + b^2 = (a + bi)(a - bi)$. Sea n el exponente de Bp en la descomposición de B$(a+bi)$ en factores primos. Como Bp es estable por el automorfismo $\sigma : u + iv \mapsto u - iv$ de B, y $\sigma(a + ib) = a - ib$, el exponente de Bp en la descomposición de B$(a - ib$ también es n. En la descomposición de B$(a^2 + b^2)$, el exponente de Bp es por lo tanto $2n$. Como ningún número primo distinto de p pertenece a Bp (pues B$p \cap \mathbf{Z} = p\mathbf{Z}$), se tiene $v_p(x) = 2n$ y $v_p(x)$ es par. LQQD.

7. Teorema de los cuatro cuadrados

En esta §, nos proponemos demostrar el siguiente teorema:

Teorema 1 (Lagrange)**.** *Todo entero natural es suma de cuatro cuadrados.*

El método empleado es análogo de aquel de §6: en vez del anillo de enteros de Gauss, nosotros trabajaremos con un anillo de **quaterniones** convenientemente elegido.

Comencemos definiendo los quaterniones. Dadu un anillo A, notaremos (1,i,j,k) la base canónica del A-módulo A^4, y definimos una multiplicación por:

$$(1) \qquad \begin{cases} 1 \text{ es el elemento unidad} \\ i^2 = j^2 = k^2 = -1. \\ ij = -ji = k, jk = -kj = i, ki = -ik = j. \end{cases}$$

Extendemos esta multiplicación a los elementos $a+bi+cj+dk$ de A^4 por linearidad. La distributividad es entonces evidente. En cuanto a la asociatividad basta verficarla en elementos de la base: así

$$i(jk) = i^2 = -1 = k^2 = (ij)k;$$

como las fórmulas donde figura 1 son evidentes, sólo restan $3^3 - 1 = 26$ fórmulas para verificar; el lector paciente e incrédulo observará reducirá el número a verificar por permutación y los demás creerán la palabra del autor ???. Equipada con esta multiplicación, A^4 es por lo tanto un **anillo no necesariamente conmutativo,** e incluso una A**-álgebra,** que llamamos **el anillo de los cuaterniones** sobre A y que notamos **H**(A) (**H** en honor a W.R. Hamilton, inventor de los cuaterniones).

Dado un cuaternión $z = a + bi + cj + dk$ sobre A (escribimos a en vez de $a \cdot 1$), llamamos **cuaternión conjugado** de z, y notamos $\overline{z}$, al cuaternión $\overline{z} = a - bi - cj - dk$.

Lema 1. *Se tiene* $\overline{z+z'} = \overline{z} + \overline{z}'$, $\overline{zz'} = \overline{z}' \cdot \overline{z}$ *y* $\overline{\overline{z}} = z$. *En términos más savants ????,* $z \mapsto \overline{z}$ *es un antihomomorfismo involutivo de* $\mathbf{H}(\mathrm{A})$.

La primer y la tercer fórmula son evidentes. Para la segunda basta demostrar, por linealidad, que $\overline{xy} = \overline{yx}$ cuando x,$y \in \{1,i,j,k\}$.

Todo está claro si $x = 1$ o si $y = 1$. Si $x = y = i$, tenemos $\overline{xy} = \overline{-1} = -1$ y $\overline{y} \cdot \overline{x} = (-i)(-i) = i^2 = -1$. Si $x = i$ y $j = j$ se tiene

$$\overline{xy} = \overline{k} = -k \quad \text{y} \quad \overline{y} \cdot \overline{x} = (-j)(-i) = ji = -k.$$

Las demás verificaciones se deducen permutando los términos. LQQD.

Dado un cuaternión z sobre A, llamamos **norma reducida** de z, y la notamos $\mathrm{N}(z)$, al cuaternión $z\overline{z}$.

Lema 2. *a) Dado un cuaternión* $z = a + bi + cj + dk$ *sobre* A, *se tiene* $\mathrm{N}(z) = a^2 + b^2 + c^2 + d^2$ *(¡cuatro cuadrados!), por lo tanto* $\mathrm{N}(z) \in \mathrm{A}$.

b) Dados dos cuaterniones z, z' *sobre* A, *se tiene* $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$.

Para *a*), desarollamos $(a + bi + cj + dk)(a - bi - cj - dk)$: por (1) los términos "rectángulos" ???? desaparecen, y lo que resta es $a^2 + b^2 + c^2 + d^2$. Vemos también que $z\overline{z} = \overline{z}z$. Entonces

$$\mathrm{N}(zz') = zz' \cdot \overline{zz'} = zz'\overline{z}'\overline{z} = z\mathrm{N}(z')\overline{z} = z\overline{z}\mathrm{N}(z')$$

(pues el elemento $\mathrm{N}(z')$ de A conmuta con cualquier cueternión), de donde $\mathrm{N}(zz') = \mathrm{N}(z) \cdot \mathrm{N}(z')$. LQQD.

> *El lema 2 muestra que, en un anillo* A *(conmutativo), el conjunto de las normas reducidas de cuaterniones, es decir, las sumas de cuatro cuadrados, es estable por multiplicación.*

Ahora consideraremos, en $\mathbf{H}(\mathbf{Q})$, el subanillo no conmutativo $\mathbf{H}(\mathbf{Z})$ y el conjunto $\mathbf{H}$ de los **"cuaterniones de Hurwitz"** $a + bi + cj + dk$ donde los a, b, c, d están todos en $\mathbf{Z}$ o bien están todos en $\frac{1}{2} + \mathbf{Z}$.

Lema 3.

1. *El conjunto* $\mathbf{H}$ *de los cuaterniones de Hurwitz es un subanillo no conmutativo de* $\mathbf{H}(\mathbf{Q})$ *que contiene a* $\mathbf{H}(\mathbf{Z})$ *y estable por* $z \mapsto \overline{z}$.
2. *Para todo* $z \in \mathbf{H}$, *se tiene* $z + \overline{z} \in \mathbf{Z}$ *y* $\mathrm{N}(z) = z\overline{z} \in \mathbf{Z}$
3. *Para que* $z \in \mathrm{H}$ *sea inversible, es neceseario y sufciente que* $\mathrm{N}(z) = 1$
4. *Todo ideal a izquierda (reps. a drecha)* $\mathfrak{a}$ *de* $\mathbf{H}$ *es principal (i.e. es de la forma* $\mathbf{H}z$ *(resp.* $z\mathbf{H}$*)).*

Para a), todas las afirmaciones son evidentes, salvo la estabilidad de $\mathbf{H}$ bajo la multiplicación. Para eso, basta verificar que, si ponemos

$$u = \frac{1}{2}(1 + i + j + k),$$

se tiene $u \cdot 1$, $u \cdot i$, $u \cdot j$, $u \cdot k$ y $u^2 \in \mathbf{H}$. Ahora bien, $u \cdot 1 = \frac{1}{2}(1 + i + j + k)$, $u \cdot i = \frac{1}{2}(-1 + i + j - k)$, $u \cdot j = \frac{1}{2}(-1 - i + j + k)$,

$$u \cdot k = \frac{1}{2}(-1 + i - j + k);$$

de donde, sumando, $2u^2 = \frac{1}{2}(-2 + 2i + 2j + 2k)$ y $u^2 \in \mathbf{H}$.

Para b), si

$$z = \frac{1}{2} + a + \left(\frac{1}{2} + b\right) i + \left(\frac{1}{2} + c\right) j + \left(\frac{1}{2} + d\right) k \quad (a,b,c,d \in \mathbf{Z}),$$

se tiene $z + \overline{z} = 1 + 2a \in \mathbf{Z}$ y

$$z\overline{z} = \left(\frac{1}{2} + a\right)^2 + \left(\frac{1}{2} + b\right)^2 + \left(\frac{1}{2} + c\right)^2 + \left(\frac{1}{2} + d\right)^2 \in \frac{4}{4} + \mathbf{Z} \subset \mathbf{Z}$$

(lema 2, b).

Si z es inversible en $\mathbf{H}$, y si z' es su inverso, tenemos

$$\mathrm{N}(z)\mathrm{N}(z') = \mathrm{N}(zz') = 1;$$

como $\mathrm{N}(z)$ y $\mathrm{N}(z')$ son enteros > 0 ((b) y lema 2, a)), necesariamente se sigue que $\mathrm{N}(z) = 1$. Reciprocamente si $z \in \mathbf{H}$ y si $\mathrm{N}(z) = 1$, se tiene $z\overline{z} = \overline{z} \cdot z = \mathrm{N}(z) = 1$ y z es inversible pues $\overline{z} \in \mathbf{H}$ por a). Esto demuestra c).

Demostremos por último d). Dado un cuaternión

$$x = a + bi + cj + dk \in \mathbf{H}(\mathbf{Q}),$$

existe cuatro enteros a',b',c',$d' \in \mathbf{Z}$ tales que

$$|a - a'| \leq \frac{1}{2}, \quad |b - b'| \leq \frac{1}{2}, \quad |c - c'| \leq \frac{1}{2}, \quad |d - d'| \leq \frac{1}{2}.$$

Pongamos $z = a' + b'i + c'j + d'k$. Entonces tenemos

$$\mathrm{N}(x - z) = (a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 \leq 4\frac{1}{4} = 1.$$

De hecho siempre tenemos la desigualdad estricta, a menos que a,b,c,d son todos en $\frac{1}{2} + \mathbf{Z}$. Pero en este caso $x \in \mathbf{H}$. Por lo tanto, para todo cuaternión $z \in \mathbf{H}(\mathbf{Q})$, existe otro cuaternión de Hurwitz $z \in \mathbf{H}$ tal que $\mathrm{N}(x - z) < 1$ (es precisamente para tener la desigualdad estricta que introdujimos los cuaterniones de Hurwitz; aquellos de $\mathbf{H}(\mathbf{Z})$ solamente no alcanzan). Sea ahora $\mathfrak{a}$ un

ideal a izquierda de $\mathbf{H}$. Para mostrar que es principal, podemos suponer que $\mathfrak{a} \neq (0)$. Elijamos, en $\mathfrak{a}$, un elemento no nulo u de norma reducida minimal (uno tal existe, pues las normas son enteros > 0 por b)). Entonces u es inversible en $\mathbf{H}(\mathbf{Q})$ pues su inversa es $\overline{u}\mathrm{N}(u)^{-1}$ (esto muestra de paso que $\mathbf{H}(\mathbf{Q})$ es un cuerpo no conmutativo). Para $y \in \mathfrak{a}$, formemos $yu^{-1} \in \mathbf{H}(\mathbf{Q})$ y tomemos un elemento $z \in \mathbf{H}$ tal que $\mathrm{N}((yu^{-1} - z)u) < \mathrm{N}(u)$. Como $y - zu \in \mathfrak{a}$ y $\mathrm{N}(u)$ es minimal, deducimos que $y - zu = 0$, $y \in \mathbf{H}u$ y $\mathfrak{a} = \mathbf{H}u$. LQQD.

Como el conjunto de las sumas de cuatro cuadrados en $\mathbf{Z}$ es multiplicativamente estable (cf. lema 2), el teorema 1 se reduce a la:

Proposición 1. *Todo número primo p es suma de cuatro cuadrados.*

Como $2 = 1^2 + 1^2 + 0^2 + 0^2$, podemos suponer que p es imar. Como p conmuta con todos los cuaterniones, el ideal a izquierda $\mathbf{H}p$ es bilátero. Luego podemos formar el anillo cociente $\mathbf{H}/\mathbf{H}p$. Como p es impar, todo $z \in \mathbf{H}$ es congruente mod $\mathbf{H}p$ a un elemento de $\mathbf{H}(\mathbf{Z})$ (si las componentes de z son todas en $\frac{1}{2} + \mathbf{Z}$, formamos $z + p \cdot \frac{1}{2}(1 + i + j + k)$); por lo tanto $\mathbf{H}/\mathbf{H}p$ es isomorfo al cociente correspondiente de $\mathbf{H}(\mathbf{Z})$, es decir a $\mathbf{H}(\mathbf{F}_p)$.

Ahora bien, como la forma $a^2 + b^2 + c^2 + d^2$ representa 0 en $\mathbf{F}_p$ (capítulo I, §7, teorema 2; ver más abajo para una demostración directa), $\mathbf{H}(\mathbf{F}_p)$ admite elementos no nulos cuyo norma reducida es nula. Un tal elemento no es inversible (lema 2, b)), por lo tanto general un ideal a izquierda no trivial. Volviendo a $\mathbf{H}$, vemos que $\mathbf{H}p$ está contenido en un ideal a izquierda $\mathbf{H}z$ distinto de $\mathbf{H}$ y de $\mathbf{H}p$. En consecuencia, tenemos $p = z'z$ con z,$z' \in \mathbf{H}$ no inversibles. Entonces $p^2 = \mathrm{N}(p) = \mathrm{N}(z)\mathrm{N}(z')$ y, como $\mathrm{N}(z)$ y $\mathrm{N}(z')$ son enteros > 1 (lema 3, b) y c)), se tiene $\mathrm{N}(z) = \mathrm{N}(z') = p$.

Pongamos $z = a + bi + cj + dk$ (a,b,c,$d \in \mathbf{Z}$ o $\in \frac{1}{2} + \mathbf{Z}$). Si a,b,c,$d \in \mathbf{Z}$, se tiene $p = \mathrm{N}(z) = a^2 + b^2 + c^2 + d^2$ y ganamos. Falta mostrar que, si a,b,c,$d \in \frac{1}{2} + \mathbf{Z}$, podemos reducirnos ?? al caos precedente multiplicando z por un elemento de norma reducida 1 de $\mathbf{H}$, más precisamente por un elemento de la forma $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. En efecto consideremos la clase η de $2z$ en $\mathbf{H}(\mathbf{Z})/4\mathbf{H}(\mathbf{Z}) \simeq \mathbf{H}(\mathbf{Z}/4\mathbf{Z})$. Como $\mathrm{N}(z) \in \mathbf{Z}$, se tiene $\mathrm{N}(2z) \in 4\mathbf{Z}$, de donde $\mathrm{N}(\eta) = 0$ y $\eta\overline{\eta} = 0$. Ahora bien, $\overline{\eta}$ es la clase de un cuaternión z' de la forma $\pm 1 \pm i \pm j \pm k$; entonces $u = \frac{1}{2}z' \in \mathbf{H}$, u es de norma reducida 1 y, como la clase de $(2z) \cdot (2u)$ es nula mod 4, se tiene $zu \in \mathbf{H}(\mathbf{Z})$. Como $p = \mathrm{N}(z) = \mathrm{N}(zu)$, la afirmación queda demostrada. LQQD.

Observación. Aquí, una demostración elemental del hecho de que, sobre un cuerpo finito K, la forma cuadrádtica $a^2 + b^2 + c^2 + d^2$ **representa** 0 (i.e. tiene un zero no trivial en K^4). Tomando $c = 1$, $d = 0$, basta demostrar que la ecuación $a^2 + b^2 = 0$ tiene una solución en K^2. Escribimos la ecuación en

la forma $b^2 + 1 = -a^2$. En característica 2, podemos tomar $b = 0$ y $a = 1$. Sino, si q es el cardinal de K, hay $\frac{q+1}{2}$ cuadrados en K (0 y los $\frac{q-1}{2}$ cuadrados no nulos). Por lo tanto, el conjunto T (resp. T′) de los elementos de K de la forma b^2+1 con $b \in$ K (resp. de la forma $-a^2$ con $a \in$ K) tiene $\frac{q+1}{2}$ elementos por traslación (resp. simetría). Como $\frac{q+1}{2} + \frac{q+1}{2} > q$, se tiene $\mathrm{T} \cap \mathrm{T}' \neq \emptyset$, lo que significa que $b^2 + 1 = -a^2$ tiene un solución LQQD..

CAPÍTULO VI

Extensiones galoisianas de cuerpos de números

1. Teoría de Galois

Esta § es un complemento a la teoría general de cuerpos conmutativos cf. capítulo II, §§3, 4, 6 y 7). Dados un cuerpo L y un conjunto G de automorfismos de L, el conjunto de los $x \in \mathrm{L}$ tales que $\sigma(x) = x$ para todo $\sigma \in \mathrm{G}$ es, como se ve fácilmente, un **subcuerpo** de L, que llamamos el **cuerpo de invariantes** de G. Por otra parte, dada una extensión L de un cuerpo K, el conjunto de K-automorfismos de L es un **grupo** con la composición de funciones.

Teorema 1. *Sea* L *una extensión de grado finito n de un cuerpo* K *finito o de característico cero. Las siguientes condiciones son equivalentes:*

c) K *es el cuerpo de invariantes del grupo* G *de* K*-automorfismos de* L*;*

b) para todo $x \in \mathrm{L}$*, el polinomio minimal de* x *sobre* K *tiene todas sus raíces en* L*;*

c) L *está generado por las raíces de un polinomio sobre* K.

Bajo estas condiciones, el grupo G *de* K*-automorfismos de* L *tiene n elementos.*

Mostremos que *a*) implica *b*). En efecto, si $x \in \mathrm{L}$, el polinomio $\prod_{\sigma \in \mathrm{G}}(\mathrm{X} - \sigma(x))$ es invariante por G (pues todo $\tau \in \mathrm{G}$ permuta los factores entre sí)[1]. Por lo tanto sus coeficientes pertenecen a K. Como el polinomio admite a x como raíz ($1 \in \mathrm{G}$), necesariamente es un múltiplo del polinomio minimal de x sobre K (capítulo II, §3, (4)), de lo que se deduce *b*).

Para ver que *b*) implica *c*), tomamos un elemento primitivo x de L sobre K (capítulo II, §4, cor. del teorema 1). Su polinomio minimal sobre K tiene todas sus raíces en L por *b*) y evidentemente éstas general L sobre K.

Probemos por último que *c*) implica *a*). Por hipótesis L está generado sobre K por un número finito de elementos $(x^{(1)}, \ldots, x^{(q)})$ y por sus conjugados

[1] La finitud de G resulta del capítulo II, §4, teorema 1.

$(x_j^{(i)})$ (capítulo II, §4). Entonces todo K-isomorfismo σ de L en una extensión de L envía a cada uno de estos generadores a otro de estos generadores. Por lo tanto se tiene que $\sigma(\mathrm{L}) \subset \mathrm{L}$, de donde $\sigma(\mathrm{L}) = \mathrm{L}$ por álgebra lineal, ya que σ es una aplicación K-lineal inyectiva. Es decir, σ es un K-**automorfismo** de L.

En este caso el grupo G de K-automorfismos de L tiene n elementos (capítulo II, §4, teorema 1 y el corolario). Sea entonces $x \in \mathrm{L}$ invariante por G, de manera que todo $\sigma \in \mathrm{G}$ es un $\mathrm{K}[x]$-automorfismo de L. Como (capítulo II, §4) hay exactamente $[\mathrm{L} : \mathrm{K}[x]]$ $\mathrm{K}[x]$-isomorfismos de L en una extensión de L, se tiene por lo tanto $n \leq [\mathrm{L} : \mathrm{K}[x]]$, de donde $n = [\mathrm{L} : \mathrm{K}[x]]$, $\mathrm{K}[x] = \mathrm{K}$ y $x \in \mathrm{K}$. Esto demuestra *a*). La igualdad $\mathrm{card}(\mathrm{G}) = n$ fue demostrada por el camino. LQQD.

Definición 1. *Si las condiciones del teorema 1 se satisfacen, decimos que* L *es una extensión galoisiana de* K *y que* G *es el grupo de Galois de* L *sobre* K. *Si* G *es abeliano (resp. cíclico) decimos que* L *es una extensión abeliana (resp. cíclica) de* K.

Corolario del teorema 1. *Sea* K *un cuerpo finito o de característica cero,* L *una extensión de* K *de grado finito n y* H *un grupo de automorfismos de* L *que tiene a* K *por su grupo de invariantes. Entonces* L *es una extensión galoisiana de* K *y* H *es su grupo de Galois.*

En efecto, si $x \in \mathrm{L}$, el polinomio $\prod_{\sigma \in \mathrm{H}}(\mathrm{X} - \sigma(x))$ es invariante por H y por lo tanto sus coeficientes están en K. Así, por el teorema 1, *b*), L es una extensión galoisiana de K. Si G denota su grupo de Galois, se tiene $\mathrm{H} \subset \mathrm{G}$ y $\mathrm{card}(\mathrm{G}) = n$ (teorema 1). Tomemos entonces un elemento primitivo x de L sobre K (capítulo II, §4, corolario del teorema 1) y consideremos el polinomio

$$\mathrm{P}(\mathrm{X}) = \prod_{\sigma \in \mathrm{H}} (\mathrm{X} - \sigma(x)).$$

Como más arriba, este polinomio tiene todos sus coeficientes en K y es múltiplo del polinomio minimal de x sobre K, de donde $n \leq d^\circ(\mathrm{P})$. Como

$$d^\circ(\mathrm{P}) = \mathrm{card}(\mathrm{H}) \leq \mathrm{card}(\mathrm{G}) = n,$$

deducimos que $\mathrm{H} = \mathrm{G}$. LQQD.

Teorema 2. *Sea* K *un cuerpo finito o de característica cero,* L *una extensión galoisiana de* K *y* G *su grupo de Galois. A todo subgrupo* G' *de* G *le asociamos el cuerpo de invariantes* $k(\mathrm{G}')$ *de* G' *y a todo subcuerpo* K' *de* L *que contiene a* K *le asociamos el subgrupo* $g(\mathrm{K}') \subset \mathrm{G}$ *de los* K'*-automorfismos de* L.

a) *Las funciones g y k son biyecciones inversas una de la otra, decrecientes para la relación de inclusión. Más aún,* L *es una extensión galoisiana de todo cuerpo intermedio* K' *(i.e.* $\mathrm{K} \subset \mathrm{K}' \subset \mathrm{L}$*).*
b) *Para que un cuerpo intermedio* K' *sea una extensión galoisiana de* K *es necesario y suficiente que* $g(\mathrm{K}')$ *sea un subgrupo normal de* G*. Entonces el grupo de Galois de* K' *sobre* K *se identifica con el grupo cociente* $\mathrm{G}/g(\mathrm{K}')$*.*

En efecto, para todo cuerpo intermedio K' y todo $x \in \mathrm{L}$, el polinomio minimal de x sobre K' divide al polinomio minimal de x sobre K. Por lo tanto tiene todas sus raíces en L por el teorema 1, *b*), de manera que L es una extensión **galoisiana** de K' por el teorema 1, *b*) nuevamente. Entonces, K' es el cuerpo de invariantes del grupo $g(\mathrm{K}')$ de los K'-automorfismos de L (teorema 1, *a*)). Es decir, $k(g(\mathrm{K}')) = \mathrm{K}'$. Sea ahora G' un subgrupo de G. Entonces G' es el grupo de Galois de L sobre $k(\mathrm{G}')$ (cor. del teorema 1). Es decir, $\mathrm{G}' = g(k(\mathrm{G}'))$. Las fórmulas $k(g(\mathrm{K}')) = \mathrm{K}'$ y $g(k(\mathrm{G}')) = \mathrm{G}'$ muestran que k y g son biyecciones inversas una de la otra. Que son decrecientes es evidente. Esto demuestra *a*).

Probemos ahora *b*). Sea K' un cuerpo intermedio ($\mathrm{K} \subset \mathrm{K}' \subset \mathrm{L}$). Si $x \in \mathrm{K}'$, las raíces del polinomio minimal de x sobre K son las $\sigma(x)$ ($x \in \mathrm{G}$). Se sigue del teorema 1, *b*), que para que K' sea una extensión galoisiana de K es necesario y suficiente que $\sigma(x) \in \mathrm{K}'$ para todo $x \in \mathrm{K}'$ y $\sigma \in \mathrm{G}$, es decir que $\sigma(\mathrm{K}') \subset \mathrm{K}'$ para todo $\sigma \in \mathrm{G}$. Ahora bien, si $\sigma(\mathrm{K}') \subset \mathrm{K}'$, $\tau \in g(\mathrm{K}')$ y si $x \in \mathrm{K}'$, se tiene $\sigma^{-1}\tau\sigma(x) = x$, de donde $\sigma^{-1}\tau\sigma \in g(\mathrm{K}')$. En otras palabras, "$\mathrm{K}'$ galoisiana sobre K" implica "$g(\mathrm{K}')$ normal en G". Reciprocamente, supongamos que $g(\mathrm{K}')$ es normal en G. Si $x \in \mathrm{K}'$, $\sigma \in \mathrm{G}$ y si $\tau \in g(\mathrm{K}')$, se tiene $\tau\sigma(x) = \sigma \cdot \sigma^{-1}\tau\sigma(x) = \sigma(x)$ pues $\sigma^{-1}\tau\sigma \in g(\mathrm{K}')$, de manera que $\sigma(x) \in \mathrm{K}'$. En consecuencia, "$g(\mathrm{K}')$ es normal en G" implica "$\sigma(\mathrm{K}') \subset \mathrm{K}'$" y por lo tanto que K' es galoisiana sobre K.

Por último, calculemos el grupo de Galois de K' sobre K en este caso. Como se tiene $\sigma(\mathrm{K}') \subset \mathrm{K}'$ para todo $\sigma \in \mathrm{G}$ (e incluso $\sigma(\mathrm{K}') = \mathrm{K}'$ por álgebra lineal), la restricción $\sigma \mid \mathrm{K}'$ de σ a K' es un K-automorfismo de K'. Por lo tanto, se tiene un "homomorfismo de restricción" $\sigma \mapsto \sigma \mid \mathrm{K}'$ de G en el grupo de Galois H de K' sobre K. Su núcleo es evidentemente $g(\mathrm{K}')$. Como se tiene

$$\begin{aligned}\operatorname{card}(\mathrm{H}) = [\mathrm{K}' : \mathrm{K}] &= [\mathrm{L} : \mathrm{K}][\mathrm{L} : \mathrm{K}']^{-1} = \operatorname{card}(\mathrm{G}) \cdot \operatorname{card}(g(\mathrm{K}'))^{-1} \\ &= \operatorname{card}(\mathrm{G}/g(\mathrm{K}')),\end{aligned}$$

este homomorfismo es sobreyectivo y por eso $\mathrm{H} \simeq \mathrm{G}/g(\mathrm{K}')$. LQQD.

Ejemplo 1 (Extensiones cuadráticas). Sea K un cuerpo de característica cero y L una extensión cuadrática (i.e. de grado 2) de K. Como en el principio de §5, capítulo II vemos que L es de la forma $K[x]$, donde x es raíz de un polinomio $X^2 - d$ ($d \in K$, d no es un cuadrado en K). Como la otra raíz de este polinomio es $-x$, L admite un K-automorfismo no trivial σ definido por $\sigma(x) = -x$, i.e.

$$\sigma(a + bx) = a - bx \quad (a,b \in K).$$

Tenemos $\sigma^2 = 1$ y K es el cuerpo de invariantes de σ. Por lo tanto L es una extensión **galoisiana** de K con el grupo **cíclico** $\{1,\sigma\}$ como grupo de Galois (teorema 1 y el corolario del teorema 1).

Ejemplo 2 (Extensiones ciclotómicas). Sea K un cuerpo de característica cero, z una raíz primitiva n-ésima de la unidad en una extensión de K y $L = K(z)$. Decimos que L es una extensión **ciclotómica** de K. El polinomio minimal $F(X)$ de z sobre K divide a $X^n - 1$ (capítulo II, §3, (4)) y por lo tanto sus raíces son raíces n-ésimas de la unidad y por lo tanto potencias de z (capítulo I, §6). Así, L es una extensión **galoisiana** de K por el teorema 1, *c*).

Sea G el grupo de Galois. Todo $\sigma \in G$ está determinado por $\sigma(z)$, que es una potencia $z^{j(\sigma)}$ de z, donde $j(\sigma)$ está bien definido sólo mod n. Si $\sigma,\tau \in G$, se tiene $\sigma\tau(z) = \sigma(z^{j(\tau)}) = \sigma(z)^{j(\tau)} = z^{j(\sigma)j(\tau)}$, de donde

$$j(\sigma\tau) \equiv j(\sigma)j(\tau)$$

(mod n). En otras palabras, podemos considerar $\sigma \mapsto j(\sigma)$ como un **homomorfismo** $G \to (\mathbf{Z}/n\mathbf{Z})^*$. Como $j(\sigma)$ determina a σ unívocamente, este homomorfismo es **inyectivo** y G es abaliano. Así **toda extensión ciclotómica es abeliana.** Si n es primo, esta extensión es incluso **cíclica,** pues G es isomorfo a un subgrupo de $(\mathbf{Z}/n\mathbf{Z})^* = \mathbf{F}_n^*$ (capítulo I, §7, teorema 1, *b*)).

> *Como todo subgrupo de un grupo abeliano es normal, todo cuerpo intermedio* K′ *de una extensión ciclotómica* L *de* K *es una extensión galoisiana (e incluso abeliana) de* K *(teorema 2, b)). En particular, todo subcuerpo de un cuerpo ciclotómica es una extensión abeliana de* **Q**. *Reciprocamente, se puede demostrar (teorema de Kronecker-Weber) que toda extensión abeliana de* **Q** *es un subcuerpo de un cuerpo ciclotómico.*

Observemos que, con la misma notación que antes, el automorfismo σ **eleva todas las raíces n-ésimas de la unidad a la potencia $j(\sigma)$,** pues

todas ellas son potencias de z. Luego, $\sigma \mapsto j(\sigma)$ es independiente de la elección de z.

Ejemplo 3 (Cuerpos finitos). Sea $\mathbf{F}_q$ un cuerpo **finito** ($q = p^s$ con p primo). Toda extensión de grado finito de $\mathbf{F}_q$ es de la forma $\mathbf{F}_{q^n}$; su grado es n (capítulo I, §7). Sabemos que $\sigma : x \mapsto x^q$ es un automorfismo de $\mathbf{F}_{q^n}$ (*ibid.*, proposición 1) y que $\mathbf{F}_q$ es su cuerpo de invariantes (*ibid.*, teorema 1, *c*)). Para todo $x \in \mathbf{F}_{q^n}$, se tiene $\sigma^j(x) = x^{q^j}$, de donde $\sigma^n = 1$ pues $\mathbf{F}^{q^n}$ es el conjunto de los x tales que $x^{q^n} = x$ (*ibid.*, teorema 1, *c*)). Por otra parte, para $1 \leq j \leq n-1$, se tiene $\sigma^j \neq 1$ pues $\mathbf{F}_{q^j} \neq \mathbf{F}_{q^n}$. Por lo tanto, $\{1,\sigma,\ldots,\sigma^{n-1}\}$ es un grupo cíclico de orden n. Así, por el corolario del teorema 1, $\mathbf{F}_{q^n}$ **es una extensión cíclica de grado** n **de** $\mathbf{F}_q$ **y su grupo de Galois tiene un generador distinguido, a saber** $x \mapsto x^q$**, que llamamos automorfismo de Frobenius.**

2. Grupo de descomposición y grupo de inercia

En esta §, A *denota un anillo de Dedekind,* K *su cuerpo de fracciones que suponemos de característica cero,* K′ *una extensión galoisiana de* K, *n su grado,* G *su grupo de Galois y* A′ *la clausura íntegra de* A *en* K′.

Aplicando $\sigma \in \mathrm{G}$ a una ecuación de dependencia entera (sobre A) de un elemento $x \in \mathrm{A}'$, vemos que $\sigma(x) \in \mathrm{A}'$. Por lo tanto:

(1) A' *es estable por* G, *i.e.* $\sigma(\mathrm{A}') = \mathrm{A}'$ *para todo* $\sigma \in \mathrm{G}$.

De hecho nosotros sólamente hemos demostrado que $\sigma(\mathrm{A}') \subset \mathrm{A}'$, *pero entonces también tenemos* $\sigma^{-1}(\mathrm{A}') \subset \mathrm{A}'$, *de donde* $\mathrm{A}' = \sigma\sigma^{-1}(\mathrm{A}') \subset \sigma(\mathrm{A}')$. *Nosotros omitiremos en general en lo que sigue este sencillo razonamiento adicional.*

Por otra parte, si $\mathfrak{p}$ es un ideal maximal de A y $\mathfrak{p}'$ es un ideal maximal de A′ tal que $\mathfrak{p}' \cap \mathrm{A} = \mathfrak{p}$ (es decir que figura en la descomposición de $\mathrm{A}'\mathfrak{p}$ en ideal primos; cf capítulo V, §2, proposición 1), se tiene evidentemente $\sigma(\mathfrak{p}') \cap \mathrm{A} = \mathfrak{p}$ y $\sigma(\mathfrak{p}')$ figura en la descomposición de $\mathrm{A}'\mathfrak{p}$ con el **mismo** exponente que $\mathfrak{p}'$. Diremos que $\mathfrak{p}'$ y $\sigma(\mathfrak{p}')$ son ideales primos **conjugados** de A′. Ahora demostraremos que no hay otros primos en la descomposición de $\mathrm{A}'\mathfrak{p}$:

Proposición 1. *Sea* $\mathfrak{p}$ *es un ideal maximal de* A. *Los ideales maximales* $\mathfrak{p}'_i$ *de* A′ *que figuran en la descomposición de* $\mathrm{A}'\mathfrak{p}$ *(i.e. tales que* $\mathfrak{p}'_i \cap \mathrm{A} = \mathfrak{p}$*) son*

conjugados dos a dos y tiene el mismo grado residual f y el mismo índice de ramificación e, de manera que $\mathrm{A}'\mathfrak{p} = (\prod_{i=1}^{g} \mathfrak{p}_i')^e$ *y* $n = efg$.

La afirmación sobre el índice de ramificación y el grado residual son evidentes, pues el automorfismo σ preserva **todas** las relaciones algebraicas. La fórmula $n = efg$ es entonces un caso particular de $\sum e_i f_i = n$ (capítulo V, §2, teorema 1). Sea ahora $\mathfrak{p}'$ uno de los $\mathfrak{p}_i'$ y supongamos que otro de los $\mathfrak{p}_i'$, que notaremos $\mathfrak{q}'$, no es conjugado con $\mathfrak{p}'$. Como $\mathfrak{q}'$ y $\sigma(\mathfrak{p}')$ ($\sigma \in \mathrm{G}$) son maximales y distintos, se tiene $\sigma(\mathfrak{p}') \not\subset \mathfrak{q}'$. Tenemos el siguiente lema

Lema 1 (lema de ????? prima)**.** *Sea* R *un anillo,* $\mathfrak{p}_1, \ldots, \mathfrak{p}_q$ *una familia finita de ideales primos de* R *y* $\mathfrak{b}$ *un ideal de* R *tal que* $\mathfrak{b} \not\subset \mathfrak{p}_i$ *para todo* i*. Entonces existe* $b \in \mathfrak{b}$ *tal que* $b \notin \mathfrak{p}_i$ *para todo* i*.*

En efecto, suprimiendo los $\mathfrak{p}_i$ no maximales de $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_q\}$, podemos suponer que se tiene que $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ si $i \neq j$. Sea entonces $x_{ij} \in \mathfrak{p}_j$ tal que $x_{ij} \notin \mathfrak{p}_i$. Por otra parte, como $\mathfrak{b} \not\subset \mathfrak{p}_i$, existe $a_i \in \mathfrak{b}$ tal que $a_i \notin \mathfrak{p}_i$. Sea entonces $b_i = a_i \prod_{j \neq i} x_{ij}$. Se tiene $b_i \in \mathfrak{b}$, $b_i \in \mathfrak{p}_j$ si $j \neq i$ y $b_i \notin \mathfrak{p}_i$ pues $\mathfrak{p}_i$ es primo. Entonces $b = b_1 + \cdots + b_q$ satisface la conclusión deseada, pues $b \in \mathfrak{b}$ y, para todo i, se tiene $\sum_{j \neq i} b_j \in \mathfrak{p}_i$, $b_i \notin \mathfrak{p}_i$. LQQD.

Luego, el lema muestra que existe un elemento $x \in \mathfrak{q}'$ tal que $x \notin \sigma(\mathfrak{p}')$ para todo $\sigma \in \mathrm{G}$. Consderemos entonces $\mathrm{N}(x) = \prod_{\tau \in \mathrm{G}} \tau(x)$ (capítulo II, §6, proposición 1). Como $\tau(x) \in \mathrm{A}'$ para todo $\tau \in \mathrm{G}$ (por (1)), tenemos $\mathrm{N}(x) \in \mathfrak{q}'$, de donde

$$\mathrm{N}(x) \in \mathfrak{q}' \cap \mathrm{A} = \mathfrak{p}.$$

Por otra parte, se tiene $x \notin \tau^{-1}(\mathfrak{p}')$, de donde $\tau(x) \notin \mathfrak{p}'$ para todo $\tau \in \mathrm{G}$. Como $\mathfrak{p}'$ es primo, deducimos que $\mathrm{N}(x) \notin \mathfrak{p}'$, lo que contradice $\mathrm{N}(x) \in \mathfrak{p}$. LQQD.

Sea ahora $\mathfrak{p}'$ uno de los ideales maximales de A' tales que $\mathfrak{p}' \cap \mathrm{A} = \mathfrak{p}$. Los $\sigma \in \mathrm{G}$ tal que $\sigma(\mathfrak{p}') = \mathfrak{p}'$ forman un subgrupo D de G, que llamamos **grupo de descomposición de** $\mathfrak{p}'$**.** Si g es el número de conjugados de $\mathfrak{p}'$ tenemos por lo tanto

$$g = \mathrm{card}(\mathrm{G}) \cdot \mathrm{card}(\mathrm{D})^{-1} \quad \text{donde} \quad \mathrm{card}(\mathrm{D}) = n/g = ef. \tag{2}$$

Si $\sigma \in \mathrm{D}$, la relación $\sigma(\mathrm{A}') = \mathrm{A}'$ y $\sigma(\mathfrak{p}') = \mathfrak{p}'$ muestra que σ define, pasando al cociente, un automorfismo $\overline{\sigma}$ de $\mathrm{A}'/\mathfrak{p}'$ (en efecto, $x \equiv y \pmod{\mathfrak{p}'}$ implica $\sigma(x) \equiv \sigma(y) \pmod{\mathfrak{p}'}$). Es claro que $\overline{\sigma}$ es un $(\mathrm{A}/\mathfrak{p})$-automorfismo. LA aplicación $\sigma \mapsto \overline{\sigma}$ es un **homomorfismo** de grupos, cuyo **núcleo** es el conjunto I de los $\sigma \in \mathrm{D}$ tales que $\sigma(x) - x \in \mathfrak{p}'$ para todo $x \in \mathrm{A}'$. Por lo tanto, I es un subgrupo **normal** de D, que llamamos **subgrupo de inercia** de $\mathfrak{p}'$.

Proposición 2. *Con la misma notación que antes, supongamos que* $\mathrm{A}/\mathfrak{p}$ *es finito o de característica cero. Entonces* $\mathrm{A}'/\mathfrak{p}'$ *es una extensión galoisiana de grado* f *de* $\mathrm{A}/\mathfrak{p}$ *y* $\sigma \mapsto \overline{\sigma}$ *es un homomorfismo sobreyectivo de* D *sobre su grupo de Galois. Además,* $\mathrm{card}(\mathrm{I}) = e$.

En efecto, sea $\mathrm{K_D}$ el cuerpo de invariantes de D, $\mathrm{A_D} = \mathrm{A}' \cap \mathrm{K_D}$ la clausura íntegral de A en $\mathrm{K_D}$ y $\mathfrak{p}_\mathrm{D}$ el ideal primo $\mathfrak{p}' \cap \mathrm{A_D}$. Por la proposición 1 y la definición de D, $\mathfrak{p}'$ es el único factor primo de $\mathrm{A}'\mathfrak{p}_\mathrm{D}$. Escribamos $\mathrm{A}'\mathfrak{p}_\mathrm{D} = \mathfrak{p}'^e$ y notemos f' el grado residual $[\mathrm{A}'/\mathfrak{p}' : \mathrm{A_D}/\mathfrak{p}_\mathrm{D}]$. Por el teorema 1 de §2, capítulo V, el teorema 1 de §1 y (2), tenemos

$$e'f' = [\mathrm{K}' : \mathrm{K_D}] = \mathrm{card}(\mathrm{D}) = ef.$$

Como $\mathrm{A}/\mathfrak{p} \subset \mathrm{A_D}/\mathfrak{p}_\mathrm{D} \subset \mathrm{A}'/\mathfrak{p}'$, se tiene $f' \leq f$. Como $\mathfrak{p}\mathrm{A_D} \subset \mathfrak{p}_\mathrm{D}$, se tiene $e' \leq e$. Junto a $e'f' = ef$, esto muestra que $e = e'$ y $f = f'$, de donde:

$$\mathrm{A}/\mathfrak{p} \simeq \mathrm{A_D}/\mathfrak{p}_\mathrm{D}. \tag{3}$$

Sea ahora $\overline{x}$ un elemento primitivo de $\mathrm{A}'/\mathfrak{p}'$ sobre $\mathrm{A}/\mathfrak{p}$ y sea $x \in \mathrm{A}'$ un representante de $\overline{x}$. Sea $\mathrm{X}^r + a_{r-1}\mathrm{X}^{r-1} + \cdots + a_0$ el polinomio minimal de x **sobre** $\mathrm{K_D}$; se tiene $a_i \in \mathrm{A_D}$ (capítulo II, §6, corolario de la proposición 2). El conjunto de sus raíces consiste en los $\sigma(x)$ con $\sigma \in \mathrm{D}$. El polinomio "reducido" $\mathrm{X}^r + \overline{a}_{r-1}\mathrm{X}^{r-1} + \cdots + \overline{a}_0$ tiene sus coeficientes en $\mathrm{A}/\mathfrak{p}$ (por (3)) y el conjunto de raíces consiste en los $\overline{\sigma}(\overline{x})$ con $\sigma \in \mathrm{D}$. Resulta primero que nada que $\mathrm{A}'/\mathfrak{p}'$ contiene a todos los conjugados de $\overline{x}$ sobre $\mathrm{A}/\mathfrak{p}$ y $\mathrm{A}'/\mathfrak{p}'$ es por lo tanto una extensión **galoisiana** de $\mathrm{A}/\mathfrak{p}$ (§1, teorema 1, *c*)). Resulta por otra parte que, como todo conjugado $\overline{x}$ sobre $\mathrm{A}/\mathfrak{p}$ es un $\overline{\sigma}(\overline{x})$ que todo $(\mathrm{A}/\mathfrak{p})$-automorfismo de $\mathrm{A}'/\mathfrak{p}'$ es un $\overline{\sigma}$. Así el grupo de Galois de $\mathrm{A}'/\mathfrak{p}'$ sobre $\mathrm{A}/\mathfrak{p}$ se identifica a D/I. Como tiene orden $[\mathrm{A}'/\mathfrak{p}' : \mathrm{A}/\mathfrak{p}] = f$, tenemos que $\mathrm{card}(\mathrm{D})/\mathrm{card}(\mathrm{I}) = f$, de donde $\mathrm{card}(\mathrm{I}) = e$ por (2). LQQD.

Corolario. *Para que* $\mathfrak{p}$ *no ramifique en* A' *es necesario y suficiente que el grupo de inercia* I *consista únicamente de la identidad.*

Observación. Si notamos $\mathrm{D}_{\mathfrak{p}'}$ y $\mathrm{I}_{\mathfrak{p}'}$ los grupos de descomposición e inercia del ideal maximal $\mathfrak{p}'$, aquellos de su **conjugado** $\sigma(\mathfrak{p}')$ ($\sigma \in \mathrm{G}$) son

$$\mathrm{D}_{\sigma(\mathfrak{p}')} = \sigma\mathrm{D}_{\mathfrak{p}'}\sigma^{-1}, \quad \mathrm{I}_{\sigma(\mathfrak{p}')} = \sigma\mathrm{I}_{\mathfrak{p}'}\sigma^{-1} \tag{4}$$

En efecto, si $\tau \in \mathrm{D}_{\mathfrak{p}'}$, se tiene $\sigma\tau\sigma^{-1} \cdot \sigma(\mathfrak{p}') = \sigma\tau(\mathfrak{p}') = \sigma(\mathfrak{p}')$, de donde $\sigma\mathrm{D}_{\mathfrak{p}'}\sigma^{-1} \subset \mathrm{D}_{\sigma(\mathfrak{p}')}$. Aplicando esto a σ^{-1} se obtiene la inclusión inversa. De la misma manera, si $\tau \in \mathrm{I}_{\mathfrak{p}'}$ y $x \in \mathrm{A}'$, se tiene

$$\sigma\tau\sigma^{-1}(x) - x = \sigma\tau(\sigma^{-1}(x)) - \sigma\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x)) - \sigma^{-1}(\sigma(x)) \in \sigma(\mathfrak{p}'),$$

de donde $\sigma \mathrm{I}_{\mathfrak{p}'} \sigma^{-1} \subset \mathrm{I}_{\sigma(\mathfrak{p}')}$ y de hecho se tiene una igualdad aplicando σ^{-1} a $\sigma(\mathfrak{p}')$.

Cuando K' es una extensión **abeliana** de K, los grupos $\mathrm{D}_{\sigma(\mathfrak{p}')}$ (resp. $\mathrm{I}_{\sigma(\mathfrak{p}')}$) ($\sigma \in \mathrm{G}$) son por lo tanto todos **iguales,** y no dependen del ideal $\mathfrak{p}$ del anillo de abajo. ????

3. Caso de un cuerpo de números. El automorfismo de Frobenius

Lo anterior se aplica a los cuerpos de números y sus anillos de enteros. En efecto, estos cuerpos son de característica cero y los cuerpos residuales de estos anillos son finitos.

Conservamos la notación de arriba ($\mathrm{K} \subset \mathrm{K}'$ cuerpos de números, K' galoisiana sobre K, grupo G, anillos A y A'). Sea $\mathfrak{p}$ un ideal maximal de A que **no ramifica** en A' y sea $\mathfrak{p}'$ un factor primo de $\mathrm{A}'\mathfrak{p}$. Entonces el grupo de inercia de $\mathfrak{p}'$ se reduce a la identidad (§2, corolario de la proposición 2) y su grupo de descomposición D es por lo tanto canónicamente isomorfo al grupo de Galois de $\mathrm{A}'/\mathfrak{p}'$ sobre $\mathrm{A}/\mathfrak{p}$ (§2, proposición 2). Pero este último es cíclico, con un generador distinguido $\overline{\sigma} : \overline{x} \mapsto \overline{x}^q$, donde $q = \mathrm{card}(\mathrm{A}/\mathfrak{p})$ (§1, ejemplo 3). Por lo tanto D también es **cíclico,** con un generador distinguido σ tal que $\sigma(x) \equiv x^q \pmod{\mathfrak{p}'}$ para todo $x \in \mathrm{A}'$. Este generador se llama **automorfismo de Frobenius** de $\mathfrak{p}$ y generalmente lo notamos $(\mathfrak{p}',\mathrm{K}'/\mathrm{K})$.

Si $\tau \in \mathrm{G}$ tenemos, como en la observación al final de §2, que

$$(\tau(\mathfrak{p}'),\mathrm{K}'/\mathrm{L}) = \tau \cdot (\mathfrak{p}',\mathrm{K}'/\mathrm{K}) \cdot \tau^{-1}. \tag{1}$$

En particular, si K' es una extensión **abeliana,** $(\mathfrak{p}',\mathrm{K}'/\mathrm{K})$ depende únicamente del ideal $\mathfrak{p}$ de A. Entonces a veces lo notamos $\left(\frac{\mathrm{K}'/\mathrm{L}}{\mathfrak{p}}\right)$.

Proposición 1. *Con las notaciones precedentes, sea* F *un cuerpo intermedio* ($\mathrm{K} \subset \mathrm{F} \subset \mathrm{K}'$). *Notemos* f *el grado residual de* $\mathfrak{p}' \cap \mathrm{F}$ *sobre* K. *Entonces*

1. *se tiene* $(\mathfrak{p}',\mathrm{K}'/\mathrm{F}) = (\mathfrak{p}',\mathrm{K}'/\mathrm{K})^f$
2. *si* F *es galoisiana sobre* K, *la restricción de* $(\mathfrak{p}',\mathrm{K}'/\mathrm{K})$ *a* F *es igual a* $(\mathfrak{p}' \cap \mathrm{F},\mathrm{F}/\mathrm{K})$.

En efecto, pongamos $\sigma = (\mathfrak{p}',\mathrm{K}'/\mathrm{K})$. Por definición, tenemos $\sigma(\mathfrak{p}') = \mathfrak{p}'$ y $\sigma(x) \equiv x^q \pmod{\mathfrak{p}'}$ para todo $x \in \mathrm{A}'$ (aquí, $q = \mathrm{card}(\mathrm{A}/\mathfrak{p})$). Tenemos por lo tanto

$$\sigma^f(\mathfrak{p}') = \mathfrak{p}' \quad \text{y} \quad \sigma^f(x) \equiv x^{q^f}$$

$\pmod{\mathfrak{p}'}$ para todo $x \in \mathrm{A}'$. Por definición de f, q^f es el cardinal del cuerpo residual $(\mathrm{A}' \cap \mathrm{F})/(\mathfrak{p}' \cap \mathrm{F})$. Además, el grupo de descomposicón de $\mathfrak{p}'$ sobre F

es evidentemnete un subgrupo del grupo de descomposicón D de $\mathfrak{p}'$ sobre K y tiene orden

$$[\mathrm{A}'/\mathfrak{p}' : (\mathrm{A}' \cap \mathrm{F})/(\mathfrak{p}' \cap \mathrm{F})] = f^{-1}[\mathrm{A}'/\mathfrak{p}' : \mathrm{A}/\mathfrak{p}] = f^{-1} \cdot \mathrm{card}(\mathrm{D})$$

por (2) de §2. Como D es cíclico y generado por σ, su único subgrupo de orden $f^{-1} \cdot \mathrm{card}(\mathrm{D})$ está generado por σ^f. Esto demuestra *a*).

Supongamos ahora que F es galoisiana sobre K y notemos σ' la restricción de σ a F (§1, teorema 1, *b*)). Como $\sigma'(\mathfrak{p}') = \mathfrak{p}'$, se tiene $\sigma'(\mathfrak{p}' \cap \mathrm{F}) = \mathfrak{p}' \cap \mathrm{F}$ y σ' pertenece al grupo de descomposición de $\mathfrak{p}' \cap \mathrm{F}$ sobre K. Además evidentemente se tiene $\sigma'(x) \equiv x^q$ para todo $x \in \mathrm{A}' \cap \mathrm{F}$, con $q = \mathrm{card}(\mathrm{A}/\mathfrak{p})$. Esto demuestra *b*).

4. Aplicación a los cuerpos ciclotómicos

Ahora utilizaremos lo anterior para demostrar un resultado que generaliza la irreducibilidad del polinomio ciclotómico y para dar una tercera demostración (cf. capítulo II, §9, teorema 1 y capítulo V, §2, ex.) de este hecho.

Teorema 1. *Sea z una raíz primitiva n-ésima de la unidad en $\mathbf{C}$. Entonces*

1. *Ningún número primo p que no divide a n ramifica en $\mathbf{Q}[z]$;*
2. *$\mathbf{Q}[z]$ es una extensión abeliana de $\mathbf{Q}$ de grado $\varphi(n)$ y de grupo de Galois isomorfo a $(\mathbf{Z}/n\mathbf{Z})^*$.*

En efecto, sea F(X) el polinomio minimal de z sobre $\mathbf{Q}$ y d su grado (tenemos $d = [\mathbf{Q}[z] : \mathbf{Q}]$). El polinomio F(X) es un divisor de $\mathrm{X}^n - 1$, digamos $\mathrm{X}^n - 1 = \mathrm{F(X)G(X)}$. Tenemos $\mathrm{D}(1,z,\ldots,z^{d-1}) = \mathrm{N}(\mathrm{F}'(z))$ (capítulo II, §7, (6)). De $n\mathrm{X}^{n-1} = \mathrm{F}'(\mathrm{X})\mathrm{G}(\mathrm{X}) + \mathrm{F}(\mathrm{X})\mathrm{G}'(\mathrm{X})$, deducimos que $nz^{n-1} = \mathrm{F}'(z)\mathrm{G}(z)$. Como z es una unidad de $\mathbf{Q}[z]$ y por lo tanto tiene norma ± 1, se deduce, tomando norma, que $\mathrm{N}(\mathrm{F}'(z))$ divide a n^d. Por último, como z es un entero de $\mathbf{Q}[z]$, el discriminante absoluto de $\mathbf{Q}[z]$ divide a $\mathrm{D}(1,z,\ldots,z^{d-1})$ y por lo tanto a n^d. Así, por el capítulo V, §3, teorema 1, ningún primo p que no divida a n ramifica en $\mathbf{Q}[z]$. Esto demuestra *a*).

Para *b*) recordemos (§1, ejemplo 2) que $\mathbf{Q}[z]$ es una extensión abeliana de $\mathbf{Q}$ y que se tiene un homomorfismo inyectivo j del grupo de Galois G de $\mathbf{Q}[z]$ sobre $\mathbf{Q}$ en $(\mathbf{Z}/n\mathbf{Z})^*$. Más precisamente el elemento $\sigma \in \mathrm{G}$ eleva todas las raíces n-ésimas de la unidad a la potencia $j(\sigma)$. Sea entonces p un número primo que no divide a n. Por *a*), el automorfismo de Frobenius $\left(\frac{\mathbf{Q}[z]/\mathbf{Q}}{p}\right)$ está definido; notémoslo σ_p. Escribiendo A por el anillo de enteros de $\mathbf{Q}[z]$ y $\mathfrak{p}$ por un factor primo cualquiera de Ap, tenemos por definición que $\sigma_p(x) \equiv x^p \bmod \mathfrak{p}$ para todo $x \in \mathrm{A}$. En particular, poniendo $j = j(\sigma_p)$,

tenemos $z^j \equiv z^p \bmod \mathfrak{p}$. Ahora bien, también tenemos

$$\prod_{\substack{0\le r\le n-1\\ r\not\equiv p \pmod n}} (z^p - z^r) = \mathrm{P}'(z^p) = nz^{p(n-1)},$$

donde $\mathrm{P}(\mathrm{X}) = \mathrm{X}^n - 1 = \prod_{0\le r\le n-1}(\mathrm{X} - z^r)$. Como n es coprimo con p, $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ y z es inversible, deducimos que

$$\prod_{\substack{0\le r\le n-1\\ r\not\equiv p \pmod n}} (z^p - z^r) \notin \mathfrak{p}.$$

La relación $z^j \equiv z^p \pmod{\mathfrak{p}}$ implica por lo tanto que j es la clase de p mod n. Así $j(\mathrm{G})$ contiene las clases mod n de todos los números rimos p que no dividen a n y por lo tanto, por multiplicatividad, las clases de todos los enteros coprimos con n. En otras palabras $j(\mathrm{G}) = (\mathbf{Z}/n\mathbf{Z})^*$ y esto demuestra b).

5. Otra demostración de la ley de reciprocidad cuadrática

Sea q un número primo **impar** y K el cuerpo ciclotómico generado por una raíz primitiva q-ésima de la unidad en $\mathbf{C}$. El grupo de Galois G de K sobre $\mathbf{Q}$ es isomorfo a $\mathbf{F}_q^*$ (§4, teorema 1, b)) y por lo tanto es **cíclico** de orden par $q-1$. Por lo tanto admite un único subgrupo H de índice 2, que corresponde al subgrupo de los cuadrados $(\mathbf{F}_q^*)^2$. Así K contiene un único subcuerpo **cuadrático** F (§1, teorema 2, b)). Ningún número primo $p \neq q$ se ramifica en F pues, sino, se ramificaría en K, lo que contradice el teorema 1, a) de §4. El cálculo del discriminante de un cuerpo cuadrático (capítulo V, §3, ex.) muestra que se tiene necesariamente $\mathrm{F} = \mathbf{Q}[\sqrt{q}]$ si $q \equiv 1 \bmod 4$ y $\mathrm{F} = \mathbf{Q}[\sqrt{-q}]$ si $q \equiv 3 \bmod 4$. Poniendo $q^* = (-1)^{\frac{q-1}{2}} q$, tenemos en todo caso que $\mathrm{F} = \mathbf{Q}[\sqrt{q^*}]$.

Sea p un número primo distinto a q. Notemos σ_p el automorfismo de Frobenius $\left(\frac{\mathrm{K}/\mathbf{Q}}{p}\right)$ (cf. §4). Su restricción a F es $\left(\frac{\mathrm{F}/\mathbf{Q}}{p}\right)$ (§3, proposición 1, b)) y es la identidad si $\sigma_p \in \mathrm{H}$, es decir si el exponente $j(\sigma_p) =$ a la clase de p mod q (cf. §4) es un **cuadrado** en $\mathbf{F}_q^*$. En el caso contrario el el automorfismo distinto a la identidad. En otras palabras, identificando el grupo de Galois G/H de F sobre $\mathbf{Q}$ con $\{+1, -1\}$, tenemos

$$\left(\frac{\mathrm{F}/\mathbf{Q}}{p}\right) = \left(\frac{p}{q}\right) \tag{1}$$

por definición del símbolo de Legendre $\left(\frac{p}{q}\right)$ (capítulo V, §5).

Por otra parte los resultados sobre la descomposición de un número primo p en $\mathrm{F} = \mathbf{Q}[\sqrt{q^*}]$ (capítulo V, §4) nos otorgan??? más información sobre $\left(\frac{\mathrm{F}/\mathbf{Q}}{p}\right)$.

Por definición, es la identidad si p se descompone totalmente en F y el automorfismo no trivial si p es inerte. Por la proposición 1 de §4, capítulo V, tenemos por lo tanto, si p es **impar**

$$\left(\frac{\mathrm{F}/\mathbf{Q}}{p}\right) = \left(\frac{q^*}{p}\right). \tag{2}$$

Comparando (1) y (2) obtenemos $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$. Como $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-2}{2}}$ por el criterio elemental de Euler (capítulo V, §5, proposición 1), se sigue que $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$ y volemos a obtener la ley de la reciprocidad cuadrática (capítulo V, §5, teorema 1).

Si $p = 2$, recordemos que 2 se descompone totalmente en F si $q^* \equiv 1 \pmod 8$ y que es inerte si $q^* \equiv 5 \pmod 8$ (capítulo V, §4, proposición 1). Como

$$(-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{q^{*2}-1}{8}}$$

vale 1 si $q^* \equiv 1 \pmod 8$ y -1 si $q^* \equiv 5 \pmod 8$, tenemos por lo tanto

$$\left(\frac{\mathrm{F}/\mathbf{Q}}{2}\right) = (-1)^{\frac{q^2-1}{8}}. \tag{3}$$

Comparando (1) y (3) obtenemos $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$, que no es otra cosa que la "fórmula comlementaria" difícil (capítulo V, §5, proposición 2, *b*)).

Complementos sin demostración

Aquí damos, sin demostración, algunos complementos a lo se hizo en el texto. Se tratan de cuestiones muy cercanas a aquellas tratadas en el texto y cuyo grado de profundida y dificultad es análogo también. No fueron incluidas para poder mantener este libro de un tamaño razonable y también porque se las trata en otras obras (ver p. ej. el capítulo V de [**21**], que se puede leer directamente después de este libro).

El autor dió marcha atrás a la idea de dar, sin demostración, una descripción de los desarollos más avanzados de la teoría de números (adèles, cuerpos de clases, funciones zeta y series L, aritmética de álgebras simples, teoría analítica, formas cuadráticas, etc.). Para eso, envía al lector a los títulos nombrados en la primera mitad de la bibliografía (que aparecen sin número).

Fórmulas de transitividad

Dados 3 cuerpos encajados $\mathrm{K} \subset \mathrm{L} \subset \mathrm{M}$, cada uno extensión de **grado finito** del anterior, tenemos las aplicaciones "traza"

$$\mathrm{Tr}_{\mathrm{L/K}} : \mathrm{L} \to \mathrm{K}, \quad \mathrm{Tr}_{\mathrm{M/L}} : \mathrm{M} \to \mathrm{L}, \quad \mathrm{Tr}_{\mathrm{M/K}} : \mathrm{M} \to \mathrm{K},$$

y las aplicaciones "norma" análogas (capítulo II, §6). Entonces, para $x \in \mathrm{M}$, se tiene

$$\begin{cases} \mathrm{Tr}_{\mathrm{M/K}}(x) = \mathrm{Tr}_{\mathrm{L/K}}(\mathrm{Tr}_{\mathrm{M/L}}(x)) \\ \mathrm{N}_{\mathrm{M/K}}(x) = \mathrm{N}_{\mathrm{L/K}}(\mathrm{N}_{\mathrm{M/L}}(x)) \end{cases} \tag{1}$$

Norma relativa de un ideal

Dados dos cuerpos de números ecajados $\mathrm{K} \subset \mathrm{K}'$ y un ideal (entero o fraccionario) $\mathfrak{a}'$ de K', el ideal de K generado por los $\mathrm{N}_{\mathrm{K}'/\mathrm{K}}(x)$ ($x \in \mathfrak{a}$) se llama **norma relativa** de $\mathfrak{a}'$, y se nota $\mathrm{N}_{\mathrm{K}'/\mathrm{K}}(\mathfrak{a}')$ (o $\mathrm{N}(\mathfrak{a}')$). Si $\mathfrak{a}'$ es un ideal principal (a') se tiene

$$\mathrm{N}_{\mathrm{K}'/\mathrm{K}}((a')) = (\mathrm{N}_{\mathrm{K}'/\mathrm{K}}(a)). \tag{2}$$

Si $K = \mathbf{Q}$ recuperamos la noción expuesta en el capítulo III, §5: si $\mathfrak{a}'$ es un ideal entero de K', y si A' es el anillo de enteros de K', se tiene

$$N_{K'/\mathbf{Q}}(\mathfrak{a}') = \mathrm{card}(A'/\mathfrak{a}')\mathbf{Z}. \tag{3}$$

Volviendo al caso genera, si $\mathfrak{a}$ es un ideal de K y si $n = [K' : K]$, tenemos

$$N_{K'/K}(A'\mathfrak{a}) = \mathfrak{a}^n. \tag{4}$$

Si $\mathfrak{a}'$ y $\mathfrak{b}'$ son dos ideales de K', tenemos una fórmula de multiplicatividad:

$$N_{K'/K}(\mathfrak{a}'\mathfrak{b}') = N_{K'/K}(\mathfrak{a}')N_{K'/K}(\mathfrak{b}') \tag{5}$$

Por último, si $\mathfrak{p}'$ es un ideal primo de K' y $\mathfrak{p} = \mathfrak{p}' \cap K$ y si f es el grado residual de $\mathfrak{p}'$ sobre K, se tiene

$$N_{K'/K}(\mathfrak{p}') = \mathfrak{p}^f. \tag{6}$$

Dados tres cuerpos encajados $K \subset K' \subset K''$, tenemos la siguiente fórmula de transitividad, donde $\mathfrak{a}''$ denota un ideal de K'':

$$N_{K''/K}(\mathfrak{a}'') = N_{K'/K}(N_{K''/K'}(\mathfrak{a}'')). \tag{7}$$

En la misma situación, la noción de norma relativa de un ideal permite dar una fórmula de transitivdad para los discriminantes (donde $\mathfrak{D}_{K'/K}$ denota el discriminante de K' sobre K; cf. capítulo V, §3, definición 1)

$$\mathfrak{D}_{K''/K} = N_{K'/K}(\mathfrak{D}_{K''/K'}) \cdot \mathfrak{D}_{K'/K}^{[K'':K']}. \tag{8}$$

Todo lo anterior se generaliza a un anillo de Dedekind A y a su clausura íntegra A' en una extensión de grado finito del cuerpo de fracciones de A.

El diferente

Lo que sigue es válido para un anillo de Dedekind A y a la clausura íntegra de A en una extensión de grado finito de su cuerpo de fracciones. Para simplificar, supondremos que estamos en el caso de un cuerpo de números.

Sean $K \subset K'$ dos cuerpos encajados, A y A' sus anillos de enteros. Decimos que un ideal maximal $\mathfrak{p}'$ de A' **es ramificado** sobre A (o sobre K) si su índice de ramificación sobre A es > 1. Entonces el ideal maximal $\mathfrak{p} = \mathfrak{p}' \cap A$ de A **ramifica** en A' (capítulo V, §3). Resulta fácilmente del capítulo V, §3, teorema 1 que sólo hay **un número finito** de ideales maximales de A' que son ramificados sobre A. Nosotros caracterizaremos un ideal $\mathfrak{d}_{K'/K}$ de A', el **"diferente"** de K' sobre K, tal que esos ideales son exactamente aquellos que contienen a $\mathfrak{d}_{K'/K}$ (observar la analogía con el capítulo V, §3, teorema 1).

Se demuestra primero que nada que el conjunto de los $x \in \mathrm{K}'$ tales que

$$\mathrm{Tr}_{\mathrm{K}'/\mathrm{K}}(x\mathrm{A}') \subset \mathrm{A} \tag{9}$$

es un ideal fraccionario $\mathfrak{C}$ de A', que lo llamamos el **codiferente** de K' sobre K. Por definición el **diferente** $\mathfrak{d}_{\mathrm{K}'/\mathrm{K}}$ es el ideal inverso $\mathfrak{C}^{-1}$. Es un ideal **entero** no nulo de A'. Se demuestra que está **generado por los** $\mathrm{F}'(x)$**,** donde x recorre A' y F denota el polinomio minimal de x sobre K. En particular, si A' es de la forma $\mathrm{A}[y]$ (que no es el caso siempre) y si G es el polinomio minimal de y sobre K, entonces el diferente $\mathfrak{d}_{\mathrm{K}'/\mathrm{K}}$ es el ideal principal de A' generado por $\mathrm{G}'(y)$.

Los ideales primos no nulos de A' que son ramificados sobre A son aquellos que contienen $\mathfrak{d}_{\mathrm{K}'/\mathrm{K}}$. Más precisamente, sea

$$\mathfrak{d}_{\mathrm{K}'/\mathrm{K}} = \prod_i \mathfrak{p}_i'^{m_i} \quad (m_i > 0) \tag{10}$$

la descomposición del diferente en ideales primos y sea e_i el índice de ramificación de $\mathfrak{p}_i'$ sobre A. Entonces los ideales primos no nulos de A' que son ramificados sobre A son los $\mathfrak{p}_i'$ y se tiene $m_i \geq e_i - 1$ para todo i. Además, se tiene $m_i = e_i - 1$ si y sólo si e_i es coprimo con la característica del cuerpo residual $\mathrm{A}'/\mathfrak{p}_i'$.

El $\mathfrak{d}_{\mathrm{K}'/\mathrm{K}}$ (ideal de A') y el discriminante $\mathfrak{D}_{\mathrm{K}'/\mathrm{K}}$ (ideal de A) están relacionados de la siguiente manera:

$$\mathfrak{D}_{\mathrm{K}'/\mathrm{K}} = \mathrm{N}_{\mathrm{K}'/\mathrm{K}}(\mathfrak{d}_{\mathrm{K}'/\mathrm{K}}) \tag{11}$$

(cf. capítulo II, §7, fórmula (6)). Así la información del diferente es más precisa que aquella del discriminante.

Por último, dados tres cuerpos encajados $\mathrm{K} \subset \mathrm{K}' \subset \mathrm{K}''$, se tiene la siguiente fórmula de transitividad para los diferentes:

$$\mathfrak{d}_{\mathrm{K}''/\mathrm{K}} = \mathfrak{d}_{\mathrm{K}''/\mathrm{K}'} \cdot \mathfrak{d}_{\mathrm{K}'/\mathrm{K}}. \tag{12}$$

Ejercicios

Los ejercicios marcados A son ejercicios "de reflexión inmediata", destinados al control directo del conocicimiento ?. Los ejercicios marcados B son más elaborados. Los "problemas de revisión" (al final) son problemas de examen, donde a veces hay menos guías que en algunos de los ejercicios B.

Capítulo I

1 B. *Sea p un número primo y $r \in \mathbf{N}$. Mostrar que el grupo multiplicativo $(\mathbf{Z}/p^r\mathbf{Z})^\times$ es cíclico, salvo si $p = 2$ y $r \geq 3$ (para p impar, mostrar que la clase de $1+p$ tiene orden p^{r-1}; para $p = 2$ estudiar el orden de la clase de 5; utilizar después el Corolario 4 del Teorema 1, §5).*

2 B.

3 B. *Rehacer la demostración claśica del hecho que hay una infinidad de números primos. Inspirandose en esa, mostrar que hay una infinidad de números primos de la forma $4k-1$ ($k \in \mathbf{N}$).*

4B. *Para que $n \in \mathbf{N}$ sea primo, es necesario y suficiente que n divida a $(n-1)!+1$. (Si n es primo, calcular el producto de los elementos de $\mathbf{F}_n^\times$; examinar a continuación el caso cuando n no es primo).*

5B. *Mostrar que, en un cuerpo finito K, todo elemento es suma de dos cuadrados (tratar primero el caso donde $q = \mathrm{card}(\mathrm{K})$ es par; si q es impar, calcular el numero de valores que toma la función $x \mapsto x^2$ y $y \mapsto a - y^2$, $x, y \in \mathrm{K}$, $a \in \mathrm{K}$ dados).*

6B. *Descomponer el polinomio $\mathrm{X}^3-\mathrm{X}+1$ sobre $\mathbf{F}_{23}$ y el polynomio $\mathrm{X}^3+\mathrm{X}+1$ sobre $\mathbf{F}_{31}$ (cada uno tiene una raíz doble y una raíz simple).*

7A. *Dar un ejemplo de dos ideales $\mathfrak{a}, \mathfrak{b}$ de un anillo A tal que $\mathfrak{a} \cap \mathfrak{b} \neq \mathfrak{ab}$. Mostrar que siempre se tiene $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.*

8B. *Sea* A *un dominio íntegro,* $a, b \in \mathrm{A}$, *y* $\mathrm{B} = \mathrm{A}[\mathrm{X}]/(a\mathrm{X}+b)$. *Mostrar que, si* $\mathrm{A}a \cap \mathrm{A}b = \mathrm{A}ab$, *entonces* B *es íntegro (considerar el elemento* $-b/a$ *del cuerpo de fracciones* K *de* A, *y mostrar que el morfismo* $\varphi : \mathrm{A}[\mathrm{X}] \to \mathrm{K}$ *definido por* $\varphi(\mathrm{X}) = -b/a$ *y* $\varphi(y) = y$ *para* $y \in \mathrm{A}$ *tiene núcleo exactamente* $(a\mathrm{X} + b)$.

9B. *Sea* A *un dominio íntegro y* i, j *dos enteros* ≥ 1 *coprimos. Mostrar que el ideal* $(\mathrm{X}^i - \mathrm{Y}^j)$ *del anillo de polinomios* A[X,Y] *es primo (definir un morfismo* A[X,Y] $\to$ A[X] *que tenga este ideal como núcleo.*

10B. *Sea* A *un dominio íntegro,* K *su cuerpo de fracciones y* b *un elemento no nulo de* A. *Mostrar*

Capítulo II

1A. *El teorema 1 de §7 también vale si, en vez de suponer que* K *es de característica cero, suponemos que* K *es finito. Explicar porqué. Es interesante el caso de* K *es finito?*

Bibliografía

[1] E. Artin. *Theory of algebraic numbers* (G. Striker, Schildweg 12, Göttingen, Allemagne-1957) (Explica el pasaje a la teoría de las valuaciones; muy eleganate; muchos ejemplos).

[2] H. Hasse. *Zahlentheorie* (Akademie Verlag, Berlin, 1949) (masivo y muy completo).

[3] H. Hasse. *Vorlesungen über Zahlen theorie* (Springer, 1964) (describe muchos aspectos de la teoría de números).

[4] G.H. Hardy y E.M. Wright. *An introduction to the theory of numbers* (Clarendon Press-Oxford, 1965) (profundo y atractivo; un notable sentido estético en la elección de los temas).

[5] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* (Chelsea, New York, 1948) (un clásico, muy eficaz y completo).

[6] S. Lang, *Algebraic Numbers,* (Addison-Wesley, 1964) (un libro pequeño, muy denso y concentrado).

[7] S. Lang, *Diophantine Geometry* (Interscience Tract n° 11, J. Wiley, New York, 1962) (orientado hacie las ecuaciones diofánticas; presenta muy claramente su conexión con la Goemetría algebrica).

[8] O'Meara, *Introduction to quadratic forms* (Springer, 1963) (una exposición muy eficaz de la teoría de números algebraicos, seguida de una de sus más bellas aplicaciones).

[9] J.P. Serre, *Corps locaux* (Hermann, Paris, 1962) (el acento se posa aquí sobre los cuerpos p-ádicos; una presentación muy clara y lúcida de los métodos algebraicos más recientes de la Teoría de números; muy rico y autocontenido; muchos ejemplos).

[10] E. Artin and J. Tate. *Class-field theory* (Math. Dept. Harvard University) (la exposición más moderna de la famosa teoría de llos "cuerpos de clases," es decir las extensiones abelianas de los cuerpos de números).

[11] A. Weil, *Basic number theory* (Springer, 1967) (utiliza los métodos de los adèles, y trata al mismo tiempo el caso de los cuerpos de números y los cuerpos de funciones).

[12] Z.I. Borovic et I.R. Safarevic. *Théorie de nombres* (Gauthiers Villars, 1966) (muy completo; excelentes capítulos sobre los métodos analíticos, complejos y p-ádicos; numerosas tablás númericas).

[13] N. Bourbaki. *Algèbre* (Paris, Hermann). Sobre todo el capítulo V para lo que concierne a los cuerpos, capítulo VI para lo que concierne la divisibilidad y el capítulo VII para lo que concierne a los módulos sobre dominios de ideales principales.

[14] N. Bourbaki. *Algèbre commutative* (*ibid*). Sobre todo el capítulo V para lo que concierne los elementos enteros, y el capítulo VII para lo concerniente a los anillos de Dedekind y de factorización única. En el capítulo II se puede encontrar una teoría muy

completa y general de los anillos de fracciones. Una buena exposición de la teoría de valuaciones en el capítulo VI.

[15] H. Cartan. *Théorie élémentaire des fonctions analytiques...* (Paris, Hermann, 1962).

[16] G. Choquet. *Cours d'analyse* (Paris, Masson, 1963).

[17] S. Lang. *On quasi-algebraic closure* (Ann. of math., 55 (1962), 373–390).

[18] P. Samuel. *A propos du théorème des unités* (Bull. Sci. math., 90, (1966) 89–96).

[19] P. Samuel. *Anneaux factoriels* (Publ. Soc. mat. São Paulo, 1964).

[20] G. Terjanian, *Sur une conjecture de M. Artin* (C.R. Acad. Sci. Paris, (1966)).

[21] O. Zariski and P. Samuel, *Commutative algebra,* Vol. I (Van Nostrand, Princeton, 1958). Capítulo II para los cuerpos, capítulo IV para los anillos noetherianos, capítulo V para los elementos enteros y los anillos de Dedekind.