Carlos Ivorra Castillo

TEORÍA ALGEBRAICA DE NÚMEROS

La aritmética superior nos proporciona un conjunto inagotable de verdades interesantes — de verdades que además no están aisladas, sino en estrecha relación unas con otras, y entre las cuales, con cada sucesivo avance de la ciencia, descubrimos nuevos y, a veces, completamente inesperados puntos de contacto.

C.F.Gauss

Índice General

Introducción

En mi libro de *Introducción a la teoría algebraica de números* [ITAl] obtuvimos numerosos resultados profundos sobre los números naturales y enteros usando una teoría algebraica mínima. En este libro iremos mucho más lejos aprovechando las técnicas más sofisticadas expuestas principalmente en mi libro de *Álgebra* [Al] y en mi libro de *Análisis matemático* [An], aunque ocasionalmente usaremos también algunos resultados que aparecen en mi libro de *Introducción a la teoría analítica de números* [ITAn] o *Introducción al cálculo diferencial* [IC].

En una ocasión usaremos un resultado de mi libro de *Teoría de grupos* [TG] y mencionaremos algunos resultados de mi libro de *Teoría analítica de números* [TAn], aunque será en comentarios marginales que no se necesitan para seguir este libro.

Más precisamente, en los capítulos XI y XII de [ITAl] vimos que el comportamiento de las formas cuadráticas binarias con coeficientes enteros está íntimamente relacionado con la aritmética de (los anillos de enteros de) los cuerpos cuadráticos, y en el capítulo XVII vimos que el Último Teorema de Fermat está relacionado con la aritmética de (los anillos de enteros de) los cuerpos ciclotómicos. En el capítulo XIII de [ITAl] vimos que la aritmética de los cuerpos cuadráticos sólo se entiende adecuadamente al tener en cuenta que existe una "aritmética ideal" que trasciende las deficiencias de la "aritmética real". Mucho más en general, en el capítulo VIII de [Al] probamos que dicha aritmética ideal es común a los anillos de enteros algebraicos de todos los cuerpos numéricos (las extensiones finitas del cuerpo $\mathbb{Q}$ de los números racionales), y que la existencia de factorización ideal en los cuerpos ciclotómicos extiende sustancialmente el alcance de los resultados de Kummer sobre el Último Teorema de Fermat.

En el capítulo I del presente libro veremos que el estudio de una clase de formas que incluye a las formas cuadráticas binarias irreducibles conduce a estudiar en cuerpos numéricos arbitrarios los conceptos que en [ITAl] introdujimos para cuerpos cuadráticos (anillos de enteros, órdenes, módulos, etc.), y en el capítulo II llevaremos el estudio de la aritmética ideal de los cuerpos numéricos más allá de lo visto en [Al].

En [Al] demostramos que a cada cuerpo numérico K le podemos asignar un anillo $\mathcal{O}_K$ de enteros algebraicos, y que éste es siempre un dominio de Dedekind, es decir, que en él todo ideal propio se descompone de forma única en producto de ideales primos. En particular, esto hace que cada primo $p \in \mathbb{Z}$ tenga una descomposición en factores primos ideales en $\mathcal{O}_K$. Uno de los principales avances

que plantearemos en el capítulo II es no limitarnos a relacionar la aritmética de un cuerpo numérico K (es decir, la aritmética de $\mathcal{O}_K$) con la de $\mathbb{Q}$ (la de $\mathbb{Z}$), sino que trabajaremos con extensiones arbitrarias E/D de dominios de Dedekind (finitas, en el sentido de que la extensión K/k de sus cuerpos de cocientes sea finita). Así, veremos que cada ideal $\mathfrak{p}$ de D se puede identificar con el ideal que genera en E y, aunque $\mathfrak{p}$ sea primo en D, puede dejar de serlo en E y admitir una factorización

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Sucede entonces que cada cuerpo de restos $E/\mathfrak{P}_i$ puede verse de forma natural como una extensión finita del cuerpo de restos $D/\mathfrak{p}$, y el grado f_i de la extensión correspondiente recibe el nombre de 'grado de inercia' de $\mathfrak{P}_i$ sobre $\mathfrak{p}$. Su importancia se debe a que, si llamamos $n = |K : k|$ al grado de la extensión,

$$n = e_1 f_1 + \cdots + e_r f_r,$$

de modo que los grados de inercia miden la "reticencia" del primo $\mathfrak{p}$ a descomponerse en factores, pues si, por ejemplo, se cumple $f_1 = n$, esto significa que $\mathfrak{p} = \mathfrak{P}_1$ se conserva primo en E.

La importancia de admitir dominios de base distintos de $\mathbb{Z}$ reside en que, incluso si estamos interesados en relacionar la aritmética de un anillo de enteros algebraicos $\mathcal{O}_K$ con la de $\mathbb{Z}$, podemos hacerlo fragmentando la extensión $K/\mathbb{Q}$ en varias extensiones intermedias. Por ejemplo, limitándonos por sencillez al caso de un cuerpo numérico normal K (es decir, tal que la extensión $K/\mathbb{Q}$ sea finita de Galois), en tal caso la factorización en $\mathcal{O}_K$ de un primo $p \in \mathbb{Z}$ es siempre de la forma

$$p = \mathfrak{P}_1^e \cdots \mathfrak{P}_r^e$$

y todos los primos $\mathfrak{P}_i$ tienen el mismo grado de inercia f, de modo que $n = efr$, y veremos que podemos encontrar dos cuerpos intermedios $\mathbb{Q} \subset K_e \subset K_i \subset K$ de modo que la factorización de p en K_e es de la forma

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

de modo que p se escinde en el mismo número r de primos que en K, pero con $e = f = 1$, luego, cada primo $\mathfrak{p}_i$ se conserva primo en K_i, por lo que el grado de inercia en este tramo es f y, finalmente $\mathfrak{p}_i = \mathfrak{P}_i^e$ en K. En otras palabras, la factorización de un primo puede descomponerse en tres etapas que se pueden estudiar por separado: en una primera etapa se produce la escisión, en la segunda se produce la extensión de los cuerpos de restos y en la tercera se produce la ramificación (un primo $\mathfrak{p}$ se ramifica respecto a otro $\mathfrak{P}$ de una extensión si $\mathfrak{P}^e \mid \mathfrak{p}$ con exponente $e > 1$. Dicho exponente se llama *índice de ramificación* de $\mathfrak{P}$ sobre $\mathfrak{p}$).

La ramificación de primos es un fenómeno excepcional, en el sentido de que veremos que en una extensión de cuerpos numéricos sólo un número finito de primos del (anillo de enteros del) cuerpo base se ramifica. Esto es algo que comprobamos en [Al] para cuerpos cuadráticos y para cuerpos ciclotómicos de orden primo, en los que los únicos primos que se ramifican son los que dividen al discriminante del cuerpo. No es trivial, pero en el capítulo IX veremos que esto es cierto en cuerpos numéricos arbitrarios.

Otra técnica potente que introduciremos en el capítulo II y de la que no disponíamos en [Al] es la localización respecto de primos. Por poner el ejemplo más simple, si $p \in \mathbb{Z}$ es primo, llamemos Q_p al conjunto de los números racionales cuyo numerador (en su expresión en fracción irreducible) no es divisible entre p. Es fácil ver que $\mathbb{Q}_p$ es un anillo en el que p es el único primo (salvo unidades). Al pasar de $\mathbb{Z}$ a $\mathbb{Q}_p$ todos los primos distintos de p se convierten en unidades, mientras que p se conserva primo. En general veremos que localizar dominios de Dedekind respecto de ideales primos ayuda a obtener resultados "globales" sobre la aritmética del dominio de Dedekind.

En el capítulo III introduciremos una teoría analítica debida a Minkowski conocida como 'geometría de los números', que nos permitirá resolver varios problemas fundamentales que no pudimos abordar en [ITAl] o ni siquiera en [Al]. En [ITAl] probamos la finitud de los grupos de clases de los cuerpos cuadráticos, y en [Al] definimos el grupo de clases de un cuerpo numérico arbitrario, pero sólo demostramos su finitud en el caso de los cuerpos ciclotómicos de orden primo. La geometría de los números nos permitirá probar la finitud del grupo de clases en general, así como determinar la estructura del grupo de las unidades del anillo de enteros algebraicos de un cuerpo numérico.

El conocimiento de las unidades de un anillo es fundamental a la hora de usar su aritmética. Por ejemplo, en [Al] probamos el teorema de Kummer, según el cual el Último Teorema de Fermat es cierto para exponentes regulares, donde un primo p es regular si cumple dos condiciones:

A) p no divide al número de clases h del cuerpo ciclotómico $\mathbb{Q}(\omega)$ de orden p.

B) Una unidad $\epsilon \in \mathbb{Z}[\omega]$ es una potencia p-ésima si y sólo si es congruente módulo p con un entero (racional).

Calcular el número de clases h no es fácil en la práctica, pero comprobar si un primo p cumple la condición B) es impensable sin un buen conocimiento de las unidades ciclotómicas. Esto hace que, en los términos enunciados en [Al], es casi imposible aplicar el teorema de Kummer para comprobar el Último Teorema de Fermat para un exponente p. A duras penas logramos hacerlo en el caso $p = 5$.

En [ITAl] vimos que los cuerpos cuadráticos imaginarios tienen un número finito de unidades (dos, salvo en unas pocas excepciones), mientras que los cuerpos cuadráticos reales tienen infinitas, pero todas son de la forma $\pm\epsilon^n$, donde $n \in \mathbb{Z}$ y ϵ es lo que se llama una unidad fundamental. En el capítulo III probaremos el teorema de Dedekind que generaliza estos hechos a cuerpos numéricos arbitrarios. Veremos que el grupo de unidades de un cuerpo numérico es el producto de un grupo finito (el grupo de las raíces de la unidad contenidas en el cuerpo) por un grupo libre cuyo rango r es fácil de calcular. Esto se traduce en que existen sistemas de r unidades fundamentales $\epsilon_1, \ldots, \epsilon_r$, de modo que toda unidad es de la forma

$$\zeta\epsilon_1^{m_1} \cdots \epsilon_r^{m_r},$$

donde ζ es una raíz de la unidad y los exponentes son enteros. En los cuerpos cuadráticos imaginarios es $r = 0$ y en los reales es $r = 1$.

Este resultado es sólo una parte de lo que necesitaremos en el capítulo VIII para probar que la condición B) de la definición de primo regular es, en realidad, consecuencia de la condición A), por lo que sencillamente puede suprimirse, sólo con eso ya simplificamos drásticamente la comprobación de que un primo es regular.

Una aplicación notable de la geometría de los números es el teorema de Minkowski que afirma que el discriminante de un cuerpo numérico no puede ser ± 1, lo cual, combinado con el hecho de que los primos que se ramifican dividen al determinante, implica que en todo cuerpo numérico (distinto de $\mathbb{Q}$) hay primos ramificados. A su vez, esto nos permite dar un ejemplo interesante:

En [Al 9.8] probamos que existen polinomios irreducibles en $\mathbb{Z}[x]$ cuyo grupo de Galois es isomorfo a Σ_n, y la prueba permite construir ejemplos concretos, pero no sencillos de enunciar. En cambio, en 9.47 probaremos que el polinomio

$$x^n - x - 1$$

tiene grupo de Galois Σ_n. La prueba tiene que esperar hasta el capítulo IX porque necesitamos el hecho de que todos los primos ramificados dividen al discriminante. El lector que esté dispuesto a aceptar esto, así como el teorema de Minkowski que probamos en el capítulo III, puede leer la prueba tras haber leído el capítulo II.

El capítulo IV contiene otra aplicación fundamental de la geometría de los números, a saber, la convergencia de la función dseta de Dedekind asociada a un cuerpo numérico arbitrario K. Ésta se define como

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{a}$ recorre los ideales (no nulos) del anillo de enteros algebraicos de K. Cuando $K = \mathbb{Q}$ se trata de la función dseta de Riemann clásica. En el capítulo XI de [ITAn] introdujimos la función dseta para el caso de los cuerpos cuadráticos y las técnicas que usamos para probar su convergencia son "geometría de los números". De hecho, los argumentos empleados allí son casos particulares de los que emplearemos en el capítulo IV para tratar con cuerpos numéricos arbitrarios.

Cuando Kummer descubrió la aritmética ideal de los cuerpos ciclotómicos, Dirichlet estudió la generalización de la función dseta de Riemann a estos cuerpos, y para reducirla a lo que hoy se conoce como una serie de Dirichlet "usual", es decir, en la que los índices recorren números naturales y no ideales, introdujo lo que ahora conocemos como los "caracteres de Dirichlet" y las "funciones L de Dirichlet", que estudiamos en el capítulo VIII de [ITAn], y con ello obtuvo una prueba analítica de lo que hoy se conoce como "teorema de Dirichlet sobre primos en progresiones aritméticas". La prueba que dimos en [ITAl 7.24] es una prueba "elemental" que resulta de despojar el argumento original de Dirichlet de toda la teoría de funciones de variable compleja y toda la teoría algebraica de números, lo que la hace mucho más sofisticada. En el capítulo IV veremos otra que sigue más de cerca el argumento de Dirichlet, y que es mucho más natural.

También obtendremos expresiones analíticas para el número de clases de un cuerpo numérico arbitrario análogas a las que obtuvimos en el capítulo VIII de [ITAn] para cuerpos cuadráticos. Kummer usó la expresión analítica para el número de clases de un cuerpo ciclotómico para obtener una caracterización sencillísima de los primos regulares. Como veremos en 8.14, un primo impar p es regular si y sólo si no divide a los denominadores de los números de Bernoulli $B_2, B_4, \ldots, B_{p-3}$. Con esta caracterización ya es fácil ver, por ejemplo, que todos los primos p menores que 100 son regulares salvo 37, 59 y 67.

Para probar esto, Kummer empleó cálculos muy sofisticados sobre los que arrojó luz un alumno suyo, Kurt Hensel, cuando en 1897 introdujo los llamados números p-ádicos. En cierto sentido, Kummer había estado operando con ellos sin saberlo (más precisamente: los cálculos de Kummer se simplifican y se entienden realmente cuando se reinterpretan en términos de números p-ádicos).

Trataremos de motivar su definición mediante un ejemplo. Consideremos la igualdad $x^2 = 2$. No existe ningún número racional que cumpla esta ecuación, pero podemos encontrar aproximaciones racionales todo lo precisas que queramos:

$$1, \quad 1.4, \quad 1.41, \quad 1.414, \quad 1.4142, \quad \ldots$$

Ahora fijamos un número primo, por ejemplo $p = 7$, y vamos a buscar aproximaciones enteras "módulo 7". Las soluciones de $x^2 \equiv 2 \pmod 7$ son $x_0 = \pm 3$. Quedémonos de momento con $x_0 = 3$. El cuadrado de 3 no es 2, pero "se parece" a 2 en el sentido de que 9 y 2 son congruentes módulo 7. Obtendremos una aproximación mejor si hacemos $x^2 \equiv 2 \pmod{7^2}$. Puesto que esta congruencia implica la anterior, una solución ha de ser de la forma $x_1 = 3 + 7t$. Se ha de cumplir además que

$$(3+7t)^2 \equiv 2 \pmod{7^2} \quad \Rightarrow \quad 9 + 6\cdot 7t + 7^2t^2 \equiv 2 \pmod{7^2},$$

$$7(1+6t) \equiv 0 \pmod{7^2} \quad \Rightarrow \quad (1+6t) \equiv 0 \pmod 7 \quad \Rightarrow \quad t \equiv 1 \pmod 7.$$

Así, $x_1 = 3 + 1\cdot 7$ es una mejor aproximación a $\sqrt{2}$ módulo 7 en el sentido de que su cuadrado es congruente con 2, no sólo módulo 7, sino módulo 7^2.

El mismo razonamiento nos lleva a $x^2 = 3 + 1\cdot 7 + 2\cdot 7^2$, cuyo cuadrado es congruente con 2 módulo 7^3. Las aproximaciones se pueden afinar tanto como se quiera. Los términos siguientes son

$$3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + 1\cdot 7^4 + 2\cdot 7^5 + 1\cdot 7^6 + 2\cdot 7^7 + 4\cdot 7^8 + \cdots$$

Nuestra intención es definir los números heptádicos de modo que esta serie infinita sea uno de ellos, una raíz cuadrada de 2 heptádica, de modo que cada suma parcial se parece a $\sqrt{2}$ en el sentido de que sus cuadrados son cada vez congruentes con 2 módulo una potencia de 7 mayor.

Ejercicio: Calcular los primeros términos de una serie de potencias de 7 similar a la anterior y que converja a la otra raíz cuadrada de 2 heptádica, la que comienza por 4.

Veremos que estas series de potencias son convergentes respecto de cierta topología, la topología heptádica, respecto a la cual dos números enteros están más "próximos" cuantas más potencias de 7 dividen a su diferencia.

Para introducirla llamamos $v_7(n)$ al exponente del 7 en la descomposición en primos del entero n y, si $r = m/n$ es un número racional definimos su 'valor heptádico' como $v_7(r) = v_7(m) - v_7(n)$. En estos términos, queremos que un número racional esté más próximo a 0 cuanto mayor sea su valor heptádico, para lo cual basta definir el 'valor absoluto heptádico' como

$$|r|_7 = 7^{-v_7(r)}.$$

No es difícil ver que el valor absoluto así definido es realmente un valor absoluto en el sentido de [An 1.17] y, del mismo modo que es posible completar $\mathbb{Q}$ respecto al valor absoluto usual para obtener el cuerpo $\mathbb{R}$ de los números reales, la compleción de $\mathbb{Q}$ respecto del valor absoluto heptádico es por definición el cuerpo $\mathbb{Q}_7$ de los números heptádicos. Evidentemente, esto puede hacerse con cualquier primo p, y así obtenemos el cuerpo de los números p-ádicos, que es un cuerpo métrico completo en el sentido de [An]. Precisamente, en [An] trabajamos en la medida de lo posible con cuerpos métricos completos en lugar de con $\mathbb{R}$ o $\mathbb{C}$ para que los resultados obtenidos fueran aplicables igualmente a los cuerpos de números p-ádicos y sus generalizaciones.

Más en general, si K es cualquier cuerpo numérico y $\mathfrak{p}$ es cualquier ideal primo de su anillo de enteros, veremos que podemos definir el cuerpo $K_\mathfrak{p}$ de los números $\mathfrak{p}$-ádicos, y el paso de K a $K_\mathfrak{p}$ es una herramienta aún más potente que la localización. En efecto, cada cuerpo $K_\mathfrak{p}$ tiene su propio anillo de enteros con un único primo, que podemos identificar con $\mathfrak{p}$, aunque en el anillo de enteros de $K_\mathfrak{p}$ es siempre un ideal principal, cosa que no tiene por qué ser cierta en el anillo de enteros de K. Los cálculos de Kummer involucraban lo que puede interpretarse como tomar logaritmos $\mathfrak{p}$-ádicos.

La topología de los cuerpos de números $\mathfrak{p}$-ádicos, aunque presenta ciertas analogías con la topología de otros cuerpos métricos completos como $\mathbb{R}$ o $\mathbb{C}$, difiere sustancialmente en muchos aspectos debido a que los valores absolutos $\mathfrak{p}$-ádicos son 'no arquimedianos', lo que significa que satisfacen una desigualdad triangular fuerte:

$$|x + y| \leq \text{máx}\{|x|, |y|\},$$

y esto da lugar a algunas propiedades insólitas, como que una serie converge *si y sólo si* su término general tiende a 0. Así pues, el capítulo V está dedicado a exponer los resultados fundamentales sobre cuerpos métricos completos más allá de lo visto en [An], haciendo especial hincapié en el caso no arquimediano.

Como primera aplicación demostraremos en el capítulo VI el teorema de Hasse-Minkowski, que es un ejemplo paradigmático de cómo un problema "global" puede reducirse a estudiar sus "versiones locales". Concretamente, el teorema de Hasse-Minkowski afirma que dos formas cuadráticas con coeficientes en $\mathbb{Q}$ son equivalentes en $\mathbb{Q}$ (en el sentido de que una se transforma en otra mediante un cambio de variables lineal con coeficientes en $\mathbb{Q}$) si y sólo si son equivalentes en $\mathbb{R}$ y en todos los cuerpos p-ádicos $\mathbb{Q}_p$, con la diferencia de que estas equivalencias locales se caracterizan con criterios sencillos en términos del llamado 'símbolo de Hilbert', mientras que la equivalencia global (en $\mathbb{Q}$) no tiene un criterio sencillo más allá del que proporciona el teorema de Hasse-Minkowski al reducirla a las equivalencias locales.

Estos resultados serán cruciales en el capítulo VII, donde profundizaremos en la teoría de Gauss sobre géneros de formas cuadráticas binarias expuesta en el capítulo XIV de [ITAl]. Allí definimos que dos formas tienen el mismo carácter módulo p si y sólo si representan los mismos enteros módulo p^n, para todo n, y ahora veremos que dos formas son del mismo género (tienen el mismo carácter módulo todos los primos) si y sólo si son equivalentes en $\mathbb{Q}$ (si una se transforma en la otra mediante un cambio de variables lineal con coeficientes en $\mathbb{Q}$).

Los cálculos con símbolos de Hilbert en cuerpos p-ádicos nos permitirán demostrar que el hecho de que el número de géneros de formas de un discriminante dado sea siempre la mitad del máximo posible *a priori* es equivalente a la ley de reciprocidad cuadrática, y mostraremos el cálculo que hizo Gauss de este número de géneros, con lo que obtendremos otra prueba de la ley de reciprocidad.

El capítulo VIII está dedicado, como ya hemos indicado a la caracterización de Kummer de los primos regulares y, finalmente, en el capítulo IX estudiaremos a fondo la ramificación en extensiones de dominios de Dedekind, donde usaremos a menudo las técnicas de localización algebraicas y analíticas. En particular, ello nos llevará a estudiar más a fondo los discriminantes de las extensiones y un concepto muy relacionado, el de los 'diferentes'. Veremos que el discriminante global de una extensión puede calcularse como producto de los discriminantes de sus localizaciones, y esto nos permitirá, por ejemplo, probar en 9.44 que el anillo de enteros de un cuerpo ciclotómico $\mathbb{Q}(\omega)$ es precisamente $\mathbb{Z}[\omega]$, cosa que en [Al] sólo pudimos probar para cuerpos ciclotómicos de orden primo, y calcular su discriminante.

Finalmente, en el apéndice A, demostraremos una versión muy general del conocido como 'lema de Hensel', que resulta fundamental en el estudio de la aritmética de los cuerpos métricos completos no arquimedianos arbitrarios, aunque en este libro no ha sido necesario debido a que no hemos trabajado con la máxima generalidad posible, y únicamente nos hará falta para eliminar la hipótesis de separabilidad en ciertos resultados del capítulo V. No obstante, aparte de esto, le daremos una aplicación curiosa: Gracias a él probaremos que en cualquier extensión de $\mathbb{Q}$ finitamente generada existe un valor absoluto no arquimediano con la propiedad de que $|2| < 1$ (usando el lema de Zorn podríamos eliminar fácilmente la condición de finitud, pero no nos hará falta), y esto a su vez nos permitirá demostrar el teorema siguiente:

> *No es posible dividir un cuadrado en un número impar de triángulos de la misma área.*

Capítulo I

Cuerpos numéricos

En este capítulo profundizaremos en el estudio de los cuerpos numéricos que iniciamos en [ITAl] y en el capítulo VIII de [Al], relacionándolo con la resolución de ecuaciones diofánticas asociadas a formas cuadráticas binarias. La primera sección está dedicada a mostrar la relación entre los cuerpos numéricos y las ecuaciones diofánticas definidas por ciertas formas.

1.1 Ecuaciones diofánticas definidas por formas

El teorema [ITAl 2.1] muestra cómo resolver las ecuaciones diofánticas lineales de la forma $ax + by = c$. Las ecuaciones diofánticas más simples después de las lineales son las definidas por formas cuadráticas binarias, es decir, las de la forma

$$ax^2 + bxy + cy^2 = d. \tag{1.1}$$

De entre ellas, las más sencillas son las reducibles, es decir, las que pueden descomponerse en la forma

$$(rx + sy)(tx + uy) = d.$$

En tal caso las soluciones pueden hallarse resolviendo un número finito de sistemas de ecuaciones diofánticas lineales. En la sección [ITAl 11.2] vimos varios ejemplos concretos, pero el método es general.

En [ITAl 11.2] probamos que una forma cuadrática es redudible si y sólo si su *discriminante* $D = b^2 - 4ac$ es un cuadrado perfecto. El caso no trivial se da, pues, cuando el discriminante D no es un cuadrado perfecto. En particular, entonces $a \neq 0 \neq c$. Si factorizamos el polinomio

$$ax^2 + bx + c = a(x - \alpha)(x - \beta),$$

la ecuación se convierte en

$$a(x - \alpha y)(x - \beta y) = d, \qquad \text{con } \alpha, \beta = \frac{-b \pm \sqrt{D}}{2a},$$

de modo que α y β son elementos del cuerpo $\mathbb{Q}(\sqrt{D}\,)$. Más aún, son conjugados en el sentido de la teoría de Galois. Si llamamos N a la norma en $\mathbb{Q}(\sqrt{D}\,)$, la ecuación se expresa en la forma

$$\mathrm{N}(x - \alpha y) = d/a. \tag{1.2}$$

Por lo tanto, la solución de una ecuación diofántica de la forma (1.1) se reduce (salvo casos triviales) a encontrar elementos de la forma $x - \alpha y$ con norma igual a d/a.

Pensar en encontrar elementos de un cuerpo con una norma determinada en lugar de en encontrar pares de enteros que cumplan una ecuación determinada es un cambio de perspectiva muy importante. Con todo, el problema no es simple. Buena muestra de ello es que la menor solución de la ecuación $x^2 - 61y^2 = 1$ es la dada por $(x, y) = (1\,766\,319\,049, 226\,153\,980)$. El caso cuadrático está tratado en la sección [ITAl 12.4], pero aquí nos proponemos presentar una teoría más general.

Ecuaciones equivalentes En la sección [ITAl 11.1] vimos que un cambio de variable adecuado puede simplificar considerablemente el tratamiento de una ecuación diofántica cuadrática. Más en general:

Definición 1.1 Diremos que dos polinomios $F(x_1, \ldots, x_n)$, $G(y_1, \ldots, y_n)$ son *equivalentes* si uno puede obtenerse del otro a partir de un cambio de variables lineal con coeficientes enteros cuya matriz tiene determinante ± 1 (con lo que el cambio de variables inverso también tiene coeficientes enteros).

Ejemplo Si tenemos la ecuación diofántica $13x^2 + 8xy + y^2 = 6$, el cambio de variables

$$x = u - 2v, \quad y = -2u + 5v$$

tiene matriz de determinante 1, luego el cambio inverso también tiene coeficientes enteros:

$$u = 5x + 2y, \quad v = 2x + y.$$

Al aplicar el cambio a la ecuación la convertimos en $u^2 - 3v^2 = 6$, que es bastante más sencilla, y resolver una es equivalente a resolver la otra. Por ejemplo, si descubrimos que una solución de la segunda es $(u, v) = (3, 1)$, el cambio de variables nos da la solución $(x, y) = (1, -1)$ para la ecuación original. ∎

Otra observación aún más elemental es que podemos transformar una ecuación en otra equivalente multiplicando sus miembros por cualquier número no nulo. Aunque en principio estamos interesados en ecuaciones con coeficientes enteros, no hay inconveniente en admitir ecuaciones con coeficientes racionales, pues siempre podemos transformarlas en ecuaciones con coeficientes enteros multiplicando sus miembros por un entero adecuado.

Módulos completos Vamos a presentar ya el marco teórico con el que trataremos las ecuaciones diofánticas definidas por formas cuadráticas con discriminante no cuadrado perfecto. Para ello introducimos el concepto siguiente:

Definición 1.2 Sea K un cuerpo numérico de grado n, es decir, [Al 8.4] una extensión finita de $\mathbb{Q}$ de grado n. Un *módulo* en K es un subgrupo M del grupo $(K,+)$ generado por un conjunto finito $\alpha_1,\dots,\alpha_r$ de elementos de K:

$$M = \langle \alpha_1,\dots,\alpha_r\rangle_{\mathbb{Z}} = \{a_1\alpha_1 + \cdots + a_r\alpha_r \mid a_1,\dots,a_r \in \mathbb{Z}\}.$$

Si M es un módulo, es obvio que para todo $\alpha \in M$ y todo $m \in \mathbb{Z}$, se cumple $m\alpha = 0$ si y sólo si $m = 0$ o $\alpha = 0$, pero esto significa que M es libre de torsión [Al 4.43], luego es libre [Al 4.44], es decir, que tiene base, y todas las bases tienen el mismo número de elementos [Al 4.27], llamado rango de M.

Es inmediato que un conjunto finito de elementos de K es independiente sobre $\mathbb{Q}$ si y sólo si es independiente sobre $\mathbb{Z}$ (una combinación lineal en $\mathbb{Q}$ se convierte en una combinación lineal en $\mathbb{Z}$ multiplicando por un entero no nulo). Consecuentemente, si M es un módulo en K, se cumple que $\operatorname{rang} M \le n$.

Los módulos de rango n se llaman *módulos completos*. Si M es un módulo completo, entonces una base de M como módulo es también una $\mathbb{Q}$-base de K.

Por [Al 5.36] existen exactamente n monomorfismos $\sigma_i : K \longrightarrow \mathbb{C}$, cuya imagen está, de hecho, en la clausura normal L de $K/\mathbb{Q}$ en $\mathbb{C}$ ([Al 5.24]). Si σ es un automorfismo de L, tenemos que $\sigma_i \circ \sigma$ es uno de los monomorfismos de K, por lo que la correspondencia $\sigma_i \mapsto \sigma_i \circ \sigma$ permuta los monomorfismos de K.

Si M es un módulo completo en K con base $\alpha_1,\dots,\alpha_n$, la función definida en $\mathbb{Q}^n$ mediante

$$\mathrm{N}(x_1\alpha_1 + \cdots + x_n\alpha_n) = \prod_{i=1}^{n} (x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n))$$

es un producto de n formas lineales (sumas de monomios de grado 1), luego es una forma de grado n (una suma de monomios de grado n). Sus coeficientes están, en principio, en L, pero la forma queda invariante cuando le aplicamos un automorfismo de L (ya que éste permuta los factores que la definen), luego todos sus coeficientes son fijados por los automorfismos de L, y esto significa, por [Al 5.32], que están en $\mathbb{Q}$.

Una de las aplicaciones de una parte de los resultados que vamos a exponer en este libro es el estudio de las ecuaciones diofánticas de la forma

$$a\,\mathrm{N}(x_1\alpha_1 + \cdots + x_n\alpha_n) = d, \tag{1.3}$$

donde $\alpha_1,\dots,\alpha_n$ es una base de un módulo completo M de un cuerpo numérico K y $a, d \in \mathbb{Q}$ son no nulos (si $a \neq 0$, la única solución para $c = 0$ sería $x_1 = \cdots = x_n = 0$).

Las soluciones enteras $(x_1,\dots,x_n)$ de (1.3) se corresponden biunívocamente con los elementos $\gamma = x_1\alpha_1 + \cdots + x_n\alpha_n \in M$ de norma $\mathrm{N}(\gamma) = d/a$.

Hemos probado que las ecuaciones de este tipo incluyen a todas las determinadas por formas cuadráticas binarias no triviales (es decir, con determinante no cuadrado perfecto). Concretamente, hemos visto que una ecuación de la forma (1.1) es equivalente a (1.2), es decir, a la ecuación (1.3) correspondiente a la base $1, -\alpha$ del módulo $M = \langle 1, -\alpha\rangle$, donde α es una raíz del polinomio $ax^2 + bx + c$.

Tal vez el lector objete que, en todo este planteamiento, el módulo M está de más, en el sentido de que cada ecuación de la forma (1.3) no está asociada a ningún módulo, sino a unos números algebraicos concretos $\alpha_1, \ldots, \alpha_n \in K$. Si cambiamos estos números (aunque sea para pasar a otra base del mismo módulo M), estamos cambiando de ecuación.

Esto es cierto, pero sucede que si $\beta_1, \ldots, \beta_n$ es otra base del mismo módulo M, entonces podemos expresar $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, donde la matriz $A = (a_{ij})$ tiene determinante ± 1, y la ecuación asociada a la nueva base es

$$a\,\mathrm{N}\Big(\sum_{i=1}^{n} y_i \sum_{j=1}^{n} a_{ij}\alpha_j\Big) = d,$$

o también

$$a\,\mathrm{N}\Big(\sum_{j=1}^{n} \alpha_j \sum_{i=1}^{n} y_i a_{ij}\Big) = d,$$

que resulta de aplicar a (1.3) el cambio de variables $x_j = \sum_{i=1}^{n} y_i a_{ij}$.

Vemos, pues, que cuando recorremos todas las bases de M, las formas que obtenemos recorren todas las formas equivalentes a (1.3). En suma, a cada módulo completo M de un cuerpo numérico le hemos asociado una clase de equivalencia de formas.

Ejemplo Consideremos de nuevo la ecuación $13x^2+8xy+y^2 = 6$, que podemos expresar como

$$13\,\mathrm{N}\Big(x + y\frac{4+\sqrt{3}}{13}\Big) = 6,$$

correspondiente al módulo $M = \Big\langle 1, \frac{4+\sqrt{3}}{13}\Big\rangle$. El cambio de variable

$$x = u - 2v, \quad y = -2u + 5v$$

se corresponde con el cambio de base

$$\frac{5-2\sqrt{3}}{13} = 1 - 2\,\frac{4+\sqrt{3}}{13}, \qquad \frac{-6+5\sqrt{3}}{13} = -2 + 5\,\frac{4+\sqrt{3}}{13},$$

de modo que también podemos expresar $M = \Big\langle \frac{5-2\sqrt{3}}{13}, \frac{-6+5\sqrt{3}}{13}\Big\rangle$, y la ecuación correspondiente a esta nueva base es

$$13\,\mathrm{N}\Big(u\frac{5-2\sqrt{3}}{13} + v\frac{-6+5\sqrt{3}}{13}\Big) = u^2 - 3v^2 = 6.$$

Resolver la ecuación equivale a encontrar todos los elementos de M que tengan norma $6/13$. ∎

Tal vez el lector haya observado que, en el ejemplo anterior, si partimos directamente de la ecuación $u^2-3v^2=6$ y tratamos de representarla en la forma (1.3) por el procedimiento que hemos visto, es decir, resolviendo la ecuación $u^2-3=0$, no llegamos a la base que hemos obtenido. Ni siquiera llegamos al módulo M, sino a

$$N = \left\langle 1, \sqrt{3} \right\rangle.$$

Ciertamente, la ecuación $\mathrm{N}(u+v\sqrt{3})=6$ es también $u^2-3v^2=6$, pero es claro que $\frac{5-2\sqrt{3}}{13} \notin N$, luego $M \neq N$. Para comprender este fenómeno debemos introducir un nuevo concepto, que generaliza a [ITAl 12.17]:

Definición 1.3 Si M es un módulo de un cuerpo numérico K y $\alpha \in K$, $\alpha \neq 0$, definimos

$$\alpha M = \{\alpha m \mid m \in M\},$$

que claramente es un módulo del mismo rango. Diremos que dos módulos M y N son *similares* si existe un $\alpha \in K$ no nulo tal que $N = \alpha M$.

La similitud es una relación de equivalencia entre los módulos de K.

Ahora, si $M = \langle \alpha_1, \ldots, \alpha_n \rangle$ es un módulo completo y, por consiguiente, su forma asociada a la base indicada es

$$\mathrm{N}(x_1\alpha_1 + \cdots + x_n\alpha_n),$$

entonces $\alpha M = \langle \alpha\alpha_1, \cdots, \alpha\alpha_n \rangle$ y la forma asociada a esta base es

$$\mathrm{N}(x_1\alpha\alpha_1 + \cdots + x_n\alpha\alpha_n) = \mathrm{N}(\alpha)\,\mathrm{N}(x_1\alpha_1 + \cdots + x_n\alpha_n),$$

donde $\mathrm{N}(\alpha) \in \mathbb{Q}$. Por consiguiente, las formas asociadas a bases de M y de αM pueden usarse para representar la misma ecuación modificando su término independiente o, en otros términos, a la hora de estudiar una ecuación diofántica asociada a un módulo M, podemos cambiarlo por otro similar.

Ejemplo Continuando con el ejemplo precedente, se comprueba inmediatamente que

$$(5+2\sqrt{3})M = \left\langle 5+2\sqrt{3}, 2+\sqrt{3} \right\rangle = \left\langle 1, \sqrt{3} \right\rangle = N,$$

de modo que los dos módulos que hemos obtenido son similares. Observemos también que $\mathrm{N}(5+2\sqrt{3})=13$, y por eso

$$\mathrm{N}\Big(u\frac{5-2\sqrt{3}}{13} + v\frac{-6+5\sqrt{3}}{13}\Big) = \frac{1}{13}(u^2-3v^2), \quad \mathrm{N}(u+v\sqrt{3}) = u^2-3v^2,$$

de modo que las dos formas que obtenemos no son exactamente la misma, sino que una determina la ecuación en la forma $\mathrm{N}(u\alpha+v\beta)=6/13$ y la otra como $\mathrm{N}(u\alpha'+v\beta')=6$. ∎

Coeficientes Vamos a introducir un último concepto que interviene en la relación entre las ecuaciones diofánticas definidas por normas y sus módulos asociados y que generaliza a [ITAl 2.8]. Lo ilustramos primero con un ejemplo:

Ejemplo Consideremos la ecuación $x^2 + 5xy + 2y^2 = 2$, que podemos expresar en la forma

$$\mathrm{N}\left(x - \frac{-5-\sqrt{17}}{2}y\right) = 2.$$

Por lo tanto la ecuación está asociada al módulo completo

$$M = \left\langle 1, \frac{5+\sqrt{17}}{2} \right\rangle,$$

correspondiente al cuerpo numérico $\mathbb{Q}\big(\sqrt{17}\big)$. Las soluciones de la ecuación se corresponden con los elementos de M de norma 2. Por ejemplo, una solución es evidentemente $(x, y) = (0, 1)$, correspondiente al segundo generador.

Consideremos ahora el número

$$\epsilon = 33 + 8\sqrt{17}.$$

Sencillos cálculos nos dan que $\mathrm{N}(\epsilon) = 1$ y que $\epsilon M \subset M$. Esto implica que los números

$$\epsilon^k \frac{5+\sqrt{17}}{2},$$

con $k \in \mathbb{Z}$, están todos en M y tienen norma 2, luego nos proporcionan nuevas soluciones de nuestra ecuación. Por ejemplo,

$$\epsilon \frac{5+\sqrt{17}}{2} = \frac{301+73\sqrt{17}}{2} = -32 + 73\frac{5+\sqrt{17}}{2}$$

nos lleva a la solución $(x, y) = (-32, 73)$. De este modo hemos encontrado infinitas soluciones de la ecuación. ∎

En general, una solución de (1.3) esta determinada por un elemento m en un módulo M tal que $\mathrm{N}(m) = d/a$. Si ϵ es un elemento de K tal que $\epsilon m \in M$ y $\mathrm{N}(\epsilon) = 1$, entonces, para todo $k \in \mathbb{Z}$, tenemos que $\epsilon^k m \in M$ y $\mathrm{N}(\epsilon^k m) = d/a$, luego cada $\epsilon^k m$ proporciona una solución de la ecuación (y en la mayoría de los casos —salvo que ϵ sea una raíz de la unidad— las soluciones obtenidas de este modo serán distintas para distintos valores de k).

Conviene separar los dos requisitos que hemos exigido a ϵ. Los números $\epsilon \in K$ que cumplen $\epsilon M \subset M$ se llaman *coeficientes* del módulo M, de modo que, en estos términos, los ϵ que permiten generar nuevas soluciones de una ecuación a partir de una dada son los coeficientes de norma 1. ∎

1.2 Módulos y órdenes

Recapitulemos los hechos que hemos presentado en la sección anterior:

Buscar las soluciones enteras de una ecuación expresable en la forma (1.3) equivale a encontrar los elementos de norma d/a de un cierto módulo completo M en un cuerpo numérico K. La solución asociada a un $m \in M$ está formada por las coordenadas de m en una base prefijada de M. Cambiar de base equivale a efectuar un cambio de variables lineales en la ecuación (con determinante ± 1) y cambiar el módulo M por otro similar αM equivale a multiplicar ambos miembros de la ecuación por $\mathrm{N}(\alpha)$. Finalmente hemos visto que al multiplicar un $m \in M$ que corresponda a una solución de la ecuación por un coeficiente de norma 1 obtenemos una nueva solución.

Empezamos aquí estudiando con detalle la noción de coeficiente de un módulo:

Definición 1.4 Sea M un módulo completo de un cuerpo numérico K. Diremos que $\alpha \in K$ es un *coeficiente* de M si $\alpha M \subset M$. Llamaremos $\mathcal{O}_M$ al conjunto de todos los coeficientes de M. Es claro que $\mathcal{O}_M$ es un subanillo de K. Lo llamaremos *anillo de coeficientes* de M.

Notemos que para que α sea un coeficiente de M basta con que $\alpha m \in M$ cuando m recorre una base de M.

Teorema 1.5 *Sea M un módulo completo de K. Entonces $\mathcal{O}_M$ es también un módulo completo.*

Demostración: Si $\gamma \in M$ es no nulo, entonces $\gamma\mathcal{O}_M \subset M$ y claramente es un subgrupo abeliano de M, luego es un módulo. Así, $\mathcal{O}_M = \gamma^{-1}(\gamma\mathcal{O}_M)$ es también un módulo. Veamos que es de rango máximo.

Sea $m_1, \dots, m_n$ una base de M. Si $\alpha \in K$ es no nulo existen números racionales a_{ij} tales que $\alpha m_i = \sum_{j=1}^n a_{ij} m_j$. Sea c el producto de los denominadores de los a_{ij}. Entonces c es un entero racional no nulo y cada $ca_{ij} \in \mathbb{Z}$, luego $ca_{ij}m_j \in M$, y así $c\alpha m_i \in M$. Como los elementos $m_1, \dots, m_n$ son una base de M podemos concluir que $c\alpha \in \mathcal{O}_M$.

Ahora aplicamos esto a una $\mathbb{Q}$-base de K, digamos $\alpha_1, \dots, \alpha_n$, y encontramos números racionales no nulos $c_1, \dots, c_n$ tales que $c_1\alpha_1, \dots, c_n\alpha_n \in \mathcal{O}_M$, luego $\mathcal{O}_M$ contiene n elementos linealmente independientes, por lo que su rango es n. ∎

Definición 1.6 Diremos que $\mathcal{O}$ es un *orden* de un cuerpo numérico K si es un módulo completo de K que además es un anillo unitario.

El teorema anterior prueba que el anillo de coeficientes de un módulo completo de K es un orden de K. Todo orden $\mathcal{O}$ es el anillo de coeficientes de un módulo completo (ya que, como $1 \in \mathcal{O}$, es su propio anillo de coeficientes).

Los órdenes son módulos muy especiales. Por lo pronto su estructura de anillo nos permite argumentar en términos de divisibilidad, unidades, ideales, etc.

Otra característica muy importante es que los elementos de un orden han de ser enteros (algebraicos). Recogemos éste y otros hechos notables en el próximo teorema:

Teorema 1.7 *Sea $\mathcal{O}$ un orden de un cuerpo numérico K de grado n.*

1. *Si $\alpha \in \mathcal{O}$ entonces α es un entero y $\mathrm{N}(\alpha)$, $\mathrm{Tr}(\alpha)$ son enteros racionales. Por lo tanto tenemos aplicaciones $\mathrm{N} : \mathcal{O} \longrightarrow \mathbb{Z}$ y $\mathrm{Tr} : \mathcal{O} \longrightarrow \mathbb{Z}$.*
2. *Si $\alpha, \beta \in \mathcal{O}$ y $\alpha \mid \beta$, entonces $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$. En particular si α y β son asociados $\mathrm{N}(\alpha) = \pm\mathrm{N}(\beta)$.*
3. *Si a y b son enteros racionales, entonces $a \mid b$ en $\mathbb{Z}$ si y sólo si $a \mid b$ en $\mathcal{O}$.*
4. *Si $\alpha \in \mathcal{O}$ entonces $\alpha \mid \mathrm{N}(\alpha)$ (en $\mathcal{O}$).*
5. *Un número $\epsilon \in \mathcal{O}$ es una unidad si y sólo si $\mathrm{N}(\epsilon) = \pm 1$.*

Demostración: 1) Si $\alpha \in \mathcal{O}$, entonces $\mathbb{Z}[\alpha] \subset \mathcal{O}$ (porque $\mathcal{O}$ un anillo), luego $\mathbb{Z}[\alpha]$ es finitamente generado (porque $\mathcal{O}$ es un módulo y por [Al 7.40]), luego [Al 8.8] concluimos que α es entero.

Los conjugados de enteros son enteros (porque tienen el mismo polinomio mínimo) y por lo tanto $\mathrm{N}(\alpha)$ y $\mathrm{Tr}(\alpha)$ son enteros (son el producto o la suma de los conjugados de α). Además son racionales.

2) Es evidente, por la propiedad multiplicativa de la norma.

3) Si $a \mid b$ en $\mathcal{O}$, entonces a/b es entero y racional.

4) Supongamos $\alpha \neq 0$ y consideremos el polinomio

$$p(x) = \big(x - \sigma_1(\alpha)\big) \cdots \big(x - \sigma_n(\alpha)\big).$$

Los automorfismos de la clausura normal de K permutan los factores de $p(x)$, luego sus coeficientes son números racionales. Como α y sus conjugados son enteros, también lo serán los coeficientes de $p(x)$, es decir, son enteros racionales.

El polinomio $p(x)$ es mónico y su término independiente es $\pm\mathrm{N}(\alpha)$. Por lo tanto podemos despejar $\mathrm{N}(\alpha)/\alpha$ como combinación de potencias de α con coeficientes enteros racionales. Consecuentemente $\mathrm{N}(\alpha)/\alpha \in \mathcal{O}$.

5) Si $\mathrm{N}(\epsilon) = \pm 1$ entonces $\epsilon \mid \mathrm{N}(\epsilon) = \pm 1$, luego ϵ es una unidad. Si ϵ es una unidad entonces $\epsilon^{-1} \in \mathcal{O}$, y $\mathrm{N}(\epsilon)\,\mathrm{N}(\epsilon^{-1}) = \mathrm{N}(1) = 1$, luego $\mathrm{N}(\epsilon) = \pm 1$ (pues los dos factores son enteros racionales). ∎

Profundicemos ahora en la relación entre un módulo y su anillo de coeficientes. En primer lugar tenemos lo siguiente:

Teorema 1.8 *Sea K un cuerpo numérico. Entonces:*

1. *Dos módulos completos similares tienen el mismo anillo de coeficientes.*
2. *Si M es un módulo completo, existe un $m \in \mathbb{Z}$ no nulo tal que $mM \subset \mathcal{O}_M$.*

DEMOSTRACIÓN: 1) es evidente.

2) Sea $m_1, \ldots, m_n$ una base de M y $\alpha_1, \ldots, \alpha_n$ una base de $\mathcal{O}_M$. Existen números racionales a_{ij} tales que $m_i = \sum_{j=1}^{n} a_{ij}\alpha_j$. Si m es el producto de los denominadores de los a_{ij} se cumple que $mm_i \in \mathcal{O}_M$, luego $mM \subset \mathcal{O}_M$. ∎

Así pues, todo módulo es similar a otro contenido en su anillo de coeficientes, pero es claro que si $M \subset \mathcal{O}_M$ entonces M es un ideal de $\mathcal{O}_M$. Por lo tanto desde un punto de vista teórico podemos limitarnos a trabajar con ideales de órdenes en lugar de módulos. El recíproco también es cierto: todos los ideales de un orden son módulos completos:

Teorema 1.9 *Sea $\mathcal{O}$ un orden de un cuerpo numérico K. Los ideales no nulos de $\mathcal{O}$ son módulos completos (aunque su anillo de coeficientes no es necesariamente $\mathcal{O}$).*

DEMOSTRACIÓN: Sea I un ideal no nulo de $\mathcal{O}$. Por [Al 4.42] I es un módulo finitamente generado. Sea $\alpha \in I$ no nulo. Entonces $\alpha\mathcal{O} \subset I$ es un módulo similar al módulo completo $\mathcal{O}$, luego es un módulo completo. El rango de I ha de ser mayor o igual que el de $\alpha\mathcal{O}$, que es el máximo, luego I es un módulo completo. ∎

Ahora podemos decir que los ϵ que nos permiten obtener nuevas soluciones de una ecuación (1.3) a partir de otras son las unidades de norma 1 del anillo de coeficientes del módulo M asociado a la ecuación. Reflejamos esto en una definición:

Definición 1.10 Dos elementos x e y de un módulo completo M son *asociados* si existe una unidad $\epsilon \in \mathcal{O}_M$ tal que $x = \epsilon y$.

No hemos introducido la exigencia de que la unidad tenga norma 1 porque así este concepto de asociación, cuando se aplica al caso en que M es un orden, se corresponde con el concepto usual de asociación en la teoría de anillos: dos elementos de un anillo son asociados si se diferencian en un factor unitario.

Así, resolver una ecuación diofántica de la forma (1.3) se reduce a encontrar un conjunto maximal de elementos no asociados en M de una norma dada junto con todas las unidades de $\mathcal{O}_M$ de norma 1. El planteamiento es razonable porque seguidamente demostramos que tal conjunto maximal es siempre finito, de modo que todos los números de una norma dada se pueden obtener a partir de un número finito de ellos multiplicando por unidades de norma 1.

Teorema 1.11 *Un módulo completo contiene sólo un número finito de elementos no asociados de una norma dada.*

DEMOSTRACIÓN: Lo probamos primero para un orden $\mathcal{O}$. Sea $\alpha_1, \ldots, \alpha_n$ una base de $\mathcal{O}$ y sea $c > 1$ un número natural. Cada elemento de $\mathcal{O}$ es congruente módulo c con un elemento de la forma

$$x_1\alpha_1 + \cdots + x_n\alpha_n \qquad \text{con } 0 \le x_i < c.$$

Por lo tanto $|\mathcal{O}/(c)| \le c^n$.

Si $\alpha \equiv \beta \pmod{c}$ y $|\,\mathrm{N}(\alpha)| = |\,\mathrm{N}(\beta)| = c$, entonces $\alpha - \beta = c\delta$, para un $\delta \in \mathcal{O}$, luego $\alpha/\beta = 1 + (c/\beta)\delta \in \mathcal{O}$, por el teorema 1.7, pues $\beta \mid \mathrm{N}(\beta) = \pm c$.

Esto significa que $\beta \mid \alpha$ y análogamente $\alpha \mid \beta$, luego α y β son asociados. Así pues, en $\mathcal{O}$ hay a lo sumo c^n elementos no asociados de norma c. Por otra parte, los elementos de norma ± 1 son unidades, luego todos son asociados.

Si M es un módulo completo, existe $m \in \mathbb{Z}$ no nulo tal que $mM \subset \mathcal{O}_M$. Si $\alpha_1, \ldots, \alpha_r$ son elementos no asociados en M de norma c, entonces $m\alpha_1, \ldots, m\alpha_r$ son elementos no asociados en $\mathcal{O}_M$ de norma $m^n c$, luego no puede haber más que un número finito de ellos. ∎

El primer apartado del teorema 1.7 nos lleva a la definición siguiente:

Definición 1.12 Llamaremos *orden maximal* de un cuerpo numérico K al anillo $\mathcal{O}_K$ de todos los enteros (algebraicos) de K.

Los teoremas [Al 8.9] y [Al 8.14] prueban que $\mathcal{O}_K$ es ciertamente un orden de K, y el teorema 1.7 implica que contiene a todos los demás órdenes de K, lo que justifica el calificativo de "maximal".

Una de las primeras cuestiones que plantea el estudio de un cuerpo numérico K es determinar su orden maximal, lo que equivale a encontrar una base de $\mathcal{O}_K$. Recordemos de [Al 8.15] que las bases de $\mathcal{O}_K$ reciben el nombre de bases enteras de K. Así, si $\alpha_1, \ldots, \alpha_n$ es una base entera de K, tenemos que

$$\begin{aligned} K &= \{a_1\alpha_1 + \cdots + a_n\alpha_n \mid a_1, \ldots, a_n \in \mathbb{Q}\},\\ \mathcal{O}_K &= \{a_1\alpha_1 + \cdots + a_n\alpha_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}. \end{aligned}$$

En otros términos, los enteros de K son los elementos con coordenadas enteras en una base entera. En la sección siguiente abordaremos el problema de determinar bases enteras, pero aquí recordamos el concepto de discriminante, que es fundamental para este propósito.

Recordemos que en [Al 8.2] definimos el discriminante $\Delta[B]$ de una base B de una extensión finita de cuerpos. Si B y B' son dos bases de un módulo M, entonces la matriz de cambio de base tiene coeficientes enteros, al igual que su inversa, luego su determinante ha de ser ± 1, y el teorema [Al 8.3] nos da que $\Delta[B] = \Delta[B']$, luego podemos definir el *discriminante* de M como el discriminante $\Delta[M]$ de cualquiera de sus bases.

En particular, el discriminante de K se define como $\Delta_K = \Delta[\mathcal{O}_K]$.

Teorema 1.13 *Sea K un cuerpo numérico.*

1. *Si $\mathcal{O}$ es un orden de K, entonces $\Delta[\mathcal{O}] \in \mathbb{Z}$ y $\Delta[\mathcal{O}] \equiv 0, 1 \pmod{4}$.*
2. *Si $\mathcal{O} \subset \mathcal{O}'$ son dos órdenes de K, entonces $\Delta[\mathcal{O}] = m^2\Delta[\mathcal{O}']$, para cierto natural m. Además $m = 1$ si y sólo si $\mathcal{O} = \mathcal{O}'$.*

DEMOSTRACIÓN: 1) es consecuencia inmediata del teorema [Al 8.13].

2) Los elementos de una base de $\mathcal{O}$ se expresan como combinación lineal de los elementos de una base de $\mathcal{O}'$ con coeficientes enteros racionales. Por lo tanto la matriz D de cambio de base tiene coeficientes enteros racionales y su determinante es un entero racional. Por el teorema [Al 8.3] tenemos que $\Delta[\mathcal{O}] = |D|^2\Delta[\mathcal{O}']$. Además los órdenes coinciden si y sólo si D es de hecho una matriz de cambio de base en $\mathcal{O}'$, lo que sucede si y sólo si $|D| = \pm 1$. ∎

El mismo argumento que acabamos de emplear prueba que si B es una base entera de un cuerpo numérico K y C es una base formada por enteros, entonces $\Delta[C] = m^2\Delta[B]$, para cierto número natural m, de manera que C es una base entera si y sólo si $m = 1$. En otras palabras, una base entera es simplemente una base formada por enteros con discriminante mínimo.

Si $K = \mathbb{Q}(\alpha)$ es un cuerpo numérico de grado n, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de K. Llamaremos $\Delta[\alpha]$ a su discriminante.

Recordemos que el teorema [Al 8.19] nos calcula los discriminantes de la forma $\Delta[\alpha]$. Concretamente, nos da que

$$\Delta[\alpha] = (-1)^{n(n-1)/2}\,\mathrm{N}(p'(\alpha)),$$

donde $p(x) = \operatorname{pol}\operatorname{mín}\alpha$ y $p'(x)$ es su derivada formal [Al 5.25].

Ejemplo *Si el polinomio $f(x) = x^3 + ax + b \in \mathbb{Q}[x]$ es irreducible y α es una raíz, entonces $\Delta[\alpha] = -27b^2 - 4a^3$.*

En efecto, si α' es cualquier conjugado de α, entonces

$$f'(\alpha') = 3\alpha'^2 + a = \frac{3\alpha'^2 + a\alpha}{\alpha'} = \frac{-2a\alpha' - 3b}{\alpha'}.$$

Multiplicamos para los tres conjugados de α, teniendo en cuenta que su producto es $-b$. Así,

$$\Delta[\alpha] = -\,\mathrm{N}\big(f'(\alpha)\big) = \frac{1}{b}\prod_{\alpha'}(-2a\alpha' - 3b) = \frac{8a^3}{b}\prod_{\alpha'}\Big(\frac{-3b}{2a} - \alpha'\Big) = \frac{8a^3}{b}\ f\left(-\frac{3b}{2a}\right).$$

Desde aquí se llega a la fórmula indicada sin más que operar. (Hemos supuesto $a \neq 0$, pero si $a = 0$ es más sencillo.) ∎

Ejercicio: Probar que si $x^5 + ax + b \in \mathbb{Q}[x]$ es irreducible y α es una raíz, entonces $\Delta[\alpha] = 5^4b^4 + 2^8a^5$.

El concepto de discriminante nos permite también asociar una norma a cada módulo completo:

Definición 1.14 Sea M un módulo completo en un cuerpo numérico K de grado n y $\mathcal{O}$ su anillo de coeficientes. Sea B una base de M y C una base de $\mathcal{O}$. Sea D_B^C la matriz cuyas filas son las coordenadas de B respecto de la base C. El teorema [Al 8.3] nos da entonces que $\Delta[M] = (\det D_B^C)^2\Delta[\mathcal{O}]$.

Definimos la *norma* de M como

$$\mathrm{N}(M) = |\det D_B^C| = \sqrt{\frac{\Delta[M]}{\Delta[\mathcal{O}]}}.$$

De este modo $\mathrm{N}(M)$ es un número racional positivo tal que

$$\Delta[M] = \mathrm{N}(M)^2\Delta[\mathcal{O}]. \tag{1.4}$$

Observemos que los órdenes tienen todos norma 1. También es obvio que si M está contenido en su anillo de coeficientes, entonces la matriz de cambio de base tiene coeficientes enteros racionales, luego $\mathrm{N}(M)$ es un entero racional, y de hecho todos los términos de la ecuación (1.4) son enteros racionales. En este caso la norma tiene una interpretación algebraica importante.

Teorema 1.15 *Sea M un módulo completo contenido en su anillo de coeficientes $\mathcal{O}$. Entonces $\mathrm{N}(M) = |\mathcal{O} : M|$.*

Demostración: Por [Al 4.53] existe una base $C = \{\alpha_1, \ldots, \alpha_n\}$ de $\mathcal{O}$ tal que para ciertos enteros racionales a_i se tiene que $B = \{a_1\alpha_1, \ldots, a_n\alpha_n\}$ es una base de M. La matriz D_B^C es en este caso particular una matriz diagonal, luego $\mathrm{N}(M) = |a_1 \cdots a_n|$.

El isomorfismo entre $\mathcal{O}$ y $\mathbb{Z}^n$ que envía C a la base canónica $\{e_1, \ldots, e_n\}$ de $\mathbb{Z}^n$, envía la base B a la base $\{a_1e_1, \ldots, a_ne_n\}$, luego envía M al módulo $a_1\mathbb{Z} \times \cdots \times a_n\mathbb{Z}$, y así

$$\mathcal{O}/M \cong (\mathbb{Z} \times \cdots \times \mathbb{Z})/(a_1\mathbb{Z} \times \cdots \times a_n\mathbb{Z}) \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}),$$

luego $|\mathcal{O} : M| = |(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z})| = |a_1| \cdots |a_n| = \mathrm{N}(M)$. ∎

Ahora es inmediato que esta definición de norma extiende a la definición [Al 8.33] de norma de un ideal del orden maximal de un cuerpo numérico.

Todo módulo es similar a uno en las condiciones del teorema anterior, y las normas de los módulos similares están relacionadas del modo siguiente:

Teorema 1.16 *Si M y αM son dos módulos completos similares, entonces $\mathrm{N}(\alpha M) = |\mathrm{N}(\alpha)|\,\mathrm{N}(M)$.*

Demostración: Sea $\{\beta_1, \ldots, \beta_n\}$ una base de M. Entonces $\{\alpha\beta_1, \ldots, \alpha\beta_n\}$ es una base de αM. Si $\sigma_1, \ldots, \sigma_n$ son los monomorfismos de K, tenemos que

$$\begin{aligned}\Delta[\alpha M] &= \Delta[\alpha\beta_1, \ldots, \alpha\beta_n] = \det\big(\sigma_i(\alpha\beta_j)\big)^2 = \det\big(\sigma_i(\alpha)\sigma_i(\beta_j)\big)^2\\ &= \mathrm{N}(\alpha)^2 \det\big(\sigma_i(\beta_j)\big)^2 = \mathrm{N}(\alpha)^2\Delta[\beta_1, \ldots, \beta_n] = \mathrm{N}(\alpha)^2\Delta[M].\end{aligned}$$

Como M y αM son similares, tienen el mismo anillo de coeficientes $\mathcal{O}$, luego $\mathrm{N}(\alpha M)^2\Delta[\mathcal{O}] = \Delta[\alpha M] = \mathrm{N}(\alpha)^2\Delta[M] = \mathrm{N}(\alpha)^2\,\mathrm{N}(M)^2\Delta[\mathcal{O}]$, y consecuentemente $\mathrm{N}(\alpha M) = |\mathrm{N}(\alpha)|\,\mathrm{N}(M)$. ∎

Ejercicio: Sea $\mathcal{O}$ el orden de un cuerpo numérico K y $\alpha \in \mathcal{O}$ no nulo. Probar que hay exactamente $|\,\mathrm{N}(\alpha)|$ clases de congruencia módulo α en $\mathcal{O}$.

Terminamos esta sección con una observación sobre la manipulación de enteros algebraicos:

Nota Al trabajar con enteros algebraicos podemos permitirnos simplificar los cálculos usando aproximaciones racionales sin más precaución que vigilar que los errores de redondeo no lleguen a media unidad, con lo que pueden ser compensados al final tomando el entero más próximo al resultado. Como ilustración consideremos una raíz α del polinomio $x^3 + 4x + 1$. Obviamente es un entero, luego también lo es $2+\alpha^2$. Supongamos que queremos conocer el polinomio mínimo de éste último. Una forma de hallarlo es buscar aproximaciones racionales de los tres conjugados de α, a saber:

$$\alpha_1 = -0.246266, \quad \alpha_2 = 0.123133 + 2.01134\ i, \quad \alpha_3 = 0.123133 - 2.01134\ i,$$

y después calcular

$$(x-2-\alpha_1^2)(x-2-\alpha_2^2)(x-2-\alpha_3^2) = x^3+2.00001x^2-4x-9.00003-2.1684\cdot 10^{-19}i.$$

Evidentemente el polinomio buscado es $\mathrm{pol\,mín}(2+\alpha^2) = x^3 + 2x^2 - 4x - 9$. Podríamos haber llegado al mismo resultado mediante un cálculo algebraico exacto, pero si disponemos de un ordenador esta técnica resulta mucho más rápida y eficiente. Se puede emplear igualmente para calcular normas, trazas, etc. Por ejemplo, para calcular la matriz $(\mathrm{Tr}(\alpha_i\alpha_j))$ de la forma bilineal asociada a la traza en la base $1, \alpha, \alpha^2$ calculamos, por ejemplo,

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = -8,00001$$

con lo que $\mathrm{Tr}(\alpha \cdot \alpha) = -8$. Similarmente se calculan las demás trazas, y el resultado es

$$A = \begin{pmatrix} 3 & 0 & -8 \\ 0 & -8 & 3 \\ -8 & 3 & 32 \end{pmatrix}.$$

El discriminante es $\Delta[\alpha] = -283$ y además

$$A^{-1} = \frac{1}{283}\begin{pmatrix} 265 & 24 & 64 \\ 24 & -32 & 9 \\ 64 & 9 & 24 \end{pmatrix}.$$

Esto nos da la base dual de la base $1, \alpha, \alpha^2$, que resulta ser

$$\frac{265}{283} + \frac{24}{283}\alpha + \frac{64}{283}\alpha^2, \quad \frac{24}{283} - \frac{32}{283}\alpha + \frac{9}{283}\alpha^2, \quad \frac{64}{283} + \frac{9}{283}\alpha + \frac{24}{283}\alpha^2.$$

■

1.3 Determinación de bases enteras

Nos ocupamos ahora del problema de calcular el orden maximal de un cuerpo numérico. En [Al 8.17] calculamos los órdenes maximales de los cuerpos cuadráticos. Vamos a recordar dicho cálculo a la vez que lo extendemos para determinar todos los órdenes cuadráticos, no necesariamente maximales:

Enteros cuadráticos Sea $K = \mathbb{Q}(\sqrt{d}\,)$ un cuerpo cuadrático, donde d es libre de cuadrados. El elemento primitivo $\sqrt{d}$ es obviamente un entero, que da lugar al orden $\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, una de cuyas bases es $\{1, \sqrt{d}\,\}$. Su discriminante vale

$$\Delta\left[\sqrt{d}\right] = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = \left(-2\sqrt{d}\right)^2 = 4d.$$

El teorema 1.13 nos da que Δ_K se diferencia de $4d$ en un cuadrado. Como d es libre de cuadrados, si $\mathbb{Z}[\sqrt{d}\,]$ no fuera el orden maximal éste tendría que tener discriminante d. Ahora bien, por el teorema 1.13 esto sólo puede ocurrir si $d \equiv 1 \pmod 4$, pues ciertamente, $4 \nmid d$.

Supongamos, pues, $d \equiv 1 \pmod 4$. Entonces el número $\alpha = (1 + \sqrt{d})/2$ cumple

$$\operatorname{pol\,mín} \alpha = x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x],$$

luego es un entero. El orden, $\mathbb{Z}[\alpha]$ tiene discriminante

$$\Delta[\alpha] = \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = \left(-\sqrt{d}\right)^2 = d.$$

Como d es libre de cuadrados concluimos que $\mathbb{Z}[\alpha]$ es en este caso el orden de K.

Si llamamos $\alpha = \sqrt{d}$ en el caso en que $d \not\equiv 1 \pmod 4$, hemos probado que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ en cualquier caso. Es inmediato que para cada número natural $m \neq 0$ el conjunto $\mathcal{O}_m = \mathbb{Z}[m\alpha] = \{a + bm\alpha \mid a, b \in \mathbb{Z}\}$ es un orden de K. Además $\Delta[\mathcal{O}_m] = m^2\Delta_K$, pues la matriz de cambio de base entre $\{1, \alpha\}$ y $\{1, m\alpha\}$ tiene determinante m. Esto prueba que los órdenes $\mathcal{O}_m$ son distintos dos a dos. Vamos a ver que son todos los órdenes de K. Lo probamos en el teorema siguiente, donde recogemos también los hechos que acabamos de demostrar.

Teorema 1.17 *Sea $K = \mathbb{Q}(\sqrt{d}\,)$ un cuerpo cuadrático. Entonces*

1. *$\mathcal{O}_K = \mathbb{Z}[\alpha]$, donde*

$$\alpha = \begin{cases} \sqrt{d} & \text{si } d \not\equiv 1 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4. \end{cases} \tag{1.5}$$

2. *El discriminante de K es*

$$\Delta_K = \begin{cases} 4d & \text{si } d \not\equiv 1 \pmod 4, \\ d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

3. Los órdenes de K son de la forma

$$\mathcal{O}_m = \mathbb{Z}[m\alpha] = \{a + bm\alpha \mid a, b \in \mathbb{Z}\}$$

y el discriminante de $\mathcal{O}_m$ es $\Delta[\mathcal{O}_m] = m^2\Delta_K$.

DEMOSTRACIÓN: Sólo falta probar que todos los órdenes de K son de la forma descrita.

Si $\mathcal{O}$ es un orden de K, sea m el mínimo natural tal que existe un elemento en $\mathcal{O}$ de la forma $a + m\alpha$, con $a \in \mathbb{Z}$. Como $\mathbb{Z} \subset \mathcal{O}$, tenemos que $m\alpha \in \mathcal{O}$, luego $\mathcal{O}_m \subset \mathcal{O}$.

Si $a + b\alpha \in \mathcal{O}$, entonces existen enteros racionales c y r tales que $b = mc + r$ y $0 \le r < m$. Claramente $(a + b\alpha) - (a + cm\alpha) = r\alpha \in \mathcal{O}$, luego por definición de m ha de ser $r = 0$, luego $a + b\alpha \in \mathcal{O}_m$ y se da la igualdad. ∎

Una consecuencia del teorema anterior es que los cuerpos cuadráticos definidos por diferentes valores de d son cuerpos distintos, pues tienen discriminantes distintos.

Ejercicio: Probar que el único orden de $\mathbb{Q}$ es $\mathbb{Z}$.

Ejercicio: Probar que, en un cuerpo cuadrático, el módulo $2\mathcal{O}_1$ es un ideal de $\mathcal{O}_2$ cuyo anillo de coeficientes es $\mathcal{O}_1$.

Volviendo al caso general, queda planteado el problema de decidir, dada una base de un cuerpo K formada por enteros, si es una base entera o si por el contrario existen bases con discriminantes menores. Una condición suficiente para el primer caso es, claramente, que el discriminante sea libre de cuadrados, pero esta condición no es necesaria, como muestran los cuerpos cuadráticos. El teorema siguiente proporciona un algoritmo para decidir cuál es el caso y obtener explícitamente una base con discriminante menor cuando ésta exista. Así siempre es posible hallar el orden de un cuerpo en un número finito de pasos, si bien hay que advertir que el proceso es demasiado laborioso para llevarlo a la práctica (por lo menos sin la ayuda de un ordenador) en la mayoría de los casos.

Teorema 1.18 *Sea K un cuerpo numérico y $M \subset \mathcal{O}_K$ un módulo completo con base $\{\alpha_1, \ldots, \alpha_n\}$. Si $M \neq \mathcal{O}_K$, entonces existe un número primo p tal que $p^2 \mid \Delta[M]$ y existen números naturales $1 \le t \le n$ y $g_1, \ldots, g_{t-1}$ tales que $0 \le g_i \le p-1$ de modo que*

$$\alpha_t^* = (g_1\alpha_1 + \cdots + g_{t-1}\alpha_{t-1} + \alpha_t)/p \in \mathcal{O}_K,$$

y si α_t^* es un número cualquiera que cumpla esto, entonces

$$M^* = \langle \alpha_1, \ldots, \alpha_{t-1}, \alpha_t^*, \alpha_{t+1}, \ldots, \alpha_n \rangle_{\mathbb{Z}}$$

es un módulo que contiene estrictamente a M y $\Delta[M^*] = \Delta[M]/p^2$.

DEMOSTRACIÓN: Sea $\{\beta_1,\dots,\beta_n\}$ una base de $\mathcal{O}_K$. Sea $\alpha_i = \sum_{j=1}^n m_{ij}\beta_j$, con $m_{ij}\in\mathbb{Z}$. Sea $m = \det(m_{ij})$. Entonces $\Delta[M] = m^2\Delta_K$ y $m \neq \pm 1$. Sea p un primo que divida a m.

Claramente existen $a_1,\dots,a_n \in \mathbb{Z}$ no todos nulos (mód p) de manera que $\sum_{i=1}^n a_i m_{ij} \equiv 0 \pmod p$. Sea t tal que $a_t \not\equiv 0 \pmod p$ pero $a_i \equiv 0 \pmod p$ para $i > t$.

Entonces $\gamma = \sum_{i=1}^t a_i\alpha_i = \sum_{i=1}^t \sum_{j=1}^n a_i m_{ij}\beta_j = \sum_{j=1}^n \left(\sum_{i=1}^t a_i m_{ij}\right)\beta_j$.

Tenemos que $p \mid \sum_{i=1}^n a_i m_{ij}$ y $p \mid \sum_{i=t+1}^n a_i m_{ij}$, luego $p \mid \sum_{i=1}^t a_i m_{ij}$ y por lo tanto $\gamma = p\beta$ para cierto $\beta\in\mathcal{O}_K$.

Sea $a^*\in\mathbb{Z}$ tal que $a_t a^* \equiv 1 \pmod p$. Definimos $p\alpha_t^* = a^*\gamma - p\gamma_0$, donde γ_0 se elige de modo que el coeficiente de α_t se reduzca a 1 y los de los α_i a sus mínimos (mód p), es decir, α_t^* es de la forma indicada en el enunciado y la matriz de cambio de base entre $\{\alpha_1,\dots,\alpha_n\}$ y $\{\alpha_1,\dots,\alpha_{t-1},\alpha_t^*,\alpha_{t+1},\dots,\alpha_n\}$ está formada por una diagonal de unos excepto la fila t-ésima, que es $(\frac{g_1}{p},\dots,\frac{g_{t-1}}{p},\frac{1}{p},0,\dots,0)$. El determinante es $1/p$, luego el discriminante de la segunda base es $\Delta[M]/p^2$. ∎

La prueba del teorema anterior muestra que en lugar de $0 \le g_i \le p-1$ podemos exigir que los g_i varíen en cualquier conjunto de representantes de las clases módulo p. A veces es cómodo tomarlos, por ejemplo, entre $-(p-1)/2$ y $(p-1)/2$.

El ejemplo de Dedekind Como aplicación del teorema anterior veamos un famoso ejemplo debido a Dedekind (más adelante veremos por qué es famoso). Es fácil ver que el polinomio x^3+x^2-2x+8 tiene una única raíz real, que no es entera (racional), y como es mónico concluimos que es irreducible en $\mathbb{Q}[x]$. Sea ξ una de sus raíces y consideremos el cuerpo cúbico $K = \mathbb{Q}(\xi)$. Vamos a calcular el orden y el discriminante de K.

Partimos del orden $\mathbb{Z}[\xi]$, cuyo discriminante vale, según el teorema [Al 8.19], $\Delta[\xi] = -\mathrm{N}(\alpha)$, donde $\alpha = 3\xi^2+2\xi-2$. Podemos hacer todos los cálculos tomando aproximaciones racionales de los conjugados de ξ, pero esta vez vamos a esbozar cómo se haría un cálculo algebraico exacto. Fácilmente obtenemos que

$$\alpha^2 = 7\xi^2 - 74\xi - 20 \quad \text{y} \quad \alpha^3 = 49\xi^2 - 518\xi + 1872.$$

Así pues, las coordenadas de los vectores $1,\alpha,\alpha^2,\alpha^3$ en la base $\xi^2,\xi,1$ son respectivamente $(0,0,1)$, $(3,2,-2)$, $(7,-74,-20)$ y $(49,-518,1872)$.

Por lo tanto todo se reduce a resolver el sistema de ecuaciones

$$p(7,-74,-20) + q(3,2,-2) + r(0,0,1) = (49,-518,1872),$$

cuyas soluciones son $p=7$, $q=0$, $r=2012$. Esto significa que $\alpha^3 = 7\alpha^2+2012$, luego $\operatorname{pol\,mín}\alpha = x^3-7x^2-2012$. El término independiente es el producto de los tres conjugados de α cambiados de signo, luego $\mathrm{N}(\alpha) = 2012 = 2^2\cdot 503$.

Concluimos que $\Delta[\xi] = -2^2 \cdot 503$. Según el teorema anterior cabe la posibilidad de que el 2 pueda ser eliminado. Esto será así si alguno de los siete números siguientes es entero:

$$\frac{1}{2}, \quad \frac{\xi}{2}, \quad \frac{1+\xi}{2}, \quad \frac{\xi^2}{2}, \quad \frac{\xi+\xi^2}{2}, \quad \frac{1+\xi^2}{2}, \quad \frac{1+\xi+\xi^2}{2}.$$

El lector puede demostrar que $\beta = \frac{\xi+\xi^2}{2}$ es entero calculando su polinomio mínimo por el mismo método con que hemos calculado el de α. Concretamente se obtiene

$$\operatorname{pol\,mín}\beta = x^3 - 2x^2 + 3x - 10.$$

El teorema anterior nos dice que $\Delta\left[1, \xi, \frac{\xi+\xi^2}{2}\right] = -503$, y como es libre de cuadrados, ha de ser el discriminante de K, o sea, $\mathcal{O}_K = \mathbb{Z}\left[\xi, \frac{\xi+\xi^2}{2}\right]$ y $\Delta_K = -503$. ∎

Ejercicio: Calcular el orden maximal y el discriminante del cuerpo $\mathbb{Q}(\zeta)$, donde ζ es una raíz del polinomio $x^3 - x - 1$.

Ejercicio: Sean K_1, K_2 y K_3 los cuerpos que resultan de adjuntar a $\mathbb{Q}$ una raíz de los polinomios

$$x^3 - 18x - 6, \quad x^3 - 36x - 78, \quad \text{o} \quad x^3 - 54x - 150$$

respectivamente. Probar que los tres tienen discriminante $\Delta = 2^2 \cdot 3^5 \cdot 23$.

Cuerpos cúbicos puros Introducimos ahora una nueva familia de cuerpos numéricos que proporcionan numerosos ejemplos de interés.

Definición 1.19 Un *cuerpo cúbico puro* es un cuerpo numérico de la forma $\mathbb{Q}\big(\sqrt[3]{m}\,\big)$, donde m es un entero racional que no sea un cubo perfecto (en particular distinto de 0 y de ± 1).

Hay que señalar que, al contrario de lo que ocurre con los cuerpos cuadráticos, no todo cuerpo cúbico es de este tipo, el ejemplo de Dedekind que acabamos de estudiar no lo es.

Tenemos que $\sqrt[3]{m}$ es un número real y $\operatorname{pol\,mín}\sqrt[3]{m} = x^3 - m$. Si llamamos ω a una raíz cúbica primitiva de la unidad (una raíz de $x^2 + x + 1$) es claro que las otras raíces de $x^3 - m$ son los números imaginarios $\omega\sqrt[3]{m}$ y $\omega^2\sqrt[3]{m}$. Esto significa que los monomorfismos del cuerpo $\mathbb{Q}\big(\sqrt[3]{m}\,\big)$ son la identidad y las conjugaciones dadas por $\sigma_1\big(\sqrt[3]{m}\,\big) = \omega\sqrt[3]{m}$, $\sigma_2\big(\sqrt[3]{m}\,\big) = \omega^2\sqrt[3]{m}$. Observemos que los conjugados de $\sqrt[3]{m}$ no están en $\mathbb{Q}\big(\sqrt[3]{m}\,\big)$, o equivalentemente, que los monomorfismos no son automorfismos, o que la extensión no es de Galois.

Podemos exigir que m no sea divisible entre ningún cubo perfecto, pues un factor cúbico puede extraerse de la raíz y eliminarse sin que el cuerpo generado varíe. Entonces, si p es un divisor primo de m, el exponente de p en m ha de ser 1 o 2. Sea a el producto de los primos que dividen a m con exponente 1 y b el producto de los primos que dividen a m con exponente 2. Entonces $m = ab^2$, $(a, b) = 1$ y a, b son libres de cuadrados.

Notemos también que el signo de m es irrelevante, pues el -1 puede introducirse y extraerse de la raíz, y al multiplicar el generador por -1 no variamos el cuerpo. Por ello podríamos exigir que m, a y b fueran todos positivos, pero no vamos a hacer tal cosa, sino que de momento dejaremos los signos indeterminados para escogerlos más adelante del modo más conveniente para los cálculos.

Para calcular el orden maximal de un cuerpo cúbico partimos del orden $\mathbb{Z}\big[\sqrt[3]{ab^2}\,\big]$, con base $1, \sqrt[3]{ab^2}, \big(\sqrt[3]{ab^2}\,\big)^2 = b\sqrt[3]{a^2b}$, pero observamos inmediatamente que salvo en el caso $b = \pm1$ no puede tratarse del orden del cuerpo, ya que no contiene al entero $\sqrt[3]{a^2b}$.

Por ello pasamos a la base $1, \theta_1, \theta_2$, donde $\theta_1 = \sqrt[3]{ab^2}$, $\theta_2 = \sqrt[3]{a^2b}$. Los cálculos se simplifican bastante si observamos la simetría entre θ_1 y θ_2, en el sentido de que se cumple $\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2)$, $\theta_1^2 = b\theta_2$, $\theta_2^2 = a\theta_1$. Estas fórmulas nos dan la acción de las conjugaciones sobre θ_1 y θ_2, a saber

$$\sigma_1(\theta_1) = \omega\theta_1, \quad \sigma_1(\theta_2) = \omega^2\theta_2, \quad \sigma_2(\theta_1) = \omega^2\theta_1, \quad \sigma_2(\theta_2) = \omega\theta_2.$$

Con ello y un poco de paciencia podemos calcular

$$\Delta[1,\theta_1,\theta_2] = \begin{vmatrix} 1 & \theta_1 & \theta_2 \\ 1 & \omega\ \theta_1 & \omega^2\theta_2 \\ 1 & \omega^2\theta_1 & \omega\ \theta_2 \end{vmatrix}^2 = -27a^2b^2.$$

Teorema 1.20 *Sea $K = \mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2)$ un cuerpo cúbico puro según la definición anterior. Entonces una base entera de K la forman $\theta_0, \theta_1, \theta_2$, donde $\theta_0 = 1$ si $a \not\equiv \pm b$* (mód 9) *(y entonces $\Delta_K = -27a^2b^2$) y $\theta_0 = (1+\theta_1+\theta_2)/3$ si $a \equiv \pm b$* (mód 9) *(y entonces $\Delta_K = -3a^2b^2$). En el segundo caso hay que escoger los signos de a y b de manera que $a \equiv b$* (mód 9) *y su resto módulo 9 sea 1, 4 o 7.*

Demostración: Vamos a aplicar el teorema 1.18 a la base $1, \theta_1, \theta_2$. En primer lugar demostraremos que no es posible eliminar ningún primo p que divida a ab. Supongamos, por ejemplo, que $p \mid a$. Si p se pudiera eliminar existiría un entero de la forma $\alpha = (u + v\theta_1 + \theta_2)/p$, o bien $\alpha = (u + \theta_1)/p$, donde u y v son enteros racionales entre 0 y $p-1$. Trataremos la primera posibilidad. La segunda es más sencilla.

Sea $\pi = \sqrt[3]{p}$ y $L = K(\pi)$. Tenemos que $ab^2 = pk$, para cierto entero racional k, luego tomando raíces $\theta_1 = \pi\beta$, donde $\beta = \sqrt[3]{k} \in L$ y es un entero. Así pues, $\pi \mid \theta_1$ en $\mathcal{O}_L$. El mismo argumento nos da que $\pi^2 \mid \theta_2$ en $\mathcal{O}_L$, y por otro lado $\pi^3\alpha = u + v\theta_1 + \theta_2$.

De aquí se sigue que $\pi \mid u$ en $\mathcal{O}_L$. Elevando al cubo, $p \mid u^3$ en $\mathcal{O}_L$ y el cociente es entero y racional, o sea, $p \mid u^3$ en $\mathbb{Z}$, de donde $p \mid u$ y ha de ser $u = 0$.

Consecuentemente $\pi^2 \mid v\theta_1$ en $\mathcal{O}_L$, y como antes llegamos a que $p^2 \mid v^3ab^2$ en $\mathbb{Z}$, de donde haciendo uso de que $p \mid a$, $(a,b) = 1$ y que a y b son libres de cuadrados, resulta que $p \mid v$, luego $v = 0$.

Ahora concluimos que $p \mid \theta_2$ en $\mathcal{O}_L$, luego $p^3 \mid a^2b$ en $\mathbb{Z}$, lo cual es contradictorio.

En consecuencia los primos que dividen a ab no pueden eliminarse. La única posibilidad es eliminar el 3, para lo cual es necesario que no divida a ab. Supongámoslo así. Según el teorema 1.18 hemos de comprobar los siguientes números (para aprovechar la simetría ordenamos la base en la forma $\theta_1, \theta_2, 1$):

$$\frac{\theta_1}{3}, \quad \frac{\theta_2}{3}, \quad \frac{\pm\theta_1+\theta_2}{3}, \quad \frac{1}{3}, \quad \frac{\pm\theta_1+1}{3}, \quad \frac{\pm\theta_2+1}{3}, \quad \frac{\pm\theta_1\pm\theta_2+1}{3}.$$

Notemos que hemos tomado como representantes de las clases módulo 3 los números -1, 0, 1 en lugar de 0, 1, 2 (véase el comentario tras el teorema 1.18).

Haciendo uso de la simetría y de que podemos elegir el signo de a y b sin cambiar de cuerpo, podemos limitarnos a estudiar los números

$$\frac{\theta_1}{3}, \quad \frac{\theta_1+\theta_2}{3}, \quad \frac{1+\theta_1}{3}, \quad \frac{1+\theta_1+\theta_2}{3}.$$

Por ejemplo, si $(-\theta_1+\theta_2)/3$ pudiera ser entero, también lo sería $(\theta_1+\theta_2)/3$ (tomando $-a$ en lugar de a), mientras que vamos a probar que $(\theta_1+\theta_2)/3$ no es entero para ningún valor de a y b, luego lo mismo ocurrirá con $(-\theta_1+\theta_2)/3$. De hecho vamos a ver que $\theta_1/3$, $(\theta_1+\theta_2)/3$, $(1+\theta_1)/3$ nunca son enteros.

Claramente $\operatorname{pol\,mín}(\theta_1/3) = x^3 - ab^2/3$, y $ab^2/3$ no es entero porque suponemos que $3 \nmid ab$. Con un poco más de cálculo se llega a

$$\begin{aligned}\operatorname{pol\,mín}\frac{1+\theta_1}{3} &= x^3 - x^2 + \frac{1}{3}x - \frac{1+ab^2}{27},\\ \operatorname{pol\,mín}\frac{\theta_1+\theta_2}{3} &= x^3 - \frac{ab}{3}x - \frac{ab^2+a^2b}{27},\end{aligned}$$

que obviamente no tienen coeficientes enteros.

Así pues, todo depende de $(1+\theta_1+\theta_2)/3$. Se puede comprobar que

$$\operatorname{pol\,mín}\frac{1+\theta_1+\theta_2}{3} = x^3 - x^2 + \frac{1-ab}{3}x - \frac{1+ab^2+a^2b-3ab}{27}.$$

Demostraremos que los coeficientes pueden hacerse enteros (escogiendo signos) exactamente cuando $a \equiv \pm b \pmod 9$, de donde se concluye inmediatamente el teorema.

Supongamos que $a \equiv \pm b \pmod 9$. Cambiando el signo a b si es preciso, podemos exigir $a \equiv b \pmod 9$. El resto no puede ser 0 ni ± 3, pues en tal caso 3 dividiría a $(a,b) = 1$. De aquí se sigue que $ab \equiv 1, 4, 7 \pmod 9$, y por lo tanto $3 \mid (1-ab)$.

Cambiando el signo a ambos enteros podemos exigir que su resto módulo 9 sea 1, 4 o 7, es decir, que $a = 9k+i$, $b = 9r+i$, donde i puede tomar el valor 1, 4 o 7. Sustituyendo en $1+ab^2+a^2b-3ab$ se obtiene que es múltiplo de 27 en cualquiera de los tres casos.

Supongamos ahora que los coeficientes del polinomio mínimo son enteros, es decir, que

$$3 \mid (1-ab), \tag{1.6}$$

$$27 \mid (1+ab^2+a^2b-3ab). \tag{1.7}$$

De (1.6) se sigue que

$$a \equiv b \equiv \pm 1 \text{ (mód 3)}. \tag{1.8}$$

El lector puede comprobar que los únicos valores posibles para los restos módulo 9 de a y b (salvo el orden, que por simetría no importa) que incumplen la condición $a \equiv \pm b$ (mód 9) pero que cumplen (1.8) son $(1,4)$, $(1,7)$, $(2,5)$, $(2,8)$, $(4,7)$, $(5,8)$. En ninguno de estos casos se cumple (1.7). ∎

La tabla siguiente resume el teorema:

Tabla 1.1: Tipos de cuerpos cúbicos puros

	Condición	Δ_K	θ_0	θ_1	θ_2
Tipo I	$a \not\equiv \pm b$ (mód 9)	$-27a^2b^2$	1	$\sqrt[3]{ab^2}$	$\sqrt[3]{a^2b}$
Tipo II	$a \equiv b \equiv 1 + 3t$ (mód 9)	$-3a^2b^2$	$(1+\theta_1+\theta_2)/3$	$\sqrt[3]{ab^2}$	$\sqrt[3]{a^2b}$

Ejercicio: Probar que el orden de $\mathbb{Q}\big(\sqrt[3]{6}\,\big)$ es $\mathbb{Z}\Big[\sqrt[3]{6}\,\Big]$.

Ejercicio: Probar que el anillo de coeficientes del módulo $M = \langle 4, \sqrt[3]{2}, \sqrt[3]{4}\,\rangle$ es igual a $\langle 1, 2\sqrt[3]{2}, 2\sqrt[3]{4}\,\rangle$.

Cuerpos ciclotómicos En [Al 8.18] probamos que si p es primo y ω es una raíz p-ésima primitiva de la unidad, entonces el orden maximal del cuerpo ciclotómico $K = \mathbb{Q}(\omega)$ es $\mathbb{Z}[\omega]$, y en [Al 8.20] vimos que $\Delta_K = (-1)^{(p-1)/2}p^{p-2}$.

Respecto a los cuerpos ciclotómicos de orden arbitrario, nos ocuparemos de ellos en 9.44. De momento nos conformaremos con el hecho siguiente:

Teorema 1.21 *Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de orden m (donde ω es una raíz m-sima primitiva de la unidad). Si p es un primo que no divide a m, entonces tampoco divide al discriminante $\Delta[\omega]$.*

Demostración: Sea $n = \phi(m)$. Según se observa tras la definición [Al 8.2], se cumple que

$$\Delta[\omega] = \prod_{1\le i<j\le n} \big(\sigma_i(\omega) - \sigma_j(\omega)\big)^2, \tag{1.9}$$

donde los números $\sigma_i(\omega)$ son las raíces del polinomio ciclotómico $p(x)$, es decir

$$p(x) = \prod_{i=1}^{n} \big(x - \sigma_i(\omega)\big).$$

Sea $\mathcal{O}$ el orden maximal de K y sea $\mathfrak{p}$ un ideal maximal de $\mathcal{O}$ que contenga a p. Sea $L = \mathcal{O}/\mathfrak{p}$. Entonces L es un cuerpo de característica p en el que el polinomio ciclotómico factoriza como

$$p(x) = \prod_{i=1}^{n} \big(x - [\sigma_i(\omega)]\big),$$

donde los corchetes [ ] indican clases módulo $\mathfrak{p}$. Tomando también clases en (1.9) tenemos que

$$[\Delta] = \prod_{1\le i<j\le n} \big([\sigma_i(\omega)] - [\sigma_j(\omega)]\big)^2.$$

Ahora bien, como $p \nmid m$, el polinomio $x^m - 1$ tiene derivada $mx^{m-1} \neq 0$ en $L[x]$, luego tiene m raíces distintas en L, y por consiguiente el polinomio ciclotómico tiene n raíces distintas en L. Consecuentemente $[\Delta] \neq 0$, es decir, que $\Delta \notin \mathfrak{p}$, luego ciertamente $p \nmid \Delta$. ∎

Veamos un ejemplo concreto:

El cuerpo ciclotómico octavo Consideremos el cuerpo ciclotómico octavo $\mathbb{Q}(\omega)$. Su grado es 4 y, de hecho, $\operatorname{pol\,mín}\omega = x^4 + 1$. El teorema [Al 8.19] nos da que el discriminante del orden $\mathbb{Z}[\omega]$ es 256. Vamos a probar que no es posible eliminar ningún 2.

Según el teorema 1.18, aplicado a la base $1, \omega, \omega^2, \omega^3$, hemos de probar que no son enteros un total de 15 números. Descartamos inmediatamente $1/2$, $\omega/2$, $\omega^2/2$ y $\omega^3/2$, que tienen norma $1/4$.

Si $(\omega + \omega^2)/2 = \omega(1 + \omega)/2$ fuera entero también lo sería $(1 + \omega)/2$, luego basta comprobar el segundo. Por este argumento eliminamos cuatro números más, y nos quedan

$$\frac{1+\omega}{2}, \frac{1+\omega^2}{2}, \frac{1+\omega^3}{2}, \frac{1+\omega+\omega^2}{2}, \frac{1+\omega+\omega^3}{2}, \frac{1+\omega^2+\omega^3}{2}, \frac{1+\omega+\omega^2+\omega^2}{2}.$$

Notemos que $(1+\omega^2)/2 = (1+i)/2$, luego no es entero. Para descartar a los restantes observamos que $x^4+1 = (x-\omega)(x-\omega^3)(x-\omega^5)(x-\omega^7)$, y evaluando en 1 concluimos que $1-\omega$ y $1-\omega^3$ tienen norma 2.

Ahora, si $\alpha = (1+\omega)/2$ fuera entero, también lo sería $-\omega^3\alpha = (1-\omega^3)/2$, pero tiene norma $1/2$. El número $(1+\omega^3)/2$ es conjugado del anterior, luego tampoco es entero.

Respecto a

$$\frac{1+\omega+\omega^2}{2} = \frac{\omega^3-1)}{2(\omega-1)} \quad \text{y} \quad \frac{1+\omega+\omega^2+\omega^3}{2} = \frac{\omega^4-1}{2(\omega-1)} = -\frac{2}{2(\omega-1)},$$

vemos que también tienen norma fraccionaria.

Por último, si el número $\alpha = (1+\omega+\omega^3)/2$ fuera entero, también lo sería $\omega\alpha + 1 = (1+\omega+\omega^2)/2$, que ya ha sido descartado, e igualmente se razona con $\omega^2(1+\omega^2+\omega^3)/2 + 1 + \omega = (1+\omega+\omega^2)/2$. ∎

Enteros ciclotómicos reales Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de orden p. En el estudio de K resulta de gran ayuda considerar el cuerpo intermedio $K' = K \cap \mathbb{R}$. Claramente K' es el cuerpo fijado por la conjugación compleja, que es un automorfismo de orden 2, luego $|K : K'| = 2$ y por consiguiente el grado de K' es $m = (p-1)/2$. Un entero de K' es en particular un entero de K,

luego se expresará como combinación lineal entera de $\omega, \dots, \omega^{p-1}$. Como ha de quedar fijo por la conjugación compleja es necesario que el coeficiente de cada potencia ω^i coincida con el de ω^{-i}, lo que implica que los enteros de K' son combinaciones lineales enteras de los números $\eta_i = \omega^i + \omega^{-i}$. El recíproco es obvio, luego en definitiva el orden maximal de K' es el anillo $\mathbb{Z}[\eta_1, \dots, \eta_m]$.

Vamos a calcular el discriminante $\Delta_{K'} = \Delta[\eta_1, \dots, \eta_m] = \det\big(\mathrm{Tr}(\eta_i\eta_j)\big)$. Para ello notamos que

$$\eta_i\eta_j = (\omega^i + \omega^{-i})(\omega^j + \omega^{-j}) = \omega^{i+j} + \omega^{-i-j} + \omega^{i-j} + \omega^{j-i} = \eta_{i+j} + \eta_{i-j},$$

donde usamos la notación η_i para todo i, no necesariamente entre 1 y m.

Por otra parte es claro que $\mathrm{Tr}(\eta_i) = \eta_1 + \ldots + \eta_m = -1$ si $p \nmid i$, mientras que $\mathrm{Tr}(\eta_i) = \mathrm{Tr}(2) = 2m = p - 1$ si $p \mid i$.

Cuando i, j varían entre 1 y m observamos que $i + j$ nunca es divisible entre p, mientras que $p \mid i - j$ sólo cuando $i = j$. Por lo tanto

$$\mathrm{Tr}(\eta_i\eta_j) = -1 + \mathrm{Tr}(\eta_{i-j}) = \begin{cases} p-2 & \text{si } i = j, \\ -2 & \text{si } i \neq j. \end{cases}$$

Hay que calcular el determinante de una matriz de orden $(p-1)/2$ que tiene los coeficientes de la diagonal principal iguales a $p-2$ y los restantes iguales a -2. Si sumamos todas las columnas a la primera hacemos que todos los coeficientes de la primera columna valgan 1. Si restamos la primera fila de todas las demás llegamos a una matriz diagonal cuya diagonal principal contiene los coeficientes $(1, p, \dots, p)$. El discriminante es, por lo tanto, $\Delta_{K'} = p^{m-1}$. ∎

Como ejemplo concreto consideremos el caso $p = 7$. Entonces K' es un cuerpo cúbico, y una base entera la forman los números η_1, η_2, η_3. Puesto que $\eta_1 + \eta_2 + \eta_3 = -1$ podemos cambiarla por 1, η_1, η_2.

Además $\eta_1^2 = (\omega + \omega^6)^2 = \omega^2 + \omega^5 + 2 = \eta_2 + 2$. Por consiguiente, si llamamos $\eta = \eta_1$ tenemos que $K' = \mathbb{Q}(\eta)$ y que una base entera viene dada por $\{1, \eta, \eta^2 - 2\}$. (Notemos que no sirve $\{1, \eta, \eta^2\}$)

Si tomamos $\omega = \cos(2\pi/7) + i\,\mathrm{sen}(2\pi/7)$, entonces $\eta = 2\cos(2\pi/7)$, y sus conjugados son $2\cos(4\pi/7)$ y $2\cos(6\pi/7)$. Aproximadamente valen

$$\eta_1 = -1.246979604, \quad \eta_2 = -0.4450418670, \quad \eta_3 = -1.801937736.$$

Con esto podemos calcular $\mathrm{pol\,mín}\,\eta = x^3 + x^2 - 2x - 1$, la matriz asociada a la traza:

$$\begin{pmatrix} 3 & -1 & -1 \\ -1 & 5 & -2 \\ -1 & -2 & 5 \end{pmatrix}$$

y el discriminante de K, que, como ya sabíamos, es $\Delta_K = 7^2$. ∎

Cuerpos cúbicos cíclicos Según la teoría de Galois, un cuerpo $K = \mathbb{Q}(\alpha)$ es normal si y sólo si los conjugados de α pertenecen a K. Si K es un cuerpo cúbico esto implica que su grupo de Galois tiene tres elementos y es, por lo tanto, un grupo cíclico. En caso contrario la clausura normal de K ha de tener grado 6 sobre $\mathbb{Q}$, y el grupo de Galois ha de ser isomorfo al grupo de permutaciones Σ_3. Es claro que el cuerpo cúbico del ejemplo anterior es cíclico. Aquí probaremos un resultado general que los caracteriza[1]:

Teorema 1.22 *Un cuerpo cúbico es cíclico si y sólo si su discriminante es un cuadrado perfecto.*

Demostración: Sea $K = \mathbb{Q}(\alpha)$ un cuerpo cúbico, donde α es un entero, y sean $\alpha_1, \alpha_2, \alpha_3$ los conjugados de α. Observemos que el discriminante de K será un cuadrado perfecto si y sólo si lo es $\Delta = \Delta[\alpha]$, pues ambos se diferencian en un factor cuadrado perfecto. A su vez, éste será un cuadrado perfecto si y sólo si $\sqrt{\Delta} = |\alpha_i^j|$ es (entero) racional.

Si K es cíclico entonces $\sqrt{\Delta} \in K$, luego $\mathbb{Q}\big(\sqrt{\Delta}\,\big)$ no puede ser un cuerpo cuadrático (pues está contenido en K), y en consecuencia $\sqrt{\Delta} \in \mathbb{Q}$.

Si por el contrario K no es cíclico, entonces el grupo de Galois de la clausura normal de K contiene 6 automorfismos que permutan los conjugados de α de todos los modos posibles. En particular existe un automorfismo σ que deja fijo a α_3 e intercambia α_1 y α_2. Es claro entonces que $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$, pues σ permuta dos columnas del determinante, con lo que $\sqrt{\Delta} \notin \mathbb{Q}$. ∎

1.4 Índices

Veamos ahora un último concepto de utilidad en el estudio de los cuerpos numéricos:

Definición 1.23 Sea K un cuerpo numérico y sea $\mathcal{O}_K$ su orden maximal. Si $\mathcal{O}$ es cualquier orden de K, llamaremos índice de $\mathcal{O}$ al único número natural $\operatorname{índ}\mathcal{O}$ tal que

$$\Delta[\mathcal{O}] = (\operatorname{índ}\mathcal{O})^2 \Delta_K. \tag{1.10}$$

Concretamente $\operatorname{índ}\mathcal{O}$ es el valor absoluto del determinante de la matriz de cambio de base entre una base de $\mathcal{O}$ y una base entera de K. El mismo argumento empleado en la prueba del teorema 1.15 nos da que

$$\operatorname{índ}\mathcal{O} = |\mathcal{O}_K : \mathcal{O}|.$$

En particular, si $K = \mathbb{Q}(\alpha)$ y α es entero, definimos $\operatorname{índ}\alpha = \operatorname{índ}\mathbb{Z}[\alpha]$.

Vamos a calcular los índices de los elementos de algunos cuerpos numéricos. Para un cuerpo cuadrático $\mathbb{Q}\big(\sqrt{d}\,\big)$, cuando $d \not\equiv 1 \pmod 4$ tenemos que una base

[1] En realidad este teorema es un caso particular de [Al 7.12], ya que, para polinomios mónicos irreducibles, el discriminante de un polinomio según [Al 7.9] coincide con el discriminante de cualquiera de sus raíces (por la fórmula previa a [Al 8.3]).

del anillo $\mathbb{Z}\big[a+b\sqrt{d}\,\big]$ es $1, a+b\sqrt{d}$, mientras que una base del orden maximal es $1, \sqrt{d}$, luego el determinante de la matriz del cambio de base es

$$\begin{vmatrix} 1 & 0 \\ a & b \end{vmatrix} = b.$$

Por lo tanto $\text{índ}\big(a+b\sqrt{d}\,\big) = |b|$.

Si $d \equiv 1 \pmod 4$ los enteros son de la forma $\big(a+b\sqrt{d}\,\big)/2$, con $a \equiv b \pmod 2$, y el índice vale igualmente

$$\text{índ}\left(\frac{a+b\sqrt{d}}{2}\right) = \text{abs}\begin{vmatrix} 1 & 0 \\ \frac{a-b}{2} & b \end{vmatrix} = |b|.$$

Ahora consideramos un cuerpo cúbico puro $\mathbb{Q}\big(\sqrt[3]{ab^2}\,\big)$. Primeramente supongamos que es de tipo I, es decir, $a \not\equiv b \pmod 9$. Usamos la notación del teorema 1.20. Una base del orden $\mathbb{Z}[x+y\theta_1+z\theta_2]$ está formada por

$$1, \quad x+y\theta_1+z\theta_2, \quad (x+y\theta_1+z\theta_2)^2 = x^2+2yzab+(z^2a+2xy)\theta_1+(y^2b+2xz)\theta_2.$$

Así pues,

$$\text{índ}(x+y\theta_1+z\theta_2) = \text{abs}\begin{vmatrix} 1 & 0 & 0 \\ x & y & z \\ x^2+2yzab & z^2a+2xy & y^2b+2xz \end{vmatrix} = |by^3-az^3|.$$

Si el cuerpo es de tipo II un entero es de la forma $(x+y\theta_1+z\theta_2)/3$, donde $x \equiv y \equiv z \pmod 3$. El lector puede comprobar sin dificultad que ahora

$$\text{índ}\left(\frac{x+y\theta_1+z\theta_2}{3}\right) = \frac{1}{9}|by^3-az^3|.$$

Los anillos de la forma $\mathbb{Z}[\alpha]$ se llaman *anillos numéricos* (de aquí procede el uso de la palabra anillo en su sentido algebraico, haciendo referencia a que las potencias de α se reducen cíclicamente). Los órdenes maximales de los cuerpos cuadráticos son anillos numéricos, pero no ocurre lo mismo en todos los cuerpos numéricos. Por ejemplo, en $\mathbb{Q}\big(\sqrt[3]{63}\,\big)$ el orden maximal sería de la forma $\mathbb{Z}[\alpha]$ si y sólo si $\text{índ}\,\alpha = 1$ para algún número α, pero es imposible que $3y^3-7z^3 = \pm 1$, ya que no hay solución módulo 7.

Finalmente calculamos el índice de los enteros del ejemplo de Dedekind $\mathbb{Q}(\xi)$ que hemos estudiado en la sección anterior. El método que usaremos será el mismo.

Un entero arbitrario es de la forma $\alpha = x+y\xi+z(\xi+\xi^2)/2$. Un simple cálculo nos da que

$$\alpha^2 = x^2-8yz-2z^2+(2xy+xz-3z^2/2+2yz)\xi+(xz+y^2+z^2/2)\xi^2.$$

Tenemos las coordenadas de la base $1, \alpha, \alpha^2$ de $\mathbb{Z}[\alpha]$ en la base $1, \xi, \xi^2$ de $\mathbb{Q}(\xi)$, al igual que las de la base $1, \xi, (\xi+\xi^2)/2$ del orden maximal. Resolviendo

un sistema de tres ecuaciones lineales obtenemos la matriz del cambio de base, que resulta ser

$$\begin{pmatrix} 1 & 0 & 0 \\ x & y & z \\ x^2 - 8yz - 2z^2 & 2xy - 2z^2 + 2yz - y^2 & 2xz + 2y^2 + z^2 \end{pmatrix},$$

de donde $\text{índ}\,\alpha = |2y^3 + 2z^3 - yz^2 + zy^2|$.

Observamos que el orden maximal de $\mathbb{Q}(\xi)$ no es tampoco un anillo numérico, pues el índice de cualquier entero es siempre un número par.

%enddocument

Capítulo II

Factorización ideal

En la sección [Al 8.4] vimos que los órdenes maximales de los cuerpos numéricos, aunque en la mayor parte de los casos no son dominios de factorización única, tienen factorización única ideal, y ésta es suficiente para demostrar muchos resultados aritméticos. Los anillos en los que se da esta factorización única ideal, es decir, los dominios íntegros en los que todo ideal no nulo ni unitario se descompone de forma única salvo el orden en producto de ideales primos[1], son los llamados dominios de Dedekind [Al 8.26].

Recordemos [Al 8.27] que si D es un dominio íntegro con cuerpo de cocientes K, los ideales fraccionales de D son los D-submódulos de K de la forma $\mathfrak{a} = c^{-1}\mathfrak{b}$, donde $\mathfrak{b}$ es un ideal no nulo de D y $c \in D$ también es no nulo. En particular, todo ideal no nulo de D es un ideal fraccional.

Un resultado fundamental [Al 8.29] es que si D es un dominio de Dedekind, entonces los ideales fraccionales forman un grupo con el producto dado por

$$\mathfrak{ab} = \{\sum_{i=1}^{n} p_i q_i \mid n \in \mathbb{N} \text{ y } p_i \in \mathfrak{a}, q_i \in \mathfrak{b} \text{ para } i = 1, \ldots, n\}.$$

El inverso de un ideal no nulo viene dado por

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset D\}.$$

Todo ideal fraccional es cociente de ideales, y entonces la unicidad de las descomposiciones en primos implica que todo ideal fraccional no unitario de un dominio de Dedekind se expresa de forma única salvo el orden como

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r},$$

donde los $\mathfrak{p}_i$ son ideales primos distintos y los exponentes n_i son enteros no nulos. Esto equivale a que el grupo de los ideales fraccionales es es $\mathbb{Z}$-módulo libre que tiene por base a los ideales primos (aunque la notación que empleamos es multiplicativa, de modo que la "suma" del módulo es el producto y el producto por un entero es la exponenciación).

[1] Cuando hablemos de ideales primos de un dominio de Dedekind se sobreentenderá que nos referimos a primos no nulos.

En el caso en que D es el orden maximal $\mathcal{O}_K$ de un cuerpo numérico K, es claro que los ideales fraccionales de $\mathcal{O}_K$ son los módulos similares a un ideal de $\mathcal{O}_K$, o, por el teorema 1.8, los módulos cuyo anillo de coeficientes es $\mathcal{O}_K$.

El teorema [Al 8.37] se puede aplicar en muchos casos para determinar cómo se descomponen en $\mathcal{O}_K$ los primos racionales, pero a la hora de estudiar cuerpos numéricos relativamente "grandes", resulta muy útil considerar extensiones intermedias $\mathbb{Q} \subset L \subset K$ y tener información, no sólo de cómo los primos de $\mathbb{Z}$ factorizan en $\mathcal{O}_L$ y en $\mathcal{O}_K$, sino también de cómo los primos de $\mathcal{O}_L$ factorizan en $\mathcal{O}_K$. Sin embargo, con la teoría que conocemos de [Al], ni siquiera está claro a qué nos referimos cuando hablamos de la factorización en $\mathcal{O}_K$ de un ideal primo de $\mathcal{O}_L$.

Por ello, en este capítulo vamos a desarrollar una teoría general de extensiones de dominios de Dedekind E/D que nos relacione la aritmética de ambos sin necesidad de que el dominio base sea precisamente $D = \mathbb{Z}$. Esto es posible en gran medida porque los dominios de Dedekind admiten una caracterización algebraica muy simple [Al 8.32]. Un dominio íntegro D es un dominio de Dedekind si y sólo si cumple tres propiedades:

1. es noetheriano,
2. los ideales primos no nulos de D son maximales,
3. si un elemento b del cuerpo de cocientes de D es raíz de un polinomio mónico con coeficientes en D, entonces $b \in D$.

Dedicaremos la primera sección a estudiar con más detalle las propiedades 1 y 3, así como a introducir el concepto de localización, con todo lo cual en las secciones siguientes podremos desarrollar la teoría general de extensiones de dominios de Dedekind y aplicarla al caso de los cuerpos numéricos.

2.1 Preliminares algebraicos

Anillos y módulos noetherianos Ya conocemos de [Al 3.6] el concepto de anillo noetheriano, pero conviene extender la definición a módulos en lugar de anillos y generalizar a este contexto las propiedades básicas.

Definición 2.1 Sea A un anillo y M un A-módulo. Se dice que M es *noetheriano* si todos sus submódulos son finitamente generados.

Un anillo A es *noetheriano* si lo es como A-módulo, es decir, si todos sus ideales son finitamente generados. En particular todo dominio de ideales principales es noetheriano.

El teorema siguiente generaliza al caso de módulos el teorema [Al 3.7]:

Teorema 2.2 *Sea A un anillo y M un A-módulo. Las siguientes afirmaciones son equivalentes:*

1. *M es noetheriano.*
2. *Toda sucesión creciente de submódulos*

$$M_0 \subset M_1 \subset M_2 \subset M_3 \subset \cdots$$

es finalmente constante.

3. *Toda familia no vacía de submódulos de M tiene un elemento maximal respecto a la inclusión.*

DEMOSTRACIÓN: 1) $\Rightarrow$ 2) La unión de todos los módulos M_i es un submódulo de M, luego tiene un generador finito, que estará contenido en alguno de los módulos M_{i_0}. Entonces $M = M_{i_0}$ y por lo tanto $M = M_i$ para todo $i \geq i_0$.

2) $\Rightarrow$ 3) Si existiera una familia de submódulos sin maximal podríamos tomar un módulo cualquiera M_0, que al no ser maximal estaría estrictamente contenido en otro módulo M_1 de la familia, que estaría contenido en otro M_2 y así formaríamos una cadena ascendente infinita, en contradicción con 2).

3) $\Rightarrow$ 1) Si N es un submódulo de M que no es finitamente generado entonces tomamos $m_0 \in N$ y se cumple $N \neq (m_0)$, luego existe un m_1 en $N \setminus (m_0)$ y $N \neq (m_0, m_1)$, luego existe un m_2 en $N \setminus (m_0, m_1)$ y $N \neq (m_0, m_1, m_2)$. De este modo construimos una familia de submódulos

$$(m_0) \subset (m_0, m_1) \subset (m_0, m_1, m_2) \subset \cdots$$

que no tiene maximal. ∎

Los teoremas siguientes justificarán de forma inmediata que todos los anillos y módulos que consideremos en lo sucesivo serán noetherianos:

Teorema 2.3 *Si A es un anillo y M es un A-módulo noetheriano, entonces todo submódulo y todo módulo cociente de M es noetheriano.*

DEMOSTRACIÓN: Sea N un submódulo de M. Entonces todo submódulo de N es también un submódulo de M, luego es finitamente generado y así N es noetheriano. Todo submódulo de M/N es de la forma R/N, donde $N \subset R \subset M$ y del hecho de que R es finitamente generado se sigue claramente que R/N también lo es. ∎

En particular si A es un anillo noetheriano e I es un ideal de A, entonces el anillo cociente A/I es noetheriano. El teorema anterior afirma en principio que es noetheriano como A-módulo, pero los A-submódulos de A/I son los mismos que los A/I-submódulos, por lo que también es noetheriano como A/I-módulo, es decir, como anillo.

También se cumple un recíproco:

Teorema 2.4 *Sea A un anillo, M un A-módulo y N un submódulo de M. Si tanto N como M/N son noetherianos, entonces M también lo es.*

DEMOSTRACIÓN: A cada submódulo L de M le asociamos el par de módulos $\big(L \cap N, (L+N)/N\big)$. Notemos que si $E \subset F$ son dos submódulos de M y sus pares asociados son iguales entonces $E = F$. En efecto, si $x \in F$, como $(E+N)/N = (F+N)/N$, existen $u \in N$ y $v \in E$ tales que $x = u+v$. Entonces $u \in F \cap N = E \cap N$, luego $x \in E$.

A una sucesión ascendente de submódulos de M le corresponden dos sucesiones ascendentes de submódulos de N y de M/N respectivamente. Como éstas han de ser finalmente constantes, la dada también lo ha de ser, luego M es noetheriano. ∎

Teorema 2.5 *Sea A un anillo y M un A-módulo. Si E y F son submódulos noetherianos de M, entonces $E+F$ también es noetheriano.*

DEMOSTRACIÓN: Tenemos que E es noetheriano y $(E+F)/E \cong F/(E \cap F)$ también lo es, luego $E+F$ es noetheriano. ∎

Teorema 2.6 *Si A es un anillo noetheriano, entonces todo A-módulo finitamente generado es noetheriano.*

DEMOSTRACIÓN: Si M admite un generador con m elementos, entonces existe un epimorfismo de anillos $f : A^m \longrightarrow M$ (pues A^m es un módulo libre de rango m y podemos extender a un epimorfismo una biyección entre una base de A^m y un generador de M). Aplicando m veces el teorema anterior concluimos que A^m es un módulo noetheriano y M es isomorfo a un cociente de A^m, luego M es noetheriano. ∎

El teorema de Hilbert [Al 3.8] afirma que si A es un anillo noetheriano, el anillo de polinomios $A[x_1, \ldots, x_n]$ también lo es. Ahora podemos afirmar, más en general:

Teorema 2.7 *Si A es un anillo noetheriano y $B = A[b_1, \ldots, b_n]$ es un anillo finitamente generado sobre A, entonces B es noetheriano.*

(Porque B es isomorfo a un cociente de $A[x_1, \ldots, x_n]$).

Extensiones enteras La propiedad 3) del teorema de Dedekind está relacionada con el concepto de "entero algebraico", que ya conocemos, pero para precisar dicha relación debemos generalizarlo ligeramente.

Definición 2.8 Diremos que E/D es una *extensión de dominios íntegros* si E es un dominio íntegro y $D \subset E$ es un subanillo tal que $1 \in D$ (con lo que D también es un dominio íntegro).

En tal caso podemos identificar el cuerpo de cocientes K de D con un subcuerpo del cuerpo de cocientes L de E, de modo que L/K es una extensión de cuerpos. Cuando digamos que E/D es una extensión finita, normal, separable, etc. de dominios íntegros nos referiremos a que lo es la extensión L/K de sus cuerpos de cocientes.

Diremos que un elemento $\alpha \in E$ es *entero* sobre D si es raíz de un polinomio mónico con coeficientes en D.

Cuando L es un cuerpo numérico y $D = \mathbb{Z}$, los elementos de L enteros sobre D son precisamente los enteros algebraicos. Todos los resultados que probaremos aquí son generalizaciones de hechos conocidos en este caso. Para empezar probaremos que los elementos enteros sobre un dominio íntegro forman un anillo, y para ello usaremos la siguiente caracterización de la integridad:

Teorema 2.9 *Sea E/D una extensión de dominios íntegros. Un $\alpha \in E$ es entero sobre D si y sólo si existe un D-módulo finitamente generado no nulo $M \subset E$ tal que $\alpha M \subset M$.*

Demostración: Si α es entero entonces $\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_1\alpha + d_0 = 0$, para ciertos $d_i \in D$. Basta considerar el módulo $M = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_D$.

Dado un módulo $M = \langle v_1, \ldots, v_n \rangle_D$ tal que $\alpha M \subset M$, existen elementos d_{ij} en D tales que

$$\alpha v_i = d_{i1}v_1 + \cdots + d_{in}v_n, \qquad \text{para } i = 1, \ldots, n.$$

Esto equivale a la ecuación vectorial $\alpha v = vA$, donde $v = (v_i)$ y $A = (d_{ij})$, o sea, que α es un valor propio de la matriz A, luego es raíz de su polinomio característico, que claramente es mónico y con coeficientes en D. ∎

Teorema 2.10 *Sea E/D una extensión de dominios íntegros. Entonces el conjunto E_0 de todos los elementos de E enteros sobre D es un subanillo de E.*

Demostración: Sean α, $\beta \in E_0$. Sean M y N dos D-módulos no nulos finitamente generados tales que $\alpha M \subset M$ y $\beta N \subset N$. Entonces es fácil ver que MN es un D-módulo no nulo finitamente generado y $(\alpha \pm \beta)MN \subset MN$, $\alpha\beta MN \subset MN$. Por lo tanto $\alpha \pm \beta \in E_0$ y $\alpha\beta \in E_0$. ∎

Ahora podemos probar que el polinomio mínimo de un elemento algebraico determina si éste es o no entero.

Teorema 2.11 *Sea D un dominio íntegro y K su cuerpo de cocientes. Sea L/K una extensión de cuerpos. Entonces un elemento $\alpha \in L$ es entero sobre D si y sólo si es algebraico sobre K y su polinomio mínimo sobre K tiene coeficientes enteros sobre D. En particular la norma y la traza de un entero sobre D son enteras sobre D.*

Demostración: Es obvio que un K-monomorfismo de L en una clausura algebraica de L envía elementos enteros a elementos enteros, luego los conjugados de los enteros son enteros. Los coeficientes del polinomio mínimo de α dependen polinómicamente de los conjugados de α, luego si α es entero dichos coeficientes también lo son. La norma y la traza son dos de estos coeficientes. ∎

Definición 2.12 Si D es un dominio íntegro contenido en un cuerpo K, el conjunto E de todos los elementos de K enteros sobre D se llama la *clausura entera* de D en K. El teorema 2.10 prueba que se trata de un dominio íntegro.

Un dominio íntegro D contenido en un cuerpo K es *íntegramente cerrado* en K si todo elemento de K entero sobre D está en D o, equivalentemente, si D coincide con su clausura entera en K.

Un dominio integro D es *íntegramente cerrado* si es íntegramente cerrado en su cuerpo de cocientes. Observemos que ésta es precisamente la condición 3) de la caracterización algebraica de los dominios de Dedekind.

El teorema [Al 3.35] afirma que todo dominio de factorización única es íntegramente cerrado.

Si en el teorema 2.11 suponemos además que D es íntegramente cerrado, entonces resulta que un elemento algebraico sobre K es entero si y sólo si su polinomio mínimo sobre K está en $D[x]$, y en particular tenemos que la norma y la traza de un entero están en D.

Definición 2.13 Sea E/D una *extensión* de dominios íntegros. Diremos que la extensión E/D es *entera* si todo elemento de E es entero sobre D.

Vamos a probar que las extensiones enteras de dominios íntegros se comportan como las extensiones algebraicas de cuerpos. El teorema 2.10 implica que si adjuntamos a un anillo un conjunto de elementos enteros obtenemos una extensión entera. Ahora probamos que si adjuntamos un número finito de elementos obtenemos además una extensión finitamente generada.

Teorema 2.14 *Sean $D \subset E$ dominios íntegros tales que $E = D[a_1, \ldots, a_n]$ con los a_i enteros sobre D. Entonces E es un D-módulo finitamente generado.*

Demostración: Si tenemos una cadena $D \subset F \subset E$ de dominios íntegros de modo que E es un F-módulo finitamente generado y F es un D-módulo finitamente generado, entonces E es un D-módulo finitamente generado. Basta observar que si $E = \langle e_1, \ldots, e_n \rangle_F$ y $F = \langle f_1, \ldots, f_m \rangle_D$ entonces $E = \langle e_i f_j \rangle_D$.

De aquí se sigue que basta probar el teorema para una sola adjunción. Supongamos que $E = D[a]$ y que a es raíz de un polinomio mónico $p(x) \in D[x]$ de grado n. Todo elemento de E es de la forma $q(a)$ con $q(x) \in D[x]$.

Podemos dividir $q(x) = p(x)c(x) + r(x)$ con $\operatorname{grad} r(x) < n$, y entonces resulta que $q(a) = r(a)$. De aquí se sigue que $E = \langle 1, a, \ldots, a^{n-1} \rangle$. ∎

De aquí deducimos la transitividad de la integridad:

Teorema 2.15 *Si F/E y E/D son extensiones enteras la extensión F/D también lo es.*

Demostración: Sea $\alpha \in F$. Entonces $\alpha^n + e_{n-1}\alpha^{n-1} + \cdots + e_1\alpha + e_0 = 0$ para ciertos $e_i \in E$. Sea $E' = D[e_0, \ldots, e_{n-1}]$. Por el teorema anterior E' es un D-módulo finitamente generado y $E'[\alpha]$ es un E'-módulo finitamente generado. Es fácil ver entonces que $E'[\alpha]$ es un D-módulo finitamente generado. Además es obvio que $\alpha E'[\alpha] \subset E'[\alpha]$, luego α es entero sobre D. ∎

Esto implica que la clausura entera de un dominio íntegro D en un cuerpo K es íntegramente cerrada en K. De hecho, es la mayor extensión entera de D contenida en K.

Veamos ahora un resultado técnico elemental que necesitaremos en el teorema siguiente y en otras ocasiones.

Teorema 2.16 *Sea D un dominio íntegro y α un elemento algebraico sobre su cuerpo de cocientes. Entonces existe un $d \in D$ no nulo tal que $d\alpha$ es entero sobre D.*

DEMOSTRACIÓN: Por hipótesis $d_n\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_1\alpha + d_0 = 0$ para ciertos $d_i \in D$ con $d_n \neq 0$. Multiplicando por d_n^{n-1} queda

$$(d_n\alpha)^n + d_{n-1}(d_n\alpha)^{n-1} + \cdots + d_1(d_n\alpha) + d_0 = 0,$$

luego $d_n\alpha$ es entero sobre D. ∎

Un hecho crucial en el estudio de los cuerpos numéricos es que el orden maximal de un cuerpo numérico de grado n es un $\mathbb{Z}$-módulo libre de rango n, lo que nos permite hablar de bases enteras. En el caso general, si L es una extensión finita del cuerpo de cocientes de un dominio íntegro D, no tenemos garantizado que la clausura entera de D en L esté finitamente generada sobre D como anillo, y mucho menos como módulo. Para asegurarlo necesitamos imponer dos hipótesis: que el dominio sea noetheriano y que la extensión sea separable. Conviene tener presente que en los casos de mayor interés a los que se aplica todo lo que estamos viendo los dominios íntegros que aparecen son de característica 0, por lo que la separabilidad es trivial.

Teorema 2.17 *Sea D un dominio íntegro noetheriano íntegramente cerrado, sea K su cuerpo de cocientes y L una extensión finita separable de K. Entonces la clausura entera de D en L es un D-módulo finitamente generado.*

DEMOSTRACIÓN: Basta probar que la clausura entera de D en L está contenida en un D-módulo finitamente generado, pues tal módulo será noetheriano y en consecuencia la clausura entera será finitamente generada.

Sea $w_1, \ldots, w_n$ una K-base de L. Por el teorema anterior podemos suponer que los w_i son enteros sobre D.

Según [Al 8.1] la traza $\mathrm{Tr} : L \longrightarrow K$ determina una forma bilineal regular en L, por lo que podemos considerar la base dual $z_1, \ldots, z_n \in L$ de $w_1, \ldots, w_n$ en el sentido de [Al 6.44], es decir, la base que cumple

$$\mathrm{Tr}(z_i w_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Sea $c \neq 0$ un elemento de D tal que cz_i es entero sobre D para $i = 1, \ldots, n$. Si x es cualquier elemento de L entero sobre D, entonces xcz_i es entero sobre D, luego lo mismo le sucede a $T(xcz_i)$ para cada i. Si $x = \sum_{j=1}^n b_j w_j$, con $b_j \in K$, entonces

$$T(xcz_i) = \sum_{j=1}^n cb_j T(z_i w_j) = cb_i \in K,$$

y como D es íntegramente cerrado, de hecho $cb_i \in D$ y

$$x = \sum_{j=1}^{n} b_j w_j = \sum_{j=1}^{n} (cb_j)(c^{-1}w_j) \in \left\langle c^{-1}w_1, \ldots, c^{-1}w_n \right\rangle_D .$$

Así pues, el módulo $\left\langle c^{-1}w_1, \ldots, c^{-1}w_n \right\rangle_D$ contiene a la clausura entera de D en L. ∎

Debemos tener presente que en las hipótesis de este teorema no podemos garantizar que la clausura entera de D en L sea un D-módulo libre. Evidentemente es libre de torsión, luego, por [Al 4.44], una condición suficiente para que sea libre es que D sea un dominio de ideales principales. Éste es el caso de $\mathbb{Z}$ y es por ello que podemos asegurar la existencia de bases enteras en los cuerpos numéricos. No obstante, si $D \subset E$ son órdenes maximales de cuerpos numéricos, no es necesariamente cierto que E tenga una base como D-módulo, por lo que en general nos tendremos que conformar con saber que E es un D-módulo finitamente generado, que es lo que afirma el teorema anterior.

Complementos sobre dominios de Dedekind Probamos aquí algunos resultados adicionales sobre dominios de Dedekind que no aparecen en [Al], pero que necesitaremos más adelante. El primero es un hecho técnico que es fácil usar inadvertidamente, pues en los dominios de factorización única es trivial:

Teorema 2.18 *Sea D un dominio de Dedekind, sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ primos de D y sean α y $\beta \in D$ no nulos tales que la multiplicidad de cada $\mathfrak{p}_i$ en β sea menor o igual que en α. Entonces $\alpha/\beta = \gamma/\delta$, para ciertos γ, $\delta \in D$, de modo que ningún $\mathfrak{p}_i$ divide a δ.*

Demostración: Sea $\beta = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}\mathfrak{a}$, donde $\mathfrak{a}$ no es divisible entre ningún primo $\mathfrak{p}_i$. Por el teorema chino del resto [Al 3.56] existe un $\delta \in D$ tal que

$$\delta \equiv 0 \ (\text{mód } \mathfrak{a}), \qquad \delta \equiv 1 \ (\text{mód } \mathfrak{p}_i), \quad i = 1, \ldots, r.$$

Esto implica que $\mathfrak{a} \mid \delta$ y no es divisible entre ningún $\mathfrak{p}_i$. Teniendo en cuenta la hipótesis, $\beta \mid \alpha\delta$, es decir, existe un $\gamma \in D$ tal que $\alpha\delta = \beta\gamma$. ∎

El resultado siguiente afirma que, dado un ideal $\mathfrak{a}$, es posible multiplicarlo por otro $\mathfrak{c}$ primo con cualquier otro ideal prefijado $\mathfrak{b}$ de modo que el producto sea principal $\mathfrak{ac} = (\alpha)$.

Teorema 2.19 *Sea D un dominio de Dedekind y $\mathfrak{a}$, $\mathfrak{b}$ dos ideales no nulos de D. Entonces existe un $\alpha \in \mathfrak{a}$ tal que $\alpha\mathfrak{a}^{-1} + \mathfrak{b} = 1$.*

Demostración: Hay que probar que α puede tomarse de modo que ninguno de los primos que dividen a $\mathfrak{b}$ divida a $\alpha\mathfrak{a}^{-1}$, o equivalentemente, que $\alpha \notin \mathfrak{ap}$ para todo $\mathfrak{p} \mid \mathfrak{b}$.

Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ los primos distintos que dividen a $\mathfrak{b}$. Si $r = 1$ basta tomar $\alpha \in \mathfrak{a} - \mathfrak{ap}_1$. Para $r > 1$ sea $\mathfrak{a}_i = \mathfrak{ap}_i^{-1}\mathfrak{b}$. Si $\mathfrak{ap}_i \subset \mathfrak{a}_i = \mathfrak{ap}_i^{-1}\mathfrak{b}$ entonces $\mathfrak{p}_i \subset \mathfrak{p}_i^{-1}\mathfrak{b}$, luego $\mathfrak{b} \mid \mathfrak{p}_i^2$, luego sería $r = 1$.

Por lo tanto podemos tomar números $\alpha_i \in \mathfrak{a}_i \setminus \mathfrak{a}\mathfrak{p}_i$ para $i = 1, \ldots, r$ y $\alpha = \alpha_1 + \cdots + \alpha_r$. Como cada $\alpha_i \in \mathfrak{a}_i \subset \mathfrak{a}$, se cumple que $\alpha \in \mathfrak{a}$. Si se cumpliera que $\alpha \in \mathfrak{a}\mathfrak{p}_i$ para algún i, entonces para $j \neq i$ tendríamos también que $\alpha_j \in \mathfrak{a}_j \subset \mathfrak{a}\mathfrak{p}_i$, luego despejando α_i en la definición de α concluiríamos que $\alpha_i \in \mathfrak{a}\mathfrak{p}_i$, en contradicción con la elección que hemos hecho. ∎

En general un dominio de Dedekind no tiene por qué ser un dominio de ideales principales, pero ahora podemos probar que sus ideales admiten generadores de a lo sumo dos elementos:

Teorema 2.20 *Sea D un dominio de Dedekind, sea $\mathfrak{a}$ un ideal no nulo de D y sea $\beta \in \mathfrak{a}$ no nulo. Entonces existe un $\alpha \in \mathfrak{a}$ tal que $\mathfrak{a} = (\alpha, \beta)$.*

Demostración: Sea $\mathfrak{b} = \beta\mathfrak{a}^{-1}$. (como $\mathfrak{a} \mid \beta$, se cumple que $\mathfrak{b}$ es un ideal). Por el teorema anterior existe un $\alpha \in \mathfrak{a}$ tal que $\alpha\mathfrak{a}^{-1} + \mathfrak{b} = 1$, o equivalentemente $\alpha\mathfrak{a}^{-1} + \beta\mathfrak{a}^{-1} = 1$. Multiplicando por $\mathfrak{a}$ queda que $\mathfrak{a} = (\alpha) + (\beta) = (\alpha, \beta)$. ∎

Las técnicas de localización que vamos a introducir en el apartado siguiente nos permitirán reducir algunos problemas sobre dominios de Dedekind al caso de dominios de Dedekind con un número finito de ideales primos. Eso vuelve especialmente útil el teorema siguiente:

Teorema 2.21 *Si D es un dominio de Dedekind con un número finito de ideales primos entonces D es un dominio de ideales principales y por lo tanto tiene factorización única.*

Demostración: Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos de D. Tomemos elementos $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Dado un ideal no nulo arbitrario $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$, por el teorema chino del resto [Al 3.56] existe un $\alpha \in D$ tal que $\alpha \equiv \pi_i^{r_i}$ (mód $\mathfrak{p}_i^{r_i+1}$). Es fácil ver que cada primo $\mathfrak{p}_i$ divide a α con multiplicidad exactamente r_i, de donde $(\alpha) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} = \mathfrak{a}$. ∎

Localización En este apartado veremos cómo construir anillos a partir de uno dado de manera que desaparezcan todos los ideales primos salvo uno prefijado, y que éste conserve sus propiedades aritméticas. Esto supondrá una simplificación esencial para el tratamiento de muchos problemas.

Definición 2.22 Sea D un dominio íntegro. Un subconjunto S de D es *multiplicativo* si $1 \in S$, $0 \notin S$ y cuando s, $t \in S$ también $st \in S$. Si S es un subconjunto multiplicativo de D definimos

$$S^{-1}D = \{a/s \mid a \in D, s \in S\}.$$

Es fácil ver que $S^{-1}D$ es un subanillo del cuerpo de cocientes de D.

Si M es un D-módulo contenido en un cuerpo que contenga a D (en particular si M es un ideal de D), llamaremos

$$S^{-1}M = \{m/s \mid m \in M,\ s \in S\},$$

que es un $S^{-1}D$-módulo.

Notemos que si $\mathfrak{p}$ es un ideal primo en D, entonces $S = D \setminus \mathfrak{p}$ es un subconjunto multiplicativo. En este caso el dominio íntegro $S^{-1}D$ se representa $D_\mathfrak{p}$ y se llama *localización* de D en $\mathfrak{p}$. Del mismo modo, escribiremos $M_\mathfrak{p}$ en lugar de $S^{-1}M$.

En definitiva, $D_\mathfrak{p}$ está formado por todas las fracciones en D cuyo denominador no está en $\mathfrak{p}$ (para un cierto representante a/s de la fracción). Una fracción a/s es una unidad de $D_\mathfrak{p}$ si y sólo si $a \notin \mathfrak{p}$, pues si $(a/s)(b/t) = 1$, entonces $ab = st \in D \setminus \mathfrak{p}$, luego $a \notin \mathfrak{p}$, y si $a \notin \mathfrak{p}$ entonces $(a/s)(s/a) = 1$.

Dicho de otro modo, un elemento $a/s \in D_\mathfrak{p}$ no es una unidad si y sólo si $a \in \mathfrak{p}$, o sea, si y sólo si a/s está en el ideal $\mathfrak{m} = S^{-1}\mathfrak{p}$. Esto implica que $\mathfrak{m}$ es el único ideal maximal del anillo $D_\mathfrak{p}$.

Se dice que un anillo A es *local* si tiene un único ideal maximal. Tenemos, pues, que cuando localizamos respecto a un ideal primo obtenemos un anillo local. Pronto veremos que cuando localizamos respecto a un primo $\mathfrak{p}$ en un dominio de Dedekind D, el ideal $\mathfrak{m}$ conserva las propiedades de $\mathfrak{p}$, mientras que los restantes ideales no tienen ningún reflejo en $D_\mathfrak{p}$.

En general se dice que una propiedad o un teorema es *local* si involucra a un único primo, mientras que si involucra a todo el sistema aritmético de un anillo se dice que la propiedad, o el teorema, es global. En estos términos, veremos que al localizar respecto a un primo se conservan las propiedades locales y se pierden las globales.

Hemos introducido la localización en términos de conjuntos multiplicativos arbitrarios porque, como veremos en la sección siguiente, otras elecciones de S nos permiten conservar un conjunto finito de primos en lugar de uno solo.

Veamos ahora las propiedades básicas de la localización:

Teorema 2.23 *Sea D un dominio íntegro y $S \subset D$ un subconjunto multiplicativo. Entonces se tienen los hechos siguientes:*

1. *Si $\mathfrak{a}$ es un ideal de D, entonces $S^{-1}\mathfrak{a}$ es un ideal de $S^{-1}D$, y todos los ideales de $S^{-1}D$ son de esta forma.*

2. *Se cumple*
$$S^{-1}\mathfrak{ab} = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$$
y
$$S^{-1}\mathfrak{a} = S^{-1}D \quad \textit{si y sólo si} \quad \mathfrak{a} \cap S \neq \varnothing.$$

3. *Si un dominio E es entero sobre D entonces $S^{-1}E$ es entero sobre $S^{-1}D$.*

4. *Si B es la clausura entera de D en un cuerpo K, entonces $S^{-1}B$ es la clausura entera de $S^{-1}D$ en K.*

5. *Si D es íntegramente cerrado $S^{-1}D$ también lo es.*

6. *Si D es un dominio de Dedekind entonces $S^{-1}D$ también lo es y la aplicación S^{-1} es un epimorfismo del grupo de los ideales fraccionales de D en el grupo de los ideales fraccionales de $S^{-1}D$. El núcleo de este epimorfismo lo forman los ideales que cortan a S.*

DEMOSTRACIÓN: 1) Es inmediato que si $\mathfrak{a}$ es un ideal de D, entonces $S^{-1}\mathfrak{a}$ es un ideal de $S^{-1}D$. Recíprocamente, si $\mathfrak{b}$ es un ideal de $S^{-1}D$ entonces $\mathfrak{a} = \mathfrak{b} \cap D$ es un ideal de D y $\mathfrak{b} = S^{-1}\mathfrak{a}$. En efecto, una inclusión es clara, y si $x \in \mathfrak{b}$, entonces $x = a/s$ con $a \in D$, $s \in S$. Por lo tanto tenemos que $sx \in \mathfrak{b} \cap D = \mathfrak{a}$, luego $x \in S^{-1}\mathfrak{a}$.

2) Se prueba sin dificultad.

3) Sea $e/s \in S^{-1}E$, con $e \in E$, $s \in S$. Sea M un D-módulo finitamente generado tal que $eM \subset M$. Entonces $S^{-1}M$ es un $S^{-1}D$-módulo finitamente generado y $(e/s)S^{-1}M \subset S^{-1}M$.

4) Sea $\alpha \in K$ entero sobre $S^{-1}D$. Entonces $p(\alpha) = 0$, donde $p(x)$ es un polinomio mónico con coeficientes en $S^{-1}D$. Si s es el producto de los denominadores de los coeficientes de $p(x)$ elevado al grado de $p(x)$, es claro que $s \in S$ y que al multiplicar por s la igualdad $p(\alpha) = 0$ obtenemos que $s\alpha$ es raíz de un polinomio mónico con coeficientes en D. Consecuentemente $s\alpha \in E$ y así $\alpha \in S^{-1}E$.

Por el apartado anterior todos los elementos de $S^{-1}E$ son enteros sobre $S^{-1}D$, luego $S^{-1}E$ es la clausura entera de $S^{-1}D$ en K.

5) Es consecuencia inmediata de 4).

6) Supongamos que D es un dominio de Dedekind. Por 1) los ideales de $S^{-1}D$ son de la forma $S^{-1}\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal de D. Como $\mathfrak{a}$ es finitamente generado $S^{-1}\mathfrak{a}$ también lo es. Por lo tanto $S^{-1}D$ es noetheriano.

Por el apartado anterior $S^{-1}D$ es íntegramente cerrado.

Sea $S^{-1}\mathfrak{p}$ un ideal primo no nulo de $S^{-1}D$ y supongamos que $ab \in \mathfrak{p}$. Entonces uno de los dos factores, digamos a, está en $S^{-1}\mathfrak{p}$. Sea $a = p/s$, con $p \in \mathfrak{p}$, $s \in S$. Entonces $p = as$ y no puede ser que $s \in \mathfrak{p}$, pues entonces $S^{-1}\mathfrak{p} = 1$, luego $a \in \mathfrak{p}$. Así pues, $\mathfrak{p}$ es primo.

Como D es un dominio de Dedekind, $\mathfrak{p}$ es maximal. Si $S^{-1}\mathfrak{p} \subset S^{-1}\mathfrak{a}$ y existe un a/s en $S^{-1}\mathfrak{a}$ que no está en $S^{-1}\mathfrak{p}$, entonces $a \notin \mathfrak{p}$, luego $1 = p + da$, para cierto $p \in \mathfrak{p}$ y $d \in D$. Esto prueba que $1 \in S^{-1}\mathfrak{a} = S^{-1}D$, luego $S^{-1}\mathfrak{p}$ es un ideal maximal.

Con esto tenemos que $S^{-1}D$ es un dominio de Dedekind. El resto es fácil de comprobar. ∎

Centrémonos ahora en la localización respecto a un primo $\mathfrak{p}$ en un dominio de Dedekind D. Ya hemos visto que el anillo $D_{\mathfrak{p}}$ está formado por las fracciones cuyo denominador no es divisible entre $\mathfrak{p}$, así como que $D_{\mathfrak{p}}$ tiene un único ideal maximal $\mathfrak{m} = S^{-1}\mathfrak{p}$ formado por las fracciones cuyo numerador está en $\mathfrak{p}$.

Además el teorema anterior nos da que $D_{\mathfrak{p}}$ es un dominio de Dedekind, luego los ideales restantes de $D_{\mathfrak{p}}$ han de ser las potencias de $\mathfrak{m}$, y los ideales fraccionales de $D_{\mathfrak{p}}$ son las potencias de $\mathfrak{m}$ con exponente entero.

Si $\mathfrak{q} \neq \mathfrak{p}$ es cualquier otro ideal primo de D entonces $\mathfrak{q}$ no puede estar contenido en $\mathfrak{p}$, luego corta a S y por lo tanto $S^{-1}\mathfrak{q} = 1$. Esto significa que el epimorfismo S^{-1} actúa sobre un ideal fraccional cualquiera eliminando todos sus factores distintos de $\mathfrak{p}$ y reemplazando a éste por $\mathfrak{m}$.

En resumen, tal y como habíamos anticipado, al localizar en $\mathfrak{p}$ estamos eliminando todos los ideales primos distintos de $\mathfrak{p}$, mientras que, como veremos, las propiedades de $\mathfrak{p}$ se transmiten muy bien a $\mathfrak{m}$. He aquí un primer ejemplo:

Teorema 2.24 *Sea D un dominio de Dedekind, sea $\mathfrak{p}$ un primo en D y sea n un número natural. Entonces*

1. *Todo elemento de $D_\mathfrak{p}$ es congruente con un elemento de D módulo $\mathfrak{m}^n$.*
2. *Dos elementos de D son congruentes mód $\mathfrak{m}^n$ si y sólo si lo son mód $\mathfrak{p}^n$.*
3. *Los cocientes $D_\mathfrak{p}/\mathfrak{m}^n$ y $D/\mathfrak{p}^n$ son isomorfos.*

Demostración: 1) Sea d/s un elemento de $D_\mathfrak{p}$. El ideal $(s, \mathfrak{p}^n)$ es un divisor de $\mathfrak{p}^n$, luego es de la forma $\mathfrak{p}^r$ para $r \leq n$, pero $s \notin \mathfrak{p}$ y por lo tanto tampoco está en ninguna potencia de $\mathfrak{p}$ salvo en $\mathfrak{p}^0 = 1$. Así pues, $(s, \mathfrak{p}^n) = 1$ y en consecuencia $1 = sb + k$, donde $b \in D$ y $k \in \mathfrak{p}^n$. De aquí resulta que $d/s = db + k/s$, con $k/s \in \mathfrak{m}^n$ y $db \in$D.

2) Si $d \in \mathfrak{m}^n$ entonces $d = d'/s$, con $d' \in \mathfrak{p}^n$, pero entonces $\mathfrak{p}^n \mid sd$ y $\mathfrak{p}^n$ es primo con s, luego $\mathfrak{p}^n \mid d$, es decir, $d \in \mathfrak{p}^n$. El recíproco es obvio. De aquí se sigue inmediatamente 2).

3) Es claro a partir de 1) y 2). ∎

Cuando D es un dominio de Dedekind el anillo $D_\mathfrak{p}$ es un dominio de Dedekind con un único primo, luego por el teorema 2.21 resulta ser un dominio de ideales principales.

En general, si D es un dominio de ideales principales local y $\mathfrak{m}$ es su ideal maximal, existe un primo $\pi \in D$ tal que $\mathfrak{m} = (\pi)$. Este primo está unívocamente determinado salvo unidades. Todo elemento $\alpha \in D$ no nulo se expresa de forma única como $\alpha = \epsilon\pi^n$, donde ϵ es una unidad de D y n es un número natural.

2.2 Extensiones de dominios de Dedekind

Ya estamos en condiciones de estudiar las extensiones de dominios de Dedekind, en el sentido de la definición siguiente:

Definición 2.25 Sean D y E dominios de Dedekind con cuerpos de cocientes k y K respectivamente ($k \subset K$). Diremos que E/D es una *extensión (finita) de dominios de Dedekind* si E es la clausura entera de D en K y además es un D-módulo finitamente generado.

Observemos que en estas condiciones la extensión K/k ha de ser finita (si E está generado sobre D por n elementos, $|K : k| \leq n$). Llamaremos *grado* de E/D al grado de K/k.

El teorema siguiente afirma que las extensiones separables de un dominio de Dedekind están en correspondencia biunívoca con las extensiones finitas separables de su cuerpo de cocientes:

Teorema 2.26 *Sea D un dominio de Dedekind y sea k su cuerpo de cocientes. Si K es una extensión finita separable de k y E es la clausura entera de D en K, entonces E/D es una extensión de dominios de Dedekind.*

DEMOSTRACIÓN: Ciertamente E es íntegramente cerrado. Por 2.17 tenemos que E es un D-módulo finitamente generado. En particular E es de la forma $E = D[a_1, \ldots, a_n]$ para ciertos elementos a_i, luego por el teorema 2.7 el anillo E es noetheriano. Falta ver que los ideales primos no nulos son maximales.

Sea $\mathfrak{P} \neq 0$ un ideal primo en E. Entonces $\mathfrak{p} = \mathfrak{P} \cap D$ es un ideal primo en D. Veamos que es no nulo.

Sea $\alpha \in \mathfrak{P}$ no nulo. Sea $p(x)$ el polinomio mínimo de α sobre el cuerpo de cocientes de D. Por el teorema 2.11 (y la observación posterior) sus coeficientes están en D. La ecuación $p(\alpha) = 0$ nos da que el término independiente de $p(x)$ está en $\mathfrak{p}$, y ciertamente es no nulo.

Como D es un dominio de Dedekind $\mathfrak{p}$ es un ideal maximal y el cociente $D/\mathfrak{p}$ es un cuerpo. Tenemos que $\mathfrak{p} \subset \mathfrak{P}$, lo que nos da la situación descrita por el esquema siguiente:

$$\begin{array}{ccc} E & \longrightarrow & E/\mathfrak{P} \\ \uparrow & & \uparrow \\ D & \longrightarrow & D/\mathfrak{p} \end{array}$$

La flecha vertical izquierda es la inclusión, las flechas horizontales son los epimorfismos canónicos y la flecha izquierda es el monomorfismo que hace conmutativo el diagrama, definido de forma natural (a la clase de α le corresponde la clase de α).

Si $E = D[a_1, \ldots, a_n]$ es claro que también $E/\mathfrak{P} = (D/\mathfrak{p})\big[[a_1], \ldots, [a_n]\big]$. El hecho de que cada a_i sea entero sobre D implica que cada $[a_i]$ es algebraico sobre el cuerpo $D/\mathfrak{p}$, pero entonces $(D/\mathfrak{p})[[a_1], \ldots, [a_n]] = (D/\mathfrak{p})([a_1], \ldots, [a_n])$ es un cuerpo. Esto implica que $\mathfrak{P}$ es un ideal maximal. ∎

En el capítulo XI de [Al] estudiamos cómo se descomponen en factores primos del orden maximal $\mathcal{O}$ de un cuerpo numérico los primos racionales, pero esto tiene sentido porque $\mathbb{Z}$ es un dominio de ideales principales y los primos de $\mathbb{Z}$ son elementos de $\mathbb{Z}$, que también pueden verse como elementos de $\mathcal{O}$, que a su vez podemos identificar con ideales principales de $\mathcal{O}$ susceptibles de ser descompuestos en primos. Sin embargo, si E/D es una extensión de dominios de Dedekind y D no es un dominio de ideales principales, no está claro en principio qué significa descomponer en factores primos en E un primo $\mathfrak{p}$ de D.

Ahora probaremos que la aplicación que a cada ideal fraccional de D le asigna el ideal fraccional que genera en E es un monomorfismo de grupos, que nos permitirá considerar a los ideales de D como parte de los ideales de E. En realidad lo único que no es trivial es probar que dicha aplicación es un monomorfismo, o sea, que ideales distintos de (1) generan ideales distintos de (1). La clave será el teorema siguiente:

Teorema 2.27 (Lema de Nakayama) *Sea D un dominio íntegro, $\mathfrak{a}$ un ideal de D no nulo contenido en todos los ideales maximales de D y M un D-módulo finitamente generado tal que $\mathfrak{a}M = M$. Entonces $M = 0$.*

DEMOSTRACIÓN: Sea $M = \langle v_1, \dots, v_n\rangle$. Entonces $v_n \in \mathfrak{a}M$, luego podemos expresar $v_n = a_1v_1 + \cdots + a_nv_n$, para ciertos $a_1, \dots, a_n \in \mathfrak{a}$. De aquí que $(1 - a_n)v_n = a_1v_1 + \cdots + a_{n-1}v_{n-1}$.

Si $1 - a_n$ no fuera una unidad estaría en un ideal maximal $\mathfrak{m}$ de D, y por hipótesis tenemos que $a_n \in \mathfrak{a} \subset \mathfrak{m}$, luego $1 \in \mathfrak{m}$, lo cual es imposible. Así pues $1 - a_n$ es una unidad de D y podemos despejar v_n en la ecuación anterior para concluir que $M = \langle v_1, \dots, v_{n-1}\rangle$. Repitiendo el argumento llegamos a que $M = \langle v_1\rangle$ y finalmente a que $v_1 = 0$. ∎

Teorema 2.28 *Sea D un dominio íntegro y E una extensión entera de D. Sea $\mathfrak{p}$ un primo en D. Entonces $\mathfrak{p}E \neq E$.*

DEMOSTRACIÓN: Supongamos que $\mathfrak{p}E = E$. Por el teorema 2.23 sabemos que $E_\mathfrak{p}$ es entero sobre $D_\mathfrak{p}$. Si llamamos $\mathfrak{m}$ al ideal maximal de $D_\mathfrak{p}$ es inmediato comprobar que $\mathfrak{m}E_\mathfrak{p} = E_\mathfrak{p}$. Así pues, el teorema es también falso en $D_\mathfrak{p}$, que además es un anillo local. Esto significa que basta probar el teorema en el caso en que D es local.

Si $\mathfrak{p}E = E$ entonces $1 = p_1e_1 + \cdots + p_ne_n$ para ciertos $p_i \in \mathfrak{p}$ y $e_i \in E$. Sea $D' = D[e_1, \dots, e_n]$. Por el teorema 2.14 tenemos que D' es un D-módulo finitamente generado y claramente $\mathfrak{p}D' = D'$. Puesto que $\mathfrak{p}$ está contenido en el único ideal maximal de D podemos aplicar el teorema anterior y concluir que $D' = 0$, lo cual es absurdo. ∎

Con esto estamos en condiciones de describir las relaciones básicas entre los primos de un dominio de Dedekind y los de una extensión.

Teorema 2.29 *Sea E/D una extensión de dominios de Dedekind.*

1. *La aplicación que a cada ideal fraccional $\mathfrak{a}$ de D le asigna el ideal fraccional $\mathfrak{a}E$ es un monomorfismo de grupos.*

2. *La correspondencia anterior asigna a ideales primos entre sí imágenes primas entre sí. Si (α) es un ideal principal de D entonces su imagen es el ideal principal (α) generado por α en E.*

3. *Cada primo de E divide a un único primo de D.*

DEMOSTRACIÓN: Es inmediato comprobar que si $\mathfrak{a}$ es un ideal fraccional de D entonces $\mathfrak{a}E$ es un ideal fraccional de E (ciertamente es un E-módulo, y si $c\mathfrak{a} \subset D$ entonces $c\mathfrak{a}E \subset DE = E$). También es claro que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales fraccionales de D entonces $\mathfrak{a}\mathfrak{b}E = (\mathfrak{a}E)(\mathfrak{b}E)$. Esto prueba que la aplicación que estamos considerando es un homomorfismo de grupos.

Si $\mathfrak{p}$ es un primo de D, el teorema anterior nos da que el ideal $\mathfrak{p}E$ que genera en E es un ideal propio (que desde luego ya no tiene por qué ser primo). Si $\mathfrak{P}$

es un factor primo de $\mathfrak{p}E$ en E, entonces $\mathfrak{p} \subset \mathfrak{p}E \subset \mathfrak{P}$, luego $\mathfrak{p} \subset \mathfrak{P} \cap D$. Por otra parte es obvio que $\mathfrak{P} \cap D$ es un ideal propio de D, y como $\mathfrak{p}$ es maximal ha de ser $\mathfrak{p} = \mathfrak{P} \cap D$.

En otras palabras, los primos de E que dividen a $\mathfrak{p}E$ son exactamente los primos $\mathfrak{P}$ que cumplen $\mathfrak{p} = \mathfrak{P} \cap D$, luego si $\mathfrak{p}$ y $\mathfrak{q}$ son primos distintos en D, entonces los primos que dividen a $\mathfrak{p}E$ son distintos de los primos que dividen a $\mathfrak{q}E$, es decir, $\mathfrak{p}E$ y $\mathfrak{q}E$ son ideales de E primos entre sí. En particular son distintos.

La unicidad de la factorización nos da ahora que ideales distintos de D generan ideales distintos de E, luego el homomorfismo es de hecho un monomorfismo.

Con esto queda probado 1) y parte de 2). El resto de 2) es trivial. Respecto a 3), si $\mathfrak{P}$ es un primo de E, en la prueba del teorema 2.26 se ve que $\mathfrak{p} = \mathfrak{P} \cap D$ es un ideal primo no nulo de D, y claramente $\mathfrak{p}E \subset \mathfrak{P}$, o sea, $\mathfrak{P} \mid \mathfrak{p}E$. La unicidad se sigue de 2). ∎

En lo sucesivo escribiremos $\mathfrak{a}$ en lugar de $\mathfrak{a}E$, es decir, consideraremos a los ideales fraccionales de D como ideales fraccionales de E. Es importante tener claro que un ideal primo en D puede no ser primo en E. Ahora ya tiene sentido estudiar cómo factorizan en E los primos de D.

Definición 2.30 Sea E/D una extensión de dominios de Dedekind. Sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E tal que $\mathfrak{P} \mid \mathfrak{p}$. Llamaremos *índice de ramificación* de $\mathfrak{p}$ en $\mathfrak{P}$ a la multiplicidad de $\mathfrak{P}$ en $\mathfrak{p}$ (el número de veces que aparece $\mathfrak{P}$ en la descomposición en factores primos de $\mathfrak{p}$) y lo representaremos por $e = e(\mathfrak{P}/\mathfrak{p})$.

De este modo, si los primos que dividen a $\mathfrak{p}$ en E son $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ y e_i es el índice de ramificación de $\mathfrak{p}$ en $\mathfrak{P}_i$ entonces la descomposición de $\mathfrak{p}$ en E es $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.

En el caso de los cuerpos numéricos, cuando $D = \mathbb{Z}$, sabemos que la norma impone una restricción al modo en que pueden factorizar los primos. Concretamente, si el grado del cuerpo es n y $N(\mathfrak{P}_i) = p^{f_i}$, entonces

$$p^n = \mathrm{N}(p) = \mathrm{N}(\mathfrak{P}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{P}_r r)^{e_r} = p^{f_1 e_1 + \cdots f_r e_r},$$

luego ha de ser

$$n = f_1 e_1 + \cdots + f_r e_r. \tag{2.1}$$

Para probar algo así en el caso general nos falta definir los números f_i. No vamos a definirlos a partir de la norma (no tenemos definida ninguna norma sobre los ideales de un dominio de Dedekind arbitrario), sino que por el contrario definiremos la norma a partir de ellos. Observemos que, en el caso de los cuerpos numéricos, si $\mathfrak{P}$ es un primo y $\mathrm{N}(\mathfrak{P}) = |E/\mathfrak{P}| = p^f$, entonces p es el único primo racional al que divide $\mathfrak{P}$ y f es el grado del cuerpo $E/\mathfrak{P}$ sobre su cuerpo primo $\mathbb{Z}/p\mathbb{Z}$. Todo esto tiene sentido en el caso general.

Definición 2.31 Si D es un dominio de Dedekind y $\mathfrak{p}$ es un primo en D, entonces el cociente $D/\mathfrak{p}$ es un cuerpo, al que en lo sucesivo llamaremos *cuerpo de restos* de $\mathfrak{p}$.

Si E es una extensión de D y $\mathfrak{P}$ es un primo en E que divide a $\mathfrak{p}$, razonando como en el teorema 2.26 podemos considerar al cuerpo de restos $\overline{E} = E/\mathfrak{P}$ como una extensión finita de $\overline{D} = D/\mathfrak{p}$ de forma natural (la clase de α se identifica con la clase de α).

Llamaremos *grado de inercia* de $\mathfrak{p}$ en $\mathfrak{P}$ al grado de la extensión de cuerpos $\overline{E}/\overline{D}$. Lo representaremos por $f = f(\mathfrak{P}/\mathfrak{p})$.

Ahora ya tiene sentido la fórmula (2.1) en el caso general (donde n es el grado de la extensión E/D), si bien todavía no estamos en condiciones de probarla. Esta fórmula indica que cuanto mayor es el grado de inercia de un primo $\mathfrak{p}$ sobre un divisor en una extensión, el número de factores en que se descompone es menor, hasta el extremo de que si $f = n$ entonces $\mathfrak{p}$ se conserva primo en E.

Para llegar a (2.1) necesitamos estudiar los índices de ramificación y los grados de inercia. En primer lugar tenemos la transitividad. La prueba es inmediata.

Teorema 2.32 *Sea $D \subset E \subset F$ una cadena de extensiones de dominios de Dedekind. Sean $\mathfrak{p}$ un primo en F, $\mathfrak{q}$ un primo en E y $\mathfrak{r}$ un primo en D tales que $\mathfrak{p} \mid \mathfrak{q} \mid \mathfrak{r}$. Entonces*

$$e(\mathfrak{p}/\mathfrak{r}) = e(\mathfrak{p}/\mathfrak{q})e(\mathfrak{q}/\mathfrak{r}) \qquad y \qquad f(\mathfrak{p}/\mathfrak{r}) = f(\mathfrak{p}/\mathfrak{q})f(\mathfrak{q}/\mathfrak{r}).$$

Ahora vamos a estudiar la localización de la descomposición de un primo.

Teorema 2.33 *Sea E/D una extensión de dominios de Dedekind de grado n, sea $\mathfrak{p}$ un primo en D y supongamos que su factorización en E es $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, donde los primos $\mathfrak{P}_i$ son distintos dos a dos. Entonces*

1. *$E_\mathfrak{p}/D_\mathfrak{p}$ es una extensión de dominios de Dedekind de grado n.*
2. *$E_\mathfrak{p}$ es un $D_\mathfrak{p}$-módulo libre de rango n.*
3. *$S^{-1}\mathfrak{p}$ es el único ideal primo de $D_\mathfrak{p}$ y $S^{-1}\mathfrak{P}_1, \ldots, S^{-1}\mathfrak{P}_r$ son los únicos ideales primos de $E_\mathfrak{p}$ (además son distintos dos a dos).*
4. *Los índices de ramificación y los grados de inercia de $S^{-1}\mathfrak{p}$ en cada $S^{-1}\mathfrak{P}_i$ son los mismos que los de $\mathfrak{p}$ en cada $\mathfrak{P}_i$.*

Demostración: 1) Estamos localizando respecto a $S = D \setminus \mathfrak{p}$, que es un subconjunto multiplicativo tanto de D como de E. Por el teorema 2.23 tanto $E_\mathfrak{p}$ como $D_\mathfrak{p}$ son dominios de Dedekind y $E_\mathfrak{p}$ es una extensión entera de $D_\mathfrak{p}$. Como los cuerpos de cocientes son los mismos, la extensión tiene también grado n.

2) Es claro que un generador de E como D-módulo es también un generador de $E_\mathfrak{p}$ como $D_\mathfrak{p}$-módulo, luego $E_\mathfrak{p}$ es un $D_\mathfrak{p}$-módulo finitamente generado, obviamente libre de torsión, y $D_\mathfrak{p}$ es un dominio de ideales principales. Por lo tanto $E_\mathfrak{p}$ es libre.

Sean K y k los cuerpos de cocientes de E y D. Un sistema $D_\mathfrak{p}$-libre es también k-libre, pues multiplicando una combinación lineal con coeficientes en k

por un elemento adecuado (no nulo) de $D_\mathfrak{p}$ obtenemos una combinación lineal con coeficientes en $D_\mathfrak{p}$ (teorema 2.16), luego el rango de $E_\mathfrak{p}$ es menor o igual que n. Por otra parte el teorema 2.16 nos da también que existe una k-base de K formada por elementos de $E_\mathfrak{p}$, que obviamente son $D_\mathfrak{p}$-libres, luego el rango de $E_\mathfrak{p}$ es exactamente n.

3) Ya sabemos que $S^{-1}\mathfrak{p}$ es el único ideal primo de $D_\mathfrak{p}$. Por el teorema 2.23 los ideales $S^{-1}\mathfrak{P}_i$ son todos no triviales, pues ninguno de los ideales $\mathfrak{P}_i$ corta a $S = D \setminus \mathfrak{p}$ (se cumple $\mathfrak{p} = \mathfrak{P}_i \cap D$).

Notemos que si $a/s \in S^{-1}\mathfrak{P}_i$ con $s \in S$, entonces $a \in \mathfrak{P}_i$, pues $a/s = b/t$ para cierto $b \in \mathfrak{P}_i$, y así $at = bs \in \mathfrak{P}_i$ y como $t \in D \setminus \mathfrak{p}$ no puede ser $t \in \mathfrak{P}_i$, pues entonces $t \in \mathfrak{P}_i \cap D = \mathfrak{p}$. Por lo tanto $a \in \mathfrak{P}_i$.

De aquí se sigue inmediatamente que los ideales $S^{-1}\mathfrak{P}_i$ son primos. Además son distintos, pues si $S^{-1}\mathfrak{P}_i = S^{-1}\mathfrak{P}_j$ todo $a \in \mathfrak{P}_i$ cumpliría $a/1 \in S^{-1}\mathfrak{P}_j$, luego $a \in \mathfrak{P}_j$ y viceversa.

Si $\mathfrak{Q}$ es otro ideal de E entonces $\mathfrak{p} \neq \mathfrak{Q} \cap D$, luego $\mathfrak{Q}$ corta a S y es $S^{-1}\mathfrak{Q} = 1$. Por lo tanto todo ideal de $E_\mathfrak{p}$ se descompone en producto de ideales $S^{-1}\mathfrak{P}_1, \ldots, S^{-1}\mathfrak{P}_r$, luego éstos son los únicos ideales primos de $E_\mathfrak{p}$.

4) Aplicando S^{-1} a la factorización de $\mathfrak{p}$ vemos que los índices de ramificación se conservan. Para probar que lo mismo sucede con los grados de inercia fijemos un primo $\mathfrak{P} = \mathfrak{P}_i$. Como $\mathfrak{P} \subset S^{-1}\mathfrak{P}$ tenemos la situación siguiente:

$$\begin{array}{ccc} E/\mathfrak{P} & \longrightarrow & E_\mathfrak{p}/S^{-1}\mathfrak{P} \\ \uparrow & & \uparrow \\ D/\mathfrak{p} & \longrightarrow & D_\mathfrak{p}/S^{-1}\mathfrak{p} \end{array}$$

Todas las flechas indican monomorfismos de cuerpos definidos de forma natural: a la clase de un α le corresponde la clase de α. Las flechas verticales determinan extensiones cuyos grados son los grados de inercia que queremos comparar. La flecha horizontal inferior es un isomorfismo por el teorema 2.24.

Basta probar que la flecha horizontal superior también es un isomorfismo, lo que equivale a probar que todo elemento de $E_\mathfrak{p}$ es congruente con uno de E módulo $S^{-1}\mathfrak{P}$, pero si $a/s \in E_\mathfrak{p}$ entonces $s \notin \mathfrak{P}$, luego es una unidad en $E/\mathfrak{P}$, es decir, existe un $b \in E$ de manera que $bs \equiv 1 \pmod{\mathfrak{P}}$, de donde se sigue que $bs \equiv 1 \pmod{S^{-1}\mathfrak{P}}$ y $a/s \equiv ab \pmod{S^{-1}\mathfrak{P}}$. ∎

Ahora ya podemos probar la relación (2.1). Notemos que la prueba se apoya en que al localizar una extensión obtenemos una extensión libre, de acuerdo con el apartado 2) del teorema anterior.

Teorema 2.34 *Sea E/D una extensión de dominios de Dedekind de grado n. Sea $\mathfrak{p}$ un primo en D, sea $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ la factorización de $\mathfrak{p}$ en E y para cada i sea f_i el grado de inercia de $\mathfrak{p}$ en $\mathfrak{P}_i$. Entonces*

$$n = f_1 e_1 + \cdots + f_r e_r.$$

DEMOSTRACIÓN: Por el teorema anterior podemos localizar en $\mathfrak{p}$ y suponer que D es un anillo local, que E es un D-módulo libre de rango n y que $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son los únicos primos de E.

Es claro que $E/\mathfrak{p}E$ es un espacio vectorial sobre $D/\mathfrak{p}$. Veamos que su dimensión es n.

Sea $\{w_1, \ldots, w_n\}$ una D-base de E. Es claro que $\{[w_1], \ldots, [w_n]\}$ es un generador de $E/\mathfrak{p}E$. Basta ver que es libre. Como D es un dominio de Dedekind con un único primo, el ideal $\mathfrak{p}$ es principal, o sea, $\mathfrak{p} = pD$, para cierto $p \in \mathfrak{p}$, luego $\mathfrak{p}E = pE$.

Si $[d_1][w_1] + \cdots + [d_n][w_n] = 0$, entonces $d_1w_1 + \cdots + d_nw_n \in pE$, luego

$$d_1w_1 + \cdots + d_nw_n = p(c_1w_1 + \cdots + c_nw_n), \qquad \text{con } c_i \in D,$$

y por la unicidad $d_i = pc_i$. Así pues, $[d_i] = 0$ para $i = 1, \ldots, n$.

Por 2.21 tenemos que E es un dominio de ideales principales, luego el teorema chino del resto [Al 3.52] nos da un isomorfismo de anillos

$$E/\mathfrak{p}E \longrightarrow \prod_{i=1}^{r} E/\mathfrak{P}_i^{e_i}.$$

Los factores son también espacios vectoriales sobre $D/\mathfrak{p}$ y el isomorfismo es también un isomorfismo de espacios vectoriales. El teorema quedará probado si vemos que la dimensión de cada factor $E/\mathfrak{P}_i^{e_i}$ es exactamente f_ie_i. Por simplificar la notación fijemos $\mathfrak{P} = \mathfrak{P}_i$, $e = e_i$, $f = f_i$, para cierto índice i. Claramente $\mathfrak{P}^e \subset \mathfrak{P}^{e-1} \subset \cdots \subset \mathfrak{P}^2 \subset \mathfrak{P} \subset E$, luego

$$1 = \mathfrak{P}^e/\mathfrak{P}^e \subset \mathfrak{P}^{e-1}/\mathfrak{P}^e \subset \cdots \subset \mathfrak{P}^2/\mathfrak{P}^e \subset \mathfrak{P}/\mathfrak{P}^e \subset E/\mathfrak{P}^e,$$

donde cada término es un subespacio vectorial. La dimensión de $E/\mathfrak{P}^e$ es la suma de las dimensiones de los espacios cociente.

Es fácil ver que

$$(E/\mathfrak{P}^e) \Big/ (\mathfrak{P}/\mathfrak{P}^e) \cong E/\mathfrak{P} \qquad \text{como } D/\mathfrak{p}\text{-espacios vectoriales}$$

(no es el teorema de isomorfía usual porque ni E ni $\mathfrak{P}$ son $D/\mathfrak{p}$-espacios vectoriales). Del mismo modo los cocientes restantes son isomorfos a los espacios $\mathfrak{P}^i/\mathfrak{P}^{i+1}$, para $i = 1, \ldots, e-1$.

Basta demostrar que todos estos espacios tienen dimensión f. Ciertamente, la dimensión de $E/\mathfrak{P}$ sobre $D/\mathfrak{p}$ es f por definición. Basta probar que todos los espacios $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ son isomorfos a $E/\mathfrak{P}$. Ahora bien, si $\mathfrak{P} = (\pi)$, con lo que $\mathfrak{P}^i = (\pi^i)$, la aplicación $\phi : E/\mathfrak{P} \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$ dada por $\phi([\alpha]) = [\pi^i\alpha]$ es claramente un isomorfismo de espacios vectoriales, luego el teorema queda probado. ∎

2.3 Factorización ideal en cuerpos numéricos

Antes de seguir desarrollando la teoría general, conviene mostrar ejemplos de su aplicación en el caso de los cuerpos numéricos. Si K es un cuerpo numérico

y $\mathcal{O}_K$ es su orden maximal, es frecuente hablar de K cuando propiamente habría que nombrar a $\mathcal{O}_K$, por ejemplo, al hablar de la descomposición en primos en K de un primo racional p. Realmente la descomposición es en $\mathcal{O}_K$. También usaremos la notación $\overline{K}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ para referirnos a los cuerpos de restos.

Recordemos que sobre los ideales de un cuerpo numérico está definida la norma [Al 8.33] que es multiplicativa [Al 8.34] y que sobre los primos viene dada por $\mathrm{N}(\mathfrak{p}) = p^f$, donde p es el único primo racional divisible entre $\mathfrak{p}$ y f es precisamente el grado de inercia que hemos definido en la sección anterior. Esto hace que en este contexto el teorema 2.34 sea inmediato.

El resultado básico para obtener la factorización de un primo racional en un cuerpo numérico es [Al 8.37], pero aquí vamos a presentar una versión ligeramente más general:

Teorema 2.35 *Sea $K = \mathbb{Q}(\zeta)$ un cuerpo numérico, donde ζ es entero y p un primo racional tal que $p \nmid \operatorname{ind}\zeta$. Sea $g(x) = \operatorname{pol\,mín}\zeta$ y $\bar{g}(x)$ la imagen de $g(x)$ por el epimorfismo de $\mathbb{Z}[x]$ sobre $(\mathbb{Z}/p\mathbb{Z})[x]$. Sea $\bar{g} = \bar{g}_1^{e_1}\cdots\bar{g}_r^{e_r}$ la descomposición de $\bar{g}$ en polinomios mónicos irreducibles en $(\mathbb{Z}/p\mathbb{Z})[x]$. Entonces los ideales $\mathfrak{p}_i = \big(p, g_i(\zeta)\big)$, para $i = 1,\ldots,r$ son primos distintos en $\mathcal{O}_K$ y la descomposición de p en primos es $p = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$. Además $\mathrm{N}(\mathfrak{p}_i) = p^{\operatorname{grad} g_i}$.*

Demostración: Para cada $i = 1,\ldots,r$, sea ζ_i una raíz de $\bar{g}_i(x)$ en una extensión de $\mathbb{Z}/p\mathbb{Z}$. Entonces $(\mathbb{Z}/p\mathbb{Z})(\zeta_i)$ es una extensión finita de $\mathbb{Z}/p\mathbb{Z}$ y $\bar{g}_i = \operatorname{pol\,mín}(\zeta_i, \mathbb{Z}/p\mathbb{Z})$.

Sea $\phi_i : \mathbb{Z}[\zeta] \longrightarrow (\mathbb{Z}/p\mathbb{Z})(\zeta_i)$ la aplicación dada por $\phi_i\big(q(\zeta)\big) = \bar{q}(\zeta_i)$. Está bien definida, pues si $q(\zeta) = r(\zeta)$, entonces $(q-r)(\zeta) = 0$, luego $g|q-r$, de donde $\bar{g} \mid \bar{q} - \bar{r}$, y también $\bar{g}_i \mid \bar{q} - \bar{r}$, luego $\bar{q}(\zeta_i) - \bar{r}(\zeta_i) = 0$.

Obviamente ϕ_i es un epimorfismo, luego $\mathbb{Z}[\zeta]/\mathrm{N}(\phi_i) \cong (\mathbb{Z}/p\mathbb{Z})(\zeta_i)$, y el segundo anillo es un cuerpo, de donde $\mathrm{N}(\phi_i)$ es un ideal maximal de $\mathbb{Z}[\zeta]$.

Llamemos $\mathfrak{q}_i$ al ideal generado por p y $g_i(\zeta)$ en $\mathbb{Z}[\zeta]$. Claramente $\mathfrak{q}_i \subset \mathrm{N}(\phi_i)$ (la imagen de p es $[p] = 0$). Veamos la otra inclusión. Si $q(\zeta) \in \mathrm{N}(\phi_i)$, entonces $\bar{q}(\zeta_i) = 0$, luego $\bar{q}(x) = \bar{h}(x)\bar{g}_i(x)$. El hecho de que $\bar{q}(x) - \bar{h}(x)\bar{g}_i(x) = 0$ significa que todos los coeficientes del polinomio $q(x) - h(x)g_i(x)$ son múltiplos de p. Consecuentemente $q(\zeta) = \big(q(\zeta) - h(\zeta)g_i(\zeta)\big) + h(\zeta)g_i(\zeta) \in \mathfrak{q}_i$. Por lo tanto, $\mathfrak{q}_i = \mathrm{N}(\phi_i)$ es un ideal maximal de $\mathbb{Z}[\zeta]$.

Sea $k = \operatorname{índ}\zeta = \big|\mathcal{O}_K : \mathbb{Z}[\zeta]\big|$. Claramente, si $\beta \in \mathcal{O}_K$, entonces $k\beta \in \mathbb{Z}[\zeta]$.

Veamos ahora que $\mathfrak{p}_i \neq 1$. En otro caso existirían enteros $\beta, \gamma \in \mathcal{O}_K$ tales que $1 = \beta p + \gamma g_i(\zeta)$. Entonces $k = k\beta p + k\gamma g_i(\zeta)$ y $k\beta, k\gamma \in \mathbb{Z}[\zeta]$, luego $k \in \mathfrak{q}_i = \mathrm{N}(\phi_i)$, luego $p \mid k$, en contra de la hipótesis.

Tomemos un entero racional x tal que $kx \equiv 1 \pmod{p}$. Dado cualquier $\beta \in \mathcal{O}_K$, sea $\gamma = kx\beta$. Entonces $\gamma \in \mathbb{Z}[\zeta]$ y $\gamma \equiv \beta \pmod{\mathfrak{p}_i}$. Esto prueba que la inclusión $\mathbb{Z}[\zeta] \longrightarrow \mathcal{O}_K/\mathfrak{p}_i$ es suprayectiva, su núcleo contiene a $\mathfrak{q}_i$ y, como éste es maximal, se da la igualdad, es decir, $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{Z}[\zeta]/\mathfrak{q}_i \cong (\mathbb{Z}/p\mathbb{Z})(\zeta_i)$. En particular, $\mathfrak{p}_i$ es un ideal primo de $\mathcal{O}_K$.

Aplicando que, en general, $(p,u)(p,v) \subset (p,uv)$ concluimos que

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset \big(p, g_1(\zeta)^{e_1} \cdots g_r(\zeta)^{e_r}\big) = \big(p, g(\zeta)\big) = (p,0) = (p).$$

Notemos que la primera igualdad se debe a que $g(\zeta)$ y $g_1(\zeta)^{e_1} \cdots g_r(\zeta)^{e_r}$ se diferencian en un entero múltiplo de p. Así pues, $p \mid \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. La igualdad la obtendremos considerando las normas.

Tenemos que $\mathrm{N}(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| = \big|(\mathbb{Z}/p\mathbb{Z})(\zeta_i)\big| = p^{\operatorname{grad} g_i}$. En total

$$\mathrm{N}(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = p^{e_1 \operatorname{grad} g_1 + \cdots + e_r \operatorname{grad} g_r} = p^n,$$

donde n es el grado de K. Así pues $\mathrm{N}(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = \mathrm{N}(p)$, lo que nos da que $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

Los primos $\mathfrak{p}_i$ son distintos, pues si $\mathfrak{p}_i = \mathfrak{p}_j$, entonces $g_j(\zeta) \in \mathfrak{p}_i$, de donde se sigue fácilmente que $kg_j(\zeta) \in \mathfrak{q}_i$, y a su vez $\bar{g}_j\big([\zeta]\big) = 0$. Así pues, los polinomios $\bar{g}_i$ y $\bar{g}_j$ tienen la raíz $[\zeta]$ en común en $\mathbb{Z}[\zeta]/\mathfrak{q}_i$, pero eso es imposible porque ambos polinomios son irreducibles en $\mathbb{Z}/p\mathbb{Z}[x]$, luego son primos entre sí. ∎

Así tenemos un método práctico para factorizar cualquier primo de cualquier cuerpo numérico salvo en un caso: salvo si un primo p divide a los índices de todos los enteros de un cuerpo numérico K. Entonces se dice que p es un *divisor esencial* de K. El ejemplo de Dedekind $\mathbb{Q}(\xi)$ que estudiamos en el capítulo anterior es precisamente un ejemplo de cuerpo con un divisor esencial: el 2, según se ve en la expresión para el índice de un entero arbitrario que allí obtuvimos:

$$\text{índ}\left(x + y\,\xi + z\,\frac{\xi+\xi^2}{2}\right) = |2y^3 + 2z^3 - yz^2 + zy^2|.$$

Ésta es la razón por la que es famoso el ejemplo de Dedekind. Existen métodos para determinar las descomposiciones en primos de los divisores esenciales, pero no entraremos en ello. No obstante, en el caso concreto del ejemplo de Dedekind no es difícil encontrar la factorización del 2, gracias a que de hecho se trata de una factorización real (en ideales principales):

El ejemplo de Dedekind Recordemos que el ejemplo de Dedekind es $\mathbb{Q}(\xi)$, donde ξ es una raíz del polinomio $x^3 + x^2 - 2x + 8$. Si aproximamos las raíces del polinomio mínimo de ξ obtenemos los valores:

$$\begin{aligned}
\xi_1 &= -2.76734574086197\ldots \\
\xi_2 &= 0.883672870430983\ldots + 1.4525766646443\ldots i \\
\xi_3 &= 0.883672870430983\ldots - 1.4525766646443\ldots i
\end{aligned}$$

Si desarrollamos

$$\left(a + b\xi_1 + c\frac{\xi_1+\xi_1^2}{2}\right)\left(a + b\xi_2 + c\frac{\xi_2+\xi_2^2}{2}\right)\left(a + b\xi_3 + c\frac{\xi_3+\xi_3^2}{2}\right)$$

y redondeamos los coeficientes, obtenemos que la norma de un entero arbitrario $a + b\xi + c\frac{\xi+\xi^2}{2}$ vale

$$a^3 - 8b^3 + 10c^3 - a^2b - 2ab^2 + 2a^2c - 8b^2c + 3ac^2 + 2bc^2 + 11abc.$$

Dando valores a (a, b, c) vemos que los enteros de coordenadas $(8, 2, -1)$, $(-7, 1, 4)$, $(1, -1, 1)$, $(3, -3, 2)$, $(4, -4, 3)$ tienen todos norma 2. Calculando los cocientes respectivos se llega a que $(8, 2, -1)$ es asociado a $(4, -4, 3)$, y que $(-7, 1, 4)$ es asociado a $(3, -3, 2)$, en ambos casos a través de la unidad

$$\epsilon = 13 + 10\xi + 6\,\frac{\xi + \xi^2}{2},$$

mientras que los restantes son no asociados entre sí. A partir de aquí es fácil llegar a que

$$2 = \left(4 - 4\xi + 3\,\frac{\xi+\xi^2}{2}\right)\left(-7 + \xi + 4\,\frac{\xi+\xi^2}{2}\right)\left(1 - \xi + \frac{\xi+\xi^2}{2}\right),$$

con lo que tenemos la factorización del único primo racional que no puede obtenerse mediante el teorema anterior. ∎

El teorema siguiente, junto con la descomposición que acabamos de obtener, proporciona una prueba alternativa de que el 2 es un divisor esencial:

Teorema 2.36 *Sea K un cuerpo numérico de grado n y $p < n$ un primo racional. Si p se descompone en K como producto de n ideales distintos, entonces p es un divisor esencial de K.*

Demostración: En caso contrario existiría un entero $\alpha \in K$ tal que $K = \mathbb{Q}(\alpha)$ y $p \nmid \operatorname{índ}\alpha$. Si $f(x) = \operatorname{pol\,mín}\alpha$ el teorema 2.35 implica que f se descompone en n factores distintos módulo p, lo cual es absurdo, pues los los grados de inercia tendrían que ser todos iguales a 1, luego los factores tendrían que ser lineales, pero $p < n$. ∎

Ejercicio: Sean K_1, K_2 y K_3 los cuerpos definidos en la página 17. Considerar las factorizaciones de 5 y 11 en cada uno de ellos para concluir que se trata efectivamente de tres cuerpos distintos.

Cuerpos cuadráticos El caso más simple al que podemos aplicar el teorema 2.35 son los cuerpos cuadráticos:

Sea $K = \mathbb{Q}(\sqrt{d}\,)$ un cuerpo cuadrático. Sabemos que su orden maximal es $\mathbb{Z}[\alpha]$, donde α es $\sqrt{d}$ o bien $\big(1 + \sqrt{d}\,\big)/2$ según el resto de d módulo 4. Según el caso, el polinomio mínimo de α será $x^2 - d$ o bien $x^2 - x + \frac{1-d}{4}$. Según el teorema 2.35, la factorización de un primo p en K dependerá de la de estos polinomios en $\mathbb{Z}/p\mathbb{Z}$. Evidentemente, para el caso de $x^2 - d$, el polinomio tendrá una raíz doble, dos raíces o ninguna según si d es 0 módulo p, es un cuadrado no nulo

módulo p o no es un cuadrado módulo p. En el caso del segundo polinomio llegamos a la misma conclusión estudiando el discriminante (suponiendo $p \neq 2$), que es también $(-1)^2 - 4(1-d)/4 = d$. El caso $p = 2$ se analiza por separado sin dificultad.

La tabla siguiente recoge todos los casos. Los números e y f son los que aparecen en el teorema 2.35.

Tabla 2.1: Factorización en cuerpos cuadráticos

Casos		Factorización	e	f
$p \mid \Delta$		$p = \mathfrak{p}^2$	2	1
$p \nmid \Delta$,	$x^2 \equiv d \pmod p$ resoluble o $p = 2,\ d \equiv 1 \pmod 8$	$p = \mathfrak{p}_1\mathfrak{p}_2$	1	1
$p \nmid \Delta$	$x^2 \equiv d \pmod p$ no resoluble o $p = 2,\ d \equiv 5 \pmod 8$	$p = p$	1	2

Ejercicio: Probar que la ecuación $x^2 - 15y^2 = 13$ no tiene soluciones enteras.

Cuerpos cúbicos puros Consideremos ahora un cuerpo $K = \mathbb{Q}\big(\sqrt[3]{ab^2}\,\big)$. Sabemos que el orden maximal es de la forma $\mathbb{Z}[\theta_0, \theta_1, \theta_2]$, donde $\theta_0, \theta_1, \theta_2$ son los enteros descritos en el teorema 1.20.

En el capítulo anterior también calculamos el índice de un entero arbitrario, que resulta ser

$$\text{índ}(x + y\theta_1 + z\theta_2) = |by^3 - az^3|$$

para los cuerpos de tipo I e

$$\text{índ}\left(\frac{x + y\theta_1 + z\theta_2}{3}\right) = \frac{|by^3 - az^3|}{9}$$

para los cuerpos de tipo II, donde $x \equiv y \equiv z \pmod 3$.

En particular el índice de θ_1 es b para los cuerpos de tipo I y $3b$ para los de tipo II. Similarmente el índice de θ_2 es a o $3a$.

Como a y b son primos entre sí, para factorizar un primo p podemos aplicar el teorema 2.35 con $\zeta = \theta_1$ o bien $\zeta = \theta_2$ excepto si $p = 3$ y el cuerpo es de tipo II. Por simetría, podemos suponer que si p divide a $m = ab^2$ entonces $p \mid a$, con lo cual podemos trabajar con θ_1 salvo en el caso exceptuado.

El polinomio mínimo de θ_1 es $x^3 - ab^2$. Hemos de estudiar sus raíces módulo p. Supongamos primero que $p \nmid 3ab$.

Sea $G = (\mathbb{Z}/p\mathbb{Z})^*$. Hemos de estudiar qué elementos de G tienen raíz cúbica y cuántas tiene cada uno. El homomorfismo $f : G \longrightarrow G$ dado por $[u] \mapsto [u]^3$ tiene por imagen al subgrupo H de todos los cubos. Claramente todos los elementos de G/H tienen orden 3, luego $|G/H|$ es potencia de 3 y por otra parte $|G/H|$ divide a $|G| = p - 1$.

Si $p \equiv -1$ (mód 3) entonces $3 \nmid p-1$, luego $G/H = 1$, $G = H$ y f es un isomorfismo. Esto significa que cada elemento de G tiene una única raíz cúbica.

Si por el contrario $p \equiv 1$ (mód 3) entonces G tiene un elemento u de orden 3. Es claro que 1, u, u^2 están en el núcleo de f y de hecho son todo el núcleo, pues el polinomio $x^3 - 1$ no puede tener más de tres raíces en el cuerpo $\mathbb{Z}/p\mathbb{Z}$. Por lo tanto $|H| = |G|/3$ y así, sólo la tercera parte de elementos tienen raíz cúbica, y cada uno tiene tres distintas.

Esto se traduce en que si $p \equiv -1$ (mód 3) el polinomio $x^3 - ab^2$ tiene una única raíz módulo p, luego se descompone en un factor de grado 1 y otro de grado 2. La factorización de p es, por lo tanto, $p = \mathfrak{p}_1\mathfrak{p}_2$, donde $\mathrm{N}(\mathfrak{p}_1) = p$ y $\mathrm{N}(\mathfrak{p}_2) = p^2$.

Si $p \equiv 1$ (mód 3) hay dos casos, según que la congruencia $x^3 \equiv ab^2$ (mód p) tenga o no solución. Si la tiene, de hecho tiene tres soluciones distintas, y p se descompone en producto de tres primos distintos $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, todos ellos de norma p. Si no hay solución p se conserva primo.

Si $p \mid ab$ (incluyendo $p = 3$), entonces $x^3 - ab^2 \equiv x^3$ (mód p), luego $p = \mathfrak{p}^3$, salvo en el caso en que no podemos aplicar el teorema, es decir, si $p = 3$ y K es de tipo II.

Si $p = 3 \nmid ab$ y K es de tipo I entonces $x^3 - ab^2 \equiv x^3 \pm 1 \equiv (x \pm 1)^3$ (mód 3), luego $p = \mathfrak{p}^3$.

Nos falta considerar $p = 3$ en los cuerpos de tipo II. Necesitamos encontrar otro entero en K cuyo índice no sea divisible entre 3. Por ejemplo vemos que $\text{índ}\,\theta_0 = |b-a|/9$, luego si $27 \nmid b - a$ podemos usar θ_0. En caso contrario

$$\text{índ}(\theta_0 - \theta_2) = \text{índ}\left(\frac{1 + 1\theta_1 - 2\theta_2}{3}\right) = \frac{|b+8a|}{9},$$

y $27 \nmid b + 8a$.

Ahora sólo queda un cálculo laborioso que involucra calcular los polinomios mínimos de estos dos enteros, reducirlos módulo 3 y factorizarlos. Por ejemplo, en la prueba del teorema 1.20 vimos que

$$\text{pol mín}\,\theta_0 = x^3 - x^2 + \frac{1-ab}{3}x - \frac{1 + ab^2 + a^2b - 3ab}{27}.$$

Para eliminar los denominadores hacemos $a = 9u + 3t + 1$, $b = 9v + 3t + 1$ y al tomar clases módulo 3 queda $x^3 - x^2 + tx - t^2 + t^3$. Sustituyendo $t = 0, 1, 2$, se ve que siempre hay una raíz doble y otra simple. Igualmente,

$$\text{pol mín}(\theta_0 - \theta_2) = x^3 - x^2 + \frac{1+2ab}{3}x + \frac{8ab^2 - 6ab - a^2b - 1}{27},$$

y tras el cambio $a = 9u + 3t + 1$, $b = 9v + 3t + 1$ y la reducción módulo 3 llegamos a $x^3 - x^2 + (t+1)x + t^3 - t^2 + t$, que también tiene exactamente dos raíces módulo 3 para $t = 0, 1, 2$.

Consecuentemente la factorización de 3 en este caso es $3 = \mathfrak{p}_1\mathfrak{p}_2^2$.

Notemos que hemos probado que los cuerpos cúbicos puros no tienen divisores esenciales. La tabla siguiente resume los resultados que hemos obtenido:

Tabla 2.2: Factorización en cuerpos cúbicos puros

Casos		Factorización	e	f
$p \nmid 3ab$	$x^3 \equiv ab^2$ (mód p) resoluble	$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1
$p \equiv 1$ (mód 3)	$x^3 \equiv ab^2$ (mód p) no resoluble	$p = p$	1	3
$p \nmid 3ab$	$p \equiv -1$ (mód 3)	$p = \mathfrak{p}_1\mathfrak{p}_2$	1	1/2
$p \mid 3ab$	(excepto $p = 3$, tipo II)	$p = \mathfrak{p}^3$	3	1
$p = 3$	tipo II	$3 = \mathfrak{p}_1\mathfrak{p}_2^2$	1/2	1

Cuerpos ciclotómicos El comportamiento de los primos racionales en los cuerpos ciclotómicos se sigue del siguiente hecho elemental sobre extensiones ciclotómicas de cuerpos finitos:

Teorema 2.37 *Sea $k = \mathbb{Z}/p\mathbb{Z}$ para un cierto primo p y sea ω una raíz m-sima primitiva de la unidad sobre $\mathbb{Z}/p\mathbb{Z}$, donde $p \nmid m$. Entonces $|k(\omega) : k|$ es igual al orden de p módulo m.*

Demostración: Sea $n = |k(\omega) : k|$. Puesto que ω tiene orden m en el grupo multiplicativo de $k(\omega)$, que tiene $p^n - 1$ elementos, concluimos que $m \mid p^n - 1$, luego $\mathrm{o}_m(p) \mid n$.

Por otra parte, todo elemento de $k(\omega)$ es de la forma $h(\omega)$, donde $h(x) \in k[x]$. Si llamamos $r = \mathrm{o}_m(p)$ es claro que $h(\omega)^{p^r} = h(\omega^{p^r}) = h(\omega)$, luego todos los elementos de $k(\omega)$ son raíces del polinomio $x^{p^r} - x$, de donde se sigue que $p^n \le p^r$, o sea, $n \le \mathrm{o}_m(p)$, y así tenemos la igualdad. ∎

Teorema 2.38 *Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de orden m y p un primo racional. Sea $m = p^k m'$, donde $p \nmid m'$. Entonces la factorización de p en K es de la forma $p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$, donde $f = \mathrm{o}_{m'}(p)$, $e = \phi(p^k)$ y $r = \phi(m)/ef$.*

Demostración: En principio será $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, para ciertos primos $\mathfrak{p}_i$ con grado de inercia f_i.

Sea $\omega_p = \omega^{m'}$ y $\omega_{m'} = \omega^{p^k}$, que son raíces primitivas de la unidad de orden p^k y m', respectivamente. Determinaremos primero las factorizaciones de p en $\mathbb{Q}(\omega_p)$ y $\mathbb{Q}(\omega_{m'})$.

Supongamos que $k \neq 0$. Las raíces p^k-ésimas primitivas de la unidad son las raíces de $x^{p^k} - 1$ que no lo son de $x^{p^{i-1}} - 1$, luego el polinomio ciclotómico es

$$\frac{x^{p^k} - 1}{x^{p^{i-1}} - 1} = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \cdots + x^{p^{k-1}} + 1.$$

Evaluando en 1 queda $p = \prod_j (1 - \omega_p^j) = \mathrm{N}(1 - \omega_p)$, donde j recorre los números menores que p^j no divisibles entre p. Ésta es la descomposición de p

en factores primos de $\mathbb{Q}(\omega_p)$. Veamos que todos los factores son asociados. En efecto, como $(1-\omega_p^j)/(1-\omega_p) = 1+\omega_p+\cdots+\omega_p^{j-1}$ es entero y los dos son primos, el cociente es una unidad, luego cada factor $1-\omega_p^j$ es asociado a $1-\omega_p$.

Por consiguiente, la factorización de p es de la forma $p = \epsilon(1-\omega_p)^{\phi(p^k)}$, donde ϵ es una unidad. El número $1-\omega_p$ no tiene por qué ser primo en $\mathbb{Q}(\omega)$, pero esto prueba al menos que los índices de ramificación cumplen $e_i \geq \phi(p^k)$.

Supongamos ahora que $m' \neq 1$. Por el teorema 1.21 sabemos que $p \nmid \Delta[\omega_{m'}]$, luego en particular $p \nmid \operatorname{índ}\omega_{m'}$, luego podemos aplicar el teorema 2.35 al orden $\mathbb{Z}[\omega_{m'}]$. El polinomio $x^{m'}-1$ tiene raíces simples módulo p, luego p se descompondrá en primos distintos cuyos grados de inercia serán los grados de los factores irreducibles de $\operatorname{pol\,mín}\omega_{m'}$ módulo p, que a su vez son iguales al grado de la extensión ciclotómica p-ésima de $\mathbb{Z}/p\mathbb{Z}$. Por el teorema anterior dicho grado es $o_{m'}(p)$.

Por consiguiente, los grados de inercia de los divisores de p en $\mathbb{Q}(\omega)$ cumplen $f_i \geq o_{m'}(p)$. Más aún, el número r de factores primos de p en $\mathbb{Q}(\omega)$ tiene que ser mayor o igual al número de factores primos en el cuerpo intermedio $\mathbb{Q}(\omega_{m'})$, es decir, $r \geq \phi(m')/o_{m'}(p)$. En definitiva los valores r, f_i, e_i cumplen

$$\phi(p^k m') = n = f_1 r_1 + \cdots + f_r e_r \geq \frac{\phi(m')}{o_{m'}(p)}\, o_{m'}(p)\phi(p^k) = n,$$

y concluimos que todas las desigualdades son realmente igualdades. ∎

Notemos que, gracias a la generalización de [Al 8.37] que estamos empleando, hemos podido calcular la descomposición en factores primos de cada primo racional en el orden maximal de $\mathbb{Q}(\omega)$ sin saber exactamente cuál es este orden. Más adelante probaremos que es $\mathbb{Z}[\omega]$.

También conviene señalar que si $p \nmid m$, entonces el tipo de factorización de p en $\mathbb{Q}(\omega)$ (es decir, los valores r, f, e) dependen únicamente del resto de p módulo m (concretamente en este caso $e = 1$).

Aunque no lo hemos necesitado, el hecho de que los índices de ramificación y los grados de inercia de todos los divisores en $\mathbb{Q}(\omega)$ de un mismo primo racional debían ser iguales era algo que podíamos saber a priori en virtud del teorema [Al 8.39], ya que los cuerpos ciclotómicos son extensiones de Galois de $\mathbb{Q}$. Dedicamos la sección siguiente a estudiar las factorizaciones de primos en extensiones de Galois de dominios de Dedekind arbitrarios. En particular veremos que [Al 8.39] vale en todas ellas.

2.4 Extensiones de Galois

Sea E/D una extensión de Galois de dominios de Dedekind, es decir, tal que los cuerpos de cocientes formen una extensión de Galois K/k. Es claro que cada $\sigma \in G(K/k)$ envía elementos de E a elementos de E (envía raíces de polinomios mónicos de $D[x]$ a raíces de polinomios mónicos de $D[x]$), luego $\sigma|_E$ es un automorfismo de E que deja fijos a los elementos de D. Recíprocamente,

cada automorfismo de E que deja fijos a los elementos de D se extiende de forma natural a un k-automorfismo de K.

Llamaremos $G(E/D)$ al grupo de los D-automorfismos de E, es decir, al grupo de los automorfismos de E que dejan fijos a los elementos de D. Según lo que acabamos de observar resulta que los grupos $G(K/k)$ y $G(E/D)$ son isomorfos y no los distinguiremos.

Puesto que $E \cap k = D$, los elementos de D son exactamente los elementos de E fijados por todos los automorfismos de $G(E/D)$.

Ahora, si $\sigma \in G(E/D)$ y $\mathfrak{a}$ es un ideal fraccional de E, definimos

$$\sigma(\mathfrak{a}) = \sigma[\mathfrak{a}] = \{\sigma(\alpha) \mid \alpha \in \mathfrak{a}\},$$

que claramente es un ideal fraccional de E, y es un ideal si $\mathfrak{a}$ lo es.

Vemos, pues, que cada $\sigma \in G(E/D)$ induce de este modo un automorfismo en el grupo de los ideales fraccionales de E que envía ideales a ideales, ideales primos a ideales primos, conserva las factorizaciones y la divisibilidad y es compatible con la acción de σ sobre K, en el sentido de que $\sigma(\alpha E) = \sigma(\alpha)E$ para todo $\alpha \in K$.

Diremos que dos ideales fraccionales $\mathfrak{a}$ y $\mathfrak{b}$ de E son *conjugados* si existe un automorfismo $\sigma \in G(E/D)$ tal que $\sigma(\mathfrak{a}) = \mathfrak{b}$.

Si $\mathfrak{a}$ es un ideal fraccional de D entonces $\sigma(\mathfrak{a}E) = \sigma(\mathfrak{a})E = \mathfrak{a}E$, o sea, que σ fija a los ideales de D. Por lo tanto, dos primos conjugados en E deben ser divisores del mismo primo de D. El recíproco también es cierto:

Teorema 2.39 *Sea E/D una extensión de Galois de dominios de Dedekind. Entonces dos ideales primos de E son conjugados si y sólo si dividen al mismo primo de D.*

Demostración: Sean $\mathfrak{P}$ y $\mathfrak{Q}$ primos en E. Si son conjugados por un automorfismo σ y $\mathfrak{P}$ divide a un primo $\mathfrak{p}$ de D entonces $\mathfrak{Q} = \sigma(\mathfrak{P}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}$.

Supongamos ahora que $\mathfrak{P} \mid \mathfrak{p}$ y $\mathfrak{Q} \mid \mathfrak{p}$ pero que $\sigma(\mathfrak{P}) \neq \mathfrak{Q}$ para todo automorfismo σ. Por el teorema chino del resto [Al 3.56] existe un $\alpha \in E$ tal que

$$\begin{aligned} &\alpha \equiv 0 \pmod{\mathfrak{Q}},\\ &\alpha \equiv 1 \pmod{\sigma(\mathfrak{P})} \quad \text{para todo } \sigma \in G(E/D). \end{aligned}$$

Pero entonces $\mathrm{N}(\alpha) = \prod_\sigma \sigma(\alpha) \equiv 1 \pmod{\mathfrak{P}}$ y por otra parte $\alpha \in \mathfrak{Q}$ y es uno de los factores de $\mathrm{N}(\alpha)$, luego $\mathrm{N}(\alpha) \in \mathfrak{Q} \cap D = \mathfrak{p} \subset \mathfrak{P}$, contradicción. ∎

Ahora es obvio que en general no es cierto que un ideal fijado por todos los D-automorfismos de E haya de ser un ideal de D. Por ejemplo, si un primo $\mathfrak{p}$ se descompone como $\mathfrak{p} = \mathfrak{P}^e$, el teorema anterior implica que $\mathfrak{P}$ está fijado por todos los D-automorfismos de E, pero si $e > 1$ no es cierto que $\mathfrak{P}$ sea un primo de D.

Con esto ya podemos probar [Al 8.39] en el contexto general:

Teorema 2.40 *Sea E/D una extensión de Galois de grado n de dominios de Dedekind, sea $\mathfrak{p}$ un primo en D y sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ los primos de E que lo dividen. Entonces todos los índices de ramificación $e(\mathfrak{P}_i/\mathfrak{p})$ son iguales a un mismo número e y todos los grados de inercia $f(\mathfrak{P}_i/\mathfrak{p}))$ son iguales a un mismo número f. Por lo tanto la factorización de $\mathfrak{p}$ en E es de la forma*

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

y se cumple la relación $n = efr$.

DEMOSTRACIÓN: Dados i, j, existe un automorfismo σ tal que $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Como σ conserva la divisibilidad, es claro que conserva las multiplicidades, luego $e(\mathfrak{P}_i/\mathfrak{p}) = e(\mathfrak{P}_j/\mathfrak{p})$.

Por otra parte es claro que σ induce un isomorfismo $E/\mathfrak{P}_i \longrightarrow E/\mathfrak{P}_j$ que deja fijos a los elementos de $D/\mathfrak{p}$ (las clases con representante en D), luego los grados de $E/\mathfrak{P}_i$ y $E/\mathfrak{P}_j$ sobre $D/\mathfrak{p}$ coinciden, es decir, $f(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}_j/\mathfrak{p})$. La relación $n = efr$ es la particularización a este caso del teorema 2.34. ∎

Así pues, la descomposición de un primo en una extensión de Galois está determinada por los tres números e, f y r. Veamos ahora que cambiando el dominio base por otro mayor podemos hacer $r = 1$ conservando e y f.

Definición 2.41 Sea E/D una extensión de Galois de dominios de Dedekind, sea $G = G(E/D)$ y sea $\mathfrak{P}$ un primo en E. Llamaremos *grupo de descomposición* de $\mathfrak{P}$ al grupo

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \leq G.$$

Los grupos de descomposición de dos primos conjugados son conjugados en el sentido de la teoría de grupos, es decir, $G_{\tau(\mathfrak{P})} = G_{\mathfrak{P}}^{\tau}$.

En efecto, se cumple $\sigma \in G_{\tau(\mathfrak{P})}$ si y sólo si $\sigma(\tau(\mathfrak{P})) = \tau(\mathfrak{P})$ si y sólo si $\tau^{-1}(\sigma(\tau(\mathfrak{P}))) = \mathfrak{P}$, si y sólo si $\tau\sigma\tau^{-1} \in G_{\mathfrak{P}}$, si y sólo si $\sigma \in \tau^{-1}G_{\mathfrak{P}}\tau = G_{\mathfrak{P}}^{\tau}$.

En particular, si G es abeliano todos los primos conjugados tienen el mismo grupo de descomposición.

Notemos también que $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$ si y sólo si $\tau\sigma^{-1} \in G_{\mathfrak{P}}$, por lo que si $G/G_{\mathfrak{P}}$ es el conjunto cociente para la congruencia por la derecha módulo $G_{\mathfrak{P}}$ (que no es un grupo en general) y $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son los primos conjugados con $\mathfrak{P}$, entonces la aplicación $f : G/G_{\mathfrak{P}} \longrightarrow \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ dada por $f([\sigma]) = \sigma(\mathfrak{P})$ es biyectiva. Consecuentemente $|G_{\mathfrak{P}}| = n/r = ef$ (con la notación del teorema anterior).

Llamaremos *cuerpo de descomposición* de $\mathfrak{P}$ al cuerpo L fijado por $G_{\mathfrak{P}}$. El *dominio de descomposición* de $\mathfrak{P}$ será la clausura entera F de D en L, que por el teorema 2.26 es un dominio de Dedekind tal que $D \subset F \subset E$ de modo que el grado de F/D es r y el de E/F es ef.

Ahora probamos que, tal y como anunciábamos, si $\mathfrak{P}$ divide a $\mathfrak{p}$ en D y a $\mathfrak{p}'$ en F, entonces el índice de ramificación y el grado de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}'$ son los mismos que sobre $\mathfrak{p}$, pero ahora $\mathfrak{P}$ es el único divisor primo de $\mathfrak{p}'$:

Teorema 2.42 *Sea E/D una extensión de Galois de dominios de Dedekind. Sea $\mathfrak{P}$ un primo en E y sea $\mathfrak{p} = \mathfrak{P} \cap D$. Sea F el dominio de descomposición de $\mathfrak{P}$ y sea $\mathfrak{p}' = \mathfrak{P} \cap F$. Entonces*

1. *$e = e(\mathfrak{P}/\mathfrak{p}') = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p}') = f(\mathfrak{P}/\mathfrak{p})$, $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$.*
2. *$\mathfrak{p}' = \mathfrak{P}^e$.*
3. *F es el menor dominio de Dedekind intermedio T entre D y E tal que $\mathfrak{P}$ es el único primo que divide a $\mathfrak{P} \cap T$.*

Demostración: En primer lugar observamos que E/F es una extensión de Galois cuyo grupo de Galois es $G_{\mathfrak{P}}$. Esto significa que $\mathfrak{P}$ es su único conjugado en esta extensión, luego por el teorema 2.39 tenemos que $\mathfrak{P}$ es el único primo de E que divide a $\mathfrak{p}'$.

1) Veamos que $f(\mathfrak{p}'/\mathfrak{p}) = 1$. Hemos de probar que el monomorfismo natural $D/\mathfrak{p} \longrightarrow F/\mathfrak{p}'$ es un isomorfismo, o sea, que todo elemento de F es congruente con un elemento de D módulo $\mathfrak{p}'$.

Sea $G = G(E/D)$. Si $\sigma \in G \setminus G_{\mathfrak{P}}$ entonces $\sigma(\mathfrak{P}) \neq \mathfrak{P}$, luego $\sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$. Como $\mathfrak{P}$ es el único primo que divide a $\mathfrak{p}'$ resulta que $\mathfrak{p}'_\sigma = \sigma^{-1}(\mathfrak{P}) \cap F \neq \mathfrak{p}'$.

Sea $\alpha \in F$. Por el teorema chino del resto existe un elemento $\beta \in F$ tal que

$$\begin{aligned} \beta &\equiv \alpha \ (\text{mód } \mathfrak{p}'), \\ \beta &\equiv 1 \ (\text{mód } \mathfrak{p}'_\sigma), \qquad \text{para todo } \sigma \in G \setminus G_{\mathfrak{P}}. \end{aligned}$$

En particular

$$\begin{aligned} \beta &\equiv \alpha \ (\text{mód } \mathfrak{P}), \\ \beta &\equiv 1 \ (\text{mód } \sigma^{-1}(\mathfrak{P})), \qquad \text{para todo } \sigma \in G \setminus G_{\mathfrak{P}}. \end{aligned}$$

La segunda congruencia implica que $\sigma(\beta) \equiv 1$ (mód $\mathfrak{P}$) para todo automorfismo $\sigma \in G \setminus G_{\mathfrak{P}}$. La norma de β en la extensión F/D es el producto de β por otros factores de la forma $\sigma(\beta)$ con $\sigma \in G \setminus G_{\mathfrak{P}}$, luego $\mathrm{N}(\beta) \equiv \alpha$ (mód $\mathfrak{P}$). Pero $\mathrm{N}(\beta) \in D$ y así $\mathrm{N}(\beta) - \alpha \in F \cap \mathfrak{P} = \mathfrak{p}'$, con lo que tenemos $\mathrm{N}(\beta) \equiv \alpha$ (mód $\mathfrak{p}'$) con $N(\beta) \in D$, que era lo que queríamos probar.

Así pues, $f(\mathfrak{p}'/\mathfrak{p}) = 1$. Por 2.32 concluimos que $f = f(\mathfrak{P}/\mathfrak{p}') = f(\mathfrak{P}/\mathfrak{p})$.

Ahora, el grado de la extensión E/F es el orden de $G_{\mathfrak{P}}$, que es ef (donde $e = e(\mathfrak{P}/\mathfrak{p})$). Por el teorema 2.40 (puesto que $r = 1$ para la extensión E/F) resulta que $e = e(\mathfrak{P}/\mathfrak{p}')$, y de la igualdad $e = e(\mathfrak{P}/\mathfrak{p}') = e(\mathfrak{P}/\mathfrak{p})$ se sigue, de nuevo por el teorema 2.32, que $e(\mathfrak{p}'/\mathfrak{p}) = 1$.

2) ya está probado.

3) Sea T un dominio de Dedekind intermedio tal que $\mathfrak{P}$ sea el único primo que divide a $\mathfrak{P} \cap T$. Esto significa que $\mathfrak{P}$ no tiene conjugados respecto a la extensión E/T, luego $G(E/T) \leq G_{\mathfrak{P}}$, luego $F \subset T$. ∎

Un caso especialmente notable se da cuando E/D es una extensión abeliana. Entonces si un primo $\mathfrak{p}$ en D se descompone en E como $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$, todos

los primos conjugados $\mathfrak{P}_i$ tienen el mismo cuerpo de descomposición F, por lo que la descomposición de $\mathfrak{p}$ en F es de la forma $\mathfrak{p} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_r$, con grados de inercia iguales a 1, y a su vez cada $\mathfrak{p}'_i$ factoriza en E como $\mathfrak{p}'_i = \mathfrak{P}_i^e$, de modo que $f(\mathfrak{P}_i/\mathfrak{p}'_i) = f(\mathfrak{P}_i/\mathfrak{p})$.

Si la extensión no es abeliana no podemos hablar en general de la descomposición intermedia $\mathfrak{p} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_r$, pero al menos tenemos una extensión E/F, distinta para cada primo $\mathfrak{P}_i$, donde éste ha perdido a sus conjugados conservando los números e y f.

Ejemplo Consideremos el cuerpo ciclotómico quinto $K = \mathbb{Q}(\omega)$ y tomemos un primo racional $p \equiv 4 \pmod 5$. Por el teorema 2.38 sabemos que su descomposición es $p = \mathfrak{p}_1\mathfrak{p}_2$, donde $\mathrm{N}(\mathfrak{p}_i) = p^2$. Por lo tanto, su cuerpo de descomposición tiene grado $r = 2$ sobre $\mathbb{Q}$, y, como la extensión es cíclica de orden 4, sólo hay un cuerpo intermedio, que es $L = K \cap \mathbb{R}$. Por consiguiente, sabemos que la factorización de p en L es de la forma $p = \mathfrak{p}'_1\mathfrak{p}'_2$, con $\mathrm{N}(\mathfrak{p}'_i) = p$ y a su vez cada $\mathfrak{p}'_i$ es primo en K.

Los primos $p \equiv 2, 3 \pmod 5$ se conservan primos en K, luego $r = 1$ y su cuerpo de descomposición es $\mathbb{Q}$. Lo mismo vale para $5 = \mathfrak{p}^4$, pues su factorización también cumple $r = 1$.

Finalmente, los primos $p \equiv 1 \pmod 5$ factorizan en la forma $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, con $\mathrm{N}(\mathfrak{p}_i) = p$, luego $r = 4$ y su cuerpo de descomposición es K. ∎

Ahora veremos que podemos separar e y f en dos extensiones sucesivas.

Si E/D es una extensión de Galois de dominios de Dedekind, $\mathfrak{p}$ es un primo en D y $\mathfrak{P}$ es un primo en E que divide a $\mathfrak{p}$, entonces cada $\sigma \in G_{\mathfrak{P}}$ induce de forma natural un $D/\mathfrak{p}$-automorfismo de $E/\mathfrak{P}$ dado por $\overline{\sigma}([\alpha]) = [\sigma(\alpha)]$ (es biyectivo porque tiene por inversa a la aplicación inducida por σ^{-1}). La aplicación $\sigma \mapsto \overline{\sigma}$ es un homomorfismo de grupos.

En general, la extensión $E/\mathfrak{P}$ sobre $D/\mathfrak{p}$ es normal y el homomorfismo anterior es un epimorfismo entre los grupos de Galois, pero la separabilidad puede perderse. Este problema no aparece en el caso de los cuerpos numéricos, pues en ellos los ideales primos dan cocientes finitos, luego perfectos. El teorema siguiente generaliza a [Al 9.5]:

Teorema 2.43 *Sea E/D una extensión de Galois de dominios de Dedekind con grupo de Galois G, sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$. Sean $\overline{E} = E/\mathfrak{P}$ y $\overline{D} = D/\mathfrak{p}$. Supongamos que la extensión $\overline{E}/\overline{D}$ es separable. Entonces $\overline{E}/\overline{D}$ es de Galois y la aplicación $\sigma \mapsto \overline{\sigma}$ descrita arriba es un epimorfismo de $G_{\mathfrak{P}}$ sobre $G(\overline{E}/\overline{D})$.*

Demostración: Veamos que la extensión $\overline{E}/\overline{D}$ es normal. Dada una clase $[\alpha] \in \overline{E}$, sea $p(x)$ el polinomio mínimo de α en la extensión E/D. Como la extensión es de Galois, $p(x)$ se escinde en factores lineales y todas las raíces son elementos de E (porque son conjugadas de α). Tomando clases módulo $\mathfrak{P}$ en la factorización de $p(x)$ llegamos a que $[\alpha]$ es la raíz de un polinomio de $\overline{D}[x]$ que se escinde en $\overline{E}[x]$, luego el polinomio mínimo de $[\alpha]$ también se escinde y la extensión es normal.

Sea F el dominio de descomposición de $\mathfrak{P}$. Sea $\mathfrak{p}' = \mathfrak{P} \cap F$. Por el teorema anterior $f(\mathfrak{p}'/\mathfrak{p}) = 1$, lo que significa que $D/\mathfrak{p} = F/\mathfrak{p}'$, o sea, que la extensión $\overline{E}/\overline{D}$ coincide con $\overline{E}/\overline{F}$. Por otra parte $G(E/F)_{\mathfrak{P}} = G(E/F) = G_{\mathfrak{P}}$, y todo esto nos da que podemos tomar como dominio base a F en lugar de D, es decir, podemos suponer que $G = G_{\mathfrak{P}}$.

Sea $[\alpha]$ un elemento primitivo de la extensión $\overline{E}/\overline{D}$ y sea $p(x)$ el polinomio mínimo de α sobre D. Entonces $p(x)$ se escinde en $E[x]$. Sean $\alpha_1, \ldots, \alpha_t$ todas sus raíces. Si $\overline{p}(x)$ es la imagen de $p(x)$ por el epimorfismo canónico de $D[x]$ sobre $\overline{D}[x]$ entonces $\overline{p}(x)$ se escinde en $\overline{E}[x]$ y sus raíces son $[\alpha_1], \ldots, [\alpha_t]$.

Un automorfismo $\tau \in G(\overline{E}/\overline{D})$ cumplirá $\tau([\alpha]) = [\alpha_i]$ para algún i, pero existe un automorfismo $\sigma \in G$ tal que $\sigma(\alpha) = \alpha_i$, luego $\bar{\sigma}([\alpha]) = [\alpha_i]$ y, como $[\alpha]$ es un elemento primitivo, esto implica que $\overline{\sigma} = \tau$. ∎

Definición 2.44 Sea E/D una extensión de Galois de dominios de Dedekind, sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$ de modo que $E/\mathfrak{p}$ sea una extensión separable de $D/\mathfrak{p}$. Llamaremos *grupo de inercia* de $\mathfrak{P}$ al núcleo $T_{\mathfrak{P}}$ del epimorfismo descrito en el teorema anterior.

El teorema nos da que $G_{\mathfrak{P}}/T_{\mathfrak{P}} \cong G(\overline{E}/\overline{D})$, y por lo tanto el orden de este grupo es f. Como $|G_{\mathfrak{P}}| = ef$ concluimos que $|T_{\mathfrak{P}}| = e$.

Teorema 2.45 *Sea E/D una extensión de Galois de grado n de dominios de Dedekind. Sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$. Supongamos que $\overline{E} = E/\mathfrak{P}$ es una extensión separable de $\overline{D} = D/\mathfrak{p}$. Sean F y Z los anillos de enteros de los cuerpos fijados por el grupo de descomposición y el grupo de inercia de $\mathfrak{p}$ respectivamente. Llamemos $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$ y r al número de primos que dividen a $\mathfrak{p}$ en E. Sean $\mathfrak{p}' = \mathfrak{P} \cap F$, $\mathfrak{p}'' = \mathfrak{P} \cap Z$. Entonces se tienen los datos contenidos en la tabla siguiente:*

Grado	r	f	e	
Anillo	D	F	Z	E
Primo	$\mathfrak{p}$	$\mathfrak{p}'$	$\mathfrak{p}''$	$\mathfrak{P}$
Índ. de ramificación	1	1	e	
Grado de inercia	1	f	1	

Demostración: Ya sabemos que los grados son los indicados en la tabla. Los valores de la extensión F/D están dados en el teorema 2.42. Consideremos los cuerpos $\overline{D} = \overline{F} \subset \overline{Z} \subset \overline{E}$. Según el teorema 2.43 tenemos un epimorfismo $G(E/F) \longrightarrow G(\overline{E}/\overline{D})$ cuyo núcleo es por definición $T_{\mathfrak{P}} = G(E/Z)$. Así pues, el epimorfismo correspondiente a $G(E/Z) \longrightarrow G(\overline{E}/\overline{Z})$ tiene imagen trivial, luego $\overline{Z} = \overline{E}$. Esto nos da que $f(\mathfrak{P}/\mathfrak{p}'') = 1$.

Por otra parte, todos los automorfismos de $G(E/Z)$ fijan a $\mathfrak{P}$, luego el grado $e = |E : Z|$ coincide con el orden del grupo de descomposición de esta extensión, o sea, con $e(\mathfrak{P}/\mathfrak{p}'')f(\mathfrak{P}/\mathfrak{p}'')$. Por consiguiente $e(\mathfrak{P}/\mathfrak{p}'') = e$.

Con esto tenemos comprobados los valores correspondientes a las extensiones F/D y E/Z. Los de la extensión Z/F se siguen del teorema 2.32. ∎

Más aún, el anillo de enteros Z asociado al grupo de inercia es la menor extensión de D en E tal que $\mathfrak{p}'' = \mathfrak{P} \cap Z$ cumple $\mathfrak{p}'' = \mathfrak{p}''^e$ y $f(\mathfrak{P}/\mathfrak{p}'') = 1$.

En efecto, si $D \subset Z' \subset E$ cumple lo mismo, el hecho de que $\mathfrak{p}''$ tenga un único factor primo en E implica que $F \subset Z'$, es decir, que $G(E/Z') \leq G_{\mathfrak{P}}$. A su vez, que el grado de inercia sea trivial se traduce en que $Z'/\mathfrak{p}''$ se identifica con $E/\mathfrak{P}$, luego todo $\sigma \in G(E/Z')$ induce la identidad $\bar{\sigma} = 1$ en $E/\mathfrak{P}$ (porque σ fija a todos los elementos de Z' y toda clase de $E/\mathfrak{P}$ tiene un representante en Z'). Por lo tanto, $G(E/Z') \leq T_{\mathfrak{P}}$, luego $Z \subset Z'$.

De nuevo la situación descrita por el teorema anterior resulta más clara en el caso de extensiones abelianas, donde los dominios F y Z son los mismos para todos los divisores de un mismo primo $\mathfrak{p}$ de D. Al pasar a F la descomposición de $\mathfrak{p}$ es, según ya sabíamos, de la forma

$$\mathfrak{p} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_r,$$

con $e(\mathfrak{p}'_i/\mathfrak{p}) = f(\mathfrak{p}'_i/\mathfrak{p}) = 1$. Al pasar a Z tenemos $\mathfrak{p}'_i = \mathfrak{p}''_i$, es decir, cada primo $\mathfrak{p}'_i$ se conserva primo en Z, pero el grado de inercia aumenta todo cuanto ha de aumentar de D a E. Finalmente, al pasar de Z a E tenemos $\mathfrak{p}''_i = \mathfrak{P}_i^e$, de manera que en este tramo se produce toda la ramificación sin que varíe el grado de inercia.

Ejemplo Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de orden $m = p^k m'$, donde $p \nmid m'$ y sea $\mathfrak{P}$ un divisor de p en K. Entonces el cuerpo de inercia de $\mathfrak{P}$ es el cuerpo ciclotómico $K' = \mathbb{Q}(\omega_{m'})$, donde $\omega_{m'} = \omega^{p^k}$ es una raíz m'-ésima primitiva de la unidad.

En efecto, el teorema 2.38 nos da que si $\mathfrak{p}$ es un divisor de p en K y $\mathfrak{p}'$ es el primo de K' divisible entre $\mathfrak{P}$, entonces

$$f(\mathfrak{p}/p) = f(\mathfrak{p}'/p) = o_{m'}(p), \qquad e(\mathfrak{p}/p) = \phi(p^k), \quad e(\mathfrak{p}'/p) = 1,$$

luego el número de factores primos de p en ambas extensiones es el mismo

$$r = \phi(m)/\phi(p^k)f = \phi(m')/f.$$

Por lo tanto, $\mathfrak{p}' = \mathfrak{p}^e$, y la observación posterior a 2.45 implica que K' está contenido en el cuerpo de inercia. Como ambas extensiones tienen grado $\phi(m')$ sobre $\mathbb{Q}$, de hecho son iguales. ∎

Enteros ciclotómicos reales La factorización en los anillos de enteros ciclotómicos reales de orden primo está determinada por el teorema siguiente:

Teorema 2.46 *Sea K el cuerpo ciclotómico de orden p y sea $K' = K \cap \mathbb{R}$, que es un cuerpo numérico de grado $m = (p-1)/2$. La factorización de p en K' es de la forma $p = \mathfrak{p}^m$, donde $\mathrm{N}(\mathfrak{p}) = p$. Si q es un primo racional distinto de p, y $f = \mathrm{o}_p(q)$, entonces q factoriza en K' de la forma*

$$q = \mathfrak{q}_1 \cdots \mathfrak{q}_r,$$

donde los primos $\mathfrak{q}_i$ son distintos dos a dos y $\mathrm{N}(\mathfrak{q}_i) = q^f$ si f es impar o bien $\mathrm{N}(\mathfrak{q}_i) = q^{f/2}$ si f es par.

DEMOSTRACIÓN: El teorema 2.38 nos da que la descomposición de p en K es $p = \mathfrak{P}^{p-1}$, luego, si llamamos $p = \mathfrak{P} \cap K'$, tenemos que

$$p - 1 = 2m = e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p),$$

donde el primer factor divide a 2 y el segundo a m, luego necesariamente $e(\mathfrak{P}/\mathfrak{p}) = 2$ y $e(\mathfrak{p}/p) = m$. Esto hace a su vez que $f(\mathfrak{p}/p) = 1$, luego la factorización de p es la indicada.

Supongamos ahora que $q \neq p$. Entonces la factorización de q en K es de la forma $q = \mathfrak{Q}_1 \cdots \mathfrak{Q}_r$, con $f(\mathfrak{Q}_i/q) = f$ y $r = (p-1)/f$. Si $\mathfrak{q}_i = \mathfrak{Q}_i \cap K'$, tenemos que

$$f = f(\mathfrak{Q}_i/q) = f(\mathfrak{Q}_i/\mathfrak{q}_i)f(\mathfrak{q}_i/q),$$

donde el primer factor divide a 2. Si f es impar, necesariamente $f(\mathfrak{Q}_i/\mathfrak{q}_i) = 1$, luego $f(\mathfrak{q}_i/q) = f$ y, como $2m = rf$, r tiene que ser par y la factorización de q es la indicada con $r/2$ factores (los $\mathfrak{q}_i$ no son distintos entre sí, sino que cada uno divide a dos primos $\mathfrak{Q}_i$).

Supongamos finalmente que f es par. Entonces tenemos un isomorfismo $G_{\mathfrak{Q}_i} \longrightarrow G(\overline{K}_{\mathfrak{Q}_i}/\overline{\mathbb{Q}}_q)$ (porque el grupo de inercia $T_{\mathfrak{Q}_i}$ es trivial, ya que su orden es $e(\mathfrak{Q}_i/q) = 1$). Como el grupo $G_{\mathfrak{Q}_i}$ tiene orden par, contiene un elemento de orden 2, pero $G(K/\mathbb{Q})$ es un grupo cíclico de orden $p-1$, que tiene un único elemento σ de orden 2 (la conjugación compleja, cuyo cuerpo fijado es precisamente K'). Así pues, $\sigma \in G_{\mathfrak{Q}_i}$, luego $\mathfrak{Q}_i$ está fijado por todos los automorfismos de $G(K/K')$ (que son σ y 1), luego $\mathfrak{q}_i$ no tiene más divisor primo en K que $\mathfrak{Q}_i$, luego la relación $n = rfe$ para la extensión K/K' (con $n = 2$, $r = e = 1$) nos da que $f(\mathfrak{Q}_i/\mathfrak{q}_i) = 2$, luego $f(\mathfrak{q}_i/q) = f/2$. ∎

2.5 Normas de ideales

Ahora estamos en condiciones de definir una norma sobre los ideales fraccionales en cualquier extensión de dominios de Dedekind. Como ya habíamos observado, en el caso de un primo $\mathfrak{p}$ de un cuerpo numérico la norma viene dada por $\mathrm{N}(\mathfrak{p}) = p^f$, donde p es el único primo racional divisible entre p y f es el grado de inercia. La definición general sigue esta línea:

Definición 2.47 Sea E/D una extensión de dominios de Dedekind. Para cada primo $\mathfrak{P}$ de E definimos $\mathrm{N}_D^E(\mathfrak{P}) = \mathfrak{p}^f$, donde $\mathfrak{p} = \mathfrak{P} \cap D$ y $f = f(\mathfrak{P}/\mathfrak{p})$. Esta norma se extiende de forma única a un homomorfismo del grupo de los ideales fraccionales de E en el grupo de los ideales fraccionales de D. La norma de un ideal de E es un ideal de D.

Del teorema 2.32 se sigue que si tenemos dos extensiones F/E y E/D entonces $\mathrm{N}_D^F(\mathrm{N}_F^E(\mathfrak{a})) = \mathrm{N}_D^E(\mathfrak{a})$ para todo ideal fraccional $\mathfrak{a}$ de E. (Se prueba primero para ideales primos).

El teorema siguiente recoge otras propiedades básicas de la norma:

Teorema 2.48 *Sea E/D una extensión de dominios de Dedekind de grado n. Entonces*

1. *Si $\mathfrak{a}$, $\mathfrak{b}$ son ideales fraccionales de E, entonces $\mathrm{N}_D^E(\mathfrak{ab}) = \mathrm{N}_D^E(\mathfrak{a})\,\mathrm{N}_D^E(\mathfrak{b})$.*
2. *Si $\mathfrak{a}$, $\mathfrak{b}$ son ideales de E y $\mathfrak{a} \mid \mathfrak{b}$, entonces $\mathrm{N}_D^E(\mathfrak{a}) \mid \mathrm{N}_D^E(\mathfrak{b})$.*
3. *Si $\mathfrak{a}$ es un ideal de E, entonces $\mathfrak{a} \mid \mathrm{N}_D^E(\mathfrak{a})$. En particular, si $\mathrm{N}_D^E(\mathfrak{a}) = 1$, también $\mathfrak{a} = 1$.*
4. *Si $\mathfrak{a}$ es un ideal de E tal que $\mathrm{N}_D^E(\mathfrak{a})$ es primo, entonces $\mathfrak{a}$ es primo.*
5. *Si $\mathfrak{a}$ es un ideal fraccional de D se cumple que $\mathrm{N}_D^E(\mathfrak{a}) = \mathfrak{a}^n$.*
6. *Si la extensión E/D es de Galois y $G = G(E/D)$ entonces*
$$\mathrm{N}_D^E(\mathfrak{a}) = \prod_\sigma \sigma(\mathfrak{a}).$$
7. *Si $\alpha \neq 0$ está en el cuerpo de cocientes de E entonces $\mathrm{N}_D^E(\alpha E) = \mathrm{N}_D^E(\alpha)D$.*
8. *Sólo un número finito de ideales de E pueden tener la misma norma.*

Demostración: 1) Es consecuencia inmediata de la definición de norma.

2) Consecuencia inmediata de 1).

3) Basta probarlo cuando $\mathfrak{a} = \mathfrak{P}$ es primo, pero entonces es trivial, pues si $\mathfrak{p}$ es el primo de D divisible entre $\mathfrak{P}$, tenemos que $\mathfrak{P} \mid \mathfrak{p} \mid \mathfrak{p}^f = \mathrm{N}_D^E(\mathfrak{P})$.

4) Por 1) y 3), una factorización no trivial de $\mathfrak{a}$ daría lugar a una factorización no trivial de su norma.

5) Basta probarlo cuando $\mathfrak{a}$ es primo, en cuyo caso basta tener en cuenta el teorema 2.34.

6) Basta probarlo para un ideal primo $\mathfrak{P}$. Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ los conjugados de $\mathfrak{P}$ y sea $\mathfrak{q}$ el primo de D al que dividen. Teniendo en cuenta las observaciones hechas tras la definición 2.41, es claro que cuando σ recorre G la expresión $\sigma(\mathfrak{P})$ toma el valor $\mathfrak{P}_i$ exactamente $|G_\mathfrak{P}| = ef$ veces. Por lo tanto

$$\prod_{\sigma\in G} \sigma(\mathfrak{p}) = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{ef} = \mathfrak{q}^f = \mathrm{N}_D^E(\mathfrak{P}).$$

7) Supongamos en primer lugar que E/D es separable y sea F la menor extensión de Galois sobre D que contiene a E. Por el apartado anterior

$$\mathrm{N}_D^F(\alpha F) = \prod_{\sigma\in G} \sigma(\alpha F) = \prod_{\sigma\in G} \sigma(\alpha)F = \mathrm{N}_D^F(\alpha)F = \mathrm{N}_D^F(\alpha)D.$$

(El último paso se debe a la identificación entre ideales de F e ideales de D). Por lo tanto

$$\mathrm{N}_D^E(\mathrm{N}_E^F(\alpha F)) = \mathrm{N}_D^E(\mathrm{N}_E^F(\alpha))D,$$

pero si $m = |F : E|$ esto equivale a

$$\mathrm{N}_D^E((\alpha E)^m) = \mathrm{N}_D^E(\alpha^m)D,$$

de donde $\mathrm{N}_D^E(\alpha E)^m = (\mathrm{N}_D^E(\alpha)D)^m$, y por la factorización única ideal concluimos que $\mathrm{N}_D^E(\alpha E) = \mathrm{N}_D^E(\alpha)D$.

Si E/D no es separable, consideramos la clausura separable K del cuerpo de cocientes de D en el cuerpo de cocientes de E. Por el teorema 2.26, la clausura entera F de D en K es una extensión de D y obviamente E/F también es una extensión de dominios de Dedekind (E es finitamente generado sobre D, luego también sobre F). La transitividad de las normas y el caso ya probado reducen el problema a la extensión puramente inseparable E/F. Sea m el grado de la extensión. Entonces, todo $\alpha \in E$ cumple que $\alpha^m \in F$, luego por el apartado 5) tenemos que

$$\mathrm{N}_F^E(\alpha E)^m = \mathrm{N}_F^E(\alpha^m E) = \alpha^{m^2} F = \big(\mathrm{N}_F^E(\alpha)F\big)^m.$$

Como en el caso anterior, podemos eliminar la m de ambos miembros.

8) Por 3), pues un ideal de E sólo tiene un número finito de divisores. ∎

La norma de un ideal de un cuerpo numérico coincide con el número de elementos del anillo cociente que determina. Esto puede usarse para definir una norma sobre los ideales de cualquier dominio de Dedekind con tal de que los anillos cociente sean finitos. Como éste será el caso en todos los dominios de Dedekind que nos van a interesar, conviene definir esta norma en un contexto general.

Definición 2.49 Diremos que un dominio de Dedekind D tiene *restos finitos* si para todo ideal primo $\mathfrak{p}$ de D se cumple que el cuerpo de restos $D/\mathfrak{p}$ es finito. En tal caso definimos la *norma absoluta* de $\mathfrak{p}$ como $\mathrm{N}\,\mathfrak{p} = |D/\mathfrak{p}|$. La norma absoluta se extiende multiplicativamente a todos los ideales fraccionales de D, de modo que, por definición $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$.

De este modo, si $\mathfrak{a}$ es un ideal fraccional, se cumple que $\mathrm{N}\,\mathfrak{a}$ es un número racional positivo, y es un número natural si $\mathfrak{a}$ es un ideal.

El teorema 2.24 implica que si $\mathfrak{p}$ es un primo de un dominio de Dedekind D con restos finitos y $D_\mathfrak{p}$ es la localización en $\mathfrak{p}$, entonces $D_\mathfrak{p}$ tiene restos finitos y, si $\mathfrak{m}$ es su único ideal maximal, se cumple $\mathrm{N}\,\mathfrak{m}^n = \mathrm{N}\,\mathfrak{p}^n$ para todo número entero n.

Teorema 2.50 *Sea D un dominio de Dedekind con restos finitos y sea $\mathfrak{a}$ un ideal de D. Entonces $\mathrm{N}\,\mathfrak{a} = |D/\mathfrak{a}|$.*

Demostración: La prueba es una variante de la del teorema 2.34. Supongamos primero que $\mathfrak{a} = \mathfrak{p}^e$. Sea p la característica de $D/\mathfrak{p}$ (que claramente es la misma que la del anillo $D/\mathfrak{p}^e$). Podemos localizar en $\mathfrak{p}$ y suponer que éste es el único ideal primo de D. Entonces

$$1 = \mathfrak{p}^e/\mathfrak{p}^e \subset \mathfrak{p}^{e-1}/\mathfrak{p}^e \subset \cdots \subset \mathfrak{p}^2/\mathfrak{p}^e \subset \mathfrak{p}/\mathfrak{p}^e \subset D/\mathfrak{p}^e,$$

y cada término es un subespacio vectorial de $D/\mathfrak{p}^e$ (considerado como espacio vectorial sobre $\mathbb{Z}/p\mathbb{Z}$). Como en el teorema 2.34 se prueba que cada cociente entre dos subespacios consecutivos es isomorfo a $D/\mathfrak{p}$, con lo que

$$|D/\mathfrak{p}^e| = |D/\mathfrak{p}|^e = (\mathrm{N}\,\mathfrak{p})^e = \mathrm{N}\,\mathfrak{p}^e.$$

En general, si $\mathfrak{a} = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$, la aplicación $D \longrightarrow \prod_{i=1}^{r} E/\mathfrak{p}_i^{e_i}$ que a cada elemento de D le asigna la r-tupla de sus clases módulo $\mathfrak{p}_i^{e_i}$ es un homomorfismo de anillos suprayectivo, por el teorema chino del resto, y su núcleo es obviamente igual a $\mathfrak{a}$. Así pues tenemos un isomorfismo

$$D/\mathfrak{a} \cong \prod_{i=1}^{r} E/\mathfrak{p}_i^{e_i}$$

de donde concluimos que

$$|D/\mathfrak{a}| = |\prod_{i=1}^{r} E/\mathfrak{p}_i^{e_i}| = \prod_{i=1}^{r} \mathrm{N}\,\mathfrak{p}_i^{e_i} = \mathrm{N}\,\mathfrak{a}.$$

■

En el caso del orden maximal de un cuerpo numérico, el teorema 1.15 implica que la norma absoluta coincide con que ya teníamos definida para módulos y, en particular, con la definida en [Al 8.33].

Observemos que si D es un dominio de Dedekind con restos finitos y E es una extensión de D, entonces E también tiene restos finitos, pues si $\mathfrak{P}$ es un primo en E y $\mathfrak{p}$ es el primo en D al cual divide, entonces $E/\mathfrak{P}$ es una extensión finita del cuerpo finito $D/\mathfrak{p}$, luego también es un cuerpo finito. Más aún, se cumple $\mathrm{N}\,\mathfrak{P} = (\mathrm{N}\,\mathfrak{p})^f$, donde $f = f(\mathfrak{P}/\mathfrak{q})$.

En particular, si aplicamos esto al caso en que $E = \mathcal{O}_K$ es el orden maximal de un cuerpo numérico K y $D = \mathbb{Z}$, tenemos que para cada primo $\mathfrak{P}$ de E, si $p \in \mathbb{Z}$ es el primo racional divisible entre $\mathfrak{P}$, se cumple que

$$(\mathrm{N}\,\mathfrak{P}) = (p)^f = \mathrm{N}_{\mathbb{Z}}^{\mathcal{O}_K}(\mathfrak{P}),$$

y esto implica a su vez que la igualdad $\mathrm{N}_{\mathbb{Z}}^{\mathcal{O}_K}(\mathfrak{a}) = (\mathrm{N}\,\mathfrak{a})$ es válida para ideales fraccionales cualesquiera, de modo que la norma absoluta N es esencialmente la misma que $\mathrm{N}_{\mathbb{Z}}^{\mathcal{O}_K}$, con la única diferencia de que una está definida como un número natural y la otra como el ideal que genera. En particular, el teorema 2.48 es válido para la norma absoluta de un cuerpo numérico.

Definición 2.51 Sea D un dominio de Dedekind con restos finitos. Llamaremos *función de Euler generalizada* de D a la función que a cada ideal $\mathfrak{a}$ de D le hace corresponder el orden $\Phi(\mathfrak{a})$ del grupo $(D/\mathfrak{a})^*$ de las unidades módulo $\mathfrak{a}$.

Es inmediato que $(D/\mathfrak{a})^*$ está formado por las clases de los $\alpha \in D$ que cumplen $\mathfrak{a} + (\alpha) = 1$. El teorema siguiente nos permite calcular fácilmente la función de Euler:

Teorema 2.52 *Sea D un dominio de Dedekind con restos finitos.*

1. *Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de D tales que $(\mathfrak{a},\mathfrak{b}) = 1$ entonces $\Phi(\mathfrak{ab}) = \Phi(\mathfrak{a})\Phi(\mathfrak{b})$.*
2. *Si $\mathfrak{p}$ es un ideal primo de D, entonces $\Phi(\mathfrak{p}^e) = \big(\mathrm{N}(\mathfrak{p}) - 1\big)\,\mathrm{N}\big(\mathfrak{p}\big)^{e-1}$.*

Demostración: 1) basta tener en cuenta que el teorema chino del resto [Al 3.54] nos da un isomorfismo de anillos

$$D/(\mathfrak{ab}) \longrightarrow (D/\mathfrak{a}) \times (D/\mathfrak{b}),$$

que se restringe a un isomorfismo entre los grupos de unidades, luego concluimos que $(D/(\mathfrak{ab}))^* \cong (D/\mathfrak{a})^* \times (D/\mathfrak{b})^*$.

2) Sea $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Si α recorre un conjunto de representantes de las $\mathrm{N}(\mathfrak{p}^e)$ clases módulo $\mathfrak{p}^e$ y β recorre un conjunto de representantes de las $\mathrm{N}(\mathfrak{p})$ clases módulo $\mathfrak{p}$, es claro que los elementos $\alpha + \pi^e\beta$ son no congruentes dos a dos módulo $\mathfrak{p}^{e+1}$, y como hay $\mathrm{N}(\mathfrak{p})^{e+1}$ de ellos, concluimos que forman un conjunto de representantes de las clases módulo $\mathfrak{p}^{e+1}$. También es claro que $\mathfrak{p} \mid \alpha + \pi^e\beta$ si y sólo si $\mathfrak{p} \mid \alpha$.

Por lo tanto, para cada unidad $[\alpha]$ módulo $\mathfrak{p}^e$ hay $\mathrm{N}(\mathfrak{p})$ unidades $[\alpha + \pi^e\beta]$ módulo $\mathfrak{p}^{e+1}$, es decir, se cumple $\Phi(\mathfrak{p}^{e+1}) = \mathrm{N}(\mathfrak{p})\Phi(\mathfrak{p}^e)$. Ahora sólo queda notar que $\Phi(\mathfrak{p}) = \mathrm{N}(\mathfrak{p}) - 1$ porque $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo. ∎

2.6 Factorización ideal en órdenes no maximales

Los órdenes no maximales de los cuerpos numéricos comparten algunas propiedades básicas con los maximales:

Teorema 2.53 *Sea $\mathcal{O}$ un orden de un cuerpo numérico. Entonces:*

1. *$\mathcal{O}$ es un anillo noetheriano.*
2. *Si $\mathfrak{a}$ es un ideal no nulo de $\mathcal{O}$, entonces el anillo cociente $\mathcal{O}/\mathfrak{a}$ es finito.*
3. *Si $\mathfrak{p}$ es un ideal primo no nulo de $\mathcal{O}$, entonces es maximal.*

Demostración: 1) Sabemos que $\mathcal{O}$ es un $\mathbb{Z}$-módulo libre finitamente generado. En particular es de la forma $\mathbb{Z}[a_1,\ldots,a_d]$, luego es noetheriano.

2) Por 1.9 sabemos que $\mathfrak{a}$ es un ideal no nulo, entonces es un módulo completo, y todos los elementos de $\mathcal{O}$ son coeficientes de $\mathfrak{a}$, luego su anillo de coeficientes es un orden $\mathcal{O}'$ tal que $\mathcal{O} \subset \mathcal{O}'$. Por 1.15 sabemos que $\mathcal{O}'/\mathfrak{a}$ es finito, luego $\mathcal{O}/\mathfrak{a}$ también lo es.

3) Si $\mathfrak{p}$ es primo, entonces $\mathcal{O}/\mathfrak{p}$ es un dominio íntegro finito, luego es un cuerpo [Al 3.40], luego $\mathfrak{p}$ es maximal. ∎

En particular, vemos que todos los órdenes numéricos cumplen dos de las tres propiedades necesarias para ser dominios de Dedekind, pero los no maximales

incumplen trivialmente la tercera: no son dominios íntegros, luego no pueden ser ni dominios de Dedekind ni dominios de factorización única. Sin embargo los fallos de la factorización ideal son mínimos y pueden ser 'acotados', como vamos a ver aquí.

Definición 2.54 Sea $\mathcal{O}$ el orden maximal de un cuerpo numérico K y $\mathcal{O}'$ cualquier orden de K. Llamaremos *conductor* de $\mathcal{O}'$ al conjunto

$$\mathfrak{f} = \{\alpha \in \mathcal{O}' \mid \alpha\mathcal{O} \subset \mathcal{O}'\}.$$

La 'f' proviene del alemán 'Führer'. El teorema siguiente contiene algunas propiedades y caracterizaciones sencillas sobre este concepto.

Teorema 2.55 *Sea K un cuerpo numérico, sea $\mathcal{O}$ su orden maximal y sea $\mathcal{O}'$ un orden de K de índice m. Sea $\mathfrak{f}$ el conductor de $\mathcal{O}'$. Entonces:*

1. *$\mathfrak{f}$ es un ideal no nulo tanto de $\mathcal{O}$ como de $\mathcal{O}'$. Además $\mathfrak{f} \mid m$.*
2. *Para todo $\alpha \in \mathcal{O}$, si $\alpha \equiv 1 \pmod{\mathfrak{f}}$ entonces $\alpha \in \mathcal{O}'$.*
3. *$\mathfrak{f}$ es el máximo común divisor de todos los ideales $\mathfrak{a}$ de $\mathcal{O}$ que cumplen la propiedad anterior, y también el de los que cumplen $\mathfrak{a} \subset \mathcal{O}'$.*

DEMOSTRACIÓN: 1) Es claro que $\mathfrak{f}$ es un ideal. Además, como $|\mathcal{O}/\mathcal{O}'| = m$, tenemos que $m\alpha \in \mathcal{O}'$ para todo $\alpha \in \mathcal{O}$, luego $m \in \mathfrak{f}$.

2) Es evidente, al igual que la segunda parte de 3). Respecto a la primera basta probar que un ideal $\mathfrak{a}$ de $\mathcal{O}$ cumple $\mathfrak{a} \subset \mathcal{O}'$ si y sólo si cumple 2). En efecto, si $\mathfrak{a}$ cumple 2) y $\alpha \in \mathfrak{a}$, entonces $\alpha + 1 \equiv 1 \pmod{\mathfrak{a}}$, luego $\alpha + 1 \in \mathcal{O}'$, luego $\alpha \in \mathcal{O}'$. La implicación opuesta es obvia. ∎

Si $\mathcal{O}$ es un orden numérico y $\mathfrak{f}$ es un ideal de $\mathcal{O}$, definimos $I_{\mathfrak{f}}(\mathcal{O})$ como el conjunto de todos los ideales $\mathfrak{a}$ de $\mathcal{O}$ tales que $\mathfrak{a} + \mathfrak{f} = \mathcal{O}$.

Teorema 2.56 *Sea K un cuerpo numérico, sea $\mathcal{O}$ su orden maximal y sea $\mathcal{O}'$ un orden cualquiera de K de conductor $\mathfrak{f}$. Entonces:*

1. *La aplicación $i : I_{\mathfrak{f}}(\mathcal{O}') \longrightarrow I_{\mathfrak{f}}(\mathcal{O})$ dada por $i(\mathfrak{a}) = \mathfrak{a}\mathcal{O}$ es biyectiva, y su inversa viene dada por $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}'$.*
2. *Las correspondencias anteriores conservan productos e inclusiones, y hacen corresponder ideales primos con ideales primos.*
3. *Todo ideal de $I_{\mathfrak{f}}(\mathcal{O}')$ se descompone de forma única salvo el orden como producto de ideales primos (que de hecho son maximales).*

DEMOSTRACIÓN: Observemos en primer lugar que si $\mathfrak{a} \in I_{\mathfrak{f}}(\mathcal{O}')$, entonces

$$\mathcal{O} = \mathcal{O}'\mathcal{O} = (\mathfrak{a} + \mathfrak{f})\mathcal{O} = \mathfrak{a}\mathcal{O} + \mathfrak{f}\mathcal{O} = i(\mathfrak{a}) + \mathfrak{f},$$

luego $i(\mathfrak{a}) \in I_{\mathfrak{f}}(\mathcal{O})$. De modo similar se comprueba que el producto de elementos de $I_{\mathfrak{f}}(\mathcal{O}')$ está en $I_{\mathfrak{f}}(\mathcal{O}')$ y que i conserva productos.

Para probar que i es inyectiva basta ver que $\mathfrak{a} = i(\mathfrak{a}) \cap \mathcal{O}'$. En efecto:

$$\mathfrak{a} \subset i(\mathfrak{a}) \cap \mathcal{O}' = i(\mathfrak{a}) \cap (\mathfrak{a} + \mathfrak{f}) = \mathfrak{a} + (i(\mathfrak{a}) \cap \mathfrak{f}) = \mathfrak{a} + i(\mathfrak{a})\mathfrak{f} = \mathfrak{a} + \mathfrak{a}\mathfrak{f} = \mathfrak{a}.$$

Hemos usado que $i(\mathfrak{a}) \cap \mathfrak{f} = \mathrm{mcm}(i(\mathfrak{a}), \mathfrak{f}) = i(\mathfrak{a})\mathfrak{f}$, porque los ideales son primos entre sí, así como que $i(\mathfrak{a})\mathfrak{f} = (\mathfrak{a}\mathcal{O})\mathfrak{f} = \mathfrak{a}(\mathcal{O}\mathfrak{f}) = \mathfrak{a}\mathfrak{f}$.

Para probar que i es suprayectiva y que su inversa es la indicada basta ver que si $\mathfrak{a} \in I_{\mathfrak{f}}(\mathcal{O})$ entonces $\mathfrak{a} \cap \mathcal{O}' \in I_{\mathfrak{f}}(\mathcal{O}')$ y que $i(\mathfrak{a} \cap \mathcal{O}') = \mathfrak{a}$.

En efecto, la primera afirmación es inmediata, y en cuanto a la segunda tenemos

$$\begin{aligned} \mathfrak{a} &= \mathfrak{a}\mathcal{O}' = \mathfrak{a}\big((\mathfrak{a} \cap \mathcal{O}') + \mathfrak{f}\big) = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}') + \mathfrak{a}\mathfrak{f} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}') + \mathfrak{a}\mathfrak{f} \\ &= \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}') + (\mathfrak{a} \cap \mathfrak{f}) = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}') + (\mathfrak{a} \cap \mathcal{O}') \cap \mathfrak{f} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O}') + (\mathfrak{a} \cap \mathcal{O}')\mathfrak{f} \\ &= (\mathfrak{a} + \mathfrak{f})(\mathfrak{a} \cap \mathcal{O}') = \mathcal{O}(\mathfrak{a} \cap \mathcal{O}') = i(\mathfrak{a} \cap \mathcal{O}'). \end{aligned}$$

En la última igualdad de la segunda línea hemos usado un hecho general: si dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ de un dominio A cumplen $\mathfrak{a} + \mathfrak{b} = 1$, entonces $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. En efecto:

$$\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b})\mathfrak{a} + (\mathfrak{a} \cap \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}.$$

El hecho de que las correspondencias de 1) hagan corresponder los ideales primos es consecuencia inmediata de que para todo $\mathfrak{a} \in I_{\mathfrak{f}}(\mathcal{O})$ se cumple

$$\mathcal{O}'/(\mathcal{O}' \cap \mathfrak{a}) \cong \mathcal{O}/\mathfrak{a}. \tag{2.2}$$

En efecto, el homomorfismo natural $\mathcal{O}' \longrightarrow \mathcal{O}/\mathfrak{a}$ dada por $\alpha \mapsto \alpha + \mathfrak{a}$ tiene núcleo $\mathcal{O}' \cap \mathfrak{a}$, y el hecho de que $\mathcal{O} = \mathfrak{a} + \mathfrak{f}$ implica que es suprayectivo.

El apartado 3) es consecuencia inmediata de los dos anteriores, ya probados ∎

El teorema anterior implica que podemos hablar de divisibilidad, exponente de un primo en un ideal, máximo común divisor, mínimo común múltiplo, etc. siempre y cuando nos restrinjamos a ideales de $I_{\mathfrak{f}}(\mathcal{O}')$. También podemos simplificar ideales no nulos, etc.

No podemos interpretar el isomorfismo (2.2) como que las correspondencias entre ideales conservan las normas. Esto sólo es cierto sobre ideales de $I_{\mathfrak{f}}(\mathcal{O}')$ cuyo anillo de coeficientes sea precisamente $\mathcal{O}'$. El teorema siguiente muestra un caso particular de esta situación.

Teorema 2.57 *Sea K un cuerpo numérico, sea $\mathcal{O}$ su orden maximal y sea $\mathcal{O}'$ un orden de K de índice m. Sea $\mathfrak{f}$ el conductor de $\mathcal{O}'$. Entonces:*

1. $I_m(\mathcal{O}') \subset I_{\mathfrak{f}}(\mathcal{O}')$.
2. $I_m(\mathcal{O}')$ *es el conjunto de los ideales $\mathfrak{a}$ de $\mathcal{O}'$ tales que* $(\mathrm{N}(\mathfrak{a}), m) = 1$.
3. *Todos los ideales de $I_m(\mathcal{O}')$ tienen anillo de coeficientes $\mathcal{O}'$.*
4. *La biyección del teorema anterior hace corresponder $I_m(\mathcal{O}')$ con $I_m(\mathcal{O})$ y conserva normas.*

DEMOSTRACIÓN: Por $I_m(\mathcal{O}')$ entendemos el conjunto de ideales $\mathfrak{a}$ de $\mathcal{O}'$ tales que $\mathfrak{a}+m\mathcal{O}'=\mathcal{O}'$ (es importante distinguir entre el ideal generado por m en $\mathcal{O}'$ y en $\mathcal{O}$). La propiedad 1) es evidente. Para probar 2) consideramos un ideal $\mathfrak{a}$ de $\mathcal{O}'$ tal que $\mathfrak{a}+(m)=\mathcal{O}'$. Sea $\mathcal{O}''$ su anillo de coeficientes. Entonces m es una unidad de $\mathcal{O}''/\mathfrak{a}$. Si existiera un primo p que dividiera a $\mathrm{N}(\mathfrak{a})$ y a m, entonces p también sería una unidad de $\mathcal{O}''/\mathfrak{a}$, pero por otra parte es un divisor de cero. Así pues, $(\mathrm{N}(\mathfrak{a}),m)=1$. La otra implicación es clara, teniendo en cuenta que $\mathrm{N}(\mathfrak{a})\in\mathfrak{a}$.

3) Sea $\mathfrak{a}$ es un ideal de $\mathcal{O}'$ tal que $(\mathrm{N}(\mathfrak{a}),m)=1$ y sea $\mathcal{O}''$ a su anillo de coeficientes. Tenemos que $\mathfrak{a}\subset\mathcal{O}'\subset\mathcal{O}''\subset\mathcal{O}$. Llamemos $k=|\mathcal{O}'':\mathcal{O}'|$. Entonces k divide a $\mathrm{N}(\mathfrak{a})=|\mathcal{O}'':\mathfrak{a}|$ y a $m=|\mathcal{O}:\mathcal{O}'|$, luego $k=1$ y en consecuencia $\mathcal{O}''=\mathcal{O}'$.

4) El isomorfismo (2.2) implica que la correspondencia i envía ideales de $I_m(\mathcal{O}')$ a ideales de $I_m(\mathcal{O})$, así como que conserva normas. Sólo falta añadir que todo ideal de $I_m(\mathcal{O})$ tiene su antiimagen en $I_m(\mathcal{O}')$. Basta probarlo para ideales primos, ahora bien, si $\mathfrak{p}$ es un primo de norma prima con m, entonces la norma de $\mathfrak{p}\cap\mathcal{O}'$ es potencia del único primo que contiene, que es el mismo que contiene $\mathfrak{p}$, luego no divide a m. ∎

En general no es fácil determinar el conductor de un orden numérico, pero el teorema anterior nos determina un conjunto suficientemente grande de ideales en el que tenemos asegurada la factorización única. Para los cuerpos cuadráticos esto no supone ninguna restricción:

Teorema 2.58 *Sea $K=\mathbb{Q}(\sqrt{d}\,)$ un cuerpo cuadrático y m un número natural no nulo. Entonces el conductor del orden $\mathcal{O}_m$ definido en* 1.17 *es $\mathfrak{f}=m\mathcal{O}$.*

DEMOSTRACIÓN: Según la definición de $\mathcal{O}_m$ es obvio que $\mathcal{O}_m\subset\mathbb{Z}+(m)$. Teniendo en cuenta además que $(m)\subset\mathfrak{f}$ vemos que

$$\mathfrak{f}=\mathfrak{f}\cap\big(\mathbb{Z}+(m)\big)\subset(\mathfrak{f}\cap\mathbb{Z})+(m)=(m)+(m)=(m).$$

Hemos usado que si $u\in\mathfrak{f}\cap\mathbb{Z}$ entonces $u\mathcal{O}\subset\mathcal{O}_m$ (por definición de $\mathfrak{f}$), y esto sólo es posible si $m\mid u$. ∎

Así, los teoremas 2.56 y 2.57 muestran que, en un cuerpo cuadrático, los ideales de $I_m(\mathcal{O})$ se corresponden con los ideales de $I_{\mathfrak{f}}(\mathcal{O}_m)$ y también con los de $I_m(\mathcal{O}_m)$, luego ambos conjuntos —que en principio son distintos— coinciden. Concluimos, pues, que en el orden $\mathcal{O}_m$ tenemos factorización única exactamente en el conjunto $I_m(\mathcal{O}_m)$ de los ideales de norma prima con m.

Ejercicio: Probar que en el orden $\mathbb{Z}\big[\sqrt{-3}\,\big]$ los ideales $\big(2\big)$, $\big(1-\sqrt{-3}\,\big)$ y $\big(1+\sqrt{-3}\,\big)$ son distintos, tienen norma 4, su anillo de coeficientes es $\mathbb{Z}\big[\sqrt{-3}\,\big]$ y los tres están contenidos en un único ideal propio: $\big(2,1+\sqrt{-3}\,\big)$. El cuadrado de éste último tiene índice 8 en $\mathbb{Z}\big[\sqrt{-3}\,\big]$, luego ninguno de los tres ideales se descompone en producto de primos.

Ejercicio: Probar que la ecuación $x^2-5y^2=7$ no tiene soluciones enteras.

2.7 Grupos de clases

Aunque hasta ahora nos hemos preocupado tan sólo de describir el modo en que se descomponen los primos racionales en un orden maximal, hemos de recordar que el teorema 2.35 nos da explícitamente los generadores de los primos que aparecen. Por ejemplo, si queremos conocer los factores primos de 2 en el anillo de enteros ciclotómicos de orden 7, puesto que $o_7(2) = 3$, el teorema 2.38 nos da que 2 ha de tener dos factores primos de norma 8. Para encontrarlos hemos de factorizar módulo 2 el polinomio ciclotómico séptimo. Los únicos polinomios de grado 3 que no tienen raíces en $\mathbb{Z}/2\mathbb{Z}$ (y que por tanto son irreducibles) son x^3+x+1 y x^3+x^2+1. Como los factores han de ser distintos, la factorización que buscamos es necesariamente $(x^3+x+1)(x^3+x^2+1)$, y en consecuencia

$$2 = (2, \omega^3 + \omega + 1)(2, \omega^3 + \omega^2 + 1). \tag{2.3}$$

Sin embargo hay una pregunta importante que no sabemos resolver, y es si los ideales que nos han aparecido son o no principales, lo que equivale a preguntarse si el 2 puede descomponerse realmente en el anillo de enteros. Observemos que un ideal $\mathfrak{a}$ es principal si y sólo si existe un entero $\alpha \in \mathfrak{a}$ tal que $\mathrm{N}(\alpha) = \mathrm{N}(\mathfrak{a})$, y entonces $\mathfrak{a} = (\alpha)$. Por lo tanto el problema de determinar si un ideal dado es principal es de la misma naturaleza que el de determinar si una ecuación diofántica definida por una forma completa tiene solución. En el próximo capítulo los resolveremos conjuntamente.

Ejercicio: Probar que el segundo generador de cada factor de (2.3) tiene norma 8, por lo que ambos factores son principales.

El interés determinar si un ideal dado es o no principal se debe, entre otras razones, a que un orden maximal es un dominio de factorización única si y sólo si todos sus ideales son principales. En el capítulo siguiente veremos también que el problema se puede reducir a determinar si un número finito de ideales son o no principales.

El primer paso para abordar estos problemas lo presentamos ya en [Al 8.40], y es definir el grupo de clases de un cuerpo numérico. Recordemos la definición:

Definición 2.59 Si K es un cuerpo numérico, definimos su *grupo de clases* como el grupo cociente del grupo de ideales fraccionales de K sobre el subgrupo generado por los ideales principales no nulos.

El subgrupo generado por los ideales principales no nulos está formado por los ideales fraccionales de la forma $(\alpha)/(\beta)$, con $\alpha, \beta \in \mathcal{O}_K$ no nulos. Dos ideales fraccionales $\mathfrak{a}$ y $\mathfrak{b}$ son congruentes módulo este subgrupo si y sólo si $\mathfrak{b} = (\alpha)/(\beta)\mathfrak{a}$, para ciertos $\alpha, \beta \in \mathcal{O}_K$ no nulos, lo cual equivale a que $\mathfrak{b} = \gamma\mathfrak{a}$, con $\gamma = \alpha/\beta \in K$ no nulo, es decir, a que los ideales fraccionales sean similares.

Así pues, las clases del grupo de clases de K no son sino las clases de similitud de ideales fraccionales, que ya conocíamos.

Por otra parte, veamos ahora que cada clase del grupo de clases tiene representantes que son ideales de $\mathcal{O}_K$ (no meros ideales fraccionales).

En efecto, basta tener en cuenta que todo ideal fraccional es de la forma $\mathfrak{b} = \beta^{-1}\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal no nulo, luego $[\mathfrak{b}] = [1/(\beta)][\mathfrak{a}] = [\mathfrak{a}]$.

Podemos expresar la relación de similitud en términos exclusivamente de ideales: Dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ son similares (es decir, determinan la misma clase del grupo de clases) si y sólo si existen ideales principales tales que $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

Un ideal $\mathfrak{a}$ de $\mathcal{O}_K$ determina la clase trivial si y sólo si es principal.

En efecto, una implicación es obvia, y si $[\mathfrak{a}] = [1]$, existen ideales principales tales que $(\alpha)\mathfrak{a} = (\beta)$, pero esto implica que $(\beta) \subset (\alpha)$, luego $\alpha \mid \beta$ y así $\mathfrak{a} = (\beta/\alpha)$ es principal.

Así pues, el problema de si un ideal es o no principal puede reformularse en términos de si determina o no la clase trivial en el grupo de clases. En particular, el orden $\mathcal{O}_K$ es un dominio de ideales principales si y sólo si el grupo de clases de K es trivial.

El interés de este planteamiento se debe en gran parte a que los grupos de clases de los cuerpos numéricos son siempre finitos. En [Al 8.41] lo probamos para el caso de los cuerpos ciclotómicos de orden primo, y en el la sección [ITAl 13.2] lo probamos para los cuerpos cuadráticos. En el capítulo siguiente probaremos en general la finitud de los grupos de clases.

Sucede que también tiene interés determinar si los ideales de los órdenes no maximales son o no principales (aunque de nuestro estudio tendremos que excluir los "patológicos").

Concretamente, supongamos que $\mathcal{O}'$ es un orden de un cuerpo numérico, $\mathfrak{f}$ es su conductor y $\mathcal{O}$ es el orden maximal. El teorema 2.56 establece una biyección entre los ideales de $\mathcal{O}'$ primos con $\mathfrak{f}$ y los análogos en $\mathcal{O}$. Esta correspondencia conserva todo lo relacionado con la divisibilidad ideal, pero en general no conserva el carácter principal de un ideal: si bien es obvio que la imagen en $\mathcal{O}$ de un ideal principal de $\mathcal{O}'$ es un ideal principal (con el mismo generador), bien puede ocurrir que un ideal principal de $\mathcal{O}$ tenga asociado un ideal no principal de $\mathcal{O}'$, debido a que ninguno sus generadores pertenezca a $\mathcal{O}'$. Por ello hemos de distinguir entre ideales de $\mathcal{O}'$ principales en $\mathcal{O}'$ (luego también en $\mathcal{O}$) de los que sólo son principales en $\mathcal{O}$. En particular, el hecho de que todos los ideales de $\mathcal{O}$ sean principales no implica necesariamente que todos los ideales de $\mathcal{O}'$ lo sean. Ni siquiera los primos con el conductor. Ahora definiremos un grupo de clases de ideales de $\mathcal{O}'$ (primos con $\mathfrak{f}$) de modo que la clase trivial la formen precisamente los ideales principales en $\mathcal{O}'$, con lo que $\mathcal{O}'$ tendrá factorización única real (para números primos con $\mathfrak{f}$) si y sólo si el grupo de clases es trivial, en completa analogía con el caso que acabamos de estudiar para órdenes maximales.

Definición 2.60 Sea K un cuerpo numérico, sea $\mathcal{O}$ su orden maximal y sea $\mathcal{O}'$ un orden cualquiera de K con conductor $\mathfrak{f}$. Llamaremos

$$I_{\mathfrak{f}}^*(\mathcal{O}) = \{\mathfrak{a}\mathfrak{b}^{-1} \mid \mathfrak{a}, \mathfrak{b} \in I_{\mathfrak{f}}(\mathcal{O})\},$$

es decir, $I_\mathfrak{f}^*(\mathcal{O})$ es el subgrupo generado por $I_\mathfrak{f}(\mathcal{O})$ en el grupo de los ideales fraccionales de K. Según el teorema 2.56, el semigrupo $I_\mathfrak{f}(\mathcal{O}')$ puede identificarse con $I_\mathfrak{f}(\mathcal{O})$, luego podemos considerar a $I_\mathfrak{f}^*(\mathcal{O})$ como un 'grupo de cocientes' de $I_\mathfrak{f}(\mathcal{O}')$. Similarmente definimos

$$\begin{aligned} P_\mathfrak{f}(\mathcal{O}') &= \big\{\alpha \in \mathcal{O}' \mid \alpha\mathcal{O} + \mathfrak{f} = 1\big\}, \\ P_\mathfrak{f}^*(\mathcal{O}') &= \big\{\alpha\mathcal{O}\beta^{-1}\mathcal{O} \mid \alpha, \beta \in P_\mathfrak{f}(\mathcal{O}')\big\}. \end{aligned}$$

De este modo $P_\mathfrak{f}^*(\mathcal{O}')$ es el subgrupo de $I_\mathfrak{f}^*(\mathcal{O})$ generado por los ideales principales de $I_\mathfrak{f}(\mathcal{O}')$ (identificados con ideales de $I_\mathfrak{f}(\mathcal{O})$).

Llamaremos *grupo de clases* de $\mathcal{O}'$ al grupo cociente $\mathcal{H}(\mathcal{O}') = I_\mathfrak{f}^*(\mathcal{O})/P_\mathfrak{f}^*(\mathcal{O}')$.

Todo $\mathfrak{a} \in I_\mathfrak{f}(\mathcal{O}')$ cumple por definición $\mathfrak{a} + \mathfrak{f} = \mathcal{O}'$, luego existen $\alpha \in \mathfrak{a}$ y $\phi \in \mathfrak{f}$ tales que $\alpha + \phi = 1$, es decir, $(\alpha) \in I_\mathfrak{f}(\mathcal{O}')$. Por la factorización única existe $\mathfrak{b} \in I_\mathfrak{f}(\mathcal{O}')$ tal que $\mathfrak{a}\mathfrak{b} = (\alpha)$. Pasando a $I_\mathfrak{f}(\mathcal{O})$ y tomando clases, esto se traduce en que $[\mathfrak{a}]^{-1} = [\mathfrak{b}]$. Esto prueba que todas las clases de $\mathcal{H}(\mathcal{O}')$ tienen un representante en $I_\mathfrak{f}(\mathcal{O}')$, luego podemos considerarlas como clases de ideales de $I_\mathfrak{f}(\mathcal{O}')$.

Además, si un ideal $\mathfrak{a} \in I_\mathfrak{f}(\mathcal{O}')$ cumple $[\mathfrak{a}] = 1$, entonces existen números $\beta, \gamma \in P_\mathfrak{f}(\mathcal{O}')$ tales que $(\beta)\mathfrak{a} = (\gamma)$. Existe un $\alpha \in \mathfrak{a}$ tal que $\gamma = \beta\alpha$. El hecho de que $\gamma \in P_\mathfrak{f}(\mathcal{O}')$ implica que lo mismo vale para α y, por la factorización única, $\mathfrak{a} = (\alpha)$. Así pues, un ideal de $I_\mathfrak{f}(\mathcal{O}')$ es principal si y sólo si su clase es trivial.

Con esto hemos probado que el grupo de clases de un orden es exactamente lo que queríamos que fuera. En estos términos, lo que hemos llamado grupo de clases de K es el grupo de clases de $\mathcal{O}_K$ (pues el orden maximal tiene conductor $\mathfrak{f} = 1$ y la definición del grupo de clases que acabamos de dar se reduce a la que hemos dado para K).

Para estudiar los grupos de clases necesitamos las técnicas geométricas que presentamos en el capítulo siguiente.

Capítulo III

Métodos geométricos

En este capítulo desarrollaremos las técnicas adecuadas para resolver dos problemas fundamentales de la teoría algebraica de números: calcular el grupo de clases de un orden numérico (y, en particular, probaremos que siempre son finitos) así como sus grupos de unidades.

Estos problemas, resueltos originalmente por distintos métodos y autores, pueden reducirse a un teorema general debido a Minkowski, y que pertenece a una rama de la teoría de números conocida como *geometría de los números*. A modo de primera aproximación podemos pensar en el anillo de los enteros de Gauss, $\mathbb{Z}[i]$. Hasta aquí hemos considerado a éste y otros anillos desde un punto de vista puramente algebraico. Ahora nos fijamos en que este anillo está contenido en el plano complejo y, más precisamente, sus elementos son los vértices de una red de cuadrados de lado unidad que cubren todo el plano. Esta 'representación geométrica', debidamente generalizada, da pie a una serie de argumentos que aportan información valiosa sobre los órdenes numéricos. El primer problema es que no tenemos una representación similar para anillos como $\mathbb{Z}\big[\sqrt{2}\,\big]$. Si vemos este anillo como subconjunto del plano complejo nos encontramos con un subconjunto denso de la recta real, algo muy distinto al caso anterior y donde no podemos aplicar directamente las técnicas que vamos a desarrollar. La diferencia básica es que en el primer ejemplo números linealmente independientes sobre $\mathbb{Q}$ son también linealmente independientes sobre $\mathbb{R}$, mientras que en el segundo todos los números son linealmente dependientes sobre $\mathbb{R}$. Nuestro primer paso será 'separar' los elementos de un cuerpo numérico de modo que la independencia lineal sobre $\mathbb{Q}$ se conserve sobre $\mathbb{R}$.

3.1 La representación geométrica

Definición 3.1 Sea K un cuerpo numérico de grado n. Para cada monomorfismo $\sigma : K \longrightarrow \mathbb{C}$ definimos el *conjugado* de σ como la composición de σ con la conjugación compleja, es decir, el monomorfismo dado por $\bar{\sigma}(\alpha) = \overline{\sigma(\alpha)}$. Diremos que σ es *real* si $\sigma = \bar{\sigma}$ o, equivalentemente, si $\sigma[K] \subset \mathbb{R}$. En caso contrario diremos que σ es *complejo*.

Es evidente que el número de monomorfismos complejos de un cuerpo numérico K ha de ser par. Llamaremos s al número de monomorfismos reales y $2t$ al de complejos, de modo que si n es el grado de K tenemos la relación $n = s+2t$. Además numeraremos los n monomorfismos de K de modo que $\sigma_1, \dots, \sigma_s$ serán los reales y $\sigma_{s+1}, \bar\sigma_{s+1}, \dots, \sigma_{s+t}, \bar\sigma_{s+t}$ serán los complejos.

Por ejemplo en el caso de los cuerpos cuadráticos tenemos $s = 2$, $t = 0$ para los cuerpos reales (de discriminante positivo) y $s = 0$, $t = 1$ para los imaginarios (de discriminante negativo). Para el cuerpo ciclotómico de orden p se tiene $s = 0$, $t = (p-1)/2$. En los cuerpos cúbicos puros $s = 1$, $t = 1$, etc.

Ejercicio: Probar que el signo del discriminante de un cuerpo numérico es $(-1)^t$.

La identificación usual $\mathbb{C} = \mathbb{R}^2$, como espacios vectoriales, nos da una identificación natural $\mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^n$. Por ejemplo, si $s = t = 1$ identificamos la terna $(1, 2, 3)$ con el par $(1, 2+3i)$.

Definimos $\mathcal{R}^{st} = \mathbb{R}^s \times \mathbb{C}^t$ considerado como anillo con el producto definido componente a componente (obviamente no es un dominio íntegro). A los elementos de $\mathcal{R}^{st}$ los llamaremos *vectores*.

Llamaremos *representación geométrica* del cuerpo K a la aplicación que a cada número $\alpha \in K$ le asigna el vector $x(\alpha) = \big(\sigma_1(\alpha), \dots, \sigma_{s+t}(\alpha)\big)$.

Es claro que esta representación es inyectiva y conserva sumas y productos. Además si a es un número racional, $x(a\alpha) = ax(\alpha)$.

Definimos en $\mathcal{R}^{st}$ la norma dada por

$$\mathrm{N}(x_1, \dots, x_{s+t}) = x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2.$$

Así $\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$, para $x, y \in \mathcal{R}^{st}$ y $\mathrm{N}\big(x(\alpha)\big) = \mathrm{N}(\alpha)$, para todo $\alpha \in K$.

Ahora probamos que esta representación geométrica cumple el objetivo que nos habíamos propuesto:

Teorema 3.2 *Sea K un cuerpo numérico. Si los números $\alpha_1, \dots, \alpha_m$ de K son linealmente independientes sobre $\mathbb{Q}$, entonces los vectores $x(\alpha_1), \dots, x(\alpha_m)$ son linealmente independientes sobre $\mathbb{R}$.*

Demostración: Completando una base podemos suponer que tenemos n números (donde n es el grado de K. Hemos de probar que el determinante

$$\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & \mathrm{Re}\,\sigma_{s+1}(\alpha_1) & \mathrm{Im}\,\sigma_{s+1}(\alpha_1) & \cdots & \mathrm{Re}\,\sigma_{s+t}(\alpha_1) & \mathrm{Im}\,\sigma_{s+t}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & \mathrm{Re}\,\sigma_{s+1}(\alpha_n) & \mathrm{Im}\,\sigma_{s+1}(\alpha_n) & \cdots & \mathrm{Re}\,\sigma_{s+t}(\alpha_n) & \mathrm{Im}\,\sigma_{s+t}(\alpha_n) \end{vmatrix}$$

es no nulo. Ahora bien, sabemos que el determinante

$$\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \bar\sigma_{s+1}(\alpha_1) & \cdots & \sigma_{s+t}(\alpha_1) & \bar\sigma_{s+t}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \bar\sigma_{s+1}(\alpha_n) & \cdots & \sigma_{s+t}(\alpha_n) & \bar\sigma_{s+t}(\alpha_n) \end{vmatrix}$$

es no nulo, pues su cuadrado es $\Delta[\alpha_1, \dots, \alpha_n]$.

Si a la columna $\big(\sigma_{s+k}(\alpha_i)\big)$ le sumamos la columna siguiente, se convierte en $\big(2\operatorname{Re}\sigma_{s+k}(\alpha_i)\big)$, y si ahora a la columna siguiente le restamos la mitad de ésta, se convierte en $\big(-i\operatorname{Im}\sigma_{s+k}(\alpha_i)\big)$. Después sacamos los coeficientes y queda el primer determinante multiplicado por $(-2i)^t$. Por consiguiente el primer determinante es, salvo signo, $\sqrt{\big|\Delta[\alpha_1,\ldots,\alpha_n]\big|}/2^t \neq 0$. ∎

3.2 Retículos

El último teorema que acabamos de obtener nos lleva a la definición siguiente:

Definición 3.3 Un *retículo* en $\mathbb{R}^n$ es un subgrupo generado por un conjunto finito de vectores linealmente independientes, es decir, un conjunto de la forma

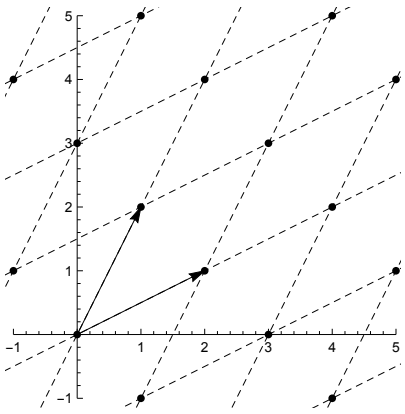
$$\mathcal{M} = \langle v_1,\ldots,v_m\rangle_{\mathbb{Z}} = \{a_1v_1+\cdots+a_mv_m \mid a_1,\ldots,a_m\in\mathbb{Z}\},$$

donde $v_1,\ldots,v_m$ son vectores linealmente independientes en $\mathbb{R}^n$.

Obviamente los vectores $v_1,\ldots,v_m$ son también linealmente independientes sobre $\mathbb{Z}$, luego $\mathcal{M}$ es un $\mathbb{Z}$-módulo libre de rango m. A este rango lo llamaremos *dimensión* de $\mathcal{M}$. La dimensión de un retículo de $\mathbb{R}^n$ es necesariamente menor o igual que n. A los retículos de dimensión n los llamaremos *retículos completos.*

El teorema 3.2 implica que la imagen de un módulo a través de la representación geométrica es un retículo, que será completo si el módulo lo es.

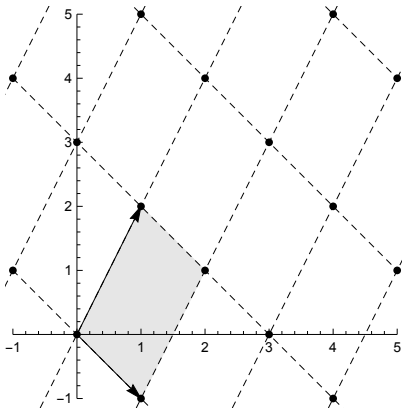
Por ejemplo, he aquí una imagen del retículo en $\mathbb{R}^2$ generado por los vectores $(1,2)$ y $(2,1)$:



A la vista de la figura resulta natural definir el *paralelepípedo fundamental* de una base $v_1,\ldots,v_m$ de un retículo $\mathcal{M}$ como el conjunto

$$T = \{a_1v_1+\cdots+a_mv_m \mid 0\le a_i<1\}.$$

El paralelepípedo fundamental no está determinado por el retículo, sino que cada base tiene uno distinto. Por ejemplo, los vectores $(1,2)$ y $(1,-1)$ generan el mismo retículo de la figura anterior y su paralelepípedo fundamental es el que muestra la figura siguiente:



Por ello, cuando digamos que T es un paralelepípedo fundamental de un retículo $\mathcal{M}$ querremos decir que es el asociado a una cierta base de $\mathcal{M}$. De todos modos, los paralelepípedos fundamentales tienen una característica invariante: su volumen. Llamaremos μ a la medida de Lebesgue en $\mathbb{R}^n$. Se sobrentiende que todos los conjuntos sobre los que apliquemos μ son medibles, por hipótesis cuando sea necesario.

Teorema 3.4 *Sea $\mathcal{M} = \langle v_1, \dots, v_n \rangle$ un retículo completo en $\mathbb{R}^n$, con $v_i = (a_{ij})$. Sea T el paralelepípedo fundamental asociado. Entonces $\mu(T) = |\det(a_{ij})|$, y este valor es independiente de la base escogida.*

Demostración: Sea $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ el isomorfismo que tiene matriz (a_{ij}), es decir, el isomorfismo que envía la base canónica de $\mathbb{R}^n$ a la base $v_1, \dots, v_n$.

Es claro que $T = f\big[[0,1[^n\big]$, luego por el teorema de cambio de variable $\mu(T) = |\det(a_{ij})|\mu\big([0,1[^n\big) = |\det(a_{ij})|$.

Si cambiamos de base la nueva matriz (a_{ij}) se diferencia de la anterior en una matriz de determinante ± 1, luego el valor absoluto del determinante sigue siendo el mismo. ∎

Cada módulo completo en un cuerpo numérico tiene asociado un retículo a través de su representación geométrica. La demostración del teorema 3.2 contiene el cálculo del volumen de su paralelepípedo fundamental:

Teorema 3.5 *Sea K un cuerpo numérico y M un módulo completo en K con anillo de coeficientes $\mathcal{O}$. La imagen de M por la representación geométrica es un retículo completo y el volumen de su paralelepípedo fundamental es*

$$c_M = \frac{\sqrt{|\Delta[M]|}}{2^t} = \frac{\sqrt{|\Delta[\mathcal{O}]|}}{2^t}\,\mathrm{N}(M).$$

Diremos que un subconjunto de $\mathbb{R}^n$ es *discreto* si no tiene puntos de acumulación, es decir, si es cerrado y como espacio topológico es discreto. Equivalentemente, un conjunto es discreto si y sólo si corta a cada bola rB en un número finito de puntos.

Si T es un paralelepípedo fundamental de un retículo $\mathcal{M}$ de $\mathbb{R}^n$ y $x \in \mathcal{M}$, llamaremos *trasladado* de T por x al conjunto

$$T_x = x + T = \{x + t \mid t \in T\}.$$

Teorema 3.6 *Sea $\mathcal{M}$ un retículo en $\mathbb{R}^n$ y sea T un paralelepípedo fundamental de $\mathcal{M}$. Entonces*

1. *Si $\mathcal{M}$ es completo los conjuntos T_x con $x \in \mathcal{M}$ son disjuntos dos a dos y cubren todo $\mathbb{R}^n$.*

2. *El conjunto $\mathcal{M}$ es discreto.*

3. *Para cada $r > 0$ sólo un número finito de conjuntos T_x corta a la bola rB.*

DEMOSTRACIÓN: 1) Sea $v_1, \ldots, v_n$ la base cuyo paralelepípedo es T. Si $x \in \mathbb{R}^n$, entonces x se expresa de forma única como $x = a_1v_1 + \cdots + a_nv_n$, donde $a_1, \ldots, a_n$ son números reales. Podemos descomponer de forma única $a_i = k_i + r_i$, donde $k_i \in \mathbb{Z}$ y $0 \leq r_i < 1$. Llamando ahora $u = k_1v_1 + \cdots + k_nv_n$ y $t = r_1v_1 + \cdots + r_nv_n$ tenemos que $x = u + t$, con $u \in \mathcal{M}$ y $t \in T$, es decir, $x \in T_u$. Si $x \in T_v$ para un $v \in \mathcal{M}$, entonces $x = v + t'$, donde $t' \in T$ es de la forma $s_1v_1 + \cdots + s_nv_n$ con $0 \leq s_i < 1$ y v es de la forma $m_1v_1 + \cdots + m_nv_n$ con $m_i \in \mathbb{Z}$.

La unicidad de las coordenadas da que $k_i + r_i = a_i = m_i + s_i$. La unicidad de la parte entera da que $k_i = m_i$ y $r_i = s_i$, luego $u = v$. Esto prueba que cada vector pertenece a un único conjunto T_u.

2) Puesto que todo retículo puede sumergirse en un retículo completo y que todo subconjunto de un conjunto discreto es discreto, podemos suponer que $\mathcal{M}$ es completo. En tal caso la aplicación lineal que transforma la base canónica de $\mathbb{R}^n$ en una base de $\mathcal{M}$ es un homeomorfismo de $\mathbb{R}^n$ en sí mismo que transforma $\mathbb{Z}^n$ en $\mathcal{M}$. Como $\mathbb{Z}^n$ es discreto, lo mismo le sucede a $\mathcal{M}$.

3) Sea $v_1, \ldots, v_m$ la base cuyo paralelepípedo es T. Sea $d = \|v_1\| + \cdots + \|v_m\|$. Para todo $u = a_1v_1 + \cdots + a_mv_m \in T$ tenemos $\|u\| \leq a_1\|v_1\| + \cdots + a_m\|v_m\| < d$.

Si un vector $x \in \mathcal{M}$ cumple que T_x corta a rB, entonces hay un vector de la forma $x + u \in rB$ con $u \in T$. Entonces $\|x\| \leq \|x + u\| + \|-u\| < r + d$, y como $\mathcal{M}$ es discreto hay sólo un número finito de vectores $x \in \mathcal{M}$ tales que $\|x\| \leq r + d$. ∎

El resultado siguiente es importante porque da una caracterización topológica del concepto de retículo, que nosotros hemos introducido algebraicamente.

Teorema 3.7 *Un subgrupo de $\mathbb{R}^n$ es un retículo si y sólo si es discreto.*

DEMOSTRACIÓN: Una implicación está vista en el teorema anterior. Sea ahora $\mathcal{M}$ un subgrupo discreto de $\mathbb{R}^n$, sea V el subespacio vectorial que genera en $\mathbb{R}^n$, sea m su dimensión, sean $v_1, \ldots, v_m \in \mathcal{M}$ linealmente independientes, sea $\mathcal{M}_0 \subset \mathcal{M}$ el retículo que generan y sea T el paralelepípedo fundamental de $\mathcal{M}_0$ asociado a $\{v_1, \ldots, v_m\}$.

El mismo argumento del teorema anterior prueba que los conjuntos T_u con $u \in \mathcal{M}_0$ constituyen una partición de V. Esto significa en particular que todo vector $x \in \mathcal{M}$ se puede expresar en la forma $x = u + z$, donde $u \in \mathcal{M}_0$ y $z \in T$. Como $\mathcal{M}$ es un subgrupo, también $z \in \mathcal{M}$, pero T es un conjunto acotado y $\mathcal{M}$ es discreto, luego sólo hay un número finito de vectores z que puedan aparecer en estas descomposiciones. Esto prueba que el grupo cociente $\mathcal{M}/\mathcal{M}_0$ es finito. Sea $j = |\mathcal{M} : \mathcal{M}_0|$. Entonces $jx \in \mathcal{M}_0$ para todo $x \in \mathcal{M}$, luego $\mathcal{M} \subset (1/j)\mathcal{M}_0$, que claramente es un retículo, y todo subgrupo de un grupo finitamente generado es finitamente generado.

Consecuentemente existen vectores $w_1, \ldots, w_r$ que generan $\mathcal{M}$, y $r \leq m$. Pero como $\mathcal{M}_0 \subset \mathcal{M}$, los vectores linealmente independientes $v_1, \ldots, v_m$ son combinación lineal de $w_1, \ldots, w_r$, luego ha de ser $r = m$ y éstos han de ser linealmente independientes. Esto prueba que $\mathcal{M}$ es un retículo. ∎

Finalmente caracterizamos la completitud de un retículo.

Teorema 3.8 *Sea $\mathcal{M}$ un retículo en $\mathbb{R}^n$. Entonces $\mathcal{M}$ es completo si y sólo si existe un subconjunto acotado U de $\mathbb{R}^n$ tal que los trasladados $x + U$ con $x \in \mathcal{M}$ cubren todo $\mathbb{R}^n$.*

DEMOSTRACIÓN: Si $\mathcal{M}$ es un retículo completo el resultado se sigue de 3.6 tomando como U un paralelepípedo fundamental de $\mathcal{M}$. Supongamos que $\mathcal{M}$ no es completo y veamos que no puede existir un conjunto U como el del enunciado.

Sea V el subespacio de $\mathbb{R}^n$ generado por $\mathcal{M}$. Como $\mathcal{M}$ no es completo $V \neq \mathbb{R}^n$, luego existe un vector $w \in \mathbb{R}^n$ ortogonal a todos los vectores de V. Podemos tomarlo de norma 1.

Sea $r > 0$ tal que $\|u\| < r$ para todo vector $u \in U$. Por la hipótesis podemos descomponer $rw = x + u$, con $x \in \mathcal{M}$ y $u \in U$.

Como w y x son ortogonales, $rww = uw$, y aplicando la desigualdad de Cauchy–Schwarz llegamos a una contradicción: $r \leq \|u\|\,\|w\| = \|u\|$. ∎

3.3 El teorema de Minkowski

Demostramos ahora el teorema central de este capítulo.Recordemos que un subconjunto A de $\mathbb{R}^n$ es *convexo* si cuando $a, b \in A$ y $0 \leq \lambda \leq 1$, entonces $(1 - \lambda)a + \lambda b \in A$. El conjunto X es *absolutamente convexo* si es convexo y cuando $a \in A$, también $-a \in A$.

Teorema 3.9 (Teorema de Minkowski) *Sea $\mathcal{M}$ un retículo completo en $\mathbb{R}^n$ cuyo paralelepípedo fundamental tenga medida c. Sea A un subconjunto absolutamente convexo y acotado de $\mathbb{R}^n$. Si $\mu(A) > 2^n c$, entonces A contiene al menos un punto no nulo de $\mathcal{M}$.*

DEMOSTRACIÓN: La prueba se basa en el hecho siguiente:

> *Si Y es un subconjunto acotado de $\mathbb{R}^n$ con la propiedad de que los trasladados Y_x para cada $x \in \mathcal{M}$ son disjuntos dos a dos, entonces $\mu(Y) \leq c$.*

Para probarlo consideramos los conjuntos $Y \cap T_{-x}$, donde T es un paralelepípedo fundamental de $\mathcal{M}$ y $T_{-x} = T - x$. Como los trasladados de T cubren todo el espacio y son disjuntos, es claro que

$$\mu(Y) = \sum_{x \in \mathcal{M}} \mu(Y \cap T_{-x})$$

(notemos que sólo hay un número finito de sumandos no nulos).

Claramente $x + (Y \cap T_{-x}) = Y_x \cap T$, y como la medida es invariante por traslaciones, tenemos que $\mu(Y \cap T_{-x}) = \mu(Y_x \cap T)$. Así pues,

$$\mu(Y) = \sum_{x \in \mathcal{M}} \mu(Y_x \cap T).$$

Dado que los conjuntos Y_x son disjuntos dos a dos y están contenidos en T, concluimos que $\mu(Y) \leq \mu(T) = c$.

Consideremos el conjunto $(1/2)A$. Por las hipótesis del teorema tenemos que

$$\mu\left(\frac{1}{2}A\right) = \frac{\mu(A)}{2^n} > c,$$

luego, según lo que hemos probado, los trasladados de $(1/2)A$ no son disjuntos dos a dos, sino que existen $x, x' \in \mathcal{M}$ tales que $x \neq x'$ y

$$\left(x + \frac{1}{2}A\right) \cap \left(x' + \frac{1}{2}A\right) \neq \varnothing.$$

Existen vectores $a, a' \in A$ tales que $x + (1/2)a = x' + (1/2)a'$, o equivalentemente, $x - x' = (1/2)a - (1/2)a'$. Este vector está en A porque A es absolutamente convexo, y por otro lado es un elemento no nulo de $\mathcal{M}$. ∎

Observamos que una pequeña variante en la prueba nos da el siguiente resultado que usaremos después.

Teorema 3.10 *Sea $\mathcal{M}$ un retículo completo en $\mathbb{R}^n$ cuyo paralelepípedo fundamental tenga medida c. Sea Y un subconjunto acotado de $\mathbb{R}^n$ cuyos trasladados por puntos de $\mathcal{M}$ cubran todo $\mathbb{R}^n$. Entonces $\mu(Y) \geq c$.*

DEMOSTRACIÓN: Razonando como en la primera parte de la prueba del teorema de Minkowski, ahora los conjuntos $Y_x \cap T$ cubren todo T (sin ser necesariamente disjuntos), luego

$$\mu(Y) = \sum_{x \in \mathcal{M}} \mu(Y_x \cap T) \geq \mu(T) = c.$$

∎

Para aplicar el teorema de Minkowski a los cuerpos numéricos usaremos el conjunto absolutamente convexo cuyo volumen calculamos a continuación. Recordemos la notación $n = s + 2t$ introducida en 3.1.

Teorema 3.11 *Para cada número real $c > 0$, el conjunto*

$$X_{st}(c) = \big\{x \in \mathcal{R}^{st} \;\big|\; |x_1| + \cdots + |x_s| + 2|x_{s+1}| + \cdots + 2|x_{s+t}| < c\big\}$$

es absolutamente convexo y acotado, y

$$\mu\big(X_{st}(c)\big) = \frac{(2c)^n}{n!}\left(\frac{\pi}{8}\right)^t.$$

Demostración: El conjunto $X_{st}(c)$ es una bola para una norma en $\mathbb{R}^n$, luego es absolutamente convexo y acotado. Para calcular su medida conviene expresarlo como subconjunto de $\mathbb{R}^n$, o sea, en la forma

$$X_{st}(c) = \big\{x \in \mathbb{R}^n \;\big|\; |x_1|+\cdots+|x_s|+2\sqrt{x_{s+1}^2+y_{s+1}^2}+\cdots+2\sqrt{x_{s+t}^2+y_{s+t}^2} < c\big\}.$$

Veámoslo primero para $t = 0$ por inducción sobre s. Claramente tenemos que $X_{10}(c) = \,]-c, c[$ y su medida es $2c$, como afirma la fórmula. Ahora, por el teorema de Fubini,

$$\begin{aligned}\mu\big(X_{(s+1)0}(c)\big) &= \int_{-c}^{c} \mu(X_{s0}\big(c - |x_{s+1}|\big))\,dx_{s+1}\\ &= \frac{2^s}{s!}\int_{-c}^{c}\big(c - |x_{s+1}|\big)^s dx_{s+1} = \frac{(2c)^{s+1}}{(s+1)!}.\end{aligned}$$

A continuación lo probamos para cualquier s, t por inducción sobre t. Lo tenemos probado para $t = 0$. Si $t = 1$ y $s = 0$ no podemos aplicar la hipótesis de inducción, pues el teorema no tiene sentido para $(s, t) = (0, 0)$, pero es fácil ver que $\mu(X_{01})$ tiene el valor requerido. En cualquier otro caso calculamos $\mu\big(X_{s(t+1)}(c)\big)$ aplicando de nuevo el teorema de Fubini para separar las dos últimas variables y cambiamos a coordenadas polares (ρ, θ), para lo cual hemos de multiplicar por el determinante jacobiano del cambio, que es ρ. Con todo esto queda:

$$\begin{aligned}\mu\big(X_{s(t+1)}(c)\big) &= \int_0^{c/2}\int_0^{2\pi}\Big(\mu\big(X_{st}(c-2\rho)\big)\rho\,d\theta\Big)d\rho\\ &= 2\pi\frac{2^{s+2t}}{(s+2t)!}\left(\frac{\pi}{8}\right)^t\int_0^{c/2}(c-2\rho)^{s+2t}\rho\,d\rho.\end{aligned}$$

La fórmula de integración por partes ($u = \rho$, $dv = (c-2\rho)^{s+2t}d\rho$) nos da

$$\mu\big(X_{s(t+1)}(c)\big) = 4\frac{2^{s+2(t+1)}}{(s+2t)!}\left(\frac{\pi}{8}\right)^{t+1}\int_0^{c/2}\frac{1}{2}\,\frac{(c-2\rho)^{s+2t+1}}{s+2t+1}\,d\rho,$$

y de aquí se llega sin dificultad al valor indicado por la fórmula. ∎

He aquí la primera consecuencia del teorema de Minkowski:

Teorema 3.12 *Sea M un módulo completo en un cuerpo numérico K de grado $n = s + 2t$. Entonces existe un número $\alpha \in M$ no nulo tal que*

$$|\,\mathrm{N}(\alpha)| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta[M]|}.$$

DEMOSTRACIÓN: Sea $X_{st}(c)$ según el teorema anterior. Vamos a aplicarle el teorema de Minkowski tomando como retículo la imagen de $\mathcal{M}$ por la representación geométrica de K, para lo cual se ha de cumplir que $\mu\big(X_{st}(c)\big) > 2^{s+2t}k$, donde k es la medida del paralelepípedo fundamental del retículo, que por el teorema 3.5 vale $k = \sqrt{\big|\Delta[M]\big|}/2^t$.

En definitiva, se ha de cumplir que $\mu\big(X_{st}(c)\big) > 2^{s+t}\sqrt{\big|\Delta[M]\big|}$. Por el teorema anterior esto es

$$\frac{(2c)^n}{n!}\left(\frac{\pi}{8}\right)^t > 2^{s+t}\sqrt{\big|\Delta[M]\big|},$$

o sea, $c^n > \left(\frac{4}{\pi}\right)^t \sqrt{\big|\Delta[M]\big|}\, n!$. Si c cumple esta condición, existe un $\alpha \in \mathcal{M}$ no nulo tal que $x(\alpha) \in X_{st}(c)$.

Usando que la media geométrica es siempre menor o igual que la media aritmética concluimos que

$$\begin{aligned}\sqrt[n]{\big|\mathrm{N}(\alpha)\big|} &= \sqrt[n]{\big|\sigma_1(\alpha)\cdots\sigma_s(\alpha)\sigma_{s+1}(\alpha)^2\cdots\sigma_{s+t}(\alpha)^2\big|}\\ &\le \frac{\big|\sigma_1(\alpha)\big| + \cdots + \big|\sigma_s(\alpha)\big| + 2\big|\sigma_{s+1}(\alpha)\big| + \cdots + 2\big|\sigma_{s+t}(\alpha)\big|}{n} < \frac{c}{n}.\end{aligned}$$

Así pues, $|\,\mathrm{N}(\alpha)| < c^n/n^n$.

Dado $0 < \epsilon < 1$, existe un $c_\epsilon > 0$ tal que $c_\epsilon^n = \left(\frac{4}{\pi}\right)^t n!\sqrt{\big|\Delta[M]\big|} + \epsilon$, a partir del cual obtenemos un $\alpha_\epsilon \in \mathcal{M}$ no nulo tal que

$$|\,\mathrm{N}(\alpha_\epsilon)| < \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\big|\Delta[M]\big|} + \frac{\epsilon}{n^n}.$$

Ahora bien, el conjunto de todos los $x(\alpha)$ que cumplen esto para algún ϵ está acotado (pues todos están en $X_{st}(c_1)$) y además todos ellos están en un retículo (discreto), por lo que sólo hay un número finito de posibles α_ϵ, luego un mismo α (en $\mathcal{M}$ y no nulo) debe cumplir la desigualdad para todos los ϵ, o sea, $|\,\mathrm{N}(\alpha)| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\big|\Delta[M]\big|}$. ∎

He aquí una aplicación sencilla:

Teorema 3.13 (Minkowski) *El discriminante de un cuerpo numérico distinto de $\mathbb{Q}$ no puede ser ± 1.*

DEMOSTRACIÓN: Si $\Delta_K = \pm 1$, tomando como módulo M el orden maximal de K, el teorema anterior nos da la existencia de un entero no nulo α tal que

$$1 \le \big|\mathrm{N}(\alpha)\big| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n},$$

donde $n = s + 2t \ge 2$ es el grado de K. Veamos que esta desigualdad es imposible.

Podemos considerar al miembro de la derecha como producto de t factores $4/\pi$ y n factores k/n, donde k varía entre 1 y n. Por otro lado $t \le n/2$, luego podemos agrupar los primeros factores con los primeros del segundo tipo, de modo que así nos quedan dos clases de factores: de tipo k/n y de tipo $4k/n\pi$ con $k \le n/2$.

Los primeros son obviamente menores que 1 (salvo n/n). Si probamos que los del segundo tipo son también menores que 1, todo el producto cumplirá lo mismo, y tendremos una contradicción.

Ahora bien, como $2 < \pi$, resulta que $n/2 < n\pi/4$, luego $k < n\pi/4$ y así $4k/n\pi < 1$. ∎

Ejercicio: Usar la fórmula de Stirling [ITAn 6.7]:

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, \quad 0 < \theta < 1,$$

para probar que si Δ es el discriminante de un cuerpo numérico de grado n entonces

$$|\Delta| > \left(\frac{\pi}{4}\right)^{2t} \frac{1}{2\pi n} e^{2n - \frac{1}{6n}}.$$

Deducir que el mínimo discriminante de un cuerpo de grado n tiende a infinito con n.

Ejercicio: Aplicar el teorema de Minkowski a los conjuntos

$$A = \left\{x \in \mathcal{R}^{st} \;\middle|\; |x_1| < \sqrt{|\Delta|},\ |x_i| < 1\ (2 \le i \le s+t)\right\} \quad \text{si } s \ne 0$$

$$A = \left\{x \in \mathcal{R}^{0t} \;\middle|\; |\operatorname{Re} x_1| < \frac{1}{2},\ |\operatorname{Im} x_1| < \sqrt{|\Delta|}, |x_i| < 1\ (2 \le i \le t)\right\} \quad \text{si } s = 0$$

para probar que todo cuerpo numérico contiene un elemento primitivo entero los coeficientes de cuyo polinomio mínimo están acotados por una cantidad que depende sólo de n y Δ. Concluir que hay un número finito de cuerpos numéricos con un mismo discriminante dado (Teorema de Hermite). Notemos que este argumento nos permite obtener explícitamente tales cuerpos.

3.4 La finitud del grupo de clases

Ya estamos en condiciones de probar que el grupo de clases de cualquier orden numérico es finito. Ello es consecuencia del teorema siguiente:

Teorema 3.14 *Sea K un cuerpo numérico de grado $n = s + 2t$ y discriminante Δ. Entonces todo ideal de $\mathcal{O}_K$ es similar a otro $\mathfrak{a}$ tal que*

$$\mathrm{N}(\mathfrak{a}) \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Demostración: Sea $\mathfrak{b}$ un ideal de $\mathcal{O}_K$. El ideal fraccional $\mathfrak{b}^{-1}$ es de la forma $\beta^{-1}\mathfrak{c}$, para cierto entero β y cierto ideal $\mathfrak{c}$. Sea $\gamma \in \mathfrak{c}$ tal que

$$\left|\mathrm{N}(\gamma)\right| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\left|\Delta[\mathfrak{c}]\right|},$$

según el teorema 3.12.

Según la definición de norma de un módulo, tenemos $\sqrt{|\Delta[\mathfrak{c}]|} = \mathrm{N}(\mathfrak{c})\sqrt{|\Delta|}$. Como $\gamma \in \mathfrak{c}$ se cumple que $\mathfrak{c} \mid \gamma$, luego $(\gamma) = \mathfrak{c}\mathfrak{a}$ para cierto ideal $\mathfrak{a}$. Por lo tanto $\mathfrak{a} = \gamma\mathfrak{c}^{-1} = \gamma\beta^{-1}\mathfrak{b}$, luego $\mathfrak{a}$ es un ideal equivalente a $\mathfrak{b}$, y además

$$\mathrm{N}(\mathfrak{a}) = \frac{\mathrm{N}\big((\gamma)\big)}{\mathrm{N}(\mathfrak{c})} = \frac{|\mathrm{N}(\gamma)|\sqrt{|\Delta|}}{\sqrt{|\Delta[\mathfrak{c}]|}} \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

■

Para aplicar este teorema conviene definir las *constantes de Minkowski*

$$M_{st} = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}.$$

Su cálculo es independiente de los cuerpos numéricos, y en estos términos el teorema 3.14 afirma que todo ideal de K es similar a otro de norma a lo sumo $M_{st}\sqrt{|\Delta|}$. La tabla siguiente contiene las primeras constantes de Minkowski redondeadas hacia arriba en la última cifra decimal mostrada para que las cotas que proporcionan sean correctas.

Tabla 3.1: Constantes de Minkowski

n	s	t	M_{st}
2	2	0	0.5
2	0	1	0.63662
3	3	0	0.22223
3	1	1	0.28295
4	4	0	0.09375
4	2	1	0.11937
4	0	2	0.15199

Nota El teorema [ITAl 12.5] es similar al teorema anterior para el caso de cuerpos cuadráticos, y la cota que proporciona, es $M = 1/\sqrt{3} \approx 0.57736$ para cuerpos imaginarios, que es un poco mejor que M_{01} y $M_{2,0} = 1/2$ para cuerpos reales. ■

El interés de esto reside en que, según el teorema 2.48 (o [Al 8.36]), sólo hay un número finito de ideales de una norma dada, luego hemos probado el grupo de clases del orden maximal de un cuerpo numérico es finito.

Definición 3.15 Se llama *número de clases* de un cuerpo numérico K al orden h_K del grupo de clases de su orden maximal. Más en general, el *número de clases* de un orden numérico es el orden de su grupo de clases.

Acabamos de probar la finitud del número de clases de los órdenes maximales, y el teorema siguiente extiende la conclusión a órdenes numéricos arbitrarios:

Teorema 3.16 *Sea $\mathcal{O}$ el orden maximal de un cuerpo numérico K. Sea $\mathcal{O}'$ un orden de K de conductor $\mathfrak{f}$ y sea h el número de clases de K. Entonces el grupo de clases de $\mathcal{O}'$ es finito, y su orden es*

$$h' = \frac{\Phi(\mathfrak{f})}{\Phi'(\mathfrak{f})e}\, h,$$

donde $\Phi(\mathfrak{f})$ y $\Phi'(\mathfrak{f})$ son, respectivamente, el número de unidades de $\mathcal{O}/\mathfrak{f}$ y de $\mathcal{O}'/\mathfrak{f}$, mientras que e es el índice del grupo de unidades de $\mathcal{O}'$ en el grupo de unidades de $\mathcal{O}$. Además el cociente que aparece en la fórmula es entero, por lo que $h \mid h'$.

Demostración: Sea $\mathcal{H}$ el grupo de clases de K. Consideremos el homomorfismo $I_{\mathfrak{f}}^*(\mathcal{O}) \longrightarrow \mathcal{H}$ dado por $\mathfrak{a} \mapsto [\mathfrak{a}]$.

Dado cualquier ideal $\mathfrak{a}$ de K, existe un ideal $\mathfrak{b}$ de manera que $[\mathfrak{a}^{-1}] = [\mathfrak{b}]$. Por el teorema 2.19 existe un ideal $\mathfrak{c} = \alpha\mathfrak{b}^{-1}$ tal que $[\mathfrak{c}] = [\mathfrak{a}]$ y $\mathfrak{c}+\mathfrak{f} = 1$. Esto implica que el homomorfismo anterior es suprayectivo. Su núcleo es evidentemente $P_{\mathfrak{f}}^*(\mathcal{O})$. Así pues

$$I_{\mathfrak{f}}^*(\mathcal{O})/P_{\mathfrak{f}}^*(\mathcal{O}) \cong \mathcal{H}.$$

Por el teorema de isomorfía podemos concluir que

$$h' = |P_{\mathfrak{f}}^*(\mathcal{O}) : P_{\mathfrak{f}}^*(\mathcal{O}')|\; h,$$

supuesto que probemos que el índice es finito.

Sea ahora U el grupo de unidades del anillo $\mathcal{O}/\mathfrak{f}$ y consideremos la aplicación $U \longrightarrow P_{\mathfrak{f}}^*(\mathcal{O})/P_{\mathfrak{f}}^*(\mathcal{O}')$ dada por $[\alpha] \mapsto \big[(\alpha)\big]$. Veamos que está bien definida.

Si $[\alpha] = [\beta]$, entonces $\alpha \equiv \beta \pmod{\mathfrak{f}}$ y por ser unidades existe un $\gamma \in \mathcal{O}$ tal que $\alpha\gamma \equiv \beta\gamma \equiv 1 \pmod{\mathfrak{f}}$. Como $\mathfrak{f} \subset \mathcal{O}'$ esto implica que $\alpha\gamma, \beta\gamma \in \mathcal{O}'$, luego $\big[(\alpha)\big] = \big[(\alpha)(\beta\gamma)\big] = \big[(\beta)(\alpha\gamma)\big] = \big[(\beta)\big]$.

Evidentemente se trata de un epimorfismo de grupos. Esto prueba ya la finitud del grupo de clases. Vamos a calcular el núcleo. Si $\big[(\alpha)\big] = 1$ entonces $(\alpha) \in P_{\mathfrak{f}}^*(\mathcal{O}')$, lo que significa que $(\alpha) = (\beta)$, donde $\beta \in P_{\mathfrak{f}}(\mathcal{O}')$. A su vez esto implica que $\alpha = \epsilon\beta$, para cierta unidad ϵ de $\mathcal{O}$. Recíprocamente, es claro que si α es de esta forma entonces (α) está en el núcleo.

Llamemos E al grupo de unidades de $\mathcal{O}$ y $\overline{E}$ al subgrupo de U formado por las clases con un representante en E. Similarmente, sea $\overline{P_{\mathfrak{f}}(\mathcal{O}')}$ el grupo de las clases de U con representantes en $P_{\mathfrak{f}}(\mathcal{O}')$. Hemos probado que el núcleo del epimorfismo que estamos estudiando es $\overline{E}\;\overline{P_{\mathfrak{f}}(\mathcal{O}')}$, de donde

$$|P_{\mathfrak{f}}^*(\mathcal{O}) : P_{\mathfrak{f}}^*(\mathcal{O}')| = \frac{\Phi(\mathfrak{f})}{\big|\overline{E}\;\overline{P_{\mathfrak{f}}(\mathcal{O}')}\big|}.$$

Claramente,

$$\big|\overline{E}\;\overline{P_{\mathfrak{f}}(\mathcal{O}')}\big| = \big|\overline{E} : \overline{E} \cap \overline{P_{\mathfrak{f}}(\mathcal{O}')}\big|\;\big|P_{\mathfrak{f}}(\mathcal{O}')\big|.$$

Si llamamos E' al grupo de las unidades de $\mathcal{O}'$, es fácil comprobar el isomorfismo $E/E' \cong \overline{E}/\big(\overline{E} \cap \overline{P_{\mathfrak{f}}(\mathcal{O}')}\big)$. Finalmente, si llamamos U' al grupo de las unidades de $\mathcal{O}'/\mathfrak{f}$, también se ve fácilmente que $U' \cong P_{\mathfrak{f}}(\mathcal{O}')$. El teorema es ahora inmediato. ∎

Para el caso de órdenes cuadráticos la fórmula admite una ligera simplificación:

Teorema 3.17 *Sea $\mathcal{O}_m$ el orden de índice m en un cuerpo cuadrático K. Sea h el número de clases de K y h_m el número de clases de $\mathcal{O}_m$. Entonces*

$$h_m = \frac{\Phi(m)}{\phi(m)e_m}\, h,$$

donde Φ es la función de Euler generalizada, ϕ es la función de Euler usual y e_m es el índice del grupo de las unidades de $\mathcal{O}_m$ en el grupo de las unidades de K.

Demostración: Sólo hay que recordar que el conductor de $\mathcal{O}_m$ es (m) y notar que $\mathcal{O}_m/(m) \cong \mathbb{Z}/m\mathbb{Z}$. ∎

En realidad es posible demostrar la finitud de los grupos de clases de órdenes arbitrarios directamente a partir del teorema 3.12. De hecho, podemos probar algo ligeramente más general:

Teorema 3.18 *Si $\mathcal{O}$ es un orden numérico, existe un número finito de clases de similitud de módulos cuyo anillo de coeficientes es $\mathcal{O}$.*

Demostración: El teorema 3.12 (teniendo en cuenta la definición de norma de un módulo) proporciona una cota C que sólo depende del cuerpo y de $\mathcal{O}$ tal que todo módulo M con anillo de coeficientes $\mathcal{O}$ contiene un elemento $\alpha \neq 0$ con $|\,\mathrm{N}(\alpha)| \leq C\,\mathrm{N}(M)$. Como $\alpha\mathcal{O} \subset M$, también $\mathcal{O} \subset \alpha^{-1}M$. Es fácil ver que

$$|\alpha^{-1}M : \mathcal{O}| = \mathrm{N}(\alpha^{-1}M)^{-1} = |\,\mathrm{N}(\alpha)|/\,\mathrm{N}(M) \leq C.$$

Así tenemos que todo módulo M es similar a otro M' tal que $\mathcal{O} \subset M'$ y $|M' : \mathcal{O}| \leq C$. Sólo hay un número finito de naturales t tales que $1 \leq t \leq C$ y, para cada uno de ellos, sólo hay un número finito de módulos M' tales que $\mathcal{O} \subset M'$ y $|M' : \mathcal{O}| = t$, pues estos módulos cumplen que $M'/\mathcal{O}$ es un grupo finito de orden t, con lo que $tM' \subset \mathcal{O}$, y en consecuencia $\mathcal{O} \subset M' \subset t^{-1}\mathcal{O}$. Ahora bien, los módulos intermedios entre $\mathcal{O}$ y $t^{-1}\mathcal{O}$ están en correspondencia biunívoca con los subgrupos del grupo cociente, que es finito porque ambos módulos son libres del mismo rango. En conclusión, hay un número finito de tales módulos M'. ∎

En [ITAl] mostramos varios ejemplos de cálculo de grupos de clases de órdenes cuadráticos. Veamos aquí otros ejemplos. Recordemos que si el orden maximal de un cuerpo numérico tiene número de clases $h = 1$ esto equivale a que es un dominio de ideales principales, luego un dominio de factorización única. Más en general, si $\mathfrak{a}$ es cualquier ideal de $\mathcal{O}_K$, se cumple que $[\mathfrak{a}]^h = 1$, es decir, $\mathfrak{a}^h$ es siempre un ideal principal.

Cuerpos ciclotómicos de orden primo El cuerpo ciclotómico de orden p tiene $s = 0$, $t = (p-1)/2$. Para $p = 3$ tenemos que todo ideal es similar a otro de norma a lo sumo $M_{01}\sqrt{3} < 1,2$, o sea, todo ideal es similar a un ideal de norma 1, o sea, a 1, y por lo tanto el número de clases resulta ser $h = 1$ y el cuerpo tiene factorización única.

Tomemos ahora $p = 5$. Se cumple que $M_{02}\sqrt{5^3} < 1.7$ y de nuevo tenemos factorización única.

Para el caso $p = 7$ resulta $M_{03}\sqrt{7^5} < 4.2$. Observemos que en realidad hay factorización única si y sólo si todos los ideales primos son principales. Limitándonos a ideales primos, cuya norma es siempre de la forma q^m para un primo racional q, sucede que las únicas normas posibles menores o iguales que 4 son 2, 3 y 4, es decir, sólo hemos de examinar los divisores primos de 2 y 3. Ahora bien, sus órdenes módulo 7 son 3 y 6 respectivamente, luego 2 se descompone en dos factores primos de norma 8 y 3 se conserva primo. Por lo tanto no hay ideales primos de norma menor o igual que 4 y todo ideal es, pues, similar a 1. También en este caso tenemos factorización única.

Para $p = 11$ tenemos $M_{05}\sqrt{11^9} < 58,97$. Vamos a estudiar los primos menores que 58. La tabla siguiente muestra el resto módulo 11 de cada uno de ellos, así como su orden f.

q	2	3	5	7	11	13	17	19	23	29
r	2	3	5	7	0	2	6	8	1	7
f	10	5	5	10	0	10	10	10	1	10
q	31	37	39	41	43	47	51	53	57	
r	9	4	6	8	10	3	7	9	2	
f	5	5	10	10	2	5	10	5	10	

Para calcular la tabla rápidamente basta tener en cuenta que una raíz primitiva módulo 11 es 2, y que sus potencias son $1, 2, 4, 8, 5, 10, 9, 7, 3, 6$.

Las normas de los divisores primos de un primo racional q son todas iguales a q^f. Como $2^{10} > 58$, descartamos los divisores de 2. Igualmente $3^5 > 58$ y $43^2 > 58$, luego los únicos primos de norma menor que 58 son los divisores de 11 y los de 23. Los divisores de 11 son los asociados de $\omega - 1$, luego son todos principales.

El 23 se descompone en producto de 10 ideales primos de norma 23. Hemos de ver si son principales. Según 2.35 cada factor es de la forma $\mathfrak{p} = (23, \omega - k)$, donde $x - k$ es uno de los diez factores en que el polinomio ciclotómico se descompone módulo 23. El número k es una raíz módulo 23 del polinomio ciclotómico o, equivalentemente, una raíz distinta de 1 de $x^{11} - 1$. Los elementos de orden 11 módulo 23 son precisamente los cuadrados, como $5^2 = 2$. Así pues, podemos tomar $\mathfrak{p} = (23, \omega - 2)$. Si probamos que es principal el anillo de enteros ciclotómicos tendrá factorización única.

Ejercicio: Probar que $\mathrm{N}(\omega - 2) = 2^{11} - 1$.

Hemos de encontrar un múltiplo de $\mathfrak{p}$ de norma 23. La técnica que vamos a emplear es esencialmente una de las que usaba Kummer para encontrar primos

ciclotómicos. En primer lugar observamos que $\omega \equiv 2 \pmod{\mathfrak{p}}$, luego los restos módulo $\mathfrak{p}$ de las potencias de ω son

ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7	ω^8	ω^9
2	4	8	-7	9	-5	3	6	-11

Se trata de buscar un polinomio en ω cuyo resto módulo $\mathfrak{p}$ sea nulo y con coeficientes pequeños para que la norma no aumente demasiado. Una posibilidad es aprovechar el $8-7$ que se ve en la tabla y tomar $p(\omega) = \omega^4+\omega^3-1$. Claramente $\mathfrak{p} \mid p(\omega)$ y un cálculo rutinario nos da que $\mathrm{N}\big(p(\omega)\big) = 23$, luego efectivamente $\mathfrak{p} = (\omega^4 + \omega^3 - 1)$ y todos sus conjugados son principales. Esto prueba la factorización única del undécimo cuerpo ciclotómico.

Observemos cómo los resultados que hemos desarrollado nos permiten resolver de una forma relativamente rápida un problema nada trivial, como es determinar la factorización única de un cuerpo numérico. En principio el mismo proceso es aplicable a los cuerpos ciclotómicos de orden 13, 17 y 19, aunque el intervalo de primos a estudiar aumenta demasiado para que los cálculos sean viables (para el tercer caso la cota es del orden de 460.000). En [Al] vimos (en el ejemplo tras [Al 8.38]) que para $p = 23$ no hay factorización única. ∎

Enteros ciclotómicos reales Veremos en la sección 8.1 que el cálculo del número de clases de un cuerpo ciclotómico K de orden primo p se puede reducir al cálculo del número de clases de $K' = K \cap \mathbb{R}$. Vamos a probar que estos cuerpos tienen factorización única cuando $p = 19$ y $p = 23$.

Para $p = 19$ hemos de estudiar los primos menores que $M_{90}\sqrt{19^8} < 122.1$. Hay un total de 30 de ellos.

Si ω es una raíz 19-ésima primitiva de la unidad, evaluando el polinomio ciclotómico se comprueba que $\mathrm{N}(\omega-1) = 19$, luego $\pi = \mathrm{N}_{K'}^{k}(\omega-1)$ es un entero en K' también de norma 19, lo cual implica que el único ideal primo en K' de norma 19 (teorema 2.46) es principal.

Si q es cualquier otro primo, dicho teorema afirma que la norma de cualquiera de sus divisores es q^f, donde f es el orden de q módulo 19 si es impar o la mitad de dicho orden si es par. Las posibilidades para f son 1, 3, 9. Ahora bien, se cumple que $\sqrt[3]{122} < 4.96$, lo que implica que cualquier primo $q > 3$ cuyo valor de f sea 3 o 9, tiene norma mayor que 122, luego no nos afecta. Por su parte, 2 y 3 tienen $f = 9$, con lo que la norma de sus divisores excede también a 122. En resumen, sólo hemos de estudiar los primos que tienen $f = 1$, que se corresponden con primos cuyo orden módulo 19 es 1 o 2, es decir, primos $q \equiv \pm 1 \pmod{19}$. Resulta que sólo hay dos primos en tales condiciones: el 37 y el 113.

Si encontramos enteros ciclotómicos reales de norma 37 y 113, habremos probado que K' tiene factorización única. Con ayuda de un ordenador un simple tanteo basta para dar con ellos. Si calculamos la expresión

$$\mathrm{N}(a_0 + a_1\eta_1 + a_2\eta_2 + a_3\eta_3 + a_4\eta_4 + a_5\eta_5 + a_6\eta_6 + a_7\eta_7 + a_8\eta_8 + a_9\eta_9),$$

(por ejemplo aproximando $\eta_k = 2\cos(2k\pi/19)$ y redondeando el resultado) encontramos decenas de ejemplos sin dar a las variables más valores que ±1 y 0. Por ejemplo

$$\mathrm{N}(1+\eta_5-\eta_6) = -37 \qquad \mathrm{N}(1+\eta_2-\eta_3) = -113.$$

Encontrarlos manualmente es más laborioso, pero no excede lo razonable. Veamos una posibilidad para el 37. Quizá la parte más laboriosa sea encontrar un factor irreducible del polinomio ciclotómico módulo 37. Por ejemplo sirve x^2+3x+1. De este modo, si consideramos el ideal $\mathfrak{q} = (37, \omega^2+3\omega+1)$ en K, tenemos que $-\omega^2-3\omega \equiv 1$ (mód $\mathfrak{q}$), luego $\omega^{-1} \equiv -3-\omega$ (mód $\mathfrak{q}$), luego $\eta_1 = \omega+\omega^{-1} \equiv -3$ (mód $\mathfrak{q}$). Ahora es fácil completar la tabla siguiente:

1	η_1	η_2	η_3	η_4	η_5	η_6	η_7	η_8	η_9
1	-3	7	-18	10	-12	-11	8	-13	-6

En ella se muestran los restos módulo $\mathfrak{q}$ de los números η_i, pero es claro que éstos han de coincidir con los restos módulo $\mathfrak{q}\cap K'$ en K'. El resto es análogo al estudio que hemos hecho antes sobre el cuerpo ciclotómico undécimo.

El análisis para $p = 23$ es similar. La cota es ahora 900, pero por el mismo motivo que antes basta estudiar los primos $q \equiv \pm1$ (mód 23) La lista siguiente contiene todos los primos en estas condiciones junto con un entero de la norma correspondiente. De nuevo vemos que basta buscar entre los enteros con coeficientes ±1 y 0, por lo que no es difícil encontrar ejemplos rápidamente.

$\mathrm{N}(1+\eta_1-\eta_3) = 47$
$\mathrm{N}(1+\eta_1+\eta_7) = 137$
$\mathrm{N}(1-\eta_1+\eta_3) = 139$
$\mathrm{N}(1-\eta_2+\eta_4+\eta_5+\eta_6) = 229$
$\mathrm{N}(1-\eta_1-\eta_2) = -277$
$\mathrm{N}(1+\eta_5+\eta_7-\eta_{10}+\eta_{11}) = 367$
$\mathrm{N}(1-\eta_2-\eta_3-\eta_5) = 461$
$\mathrm{N}(1+\eta_3+\eta_5+\eta_7-\eta_8+\eta_{11}) = -599$
$\mathrm{N}(1-\eta_5+\eta_7-\eta_8+\eta_{10}+\eta_{11}) = 643$
$\mathrm{N}(1-\eta_1-\eta_4+\eta_5+\eta_6+\eta_9) = -827$
$\mathrm{N}(1-\eta_5+\eta_7-\eta_8-\eta_{10}+\eta_{11}) = 829$

$$\mathrm{N}(1-\eta_1-\eta_2-\eta_3-\eta_4-\eta_5-\eta_6-\eta_7-\eta_8-\eta_{10}) = 691$$

Esto prueba que el anillo de enteros ciclotómicos reales de orden 23 tiene factorización única. ∎

Ejercicio: Probar que $\mathbb{Q}\left(\sqrt[3]{2}\right)$ tiene factorización única.

El ejemplo de Dedekind Para el ejemplo de Dedekind $\mathbb{Q}(\xi)$, tenemos que $s = t = 1$ y $\Delta = -503$, de donde concluimos fácilmente que todo ideal es similar a uno de norma menor o igual que 6. Un primo de norma menor o igual que 6 debe dividir a 2, 3 o 5. Ya vimos en el capítulo anterior (página 47) que 2 se descompone en tres ideales primos principales. Como $\operatorname{ind}\xi = 2$, para factorizar los demás primos podemos considerar el polinomio x^3+x^2-2x+8, que es irreducible módulo 3, luego 3 es primo en $\mathbb{Q}(\xi)$, mientras que dicho polinomio se descompone como $(x+1)(x^2+3)$ módulo 5. Por lo tanto 5 se descompone

en producto de un ideal de norma 25 y del ideal $\mathfrak{p} = (5, 1+\xi)$, de norma 5. Si probamos que $\mathfrak{p}$ es principal entonces todo ideal de norma menor o igual que 6 será producto de ideales principales, y por lo tanto principal. Ahora bien, es fácil ver que $\mathrm{N}(1+\xi) = 10$, lo que implica que $1+\xi$ factoriza como producto de $\mathfrak{p}$ por un ideal (principal) de norma 2, luego $\mathfrak{p}$ también es principal, y así $\mathbb{Q}(\xi)$ tiene factorización única. ∎

Nota En todos los ejemplos precedentes hemos tenido que buscar por tanteo enteros algebraicos de ciertas normas prefijadas para probar que determinados ideales eran principales. Ello se debe a que de momento no tenemos ningún método sistemático para estudiar si un ideal dado de un orden numérico es o no principal, ni, por consiguiente, para determinar si dos ideales dados son o no similares.[1] Para resolver este problema que se nos plantea necesitamos resolver antes otro de los problemas que habíamos anunciado que íbamos a resolver: la determinación de los grupos de unidades de los órdenes numéricos. Nos ocupamos de ello en la sección siguiente. ∎

3.5 Unidades fundamentales

En esta sección obtendremos la estructura del grupo de unidades de un orden numérico arbitrario. Este grupo es multiplicativo, mientras que el teorema de Minkowski se aplica a retículos, que son grupos aditivos. Para relacionar unos con otros usaremos logaritmos.

Definición 3.19 Recordemos que $\mathcal{R}^{st} = \mathbb{R}^s \times \mathbb{C}^t$. Llamaremos *representación logarítmica* de $\mathcal{R}^{st}$ a la aplicación l cuyo dominio lo forman los vectores x de $\mathcal{R}^{st}$ cuyas componentes son todas no nulas (o sea, tales que $\mathrm{N}(x) \neq 0$) y dado por $l(x) = \big(l_1(x), \ldots, l_{s+t}(x)\big)$, donde

$$l_k(x) = \begin{cases} \log|x_k| & \text{para } k = 1, \ldots, s, \\ \log|x_k|^2 & \text{para } k = s+1, \ldots, s+t. \end{cases}$$

Es inmediato que si $\mathrm{N}(x) \neq 0 \neq \mathrm{N}(y)$, entonces $l(xy) = l(x) + l(y)$. También es obvio por la definición de norma en $\mathcal{R}^{st}$ que

$$\log\big|\mathrm{N}(x)\big| = l_1(x) + \cdots + l_{s+t}(x). \tag{3.1}$$

Si K es un cuerpo numérico llamaremos *representación logarítmica* de K a laaplicación $l : K \setminus \{0\} \longrightarrow \mathbb{R}^{s+t}$ dada por $l(\alpha) = l\big(x(\alpha)\big)$, donde x es la representación geométrica de K. Así pues:

$$l(\alpha) = \big(\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_s(\alpha)|, \log|\sigma_{s+1}(\alpha)|^2, \ldots, \log|\sigma_{s+t}(\alpha)|^2\big).$$

[1] En [ITAl] hemos dado un método para el caso de los cuerpos cuadráticos. Concretamente, en la sección [ITAl 11.4] hemos visto cómo encontrar todas las clases de similitud estricta de formas cuadráticas de un determinante dado, en la sección [ITAl 12.2] hemos visto cómo biyectar las clases de similitud estricta de módulos de un orden cuadrático con las clases de equivalencia estricta de formas cuadráticas de su discriminante, de modo que un ideal $\mathfrak{a}$ es principal si y sólo si se corresponde con la clase principal o si —en caso de que haya elementos γ de norma negativa, si $\gamma\mathfrak{a}$ se corresponde con la clase principal.

El vector $l(\alpha)$ se llama *representación logarítmica* del número α. El espacio $\mathbb{R}^{s+t}$ se llama *espacio logarítmico* de K.

Es claro que si α y β son números no nulos, entonces $l(\alpha\beta) = l(\alpha) + l(\beta)$. De aquí se sigue que $l(\alpha^{-1}) = -l(\alpha)$. Por otro lado

$$\log\big|\mathrm{N}(\alpha)\big| = \log\Big|\mathrm{N}\big(x(\alpha)\big)\Big| = l_1(\alpha) + \cdots + l_{s+t}(\alpha).$$

Un primer resultado elemental es el siguiente:

Teorema 3.20 *Sea K un cuerpo numérico y $\mathcal{O}$ un orden cualquiera de K. Entonces la restricción de la representación logarítmica de K al grupo de las unidades de $\mathcal{O}$ es un homomorfismo de grupos cuyo núcleo está formado por las raíces de la unidad en $\mathcal{O}$, y es un grupo cíclico finito de orden par.*

Demostración: Sea W el núcleo indicado en el enunciado. Si $\alpha \in W$ resulta que $l_k(\alpha) = 0$, luego $|\sigma_k(\alpha)| = 1$ para $k = 1, \ldots, s+t$. Esto implica que el conjunto $\big\{x(\alpha) \;\big|\; \alpha \in W\big\}$ está acotado, y como sus elementos pertenecen a un retículo, que es un conjunto discreto, necesariamente ha de ser finito y, como la representación geométrica x es biyectiva, concluimos que el subgrupo W es finito.

En particular los elementos de W tienen orden finito, luego son raíces de la unidad. Recíprocamente si un $\omega \in \mathcal{O}$ cumple $\omega^n = 1$, entonces todos los conjugados de ω cumplen lo mismo, luego todos tienen módulo 1, y los logaritmos de los módulos son 0, luego concluimos $l(\omega) = 0$.

Así pues, W contiene exactamente a las raíces de la unidad de $\mathcal{O}$. En particular contiene al -1, de orden 2, luego W es un grupo abeliano finito de orden par. Además es cíclico porque todo subgrupo finito del grupo multiplicativo de un cuerpo es un grupo cíclico. ∎

Ejercicio: Probar que si un cuerpo numérico cumple $s > 1$ entonces sus únicas raíces de la unidad son ± 1.

Ahora ya podemos aplicar el teorema de Minkowski al estudio de las unidades:

Teorema 3.21 *Sea K un cuerpo numérico y $\mathcal{O}$ un orden de K. Entonces la imagen del grupo de las unidades de $\mathcal{O}$ a través de la representación logarítmica es un retículo de dimensión $s + t - 1$.*

Demostración: Sea $\mathcal{M}$ dicha imagen. Obviamente $\mathcal{M}$ es un subgrupo del espacio logarítmico de K. Por el teorema 3.7, para demostrar que es un retículo basta ver que es discreto. Sea $r > 0$ y vamos a probar que sólo hay un número finito de unidades ϵ tales que $\|l(\epsilon)\| < r$.

Para ello vemos que $l_k(\epsilon) \le |l_k(\epsilon)| \le \|l(\epsilon)\| < r$, luego $\big|\sigma_k(\epsilon)\big| < e^r$ si $k = 1, \ldots, s$ y $\big|\sigma_k(\epsilon)\big|^2 < e^r$ si $k = s+1, \ldots, t$. Esto significa que el conjunto de los $x(\epsilon)$, cuando ϵ es una unidad con $\|l(\epsilon)\| < r$, está acotado, pero los vectores $x(\epsilon)$ forman parte de un retículo, luego son un número finito. Como la representación geométrica es biyectiva, el número de unidades ϵ es también finito.

Esto demuestra que $\mathcal{M}$ es un retículo en $\mathbb{R}^{s+t}$. Si ϵ es una unidad de $\mathcal{O}$, sabemos que $\mathrm{N}(\epsilon) = \pm 1$, luego $0 = \log\bigl|\mathrm{N}(\epsilon)\bigr| = l_1(\epsilon) + \cdots + l_{s+t}(\epsilon)$.

Por lo tanto el retículo $\mathcal{M}$ está contenido en el subespacio

$$V = \{x \in \mathbb{R}^{s+t} \mid x_1 + \cdots + x_{s+t} = 0\},$$

y su dimensión es a lo sumo $s + t - 1$.

Para probar que su dimensión es exactamente ésta basta demostrar que existe un subconjunto acotado U de V tal que los trasladados de U por los elementos de $\mathcal{M}$ cubren todo el espacio V. Esto puede probarse modificando levemente la prueba del teorema 3.8 o bien aplicando el teorema 3.8 a la imagen de $\mathcal{M}$ a través de un isomorfismo entre V y $\mathbb{R}^{s+t-1}$.

Es claro que todo vector de $\mathbb{R}^{s+t}$ es la imagen por la representación logarítmica de un vector de $\mathcal{R}^{st}$. Por (3.1) resulta que un vector x de $\mathcal{R}^{st}$ con coordenadas no nulas cumple $l(x) \in V$ si y sólo si $\mathrm{N}(x) = \pm 1$. Sea S el conjunto de todos los $x \in \mathcal{R}^{st}$ tales que $\mathrm{N}(x) = \pm 1$. Así $l[S] = V$. Sea $X \subset S$ un conjunto acotado cualquiera.

Se cumple que $l[X]$ está acotado, pues si un vector $(x_1, \ldots, x_{s+t})$ cumple $|x_k| < C$ para $k = 1, \ldots, s$ y $|x_k|^2 < C$ para $k = s+1, \ldots, s+t$, entonces $l_k(x) < \log C$ y por lo tanto $l_k(x) = -\sum_{i \neq k} l_i(x) > -(s+t-1)C$, con lo que $l_k(X)$ está acotado.

Como la norma es multiplicativa, si ϵ es una unidad de $\mathcal{O}$, se cumple que $x(\epsilon)X \subset S$, y si todos los trasladados $x(\epsilon)X$ cubren S, entonces los trasladados $l(\epsilon) + l[X]$ cubren V. Así pues, basta demostrar que existe un conjunto acotado $X \subset S$ tal que los trasladados $x(\epsilon)X$ cubren S.

Sea $y = (x_1, \ldots, x_s, y_1 + iz_1, \ldots, y_t + iz_t) \in S$ y sea $f : \mathcal{R}^{st} \longrightarrow \mathcal{R}^{st}$ la aplicación dada por $f(x) = yx$ (el producto se calcula componente a componente en $\mathcal{R}^{st} = \mathbb{R}^s \times \mathbb{C}^t$). Si ahora consideramos $\mathcal{R}^{st} = \mathbb{R}^{s+2t}$ la aplicación f es lineal y el determinante de su matriz (por ejemplo en la base canónica) es

$$\begin{vmatrix}
x_1 & & & & & & & \\
& \ddots & & & & & & \\
& & x_s & & & & & \\
& & & y_1 & z_1 & & & \\
& & & -z_1 & y_1 & & & \\
& & & & & \ddots & & \\
& & & & & & y_t & z_t \\
& & & & & & -z_t & y_t
\end{vmatrix} = \mathrm{N}(y) = \pm 1.$$

Llamemos $\mathcal{N} \subset \mathcal{R}^{st}$ a la imagen de $\mathcal{O}$ por la representación geométrica. Las aplicaciones lineales de determinante ± 1 conservan la medida, luego los paralelepípedos fundamentales de los retículos $\mathcal{N}$ e $y\mathcal{N}$ tienen la misma medida. Llamémosla k (observemos que k no depende de y).

Sea $Q > \left(\frac{4}{\pi}\right)^t k$ y sea $c = \sqrt[s+t]{Q}$. Llamemos A al conjunto de los puntos $x \in \mathcal{R}^{st}$ tales que $|x_i| < c$ para $i = 1, \ldots, s$, $|x_i|^2 < c$ para $i = s+1, \ldots, s+t$.

Es fácil comprobar que A es absolutamente convexo y acotado, así como que $\mu(A) = 2^s\pi^t c^{s+t} > 2^{s+2t}k$ (pues A es un producto de s intervalos de longitud $2c$ y t círculos de radio $\sqrt{c}$).

El teorema de Minkowski nos da un punto no nulo $p \in A \cap y\mathcal{N}$, es decir, un punto de la forma $p = yx(\alpha)$ para cierto $\alpha \in \mathcal{O}$ no nulo y de manera que $|\,\mathrm{N}(p)| < c^{s+t} = Q$. Puesto que $\mathrm{N}(y) = \pm 1$ también se cumple que $|\,\mathrm{N}(\alpha)| = |x(\alpha)| = |\,\mathrm{N}(p)| < Q$.

Por el teorema 1.11 existe sólo un número finito $\alpha_1, \ldots, \alpha_m \in \mathcal{O}$ de elementos no asociados dos a dos con norma menor que Q en módulo. Así pues, cualquier otro $\alpha \in \mathcal{O}$ con $\mathrm{N}(\alpha) < Q$ será asociado en $\mathcal{O}$ a un α_i. Notemos que Q no depende de y, luego $\alpha_1, \ldots, \alpha_m$ tampoco (podríamos haberlos tomado al principio de la prueba). Ahora el α que habíamos encontrado se expresa como $\alpha = \epsilon\alpha_i$ para un cierto i y una cierta unidad ϵ de $\mathcal{O}$. Hemos demostrado que todo $y \in S$ se puede expresar en la forma $y = px(\alpha_i^{-1})x(\epsilon)$.

Definimos $X = S \cap \bigcup_{i=1}^m x(\alpha_i^{-1})A$. Se trata claramente de un conjunto acotado y tenemos que todo $y \in S$ cumple $y \in x(\epsilon)X$ para cierta unidad ϵ de $\mathcal{O}$, tal y como queríamos probar. ∎

Esto determina la estructura del grupo de las unidades de cualquier orden de cualquier cuerpo numérico.

Teorema 3.22 (Teorema de Dirichlet) *Sea $\mathcal{O}$ un orden de un cuerpo numérico de grado $n = s + 2t$. Entonces existen unidades $\epsilon_1, \ldots, \epsilon_r$ en $\mathcal{O}$ (donde $r = s + t - 1$) tales que toda unidad $\epsilon \in \mathcal{O}$ se expresa de forma única como $\epsilon = \zeta\epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$, donde $\zeta \in \mathcal{O}$ es una raíz de la unidad y $m_1, \ldots, m_r$ son enteros racionales.*

Demostración: Sea U el grupo de las unidades de $\mathcal{O}$. Basta tomar unidades $\epsilon_1, \ldots, \epsilon_r \in U$ tales que $l(\epsilon_1), \ldots, l(\epsilon_r)$ sean una base de $l[U]$. ∎

Definición 3.23 Un conjunto de unidades $\epsilon_1, \ldots, \epsilon_r$ en las condiciones de teorema anterior se llama un *sistema fundamental de unidades* de $\mathcal{O}$.

Los sistemas fundamentales de unidades de un orden pueden ser vacíos. Esto ocurre cuando $r = s+t-1 = 0$, lo cual sólo es posible si $s = 1$, $t = 0$ (y entonces $n = s + 2t = 1$, o sea, $K = \mathbb{Q}$), o bien $s = 0$, $t = 1$ (y entonces $n = 2$ y K es un cuerpo cuadrático imaginario).

Esto demuestra que $\mathbb{Q}$ y los cuerpos cuadráticos imaginarios son los únicos cuerpos con un número finito de unidades. Las unidades de $\mathbb{Q}$ son obviamente ± 1. Las de los cuerpos cuadráticos imaginarios son las raíces de la unidad que contienen. Ahora bien, los únicos cuerpos ciclotómicos de grado 2 son $\mathbb{Q}(i)$ (de orden 4) y $\mathbb{Q}\big(\sqrt{-3}\,\big)$ (de orden 3 y 6 a la vez). Así pues, las unidades de cualquier otro cuerpo cuadrático imaginario son también $\{\pm 1\}$, mientras que las de $\mathbb{Q}(i)$ son $\{\pm 1, \pm i\}$ y las de $\mathbb{Q}\big(\sqrt{-3}\,\big)$ son las raíces sextas de la unidad $\{\pm 1, \pm\omega, \pm\omega^2\}$, donde $\omega = \big(-1 + \sqrt{-3}\,\big)/2$. Para órdenes cuadráticos imaginarios no maximales todos los grupos de unidades se reducen claramente a $\{\pm 1\}$ (véase el teorema [ITAl 9.4]).

Los sistemas fundamentales de los cuerpos cuadráticos reales y de los cúbicos puros tienen un sólo miembro. En estos casos si ϵ es un sistema fundamental de unidades se dice simplemente que es una *unidad fundamental.*

La prueba del teorema de Dirichlet no es constructiva, es decir, no nos permite obtener en la práctica un sistema fundamental de unidades. Resolveremos enseguida este problema, pero antes observemos lo siguiente:

Un sistema fundamental de unidades no es más que una base de un cierto $\mathbb{Z}$-módulo, luego no es único. Sin embargo podemos asociar a cada orden un invariante concerniente a sus sistemas fundamentales de unidades de forma similar a como asociamos el discriminante a las bases de un módulo.

Sea $\epsilon_1, \ldots, \epsilon_r$ un sistema fundamental de unidades de un orden $\mathcal{O}$ de un cuerpo numérico. Entonces $l(\epsilon_1), \ldots, l(\epsilon_r)$ forman una base del retículo $l[U]$, donde U es el grupo de las unidades de $\mathcal{O}$. El vector $l_0 = \frac{1}{\sqrt{s+t}}(1, \ldots, 1)$ es unitario y ortogonal al subespacio V formado por los vectores cuyas coordenadas suman 0.

Los vectores $l_0, l(\epsilon_1), \ldots, l(\epsilon_r)$ generan un retículo completo cuyo paralelepípedo fundamental tiene medida independiente de la elección del sistema fundamental de unidades (pues un cambio de sistema da lugar a un cambio de base del retículo).

Sabemos que esta medida k es igual al módulo del determinante de la matriz que tiene por filas a $l_0, l(\epsilon_1), \ldots, l(\epsilon_r)$. Si sumamos todas las columnas a la columna i-ésima y tenemos en cuenta que las componentes de $l(\epsilon_1), \ldots, l(\epsilon_r)$ suman 0, podemos desarrollar el determinante por dicha columna i-ésima y concluir que $k = \sqrt{s+t}\,R$, donde R es el módulo de cualquiera de los menores de orden r de la matriz que tiene por filas a $l(\epsilon_1), \ldots, l(\epsilon_r)$.

Este valor R es independiente de la elección del sistema fundamental de unidades y se llama *regulador* del orden $\mathcal{O}$. El regulador de un cuerpo numérico es el regulador de su orden maximal. Para $\mathbb{Q}$ y los cuerpos cuadráticos imaginarios se define $R = 1$.

El cálculo de un sistema fundamental de unidades (y por lo tanto del regulador) de un cuerpo numérico dado es, a nivel práctico, uno de los problemas más complicados de la teoría algebraica de números, y conocer tales sistemas resulta ser indispensable para tener un control satisfactorio del cuerpo en cuestión. Desde un punto de vista teórico no hay dificultad. Vamos a ver que siempre es posible encontrar un sistema fundamental en un número finito de pasos. Un hecho clave en esta dirección es el teorema siguiente:

Teorema 3.24 *Sea M un módulo completo de un cuerpo numérico K de grado n. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de M. Entonces existe una constante A tal que todos los elementos $\alpha \in M$ que cumplen $|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_n(\alpha)| < c_n$, para ciertos números reales positivos $c_1, \ldots, c_n$ tienen sus coordenadas (en la base dada) acotadas en módulo por $A \sum_{j=1}^{n} c_j$.*

DEMOSTRACIÓN: Si conocemos explícitamente la base dada, entonces la matriz $\big(\mathrm{Tr}(\alpha_i\alpha_j)\big)$ puede ser calculada en la práctica y con ella, resolviendo sistemas de ecuaciones lineales (o calculando su inversa), podemos calcular la base dual $\{\beta_1,\dots,\beta_n\}$ respecto de la forma bilineal determinada por la traza [Al 8.1], caracterizada por que

$$\mathrm{Tr}(\alpha_i\beta_j) = \begin{cases} 1 & \text{si } i = j,\\ 0 & \text{si } i \neq j, \end{cases}$$

Sea $A > 0$ tal que $|\sigma_i(\beta_j)| \leq A$ para todo i, j. En el peor de los casos podemos obtener A calculando los polinomios mínimos de los β_j y aproximando sus raíces. Ahora, un número de M que cumpla lo pedido es de la forma

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n, \qquad a_i \in \mathbb{Z},$$

donde

$$|a_i| = \big|\mathrm{Tr}(\alpha\beta_i)\big| = \Big|\sum_{j=1}^{n} \sigma_j(\alpha)\sigma_j(\beta_i)\Big| \leq A\sum_{j=1}^{n}\big|\sigma_j(\alpha)\big| < A\sum_{j=1}^{n} c_j. \qquad \blacksquare$$

El próximo teorema contiene las ideas centrales del algoritmo para obtener sistemas fundamentales de unidades de cuerpos numéricos.

Teorema 3.25 *Sea $\mathcal{M}$ un retículo en $\mathbb{R}^m$ de dimensión $r > 1$, sea V el subespacio generado por $\mathcal{M}$, sea $u \in \mathcal{M}$ no nulo, sea V' el subespacio de V ortogonal a u y sea $\mathcal{N}$ la proyección de $\mathcal{M}$ en V'. Entonces:*

1. *$\mathcal{N}$ es un retículo de dimensión $r - 1$.*
2. *Supongamos que $u \neq nv$ para todo $v \in \mathcal{M}$ y todo número natural n. Si $u_2,\dots,u_r \in \mathcal{M}$ y sus proyecciones en V son una base de $\mathcal{N}$, entonces $u, u_2,\dots,u_r$ son una base de $\mathcal{M}$.*
3. *Todo elemento $x' \in \mathcal{N}$ es la proyección de un $x \in \mathcal{M}$ tal que*

$$\|x\| \leq \sqrt{\frac{\|u\|^2}{4} + \|x'\|^2}.$$

DEMOSTRACIÓN: 1) Obviamente $\mathcal{N}$ es un subgrupo. El apartado 3) implica que es discreto, luego es un retículo. Las proyecciones de $r - 1$ elementos de $\mathcal{M}$ linealmente independientes de u son linealmente independientes, luego la dimensión de $\mathcal{N}$ es $r - 1$.

2) Sean $u_i = a_iu + u_i'$, donde cada u_i' es ortogonal a u. Similarmente, dado cualquier $v \in \mathcal{M}$, sea $v = au + v'$, donde v' es ortogonal a u. Entonces $v' = \sum_{i=2}^{r} b_iu_i'$, para ciertos enteros racionales b_i. Consecuentemente:

$$v = \left(a - \sum_{i=2}^{r} a_ib_i\right)u + \sum_{i=2}^{r} b_iu_i.$$

De aquí se sigue que el primer sumando del segundo miembro está en $\mathcal{M}$ y por la hipótesis sobre u el coeficiente $b_1 = a - \sum_{i=2}^{r} a_ib_i$ ha de ser un entero (los elementos de $\mathcal{M}$ de la forma αu son claramente un retículo de base u). Esto prueba lo pedido.

3) Sea $x = \alpha u + x'$. Restando el oportuno tu, con t entero racional, podemos exigir que $|\alpha| \leq 1/2$. Entonces

$$\|x\|^2 = |\alpha|^2\|u\|^2 + \|x'\|^2 \leq \|u\|^2/4 + \|x'\|^2. \qquad \blacksquare$$

Cálculo de las unidades fundamentales Veamos ahora cómo podemos calcular en la práctica (¡al menos en teoría!) un sistema fundamental de unidades de un cuerpo numérico K. Por simplificar la notación supondremos que $r = 3$, aunque el método es completamente general. En primer lugar calculamos una base entera de K, su base dual y la constante A del teorema 3.24 para el orden maximal de K.

Ordenando lexicográficamente las n-tuplas de enteros racionales podemos enumerar los enteros de K. Eliminamos los que no tengan norma ± 1 y así tenemos una enumeración de las unidades de K. Cuando encontramos una unidad calculamos su representación logarítmica y, si es nula, pasamos a otra. Seguimos hasta hacernos con r unidades cuyas representaciones logarítmicas sean linealmente independientes, digamos l_1, l_2, l_3. Llamemos V_1 al subespacio de $\mathbb{R}^4$ formado por las cuádruplas cuyas coordenadas suman 0, sea $l'_1 = l_1$, sea V_2 el subespacio de V_1 ortogonal a l'_1, sea l'_2 la proyección de l_2 en V_2, sea V_3 el subespacio de V_2 ortogonal a l'_2 y l'_3 la proyección de l_3 en V_3. Además, llamamos $\mathcal{M}_1$ a la imagen del grupo de unidades por la representación logarítmica, $\mathcal{M}_2$ a la proyección de $\mathcal{M}_1$ en V_2 y $\mathcal{M}_3$ a la proyección de $\mathcal{M}_3$ en V_3.

Entonces $\mathcal{M}_3$ es un retículo de dimensión 1 que contiene al vector l'_3. Si éste no fuera una base, existiría un vector $x \in \mathcal{M}_3$ tal que $\|x\| \leq \|l'_3\|/2$. Por el teorema anterior x sería la proyección de un vector de $\mathcal{M}_2$ de norma menor o igual que $\frac{1}{2}\sqrt{\|l'_2\|^2 + \|l'_3\|^2}$, que a su vez será la proyección de un vector de $\mathcal{M}_1$ de norma menor o igual que $\rho = \frac{1}{2}\sqrt{\|l'_1\|^2 + \|l'_2\|^2 + \|l'_3\|^2}$. Similarmente, si l'_2 es múltiplo de un elemento de $\mathcal{M}_2$, éste tendrá que ser la proyección de un elemento de $\mathcal{M}_1$ de norma menor o igual que ρ.

Si una unidad ϵ cumple que $\|l(\epsilon)\| \leq \rho$, entonces $\log|\sigma(\epsilon)| \leq \rho$ si σ es real y $\log|\sigma(\epsilon)|^2 \leq \rho$ si σ es complejo. Por lo tanto $|\sigma(\epsilon)| \leq e^\rho$ si σ es real y $|\sigma(\epsilon)| \leq e^{\rho/2}$ si σ es complejo. Continuamos nuestra enumeración de unidades hasta que el teorema 3.24 nos garantice que hemos pasado por todas las posibles unidades ϵ. Cada vez que nos encontremos con una unidad hemos de comprobar si su representación logarítmica l es múltiplo de l'_1 con norma menor, y si es así sustituir l'_1 por l. En caso contrario comprobamos si la proyección sobre V_2 es múltiplo de l'_2 con norma menor. En tal caso sustituimos l_2 por l, y en caso contrario hacemos lo mismo con la proyección sobre V_3. Al terminar el proceso tendremos un sistema fundamental de unidades de K.

Naturalmente, el procedimiento que acabamos de describir no es nada eficiente, y lo presentamos únicamente para mostrar que en teoría el cálculo de las unidades fundamentales es posible. En la práctica existen algoritmos mucho más eficientes, pero no vamos a discutirlos aquí. $\blacksquare$

Ejemplo Consideremos el cuerpo $K = \mathbb{Q}(\xi)$, donde ξ es una raíz del polinomio $x^3 + x^2 - 2x + 8$, es decir, el ejemplo de Dedekind del que ya hemos hablado en

otras ocasiones. Sabemos que una base entera de K la forman los números

$$\alpha_1 = 1, \quad \alpha_2 = \xi, \quad \alpha_3 = \frac{\xi + \xi^2}{2}.$$

No es difícil calcular la matriz $\big(\mathrm{Tr}(\alpha_i\alpha_j)\big)$, que resulta ser

$$\begin{pmatrix} 3 & -1 & 2 \\ -1 & 5 & -13 \\ 2 & -13 & -2 \end{pmatrix}.$$

Su inversa es

$$\frac{1}{503}\begin{pmatrix} 179 & 28 & -3 \\ 28 & 10 & -37 \\ -3 & -37 & -14 \end{pmatrix}.$$

Esto nos da la base dual

$$\begin{aligned} \alpha_1^* &= \frac{1}{503}\left(179 + 28\,\xi - 3\,\frac{\xi+\xi^2}{2}\right), \\ \alpha_2^* &= \frac{1}{503}\left(28 + 10\,\xi - 37\,\frac{\xi+\xi^2}{2}\right), \\ \alpha_3^* &= \frac{1}{503}\left(-3 - 37\,\xi - 14\,\frac{\xi+\xi^2}{2}\right). \end{aligned}$$

Sustituimos ξ por aproximaciones complejas de los tres conjugados de ξ (están dadas en el capítulo anterior) y calculamos el mayor módulo de los números obtenidos. Éste resulta ser $A = 0.42$ (redondeado hacia arriba).

Si enumeramos los enteros de K y buscamos los de norma 1, el primero que encontramos (aparte de ± 1) es la unidad

$$\epsilon = 13 + 10\,\xi + 6\,\frac{\xi+\xi^2}{2}.$$

Su representación logarítmica es

$$l(\epsilon) = (\log|\epsilon(\xi_1)|, \log|\epsilon(\xi_2)|^2) = (-7.02735, 7.02735),$$

cuya norma es menor que 9.94, luego si ϵ no fuera una unidad fundamental de K habría otra unidad cuya representación logarítmica tendría norma menor que $9.94/2$, y sus coordenadas en la base entera que estamos considerando estarían acotadas por $A(e^{9.94/2}+2e^{9.94/4}) < 71$. Si comprobamos todos los enteros cuyas coordenadas son menores o iguales que 70 en módulo, veremos que no hay más unidades, luego ϵ es una unidad fundamental y el regulador es $R = 7.02735$. ∎

Ejercicio: Comprobar que $1 - 6\,\sqrt[3]{6} + 3\,\sqrt[3]{36}$ es una unidad fundamental de $\mathbb{Q}\Big(\sqrt[3]{6}\Big)$.

A la hora de calcular sistemas fundamentales de unidades cuerpos ciclotómicos es útil el teorema siguiente:

Teorema 3.26 *Sea K el cuerpo ciclotómico de grado p y sea $K' = K \cap \mathbb{R}$. Entonces un sistema fundamental de unidades para K' es también un sistema fundamental de unidades para K. Si R es el regulador de K y R' el regulador de K', entonces $R = 2^{m-1}R'$, donde $m = (p-1)/2$ es el grado de K'.*

DEMOSTRACIÓN: Sea $\epsilon_1, \ldots, \epsilon_r$ un sistema fundamental de unidades de K'. Si ϵ es una unidad de K, por el lema de Kummer [Al 8.42] $\epsilon = \omega^i\eta$ para una cierta unidad real, o sea, una unidad de K'.

Entonces $\eta = \pm\epsilon_1^{m_1}\cdots\epsilon_r^{m_r}$, para ciertos enteros racionales $m_1, \ldots, m_r$, luego tenemos la descomposición $\epsilon = \pm\omega^i\epsilon_1^{m_1}\cdots\epsilon_r^{m_r}$ tal y como exige el teorema de Dirichlet.

Falta ver que la expresión es única, pero si tenemos dos expresiones

$$\pm\omega^i\epsilon_1^{m_1}\cdots\epsilon_r^{m_r} = \pm\omega^j\epsilon_1^{k_1}\cdots\epsilon_r^{k_r}$$

entonces ω^{i-j} es una raíz de la unidad real, luego $\omega^{i-j} = \pm 1$ y por consiguiente $\epsilon_1^{m_1}\cdots\epsilon_r^{m_r} = \pm\epsilon_1^{k_1}\cdots\epsilon_r^{k_r}$. Por la unicidad que nos da el teorema de Dirichlet, el signo ha de ser $+1$ y los exponentes han de coincidir.

Sea ahora $\{\epsilon_1, \ldots, \epsilon_{m-1}\}$ un sistema fundamental de unidades de K', luego de K. Los automorfismos de K' son todos reales, luego el regulador R' es el módulo del determinante de uno cualquiera de los menores de orden $m-1$ de la matriz $\big(\log|\sigma_i(\epsilon_j)|\big)$. Por el contrario, los automorfismos de K son todos complejos, (pero extienden a los de K') luego el regulador de K es un menor de la matriz $\big(\log|\sigma_i(\epsilon_j)|^2\big) = \big(2\log|\sigma_i(\epsilon_j)|\big)$. Así pues, $R = 2^{m-1}R'$. ∎

Ejemplo Vamos a calcular un sistema fundamental de unidades de $\mathbb{Q}(\omega)$, donde $\omega^7 = 1$. Sea $\eta = \omega + \omega^6$. En virtud del teorema anterior podemos trabajar en el cuerpo $\mathbb{Q}(\eta)$. En la página 22 vimos que una base entera de este cuerpo es $\{1, \eta, \eta^2 - 2\}$. Mediante las aproximaciones racionales de η dadas allí también obtenemos fácilmente la norma de un entero arbitrario:

$$\mathrm{N}\big(a + b\eta + c(\eta^2 - 2)\big) = a^3 + b^3 + c^3 - a^2b - 2ab^2 - a^2c + 3b^2c - 2ac^2 - 4bc^2 + 3abc.$$

También podemos calcular la constante $A = 0.68$ del teorema 3.24.

Si comenzamos a enumerar los enteros para buscar unidades enseguida encontramos dos independientes, a saber η y $1 + \eta$. Calculamos:

$$\begin{aligned} l(\eta) &= (0.220724, -0.809587, 0.58886) \\ l(1+\eta) &= (0.809587, -0.58886, -0.220724) \end{aligned}$$

Calculamos la proyección de $l(1+\eta)$ sobre el espacio ortogonal a $l(\eta)$. Si la llamamos x, ha de ser de la forma $x = l(1+\eta) + \lambda l(\eta)$, donde λ está determinado por la ecuación $\big(l(1+\eta) + \lambda l(\eta)\big)l(\eta) = 0$. Calculando sale $\lambda = -0.5$ y

$$x = (0.699225, -0.184069, -0.515156).$$

Ahora calculamos $\rho = \frac{1}{2}\sqrt{\|l(\eta)\|^2 + \|x\|^2} = 0.68$. Por lo tanto hemos de comprobar todos los enteros cuyas coordenadas no superen en módulo la cota $A \cdot 3 \cdot e^{\rho} = 4.03$.

Descartando duplicidades por el signo, hay 40 unidades a considerar. Puede comprobarse que las representaciones logarítmicas de todas ellas tienen coordenadas enteras respecto a la base $l(\eta)$ y $l(1+\eta)$. Por ejemplo, una de las unidades es $3-2\eta+(\eta^2-2)$, cuya representación logarítmica resulta ser $2l(\eta)-4l(1+\eta)$. Así llegamos a que un sistema fundamental de unidades de $\mathbb{Q}(\omega)$ es $\{\eta, 1+\eta\}$, y por lo tanto cada unidad se expresa de forma única como

$$\pm\omega^i(\omega+\omega^6)^m(1+\omega+\omega^6)^n,$$

donde i, m, n son enteros racionales ($0 \le i < 7$). El regulador de K' es

$$R' = \begin{vmatrix} 0.220724 & -0.809587 \\ 0.809587 & -0.58886 \end{vmatrix} = 0.53.$$

El regulador de K es $R = 4R' = 2.12$. ∎

Terminamos esta sección observando que a partir de un sistema fundamental de unidades podemos obtener una expresión para las unidades de norma positiva.

Sea K un cuerpo numérico y sea $\epsilon_1, \ldots, \epsilon_r$ un sistema fundamental de unidades de K.

Supongamos primero que el grado n de K es impar. Puesto que $n = s + 2t$, se ha de cumplir $s \neq 0$, luego K tiene un monomorfismo real y por lo tanto uno de los cuerpos conjugados de K está formado por números reales. Pero las únicas raíces de la unidad reales son ± 1, luego dicho cuerpo conjugado tiene sólo estas dos raíces de la unidad, y consecuentemente K también.

Entonces toda unidad de K es de la forma $\pm\epsilon_1^{m_1}\cdots\epsilon_r^{m_r}$. Si alguna de las unidades ϵ_i cumple $\mathrm{N}(\epsilon_i) = -1$, entonces $\mathrm{N}(-\epsilon_i) = (-1)^n\,\mathrm{N}(\epsilon_i) = 1$. Sustituyendo ϵ_i por $-\epsilon_i$ tenemos un sistema fundamental de unidades todas ellas con norma positiva.

Claramente, $\mathrm{N}(\pm\epsilon_1^{m_1}\cdots\epsilon_r^{m_r}) = \pm 1$, luego las unidades de norma 1 de K son exactamente las de la forma $\epsilon_1^{m_1}\cdots\epsilon_r^{m_r}$.

Supongamos ahora que n es par. Si K contiene una raíz de la unidad distinta de ± 1, entonces lo mismo les ocurre a todos sus conjugados, luego ninguno de ellos puede ser real, o sea, $s = 0$. Entonces la norma de cualquier elemento de K se calcula como producto de pares de conjugados complejos, pero el producto de un par de conjugados complejos es siempre un número real positivo y así todas las normas son positivas.

Si K no contiene más raíces de la unidad que ± 1, entonces, como el grado es par, concluimos que $\mathrm{N}(\pm 1) = 1$, y en cualquier caso tenemos que las raíces de la unidad de K tienen norma 1.

Supongamos que $\epsilon_1, \ldots, \epsilon_k$ tienen norma positiva y que $\epsilon_{k+1}, \ldots, \epsilon_r$ la tienen negativa. Entonces $\epsilon_1, \ldots, \epsilon_k, \epsilon_r\epsilon_{k+1}, \ldots, \epsilon_r\epsilon_{r-1}, \epsilon_r$ es un sistema fundamental de unidades donde sólo la última tiene norma negativa. En general, podemos tomar un sistema fundamental de unidades $\epsilon_1, \ldots, \epsilon_r$ donde todas tienen norma positiva salvo quizá la última.

Si todas tienen norma positiva, entonces todas las unidades de K tienen norma positiva y el problema está resuelto. Si $\mathrm{N}(\epsilon_r) = -1$ entonces es claro que $\mathrm{N}(\omega\epsilon_1^{m_1}\cdots\epsilon_r^{m_r}) = (-1)^{m_r}$.

Por lo tanto las unidades de norma positiva son las de la forma $\omega\epsilon_1^{m_1}\cdots\epsilon_r^{2m_r}$, luego las unidades $\epsilon_1, \ldots, \epsilon_{r-1}, \epsilon_r^2$ generan las unidades de norma positiva (junto con una raíz primitiva de la unidad). ∎

3.6 Cálculo de grupos de clases

En esta sección veremos cómo puede calcularse el número de clases de un cuerpo numérico. El último problema que nos falta resolver para calcular números de clases es determinar si un módulo completo contiene elementos de una norma dada. Más en general, vamos a dar un método para encontrar un conjunto finito de números con la norma deseada tal que cualquier otro sea asociado a uno de ellos.

Partimos de un módulo completo M en un cuerpo numérico K. Sea $\mathcal{O}$ su anillo de coeficientes. Sea $\epsilon_1, \ldots, \epsilon_r$ un sistema fundamental de unidades de $\mathcal{O}$. Los vectores $l(\epsilon_1), \ldots, l(\epsilon_r)$ junto con $l_0 = (1, \ldots, 1)$ forman una base de $\mathbb{R}^{s+t}$.

Si $\mu \in M$ es no nulo, entonces $l(\mu) = \alpha l_0 + \sum_{i=1}^r \alpha_i l(\epsilon_i)$, donde los coeficientes son números reales. Usando (3.1) vemos que $\log\big|\mathrm{N}(\mu)\big| = (s+t)\alpha$, o sea,

$$\alpha = \frac{\log\big|\mathrm{N}(\mu)\big|}{s+t}.$$

Podemos descomponer $\alpha_i = k_i + \beta_i$, con k_i entero racional y $|\beta_i| \le 1/2$. El número $\mu' = \mu\epsilon_1^{-k_1}\cdots\epsilon_r^{-k_r}$ es asociado a μ y cumple que

$$l(\mu') = \alpha l_0 + \sum_{i=1}^r \beta_i l(\epsilon_i).$$

Así pues, todo número de una norma dada en M tiene un asociado cuya representación logarítmica se encuentra en un cierto conjunto acotado. Sabemos enumerar los elementos en estas condiciones y entre ellos obtener un sistema maximal de números no conjugados. ∎

Ejemplo Vamos a calcular el número de clases del cuerpo $\mathbb{Q}(\alpha)$, donde α es una raíz del polinomio $x^3 + 4x + 1$. Los cálculos de la página 13 muestran que una base entera de K es $1, \alpha, \alpha^2$, pues el discriminante de esta base es $\Delta = -283$, primo. Es fácil ver que la norma viene dada por

$$\mathrm{N}(a + b\alpha + c\alpha^2) = a^2 - b^3 + c^3 + 4ab^2 - 8a^2c + 16ac^2 - 4bc^2 + 3abc.$$

Según el teorema 3.14, todo ideal de K es similar a uno de norma menor o igual que $M_{11}\sqrt{|\Delta|} < 80.1$. La tabla siguiente contiene todos los primos de K de norma menor o igual que 80, obtenidos mediante el teorema 2.35.

$\mathfrak{p}=(p,\eta)$	$\lvert\mathrm{N}(\eta)\rvert$	$\mathfrak{p}=(p,\eta)$	$\lvert\mathrm{N}(\eta)\rvert$	$\mathfrak{p}=(p,\eta)$	$\lvert\mathrm{N}(\eta)\rvert$
$(2,1+\alpha)$	2^2	$(19,3+\alpha)$	$2\cdot 19$	$(71,12+\alpha)$	$5^2\cdot 71$
$(2,1+\alpha+\alpha^2)$	–	$(31,-7+\alpha)$	$-2^2\cdot 3\cdot 31$	$(71,26+\alpha)$	–
$(3,-1+\alpha)$	$2\cdot 3$	$(37,7+\alpha)$	$2\cdot 5\cdot 37$	$(71,33+\alpha)$	–
$(3,-1+\alpha+\alpha^2)$	–	$(43,-11+\alpha)$	$2^5\cdot 43$	$(73,21+\alpha)$	$2^7\cdot 73$
$(5,2+\alpha)$	$3\cdot 5$	$(47,-17+\alpha)$	$2\cdot 47\cdot 53$	$(73,-16+\alpha)$	$3\cdot 19\cdot 73$
$(5,-2-2\alpha+\alpha^2)$	–	$(53,-17+\alpha)$	–	$(73,-5+\alpha)$	$2\cdot 73$
$(17,-2+\alpha)$	17	$(67,-32+\alpha)$	–	$(79,4+\alpha)$	79

También hemos calculado la norma de los segundos generadores de algunos de ellos. Llamemos $\mathfrak{p}=(2,1+\alpha)$.

Claramente $\mathfrak{p}\mid 1+\alpha$, y como no hay mas ideales de norma 2, necesariamente $1+\alpha=\mathfrak{p}^2$. Esto implica que en el grupo de clases $[\mathfrak{p}^2]=1$, luego $[\mathfrak{p}]=[\mathfrak{p}]^{-1}$. Por otra parte, si $\mathfrak{q}=(2,1+\alpha+\alpha^2)$, entonces $2=\mathfrak{pq}$, con lo que $[\mathfrak{q}]=[\mathfrak{p}]^{-1}=[\mathfrak{p}]$.

Similarmente, $-1+\alpha=\mathfrak{p}(3,-1+\alpha)$, con lo que $[(3,-1+\alpha)]=[\mathfrak{p}]^{-1}=[\mathfrak{p}]$. Así mismo $[(3,-1+\alpha+\alpha^2)]=[(3,-1+\alpha)]^{-1}=[\mathfrak{p}]$.

El mismo argumento justifica que los ideales de norma 5 y 25 son similares a $\mathfrak{p}$. El ideal de norma 17 es principal. También son principales los ideales de norma 53 y 67, pues $\mathrm{N}(2+3\alpha)=53$ y $\mathrm{N}(3+2\alpha)=67$. Teniendo esto en cuenta, todos los ideales de la segunda columna resultan ser similares a 1 o a $\mathfrak{p}$.

Respecto a la tercera columna, todos los ideales son claramente similares a 1 o a $\mathfrak{p}$ salvo quizá el segundo y el tercero. Tanteando un poco observamos que $\mathrm{N}(-1+3\alpha^2)=-2\cdot 71$, luego uno de los tres ideales de norma 71 divide a este número. Para saber cuál de los tres, notamos que α es congruente con -12, -26 y -33 módulo cada uno de ellos, luego $-1+3\alpha^2$ sólo es congruente con 0 módulo el tercero. Así pues, $-1+3\alpha^2=\mathfrak{p}(71,33+\alpha)$, luego $(71,33+\alpha)$ es similar a $\mathfrak{p}$. Como el producto de los tres ideales es 71 y el primero es también similar a $\mathfrak{p}$, concluimos que el segundo es principal.

En resumen, hemos probado que todo primo de norma menor que 80 es similar a 1 o a $\mathfrak{p}$. Todo ideal de norma menor o igual que 80 es producto de algunos de estos primos, luego es similar a una potencia de $\mathfrak{p}$, pero como la clase de $\mathfrak{p}$ tiene orden 2, de hecho es similar a 1 o a $\mathfrak{p}$. Por lo tanto el grupo de clases tiene uno o dos elementos, según si $\mathfrak{p}$ es principal o no lo es.

Puesto que $\mathfrak{p}$ es el único ideal de norma 2, será principal si y sólo si existe un entero de norma ± 2. Vamos a probar que no es así, con lo que definitivamente, el número de clases será $h=2$. La constante del teorema 3.24 es menor que $A=1$.

Es fácil ver que α es una unidad fundamental de K, pues se cumple que $l(\alpha)=(-1.40138,1.40138)$ y su norma es menor que 2, luego si no fuera una unidad fundamental, habría otra de norma menor que 1, y sus coordenadas estarían acotadas en módulo por $e+2e^{1/2}=6.02$. Las únicas unidades que cumplen estas cotas son ± 1, $\pm\alpha$, $\pm\alpha^3$ y $\pm\alpha^4$.

Según hemos razonado antes, si existiera un entero de norma ± 2, multiplicando por una unidad existiría uno ξ cuya representación logarítmica sería de la forma

$$l(\xi) = \frac{\log 2}{2}(1,1) + \beta l(\alpha),$$

con $|\beta| \leq 1/2$, lo que lleva a que los conjugados de ξ han de estar acotados por $e^{1.05}$ (el real) y $e^{1.05/2}$ (los imaginarios). Según el teorema 3.24, las coordenadas de ξ están acotadas por $A(e^{1.5} + 2e^{1.5/2}) < 7.4$. Se comprueba sin dificultad que no hay números de norma ± 2 en ese rango. ∎

Ejercicio: Mostrar un ejemplo de factorización no única en el cuerpo anterior.

En general, para saber si dos ideales dados $\mathfrak{a}$ y $\mathfrak{b}$ son o no similares factorizamos $\mathrm{N}(\mathfrak{b})$ en ideales primos y multiplicamos los factores diferentes de $\mathfrak{b}$, con lo que obtenemos un ideal $\mathfrak{c}$ tal que $\mathfrak{bc} = \mathrm{N}(\mathfrak{b})$, y por lo tanto $[\mathfrak{c}] = [\mathfrak{b}]^{-1}$. Entonces $[\mathfrak{a}] = [\mathfrak{b}]$ si y sólo si $[\mathfrak{ab}^{-1}] = [\mathfrak{ac}] = 1$, es decir, si y sólo si el ideal $\mathfrak{ac}$ es principal, si y sólo si éste contiene un número de norma $\mathrm{N}(\mathfrak{ac})$. Esto nos permite calcular explícitamente el grupo de clases de un cuerpo numérico dado: se obtiene un conjunto finito de representantes de las clases, se eliminan los redundantes y para cada producto $\mathfrak{ab}$ se calcula el ideal del conjunto de representantes al cual es similar.

En realidad nos falta algo para poder realizar en la práctica estos cálculos, y es que en los algoritmos que hemos visto hasta ahora siempre hemos supuesto que conocida una base de los módulos que hemos manejado. Esto es cierto en general, excepto cuando el módulo es un ideal, en cuyo caso es frecuente que lo que conozcamos sea un generador como ideal y no una base como módulo. En lugar de describir en general el método para calcular bases (que sería engorroso) lo mostraremos con un ejemplo ilustrativo: Calcularemos una base del ideal generado por $\omega^3 + \omega + 1$ en el anillo de enteros ciclotómicos de orden 7.

Un elemento arbitrario de este ideal es de la forma

$$(a\omega^5 + b\omega^4 + c\omega^3 + d\omega^2 + e\omega + f)(\omega^3 + \omega + 1) = (b - c + d)\omega^5 + (-a + b + e)\omega^4$$
$$+(-a + d + f)\omega^3 + (-a - c + d + e)\omega^2 + (-c + e + f)\omega + (-a + b - c + f).$$

Como sólo nos interesa la estructura de módulo conviene escribir simplemente

$$(b - c + d, -a + b + e, -a + d + f, -a - c + d + e, -c + e + f, -a + b - c + f).$$

Si el ideal tuviera dos generadores llegaríamos a una expresión similar pero con el doble número de parámetros. Llamemos $M \subset \mathbb{Z}^6$ a este módulo. Podemos llegar a una expresión similar si partimos de un módulo dado por un conjunto de generadores.

Igualamos a 0 la primera componente $b - c + d = 0$, con lo que $b = c - d$. Si sustituimos llegamos a la expresión general de un elemento del módulo $M_2 = M \cap (0 \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})$, que es

$$(0, -a + c - d + e, -a + d + f, -a - c + d + e, -c + e + f, -a - d + f).$$

Restando ambas expresiones obtenemos $(b - c + d, b - c + d, 0, 0, 0, b - c + d)$, luego si llamamos $v_1 = (1, 1, 0, 0, 0, 1) \in M$, tenemos que $M = \langle v_1 \rangle + M_2$.

Igualamos a 0 la segunda componente de la expresión general de un elemento de M_2 y obtenemos $a = c - d + e$. Sustituyendo obtenemos una expresión de un elemento genérico de $M_3 = M \cap (0 \times 0 \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})$, que es

$$(0, 0, -c + 2d - e + f, -2c + 2d, -c + e + f, -c - e + f).$$

Al restar queda

$$(0, -a + c - d + e, -a + c - d + e, -a + c - d + e, 0, -a - c - d + e),$$

luego llamando $v_2 = (0, 1, 1, 1, 0, 1) \in M_2$ resulta que $M = \langle v_1, v_2 \rangle + M_3$.

Ahora $c = 2d - e + f$, la expresión de un elemento de M_4 es

$$(0, 0, 0, -2d + 2e - 2f, -2d + 2e, -2d),$$

y al restar queda

$$(0, 0, -c + 2d - e + f, -2c + 4d - 2e + 2f, -c + 2d - e + f, -c + 2d - e + f),$$

luego haciendo $v_3 = (0, 0, 1, 2, 1, 1) \in M_3$ llegamos a que $M = \langle v_1, v_2, v_3 \rangle + M_4$.

Ahora $d = e - f$, luego los elementos de M_5 son de la forma

$$(0, 0, 0, 0, 2f, -2e + 2f)$$

y la resta da $(0, 0, 0, -2d+2e-2f, -2d+2e-2f, -2d+2e-2f)$, luego podemos tomar $v_4 = (0, 0, 0, 2, 2, 2) \in M_4$ y así $M = \langle v_1, v_2, v_3 v_4 \rangle + M_5$.

La siguiente ecuación es $f = 0$, que da $(0, 0, 0, 0, 0, -2e)$ para los elementos de M_6 y $v_5 = (0, 0, 0, 0, 2, 2) \in M_5$. Claramente $v_6 = (0, 0, 0, 0, 0, 2) \in M_6$ completa un sistema generador de M, que por ser triangular es obviamente una base. En resumen, una base del ideal $(\omega 3 + \omega + 1)$ la forman los enteros

$$\omega^5 + \omega^4 + 1, \quad \omega^4 + \omega^3 + \omega^2 + 1, \quad \omega^3 + 2\omega^2 + \omega + 1, \quad 2\omega^2 + 2\omega + 2, \quad 2\omega + 2, \quad 2.$$

El método que hemos seguido tiene la ventaja de que se justifica a sí mismo cada vez que se emplea, pero si el lector desea algo más rápido puede probar que no es necesario restar las nuevas expresiones de las anteriores para obtener los generadores, sino que basta asignar a los parámetros los valores adecuados para que la primera componente no nula tome valor mínimo mayor que 0. Por ejemplo, para obtener v_1 basta hacer $b = 1$ y los demás parámetros nulos en la expresión general de un elemento de M y quedarnos con $v_1 = (1, 1, 0, 0, 0, 1)$, luego hacemos $c = 1$ en M_2 y sale $v_2 = (0, 1, 0, -1, -1, 0)$. En la expresión de M_3 hacemos $c = -1$ y queda $v_3 = (0, 0, 1, 2, 1, 1)$. En M_4 hacemos $e = 1$ y así $v_4 = (0, 0, 0, 2, 2, 0)$. En M_5 tomamos $f = 1$, con lo que $v_5 = (0, 0, 0, 0, 2, 2)$, y finalmente $v_6 = (0, 0, 0, 0, 0, 2)$.

Es fácil ver que estos elementos generan el mismo módulo. De hecho, eligiendo adecuadamente los parámetros según este criterio, podríamos haber llegado a la misma base.

El único inconveniente adicional que puede surgir es que no podamos despejar ninguna variable en una ecuación porque todas tengan los coeficientes

distintos de ± 1. En tal caso, puesto que igualamos a 0, tendremos siempre los coeficientes primos entre sí (no necesariamente dos a dos), y no es difícil ver que siempre es posible hacer un cambio de variables lineal de determinante 1 que deje una variable con coeficiente 1.

Una aplicación del cálculo de bases es, por ejemplo, decidir si dos módulos dados son o no el mismo módulo. Lo serán si la matriz de cambio de base tiene determinante ± 1.

Por último hemos de notar que en este capítulo hemos proporcionado las técnicas necesarias para resolver, al menos en teoría, cualquier ecuación diofántica de la forma (1.3), pues al principio de esta sección hemos visto cómo encontrar un conjunto finito de elementos $\alpha_1, \ldots, \alpha_m$ de una norma dada en un módulo completo M de modo que cualquier otro sea asociado a uno de ellos, y por otra parte sabemos generar todas las unidades de $\mathcal{O}_M$ de norma 1. Con esto sabemos generar todos los elementos de M de una norma dada, los cuales determinan a su vez todas las soluciones enteras de (1.3).

Capítulo IV

La función dseta de Dedekind

En la sección [ITAn 7.6] demostramos el teorema de Dirichlet sobre primos en progresiones aritméticas. Recordemos su enunciado:

Teorema de Dirichlet *Si m y n son números naturales no nulos primos entre sí, la sucesión $mk+n$, para $k = 1, 2, 3, \ldots$ contiene infinitos primos.*

Si llamamos U_m al grupo de las unidades del anillo $\mathbb{Z}/m\mathbb{Z}$, es decir [Al 6.43]

$$U_m = \{[n] \in \mathbb{Z}/m\mathbb{Z} \mid (m,n) = 1\},$$

el teorema de Dirichlet implica que cada clase de U_m contiene infinitos primos.

La prueba que dimos allí es una versión "elemental" que resulta de despojar la prueba original de Dirichlet de todo uso del análisis complejo. Aquí vamos a dar una prueba mucho más próxima al argumento original de Dirichlet, que es conceptualmente mucho más simple. El punto de partida de Dirichlet fue un resultado de Euler [ITAn 8.26]:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}},$$

donde p recorre los números primos y $s > 1$.

Esta fórmula puede considerarse como la primera piedra de la teoría analítica de números. En ella se relacionan una serie y un producto infinito (objetos analíticos) con la sucesión de los números primos. La demostración utiliza por una parte resultados analíticos sobre convergencia de series y por otra el teorema fundamental de la aritmética.

Gauss estudió más a fondo la fórmula de Euler y definió la que hoy se conoce como *función dseta de Riemann:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{para } s > 1.$$

En [ITAn 4.9] probamos que la serie converge efectivamente para $s > 1$, y además

$$\lim_{s\to 1^+} (s-1)\zeta(s) = 1. \tag{4.1}$$

Euler notó que esto implica la existencia de infinitos números primos. En efecto, (4.1) implica que el miembro izquierdo de la fórmula de Euler tiende a infinito cuando s tiende a 1, pero el miembro derecho estaría acotado si el producto fuera finito. Por supuesto la existencia de infinitos primos puede probarse por medios mucho más elementales (ya hay una prueba en los Elementos, de Euclides), sin embargo, tras intentar sin éxito generalizar la prueba de Euclides para demostrar que toda sucesión aritmética contiene números primos, Dirichlet se planteó la posibilidad de lograrlo mediante el argumento de Euler aplicado a la teoría de Kummer sobre factorización ideal en cuerpos ciclotómicos. A su vez, luego Kummer usó los resultados de Dirichlet para dar una caracterización sencilla de los primos regulares [Al 8.44] a los que era aplicable su prueba del Último Teorema de Fermat.

Aquí expondremos los resultados de Dirichlet sobre la función dseta generalizada en el caso más general de cuerpos numéricos arbitrarios, tal y como fue desarrollada por Dedekind. Notemos que en la sección [ITAn 11.1] definimos y estudiamos las funciones dseta de Dedekind asociadas a los cuerpos cuadráticos.

4.1 Convergencia de la función dseta

Definición 4.1 Sea K un cuerpo numérico. Se llama *función dseta de Dedekind* de K a la función

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{a}$ recorre todos los ideales no nulos de K y $s > 1$.

Observemos que la función dseta de $\mathbb{Q}$ es precisamente la función dseta de Riemann.

Nuestro primer problema es demostrar que esta serie converge para $s > 1$. Notemos que, puesto que los términos de la serie son todos positivos, no importa que no hayamos prefijado ninguna ordenación en los ideales de K. Si la serie converge ordenando los sumandos con una ordenación cualquiera, convergerá con cualquier otra ordenación, por lo que no es necesario especificar ninguna.

Aunque podríamos trabajar con la serie tal cual la acabamos de definir, conviene hacerle una manipulación:

$$\zeta_K(s) = \sum_{C} \sum_{\mathfrak{a}\in C} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde C recorre las clases de similitud de ideales de K.

Por [An 2.88], la convergencia de la serie $\zeta_K(s)$ es equivalente a la convergencia de las h series

$$\zeta_C(s) = \sum_{\mathfrak{a}\in C} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde h es el número de clases de K. Más aún, por ese mismo teorema,

$$\zeta_C(s) = \sum_{k=1}^{\infty} \frac{f_C(k)}{k^s},$$

donde $f_C(k)$ es el número de ideales[1] en C de norma k. La igualdad hay que entenderla como que si la segunda serie es convergente, también lo será la primera. De este modo hemos reducido el problema a tratar con series "usuales" de números reales.

La convergencia la obtendremos a partir de una estimación de la sucesión de coeficientes. Más exactamente, estimaremos la función $j_C(r)$ que da el número de ideales de C de norma menor o igual que r.

Fijamos un ideal $\mathfrak{b}$ perteneciente a la clase inversa C^{-1} en el grupo de clases. Entonces para cada ideal $\mathfrak{a} \in C$ el producto $\mathfrak{ab}$ está en la clase principal, es decir, es un ideal principal $\mathfrak{ab} = (\alpha)$. La aplicación que a cada ideal $\mathfrak{a} \in C$ le asigna el ideal $\mathfrak{ab}$ es una biyección entre los ideales de C y los ideales principales (α) de K divisibles entre $\mathfrak{b}$. Además $\mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b}) = |\,\mathrm{N}(\alpha)|$, luego $j_C(r)$ es el número de ideales principales de K divisibles entre $\mathfrak{b}$ y de norma menor o igual que $r\,\mathrm{N}(\mathfrak{b})$.

En lugar de contar ideales principales contaremos enteros $\alpha \in \mathfrak{b}$ tales que $|\,\mathrm{N}(\alpha)| \le r\,\mathrm{N}(\mathfrak{b})$, pero, para no contar varias veces—infinitas, de hecho— el mismo ideal, hemos de considerar sólo un representante de cada clase de equivalencia respecto a la asociación.

El proceso de selección de los representantes lo llevaremos a cabo con la ayuda de los métodos geométricos desarrollados en el capítulo anterior. Conservamos la notación que introdujimos allí. Concretamente $\sigma_1, \ldots, \sigma_s$ serán los monomorfismos reales de K, mientras que $\sigma_{s+1}, \bar\sigma_{s+1}, \ldots, \sigma_{s+t}, \bar\sigma_{s+t}$ serán los monomorfismos complejos. Así, el grado de K será $n = s+2t$. La representación geométrica de un número $\alpha \in K$ es

$$x(\alpha) = \big(\sigma_1(\alpha), \ldots, \sigma_{s+t}(\alpha)\big) \in \mathcal{R}^{st}.$$

En $\mathcal{R}^{st}$ se define la norma $\mathrm{N}(x_1, \ldots, x_{s+t}) = x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2$, de modo que $\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$ y $\mathrm{N}\big(x(\alpha)\big) = \mathrm{N}(\alpha)$.

Los elementos $x \in \mathcal{R}^{st}$ con $\mathrm{N}(x) \ne 0$ tienen asignada la representación logarítmica dada por $l(x) = \big(l_1(x), \ldots, l_{s+t}(x)\big)$, donde

$$l_k(x) = \begin{cases} \log|x_k| & \text{para } k = 1, \ldots, s, \\ \log|x_k|^2 & \text{para } k = s+1, \ldots, s+t. \end{cases}$$

[1] Recordemos que por 2.48 (o [Al 8.36]) el número de ideales de K con una norma dada es finito.

Sea $\epsilon_1, \ldots, \epsilon_r$ un sistema fundamental de unidades de K. Sabemos que los vectores $l(\epsilon_1), \ldots, l(\epsilon_r)$ forman una base del subespacio

$$V = \{x \in \mathbb{R}^{s+t} \mid x_1 + \cdots + x_{s+t} = 0\},$$

de dimensión $r = s + t - 1$.

Si a estos vectores les añadimos $l^* = (1, \overset{s)}{\ldots}, 1, 2, \overset{t)}{\ldots}, 2)$ obtenemos una base de $\mathbb{R}^{s+t}$. Así, la representación logarítmica de cada vector $x \in \mathcal{R}^{st}$ de norma no nula se expresa de forma única como $l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r)$, donde $\xi, \xi_1, \ldots, \xi_r$ son números reales. Por último, sea m el número de raíces de la unidad contenidas en K.

Definición 4.2 Con la notación anterior, un subconjunto X de $\mathcal{R}^{st}$ es un *dominio fundamental* de K si es el conjunto de los puntos x que cumplen las condiciones siguientes:

1. $\mathrm{N}(x) \neq 0$,
2. $l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r)$, con $0 \leq \xi_i < 1$.

El dominio fundamental de K está unívocamente determinado si fijamos un sistema fundamental de unidades de K. El teorema siguiente prueba que todo entero de K tiene un único asociado en el dominio fundamental salvo raíces de la unidad, es decir, que en realidad tiene m asociados. Podríamos haber dado una definición ligeramente más restrictiva de modo que sólo hubiera un asociado, pero esto complicaría ligeramente las pruebas, y a la hora de contar ideales no importa que cada uno aparezca repetido m veces, pues basta dividir entre m el resultado final.

Teorema 4.3 *Cada elemento no nulo de K tiene exactamente m asociados cuya representación geométrica se encuentra en el dominio fundamental de K.*

Para probarlo demostramos primero lo siguiente:

Teorema 4.4 *Si $y \in \mathcal{R}^{st}$ y $\mathrm{N}(y) \neq 0$, entonces y admite exactamente m representaciones de la forma $y = x\,x(\epsilon)$, donde x pertenece al dominio fundamental de K y ϵ es una unidad de K.*

Demostración: Sea $l(y) = \gamma l^* + \gamma_1 l(\epsilon_1) + \cdots + \gamma_r l(\epsilon_r)$. Para $j = 1, \ldots, r$ descompongamos $\gamma_j = k_j + \xi_j$, donde k_j es un entero racional y $0 \leq \xi_j < 1$.

Sea $\epsilon = \epsilon_1^{k_1} \cdots \epsilon_r^{k_r}$ y $x = y\,x(\epsilon^{-1})$. Entonces $y = x\,x(\epsilon)$, $\mathrm{N}(x) = \mathrm{N}(y) \neq 0$ y $l(x) = l(y) + l(\epsilon^{-1}) = l(y) - k_1 l(\epsilon_1) - \cdots - k_r l(\epsilon_r) = \gamma l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r)$, luego x está en el dominio fundamental de K.

Por otra parte, si $x\,x(\epsilon) = x'\,x(\epsilon')$, entonces $l(x) + l(\epsilon) = l(x') + l(\epsilon')$. Las coordenadas de $l(\epsilon)$ y $l(\epsilon')$ en la base $l(\epsilon_1), \ldots, l(\epsilon_r)$ son enteros racionales, y las de $l(x)$ y $l(x')$ están entre 0 y 1. La unicidad de la parte entera de un número real nos da que $l(\epsilon) = l(\epsilon')$. Consecuentemente $\epsilon' = \epsilon\omega$, donde ω es una raíz m-sima de la unidad, y por lo tanto las representaciones de y en la forma indicada son exactamente $y = x\,x(\epsilon)x(\omega)$, donde x y ϵ son fijos y ω recorre las m raíces de la unidad de K. ∎

DEMOSTRACIÓN (del teorema 4.3): Si $\beta \in K$ es no nulo entonces por el teorema anterior existen m representaciones distintas $x(\beta) = x\,x(\epsilon)$ con $x \in X$ y ϵ una unidad de K. Los números $\beta\epsilon^{-1}$ son m asociados de β que cumplen $x(\beta\epsilon^{-1}) = x \in X$.

Recíprocamente, cada asociado de $\beta\epsilon$ tal que $x = x(\beta)x(\epsilon) \in X$ da lugar a una representación distinta $x(\beta) = x\,x(\epsilon^{-1})$, luego hay exactamente m. ∎

Antes de seguir con el problema de la convergencia de las funciones dseta señalamos una propiedad importante de los dominios fundamentales:

Si $\xi > 0$ es un número real y $x \in \mathcal{R}^{st}$ tiene norma no nula, entonces

$$\begin{aligned} l_k(\xi x) &= \log|\xi x_k| = \log\xi + l_k(x), \quad \text{para } 1 \le k \le s,\\ l_j(\xi x) &= \log|\xi x_j|^2 = 2\log\xi + l_k(x), \quad \text{para } 1 \le j \le t. \end{aligned}$$

En consecuencia, $l(\xi x) = \log\xi\, l^* + l(x)$ y las coordenadas $\xi_1, \dots, \xi_r$ de los vectores $l(\xi x)$ y $l(x)$ en la base $l^*, l(\epsilon_1), \dots, l(\epsilon_r)$ son las mismas.

Todo esto implica que si el dominio fundamental de K contiene a un vector x, también contiene a todos sus múltiplos positivos. Los subconjuntos de $\mathcal{R}^{st}$ con esta propiedad se llaman *conos.*

Recordemos que estamos buscando una estimación de la función $j_C(r)$, que puede calcularse como el número de ideales principales (α) tales que $\alpha \in \mathfrak{b}$ y $|\,\mathrm{N}(\alpha)| \le r\,\mathrm{N}(\mathfrak{b})$. Si llamamos $\mathcal{M}$ a la imagen de $\mathfrak{b}$ por la representación geométrica, que es un retículo completo de $\mathbb{R}^n$, cada ideal tiene exactamente m generadores en el dominio fundamental X, luego $mj_C(r)$ es el número de vectores $x \in \mathcal{M} \cap X$ que cumplen $|\,\mathrm{N}(x)| \le r\,\mathrm{N}(\mathfrak{b})$.

Llamemos $T = \{x \in X \mid |\,\mathrm{N}(x)| \le 1\}$. Teniendo en cuenta que si $r > 0$ es un número real entonces $\mathrm{N}(rx) = r^n\,\mathrm{N}(x)$ (donde n es el grado de K), así como que X es un cono, resulta que

$$\{x \in X \mid |\,\mathrm{N}(x)| \le r\} = \left\{ \sqrt[n]{r}\left(\frac{x}{\sqrt[n]{r}}\right) \in X \mid \left|\mathrm{N}\left(\frac{x}{\sqrt[n]{r}}\right)\right| \le 1 \right\} = \sqrt[n]{r}\,T,$$

luego $m\,j_C(r)$ es también el número de puntos de $\mathcal{M} \cap \sqrt[n]{\mathrm{N}(\mathfrak{b})\,r}\,T$, y nuestro problema se reduce a estimar el número de puntos de un retículo completo en un determinado conjunto. Para resolverlo daremos un teorema general que requiere algunos conceptos nuevos:

Definición 4.5 Un *cubo* en $\mathbb{R}^k$ es un producto cartesiano de k intervalos cerrados y acotados. Si todos ellos son iguales a $[0,1]$ tenemos el *cubo unitario.*

Si $S \subset \mathbb{R}^k$, una función $\phi : S \longrightarrow \mathbb{R}^n$ tiene la *propiedad de Lipschitz* si existe una constante C tal que para todo $x, y \in S$ se cumple $\|\phi(x) - \phi(y)\| \le C\|x - y\|$. (Compárese con [An 2.52].)

Usando el teorema del valor medio es fácil ver que toda función de clase C^1 tiene la propiedad de Lipschitz en compactos.[2]

Un subconjunto $D \subset \mathbb{R}^n$ es *parametrizable Lipschitz* de grado k si existe un número finito de funciones de Lipschitz con dominio $[0,1]^k$ cuyas imágenes cubren a D.

Dadas tres funciones f, g, $h :]0,+\infty[\longrightarrow \mathbb{R}$, diremos que

$$f(r) = g(r) + O\big(h(r)\big)$$

si la función $\big(f(r) - g(r)\big)/h(r)$ está acotada.

Con esto podemos probar el resultado general sobre cómputo de los puntos de un retículo en un recinto:

Teorema 4.6 *Sea T un subconjunto acotado de $\mathbb{R}^n$ medible Lebesgue cuya frontera sea parametrizable Lipschitz de grado $n-1$, sea $\mathcal{M}$ un retículo completo en $\mathbb{R}^n$, sea V la medida de su paralelepípedo fundamental, sea $v = \mu(T)$ y sea $u \in \mathbb{R}^n$. Si $n(r)$ es el número de puntos de $u + \mathcal{M}$ contenidos en rT, entonces*

$$n(r) = \frac{v}{V}\, r^n + O(r^{n-1}),$$

donde la cota en O depende sólo de $\mathcal{M}$, de n y de las constantes de Lipschitz.

Demostración: Sea P el paralelepípedo fundamental de $\mathcal{M}$. Sea $m(r)$ el número de puntos $x \in u + \mathcal{M}$ tales que $x + P$ está contenido en el interior de rT y sea $f(r)$ el número de puntos $x \in u + \mathcal{M}$ tales que $x + P$ corta a la frontera de rT. Claramente $m(r) \le n(r) \le m(r) + f(r)$.

Los $m(r)$ trasladados de P son disjuntos y están contenidos en rT, que a su vez está contenido en la unión de los $m(r) + f(r)$ trasladados de P, también disjuntos. Tomando medidas queda $m(r)V \le r^n v \le m(r)V + f(r)V$, luego

$$m(r) \le \frac{v}{V}\, r^n \le m(r) + f(r).$$

Así pues, $|n(r) - (v/V)r^n| \le f(r)$, y sólo hay que probar que $f(r) \le Cr^{n-1}$. Para ello nos apoyaremos en el hecho siguiente: el número de puntos $x \in u + \mathcal{M}$ tales que $x + P$ corta a un conjunto de diámetro dado d está acotado por una cantidad que sólo depende de $\mathcal{M}$ y de d, pero no del conjunto. En efecto, mediante una traslación podemos suponer que $u = 0$ y que uno de tales puntos es el 0, y entonces dichos puntos están contenidos en la bola de centro 0 y radio la suma de d más el diámetro de P, y el conjunto de puntos de $\mathcal{M}$ en esta bola es la constante buscada.

[2] En [An 5.44] está probado esencialmente para compactos convexos (con la norma ∞, que puede sustituirse por cualquier otra norma equivalente), pero un compacto arbitrario se puede cubrir por un número finito de bolas cerradas convexas, y si una función es lipschitziana en una familia finita de conjuntos es claro que también lo es en su unión.

Sea $\phi : [0,1]^{n-1} \longrightarrow \mathbb{R}^n$ una función de Lipschitz que cubra una porción de la frontera de T. Entonces $r\phi$ sigue siendo de Lipschitz y cubre la porción correspondiente de la frontera de rT. Sea $[r]$ la parte entera de r.

Si dividimos el intervalo $[0,1]$ en $[r]$ segmentos de longitud $1/[r]$, el cubo unidad queda dividido en $[r]^{n-1}$ cubos cuyas imágenes por ϕ tienen diámetro a lo sumo $C_0/[r]$, donde C_0 depende sólo de n y de la constante de ϕ, luego la imagen por $r\phi$ de cada uno de estos cubos tiene diámetro a lo sumo C_1 (independiente de r).

El número de puntos $x \in u + \mathcal{M}$ tales que $x + P$ corta a esta imagen está acotado por una cantidad C_2 que sólo depende de $\mathcal{M}$, de n y de la constante de ϕ, luego el número de puntos $x \in u + \mathcal{M}$ tales que $x + P$ corta a la imagen de $r\phi$ es a lo sumo $C_2[r]^{n-1} \le C_2 r^{n-1}$.

Como toda la frontera está cubierta por un número finito de tales imágenes, concluimos que $f(r) \le Cr^{n-1}$, para una cierta constante C. ∎

Ahora hemos de aplicar este teorema cuando $\mathcal{M}$ es la imagen del ideal $\mathfrak{b}$ por la representación geométrica, $u = 0$ y

$$T = \big\{x \in X \;\big|\; |\,\mathrm{N}(x)| \le 1\big\}.$$

Ejercicio: Representar gráficamente el conjunto T para un cuerpo cuadrático real y para un cuerpo cuadrático imaginario.

Hemos visto que, en términos de la función $n(r)$ la función j_C es

$$j_C(r) = \frac{n\big(\sqrt[n]{r\,\mathrm{N}(\mathfrak{b})}\big)}{m}. \tag{4.2}$$

Para aplicar el teorema hemos de probar que T satisface las hipótesis. Esto nos lleva a un cálculo bastante largo:

Todo $x \in \mathcal{R}^{st}$ de norma no nula cumple

$$l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r), \tag{4.3}$$

donde $\xi, \xi_1, \ldots, \xi_r$ son números reales. El conjunto T está formado por los vectores x que cumplen:

1. $0 < \big|\mathrm{N}(x)\big| \le 1$,
2. $0 \le \xi_i < 1$.

En la prueba del teorema 3.21 observamos que la aplicación de $\mathcal{R}^{st}$ en $\mathcal{R}^{st}$ que a cada x le asigna yx (para un cierto $y \in \mathcal{R}^{st}$ fijo) es lineal (considerando a $\mathcal{R}^{st}$ como espacio vectorial sobre $\mathbb{R}$) y que su determinante es $\mathrm{N}(y)$.

Sea T' el conjunto de los puntos de T cuyas s coordenadas reales sean positivas. Si fijamos un conjunto de s signos $\delta_1, \ldots, \delta_s = \pm 1$, entonces la multiplicación por el punto $(\delta_1, \ldots, \delta_s, 1, \ldots, 1)$ es una aplicación lineal de determinante ± 1. En total hay 2^s aplicaciones de este tipo, que transforman el conjunto

T' en 2^s conjuntos disjuntos de la misma medida y cuya unión es T. Basta probar que T' es acotado, medible y que su frontera es parametrizable Lipschitz de grado $n-1$, pues entonces T también será medible y acotado, $\mu(T) = \mu(T')2^s$ y su frontera será parametrizable Lipschitz de grado $n-1$ (ya que está contenida en la unión de las fronteras de las 2^s imágenes de T').

Representemos las coordenadas de un punto $x \in \mathcal{R}^{st}$ como

$$x = (x_1, \ldots, x_s, y_1 + iz_1, \ldots, y_t + iz_t).$$

Estamos identificando $\mathcal{R}^{st}$ con $\mathbb{R}^n$, con lo que x se identifica con la n-tupla

$$(x_1, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t).$$

Según la ecuación (3.1), las componentes de $l(x)$ suman $\log\bigl|\mathrm{N}(x)\bigr|$, pero sumando en el miembro derecho de (4.3) y teniendo en cuenta que las componentes de $l(\epsilon_i)$ suman $\log 1 = 0$, tenemos que $\log\bigl|\mathrm{N}(x)\bigr| = \xi(s+2t) = n\xi$.

Por lo tanto (4.3) se convierte en

$$l(x) = \frac{1}{n}\log\bigl|\mathrm{N}(x)\bigr| l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r). \tag{4.4}$$

Ahora hacemos el cambio de variables

$$\begin{array}{rcll} x_i &=& \rho_i, & i = 1, \ldots, s, \\ y_j &=& \rho_{s+j}\cos\theta_j, & j = 1, \ldots, t, \\ z_j &=& \rho_{s+j}\operatorname{sen}\theta_j, & j = 1, \ldots, t. \end{array}$$

Se comprueba fácilmente que el determinante jacobiano es $\rho_{s+1}\cdots\rho_{s+t}$. Veamos cuál es la expresión de T' en estas coordenadas.

En primer lugar, si $x \in T'$, entonces $\mathrm{N}(x) = \prod_{i=1}^{s+t} \rho_i^{e_i}$, donde $e_i = 1$ para $i = 1, \ldots, s$ y $e_i = 2$ para $i = s+1, \ldots, t$, y $l_i(x) = \log \rho_i^{e_i}$. La ecuación (4.4) equivale al sistema de ecuaciones

$$\log \rho_j^{e_j} = \frac{e_j}{n}\log\prod_{i=1}^{s+t}\rho_i^{e_i} + \sum_{k=1}^{r}\xi_k l_j(\epsilon_k). \tag{4.5}$$

Por lo tanto el conjunto T' está formado por los puntos de coordenadas

$$(\rho_1, \ldots, \rho_{s+t}, \theta_1, \ldots, \theta_t)$$

tales que

1. $0 < \prod_{i=1}^{s+t} \rho_i^{e_i} \le 1, \quad 0 \le \theta_1, \ldots, \theta_t < 2\pi.$

2. En (4.5) se cumple $0 \le \xi_k < 1$.

Para probar que T' está acotado basta ver que lo están las coordenadas ρ_i de todos sus puntos. Ahora observamos que las ecuaciones

$$\log \rho_j^{e_j} = \frac{e_j}{n} \log \xi + \sum_{k=1}^{r} \xi_k l_j(\epsilon_k). \tag{4.6}$$

definen un cambio de variables

$$(\rho_1, \ldots, \rho_{s+t}, \theta_1, \ldots, \theta_t) \mapsto (\xi, \xi_1, \ldots, \xi_r, \theta_1, \ldots, \theta_t)$$

y, respecto a éstas últimas, el conjunto F' está definido por las condiciones

$$0 < \xi \leq 1, \quad 0 \leq \xi_k < 1, \quad 0 \leq \theta_j < 2\pi. \tag{4.7}$$

En efecto, las ecuaciones (4.6) pueden escribirse también como

$$\log \rho_j = \frac{1}{n} \log \xi + \sum_{k=1}^{r} \xi_k \log |\sigma_j(\epsilon_k)|, \qquad j = 1, \ldots, s+t,$$

o también

$$\rho_j = \xi^{1/n} \exp\left(\sum_{k=1}^{r} \xi_k \log |\sigma_j(\epsilon_k)| \right), \qquad j = 1, \ldots, s+t. \tag{4.8}$$

Esto nos da $(\rho_1, \ldots, \rho_{s+t}, \theta_1, \ldots, \theta_t)$ a partir de $(\xi, \xi_1, \ldots, \xi_r, \theta_1, \ldots, \theta_t)$. Para la transformación inversa notamos que al sumar las ecuaciones (4.6) queda $\xi = \prod_{i=1}^{s+t} \rho_i^{e_i}$ y las coordenadas ξ_i están determinadas por un sistema de r ecuaciones lineales con determinante no nulo (notemos que la determinación de ξ hace que se cumpla la suma de las $s+t$ ecuaciones, luego si los ξ_i se escogen de modo que cumplan las $s+t-1$ primeras, la última se cumple automáticamente).

Ahora ya es claro que T' está acotado. Para calcular el determinante jacobiano comprobamos que

$$\frac{\partial \rho_j}{\partial \xi} = \frac{\rho_j}{n\xi}, \quad \frac{\partial \rho_j}{\partial \xi_k} = \frac{\rho_j}{e_j} l_j(\epsilon_k).$$

Por consiguiente el jacobiano es

$$\begin{aligned} J &= \begin{vmatrix} \dfrac{\rho_1}{n\xi} & \dfrac{\rho_1}{e_1} l_1(\epsilon_1) & \cdots & \dfrac{\rho_1}{e_1} l_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ \dfrac{\rho_{s+t}}{n\xi} & \dfrac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\epsilon_1) & \cdots & \dfrac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\epsilon_r) \end{vmatrix} \\ &= \frac{\rho_1 \cdots \rho_{s+t}}{n\xi\, 2^t} \begin{vmatrix} e_1 & l_1(\epsilon_1) & \cdots & l_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ e_{s+t} & l_{s+t}(\epsilon_1) & \cdots & l_{s+t}(\epsilon_r) \end{vmatrix}. \end{aligned}$$

En el último determinante sumamos todas las filas a la primera, con lo que ésta se convierte en $(n, 0, \dots, 0)$. Desarrollando el determinante y recordando la definición del regulador R de K dada en 3.23, obtenemos que el determinante jacobiano vale

$$J = \frac{\rho_1 \cdots \rho_{s+t}}{\xi\, 2^t} R = \frac{R}{2^t \rho_{s+1} \cdots \rho_{s+t}}.$$

Recordemos que el primer cambio de variables tenía jacobiano $\rho_{s+1} \cdots \rho_{s+t}$, luego el jacobiano de la composición es $R/2^t$.

Puesto que T' se obtiene de un cubo mediante un cambio de variables de clase C^1, podemos concluir que T' es medible y su medida es $(R/2^t)(2\pi)^t = \pi^t R$. Por consiguiente $\mu(T) = 2^s \pi^t R$.

Falta probar que la frontera de T' es parametrizable Lipschitz. Ahora bien, cambiando $\xi^{1/n}$ por ξ, el cambio de coordenadas (4.8) se transforma en

$$\rho_j = \xi \exp\left(\sum_{k=1}^{r} \xi_k \log|\sigma_j(\epsilon_k)|\right), \qquad j = 1, \dots, s+t,$$

que, compuesto con el cambio a polares, nos da una aplicación h de clase C^1 que biyecta el cubo $]0,1] \times [0,1[^r \times [0, 2\pi[^t$ con el conjunto T'. Con un cambio de variables obvio podemos sustituir este cubo por $]0,1] \times [0,1[^{r+t}$.

Ahora bien, esta aplicación está definida de hecho en todo $\mathbb{R}^n$, y la imagen del cubo $[0,1]^n$ es un compacto que contiene a la clausura de T'. Por consiguiente los puntos de la frontera de T' deben ser imagen de puntos de la frontera del cubo.

Esta frontera es la unión de las $2n$ caras formadas por las n-tuplas con una coordenada constante igual a 0 o a 1. Las $2n$ funciones que resultan de sumergir $\mathbb{R}^{n-1}$ en $\mathbb{R}^n$ fijando una coordenada igual a 0 o a 1 son de clase C^1 y las imágenes del cubo $[0,1]^{n-1}$ cubren la frontera del cubo unitario en $\mathbb{R}^n$, por lo que al componerlas con h obtenemos $2n$ funciones de clase C^1 tales que la frontera de T' está cubierta por las imágenes del cubo unitario. Como son de clase C^1, las restricciones al cubo unitario tienen la propiedad de Lipschitz.

Recapitulando, podemos aplicar el teorema 4.6, y las constantes que aparecen son

$$v = \mu(T) = 2^s \pi^t R$$

y, según el teorema 3.5, la medida del paralelepípedo fundamental de la imagen del ideal $\mathfrak{b}$ por la representación geométrica es

$$V = \frac{\sqrt{|\Delta_K|}}{2^t}\, \mathrm{N}(\mathfrak{b}),$$

donde Δ_K es el discriminante de K. La conclusión es que

$$n(r) = \frac{2^{s+t} \pi^t R}{\sqrt{|\Delta_K|}\, \mathrm{N}(\mathfrak{b})}\, r^n + O(r^{n-1}).$$

Teniendo en cuenta la relación (4.2), hemos probado el teorema siguiente (comparar con [ITAn 11.1, 11.3]):

Teorema 4.7 *Sea K un cuerpo numérico de discriminante Δ, sea R el regulador de K, sea m el número de raíces de la unidad contenidas en K y sea C una clase de similitud de ideales de K. Entonces la función $j_C(r)$, definida como el número de ideales en C de norma menor o igual que r, verifica*

$$j_C(r) = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}}\, r + O(r^{1-1/n}).$$

Observemos que en particular se cumple

$$\lim_{r\to+\infty} \frac{j_C(r)}{r} = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}},$$

y hay que destacar que este límite no depende de la clase C. De aquí se sigue precisamente la conexión entre las funciones dseta y el número de clases de K:

Teorema 4.8 *Con la notación del teorema anterior, se cumple*

1. *La función $\zeta_C(s)$ converge uniformemente en los compactos de $]1,+\infty[$ y existe*
$$\lim_{s\to 1^+} (s-1)\zeta_C(s) = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}},$$
2. *La función $\zeta_K(s)$ converge uniformemente en los compactos de $]1,+\infty[$ y*
$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}}\, h, \tag{4.9}$$
donde h es el número de clases de K.

Demostración: El segundo apartado es consecuencia clara del primero. Para probar éste consideremos la sucesión $\{x_k\}$ que comienza con tantos unos como ideales tiene C de norma 1, seguido de tantos doses como ideales tiene C de norma 2, etc. Entonces

$$\zeta_C(s) = \sum_{\mathfrak{a}\in C} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \sum_{k=1}^{\infty} \frac{1}{x_k^s}.$$

Claramente, $j_C(x_k)$ es el número de términos de la sucesión menores o iguales que x_k, luego claramente $j_C(x_k-1) < m \le j_C(x_k)$. Por lo tanto:

$$\left(\frac{x_k-1}{x_k}\right)\frac{j_C(x_k-1)}{x_k-1} < \frac{k}{x_k} \le \frac{j_C(x_k)}{x_k}.$$

Es obvio que x_k tiende a infinito, luego al tomar límites en k queda

$$\lim_k \frac{k}{x_k} = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}}.$$

Llamemos L a este límite. Entonces, dado $\epsilon > 0$, existe un n_0 tal que si $k \geq k_0$ entonces

$$L - \epsilon < \frac{k}{x_k} < L + \epsilon,$$

luego

$$(L-\epsilon)^s \frac{1}{k^s} < \frac{1}{x_k^s} < (L+\epsilon)^s \frac{1}{k^s}.$$

Todo compacto contenido en $]1, +\infty[$ está contenido en un intervalo $[s_0, s_1]$, donde $1 < s_0$, y vemos entonces que la serie $\zeta_C(s)$ está mayorada en dicho compacto por la serie convergente

$$\sum_{k=k_0}^{\infty} (L+\epsilon)^{s_1} \frac{1}{k^{s_0}},$$

luego converge uniformemente. Más aún,

$$(L-\epsilon)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s} \leq \sum_{k=k_0}^{\infty} \frac{1}{x_k^s} \leq (L+\epsilon)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s}.$$

Llamemos $r_1(s)$ y $r_2(x)$ a las sumas de los $n_0 - 1$ primeros términos de las funciones $\zeta(s)$ y $\zeta_C(s)$ (que son funciones continuas en todo $\mathbb{R}$). Así

$$(L-\epsilon)^s \zeta(s) - (L-\epsilon)^s r_1(s) \leq \zeta_C(s) - r_2(s) \leq (L+\epsilon)^s \zeta(s) - (L+\epsilon)^s r_1(s).$$

Multiplicando por $s-1$ y tomando límites cuando s tiende a 1 queda

$$L - \epsilon \leq \liminf_{s \to 1^+} \zeta_C(s) \leq \limsup_{s \to 1^+} \zeta_C(s) \leq L + \epsilon.$$

Como ϵ es arbitrario concluimos que existe

$$\lim_{s \to 1^+} (s-1)\zeta_C(s) = L = \frac{2^s (2\pi)^t R}{m\sqrt{|\Delta_K|}}.$$

∎

Vemos así que la función dseta de Dedekind de un cuerpo K es un objeto analítico que contiene información algebraica importante sobre K precisamente donde no está definida: en el 1.

Notas Aunque no lo vamos a necesitar aquí, se cumple que las funciones $\zeta_C(s)$ definen funciones holomorfas en el semiplano $\operatorname{Re} s > 1$ que se prolongan a funciones holomorfas en el semiplano $\operatorname{Re} s > 1 - 1/n$ salvo en $s = 1$, donde tienen un polo simple, y el límite dado por el teorema anterior calcula precisamente el residuo de dicho polo.

En efecto, esto es consecuencia inmediata del teorema [An 10.34], pues, con la notación de dicho teorema, si $a_n = f_C(n)$, entonces $j_C(k) = \sum_{n=1}^{k} a_n$, y el teorema 4.7 afirma precisamente que existe una constante C que cumple la hipótesis de [An 10.34] con $\sigma_0 = 1 - 1/n$.

A su vez, esto implica inmediatamente que lo mismo vale para $\zeta_K(s)$.

Aunque para probar el teorema anterior nos ha interesado descomponer la función $\zeta_K(s)$ en suma de h series correspondientes a los elementos del grupo de clases de K (precisamente para que apareciera h en la fórmula que hemos obtenido), podemos reducir $\zeta_K(s)$ a una serie "ordinaria" sin necesidad de tal descomposición. Basta definir $f_K(n)$ como el número de ideales de K de norma n, y entonces

$$\zeta_K(s) = \sum_{k=1}^{\infty} \frac{f_K(k)}{k^s}.$$

En términos de [ITAn 7.9], la función $f_K(k)$ es una función aritmética multiplicativa, es decir, que cumple $f_K(k_1k_2) = f_K(k_1)f_K(k_2)$, cuando $(k_1, k_2) = 1$. Esto no es trivial, sino que es consecuencia de la factorización única ideal de K, que garantiza que todo ideal de K de norma k_1k_2 se expresa de forma única como producto de un ideal de norma k_1 por otro de norma k_2. ∎

4.2 Productos de Euler

Ahora demostramos la generalización de la fórmula de Euler citada al comienzo del tema. Ésta presenta la ventaja de que depende sólo de los ideales primos de K. Los resultados más importantes que vamos a obtener se basan en esta igualdad.

Teorema 4.9 *Sea K un cuerpo numérico. Para cada $s > 1$ se cumple*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}},$$

donde $\mathfrak{p}$ recorre los ideales primos de K. La convergencia del producto es absoluta.

Demostración: Para probar que el producto converge absolutamente observamos que

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}} = \prod_{\mathfrak{p}} \left(1 + \frac{1}{\mathrm{N}(\mathfrak{p})^s - 1}\right),$$

y así, por [ITAn 8.5], es suficiente probar que la serie

$$\sum_{\mathfrak{p}} \frac{1}{\mathrm{N}(\mathfrak{p})^s - 1}$$

converge (absolutamente). Ahora bien, la convergencia de esta serie se sigue inmediatamente de la convergencia de $\sum_{\mathfrak{p}} \frac{1}{\mathrm{N}(\mathfrak{p})^s}$, que a su vez es consecuencia de la convergencia de $\sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s}$ (donde ahora $\mathfrak{a}$ recorre todos los ideales no nulos de K). Ahora pasamos a probar la igualdad.

Para cada ideal primo $\mathfrak{p}$ se cumple que

$$\frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}} = \sum_{k=0}^{\infty} \frac{1}{\mathrm{N}(\mathfrak{p})^{ks}}.$$

Sea N un número natural y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ los primos de K de norma menor o igual que N. Multiplicando las series anteriores para estos primos obtenemos

$$\prod_{\mathrm{N}(\mathfrak{p})\leq N} \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}} = \sum_{k_1,\ldots,k_r=0}^{\infty} \frac{1}{\mathrm{N}(\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r})^s} = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{a}$ recorre los ideales no divisibles entre primos de norma mayor que N. Así pues,

$$\left| \prod_{\mathrm{N}(\mathfrak{p})\leq N} \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}} - \zeta_K(s) \right| < \sum_{\mathrm{N}(\mathfrak{a})>N} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

pero esta última expresión tiende a 0 con N, luego se tiene la igualdad buscada. ∎

Según explicábamos, la fórmula anterior es el punto de partida del argumento de Dirichlet que le permitió demostrar el teorema sobre primos en progresiones aritméticas. A su vez, la presencia del factor h en el residuo de la función dseta fue aprovechada por Kummer para caracterizar de forma práctica sus primos regulares. Aún estamos lejos de llegar a estos resultados, pero podemos probar hechos más simples igualmente importantes y que dan idea del papel que representa la fórmula de Euler generalizada en los problemas que nos ocupan.

Por ejemplo, Gauss utilizó la fórmula de Euler para probar que la serie $\sum \frac{1}{p}$ es divergente [TAn 3.27], donde p recorre los números primos, lo que no sólo implica la existencia de infinitos primos, sino que, en cierto sentido, los primos son relativamente abundantes entre los números naturales. El argumento de Gauss se generaliza sin dificultad a cuerpos numéricos arbitrarios. Mas aún, permite probar que existen infinitos primos de norma prima:

Teorema 4.10 *Todo cuerpo numérico tiene infinitos primos de norma prima. De hecho, si $\mathfrak{p}_1$ recorre los primos de norma prima de un cuerpo numérico, entonces*

$$\sum_{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)} = +\infty.$$

Demostración: Si en la fórmula del teorema anterior tomamos logaritmos [ITAn 8.3] nos queda

$$\log \zeta_K(s) = -\sum_{\mathfrak{p}} \log\left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right),$$

y usando el desarrollo de Taylor

$$\log(1+x) = \sum_{m=1}^{\infty} \frac{(-1)^m}{m}\, x^m, \quad \text{para } |x| < 1,$$

obtenemos

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{1}{m\,\mathrm{N}(\mathfrak{p})^{ms}} \tag{4.10}$$

(notemos que todas las series convergen absolutamente). Sea

$$P(s) = \sum_{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s},$$

donde $\mathfrak{p}_1$ recorre los primos de norma prima de K, y sea $G(s)$ la suma de los términos restantes de (4.10), es decir,

$$G(s) = \sum_{\mathfrak{p}_1} \sum_{m=2}^{\infty} \frac{1}{m\,\mathrm{N}(\mathfrak{p}_1)^{ms}} + \sum_{\mathfrak{q}} \sum_{m=1}^{\infty} \frac{1}{m\,\mathrm{N}(\mathfrak{q})^{ms}},$$

donde $\mathfrak{q}$ recorre los primos tales que $\mathrm{N}(\mathfrak{q}) = q^f$ con $f > 1$. Para cada uno de estos primos

$$\sum_{m=1}^{\infty} \frac{1}{m\,\mathrm{N}(\mathfrak{q})^{ms}} < \sum_{m=1}^{\infty} \frac{1}{q^{2ms}} = \frac{1}{q^{2s}-1} \le \frac{2}{q^{2s}}.$$

Por otra parte

$$\sum_{m=2}^{\infty} \frac{1}{m\,\mathrm{N}(\mathfrak{p}_1)^{ms}} < \sum_{m=2}^{\infty} \frac{1}{p^{ms}} = \frac{1}{p^s(p^s-1)} \le \frac{2}{p^{2s}}.$$

Si el grado de K es n, entonces el número de primos que dividen a un mismo primo racional p es a lo sumo n, luego

$$G(s) < 2n \sum_{p} \frac{1}{p^{2s}} < 2n \sum_{m=1}^{\infty} \frac{1}{m^{2s}} = 2n\zeta(2s).$$

Esto implica que la función $G(s)$ está acotada en el intervalo $]1, 2]$. Pero por otra parte $\log \zeta_K(s) = P(s) + G(s)$ y el logaritmo tiende a infinito cuando s tiende a 1, luego la función $P(s)$ no puede estar acotada en $]1, 2]$. Sin embargo, si la serie del enunciado convergiera, como $\mathrm{N}(\mathfrak{p}_1) \le \mathrm{N}(\mathfrak{p}_1)^s$, llegaríamos a que

$$P(s) = \sum_{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} \le \sum_{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)},$$

para todo $s > 1$. ∎

La prueba del teorema de Dirichlet se basa en un argumento similar al anterior, pero hay que separar los primos según la clase de similitud a la que pertenecen, y esto requiere un análisis más fino de la fórmula de Euler, lo cual a su vez requiere considerar lo que ahora se conoce como caracteres de Dirichlet.

4.3 Caracteres de grupos abelianos

Los caracteres de Dirichlet los estudiamos en las secciones [ITAl 9.8] e [ITAn 7.5]. Por comodidad recogemos aquí de forma más concisa los resultados que necesitamos. Empezamos introduciendo un concepto algo más general de carácter de un grupo abeliano, que a su vez es un caso particular del concepto de carácter de un grupo estudiado en el capítulo VI de [TG]:

Definición 4.11 Sea G un grupo abeliano finito. Un *carácter* de G es un homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$.

Observemos que si $g \in G$ tiene orden n, entonces $g^n = 1$, luego cualquier carácter de G cumplirá que $\chi(g)^n = \chi(g^n) = \chi(1) = 1$. Por lo tanto los caracteres de un grupo de orden n sólo toman valores en el grupo de las raíces n-simas de la unidad.

Llamaremos G^* al conjunto de todos los caracteres de G. Es claro que G^* es un grupo abeliano si definimos el producto de dos caracteres χ y ψ como el carácter determinado por $(\chi\psi)(g) = \chi(g)\psi(g)$ para todo $g \in G$.

El elemento neutro de G^* es el llamado *carácter principal* de G, que viene dado por $1(g) = 1$ para todo $g \in G$. El grupo G^* se llama *grupo dual* de G.

Examinemos en primer lugar cómo son los caracteres de los grupos cíclicos. Sea G un grupo cíclico de orden n. Sea g un generador de G y sea $\omega \in \mathbb{C}$ una raíz n-sima primitiva de la unidad.

Entonces los grupos $G = \langle g\rangle$ y $\langle\omega\rangle$ son cíclicos de orden n, luego son isomorfos. Un isomorfismo entre ellos es, por ejemplo, la aplicación $\chi : G \longrightarrow \langle\omega\rangle$ dada por $\chi(g^m) = \omega^m$. Claramente χ es un carácter de G con la propiedad de que $\chi(g) = \omega$.

Para cada $m = 0, \ldots, n-1$ se cumple que $\chi^m(g) = \chi(g)^m = \omega^m$, y como ω es una raíz primitiva de la unidad, los caracteres χ^m son distintos dos a dos.

Por otro lado, si $\psi \in G^*$ se tiene que cumplir que $\psi(g)$ es una raíz n-sima de la unidad, o sea, $\psi(g) = \omega^m = \chi^m(g)$ para un cierto m, y si dos homomorfismos coinciden sobre un generador, han de ser iguales, es decir, se cumple $\psi = \chi^m$ para $m = 0, \ldots, n-1$.

Esto prueba que G^* es un grupo cíclico de orden n generado por χ. En particular tenemos que G^* es isomorfo a G.

Vamos a ver que esto es cierto para todo grupo G aunque no sea cíclico. Para ello nos basaremos en que todo grupo abeliano finito se descompone en producto cartesiano de grupos cíclicos y aplicaremos el teorema siguiente.

Teorema 4.12 *Sean G y H grupos abelianos finitos. Entonces si $\chi \in G^*$ y $\psi \in H^*$, la aplicación $\chi \times \psi : G \times H \longrightarrow \mathbb{C}$ dada por $(\chi \times \psi)(g, h) = \chi(g)\psi(h)$ es un carácter del grupo $G \times H$ y además la aplicación $f : G^* \times H^* \longrightarrow (G \times H)^*$ dada por $f(\chi, \psi) = \chi \times \psi$ es un isomorfismo de grupos.*

La prueba es inmediata. La dejamos a cargo del lector.

Teorema 4.13 *Si G es un grupo abeliano finito, G^* es isomorfo a G.*

DEMOSTRACIÓN: El grupo G se descompone en producto cartesiano de grupos cíclicos y por el teorema anterior G^* es isomorfo al producto cartesiano de los grupos de caracteres de sus factores, que según hemos visto son cíclicos del mismo orden. Así pues G y G^* se descomponen en producto de grupos cíclicos de los mismos órdenes, luego son isomorfos. ∎

Sucede que no existe un isomorfismo canónico entre G y G^*, es decir, un isomorfismo que asigne a cada elemento un carácter construido a partir de él. El isomorfismo depende de la estructura del grupo G.

Por el contrario sí es posible definir un isomorfismo canónico entre G y su bidual G^{**}, concretamente, si llamamos $\epsilon(g) : G^* \longrightarrow \mathbb{C}$ a la aplicación dada por $\epsilon(g)(\chi) = \chi(g)$ para todo $\chi \in G^*$, se ve fácilmente que $\epsilon : G \longrightarrow G^{**}$ es un isomorfismo.

Ahora vamos a relacionar los caracteres de un grupo con los de sus subgrupos.

Teorema 4.14 *Sea G un grupo abeliano finito y H un subgrupo de G. Entonces todo carácter de H se extiende a un carácter de G, y el número de extensiones es igual al índice $|G : H|$.*

DEMOSTRACIÓN: La aplicación $G^* \longrightarrow H^*$ que cada carácter de G lo restringe a H es obviamente un homomorfismo de grupos. Sea N el núcleo de este homomorfismo. Un carácter χ está en N si y sólo si $\chi(h) = 1$ para todo $h \in H$. Esto significa que H está contenido en el núcleo de χ, luego χ induce un carácter $\chi' : G/H \longrightarrow \mathbb{C}$ dado por $\chi'\big([g]\big) = \chi(g)$.

La aplicación $N \longrightarrow (G/H)^*$ dada por $\chi \mapsto \chi'$ es también un homomorfismo de grupos. Es fácil ver que de hecho es un isomorfismo. En efecto, si $\chi' = 1$ entonces obviamente $\chi = 1$, y si tomamos $\psi \in (G/H)^*$, entonces ψ define el carácter $\chi(g) = \psi\big([g]\big)$, que claramente está en N y $\chi' = \psi$.

Consecuentemente $|N| = |(G/H)^*| = |G : H|$ y por lo tanto la imagen de la restricción tiene orden $|G^* : N| = |H|$, por lo que la restricción es un epimorfismo y cada carácter de H^* tiene exactamente $|N| = |G : H|$ antiimágenes, o sea, extensiones. ∎

El teorema siguiente es fundamental a la hora de trabajar con caracteres.

Teorema 4.15 (relaciones de ortogonalidad) *Sea G un grupo abeliano de orden n. Sea $\chi \in G^*$ y $g \in G$. Entonces*

$$\sum_{g\in G} \chi(g) = \begin{cases} n & si\ \chi = 1 \\ 0 & si\ \chi \neq 1 \end{cases} \qquad \sum_{\chi\in G^*} \chi(g) = \begin{cases} n & si\ \chi = 1 \\ 0 & si\ \chi \neq 1 \end{cases}$$

DEMOSTRACIÓN: La primera relación es obvia para $\chi = 1$. Si $\chi \neq 1$ entonces existe un $x \in G$ tal que $\chi(x) \neq 1$. Por consiguiente

$$\chi(x) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(xg) = \sum_{g\in G} \chi(g),$$

(pues cuando g recorre G, xg también recorre G).

Por lo tanto

$$(\chi(x)-1)\sum_{g\in G}\chi(g)=0,$$

de donde

$$\sum_{g\in G}\chi(g)=0.$$

La segunda relación se deduce de la primera aplicándola al grupo G^* y al carácter dado por $\epsilon(g)(\chi)=\chi(g)$. ∎

El nombre de relaciones de ortogonalidad proviene de la interpretación siguiente, que nos va a ser útil en algunas ocasiones. Sea G un grupo abeliano de orden n y sea V el conjunto de todas las aplicaciones de G en $\mathbb{C}$. Claramente V es un espacio vectorial de dimensión n sobre $\mathbb{C}$. Una biyección de G con $\{1,\dots,n\}$ induce de forma natural un isomorfismo entre V y $\mathbb{C}^n$. La base canónica de $\mathbb{C}^n$ se identifica con la base formada por las funciones $\{f_u\}_{u\in G}$ dadas por

$$f_u(t)=\begin{cases}1 & \text{si } t=u\\ 0 & \text{si } t\neq u\end{cases}$$

Definimos el producto en V dado por

$$(f,g)=\frac{1}{n}\sum_{t\in G}f(t)\overline{g(t)},$$

donde la barra indica la conjugación compleja. La aplicación $(\ ,\ )$ es lo que se llama un *producto sesquilineal,* es decir, es lineal en la primera componente y semilineal en la segunda (conserva la suma y además $(f,\alpha g)=\bar{\alpha}(f,g)$).

Ahora, si χ y ψ son dos caracteres de G, el teorema anterior nos da que

$$(\chi,\psi)=\frac{1}{n}\sum_{t\in G}\chi(t)\overline{\psi(t)}=\frac{1}{n}\sum_{t\ nG}(\chi\psi^{-1})(t)=\begin{cases}1 & \text{si } \chi=\psi\\ 0 & \text{si } \chi\neq\psi\end{cases}$$

Esto significa que los caracteres son ortogonales respecto al producto $(\ ,\ )$. De la ortogonalidad se sigue que los caracteres son linealmente independientes, pues si C es una combinación lineal nula de los caracteres, entonces $(C,\chi)=0$, y por otro lado es igual al coeficiente de χ en C. Esto a su vez implica que los caracteres forman una base de V, una base ortonormal.

Caracteres modulares Estudiamos ahora con más detalle los caracteres de los grupos de unidades módulo un número natural m. Conviene considerarlos definidos sobre $\mathbb{Z}$:

Definición 4.16 Un *carácter* módulo m es una aplicación $\chi:\mathbb{Z}\longrightarrow\mathbb{C}$ que cumple las condiciones siguientes:

1. Para todo $a\in\mathbb{Z}$ se cumple $\chi(a)=0$ si y sólo si $(a,m)\neq 1$.
2. Si $a\equiv a'$ (mód m), entonces $\chi(a)=\chi(a')$.
3. Si $a,b\in\mathbb{Z}$, entonces $\chi(ab)=\chi(a)\chi(b)$.

Obviamente todo carácter χ módulo m define un carácter χ' del grupo de unidades U_m mediante $\chi'\big([a]\big) = \chi(a)$ y, recíprocamente, todo carácter de U_m está inducido por un único carácter módulo m. En la práctica identificaremos los caracteres módulo m con los caracteres de U_m. En general, los caracteres módulo m para un módulo cualquiera se llaman *caracteres modulares.* Por ejemplo, es claro que el símbolo de Legendre (x/p) es un carácter módulo p.

Notemos que si χ es un carácter modular $\chi(-1)^2 = \chi\big((-1)^2\big) = \chi(1) = 1$, luego $\chi(-1) = \pm 1$. Si $\chi(-1) = 1$ se dice que χ es un carácter *par,* y si $\chi(-1) = -1$ se dice que χ es *impar.* Los caracteres pares cumplen en general que $\chi(-n) = \chi(n)$, mientras que los impares cumplen $\chi(-n) = -\chi(n)$.

Si $m \mid m'$ entonces todo carácter χ módulo m determina un carácter módulo m' dado por

$$\chi'(a) = \begin{cases} \chi(a) & \text{si } (a, m') = 1, \\ 0 & \text{si } (a, m') \neq 1. \end{cases}$$

Llamaremos a χ' el *carácter inducido* por χ. Observemos que el valor de $\chi'(a)$ depende en realidad del resto de a módulo m y no del resto módulo m'.

En términos de caracteres ordinarios la interpretación es la siguiente: si $m \mid m'$ entonces existe un homomorfismo $f : U_{m'} \longrightarrow U_m$ dado por $f\big([a]\big) = [a]$. Si χ es un carácter de U_m entonces χ' es la composición de χ con f.

En realidad f es un epimorfismo, pues si $(a, m) = 1$, por el teorema chino del resto existe un a' que cumple $a' \equiv a \pmod m$ y $a' \equiv 1 \pmod p$ para todo primo p que divida a m' pero no a m. Entonces $(a', m') = 1$ y $f\big([a']\big) = [a]$. A f lo llamaremos *epimorfismo canónico* de $U_{m'}$ en U_m.

Visto así, es claro que el carácter inducido χ' determina a χ, pues $\chi\big([a]\big)$ se puede calcular como $\chi'\big([b]\big)$, donde $[b]$ es una antiimagen de $[a]$ por f.

También es claro que si $m \mid n \mid r$, χ es un carácter módulo m y χ' es el carácter que induce módulo n, entonces χ y χ' inducen el mismo carácter módulo r. En efecto, tenemos

$$U_r \xrightarrow{f} U_n \xrightarrow{g} U_m \xrightarrow{\chi} \mathbb{C},$$

de modo que $\chi' = g \circ \chi$ y los caracteres que χ y χ' inducen módulo r son $(f \circ g) \circ c$ y $f \circ (g \circ c)$ respectivamente.

Teorema 4.17 *Si un carácter χ módulo m está inducido por un carácter χ_1 módulo m_1 y por un carácter χ_2 módulo m_2 entonces también está inducido por un carácter módulo $d = (m_1, m_2)$.*

Demostración: Sea m' el mínimo común múltiplo de m_1 y m_2. Tenemos la situación siguiente:

$$\begin{array}{ccccc} & & U_{m_1} & \xrightarrow{\chi_1} & \mathbb{C} \\ & \nearrow & & \searrow & \\ U_m \longrightarrow & U_{m'} & & U_d & \\ & \searrow & & \nearrow & \\ & & U_{m_2} & \xrightarrow{\chi_2} & \mathbb{C} \end{array}$$

donde todas las flechas sin nombre son los epimorfismos canónicos.

Por hipótesis χ_1 y χ_2 inducen el mismo carácter χ módulo m, pero los caracteres inducidos por χ_1 y χ_2 módulo m' también inducen el carácter χ, luego han de coincidir. Sea pues χ' el carácter inducido por χ_1 y χ_2 módulo m'.

Sean N_1 y N_2 los núcleos de los epimorfismos canónicos de $U_{m'}$ en U_{m_1} y U_{m_2}, es decir,

$$N_1 = \big\{[a] \in U_{m'} \mid a \equiv 1 \text{ (mód } m_1)\big\} \quad \text{y} \quad N_2 = \big\{[a] \in U_{m'} \mid a \equiv 1 \text{ (mód } m_2)\big\}.$$

Por el teorema de isomorfía sus órdenes son $\phi(m')/\phi(m_1)$ y $\phi(m')/\phi(m_2)$ respectivamente. Es obvio que ambos están contenidos en el núcleo N del epimorfismo canónico de $U_{m'}$ en U_d, que es $N = \big\{[a] \in U_{m'} \mid a \equiv 1 \text{ (mód } d)\big\}$ y tiene orden $\phi(m')/\phi(d)$.

También es claro que $N_1 \cap N_2 = 1$, luego $|N_1N_2| = |N_1||N_2| = |N|$, pues la última igualdad equivale a que $\phi(m')\phi(d) = \phi(m_1)\phi(m_2)$, lo cual se demuestra sin dificultad para toda función aritmética multiplicativa. Como $N_1N_2 \leq N$, de hecho se tiene la igualdad $N = N_1N_2$.

Para todo $[a] \in U_{m'}$ se cumple que $\chi'(a) = \chi_1(a) = \chi_2(a)$, luego $\chi'(a) = 1$ tanto si $[a] \in N_1$ como si $[a] \in N_2$, luego $\chi'(a) = 1$ siempre que $[a] \in N$, es decir, para todas las clases $[a]$ que cumplen $a \equiv 1$ (mód d). De aquí se sigue que si $a \equiv a'$ (mód d) entonces $\chi'(a) = \chi'(a')$.

Dado $[a] \in U_d$ existe un $[a'] \in U_{m'}$ tal que $a' \equiv a$ (mód d) (por la suprayectividad del epimorfismo canónico). Podemos definir $\psi(a) = \chi'(a')$ sin que importe la elección de a' (por lo que acabamos de probar). Claramente ψ es un carácter módulo d que induce a χ' y por lo tanto a χ. ∎

Si un carácter ψ está inducido por un carácter χ, entonces ψ 'contiene menos información' que χ, en el sentido de que ambos coinciden sobre los números primos con el módulo de ψ, mientras que ψ se anula sobre algunos números en los que χ no lo hace. Por eso tiene mucha importancia el concepto siguiente:

Definición 4.18 Un carácter modular es *primitivo* si no está inducido por un carácter de módulo menor.

Del teorema anterior se desprende que todo carácter modular χ está inducido por un único carácter primitivo. En efecto, basta tomar un carácter que lo induzca χ' de módulo mínimo. Entonces χ' no puede estar inducido por ningún carácter de módulo menor porque tal carácter también induciría a χ en contradicción con la elección de χ. La unicidad se debe a que si χ estuviera inducido por dos caracteres primitivos χ_1 y χ_2 de módulos m_1 y m_2, entonces por el teorema anterior ambos serían inducidos por un carácter de módulo $d = (m_1, m_2)$. Por ser primitivos ha de ser $d = m_1 = m_2$, y de aquí que $\chi_1 = \chi_2$.

Dado un carácter χ, llamaremos χ_0 al carácter primitivo que lo induce. El módulo de χ_0 se llama *conductor* de χ.

El teorema siguiente es útil para reconocer caracteres primitivos.

Teorema 4.19 *Un carácter χ módulo m es primitivo si y sólo si para todo divisor propio d de m existe un entero x tal que $(x, m) = 1$, $x \equiv 1$ (mód d) y $\chi(x) \neq 1$.*

DEMOSTRACIÓN: Si χ no es primitivo está inducido por un carácter χ_0 módulo d, donde d es un divisor propio de m. Si $x \equiv 1 \pmod d$ entonces $(x,m) = 1$ y $\chi(x) = \chi_0(x) = \chi_0(1) = 1$.

Recíprocamente, si existe un divisor d de m tal que para todo $x \equiv 1 \pmod d$, $(x,m) = 1$ se cumple $\chi(x) = 1$, entonces si $x \equiv x' \pmod d$ y x, x' son primos con m se cumple $\chi(x) = \chi(x')$. De aquí que podamos definir un carácter ψ módulo d mediante $\psi(a) = \chi(x)$, para cualquier x tal que $(x,m) = 1$ y $x \equiv a \pmod d$. Existe tal x por la suprayectividad del epimorfismo canónico de U_m en U_d. Claramente ψ induce a χ. ∎

El carácter de un cuerpo cuadrático Si $K = \mathbb{Q}(\sqrt{d})$ es un cuerpo cuadrático de discriminante Δ, en [ITAl 9.14] definimos $\chi_K : U_{|\Delta|} \longrightarrow \{1,-1\}$, que es un epimorfismo cuyo núcleo consta de las clases de los primos racionales que se escinden en K. Según hemos visto, podemos identificarlo con un carácter modular

$$\chi_K : \mathbb{Z} \longrightarrow \mathbb{C}^*,$$

al que llamaremos *carácter* del cuerpo cuadrático K. Su propiedad fundamental es que si p es un primo racional, entonces

$$\chi_K(p) = \begin{cases} 1 & \text{si } p \text{ se escinde en } K, \\ 0 & \text{si } p \text{ se ramifica en } K, \\ -1 & \text{si } p \text{ se conserva en } K. \end{cases}$$

El teorema de Dirichlet que probaremos en la sección siguiente implica que esta relación determina completamente a χ_K, pues toda clase de $U_{|\Delta|}$ contiene primos p con los que podemos calcular su imagen según este criterio.

Tras [ITAl 9.15] probamos que $\chi_K(-1) = \Delta/|\Delta|$ o, equivalentemente, que los caracteres de los cuerpos cuadráticos reales son pares, mientras que los de los cuerpos imaginarios son impares.

La construcción dada en [ITAl] de χ_K se basa en la ley de reciprocidad cuadrática expresada en términos del símbolo de Jacobi. En la sección 7.3 veremos otra construcción alternativa más conceptual.

Ahora vamos a dar una caracterización puramente algebraica de los caracteres de los cuerpos cuadráticos. Obviamente, una condición necesaria para que un carácter modular χ sea el carácter de un cuerpo cuadrático es que sólo tome los valores $1, 0, -1$. Supuesto esto, la condición necesaria y suficiente para que χ sea realmente el carácter de un cuerpo cuadrático es que sea primitivo.

Definición 4.20 Un carácter modular χ es un *carácter cuadrático* si y sólo si no es el carácter principal y sólo toma los valores 0 y ± 1.

Teorema 4.21 *Los caracteres de los cuerpos cuadráticos son primitivos. Todo carácter cuadrático primitivo es el carácter de un único cuerpo cuadrático.*

DEMOSTRACIÓN: Sea K un cuerpo cuadrático de discriminante Δ y sea p un divisor primo de Δ. Para probar que χ_K es primitivo basta ver que existe un entero x tal que $(x,\Delta)=1$, $x\equiv 1 \pmod{|\Delta|/p}$ y $\chi(x)=-1$.

Supongamos primero que $p\neq 2$. Sea s un resto no cuadrático módulo p. Como p tiene exponente 1 en Δ, existe un entero x tal que

$$x\equiv s \pmod{p}, \quad x\equiv 1 \pmod{2|\Delta|/p}.$$

Entonces $\chi(x)=(x/p)=(s/p)=-1$.

Supongamos ahora que $p=2$. Sea $K=\mathbb{Q}\big(\sqrt{d}\,\big)$. Si $d\equiv -1 \pmod 4$ entonces $\Delta=4d$ y basta tomar x tal que $x\equiv -1 \pmod 4$, $x\equiv 1 \pmod{|d|}$, con lo que $\chi(x)=-1$. Observemos que de hecho se cumple $x\equiv 1 \pmod{2|d|}$, tal y como se requiere.

Si $d=2d'$, entonces $\Delta=8d'$ y tomamos $x\equiv 5 \pmod 8$, $x\equiv 1 \pmod{|d'|}$. Entonces $x\equiv 1 \pmod{4|d'|}$ y $\chi(x)=-1$.

Investiguemos ahora para qué naturales m existen caracteres cuadráticos primitivos módulo m. Supongamos primero que $m=p^n$, donde p es un primo impar.

Es claro que un carácter cuadrático de U_{p^n} está determinado por su núcleo (toma el valor 1 en el núcleo y -1 en el complementario). Pero el grupo U_{p^n} es cíclico [TG 3.8], luego tiene un único subgrupo de índice 2, luego un único carácter cuadrático. El carácter cuadrático de U_{p^n} ha de coincidir con el carácter inducido por el carácter cuadrático de U_p, luego el único caso en que es primitivo se da cuando $n=1$. En tal caso, el carácter en cuestión es claramente el símbolo de Legendre $\chi(a)=(a/p)$.

Consideremos ahora $m=2^n$. El grupo U_2 es trivial, luego no tiene caracteres cuadráticos. El grupo U_4 es cíclico de orden 2, y tiene un único carácter cuadrático, que será primitivo porque no hay módulos menores que lo puedan inducir. Claramente se trata del carácter del cuerpo $\mathbb{Q}[i]$, es decir:

$$\delta(k)=\begin{cases} 1 & \text{si } k\equiv \ \ 1 \pmod 4,\\ 0 & \text{si } 2\mid k,\\ -1 & \text{si } k\equiv -1 \pmod 4.\end{cases}$$

El grupo U_8 tiene cuatro caracteres, de los cuales uno es el principal (que no es cuadrático), otro es el inducido por el carácter cuadrático módulo 4 (que no es primitivo) y los dos restantes tienen que ser primitivos a falta de módulos menores que los induzcan. Uno de ellos tiene que ser el carácter del cuerpo cuadrático $\mathbb{Q}\big(\sqrt{2}\,\big)$, que es

$$\epsilon(k)=\begin{cases} 1 & \text{si } k\equiv \pm 1 \pmod 8,\\ -1 & \text{si } k\equiv \pm 5 \pmod 8,\\ 0 & \text{si } 2\mid k,\end{cases}$$

y el otro el del cuerpo cuadrático $\mathbb{Q}\big(\sqrt{-2}\,\big)$, que es $\delta\epsilon$.

En general [TG 3.8] el grupo U_{2^n} es el producto de un grupo cíclico de orden 2 por un grupo cíclico de orden 2^{n-2}. Tomemos $a \in U_{2^n}$ de orden 2^{n-2}. Si $H \leq U_{2^n}$ tiene índice índice 2 entonces

$$|H\,\langle a\rangle\,| = \frac{|H|\,|\,\langle a\rangle\,|}{|H \cap \langle a\rangle\,|} \leq 2^{n-1},$$

de donde $|H \cap \langle a\rangle\,| \geq 2^{n-3}$, luego $\langle a^2\rangle \leq H$ y así

$$H/\langle a^2\rangle \leq U_{2^n}/\langle a^2\rangle \cong C_2 \times C_2.$$

Esto da sólo tres posibilidades para H, con lo que U_{2^n} tiene exactamente tres caracteres cuadráticos, que coinciden con los inducidos por los tres caracteres no principales módulo 8.

Supongamos ahora que $m > 1$ es cualquier número natural y χ es un carácter cuadrático primitivo módulo m. Descomponemos m en producto de potencias de primos distintos. Entonces, siempre según [TG 3.8], el grupo U_m factoriza en el producto de los grupos de unidades correspondientes a dichas potencias y, por 4.12, el carácter χ factoriza en producto de caracteres de módulos potencias de primo. Todos los factores son caracteres primitivos, pues basta que uno de ellos pueda inducirse desde un módulo menor para que lo mismo le ocurra a χ. Además, como χ tiene orden 2, todos sus factores tienen orden 2 (el orden de χ es el mínimo común múltiplo de estos órdenes, y ninguno de los factores puede tener orden 1 porque son primitivos).

Todo esto implica que m ha de ser un número natural impar d libre de cuadrados, o bien $4d$ o bien $8d$. Más aún, si $m = d$ o $m = 4d$ hay un único carácter cuadrático primitivo módulo m, a saber, el producto de los únicos caracteres cuadráticos primitivos módulo los primos $p \mid m$ y módulo 4 en su caso (en realidad hemos probado que hay a lo sumo uno, pero esto basta). Si $m = 8d$ hay a lo sumo dos caracteres, pues puede variar el carácter módulo 8.

En todos estos casos existe un cuerpo cuadrático K de discriminante Δ de manera que $m = |\Delta|$. En efecto, si $m = d$ y $d \equiv 1 \pmod 4$, entonces $K = \mathbb{Q}\big(\sqrt{d}\big)$, y si $d \equiv -1 \pmod 4$, entonces $K = \mathbb{Q}\big(\sqrt{-d}\big)$. De hecho hay un único cuerpo K con discriminante $\pm m$, y su carácter es primitivo, luego ciertamente hay un único carácter primitivo módulo m en correspondencia con un único cuerpo cuadrático.

Si $m = 4d$ tomamos $K = \mathbb{Q}\big(\sqrt{-d}\big)$ si $d \equiv 1 \pmod 4$, o bien $K = \mathbb{Q}\big(\sqrt{d}\big)$ si $d \equiv -1 \pmod 4$, con lo que la situación es similar.

Finalmente, si $m = 8d$, los cuerpos $\mathbb{Q}\big(\sqrt{\pm 2d}\big)$ tienen ambos discriminante $\pm m$, pero sus caracteres son distintos, ya que uno es par y el otro impar. Por lo tanto también, hay exactamente dos caracteres cuadráticos primitivos módulo m en correspondencia con dos cuerpos cuadráticos. ∎

Terminamos esta sección con una variante de la fórmula del teorema 3.17 en la que sustituimos la función de Euler por el carácter del cuerpo cuadrático.

Teorema 4.22 *Sea K un cuerpo cuadrático, sea h su número de clases y h_m el número de clases del orden $\mathcal{O}_m$. Sea e_m el índice del grupo de las unidades de $\mathcal{O}_m$ en el grupo de las unidades del orden maximal. Entonces*

$$h_m = \frac{m}{e_m} \prod_{p|m} \left(1 - \frac{\chi_K(p)}{p}\right) h.$$

DEMOSTRACIÓN: Por las propiedades de la función de Euler generalizada,

$$\Phi(m) = \prod_{p|m} \Phi(p^{k_p}),$$

donde k_p es el exponente de p en m.

Si $\chi_K(p) = 1$ entonces $p = \mathfrak{p}_1\mathfrak{p}_2$, con $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p$, luego

$$\Phi(p^{k_p}) = \Phi(\mathfrak{p}_1^{k_p})\Phi(\mathfrak{p}_2^{k_p}) = \left(p^{k_p-1}(p-1)\right)^2.$$

Si $\chi_K(p) = 0$ entonces $p = \mathfrak{p}^2$, con $\mathrm{N}(\mathfrak{p}) = p$.

$$\Phi(p^{k_p}) = \Phi(\mathfrak{p}^{2k_p}) = p^{2k_p-1}(p-1).$$

Si $\chi(p) = -1$ entonces $\mathrm{N}(p) = p^2$ y $\Phi(p^{k_p}) = p^{2k_p-2}(p^2-1)$.

Es fácil comprobar que los tres casos se reúnen en la fórmula

$$\Phi(p^{k_p}) = p^{2k_p-1}(p-1) - p^{2k_p-2}(p-1)\chi_K(p) = \phi(p^{k_p})p^{k_p}\left(1 - \frac{\chi_K(p)}{p}\right).$$

Multiplicando sobre p obtenemos $\Phi(m) = m\,\phi(m) \prod_{p|m} \left(1 - \frac{\chi_K(p)}{p}\right)$. Sustituyendo en la fórmula del teorema 3.17 obtenemos la expresión buscada. ∎

Ejercicio: Usar la fórmula del teorema anterior para calcular el número de clases del orden $\mathcal{O}_3$ de $\mathbb{Q}\left(\sqrt{-2}\right)$.

4.4 Las funciones L de Dirichlet

La relación entre los caracteres modulares y las funciones dseta se establece a través de las funciones L:

Definición 4.23 Si χ es un carácter modular y χ_0 es el carácter primitivo que lo induce, definimos la *función L de Dirichlet* asociada a χ como la función

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s}.$$

Las funciones L son un caso particular de las llamadas series de Dirichlet (secciones [ITAn 8,4], [An 10.6]), que definen funciones holomorfas, si bien aquí sólo nos interesan los valores que toman sobre los números reales. El teorema siguiente recoge las propiedades básicas de las funciones L que se deducen inmediatamente de la definición o de la teoría general sobre series de Dirichlet (véase [ITAn 8.33]):

Teorema 4.24 *Sea χ un carácter modular y sea χ_0 el carácter primitivo que lo induce. Entonces:*

1. *Si $\chi = 1$ es un carácter principal, entonces $L(s,\chi) = \zeta(s)$, luego converge absolutamente para todo $s > 1$ a una función continua y cumple que*

$$\lim_{s\to 1^+} L(s,\chi) = 1.$$

2. *Si $\chi \neq 1$, entonces $L(s,\chi)$ converge para todo $s > 0$ a una función continua, y la convergencia es absoluta para $s > 1$.*

3. *Para todo $s > 1$ se cumple la relación*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi_0(p)}{p^s}},$$

donde p recorre todos primos racionales, y la convergencia del producto es absoluta.

En particular, para un carácter no principal χ, tenemos que

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}. \tag{4.11}$$

La función L de un cuerpo cuadrático La función L asociada al carácter de un cuerpo cuadrático la estudiamos ya en la sección [ITAn 11.2]. Consideramos la fórmula de Euler generalizada para un cuerpo cuadrático K y en ella agrupamos los primos que dividen a un mismo primo racional, es decir,

$$\zeta_K(s) = \prod_p \prod_{\mathfrak{p}|p} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}}.$$

Para cada primo p, el producto asociado puede ser de tres tipos:

$$\frac{1}{1-\frac{1}{p^{2s}}} = \begin{cases} \dfrac{1}{1-\frac{1}{p^s}}\dfrac{1}{1-\frac{1}{p^s}} & \text{si } p \text{ se escinde,} \\ \dfrac{1}{1-\frac{1}{p^s}}\dfrac{1}{1+\frac{1}{p^s}} & \text{si } p \text{ se conserva,} \\ \dfrac{1}{1-\frac{1}{p^s}} & \text{si } p \text{ se ramifica.} \end{cases}$$

Ahora observamos que los tres casos se engloban en la fórmula

$$\frac{1}{1-\frac{1}{p^s}}\frac{1}{1-\frac{\chi_K(p)}{p^s}}.$$

Por lo tanto

$$\zeta_K(s) = \prod_p \frac{1}{1-\frac{1}{p^s}} \prod_p \frac{1}{1-\frac{\chi_K(p)}{p^s}} = \zeta(s)L(s,\chi_K),$$

donde hemos usado la fórmula de Euler para la función dseta de Riemann (la función dseta de $\mathbb{Q}$). Multiplicamos ambos miembros por $(s-1)$ y tomamos límites cuando s tiende a 1. El teorema 4.8 nos da que

$$L(1,\chi_K) = \frac{2^{s+t}\pi^t R}{m\sqrt{|\Delta_K|}}\, h.$$

Puesto que estamos considerando un cuerpo cuadrático, la expresión de $L(1,\chi_K)$ se simplifica considerablemente, aunque es mejor presentar la igualdad anterior como una fórmula para calcular el número de clases:

Teorema 4.25 *Sea K un cuerpo cuadrático de discriminante Δ. Entonces el número de clases de K viene dado por*

$$h = \begin{cases} \dfrac{\sqrt{\Delta}}{2\log\epsilon}\, L(1,\chi_K) & \text{si } \Delta > 0 \text{ y } \epsilon > 1 \text{ es la unidad fundamental de } K, \\ \dfrac{m\sqrt{-\Delta}}{2\pi}\, L(1,\chi_K) & \text{si } \Delta < 0 \text{ y } m \text{ es el número de unidades de } K. \end{cases}$$

En particular vemos que $L(1,\chi_K) \neq 0$. ∎

Ejemplo Veamos ahora una versión débil del teorema de Dirichlet cuya prueba contiene las ideas esenciales de la demostración general. Vamos a probar que en un cuerpo cuadrático K hay infinitos primos que se escinden e infinitos primos que se conservan. El teorema 4.10 ya prueba la existencia de infinitos primos que se escinden, pero no vamos a usar este hecho para no ocultar la idea principal.

Consideramos los dos factores de la función $\zeta_K(s)$, es decir, las funciones $\zeta(s)$ y $L(s,\chi_K)$. El argumento del teorema 4.10 es aplicable a ambas, lo que nos da las ecuaciones

$$\begin{aligned} \log\zeta(s) &= \sum_p \frac{1}{p^s} + G_1(s), \\ \log L(s,\chi_K) &= \sum_p \frac{\chi_K(p)}{p^s} + G_2(s), \end{aligned}$$

donde G_1 y G_2 son funciones acotadas en $]1,2]$. Además es importante que $\log L(s,\chi_K)$ también está acotado (porque $L(1,\chi_K) \neq 0$).

Llamemos A y B a los conjuntos de primos que se escinden y conservan, respectivamente. Entonces A y B cubren todos los primos salvo un número finito de ellos. Si en la primera ecuación separamos los sumandos $1/p$ correspondientes a éstos y los incorporamos a $G_1(s)$, tenemos

$$\begin{aligned} \log\zeta(s) &= \sum_{p\in A} \frac{1}{p^s} + \sum_{p\in B} \frac{1}{p^s} + G_1(s), \\ \log L(s,\chi_K) &= \sum_{p\in A} \frac{1}{p^s} - \sum_{p\in B} \frac{1}{p^s} + G_2(s). \end{aligned}$$

Sumando y restando ambas ecuaciones concluimos ninguna de las dos series está acotada cuando s tiende a 1, y por lo tanto las dos series

$$\sum_{p\in A}\frac{1}{p} \quad \text{y} \quad \sum_{p\in B}\frac{1}{p}$$

son divergentes.

Si llamamos m al valor absoluto del discriminante de K, el carácter χ_K divide las clases de U_m en dos conjuntos. Lo que hemos probado es que hay infinitos primos en cada uno de los dos grupos de clases. Para probar el teorema de Dirichlet hemos de refinar el argumento para distinguir cada una de las clases de U_m. Esto lo lograremos sustituyendo los cuerpos cuadráticos por cuerpos ciclotómicos. ∎

La función dseta de un cuerpo ciclotómico Consideremos ahora el cuerpo ciclotómico $\mathbb{Q}(\omega)$ de orden m. En la fórmula de Euler agrupamos todos los factores que dividen a un mismo primo racional p:

$$\zeta_K(s)=\prod_p\prod_{\mathfrak{p}|p}\frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}}.$$

Si p es un primo y $m=p^im'$, el teorema 2.38 nos da que p tiene $\phi(m')/f_p$ factores primos, donde f_p es el orden de p en $U_{m'}$, y la norma de cada factor es igual a p^{f_p}. Por lo tanto

$$\zeta_K(s)=\prod_p\left(1-\frac{1}{p^{f_ps}}\right)^{-\phi(m')/f_p}. \tag{4.12}$$

Para simplificar esta expresión consideramos

$$\omega_p=\cos(2\pi/f_p)+i\,\mathrm{sen}(2\pi/f_p),$$

es decir, una raíz f_p-ésima primitiva de la unidad. Entonces

$$x^{f_p}-1=\prod_{k=0}^{f_p-1}(x-\omega_p^k),$$

de donde, sustituyendo $x=p^s$ y dividiendo entre p^{f_ps},

$$1-\frac{1}{p^{f_ps}}=\prod_{k=0}^{f_p-1}\left(1-\frac{\omega_p^k}{p^s}\right). \tag{4.13}$$

Entonces el producto

$$\prod_{k=0}^{f_p-1}\left(1-\frac{\omega_p^k}{p^s}\right)^{\phi(m')/f_p}=\left(1-\frac{1}{p^{f_ps}}\right)^{\phi(m')/f_p}$$

tiene $\phi(m)$ factores, de los cuales $\phi(m)/f_p$ son iguales a $1-\omega_p^k/p^s$ para cada k, pero el número total de factores es independiente de p.

Si χ es un carácter módulo m', puesto que $p^{f_p} \equiv 1 \pmod{m'}$, se cumple que

$$\chi(p)^{f_p} = \chi(p^{f_p}) = \chi(1) = 1,$$

luego $\chi(p) = \omega_p^k$, para un cierto k.

Recíprocamente, si partimos de un cierto ω_p^k, existe un único carácter ψ del subgrupo cíclico generado por $[p]$ en $U_{m'}$ que cumple $\psi\big([p]\big) = \omega_p^k$ y, por el teorema 4.14, este carácter se extiende a exactamente $\phi(m')/f_p$ caracteres distintos de $U_{m'}$, o sea, existen exactamente $\phi(m')/f_p$ caracteres módulo m' que cumplen $\chi(p) = \omega_p^k$ o, dicho de otro modo, si χ recorre todos los caracteres módulo m', entonces $\chi(p)$ recorre $\phi(m')/f_p$ veces cada raíz de la unidad.

Llamemos χ_0 al carácter primitivo que induce a un carácter dado χ. De nuevo por 4.14, cada carácter módulo m' induce $\phi(p^i)$ caracteres módulo m, luego, cuando χ recorre los caracteres módulo m cuyo conductor divide a m', la expresión $\chi_0(p)$ recorre $\phi(m)/f_p$ veces cada raíz f_p-ésima de la unidad. Los restantes caracteres módulo m tienen conductor múltiplo de p, luego para ellos $\chi_0(p) = 0$. Estos cálculos prueban que

$$\left(1 - \frac{1}{p^{f_p s}}\right)^{\phi(m)/f_p} = \prod_\chi \left(1 - \frac{\chi_0(p)}{p^s}\right),$$

donde χ recorre los caracteres módulo m. Así la fórmula (4.12) se convierte en

$$\zeta_K(s) = \prod_p \prod_\chi \frac{1}{1 - \frac{\chi_0(p)}{p^s}}.$$

Finalmente invertimos el orden de los productos, con lo que obtenemos el teorema siguiente:

Teorema 4.26 *Sea K el cuerpo ciclotómico de orden m. Entonces*

$$\zeta_K(s) = \prod_\chi L(s,\chi), \quad \textit{para todo } s > 1,$$

donde χ recorre los caracteres módulo m.

Como consecuencia obtenemos una expresión analítica para el número de clases de un cuerpo ciclotómico:

Teorema 4.27 *Sea K el cuerpo ciclotómico de orden $2m$, sea Δ su discriminante y R su regulador. Entonces, el número de clases de K es*

$$h = \frac{2m\sqrt{|\Delta|}}{(2\pi)^{\phi(2m)/2}\, R} \prod_{\chi \neq 1} L(1,\chi),$$

donde χ recorre los caracteres no principales módulo m.

DEMOSTRACIÓN: Notemos que si m es impar, entonces el cuerpo ciclotómico de orden m es el mismo que el de orden $2m$. Así, el cuerpo ciclotómico de orden $2m$ tiene $2m$ raíces de la unidad. Por 4.26 tenemos que

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \lim_{s\to 1^+}(s-1)\zeta(s)\prod_{\chi\neq 1} L(s,\chi) = \prod_{\chi\neq 1} L(1,\chi).$$

Ahora basta aplicar el teorema 4.8. ∎

Una consecuencia inmediata es que si χ es un carácter modular no principal, entonces $L(1,\chi)\neq 0$. Esto es exactamente lo que necesitamos para probar el teorema de Dirichlet:

Teorema 4.28 (Dirichlet) *Si m y n son números naturales primos entre sí, entonces la sucesión $mk+n$, para $k=1,2,3,\ldots$ contiene infinitos primos.*

DEMOSTRACIÓN: Consideremos el logaritmo complejo que extiende al real alrededor de 1. Su desarrollo de Taylor es

$$\log(1+z) = \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}z^n \quad \text{para } |z|<1.$$

Sea ahora un carácter modular primitivo χ. Entonces

$$-\log\left(1-\frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\infty}\frac{\chi(p)^n}{np^{ns}}$$

para todo primo p y todo $s>1$. Por [ITAn 8.3], la convergencia absoluta del producto del teorema 4.24 implica que la serie

$$\log L(s,\chi) = \sum_p\sum_{n=1}^{\infty}\frac{\chi(p)^n}{np^{ns}}$$

converge a un logaritmo del producto para $s>1$. Observemos que $\log L(s,1)$ es simplemente la composición de la función real $L(s,1)$ con la función logaritmo real. Descomponemos

$$\log L(s,\chi) = \sum_p\frac{\chi(p)}{p^s} + R(s,\chi),$$

donde

$$R(s,\chi) = \sum_p\sum_{n=2}^{\infty}\frac{\chi(p)^n}{np^{ns}}.$$

Ahora observamos que

$$|R(s,\chi)| \leq \sum_p\sum_{n=2}^{\infty}\frac{1}{p^{ns}} = \sum_p\frac{1}{p^s(p^s-1)} \leq \sum_p\frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty}\frac{1}{n(n-1)} = 1.$$

Si hacemos variar C en U_m tenemos

$$\log L(s,\chi) = \sum_C \chi(C) \sum_{p\in C} \frac{1}{p^s} + R(s,\chi).$$

Podemos ver estas ecuaciones como un sistema de $\phi(m)$ ecuaciones lineales en el que las incógnitas son las series sobre los primos de las clases de U_m. Vamos a despejar una de ellas, digamos la correspondiente a la clase A, para lo cual multiplicamos por $\chi(A^{-1})$ y sumamos todas las ecuaciones:

$$\sum_\chi \chi(A^{-1}) \log L(s,\chi) = \sum_C \Big(\sum_\chi \chi(CA^{-1})\Big) \sum_{p\in C} \frac{1}{p^s} + R_A(s),$$

donde

$$|R_A(s)| = \Big|\sum_\chi \chi(A^{-1}R(s,\chi))\Big| \le \sum_\chi |R(s,\chi)| \le \phi(m), \quad \text{para todo } s > 1.$$

Por las relaciones de ortogonalidad de los caracteres la ecuación se reduce a

$$\sum_\chi \chi(A^{-1}) \log L(s,\chi) = \phi(m) \sum_{p\in A} \frac{1}{p^s} + R_A(s). \tag{4.14}$$

Ahora tomaremos límites cuando $s \to 1^+$. Debemos detenernos en el comportamiento de $\log L(s,\chi)$. Puesto que $L(1,\chi)$ (para χ no principal) es un número complejo no nulo, por [IC 7.29] en un entorno de $L(1,\chi)$ existe una determinación continua del logaritmo. Componiéndola con $L(s,\chi)$ obtenemos una función continua $\log' L(s,\chi)$ definida en un entorno de 1, digamos $]1-\epsilon, 1+\epsilon[$. La función $\log L(s,\chi) - \log' L(s,\chi)$ es continua en el intervalo $]1, 1+\epsilon[$ y sólo puede tomar los valores $2k\pi i$, para k entero, luego por conexión k ha de ser constante en $]1, 1+\epsilon[$ y consecuentemente existe

$$\lim_{s\to 1^+} \log L(s,\chi) = \log' L(1,\chi) + 2k\pi i.$$

Agrupamos todos los sumandos acotados en (4.14) junto con $R_A(s)$ y queda

$$\log L(s,1) = \phi(m) \sum_{p\in A} \frac{1}{p^s} + T_A(s),$$

donde $T_A(s)$ es una función acotada en un entorno de 1.

Por otro lado $L(s,1)$ tiende a infinito cuando s tiende a 1, luego lo mismo le ocurre a $\log L(s,1)$. Esto implica que la función $\sum_{p\in A} \frac{1}{p^s}$ no está acotada en un entorno de 1, lo que sólo es posible si tiene infinitos sumandos. Más aún, es claro que esto sólo es posible si

$$\sum_{p\in A} \frac{1}{p} = +\infty.$$

Como A es una clase cualquiera de U_m, digamos $A = \{km+n \mid k \in \mathbb{Z}\}$, con $(m,n) = 1$, esto prueba el teorema. ∎

Nota La prueba precedente consiste simplemente en una manipulación de series y logaritmos, en la que el único ingrediente no trivial ha sido el hecho de que $L(1,\chi) \neq 0$ cuando χ no es principal. Esto lo hemos probado factorizando la función dseta del cuerpo ciclotómico, pero también es posible obtener una prueba mediante técnicas de la teoría de funciones holomorfas que no requieren apenas álgebra. Así lo hacemos en [TAN 3.31]. La prueba del teorema de Dirichlet que presentamos allí a continuación es esencialmente la misma que hemos dado aquí. ∎

Enteros ciclotómicos reales Por último estudiamos la función dseta de los cuerpos $K^* = K \cap \mathbb{R}$, donde K es el cuerpo ciclotómico de orden p. Razonamos exactamente igual que como hemos hecho para el cuerpo ciclotómico. En primer lugar agrupamos los factores del producto de Euler correspondientes a un mismo primo racional:

$$\zeta_{K^*}(s) = \prod_q \prod_{\mathfrak{q}|q} \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{q})^s}}.$$

Ahora tenemos en cuenta el teorema 2.46, que nos da el número de divisores primos de cada primo racional y la norma de cada uno. Separamos el factor correspondiente a p, para el que tenemos un único ideal de norma p. Para los primos restantes q, hay $(p-1)/2f_q$ ideales de norma q^{f_q}, donde f^q es $\mathrm{o}_p(q)$ o bien $\mathrm{o}_p(q)/2$. Según esto

$$\zeta_{K^*}(s) = \frac{1}{1-\frac{1}{p^s}} \prod_{q\neq p} \left(1-\frac{1}{q^{f_q}}\right)^{-\frac{p-1}{2f_q}}.$$

Ahora tomamos $\omega_q = \cos(2\pi/f_q) + i\,\mathrm{sen}(2\pi/f_q)$ y usamos la fórmula (4.13), en virtud de la cual podemos afirmar

$$\left(1-\frac{1}{q^{f_q}}\right)^{\frac{p-1}{2f_q}} = \prod_{k=0}^{f_q-1} \left(1-\frac{\omega_q^k}{q^s}\right)^{\frac{p-1}{2f_q}}.$$

El número total de factores es $(p-1)/2$ y por otra parte hay $p-1$ caracteres módulo p, de los cuales la mitad son pares y la mitad impares. Veamos que

$$\prod_{k=0}^{f_q-1} \left(1-\frac{\omega_q^k}{q^s}\right)^{\frac{p-1}{2f_q}} = \prod_{\chi(1)=1} \left(1-\frac{\chi(q)}{q^s}\right).$$

Supongamos primero que $\mathrm{o}_p(q)$ es impar. Entonces $[-1]$ no pertenece al subgrupo generado por $[q]$ en U_p. Dado un k, existe un único carácter ψ de $\langle[q]\rangle$ tal que $\psi\big([q]\big) = \omega_q^k$, que se extiende exactamente a dos caracteres del grupo $\langle[q],[-1]\rangle$, de los cuales uno será par y el otro impar (si ambos coincidieran sobre $[-1]$ coincidirían en todo el grupo).

El carácter par se extiende a $(p-1)/2f_q$ caracteres pares módulo p. Por lo tanto cuando χ varía entre los caracteres pares módulo p tenemos que $\chi(q)$ toma $(p-1)/2f_q$ veces el valor ω^k para cada k entre 0 y f_q-1. De aquí se sigue lo pedido en este caso.

Supongamos ahora que $\mathrm{o}_p(q)$ es par y por tanto $f_q = \mathrm{o}_p(q)/2$. En este caso, el carácter ψ de $\langle [q]\rangle$ que cumple $\psi\big([q]\big) = \omega_q^k$, cumple también que

$$\psi\big([-1]\big) = \psi\big([q]^{f_q}\big) = (\omega_p^k)^{f_q} = 1^k = 1.$$

Por lo tanto ψ se extiende a $(p-1)/2f_q$ caracteres módulo p, todos ellos pares, y de nuevo cuando χ varía entre los caracteres pares módulo p se cumple que $\chi(q)$ toma $(p-1)/2f_q$ veces el valor ω_q^p para cada k entre 0 y $f_q - 1$.

Con esto tenemos que

$$\zeta_{K^*}(s) = \frac{1}{1-\frac{1}{p^s}} \prod_{q\neq p} \prod_{\chi(1)=1} \frac{1}{1-\frac{\chi(q)}{q^s}}.$$

Ahora observamos que el producto de la derecha para $q = p$ coincide con el factor de la izquierda, luego en realidad

$$\zeta_{K^*}(s) = \prod_q \prod_{\chi(1)=1} \frac{1}{1-\frac{\chi(q)}{q^s}} = \prod_{\chi(1)=1} L(s,\chi).$$

Recogemos esto y su consecuencia inmediata sobre el número de clases en el teorema siguiente:

Teorema 4.29 *Sea K el cuerpo ciclotómico de orden p y $K^* = K \cap \mathbb{R}$. Sea $m = (p-1)/2$ el grado de K^* y R^* su regulador. Entonces*

1. *La función dseta de K^* factoriza como*

$$\zeta_{K^*}(s) = \prod_{\chi(1)=1} L(s,\chi),$$

   donde χ recorre los caracteres pares módulo p.

2. *El número de clases h^* de K^* viene dado por*

$$h^* = \frac{\sqrt{p}^{\,m-1}}{2^{m-1}R^*} \prod_{\substack{\chi(1)=1\\ \chi\neq 1}} L(1,\chi).$$

4.5 El cálculo de $L(1,\chi)$

Una vez probado el teorema de Dirichlet, nuestro interés por las funciones L se centra ahora en encontrar una expresión lo más simple posible para los números $L(1,\chi)$, de modo que las fórmulas de los teoremas 4.25 y 4.27 nos permitan calcular lo más eficientemente posible el número de clases de los cuerpos cuadráticos y ciclotómicos. Ciertamente, las expresiones que vamos a obtener para las funciones L serán completamente satisfactorias, pero en la fórmula de 4.27 interviene también el regulador del cuerpo, cuyo cálculo involucra determinar un sistema fundamental de unidades, y esto no es sencillo.

La única expresión con que contamos para calcular $L(1,\chi)$ es (4.11), pues el producto de Euler diverge en 1. Aunque no es el camino que vamos a seguir, es interesante notar que en el caso de caracteres cuadráticos las series $L(1,\chi)$ pueden calcularse directamente por técnicas elementales en cada caso particular.

Ejemplo Sea $K = \mathbb{Q}(\sqrt{5}\,)$. Vamos a calcular directamente

$$L(1,\chi_K) = \frac{1}{1} - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \frac{1}{11} - \frac{1}{12} - \frac{1}{13} + \frac{1}{14} + \cdots \tag{4.15}$$

Para ello observamos que

$$L(1,\chi_K) = \int_0^1 (1 - x - x^2 + x^3 + x^5 - x^6 - x^7 + x^8 + \cdots)\,dx. \tag{4.16}$$

En efecto: para justificar el cambio de la integral y la suma podemos agrupar los términos en la forma

$$\int_0^1 \big((1 - x - x^2) + (x^3 + x^5 - x^6 - x^7) + (x^8 + x^{10} - x^{11} - x^{12}) + \cdots\big)\,dx,$$

con lo que podemos aplicar el teorema de la convergencia monótona de Lebesgue, según el cual la integral coincide con

$$\left(\frac{1}{1} - \frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8}\right) + \left(\frac{1}{9} + \frac{1}{11} - \frac{1}{12} - \frac{1}{13}\right) + \cdots$$

Las sumas parciales de esta serie son una subsucesión de las de (4.15), luego el límite es el mismo. De (4.16) obtenemos

$$\begin{aligned} L(1,\chi_K) &= \int_0^1 (1 - x - x^2 + x^3)(1 + x^5 + x^{10} + \cdots)\,dx \\ &= \int_0^1 (1 - x - x^2 + x^3)\frac{1}{1 - x^5}\,dx \\ &= \int_0^1 \frac{1 - x^2}{x^4 + x^3 + x^2 + x + 1}\,dx \end{aligned}$$

Esta integral puede calcularse por las técnicas habituales. No obstante, el truco siguiente proporciona un camino más rápido: hacemos $y = x + 1/x$, con lo que $dy = (1 - 1/x^2)\,dx$.

$$\begin{aligned} L(1,\chi_K) &= -\int_0^1 \frac{1 - 1/x^2}{x^2 + x + 1 + 1/x + 1/x^2}\,dx = \int_2^{+\infty} \frac{dy}{y^2 + y - 1} \\ &= \int_{5/2}^{+\infty} \frac{dz}{z^2 - 5/4} = \left[-\frac{1}{\sqrt{5}} \log \frac{z + \sqrt{5}/2}{z - \sqrt{5}/2}\right]_{5/2}^{+\infty} \\ &= \frac{2}{\sqrt{5}} \log \frac{1 + \sqrt{5}}{2}. \end{aligned}$$

El teorema 4.25 nos da que el número de clases de $\mathbb{Q}(\sqrt{5}\,)$ es $h = 1$. ∎

Este método puede emplearse para evaluar cualquier función L asociada a un cuerpo cuadrático. Si en lugar de calcular formalmente la integral usamos un ordenador que la aproxime con precisión suficiente, el resultado es una forma muy rápida de calcular números de clases (los errores de cálculo se cancelan al aplicar el teorema 4.25 porque sabemos que el resultado ha de ser entero).[3]

Ejercicio: Sea $K = \mathbb{Q}(i)$. Probar que $L(1, \chi_K) = \pi/4$. Se trata de la famosa fórmula de Leibniz para el cálculo de π.

Ejemplo Vamos a calcular el número de clases del cuerpo ciclotómico octavo mediante la fórmula del teorema 4.27.

Sea ω una raíz octava primitiva de la unidad. Tras el teorema 1.21 vimos que el anillo de enteros de $\mathbb{Q}(\omega)$ es $\mathbb{Z}[\omega]$, y que su discriminante es 256. Más delicado es el cálculo del regulador. Vamos a probar que $\mathbb{Q}(\omega)$ tiene una unidad fundamental real, con lo que ésta será la unidad fundamental de $\mathbb{Q}(\omega) \cap \mathbb{R} = \mathbb{Q}\big(\sqrt{2}\,\big)$, es decir, $\epsilon = 1 + \sqrt{2}$.

En efecto, sea ϵ una unidad fundamental. Si σ es cualquier automorfismo del cuerpo, entonces $\sigma(\epsilon/\bar{\epsilon}) = \sigma(\epsilon)/\overline{\sigma(\epsilon)}$, luego $|\sigma(\epsilon/\bar{\epsilon})| = 1$. Esto significa que $\epsilon/\bar{\epsilon}$ está en el núcleo de la representación logarítmica, luego es una raíz de la unidad, $\epsilon = \omega^{2k+i}\bar{\epsilon}$, donde $i = 0, 1$. Si cambiamos ϵ por $\omega^k\epsilon$ tenemos una unidad fundamental que cumple $\epsilon = \omega^i\bar{\epsilon}$. Basta probar que $i = 1$ es imposible.

Sea $\epsilon = a + b\omega + c\omega^2 + d\omega^3$. Entonces igualdad $\epsilon = \omega\bar{\epsilon}$ nos da que

$$a + b\omega + c\omega^2 + d\omega^3 = \omega(a - d\omega - c\omega^2 - b\omega^3) = b + a\omega - d\omega^2 - c\omega^3,$$

de donde $a = b$ y $c = -d$, luego $\epsilon = a(1 + \omega) + c(\omega^2 - \omega^3)$.

Ahora bien, $\pi = \omega - 1$ es primo (tiene norma 2) y $\omega \equiv 1$ (mód π), por lo que $\epsilon \equiv 0$ (mód π), lo cual es imposible porque es una unidad.

Según lo dicho, esto prueba que una unidad fundamental es $\epsilon = 1 + \sqrt{2}$, luego el regulador es

$$R = \log\big(1 + \sqrt{2}\,\big)^2 = 2\log\big(1 + \sqrt{2}\,\big).$$

Por último, los caracteres no principales módulo 8 son los tres caracteres cuadráticos δ, ϵ, $\delta\epsilon$ definidos en la prueba del teorema 4.21, y que se corresponden respectivamente con los cuerpos $\mathbb{Q}[i]$, $\mathbb{Q}\big(\sqrt{2}\,\big)$ y $\mathbb{Q}\big(\sqrt{-2}\,\big)$. Según 4.27, el número de clases que buscamos es

$$h = \frac{8 \cdot 16}{(2\pi)^2 \cdot 2\log\big(1 + \sqrt{2}\,\big)} L(1, \delta)L(1, \epsilon)L(1, \delta\epsilon).$$

[3]Puede probarse en general que el cambio de la serie y la integral siempre es lícito, aunque este punto es delicado: una forma de probarlo es integrar entre 0 y $t < 1$, donde el cambio es posible por la convergencia uniforme, y después aplicar la continuidad de la integral en un miembro y el teorema de Fatou en el otro, según el cual si una serie de potencias tiene radio de convergencia 1, sus coeficientes tienden a 0 y converge a una función holomorfa definida en 1, entonces la serie converge también en 1 a dicha función.

Por otra parte, la fórmula del teorema 4.25 nos permite calcular fácilmente

$$L(1,\delta)=\frac{\pi}{4},\quad L(1,\epsilon)=\frac{\log\bigl(1+\sqrt{2}\bigr)}{\sqrt{2}},\quad L(1,\delta\epsilon)=\frac{\pi}{\sqrt{8}}.$$

Concluimos que $h=1$. ∎

Ejercicio: Llegar al mismo resultado por las técnicas del capítulo anterior.

Veamos ahora una técnica mucho más eficiente para el cálculo de $L(1,\chi)$. Dado un carácter modular no principal χ, que podemos suponer primitivo, en primer lugar agrupamos los sumandos de la serie $L(s,\chi)$ según las clases de U_m, donde m es el conductor de χ. Trabajamos con $s>1$, de modo que la serie converge absolutamente y las reordenaciones son lícitas:

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\sum_C\chi(C)\sum_{n=1}^{\infty}\frac{a_n}{n^s},$$

donde

$$a_n=\begin{cases}1 & \text{si } n\in C,\\ 0 & \text{si } n\notin C.\end{cases}$$

Ahora consideramos el carácter ψ de $\mathbb{Z}/mZ$ determinado por $\psi(1)=\omega$, donde $\omega=\cos(2\pi/m)+i\,\mathrm{sen}(2\pi/m)$, y notamos que por las relaciones de ortogonalidad

$$(\psi^r,1)=\frac{1}{m}\sum_{k=0}^{m-1}\omega^{rk}=\begin{cases}1 & \text{si } m\mid r,\\ 0 & \text{si } m\nmid r.\end{cases}$$

Por consiguiente

$$a_n=\frac{1}{m}\sum_{k=0}^{m-1}\omega^{(r-n)k},$$

donde $r\in C$ y, volviendo a la función L,

$$L(s,\chi)=\sum_r\chi(r)\sum_{n=1}^{\infty}\frac{1}{m}\sum_{k=0}^{m-1}\omega^{(r-n)k}\frac{1}{n^s}=\frac{1}{m}\sum_{k=0}^{m-1}\Bigl(\sum_r\chi(r)\omega^{rk}\Bigr)\sum_{n=1}^{\infty}\frac{\omega^{-nk}}{n^s},$$

donde r varía en un conjunto completo de representantes de las clases de U_m.

Con esto nos hemos encontrado un concepto famoso en la teoría de números:

Definición 4.30 [ITAl 9.21] Sea m un número natural y a un número entero, sea χ un carácter módulo m y $\omega=\cos(2\pi/m)+i\,\mathrm{sen}(2\pi/m)$. Se llama *suma de Gauss* de χ a la expresión

$$G_a(\chi)=\sum_r\chi(r)\omega^{ar},$$

donde r recorre un conjunto completo de representantes de las clases de U_m. Escribiremos $G(\chi)$ en lugar de $G_1(\chi)$.

En términos de las sumas de Gauss, la expresión que hemos obtenido para $L(1,\chi)$ es

$$L(s,\chi) = \frac{1}{m}\sum_{k=1}^{m-1} G_k(\chi)\sum_{n=1}^{\infty}\frac{\omega^{-nk}}{n^s}. \tag{4.17}$$

Dedicaremos la sección siguiente al estudio de estas sumas. Por ejemplo, allí probaremos de nuevo (teorema 4.35) el teorema [ITAl 9.22], según el cual, si χ es un carácter primitivo, se cumple la relación:

$$G_a(\chi) = \overline{\chi(a)}G(\chi).$$

Sabiendo esto, la fórmula (4.17) se simplifica:

$$L(s,\chi) = \frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\sum_{n=1}^{\infty}\frac{\omega^{-nk}}{n^s},$$

donde ahora k recorre un conjunto de representantes de las clases de U_m (siempre suponiendo que χ es primitivo o, equivalentemente, que m es el conductor del carácter χ).

El paso siguiente es notar que, por las relaciones de ortogonalidad, las sumas $\sum_{n=1}^{N}\omega^{-nk}$ se anulan cada vez que $m \mid N$, y en consecuencia toman un número finito de valores. Podemos aplicar el teorema [ITAn 8.31] y concluir que la serie

$$\sum_{n=1}^{\infty}\frac{\omega^{-nk}}{n^s}$$

converge para $s > 0$ a una función continua. Ahora hacemos que s tienda a 1 y resulta que

$$L(1,\chi) = \frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\sum_{n=1}^{\infty}\frac{\omega^{-nk}}{n}.$$

La última serie se simplifica si tenemos presente que, por [ITAn 2.33], la serie de Taylor

$$-\log(1-z) = \sum_{n=1}^{\infty}\frac{z^n}{n}$$

converge en realidad siempre que $|z| \le 1$, excepto en $z = 1$. Con ello tenemos probado el teorema siguiente:

Teorema 4.31 *Sea m un número natural, sea χ un carácter primitivo módulo m no principal y sea $\omega = cos(2\pi/m) + i\,\mathrm{sen}(2\pi/m)$. Entonces*

$$L(1,\chi) = -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log(1-\omega^{-k}),$$

donde k recorre un conjunto de representantes de las clases de U_m y el logaritmo tiene parte imaginaria en $]-\pi/2,\pi/2[$.

Lo importante de esta fórmula es que la serie infinita ha sido absorbida por el logaritmo. Pronto veremos que podemos reducir los logaritmos complejos a logaritmos reales, pero quizá sea clarificador considerar un caso concreto antes de seguir:

Ejemplo Vamos a aplicar el teorema anterior al carácter ϵ del cuerpo $\mathbb{Q}\big(\sqrt{2}\big)$.

Para calcular la suma de Gauss consideramos la raíz octava de la unidad

$$\omega = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i.$$

Claramente

$$G(\epsilon) = \omega - \omega^3 - \omega^5 + \omega^7 = \sqrt{2} + \sqrt{2} = \sqrt{8}.$$

Por consiguiente

$$\begin{aligned} L(1,\epsilon) &= \frac{-1}{\sqrt{8}}\left(\log(1-\omega^{-1}) - \log(1-\omega^{-3}) - \log(1-\omega^{-5}) + \log(1-\omega^{-7})\right) \\ &= \frac{-1}{\sqrt{8}} \log \frac{|1-\omega\ |^2}{|1-\omega^3|^2} = \frac{1}{\sqrt{8}} \log \frac{2+\sqrt{2}}{2-\sqrt{2}} \\ &= \frac{1}{\sqrt{8}} \log\big(1+\sqrt{2}\big)^2 = \frac{\log\big(1+\sqrt{2}\big)}{\sqrt{2}}. \end{aligned}$$

■

Ejercicio: Comprobar que las sumas $G_a(\epsilon)$ cumplen el teorema 4.35.

Ejercicio: Calcular las sumas de Gauss correspondientes al carácter $\delta\epsilon$.

Los cálculos del ejemplo y los ejercicios anteriores se pueden seguir fácilmente en general. En las condiciones del teorema 4.31 tenemos que

$$1-\omega^{-k} = 2\,\mathrm{sen}\,\frac{k\pi}{m}\left(\cos\left(\frac{\pi}{2}-\frac{k\pi}{m}\right) + i\,\mathrm{sen}\left(\frac{\pi}{2}-\frac{k\pi}{m}\right)\right).$$

(basta desarrollar el miembro derecho usando la trigonometría).

Si $0 < k < m$ entonces $-\pi/2 < \pi/2 - k\pi/m < \pi/2$, luego

$$\log(1-\omega^{-k}) = \log|1-\omega^{-k}| + i\pi\left(\frac{1}{2}-\frac{k}{m}\right),$$

(recordemos que tomamos el logaritmo con parte imaginaria entre $-\pi/2$ y $\pi/2$). Como $1-\omega^{-k}$ y $1-\omega^k$ son conjugados, se cumple también

$$\log(1-\omega^{k}) = \log|1-\omega^{k}| - i\pi\left(\frac{1}{2}-\frac{k}{m}\right).$$

Supongamos ahora que el carácter χ es par. Según el teorema 4.31

$$\begin{aligned} L(1,\chi) &= -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log(1-\omega^{-k}), \\ L(1,\chi) &= -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log(1-\omega^{k}). \end{aligned}$$

Sumando ambas expresiones

$$\begin{aligned} 2L(1,\chi) &= -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\big(\log(1-\omega^{-k})+\log(1-\omega^k)\big)\\ &= -2\,\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log|1-\omega^k|\\ &= -2\,\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log 2\operatorname{sen}\frac{k\pi}{m}. \end{aligned}$$

Si el carácter χ es impar obtenemos

$$\begin{aligned} 2L(1,\chi) &= -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\big(\log(1-\omega^{-k})-\log(1-\omega^k)\big)\\ &= -2\,\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\,i\pi\left(\frac{1}{2}-\frac{k}{m}\right). \end{aligned}$$

Finalmente, por las relaciones de ortogonalidad se cumple $\sum_k \overline{\chi(k)} = 0$, lo que nos permite simplificar ambas fórmulas. Recogemos su forma definitiva en el teorema siguiente:

Teorema 4.32 *Sea χ un carácter primitivo módulo m.*

1. *Si χ es par entonces*

$$L(1,\chi) = -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log\operatorname{sen}\frac{k\pi}{m}.$$

2. *Si χ es impar*

$$L(1,\chi) = \frac{i\pi G(\chi)}{m^2}\sum_k \overline{\chi(k)}\,k.$$

En ambos casos k recorre los números $0<k<m$ primos con m.

En el caso de los caracteres cuadráticos, estas fórmulas se simplifican aún más gracias al resultado siguiente:

Teorema 4.33 *Sea χ un carácter cuadrático primitivo módulo m. Entonces:*

$$G(\chi) = \begin{cases} \sqrt{m} & \text{si } \chi(-1) = 1,\\ i\sqrt{m} & \text{si } \chi(-1) = -1. \end{cases}$$

Está demostrado en [ITAl 9.24], pero en la sección siguiente daremos una prueba distinta. Si en las fórmulas del teorema 4.25 evaluamos la función L mediante las fórmulas del teorema 4.32 y en éstas evaluamos la suma de Gauss, el resultado es [ITAn 11.6]:

Teorema 4.34 *Sea K un cuerpo cuadrático de discriminante Δ y sea h su número de clases. Entonces*

1. *Si K es real y $\epsilon > 1$ es su unidad fundamental,*

$$h = -\frac{1}{\log \epsilon} \sum_k \chi_K(k) \log \operatorname{sen} \frac{k\pi}{\Delta},$$

   donde k recorre los números naturales $0 < k < \Delta/2$, $(k, \Delta) = 1$.

2. *Si K es imaginario y $\Delta < -4$,*

$$h = -\frac{1}{|\Delta|} \sum_k \chi(k) k,$$

   donde k recorre los números $0 < k < |\Delta|$, $(k, \Delta) = 1$.

Observemos que en el caso real k debería variar entre 0 y Δ y faltaría un factor $1/2$, pero claramente el sumando correspondiente a $\Delta - k$ es igual al sumando correspondiente a k, luego podemos reducir a la mitad el número de sumandos y simplificar el 2. En el caso imaginario suponemos $\Delta < -4$ para evitar distinguir el número de unidades. Los casos exceptuados tienen $h = 1$.

Nota En el caso real podemos definir

$$\theta = \frac{\prod_b \operatorname{sen}(\pi b/\Delta)}{\prod_a \operatorname{sen}(\pi a/\Delta)},$$

donde a y b recorren los números entre 0 y $\Delta/2$ primos con Δ y tales que $\chi_K(a) = 1$, $\chi_K(b) = -1$. Entonces la fórmula del teorema anterior equivale a que

$$h = \frac{1}{\log \epsilon} \log \theta,$$

de donde $\theta = e^{h \log \epsilon} = \epsilon^h$. En particular θ es una unidad de K.

La fórmula $\theta = \epsilon^h$ tiene interés entre otros motivos porque no existe ninguna demostración puramente aritmética de este hecho. Ni siquiera se conoce una prueba elemental de que $\theta > 0$. ∎

4.6 Sumas de Gauss

Terminamos el capítulo estudiando la suma de Gauss asociada a un carácter χ módulo m, que hemos definido como

$$G(\chi) = \sum_r \chi(r) \omega^r,$$

donde r recorre un conjunto completo de representantes de las clases de U_m y $\omega = e^{2\pi i/m}$.

En primer lugar recordamos la prueba de [ITAn 9.22], que es uno de los resultados que ya hemos empleado sobre ellas:

Teorema 4.35 *Sea χ un carácter primitivo. Entonces*

$$G_a(\chi) = \overline{\chi(a)}G(\chi),$$

donde la barra denota la conjugación compleja.

DEMOSTRACIÓN: Sea $d = (a, m)$ y sea $m = td$. Entonces ω^a es una raíz t-ésima primitiva de la unidad y $\omega^{au} = \omega^a$ siempre que $u \equiv 1 \pmod{t}$. Si $d \neq 1$ entonces t es un divisor propio de m y por el teorema 4.19 existe un entero u tal que $u \equiv 1 \pmod{t}$, $(u, m) = 1$ y $\chi(u) \neq 1$.

Cuando r recorre un conjunto completo de representantes de las clases de U_m lo mismo le sucede a ur, luego

$$G_a(\chi) = \sum_r \chi(ur)\omega^{aur} = \chi(u)\sum_r \chi(r)\omega^{ar} = \chi(u)G_a(\chi).$$

Puesto que $\chi(u) \neq 1$ ha de ser $G_a(\chi) = 0$. Así mismo, $\overline{\chi(a)} = 0$, luego se cumple la igualdad.

Por el contrario, si $(a, m) = 1$, cuando r recorre un conjunto completo de representantes de las clases de U_m lo mismo le sucede a ar, luego

$$\chi(a)G_a(\chi) = \sum_r \chi(ar)\omega^{ar} = \sum_r \chi(r)\omega^r = G(\chi),$$

y multiplicando por $\overline{\chi(a)} = \chi(a)^{-1}$ obtenemos la igualdad. ∎

Ejemplo Consideremos el carácter χ módulo 5 dado por

$$\chi(1) = 1, \quad \chi(2) = i, \quad \chi(3) = -i, \quad \chi(4) = -1.$$

Vamos a calcular $G(\chi)$. Sea

$$\omega = \cos\frac{2\pi}{5} + i\,\operatorname{sen}\frac{2\pi}{5}.$$

Las relaciones $(\omega + \omega^4) + (\omega^2 + \omega^3) = (\omega + \omega^4)(\omega^2 + \omega^3) = -1$ implican que $\omega + \omega^4$ y $\omega^2 + \omega^3$ son las raíces del polinomio $x^2 + x - 1$, de donde

$$\omega + \omega^4 = \frac{-1 + \sqrt{5}}{2}, \quad \omega^2 + \omega^3 = \frac{-1 - \sqrt{5}}{2}.$$

De aquí que ω y ω^4 son raíces del polinomio $x^2 - \frac{-1+\sqrt{5}}{2}\,x + 1$, mientras que ω^2 y ω^3 lo son de $x^2 - \frac{-1-\sqrt{5}}{2}\,x + 1$, por lo que

$$\omega = \frac{-1 + \sqrt{5}}{4} + \sqrt{\frac{5 + \sqrt{5}}{8}}, \qquad \omega^2 = \frac{-1 - \sqrt{5}}{4} + \sqrt{\frac{5 - \sqrt{5}}{8}},$$

$$\omega^3 = \frac{-1 - \sqrt{5}}{4} + \sqrt{\frac{5 - \sqrt{5}}{8}}, \qquad \omega^4 = \frac{-1 + \sqrt{5}}{4} + \sqrt{\frac{5 + \sqrt{5}}{8}}.$$

Ahora un simple cálculo nos da que

$$G(\chi) = \omega + i\omega^2 - i\omega^3 - \omega^4 = -\sqrt{\frac{5-\sqrt{5}}{2}} + \sqrt{\frac{5+\sqrt{5}}{2}}\, i.$$

Observemos que $|G(\chi)| = \sqrt{5}$. ∎

Ejercicio: Sea χ el carácter definido por el símbolo de Legendre $\chi(n) = (n/5)$. Probar que $G(\chi) = \sqrt{5}$.

Ejercicio: Usar el ejemplo anterior para sumar las series

$$1 - \frac{1}{4} + \frac{1}{6} - \frac{1}{9} + \frac{1}{11} - \frac{1}{14} + \frac{1}{16} - \frac{1}{19} + \cdots$$

y

$$\frac{1}{2} - \frac{1}{3} + \frac{1}{7} - \frac{1}{8} + \frac{1}{12} - \frac{1}{13} + \frac{1}{17} - \frac{1}{18} + \cdots$$

Aunque el valor de una suma de Gauss no es predecible en general, su módulo está perfectamente determinado por el teorema [ITAl 9.23], que volvemos a demostrar aquí con una prueba que contiene una interesante interpretación algebraica de las sumas de Gauss:

Teorema 4.36 *Todo carácter primitivo χ módulo m cumple $|G(\chi)| = \sqrt{m}$.*

Demostración: Consideremos el conjunto V formado por todas las aplicaciones $f : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{C}$. Según explicamos en el capítulo anterior, V es un espacio vectorial sobre $\mathbb{C}$ que tiene como base a los caracteres de $\mathbb{Z}/m\mathbb{Z}$. Para cada $k \in \mathbb{Z}/m\mathbb{Z}$ sea f_k el carácter determinado por $f_k(1) = \omega^{-k}$. Las aplicaciones $f_1, \ldots, f_m$ son todos los caracteres de $\mathbb{Z}/m\mathbb{Z}$. Es importante notar que no son caracteres modulares, pues éstos son los caracteres del grupo multiplicativo U_m, mientras que aquéllos son los caracteres del grupo aditivo $\mathbb{Z}/m\mathbb{Z}$.

También sabemos que en V está definido el producto sesquilineal

$$(f, g) = \frac{1}{m} \sum_{k=1}^{m} f(k)\overline{g(k)},$$

respecto al cual los caracteres f_k son una base ortonormal. Puesto que $\chi \in V$, podemos expresarlo como combinación lineal

$$\chi = \sum_{k=1}^{m} \alpha_k f_k, \qquad \alpha_k \in \mathbb{C}.$$

Los coeficientes se pueden calcular como

$$\alpha_a = (\chi, f_a) = \frac{1}{m} \sum_{k=1}^{m} \chi(k)\omega^{ak} = \frac{G_a(\chi)}{m}.$$

Vemos, pues, que salvo el factor $(1/m)$ las sumas de Gauss de χ son las coordenadas del carácter multiplicativo χ en la base de los caracteres aditivos módulo m. Explícitamente:

$$\chi = \frac{G(\chi)}{m}\sum_{k=1}^{m}\overline{\chi(k)}f_k,$$

Usando la sesquilinealidad del producto y la ortonormalidad de la base obtenemos

$$(\chi,\chi) = \frac{|G(\chi)|^2}{m^2}\sum_{k,\,r=1}^{m}\overline{\chi(k)}\chi(r)(f_k,f_r) = \frac{|G(\chi)|^2}{m^2}\phi(m),$$

pero por otra parte, usando la definición del producto sesquilineal,

$$(\chi,\chi) = \frac{1}{m}\sum_{k=1}^{m}\chi(k)\overline{\chi(k)} = \frac{1}{m}\sum_{k=1}^{m}|\chi(k)|^2 = \frac{1}{m}\,\phi(m).$$

Comparando los dos resultados concluimos que $|G(\chi)|^2 = m$. ∎

Sumas de Gauss y la ley de reciprocidad Para entender cómo llegó Gauss al estudio de las sumas que llevan su nombre hemos de remontarnos al trabajo de Euler en torno a la ley de reciprocidad cuadrática. Euler la descubrió empíricamente, pero sólo pudo probar la primera ley suplementaria y parte de la segunda. Respecto a la primera se basó en [ITAl 5.8], que afirma que si p es un primo impar, entonces

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}.$$

Haciendo $n = -1$ se obtiene que $(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$, y como ambos miembros son ± 1 y $1 \not\equiv -1 \pmod{p}$, la congruencia ha de ser de hecho una igualdad, lo que prueba la primera ley suplementaria.

Respecto a la segunda ley suplementaria, Euler sólo probó que si p es un primo $p \equiv 1 \pmod{8}$, entonces 2 es un resto cuadrático módulo p. Para ello se basó en la existencia de una raíz primitiva de la unidad módulo p (de lo cual sólo tenía una evidencia empírica y fue demostrado más tarde por Gauss). Tomemos una raíz primitiva u módulo p y sea $\omega = [u^{(p-1)/8}]$. Entonces $\omega^8 = 1$, y 8 es el menor exponente que cumple esto, luego $\omega^4 = -1$, $\omega^2 = -\omega^{-2}$ y así $\omega^2 + \omega^{-2} = 0$. Esto implica que

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

como queríamos probar.

Si $p \not\equiv 1 \pmod{8}$ el argumento anterior es aparentemente inviable, pero en realidad la idea puede aprovecharse si contamos con el álgebra moderna, concretamente con la teoría de cuerpos finitos. En esencia, lo que nos impide empezar el razonamiento es que necesitamos una raíz octava de la unidad en $\mathbb{Z}/p\mathbb{Z}$ y puede que no la haya, pero podemos obtenerla en un cuerpo mayor.

Sea p un primo impar cualquiera y sea ω una raíz octava primitiva de la unidad en una extensión K de $\mathbb{Z}/p\mathbb{Z}$. Si llamamos $\gamma = \omega + \omega^{-1}$, el mismo argumento de antes prueba que $\gamma^2 = 2$, pero esto no significa que 2 sea un resto cuadrático módulo p, ya que γ no tiene por qué estar en $\mathbb{Z}/p\mathbb{Z}$ (no hay que olvidar que al fin y al cabo 2 no tiene por qué ser un resto cuadrático).

Tenemos que $(2/p) = 1$ si y sólo si $\gamma \in \mathbb{Z}/p\mathbb{Z}$ (pues en K no puede haber más raíces cuadradas de 2 que $\pm\gamma$, pero los elementos de $\mathbb{Z}/p\mathbb{Z}$ son exactamente los elementos de K que cumplen $x^p = x$. Calculamos, pues, $\gamma^p = \omega^p + \omega^{-p}$. Para ello observamos que, como $\omega^8 = 1$, se cumple

$$\begin{aligned} &\omega^p + \omega^{-p} = \omega + \omega^{-1} = \gamma && \text{si } p \equiv \pm 1 \text{ (mód 8)},\\ &\omega^p + \omega^{-p} = \omega^3 + \omega^{-3} = -(\omega + \omega^{-1}) = -\gamma && \text{si } p \equiv \pm 3 \text{ (mód 8)}. \end{aligned}$$

O sea, $\gamma^p = (-1)^{(p^2-1)/8}\gamma$, con lo que $\gamma^p = \gamma$ si y sólo si $(-1)^{(p2-1)/8} = 1$ y, según lo visto, esto equivale a que $(2/p) = (-1)^{(p^2-1)/8}$. ∎

Como ya hemos advertido, esta técnica es demasiado moderna, pero Gauss encontró un argumento intermedio que proporciona una prueba ligeramente más larga, pero que da cuenta del caso general, al contrario de lo que ocurre con el argumento de Euler. No es difícil imaginar de qué se trata: en lugar de considerar una raíz octava de la unidad en un cuerpo de característica p, Gauss tomó una raíz octava de la unidad en $\mathbb{C}$ y consideró congruencias módulo p. Sea

$$\omega = cos(2\pi/8) + i\,\mathrm{sen}(2\pi/8) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\,i.$$

Entonces es claro que $\gamma = \omega + \omega^{-1} = \sqrt{2}$, y en particular $\gamma^2 = 2$. Conviene observar que aunque la prueba de $\gamma^2 = 2$ es ahora inmediata, podríamos haber obtenido esto mismo por medios puramente algebraicos sin más que repetir el argumento anterior (esto indica que no se trata de una mera casualidad y hace plausible que el argumento pueda ser generalizado).

Ahora tomamos congruencias en $\mathbb{Z}[\omega]$ y usamos [ITAl 5.8]:

$$\gamma^{p-1} = (\gamma^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \text{ (mód } p).$$

De aquí que $\gamma^p \equiv (2/p)\gamma$ (mód p). Como el cociente módulo p es un anillo de característica p tenemos que $\gamma^p = (\omega+\omega^{-1})^p \equiv \omega^p+\omega^{-p}$ (mód p) y podemos concluir como antes que

$$(-1)^{(p^2-1)/8}\gamma \equiv \left(\frac{2}{p}\right)\gamma \text{ (mód } p).$$

Multiplicamos por γ ambos miembros y queda

$$(-1)^{(p^2-1)/8}\,2 \equiv \left(\frac{2}{p}\right) 2 \text{ (mód } p),$$

luego $(-1)^{(p^2-1)/8} \equiv (2/p)$ (mód p), y así $(-1)^{(p^2-1)/8} = (2/p)$. ∎

La clave de la prueba ha sido la fórmula $(\gamma+\gamma^{-1})^2=2$. Gauss se planteó el encontrar relaciones similares para primos impares con las que obtener una prueba más simple de la ley de reciprocidad cuadrática en toda su generalidad. Así es como llegó a las sumas de Gauss y, más exactamente, al siguiente caso particular:

Definición 4.37 Sea p un primo impar. Llamaremos *sumas cuadráticas de Gauss* módulo p a las sumas

$$G_a(p)=\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\omega^{ar},$$

donde $\omega=\cos 2\pi/p+i\,\mathrm{sen}\,2\pi/p$.

Claramente $G_a(p)=G_a(\chi)$, donde χ es el carácter módulo p determinado por el símbolo de Legendre. En particular llamaremos $G(p)=G_1(p)$.

El teorema 4.35 implica que si $p\nmid a$ entonces $G_a(p)=(a/p)G(p)$.

En realidad Gauss definió

$$G_a(p)=\sum_{x=0}^{p-1}\omega^{ax^2}. \tag{4.18}$$

Es fácil ver que se trata de una definición equivalente: podemos descomponer $G_a(p)=R-N$, donde R y N son las sumas de las potencias de ω^a con exponentes respectivamente restos y no restos cuadráticos. Entonces $1+N+R=0$, pues se trata de la suma de todas las potencias de ω (repetidas varias veces si a no es primo con m), y en consecuencia $R-N=2R+1$, que coincide con (4.18), pues x^2 recorre dos veces los restos cuadráticos más el cero. De hecho, Gauss estudió las sumas $G_a(b)$ definidas de este modo para todo b, no necesariamente primo, pero la sumas asociadas a primos son las únicas relevantes en el problema que nos ocupa.

Como consecuencia del teorema 4.36 sabemos que $|G(p)|=\sqrt{p}$, pero Gauss probó algo más fuerte:

Teorema 4.38 *Sea p un primo impar. Entonces*

$$G(p)^2=(-1)^{(p-1)/2}p.$$

Demostración: Aplicando la conjugación compleja a la definición de $G(p)$ resulta

$$\overline{G(p)}=\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\omega^{-r}=G_{-1}(p)=\left(\frac{-1}{p}\right)G(p).$$

Así pues, si $(-1/p)=1$ tenemos que $G(p)=\overline{G(p)}$, luego $G(p)\in\mathbb{R}$ y $G(p)^2>0$. Por el teorema 4.36 ha de ser $G(p)^2=p$.

Por el contrario, si $(-1/p) = -1$. entonces $G(p) = -\overline{G(p)}$, lo que implica que $G(p)$ es imaginario puro, y así $G(p)^2 < 0$. El teorema 4.36 nos da que $G(p)^2 = -p$. En resumen queda que $G(p)^2 = (-1/p)p = (-1)^{(p-1)/2}p$. ∎

Ejercicio: Usar el teorema 4.31 para probar en general que si χ es un carácter cuadrático primitivo módulo m, entonces $G(\chi)^2 = \chi(-1)\, m$.

Veamos ahora cómo la relación que proporciona el teorema anterior permite probar fácilmente la ley de reciprocidad.

Sean p y q primos impares distintos. Sea $p' = (-1)^{(p-1)/2}p$. Consideraremos congruencias módulo q en el anillo ciclotómico p-ésimo y usamos el teorema de Euler [Al 12.9]:

$$G(p)^{q-1} = (G(p)^2)^{(q-1)/2} = p'^{(q-1)/2} \equiv \left(\frac{p'}{q}\right) \pmod{q}.$$

Por otra parte, si consideramos la definición de $G(p)$ tenemos

$$G(p)^q = \left(\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\omega^r\right)^q \equiv \sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\omega^{qr} = G_q(p) = \left(\frac{q}{p}\right)G(p) \pmod{q}.$$

Combinando las dos congruencias queda

$$\left(\frac{p'}{q}\right)G(p) \equiv G(p)^q \equiv \left(\frac{q}{p}\right)G(p) \pmod{q}.$$

Multiplicamos por $G(p)$ y así $(p'/q)p' \equiv (q/p)p' \pmod{q}$, de donde concluimos

$$\left(\frac{q}{p}\right) = \left(\frac{p'}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) = (-1)^{(q-1)(p-1)/4}\left(\frac{p}{q}\right).$$

∎

Al igual que ocurre con el caso del 2, la demostración se simplifica si usamos cuerpos finitos en lugar de congruencias. El argumento está expuesto en la sección [ITAl 7.3].

El signo de las sumas cuadráticas Una de las características de Gauss era su extremada meticulosidad. En sus trabajos no dejaba de discutir el menor aspecto de cualquier problema, y así, a pesar de que la fórmula del teorema 4.38 era suficiente para demostrar la ley de reciprocidad cuadrática, quedaba planteado el problema de calcular el valor exacto de $G(p)$. Por 4.38 podemos afirmar que

$$G(p) = \begin{cases} \pm\sqrt{p} & \text{si } p \equiv \ \ 1 \pmod 4, \\ \pm\sqrt{p}\, i & \text{si } p \equiv -1 \pmod 4. \end{cases} \tag{4.19}$$

La cuestión era determinar el signo. El caso es que los cálculos explícitos muestran que siempre aparece el signo positivo, pero Gauss tardó tres años

en encontrar una prueba de ello. Con sus propias palabras: "*... este estudio, que a primera vista parece muy sencillo, conduce directamente a dificultades inesperadas, y su desarrollo, que ha llegado hasta aquí sin obstáculos, requiere métodos completamente nuevos.*". El teorema siguiente es [ITAl 7.10], pero aquí vamos a dar otra prueba, debida a Schur:

Teorema 4.39 *Sea p un primo impar. Entonces*

$$G(p) = \begin{cases} \sqrt{p} & \text{si } p \equiv \ \ 1 \text{ (mód 4)}, \\ \sqrt{p}\,i & \text{si } p \equiv -1 \text{ (mód 4)}. \end{cases}$$

Demostración: Sea $\omega = \cos(2\pi/p) + i\,\mathrm{sen}(2\pi/p)$. Consideremos la matriz $A = (\omega^{xy})$, donde x, y varían entre 0 y $p-1$. La expresión (4.18) para la suma $G(p)$ prueba que ésta es la traza de la matriz A. Sean $\lambda_1, \ldots, \lambda_p$ los valores propios de A. Entonces $G(p) = \lambda_1 + \cdots + \lambda_p$, y todo se reduce a calcular los valores propios de A. Calculamos ahora A^2. El coeficiente x, y de A^2 es

$$\sum_{t=1}^{p} \omega^{t(x+y)} = \begin{cases} p & \text{si } x+y \equiv 0 \text{ (mód } p), \\ 0 & \text{si } x+y \not\equiv 0 \text{ (mód } p). \end{cases}$$

Es obvio que los valores propios de A^2 son los cuadrados de los valores propios de A, pero el polinomio característico de A^2 es fácil de calcular:

$$\mathrm{pol\,car} A^2 = (t-p)^{(p+1)/2}(t+p)^{(p-1)/2}.$$

(Esbozamos el cálculo: el determinante de $tI - A^2$ puede desarrollarse por la primera fila, de modo que queda $(t-p)|B|$, donde B es una matriz de orden $p-1$ que tiene a t en toda la diagonal principal y $-p$ en la otra diagonal. Desarrollando este determinante por la primera fila queda $(t-p)(t|C| + p|D|)$, y los dos determinantes pueden desarrollarse por la última fila para llegar a

$$(t-p)(t^2|B'| - p^2|B'|) = (t-p)(t^2-p^2)|B'|,$$

donde B' es como B pero con dos filas y columnas menos).

Así pues, los valores propios de A^2 son $(p+1)/2$ números iguales a p y $(p-1)/2$ números iguales a $-p$, luego cada valor propio de A es de la forma $\pm\sqrt{p}$ o $\pm i\sqrt{p}$. Más aún, si llamamos a, b, c, d a las multiplicidades de los valores propios $\sqrt{p}$, $-\sqrt{p}$, $i\sqrt{p}$, $-i\sqrt{p}$, ha de cumplirse

$$a + b = (p+1)/2, \qquad c + d = (p-1)/2. \tag{4.20}$$

Además tenemos

$$G(p) = \big(a - b + (c-d)i\big)\sqrt{p}. \tag{4.21}$$

Comparando con (4.19) concluimos que

$$\begin{aligned} &a - b = \pm 1, \quad c = d \qquad \text{cuando } p \equiv \ \ 1 \text{ (mód 4)}, \\ &c - d = \pm 1, \quad a = b \qquad \text{cuando } p \equiv -1 \text{ (mód 4)}. \end{aligned} \tag{4.22}$$

Calculemos por otro lado el determinante de A. Para ello observamos que

$$|A^2| = (-1)^{p(p-1)/2}p^p,$$

luego $|A| = \pm i^{p(p-1)/2}p^{p/2}$. Nos falta determinar el signo. Para ello observamos que $|A|$ es un determinante de Vandermonde. Sea $\eta = \cos(\pi/p) + i\,\mathrm{sen}(\pi/p)$. Entonces

$$\begin{aligned}|A| &= \prod_{0\le r<s\le p-1}(\omega^s - \omega^r) = \prod_{0\le r<s\le p-1}(\eta^{2s} - \eta^{2r})\\ &= \prod_{0\le r<s\le p-1}\eta^{r+s}(\eta^{s-r} - \eta^{-(s-r)}) \prod_{0\le r<s\le p-1}\eta^{r+s}\left(2i\,\mathrm{sen}\,\frac{(s-r)\pi}{p}\right).\end{aligned}$$

El primer producto del último término es η elevado a [4]

$$\sum_{0\le r<s\le p-1}(r+s) = \sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s) = \sum_{r=1}^{p-1}\left(r^2 + \frac{r(r-1)}{2}\right) = 2p\left(\frac{p-1}{2}\right)^2.$$

Como el orden de η es $2p$, dicho producto es 1 y queda

$$|A| = i^{p(p-1)/2}2^{p(p-1)/2}\prod_{0\le r<s\le p-1}\mathrm{sen}\,\frac{(s-r)\pi}{p},$$

donde todos los senos son positivos. Comparando las dos expresiones que hemos obtenido llegamos a que $|A| = i^{p(p-1)/2}p^{p/2}$.

Por otro lado $|A|$ es el producto de los valores propios de A, o sea,

$$|A| = (-1)^b i^c (-i)^d p^{p/2} = i^{2b+c-d}p^{p/2}.$$

De aquí obtenemos que $2b + c - d \equiv p(p-1)/2 \pmod 4$. Uniendo esto a (4.20) y (4.22) resulta que si $p \equiv 1 \pmod 4$ entonces $c = d$, y

$$a - b = a + b - 2b = \frac{p+1}{2} - 2b \equiv \frac{p+1}{2} - \frac{p-1}{2} \equiv p \equiv 1 \pmod 4,$$

luego $a - b = 1$, y si $p \equiv -1 \pmod 4$ entonces $a = b$ y

$$c - d \equiv -(p-1)/2 - 2b = -\frac{p-1}{2} - \frac{p+1}{2} \equiv -p \equiv 1 \pmod 4,$$

luego $c - d = 1$. En ambos casos (4.21) nos da el resultado. ∎

Con esto hemos probado un caso particular del teorema 4.33, que tenemos pendiente de probar. Para pasar al caso general nos basaremos en el resultado siguiente, que es [ITAl 9.25]:

[4] Usamos aquí la fórmula de Bernoulli: $\sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1)}{6}$. Está probada al final de la sección [ITAn 6.5], aunque puede probarse fácilmente por inducción.

Teorema 4.40 *Sean $\chi_1, \ldots, \chi_n$ caracteres módulo $m_1, \ldots, m_n$ respectivamente, donde los números m_i son primos entre sí dos a dos. Sea $\chi = \chi_1 \times \cdots \times \chi_n$ y $m = m_1 \cdots m_n$. Entonces*

$$G_a(\chi) = G_a(\chi_1) \cdots G_a(\chi_n)\, \chi_1(m/m_1) \cdots \chi_n(m/m_n).$$

DEMOSTRACIÓN: Basta probarlo cuando $n = 2$ y el caso general se sigue por inducción. Concretamente hemos de ver que

$$G_a(\chi_1 \times \chi_2) = G_a(\chi_1) G_a(\chi_2)\, \chi_1(m_2)\chi_2(m_1).$$

Para ello observamos que la aplicación $U_{m_1} \times U_{m_2} \longrightarrow U_m$ definida como $\big([u],[v]\big) \mapsto [um_2 + vm_1]$ es biyectiva (aunque no es un homomorfismo). Además, si $\omega = \cos(2\pi/m) + i\,\mathrm{sen}(2\pi/m)$, entonces

$$\omega^{m_2} = \cos(2\pi/m_1) + i\,\mathrm{sen}(2\pi/m_1) \quad \text{y} \quad \omega^{m_1} = \cos(2\pi/m_2) + i\,\mathrm{sen}(2\pi/m_2).$$

Por lo tanto,

$$G_a(\chi_1)G_a(\chi_2)\,\chi_1(m_2)\chi_2(m_1) = \Big(\sum_{u,v} \chi_1(u)\chi_2(v)\omega^{m_2au+m_1av}\Big)\chi_1(m_2)\chi_2(m_1)$$

$$= \sum_{u,v} \chi_1(m_2u)\chi_2(m_1v)\omega^{a(m_2u+m_1v)}$$

$$= \sum_{u,v} \chi_1(m_2u+m_1v)\chi_2(m_2u+m_1v)\omega^{a(m_2u+m_1v)} = \sum_r \chi_1(r)\chi_2(r)\omega^{ar}$$

$$= \sum_r \chi(r)\omega^{ar} = G_a(\chi),$$

donde u varía en U_{m_1}, v varía en U_{m_2} y r en U_m. ∎

DEMOSTRACIÓN (de 4.33): Por el teorema 4.21 sabemos que m ha de ser el discriminante de un cuerpo cuadrático, es decir, que existe un número impar r libre de cuadrados de modo que $m = r$, $m = 4r$ o $m = 8r$. Digamos que $r = p_1 \cdots p_s$. Llamemos $r_i = r/p_i$.

Sea χ_i el único carácter cuadrático módulo p_i, es decir, el determinado por $\chi_i(a) = (a/p_i)$ para $(a, p_i) = 1$. Sea $\psi = \chi_1 \times \cdots \times \chi_s$. Por el teorema anterior

$$G(\psi) = G(\chi_1) \cdots G(\chi_s)\, \chi_1(r/p_1) \cdots \chi_s(r/p_s).$$

Sea t el número de primos p_i congruentes con -1 módulo 4. Entonces el teorema 4.39 nos da que

$$\begin{aligned} G(\psi) &= i^t \sqrt{r} \left(\frac{r_1}{p_1}\right) \cdots \left(\frac{r_s}{p_s}\right) = i^t \sqrt{r} \prod_{i \neq j} \left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right) \\ &= i^t \sqrt{r}\,(-1)^{t(t-1)/2} = i^{t^2}\sqrt{r} = \begin{cases} \sqrt{r} & \text{si } t \text{ es par} \\ i\sqrt{r} & \text{si } t \text{ es impar} \end{cases} \end{aligned}$$

Por otra parte, $\chi_i(-1) = -1$ si y sólo si $p_i \equiv -1$ (mód 4), luego $\psi(-1) = 1$ si y sólo si t es par. Esto prueba el teorema cuando $m = r$.

Supongamos ahora que $m = 4r$. Entonces $\chi = \delta \times \psi$, donde δ es el carácter primitivo módulo 4. Es fácil comprobar que $G(\delta) = i - (-i) = 2i$. Por el teorema anterior $G(\chi) = G(\delta)G(\psi)\delta(r)\psi(4) = 2iG(\psi)\delta(r)$.

Si $r \equiv 1$ (mód 4) entonces t es par y $\delta(r) = 1$, luego $G(\chi) = 2i\sqrt{r} = i\sqrt{m}$, y por otra parte $\chi(-1) = \delta(-1)\psi(-1) = -1$, luego se cumple el teorema.

Si $r \equiv -1$ (mód 4) entonces t es impar y $\delta(r) = -1$, de donde llegamos a que $G(\chi) = 2i \cdot i\sqrt{r}(-1) = \sqrt{m}$, y por otra parte $\chi(-1) = \delta(-1)\psi(-1) = 1$. Esto completa la prueba para el caso $m = 4r$.

En el caso $m = 8r$ se razona igualmente, con la única diferencia de que ahora tenemos que considerar dos posibilidades para el carácter módulo 8, a saber, los caracteres ϵ y $\delta\epsilon$. ∎

El número de clases de un cuerpo cuadrático imaginario Terminamos mostrando que la fórmula que proporciona el teorema 4.34 para el caso de cuerpos cuadráticos imaginarios puede simplificarse más todavía. Sea $m = |\Delta|$ y supongamos primero que m es par.

Observemos que $\chi_K(k + m/2) = -\chi_K(k)$. En efecto, con la notación de la prueba del teorema 4.33 es evidente que $\psi(k+m/2) = \psi(k)$. Si $m = 4r$ entonces $\chi_K = \delta \times \psi$, y es claro que $\delta(k+2) = -\delta(k)$. Si $m = 8r$ entonces $\chi_K = \epsilon \times \psi$ o bien $\chi_K = \delta\epsilon \times \psi$, y también es claro que $\epsilon(k+4) = -\epsilon(k)$, de donde se sigue la relación.

En las sumas siguientes k recorre sólo los números primos con m en los rangos indicados:

$$\begin{aligned} hm &= -\sum_k \chi_K(k)k = -\sum_{k=1}^{m/2} \chi_K(k)k - \sum_{k=1}^{m/2} \chi_K\left(k+\frac{m}{2}\right)\left(k+\frac{m}{2}\right) = \\ &= -\sum_{k=1}^{m/2} \chi_K(k)k + \sum_{k=1}^{m/2} \chi_K(k)\left(k+\frac{m}{2}\right) = \frac{m}{2}\sum_{k=1}^{m/2} \chi_K(k), \end{aligned}$$

luego

$$h = \frac{1}{2}\sum_{k=1}^{m/2} \chi_K(k).$$

Si, por el contrario, m es impar, entonces

$$\begin{aligned} hm &= -\sum_k \chi_K(k)k = -\sum_{k=1}^{m/2} \chi_K(k)k - \sum_{k=1}^{m/2} \chi_K(m-k)(m-k) \\ &= -\sum_{k=1}^{m/2} \chi_K(k)k + \sum_{k=1}^{m/2} \chi_K(k)(m-k) \\ &= -2\sum_{k=1}^{m/2} \chi_K(k)k + m\sum_{k=1}^{m/2} \chi_K(k). \end{aligned} \tag{4.23}$$

Por otra parte separamos los sumandos pares de los impares:

$$\begin{aligned} hm &= -\sum_k \chi_K(k)k = -\sum_{k=1}^{m/2} \chi_K(2k)2k - \sum_{k=1}^{m/2} \chi_K(m-2k)(m-2k) \\ &= -2\chi_K(2)\sum_{k=1}^{m/2} \chi_K(k)k + \sum_{k=1}^{m/2} \chi_K(2k)(m-2k) \\ &= -4\chi_K(2)\sum_{k=1}^{m/2} \chi_K(k)k + m\,\chi_K(2)\sum_{k=1}^{m/2} \chi_K(k). \end{aligned}$$

Por lo tanto

$$hm\,\chi_K(2) = -4\sum_{k=1}^{m/2} \chi_K(k)k + m\sum_{k=1}^{m/2} \chi_K(k). \tag{4.24}$$

Multiplicamos (4.23) por 2 y le restamos (4.24):

$$hm\big(2-\chi_K(2)\big) = m\sum_{k=1}^{m/2} \chi_K(k).$$

Finalmente observamos que la ecuación obtenida en el caso m par es ésta misma, puesto que entonces $\chi_K(2) = 0$. En resumen, llegamos a [ITAn 11.7]:

Teorema 4.41 *Sea K un cuerpo cuadrático de discriminante $\Delta < -4$. Entonces el número de clases de K viene dado por la fórmula*

$$h = \frac{1}{2-\chi(2)}\sum_{k=1}^{|\Delta|/2} \chi(k),$$

donde k recorre los números primos con Δ.

Esta fórmula, ya simple de por sí, se simplifica aún más cuando se aplica a cuerpos de discriminante primo. Concretamente tendrán que ser cuerpos de la forma $K = \mathbb{Q}\big(\sqrt{-p}\,\big)$, donde $p \equiv -1$ (mód 4). Entonces el carácter de K es el símbolo de Legendre y $\chi(2)$ depende del resto de p módulo 8. Con esto llegamos a [ITAn 11.8]:

Teorema 4.42 *Sea $p \equiv -1$ (mód 4) un primo racional y sean respectivamente R y N el número de restos cuadráticos y restos no cuadráticos módulo p en el intervalo $[0, p/2]$. Entonces el número de clases de $\mathbb{Q}\big(\sqrt{-p}\,\big)$ viene dado por*

$$h = \begin{cases} R-N & \text{si } p \equiv 7 \text{ (mód 8)} \\ \frac{1}{3}(R-N) & \text{si } p \equiv 3 \text{ (mód 8)} \end{cases}$$

Ejercicio: Probar que en las condiciones del teorema anterior h es impar.

El teorema anterior implica en particular que $R > N$. No se conoce ninguna prueba elemental de este hecho. Nuestra prueba depende—entre otras cosas—de la determinación del signo de las sumas de Gauss cuadráticas.

Capítulo V

Cuerpos métricos completos

Introducimos ahora las técnicas necesarias para el estudio de los números p-ádicos de Hensel y sus generalizaciones, de los que ya hemos hablado en la introducción. Como hemos indicado, éstos fueron introducidos por Hensel en 1897 y, a partir del trabajo de Helmut Hasse, alumno de Hensel, se situaron en el núcleo de la teoría algebraica de números del siglo XX.

5.1 Valores absolutos

Recordemos de [An 1.17] la definición general de valor absoluto:[1]

Definición 5.1 Sea K un cuerpo. Un *valor absoluto* en K es una aplicación $|\ |: K \longrightarrow [0, +\infty[$ que cumpla las propiedades siguientes:

1. $|\alpha| = 0$ si y sólo si $\alpha = 0$,
2. $|\alpha + \beta| \leq |\alpha| + |\beta|$,
3. $|\alpha\beta| = |\alpha||\beta|$.

Es obvio que el valor absoluto usual en $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es un valor absoluto en el sentido de la definición anterior. En general, la restricción de un valor absoluto a un subcuerpo es un valor absoluto en dicho subcuerpo.

Por otro lado todo cuerpo K admite al menos un valor absoluto: el llamado *valor absoluto trivial,* dado por

$$|\alpha|_0 = \begin{cases} 0 & \text{si } \alpha = 0, \\ 1 & \text{si } \alpha \neq 0. \end{cases}$$

[1] En la definición [An 1.17] se admite que la imagen de un valor absoluto sea cualquier cuerpo ordenado arquimediano R, porque en ese punto todavía no teníamos definidos los números reales, pero el teorema [An 1.14] prueba que no perdemos generalidad si tomamos $R = \mathbb{R}$.

Propiedades elementales Tras la definición [An 1.17] están demostradas las propiedades siguientes, aunque, dada su sencillez, repetimos aquí la prueba de todas ellas menos la última:

Las propiedades 1) y 3) de la definición 5.1 afirman que todo valor absoluto en un cuerpo K es un homomorfismo entre el grupo multiplicativo K^* de K y el grupo $]0,+\infty[$. En particular esto implica que $|1| = 1$ y $|\alpha^{-1}| = |\alpha|^{-1}$. Por lo tanto, $|-1|^2 = |(-1)^2| = 1$, luego $|-1| = 1$. Más en general, $|-\alpha| = |\alpha|$. Por último, se cumple que $|\alpha - \beta| \geq \big||\alpha| - |\beta|\big|$.

Ejercicio: Probar que un cuerpo finito no admite más valor absoluto que el trivial.

Otro hecho elemental es que todo valor absoluto en un cuerpo K induce una distancia $d : K \longrightarrow \mathbb{R}$ dada por $d(\alpha,\beta) = |\alpha - \beta|$, la cual a su vez define una topología en K.

Equivalencia Diremos que dos valores absolutos en un mismo cuerpo K son *equivalentes* si inducen la misma topología en K. El teorema siguiente prueba que dos valores absolutos equivalentes han de ser muy parecidos:

Teorema 5.2 *Sean $|\ |_1$ y $|\ |_2$ dos valores absolutos en un mismo cuerpo K. Las afirmaciones siguientes son equivalentes:*

1. *$|\ |_1$ y $|\ |_2$ son equivalentes.*
2. *Para todo $\alpha \in K$, se cumple $|\alpha|_1 < 1$ si y sólo si $|\alpha|_2 < 1$.*
3. *Para todo $\alpha, \beta \in K$, se cumple $|\alpha|_1 < |\beta|_1$ si y sólo si $|\alpha|_2 < |\beta|_2$.*
4. *Existe un número real $\rho > 0$ tal que para todo $\alpha \in K$, $|\alpha|_1 = |\alpha|_2^\rho$.*

DEMOSTRACIÓN: 1) $\Rightarrow$ 2), pues $|\alpha| < 1$ equivale a que $\lim_n \alpha^n = 0$.

2) $\Rightarrow$ 3) es evidente. Para probar 3) $\Rightarrow$ 1) observamos que el conjunto de bolas abiertas

$$\{B(\alpha, |\beta|) \mid \alpha, \beta \in K, \beta \neq 0\}$$

forman una base de K. En efecto, si el valora absoluto es trivial es inmediato, y si no lo es existe un $\beta \in K$ no nulo con $|\beta| < 1$ (existe un elemento no nulo que cumple $|\beta| \neq 1$ y si es necesario tomamos su inverso), con lo que los radios $|\beta^n|$ son arbitrariamente pequeños. La propiedad 3) implica entonces que las topologías inducidas por los dos valores absolutos tienen una misma base.

4) $\Rightarrow$ 2) es evidente. Sólo falta demostrar 4) a partir de las propiedades anteriores.

Si ambos valores absolutos son el trivial no hay nada que probar. Supongamos que el primero no es trivial, con lo que existe un $\alpha \in K$ no nulo tal que $|\alpha|_1 < 1$. Sea β cualquier elemento no nulo de K que cumpla $|\beta|_1 < 1$. Un par de números naturales (m,n) cumple $|\alpha^m|_1 < |\beta^n|_1$ si y sólo si cumple $|\alpha^m|_2 < |\beta^n|_2$. Pero $|\alpha^m|_1 < |\beta^n|_1$ equivale a $|\alpha|_1^m < |\beta|_1^n$, y a su vez a que

$$\frac{\log|\alpha|_1}{\log|\beta|_1} < \frac{n}{m}.$$

Como lo mismo vale para $|\ |_2$ concluimos que todo número racional r cumple

$$r > \frac{\log|\alpha|_1}{\log|\beta|_1} \quad \text{si y sólo si} \quad r > \frac{\log|\alpha|_2}{\log|\beta|_2},$$

La densidad de $\mathbb{Q}$ en $\mathbb{R}$ implica que los cocientes de logaritmos son iguales, luego para todo $\beta \in K$ con $|\beta|_1 < 1$ se cumple

$$\rho = \frac{\log|\alpha|_1}{\log|\alpha|_2} = \frac{\log|\beta|_1}{\log|\beta|_2},$$

donde ρ es una constante positiva, ya que $|\alpha|_1 < 1$ implica que $|\alpha|_2 < 1$. De aquí se sigue que $|\beta|_1 = |\beta|_2^\rho$ para todo β de K con $|\beta|_1 < 1$. Tomando inversos también vale si $|\beta|_1 > 1$, pero la equivalencia implica que si $|\beta|_1 = 1$ también $|\beta|_2 = 1$, luego también se cumple la igualdad. ∎

Es importante notar que la propiedad 4 del teorema anterior no afirma que si $|\ |$ es un valor absoluto en un cuerpo K y $\rho > 0$ entonces $|\ |^\rho$ sea un valor absoluto equivalente. Lo será si de hecho es un valor absoluto, pero puede no serlo. Las propiedades 1) y 3) de la definición se cumplen sin duda, pero la 2) puede fallar. A este respecto es útil el resultado siguiente:

Teorema 5.3 *Si $|\ |$ es un valor absoluto en un cuerpo K y $0 < \rho \leq 1$, entonces $|\ |^\rho$ es un valor absoluto equivalente al dado.*

Demostración: La única propiedad no evidente es la desigualdad triangular, pero si $|\alpha| \geq |\beta| > 0$, entonces

$$\begin{aligned} |\alpha+\beta|^\rho &= |\alpha|^\rho\,|1+\beta/\alpha|^\rho \leq |\alpha|^\rho\,\big(1+|\beta/\alpha|\big)^\rho \\ &\leq |\alpha|^\rho\,\big(1+|\beta/\alpha|\big) \leq |\alpha|^\rho\,\big(1+|\beta/\alpha|^\rho\big) = |\alpha|^\rho + |\beta|^\rho. \end{aligned}$$

∎

Cuerpos métricos En [An 1.8] definimos un cuerpo métrico como un par ordenado formado por un cuerpo K y un valor absoluto en K. Sin embargo, a la luz del teorema 5.2, conviene dar una definición ligeramente distinta:

Definición 5.4 Un cuerpo métrico es un par $(K, \mathcal{T})$, donde K es un cuerpo y y $\mathcal{T}$ es una topología en K determinada por un valor absoluto.

Dado un cuerpo métrico K, llamaremos valores absolutos de K a los valores absolutos que inducen la topología de K.

Esta definición enfatizará el hecho de que todos los conceptos que vamos a introducir dependen exclusivamente de la topología, y no del valor absoluto que la induce.

Isometrías e isomorfismos topológicos Sean K y K' dos cuerpos dotados de sendos valores absolutos $|\ |_K$ y $|\ |_{K'}$. Una *isometría* de K en K' respecto a los valores absolutos indicados es un monomorfismo de cuerpos $\phi : K \longrightarrow K'$ tal que $\big|\phi(\alpha)\big|_{K'} = |\alpha|_K$, para todo $\alpha \in K$.

Un *isomorfismo topológico* $\phi : K \longrightarrow K'$ entre dos cuerpos métricos es una aplicación que es a la vez isomorfismo y homeomorfismo. Dejamos al lector la prueba del teorema siguiente:

Teorema 5.5 *Sea $\phi : K \longrightarrow K'$ un isomorfismo topológico entre dos cuerpos métricos. Para cada valor absoluto de K existe un único valor absoluto de K' de modo que ϕ es una isometría entre ambos. Esta correspondencia define una biyección entre los valores absolutos de K y los de K'.*

La propiedad arquimediana Un principio básico del cálculo infinitesimal es que si x e y son dos cantidades positivas existe un número natural n tal que $y < nx$ (o si se prefiere, tal que $y/n < x$). La primera referencia conocida de esta propiedad data del siglo IV a.C. y se debe a Eudoxo. Sin embargo, hoy se la conoce como propiedad arquimediana, por el uso sistemático que Arquímedes hizo de ella en sus trabajos. La propiedad arquimediana puede expresarse en términos de valores absolutos arbitrarios:

Un valor absoluto $|\ \ |$ en un cuerpo K es *arquimediano* si para todo $\alpha \in K$ no nulo y todo número real $r > 0$ existe un número natural n tal que $|n\alpha| > r$.

La propiedad 4) del teorema 5.2 implica que un valor absoluto es arquimediano si y sólo si lo es cualquier otro equivalente a él. Por ello podemos decir que un cuerpo métrico es *arquimediano* si lo es cualquiera de sus valores absolutos.

Al final de este capítulo probamos que los únicos cuerpos métricos arquimedianos son los subcuerpos de $\mathbb{C}$, por lo que la teoría que estamos desarrollando sólo aporta cosas nuevas cuando se aplica a cuerpos no arquimedianos. Aparentemente la mera propiedad — puramente negativa — de no ser arquimediano es muy débil. Sin embargo el teorema siguiente prueba lo errónea que resulta dicha impresión:

Teorema 5.6 *Sea K un cuerpo métrico y $|\ \ |$ cualquiera de sus valores absolutos. Las afirmaciones siguientes son equivalentes:*

1. *K no es arquimediano.*
2. *Para todo número natural n, se cumple $|n| \leq 1$.*
3. *Para todo $\alpha, \beta \in K$, se cumple $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$.*
4. *Para todo número real $\rho > 0$ se cumple que $|\ \ |^\rho$ es un valor absoluto (equivalente al dado).*

Demostración: 1) $\Leftrightarrow$ 2) Si existe un número natural n tal que $|n| > 1$ entonces, para todo α no nulo $|n^k\alpha| = |n|^k\,|\alpha|$ toma valores arbitrariamente grandes. Recíprocamente, si $|n| \leq 1$ para todo natural n, entonces $|n\alpha| \leq |\alpha|$ para todo n, luego K no es arquimediano.

2) ⇒ 3) Para todo natural n se cumple

$$\begin{aligned} |\alpha+\beta|^n &= \Big|\sum_{k=0}^{n}\binom{n}{k}\alpha^k\beta^{n-k}\Big| \le \sum_{k=0}^{n}|\alpha|^k|\beta|^{n-k} \\ &\le (n+1)\,\text{máx}\big\{|\alpha|,|\beta|\big\}^n. \end{aligned}$$

Tomando raíces n-simas queda $|\alpha+\beta| \le \sqrt[n]{n+1}\,\text{máx}\big\{|\alpha|,|\beta|\big\}$, y tomando el límite en n obtenemos la desigualdad buscada.

3) ⇒ 2) es inmediato por inducción.

3) ⇒ 4) Sólo hay que probar que $|\ |^\rho$ cumple la desigualdad triangular, pero es fácil ver que si $|\ |$ cumple 3) entonces $|\ |^\rho$ también cumple 3), así como que 3) implica la desigualdad triangular.

4) ⇒ 3) Para cada $\rho > 0$, aplicando la desigualdad triangular de $|\ |^\rho$ tenemos

$$|\alpha+\beta| = \big(|\alpha+\beta|^\rho\big)^{1/\rho} \le \big(|\alpha|^\rho+|\beta|^\rho\big)^{1/\rho} \le 2^{1/\rho}\,\text{máx}\big\{|\alpha|,|\beta|\big\},$$

y haciendo tender ρ a infinito obtenemos la desigualdad de 3). ∎

La propiedad 2) del teorema anterior implica, entre otras cosas, que el carácter arquimediano de un valor absoluto en un cuerpo K sólo depende de su comportamiento sobre el cuerpo primo de K. En particular todo subcuerpo de un cuerpo (no) arquimediano es (no) arquimediano. Por otra parte, la propiedad 3) — la desigualdad triangular fuerte — es la que confiere a los cuerpos no arquimedianos sus propiedades más características, como pronto veremos.

Ejercicio: Probar que todo valor absoluto en un cuerpo de característica prima es no arquimediano.

Ejercicio: Probar que si K es un cuerpo no arquimediano y $\alpha,\beta \in K$, $|\alpha| \ne |\beta|$ entonces $|\alpha+\beta| = \text{máx}\{|\alpha|,|\beta|\}$.

Compleciones De acuerdo con la topología general [An 1.29], una sucesión (α_n) en un cuerpo métrico es *de Cauchy* si para todo número real $\epsilon > 0$ existe un número natural r tal que si $m,n \ge r$ entonces $|\alpha_m - \alpha_n| < \epsilon$. Notemos que por el apartado 4) del teorema 5.2 esta propiedad no depende del valor absoluto considerado.[2]

En particular, podemos definir un *cuerpo métrico completo* como un cuerpo métrico en el que toda sucesión de Cauchy es convergente, y la definición es correcta porque no depende del valor absoluto que induce la topología del cuerpo.

Las sucesiones de Cauchy tienen una caracterización muy simple en los cuerpos métricos no arquimedianos:

[2]La propiedad de que una sucesión sea de Cauchy es métrica y no topológica, en el sentido de que dos distancias pueden definir la misma topología y una sucesión puede ser de Cauchy para una y no para otra. Lo que acabamos de afirmar es que en un cuerpo métrico depende sólo de la topología, pero a condición de que hablemos únicamente de topologías inducidas por valores absolutos.

Teorema 5.7 *Una sucesión (α_n) en un cuerpo métrico no arquimediano es de Cauchy si y sólo si $\lim_n(\alpha_n - \alpha_{n-1}) = 0$.*

DEMOSTRACIÓN: Supongamos que la sucesión cumple esta propiedad y sea $\epsilon > 0$. Por definición de límite existe un $r > 0$ tal que si $n \geq r$ entonces $|\alpha_n - \alpha_{n-1}| < \epsilon$. Si tomamos $r \leq m \leq n$, entonces

$$|\alpha_n - \alpha_m| = \big|(\alpha_n - \alpha_{n-1}) + \cdots + (\alpha_{m+1} - \alpha_m)\big| \leq \max_{m<i\leq n} |\alpha_i - \alpha_{i-1}| < \epsilon,$$

luego la sucesión es de Cauchy. El recíproco es claro. ∎

Como consecuencia inmediata:

Teorema 5.8 *En un cuerpo métrico completo no arquimediano, la serie $\sum_{n=1}^{\infty} x_n$ es convergente si y sólo si $\lim_n x_n = 0$.*

Por [An 1.45] sabemos que todo cuerpo métrico k admite una compleción K, que es un cuerpo métrico completo que contiene a k como subcuerpo denso, y dicha compleción es única salvo isomorfismo topológico. Más precisamente:

Teorema 5.9 *Si k es un cuerpo métrico, existe un cuerpo métrico completo K tal que k es denso en K. Además K es único salvo isomorfismo topológico, es decir, si K y K' son cuerpos métricos completos que contienen a k como conjunto denso, entonces existe un isomorfismo topológico de K en K' que deja fijos a los elementos de k.*

Más aún, la construcción de la compleción muestra que cada valor absoluto de k se extiende a K (de forma única, pues el valor absoluto es continuo y k es denso en K).

Por ejemplo, $\mathbb{R}$ es la compleción de $\mathbb{Q}$ respecto al valor absoluto usual.

Terminamos recordando que en el capítulo II de [An] demostramos varios resultados sobre la topología de los cuerpos métricos y la de los espacios normados sobre cuerpos métricos (definición [An 2.1]). Por ejemplo, la observación tras [An 2.53] muestra que el valor absoluto $|\ \ | : K \longrightarrow \mathbb{R}$ es una aplicación continua, y en las páginas siguientes se prueba que también lo son la suma y el producto en K, y la aplicación $1/x$ en su dominio, de donde también son continuos todos los polinomios, etc.

5.2 Cuerpos métricos discretos

Retomemos las ideas con las que comenzábamos el capítulo: Nuestra intención es definir un valor absoluto sobre los números racionales de forma que dos números enteros estén próximos si su diferencia es divisible muchas veces entre un primo prefijado p. Más en general:

Definición 5.10 Si K es el cuerpo de cocientes de un dominio de Dedekind D y $\mathfrak{p}$ es un ideal primo en D, se define el valor $\mathfrak{p}$-ádico de un elemento $\alpha \in D$ no nulo como el exponente $v_\mathfrak{p}(\alpha)$ de $\mathfrak{p}$ en la factorización del ideal (α). Si $\gamma = \alpha/\beta$ es un elemento no nulo de K definimos $v_\mathfrak{p}(\gamma) = v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta)$.

Notemos que esto no depende de la representación de γ como fracción, pues, claramente, si $\alpha, \beta \in D$, se cumple que $v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha)+v_\mathfrak{p}(\beta)$, luego si tenemos dos representaciones $\alpha/\beta = \alpha'/\beta'$, resulta que $\alpha\beta' = \alpha'\beta$, luego

$$v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta') = v_\mathfrak{p}(\alpha') + v_\mathfrak{p}(\beta),$$

luego

$$v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta) = v_\mathfrak{p}(\alpha') - v_\mathfrak{p}(\beta').$$

A su vez, de aquí se sigue que la relación $v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta)$ es válida de hecho para todos los $\alpha, \beta \in K$ no nulos.

Las valoraciones $\mathfrak{p}$-ádicas son casos particulares de la definición siguiente:

Definición 5.11 Si K es un cuerpo, una *valoración* en K es una aplicación $v : K \setminus \{0\} \longrightarrow \mathbb{Z}$ que cumpla las propiedades siguientes:

1. v es suprayectiva,
2. $v(\alpha\beta) = v(\alpha) + v(\beta)$, para $\alpha, \beta \in K \setminus \{0\}$
3. $v(\alpha + \beta) \geq \text{mín}\big\{v(\alpha), v(\beta)\big\}$, para $\alpha, \beta \in K \setminus \{0\}$, $\alpha \neq -\beta$.

Según indicábamos, es fácil comprobar que las valoraciones $\mathfrak{p}$-ádicas que hemos definido más arriba cumplen realmente estas propiedades. Ya hemos comprobado la propiedad 2) y la 3) se comprueba análogamente, probándola primero sobre elementos de D y después sobre elementos de K arbitrarios. Para 1) consideramos un número $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, de modo que $v_\mathfrak{p}(\pi) = 1$. Entonces $v_\mathfrak{p}(\pi^n) = n$.

Si v es una valoración en un cuerpo K, conviene definir $v(0) = +\infty$. Si convenimos en que $n+\infty = +\infty+\infty = +\infty$, las propiedades 2) y 3) son válidas para todo $\alpha, \beta \in K$. Dejamos al lector la prueba de las siguientes propiedades adicionales:

1. $v(\pm 1) = 0$,
2. $v(-\alpha) = v(\alpha)$,
3. $v(\alpha/\beta) = v(\alpha) - v(\beta)$,
4. Si $v(\alpha) \neq v(\beta)$ entonces $v(\alpha + \beta) = \text{mín}\big\{v(\alpha), v(\beta)\big\}$.

En estos términos, queremos considerar que dos elementos α y β de un dominio de Dedekind D están más próximos respecto a un primo $\mathfrak{p}$ de D cuanto mayor sea $v_\mathfrak{p}(\alpha - \beta)$. Si queremos reducir esta noción de proximidad a un valor absoluto, éste deberá ser menor cuanto mayor sea $v_\mathfrak{p}$. Además tenemos que transformar las propiedades aditivas de las valoraciones en las propiedades multiplicativas de los valores absolutos. La forma de hacerlo es obvia:

Si v es una valoración en un cuerpo K y $0 < \rho < 1$, definimos $|\alpha| = \rho^{v(\alpha)}$ (entendiendo que $|0| = \rho^{+\infty} = 0$).

Es claro que $|\ \ |$ así definido es un valor absoluto no arquimediano en K. El teorema 5.2 implica que distintos valores de ρ dan lugar a valores absolutos equivalentes, por lo que cada valoración dota a K de una única estructura de cuerpo métrico.

Ejercicio: Probar que si un valor absoluto está determinado por una valoración, entonces todos los valores absolutos equivalentes están definidos a partir de la misma valoración tomando distintos valores de ρ.

Un cuerpo métrico K es *discreto* si sus valores absolutos vienen inducidos por una valoración. En particular todo cuerpo métrico discreto es no arquimediano.

Ejercicio: Probar que un cuerpo métrico K no trivial es discreto si y sólo si la imagen de K^* por uno cualquiera de sus valores absolutos es un subgrupo discreto (como espacio topológico) de $\mathbb{R}^*$.

Ejercicio: Probar que los valores absolutos de un cuerpo métrico discreto están inducidos por una única valoración (porque ρ es necesariamente el mayor valor absoluto menor que 1).

Notemos que una valoración puede ser recuperada a partir de uno cualquiera de los valores absolutos que induce mediante la relación $v(\alpha) = \log|\alpha|/\log\rho$. Puesto que $-\log : [0, +\infty[\longrightarrow \mathbb{R} \cup \{+\infty\}$ es una aplicación continua, al igual que lo es el valor absoluto, concluimos que $v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$ también es continua.

Teorema 5.12 *Si k es un cuerpo métrico discreto, su valoración se extiende de forma única a una valoración en su compleción K, que es, por tanto, un cuerpo métrico discreto.*

Demostración: Dado $\alpha \in K \setminus \{0\}$, existe una sucesión (α_n) en k convergente a α. Por continuidad $\big(|\alpha_n|\big)$ converge a $|\alpha| \neq 0$. Por la continuidad del logaritmo concluimos que $\big(v(\alpha_n)\big)$ ha de converger a $\log|\alpha|/\log\rho$, pero se trata de una sucesión de números enteros, luego el límite ha de ser entero. Así pues, si definimos $v(\alpha) = \log|\alpha|/\log\rho$ tenemos una aplicación continua $v : K\setminus\{0\} \longrightarrow \mathbb{Z}$ que extiende a la valoración de k. Es fácil ver que se trata de una valoración en K que induce sus valores absolutos. ∎

Definición 5.13 Si $\mathfrak{p}$ es un ideal primo en un dominio de Dedekind D con cuerpo de cocientes K, representaremos por $|\ \ |_\mathfrak{p}$ a cualquiera de los valores absolutos inducidos por la valoración $\mathfrak{p}$-ádica en K y lo llamaremos *valor absoluto $\mathfrak{p}$-ádico*). A su vez, representaremos por $K_\mathfrak{p}$ a la compleción de K respecto a dicho valor absoluto. Llamaremos también $v_\mathfrak{p}$ y $|\ \ |_\mathfrak{p}$ a las extensiones a $K_\mathfrak{p}$ de la valoración y el valor absoluto $\mathfrak{p}$-ádicos.

Esto se aplica en particular al caso en que $\mathfrak{p}$ es un ideal primo en un cuerpo numérico K (es decir, un ideal de su anillo de enteros algebraicos $\mathcal{O}_K$). En tal caso la compleción $K_\mathfrak{p}$ recibe el nombre de cuerpo de los *números $\mathfrak{p}$-ádicos,* que es un cuerpo métrico discreto completo.

Más en particular, para cada primo $p \in \mathbb{Z}$, tenemos definido el cuerpo $\mathbb{Q}_p$ de los *números p-ádicos.*

A lo largo de este capítulo estudiaremos la estructura de estos cuerpos y su relación con los cuerpos numéricos.

Ejercicio: Si p es un primo en $\mathbb{Z}$, probar que la sucesión (p^n) converge a 0 en $\mathbb{Q}_p$, y que $\sum_{n=0}^{\infty} p^n = 1/(1-p)$.

Ejercicio: Si p es un primo en $\mathbb{Z}$, probar que la serie $\sum_{n=1}^{\infty} 1/n$ es divergente en $\mathbb{Q}_p$, porque su término general no tiende a 0.

Sea K un cuerpo métrico discreto y sea v su valoración. Definimos

$$\begin{aligned} D &= \{\alpha \in K \mid v(\alpha) \geq 0\} = \big\{\alpha \in K \;\big|\; |\alpha| \leq 1\big\}, \\ U &= \{\alpha \in K \mid v(\alpha) = 0\} = \big\{\alpha \in K \;\big|\; |\alpha| = 1\big\}, \\ \mathfrak{p} &= \{\alpha \in K \mid v(\alpha) \geq 1\}. \end{aligned}$$

Es inmediato comprobar que D es un anillo, U su grupo de unidades y $\mathfrak{p}$ un ideal primo de D. Diremos que D es el *anillo de enteros* de K y que U es el *grupo de unidades* de K.

En particular, si $p \in \mathbb{Z}$ es primo, el anillo de enteros del cuerpo $\mathbb{Q}_p$ de los números p-adicos se representa por $\mathbb{Z}_p$, y sus elementos se llaman simplemente *enteros p-ádicos.*

Ejercicio: Probar que los conjuntos $\alpha + \beta D$, con $\alpha, \beta \in K$, $\beta \neq 0$ son abiertos y cerrados y forman una base de K.

Fijemos un elemento $\pi \in K$ tal que $v(\pi) = 1$. Para todo $\alpha \in K$ no nulo, si $v(\alpha) = n$, entonces $\epsilon = \alpha/\pi^n$ cumple $v(\epsilon) = 0$, luego $\alpha = \epsilon\pi^n$ y $\epsilon \in U$. Esta descomposición es única, pues si $\epsilon\pi^n = \epsilon'\pi^m$, entonces

$$n = v(\epsilon\pi^n) = v(\epsilon'\pi^m) = m,$$

y simplificando las potencias de π llegamos a que $\epsilon = \epsilon'$.

En particular vemos que $\mathfrak{p} = (\pi)$, con lo que π es primo, y la descomposición que acabamos de obtener (cuando α es entero) es de hecho una descomposición de α en factores primos. El teorema siguiente recoge todo lo que acabamos de probar:

Teorema 5.14 *Sea K un cuerpo métrico discreto. Entonces su anillo de enteros D es un dominio de factorización única. Sus primos son exactamente los elementos π que cumplen $v(\pi) = 1$. Todos son asociados, por lo que $\mathfrak{p}$ es el único ideal primo de D, y está generado por cualquiera de ellos. Fijado un primo π, todo elemento no nulo de K se expresa de forma única como $\alpha = \epsilon\pi^n$, donde $\epsilon \in U$ y, necesariamente, $n = v(\alpha)$. En particular K es el cuerpo de cocientes de D.*

En realidad el anillo de enteros de un cuerpo discreto es mucho más que un dominio de factorización única. Es trivialmente un dominio euclídeo, tomando como norma la propia valoración. Efectivamente, se cumple que $v(\alpha) \le v(\alpha\beta)$, para α y β no nulos, y dados $\Delta, \delta \in D$ con $\delta \neq 0$, la división euclídea es simplemente $\Delta = \delta \cdot 0 + \Delta$ si $v(\Delta) < v(\delta)$ o bien $\Delta = \frac{\Delta}{\delta}\,\delta + 0$ en caso contrario.

En particular todos los ideales de D son principales y, teniendo en cuenta la estructura aritmética de D, son fáciles de determinar:

Teorema 5.15 *Sea K un cuerpo métrico discreto. Entonces su anillo de enteros es un dominio euclídeo, y sus ideales son exactamente*

$$0 \subset \cdots \subset \mathfrak{p}^3 \subset \mathfrak{p}^2 \subset \mathfrak{p} \subset 1.$$

En particular, si $p \in \mathbb{Z}$ es primo, tenemos que p es, salvo unidades, el único primo del anillo $\mathbb{Z}_p$ de los enteros p-ádicos. Todo número p-ádico no nulo (no necesariamente entero) se expresa de forma única como $\alpha = \epsilon p^n$, donde $\epsilon \in U_p$ es una unidad p-ádica y $n = v_p(\alpha)$.

El teorema siguiente nos da una primera muestra de la estrecha relación que existe entre la aritmética de un dominio de Dedekind y la de sus compleciones:

Teorema 5.16 *Sea D un dominio de Dedekind, sea K su cuerpo de cocientes y sea $\mathfrak{p}$ un ideal primo en D. Sea $D_\mathfrak{p}$ el anillo de enteros de $K_\mathfrak{p}$ y sea $\mathfrak{m}_\mathfrak{p}$ el único primo de $D_\mathfrak{p}$. Entonces:*

1. *$D_\mathfrak{p}$ es la clausura de D.*
2. *$\mathfrak{m}_\mathfrak{p}^n$ es la clausura de $\mathfrak{p}^n$.*
3. *La aplicación $[\alpha] \mapsto [\alpha]$ determina un isomorfismo $D/\mathfrak{p}^n \cong D_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n$.*

Demostración: 1) Como $D \subset D_\mathfrak{p}$ y $D_\mathfrak{p}$ es cerrado en $K_\mathfrak{p}$ (es la bola unitaria cerrada), tenemos que la clausura de D está contenida en $D_\mathfrak{p}$.

Tomemos ahora $\alpha \in D_\mathfrak{p}$ y fijemos un número real $0 < \epsilon < 1$. Como K es denso en $K_\mathfrak{p}$ existe un $\beta \in K$ tal que $|\alpha - \beta|_\mathfrak{p} < \epsilon$. Entonces

$$|\beta|_\mathfrak{p} = |\alpha + (\beta - \alpha)|_\mathfrak{p} \le \max\big\{|\alpha|_\mathfrak{p}, |\beta - \alpha|_\mathfrak{p}\big\} \le 1.$$

Sea $\beta = a/b$, donde $a, b \in D$. Por el teorema 2.18 podemos exigir que $\mathfrak{p} \nmid b$. Si $x \in D$, la desigualdad $|x - \beta|_\mathfrak{p} < \epsilon$ equivale a que $|bx - a|_\mathfrak{p} < \epsilon$, lo que a su vez equivale a que $bx \equiv a \pmod{\mathfrak{p}^n}$ para un n suficientemente grande. Puesto que b es una unidad módulo $\mathfrak{p}$, siempre podemos encontrar un x en estas condiciones, luego en total

$$|\alpha - x|_\mathfrak{p} \le \max\big\{|\alpha - \beta|_\mathfrak{p}, |\beta - x|_\mathfrak{p}\big\} < \epsilon.$$

Esto prueba que α está en la clausura de D.

2) Por el apartado anterior, todo elemento de $D_\mathfrak{p}$ es de la forma $\alpha = \lim_k \alpha_k$, con $\alpha_k \in D$. Por la continuidad de la valoración, $v_\mathfrak{p}(\alpha) = \lim_n v_\mathfrak{p}(\alpha_k)$, luego $\alpha \in \mathfrak{m}_\mathfrak{p}^n$ si y sólo si $\alpha_k \in \mathfrak{p}^n$ para todo n suficientemente grande.

3) Es claro que la aplicación está bien definida y es un homomorfismo. Observemos que $\alpha \equiv \beta$ (mód $\mathfrak{p}^n$) equivale a $v_\mathfrak{p}(\alpha - \beta) \geq n$, y lo mismo es válido para $\mathfrak{m}_\mathfrak{p}$, luego la aplicación es inyectiva. Por último el apartado 1) implica que para todo $\alpha \in D_\mathfrak{p}$ existe un $\beta \in D$ tal que $v_\mathfrak{p}(\alpha - \beta) \geq n$, lo que se traduce en que todo elemento de $D_\mathfrak{p}$ es congruente módulo $\mathfrak{m}_\mathfrak{p}^n$ con un elemento de D, es decir, que la aplicación es suprayectiva. ∎

Ejercicio: Sea D un dominio de Dedekind y $\mathfrak{p}$ un ideal primo de D. Determinar la clausura en $K_\mathfrak{p}$ de un ideal cualquiera de D.

Enseguida probaremos que todo número p-ádico se expresa como serie de potencias en p, pero antes conviene probar que los cuerpos p-ádicos son localmente compactos. Más en general:

Teorema 5.17 *Sea K un cuerpo métrico discreto y completo, D su anillo de enteros y $\mathfrak{p}$ su ideal primo. Las afirmaciones siguientes son equivalentes:*

1. *El cuerpo de restos $D/\mathfrak{p}$ es finito.*
2. *Un subconjunto de K es compacto si y sólo si es cerrado y acotado.*

Demostración: Supongamos que $D/\mathfrak{p}$ es finito. Sea F un conjunto de representantes de las clases de equivalencia. Sea π un primo en D, de modo que $\mathfrak{p} = (\pi)$. Basta probar que D es compacto, pues entonces lo serán todas las bolas cerradas y también todos los conjuntos cerrados y acotados. A su vez basta ver que toda sucesión de enteros (α_n) tiene una subsucesión convergente.

Tiene que haber infinitos términos de la sucesión congruentes módulo π con un mismo $x_0 \in F$. Sea, pues, (α_n^1) una subsucesión tal que para todo número natural n se cumpla $\alpha_n^1 \equiv x_0$ (mód π). Digamos $\alpha_n^1 = x_0 + \beta_n^1\pi$, con $\beta_n^1 \in D$.

Similarmente podemos tomar una subsucesión (α_n^2) de (α_n^1) tal que los correspondientes β_n^2 sean todos congruentes con un mismo $x_1 \in F$ módulo π. De este modo $\alpha_n^2 = x_0 + x_1\pi + \beta_n^2\,\pi^2$.

En general podemos ir obteniendo una sucesión de subsucesiones (α_n^k) (cada cual subsucesión de la anterior) de modo que

$$\alpha_n^k = \sum_{i=0}^{k-1} x_i\pi^i + \beta_n^k\,\pi^k,$$

con $x_i \in F$, $\beta_n^k \in D$. En particular,

$$\alpha_n^n = \sum_{i=0}^{n-1} x_i\pi^i + \beta_n^n\,\pi^n.$$

Es claro que (α_n^n) es una subsucesión de la sucesión de partida. Claramente las sucesiones $(x_i\pi^i)$ y $(\beta_n^n\,\pi^n)$ convergen a 0, luego, teniendo en cuenta el teorema 5.8, existe

$$\lim_n \alpha_n^n = \sum_{i=0}^{\infty} x_i\pi^i,$$

pues la serie es convergente y $\beta_n^n\,\pi^n$ tiende a 0.

Recíprocamente, si $D/\mathfrak{p}$ es infinito, las clases de congruencia módulo $\mathfrak{p}$ son una partición de D (cerrado y acotado) en conjuntos abiertos, luego D no es compacto. ∎

La propiedad 2) del teorema anterior es simplemente la compacidad local. Hemos visto, pues, que un cuerpo métrico discreto completo es localmente compacto si y sólo si su cuerpo de restos es finito.

En la prueba del teorema anterior está contenida la mayor parte del resultado siguiente:

Teorema 5.18 *Sea K un cuerpo métrico discreto. Sea $\mathfrak{p}$ su ideal primo y sea F un conjunto de representantes de las clases módulo $\mathfrak{p}$ tal que $0 \in F$. Sea π un primo de K. Entonces todo elemento $\alpha \in K$ no nulo se expresa de forma única como*

$$\alpha = \sum_{n=k}^{\infty} x_n \pi^n, \tag{5.1}$$

donde $x_n \in F$, $k \in \mathbb{Z}$ y $x_k \neq 0$. Además $k = v(\alpha)$. Si K es completo cada serie de esta forma determina un elemento de K.

Demostración: Sea $k = v(\alpha)$. Aplicamos el proceso de la prueba del teorema anterior a la sucesión constante igual al entero $\pi^{-k}\,\alpha$, con la particularidad de que, al ser todos los términos iguales, no es necesario tomar subsucesiones ni suponer que F es finito. El resultado es un desarrollo de tipo (5.1) para $\pi^{-k}\,\alpha$, y multiplicando por π^k obtenemos otro para α.

Observemos que si en (5.1) multiplicamos ambos miembros por π^{-k} obtenemos una serie todos cuyos términos son enteros, luego el límite también (el anillo de enteros de K es claramente cerrado). De hecho, el resto módulo $\mathfrak{p}$ de dicho límite es $x_k \neq 0$. Por lo tanto $v(\pi^{-k}\alpha) = 0$ y $v(\alpha) = k$.

Si un mismo α admite dos desarrollos de tipo (5.1), ambos tendrán el mismo $k = v(\alpha)$:

$$x_k\pi^k + x_{k+1}\pi^{k+1} + x_{k+2}\pi^{k+2} + \cdots = y_k\pi^k + y_{k+1}\pi^{k+1} + y_{k+2}\pi^{k+2} + \cdots$$

Multiplicamos por π^{-k} y obtenemos una igualdad de enteros:

$$x_k + x_{k+1}\pi + x_{k+2}\pi^2 + \cdots = y_k + y_{k+1}\pi + y_{k+2}\pi^2 + \cdots$$

Claramente entonces $x_k \equiv y_k$ (mód π), y como ambos están en F, necesariamente $x_k = y_k$. Restando y dividiendo entre π queda

$$x_{k+1} + x_{k+2}\pi + \cdots = y_{k+1} + y_{k+2}\pi + \cdots$$

Del mismo modo concluimos que $x_{k+1} = y_{k+1}$, e inductivamente llegamos a que todos los coeficientes coinciden. La completitud de K implica la convergencia de las series. ∎

En particular, en las condiciones del teorema anterior, α es entero si y sólo si $k \geq 0$. Si no es así, α se descompone como

$$\alpha = \sum_{n=k}^{-1} x_n\pi^n + \sum_{n=0}^{\infty} x_n\pi^n,$$

es decir, que su desarrollo en serie de potencias tiene una parte fraccionaria finita y una parte entera infinita, al contrario que el desarrollo decimal de los números reales.

Ejercicio: Sea p un primo racional y consideremos en el cuerpo $\mathbb{Q}_p$ las representaciones de la forma (5.1) con $\pi = p$ y $0 \le x_n < p$. Probar que los números naturales se caracterizan por que sus desarrollos son finitos, los números enteros tienen desarrollos finalmente iguales a $p-1$ y los números racionales se corresponden con las series con coeficientes finalmente periódicos

Ejercicio: Probar que si K es un cuerpo métrico discreto localmente compacto, entonces todos los anillos de restos $D/\mathfrak{p}^n$ son finitos.

Nota Ahora ya podemos ver en la expresión

$$\sqrt{2} = 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + 1\cdot 7^4 + 2\cdot 7^5 + 1\cdot 7^6 + 2\cdot 7^7 + 4\cdot 7^8 + \cdots$$

un ejemplo típico de número heptádico... supuesto que exista, ya que no hemos garantizado que el proceso que nos va dando los coeficientes de la serie pueda continuarse indefinidamente. Esto se sigue inmediatamente de un hecho conocido sobre restos cuadráticos: si p es un primo impar, un entero m no divisible entre p es un resto cuadrático módulo p^r si y sólo si m es un resto cuadrático módulo p. Este hecho puede probarse estudiando con detalle los grupos de unidades módulo p^r, pero más adelante lo deduciremos de las propiedades de los números p-ádicos.

Concretamente, bastará demostrar que si m es un resto cuadrático módulo p, entonces en $\mathbb{Z}_p$ existe $\sqrt{m}$, pues entonces, dado que $\mathbb{Z}_p/(p^n) \cong \mathbb{Z}/(p^n)$, existirá un $r \in \mathbb{Z}$ tal que $\sqrt{m} \equiv r \pmod{p^n}$, luego $m \equiv r^2 \pmod{p^n}$, en $\mathbb{Z}_p$, luego también en $\mathbb{Z}$. ∎

Seguidamente vamos a ver que, en el caso de los cuerpos numéricos, es posible asociar de forma canónica un valor absoluto a cada ideal primo. Esto será inmediato en el caso de $\mathbb{Q}$, pero para el caso general necesitamos el resultado siguiente:

Teorema 5.19 *Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de sus cuerpos de cocientes. Sea $\mathfrak{p}$ un ideal primo en D y $\mathfrak{P}$ un ideal primo en E. Entonces $\mathfrak{P} \mid \mathfrak{p}$ si y sólo si existe un valor absoluto asociado a $\mathfrak{p}$ que se extiende a un valor absoluto asociado a $\mathfrak{P}$. En tal caso cada valor absoluto asociado a $\mathfrak{p}$ se extiende a un único valor absoluto asociado a $\mathfrak{P}$ y la restricción a k de todo valor absoluto asociado a $\mathfrak{P}$ es un valor absoluto asociado a $\mathfrak{p}$.*

DEMOSTRACIÓN: Si $\mathfrak{P} \mid \mathfrak{p}$ sea e el índice de ramificación $e(\mathfrak{P}/\mathfrak{p})$. Entonces $\mathfrak{P}$ divide e veces a $\mathfrak{p}$, lo que se traduce en que las valoraciones asociadas a ambos primos satisfacen la relación $v_{\mathfrak{P}}(\alpha) = e\, v_{\mathfrak{p}}(\alpha)$, para todo $\alpha \in k$.

Cada valor absoluto asociado a $\mathfrak{p}$ es de la forma $|\alpha| = \rho^{v_{\mathfrak{p}}(\alpha)}$, para todo $\alpha \in k$, y se extiende al valor absoluto asociado a $\mathfrak{P}$ dado por $|\alpha| = (\rho^{1/e})^{v_{\mathfrak{P}}(\alpha)}$ para todo $\alpha \in K$.

Recíprocamente, tenemos que todo valor absoluto asociado a $\mathfrak{P}$ es de la forma $|\alpha| = \rho^{v_{\mathfrak{P}}(\alpha)}$, para todo $\alpha \in K$, y su restricción a k es de la forma $|\alpha| = (\rho^e)^{v_{\mathfrak{p}}(\alpha)}$, luego está asociado a $\mathfrak{p}$.

Cada valor absoluto asociado a $\mathfrak{p}$ tiene una única extensión asociada a $\mathfrak{P}$ porque dos extensiones serían equivalentes, luego una sería una potencia de la otra, y como en k coinciden, el exponente sería 1.

Finalmente, si existe un valor absoluto asociado a $\mathfrak{p}$ que se extiende a un valor absoluto asociado a $\mathfrak{P}$, entonces $\mathfrak{p}$ ha de ser el único ideal primo de k al que divide $\mathfrak{P}$, pues ya hemos visto que todas las restricciones de los valores absolutos de $\mathfrak{P}$ se corresponden con dicho primo. ∎

Definición 5.20 Si p es un primo en $\mathbb{Z}$, llamaremos *valor absoluto canónico* asociado a p al valor absoluto en $\mathbb{Q}$ dado por $|r|_p = (1/p)^{v_p(r)}$, para todo $r \in \mathbb{Q}$.

Si $\mathfrak{p}$ es un ideal primo en un cuerpo numérico K y p es el único primo racional al cual divide, llamaremos *valor absoluto canónico* asociado a $\mathfrak{p}$ al único valor absoluto asociado a $\mathfrak{p}$ que extiende al valor absoluto canónico de p. Lo representaremos por $|\ |_{\mathfrak{p}}$.

Teorema 5.21 *Sea K/k una extensión de cuerpos numéricos, sea $\mathfrak{P}$ un ideal primo en K y $\mathfrak{p}$ un ideal primo en k. Se cumple que $\mathfrak{P} \mid \mathfrak{p}$ si y sólo si el valor absoluto canónico de $\mathfrak{P}$ extiende al valor absoluto canónico de $\mathfrak{p}$.*

Demostración: Si $\mathfrak{P} \mid \mathfrak{p}$ entonces la restricción a k del valor absoluto canónico de $\mathfrak{P}$ es un valor absoluto asociado a $\mathfrak{p}$ que extiende al valor absoluto canónico del único primo racional p al cual dividen ambos ideales, luego por la unicidad dicha restricción ha de ser el valor absoluto canónico de $\mathfrak{p}$. El recíproco es una consecuencia inmediata del teorema 5.19. ∎

Recapitulando lo visto hasta ahora, si k es un cuerpo numérico, $\mathcal{O}_k$ es su anillo de enteros algebraicos y es un ideal primo en $\mathcal{O}_k$, tenemos definido el cuerpo $k_{\mathfrak{p}}$ de los números $\mathfrak{p}$-ádicos, su anillo de enteros $D_{\mathfrak{p}}$ y su único ideal primo $\mathfrak{m}_{\mathfrak{p}}$. El teorema 5.16 nos da que $D_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \cong \mathcal{O}_k/\mathfrak{p}$. En particular, como el cuerpo de restos $\bar{k}_{\mathfrak{p}} = \mathcal{O}_k/\mathfrak{p}$ es un cuerpo finito, el teorema 5.17 nos da que $k_{\mathfrak{p}}$ es localmente compacto.

Si K/k es una extensión de cuerpos numéricos y $\mathfrak{P}$ es un divisor primo en K que divide a $\mathfrak{p}$, el teorema anterior nos da que el valor absoluto canónico de $\mathfrak{P}$ extiende al de $\mathfrak{p}$. El primero se extiende a la compleción $K_{\mathfrak{P}}$, y la clausura de k en $K_{\mathfrak{P}}$ es una compleción de k respecto de su valor absoluto canónico, luego, por la unicidad de la compleción, podemos identificarla con $k_{\mathfrak{p}}$. Así pues, podemos considerar que $k_{\mathfrak{p}} \subset K_{\mathfrak{P}}$. Definimos el *grado local*

$$n(\mathfrak{P}/\mathfrak{p}) = |K_{\mathfrak{P}} : k_{\mathfrak{p}}|.$$

Por otra parte, también tenemos la inclusión $\mathcal{O}_k \subset \mathcal{O}_K$ entre los anillos de enteros y sabemos que ésta induce una identificación $\bar{k}_{\mathfrak{p}} \subset \bar{K}_{\mathfrak{P}}$ entre los cuerpos de restos. El teorema siguiente muestra, entre otras cosas, que esta identificación es consistente con el isomorfismo dado por el teorema 5.16:

Teorema 5.22 *Sea K/k una extensión de cuerpos numéricos, sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{p}$ un primo finito en D y sea $\mathfrak{P}$ un primo en E que lo divida. Sea $e = e(\mathfrak{P}/\mathfrak{p})$ y $f = f(\mathfrak{P}/\mathfrak{p})$. Sean $K_\mathfrak{P}$ y $k_\mathfrak{p}$ las completaciones de ambos cuerpos y sean $E_\mathfrak{P}$ y $D_\mathfrak{p}$ los correspondientes anillos de enteros. Entonces*

1. *La extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es finita y su grado es $n(\mathfrak{P}/\mathfrak{p}) = ef$.*
2. *$E_\mathfrak{P}$ es la clausura entera de $D_\mathfrak{p}$ en $K_\mathfrak{P}$, luego $E_\mathfrak{P}/D_\mathfrak{p}$ es una extensión de dominios de Dedekind.*
3. *Si $\mathfrak{m}_\mathfrak{p}$ y $\mathfrak{m}_\mathfrak{P}$ son los ideales maximales de $D_\mathfrak{p}$ y $E_\mathfrak{P}$, tenemos la situación descrita por el diagrama siguiente:*

$$\begin{array}{ccc} E/\mathfrak{P} & \longrightarrow & E_\mathfrak{P}/\mathfrak{m}_\mathfrak{P} \\ \uparrow & & \uparrow \\ D/\mathfrak{p} & \longrightarrow & D_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} \end{array}$$

   Todas las aplicaciones están definidas de forma natural ($[\alpha] \mapsto [\alpha]$). Las flechas horizontales son los isomorfismos descritos en 5.16. *Las flechas verticales son monomorfismos de cuerpos.*

4. *Se cumple $e = e(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ y $f = f(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$. En particular $\mathfrak{m}_\mathfrak{p} = \mathfrak{m}_\mathfrak{P}^e$.*

DEMOSTRACIÓN: Sea $\alpha_1, \dots, \alpha_n$ un generador de E como D-módulo. Sea $\gamma \in E_\mathfrak{P}$. Por 5.16 sabemos que $E_\mathfrak{P}$ es la clausura de E, luego existe una sucesión $\{x_k\}$ de elementos de E que converge a γ.

Digamos que $x_k = d_{k1}\alpha_1 + \cdots + d_{kn}\alpha_n$, para ciertos coeficientes $d_{kj} \in D$.

Como $D_\mathfrak{p}$ es compacto (es la bola unidad cerrada de $k_\mathfrak{p}$), también lo es $D_\mathfrak{p}^n$, y la sucesión $(d_{k1}, \dots, d_{kn})$ tiene una subsucesión convergente a un cierto $(d_1, \dots, d_n) \in D_\mathfrak{p}^n$. Entonces es claro que x_k converge a $d_1\alpha_1 + \cdots + d_n\alpha_n = \gamma$. Esto prueba que $\alpha_1, \dots, \alpha_n$ es también un generador de $E_\mathfrak{P}$ como $D_\mathfrak{p}$-módulo.

En particular $E_\mathfrak{P} = D_\mathfrak{p}[\alpha_1, \dots, \alpha_n]$ y, como los α_i son enteros sobre D, también lo son sobre $D_\mathfrak{p}$, con lo que $E_\mathfrak{P}$ es una extensión entera de $D_\mathfrak{p}$. Como $E_\mathfrak{p}$ es íntegramente cerrado (es DIP), tenemos que $E_\mathfrak{P}$ es la clausura entera de $D_\mathfrak{p}$ en $K_\mathfrak{P}$.

Otra consecuencia es que $k_\mathfrak{p}(\alpha_1, \dots, \alpha_n)$ es un cuerpo que contiene a $E_\mathfrak{P}$, y como $K_\mathfrak{P}$ es el cuerpo de cocientes de $E_\mathfrak{P}$, ha de ser $K_\mathfrak{P} = k_\mathfrak{p}(\alpha_1, \dots, \alpha_n)$. Los números $\alpha_1, \dots, \alpha_n$ son algebraicos sobre k, luego también sobre $k_\mathfrak{p}$, luego la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es finita.

Con esto tenemos probado 2). En 3) no hay nada que probar, pero de 3) se deduce que el grado de la extensión de la izquierda del diagrama coincide con el grado de la extensión de la derecha, o sea, que $f = f(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$.

La relación entre la valoración inducida por $\mathfrak{P}$ y la valoración inducida por $\mathfrak{p}$ es que para todo $\alpha \in k$ se cumple $v_\mathfrak{P}(\alpha) = e\, v_\mathfrak{p}(\alpha)$. Como las valoraciones definidas por $\mathfrak{m}_\mathfrak{p}$ y $\mathfrak{m}_\mathfrak{P}$ extienden a éstas, se cumple $v_{\mathfrak{m}_\mathfrak{P}}(\alpha) = e\, v_{\mathfrak{m}_\mathfrak{p}}(\alpha)$

para todo $\alpha \in k$, y por continuidad para todo $\alpha \in k_\mathfrak{p}$. Esto implica que $e = e(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$, con lo que queda probado 4).

Por último, el grado de la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es ef por el teorema 2.34, lo que prueba 1). ∎

Hasta aquí hemos distinguido entre $\mathfrak{p}$ y $\mathfrak{m}_\mathfrak{p}$, pero en lo sucesivo representaremos por $\mathfrak{p}$ ambos ideales.

Lo que afirma el teorema anterior es que, si la factorización de $\mathfrak{p}$ en K es $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, en las extensiones locales $K_{\mathfrak{P}_i}/k_\mathfrak{p}$ es $\mathfrak{p} = \mathfrak{P}_i^{e_i}$, con el mismo grado de inercia, lo que significa que el índice de ramificación $e(\mathfrak{P}_i/\mathfrak{p})$ y el grado de inercia $f(\mathfrak{P}_i/\mathfrak{p})$ pueden calcularse indistintamente con la factorización de $\mathfrak{p}$ en la extensión K/k y con la extensión de los cuerpos de restos $\bar{K}/\bar{k}$ calculados a partir de ella o con la factorización de $\mathfrak{p}$ en la extensión local $K_{\mathfrak{P}_i}/k_\mathfrak{p}$ y con su extensión de cuerpos de restos correspondiente. Además, el teorema 2.34 nos da que el grado global n es la suma de los grados locales:

$$n = n_{\mathfrak{P}_1} + \cdots + n_{\mathfrak{P}_r}.$$

Ejemplos Veamos algunas aplicaciones de estos hechos:

> *Sea $p \in \mathbb{Z}$ un primo impar y sea $m \in \mathbb{Z}$ tal que $p \nmid m$. Entonces m es un cuadrado en $\mathbb{Q}_p$ si y sólo si es un resto cuadrático módulo p.*

En efecto, una implicación es inmediata: si $m = \delta^2$, entonces $\delta \in \mathbb{Z}_p$, pues es raíz del polinomio $X^2 - m \in \mathbb{Z}_p[X]$ y $\mathbb{Z}_p$ es íntegramente cerrado. Como $\mathbb{Z}_p/(p) \cong \mathbb{Z}/p\mathbb{Z}$, existe un $r \in \mathbb{Z}$ tal que $\delta \equiv r \pmod p$, luego $m \equiv r^2 \pmod p$, en principio en $\mathbb{Z}_p$, pero el isomorfismo entre los cuerpos de restos implica que lo mismo vale en $\mathbb{Z}$.

Recíprocamente, si m es un resto cuadrático módulo p, podemos expresarlo como $m = s^2 d$, donde d es libre de cuadrados (pero es igualmente un resto cuadrático módulo p). Podemos suponer que $d \neq 1$. Consideremos entonces la extensión $\mathbb{Q}\big(\sqrt{d}\,\big)/\mathbb{Q}$, en la cual, según lo visto en la sección 2.3 sobre factorización ideal en cuerpos cuadráticos, $p = \mathfrak{P}_1\mathfrak{P}_2$, con $e(\mathfrak{P}_i/p) = f(\mathfrak{P}_i/p) = 1$, luego $n(\mathfrak{P}_i/p) = 1$, luego $\mathbb{Q}[\sqrt{d}]_{\mathfrak{P}_1} = \mathbb{Q}_p$ y $\sqrt{m} = s\sqrt{d} \in \mathbb{Q}_p$. ∎

En particular vemos que existe $\sqrt{2} \in \mathbb{Q}_7$, tal y como habíamos afirmado.

Más aún, si m es un resto cuadrático módulo p, tenemos que $\sqrt{m} \in \mathbb{Q}_p$, y de hecho $\sqrt{m} \in \mathbb{Z}_p$, por lo que, para cada natural $n \geq 1$, existe un $s \in \mathbb{Z}$ tal que $\sqrt{m} \equiv s \pmod{p^n}$ (ya que $\mathbb{Z}_p/(p^n) \cong \mathbb{Z}/p^n\mathbb{Z}$), luego $m \equiv s^2 \pmod{p^n}$, y así vemos que todo cuadrado módulo p es un cuadrado módulo p^n, como también habíamos afirmado.

> *Si p y q son primos distintos, los cuerpos $\mathbb{Q}_p$ y $\mathbb{Q}_q$ no son isomorfos.*

En efecto, basta tomar a un resto cuadrático módulo p y b un resto no cuadrático módulo q. Luego tomamos $c \equiv a \pmod p$, $c \equiv b \pmod q$, de modo que c tiene raíz cuadrada en $\mathbb{Q}_p$ pero no en $\mathbb{Q}_q$. ∎

Observemos que 2 es un resto cuadrático módulo 7, pero la descomposición de 7 en $\mathbb{Q}(\sqrt{2})$ es $2 = \mathfrak{p}^2$, por lo que $|\mathbb{Q}(\sqrt{7})_{\mathfrak{p}} : \mathbb{Q}_2| = 2$. De aquí no podemos deducir si $\sqrt{7} \in \mathbb{Q}_2$, pues podría ocurrir que $\mathbb{Q}_2[\sqrt{7}] = \mathbb{Q}_2 \subsetneq \mathbb{Q}(\sqrt{7})_{\mathfrak{p}}$.

En la sección siguiente veremos que, en realidad, esto es imposible, pues, en general, se cumple que si $K = \mathbb{Q}(A)$, entonces $K_{\mathfrak{p}} = \mathbb{Q}_p(A)$. Para obtener resultados de este tipo necesitamos estudiar primero las extensiones de cuerpos métricos completos.

5.3 Extensiones de cuerpos métricos completos

Vamos a abordar aquí parcialmente el problema de cuándo un valor absoluto en un cuerpo métrico completo se extiende a una extensión del cuerpo. En primer lugar observamos que para extensiones algebraicas la extensión, si existe, es única:

Teorema 5.23 *Sea k un cuerpo métrico completo y sea K una extensión finita de k. Si un valor absoluto de k admite una extensión a K entonces dicha extensión es única y, concretamente, viene dada por*

$$|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}, \qquad \textit{para todo } \alpha \in L,$$

donde $\mathrm{N} : K \longrightarrow k$ es la norma de la extensión y n es su grado. Además K es un cuerpo métrico completo con dicho valor absoluto.

Demostración: Si $|\ |_1$ y $|\ |_2$ son dos valores absolutos en K que extienden al de k entonces podemos considerarlos como dos normas en K como k-espacio vectorial (definición [An 2.1]). Por el teorema [An 3.32] son equivalentes y K es completo con cualquiera de ellas. En particular inducen la misma topología en K, luego son equivalentes como valores absolutos, luego uno es una potencia del otro, pero, como coinciden en k, el exponente ha de ser 1, luego son iguales.

Sea, pues, $|\ |$ la única extensión a K del valor absoluto de k. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una k-base de K. Si $\alpha \in K$ se expresa como

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n, \qquad \text{con } x_1, \ldots, x_n \in k,$$

el teorema [An 2.3] implica que la aplicación

$$\|\alpha\| = \max_{1 \le i \le n} |x_i|$$

es una norma en K, que según ya hemos señalado, será equivalente al valor absoluto de K.

Tomemos un $\alpha \in K$ tal que $|\alpha| < 1$. Entonces la sucesión $\{\alpha^m\}$ tiende a 0 (para el valor absoluto y, por lo tanto, para la norma). Sea

$$\alpha^m = x_{m1}\alpha_1 + \cdots + x_{mn}\alpha_n, \qquad \text{con } x_{mj} \in k.$$

La convergencia en norma implica que las sucesiones $\{x_{mj}\}_m$ tienden a 0 (respecto al valor absoluto de k).

Notemos que $N(x_{m1}\alpha_1 + \cdots + x_{mn}\alpha_n)$ se calcula como producto de n polinomios homogéneos lineales en las variables $x_1, \ldots, x_n$. No es difícil ver que sus coeficientes están en k, luego concluimos[3] que $\{N(\alpha^m)\}$ converge a 0 en k.

Como $\mathrm{N}(\alpha^m) = \mathrm{N}(\alpha)^m$, concluimos que $|\mathrm{N}(\alpha)| < 1$. Tomando inversos deducimos que si $|\alpha| > 1$ entonces $|\mathrm{N}(\alpha)| > 1$. Por lo tanto $|\alpha| = 1$ si y sólo si $|\mathrm{N}(\alpha)| = 1$.

Ahora, si $\alpha \in k$ es no nulo, tenemos $\mathrm{N}(\alpha^n/\mathrm{N}(\alpha)) = 1$, luego $|\alpha^n/\mathrm{N}(\alpha)| = 1$ y así $|\alpha|^n = |\mathrm{N}(\alpha)|$. Como $|\alpha| > 0$ podemos tomar raíces n-simas. ∎

Notemos que el teorema anterior no garantiza que $|\alpha| = \sqrt[n]{|\mathrm{N}(\alpha)|}$ defina realmente un valor absoluto en k. Sólo afirma que si el valor absoluto se puede extender, la extensión tiene que venir dada por esta fórmula. Es fácil probar que esta función cumple las propiedades 1) y 3) de la definición de valor absoluto, pero en principio la segunda podría fallar.

En realidad no es así. En A.6 probaremos que la fórmula del teorema anterior siempre define un valor absoluto en K. Aquí, mediante un argumento mucho más simple, lo probaremos únicamente en el caso en que el valor absoluto de k es discreto y la extensión K/k es separable. En primer lugar veamos lo que podemos añadir al teorema anterior si suponemos que el valor absoluto de partida es discreto:

Teorema 5.24 *Sea k un cuerpo métrico discreto completo y sea K una extensión finita de k tal que un valor absoluto de k admita una extensión a K. Entonces:*

1. *La extensión a K del valor absoluto de k está inducida por una valoración v tal que la valoración de k es $v/e|_{k^*}$, para cierto número natural $e \geq 1$. Por lo tanto, K es un cuerpo métrico discreto completo.*
2. *La extensión de cuerpos de restos $\overline{K}/\overline{k}$ es finita.*
3. *Si $|\overline{K} : \overline{k}| = f$, entonces se cumple la relación $n = ef$.*
4. *Si D y E son los anillos de enteros de k y K, respectivamente, entonces E es un D-módulo libre de rango n.*
5. *Si el valor absoluto de k se extiende a la clausura normal de K sobre k, entonces E es la clausura entera de D, por lo que E/D es una extensión de dominios de Dedekind.*

Demostración: Sea v^* la valoración de k y sea $|\alpha| = r^{v^*(\alpha)}$, con $0 < r < 1$, el valor absoluto en k que admite una extensión a K. Por el teorema anterior sabemos que dicha extensión es $|\alpha| = \sqrt[n]{|\mathrm{N}(\alpha)|}$.

La imagen de k^* por el valor absoluto es el subgrupo cíclico de $\mathbb{R}^*$ generado por r. La imagen de K^* por la norma es un subgrupo de k^*, y la imagen de éste por el valor absoluto de k es un subgrupo de $\langle r\rangle$, luego será de la forma $\langle r^f\rangle$,

[3]Alternativamente, los coeficientes están en una extensión finita de k, las sucesiones $\{x_{mj}\}_m$ tienden a 0 respecto a la norma en dicha extensión, luego la sucesión $\{N(\alpha^m)\}$ converge a 0 en dicha extensión y, al estar en k, converge a 0 en k.

para un cierto natural no nulo f. Las raíces n-simas de los elementos de este grupo forman el grupo $\langle r^{f/n}\rangle$. Así pues, para cada $\alpha \in K^*$ existe un único entero $v(\alpha)$ tal que $|\alpha| = r^{(f/n)v(\alpha)}$. Equivalentemente,

$$v(\alpha) = \frac{n \log |\alpha|}{f \log r}.$$

Es fácil ver que v es una valoración en K que induce su valor absoluto. También es claro que si $\alpha \in k^*$ entonces $v(\alpha) = ev^*(\alpha)$, donde $e = n/f$. Tomando un $\alpha \in k^*$ tal que $v^*(\alpha) = 1$ concluimos que e es un número natural. Más aún, si π es un primo en K y ρ es un primo en k (es decir, $v(\pi) = 1$ y $v^*(\rho) = 1$), tenemos que $|\rho| = |\pi|^e$. Esto termina la prueba de 1).

Sea π un primo en K y sea $\{[\omega_1], \ldots, [\omega_f]\}$ un conjunto $\overline{k}$-linealmente independiente en $\overline{K}$ (donde f es arbitrario). Veamos que $\omega_i \pi^j$, para $i = 1, \ldots, f$, $j = 0, \ldots, e-1$ son k-linealmente independientes en K. Consideremos una combinación lineal

$$\sum_{i,j} c_{ij}\, \omega_i\, \pi^j, \qquad \text{con } c_{ij} \in k.$$

Fijado j, supongamos que algún coeficiente c_{ij} es no nulo. Reordenándolos podemos suponer que $c_{1j} \neq 0$ es el coeficiente con mayor valor absoluto. Entonces

$$\Big|\sum_i c_{ij}\, \omega_i\Big| = |c_{1j}| \left|\omega_1 + \frac{c_{2j}}{c_{1j}}\, \omega_2 + \cdots + \frac{c_{fj}}{c_{1j}}\, \omega_f\right|.$$

Todos los coeficientes de la última combinación lineal son enteros, luego podemos tomar clases módulo el primo de K. Como el coeficiente de $[\omega_1]$ es 1, concluimos que toda la combinación lineal es no nula, es decir, que no está en el ideal primo de K (pero es entera), luego es una unidad y tiene valor absoluto 1. En definitiva (y teniendo en cuenta la reordenación que hemos hecho)

$$\Big|\sum_i c_{ij}\, \omega_i\Big| = \text{máx}_i\, |c_{ij}|.$$

Obviamente, si todos los coeficientes fueran nulos esta igualdad se sigue cumpliendo. Por lo tanto

$$\Big|\sum_i c_{ij}\, \omega_i\, \pi^j\Big| = |\pi|^j\ \text{máx}_i\, |c_{ij}|.$$

La imagen de K^* por el valor absoluto es el subgrupo $G_K = \langle|\pi|\rangle$ de $\mathbb{R}^*$, mientras que la imagen de k^* es el subgrupo $G_k = \langle|\pi|^e\rangle$. Claramente, las potencias $|\pi|^j$, para $j = 0, \ldots, e-1$, son representantes de las e clases del cociente G_K/G_k, luego los miembros derechos de la igualdad anterior son representantes de esas mismas clases. En particular son distintos dos a dos, luego la desigualdad triangular no arquimediana para su suma es de hecho una igualdad:

$$\Big|\sum_{i,j} c_{ij}\, \omega_i\, \pi^j\Big| = \text{máx}_j \Big|\sum_i c_{ij}\, \omega_i\, \pi^j\Big| = \text{máx}_{i,j}\, |c_{ij}|\, |\pi|^j. \tag{5.2}$$

Ahora es claro que los elementos $\omega_i\,\pi^j$ son linealmente independientes (en particular distintos dos a dos), pues si el miembro izquierdo es nulo el miembro derecho muestra que todos los c_{ij} son nulos.

En particular esto prueba que la extensión de cuerpos de restos $\overline{K}/\overline{k}$ es finita y tenemos probado 2).

Supongamos ahora que $[\omega_1],\dots,[\omega_f]$ son una $\overline{k}$-base de $\overline{K}$ y veamos que los elementos $\omega_i\,\pi^j$ son una k-base de K. Esto probará la relación $n = ef$.

Aplicaremos 5.18. Para cada entero n sea $n = ke + r$, con $0 \le r < e$. Definimos $\pi_n = \rho^k\pi^r$. De este modo $v^*(\pi_n) = n$. Sea A un conjunto de representantes de las clases de $\overline{K}$ formado por combinaciones lineales de $\omega_1,\dots,\omega_f$ con coeficientes en k (enteros). Según el teorema 5.18 todo $\alpha \in K$ se expresa en la forma

$$\alpha = \sum_{n=s}^{+\infty} x_n\pi_n, \qquad \text{con } x_n \in A, \quad s \in \mathbb{Z}.$$

Equivalentemente[4]

$$\alpha = \sum_{n=s}^{+\infty}\sum_{r=0}^{e-1}\left(\sum_{i=1}^{f} a_{kri}\,\omega_i\right)\rho^k\pi^r = \sum_{r=0}^{e-1}\sum_{i=1}^{f}\left(\sum_{k=s}^{+\infty} a_{kri}\,\rho^k\right)\omega_i\,\pi^r.$$

Esto prueba que los elementos $\omega_i\,\pi^j$ son ciertamente una k-base de K y así tenemos 3).

Más aún, vamos a ver que los enteros de K son exactamente los elementos con coordenadas enteras en esta base, lo que probará 4). Obviamente los elementos con coordenadas enteras son enteros. Supongamos ahora que

$$\alpha = \sum_{i,j} c_{ij}\,\omega_i\,\pi^j, \qquad |\alpha| \le 1.$$

La igualdad (5.2) prueba que $|c_{ij}\pi^j| \le 1$, luego

$$|c_{ij}| \le |\pi|^{-j} < |\pi|^{-e} = |\rho|^{-1}.$$

Equivalentemente, $v(c_{ij}) > -v(\rho) = -1$, luego $v(c_{ij}) \ge 0$ y así cada c_{ij} es entero.

Veamos finalmente 5). Dado un entero $\alpha \in K$, la clausura normal de K sobre k contiene a todos los conjugados de α. La unicidad de la extensión del valor absoluto dada por el teorema anterior hace que los k-isomorfismos de L sean isometrías, por lo que todos los conjugados de α tienen valor absoluto menor o igual que 1, es decir, son enteros. Por consiguiente lo mismo vale para los coeficientes del polinomio mínimo de α, que son, por tanto, enteros de k. Así pues, α es entero sobre el anillo de los enteros de k.

[4]Véase la sección 5.6, más abajo, para la justificación de estas manipulaciones de series en cuerpos no arquimedianos.

Recíprocamente, si $\alpha \in K$ es entero sobre el anillo de enteros de k, en particular es entero sobre el anillo de enteros de K, que es íntegramente cerrado, por ser un dominio de ideales principales, luego α es un entero de K. ∎

Nota Admitiendo 5), los apartados 2) y 3) del teorema anterior son triviales, pues e y f son simplemente el índice de ramificación y el grado de inercia de los (únicos) primos de D y E, pero lo relevante es que en la prueba hemos construido explícitamente una base de E sobre D: hemos visto que si π es un primo en K y $\{[\omega_1], \ldots, [\omega_f]\}$ es una $\overline{k}$-base de $\overline{K}$ entonces los elementos $\omega_i\, \pi^j$ son una k-base de K. ∎

Ahora probamos la existencia de extensiones de valores absolutos a las extensiones separables:

Teorema 5.25 *Sea k un cuerpo métrico discreto completo.*

1. *Cada valor absoluto de k se extiende de forma única a cada una de sus extensiones separables.*

2. *Si K es una extensión finita separable de k, entonces la extensión de cualquier valor absoluto de k está inducida por una valoración con la que K resulta ser un cuerpo métrico discreto completo. Los anillos de enteros forman una extensión separable de dominios de Dedekind.*

3. *Cualquier k-isomorfismo entre dos extensiones separables de k es una isometría respecto a las extensiones de un mismo valor absoluto de k.*

Demostración: Sea D el anillo de los enteros de k. Si K es cualquier extensión finita separable de k, entonces la clausura entera E de D en K es un dominio de Dedekind que extiende a D (teorema 2.26). Si $\mathfrak{P}$ es un primo de E (que dividirá al único primo $\mathfrak{p}$ de D), el teorema 5.19 nos da que cada valor absoluto de k se extiende a un valor absoluto en K inducido por la valoración asociada a $\mathfrak{P}$. El teorema anterior nos da que la extensión es única, de donde se sigue que $\mathfrak{P}$ es el único primo de E (dos primos distintos darían lugar a dos extensiones distintas). Así pues E es un anillo local, luego es el anillo de enteros de la valoración inducida por su único primo $\mathfrak{P}$. Por el teorema anterior K es completo, y así queda probado 2).

Fijemos un valor absoluto $|\ |_k$ en k. Si K es una extensión separable de k, entonces sobre cada extensión finita intermedia L hay una única extensión del valor absoluto de k, llamémosla $|\ |_L$. Es claro que si $k \subset L \subset N \subset K$ entonces $|\ |_N$ extiende a $|\ |_L$.

Para cada $\alpha \in K$, la extensión $k(\alpha)/k$ es finita separable, y podemos definir $|\alpha| = |\alpha|_{k(\alpha)}$. Por la unicidad es claro que si $L \subset K$ es cualquier extensión finita de k y $\alpha \in L$ entonces $|\alpha| = |\alpha|_L$. De aquí se sigue inmediatamente que $|\ |$ es un valor absoluto sobre K que extiende al valor absoluto de k. La extensión es única pues, si tuviéramos dos, coincidirían sobre todas las extensiones finitas de k, luego sobre todos los elementos de K. Esto prueba 1).

Si $\sigma : K \longrightarrow L$ es un k-isomorfismo entre dos extensiones algebraicas de k, entonces es claro que $|\alpha|^* = |\sigma(\alpha)|$ es un valor absoluto en K que extiende al de k, luego por la unicidad es precisamente el valor absoluto de K, y por tanto $|\alpha| = |\sigma(\alpha)|$ para todo $\alpha \in K$, es decir, σ es una isometría. ∎

La parte principal de este teorema puede expresarse estrictamente en términos de cuerpos métricos, es decir, en función de sus topologías y no de sus valores absolutos:

Teorema 5.26 *Sea k un cuerpo métrico discreto completo y K una extensión separable de k. Entonces K admite una única topología de cuerpo métrico que induce la topología de k. Si la extensión es finita entonces K es discreto y completo. Cualquier k-isomorfismo entre dos extensiones separables de k es un isomorfismo topológico.*

Demostración: Sea D el anillo de enteros de k y $\mathfrak{p}$ su único primo. Si la extensión K/k es finita, y E es la clausura entera de D en K, entonces el teorema anterior nos da que E es un dominio de Dedekind con un único primo $\mathfrak{P}$. Puesto que obviamente $\mathfrak{P} \mid \mathfrak{p}$, por el teorema 5.19 cada valor absoluto de k se extiende a un valor absoluto de K asociado a $\mathfrak{P}$, y por el teorema anterior la extensión es única.

Cualquier valor absoluto en K que induzca la topología de k es extensión de un valor absoluto de $\mathfrak{p}$, luego es uno de los valores absolutos de $\mathfrak{P}$ y por consiguiente induce la topología $\mathfrak{P}$-ádica. Por el teorema anterior K es discreto y completo.

Si la extensión K/k no es finita basta observar que un valor absoluto en K está completamente determinado por su restricción a las extensiones finitas de k. La afirmación sobre los k-isomorfismos se sigue inmediatamente del teorema anterior. ∎

Ahora ya podemos demostrar el resultado que habíamos anticipado al final de la sección precedente.

Notemos que los cuerpos numéricos son perfectos, por lo que al aplicarles el teorema anterior podemos sustituir "extensión separable" por "extensión algebraica".

Teorema 5.27 *Sea K/k una extensión de cuerpos numéricos, sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{p}$ un primo en D y sea $\mathfrak{P}$ un primo en E que lo divida.*

1. *Si $K = k(A)$, para cierto conjunto $A \subset K$, entonces $K_{\mathfrak{P}} = k_{\mathfrak{p}}(A)$.*
2. *En particular $K_{\mathfrak{P}} = k_{\mathfrak{p}}K$.*
3. *Si la extensión K/k es de Galois, la extensión $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ también lo es.*

Demostración: 1) Podemos suponer que A es finito. Entonces tenemos $k_{\mathfrak{p}} \subset k_{\mathfrak{p}}(A) \subset K_{\mathfrak{P}}$, y la extensión $k_{\mathfrak{p}}(A)/k_{\mathfrak{p}}$ es finita, luego por el teorema 5.26

el cuerpo $k_\mathfrak{p}(A)$ es completo, luego es cerrado en $K_\mathfrak{P}$. Por otra parte $K \subset k_\mathfrak{p}(A)$ y K es denso en $K_\mathfrak{P}$, luego ha de ser $K_\mathfrak{P} = k_\mathfrak{p}(A)$.

2) es inmediato a partir de 1).

3) Si K/k es una extensión de Galois entonces $K = k(A)$, donde A es el conjunto de las raíces de un polinomio de $k[x]$, y como $K_\mathfrak{P} = k_\mathfrak{P}(A)$ la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ también es de Galois. ∎

Ejemplo *Si m es un número impar, entonces se cumple que $\sqrt{m} \in \mathbb{Q}_2$ si y sólo si $m \equiv 1$ (mód 8).*

En efecto, no perdemos generalidad si suponemos que m es libre de cuadrados. Entonces, por el teorema anterior, la condición $\sqrt{m} \in \mathbb{Q}_2$ equivale a que $\mathbb{Q}_2(\sqrt{m}) = \mathbb{Q}\big(\sqrt{m}\,\big)_\mathfrak{p} = \mathbb{Q}_2$, donde $\mathfrak{p}$ es un divisor de 2 en $\mathbb{Q}\big(\sqrt{m}\,\big)$, lo cual equivale a que $e(\mathfrak{p}/2) = f(\mathfrak{p}/2) = 1$ y, según hemos visto al estudiar la factorización en cuerpos cuadráticos, esto sucede precisamente cuando $p \equiv 1$ (mód 8). ∎

Definición 5.28 En lo sucesivo, para cada primo $\mathfrak{p}$ de un cuerpo numérico k fijaremos una clausura algebraica $\mathbb{K}_\mathfrak{p}$ del cuerpo $\mathfrak{p}$-ádico $k_\mathfrak{p}$. Según 5.25 el valor absoluto canónico de $k_\mathfrak{p}$ se extiende de forma única a $\mathbb{K}_\mathfrak{p}$. Representaremos esta extensión por $|\ |_\mathfrak{p}$ y la llamaremos *valor absoluto canónico* de $\mathbb{K}_\mathfrak{p}$. Dicho teorema implica también que todo $k_\mathfrak{p}$-isomorfismo entre dos extensiones algebraicas de $k_\mathfrak{p}$ (contenidas en $\mathbb{K}_\mathfrak{p}$) es una isometría respecto al valor absoluto canónico.

Observemos que si p es el primo racional al que divide $\mathfrak{p}$, entonces $k_\mathfrak{p}$ es una extensión finita de $\mathbb{Q}_p$, luego $\mathbb{K}_\mathfrak{p}$ es también una clausura algebraica de $\mathbb{Q}_p$, es decir, $\mathbb{K}_\mathfrak{p}$ es topológicamente isomorfo a $\mathbb{K}_p$ (e isométrico respecto a los valores absolutos canónicos). De este modo, para cuestiones puramente algebraicas es suficiente tratar con los cuerpos $\mathbb{K}_p$, pero debemos tener presente que si $\mathfrak{p}$ y $\mathfrak{q}$ son dos divisores de p en un mismo cuerpo métrico k, entonces la isometría entre $\mathbb{K}_\mathfrak{p}$ y $\mathbb{K}_\mathfrak{q}$ no es la identidad sobre k, (o de lo contrario $|\ |_\mathfrak{p}$ y $|\ |_\mathfrak{q}$ serían el mismo valor absoluto), por lo que no podemos identificar ambos cuerpos a ciertos efectos. En particular no podemos identificar ambos con $\mathbb{K}_p$.

Notemos que el criterio de irreducibilidad de Eisenstein es aplicable al anillo de enteros de $\mathbb{Q}_p$, lo que nos da polinomios irreducibles en $\mathbb{Q}_p[x]$ de grado arbitrariamente grande. Por consiguiente $\mathbb{K}_p$ tiene grado infinito sobre $\mathbb{Q}_p$.

Ahora probaremos un sencillo resultado técnico que nos será útil en varias ocasiones más adelante. De momento lo usaremos para probar, entre otras cosas, que la clausura algebraica de $\mathbb{Q}$ es densa en $\mathbb{K}_p$.

La prueba de este teorema y los siguientes se basa en el teorema 5.25, que tenemos probado para cuerpos métricos discretos completos, aunque ya comentamos que vale en realidad para cuerpos métricos completos arbitrarios. Admitiendo esto, las demostraciones que veremos a continuación son válidas para cuerpos métricos completos no arquimedianos cualesquiera.

Teorema 5.29 (Lema de Krasnel) *Sea k un cuerpo métrico discreto completo y sean α y β dos elementos de su clausura separable K. Supongamos que para todo k-monomorfismo $\sigma : k(\alpha) \longrightarrow K$ distinto de la identidad se cumple $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. Entonces $k(\alpha) \subset k(\beta)$.*

DEMOSTRACIÓN: Se entiende que el valor absoluto que aparece en el enunciado es la extensión a K de cualquier valor absoluto en k (cuya existencia está garantizada por el teorema 5.25).

Basta ver que todo $k(\beta)$-monomorfismo $\tau : k(\alpha, \beta) \longrightarrow K$ fija a α. El teorema 5.25 nos da que τ es una isometría, luego $|\tau(\beta-\alpha)| = |\beta-\alpha|$. Entonces

$$|\tau(\alpha)-\alpha| = |\tau(\alpha)-\beta+\beta-\alpha| \leq \text{máx}\big\{|\tau(\alpha-\beta)|, |\beta-\alpha|\big\} = |\beta-\alpha| < |\sigma(\alpha)-\alpha|$$

para todo $\sigma : k(\alpha) \longrightarrow K$ distinto de la identidad, luego τ ha de ser la identidad en $k(\alpha)$. ∎

Geométricamente, el teorema anterior afirma que, si α es separable sobre k, entonces $k(\alpha)$ está contenido en cualquier extensión de k que contenga a un punto de una bola de centro α en la clausura separable de k que no contenga a ningún conjugado de α aparte de a él mismo. Con esto podemos probar una especie de continuidad de las raíces de un polinomio respecto de sus coeficientes.

Si k es un cuerpo métrico discreto completo y fijamos en él un valor absoluto, para cada polinomio $g \in k[x]$ definimos $\|g\|$ como el máximo de los valores absolutos de sus coeficientes. Es claro que esta aplicación es una norma en $k[x]$.

Teorema 5.30 *Sea k un cuerpo métrico discreto completo. Para cada polinomio $f(x) \in k[x]$ mónico irreducible separable de grado n, existe un $\delta > 0$ tal que si $g(x) \in k[x]$ es mónico de grado n y $\|f - g\| < \delta$, entonces g es irreducible en $k[x]$ y cada raíz α de f (en una clausura algebraica fija de k) se corresponde biunívocamente con una raíz β de g de modo que $k(\alpha) = k(\beta)$.*

DEMOSTRACIÓN: Sea C una clausura separable de k. Entonces sobre C tenemos definido un único valor absoluto que extiende al de k. Si $g \in k[x]$ es un polinomio mónico de grado n, podemos expresarlo en la forma

$$g(x) = x^n(1 + a_{n-1}x^{-1} + \cdots + a_1x_1^{-n} + a_0x^{-n}).$$

Así queda claro que si un $x \in C$ cumple $|x| \geq 2\|g\|$ entonces

$$|a_{n-1}x^{-1} + \cdots + a_1x_1^{-n} + a_0x^{-n}| \leq 1/2,$$

$$|1 + a_{n-1}x^{-1} + \cdots + a_1x_1^{-n} + a_0x^{-n}| \geq 1/2,$$

de donde $|g(x)| \geq 1$. En particular toda raíz de g en C ha de cumplir $|\alpha| < 2\|g\|$.

Fijemos un polinomio $f \in k[x]$ mónico separable de grado n. Para todo polinomio g mónico y de grado n y todo $\alpha \in C$, tomando M tal que $M > 1$, $M > |\alpha|$ tenemos que $|f(\alpha) - g(\alpha)| \leq \|f - g\|M^n$.

De aquí se sigue que si una sucesión de polinomios mónicos de grado n converge a f en norma, entonces converge puntualmente a f. En particular, si α es una raíz de g en C, se cumple

$$|f(\alpha)| = |f(\alpha) - g(\alpha)| \leq \|f - g\|(2\|g\|)^n \leq 2^n\|f - g\|(\|f - g\| + \|f\|),$$

y de aquí deducimos que para todo $\epsilon > 0$ existe un $\delta > 0$ tal que si g es un polinomio mónico de grado n con $\|f - g\| < \delta$, entonces $|f(\alpha)| < \epsilon^n$ para toda raíz α de g en C.

Descomponiendo f en producto de factores lineales es claro que si un $\alpha \in C$ dista de cada raíz de f más que ϵ, entonces $|f(x)| \geq \epsilon^n$. Reuniendo lo dicho concluimos que para cada $\epsilon > 0$ existe un $\delta > 0$ tal que si g es un polinomio mónico de grado n con $\|f - g\| < \delta$ entonces cada raíz de g en C dista menos de ϵ de una raíz de f.

Más aún, tomando δ suficientemente pequeño podemos asegurar que, fijada una raíz β de f, todo polinomio g mónico de grado n tal que $\|f - g\| < \delta$ tiene una raíz en C que dista de β menos que ϵ. En efecto, en caso contrario existiría una sucesión de polinomios mónicos de grado n, digamos $\{g_i\}$, que convergería a f en norma y de modo que las raíces de cada g_i en C se acercaran a las restantes raíces de f, pero eso implicaría que el valor absoluto de $g_i(x)$ estaría acotado inferiormente en un entorno de β, mientras que por otra parte $g_i(\beta)$ debería tender a 0.

Ahora supongamos que f es irreducible. Sea ϵ menor que la distancia entre dos cualesquiera de sus raíces. Sea $\delta > 0$ tal que si $\|f - g\| < \delta$ entonces las raíces de g en C distan menos que ϵ de las raíces de f. Por la elección de ϵ una misma raíz de g en C no puede distar menos que ϵ de dos raíces distintas de f, y como f tiene n raíces distintas, lo mismo le sucede a g y cada raíz β de g dista menos que ϵ de una única raíz α de f. En particular g es separable, y si α y β se corresponden en este sentido, $|\beta - \alpha| < \epsilon < |\gamma - \alpha|$, para cualquier otra raíz γ de f. El teorema anterior implica entonces que $k(\alpha) \subset k(\beta)$, pero como α es raíz de un polinomio irreducible de grado n, tenemos $|k(\alpha) : k| = n$, y como β es raíz de un polinomio de grado n, ha de ser $k(\alpha) = k(\beta)$, de donde se sigue que g es irreducible. ∎

Veamos algunas aplicaciones de estos teoremas. Llamaremos *cuerpos p-ádicos* a las extensiones finitas de $\mathbb{Q}_p$.

Teorema 5.31 *Sea K un cuerpo p-ádico. Entonces existe un cuerpo numérico $k \subset K$ tal que $|k : \mathbb{Q}| = |K : \mathbb{Q}_p|$ y k es denso en K.*

Demostración: Sea $K = \mathbb{Q}_p(\alpha)$. Basta aplicar el teorema anterior tomando como f el polinomio mínimo de α y como g un polinomio mónico con coeficientes racionales lo suficientemente cercano a f. Si β es una raíz de éste último (que está en K por el teorema anterior), definimos $k = \mathbb{Q}(\beta)$. ∎

En particular, tal y como afirmábamos, la clausura algebraica de $\mathbb{Q}$ es densa en $\mathbb{K}_p$. Las observaciones siguientes (hasta el final de la sección) no serán necesarias en el resto del libro.

Si k es un cuerpo numérico, su clausura en $\mathbb{Q}_p$ es $k\mathbb{Q}_p$, luego tiene grado finito sobre $\mathbb{Q}_p$. Esto implica que $\overline{k} \neq \mathbb{K}_p$ (pues hemos visto que la extensión $\mathbb{K}_p/\mathbb{Q}_p$ es infinita). El teorema anterior implica que $\mathbb{K}_p$ es la unión de las clausuras de los cuerpos numéricos, que son subcuerpos propios cerrados. Es fácil ver que todo subcuerpo propio de un cuerpo métrico tiene interior vacío,[5] luego el teorema de Baire implica que la clausura algebraica $\mathbb{K}_p$ no es completa. Por otra parte su compleción sigue siendo algebraicamente cerrada:

Teorema 5.32 *Sea k un cuerpo métrico discreto completo, sea $\mathbb{K}$ su clausura algebraica y $\overline{\mathbb{K}}$ su compleción. Entonces $\overline{\mathbb{K}}$ es algebraicamente cerrado.*

Demostración: En primer lugar probamos que $\overline{\mathbb{K}}$ es un cuerpo perfecto. Hemos de ver que si tiene característica prima p, entonces todos sus elementos tienen raíz p-ésima.

Ahora bien, cada $x \in \overline{\mathbb{K}}$ es el límite de una sucesión $\{x_n\}$ de elementos de $\mathbb{K}$, cada uno de los cuales tiene una (única) raíz p-ésima en $\mathbb{K}$, por ser éste algebraicamente cerrado. La sucesión $\{\sqrt[p]{x_n}\}$ es de Cauchy, pues

$$|\sqrt[p]{x_m} - \sqrt[p]{x_m}| = (|\sqrt[p]{x_m} - \sqrt[p]{x_m}|^p)^{1/p} = |x_m - x_n|^{1/p}.$$

Claramente $\lim_n \sqrt[p]{x_n}$ es una raíz p-ésima de x en $\overline{\mathbb{K}}$.

Sea ahora $f(x) \in \overline{\mathbb{K}}[x]$ un polinomio mónico irreducible. Según acabamos de probar, f es separable. Podemos aproximar sus coeficientes desde $\mathbb{K}$ y obtener así un polinomio $g(x) \in \mathbb{K}[x]$ mónico y del mismo grado al que podemos aplicar el teorema 5.30. Entonces $g(x)$ es irreducible (en $\overline{K}[x]$, luego también en $\mathbb{K}[x]$) luego tiene grado 1 y f también. ∎

5.4 Divisores primos

Cada ideal primo en un orden maximal de un cuerpo numérico K induce una valoración en K que convierte a éste en un cuerpo métrico discreto. Sin embargo, los cuerpos numéricos tienen otros valores absolutos no inducidos por primos (p. ej. el valor absoluto usual en $\mathbb{Q}$, que es arquimediano). Sucede que ciertos resultados se expresan de forma más simétrica y elegante si a los primos de un cuerpo numérico añadimos ciertos "primos infinitos", definidos por valores absolutos arquimedianos y los tratamos formalmente como si fueran ideales primos. Para concretar estas ideas comenzamos dando la siguiente definición:

Definición 5.33 Sea k un cuerpo. Llamaremos *divisores primos* de k a las clases de equivalencia de valores absolutos en k distintas de la clase del valor absoluto trivial.

[5] Si $K \subset L$ y K no tiene interior vacío, entonces contiene una bola de centro 0, lo cual significa que todo elemento de L de valor absoluto suficientemente pequeño está en K, pero tomando $\alpha \in K$ con $|\alpha| > 1$ vemos que, para todo $\beta \in L$ existe un n tal que $\beta/\alpha^n \in K$, luego $\beta \in K$, con lo que $K = L$.

Un divisor primo es *arquimediano* o *no arquimediano* si lo son los valores absolutos que lo componen. Un divisor primo es *discreto* si sus valores absolutos están inducidos por una valoración. Todo divisor discreto es no arquimediano.

Si K es un cuerpo numérico y D es su orden maximal, cada ideal primo $\mathfrak{p}$ de D determina una valoración $v_\mathfrak{p}$ en K, que a su vez determina un divisor primo de K que representaremos igualmente por $\mathfrak{p}$.

Notemos que si $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos distintos de D y $|\ |_\mathfrak{p}$, $|\ |_\mathfrak{q}$, son valores absolutos inducidos por ellos en k, éstos no son equivalentes, pues si $\alpha \in \mathfrak{p} \setminus \mathfrak{q}$ y $\beta \in \mathfrak{q} \setminus \mathfrak{p}$ se cumple que $v_\mathfrak{p}(\alpha) \geq 1$, $v_\mathfrak{p}(\beta) = 0$, $v_\mathfrak{q}(\beta) \geq 1$, $v_\mathfrak{q}(\alpha) = 0$, luego

$$|\alpha|_\mathfrak{p} < 1 = |\beta|_\mathfrak{p}, \qquad |\beta|_\mathfrak{q} < 1 = |\alpha|_\mathfrak{q}.$$

Así pues, ideales primos distintos inducen divisores primos distintos y podemos considerar que el conjunto de los divisores primos de k contiene a los ideales primos de D.

Según comentábamos, hemos introducido la noción de "divisor primo" para añadir primos infinitos al conjunto de los ideales primos de un cuerpo numérico. Los primos que nos faltan son los inducidos por los valores absolutos siguientes:

Definición 5.34 Sea k un cuerpo numérico y $\sigma : k \longrightarrow \mathbb{C}$ un monomorfismo. Definimos el valor absoluto en k dado por

$$|\alpha|_\sigma = |\sigma(\alpha)|,$$

donde el valor absoluto del segundo miembro es el usual en $\mathbb{C}$.

Obviamente $|\ |_\sigma$ es un valor absoluto arquimediano en k. Ahora hemos de determinar si dos de ellos pueden ser equivalentes. La respuesta es que sí, pero sólo en un caso muy concreto:

Teorema 5.35 *Sea k un cuerpo numérico y sean $\sigma, \tau : k \longrightarrow \mathbb{C}$ dos monomorfismos. Entonces σ y τ inducen valores absolutos equivalentes en k si y sólo si $\sigma = \tau$ o bien $\sigma = \overline{\tau}$ (la composición de τ con la conjugación compleja).*

DEMOSTRACIÓN: Si σ y τ inducen valores absolutos equivalentes, entonces ambos dan lugar a la misma compleción K de k. Por otro lado, las clausuras $\overline{\sigma[k]}$ y $\overline{\tau[k]}$ son compleciones de $\sigma[k]$ y $\tau[k]$ respectivamente. Consecuentemente σ y τ se extienden a isomorfismos topológicos $\sigma : K \longrightarrow \overline{\sigma[k]}$ y $\tau : K \longrightarrow \overline{\tau[k]}$.

Ahora observamos que $\overline{\sigma[k]}$ y $\overline{\sigma[k]}$ son subcuerpos cerrados de $\mathbb{C}$ que contienen a $\mathbb{Q}$, luego a $\mathbb{R}$. Tienen que ser concretamente $\mathbb{R}$ o $\mathbb{C}$, y como $\tau^{-1} \circ \sigma$ es un isomorfismo entre ellos, tienen que ser iguales y $\tau^{-1} \circ \sigma$ es un $\mathbb{R}$-automorfismo entre ellos (es un automorfismo continuo que fija a $\mathbb{Q}$, luego por continuidad fija a $\mathbb{R}$).

Por consiguiente, $\tau^{-1} \circ \sigma$ es la identidad en $\mathbb{R}$, la identidad en $\mathbb{C}$ o bien la conjugación en $\mathbb{C}$. En cualquier caso $\sigma = \tau$ o bien $\sigma = \overline{\tau}$. Restringiendo a k tenemos la conclusión. ∎

Notemos que si $\sigma = \overline{\tau}$, entonces los valores absolutos que inducen no sólo son equivalentes, sino que de hecho son iguales.

Definición 5.36 Siguiendo la notación usual introducida en 3.1, si k es un cuerpo numérico de grado n llamaremos $\sigma_1, \dots, \sigma_s : k \longrightarrow \mathbb{R}$ a sus monomorfismos reales y $\sigma_{s+1}, \overline{\sigma}_{s+1}, \dots, \sigma_{s+t}, \overline{\sigma}_{s+t} : k \longrightarrow \mathbb{C}$ a sus monomorfismos complejos. De este modo $n = s + 2t$ y llamamos $r = s + t$.

Según el teorema anterior, los r valores absolutos arquimedianos inducidos por $\sigma_1, \dots, \sigma_r$ son no equivalentes dos a dos, luego inducen r divisores primos arquimedianos distintos en k. Los llamaremos *divisores primos infinitos* de k. Por oposición, los divisores primos inducidos por los ideales primos del orden maximal de k serán los *divisores primos finitos* de k. Un primo infinito de un cuerpo numérico es *real* o *complejo* según si está inducido por un monomorfismo real o complejo.

Así, por ejemplo, $\mathbb{Q}$ tiene un único primo arquimediano (real), correspondiente a la inclusión $\mathbb{Q} \longrightarrow \mathbb{R}$, y que representaremos por ∞.

En lo sucesivo, cuando hablemos de *divisores primos* de un cuerpo numérico sobrentenderemos que nos referimos únicamente a divisores de uno de estos tipos: o los divisores finitos inducidos por ideales o los divisores infinitos inducidos por monomorfismos. Al final de este capítulo (teorema 5.60) probamos que en realidad éstos son todos los divisores del cuerpo, pero nunca necesitaremos este hecho, sino que nos bastará con el convenio de que no hablamos de ningún otro posible divisor.

Observemos que en el contexto de los cuerpos numéricos "divisor primo finito" es sinónimo de "divisor primo no arquimediano" o "divisor primo discreto", mientras que "divisor primo infinito" es sinónimo de "divisor primo arquimediano". A menudo diremos únicamente "primo", en vez de "divisor primo".

Podemos tomar como *valor absoluto canónico* para un divisor primo arquimediano $\mathfrak{p}$ de un cuerpo numérico al dado por la definición 5.34. Lo representaremos por $|\ |_\mathfrak{p}$. Observemos que si σ es un monomorfismo complejo, entonces σ y $\overline{\sigma}$ inducen el mismo valor absoluto, luego no tenemos dos valores absolutos canónicos para un mismo divisor.

Convertimos el teorema 5.21 en una definición para el caso arquimediano:

Sea K/k una extensión de cuerpos numéricos, sea $\mathfrak{p}$ un primo infinito de k y $\mathfrak{P}$ un primo infinito de K. Diremos que $\mathfrak{P}$ divide a $\mathfrak{p}$ si el valor absoluto canónico de $\mathfrak{P}$ extiende al valor absoluto canónico de $\mathfrak{p}$. Lo representaremos con la notación habitual: $\mathfrak{P} \mid \mathfrak{p}$.

Resultados elementales de la teoría de cuerpos nos dan que cada primo arquimediano de K divide a un único primo de k, así como que todo primo arquimediano de k es divisible entre al menos un primo de K. Los primos infinitos de un cuerpo numérico son exactamente los divisores del primo ∞ de $\mathbb{Q}$.

Si k es un cuerpo numérico y $\mathfrak{p}$ es un divisor primo en k, llamaremos $k_\mathfrak{p}$ a la compleción de k respecto a los valores absolutos de $\mathfrak{p}$. Llamaremos $|\ |_\mathfrak{p}$ a la extensión a $k_\mathfrak{p}$ del valor absoluto canónico de $\mathfrak{p}$ en k.

Las compleciones de los primos arquimedianos de un cuerpo numérico son fáciles de calcular:

Si $\mathfrak{p}$ es un primo infinito real de un cuerpo numérico k, inducido por un monomorfismo $\sigma : k \longrightarrow \mathbb{R}$, entonces σ es un isomorfismo topológico entre k con la topología inducida por $|\ |_\mathfrak{p}$ y la topología usual de $\mathbb{R}$, luego se extiende a un isomorfismo topológico entre $k_\mathfrak{p}$ y la compleción de $\sigma[k]$, que obviamente es $\mathbb{R}$. Así pues, $k_\mathfrak{p} \cong \mathbb{R}$. Similarmente, si $\mathfrak{p}$ es un primo infinito complejo de k entonces $k_\mathfrak{p} \cong \mathbb{C}$.

En cualquier caso, la clausura algebraica de la compleción de un primo infinito $\mathfrak{p}$ es $\mathbb{C}$, por lo que, para unificar la notación con el caso finito, convendremos en llamar $\mathbb{K}_\mathfrak{p} = \mathbb{C}$. El valor absoluto canónico en $\mathbb{K}_\mathfrak{p}$ lo definimos como el valor absoluto usual en $\mathbb{C}$.

Conviene tener presente que muchos de los resultados que hemos probado para compleciones respecto a primos finitos resultan trivialmente ciertas para primos infinitos. Por ejemplo, si K/k es una extensión de cuerpos numéricos, $\mathfrak{p}$ es un primo en k y $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, la igualdad $K_\mathfrak{P} = k_\mathfrak{p}K$, que el teorema 5.27 prueba en el caso finito, también vale en el caso infinito, pues el miembro derecho ha de ser $\mathbb{R}$ o $\mathbb{C}$, completo en cualquier caso, luego cerrado en $K_\mathfrak{P}$, y al contener a K es denso.

Si K/k es una extensión de cuerpos numéricos, $\mathfrak{p}$ es un divisor primo en k y $\mathfrak{P}$ es un divisor primo en K que divida a $\mathfrak{p}$, la definición de grado local

$$n(\mathfrak{P}/\mathfrak{p}) = |K_\mathfrak{P} : k_\mathfrak{p}|.$$

tiene sentido ahora incluso si los divisores son infinitos.

Teorema 5.37 *Sea K/k una extensión de grado n de cuerpos numéricos y sea $\mathfrak{p}$ un primo en k. Entonces*

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} n(\mathfrak{P}/\mathfrak{p}).$$

Demostración: Se entiende que la suma recorre los divisores primos de $\mathfrak{p}$ en K. Para primos finitos lo tenemos probado ya (como consecuencia inmediata de los teoremas 5.22 y 2.34). Supongamos ahora que $\mathfrak{p}$ es un primo infinito, digamos que inducido por el monomorfismo $\sigma : k \longrightarrow \mathbb{C}$, y veamos que hay exactamente n monomorfismos $\tau : K \longrightarrow \mathbb{C}$ que extienden a σ. En efecto, fijado uno de ellos, cualquier otro es de la forma $\tau \circ \rho$, donde ρ es un $\sigma[k]$-monomorfismo de $\tau[K]$, y ρ puede tomar n valores posibles.

Estos n monomorfismos determinan todos los divisores de $\mathfrak{p}$ en K, pero hemos de tener presente que cada par de monomorfismos conjugados dan lugar al mismo divisor. Si $\mathfrak{p}$ es un primo complejo, entonces todas las extensiones de σ serán monomorfismos complejos y todos los grados locales serán $n(\mathfrak{P}/\mathfrak{p}) = 1$. Por otra parte, la conjugación de una extensión de σ ya no será una extensión de σ, luego las n extensiones son no conjugadas dos a dos y dan lugar a n divisores distintos. La relación buscada es en este caso $n = 1 + \cdots + 1$.

Si $\mathfrak{p}$ es real, entonces σ puede tener s extensiones reales y t pares de extensiones conjugadas. Tenemos entonces que $n = s + 2t$. Las extensiones reales dan lugar a s primos reales distintos en K para los cuales $n(\mathfrak{P}/\mathfrak{p}) = 1$. Las

extensiones complejas dan lugar a t primos complejos distintos para los cuales $n(\mathfrak{P}/\mathfrak{p}) = 2$. Claramente también en este caso se cumple la relación entre los grados. ∎

La relación $n(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ sólo tiene sentido, en principio, para primos finitos. Podemos extenderla al caso infinito adoptando el convenio de que si $\mathfrak{P}$ y $\mathfrak{p}$ son primos infinitos tales que $\mathfrak{P} \mid \mathfrak{p}$, entonces su *grado de inercia* es $f(\mathfrak{P}/\mathfrak{p}) = 1$ y su *índice de ramificación* es $e(\mathfrak{P}/\mathfrak{p}) = n(\mathfrak{P}/\mathfrak{p})$.

Para completar la analogía convendremos también en que un primo infinito factoriza como producto de los primos que lo dividen con las multiplicidades determinadas por los índices de ramificación. Por ejemplo, en los cuerpos cuadráticos reales el primo ∞ de $\mathbb{Q}$ se escinde en dos factores primos reales distintos: $\infty = \infty_1\infty_2$, mientras que en los cuerpos cuadráticos imaginarios se ramifica: $\infty = \infty_1^2$.

En el teorema anterior hemos empleado argumentos completamente distintos para los primos finitos y para los infinitos. Ahora probaremos un resultado que generaliza la construcción que hemos hecho de los primos arquimedianos de un cuerpo numérico y la extiende al caso de los primos finitos. Con su ayuda podremos probar muchos resultados sobre primos sin necesidad de distinguir si son finitos o no.

Teorema 5.38 *Sea K/k una extensión de cuerpos numéricos y $\mathfrak{p}$ un divisor primo de k. Entonces:*

1. *Para cada k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ existe un primo $\mathfrak{P}$ en K divisor de $\mathfrak{p}$ tal que $|\alpha|_\mathfrak{P} = |\sigma(\alpha)|_\mathfrak{p}$ para todo $\alpha \in K$.*

2. *Para cada primo $\mathfrak{P}$ de K que divide a $\mathfrak{p}$, los k-monomorfismos que inducen el primo $\mathfrak{P}$ según el apartado 1) son exactamente las restricciones a K de los $k_\mathfrak{p}$-monomorfismos $\sigma : K_\mathfrak{P} \longrightarrow \mathbb{K}_\mathfrak{p}$, y hay exactamente $n(\mathfrak{P}/\mathfrak{p})$ de ellos.*

3. *Dos k-monomorfismos σ y τ inducen el mismo valor absoluto si y sólo si existe un $k_\mathfrak{p}$-automorfismo $\phi : \mathbb{K}_\mathfrak{p} \longrightarrow \mathbb{K}_\mathfrak{p}$ tal que $\sigma \circ \phi = \tau$.*

Demostración: Si $\mathfrak{P}$ es un divisor primo de $\mathfrak{p}$ en K, el teorema 5.23 implica que cada $k_\mathfrak{p}$-monomorfismo $\tau : K_\mathfrak{P} \longrightarrow \mathbb{K}_\mathfrak{p}$ es una isometría, pues el valor absoluto en $K_\mathfrak{P}$ dado por $|\alpha| = |\tau(\alpha)|_\mathfrak{p}$ extiende al valor absoluto canónico de $k_\mathfrak{p}$, luego ha de ser el valor absoluto canónico de $K_\mathfrak{P}$.

Por lo tanto, su restricción a K es un k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ que cumple $|\alpha|_\mathfrak{P} = |\sigma(\alpha)|_\mathfrak{p}$, para todo $\alpha \in K$, es decir, que induce el primo $\mathfrak{P}$ en el sentido del apartado 1).

Como K es denso en $K_\mathfrak{P}$, las restricciones de dos $k_\mathfrak{p}$-monomorfismos distintos han de ser dos k-monomorfismos distintos, luego así obtenemos $n(\mathfrak{P}/\mathfrak{p})$ de ellos.

Además, dos k-monomorfismos obtenidos por restricción desde dos compleciones correspondientes a primos distintos en K han de ser distintos entre sí, pues cada uno induce en K valor absoluto distinto. Por el teorema anterior,

si el grado de K/k es n, tenemos n monomorfismos distintos que cumplen el apartado 1), pero éstos son todos los k-monomorfismos de K, luego a) es cierto para todos los k-monomorfismos. Este razonamiento prueba también 2).

3) Si σ y τ inducen el mismo valor absoluto en K, digamos $|\ |_\mathfrak{P}$, por b) ambos se extienden a sendos $k_\mathfrak{p}$-monomorfismos $\sigma, \tau : K_\mathfrak{P} \longrightarrow \mathbb{K}_\mathfrak{p}$. Entonces $\sigma^{-1} \circ \tau : \sigma[K_\mathfrak{P}] \longrightarrow \tau[K_\mathfrak{P}]$ es un $k_\mathfrak{p}$-isomorfismo que se extiende a un $k_\mathfrak{p}$-automorfismo $\phi : \mathbb{K}_\mathfrak{p} \longrightarrow \mathbb{K}_\mathfrak{p}$ (porque $\mathbb{K}_\mathfrak{p}$ es la clausura algebraica de los cuerpos $\sigma[K_\mathfrak{p}]$ y $\tau[K_\mathfrak{p}]$). Claramente entonces $\sigma \circ \phi = \tau$.

Recíprocamente, supongamos que $\sigma\circ\phi = \tau$ para un cierto $k_\mathfrak{p}$-automorfismo ϕ. Entonces para todo $\alpha \in K$ se tiene $|\tau(\alpha)|_\mathfrak{p} = |\phi(\sigma(\alpha))|_\mathfrak{p} = |\sigma(\alpha)|_\mathfrak{p}$, porque los $k_\mathfrak{p}$-automorfismos son isometrías (en el caso infinito son la identidad en $\mathbb{R}$ o $\mathbb{C}$ o la conjugación compleja). Vemos, pues, que ambos monomorfismos inducen el mismo valor absoluto. ∎

De este teorema se siguen relaciones muy importantes entre los primos de un cuerpo numérico.

Definición 5.39 Sea K/k una extensión de cuerpos numéricos. Sea $\mathfrak{p}$ un primo en k y $\mathfrak{P}$ un primo en K que divida a $\mathfrak{p}$. Llamaremos *norma local* $\mathrm{N}_\mathfrak{P}$ y *traza local* $\mathrm{Tr}_\mathfrak{P}$ a la norma y la traza de la extensión $K_\mathfrak{P}/k_\mathfrak{p}$.

Si $\alpha \in K$, la norma de α (en la extensión K/k) es el producto las imágenes de α por los k-monomorfismos de K. Sin más que agrupar los factores correspondientes a monomorfismos que inducen un mismo primo $\mathfrak{P}$ según el teorema anterior obtenemos que

$$\mathrm{N}_k^K(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_\mathfrak{P}(\alpha), \tag{5.3}$$

y análogamente para la traza:

$$\mathrm{Tr}_k^K(\alpha) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_\mathfrak{p}(\alpha). \tag{5.4}$$

Más aún, en el caso en que $k = \mathbb{Q}$ y $\mathfrak{p} = p$ es un primo racional (finito o no), entonces $\mathrm{N}_\mathfrak{P}(\alpha)$ es el producto de todos los conjugados de α por los monomorfismos que inducen el valor absoluto de $\mathfrak{P}$, o sea por los monomorfismos que cumplen $|\alpha|_\mathfrak{P} = |\sigma(\alpha)|_p$. Por lo tanto, si llamamos $n_\mathfrak{P} = n(\mathfrak{P}/p)$, resulta que $|\,\mathrm{N}_\mathfrak{P}(\alpha)|_p = |\alpha|_\mathfrak{P}^{n_\mathfrak{P}}$. Por consiguiente

$$|\,\mathrm{N}_\mathbb{Q}^K(\alpha)|_p = \prod_{\mathfrak{P}|p} |\alpha|_\mathfrak{P}^{n_\mathfrak{P}}. \tag{5.5}$$

De aquí obtenemos:

Teorema 5.40 (Fórmula del producto) *Sea K un cuerpo numérico. Para cada primo $\mathfrak{p}$ de K sea p el primo racional divisible entre $\mathfrak{p}$ y sea $n_\mathfrak{p}$ el grado local $n(\mathfrak{p}/p)$. Entonces para todo $\alpha \in K$ no nulo se cumple*

$$\prod_\mathfrak{p} |\alpha|_\mathfrak{p}^{n_\mathfrak{p}} = 1,$$

donde $\mathfrak{p}$ recorre todos los primos de K.

DEMOSTRACIÓN: Notemos en primer lugar que si r es un número racional no nulo y p recorre todos los primos de $\mathbb{Q}$ se cumple

$$\prod_p |r|_p = 1.$$

En efecto, si q es un número primo entonces

$$|q|_p = \begin{cases} 1/q & \text{si } p = q, \\ 1 & \text{si } q \neq p \neq \infty \\ q & \text{si } p = \infty \end{cases}$$

Claramente entonces la fórmula es cierta para todo primo q. Trivialmente es cierta para ± 1 y, como el producto es multiplicativo, la fórmula es válida para todo número racional no nulo. Por la fórmula (5.5) concluimos

$$1 = \prod_p |\,\mathrm{N}(\alpha)|_p = \prod_p \prod_{\mathfrak{p}|p} |\alpha|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = \prod_{\mathfrak{p}} |\alpha|_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

■

Definición 5.41 Sea $\mathfrak{p}$ un primo de un cuerpo numérico K, sea p el primo racional al cual divide y sea $n_{\mathfrak{p}}$ el grado local $n(\mathfrak{p}/p)$. Para cada $\alpha \in K$ definimos

$$\|\alpha\|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

Claramente $\|\ \|_{\mathfrak{p}}$ es un valor absoluto asociado a $\mathfrak{p}$ excepto cuando $\mathfrak{p}$ es un primo complejo, en cuyo caso se trata del cuadrado del valor absoluto canónico. En estos términos la fórmula del producto se expresa como

$$\prod_{\mathfrak{p}} \|\alpha\|_{\mathfrak{p}} = 1. \tag{5.6}$$

En el caso de los primos no arquimedianos $\|\ \|_{\mathfrak{p}}$ es un valor absoluto muy natural. En efecto, si $v_{\mathfrak{p}}(\pi) = 1$ y p es el primo racional divisible entre $\mathfrak{p}$ (digamos $p = \mathfrak{p}^e$), entonces $p = \epsilon\pi^e$, para una cierta unidad ϵ (de $K_{\mathfrak{p}}$). Así, $1/p = |p|_p = |p|_{\mathfrak{p}} = |\pi^e|_{\mathfrak{p}}$, luego $|\pi|_{\mathfrak{p}} = (1/p)^{1/e}$ y, en definitiva,

$$\|\pi\|_{\mathfrak{p}} = \left(\frac{1}{p^{1/e}}\right)^{ef} = \frac{1}{p^f} = \frac{1}{N\mathfrak{p}}. \tag{5.7}$$

Esto caracteriza a $\|\ \|_{\mathfrak{p}}$ como el valor absoluto dado por $\|\alpha\|_{\mathfrak{p}} = (1/N\mathfrak{p})^{v_{\mathfrak{p}}(\alpha)}$.

Señalemos ahora otra consecuencia del teorema 5.38. En la sección anterior hemos visto que, si p es un primo finito, la clausura algebraica $\mathbb{K}_p$ no es completa, pero si $K \subset \mathbb{K}_p$ es un cuerpo numérico (notemos que $\mathbb{K}_p$ contiene una clausura algebraica de $\mathbb{Q}$, y por lo tanto a todos los cuerpos numéricos) entonces la inclusión de K en $\mathbb{K}_p$ es un $\mathbb{Q}$-monomorfismo que determina un primo $\mathfrak{p}$ en K. Dicha inclusión se extiende a una isometría $K_{\mathfrak{p}} \longrightarrow \mathbb{K}_p$, cuya imagen es la clausura de K en $\mathbb{K}_p$. Así pues, $\overline{K}$ es completo aunque $\mathbb{K}_p$ no lo sea.

Veamos ahora qué podemos añadir para extensiones de Galois. Para empezar, el grupo de Galois actúa sobre los primos. Conviene dar una definición en el caso general:

Definición 5.42 Sea $\sigma : K \longrightarrow L$ un isomorfismo de cuerpos numéricos y sea $\mathfrak{p}$ un divisor primo en K. Definimos $\sigma(\mathfrak{p})$ como el divisor primo de L inducido por el valor absoluto dado por $|\alpha|_{\sigma(\mathfrak{p})} = |\sigma^{-1}(\alpha)|_{\mathfrak{p}}$ para todo $\alpha \in L$.

Entonces σ es una isometría si en K consideramos el valor absoluto de $\mathfrak{p}$ y en L el de $\sigma(\mathfrak{p})$, luego σ se extiende a una isometría $\sigma : K_{\mathfrak{p}} \longrightarrow L_{\sigma(\mathfrak{p})}$.

Pasemos ya al caso en que K/k es una extensión de Galois de cuerpos numéricos y $\sigma \in G(K/k)$. Entonces si $\mathfrak{p}$ es un primo de k y $\mathfrak{P} \mid \mathfrak{p}$ se cumple que $\sigma(\mathfrak{P}) \mid \mathfrak{p}$ (pues el valor absoluto $|\ |_{\sigma(\mathfrak{P})}$ extiende al valor absoluto de $\mathfrak{p}$), o sea, que σ permuta los divisores de $\mathfrak{p}$.

Observemos que si el primo $\mathfrak{P}$ es no arquimediano entonces el primo $\sigma(\mathfrak{P})$ que acabamos de definir es el definido en la sección 2.4 pues, considerados como ideales, $\alpha \in \sigma(\mathfrak{p})$ si y sólo si $|\alpha|_{\sigma(\mathfrak{p})} < 1$, si y sólo si $|\sigma^{-1}(\alpha)|_{\mathfrak{p}} < 1$, si y sólo si $\sigma^{-1}(\alpha) \in \mathfrak{p}$, si y sólo si $\alpha \in \sigma[\mathfrak{p}]$.

Ahora podemos definir el *grupo de descomposición*

$$G_{\mathfrak{p}} = \{\sigma \in G(K/k) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\} \leq G(K/k),$$

para cualquier divisor primo de K, incluso si es infinito. El teorema siguiente generaliza los resultados que probamos en la sección 2.4 para el caso finito:

Teorema 5.43 *Sea K/k una extensión de Galois de cuerpos numéricos. Sea $\mathfrak{p}$ un divisor primo en k. Entonces*

1. *Si $\mathfrak{P}_1$ y $\mathfrak{P}_2$ son divisores de $\mathfrak{p}$ en K existe un automorfismo $\sigma \in G(K/k)$ tal que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.*

2. *Si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, el grupo de Galois local $G(K_{\mathfrak{p}}/k_{\mathfrak{p}})$ es isomorfo al grupo de descomposición $G_{\mathfrak{P}}$ (el isomorfismo es la restricción). En particular $|G_{\mathfrak{P}}| = n(\mathfrak{P}/\mathfrak{p})$.*

3. *Si $\tau \in G(K/k)$ y $\mathfrak{P}$ es un primo de K, entonces $G_{\tau(\mathfrak{P})} = G_{\mathfrak{p}}^{\tau}$.*

Demostración: 1) Tomamos como $\mathbb{K}_{\mathfrak{p}}$ una clausura algebraica de $K_{\mathfrak{P}_2}$ y así $K_{\mathfrak{P}_2} \subset \mathbb{K}_{\mathfrak{p}}$, y el valor absoluto asociado a $\mathfrak{P}_2$ coincide con el de $K_{\mathfrak{p}}$.

Sea $\sigma : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$ que induce el valor absoluto de $\mathfrak{P}_1$, es decir, tal que $|\alpha|_{\mathfrak{P}_1} = |\sigma(\alpha)|_{\mathfrak{p}} = |\sigma(\alpha)|_{\mathfrak{P}_2}$.

Como K/k es de Galois se cumple que $\sigma \in G(K/k)$, y así $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

2) Si $\sigma \in G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ entonces $\sigma : K_{\mathfrak{P}} \longrightarrow K_{\mathfrak{P}}$ es una isometría, luego su restricción a K es una isometría para el valor absoluto de $\mathfrak{P}$, luego $\sigma(\mathfrak{P}) = \mathfrak{P}$.

Recíprocamente, si $\sigma(\mathfrak{P}) = \mathfrak{P}$ entonces σ se extiende a un automorfismo de $K_{\mathfrak{p}}$ que fija a k, luego a $k_{\mathfrak{p}}$ (por continuidad).

La restricción es inyectiva porque K es denso en $K_{\mathfrak{P}}$, y claramente es un isomorfismo de grupos.

3) El argumento empleado en el caso finito es válido en general. ∎

Observemos que el teorema anterior implica que en las extensiones de Galois el índice de ramificación de todos los divisores de un mismo primo es constante (los grupos tienen todos el mismo número de elementos).

Como aplicación de los resultados de esta sección probaremos un teorema sobre escisión de primos.

Definición 5.44 Sea K/k una extensión de grado n de cuerpos numéricos. Diremos que un divisor primo $\mathfrak{p}$ de k se *escinde completamente* en K si tiene exactamente n divisores en K. Por el teorema 5.37 esto equivale a que los grados locales $n(\mathfrak{P}/\mathfrak{p})$ sean 1 para todos los divisores $\mathfrak{P}$ de $\mathfrak{p}$ en K, lo que a su vez equivale a que $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$.

Teorema 5.45 *Se cumple:*

1. *Si $k \subset K \subset L$ son cuerpos numéricos, un primo $\mathfrak{p}$ de k se escinde completamente en L si y sólo si se escinde completamente en K y cada divisor de $\mathfrak{p}$ en K se escinde completamente en L.*

2. *Si K/k y L/k son extensiones de cuerpos numéricos, $\mathfrak{p}$ es un primo de k que se escinde completamente en K y $\mathfrak{P}$ es un primo en L que divide a $\mathfrak{p}$, entonces $\mathfrak{P}$ se escinde completamente en KL.*

3. *Si K/k y L/k son extensiones de cuerpos numéricos y $\mathfrak{p}$ es un primo de k que se escinde completamente en K y en L, entonces $\mathfrak{p}$ se escinde completamente en KL.*

Demostración: 1) es inmediato a partir de la definición.

3) es consecuencia de 1) y 2): todo divisor de $\mathfrak{p}$ en L se escinde completamente en KL, luego $\mathfrak{p}$ se escinde completamente en KL.

Para probar 2) observemos en general que cada divisor de $\mathfrak{p}$ en una extensión T de k de grado n viene determinado por uno de los k-monomorfismos $T \longrightarrow \mathbb{K}_\mathfrak{p}$. Como hay n de ellos, $\mathfrak{p}$ se escindirá completamente si y sólo si no hay dos k-monomorfismos que determinen el mismo valor absoluto. Pero sabemos que dos k-monomorfismos σ y τ determinan el mismo valor absoluto si y sólo si $\sigma = \tau \circ \phi$, donde ϕ es un $k_\mathfrak{p}$-monomorfismo de $\mathbb{K}_\mathfrak{p}$. La conclusión es, pues, que $\mathfrak{p}$ se escinde en T si y sólo si para todo k-monomorfismo $\sigma : T \longrightarrow \mathbb{K}_\mathfrak{p}$ se cumple que cualquier $k_\mathfrak{p}$-monomorfismo de $\mathbb{K}_\mathfrak{p}$ es la identidad en $\sigma[T]$, o sea, si para todo k-monomorfismo σ se cumple que $\sigma[T] \subset k_\mathfrak{p}$.

Ahora notamos que, puesto que $K_\mathfrak{P}/k_\mathfrak{p}$ es una extensión finita, la clausura algebraica $\mathbb{K}_\mathfrak{P}$ es también una clausura algebraica de $k_\mathfrak{p}$, luego podemos considerar $\mathbb{K}_\mathfrak{P} = \mathbb{K}_\mathfrak{p}$.

Para ver que $\mathfrak{P}$ se escinde completamente en KL consideramos un L-monomorfismo $\sigma : KL \longrightarrow \mathbb{K}_\mathfrak{P}$. Puesto que σ se restringe a un k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ y $\mathfrak{p}$ se escinde completamente en K, ha de ser $\sigma[K] \subset k_\mathfrak{p}$ y, dado que σ fija a los elementos de L, resulta que $\sigma[KL] \subset k_\mathfrak{p}L = L_\mathfrak{P}$. Por lo tanto $\mathfrak{P}$ se escinde completamente en KL. ∎

Ejemplo Consideremos un cuerpo cúbico puro $\mathbb{Q}(\sqrt[3]{m})$. Su clausura normal se obtiene adjuntando una raíz cúbica de la unidad o, equivalentemente, adjuntando $\sqrt{-3}$, pues una raíz cúbica de la unidad es $\omega = (-1+\sqrt{-3})/2$ y los conjugados de $\sqrt[3]{m}$ son $\omega\sqrt[3]{m}$ y $\omega^2\sqrt[3]{m}$.

Por lo tanto, el cuerpo $K = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$ es una extensión finita de Galois sobre $\mathbb{Q}$ de grado 6. El teorema anterior nos permite determinar la factorización en K de los primos racionales a partir de la factorización en $\mathbb{Q}(\sqrt[3]{m})$ y en $\mathbb{Q}(\sqrt{-3})$, ambas vistas en la sección 2.3.

La tabla siguiente recoge todos los casos posibles (la notación es la introducida en la sección 2.3):

Casos		$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt[3]{m})$	K	e	f
$p \nmid ab$	$p \equiv 1(3)$ $x^3 \equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$	1	1
	$x^3 \not\equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	p	$\mathfrak{p}_1\mathfrak{p}_2$	1	3
	$p \equiv -1(3)$	p	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	2
$p \mid ab$	$p \equiv 1(3)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}^3$	$(\mathfrak{p}_1\mathfrak{p}_2)^3$	3	1
	$p \equiv -1(3)$	p	$\mathfrak{p}^3$	$\mathfrak{p}^3$	3	2
$p = 3$	Tipo I	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^6$	6	1
	Tipo II	$\mathfrak{p}^2$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$	2	1

La primera fila se obtiene aplicando el teorema anterior: p se escinde completamente tanto en $\mathbb{Q}(\sqrt{-3})$ como en $\mathbb{Q}(\sqrt[3]{m})$, luego se escinde completamente en el producto. Las restantes se deducen elementalmente usando la transitividad de e y f. Tomemos por ejemplo la tercera fila. Sabemos que f ha de ser múltiplo de 2 (porque vale 2 en $\mathbb{Q}(\sqrt{-3})$) y divisor de 6, pero no puede ser 6 porque el número de primos ha de ser $r \geq 2$ (por $\mathbb{Q}(\sqrt[3]{m})$), luego ha de ser $f = 2$, y la única posibilidad es $r = 3$, $f = 2$, $e = 1$. En los demás casos se razona de forma similar. ∎

Ejercicio: Factorizar ∞ en las tres extensiones del ejemplo anterior.

Terminamos la sección con un teorema muy útil sobre valores absolutos que generaliza al teorema chino del resto:

Teorema 5.46 (Teorema de aproximación (Artin-Whaples)) *Sea K un cuerpo y sean $|\ |_1, \ldots, |\ |_n$ valores absolutos en K no triviales y no equivalentes dos a dos. Sean $x_1, \ldots, x_n \in K$ y $\epsilon > 0$. Entonces existe un $x \in K$ tal que $|x - x_i|_i < \epsilon$ para $i = 1, \ldots, n$.*

Demostración: Notemos en primer lugar que si dos valores absolutos no triviales cumplen que cuando $|\alpha|_1 \leq 1$ también $|\alpha|_2 \leq 1$, entonces ambos son equivalentes.

En efecto, existe un cierto $c \in K$ tal que $0 < |c|_2 < 1$. De este modo $|\alpha|_1 < 1$ implica que $|\alpha^n|_1 \leq |c|_1$ para n suficientemente grande, luego $|\alpha^n/c|_1 \leq 1$, luego $|\alpha^n/c|_2 \leq 1$, luego $|\alpha^n|_2 \leq |c|_2 < 1$, y por lo tanto $|\alpha|_2 < 1$. Recíprocamente, $|\alpha|_1 \geq 1$ implica que $|1/\alpha|_1 \leq 1$, luego $|1/\alpha|_2 \leq 1$ y $|\alpha|_2 \geq 1$.

Así pues, $|\alpha|_1 < 1$ si y sólo si $|\alpha|_2 < 1$. De aquí se sigue claramente la equivalencia.

Ahora las hipótesis del teorema nos dan que existen $\alpha, \beta \in K$ tales que

$$|\alpha|_1 < 1, \quad |\alpha|_2 \geq 1, \quad |\beta|_1 \geq 1, \quad |\beta|_2 < 1.$$

Llamando $y = \beta/\alpha$ resulta que $|y|_1 > 1$, $|y|_2 < 1$.

Veamos por inducción sobre n que existe un cierto $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n$. Lo tenemos probado para $n = 2$. Supongamos que existe un $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n-1$. Tomemos también un $z \in K$ que cumpla $|z|_1 > 1$, $|z|_n < 1$.

Si se cumple $|y|_n \leq 1$ entonces $y^m z$ cumple lo pedido cuando m es suficientemente grande. Si $|y|_n > 1$ consideramos la sucesión $u_m = y^m/(1 + y^m)$, que claramente tiende a 1 respecto a los valores absolutos $|\ |_1$ y $|\ |_n$ y tiende a 0 respecto a los restantes. Cuando m es suficientemente grande $u_m z$ cumple lo pedido.

Sea, pues, $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n$. Usamos de nuevo que la sucesión $y^m/(1+y^m)$ tiende a 1 respecto al primer valor absoluto y tiende a 0 respecto a los demás. Multiplicándola por x_1 y tomando un término suficientemente lejano obtenemos un elemento $y_1 \in K$ tal que $|x_1 - y_1|_1 < \epsilon/n$ y $|y_1|_i < \epsilon/n$ para $i = 2, \ldots, n$.

Del mismo modo podemos obtener elementos y_i tales que $|x_i - y_i|_i < \epsilon/n$, $|y_i|_j < \epsilon/n$ para $j \neq i$. El teorema se cumple con $x = y_1 + \cdots + y_n$. ∎

5.5 Criterios de existencia de raíces

Presentamos ahora unos resultados sobre existencia de raíces de polinomios en cuerpos métricos completos discretos que serán necesarios en capítulos posteriores. Por ejemplo, tras el teorema 5.22 hemos visto que, si p es un primo impar y $p \nmid m$, el polinomio $x^2 - m$ tiene una raíz en $\mathbb{Q}_p$ si y sólo si tiene una raíz módulo p. Eso es un caso particular del teorema siguiente (con $k = 0$):

Teorema 5.47 *Sea K un cuerpo métrico discreto completo. Sea D su anillo de enteros y $\mathfrak{p}$ su ideal primo. Sea $F(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$ y sean $\gamma_1, \ldots, \gamma_n$ enteros tales que para cierto i $(1 \leq i \leq n)$ y cierto $k \geq 0$ se cumpla:*

$$\begin{aligned} F(\gamma_1, \ldots, \gamma_n) &\equiv 0 \ (\text{mód } \mathfrak{p}^{2k+1}), \\ F'_i(\gamma_1, \ldots, \gamma_n) &\equiv 0 \ (\text{mód } \mathfrak{p}^{k}), \\ F'_i(\gamma_1, \ldots, \gamma_n) &\not\equiv 0 \ (\text{mód } \mathfrak{p}^{k+1}), \end{aligned}$$

donde F'_i representa la derivada parcial formal respecto a la indeterminada x_i. Entonces existen enteros $\delta_1, \ldots, \delta_n$ tales que $F(\delta_1, \ldots, \delta_n) = 0$ y además para cada j se cumple $\delta_j \equiv \gamma_j$ (mód $\mathfrak{p}^{k+1}$).

Demostración: Consideremos el polinomio

$$f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n).$$

Basta encontrar un entero α tal que $f(\alpha) = 0$ y $\alpha \equiv \gamma_i \pmod{\mathfrak{p}^{k+1}}$. Por simplificar la notación llamaremos $\gamma = \gamma_i$.

Vamos a construir una sucesión de enteros $\alpha_0, \alpha_1, \ldots$, todos congruentes con γ módulo $\mathfrak{p}^{k+1}$ y de modo que $f(\alpha_m) \equiv 0 \pmod{\mathfrak{p}^{2k+1+m}}$. Por hipótesis podemos partir de $\alpha_0 = \gamma$. Dados $\alpha_0, \ldots, \alpha_{m-1}$ en estas condiciones, tenemos en particular que

$$\alpha_{m-1} \equiv \gamma \pmod{\mathfrak{p}^{k+1}}, \qquad f(\alpha_{m-1}) \equiv 0 \pmod{\mathfrak{p}^{2k+m}}.$$

Desarrollemos $f(x)$ en potencias de $x - \alpha_{m-1}$:

$$f(x) = \beta_0 + \beta_1(x - \alpha_{m-1}) + \beta_2(x - \alpha_{m-1})^2 + \cdots,$$

donde los coeficientes β_j son enteros.

Así, $\beta_0 = f(\alpha_{m-1}) = \pi^{2k+m}A$, para un cierto entero A y un primo π, y $\beta_1 = f'(\alpha_{m-1}) \equiv f'(\gamma) \pmod{\mathfrak{p}^{k+1}}$, luego $\beta_1 = \pi^k B$ para un cierto entero B no divisible entre $\mathfrak{p}$.

Esta última condición nos asegura que existe un entero C de manera que $A + BC \equiv 0 \pmod{\mathfrak{p}}$. Si hacemos $\alpha_m = \alpha_{m-1} + \pi^{k+m}C$ tenemos ciertamente que $\alpha_m \equiv \alpha_{m-1} \equiv \gamma \pmod{\mathfrak{p}^{k+1}}$ y además

$$\begin{aligned} f(\alpha_m) &= \pi^{2k+m}A + \pi^k B(\pi^{k+m}C) + \beta_2(\pi^{k+m}C)^2 + \cdots \\ &= \pi^{2k+m}(A + BC) + \beta_2(\pi^{k+m}C)^2 + \cdots \equiv 0 \pmod{\mathfrak{p}^{2k+1+m}}, \end{aligned}$$

puesto que para $r \geq 2$ se cumple que $kr + mr \geq 2k + 1 + m$.

Con esto queda justificada la existencia de la sucesión $\alpha_0, \alpha_1, \ldots$, y de hecho, según la construcción, $\alpha_m = \alpha_{m-1} + \pi^{k+m}C$, o sea, $v(\alpha_m - \alpha_{m-1}) \geq k + m$, luego por el teorema 5.7 resulta que existe $\alpha = \lim_m \alpha_m \in D$. Puesto que la sucesión $(\alpha_m - \gamma)/\pi^{k+1}$ también está contenida en D, su límite, $(\alpha - \gamma)/\pi^{k+1}$, es un entero, luego se cumple que $\alpha \equiv \gamma \pmod{\mathfrak{p}^{k+1}}$.

Además por construcción $v\big(f(\alpha_m)\big) \geq 2k + 1 + m$, luego $\lim_m f(\alpha_m) = 0$. Como los polinomios son funciones continuas, $f(\alpha) = 0$. ∎

A menudo nos bastará aplicar el caso particular $k = 0$, que enunciamos a continuación:

Teorema 5.48 *Sea K un cuerpo métrico discreto completo. Sea D su anillo de enteros y $\mathfrak{p}$ su ideal primo. Sea $F(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$ y sean $\gamma_1, \ldots, \gamma_n$ enteros tales que para cierto i $(1 \leq i \leq n)$ se cumpla:*

$$\begin{aligned} F(\gamma_1, \ldots, \gamma_n) &\equiv 0 \pmod{\mathfrak{p}}, \\ F'_i(\gamma_1, \ldots, \gamma_n) &\not\equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

Entonces existen enteros $\delta_1, \ldots, \delta_n$ tales que $F(\delta_1, \ldots, \delta_n) = 0$ y además para cada j se cumple $\delta_j \equiv \gamma_j \pmod{\mathfrak{p}}$.

El teorema siguiente es menos práctico, porque reduce la existencia de raíces de un polinomio en un cuerpo métrico discreto y completo a la solubilidad de infinitas congruencias, pero muestra de la forma más clara posible la relación entre existencia de raíces y congruencias. Dejamos la prueba a cargo del lector.

Teorema 5.49 *Sea K un cuerpo métrico discreto completo. Sea D su anillo de enteros y $\mathfrak{p}$ su ideal primo. Sea $F(x_1,\dots,x_n) \in D[x_1,\dots,x_n]$. Entonces la ecuación $F(x_1,\dots,x_n) = 0$ tiene solución en D si y sólo si las congruencias $F(x_1,\dots,x_n) \equiv 0 \pmod{\mathfrak{p}^m}$ tienen solución para todo m.*

5.6 Series en cuerpos métricos discretos

En esta sección mostramos que las series convergentes en cuerpos completos no arquimedianos se comportan como las series absolutamente convergentes en los cuerpos completos arquimedianos. Esto es consecuencia del teorema siguiente:

Teorema 5.50 *La convergencia y la suma de una serie en un cuerpo completo no arquimediano no se altera si se reordenan sus términos.*

Demostración: Es claro que una sucesión de números reales tiende a cero si y sólo si cualquier reordenación suya tiende a cero. Por el teorema 5.8, una serie $\sum_{n=0}^{\infty} \alpha_n$ es convergente si y sólo si (α_n) tiende a 0, si y sólo si $\big(|\alpha_n|\big)$ tiende a 0, y esto no depende de la ordenación.

Supongamos ahora que $\sum_{n=0}^{\infty} \alpha_n$ converge a S pero una reordenación suya $\sum_{n=0}^{\infty} \beta_n$ converge a $S' \neq S$. Sea $\epsilon = |S - S'|$. Existe un k tal que si $m \geq k$ entonces $\left|\sum_{n=0}^{m} \alpha_n - S\right| < \epsilon$. También podemos exigir que $|\alpha_n| < \epsilon$ para $n \geq k$. Sea $k' \geq k$ tal que $\{\alpha_1,\dots,\alpha_k\} \subset \{\beta_1,\dots,\beta_{k'}\}$ y

$$\left|\sum_{n=0}^{k'} \beta_n - S'\right| < \epsilon.$$

Entonces

$$\begin{aligned} |S - S'| &= \left|\Big(S - \sum_{n=0}^{k'} \beta_n\Big) + \Big(\sum_{n=0}^{k'} \beta_n - S'\Big)\right| \\ &= \left|\Big(S - \sum_{n=0}^{k} \alpha_n\Big) - R + \Big(\sum_{n=0}^{k'} \beta_n - S'\Big)\right|, \end{aligned}$$

donde R es la suma de los elementos de $\{\beta_1,\dots,\beta_{k'}\} \setminus \{\alpha_1,\dots,\alpha_k\}$, todos ellos con valor absoluto menor que ϵ.

La desigualdad triangular no arquimediana nos da que $|S - S'| < \epsilon$, en contradicción con la elección de ϵ. Por lo tanto $S = S'$. ∎

De aquí se sigue que (en los cuerpos completos no arquimedianos) podemos definir series de la forma $\sum_{i\in I} \alpha_i$, donde I es un conjunto numerable, sin especificar el orden de los sumandos. Bajo esta notación se incluyen las sumas finitas.

Observemos que si la serie es convergente, para todo $\epsilon > 0$ existe un $F_0 \subset I$ finito tal que para todo $F_0 \subset F \subset I$ finito se cumple $|\sum_{i\in I} \alpha_i - \sum_{i\in F} \alpha_i| < \epsilon$. En efecto, basta tomar F_0 de modo que $|\alpha_i| < \epsilon/2$ para $i \in I \setminus F_0$, pues entonces todas las sumas parciales de la serie $\sum_{i\in I\setminus F} \alpha_i = \sum_{i\in I} \alpha_i - \sum_{i\in F} \alpha_i$ tienen valor absoluto menor que $\epsilon/2$, luego el límite cumple $|\sum_{i\in I} \alpha_i - \sum_{i\in F} \alpha_i| \le \epsilon/2 < \epsilon$.

De hecho esto es una caracterización de la convergencia que no depende de ninguna ordenación en particular. Esto hace que todas las series convergentes en un cuerpo métrico completo no arquimediano se comporten como las series absolutamente convergentes en un cuerpo métrico completo arquimediano. Por ejemplo, se cumple la asociatividad infinita:

Teorema 5.51 *Sea $(\alpha_i)_{i\in I}$ una familia de elementos de un cuerpo completo no arquimediano. Sea $I = \bigcup_{i=0}^{\infty} I_n$ una división de I en partes disjuntas. Si $\sum_{i\in I} \alpha_i$ es convergente también lo son las series $\sum_{i\in I_n} \alpha_i$ y $\sum_{n=0}^{\infty} \sum_{i\in I_n} \alpha_i$, y además entonces $\sum_{i\in I} \alpha_i = \sum_{n=0}^{\infty} \sum_{i\in I_n} \alpha_i$.*

Demostración: Las series $\sum_{i\in I_n} \alpha_i$ son convergentes porque son finitas o bien los sumandos (ordenados de algún modo) forman una subsucesión de una sucesión convergente a cero.

Dado $\epsilon > 0$, todos los α_j salvo un número finito cumplen que $|\alpha_i| < \epsilon$, luego todas las series $\sum_{i\in I_n} \alpha_i$ salvo quizá un número finito de ellas cumplen que $|\sum_{i\in I_n} \alpha_i| \le \epsilon$ (lo cumplen las sumas parciales y por continuidad el límite), lo que significa que el término general de la serie $\sum_{n=0}^{\infty} \sum_{i\in I_n} \alpha_i$ tiende a 0, luego la serie es convergente.

Sea ahora $\epsilon > 0$. Existe un número natural n_0 tal que $|\sum_{n=n_0+1}^{\infty} \sum_{i\in I_n} \alpha_i| < \epsilon$.

Para cada $n \le n_0$ existe un conjunto finito $F_n \subset I_n$ tal que si $F_n \subset F \subset I_n$, entonces $|\sum_{i\in I_n} \alpha_i - \sum_{i\in F_n} \alpha_i| < \epsilon$.

Sea F un conjunto finito que contenga a todos los F_n y de manera que $|\sum_{i\in I} \alpha_i - \sum_{i\in F} \alpha_i| < \epsilon$. Entonces

$$\left|\sum_{n=0}^{\infty} \sum_{i\in I_n} \alpha_i - \sum_{i\in I} \alpha_i\right|$$

$$\le \left|\Big(\sum_{n=n_0+1}^{\infty} \sum_{i\in I_n} \alpha_i\Big) + \Big(\sum_{n=0}^{n_0} \sum_{i\in I_n} \alpha_i - \sum_{i\in F} \alpha_i\Big) + \Big(\sum_{i\in F} \alpha_i - \sum_{i\in I} \alpha_i\Big)\right| < \epsilon.$$

Por lo tanto ambas sumas coinciden. ∎

Ejercicio: Probar que aunque las series $\sum_{i\in I_n} \alpha_i$ y $\sum_{n=0}^{\infty} \sum_{i\in I_n} \alpha_i$ converjan, la serie $\sum_{i\in I} \alpha_i$ no tiene por qué converger.

Ahora es claro el teorema del producto de series, es decir,

$$\sum_{(i,j)\in I\times J}\alpha_i\beta_j=\Big(\sum_{i\in I}\alpha_i\Big)\Big(\sum_{j\in J}\beta_j\Big),$$

donde la serie de la izquierda converge si convergen las dos series de la derecha. En efecto, la convergencia es obvia, y aplicando el teorema anterior,

$$\sum_{(i,j)\in I\times J}\alpha_i\beta_j=\sum_{i\in I}\Big(\sum_{j\in J}\alpha_i\beta_j\Big)=\sum_{i\in I}\Big(\alpha_i\Big(\sum_{j\in J}\beta_j\Big)\Big)=\Big(\sum_{i\in I}\alpha_i\Big)\Big(\sum_{j\in J}\beta_j\Big).$$

Anillos de series formales de potencias Vamos a estudiar las series de potencias en cuerpos completos no arquimedianos, pero antes conviene introducir un "marco algebraico":

Definición 5.52 Si K es un cuerpo, definimos el *anillo de las series formales de potencias* en K (de una indeterminada) como el conjunto $K[[x]]$ de todas las sucesiones en K.

En lugar de representar sus elementos en la forma $\{a_n\}_{n=0}^\infty$, los representaremos en la forma

$$\sum_{n=0}^\infty a_nx^n,$$

pero hay que entender que la suma es "formal", es decir, que no hay en realidad ninguna suma, sino que la "suma" no es más que la sucesión de los coeficientes. Es fácil ver que $K[[x]]$ se convierte en un anillo conmutativo y unitario con las operaciones

$$\begin{aligned}\sum_{n=0}^\infty a_nx^n+\sum_{n=0}^\infty b_nx^n &= \sum_{n=0}^\infty (a_n+b_n)x^n,\\ \Big(\sum_{n=0}^\infty a_nx^n\Big)\Big(\sum_{n=0}^\infty b_nx^n\Big) &= \sum_{n=0}^\infty\Big(\sum_{k=0}^n a_kb_{n-k}\Big)x^n.\end{aligned}$$

También es claro que podemos considerar al anillo de polinomios $K[x]$ como subanillo de $K[[x]]$ sin más que identificar los polinomios con las series formales que tienen nulos sus coeficientes a partir de uno dado.

Notemos que $K[[x]]$ es un dominio íntegro, pues si

$$F=\sum_{n=0}^\infty a_nx^n,\qquad G=\sum_{n=0}^\infty b_nx^n$$

son dos series formales de potencias no nulas, podemos considerar los mínimos índices tales que $a_{m_0}\neq 0\neq b_{m_0}$, y es claro entonces que $a_{m_0}b_{n_0}\neq 0$ es el menor coeficiente no nulo de FG, lo que prueba que $FG\neq 0$.

Más aún, podemos definir $v : K[[x]]\setminus\{0\}\longrightarrow\mathbb{N}$ de modo que $v(F)$ sea el menor índice n tal que el coeficiente a_n de F es no nulo, y es inmediato comprobar que v cumple las propiedades de la definición de valoración 5.11 salvo por el hecho de que $K[[x]]$ no es un cuerpo.

Ahora bien, si llamamos $K((x))$ al cuerpo de cocientes de $K[[x]]$, también es inmediato que v se extiende a una valoración $v : K((x)) \setminus \{0\} \longrightarrow \mathbb{Z}$ mediante $v(F/G) = v(F) - v(G)$.

Notemos que la restricción de v a $K(x)$ no es sino la valoración definida por el primo x del dominio de Dedekind $K[x]$. Vamos a probar que $K((x))$, con su estructura de cuerpo métrico discreto dada por la valoración v, es precisamente la compleción del cuerpo $K(x)$. Primero conviene probar lo siguiente:

Teorema 5.53 *Si K es un cuerpo, una serie $F = \sum_{n=0}^{\infty} a_n x^n$ es una unidad en $K[[x]]$ si y sólo si $a_0 \neq 0$ o, equivalentemente, si y sólo si $v(F) = 0$.*

Demostración: Si F es una unidad y $F^{-1} = \sum_{n=0}^{\infty} b_n x^n$, es claro que la relación $FF^{-1} = 1$ implica $a_0 b_0 = 1$, luego $a_0 \neq 0$.

Recíprocamente, si $a_0 \neq 0$, podemos definir recurrentemente una sucesión de coeficientes $\{b_n\}_{n=0}^{\infty}$ despejando en las relaciones

$$a_0 b_0 = 1, \quad a_0 b_1 + a_1 b_0 = 0, \quad a_0 b_2 + a_1 b_1 + a_2 b_0 = 0, \quad \ldots$$

y es claro que la serie F^{-1} definida por esta sucesión cumple $FF^{-1} = 1$. ∎

Como consecuencia, si $F = \sum_{n=0}^{\infty} a_n x^n$ cumple $v(F) = k$, eso significa que $a_0 = \cdots a_{k-1} = 0$ y podemos factorizar

$$F = x^k \sum_{n=0}^{\infty} a_{n+k} x^n,$$

donde el segundo factor es una unidad, es decir, que todo elemento no nulo de $K[[x]]$ se expresa (claramente de forma única) como $F = x^k E$, donde $E \in K[[x]]$ es una unidad (es decir, que cumple $v(E) = 0$) y $k = v(F)$. Por lo tanto, toda fracción no nula de $K((x))$ se expresa de forma única como

$$\frac{F}{G} = \frac{x^k E_1}{x^l E_2} = x^m E,$$

donde $E \in K[[x]]$ es una unidad y $m = k - l = v(F) - v(G) = v(F/G)$.

A partir de aquí adoptamos el convenio de escribir

$$x^k \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n x^{n+k} = \sum_{n=k}^{\infty} a_{n-k} x^n$$

incluso si k es negativo, y así hemos probado lo siguiente:

Teorema 5.54 *Si K es un cuerpo, cada elemento $F \in K((x))$ no nulo se expresa en forma única como serie*

$$F = \sum_{n=k}^{\infty} a_n x^n,$$

donde $k = v(F) \in \mathbb{Z}$ y $a_k \neq 0$.

Así, $v(F)$ es el menor índice de un coeficiente no nulo de la serie F, incluso si dicho índice es negativo. Ahora es inmediato que $K[[x]]$ es el anillo de enteros de $K((x))$ como cuerpo métrico discreto.

Teorema 5.55 *Si K es un cuerpo, $K((x))$ es la compleción del cuerpo $K(x)$ respecto de la valoración inducida por el primo x de $K[x]$.*

Demostración: Para probar que $K((x))$ es completo consideramos una sucesión de Cauchy en $K((x))$, digamos

$$S_k = \sum_{n=m_k}^{\infty} a_{k,n}x^n.$$

Esto significa que, para cada número natural N, existe un k_0 tal que si $k_0 \le k \le k'$, se cumple que $v(S_{k'} - S_k) \ge N$, lo que a su vez significa que $a_{k,n} = a_{k',n}$ para todo $n < N$. En otros términos, cada sucesión $\{a_{k,n}\}_{k=0}^{\infty}$ es finalmente igual a un valor constante a_n, con lo que podemos definir una serie

$$S = \sum_{n=m}^{\infty} a_n x^n \in K((x)).$$

Notemos que tiene que haber un mínimo índice m tal que $a_m \neq 0$, pues toda sucesión de Cauchy está acotada, es decir, $|S_n|$ tiene una cota superios, lo que equivale a que $v(S_n)$ tiene una cota inferior $m \in \mathbb{Z}$, de modo que si $n < m$ entonces $a_{k,n} = 0$ para todo k, luego $a_n = 0$. Ahora es fácil ver que $\lim_k S_k = S$.

Por otra parte, dado cualquier $S \in K((x))$ es claro que la sucesión de sus sumas parciales

$$S_N = \sum_{n=m}^{N} a_n x^n \in K(x)$$

converge a S, luego $K(x)$ es denso en $K((x))$, y esto implica que $K((x))$ es la compleción de $K(x)$. ∎

Si K es un cuerpo métrico completo, el teorema [An 3.59] prueba que cada elemento $F \in K[[x]]$ converge absolutamente en una bola abierta B de centro 0 (o en $\varnothing$ o en todo K), en la cual determina una función $F : B \longrightarrow K$.

Es evidente que la función asociada a $F + G$ es la suma de las funciones asociadas a F y G, mientras que, por [An 2.86], la función asociada a FG es el producto de las funciones asociadas a F y G. Si F es un polinomio, converge en todo K y su función asociada es la sustitución usual.

Podemos definir como sigue una sustitución en $K[[x]]$: Sean dos series

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \quad \text{y} \quad g(x) = \sum_{n=1}^{\infty} b_n x^n,$$

la segunda sin término independiente.

Para cada natural n sea $a_n\, g(x)^n = \sum_{k=n}^{\infty} c_{nk}x^k$. Entonces definimos

$$(g \circ f)(x) = a_0 + \sum_{k=1}^{\infty}\sum_{n=1}^{k} c_{nk}x^k.$$

Si f y g son series de $\mathbb{C}[[x]]$ de modo que g no tiene término independiente, g converge en un disco de centro 0 y f converge en la imagen por g de dicho disco, entonces $g \circ f$ converge en el disco a la composición de g y f. En efecto, la serie

$$a_0 + \sum_{n=1}^{\infty}\sum_{k=n}^{\infty} c_{nk}x^k$$

converge a $g \circ f$ en un entorno de 0, su derivada r-ésima es

$$\sum_{n=1}^{\infty}\sum_{k=\text{máx}\{n,r\}}^{\infty} c_{nk}k(k-1)\cdots(k-r+1)x^{k-r},$$

y en 0 queda

$$r!\sum_{n=1}^{r} c_{nr},$$

luego su serie de Taylor es la que hemos definido como $g \circ f$. Ahora vamos a probar que el mismo resultado es válido en nuestro contexto.

Teorema 5.56 *Sea K un cuerpo métrico discreto completo. Sean f y g dos series de potencias en K tales que $f(x)$ converja para $v(x) \geq r$, $g(x)$ tenga término independiente nulo, converja para un cierto $y \in K$ y $v(b_m y^m) \geq r$ para todo $m \geq 1$ (siendo b_m el coeficiente m-simo de g). Entonces $(g\circ f)(y)$ converge a $f\big(g(y)\big)$.*

Demostración: Siguiendo la notación que hemos empleado para definir $g \circ f$, consideremos la serie $\sum_{i,j} c_{ij}y^j$. Por definición de c_{nm} tenemos que

$$c_{nm}y^m = \sum_{\substack{t_1,\ldots,t_n\geq 1\\ t_1+\cdots+t_n=m}} a_n b_{t_1}y^{t_1}\cdots b_{t_n}y^{t_n}.$$

Sea $N = \text{mín}\big\{v(b_m y^m)\big\} \geq r$. Entonces

$$v(c_{nm}y^m) \geq \text{mín}\big\{v(a_n b_{t_1}y^{t_1}\cdots b_{t_n}y^{t_n})\big\} \geq v(a_n) + nN.$$

Como $N = v(x_0)$ para un x_0 y $f(x_0)$ converge, resulta que $v(a_n)+nN = v(a_n x_0^n)$ tiende a infinito, luego lo mismo le ocurre a $v(c_{nm}y^m)$ (uniformemente en m). Esto significa que $v(c_{nm}y^m)$ se hace arbitrariamente grande para todo $n \geq n_0$ y todo m. Para los $n < n_0$ usamos que $a_n\, g(y)^n = \sum_{m=n}^{\infty} c_{nm}y^m$ converge, luego $v(c_{nm}y^m)$ tiende a infinito para cada n. En definitiva, existe un m_0 tal que si

$n \geq n_0$ o $m \geq m_0$ entonces $v(c_{nm}y^m)$ es arbitrariamente grande. Esto garantiza la convergencia de la serie doble

$$(g \circ f)(y) = a_0 + \sum_{k=1}^{\infty} \sum_{n=1}^{k} c_{nk} y^k$$

y, como entonces podemos reordenar los sumandos, resulta que

$$(g \circ f)(y) = \sum_{n=0}^{\infty} \sum_{k=n}^{\infty} c_{nk} y^k = \sum_{n=0}^{\infty} a_n \big(g(y)\big)^n = f\big(g(y)\big). \qquad \blacksquare$$

Fijemos ahora un cuerpo numérico K y sea $\mathfrak{p}$ un ideal primo de su anillo de enteros. Sea p el primo racional divisible entre $\mathfrak{p}$. Digamos que $p = \mathfrak{p}^e\mathfrak{a}$, para cierto ideal $\mathfrak{a}$ primo con $\mathfrak{p}$. Tenemos entonces la relación $v_\mathfrak{p}(r) = ev_p(r)$ para todo número racional r. Vamos a estudiar el comportamiento de las series de potencias en $K_\mathfrak{p}$

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \qquad \log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n.$$

En primer lugar calcularemos su dominio de convergencia. Claramente

$$v_p(n!) = E(n/p) + E(n/p^2) + \cdots,$$

donde E denota la parte entera (observemos que $E(n/p^i)$ es el número de múltiplos de p^i menores que n), luego

$$v_\mathfrak{p}(n!) = e(E(n/p) + E(n/p^2) + \cdots) < e(n/p + n/p^2 + \cdots) = \frac{en}{p-1},$$

con lo que

$$v_\mathfrak{p}\left(\frac{x^n}{n!}\right) = nv_\mathfrak{p}(x) - v_\mathfrak{p}(n!) > n\left(v_\mathfrak{p}(x) - \frac{e}{p-1}\right).$$

Si $v_\mathfrak{p}(x) > e/(p-1)$, entonces $v_\mathfrak{p}(x^n/n!)$ tiende a infinito y $\exp x$ converge. Por el contrario, si $v_\mathfrak{p}(x) \leq e/(p-1)$, para $n = p^m$ tenemos

$$\begin{aligned} v_\mathfrak{p}\left(\frac{x^n}{n!}\right) &= nv_\mathfrak{p}(x) - e(p^{m-1} + \cdots + p + 1) = nv_\mathfrak{p}(x) - e\,\frac{n-1}{p-1} \\ &= n\left(v_\mathfrak{p}(x) - \frac{e}{p-1}\right) + \frac{e}{p-1} \leq \frac{e}{p-1}, \end{aligned}$$

luego el término general de $\exp x$ no converge a 0 y la serie diverge.

Concluimos que la serie $\exp x$ converge exactamente en $\mathfrak{p}^\kappa$, siendo

$$\kappa = E\left(\frac{e}{p-1}\right) + 1.$$

La fórmula del producto de series nos da sin dificultad que, para todo par de elementos de $\mathfrak{p}^\kappa$, se cumple $\exp(x+y) = \exp x \exp y$.

Nos ocupamos ahora del logaritmo. Si $v_\mathfrak{p}(x) \leq 0$ es claro que el término general de $\log(1+x)$ no converge a 0. Si $v_\mathfrak{p}(x) \geq 1$ entonces para cada natural $n = p^a m$ se cumple que $p^a \leq n$ y $v_\mathfrak{p}(n) = ea \leq e(\log n/\log p)$. Por lo tanto

$$v_\mathfrak{p}\left(\frac{x^n}{n}\right) = nv_\mathfrak{p}(x) - v_\mathfrak{p}(n) \geq nv_\mathfrak{p}(x) - e\,\frac{\log n}{\log p},$$

y la expresión de la derecha tiende a infinito con n, lo que significa que el término general de $\log(1+x)$ tiende a 0 y en consecuencia la serie converge.

La conclusión es que $\log(1+x)$ converge exactamente cuando $v_\mathfrak{p}(x) \geq 1$ o, lo que es lo mismo, $\log x$ está definido en $1+\mathfrak{p}$. Probemos que si $\epsilon_1, \epsilon_2 \in 1+\mathfrak{p}$, entonces $\log \epsilon_1\epsilon_2 = \log \epsilon_1 + \log \epsilon_2$.

En efecto, sea $\epsilon_1 = 1+x$, $\epsilon_2 = 1+y$. Supongamos que $v_\mathfrak{p}(y) \geq v_\mathfrak{p}(x)$, de modo que $y = tx$, con $v_\mathfrak{p}(t) \geq 0$ (suponemos $x \neq 0$, pues en caso contrario el resultado es trivial).

Vamos a considerar paralelamente el caso en que t y x son números complejos de módulo menor que 1. En cualquier caso se cumple

$$(1+x)(1+y) = 1 + (t+1)x + tx^2.$$

Consideramos $(t+1)x + tx^2$ como una serie de potencias en x. Puesto que $v_\mathfrak{p}(x) \geq 1$, el teorema 5.56 nos da que

$$\log \epsilon_1\epsilon_2 = \sum_{k=1}^{\infty} c_k(t)x^k,$$

donde $c_k(t)$ es un cierto polinomio en t con coeficientes racionales. Esto también es cierto (con el mismo polinomio) en el caso complejo. También en ambos casos se cumple

$$\log \epsilon_1 + \log \epsilon_2 = \log(1+x) + \log(1+tx) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}(1+t^k)x^k.$$

Pero en el caso complejo sabemos que ambas series son iguales, luego

$$c_k(t) = \frac{(-1)^{k+1}}{k}(1+t^k)$$

para todo número complejo t tal que $|t| < 1$, pero esto implica que ambos polinomios son idénticos, luego la igualdad es cierta también cuando t está en K, y de aquí se sigue la igualdad de las series en este caso último caso.

Con esto hemos demostrado el teorema siguiente:

Teorema 5.57 *Sea K un cuerpo métrico discreto completo de característica 0. Supongamos que $v(r) = ev_p(r)$ para todo número racional r y sea*

$$\kappa = E\left(\frac{e}{p-1}\right) + 1.$$

Entonces las funciones

$$\exp : \mathfrak{p}^\kappa \longrightarrow K_\mathfrak{p}^\times, \qquad \log : 1+\mathfrak{p} \longrightarrow K_\mathfrak{p}^+$$

son homomorfismos de grupos.

En general no es cierto que estas funciones sean una la inversa de la otra. No obstante sí es cierto cuando restringimos el logaritmo a un dominio menor.

Teorema 5.58 *En las condiciones del teorema anterior,* $\exp : \mathfrak{p}^\kappa \longrightarrow 1+\mathfrak{p}^\kappa$ *es un isomorfismo y su inversa es* $\log : 1+\mathfrak{p}^\kappa \longrightarrow \mathfrak{p}^\kappa$.

Demostración: En primer lugar demostraremos que $\exp : \mathfrak{p}^\kappa \longrightarrow 1+\mathfrak{p}^\kappa$ y $\log : 1+\mathfrak{p}^\kappa \longrightarrow \mathfrak{p}^\kappa$. Si $1+x \in 1+\mathfrak{p}^\kappa$ entonces $v_\mathfrak{p}(x) \geq \kappa$. En el caso $1 \leq n \leq p-1$ se cumple $v_\mathfrak{p}(x^n/n) \geq n\kappa \geq \kappa$, mientras que si $2 \leq p \leq n$ tenemos

$$\begin{aligned} v_\mathfrak{p}\left(\frac{x^n}{n}\right) - \kappa &\geq (n-1)\kappa - v_\mathfrak{p}(n) > (n-1)\,\frac{e}{p-1} - e\,\frac{\log n}{\log p} \\ &= \frac{e(n-1)}{\log p}\left(\frac{\log p}{p-1} - \frac{\log n}{n-1}\right) \geq 0, \end{aligned}$$

(usando que la función $\log t/(t-1)$ es monótona decreciente para $t \geq 2$).

Así, todos los términos de la serie $\log(1+x)$ cumplen $v_\mathfrak{p}(x^n/n) \geq \kappa$, y por la continuidad de $v_\mathfrak{p}$ podemos concluir que $v_\mathfrak{p}\big(\log(1+x)\big) \geq \kappa$, o sea, $\log(1+x) \in A$.

Sea ahora $x \in A$. Hemos de probar que $v_\mathfrak{p}(x^n/n!) \geq \kappa$ para $n \geq 1$. Sea $p^s \leq n < p^{s+1}$. Así

$$\begin{aligned} v_\mathfrak{p}(x^n/n!) - \kappa &\geq (n-1)\kappa - e\big(E(n/p) + E(n/p^2) + \cdots + E(n/p^s)\big) \\ &\geq \frac{(n-1)e}{p-1} - \frac{en}{p^s}\,\frac{p^s-1}{p-1} \geq 0. \end{aligned}$$

Para probar que las dos aplicaciones son mutuamente inversas tomamos $x \in A$ y consideramos $\log\exp x = \log\big(1 + (\exp x - 1)\big)$. La serie $\exp x - 1$ tiene término independiente nulo y los razonamientos anteriores muestran que podemos aplicar el teorema 5.56, con lo que $\log\exp x$ es la serie de potencias que resulta de componer las series de ambas funciones.

Pero lo mismo es válido para las funciones complejas, y en este caso se cumple que $\log\exp x = x$, es decir, la composición formal de las series de potencias es simplemente la serie x, por lo que $\log\exp x = x$ para todo $x \in A$. Igualmente se razona con la composición en sentido inverso. ∎

Para el caso concreto de los números p-ádicos, donde p es un primo impar, se cumple $\kappa = 1$. Observemos que los números de la forma $1+x$ tales que $p \mid x$ son exactamente las unidades p-ádicas congruentes con 1 módulo p. A estas unidades se las llama *unidades principales* de $\mathbb{Q}_p$. Así pues, las funciones exponencial y logarítmica p-ádicas son isomorfismos entre el grupo aditivo de los enteros p-ádicos múltiplos de p y el grupo multiplicativo de las unidades principales. Si $p = 2$ se cumple $\kappa = 2$, y en efecto el logaritmo no es biyectivo en todo su dominio: $\log 1 = \log(-1) = 0$.

5.7 Complementos

Recogemos aquí algunos hechos variados de interés sobre los cuerpos numéricos y sus compleciones. Ninguno de ellos será necesario después.

Los divisores primos de los cuerpos numéricos Comenzamos probando que los únicos divisores primos en un cuerpo numérico k son los que de hecho estamos considerando, es decir, los inducidos por los monomorfismos $k \longrightarrow \mathbb{K}_p$ para cada primo racional p (finito o infinito). Esto se prueba fácilmente una vez lo tenemos para $\mathbb{Q}$:

Teorema 5.59 (Teorema de Ostrowski) *Los únicos divisores primos de $\mathbb{Q}$ son los inducidos por los primos de $\mathbb{Z}$ y el divisor ∞ inducido por el valor absoluto usual.*

Demostración: Fijemos un valor absoluto no trivial en $\mathbb{Q}$. Supongamos en primer lugar que existe un número natural a tal que $|a| > 1$. Puesto que, para todo natural n,

$$|n| = |1 + \cdots + 1| \leq |1| + \cdots + |1| = n,$$

se cumple $|a| = a^\alpha$, con $0 < \alpha \leq 1$.

Cada número natural N puede expresarse en base a, es decir, en la forma

$$N = x_0 + x_1 a + \cdots + x_{k-1} a^{k-1},$$

donde cada x_i es un número natural $0 \leq x_i < a$ y $x_{k-1} \neq 0$. De aquí se sigue que $a^{k-1} \leq N < a^k$. Entonces

$$|N| \leq |x_0| + |x_1|\,|a| + \cdots + |x_{k-1}|\,|a|^{k-1} \leq (a-1)(1 + a^\alpha + \cdots + a^{(k-1)\alpha})$$

$$= (a-1)\,\frac{a^{k\alpha}-1}{a^\alpha - 1} < (a-1)\,\frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1)a^\alpha}{a^\alpha - 1}\,a^{(k-1)\alpha} \leq KN^\alpha,$$

donde K es una constante que no depende de N. Cambiando N por N^m obtenemos $|N|^m \leq KN^{m\alpha}$, luego $|N| \leq \sqrt[m]{K}\,N^\alpha$, y haciendo tender m a infinito llegamos a que $|N| \leq N^\alpha$, para todo natural N.

Ahora tomamos $N = a^k - b$, donde $0 < b \leq a^k - a^{k-1}$. Por la desigualdad triangular

$$|N| \geq |a^k| - |b| = a^{\alpha k} - |b| \geq a^{\alpha k} - b^\alpha \geq a^{\alpha k} - (a^k - a^{k-1})^\alpha$$

$$= \left(1 - \left(1 - \frac{1}{a}\right)^\alpha\right) a^{\alpha k} = K_1 a^{\alpha k} > K_1 N^\alpha,$$

donde la constante K_1 no depende de N.

De nuevo cambiamos N por N^m, lo que nos da $|N|^m > K_1 N^{m\alpha}$, y de aquí $|N| > \sqrt[n]{K_1}\,N^\alpha$. Haciendo tender m a infinito queda $|N| \geq N^\alpha$.

En resumen, hemos probado que $|N| = N^\alpha$ para todo número natural N, y es claro que de aquí se sigue que $|r| = |r|_\infty^\alpha$ para todo $r \in \mathbb{Q}$, luego el valor absoluto dado induce el primo ∞.

Supongamos ahora que $|a| \leq 1$ para todo número natural a. No puede ser que $|a| = 1$ para todo número natural, pues en tal caso el valor absoluto sería trivial. Claramente ha de haber un primo p tal que $|p| < 1$. Veamos que es único. Si $|q| < 1$ para otro primo q, entonces podemos tomar exponentes k y l tales que $|p^k| < 1/2$ y $|q^l| < 1/2$. Existen enteros u y v tales que $up^k + vq^l = 1$, y esto nos lleva a una contradicción:

$$1 = |1| = |up^k + vq^l| \leq |u|\,|p^k| + |v|\,|q^l| < \frac{1}{2} + \frac{1}{2} < 1.$$

Así pues, $|q| = 1$ para todo primo $q \neq p$. Sea $|p| = \rho < 1$. Todo número racional no nulo puede expresarse como $r = p^m(a/b)$, donde $m \in \mathbb{Z}$ y a y b son números naturales primos con p. Claramente entonces $|r| = \rho^m$, luego el valor absoluto dado es el inducido por p. ∎

En la prueba del teorema se ve que los únicos valores absolutos arquimedianos de $\mathbb{Q}$ son los de la forma $|\ |_\infty^\alpha$, para $0 < \alpha \leq 1$. De aquí se sigue que cada valor absoluto arquimediano en $\mathbb{R}$ ha de ser también de esta forma, luego cada valor absoluto arquimediano de $\mathbb{R}$ se extiende a un valor absoluto en $\mathbb{C}$ equivalente al usual (usando 5.3).

Teorema 5.60 *Los únicos divisores en un cuerpo numérico k son los inducidos por los monomorfismos $k \longrightarrow \mathbb{K}_p$, donde p es un primo en $\mathbb{Q}$.*

Demostración: Fijemos un valor absoluto no trivial en k y veamos que su restricción a $\mathbb{Q}$ no puede ser trivial. En efecto, si lo fuera tomamos una $\mathbb{Q}$-base de k, digamos $v_1, \ldots, v_n$, y entonces todo $x \in k$ se expresa en la forma $x = r_1v_1 + \cdots + r_nv_n$, con lo que

$$|x| \leq |x_1|\,|v_1| + \cdots + |x_n|\,|v_n| \leq |v_1| + \cdots + |v_n|,$$

pero un valor absoluto no trivial no puede estar acotado (existe un $x \in k$ con $|x| > 1$ y sus potencias tienen valor absoluto arbitrariamente grande).

Según el teorema anterior, la restricción a $\mathbb{Q}$ del valor absoluto dado es el inducido por un primo p de $\mathbb{Q}$ (finito o infinito).

Sea $\overline{k}$ la compleción de k respecto al valor absoluto dado. Entonces la clausura de $\mathbb{Q}$ en $\overline{k}$ es topológicamente isomorfa a $\mathbb{Q}_p$ y el cuerpo $\mathbb{Q}_p\,k$ es una extensión finita de $\mathbb{Q}_p$, luego es completo por el teorema 5.25. En definitiva, es cerrado y denso en $\overline{k}$, luego $\overline{k} = \mathbb{Q}_p\,k$. Podemos tomar una clausura algebraica $\mathbb{K}_p$ de $\mathbb{Q}_p$ que contenga a $\overline{k}$, y entonces la inclusión $k \longrightarrow \mathbb{K}_p$ induce el valor absoluto de partida. ∎

Cuerpos completos arquimedianos Ahora probamos que los únicos cuerpos métricos completos arquimedianos son $\mathbb{R}$ y $\mathbb{C}$ con sus divisores usuales.

En efecto, sea K un cuerpo arquimediano completo. Fijado un valor absoluto en K, su restricción a $\mathbb{Q}$ ha de corresponder al único divisor primo arquimediano de $\mathbb{Q}$, es decir, a la clase de equivalencia del valor absoluto usual. Por lo tanto, la clausura de $\mathbb{Q}$ en K es un cuerpo isomorfo a $\mathbb{R}$ (al que llamaremos $\mathbb{R}$) y la restricción a $\mathbb{R}$ del valor absoluto de K es equivalente al valor absoluto usual en $\mathbb{R}$. Basta probar que la extensión $K/\mathbb{R}$ es algebraica, pues entonces K será $\mathbb{R}$ o $\mathbb{C}$, y su valor absoluto será equivalente al usual por el teorema 5.23.

Fijemos $\xi \in K$ y veamos que es algebraico sobre $\mathbb{R}$. Para cada $z \in \mathbb{C}$, los números $z + \overline{z}$ y $z\overline{z}$ son reales, luego podemos definir la aplicación $f : \mathbb{C} \longrightarrow \mathbb{R}$ dada por $f(z) = |\xi^2 - (z + \overline{z})\xi + z\overline{z}|$, donde el valor absoluto es el de K.

La aplicación f es continua, pues

$$|f(z_1) - f(z_2)| \leq |(z_2 + \overline{z}_2) - (z_1 + \overline{z}_1)|\,|\xi| + |z_1\overline{z}_1 - z_2\overline{z}_2|$$

$$\leq |z_2 - z_1|\,|\xi| + |\overline{z}_2 - \overline{z}_1|\,|\xi| + |z_1\overline{z}_1 - z_2\overline{z}_2|,$$

considerando en $\mathbb{C}$ la extensión de la restricción a $\mathbb{R}$ del valor absoluto de K (véase el comentario tras el teorema de Ostrowski).

Por otra parte, $\lim_{z\to\infty} f(z) = +\infty$, pues

$$f(z) \geq |z\overline{z}| - |\xi^2| - |z + \overline{z}|\,|\xi| \geq |z|^2 - |\xi^2| - 2|\xi|\,|z|,$$

(pues la conjugación es una isometría).

Sea $m = \text{ínf}\{f(z) \mid z \in \mathbb{C}\} \geq 0$. El hecho de que f tienda a infinito en infinito implica que m es también el ínfimo de f en un compacto, luego existe un $z \in \mathbb{C}$ tal que $f(z) = m$.

Sea $S = \{z \in \mathbb{C} \mid f(z) = m\}$. Se trata de un compacto no vacío, luego existe un número $z_0 \in S$ tal que $|z_0| \geq |z|$ para todo $z \in S$.

Basta probar que $m = 0$, pues entonces la ecuación $f(z_0) = 0$ probará que ξ es algebraico sobre $\mathbb{R}$. SI m es positivo tomamos $0 < \epsilon < \text{mín}\{m, 1\}$ y consideramos el polinomio

$$g(x) = x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0 + \epsilon \in \mathbb{R}[x].$$

Sean z_1, z_2 sus raíces en $\mathbb{C}$. Entonces $z_1 z_2 = z_0\overline{z}_0 + \epsilon$, luego $|z_1| > |z_0|$ o bien $|z_2| > |z_0|$. Supongamos por ejemplo la primera desigualdad. Entonces $z_1 \notin S$.

Tomemos un número natural $n \geq 1$ y definamos

$$G(x) = (x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0)^n - (-\epsilon)^n.$$

Entonces $G(x)$ es un polinomio en $\mathbb{R}[x]$ de grado $2n$. Sean $\beta_1, \ldots, \beta_{2n}$ sus raíces en $\mathbb{C}$. Como $G(z_1) = 0$ podemos suponer que $z_1 = \beta_1$. Se cumple

$$G(x) = \prod_{i=1}^{2n}(x - \beta_i) = \prod_{i=1}^{2n}(x - \overline{\beta}_i),$$

luego

$$G(x)^2 = \prod_{i=1}^{2n}(x - \beta_i)(x - \overline{\beta}_i) = \prod_{i=1}^{2n}\big(x^2 - (\beta_i + \overline{\beta}_i)x + \beta_i\overline{\beta}_i\big).$$

Como todos los factores son polinomios en $\mathbb{R}[x]$ tiene sentido calcular

$$|G(\xi)^2| = \prod_{i=1}^{2n} f(\beta_i) \geq f(z_1)\, m^{2n-1}.$$

Por otra parte

$$|G(\xi)| \leq f(z_0)^n + \epsilon^n = m^n + \epsilon^n.$$

Uniendo ambas desigualdades resulta que $f(z_1)m^{2n-1} \leq (m^n + \epsilon^n)^2$, luego

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\epsilon}{m}\right)^n\right)^2,$$

y haciendo tender n a infinito queda $f(z_1) \leq m$, luego $f(z_1) = m$ y $z_1 \in S$, contradicción. ∎

Cuerpos ordenados "completos" no arquimedianos Sea K un cuerpo ordenado y llamemos $P \subset K((x))$ al conjunto formado por la serie nula y las series

$$F = \sum_{n=k}^{\infty} a_n x^n,$$

tales que $a_k > 0$. Es inmediato comprobar que P es un cono positivo en $K((x))$ [Al 5.63], es decir, que cumple:

1. Si $F, G \in P$, entonces $F + G \in P$ y $FG \in P$,
2. $P \cap (-P) = \{0\}$,

lo que se traduce en que $K((x))$ se convierte en un cuerpo ordenado cuando consideramos en él la relación $F \leq G$ si y sólo si $G - F \in P$.

Se trata de un cuerpo ordenado no arquimediano, en el sentido de la definición [An 1.6], pues si tomamos $M = 1/x > 0$ y $\epsilon = 1 > 0$ no existe ningún número natural tal que $M < n\epsilon$, es decir, que se cumplen $n < 1/x$ para todo número natural n, ya que (como $n, x > 0$) esto equivale a que $nx < 1$ o a que $1 - nx > 0$, lo cual es cierto, pues $1 - nx \in P$.

La aplicación $d : K((x)) \times K((x)) \longrightarrow K((x))$ dada por $d(F, G) = |F - G|$ es una distancia en $K((x))$ en el sentido de la definición [An 1.18] salvo por el hecho de que el cuerpo ordenado $R = K((x))$ no es arquimediano. Pese a ello, tiene sentido hablar de sucesiones convergentes y sucesiones de Cauchy en $K((x))$ en el sentido de las definiciones [An 1.20] y [An 1.29], respectivamente.

Veamos que una sucesión $\{F_r\}_{r=0}^{\infty}$ en $K((x))$ converge a $F \in K((x))$ en el sentido de [Am 1.20] si y sólo si converge a F respecto de la topología de $K((x))$ determinada por la valoración v.

En efecto, si la sucesión converge respecto de v, sea $\epsilon > 0$ en $K((x))$, de modo que

$$\epsilon = \sum_{n=k}^{\infty} a_n x^n, \qquad a_k > 0.$$

Entonces existe un $r_0 \in \mathbb{N}$ tal que si $r \geq r_0$ se cumple $v(F_r - F) \geq k+1$. Esto significa que $F_r - F$ tiene nulos sus coeficientes de índice menor o igual que k, y lo mismo vale para $|F_r - F|$, luego el menor coeficiente no nulo de $\epsilon - |F_r - F|$ es $a_k > 0$, luego $\epsilon - |F_r - F| \in P$, luego $|F_r - F| < \epsilon$ y la sucesión converge en el sentido de [An 1.20].

Recíprocamente, si la sucesión converge en el sentido de [An 1.20], dado $N \in \mathbb{N}$, tomamos $\epsilon = x^N$ y tenemos que existe un $r_0 \in \mathbb{N}$ tal que si $r \geq r_0$ entonces $0 \leq |F_r - F| < x^N$, luego $x^N - |F_r - F| \in P$, y esto requiere que todos los coeficientes de $|F_r - F|$ de índice menor que N sean nulos (pues en caso contrario, el de menor índice sería positivo y el coeficiente de menor índice en $x^N - |F_r - F|$ sería negativo). Por lo tanto, $v(F_r - F) \geq N$ y la sucesión converge respecto de v.

Más precisamente, la "distancia" d que toma valores en $K((x))$ aunque éste no sea un cuerpo arquimediano define igualmente una topología en $K((x))$ en el sentido de [An 2.7] y dicha topología coincide con la inducida por la valoración v (que a su vez está inducida por una distancia "auténtica" en $K((x))$).

En efecto, una base de entornos de $F \in K((x))$ respecto de la topología inducida por d la forman las bolas abiertas $B_\epsilon(F)$, con $\epsilon > 0$, pero si

$$\epsilon = \sum_{n=k}^{\infty} a_n x^n, \qquad a_k > 0,$$

es claro que $0 < x^{k+1} < \epsilon$, luego $F \in B_{x^{k+1}}(F) \subset B_\epsilon(F)$, luego en realidad una base de entornos de F la forman las bolas $B_{x^k}(F)$, con $k \in \mathbb{N}$.

Ahora basta observar que $|F - G| < x^k$ implica que $v(F - G) \geq k$ y, recíprocamente, $v(F - G) \geq k + 1$ implica que $|F - G| < x^k$, por lo que toda bola abierta de centro F respecto de v contiene una bola abierta respecto de d y viceversa.

Finalmente probamos las sucesiones de Cauchy en $K((x))$ en el sentido de [An 1.29] son convergentes.

En efecto, si $\{F_r\}_{r=0}^{\infty}$ es una sucesión de Cauchy en $K((x))$, dado $N \in \mathbb{N}$, tomamos $\epsilon = x^N > 0$, y por definición existe un $r_0 \in \mathbb{N}$ tal que si $r, s \geq r_0$, entonces $0 \leq |F_r - F_s| < x^N$, lo que implica que $F_r - F_s$ tiene nulos todos sus coeficientes de índice menor que N, luego $v(F_r - F_s) \geq N$, luego la sucesión es de Cauchy respecto de v, luego converge respecto de v, luego también en el sentido de [An 1.20].

Vemos así que $K((x))$ es un cuerpo ordenado "completo" respecto del concepto de sucesión de Cauchy que podemos definir a partir de su relación de orden (olvidando el requisito de que la "distancia" tome valores en $\mathbb{R}$ o, al menos, en un cuerpo ordenado arquimediano), pero no es completo en el sentido del orden (definición [An 1.4]), ya que todo cuerpo ordenado completo en este sentido es arquimediano (teorema [An 1.7]).

Este ejemplo muestra que cuando en [An 1.13] definimos $\mathbb{R}$ como cualquier cuerpo ordenado completo, es fundamental entender que hablamos de un cuerpo completo como conjunto ordenado, es decir, en el sentido de [An 1.4], lo cual implica ya que es arquimediano, pero no podríamos definir $\mathbb{R}$ como "el único" cuerpo ordenado completo en el sentido de [An 1.33], es decir, en el sentido de que las sucesiones de Cauchy definidas según [An 1.29] a partir de su relación de orden son convergentes en el sentido de [An 1.20], pues cualquier cuerpo $K((x))$ (para cualquier cuerpo ordenado K) es un cuerpo ordenado completo en este sentido y no es isomorfo a $\mathbb{R}$.

Si queremos caracterizar a $\mathbb{R}$ en términos de la completitud métrica tenemos que decir que $\mathbb{R}$ es el único cuerpo ordenado arquimediano y completo, es decir, el único cuerpo ordenado arquimediano en el que las sucesiones de Cauchy en el sentido de [An 1.29] son convergentes en el sentido de [An 1.20], pero ahora no podemos suprimir el requisito de que el cuerpo sea arquimediano pues esta completitud "métrica" (sin garantías de que la "distancia" tome valores en un cuerpo ordenado arquimediano) no implica la propiedad arquimediana.

Capítulo VI

Formas cuadráticas

En este capítulo mostraremos cómo usar los cuerpos de números p-ádicos en el estudio de las formas cuadráticas sobre cuerpos numéricos. Los resultados que obtendremos nos servirán para presentar con un enfoque moderno la teoría de Gauss los géneros de las formas cuadráticas binarias.

6.1 Hechos básicos

En todo lo que sigue se entenderá que K es un cuerpo, del que tan sólo supondremos que su característica es distinta de 2.

Definición 6.1 Una *forma cuadrática* sobre K es un polinomio homogéneo de grado 2, es decir, una suma de monomios de grado 2.

Por ejemplo: $3x^2 - 2y^2 + 6xz - 12xy + 5yz$ es una forma cuadrática sobre $\mathbb{Q}$ con tres variables. Observemos que la forma anterior puede escribirse como

$$3x^2 - 2y^2 + 0z^2 - 6xy - 6yx + 3xz + 3zx + (5/2)yz + (5/2)zy$$
$$= (x, y, z) \begin{pmatrix} 3 & -6 & 3 \\ -6 & -2 & 5/2 \\ 3 & 5/2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

y que, en general, toda forma cuadrática se puede expresar como

$$f(x_1, \ldots, x_n) = (x_1, \ldots, x_n) A (x_1, \ldots, x_n)^t,$$

donde A es una matriz simétrica en K unívocamente determinada por f.

Se llama *determinante* de una forma f al determinante de la matriz A. Una forma cuadrática es *regular* si su determinante es distinto de 0. En caso contrario se dice que la forma cuadrática es *singular*.

Diremos que una forma cuadrática f *representa* un elemento $\alpha \in K$ si existe un cierto $X \in K^n$ tal que $f(X) = \alpha$. En este sentido, toda forma cuadrática representa a 0. Sin embargo, es útil convenir en que una forma cuadrática *representa* 0 en K si y sólo si se tiene $f(X) = 0$ para un cierto $X \neq 0$.

A la hora de estudiar si un elemento está representado o no por una forma cuadrática, resulta de gran ayuda el concepto de equivalencia de formas:

Dos formas cuadráticas f y g son *equivalentes* si una se obtiene de la otra a partir de un cambio de variables lineal de determinante no nulo.

Es claro que dos formas cuadráticas equivalentes representan a los mismos elementos de K.

En otras palabras, si $f(X) = XAX^t$, las formas equivalentes a f son las que se obtienen haciendo $X = YC$, donde C es una matriz cuadrada con determinante no nulo, es decir, son las formas del tipo $g(Y) = f(YC) = Y\,CAC^t\,Y^t$. En resumen:

Dos formas cuadráticas $f(X) = XAX^t$, $g(X) = XBX^t$, son equivalentes si y sólo si existe una matriz regular C tal que $B = CAC^t$.

Observemos que si A es una matriz simétrica, una matriz del tipo CAC^t siempre es simétrica. Notemos también que si dos formas cuadráticas son equivalentes, una es regular si y sólo si lo es la otra. En [ITAl 11.16] exigíamos que la matriz de cambio de variables tuviera determinante ± 1. Ello se debía a que estábamos considerando formas cuadráticas sobre $\mathbb{Z}$, y al definir la equivalencia en un anillo hay que exigir que la matriz de cambio tenga inversa en el anillo. Así pues, al hablar de formas cuadráticas con coeficientes enteros habremos de distinguir entre *equivalencia entera* y *equivalencia racional.* Obviamente la primera implica la segunda.

Es claro que una condición necesaria para que dos formas cuadráticas sean equivalentes sobre un cuerpo K es que sus determinantes difieran en un factor que sea un cuadrado en K.

Vamos a buscar en cada clase de equivalencia de formas un representante lo más sencillo posible. Para ello nos basaremos en el teorema siguiente.

Teorema 6.2 *Si una forma cuadrática $f(x_1, \ldots, x_n)$ representa a un $\alpha \neq 0$ entonces es equivalente a una forma del tipo $\alpha x_1^2 + g(x_2, \ldots, x_n)$, donde g es una forma cuadrática con $n-1$ variables.*

Demostración: Sea A la matriz de f. Consideremos el espacio vectorial K^n y sea $v \in K^n$ de manera que $f(v) = \alpha$, o sea, $vAv^t = \alpha$. Claramente $v \neq 0$.

Sea $W = \{w \in K^n \mid vAw^t = 0\}$. Es fácil comprobar que se trata de un subespacio vectorial de K^n. Dado cualquier $x \in K^n$, la ecuación $vA(x-\lambda v)^t = 0$ tiene siempre solución $\lambda = (vAx^t)/\alpha$, es decir, para este valor de λ se cumple que $w = x - \lambda v \in W$, y así hemos probado que todo $x \in K^n$ se expresa como $x = \lambda v + w$, con $\lambda \in K$ y $w \in W$.

Así pues, $K^n = \langle v \rangle + W$, y obviamente la suma es directa, luego podemos tomar una base de K^n de la forma $v_1, \ldots, v_n$ con $v_1 = v$ y $v_2, \ldots, v_n \in W$.

Sea $e_1, \ldots, e_n$ la base canónica de K^n y C la matriz de cambio de base, es decir, tal que para todo i se cumple $v_i = e_i C$.

La matriz $B = CAC^t$ determina una forma cuadrática g equivalente a la dada. La primera fila de esta matriz es $e_1CAC^t = vAC^t$, y el coeficiente i-ésimo de este vector es $vAC^te_i^t = vAv_i^t = 0$ si $i \neq 1$ (pues entonces $v_i \in W$), mientras que para $i = 1$ queda $vAv^t = \alpha$. En resumen, la primera fila de B es $(\alpha, 0, \ldots, 0)$. Lo mismo ocurre con la primera columna porque la matriz B es simétrica.

Es claro entonces que la expresión explícita de g como $g(X) = XBX^t$ no contiene más monomios con x_1 que αx_1^2, luego g tiene la forma indicada en el enunciado. ∎

Aplicando repetidas veces el teorema anterior obtenemos lo siguiente:

Teorema 6.3 *Toda forma cuadrática $f(x_1, \ldots, x_n)$ es equivalente a otra del tipo $\alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$.*

A estas formas cuadráticas se les llama formas *diagonales,* pues son aquellas cuya matriz asociada es diagonal. Observemos que el determinante de una forma diagonal es el producto de sus coeficientes (de la diagonal), por lo que es regular si y sólo si todos son no nulos.

Nota En [Al 6.43] dimos una definición más general de forma cuadrática en un espacio vectorial. Hemos probado que dos formas cuadráticas son equivalentes si y sólo si sus matrices son congruentes en el sentido de [Al 6.47]. El teorema anterior es un caso particular de [Al 6.49]. Los teoremas [Al 6.50] y [Al 6.51] determinan las clases de equivalencia de formas cuadráticas sobre $\mathbb{C}$ y sobre $\mathbb{R}$, respectivamente. En este capítulo obtendremos una clasificación análoga de las formas cuadráticas sobre $\mathbb{Q}$. ∎

El teorema anterior simplifica muchas demostraciones, por ejemplo la siguiente:

Teorema 6.4 *Si una forma cuadrática regular representa 0 en un cuerpo K, entonces representa a todos los elementos de K.*

Demostración: Puesto que las formas equivalentes representan a los mismos elementos, podemos suponer que la dada es del tipo $f = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$, donde por ser regular todos los coeficientes son no nulos. Supongamos que

$$\alpha_1 a_1^2 + \cdots + \alpha_n a_n^2 = 0$$

es una representación de 0 en K. Podemos suponer que $a_1 \neq 0$. Sea γ cualquier elemento de K. Tomemos un cierto $t \in K$ que determinaremos después. Si calculamos

$$\begin{aligned} &f\big(a_1(1+t), a_2(1-t), \ldots, a_n(1-t)\big) \\ &= \alpha_1 a_1^2 + \cdots + \alpha_n a_n^2 + t^2(\alpha_1 a_1^2 + \cdots + \alpha_n a_n^2) \\ &+2\alpha_1 a_1^2 t - 2\alpha_2 a_2^2 t - \cdots - 2\alpha_n a_n^2 t = 4\alpha_1 a_1^2 t, \end{aligned}$$

vemos que basta hacer $t = \gamma/4\alpha_1 a_1^2$ para que

$$f\big(a_1(1+t), a_2(1-t), \ldots, a_n(1-t)\big) = \gamma.$$

∎

De aquí deducimos que el problema de si una forma cuadrática regular representa a un elemento se puede reducir siempre al problema de si una forma cuadrática representa 0. En efecto:

Teorema 6.5 *Una forma cuadrática regular $f(x_1,\dots,x_n)$ representa un elemento $\gamma\neq 0$ en un cuerpo K si y sólo si la forma $-\gamma x_0^2+f(x_1,\dots,x_n)$ representa* 0.

DEMOSTRACIÓN: Es obvio que si $f(a_1,\dots,a_n)=\gamma$ para ciertos valores $(a_1,\dots,a_n)$, entonces $-\gamma 1^2+f(a_1,\dots,a_n)=0$ es una representación de 0.

Supongamos ahora que $-\gamma a_0^2+f(a_1,\dots,a_n)=0$, donde no todos los a_i son nulos. Si es $a_0\neq 0$, entonces $\gamma=-f(a_1/a_0,\dots,a_n/a_0)$. Si por el contrario $a_0=0$ entonces tenemos que la forma $f(x_1,\dots,x_n)$ representa 0 en K, luego por el teorema anterior representa también a γ. ∎

El comportamiento de las formas cuadráticas binarias (que son las que más nos van a interesar) es especialmente simple. Los teoremas siguientes lo ponen de manifiesto:

Teorema 6.6 *Todas las formas cuadráticas binarias regulares que representan* 0 *en un cuerpo K son equivalentes.*

DEMOSTRACIÓN: Si una forma $f(x,y)$ representa 0, por el teorema 6.4 también representa a 1, luego por el teorema 6.2 la forma f es equivalente a una forma del tipo $x^2+\alpha y^2$, donde $\alpha\neq 0$. Existen $u,v\in K$ tales que $u^2+\alpha v^2=0$ con $u\neq 0$ o $v\neq 0$, pero de hecho esto implica que ambos son no nulos. Así, $\alpha=-(u/v)^2$. Haciendo el cambio $x=x'$, $y=(v/u)y'$ llegamos a que f es equivalente a la forma x^2-y^2. ∎

Teorema 6.7 *Una forma cuadrática binaria regular f con determinante d representa* 0 *en un cuerpo K si y sólo si $-d$ es un cuadrado en K.*

DEMOSTRACIÓN: Si f representa 0 entonces por el teorema anterior es equivalente a la forma x^2-y^2 de determinante -1, luego los determinantes d y -1 se diferencian en un factor que es un cuadrado en K.

Si el determinante de f (cambiado de signo) es un cuadrado en K, lo mismo le sucede a los determinantes de todas las formas equivalentes. En particular f es equivalente a una forma del tipo $g(x,y)=ax^2+by^2$, donde $-ab=\alpha^2\neq 0$.

Entonces $g(\alpha,a)=-a^2b+ba^2=0$ es una representación de 0. ∎

Teorema 6.8 *Dos formas cuadráticas binarias regulares de K son equivalentes si y sólo si sus determinantes difieren en un factor que es un cuadrado en K y existe un elemento no nulo de K representado por ambas.*

DEMOSTRACIÓN: Las condiciones son claramente necesarias. Si tenemos dos formas regulares que representan a un mismo elemento $\alpha\neq 0$, entonces por el teorema 6.2 son equivalentes respectivamente a las formas $f(x,y)=\alpha x^2+\beta y^2$, $g(x,y)=\alpha x^2+\gamma y^2$. Como los determinantes $\alpha\beta$ y $\alpha\gamma$ difieren en un cuadrado, $\beta=\gamma\delta^2$, luego el cambio de variables $x=x'$, $y=\delta y'$ transforma g en f, y por lo tanto las formas son equivalentes. ∎

6.2 Formas cuadráticas sobre cuerpos *p*-ádicos

Nuestro siguiente objetivo es estudiar las formas cuadráticas sobre los cuerpos p-ádicos. Para estudiar las formas cuadráticas sobre un cuerpo K es importante conocer sus cuadrados. El conjunto $K^{*2} = \{x^2 \mid x \in K \setminus \{0\}\}$ es claramente un subgrupo del grupo multiplicativo $K^* = K \setminus \{0\}$.

Por ejemplo, en el caso del cuerpo $\mathbb{C}$ es claro que $\mathbb{C}^{*2} = \mathbb{C}^*$, lo cual tiene como consecuencia que todas las formas cuadráticas regulares (con el mismo número de variables) son equivalentes. En efecto, toda forma regular es equivalente a una del tipo

$$a_1^2x_1^2 + \cdots + a_n^2x_n^2,$$

y haciendo el cambio $y_i = a_ix_i$, resulta equivalente a la forma $x_1^2 + \cdots + x_n^2$.

El caso de los números reales también es sencillo. Aquí $\mathbb{R}^{*2} =]0, +\infty[$, y el grupo cociente $\mathbb{R}^*/\mathbb{R}^{*2}$ tiene orden 2. Un conjunto de representantes de las clases es ± 1. En términos más simples, todo número real no nulo es de la forma $\pm\alpha^2$. El mismo razonamiento que en el caso complejo nos lleva ahora a que toda forma cuadrática regular de n variables es equivalente a una del tipo $\pm x_1^2 \pm \ldots \pm x_n^2$. Así pues, hay a lo sumo $n+1$ clases de equivalencia de formas regulares, según el número de signos negativos que aparezcan. De hecho no es difícil probar que hay exactamente $n+1$ clases.

Los dos resultados precedentes son los teoremas [Al 6.50] y [Al 6.51] que ya habíamos mencionado antes. Ahora pretendemos obtener resultados similares para los cuerpos p-ádicos $\mathbb{Q}_p$. Llamaremos $\mathbb{Z}_p$ al anillo de los enteros p-ádicos. Hemos de estudiar los grupos $\mathbb{Q}_p^{*2}$ así como los cocientes $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

La primera observación es que los cuadrados p-ádicos no nulos son de la forma $(\epsilon p^n)^2 = \epsilon^2 p^{2n}$, donde ϵ es una unidad de $\mathbb{Z}_p$ y n es un número entero. Así pues, caracterizar los cuadrados de $\mathbb{Q}_p$ equivale a caracterizar las unidades de $\mathbb{Z}_p$ que son cuadrados en $\mathbb{Z}_p$. Por el criterio de irreducibilidad de Gauss un entero p-ádico es un cuadrado en $\mathbb{Z}_p$ si y sólo si lo es en $\mathbb{Q}_p$.

Si llamamos U_p al grupo de las unidades de $\mathbb{Z}_p$, concluimos que estudiar el grupo $\mathbb{Q}_p^{*2}$ se reduce a estudiar el grupo U_p^2. Cuando p es un primo impar la situación es la siguiente:

Teorema 6.9 *Sea p un primo impar. Entonces una unidad $\epsilon \in U_p$ es un cuadrado si y sólo si es un cuadrado módulo p.*

Demostración: Si $\epsilon = \eta^2$, para una cierta unidad η, entonces, como $\mathbb{Z}_p/(p) \cong \mathbb{Z}/p\mathbb{Z}$, existe un entero racional $0 < d < p$ tal que $\eta \equiv d \pmod p$ (no es 0 porque η es una unidad). Entonces $\epsilon \equiv d^2 \pmod p$.

Recíprocamente, si $\epsilon \equiv d^2 \pmod p$ para un cierto d (no divisible entre p), consideramos el polinomio $F(x) = x^2 - \epsilon$. Tenemos que $F(d) \equiv 0 \pmod p$ mientras que $F'(d) = 2d \not\equiv 0 \pmod p$. El teorema 5.48 nos da que existe un $\eta \in \mathbb{Z}_p$ tal que $\epsilon = \eta^2$. ∎

Definición 6.10 Definimos el *símbolo de Legendre extendido* de una unidad $\epsilon \in U_p$ respecto a un primo impar p como

$$\left(\frac{\epsilon}{p}\right) = \begin{cases} 1 & \text{si } \epsilon \in U_p^2, \\ -1 & \text{si } \epsilon \notin U_p^2. \end{cases}$$

El teorema anterior implica que este símbolo de Legendre extiende al usual. De hecho (ϵ/p) depende sólo del resto de ϵ módulo p, de donde se concluye inmediatamente que sigue siendo multiplicativo.

El símbolo de Legendre (extendido) es un epimorfismo del grupo U_p en el grupo $\{\pm 1\}$ cuyo núcleo es precisamente U_p^2. Así pues, $|U_p : U_p^2| = 2$.

Teorema 6.11 *Si p es un primo impar, entonces $|\mathbb{Q}_p^* : \mathbb{Q}_p^{*2}| = 4$.*

Demostración: Sea ϵ una unidad que no sea un cuadrado. Entonces $U_p/U_p^2 = \big\{[1], [\epsilon]\big\}$, luego toda unidad es de la forma η^2 o bien $\epsilon\eta^2$. Todo elemento de $\mathbb{Q}_p^*$ es de la forma $\eta^2 p^{2n+i}$ o bien $\epsilon\eta^2 p^{2n+i}$, con $i = 0, 1$, luego $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \big\{[1], [\epsilon], [p], [p\epsilon]\big\}$. Es claro que estas cuatro clases son distintas. ∎

Ahora nos ocupamos del caso $p = 2$.

Teorema 6.12 *Una unidad $\epsilon \in U_2$ es un cuadrado si y sólo si $\epsilon \equiv 1$ (mód 8).*

Demostración: Si $\epsilon = \eta^2$ existe un entero racional k tal que $\eta \equiv k$ (mód 8). Como $\eta \equiv 1$ (mód 2), k es impar y además $\epsilon \equiv k^2$ (mód 8). Pero el cuadrado de un número impar siempre es congruente con 1 módulo 8 (basta verlo en los casos 1, 3, 5, 7).

Supongamos ahora que $\epsilon \equiv 1$ (mód 8). Tomamos $F(x) = x^2 - \epsilon$ y vemos que $F(1) \equiv 0$ (mód 8), $F'(1) = 2 \equiv 0$ (mód 2) y $F'(1) = 2 \not\equiv 0$ (mód 4). El teorema 5.47 nos da que ϵ es un cuadrado. ∎

Toda unidad diádica ϵ es congruente módulo 8 con un número impar, o sea, con una de las unidades $u = 1, 3, 5$ o 7. Entonces $\epsilon u^{-1} \equiv 1$ (mód 8), luego es un cuadrado. Así pues toda unidad diádica es de la forma $\epsilon = u\eta^2$, donde u toma uno de los cuatro valores citados. Esto significa que $U_2/U_2^2 = \big\{[1], [3], [5], [7]\big\}$ y todas las clases son distintas, porque ningún cociente entre ellas es congruente con 1 módulo 8.

Teorema 6.13 *Se cumple que $|\mathbb{Q}_2^* : \mathbb{Q}_2^{*2}| = 8$.*

Demostración: Razonando como en el teorema 6.11 se llega a que

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \big\{[1], [3], [5], [7], [2\cdot 1], [2\cdot 3], [2\cdot 5], [2\cdot 7]\big\}$$

y a que las ocho clases son distintas. ∎

Ahora podemos razonar como hemos hecho antes con las formas cuadráticas sobre $\mathbb{R}$ y sobre $\mathbb{C}$ (eliminando los cuadrados) hasta concluir que toda forma cuadrática regular sobre $\mathbb{Q}_p$ es equivalente a una de la forma $\alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$, donde cada α_i es una unidad de U_p o, más precisamente, un miembro de un conjunto fijo de representantes de las clases de congruencia de U_p/U_p^2.

Agrupando las variables adecuadamente tenemos que toda forma cuadrática regular es equivalente a una forma F del tipo

$$F = F_0 + pF_1 = (\epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2) + p(\epsilon_{r+1} x_{r+1}^2 + \cdots + \epsilon_n x_n^2), \tag{6.1}$$

donde $\epsilon_1, \ldots, \epsilon_n$ son unidades.

Para estudiar la representación de cero por una forma F podemos suponer $r \geq n - r$, pues pF es claramente equivalente a $F_1 + pF_0$ y las formas F y pF, aunque no son equivalentes, representan cero ambas o ninguna. Nuestro primer resultado es el siguiente:

Teorema 6.14 *Con la notación anterior, sea $p \neq 2$, $0 < r < n$. Entonces la forma F representa 0 en $\mathbb{Q}_p$ si y sólo si lo hace una de las formas F_0 o F_1.*

Demostración: Una implicación es obvia. Supongamos que F representa 0, es decir,

$$(\epsilon_1 a_1^2 + \cdots + \epsilon_r a_r^2) + p(\epsilon_{r+1} a_{r+1}^2 + \cdots + \epsilon_n a_n^2) = 0 \tag{6.2}$$

para ciertos números p-ádicos $a_1, \ldots, a_n$ no todos nulos. Multiplicando por la potencia de p adecuada podemos suponer que todos son enteros y que al menos uno de ellos no es divisible entre p. Supongamos primeramente que entre $a_1, \ldots, a_r$ hay alguno no divisible entre p, digamos a_i. Entonces

$$F_0(a_1, \ldots, a_r) \equiv 0 \pmod{p} \quad \text{y} \quad (F_0)'_i(a_1, \ldots, a_r) = 2\epsilon_i a_i \not\equiv 0 \pmod{p}.$$

Por el teorema 5.48 la forma F_0 representa 0.

Si por el contrario $a_1, \ldots, a_r$ son todos divisibles entre p, entonces podemos sacar factor común p en (6.2) y concluir que $F_1(a_{r+1}, \ldots, a_n) \equiv 0 \pmod{p}$, donde alguno de los números $a_{r+1}, \ldots, a_n$ no es divisible entre p. Razonando como en el caso anterior concluimos ahora que F_1 representa 0. ∎

En realidad en la demostración anterior no se ha usado la igualdad (6.2), sino tan sólo la congruencia

$$(\epsilon_1 a_1^2 + \cdots + \epsilon_r a_r^2) + p(\epsilon_{r+1} a_{r+1}^2 + \cdots + \epsilon_n a_n^2) \equiv 0 \pmod{p^2}.$$

Teniendo esto en cuenta podemos afirmar lo siguiente:

Teorema 6.15 *Con la notación anterior, si $p \neq 2$, la forma F representa 0 en $\mathbb{Q}_p$ si y sólo si la congruencia $F \equiv 0 \pmod{p^2}$ tiene una solución en $\mathbb{Z}_p$ en la que no todos los números sean divisibles entre p.*

Por otra parte el teorema 6.14 reduce el problema de la representación de 0 por una forma arbitraria a la representación de 0 por una forma del tipo $f = \epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2$, donde $\epsilon_1, \ldots, \epsilon_r$ son unidades p-ádicas (siempre con $p \neq 2$). Además, aplicando el teorema 5.48 como lo hemos hecho en la prueba del teorema 6.14, obtenemos el criterio siguiente para este tipo de formas:

Teorema 6.16 *Sean $\epsilon_1, \dots, \epsilon_r$ unidades p-ádicas, con $p \neq 2$. Entonces la forma cuadrática $f = \epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2$ representa 0 en $\mathbb{Q}_p$ si y sólo si la congruencia $f \equiv 0 \pmod{p}$ tiene una solución en la que no todos los números son divisibles entre p.*

Notemos que todo entero p-ádico es congruente con un entero racional módulo p y módulo p^2, luego las congruencias $f \equiv 0 \pmod{p}$ y $F \equiv 0 \pmod{p^2}$ pueden reducirse a congruencias de formas con coeficientes enteros racionales, y pueden resolverse en la práctica porque las soluciones posibles forman un conjunto finito. Ahora resolvemos el caso $p = 2$:

Teorema 6.17 *Con la notación anterior, para $p = 2$, la forma F representa 0 en $\mathbb{Q}_2$ si y sólo si la congruencia $F \equiv 0 \pmod{16}$ tiene una solución donde alguna de las variables toma un valor impar.*

Demostración: De nuevo, una implicación es obvia. Supongamos que $F(a_1, \dots, a_n) \equiv 0 \pmod{16}$ donde alguno de los enteros a_i es impar. Si esto sucede para $i \leq r$, entonces tenemos que

$$F(a_1, \dots, a_n) \equiv 0 \pmod{8}, \qquad F_i'(a_1, \dots, a_n) = 2\epsilon_i a_i \not\equiv 0 \pmod{4},$$

luego el teorema 5.47 nos da que F representa 0.

Si los números $a_1, \dots, a_r$ son todos pares, digamos $a_i = 2b_i$, entonces tenemos que

$$4(\epsilon_1 b_1^2 + \cdots + \epsilon_r b_r^2) + 2(\epsilon_{r+1} a_{r+1}^2 + \cdots + \epsilon_n a_n^2) \equiv 0 \pmod{16},$$

luego

$$2(\epsilon_1 b_1^2 + \cdots + \epsilon_r b_r^2) + (\epsilon_{r+1} a_{r+1}^2 + \cdots + \epsilon_n a_n^2) \equiv 0 \pmod{8},$$

y como en el caso anterior podemos concluir que la forma $2F_0 + F_1$ representa 0 en $\mathbb{Q}_2$, luego lo mismo le ocurre a la forma $4F_0 + 2F_1$, que es equivalente a F. ∎

En la prueba anterior hemos obtenido el criterio siguiente:

Teorema 6.18 *Con la notación anterior, si $F \equiv 0 \pmod{8}$ tiene una solución en la que alguna variable $x_1, \dots, x_r$ toma valor impar, entonces F representa 0 en $\mathbb{Q}_2$.*

Ahora probamos un hecho elemental sobre congruencias del que sacaremos muchas aplicaciones al tema que nos ocupa.

Teorema 6.19 *Sean a, b, c enteros racionales y p un primo impar. Entonces la congruencia $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ tiene una solución no trivial (es decir, donde no todas las variables son múltiplos de p).*

Demostración: Si algún coeficiente es nulo módulo p es evidente. En otro caso podemos dividir entre uno de ellos y probar que la ecuación $ax^2 + by^2 = z^2$ tiene soluciones no nulas. Esto es lo mismo que probar que la forma $ax^2 + by^2$

representa a un cuadrado no nulo en $\mathbb{Z}/p\mathbb{Z}$. Como el número de no cuadrados es $(p-1)/2$, basta probar que ax^2+by^2 toma más de $(p-1)/2$ valores no nulos, pues entonces alguno de ellos será un cuadrado. El número de valores no nulos que toma esta forma (para a, b genéricos) es el mismo que el de los que toma la forma x^2+ay^2 (para a genérico). Si a no es un cuadrado módulo p entonces la forma x^2+ay^2 representa a todos los elementos de $\mathbb{Z}/p\mathbb{Z}$: los cuadrados haciendo $y=0$ y los no cuadrados haciendo $x=0$. Si a es un cuadrado, entonces la forma x^2+ay^2 representa a los $(p-1)/2$ cuadrados (con $y=0$) y basta probar que también representa a algún no cuadrado. Como ay^2 recorre todos los cuadrados, basta probar que la suma de dos cuadrados (mód p) no siempre es un cuadrado (mód p), pero esto es obvio, ya que todo elemento de $\mathbb{Z}/p\mathbb{Z}$ se expresa como suma de unos, y si la suma de cuadrados fuera siempre un cuadrado, todos los elementos de $\mathbb{Z}/p\mathbb{Z}$ serían cuadrados. ∎

Teorema 6.20 *Toda forma cuadrática con cinco o más variables representa* 0 *en cualquier cuerpo p-ádico.*

DEMOSTRACIÓN: Las formas singulares siempre representan 0, luego podemos suponer que tenemos una forma regular del tipo F_0+pF_1, según (6.1), y de acuerdo con la observación posterior a (6.1) podemos suponer que $r \geq n-r$, luego $r \geq 3$.

Supongamos primero $p \neq 2$. Basta probar que F_0 representa 0, y por el teorema 6.16 basta probar que la congruencia $F_0 \equiv 0$ (mód p) tiene una solución no trivial. La forma F_0 es congruente (mód p) a otra del tipo $a_1x_1^2+\cdots+a_rx_r^2$, donde los a_i son enteros racionales y $r \geq 3$. El teorema anterior nos da lo pedido.

Suponemos ahora que $p=2$ y $3 \leq r < n$. Consideramos la forma

$$f = \epsilon_1x_1^2+\epsilon_2x_2^2+\epsilon_3x_3^2+2\epsilon_nx_n^2.$$

Es claro que si f representa 0 lo mismo le ocurrirá a F. Al ser unidades, los coeficientes son congruentes con 1 módulo 2, luego $\epsilon_1+\epsilon_2 = 2\alpha$ para un cierto entero diádico α. Entonces

$$\epsilon_1+\epsilon_2+2\epsilon_n\alpha^2 = 2\alpha+2\epsilon_n\alpha^2 = 2\alpha(1+\epsilon_n\alpha) \equiv 0 \text{ (mód 4)},$$

y así $\epsilon_1+\epsilon_2+2\epsilon_n\alpha^2 = 4\beta$, donde β es un entero diádico. Entonces:

$$\epsilon_1\cdot 1^2+\epsilon_2\cdot 1^2+\epsilon_3\cdot(2\beta)^2+2\epsilon_n\alpha^2 = 4\beta+\epsilon_3\cdot 4\beta^2 = 4\beta(1+\epsilon_3\beta) \equiv 0 \text{ (mód 8)}.$$

Por el teorema 6.18 resulta que f representa 0.

En el caso en que $r=n \geq 5$ tomamos $f=\epsilon_1x_1^2+\epsilon_2x_2^2+\epsilon_3x_3^2+\epsilon_4x_4^2+\epsilon_5x_5^2$ y de nuevo basta probar que f representa 0.

Los cinco coeficientes son congruentes con ± 1 (mód 4) y, como hay cinco, debe haber dos pares congruentes (mód 4), digamos

$$\epsilon_1 \equiv \epsilon_2 \text{ (mód 4)} \quad \text{y} \quad \epsilon_3 \equiv \epsilon_4 \text{ (mód 4)}.$$

Entonces $\epsilon_1 + \epsilon_2 \equiv \epsilon_3 + \epsilon_4 \equiv 2$ (mód 4), luego $\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 = 4\gamma$, donde γ es un entero diádico. Tomando $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = 2\gamma$ resulta que

$$f(x_1, x_2, x_3, x_4, x_5) = 4\gamma + \epsilon_5 4\gamma^2 = 4\gamma(1 + \epsilon_5\gamma) \equiv 0 \text{ (mód 8)}$$

y se concluye como en el caso anterior. ∎

El teorema 6.5 nos da la siguiente consecuencia inmediata:

Teorema 6.21 *Toda forma cuadrática regular con cuatro o más variables representa a todos los números p-ádicos no nulos.*

Otra consecuencia importante del teorema 6.19 (junto con el teorema 6.16) es la siguiente:

Teorema 6.22 *Si $\epsilon_1, \ldots, \epsilon_r$ son unidades p-ádicas con $p \neq 2$ y $r \geq 3$, entonces la forma cuadrática $\epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2$ representa 0 en $\mathbb{Q}_p$.*

6.3 Formas binarias en cuerpos *p*-ádicos

Ahora nos ocupamos de las formas cuadráticas binarias. El problema de si una forma binaria regular representa un número p-ádico dado se reduce, pasando a una forma equivalente y dividiendo entre un coeficiente, a si una forma del tipo $x^2 - \alpha y^2$ representa a un cierto número p-ádico, con $\alpha \neq 0$. Llamemos N_α al conjunto de los números p-ádicos no nulos representados por esta forma. Teniendo en cuenta el teorema 6.5

$$\beta \in N_\alpha \quad \Leftrightarrow \quad x^2 - \alpha y^2 \text{ representa } \beta \quad \Leftrightarrow \quad \alpha x^2 + \beta y^2 - z^2 \text{ representa } 0.$$

Observemos que si α no es un cuadrado en $\mathbb{Q}_p$ entonces

$$x^2 - \alpha y^2 = \big(x - y\sqrt{\alpha}\,\big)\big(x + y\sqrt{\alpha}\,\big) = \mathrm{N}\big(x + y\sqrt{\alpha}\,\big),$$

donde N es la norma de la extensión $\mathbb{Q}_p\big(\sqrt{\alpha}\,\big)/\mathbb{Q}_p$, con lo que N_α es la imagen por la norma del grupo multiplicativo de $\mathbb{Q}_p\big(\sqrt{\alpha}\,\big)$. En particular es un subgrupo de $\mathbb{Q}_p^*$. Si por el contrario α es un cuadrado en $\mathbb{Q}_p$ entonces la forma $x^2 - \alpha y^2$ representa 0 y en consecuencia a todos los números p-ádicos, por lo que $N_\alpha = \mathbb{Q}_p^*$. De hecho en este caso la extensión $\mathbb{Q}_p\big(\sqrt{\alpha}\,\big)/\mathbb{Q}_p$ es trivial, y N_α sigue siendo el grupo de las normas no nulas de la extensión.

Puesto que la forma $x^2 - \alpha y^2$ representa todos los cuadrados, tenemos las inclusiones $\mathbb{Q}_p^{*2} \subset N_\alpha \subset \mathbb{Q}_p^*$. Los teoremas 6.11 y 6.13 prueban que el índice $|\mathbb{Q}_p^* : N_\alpha|$ es finito. Ya hemos dicho que si α es un cuadrado entonces $N_\alpha = \mathbb{Q}_p^*$. En el caso contrario tenemos:

Teorema 6.23 *Si $\alpha \in \mathbb{Q}_p^*$ no es un cuadrado, entonces $|\mathbb{Q}_p^* : N_\alpha| = 2$.*

DEMOSTRACIÓN: Supongamos primero que $p \neq 2$. Veamos que $N_\alpha \neq \mathbb{Q}_p^{*2}$. En efecto, como $-\alpha \in N_\alpha$, esto es cierto si $-\alpha$ no es un cuadrado. Si lo es entonces la forma $x^2 - \alpha y^2$ es equivalente a $x^2 + y^2$, y por el teorema 6.5 esta forma representa a toda unidad ϵ (incluyendo a las que no son cuadrados), pues según el teorema 6.22 la forma $x^2 + y^2 - \epsilon z^2$ representa 0. Por lo tanto N_α contiene a todas las unidades y en consecuencia $N_\alpha \neq \mathbb{Q}_p^{*2}$.

Ahora probamos que $N_\alpha \neq \mathbb{Q}_p^*$. Sea ϵ una unidad que no es un cuadrado. Hemos de probar que la forma $\alpha x^2 + \beta y^2 - z^2$ no representa a 0 para todo valor de β, ahora bien, si multiplicamos α por un cuadrado no nulo, la forma resultante representa 0 en los mismos casos, luego podemos suponer que α es ϵ, p o $p\epsilon$ (por la prueba del teorema 6.11). Ahora bien, si $\alpha = \epsilon$ y $\beta = p$ o si $\alpha = p$, $p\epsilon$ y $\beta = \epsilon$, el teorema 6.14 implica que la forma $\alpha x^2 + \beta y^2 - z^2$ no representa 0, luego en cualquier caso existe un β que no está en N_α.

Puesto que $|\mathbb{Q}_p^* : \mathbb{Q}_p^{*2}| = 4$, necesariamente $|\mathbb{Q}_p^* : N_\alpha| = 2$.

Nos queda el caso en que $p = 2$. Ahora $|\mathbb{Q}_2^* : \mathbb{Q}_2^{*2}| = 8$ y como representantes de las clases podemos tomar 1, 3, 5, 7, 2, 6, 10, 14. Vamos a comprobar que cuando α y β varían en este conjunto de representantes la forma $\alpha x^2 + \beta y^2 - z^2$ representa 0 en los casos indicados con un + en la tabla siguiente:

	1	3	5	7	2	6	10	14
1	+	+	+	+	+	+	+	+
3	+		+			+		+
5	+	+	+	+				
7	+		+		+		+	
2	+			+	+			+
6	+	+					+	+
10	+			+		+	+	
14	+	+			+	+		

Una vez probado esto, la tabla indica que cuando $\alpha \neq 1$, o sea, cuando α no es un cuadrado perfecto, la forma $\alpha x^2 + \beta y^2 - z^2$ representa 0 para todos los β que pertenecen a cuatro de las ocho clases posibles, luego $|N_\alpha : \mathbb{Q}_p^{*2}| = 4$. Puesto que $|\mathbb{Q}_p^* : \mathbb{Q}_p^{*2}| = 8$ se concluye que $|\mathbb{Q}_p^* : N_\alpha| = 2$.

Supongamos primero que $\alpha = 2\epsilon$, $\beta = 2\eta$, donde ϵ, η son unidades (1, 3, 5 o 7). Si se cumple que $2\epsilon x^2 + 2\eta y^2 - z^2 = 0$, podemos suponer que x, y, z son enteros p-ádicos no todos pares. Claramente z es par, pero x e y son ambos impares, pues si uno de ellos fuera par, digamos y, entonces $2\epsilon x^2$ sería divisible entre 4, luego x también sería par.

Haciendo $z = 2t$ la ecuación se reduce a $\epsilon x^2 + \eta y^2 - 2t^2 = 0$. Tenemos, pues, que la forma $2\epsilon x^2 + 2\eta y^2 - z^2$ representa 0 si y sólo si la forma $\epsilon x^2 + \eta y^2 - 2t^2$ representa 0 (y entonces x e y pueden tomarse impares). Por el teorema 6.18 esto equivale a que la congruencia $\epsilon x^2 + \eta y^2 - 2t^2 \equiv 0$ (mód 8) tenga solución con x e y impares. El cuadrado de un impar es siempre congruente con 1 (mód 8), mientras que $2t^2$ puede ser congruente con 0 o con 2 (mód 8). Consecuentemente la congruencia tiene solución si y sólo si $\epsilon + \eta \equiv 2$ (mód 8) o $\epsilon + \eta \equiv 0$ (mód 8). Esto da los valores del cuadrante inferior derecho de la tabla.

Ahora sea $\alpha = 2\epsilon$, $\beta = \eta$. En la ecuación $2\epsilon x^2 + \eta y^2 - z^2 = 0$ podemos suponer que x, y, z son enteros p-ádicos no todos pares. Pero de hecho y, z han de ser ambos impares, pues si uno de ellos es par, digamos y, entonces $2 \mid z$, luego $4 \mid 2\epsilon x^2$ luego los tres serían pares.

Por el argumento anterior esto equivale a que $2\epsilon x^2 + \eta y^2 - z^2 \equiv 0 \pmod 8$ tenga solución con y, z impares, y a su vez a que $2\epsilon+\eta \equiv 1 \pmod 8$ o bien $\eta \equiv 1 \pmod 8$. Esto nos da el cuadrante superior derecho de la tabla y por simetría el inferior izquierdo.

Finalmente sea $\alpha = \epsilon$, $\beta = \eta$. Ahora en $\epsilon x^2 + \eta y^2 - z^2 = 0$ se cumple que entre x, y, z hay exactamente un par y dos impares.

Si z es par $\epsilon x^2 + \eta y^2 \equiv \epsilon + \eta \equiv 0 \pmod 4$, luego o bien $\epsilon \equiv 1 \pmod 4$ o bien $\eta \equiv 1 \pmod 4$.

Si z es impar entonces $\epsilon x^2 + \eta y^2 \equiv 1 \pmod 4$, y como entre x, y hay un par y un impar, llegamos otra vez a que $\epsilon \equiv 1 \pmod 4$ o bien $\eta \equiv 1 \pmod 4$.

Recíprocamente, si se cumple, digamos, $\epsilon \equiv 1 \pmod 4$, entonces ha de ser $\epsilon \equiv 1 \pmod 8$ o bien $\epsilon \equiv 5 \pmod 8$. En el primer caso $\epsilon x^2+\eta y^2-z^2 \equiv 0 \pmod 8$ tiene solución $(1, 0, 1)$, en el segundo $(1, 2, 1)$. Esto implica que $\epsilon x^2 + \eta y^2 - z^2$ representa 0. En resumen la condición es $\epsilon \equiv 1 \pmod 4$ o $\eta \equiv 1 \pmod 4$, o sea, $\epsilon = 5$ o $\eta = 5$, lo que nos da el resto de la tabla. ∎

Como consecuencia, si α no es un cuadrado, el grupo cociente $\mathbb{Q}_p^*/N_\alpha$ es isomorfo al grupo $\{\pm 1\}$. Componiendo la proyección en el cociente con este isomorfismo obtenemos un homomorfismo de $\mathbb{Q}_p^*$ en $\{\pm 1\}$ cuyo núcleo es exactamente N_α. Si α es un cuadrado entonces $N_\alpha = \mathbb{Q}_p^*$ y dicho homomorfismo también existe trivialmente. En definitiva estamos hablando que la aplicación que asigna a cada β un signo ± 1 según si β está o no en N_α. A este homomorfismo llegaron independientemente Hasse y Hilbert, el primero siguiendo más o menos nuestra línea de razonamientos en términos de representación de números p-ádicos por formas binarias, el segundo estudiando los grupos de normas de las extensiones cuadráticas de los cuerpos p-ádicos.

Definición 6.24 Para cada par de números p-ádicos no nulos α y β se define el *símbolo de Hilbert* como

$$(\alpha, \beta)_p = \begin{cases} 1 & \text{si } \beta \in N_\alpha \\ -1 & \text{si } \beta \notin N_\alpha \end{cases}$$

Teniendo en cuenta la definición de N_α y el teorema 6.5, tenemos las equivalencias siguientes:

1. $(\alpha, \beta)_p = 1$
2. $x^2 - \alpha y^2$ representa a β en $\mathbb{Q}_p$,
3. $\alpha x^2 + \beta y^2 - z^2$ representa 0 en $\mathbb{Q}_p$
4. $\alpha x^2 + \beta y^2$ representa 1 en $\mathbb{Q}_p$.

Si sabemos calcular símbolos de Hilbert, estamos en condiciones de determinar si cualquier forma cuadrática binaria representa o no a un número p-ádico dado. El cálculo del símbolo de Hilbert es muy sencillo a partir de las propiedades que recogemos en el teorema siguiente:

Teorema 6.25 *Sea p un número primo, sean α, β, α', β' números p-ádicos no nulos y sean ϵ, η unidades p-ádicas. Entonces*

1. $(\alpha,\beta)_p = (\beta,\alpha)_p$.
2. $(\alpha,\beta\beta')_p = (\alpha,\beta)_p(\alpha,\beta')_p$, $\quad(\alpha\alpha',\beta)_p = (\alpha,\beta)_p(\alpha',\beta)_p$.
3. *Si α o β es un cuadrado en $\mathbb{Q}_p$ entonces* $(\alpha,\beta)_p = 1$.
4. $(\alpha,-\alpha)_p = 1$, $\quad(\alpha,\alpha)_p = (\alpha,-1)_p$.
5. *Si $p \neq 2$ entonces* $(p,\epsilon)_p = (\epsilon/p)$ *(símbolo de Legendre),* $(\epsilon,\eta)_p = 1$.
6. $(2,\epsilon)_2 = 1$ *si y sólo si* $\epsilon \equiv \pm 1 \pmod 8$,
   $(\epsilon,\eta)_2 = 1$ *si y sólo si* $\epsilon \equiv 1 \pmod 4$ *o bien* $\eta \equiv 1 \pmod 4$.

Demostración: 1) Es inmediato.

2) Por la observación previa a la definición anterior: el símbolo de Hilbert para un α fijo y como función de β es el homomorfismo de $\mathbb{Q}_p^*$ en $\{\pm 1\}$ con núcleo N_α.

3) Si $\alpha = \gamma^2$ entonces $(\alpha,\beta)_p = (\gamma,\beta)_p^2 = 1$.

4) La ecuación $\alpha x^2 - \alpha y^2 - z^2 = 0$ tiene solución $(1,1,0)$.
Por 2) $1 = (\alpha,-\alpha)_p = (\alpha,\alpha)_p(\alpha,-1)_p$, luego $(\alpha,\alpha)_p = (\alpha,-1)_p$.

5) Por el teorema 6.14, la forma $px^2 + \epsilon y^2 - z^2$ representa 0 si y sólo si la forma $\epsilon y^2 - z^2$ representa 0, lo cual sucede si y sólo si ϵ es un cuadrado.
Por el teorema 6.22, la forma $\epsilon x^2 + \eta y^2 - z^2$ siempre representa 0.

6) En la tabla construida en la prueba del teorema 6.23 vemos que la forma $2\epsilon x^2 + \eta y^2 - z^2$ representa 0 si y sólo si $2\epsilon + \eta \equiv 1 \pmod 8$ o $\eta \equiv 1 \pmod 8$. En particular, para $\epsilon = 1$ tenemos que $2x^2 + \eta y^2 - z^2$ representa 0 si y sólo si $\eta \equiv \pm 1 \pmod 8$.
También allí hemos probado que la forma $\epsilon x^2 + \eta y^2 - z^2$ representa 0 si y sólo si $\epsilon \equiv 1 \pmod 4$ o bien $\eta \equiv 1 \pmod 4$. ∎

Notemos que una consecuencia de 2) y 3) es que

$$(\alpha^{-1},\beta)_p = (\alpha,\beta)_p \qquad (\alpha,\beta^{-1})_p = (\alpha,\beta)_p.$$

Para calcular un símbolo de Hilbert arbitrario $(p^k\epsilon, p^l\eta)_p$ usando el teorema anterior, en primer lugar 1) y 2) y 3) nos lo reducen a los casos $(\epsilon,\eta)_p$, $(p\epsilon,\eta)_p$, $(p,p)_p$. El último caso se reduce a los anteriores por 4) y éstos se resuelven mediante 5) y 6).

Ejemplo Consideremos la forma $2x^2 - 5y^2$. No es fácil a priori determinar qué números están representados por ella. Por ejemplo, $53 = 2\cdot 7^2 - 5\cdot 3^3$ sí está representado en $\mathbb{Q}$, mientras que 47 no lo está. Para probarlo basta ver que no está representado en $\mathbb{Q}_2$. En efecto:

$$2x^2 - 5y^2 = 47 \Leftrightarrow x^2 - \frac{5}{2}\,y^2 = \frac{47}{2}$$

y la última ecuación tiene solución en $\mathbb{Q}_2$ si y sólo si $(5/2, 47/2)_2 = 1$. Ahora bien,

$$(5/2, 47/2)_2 = (5, 47)_2\,(2, 47)_2\,(5, 2)_2\,(2, 2)_2 = 1\cdot 1\cdot(-1)\cdot 1 = -1.$$

Por otro lado, la forma sí representa a 47 en $\mathbb{Q}_5$. En efecto, al igual que antes esto equivale a que $(5/2, 47/2)_5 = 1$, y ahora

$$(5/2, 47/2)_5 = (5, 47)_5\,(2, 47)_5\,(5, 2)_5\,(2, 2)_5 = (-1)\cdot 1\cdot(-1)\cdot 1 = 1.$$

Si queremos una representación concreta observamos que $47 \equiv 2 \pmod 5$, luego $47/2 \equiv 1 \pmod 5$ (en $\mathbb{Q}_5$) y por el teorema 6.9 existe $\sqrt{47/2} \in \mathbb{Q}_5$. Así

$$2\sqrt{\frac{47}{2}}^{\,2} - 5\cdot 0^2 = 47.$$

∎

Ejercicio: Determinar qué primos p cumplen que la forma anterior representa a 47 en $\mathbb{Q}_p$. Determinar también los números representados por dicha forma en $\mathbb{Q}_5$.

Ahora veremos cómo decidir si dos formas cuadráticas dadas son equivalentes en $\mathbb{Q}_p$.

Teorema 6.26 *Sea f una forma cuadrática binaria con coeficientes en $\mathbb{Q}_p$ y determinante $d \neq 0$. Entonces $(\alpha, -d)_p$ toma el mismo valor sobre todos los números p-ádicos $\alpha \neq 0$ representados por f.*

Demostración: Si $\alpha x^2 + \beta y^2$ es una forma equivalente a f, su determinante se diferencia del de f en un cuadrado, luego

$$(\alpha, -d)_p = (\alpha, -\alpha\beta)_p = (\alpha, \beta)_p,$$

y este símbolo vale 1 si y sólo si $\alpha x^2 + \beta y^2$ representa 1, si y sólo si f representa 1. Esta condición no depende de α. ∎

Definición 6.27 Sea f una forma cuadrática binaria regular con coeficientes en $\mathbb{Q}_p$. Llamaremos $d(f)$ al determinante de f y $\psi_p(f) = \big(\alpha, -d(f)\big)_p$, donde α es cualquier número p-ádico no nulo representado por f.

Según hemos visto, $\psi_p(f) = 1$ si y sólo si f representa 1 en $\mathbb{Q}_p$.

Teorema 6.28 *Sean f y g dos formas cuadráticas binarias regulares sobre $\mathbb{Q}_p$. Entonces f y g son equivalentes si y sólo si $d(f)/d(g) \in \mathbb{Q}_p^{*2}$ y $\psi_p(f) = \psi_p(g)$.*

DEMOSTRACIÓN: Las condiciones son claramente necesarias. Suponiendo estas condiciones vamos a ver que f y g representan los mismos números. Sea $\gamma \neq 0$ un número representado por g. Podemos suponer que f es del tipo $\alpha x^2 + \beta y^2$. Entonces

$$(\alpha, -\alpha\beta)_p = \psi_p(f) = \psi_p(g) = \big(\gamma, -d(\gamma)\big)_p = (\gamma, -\alpha\beta)_p,$$

luego $(\gamma\alpha^{-1}, -\alpha\beta)_p = 1$, y la ecuación $\gamma\alpha^{-1}x^2 - \alpha\beta y^2 - z^2 = 0$ tiene una solución no trivial.

Si $x = 0$ entonces $-\alpha\beta$ es un cuadrado, luego por el teorema 6.7 las dos formas representan 0 y consecuentemente a todos los números p-ádicos. Si $x \neq 0$ entonces

$$\gamma = \alpha\left(\frac{z}{x}\right)^2 + \beta\left(\frac{\alpha y}{x}\right)^2,$$

luego f también representa a γ. En cualquier caso, las formas f y g son equivalentes por el teorema 6.8. ∎

Hemos visto cómo la representación de números y la equivalencia de formas binarias sobre los cuerpos $\mathbb{Q}_p$ se rigen por reglas sencillas y relativamente fáciles de obtener. En el núcleo de los resultados que hemos obtenido se halla el teorema 5.47, que permite encontrar fácilmente soluciones de ecuaciones y cuya prueba es esencialmente topológica. Con los cuerpos p-ádicos sucede lo mismo que con el cuerpo $\mathbb{R}$, que la topología (más exactamente la completitud) permite demostrar fácilmente que ciertas ecuaciones tienen solución.

De hecho todos los resultados que hemos obtenido son todavía más sencillos en el caso de $\mathbb{R}$: Para cada número real α no nulo podemos definir N_α exactamente igual a como hemos hecho para los números p-ádicos, y es inmediato que $N_\alpha = \mathbb{R}^*$ si $\alpha > 0$ o bien $N_\alpha =]0, +\infty[$ si $\alpha < 0$. Por lo tanto sigue siendo cierto que el índice $|\mathbb{R}^* : N_\alpha|$ vale siempre 1 o 2 y es posible definir el símbolo de Hilbert:

Definición 6.29 Si α y β son números reales no nulos definimos

$$(\alpha, \beta)_\infty = \begin{cases} 1 & \text{si } x^2 - \alpha\, y^2 \text{ repesenta a } \beta \text{ en } \mathbb{R}, \\ -1 & \text{en caso contrario.} \end{cases}$$

Las propiedades de $(\alpha, \beta)_\infty$ son las mismas que sobre los cuerpos p-ádicos, aunque las comprobaciones son mucho más sencillas. Respecto al cálculo explícito, es fácil comprobar que $(\alpha, \beta)_\infty = 1$ si y sólo si $\alpha > 0$ o $\beta > 0$.

Ejercicio: Interpretar el invariante $\psi_\infty(f)$ y comprobar que determina la equivalencia de formas cuadráticas binarias en $\mathbb{R}$ exactamente igual que en el caso p-ádico.

Sucede que la ley de reciprocidad cuadrática (junto con las leyes suplementarias) admite una formulación equivalente en términos del símbolo de Hilbert:

Teorema 6.30 *La ley de reciprocidad cuadrática es equivalente a la siguiente afirmación: para todos los números racionales no nulos a y b se cumple*

$$\prod_p (a, b)_p = 1,$$

donde p recorre todos los primos, incluido $p = \infty$.

DEMOSTRACIÓN: Observemos que el producto es finito, en el sentido de que casi todos sus factores son iguales a 1. Concretamente, si $p \neq 2$ y p no divide al numerador ni al denominador de ab, entonces de acuerdo con las propiedades de los símbolos de Hilbert, $(a,b)_p = 1$.

Por estas mismas propiedades, todo producto de este tipo se descompone en un número finito de productos similares donde a y b están en uno de los casos siguientes:

1. $a = b = -1$.
2. $a = q$ (primo), $b = -1$.
3. $a = q$, $b = q'$ (primos distintos).

Basta, pues, considerar productos asociados a pares en uno de estos casos.

1) En cualquier caso se cumple

$$\prod_p (-1,-1)_p = (-1,-1)_2(-1,-1)_\infty = (-1)(-1) = 1.$$

2) Igualmente:

$$\prod_p (2,-1)_p = (2,-1)_2(2,-1)_\infty = 1 \cdot 1 = 1.$$

La primera ley suplementaria se cumple si y sólo si

$$\prod_p (q,-1)_p = (q,-1)_2(q,-1)_q = (-1)^{(q-1)/2}\left(\frac{-1}{q}\right) = 1.$$

3) La segunda ley suplementaria se cumple si y sólo si

$$\prod_p (2,q)_p = (2,q)_2(2,q)_q = (-1)^{(q^2-1)/8}\left(\frac{2}{q}\right) = 1.$$

Y la ley de reciprocidad principal se cumple si y sólo si

$$\prod_p (q,q')_p = (q,q')_2(q,q')_q(q,q')_{q'} = (-1)^{(q-1)(q'-1)/4}\left(\frac{q}{q'}\right)\left(\frac{q'}{q}\right) = 1.$$

■

En el próximo capítulo demostraremos la fórmula del producto de los símbolos de Hilbert sin apoyarnos en la ley de reciprocidad cuadrática, con lo que tendremos una prueba alternativa.

6.4 El teorema de Hasse-Minkowski

El problema de la representación de números por formas cuadráticas en $\mathbb{Q}$ se resuelve en virtud del teorema siguiente:

Teorema 6.31 (Teorema de Hasse-Minkowski) *Una forma cuadrática con coeficientes racionales representa* 0 *en* $\mathbb{Q}$ *si y sólo si representa* 0 *en todos los cuerpos* $\mathbb{Q}_p$*, para todo primo* p*, incluido* $p = \infty$*.*

Aplicando el teorema 6.5 tenemos la siguiente consecuencia inmediata:

Teorema 6.32 *Una forma cuadrática con coeficientes racionales representa a un número racional* r *en* $\mathbb{Q}$ *si y sólo si representa a* r *en todos los cuerpos* $\mathbb{Q}_p$*, para todo primo* p*, incluido* $p = \infty$*.*

Así pues, el problema de si un número racional está representado en $\mathbb{Q}$ por una forma cuadrática se reduce al mismo problema sobre los cuerpos p-ádicos, donde la solución es mucho más sencilla gracias esencialmente a la completitud. De hecho los problemas de representación de números por formas cuadráticas en cuerpos p-ádicos pueden resolverse sistemáticamente. Nosotros sólo hemos expuesto la teoría completa para formas binarias, pero se pueden dar resultados generales. Un ataque directo del problema en $\mathbb{Q}$ es inviable en general y termina siempre en comprobaciones laboriosas en cada caso particular.

Pero aparte del interés del teorema de Hasse-Minkowski para la teoría de ecuaciones diofánticas, podemos ver en él un indicio de un principio alrededor del cual gira la teoría algebraica de números moderna. Vagamente puede ser enunciado como sigue: Los resultados 'globales', referentes a la aritmética de $\mathbb{Q}$ o de un cuerpo numérico, pueden descomponerse en resultados análogos 'locales' en torno a las compleciones del cuerpo respecto todos sus primos (incluyendo los primos infinitos asociados a valores absolutos arquimedianos), de tal forma que la totalidad de los resultados locales equivale al correspondiente resultado global. Este *principio de localización,* conjeturado por Hensel y puesto de manifiesto por Hasse, se aplica igualmente al cálculo de discriminantes, a la determinación de las descomposiciones en primos y al trabajo con muchos conceptos adicionales de la teoría de números que nosotros no tocaremos. Añadamos tan sólo que Hensel descubrió los números p-ádicos mientras investigaba los exponentes de los primos que dividen al discriminante de un cuerpo numérico y, efectivamente, este problema puede reducirse a estudiar los discriminantes de extensiones locales asociadas, cada uno de los cuales es divisible únicamente entre un primo.

Empezamos demostrando el teorema de Hasse-Minkowski para formas de hasta tres variables, con lo que el teorema 6.32 estará probado para formas binarias. El resto de la prueba requerirá consideraciones adicionales que incluyen la ley de reciprocidad cuadrática y el teorema de Dirichlet sobre primos en progresiones aritméticas. Por otra parte, en lo sucesivo sólo necesitaremos los casos que vamos a probar ahora.

Demostración: (del T$^{\text{a}}$ 6.31 para formas de hasta 3 variables):

Como observación general podemos suponer que la forma cuadrática considerada es regular, porque las formas singulares representan 0 en todos los cuerpos. Además una implicación es inmediata.

Cuando el número n de variables es 1 el teorema es trivial: una forma con una variable nunca representa 0.

Para $n = 2$ la prueba es muy sencilla: Sea f una forma cuadrática binaria con coeficientes racionales. Sea d su discriminante. Por el teorema 6.7, f representa 0 en un cuerpo K si y sólo si $-d$ es un cuadrado en K. Como f representa 0 en $\mathbb{R}$, tenemos $-d > 0$. Sea $-d = p_1^{k_1} \cdots p_r^{k_r}$, donde $p_1, \ldots, p_r$ son primos (naturales) distintos y $k_1, \ldots, k_r$ son enteros racionales. Como $-d$ es un cuadrado en cada $\mathbb{Q}_{p_i}$ resulta que cada exponente k_i es par, luego $-d$ es un cuadrado en $\mathbb{Q}$.

Observemos que los casos $n = 1, 2$ no aportan nada, pues disponemos de criterios directos para decidir si una forma con una o dos variables representa 0 o no en $\mathbb{Q}$. En cambio el caso $n = 3$ sí aporta información relevante y la prueba ya no es tan simple.

Pasando a una forma equivalente y multiplicando por un entero racional si es preciso, podemos suponer que la forma considerada es del tipo $ax^2+by^2+cz^2$ con coeficientes enteros (esto no modifica la representación de 0).

Observemos que para aquellos primos p que no dividan a abc los coeficientes son unidades p-ádicas, y por el teorema 6.22 la forma representa 0 en $\mathbb{Q}_p$. Esto significa que las condiciones del teorema para la representación de 0 en $\mathbb{Q}$ son en realidad un número finito (y esto es válido para formas con cualquier número de variables). El teorema de Hasse-Minkowski nos da, pues, un criterio explícito y verificable en un número finito de pasos para saber si una forma cuadrática representa o no 0 en $\mathbb{Q}$. Para el caso $n = 3$ tal criterio (en otros términos que no involucran números p-ádicos) era ya conocido por Legendre.

Puesto que la forma $ax^2 + by^2 + cz^2$ representa 0 en $\mathbb{R}$, no puede ocurrir que los tres coeficientes sean del mismo signo. Multiplicando por -1 si es preciso podemos suponer que dos son positivos y uno negativo. Mediante un cambio de variables podemos eliminar todos los cuadrados, con lo que podemos suponer que a, b, c son libres de cuadrados y primos entre sí. Más aún, si dos de ellos tienen un factor común p, digamos $p \mid a$, $p \mid b$, entonces multiplicando por p y eliminando el cuadrado pasamos a una forma con coeficientes a/p, b/p, pc. Repitiendo este proceso llegamos a una forma $ax^2 + by^2 - cz^2$ donde a, b, c son números naturales libres de cuadrados y primos entre sí dos a dos.

Sea p un divisor primo impar del coeficiente c. Como f representa 0 en $\mathbb{Q}_p$, por el teorema 6.14 la forma ax^2+by^2 también representa 0 en $\mathbb{Q}_p$ y, claramente entonces, la congruencia $ax^2 + by^2 \equiv 0 \pmod{p}$ tiene una solución no trivial, digamos (x_0, y_0) con $y_0 \not\equiv 0 \pmod{p}$. Esto nos da la factorización

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Como c es 0 módulo p en realidad tenemos una factorización de la forma original:

$$ax^2 + by^2 - cz^2 \equiv L^p(x, y, z)M^p(x, y, z) \pmod{p},$$

donde L^p y M^p son formas lineales con coeficientes enteros. Lo mismo vale para los divisores primos impares de a y b. Para $p = 2$ también es cierto, aunque no necesitamos las hipótesis:

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \text{ (mód } p).$$

Si para cada primo $p \mid abc$ tomamos $r_p \in \mathbb{Z}$ de modo que $r_p \equiv 1$ (mód p), $r_p \equiv 0$ (mód abc/p) y sumamos las formas $r_p L^p(x, y, z)$, por una parte y por otra las formas $r_p M^p(x, y, z)$, obtenemos formas lineales $L(x, y, z)$, $M(x, y, z)$ con coeficientes enteros tales que

$$L(x, y, z) \equiv L^p(x, y, z) \text{ (mód } p), \qquad M(x, y, z) \equiv M^p(x, y, z) \text{ (mód } p)$$

para todos los divisores primos de abc. Claramente entonces

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)M(x, y, z) \text{ (mód } abc)$$

Podemos ignorar el caso $a = b = c = 1$, pues la forma $x^2 + y^2 - z^2$ representa 0 en $\mathbb{Q}$, luego no hay nada que probar.

Ahora daremos valores enteros a las variables (x, y, z) de modo que

$$0 \le x < \sqrt{bc}, \quad 0 \le y < \sqrt{ac}, \quad 0 \le z < \sqrt{ab}. \tag{6.3}$$

Puesto que a, b, c son libres de cuadrados y primos entre sí dos a dos, los números $\sqrt{bc}$, $\sqrt{ac}$, $\sqrt{ab}$ no son enteros. El número de ternas que cumplen 6.3 es el producto de las partes enteras por exceso de $\sqrt{bc}$, $\sqrt{ac}$, $\sqrt{ab}$, que es estrictamente mayor que

$$\sqrt{bc}\sqrt{ac}\sqrt{ab} = abc.$$

Como $L(x, y, z)$ sólo puede tomar abc valores módulo abc, han de existir dos ternas distintas (x_1, y_1, z_1) y (x_2, y_2, z_2) tales que

$$L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \text{ (mód } abc).$$

Llamando (x_0, y_0, z_0) a la diferencia de ambas ternas, la linealidad de L implica que $L(x_0, y_0, z_0) \equiv 0$ (mód abc). Así,

$$ax_0^2 + by_0^2 - cz_0^2 \equiv L(x_0, y_0, z_0)M(x_0, y_0, z_0) \equiv 0 \text{ (mód } abc).$$

Además tenemos que $|x_0| < \sqrt{bc}$, $|y_0| < \sqrt{ac}$, $|z_0| < \sqrt{ab}$, de donde se sigue que $-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc$.

Esto sólo es posible si $ax_0^2 + by_0^2 - cz_0^2 = 0$ o bien $ax_0^2 + by_0^2 - cz_0^2 = abc$. En el primer caso ya tenemos que $ax^2 + by^2 - cz^2$ representa 0 en $\mathbb{Q}$ (pues la terna (x_0, y_0, z_0) no es nula). En el segundo caso se comprueba que

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

Si $z_0^2 + ab \neq 0$ tenemos que $ax^2 + by^2 - cz^2$ representa 0 en $\mathbb{Q}$. Si $-ab = z_0^2$, entonces la forma $ax^2 + by^2$ representa 0 (por el teorema 6.7), luego $ax^2 + by^2 - cz^2$ también. ∎

Observemos que en la demostración anterior no hemos usado la hipótesis de que la forma represente 0 en $\mathbb{Q}_2$. Como consecuencia resulta que si una forma cuadrática de tres variables representa 0 en todos los cuerpos $\mathbb{Q}_p$, incluido $p = \infty$, salvo quizá para $p = 2$, entonces representa 0 en $\mathbb{Q}$, y por lo tanto también en $\mathbb{Q}_2$. La causa de este fenómeno se encuentra en la ley de reciprocidad cuadrática: a efectos de representación de 0 toda forma f con tres variables puede expresarse como $ax^2 + by^2 - z^2$ (tomando una equivalente diagonal y dividiendo entre el tercer coeficiente). Entonces, $(a, b)_p = 1$ equivale a que f represente 0 en $\mathbb{Q}_p$, y la fórmula del producto 6.30 implica que si esto sucede para todos los primos salvo quizá uno (incluido $p = \infty$) también ha de cumplirse para éste último.

El teorema de Hasse-Minkowski también nos permite reducir la equivalencia de formas cuadráticas en $\mathbb{Q}$ a la equivalencia en los cuerpos p-ádicos. Para verlo necesitamos un resultado general:

Definición 6.33 Si f y g son dos formas cuadráticas sobre un cuerpo K con m y n variables respectivamente, llamaremos *suma directa* de f y g a la forma cuadrática dada por

$$(f \oplus g)(x_1, \ldots, x_{m+n}) = f(x_1, \ldots, x_m) + g(x_{m+1}, \ldots, x_{m+n}).$$

Claramente la suma directa de formas cuadráticas regulares es de nuevo una forma cuadrática regular (su determinante es el producto de los determinantes).

Teorema 6.34 (Teorema de Witt) *Sean f, g, h formas cuadráticas regulares en un cuerpo K. Si $f \oplus g$ es equivalente a $f \oplus h$, entonces g es equivalente a h.*

Demostración: Si cambiamos f por una forma equivalente sigue cumpliéndose la hipótesis, luego podemos suponer que f es diagonal. De aquí se sigue que es suficiente probar el teorema para el caso en que $f(x) = ax^2$ con $a \neq 0$. Sean A y B las matrices de g y h. Entonces las matrices de $f \oplus g$ y $f \oplus h$ son respectivamente

$$\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix},$$

donde 0 representa en cada caso a una fila o a una columna de ceros.

Como $ax^2 \oplus g$ y $ax^2 \oplus h$ son equivalentes, sus matrices verifican la relación

$$\begin{pmatrix} \gamma & T' \\ S' & Q' \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix},$$

para una cierta matriz regular. Esto equivale a las ecuaciones

$$\begin{aligned} \gamma^2 a + T'AT &= a, \\ \gamma a S + T'AQ &= 0, \\ S'aS + Q'AQ &= B. \end{aligned}$$

Sea $M = Q + kTS$ para un cierto $k \in K$. Vamos a ver que eligiendo k adecuadamente se cumplirá que M es regular y $M'AM = B$, con lo que g y h serán equivalentes. Tenemos

$$M'AM = (Q'+kS'T')A(Q+kTS) = Q'AQ+kS'T'AQ+kQ'ATS+k^2S'T'ATS$$

$$= Q'AQ-k\gamma aS'S-k\gamma aS'S+k^2(a-\gamma^2a)S'S = Q'AQ+a\big((1-\gamma^2)k^2-2k\gamma\big)S'S.$$

Esto será igual a B si $(1-\gamma^2)k^2 - 2k\gamma = 1$, o sea, si $k^2 - (\gamma k + 1)^2 = 0$.

Basta tomar k de modo que $k = \gamma k + 1$, es decir, $k = 1/(1-\gamma)$ salvo que $\gamma = 1$, en cuyo caso la ecuación se reduce a $-2k = 1$ y sirve $k = -1/2$ (suponemos siempre que la característica de K es impar).

Así pues, para el k adecuado, tenemos $M'AM = B$, y como B es regular, M también ha de serlo. ∎

Teorema 6.35 *Dos formas cuadráticas regulares con coeficientes racionales son racionalmente equivalentes si y sólo si son equivalentes en $\mathbb{Q}_p$ para todo primo p, incluido $p = \infty$.*

Demostración: Por inducción sobre el número n de variables. Si $n = 1$ dos formas ax^2 y bx^2 son equivalentes en un cuerpo si y sólo si a/b es un cuadrado. Pero, como hemos visto en la prueba del teorema 6.31 para $n = 1$, si a/b es un cuadrado en todos los cuerpos $\mathbb{Q}_p$ entonces es un cuadrado en $\mathbb{Q}$.

Supongamos que $n > 1$. Sean dos formas f y g según las hipótesis. Sea r un número racional no nulo representado por f. Como f y g son equivalentes en los cuerpos $\mathbb{Q}_p$, tenemos que g representa a r en todos estos cuerpos, y por el teorema 6.32 resulta que g representa a r en $\mathbb{Q}$.

Por el teorema 6.2 tenemos que f y g son equivalentes a formas $rx^2 \oplus f'$ y $rx^2 \oplus g'$. Por el teorema anterior f' y g' son equivalentes en todos los cuerpos $\mathbb{Q}_p$, luego por hipótesis de inducción tenemos que f' y g' son equivalentes en $\mathbb{Q}$, con lo que f y g también lo son. ∎

Observemos que con la prueba del teorema de Hasse-Minkowski para formas de hasta tres variables tenemos probado el teorema anterior para formas cuadráticas binarias. Para este caso, podemos dar condiciones mucho más simples en términos de los invariantes definidos en 6.27.

Definición 6.36 Sea f una forma cuadrática binaria sobre $\mathbb{Q}$. Entonces el determinante de f se expresa de forma única como $d(f) = \delta(f)c^2$, donde $\delta(f)$ es un número racional libre de cuadrados. Es claro que $\delta(f)$ es un invariante, es decir, que si f y g son formas equivalentes, entonces $\delta(f) = \delta(g)$.

Para cada primo p tenemos definido $\psi_p(f) = \big(r, -\delta(f)\big)_p$, donde r es cualquier número racional no nulo representado por f (definición 6.27).

También es obvio que si f y g son (racionalmente) equivalentes también son equivalentes en $\mathbb{Q}_p$, y entonces $\psi_p(f) = \psi_p(g)$. Todo esto se cumple trivialmente en el caso $p = \infty$.

Combinando los teoremas 6.28 y 6.35 (junto con sus versiones para ∞) obtenemos:

Teorema 6.37 *Dos formas cuadráticas binarias f y g sobre $\mathbb{Q}$ son (racionalmente) equivalentes si y sólo si $\delta(f) = \delta(g)$ y $\psi_p(f) = \psi_p(g)$ para todo primo p, incluido $p = \infty$.*

Para calcular $\psi_p(f)$ podemos tomar una forma equivalente, luego podemos suponer que f es del tipo $ax^2 + by^2$. Se cumplirá que $\psi_p(f) = 1$ si y sólo si $ax^2 + by^2 - z^2$ representa 0 en $\mathbb{Q}_p$. Por el teorema 6.22 esto se cumple siempre que p es impar y no divide a ab. Por lo tanto las condiciones en el teorema anterior se reducen a un número finito y son decidibles en la práctica.

Pasamos ahora a probar el teorema de Hasse-Minkowski en el caso general. Para ello necesitaremos el siguiente hecho auxiliar:

Teorema 6.38 *Sea K un cuerpo de característica distinta de 2 y con más de cinco elementos. Si una forma cuadrática diagonal representa 0 en K, entonces tiene una representación de 0 en la que ninguna variable toma el valor 0.*

Demostración: Primeramente demostramos que si $ax^2 = c \neq 0$, entonces para todo $b \neq 0$ existen elementos no nulos α y β tales que $a\alpha^2 + b\beta^2 = c$. Para ello consideramos la identidad

$$\frac{(t-1)^2}{(t+1)^2} + \frac{4t}{(t+1)^2} = 1.$$

Multiplicamos por $ax^2 = c$ y queda

$$a\left(x\,\frac{t-1}{t+1}\right)^2 + at\left(\frac{2x}{t+1}\right)^2 = c.$$

Existe un $\gamma \in K$ tal que $\gamma \neq 0$ y $t = b\gamma^2/a \neq \pm 1$. Esto se debe a que las ecuaciones $b\gamma^2 = \pm 1$ tienen a lo sumo dos soluciones cada una, y K contiene al menos un sexto elemento, aparte de las posibles cuatro soluciones y el 0.

Para este valor de t se cumple

$$a\left(x\,\frac{t-1}{t+1}\right)^2 + b\left(\frac{2x\gamma}{t+1}\right)^2 = c,$$

tal y como queríamos.

Sea ahora $a_1x_1^2 + \cdots + a_nx_n^2 = 0$ una representación de 0 de una forma cuadrática diagonal sobre K.

Podemos ordenar las variables de modo que sean todas no nulas hasta x_r mientras que $x_{r+1} = \cdots = x_n = 0$. Obviamente $r \geq 2$. Según lo probado, existen α y β no nulos en K tales que $a_rx_r^2 = a_r\alpha^2 + a_{r+1}\beta^2$.

Esto nos da una representación de 0 donde el número de variables no nulas ha aumentado en una unidad. Repitiendo el proceso se llega a una representación sin variables nulas. ∎

Conclusión de la prueba de 6.31:

Consideremos ahora una forma con cuatro variables

$$aw^2 + bx^2 + cy^2 + dz^2,$$

donde, como en el caso $n = 3$, podemos suponer que los coeficientes son enteros libres de cuadrados. Además, como la forma representa 0 en $\mathbb{R}$, no todos los coeficientes tienen el mismo signo. Podemos suponer que $a > 0$ y $d < 0$.

Consideraremos también las formas $g = aw^2 + bx^2$ y $h = -cy^2 - dz^2$. Vamos a demostrar que g y h representan en $\mathbb{Q}$ a un mismo entero racional no nulo, con lo que tendremos una representación de 0 en $\mathbb{Q}$ de la forma dada.

Sean $p_1, \ldots, p_s$ los primos impares distintos que dividen a los coeficientes a, b, c, d. Para cada uno de estos primos, así como para $p = 2$, podemos encontrar una representación de 0 en $\mathbb{Q}_p$ de la forma $aw^2 + bx^2 + cy^2 + dz^2 = 0$ donde ninguna de las variables sea nula. Además podemos exigir que todas tomen valores enteros y que uno de ellos no sea divisible entre p.

Sea $b_p = aw^2 + bx^2 = -cy^2 - dz^2 \in \mathbb{Z}_p$. Podemos exigir que $b_p \neq 0$, pues si el así obtenido es 0, las formas g y h representan 0 en $\mathbb{Q}_p$, luego representan a todos los números p-ádicos y podemos tomar cualquier otro.

Además podemos exigir que $p^2 \nmid b_p$, pues si $p^{2k} \mid b_p$ podemos cambiar b_p por b_p/p^{2k}, w por w/p^k, x por x/p^k, etc.

Consideremos el sistema de congruencias

$$\begin{aligned} t &\equiv b_2 \pmod{16}, \\ t &\equiv b_{p_1} \pmod{p_1^2}, \\ &\vdots \qquad\quad \vdots \\ t &\equiv b_{p_s} \pmod{p_s^2}. \end{aligned} \tag{6.4}$$

Podemos sustituir cada b_p por un número entero congruente respecto al módulo indicado y aplicar el teorema chino del resto para obtener un entero t que satisfaga estas ecuaciones, y que estará unívocamente determinado módulo $m = 16\, p_1^2 \cdots p_2^2$.

Para cada índice i tenemos que $v_{p_i}(t) = v_{p_i}(b_{p_i})$, luego $b_{p_i} t^{-1}$ es una unidad, y además $b_{p_i} t^{-1} \equiv 1 \pmod{p_i}$. Por el teorema 6.9 tenemos que $b_{p_i} t^{-1}$ es un cuadrado en $\mathbb{Q}_{p_i}$. Igualmente, $b_2 t^{-1}$ es una unidad y $b_2 t^{-1} \equiv 1 \pmod 8$, luego por el teorema 6.12 también es un cuadrado.

Así pues, para $p = 2, p_1, \ldots, p_s$ se cumple que $b_p t^{-1}$ es un cuadrado en $\mathbb{Q}_p$, luego las formas $-tx_0^2 \oplus g$ y $-tx_0^2 \oplus h$ representan 0 en $\mathbb{Q}_p$. Podemos tomar $t > 0$ y entonces, puesto que $a > 0$ y $d < 0$, tenemos que $-tx_0^2 \oplus g$ y $-tx_0^2 \oplus h$ también representan 0 en $\mathbb{R}$.

Si p es cualquier otro primo que además no divida a t, como no divide a ninguno de los coeficientes de g y de h, todos los coeficientes de las formas $-tx_o^2 \oplus g$ y $-tx_0^2 \oplus h$ son unidades en $\mathbb{Q}_p$, luego por el teorema 6.22 ambas formas representan 0.

Vamos a probar que podemos elegir t de modo que a lo sumo haya un único primo q que divida a t y sea distinto de $2, p_1, \ldots, p_s$. Entonces tendremos que las formas $-tx_0^2 \oplus g$ y $-tx_o^2 \oplus h$ representan 0 en todos los cuerpos $\mathbb{Q}_p$, incluyendo

$p = \infty$, salvo quizá para el primo q. Usando la fórmula del teorema 6.30 (aún no demostrada) resulta que también representan 0 en el caso exceptuado (ver la observación tras el teorema). Por el teorema 6.31 para formas de tres variables resulta que $-tx_0^2 \oplus g$ y $-tx_0^2 \oplus h$ representan 0 en $\mathbb{Q}$. Por el teorema 6.5 las formas g y h representan ambas a t y el teorema quedará probado (para cuatro variables).

Sea t cualquier entero que cumpla las congruencias (6.4). En su lugar podemos tomar cualquier otro número de la forma $t + km$. Veamos que uno de éstos nos sirve.

Sea d el máximo común divisor de t y m. Sean $t' = t/d$ y $m' = m/d$. Entonces t' y m' son primos entre sí. Ahora usamos el teorema de Dirichlet sobre primos en progresiones aritméticas, que nos garantiza la existencia de un primo de la forma $q = t' + km'$. Entonces $t^* = t + km = dq$ sólo es divisible entre un primo distinto de $2, p_1, \ldots, p_s$, tal y como queríamos.

Probamos ahora el teorema para formas con cinco variables:

$$av^2 + bw^2 + cx^2 + dy^2 + ez^2.$$

Como en los casos anteriores podemos suponer que los coeficientes son enteros y libres de cuadrados. Si esta forma representa 0 en $\mathbb{R}$ entonces no todos los coeficientes tienen el mismo signo. Digamos $a > 0$, $e < 0$. Sea $g = av^2 + bw^2$, $h = -cx^2 - dy^2 - ez^2$.

Razonamos exactamente igual como en el caso $n = 4$ (usando el teorema de Dirichlet) para probar que existe un número natural t representado por las formas g y h en todos los cuerpos $\mathbb{Q}_p$, incluyendo $p = \infty$, salvo quizá para un primo impar q que no divide a los coeficientes a, b, c, d, e.

Igualmente se prueba que la forma g representa a t también en $\mathbb{Q}_q$, luego en $\mathbb{Q}$. Para la forma h usamos otro argumento: por el teorema 6.22 representa 0 en $\mathbb{Q}_q$, luego por el teorema 6.4 también representa a t. Con esto concluimos que g y h representan a t en $\mathbb{Q}$ y la prueba termina.

Observemos que por el teorema 6.20 toda forma cuadrática con cinco o más variables representa 0 en todos los cuerpos p-ádicos, luego lo que hemos probado es que una forma con cinco variables representa 0 en $\mathbb{Q}$ si y sólo si representa 0 en $\mathbb{R}$, y lo mismo hay que probar para formas de más de cinco variables. Ahora bien, toda forma con más de cinco variables es equivalente a una forma diagonal, y si representa 0 en $\mathbb{R}$ no todos los coeficientes tendrán el mismo signo, luego podemos ordenar las variables de modo que los dos primeros coeficientes tengan signos distintos, y así la forma dada se descompone como $f \oplus g$, donde f es una forma diagonal con cinco variables que representa 0 en $\mathbb{R}$ y g es cualquier forma. Por el caso $n = 5$ tenemos que f representa 0 en $\mathbb{Q}$, luego $f \oplus g$ también. ∎

6.5 Sumas de cuadrados

Terminamos este capítulo demostrando a partir del teorema de Hasse-Minkowski los teoremas [ITAl 7.8], [ITAl 3.5]. Nos apoyaremos en el teorema siguiente:

Teorema 6.39 *Sea f una forma cuadrática con coeficientes enteros definida positiva (es decir, $f(x) \geq 0$ para todo $x \in \mathbb{Q}^n$ y $f(x) = 0$ si y sólo si $x = 0$) y supongamos que para todo $x \in \mathbb{Q}^n$ existe un $x' \in \mathbb{Z}^n$ tal que $f(x - x') < 1$. Entonces todos los números naturales representados por f en $\mathbb{Q}$ son representados también en $\mathbb{Z}$.*

DEMOSTRACIÓN: Sea A la matriz simétrica asociada a f, es decir, la matriz que cumple $f(x) = xAx^t$ para todo $x \in \mathbb{Q}^n$. Los coeficientes de A son enteros o semienteros.

Para cada par de n-tuplas $x, y \in \mathbb{Q}^n$ definimos $g(x, y) = xAy^t$. La aplicación g es una forma bilineal simétrica y $f(x) = g(x, x)$. Además g toma valores enteros o semienteros sobre los números enteros.

Sea n un número natural representado racionalmente por f. Entonces existe un $x \in \mathbb{Z}^n$ tal que $f(x) = t^2 n$ para cierto número natural $t > 0$, que podemos tomar mínimo. Basta probar que $t = 1$.

Por hipótesis existe un $y \in \mathbb{Z}^n$ tal que $z = x/t - y$ cumple $g(z, z) < 1$.

Si fuera $g(z, z) = 0$ entonces $z = 0$ (porque f no representa cero) y así resulta que $x/t = y + z$ tiene coeficientes enteros. Como $f(x/t) = n$ la minimalidad de t implica que $t = 1$.

Si $g(z, z) \neq 0$ sean

$$a = g(y, y) - n, \quad b = 2\big(nt - g(x, y)\big), \quad t' = at + b, \quad x' = ax + by.$$

Entonces a, b, t' son enteros y

$$\begin{aligned} tt' &= at^2 + bt = t^2 g(y, y) - nt^2 + 2nt^2 - 2t\, g(x, y) \\ &= t^2\, g(y, y) - 2t\, g(x, y) + g(x, x) = g\big((ty - x), (ty - x)\big) = t^2\, g(z, z). \end{aligned}$$

Así pues, $t' = tg(z, z)$ y, como $0 < g(z, z) < 1$, resulta que $0 < t' < t$. Por otra parte,

$$\begin{aligned} g(x', x') &= a^2\, g(x, x) + 2ab\, g(x, y) + b^2\, g(y, y) \\ &= a^2 t^2 n + ab(2nt - b) + b^2(n + a) = n(a^2 t^2 + 2abt + b^2) = t'^2 n, \end{aligned}$$

lo que contradice la minimalidad de t ∎

Teorema 6.40 (Gauss) *Un número natural es suma de tres cuadrados si y sólo si no es de la forma $4^n(8m - 1)$.*

DEMOSTRACIÓN: La forma cuadrática $f(x, y, z) = x^2 + y^2 + z^2$ está en las hipótesis del teorema anterior, pues sin duda es definida positiva y, dada una terna (x, y, z) de números racionales, siempre podemos encontrar una terna (x', y', z') de números enteros tales que

$$|x - x'| < 1/2, \quad |y - y'| < 1/2, \quad |z - z'| < 1/2,$$

con lo que $f(x - x', y - y', z - z') \leq 1/4 + 1/4 + 1/4 = 3/4 < 1$. Por lo tanto basta probar que un número natural está representado racionalmente por f si y sólo

si no es de la forma indicada. Por el teorema 6.32 los números representados racionalmente por f son los representados por f en $\mathbb{R}$ y en todos los cuerpos p-ádicos.

Obviamente los números racionales representados por f en $\mathbb{R}$ son exactamente los mayores que 0 y por el teorema 6.22 f representa 0 en todos los cuerpos $\mathbb{Q}_p$ con $p \neq 2$, luego también a cualquier número racional.

Concluimos que un número natural a es suma de tres cuadrados si y sólo si está representado por f en $\mathbb{Q}_2$.

Ahora bien, f representa a a en $\mathbb{Q}_2$ si y sólo si la forma $x^2+y^2+z^2-at^2$ representa 0 (teorema 6.5) y a su vez esto equivale a que exista un número diádico no nulo u tal que x^2+y^2 represente a u y z^2-at^2 represente a $-u$ (en principio u podría ser 0, pero en tal caso ambas formas binarias representan 0 y podemos tomar cualquier u.

De nuevo por el teorema 6.5 esto equivale a que exista un número diádico u tal que las formas $x^2+y^2-uw^2$ y $z^2-at^2+uw^2$ representen 0, y en términos del símbolo de Hilbert esto se expresa como que $(-1,u)_2 = 1 = (a,-u)_2$.

Esta condición depende sólo de las clases de a y de u módulo $\mathbb{Q}_2^{*2}$. Un conjunto de representantes de estas clases es $1,3,5,7,2,6,10,14$. La condición $(-1,u)_2=1$ la cumplen los números congruentes con $1,5,2,10$ (observemos que -1 es congruente con 7 y considerar la tabla calculada en la prueba de 6.23). Los valores de $-u$ son, pues, $7,3,14,6$. La misma tabla nos da que para cualquier a podemos encontrar un $-u$ entre estos cuatro que haga $(a,-u)_2=1$ salvo si $a \equiv 7 \pmod{\mathbb{Q}_2^{*2}}$.

Por lo tanto los números naturales n representados por f son todos excepto los que cumplen $a \equiv 7 \pmod{\mathbb{Q}_2^{*2}}$, o equivalentemente, $-a \equiv 1 \pmod{\mathbb{Q}_2^{*2}}$, o sea, excepto los que cumplen que $-a$ es un cuadrado en $\mathbb{Q}_2$.

Por el teorema 6.12 esto equivale a que $-a$ sea de la forma $4^n(8m+1)$, o equivalentemente, a que a sea de la forma $4^n(8m-1)$. ∎

Teorema 6.41 (Lagrange) *Todo número natural es suma de cuatro cuadrados.*

Demostración: Todo número natural a es de la forma $a = 4^n m$, donde m no es divisible entre 4. Si m es congruente con $1,2,3,5,6$, módulo 8 entonces a es suma de tres cuadrados. En caso contrario $m \equiv 7 \pmod 8$ y por lo tanto $m-1 \equiv 6 \pmod 8$ sí es suma de tres cuadrados.

Así pues, si $m-1 = x^2+y^2+z^2$, tenemos que

$$a = 4^n m = (2^n x)^2 + (2^n y)^2 + (2^n z)^2 + (2^n)^2.$$

∎

Ejercicio: Probar que un número natural a es suma de dos cuadrados si y sólo sí los primos impares que lo dividen con exponente impar son congruentes con 1 módulo 4.

Capítulo VII

La teoría de los géneros

Presentamos aquí, con un enfoque moderno, la teoría de Gauss sobre géneros de formas cuadráticas binarias que expusimos en el capítulo XIV de [ITAl]. En este capítulo, y mientras no se indique lo contrario, la expresión 'forma cuadrática' la usaremos exclusivamente en el sentido de la sección [ITAl 11.1], es decir, que nos referiremos a formas cuadráticas binarias, con coeficientes enteros, regulares (es decir, con determinante o discriminante no nulo), primitivas y definidas positivas en caso de que el discriminante sea negativo.

7.1 Géneros de formas y módulos

El punto de partida de la teoría de géneros es el hecho evidente de que para que la ecuación $f(x,y) = m$ tenga soluciones enteras, donde f es una forma cuadrática, es necesario que las congruencias $f(x,y) \equiv m \pmod{n}$ tengan solución para todo número natural n. Esto nos lleva al concepto de equivalencia modular [ITAl 14.1] que recordamos aquí:

Definición 7.1 Diremos que dos formas cuadráticas f y g son *equivalentes* módulo un natural $n > 1$ si existen enteros a, b, c, d tales que

$$f(x,y) \equiv g(ax+by, cx+dy) \pmod{n} \qquad (ad-bc, n) = 1.$$

Al exigir que el determinante del cambio de variables sea primo con n garantizamos que tenga inverso módulo n, de modo que dos formas equivalentes módulo n representan los mismos números módulo n. Es obvio que la equivalencia módulo n es una relación de equivalencia en el sentido usual del término, así como que dos formas equivalentes (en $\mathbb{Z}$) son equivalentes módulo cualquier natural n. El teorema siguiente [ITAl 14.2] nos indica que es suficiente estudiar la equivalencia módulo potencias de primos:

Teorema 7.2 *Sean m y n dos números naturales primos entre sí. Entonces dos formas cuadráticas son equivalentes módulo mn si y sólo si son equivalentes módulo m y módulo n.*

En [ITAl 14.3] probamos que, si p es un primo impar y r es cualquier resto no cuadrático módulo p prefijado, toda forma cuadrática de discriminante D es equivalente módulo p^n a una de las formas

$$x^2 - Dy^2 \qquad \text{o} \qquad r(x^2 - Dy^2).$$

Si $p \nmid D$ ambas formas resultan ser equivalentes módulo p^n, por lo que hay una única clase de equivalencia de formas módulo p^n, mientras que si $p \mid D$ la primera representa únicamente restos cuadráticos módulo p y la segunda restos no cuadráticos, por lo que tenemos dos clases de formas. Para distinguirlas Gauss introdujo el concepto de 'carácter módulo p' [ITAl 14.4]:

Definición 7.3 Sea f una forma cuadrática de discriminante D y p un primo impar tal que $p \mid D$. Diremos que f tiene *carácter positivo* módulo p si f representa restos cuadráticos módulo p. En caso contrario se dice que f tiene *carácter negativo* módulo p. Equivalentemente, definimos el *carácter* módulo p de f como

$$\chi_p(f) = \left(\frac{a}{p}\right),$$

donde a es cualquier número representado por f que sea primo con p. Si $p \nmid D$ definimos $\chi_p(f) = 1$.

En estos términos, tenemos que dos f y g de discriminante D son equivalentes módulo p^n si y sólo si tienen el mismo carácter módulo p.

Si $p = 2$, la equivalencia módulo p^n requiere considerar cuatro caracteres posibles, incluyendo el trivial:

Definición 7.4 Las funciones δ y ϵ, definidas sobre los enteros impares, son las dadas por

$$\delta(k) = (-1)^{(k-1)/2} = \begin{cases} 1 & \text{si } k \equiv 1 \pmod 4 \\ -1 & \text{si } k \equiv -1 \pmod 4 \end{cases}$$

$$\epsilon(k) = (-1)^{(k^2-1)/8} = \begin{cases} 1 & \text{si } k \equiv \pm 1 \pmod 8 \\ -1 & \text{si } k \equiv \pm 5 \pmod 8 \end{cases}$$

Podemos considerar a δ y ϵ como funciones en U_8, y entonces δ distingue a $\{1, 5\}$ de $\{-1, -5\}$, mientras que ϵ distingue a $\{1, -1\}$ de $\{5, -5\}$ y su producto $\epsilon\delta$ distingue a $\{1, -5\}$ de $\{-1, 5\}$.

Si f es una forma cuadrática de discriminante par D y a es cualquier número impar representado por f, definimos el *carácter* módulo 2 de f como

$$\chi_2(f) = \begin{cases} 1 & \text{si} \quad D/4 \equiv 1, 5 \pmod 8 \\ \epsilon(a) & \text{si} \quad D/4 \equiv 2 \pmod 8 \\ \delta(a) & \text{si} \quad D/4 \equiv 3, 4, 7 \pmod 8 \\ \delta(a)\epsilon(a) & \text{si} \quad D/4 \equiv 6 \pmod 8 \end{cases}$$

Si $D/4 \equiv 0 \pmod 8$ definimos tres caracteres de f módulo 2, dados por

$$\chi_{21}(f) = \delta(a), \quad \chi_{22}(f) = \epsilon(a), \quad \chi_{23}(f) = \delta(a)\epsilon(a).$$

Finalmente, si D es impar, definimos $\chi_2(f) = 1$.

En estos términos, se cumple que dos formas cuadráticas son equivalentes módulo 2^n (con $n \geq 3$) si y sólo si tienen el mismo carácter módulo 2 (o los mismos caracteres en el caso en que $D/4 \equiv 0$ (mód 8)).

En resumen, para cada discriminante D y para cada primo p tenemos definido un carácter $\chi_p^* : U_p \longrightarrow \{\pm 1\}$ si p es impar, o $\chi_2^* : U_8 \longrightarrow \{\pm 1\}$ si $p = 2$ (en este caso pueden ser tres caracteres), de manera que para cada forma cuadrática f de discriminante D se cumple que $\chi_p(f) = \chi_p^*\big([a]\big)$, donde a es cualquier número primo con p representado por f.

El carácter χ_p^* es constante igual a 1 si $p \nmid D$, es el símbolo de Legendre de p si $p \mid D$ es impar y es una de las funciones $1, \delta, \epsilon, \epsilon\delta$ (o las tres) si $p = 2$, y se cumple el teorema [ITAl 14.6]:

Teorema 7.5 *Si p es primo, dos formas cuadráticas de discriminante D son equivalentes módulo p^n (para $n \geq 3$ si $p = 2$) si y sólo si tienen el mismo carácter módulo p. Esto ocurre siempre que $p \nmid D$.*

En particular, si C es una clase de equivalencia (estricta o no estricta) de formas cuadráticas de discriminante D, podemos definir $\chi_p(C)$ como el carácter de cualquiera de sus miembros. Recordamos ahora el concepto de género de una forma cuadrática, definido en [ITAl 14.8]:

Definición 7.6 Diremos que dos formas cuadráticas de un mismo discriminante D son del mismo *género* si tienen los mismos caracteres.

Según los teoremas 7.2 y 7.5, dos formas son del mismo género si y sólo si representan los mismos enteros módulo cualquier número natural $n > 1$.

Más aún, en [ITAl 12.19] establecimos una biyección entre las clases de equivalencia estricta de formas cuadráticas de un discriminante dado D y las clases de similitud estricta de módulos cuyo anillo de coeficientes es el orden cuadrático de discriminante D. A través de esta correspondencia podemos definir [ITAl 14.10] los *caracteres* y el *género* de una clase de similitud estricta de módulos C como los caracteres y el género de su clase de formas asociada. A su vez, definimos los *caracteres* y el *género* de un módulo en particular como los de su clase de similitud estricta.

Recordemos ahora el teorema [ITAl 13.27], en virtud del cual si $\mathcal{O}$ es un orden cuadrático, toda clase de similitud estricta de módulos de $\mathcal{O}$ admite como representante a un ideal de norma prima con cualquier entero prefijado n. Cuando hablemos de un ideal de un orden cuadrático $\mathcal{O}$, sobrentenderemos siempre que su norma es prima con el índice de $\mathcal{O}$ en su orden maximal. Se cumple el teorema [ITAl 14.2]:

Teorema 7.7 *Sea $\mathcal{O}$ un orden cuadrático, $\mathfrak{a}$ un ideal de $\mathcal{O}$ y p un primo que no divida a $\mathrm{N}(\mathfrak{a})$. Entonces $\chi_p(\mathfrak{a}) = \chi_p^*\big(\mathrm{N}(\mathfrak{a})\big)$.*

Este teorema tiene muchas consecuencias. La más importante es que, en términos de módulos, los caracteres son homomorfismos de grupos, es decir, son caracteres en el sentido de la teoría de grupos [ITAl 14.3]:

Teorema 7.8 *Si M y N son módulos de un mismo orden cuadrático $\mathcal{O}$ y p es un primo, entonces $\chi_p(MN) = \chi_p(M)\chi_p(N)$. En términos algebraicos, los caracteres son homomorfismos del grupo de los módulos de $\mathcal{O}$ (o del grupo de clases estrictas de $\mathcal{O}$) en el grupo $\{\pm 1\}$.*

Si $\mathcal{O}$ es un orden cuadrático, $\chi_1, \ldots, \chi_m$ son sus caracteres, H es su grupo de clases estrictas y llamamos $C_2 = \{\pm 1\}$, entonces tenemos un homomorfismo de grupos

$$\chi : H \longrightarrow \overset{m \text{ veces}}{C_2 \times \cdots \times C_2}$$

que a cada clase le hace corresponder su sistema de caracteres. Dos clases de H son del mismo género si y sólo si tienen la misma imagen por χ. En particular el núcleo de χ es el género formado por las clases cuyos caracteres son todos positivos. A este género lo llamaremos *género principal* G_0. Los géneros son las clases del grupo cociente H/G_0. A este grupo lo llamaremos *grupo de géneros* del orden $\mathcal{O}$. Su orden es potencia de 2 (de hecho, divide a 2^m). También es obvio ahora que todos los géneros contienen el mismo número de clases de similitud estricta.

Hasta aquí nos hemos limitado a citar los hechos probados en [ITAl]. El aporte de la teoría que hemos desarrollado en los capítulos precedentes tiene que ver con el teorema [ITAl 14.17], que justifica que el número de géneros es siempre la mitad del que (*a priori*) podría ser, y que demostramos haciendo cálculos basados en la ley de reciprocidad cuadrática. Ahora vamos a probar que [ITAl 14.17] es, de hecho, equivalente a la ley de reciprocidad cuadrática y usaremos esto para demostrarla. Conviene introducir algunas definiciones:

Definición 7.9 Diremos que un número entero D es un *discriminante fundamental* si es el discriminante del orden maximal de un cuerpo cuadrático.

Si D es el discriminante de un orden cuadrático arbitrario, entonces D se descompone de forma única como $D = m^2 D_0$, donde m es un número natural (el índice del orden) y D_0 es un discriminante fundamental.

Llamaremos *caracteres fundamentales* del orden cuadrático de discriminante D a los caracteres χ_p correspondientes a primos p que dividen al discriminante fundamental D_0, salvo que haya tres caracteres módulo 2, en cuyo caso sólo consideraremos fundamental a uno de ellos, al único que cumple el teorema siguiente, que expresa los caracteres de una forma cuadrática en términos del símbolo de Hilbert:

Teorema 7.10 *Sea $\mathcal{O}$ un orden cuadrático de discriminante D y sea χ_p un carácter fundamental de $\mathcal{O}$. Entonces*

1. *Si f es una forma cuadrática de discriminante D,*

$$\chi_p(f) = (a, D)_p = \psi_p(f),$$

   donde a es cualquier número racional representado racionalmente por f y $\psi_p(f)$ es el invariante definido en 6.27.

2. *Si M es un módulo de $\mathcal{O}$, entonces $\chi_p(M) = (\mathrm{N}(M), D)_p$.*

DEMOSTRACIÓN: 1) Supongamos en primer lugar que p es impar y que a es primo con p. Como D_0 es libre de cuadrados (salvo una posible potencia de 2) se cumple que el exponente de p en $D = m^2 D_0$ es impar. Así pues, teniendo en cuenta las propiedades del símbolo de Hilbert (teorema 6.25)

$$\chi_p(f) = \left(\frac{a}{p}\right) = (a,p)_p = (a,D)_p.$$

Si $p = 2$ (y a es impar) distinguimos casos según el resto de $D/4$ módulo 8. Observemos que en general $(a,D)_2 = (a,D/4)_2$.

- Si $D/4 \equiv 1$ (mód 4) entonces $(a,D/4)_2 = 1 = \chi_2(f)$.
- Si $D/4 \equiv -1$ (mód 4) entonces $(a,D/4)_2 = \delta(a) = \chi_2(a)$.
- Si $D/4 \equiv 2$ (mód 8) entonces $D/4 = 2u$, donde $u \equiv 1$ (mód 4) y así

$$(a,D/4)_2 = (a,2)_2\,(a,u)_2 = (a,2)_2 = \epsilon(a) = \chi_2(f).$$

- Si $D/4 \equiv 6$ (mód 8) entonces $D/4 = 2u$, donde $u \equiv -1$ (mód 4) y

$$(a,D/4)_2 = (a,2)_2\,(a,u)_2 = \epsilon(a)\delta(a) = \chi_2(f).$$

- Si $D/4 \equiv 0$ (mód 8) entonces tenemos tres caracteres módulo 2. Vamos a ver que uno de ellos es $(a,D/4)_2$ (el mismo para toda forma f y todo a). Sea $D/4 = 2^i u$, donde u es impar. Entonces $(a,D/4) = (a,2^i)_2\,(a,u)_2$. El primer factor es 1 o $\epsilon(a)$, según si i es par o impar. El segundo factor es 1 o $\delta(a)$ según el resto de u módulo 4. No pueden ser ambos iguales a 1, pues si i es par, entonces $D_0 = 4d$ (pues $2 \mid D_0$ por definición de carácter fundamental) y como D_0 es un discriminante maximal $d \equiv -1$ (mód 4). Así pues, $(a,D)_2$ es uno de los tres caracteres $\delta(a), \epsilon(a), \delta(a)\epsilon(a)$.

Por otra parte, el discriminante D y el determinante d de la forma f satisfacen la relación $d = -D/4$, por lo que $\psi_p(f) = (a,D/4)_p = (a,D)_p$. Pero el teorema 6.26 nos da que $\psi(f)$ se puede calcular en realidad con cualquier número p-ádico representado por f. En particular con cualquier número racional.

2) Sea (α,β) una base orientada de M. Una forma asociada a M es

$$f(x,y) = \frac{\mathrm{N}(\alpha x + \beta y)}{\mathrm{N}(M)}.$$

Como (α,β) es una $\mathbb{Q}$-base del cuerpo cuadrático al que pertenece M, existen números racionales α, β tales que $\alpha x + \beta y = \mathrm{N}(M)$. Entonces, $f(\alpha,\beta) = \mathrm{N}(M)$, es decir, f representa racionalmente a $\mathrm{N}(M)$, y concluimos por el apartado anterior. ∎

De aquí se siguen muchas consecuencias importantes. Por ejemplo, si H_m es el grupo de clases de un orden $\mathcal{O}_m$ y H es el grupo de clases del orden maximal $\mathcal{O}$, tenemos un epimorfismo α entre ellos dado por $\alpha\big([\mathfrak{a}]\big) = [\mathfrak{a}]$. Si χ_p es un carácter fundamental de $\mathcal{O}_m$, trivialmente lo es de $\mathcal{O}$ también, y por el teorema anterior se cumple

$$\chi_p\Big(\alpha\big([\mathfrak{a}]\big)\Big) = (\mathrm{N}(\mathfrak{a}), D_0)_p = (\mathrm{N}(\mathfrak{a}), m^2 D_0)_p = \chi_p\big([\mathfrak{a}]\big).$$

Esto significa que los caracteres de $\alpha\big([\mathfrak{a}]\big)$ se obtienen sin más que suprimir los caracteres no fundamentales de $[\mathfrak{a}]$. En particular α envía clases del mismo género a clases del mismo género.

Para órdenes maximales el teorema 7.10 puede mejorarse.

Teorema 7.11 *Sea $\mathcal{O}$ un orden cuadrático maximal de discriminante D y sea χ_p cualquier carácter de $\mathcal{O}$. Entonces*

1. *Si f es una forma cuadrática de discriminante D,*

$$\chi_p(f) = (a, D)_p = \psi_p(f),$$

   donde a es cualquier número racional representado racionalmente por f.

2. *Si M es un módulo de $\mathcal{O}$, entonces $\chi_p(M) = (\mathrm{N}(M), D)_p$.*

Demostración: El teorema 7.10 prueba estos hechos en el caso en que $p \mid D$. Si $p \nmid D$ sabemos que $\chi_p(f) = 1$ para toda forma de discriminante D. Por otro lado, a puede tomarse primo con p y entonces, si p es impar, $\psi_p(f) = (a, D)_p = 1$ (pues p divide a D con multiplicidad 1). Si $p = 2$ entonces podemos tomar a impar, y necesariamente $D \equiv 1 \pmod 4$, luego también $\psi_2(f) = (a, D)_2 = 1$. La versión en términos de módulos se deduce de la de formas como en el teorema 7.10. ∎

Ahora podemos comprender por qué el número de géneros es siempre la mitad del que podría ser. En un orden maximal, el número de caracteres negativos de un género ha de ser par, como consecuencia del teorema 6.30 (admitiendo la ley de reciprocidad cuadrática). En efecto, la fórmula producto que aparece en dicho teorema tiene como caso particular que

$$\prod_p \chi_p(M) = \prod_p (\mathrm{N}(M), D)_p = 1.$$

(Falta el factor $(\mathrm{N}(M), D)_\infty$, pero siempre vale 1, porque $\mathrm{N}(M) > 0$.) De hecho vamos a probar que esta propiedad equivale a la ley de reciprocidad cuadrática, y nos basaremos en ello para demostrarla.

Teorema 7.12 *Las siguientes afirmaciones son equivalentes:*

1. *La ley de reciprocidad cuadrática.*

2. *Si M es un módulo de un orden cuadrático maximal de discriminante D, entonces*
$$\prod_p \chi_p(M) = 1,$$
es decir, el número de caracteres negativos de M es par.

3. *Si D es un discriminante fundamental y m es el número de primos distintos que dividen a D, entonces el número de géneros g del orden de discriminante D cumple $g \le 2^{m-1}$.*

DEMOSTRACIÓN: Acabamos de probar que 1) implica 2).

2) implica 3) es evidente, pues de los 2^m géneros posibles, la mitad de ellos tendrían un número impar de caracteres negativos, luego según 2) no se dan. Vamos a probar que 3) implica la ley de reciprocidad cuadrática.

1. Si p es un primo $p \equiv -1$ (mód 4) entonces $(-1/p) = -1$.

   Consideremos $K = \mathbb{Q}\big(\sqrt{-1}\,\big)$, $D = -4$, $m = 1$. Entonces hay un solo género, el principal. Si fuera $(-1/p) = (-4/p) = 1$, entonces p se descompone como producto de dos primos de norma p. Si $\mathfrak{p}$ es uno de estos primos,
   $$\chi_2(\mathfrak{p}) = (p, -4)_2 = (p, -1)_2 = -1,$$
   con lo que el género de p no sería el principal, contradicción.

2. Si p es un primo $p \equiv 1$ (mód 4) entonces $(-1/p) = 1$.

   Consideramos $K = \mathbb{Q}\big(\sqrt{p}\,\big)$, $D = p$, $m = 1$, $g = 1$. Como el único género es el principal, aplicando [ITAl 11.14] tenemos que $1 = \chi_p\big(-1\big) = (-1/p)$.

   Las afirmaciones 1) y 2) prueban la primera ley suplementaria.

3. Si p es un primo $p \equiv 1$ (mód 8) entonces $(2/p) = 1$.

   Consideramos $K = \mathbb{Q}\big(\sqrt{p}\,\big)$, $D = p$, $m = 1$, $g = 1$. Entonces $\big(1 + \sqrt{p}\,\big)/2$ tiene norma par, pero no es divisible entre 2, lo que prueba que 2 se descompone en producto de dos primos de norma 2. Si $\mathfrak{q}$ es uno de estos primos, $1 = \chi_p(\mathfrak{q}) = (2, p)_p = (2/p)$.

4. Si p es un primo $p \equiv 3, 5$ (mód 8) entonces $(2/p) = -1$.

   Tomamos $K = \mathbb{Q}\big(\sqrt{2}\,\big)$, $D = 8$, $m = 1$, $g = 1$. Si $(2/p) = 1$ entonces p se descompone en dos factores de norma p. Si $\mathfrak{p}$ es uno de estos factores $1 = \chi_2(\mathfrak{p}) = (p, 8)_2 = (p, 2)_2 = -1$, contradicción.

5. Si $p \equiv 7$ (mód 8) entonces $(-2/p) = -1$.

   Tomamos$K = \mathbb{Q}\big(\sqrt{-2}\,\big)$, $D = -8$, $m = 1$, $g = 1$ y razonamos igual que en el caso anterior.

6. Si $p \equiv 7$ (mód 8) entonces por 1) y 5)
$$(2/p) = (-1/p)(-2/p) = (-1)(-1) = 1.$$

   Las afirmaciones 3), 4) y 6) prueban la segunda ley suplementaria.

7. Si p y q son primos impares $p \equiv 1 \pmod 4$ y $(q/p) = -1$, entonces también $(p/q) = -1$.

   Tomamos $K = \mathbb{Q}\big(\sqrt{p}\,\big)$, $D = p$, $m = 1$, $g = 1$. Si $(p/q) = 1$, entonces q se escinde en dos primos de norma q. Si $\mathfrak{q}$ es uno de ellos, $1 = \chi_p(\mathfrak{q}) = (q, p)_p = (q/p)$.

8. Si p y q son primos impares $p \equiv -1 \pmod 4$ y $(q/p) = -1$, entonces $(-p/q) = -1$.

   Tomamos $K = \mathbb{Q}\big(\sqrt{-p}\,\big)$, $D = -p$, $m = 1$, $g = 1$ y razonamos igual que en el caso anterior.

   Por 1) y 2), tenemos $(-1/q) \equiv q \pmod 4$, luego 8) implica que $(p/q) = -1$ si $q \equiv 1 \pmod 4$ y $(p/q) = 1$ si $q \equiv -1 \pmod 4$.

9. Si p y q son primos impares $p \equiv 1 \pmod 4$ y $(q/p) = 1$, entonces $(p/q) = 1$.

   Si $q \equiv 1 \pmod 4$, entonces $(p/q) = -1$ implicaría $(q/p) = -1$ por 7).

   Si $q \equiv -1 \pmod 4$, entonces $(p/q) = -1$ implicaría $(q/p) = -1$ por el comentario posterior a 8).

   Los apartados 7) y 9) prueban la mitad de la ley de reciprocidad.

10. Si p y q son primos $p, q \equiv -1 \pmod 4$ y $(q/p) = 1$, entonces $(p/q) = -1$.

    Tomamos $K = \mathbb{Q}\big(\sqrt{pq}\,\big)$, $D = pq$, $m = 2$, $g \le 2$. Entonces $\chi_p(-1) = (-1/p) = -1$ por 1), e igualmente $\chi_q(-1) = -1$, luego $g = 2$ y los géneros son $(++)$, $(--)$.

    Claramente $p = \mathfrak{p}^2$, $q = \mathfrak{q}^2$, para ciertos ideales $\mathfrak{p}$, $\mathfrak{q}$. Como $\mathrm{N}(\sqrt{pq}) = -pq$ ha de ser $\big(\sqrt{pq}\,\big) = \mathfrak{pq}$, luego $[\mathfrak{pq}] = -1$, $[\mathfrak{p}]^2 = 1$, $[\mathfrak{q}]^2 = 1$. Esto implica que $[\mathfrak{p}] = -[\mathfrak{q}]$.

    Ahora bien, $\chi_p\big(-[\mathfrak{q}]\big) = -\chi_p\big([\mathfrak{q}]\big) = -(q/p) = -1$ y $\chi_q\big([\mathfrak{p}]\big) = (p/q)$. Como ambos caracteres han de ser iguales, $\chi_q\big([\mathfrak{p}]\big) = -1$.

    La afirmación 10) y la observación tras 8) completan la prueba. ∎

Ejercicio: Admitiendo la ley de reciprocidad cuadrática, probar que el número de géneros de cualquier orden cuadrático es a lo sumo 2^{m-1}, donde m es el número de caracteres. Si hay tres caracteres módulo 2, el número de géneros es a lo sumo 2^{m-2}.

Dedicaremos la sección siguiente a demostrar la ley de reciprocidad cuadrática. Ahora seguiremos extrayendo consecuencias de los teoremas 7.10 y 7.11. El teorema siguiente es inmediato si tenemos en cuenta 6.37:

Teorema 7.13 *Si D es un discriminante fundamental, entonces dos formas cuadráticas de discriminante D son racionalmente equivalentes si y sólo si son del mismo género. Si D no es fundamental, dos formas del mismo género son racionalmente equivalentes, pero el recíproco es falso en general.*

Ejercicio: Sea D un discriminante fundamental y f, g dos formas de discriminante D. Si f representa un número a y g representa un número b^2a, entonces f y g son del mismo género. El recíproco es cierto aunque el orden no sea maximal.

Una consecuencia inmediata del teorema 7.11 es que en un orden maximal, el género de un módulo depende sólo de su norma. Más exactamente, la situación es ésta:

Teorema 7.14 *Si dos módulos M y M' del orden $\mathcal{O}_m$ de un cuerpo cuadrático K son del mismo género, entonces existe un $\gamma \in K$ de norma positiva tal que $\mathrm{N}(M) = \mathrm{N}(\gamma)\,\mathrm{N}(M')$. Si el orden es el maximal ($m = 1$) entonces el recíproco también es cierto.*

Demostración: Sea $M = \langle u, v\rangle$, $M' = \langle u', v'\rangle$. Las formas asociadas a estos módulos son

$$f(x,y) = \frac{\mathrm{N}(ux+vy)}{\mathrm{N}(M)} \qquad \text{y} \qquad g(x,y) = \frac{\mathrm{N}(u'x+v'y)}{\mathrm{N}(M')}.$$

Si módulos son del mismo género entonces las formas f y g son racionalmente equivalentes (y el recíproco es cierto si el orden es maximal). Por el teorema 6.8, esto ocurre si y sólo si ambas formas representan racionalmente a un mismo número, es decir, si y sólo si existen números racionales no nulos r, s, r', s' tales que $\mathrm{N}(ur+vs)/\mathrm{N}(M) = \mathrm{N}(u'r'+v's')/\mathrm{N}(M')$ o, en otros términos, si y sólo si existen elementos no nulos ξ y ξ' en K tales que $\mathrm{N}(\xi)/\mathrm{N}(M) = \mathrm{N}(\xi')/\mathrm{N}(M')$ o, equivalentemente $\mathrm{N}(M) = \mathrm{N}(M')N(\xi/\xi')$. Entonces $\gamma = \xi/\xi'$ cumple el teorema. ∎

Ejercicio: Probar que, en un orden cuadrático arbitrario, dos ideales con la misma norma son del mismo género (tener en cuenta que dos ideales primos con la misma norma son conjugados, y que dos ideales conjugados son del mismo género).

7.2 El número de géneros

En esta sección presentamos una prueba de la ley de reciprocidad cuadrática basada en el cómputo del número de géneros. De acuerdo con el teorema 7.12 es suficiente probar que en un orden maximal el número de géneros g es a lo sumo 2^{m-1}, donde m es el número de primos que dividen al discriminante.

Para ello nos basaremos en la siguiente observación trivial: Si C es una clase de similitud estricta (no necesariamente de un orden maximal), entonces C^2 pertenece al género principal, pues para cualquier carácter se cumple $\chi_p(C^2) = \chi_p(C)^2 = 1$. Así, si llamamos H al grupo de clases, H^2 al subgrupo de los cuadrados y G_0 al género principal, tenemos que $g = |H : G_0| \le |H : C^2|$, luego basta probar que este último índice es a lo sumo 2^{m-1}.

En realidad el número de géneros es exactamente igual a 2^{m-1}, y este hecho tiene interés teórico por sí mismo. Para probarlo necesitamos probar a su vez que el género principal coincide con el grupo de los cuadrados. Esto se conoce como

teorema de duplicación de Gauss. Demostramos primero un resultado técnico que podemos evitar si nos restringimos a órdenes maximales (el único caso necesario para determinar el número de géneros y probar la ley de reciprocidad).

Teorema 7.15 *Sea K un cuerpo cuadrático y m un número natural. Si existe un $\gamma \in K$ no nulo cuya norma es positiva y se expresa como cociente de enteros primos con m, entonces γ puede escogerse de la forma $\gamma = \alpha/\beta$, donde α y β son enteros de norma positiva prima con m.*

DEMOSTRACIÓN: Sea $\gamma = \alpha/\beta$, donde α y β son enteros en K. Sean $p_1, \dots, p_r$ los primos que dividen a m y que en K se descomponen como $p_i = \mathfrak{p}_i\mathfrak{q}_i$, donde $\mathfrak{p}_i \neq \mathfrak{q}_i$. Sean a_i y a_i' los exponentes de $\mathfrak{p}_i$ y $\mathfrak{q}_i$ en α. Sean b_i y b_i' los exponentes en β. Por hipótesis ha de ser $a_i + a_i' = b_i + b_i'$. Llamemos $c_i = a_i - b_i = b_i' - a_i'$. Para cada i, sea $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Por el teorema chino del resto existe un entero $\zeta \in K$ tal que

$$\begin{aligned} \zeta &\equiv \pi_i^{c_i} \ (\text{mód } \mathfrak{p}_i^{c_i+1}), \\ \zeta &\equiv 1 \ (\text{mód } \mathfrak{q}_i^{c_i+1}). \end{aligned}$$

De este modo, $\mathfrak{p}_i$ divide a ζ con exponente c_i, mientras que $\mathfrak{q}_i$ no divide a ζ. Sea ζ' el conjugado de ζ. Claramente ζ y ζ' tienen la misma norma, luego $\gamma^* = (\zeta'\alpha)/(\zeta\beta)$ tiene la misma norma que γ. Ahora, el exponente de $\mathfrak{p}_i$ tanto en $\zeta'\alpha$ como en $\zeta\beta$ es a_i, y el exponente de $\mathfrak{q}_i$ en $\zeta'\alpha$ y en $\zeta\beta$ es b_i'.

Así pues, todo divisor primo de m divide a $\zeta'\alpha$ y en $\zeta\beta$ con la misma multiplicidad (para otros divisores distintos de los que hemos tratado —véase la tabla 2.1— se sigue inmediatamente de la hipótesis). Podemos aplicar el teorema 2.18 para concluir que $\gamma^* = \alpha^*/\beta^*$, donde ningún primo que divida a m divide a β^* (luego tampoco a α^*). Por consiguiente, α^* y β^* tienen norma prima con m. Si no es positiva los multiplicamos por α^*. ∎

Teorema 7.16 (Teorema de duplicación) *El género principal de un orden cuadrático $\mathcal{O}_m$ está formado por los cuadrados del grupo de clases.*

DEMOSTRACIÓN: Consideremos una clase $[\mathfrak{a}]$ del género principal. Por el teorema [ITAl 13.27] podemos suponer que $\mathfrak{a}$ es un ideal de norma prima con m. El teorema 7.14 nos da que $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\gamma)$ para un cierto γ con $\mathrm{N}(\gamma) > 0$. Por el teorema anterior podemos tomar $\gamma = \alpha/\beta$, donde $\alpha, \beta \in \mathcal{O}$ tienen norma positiva prima con m. Entonces $[\mathfrak{a}] = [\beta\mathfrak{a}]$ y $\mathrm{N}(\beta\mathfrak{a}) = \mathrm{N}(\alpha)$. Esto significa que podemos suponer que $\gamma \in \mathcal{O}$. Ahora veremos que podemos tomarlo en $\mathcal{O}_m$. En efecto, existen u y v enteros en K tales que $u\gamma + vm = 1$. Así $u\gamma \in 1 + (m) \subset \mathcal{O}_m$ y sigue siendo primo con m. Lo mismo vale para $(u\gamma)^2$. Además $\mathrm{N}(u^2\gamma\mathfrak{a}) = \mathrm{N}\big((u\gamma)^2\big)$ y tanto $u^2\gamma$ como $(u\gamma)^2$ tienen norma positiva. Por consiguiente $[\mathfrak{a}] = [u^2\gamma\mathfrak{a}]$ y podemos sustituir γ por $(u\gamma)^2$. Descompongamos en ideales primos de $\mathcal{O}_m$:

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i}\,\mathfrak{q}_i^{b_i} \prod_j \mathfrak{r}_j^{c_j}, \qquad \gamma = \prod_i \mathfrak{p}_i^{u_i}\,\mathfrak{q}_i^{v_i} \prod_j \mathfrak{r}_j^{w_j},$$

donde hemos distinguido entre los primos $\mathfrak{p}_i$ de norma p_i tales que $p_i = \mathfrak{p}_i\mathfrak{q}_i$ con $\mathfrak{p}_i \neq \mathfrak{q}_i$ y los primos restantes $\mathfrak{r}_j$ de norma $r_j^{t_j}$ $(t_j = 1, 2)$ tales que $r_j = \mathfrak{r}_j^2$ o bien $r_j = \mathfrak{r}_j$.

Al igualar las normas y teniendo en cuenta que la factorización es única, resulta que $a_i + b_i = u_i + v_i$ y $c_j = w_j$. Tomando clases estrictas tenemos

$$[\mathfrak{a}] = [\gamma^{-1}\mathfrak{a}] = \prod_i [\mathfrak{p}_i]^{a_i}[\mathfrak{q}_i]^{b_i}[\mathfrak{p}_i]^{-u_i}[\mathfrak{q}_i]^{-v_i},$$

pero $[1] = [p_i] = [\mathfrak{p}_i][\mathfrak{q}_i]$, luego $[\mathfrak{q}_i] = [\mathfrak{p}_i]^{-1}$ y así

$$[\mathfrak{a}] = \prod_i [\mathfrak{p}_i]^{a_i-u_i+v_i-b_i} = \prod_i [\mathfrak{p}_i]^{2(a_i-u_i)} = \Big[\prod_i \mathfrak{p}_i^{a_i-u_i}\Big]^2. \qquad \blacksquare$$

El grupo de clases de un orden cuadrático se descompone en producto de grupos cíclicos de órdenes potencias de primos (los llamados divisores elementales). Digamos que

$$H = \langle c_1\rangle \times \cdots \times \langle c_r\rangle \times \langle d_1\rangle \times \cdots \times \langle d_s\rangle\,, \tag{7.1}$$

donde $c_1, \ldots, c_r$ tienen orden 2^{t_i} y $d_1, \ldots, d_s$ tienen orden impar. Por consiguiente el género principal es

$$G_0 = \langle c_1^2\rangle \times \cdots \times \langle c_r^2\rangle \times \langle d_1^2\rangle \times \cdots \times \langle d_2^2\rangle\,.$$

Pero $d_i = \big(d_i^2\big)^{(t-1)/2}$, donde t es el orden de d_i, luego $\langle d_i^2\rangle = \langle d_i\rangle$, y así

$$G_0 = \langle c_1^2\rangle \times \cdots \times \langle c_r^2\rangle \times \langle d_1\rangle \times \cdots \times \langle d_s\rangle\,.$$

Esto nos da la siguiente expresión para el grupo de géneros:

$$G = H/G_0 = \big(\langle c_1\rangle\,/\,\langle c_1^2\rangle\big) \times \cdots \times \big(\langle c_r\rangle\,/\,\langle c_r^2\rangle\big)\,.$$

Resulta, pues, que el número de géneros es $g = 2^n$, donde n es el número de divisores elementales pares de H. Puesto que cada clase $c_i^{2^{t_i-1}}$ tiene orden 2, el grupo

$$A = \Big\langle c_1^{2^{t_1-1}}\Big\rangle \times \cdots \times \Big\langle c_r^{2^{t_r-1}}\Big\rangle \le H$$

es isomorfo al grupo de géneros.

Pero por otro lado $A = \{C \in H \mid C^2 = 1\}$ (teniendo en cuenta (7.1), un elemento de H tiene orden 2 si y sólo si todos sus factores tienen orden 2, si y sólo si está en A).

Definición 7.17 Una clase C del grupo de clases estrictas H es *ambigua* si cumple $C^2 = 1$.

Hemos probado que el grupo de géneros es isomorfo al grupo de clases ambiguas. Gauss demostró la ley de reciprocidad cuadrática contando el número de clases ambiguas, que es lo que vamos a hacer a continuación. En lo sucesivo consideraremos únicamente clases de similitud estricta en un orden cuadrático maximal (trabajar en el caso general no aprovecharía para nada).

Si C es una clase de H, llamaremos $\overline{C}$ a la clase conjugada de C, es decir, la formada por los módulos conjugados de los módulos de C. Si $\mathfrak{a}$ es un ideal y $\bar{\mathfrak{a}}$ es su conjugado, entonces $\mathfrak{a}\bar{\mathfrak{a}} = \big(\mathrm{N}(\mathfrak{a})\big)$, luego para toda clase C se cumple que $C\overline{C} = 1$. Por lo tanto C es una clase ambigua si y sólo si $C = \overline{C}$.

Un ideal $\mathfrak{a}$ es *ambiguo* si $\mathfrak{a} = \bar{\mathfrak{a}}$ y no es divisible entre enteros racionales no unitarios.

Consideremos un ideal ambiguo $\mathfrak{a} \neq 1$ y descompongámoslo en factores primos. Si $\mathfrak{p}$ es uno de los primos de $\mathfrak{a}$, según probamos en el capítulo II (véase la tabla 2.1) hay tres posibilidades: o bien $\mathfrak{p} = p$ es un primo racional, o bien $\mathrm{N}(\mathfrak{p}) = p = \mathfrak{p}\mathfrak{q}$, con $\mathfrak{q} \neq \mathfrak{p}$ (y entonces $\mathfrak{q} = \bar{\mathfrak{p}}$, por el teorema 2.39), o bien $\mathrm{N}(\mathfrak{p}) = p = \mathfrak{p}^2$.

Descartamos la primera posibilidad por definición de ideal ambiguo. El segundo caso tampoco puede darse, pues como $\mathfrak{p} \mid \mathfrak{a}$, también $\bar{\mathfrak{p}} \mid \bar{\mathfrak{a}} = \mathfrak{a}$, luego $p = \mathfrak{p}\bar{\mathfrak{p}} \mid \mathfrak{a}$, en contra de la definición de ideal ambiguo.

Esto prueba que los únicos factores primos posibles de los ideales ambiguos son los primos $\mathfrak{p}$ tales que $\mathrm{N}(\mathfrak{p}) = \mathfrak{p}^2$, y éstos son exactamente los que dividen al discriminante D del orden que estamos considerando. Más aún, la multiplicidad de $\mathfrak{p}$ en $\mathfrak{a}$ tiene que ser 1, o de lo contrario $\mathrm{N}(\mathfrak{p}) = \mathfrak{p}^2$ dividiría a $\mathfrak{a}$.

Recíprocamente, si $\mathfrak{a}$ es un ideal formado por productos de divisores primos de D con multiplicidad 1, es claro que $\mathfrak{a}$ es un ideal ambiguo. Si llamamos m al número de divisores primos de D, tenemos que el número de ideales ambiguos es 2^m (incluyendo al ideal 1, que no tiene factores primos).

Si demostramos que cada clase ambigua contiene exactamente dos ideales ambiguos habremos demostrado que hay exactamente 2^{m-1} clases ambiguas, luego también 2^{m-1} géneros, tal y como queremos demostrar.

La clave de la prueba es un sencillo resultado debido a Gauss y a Kummer, que Hilbert generalizó hasta lo que ahora se conoce como el teorema 90 de Hilbert.

Teorema 7.18 *Sea $K = \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático y $\mathcal{O}$ su orden maximal. Si $\alpha \in K$ cumple que $\mathrm{N}(\alpha) = 1$, entonces existe un $\rho \in \mathcal{O}$ tal que $\alpha = \rho/\bar{\rho}$. Además ρ es único salvo múltiplos por números racionales.*

Demostración: Si $\alpha = -1$ basta tomar $\rho = \sqrt{d}$. En otro caso se cumple que $\alpha = (1+\alpha)/(1+\bar{\alpha})$. Multiplicando por un entero racional podemos exigir que el numerador esté en $\mathcal{O}$, y se cumple lo pedido.

Si $\rho/\bar{\rho} = \sigma/\bar{\sigma}$ entonces $\rho\bar{\sigma} = \bar{\rho}\sigma = r \in \mathbb{Q}$, pues r es invariante por conjugación. Por lo tanto

$$\rho = \frac{r}{\bar{\sigma}} = \frac{r\sigma}{\sigma\bar{\sigma}} = \frac{r}{\mathrm{N}(\sigma)}\sigma = s\sigma,$$

con $s \in \mathbb{Q}$. ∎

Teorema 7.19 *Cada clase ambigua de un orden cuadrático maximal $\mathcal{O}$ contiene exactamente dos ideales ambiguos. Por lo tanto $\mathcal{O}$ tiene exactamente 2^{m-1} clases ambiguas, luego también 2^{m-1} géneros, donde m es el número de divisores primos del discriminante de $\mathcal{O}$.*

DEMOSTRACIÓN: Veamos en primer lugar que toda clase ambigua contiene al menos un ideal ambiguo. Toda clase ambigua contiene un ideal $\mathfrak{a}$. Que la clase sea ambigua significa que $[\mathfrak{a}] = [\bar{\mathfrak{a}}]$, es decir, que $\bar{\mathfrak{a}} = \alpha\mathfrak{a}$ para un cierto número α de norma positiva. Como $\mathfrak{a}$ y $\bar{\mathfrak{a}}$ tienen la misma norma ha de ser $\mathrm{N}(\alpha) = 1$, luego por el teorema anterior $\bar{\mathfrak{a}} = (\rho/\bar{\rho})\mathfrak{a}$, con $\rho \in \mathcal{O}$. Por lo tanto $\rho\mathfrak{a} = \overline{\rho\mathfrak{a}}$.

Si $\mathrm{N}(\rho) < 0$ hacemos $\sqrt{d}\rho\mathfrak{a} = -\overline{\sqrt{d}\rho\mathfrak{a}} = \overline{\sqrt{d}\rho\mathfrak{a}}$ y $\mathrm{N}(\sqrt{d}\rho) > 0$. De este modo tenemos un ideal $\mathfrak{b}$ estrictamente similar a $\mathfrak{a}$ y tal que $\mathfrak{b} = \bar{\mathfrak{b}}$. Si $\mathfrak{b}$ es divisible entre enteros racionales hacemos $\mathfrak{b} = m\mathfrak{c}$, donde $\mathfrak{c}$ ya no es divisible entre enteros racionales. Entonces $\mathfrak{c}$ es estrictamente similar a $\mathfrak{a}$ y es claro que se trata de un ideal ambiguo.

Ahora basta probar que la clase principal contiene exactamente dos ideales ambiguos, pues si (1) y (α) son los únicos ideales estrictamente principales ambiguos, toda clase contiene al menos dos ideales ambiguos: el que ya hemos probado que existe, digamos $\mathfrak{a}$ y el ideal $\alpha\mathfrak{a}$. Por otro lado, si una clase contuviera tres ideales ambiguos, digamos $\mathfrak{a}$, $\beta\mathfrak{a}$ y $\gamma\mathfrak{a}$, con $\mathrm{N}(\beta)$, $\mathrm{N}(\gamma) > 0$, entonces los ideales (1), (β), (γ) estarían en la clase principal y serían ambiguos.

Supongamos que (α) es un ideal ambiguo con $\mathrm{N}(\alpha) > 0$ y veamos qué posibilidades hay. Tenemos que $(\alpha) = (\bar{\alpha})$, luego $\alpha/\bar{\alpha} = \epsilon$ es una unidad de $\mathcal{O}$ de norma $+1$.

Si $d \neq -1, -3$, $d < 0$, entonces $\epsilon = \pm 1$, y si $\alpha = a + b\sqrt{d}$ (con a, b enteros o semienteros) la condición $\alpha = \pm\bar{\alpha}$ nos da $\alpha = a$ o bien $\alpha = b\sqrt{d}$ (con lo que a y b han de ser enteros). Como además (α) no ha de ser divisible entre enteros racionales, las únicas posibilidades son (1) y $\left(\sqrt{d}\right)$.

Si $d = -1, -3$ no es necesario hacer cálculos: en ambos casos el número de clases es 1 y $m = 1$, luego el número de ideales ambiguos es 2 y, efectivamente, hay dos ideales en la clase principal. Con esto tenemos probado el teorema para cuerpos imaginarios.

Supongamos ahora que $d > 0$ y que la unidad fundamental tiene norma negativa. Como $\mathrm{N}(\epsilon) > 0$, necesariamente, $\pm\epsilon$ ha de ser una potencia par de la unidad fundamental, luego $\epsilon = \pm\eta^2$ para una cierta unidad η. Tenemos que $\alpha = \pm\eta^2$. Multiplicando por $\bar{\eta}$ queda $\alpha\bar{\eta} = \pm\eta\bar{\alpha}$.

Sea $\alpha\bar{\eta} = a + b\sqrt{d}$. Este número tiene la propiedad de que su conjugado es él mismo o su simétrico. Esto lleva a que $\alpha\bar{\eta} = a$ o bien $\alpha\bar{\eta} = b\sqrt{d}$, luego (α) ha de ser (a) o $\left(b\sqrt{d}\right)$ y, como no ha de ser divisible entre enteros, sólo hay dos posibilidades: (1) y $\left(\sqrt{d}\right)$.

Nos queda el caso en que $d > 0$ y la unidad fundamental η tiene norma positiva. Por el teorema anterior, $\eta = \rho/\bar{\rho}$ para un cierto entero ρ. Podemos suponer que $\mathrm{N}(\rho) > 0$, pues en caso contrario cambiamos ρ por $\sqrt{d}\rho$, y η por $-\eta$ (que es también una unidad fundamental). También podemos suponer que ρ no es divisible entre enteros racionales.

Notemos que ρ no es una unidad, o de lo contrario $\eta = \rho^2$, lo cual es imposible dado que η es una unidad fundamental. Por lo tanto los ideales (1) y (ρ) son distintos y claramente son ambiguos. Vamos a probar que no hay ninguno más.

Si (α) es un ideal ambiguo (con $\mathrm{N}(\alpha) > 0$) tenemos que $\alpha = \epsilon\bar{\alpha}$ para una unidad ϵ, que será de la forma $\epsilon = \pm\eta^t = \pm\rho^t/\bar{\rho}^t$. Entonces $\alpha\bar{\rho}^t = \pm\bar{\alpha}\rho^t$. Expresando este número como $a + b\sqrt{d}$ (con a, b enteros o semienteros), esta ecuación conduce a que $\alpha\bar{\rho}^t = a$ o bien $\alpha\bar{\rho}^t = b\sqrt{d}$ (con a, b enteros). Teniendo en cuenta los signos de las normas, el segundo caso es imposible, luego $\alpha\bar{\rho}^t = a$.

Digamos que $t = 2k + u$, donde $u = 0, 1$. Se cumple que $\bar{\rho}^2 = \mathrm{N}(\rho)/\eta$, luego podemos escribir $\alpha\bar{\rho}^u/\eta^k = a/\mathrm{N}(\rho)^k$. El primer miembro es entero y el segundo es racional, luego $\alpha\bar{\rho}^u/\eta^k = a' \in \mathbb{Z}$.

Si $u = 0$ queda $(\alpha) = (a') = (1)$, puesto que (α) no es divisible entre enteros racionales. Supongamos finalmente que $u = 1$, de modo que $(\alpha) = (a'/\bar{\rho})$.

Tenemos que $\rho \mid a'$. El hecho de que (ρ) sea ambiguo implica que los factores primos de (ρ) son todos distintos dos a dos y, si $\mathfrak{p}$ es uno de ellos, entonces $\mathfrak{p}^2 = p$ para un cierto primo p tal que $p \mid \mathrm{N}(\rho) \mid \mathrm{N}(a')$, luego $p \mid a'$ y así concluimos que $\mathrm{N}(\rho) \mid a'$.

Consecuentemente $a'/\bar{\rho} = a'\rho/\mathrm{N}(\rho) = a''\rho$, para un cierto entero racional a'', y nos queda $(\alpha) = (a''\rho) = (\rho)$. ∎

Con esto queda demostrada la ley de reciprocidad cuadrática. Notemos que, sin el teorema 7.16, el teorema anterior prueba que $|H : H^2| = 2^{m-1}$, lo cual es suficiente para probar la ley de reciprocidad. Todavía no hemos probado que el número de géneros es exactamente la mitad del número de géneros posibles en órdenes no maximales. Esto lo veremos más tarde. Terminamos la sección con algunas consecuencias inmediatas del teorema anterior:

- Hay cuerpos cuadráticos (tanto reales como imaginarios) con un número de clases arbitrariamente grande, pues si llamamos n al número de clases en cada género, tenemos la relación $h' = gn = 2^{m-1}n$, y basta tomar determinantes divisibles entre muchos primos.
- El número de clases estrictas h' es impar si y sólo si el discriminante D es divisible por un único primo (pues el número de géneros es el número de divisores elementales pares del grupo de clases).
- En particular, una condición necesaria para que un cuerpo tenga factorización única ($h = 1$) es que el discriminante sea divisible por un solo primo en el caso de los cuerpos imaginarios o cuerpos reales con unidades de norma negativa, y que el discriminante sea divisible por a lo sumo dos primos en el caso de cuerpos reales sin unidades de norma negativa.

7.3 El carácter de un cuerpo cuadrático

Al final de la sección 4.3 hemos introducido el concepto de carácter de un cuerpo cuadrático K, que en realidad habíamos presentado ya en [ITAl 9.14]. Aquí presentamos una construcción alternativa a partir del símbolo de Hilbert. Concretamente, definimos $\chi_K : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ mediante

$$\chi_K(a) = \begin{cases} \prod_{p\mid\Delta_K} (a, \Delta_K)_p & \text{si } (a, \Delta_K) = 1, \\ 0 & \text{si } (a, \Delta_K) \neq 1. \end{cases}$$

El teorema siguiente prueba que esta definición es equivalente a la dada en [ITAl]. Notemos que la ley de reciprocidad cuadrática interviene a través de la fórmula del producto:

Teorema 7.20 *Sea K un cuerpo cuadrático y q un primo racional. Entonces*

$$\chi_K(q) = \begin{cases} 0 & \text{si } q \text{ se ramifica en } K, \\ 1 & \text{si } q \text{ se escinde en } K, \\ -1 & \text{si } q \text{ se conserva en } K. \end{cases}$$

Demostración: El caso de los primos que se ramifican es claro. Supongamos que q se escinde. Entonces existe un ideal $\mathfrak{q}$ tal que $\mathrm{N}(\mathfrak{q}) = q$.

$$\chi_K(q) = \prod_{p|\Delta_K} (q, \Delta_K)_p = \prod_{p|\Delta_K} (\mathrm{N}(\mathfrak{q}), \Delta_K)_p = \prod_{p|\Delta_K} \chi_p(\mathfrak{q}) = 1.$$

Recíprocamente, supongamos que $\chi_K(q) = \prod_{p|\Delta_K} (q, \Delta_K)_p = 1$. La fórmula del producto 6.30 nos da que

$$\prod_p (q, \Delta_K)_p = 1, \tag{7.2}$$

cuando p recorre todos los primos incluido $p = \infty$. Si $p \nmid \Delta_K$, $p \neq q$ se cumple que $(q, \Delta_K)_p = 1$, pues si p es impar es inmediato y si $p = 2$ entonces tenemos que $\Delta_K \equiv 1 \pmod 4$, con lo que también se cumple. Además $(q, \Delta_K)_\infty = 1$, ya que $q > 0$. Esto implica que si eliminamos el factor $(q, \Delta_K)_q$ en (7.2) el producto sigue dando 1, luego $(q, \Delta_K)_q = 1$.

Si q es impar $(q, \Delta_K)_q = (\Delta_K/q) = 1$, luego q se escinde en K. Si $q = 2$ la condición $(2, \Delta_K)_2 = 1$ equivale a que $D \equiv \pm 1 \pmod 8$, y puesto que entonces Δ_K es impar, $\Delta_K \equiv 1 \pmod 4$, luego ha de ser de hecho $\Delta_K \equiv 1 \pmod 8$, y esto implica que 2 se escinde. ∎

Ahora las propiedades de los caracteres de los cuerpos cuadráticos (incluyendo el hecho de que son caracteres modulares) se siguen de las propiedades del símbolo de Hilbert:

Teorema 7.21 *Sea K un cuerpo cuadrático de discriminante Δ y sean m y n enteros racionales.*

1. $\chi_K(mn) = \chi_K(m)\chi_K(n)$.
2. *Si* $m \equiv n \pmod \Delta$, *entonces* $\chi_K(m) = \chi_K(n)$.
3. χ_K *toma los tres valores* $-1, 0, 1$.
4. $\chi_K(-1) = \Delta/|\Delta|$.

Demostración: 1) Es inmediato a partir de la definición de χ_K y de las propiedades del símbolo de Hilbert.

2) Si m y n no son primos con Δ, entonces $\chi_K(m) = \chi_K(n) = 0$. En caso contrario es claro que

$$\chi_K(m) = \prod_{p|\Delta} \chi_p^*(m),$$

y las funciones $\chi_p^*(m)$ dependen sólo del resto de m módulo Δ.

3) Obviamente χ_K toma el valor 0 y $\chi_K(1) = \chi_K(1^2) = \chi_K(1)^2 = 1$. Hay que probar que también toma el valor -1.

El discriminante Δ sólo es potencia de 2 cuando $\Delta = \pm 8$, $\Delta = -4$. En estos casos podemos encontrar explícitamente un primo que se conserve en el cuerpo en cuestión. Supongamos, pues que Δ es divisible entre un primo impar q.

Sea $\Delta = qm$, donde $(q, m) = 1$, puesto que salvo potencias de 2 se cumple que Δ es libre de cuadrados. Por el teorema chino del resto existe un entero r tal que r es un resto no cuadrático módulo q y $r \equiv 1$ (mód $8m$). Entonces, si $p \mid \Delta$, $p \neq q$ tenemos que $(r, \Delta)_p = (r, p)_p = (r/p) = 1$ si p es impar, y también si $p = 2$, usando que $r \equiv 1$ (mód 8). Por consiguiente

$$\chi_K(r) = (r, \Delta)_q = (r/q) = -1.$$

4) Sea $\Delta = 2^i m$, donde m es impar libre de cuadrados. Para cada primo $p \mid m$ tenemos que $(-1, \Delta)_p = (-1, p)_p = (-1/p) \equiv p$ (mód 4).

Por otra parte $(-1, \Delta)_2 = (-1, 2)_2^i\, (-1, m)_2 = (-1, m)_2 \equiv m$ (mód 4).

Al multiplicar todas las congruencias queda $\chi_K(-1) \equiv m\,|m|$ (mód 4). Notemos que si Δ es impar hemos incluido un factor de más, pero no importa, pues en tal caso $(-1, \Delta)_2 \equiv m \equiv 1$ (mód 4).

Claramente entonces $\chi_K(-1) = m/|m| = \Delta/|\Delta|$. ∎

Definición 7.22 Sea K un cuerpo cuadrático de discriminante Δ. Sea U_Δ el grupo de las unidades del anillo de restos módulo $|\Delta|$, esto es, el formado por las clases $[m]$ tales que $(m, \Delta) = 1$. El teorema anterior permite considerar a χ_K como un carácter $\chi_K : U_\Delta \longrightarrow \{\pm 1\}$, de U_δ, es decir, como un homomorfismo de grupos, que, de hecho, es suprayectivo.

Llamaremos *clases de escisión* de K a las clases cuya imagen por χ_K es 1.

Las clases de escisión forman el núcleo de χ_K, luego son un subgrupo de U_Δ que contiene exactamente a la mitad de las clases. Teniendo en cuenta que $\chi_K^2 = 1$ es evidente que las clases que son cuadrados son de escisión.

El apartado 4) del teorema anterior nos dice que si $\Delta > 0$ entonces $[m]$ es una clase de escisión si y sólo si lo es $[-m]$, mientras que si $\Delta < 0$ entonces $[m]$ es una clase de escisión si y sólo si $[-m]$ no lo es.

Estas propiedades permiten determinar fácilmente las clases de escisión. Según el teorema 7.20, un primo $p \nmid \Delta$ se escinde en K si y sólo si $[p]$ es una clase de escisión (y se conserva en caso contrario). Notemos que el teorema de Dirichlet asegura que todas las clases de U_Δ contienen infinitos números primos, si bien hemos podido definir el concepto de clase de escisión sin necesidad de este hecho.

Todas estas propiedades de la factorización de los primos en cuerpos cuadráticos eran ya conocidas por Euler, aunque fue Gauss el primero en demostrarlas gracias a la ley de reciprocidad cuadrática.

Ahora podemos probar calcular el número de géneros de los órdenes no maximales. [ITAl 14.19]:

Teorema 7.23 *Sea $\mathcal{O}$ un orden cuadrático. Entonces una combinación de caracteres (no triviales) se corresponde con un género de $\mathcal{O}$ si y sólo si el número de caracteres fundamentales negativos es par y, en caso de que haya tres caracteres módulo 2, el número de caracteres negativos módulo 2 es par.*

Demostración: Sea K el cuerpo cuadrático al que pertenece $\mathcal{O}$. Puesto que los valores de $\chi_p^*(x)$ dependen sólo del resto de x módulo p (o módulo 8), el teorema chino del resto nos da un entero m primo con el discriminante Δ de $\mathcal{O}$ tal que $\chi_p^*(m)$ toma cualquier juego de valores prefijado, y m está determinado módulo Δ (aquí se usa la restricción sobre los caracteres módulo 2). Si probamos que $\mathcal{O}$ tiene un ideal de norma m, evidentemente su género tendrá la combinación de caracteres prefijada.

No es fácil probar la existencia de tal ideal, así que simplificaremos el problema haciendo uso del teorema de Dirichlet sobre primos en progresiones aritméticas. La sucesión $m+k\Delta$ contiene un primo q, de modo que podemos razonar con q en lugar de m. Ahora basta observar que

$$\chi_K(q) = \prod_{p|\Delta_K} \chi_p^*(q) = 1,$$

por hipótesis, y esto significa que q se escinde en K, luego existe un primo $\mathfrak{q}$ de norma q, y como $(q, \Delta) = 1$, la correspondencia entre los ideales de $\mathcal{O}$ y los de K implica que $\mathcal{O}$ también tiene un primo de norma q ∎

7.4 Representaciones por formas cuadráticas

Hemos iniciado el capítulo explicando que nuestra intención al estudiar los géneros era buscar condiciones suficientes para que un entero esté representado por una forma cuadrática, pero pronto nos hemos desviado hacia consideraciones teóricas sobre los géneros. Ahora estudiaremos la parte práctica. Como punto de partida, consideremos el teorema [ITAl 12.29], según el cual una forma representa un número natural m si y sólo si la clase inversa de su clase de ideales asociada contiene un ideal de norma m. Usando la factorización única es fácil determinar si existen o no ideales con una norma dada. El problema es decidir a qué clase pertenecen si existen. Si eliminamos esa parte de la conclusión obtenemos este enunciado más débil: si $\mathcal{O}$ es un orden cuadrático de discriminante D, un número natural m está representado por alguna forma cuadrática de discriminante D si y sólo si $\mathcal{O}$ tiene ideales de norma m. Ahora reformulamos la condición sobre la existencia de ideales.

Teorema 7.24 *Sea K un cuerpo cuadrático con discriminante Δ y sean m, k números naturales primos entre sí. Las afirmaciones siguientes son equivalentes:*

1. *k está representado por una forma cuadrática de discriminante $m^2\Delta$.*
2. *Los primos p que dividen a k y tales que $\chi_K(p) = -1$ tienen exponente par.*
3. *$(k, \Delta)_p = 1$ para todo primo $p \nmid \Delta$.*

DEMOSTRACIÓN: Sabemos que una forma f de discriminante $m^2\Delta$ representa a k si y sólo si el orden $\mathcal{O}_m$ tiene ideales de norma k. Como k es primo con m esto equivale a que el orden maximal de K tenga ideales de norma k. Todo ideal de K se descompone en producto de ideales primos que tendrán norma p (para los primos p tales que $\chi_K(p) \neq -1$) o p^2 (cuando $\chi_K(p) = -1$).

Es claro entonces que K tiene un ideal de norma k si y sólo si los primos que cumplen $\chi_K(p) = -1$ aparecen en k con exponente par. Esto nos da primera equivalencia.

Respecto a la segunda, notemos que si $p \nmid \Delta$ y $k = p^r n$ (quizá con $r = 0$), entonces para $p \neq 2$ se cumple

$$(k, \Delta)_p = (n, \Delta)_p\,(p^r, \Delta)_p = (\Delta/p)^r = \chi_K(p)^r.$$

Si $p = 2$, entonces Δ es impar, luego $\Delta \equiv 1 \pmod 4$.

$$(k, \Delta)_2 = (n, \Delta)_2\,(2^r, \Delta)_2 = (2, \Delta)_2^r = \chi_K(2)^r.$$

Así pues, para todo primo $p \nmid \Delta$ se cumple $(k, \Delta)_p = \chi_K(p)^r$, con lo que la tercera afirmación equivale a las anteriores. ∎

Notemos que la afirmación 3) impone sólo un número finito de restricciones, ya que si p es un primo que no divida a Δ ni a k, entonces $(k, \Delta)_p = 1$.

También es interesante notar que k está representado por una forma de discriminante $m^2\Delta$ si y sólo si lo está su parte libre de cuadrados, si y sólo si lo están los primos que dividen a ésta. Además, si p es primo y $p \nmid m$, entonces la representabilidad de p por una forma del determinante considerado sólo depende de su resto módulo Δ.

Todo esto es especialmente útil en los cuerpos cuadráticos con una sola clase de similitud. Si todas las formas cuadráticas son equivalentes, entonces todas representan a los mismos números, luego un número es representado por una forma cuadrática (cualquiera) de discriminante D si y sólo si es representado por una forma cuadrática particular con dicho discriminante, y las condiciones que proporciona el teorema son condiciones necesarias y suficientes para que una forma dada represente a un número.

Números de la forma $x^2 + ny^2$ Vamos a aplicar los resultados que conocemos a las formas de tipo $x^2 + ny^2$. Tal y como acabamos de señalar, la situación es más simple cuando el número de clases de formas con dicho discriminante es $h = 1$. Puede probarse que esto sólo sucede para $n = 1, 2, 3, 4, 7$. Veamos en primer lugar estos casos:

$n = 1$ *Un número es de la forma $x^2 + y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 2$ o $p \equiv 1$ (mód 4).*

En efecto, $x^2 + y^2$ es la forma principal de discriminante $\Delta = -4$, que corresponde al orden maximal del cuerpo $\mathbb{Q}(i)$. Como su número de clases es $h = 1$, todas las formas de discriminante -4 representan los mismos números. El grupo U_4 está formado por las clases $\{\pm[1]\}$, y como $\chi_K(1) = 1$, ha de ser $\chi_K(-1) = -1$. Por el teorema anterior, los números representados por la forma son aquellos cuya parte libre de cuadrados no contiene primos congruentes con -1 módulo 4.

$n = 2$ *Un número es de la forma $x^2 + 2y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 2$ o $p \equiv 1, 3$ (mód 8).*

Ahora $\Delta = -8$ y $U_8 = \{[1], [3], [5], [7]\}$. Como [3] es un cuadrado en U_8, tiene que ser $\chi_K(3) = 1$, luego $\chi_K(5) = \chi_K(7) = -1$. Concluimos como en el caso anterior.

$n = 3$ *Un número es de la forma $x^2 + 3y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados es $p = 3$ o $p \equiv 1$ (mód 3).*

El discriminante de $x^2 + 3y^2$ es $D = -2^2 \cdot 3$, luego la forma está asociada al orden $\mathcal{O}_2$ de $K = \mathbb{Q}(\sqrt{-3})$, cuyo discriminante es $\Delta = -3$ y $m = 2$. El grupo de las unidades es $U_3 = \{\pm[1]\}$.

Por el teorema anterior, un número k primo con m, es decir, impar, es de la forma $x^2 + 3y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 3$ o $p \equiv 1$ (mód 3). Vamos a ver que esto vale también si k es par. Claramente, si k es par y es de esta forma, entonces $k = 2^{2r}k'$, donde k' es impar y tiene la misma parte libre de cuadrados que k, luego $k' = x^2 + 3y^2$ y $k = (2^r x)^2 + 3(2^r y)^2$.

Recíprocamente, si $k = x^2 + 3y^2$, como 2 es primo en K, tiene que dividir a los dos conjugados $x \pm y\sqrt{-3}$ con la misma multiplicidad, luego 2 divide a $k = \big(x + y\sqrt{-3}\,\big)\big(x - y\sqrt{-3}\big)$ con multiplicidad par. Por lo tanto, si un primo p divide a la parte libre de cuadrados de k, necesariamente es impar, y tiene que ser la norma de uno de los primos en que se descompone k, luego p es de la forma $x^2 + 3y^2$ y, por el caso en que $k = p$ es impar, es de la forma requerida.

$n = 4$ *Un número es de la forma $k = x^2 + 4y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados es $p = 2$ o $p \equiv 1$ (mód 4), con la condición adicional de que si $p = 2$, su multiplicidad en k sea > 1.*

La forma $x^2 + 4y^2$ tiene discriminante $D = -16$ y está asociada al orden $\mathcal{O}_2$ de $K = \mathbb{Q}(i)$, de discriminante $\Delta = -4$. El teorema anterior nos da que un número impar k es de esta forma si y sólo si su parte libre de cuadrados consta de primos congruentes con 1 módulo 4.

Si $k = x^2 + 4y^2$ es par, necesariamente x es par, luego $k = 4x^2 + 4y^2$, luego, por el caso $n = 1$, tenemos que los primos que dividen a la parte libre de cuadrados de k, que es la misma que la de $k/4$, son de la forma

requerida (y el exponente de 2 en k es mayor que 1). Recíprocamente, si $4 \mid k$ y los primos de la parte libre de cuadrados de k son de la forma requerida, tenemos que $k/4 = x^2 + y^2$, luego $k = (2x)^2 + 4y^2$.

$n = 7$ *Un número es de la forma $k = x^2 + 7y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 2, 7$ o $p \equiv 1, 2, 4$ (mód 7), con la condición adicional de que si $p = 2$, su multiplicidad en k sea > 1.*

La forma x^2+7y^2 tiene discriminante $D = -28$ y está asociada al orden $\mathcal{O}_2$ de $K = \mathbb{Q}(\sqrt{-7})$ con $\Delta = -7$ y $m = 2$. Ahora $U_7 = \{[1], [2], [3], [4], [5], [6]\}$, y los cuadrados son $1, 2, 4$, luego $\chi_K(3) = \chi_K(5) = \chi_K(6) = -1$. Por el teorema anterior, un número impar es de la forma $x^2 + 7y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados son de la forma requerida. Supongamos ahora que k es par y que los primos que dividen a su parte libre de cuadrados son de la forma indicada. Si entre ellos no está el 2, por el caso impar tenemos que la parte libre de cuadrados es de la forma $x^2 + 7y^2$ y k también. Si 2 divide a la parte libre de cuadrados, entonces $k = 8k'$, donde k' tiene parte libre de cuadrados impar. Por el caso impar k' es la norma de un elemento de $\mathbb{Z}\big[\sqrt{-3}\,\big]$ y $8 = \mathrm{N}(1 + \sqrt{-7})$ también, luego k también y, por consiguiente, tiene la forma requerida.

Recíprocamente, si $k = x^2 + 7y^2$ es par, entonces x e y son ambos pares o ambos impares. Tomando restos módulo 4 concluimos en ambos casos que $4 \mid k$. ∎

Muy diferente es el caso de la forma $x^2 + 5y^2$. Se trata de la forma principal de discriminante -20, asociada a $K = \mathbb{Q}(\sqrt{-5})$, pero el número de clases de este cuerpo es 2. Esto significa que hay otra forma no equivalente con el mismo discriminante. Es fácil ver que se trata de $2x^2 + 2xy + 3y^2$.

Así pues, las condiciones del teorema anterior son necesarias y suficientes para que un número k esté representado por una de las dos formas,

$$f(x, y) = x^2 + 5y^2 \quad \text{o} \quad g(x, y) = 2x^2 + 2xy + 3y^2.$$

Más aún, ningún número puede estar representado a la vez por las dos formas, o de lo contrario ambas serían del mismo género, pero como -20 es divisible entre dos primos, K tiene dos géneros y las dos clases son de géneros diferentes.

Por ejemplo, $g(1, 0) = 2$ y $g(0, 1) = 3$, mientras que $f(1, 1) = 6$. Vemos así que f representa a un número libre de cuadrados pero no representa a ninguno de los primos que lo componen (mientras que en los ejemplos anteriores, f representaba a un número si y sólo si representaba a todos los primos de su parte libre de cuadrados).

Veamos de todos modos cuáles son las condiciones del teorema anterior. Consideramos

$$U_{20} = \big\{[1], [3], [7], [9], [11], [13], [17], [19]\big\}.$$

Los cuadrados son [1] y [9], luego ambos tienen carácter positivo. Calculamos por ejemplo $\chi_K(3) = (-20/3) = (1/3) = 1$, y $1 = \chi_K(3)\chi_K(9) = \chi_K(7)$, luego las clases de escisión son $\big\{[1], [3], [7], [9]\big\}$.

Sabemos que un número está representado por una de las formas f o g si y sólo si su parte libre de cuadrados consta de primos congruentes con 1, 3, 7, 9 módulo 20 además del 2 y el 5.

Esto lo cumplen ciertamente los números 2, 3 y 6, pero nada nos dice cómo distinguir cuándo la forma que los representa es f y cuándo es g. La respuesta nos la proporciona la teoría de géneros:

Teorema 7.25 *Sea K un cuerpo cuadrático con discriminante Δ, sean m y k números naturales primos entre sí y sea G un género del orden $\mathcal{O}_m$. Entonces k está representado por una forma de género G si y sólo si $(k,\Delta)_p = \chi_p(G)$ para todo primo p.*

Demostración: La condición es necesaria por la propia definición de χ_p. Si un número k cumple esta condición, en particular cumple que $(k,\Delta)_p = 1$ para todos los primos $p \nmid \Delta$, luego por el teorema 7.24 sabemos que k está representado por una forma f de discriminante $m^2\Delta$. Entonces

$$\chi_p(f) = (k,\Delta)_p = \chi_p(G),$$

luego la forma es de género G. ∎

Notemos que la representabilidad de un primo que no divide a m por una forma de género G depende sólo de su resto módulo $m^2\Delta$.

Ejercicio: Probar que k está representado por una forma de género G si y sólo si G (visto como conjunto de ideales) contiene un ideal de norma k.

Con esto podemos resolver el problema que teníamos planteado. Las formas f y g son de géneros distintos, concretamente f es de género $(++)$ y g es de género $(--)$ (los caracteres relevantes son χ_2 y χ_5).

Un número k que cumpla las condiciones del teorema 7.24 estará representado por la forma f si además cumple $(k,-20)_2 = (k,-20)_5 = 1$. En realidad sabemos que los dos signos han de coincidir en cualquier caso, luego la condición se puede reducir a $(k,-20)_5 = 1$.

Si $k = 5^i r$ esto equivale a

$$(k,-20)_5 = (5^i r,-5)_5 = (5,-5)_5^i (r,-5)_5 = (r,-1)_5 (r,5)_5 = (r/5) = 1.$$

Así, si k está representado por una de las formas f o g, será representado concretamente por f si y sólo si el número r que resulta de eliminar el 5 en la descomposición en primos de k cumple $r \equiv \pm 1$ (mód 5). Esto confirma que es g quien representa a 2 y 3, pero es f quien representa a 6. En resumen:

Un número es de la forma

$$k = x^2 + 5y^2 \quad o \quad k = 2x^2 + 2xy + 3y^2$$

si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 2, 5$ o $p \equiv 1, 3, 7, 9$ (mód 20), y será concretamente de la primera forma si además el número que resulta de eliminar el 5 de su descomposición en primos cumple $r \equiv \pm 1$ (mód 5).

La situación es más sencilla si la restringimos a primos:

Un primo $p \neq 2, 5$ cumple

$$p = x^2 + 5y^2 \quad \textit{si y sólo si} \quad p \equiv 1, 9 \pmod{20},$$
$$p = 2x^2 + 2xy + 3y^2 \quad \textit{si y sólo si} \quad p \equiv 3, 7 \pmod{20}.$$

Ejercicio: Probar que un primo $p \neq 2, 3$ es de la forma $p = x^2 + 6y^2$ si y sólo si $p \equiv 1, 7 \pmod{24}$ y es de la forma $p = 2x^2 + 3y^2$ si y sólo si $p \equiv 5, 11 \pmod{24}$. Dar condiciones para que un número natural arbitrario sea de una de estas dos formas.

En general, el teorema anterior nos permite separar los números que son representados por las distintas formas de un discriminante dado si cada género contiene una única clase de similitud. La tabla 7.1 contiene los primeros discriminantes negativos con esta propiedad junto con los coeficientes (a, b, c) de formas cuadráticas representantes de cada clase.

Más en particular, a la hora de estudiar los números representados por las formas $x^2 + ny^2$, interesan lo que se conoce como *números idóneos,* que son los números n tales que cada género de discriminante $-4n$ contiene una única clase de similitud. Véase [ITAl 14.16] y la definición previa.

Formas de discriminante -56 Las formas reducidas de discriminante -56 (véase [ITAl 11.17, 11.18]) son:

$$x^2 + 14y^2, \qquad 2x^2 + 7y^2, \qquad 3x^2 \pm 2xy + 5y^2.$$

Las dos últimas son similares, aunque no estrictamente similares, por lo que representan los mismos números. Como -56 es divisible entre dos primos, tenemos dos géneros. Las dos primeras formas son de género $(++)$ y las dos últimas son de género $(--)$. Combinando los teoremas 7.24 y 7.25 obtenemos:

Un número es de la forma

$$k = x^2 + 14y^2 \quad o \quad k = 2x^2 + 7y^2 \quad o \quad k = 3x^2 + 2xy + 5y^2$$

si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 2, 7$ o $p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}$. Más concretamente, estará representado por una de las dos primeras si además el número que resulta de eliminar el 7 de su descomposición en primos cumple $r \equiv 1, 2, 4 \pmod{7}$.

Para números primos tenemos una condición más simple:

Un primo $p \neq 2, 7$ cumple

$$p = x^2 + 14y^2 \text{ o } p = 2x^2 + 7y^2 \quad \textit{syss} \quad p \equiv 1, 9, 15, 23, 25, 39 \pmod{56},$$
$$p = 3x^2 + 2xy + 5y^2 \quad \textit{syss} \quad p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

Sin embargo, no tenemos ningún criterio para distinguir los números (o los primos) representados por las dos primeras formas. ∎

Ejercicio: Estudiar la representación de primos por formas de discriminante -44.

Tabla 7.1: Algunos discriminantes negativos para los que cada género contiene una única clase de similitud de ideales.

$-D$	a,b,c	$-D$	a,b,c	$-D$	a,b,c	$-D$	a,b,c	$-D$	a,b,c
3	$1,1,1$	52	$1,0,13$	115	$1,1,29$	187	$1,1,47$	288	$1,0,72$
4	$1,0,1$		$2,2,7$		$5,5,7$		$7,3,7$		$4,4,19$
7	$1,1,2$	60	$1,0,15$	120	$1,0,30$	192	$1,0,48$		$8,0,9$
8	$1,0,2$		$3,0,5$		$2,0,15$		$3,0,16$		$8,8,11$
11	$1,1,3$	64	$1,0,16$		$3,0,10$		$4,4,13$	312	$1,0,78$
12	$1,0,3$		$4,4,5$		$5,0,6$		$7,2,7$		$2,0,39$
15	$1,1,4$	67	$1,1,17$	123	$1,1,31$	195	$1,1,49$		$3,0,26$
	$2,1,2$	72	$1,0,18$		$3,3,11$		$3,3,17$		$6,0,13$
16	$1,0,4$		$2,0,9$	132	$1,0,33$		$5,5,11$	315	$1,1,79$
19	$1,1,5$	75	$1,1,19$		$2,2,17$		$7,1,7$		$5,5,17$
20	$1,0,5$		$3,3,7$		$3,0,11$	228	$1,0,57$		$7,7,13$
	$2,2,3$	84	$1,0,21$		$6,6,7$		$2,2,29$		$9,9,11$
24	$1,0,6$		$2,2,11$	147	$1,1,37$		$3,0,19$	340	$1,0,85$
	$2,0,3$		$3,0,7$		$3,3,13$		$6,6,11$		$2,2,43$
27	$1,1,7$		$5,4,5$	148	$1,0,37$	232	$1,0,58$		$5,0,17$
28	$1,0,7$	88	$1,0,22$		$2,2,19$		$2,0,29$		$10,10,11$
32	$1,0,8$		$2,0,11$	160	$1,0,40$	235	$1,1,59$	352	$1,0,88$
	$3,2,3$	91	$1,1,23$		$4,4,11$		$5,5,13$		$4,4,23$
35	$1,1,9$		$5,3,5$		$5,0,8$	240	$1,0,60$		$8,0,11$
	$3,1,3$	96	$1,0,24$		$7,6,7$		$3,0,20$		$8,8,13$
36	$1,0,9$		$3,0,8$	163	$1,1,41$		$4,0,15$	372	$1,0,93$
	$2,2,5$		$4,4,7$	168	$1,0,42$		$5,0,12$		$2,2,47$
40	$1,0,10$		$5,2,5$		$2,0,21$	267	$1,1,67$		$3,0,31$
	$2,0,5$	99	$1,1,25$		$3,0,14$		$3,3,23$		$6,6,17$
43	$1,1,11$		$5,1,5$		$6,0,7$	280	$1,0,70$		
48	$1,0,12$	100	$1,0,25$	180	$1,0,45$		$2,0,35$		
	$3,0,4$		$2,2,13$		$2,2,23$		$5,0,14$		
51	$1,1,13$	112	$1,0,28$		$5,0,9$		$7,0,10$		
	$3,3,5$		$4,0,7$		$7,4,7$				

Números de la forma $x^2 - ny^2$ Consideramos ahora las formas de tipo $x^2 - ny^2$, donde supondremos que n no es un cuadrado perfecto, pues si $n = k^2$ entonces factorizan como$(x+ky)(x-ky)$ y los números que representan pueden analizarse con técnicas mucho más elementales (y laboriosas).[1] Estas formas están asociadas a órdenes de los cuerpos cuadráticos reales $\mathbb{Q}(\sqrt{n})$. Como en el caso imaginario, la situación es más simple cuando el número de clases es $h = 1$.

[1]Por ejemplo, los números de la forma $x^2 - y^2$ son los impares y los múltiplos de 4. Las fórmulas $2k+1 = (k+1)^2-k^2$, $4k = (k+1)^2-(k-1)^2$ muestran que la condición es suficiente, y tomando restos módulo 4 se ve fácilmente que la condición es necesaria. En particular, todo primo impar es diferencia de dos cuadrados.

De aquí se sigue a su vez que los números de la forma $x^2 - 4y^2$ son los de la forma $4k+1$, $4(2k+1)$ y $8k$.

$n = 2$ *Un número es de la forma $x^2 - 2y^2$ si y sólo si los primos que dividen a su parte libre de cuadrados son $p = 2$ o bien $p \equiv \pm 1$ (mód 8).*

En efecto, la forma $x^2 - 2y^2$ es la forma principal de discriminante $D = 8$, y corresponde al orden maximal de $K = \mathbb{Q}(\sqrt{2})$, cuyo número de clases es $h = 1$ y, como la unidad fundamental tiene norma negativa, este número de clases es también el número de clases de similitud estricta de módulo, que a su vez es igual al número de clases de equivalencia estricta de formas cuadráticas, por lo que todas las formas de discriminante 8 representan los mismos números. Aplicamos el teorema 7.24, para lo que observamos que $U_8 = \{[1], [3], [5], [7]\}$. Se cumple $\chi_K(-1) = \chi_K(1) = 1$ (porque $\Delta > 0$ teorema [Al 12.19]), luego el teorema 7.24 nos da la condición del enunciado.

$n = 3$ *Un primo $p > 0$ es de la forma $p = x^2 - 3y^2$ si y sólo si $p \equiv 1$ (mód 12).*

Ahora tenemos la forma principal de discriminante $D = 12$, que corresponde al orden maximal del cuerpo $K = \mathbb{Q}(\sqrt{3})$. Su número de clases es $h = 1$, pero ahora la unidad fundamental tiene norma positiva, por lo que hay dos clases de similitud estricta de módulos, que se corresponden con dos clases de equivalencia estricta de formas cuadráticas. Podemos tomar como representantes las formas

$$x^2 - 3y^2, \qquad 3x^2 - y^2.$$

Notemos que no son equivalentes, pues la primera representa a 1 y la segunda no, ya que no hay unidades de norma -1.

Tenemos que $U_{12} = \{[1], [5], [7], [11]\}$, y nuevamente $\chi_K(-1) = \chi_K(1) = 1$, por lo que el teorema 7.24 nos da que un primo p cumple $\pm p = x^2 - 3y^2$ si y sólo si $p = 2$, $p = 3$ o $p \equiv \pm 1$ (mód 12).

Sin embargo, falta distinguir qué primos son de esta forma con signo positivo y cuáles con signo negativo. Para ello aprovechamos que ambas formas son de géneros distintos, la principal de género $(++)$ y la opuesta de género $(--)$, lo que nos permite aplicar el teorema 7.25. Un primo p estará representado por la forma principal si y sólo si, además de cumplir la condición precedente, cumple

$$(p, 12)_3 = (p, 3)_3 = 1.$$

Si $p \neq 3$, esto equivale a que $(p/3) = 1$, lo que a su vez equivale a que $p \equiv 1$ (mód 3). Para $p = 3$ sucede que $(3, 3)_3 = (3, -1)_3 = (-1/3) = -1$, luego lo descartamos. Las condiciones $p \equiv \pm 1$ (mód 12) y $p \equiv 1$ (mód 3) equivalen a $p \equiv 1$ (mód 12).

Ejercicio: Dar una condición para que un número arbitrario, no necesariamente primo, sea de la forma $x^2 - 3y^2$.

Ejercicio: Probar que un primo $p > 0$ es de la forma $p = x^2 - 10y^2$ si y sólo si $p \equiv \pm 1, \pm 9$ (mód 40), y es de la forma $p = 2x^2 - 5y^2$ si y sólo si $p = 2, 5$ o $p \equiv \pm 3, \pm 13$ (mód 40).

Si vamos analizando los casos correspondientes a los valores siguientes de n (que no sean cuadrados perfectos) nos encontraremos siempre con uno de los dos casos anteriores (o bien $h' = 1$ o bien $h' = 2$ y $g = 2$), por lo que la teoría de géneros nos caracteriza los primos (y, afinando más, los enteros) de la forma $k = x^2 - ny^2$ en términos del resto de k módulo el discriminante del orden cuadrático asociado. El primer caso en el que se rompe este esquema es el siguiente:

$n = 34$ La forma $x^2 - 34y^2$ es la forma principal de discriminante $D = 2^3 \cdot 17$, asociada al orden maximal del cuerpo $K = \mathbb{Q}(\sqrt{34})$. En la sección siguiente mostramos que su número de clases estrictas es $h' = 4$, mientras que $g = 2$. Concretamente, un sistema de representantes de las cases de equivalencia estricta de las formas cuadráticas de discriminante D es

$$x^2 - 34y^2, \qquad 34x^2 - y^2, \qquad 3x^2 + 2xy - 11y^2, \qquad -3x^2 + 2xy + 11y^2,$$

de las cuales las dos primeras formas tienen género $(++)$ y las dos últimas $(--)$. Las dos últimas son equivalentes, luego representan los mismos números.

El teorema 7.24 nos asegura que un primo p es de una de las formas

$$p = x^2 - 34y^2, \qquad p = 34x^2 - y^2, \qquad p = 3x^2 + 2xy - 11y^2$$

si y sólo si $p = 2, 17$ o bien

$$\begin{aligned} p \quad \equiv \quad & \pm1, \pm3, \pm5, \pm9, \pm11, \pm15, \pm25, \pm27, \pm29, \\ & \pm33, \pm37, \pm45, \pm47, \pm49, \pm55, \pm61, \ (\text{mód } 136). \end{aligned}$$

El teorema 7.25 nos permite matizar. Restringiéndonos a la representación de primos, por simplicidad, para que un primo p esté representado por una forma del género principal, un condición necesaria y suficiente es que

$$(p, 136)_{17} = (p, 2 \cdot 17)_{17} = (p, 2)_{17}(p, 17)_{17} = 1.$$

Si $p = 17$ tenemos que

$$(17, 2)_{17}(17, 17)_{17} = (2/17)(-1/17) = 1.$$

Para cualquier otro primo la condición es $(p/17) = 1$, lo cual sucede si y sólo si

$$p \equiv \pm1, \pm2, \pm4, \pm8 \ (\text{mód } 17).$$

En conclusión, un primo p cumple:

$$\begin{aligned} \pm p = x^2 - 34y^2 \quad & \text{syss} \quad p = 2, 17 \text{ o } p \equiv \pm1, \pm9, \pm15, \pm25, \\ & \qquad \pm33, \pm47, \pm49, \pm55 \ (\text{mód } 136), \\ p = 3x^2 + 2xy - 11y^2 \quad & \text{syss} \quad p \equiv \pm3, \pm5, \pm11, \pm27, \\ & \qquad \pm29, \pm37, \pm45, \pm61 \ (\text{mód } 136), \end{aligned}$$

pero no tenemos ningún criterio para saber si los primos de la primera forma aparecen con signo positivo o negativo. ∎

7.5 Grupos de clases y unidades

Dos de los invariantes más caóticos en la teoría de cuerpos cuadráticos son el número de clases y, en el caso de los cuerpos reales, el signo de la unidad fundamental. A su vez éste último interviene en la relación entre la similitud estricta y la no estricta y por lo tanto en la relación entre el número h' de clases estrictas y el número h de clases no estrictas. La teoría de los géneros aporta algunos datos sobre ambos invariantes. El teorema siguiente nos muestra un ejemplo sencillo:

Teorema 7.26 *Si K es un cuerpo cuadrático real y su discriminante es divisible entre un primo $p \equiv -1$ (mód 4), entonces la unidad fundamental de K cumple $\mathrm{N}(\epsilon) = 1$.*

Demostración: Por [ITAl 11.14] sabemos que $\chi_p(-1) = (-1/p) = -1$, luego la clase de similitud estricta -1 no coincide con la clase 1, es decir, los ideales generados por elementos de norma negativa no son estrictamente similares a los generados por elementos de norma positiva, aunque evidentemente sí son similares. ∎

Una forma concisa de expresar la hipótesis del teorema es $\Delta_K \neq x^2 + y^2$. Ahora estamos en condiciones de precisar la relación entre la similitud estricta y la no estricta en un cuerpo cuadrático real. Más en general, conviene clasificar los cuerpos cuadráticos en los cuatro tipos siguientes:

Tabla 7.2: Clasificación de los cuerpos cuadráticos

Tipo	Discriminante	$\chi_p(-1)$	$\mathrm{N}(\epsilon)$	h'	H'
I	$\Delta_K < 0$	—	—	h	$H' = H$
II	$\Delta_K = x^2 + y^2$	Todos $+1$	-1	h	$H' = H$
III	$0 < \Delta_K \neq x^2 + y^2$	Alguno -1	$+1$	$2h$	$H' \cong H \times \{\pm 1\}$
IV	$\Delta_K = x^2 + y^2$	Todos $+1$	$+1$	$2h$	$H' \ncong H \times \{\pm 1\}$

Los cuerpos cuadráticos de tipo I son los cuerpos imaginarios. Los de tipo II son los cuerpos reales cuya unidad fundamental tiene norma negativa. Acabamos de ver que esto implica que $\Delta_K = x^2 + y^2$ o, equivalentemente, que $\chi_p(-1) = 1$ para todos los caracteres. En ambos casos la similitud estricta coincide con la no estricta. Los cuerpos reales con unidad fundamental de norma positiva son de tipo III o de tipo IV según si el discriminante Δ_K es divisible o no entre un primo $p \equiv -1$ (mód 4) o, equivalentemente, si $\chi_p(-1) = -1$ para algún primo p. La razón de esta distinción es que de ella depende que el grupo de clases no estrictas H se pueda representar como factor directo del grupo de clases estrictas H', en el sentido preciso indicado en el teorema siguiente:

Teorema 7.27 *Sea K un cuerpo cuadrático de tipo* III. *Entonces existe un subgrupo H del grupo de clases estrictas H' de K, de modo que la aplicación $[x] \mapsto [x]$ es un isomorfismo de H en el grupo de clases no estrictas de K, y $H' = H \times \{\pm 1\}$. Si K es de tipo* IV *no existe tal subgrupo.*

DEMOSTRACIÓN: Sea p un primo tal que $\chi_p(-1) = -1$ Como el número de signos negativos ha de ser par, podemos suponer que p es impar. Sea H el conjunto de todas las clases x tales que $\chi_p(x) = 1$, o sea, el núcleo de χ_p. Claramente H es un subgrupo de índice 2 en H'. Basta probar que la aplicación $[x] \mapsto [x]$ es inyectiva en H, pues ciertamente es un homomorfismo de grupos y su imagen tiene el mismo número de elementos de H. Si $[M]$, $[M']$ son dos clases de H con la misma imagen, es decir, si M y M' son similares, entonces existe un $\alpha \in K$ tal que $M = \alpha M'$, luego $\chi_p(M) = \chi_p\big((\alpha)\big)\chi_p(M')$, lo que implica que $\chi_p\big((\alpha)\big) = 1$.

Por lo tanto $\big[(\alpha)\big] \neq -1$, es decir, $\mathrm{N}(\alpha) = 1$, luego M y M' son estrictamente similares y $[M] = [M']$. Como $-1 \notin H$, es claro que $H' = H \times \{\pm 1\}$.

Si K es de tipo IV entonces -1 está en el género principal, luego el teorema 7.16 nos da que $-1 = x^2$ para cierta clase $x \in H'$. Si $H' = H \times \{\pm 1\}$ para cualquier subgrupo H (sin más hipótesis) entonces tendríamos que $\pm x \in H$ para una elección adecuada del signo, luego $-1 = (\pm x)^2 \in H$, lo cual es imposible. ∎

Así pues, la extensión H'/H no es trivial en los cuerpos de tipo IV. El hecho de que existan tales cuerpos equivale a decir que el recíproco del teorema 7.26 es falso. Sirvan como ejemplos $\mathbb{Q}\big(\sqrt{34}\big)$ (el menor de todos) y $\mathbb{Q}\big(\sqrt{221}\big)$.

Un recíproco parcial al teorema 7.26 es que si $\Delta_K > 0$ es divisible entre un solo primo, entonces $\mathrm{N}(\epsilon) = -1$. En efecto, en tal caso K tiene un solo género, luego una sola clase ambigua, pero -1 y 1 son ambiguas, luego $1 = -1$.

Ejercicio: Si Δ_K es divisible entre un solo primo, entonces h es impar

Ejercicio: Si $\Delta_K = x^2 + y^2$ y cada género contiene un número impar de clases estrictas, entonces $\mathrm{N}(\epsilon) = 1$, es decir, K es de tipo IV.

Una consecuencia obvia de la teoría de géneros es que predice la presencia de potencias de 2 en el número de clases. No se conoce nada parecido para otros primos. El menor cuerpo cuadrático imaginario cuyo número de clases es divisible entre un primo impar al cuadrado es $\mathbb{Q}\big(\sqrt{-2\,299}\big)$. El grupo de clases contiene un factor $C_3 \times C_3$. El menor cuerpo cuadrático real en estas condiciones es $\mathbb{Q}\big(\sqrt{62\,501}\big)$ (con idéntico factor). Respecto a la presencia de primos impares en el número de clases, terminamos el capítulo con un resultado elemental sobre la cuestión. Notemos que no requiere teoría de géneros.

Teorema 7.28 *Supongamos que $d = r^2 - 4g^p < 0$ es libre de cuadrados, donde g y p son primos y r es impar. Supongamos además que $|d| > 4g$. Entonces p divide al número de clases de $\mathbb{Q}\big(\sqrt{d}\big)$.*

DEMOSTRACIÓN: Notemos que $d \equiv 1 \pmod 4$. Sea

$$\alpha = \frac{r-1}{2} + \frac{1+\sqrt{d}}{2}.$$

Claramente $\mathrm{N}(\alpha) = g^p$. Por lo tanto $\alpha = \mathfrak{p}^p$, donde $\mathfrak{p} \mid g$ (no puede haber dos primos distintos, pues serían los divisores conjugados de g, y entonces $g \mid \alpha$, pero α no es divisible entre enteros racionales).

Basta probar que $\mathfrak{p}$ no es principal, pues entonces $[\mathfrak{p}]$ tendrá orden p en el grupo de clases. A su vez, basta probar que no hay números de norma g. En caso contrario existirían a y b enteros o semienteros de modo que

$$g = \mathrm{N}\left(\frac{a}{2} + \frac{b}{2}\sqrt{d}\right) = \frac{a^2 - bd^2}{4},$$

pero $a^2 - bd^2 = 4g$ implica (teniendo en cuenta la hipótesis) que $b = 0$, luego $g = (a/2)^2$, contradicción. ∎

Esta situación es relativamente frecuente. Por ejemplo:

$$-15 = 1^2 - 4\cdot 2^2, \quad -23 = 3^2 - 4\cdot 2^3, \quad -31 = 1^2 - 4\cdot 2^3,$$
$$-47 = 9^2 - 4\cdot 2^5, \quad -71 = 21^2 - 4\cdot 2^7, \quad -79 = 7^2 - 4\cdot 2^5,$$
$$-271 = 89^2 - 4\cdot 2^{11}.$$

Terminamos este capítulo con tablas con los grupos de clases de los cuerpos cuadráticos con discriminante $|\Delta| < 100$. Antes mostramos algunos ejemplos de cómo pueden calcularse con las técnicas que hemos expuesto aquí y en [ITAl].

Ejemplo Calculemos el grupo de clases del orden maximal del cuerpo $\mathbb{Q}\big(\sqrt{34}\,\big)$.

Por 7.26 sabemos que la unidad fundamental tiene norma 1. Como se trata de un orden maximal podemos aplicar el teorema 3.14 y concluir que todo ideal es semejante a otro de norma a lo sumo 5. Hemos de buscar todos los ideales de norma menor o igual que 5.

Buscaremos primero los ideales primos. Puesto que $x^2 - 34 \equiv x^2$ (mód 2), el teorema 2.35 nos da la factorización $2 = \big(2, \sqrt{34}\,\big)^2$, luego hay un único ideal de norma 2.

Por otra parte, $x^2 - 34 \equiv x^2 - 1 \equiv (x+1)(x-1)$ (mód 3), luego

$$3 = (3, \sqrt{34} - 1)(3, \sqrt{34} + 1)$$

y por lo tanto hay dos ideales de norma 3. Para el 5 resulta que $x^2 - 34 \equiv x^2 - 4 \cong (x-2)(x+2)$ (mód 5), luego

$$5 = (5, \sqrt{34} - 2)(5, \sqrt{34} + 2).$$

En total hemos encontrado los siguientes ideales primos:

$$\mathfrak{p} = \big(2, \sqrt{34}\big), \quad \mathfrak{q}_1 = (3, \sqrt{34} - 1), \quad \mathfrak{q}_2 = (3, \sqrt{34} + 1),$$

$$\mathfrak{r}_1 = (5, \sqrt{34} - 2)(5, \sqrt{34} + 2).$$

Con ellos podemos formar estos ideales de norma menor o igual que 5:

$$1, \qquad \mathfrak{p}, \qquad \mathfrak{p}^2, \qquad \mathfrak{q}_1, \qquad \mathfrak{q}_2, \qquad \mathfrak{r}_1, \qquad \mathfrak{r}_2,$$

pero claramente $\mathfrak{p}^2 = 2$, es principal, luego la lista de representantes de clases de similitud se reduce a

$$1, \qquad \mathfrak{p}, \qquad \mathfrak{q}_1, \qquad \mathfrak{q}_2, \qquad \mathfrak{r}_1, \qquad \mathfrak{r}_2,$$

Para estudiar las relaciones de similitud entre ellos necesitamos conocer bases. El teorema [ITAl 12.16] nos da que

$$1 = \left\langle 1, \sqrt{34}\right\rangle, \quad \mathfrak{p} = \left\langle 2, \sqrt{34}\right\rangle \quad \mathfrak{q}_1 = \left\langle 3, -1+\sqrt{34}\right\rangle, \quad \mathfrak{q}_2 = \left\langle 3, 1+\sqrt{34}\right\rangle,$$
$$\mathfrak{r}_1 = \left\langle 5, -2+\sqrt{34}\right\rangle, \quad \mathfrak{r}_2 = \left\langle 5, 2+\sqrt{34}\right\rangle.$$

Consideramos los desarrollos

$$\sqrt{34} = \left[5, \overline{1,4,1,10}\right], \qquad \frac{\sqrt{34}}{2} = \left[2, \overline{1,10,1,4}\right],$$
$$\frac{-1+\sqrt{34}}{3} = \left[1, \overline{1,1,1,1,3,3}\right], \quad \frac{1+\sqrt{34}}{3} = \left[2, \overline{3,1,1,1,1,3}\right],$$
$$\frac{-2+\sqrt{34}}{5} = \left[0, \overline{1,3,3,1,1,1}\right], \quad \frac{2+\sqrt{34}}{5} = \left[1, \overline{1,1,3,3,1,1}\right].$$

Concluimos que $\mathfrak{p}$ es similar a 1 y que los otros cuatro ideales son similares entre sí. Por lo tanto, el número de clases es $h = 2$ y hay dos clases similitud de ideales, la de los ideales principales y la determinada, por ejemplo, por el ideal $\mathfrak{q} = (3, 1+\sqrt{34})$.

Como no hay unidades de norma negativa, el grupo de clases de similitud estricta tiene orden $h' = 4$ y para calcularlo tomamos cualquier elemento de norma negativa, por ejemplo, $\sqrt{34}$. Así, los ideales

$$1, \qquad (\sqrt{34}), \qquad (3, 1+\sqrt{34}), \qquad \sqrt{34}(3, 1+\sqrt{34})$$

son un sistema de representantes de las clases de similitud estricta. Las formas cuadráticas asociadas son

$$x^2 - 34y^2, \qquad 34x^2 - y^2, \qquad 3x^2 + 2xy - 11y^2, \qquad -3x^2 + 2xy + 11y^2,$$

luego éstas forman un sistema completo de representantes de las clases de equivalencia estricta. Es fácil ver que las dos primeras formas tienen género $(++)$ y las dos últimas $(--)$. En particular, esto implica que la clase de la segunda forma es un cuadrado en el grupo de clases, luego éste es cíclico generado por cualquiera de las dos últimas formas (cosa que también puede comprobarse directamente en términos de los ideales correspondientes).

Observemos también que las dos primeras formas no son equivalentes, pues la primera representa al 1 y la segunda no (ya que no hay unidades de norma negativa), mientras que las dos últimas formas, aunque sabemos que no son estrictamente equivalentes, sí que son equivalentes. Un cambio de variables que transforma la tercera en la cuarta es

$$x \mapsto 2x - 5y, \qquad y \mapsto -x + 2y.$$

Por lo tanto, hay tres clases de equivalencia no estricta de formas de discriminante 136. ∎

Ejemplo Calculemos el grupo de clases del orden maximal del cuerpo $\mathbb{Q}\big(\sqrt{82}\,\big)$. Se comprueba (por ejemplo, usando [ITAl 10.17]) que una unidad fundamental es $\epsilon = 9 + \sqrt{82}$, que tiene norma -1, por lo que la similitud coincide con la similitud estricta. Seguimos los mismos pasos que en el ejemplo precedente. Por el teorema 3.14, todo ideal es semejante a otro de norma a lo sumo 9. Puesto que $x^2 - 82 \equiv x^2 \pmod 2$, el teorema 2.35 nos da la factorización $2 = \big(2, \sqrt{82}\,\big)^2$, luego hay un único ideal de norma 2.

Por otra parte, $x^2 - 82 \equiv x^2 - 1 \equiv (x+1)(x-1) \pmod 3$, luego

$$3 = (3, \sqrt{82} - 1)(3, \sqrt{82} + 1)$$

y por lo tanto hay dos ideales de norma 3.

Para el 5 resulta que $x^2 - 82 \equiv x^2 - 2 \pmod 5$ es irreducible, luego 5 es primo y no hay ideales de norma 5. Lo mismo ocurre con el 7.

En total hemos encontrado los siguientes ideales primos:

$$\mathfrak{p} = \big(2, \sqrt{82}\big), \quad \mathfrak{q} = (3, \sqrt{82} - 1), \quad \mathfrak{r} = (3, \sqrt{82} + 1).$$

Con ellos se forman los ideales siguientes de norma menor o igual que 9:

$$1, \quad \mathfrak{p}, \quad \mathfrak{p}^2, \quad \mathfrak{p}^3, \quad \mathfrak{q}, \quad \mathfrak{q}^2, \quad \mathfrak{r}, \quad \mathfrak{r}^2, \quad \mathfrak{pq}, \quad \mathfrak{pr}, \quad \mathfrak{qr}.$$

Sin embargo sabemos que $\mathfrak{p}^2 = 2$ es principal, así como $\mathfrak{qr} = 3$, luego la lista de representantes de clases de similitud se reduce a

$$1, \quad \mathfrak{p}, \quad \mathfrak{q}, \quad \mathfrak{q}^2, \quad \mathfrak{r}, \quad \mathfrak{r}^2, \quad \mathfrak{pq}, \quad \mathfrak{pr}.$$

El teorema [ITAl 12.16] nos da que

$$\mathfrak{p} = \left\langle 2, \sqrt{82} \right\rangle \quad \mathfrak{q} = \left\langle 3, -1 + \sqrt{82} \right\rangle, \quad \mathfrak{r} = \left\langle 3, 1 + \sqrt{82} \right\rangle.$$

Así pues,

$$1 = \left\langle 1, \sqrt{82} \right\rangle, \ \mathfrak{p} = 2\left\langle 1, \frac{\sqrt{82}}{2} \right\rangle, \ \mathfrak{q} = 3\left\langle 1, \frac{-1+\sqrt{82}}{3} \right\rangle, \ \mathfrak{r} = 3\left\langle 1, \frac{1+\sqrt{82}}{3} \right\rangle.$$

Los desarrollos en fracción continua son

$$\sqrt{82} = \big[9, \overline{18}\,\big], \qquad \frac{\sqrt{82}}{2} = \big[4, \overline{1, 1, 8}\,\big],$$

$$\frac{-1+\sqrt{82}}{3} = \big[2, \overline{1, 2, 5}\,\big], \quad \frac{1+\sqrt{82}}{3} = \big[3, \overline{2, 1, 5}\,\big].$$

Vemos, pues, que ningún par es similar. Estudiemos ahora

$$\mathfrak{q}^2 = \left\langle 9, -3 + 3\sqrt{82}, 83 - 2\sqrt{82} \right\rangle = \left\langle 9, -1 + \sqrt{82} \right\rangle.$$

Calculamos

$$\frac{-1+\sqrt{82}}{9} = \big[0, \overline{1, 8, 1}\,\big],$$

y así concluimos que $[\mathfrak{q}^2] = [\mathfrak{p}]$.

Podríamos seguir estudiando los ideales, pero las reglas elementales de la teoría de grupos nos permiten acabar sin más cálculos. En efecto, puesto que $[\mathfrak{p}]$ tiene orden 2 y $[\mathfrak{q}]^2 = [\mathfrak{p}]$, concluimos que $[\mathfrak{q}]$ tiene orden 4. Si eliminamos $\mathfrak{q}^2$ de la lista de representantes nos quedan siete ideales, luego $h \leq 7$, pero como hay una clase de orden 4 ha de ser $4 \mid h$, lo que obliga a que $h = 4$. Sabemos que las cuatro clases $[1]$, $[\mathfrak{p}]$, $[\mathfrak{q}]$, $[\mathfrak{r}]$ son distintas, luego $[\mathfrak{q}]^3 = [\mathfrak{r}]$ y esto ya determina el producto de cualquier par de clases.

Es fácil ver que las clases de similitud estricta de formas cuadráticas de discriminante 328 son

$$[x^2 - 82y^2], \qquad [2x^2 - 41y^2], \qquad [3x^2 - 2xy - 27y^2], \qquad [3x^2 + 2xy - 27y^2].$$

Las dos primeras tienen género $(++)$ y las dos últimas $(--)$.

Es claro que las dos últimas formas son equivalentes, mientras que las dos primeras no lo son, pues la segunda no representa a 1. En efecto, por el teorema [ITAl 12.29], para que representara a 1 haría falta que la clase de similitud estricta $[\mathfrak{p}]$ contuviera al ideal 1, y no es el caso. Por lo tanto, tenemos tres clases de equivalencia de formas cuadráticas. ∎

Ejemplo Vamos a calcular el grupo de clases asociado al orden maximal del cuerpo $\mathbb{Q}(\sqrt{-161}\,)$.

En general conviene observar que si tenemos un ideal en la forma indicada por el teorema [ITAl 12.16], es decir, $\mathfrak{a} = \langle a, u + m\omega\rangle$, donde a, u son enteros racionales y $\mathrm{N}(u + m\omega) = av$, entonces la forma asociada es

$$\frac{\mathrm{N}(ax + (u + m\omega)y)}{a} = ax^2 + \mathrm{Tr}(u + m\omega)xy + vy^2.$$

Tenemos $D = -644$ y por el teorema 3.14 todo ideal es similar a uno de norma menor o igual que 16. El comportamiento de los primos menores que 16 es el siguiente:

$$2 = 2_0^2, \quad 3 = 3_1\,3_2, \quad 5 = 5_1\,5_2, \quad 7 = 7_0^1, \quad 11 = 11_1\,11_2.$$

Los ideales de norma menor o igual que 16 son (eliminando los que obviamente son similares):

$$1, \quad 2_0, \quad 3_1, \quad 3_2, \quad 5_1, \quad 5_2, \quad 2_0\,3_1, \quad 2_0\,3_2, \quad 7_0, \quad 3_1^2, \quad 3_2^2, \quad 2_0\,5_1,$$
$$2_0\,5_2, \quad 11_1, \quad 11_2, \quad 2_0\,7_0, \quad 3_1\,5_1, \quad 3_1\,5_2, \quad 3_2\,5_1, \quad 3_2\,5_2.$$

El ideal 1 corresponde a la forma principal $x^2 + 161y^2$.

El ideal $2_0 = \langle 2, 1 + \sqrt{-161}\rangle$ se corresponde con

$$\mathrm{N}\left(2x + \left(1 + \sqrt{-161}\,\right)y\right)/2 = 2x^2 + 2xy + 81y^2,$$

que ya está reducida. Como no es la forma principal, el ideal 2_0 no es principal. El orden de la clase $[2_0]$ es obviamente 2.

Consideremos los ideales $3_1 = \langle 3, 1+\sqrt{-161}\rangle$, $3_2 = \langle 3, -1+\sqrt{-161}\rangle$, cuyas formas asociadas son, respectivamente, $3x^2+2xy+54y^2$ y $3x^2-2xy+54y^2$, que ya están reducidas. Como no son la forma principal, ninguno de estos ideales es principal.

Vamos a calcular el orden de $[3_1]$. Se comprueba fácilmente que

$$3_1^2 = \langle 9, 3+3\sqrt{-161}, -160+2\sqrt{-161}\rangle = \langle 9, 1+\sqrt{-161}\rangle,$$

luego la forma asociada es $9x^2+2xy+18y^2$, que ya está reducida, por lo que el ideal tampoco es principal.

Ahora $3_1^4 = \langle 81, 9+9\sqrt{-161}, -160+2\sqrt{-161}\rangle = \langle 81, 1+\sqrt{-161}\rangle$, y su forma es $81x^2+2xy+2y^2$, que se reduce a $2x^2+2xy+81y^2$. Ésta es la forma asociada a 2_0, luego $[3_1]^4 = [2_0]$. Por lo tanto $[3_1]^8 = [2_0]^2 = 1$ y el orden de $[3_1]$ resulta ser 8.

Como el número de clases es a lo sumo 20, en realidad ha de ser 8 o bien 16. Ahora bien, si estudiamos $7_0 = \langle 7, \sqrt{-161}\rangle$ vemos que su forma asociada es $7x^2+23y^2$, distinta de la principal y de la asociada a $[2_0]$. Por lo tanto $[7_0]$ es una clase de orden 2 que no es potencia de $[3_1]$ (la única potencia de orden 2 es $[2_0]$). Por consiguiente el número de clases es 16 y el grupo de clases está generado por $[3_1]$ y $[7_0]$. ∎

Ejercicio: Calcular la tabla del grupo de clases del ejemplo anterior.

Tabla 7.3: Grupos de clases de cuerpos cuadráticos imaginarios
Los valores de d marcados con un asterisco son los congruentes con 1 módulo 4.
El número α es $\sqrt{d}$ o $(1+\sqrt{d})/2$.

d	Δ	h	Clases	Relaciones	Caracteres
-1	-2^2	1	(1)	1	$+$
-2	-2^3	1	(1)	1	$+$
-3^*	-3	1	(1)	1	$+$
-5	$-2^2\cdot 5$	2	(1)	A^2	$++$
			$(2,1+\alpha)$	A	$--$
-6	$-2^3\cdot 3$	2	(1)	A^2	$++$
			$(2,\alpha)$	A	$--$
-7^*	-7	1	(1)	1	$+$
-10	$-2^3\cdot 5$	2	(1)	A^2	$++$
			$(2,\alpha)$	A	$--$
-11^*	-11	1	(1)	1	$+$
-13	$-2^2\cdot 13$	2	(1)	A^2	$++$
			$(2,1+\alpha)$	A	$--$
-14	$-2^3\cdot 7$	4	(1)	L^4	$++$
			$(3,2+\alpha)$	L^3	$--$
			$(2,\alpha)$	L^2	$++$
			$(3,1+\alpha)$	L	$--$
-15^*	$-3\cdot 5$	2	(1)	A^2	$++$
			$(2,1+\alpha)$	A	$--$
-17	$-2^2\cdot 17$	4	(1)	L^4	$++$
			$(3,2+\alpha)$	L^3	$--$
			$(2,1+\alpha)$	L^2	$++$
			$(3,1+\alpha)$	L	$--$
-19^*	-19	1	(1)	1	$+$
-21	$-2^2\cdot 3\cdot 7$	4	(1)	A^2B^2	$+++$
			$(5,3+\alpha)$	AB	$--+$
			$(3,\alpha)$	B	$-+-$
			$(2,1+\alpha)$	A	$+--$
-22	$-2^3\cdot 11$	2	(1)	A^2	$++$
			$(2,\alpha)$	A	$--$
-23^*	-23	3	(1)	L^3	$+$
			$(2,1+\alpha)$	L^2	$+$
			$(2,\alpha)$	L	$+$
-26	$-2^3\cdot 13$	6	(1)	L^6	$++$
			$(5,3+\alpha)$	L^5	$--$
			$(3,1+\alpha)$	L^4	$++$
			$(2,\alpha)$	L^3	$--$
			$(3,2+\alpha)$	L^2	$++$
			$(5,2+\alpha)$	L	$--$
-29	$-2^2\cdot 29$	6	(1)	L^6	$++$
			$(3,2+\alpha)$	L^5	$--$
			$(5,4+\alpha)$	L^4	$++$
			$(2,1+\alpha)$	L^3	$--$
			$(5,1+\alpha)$	L^2	$++$
			$(3,1+\alpha)$	L	$--$

d	Δ	h	Clases	Relaciones	Caracteres
-30	$-2^3 \cdot 3 \cdot 5$	4	(1)	A^2B^2	$+++$
			$(2,\alpha)$	AB	$--+$
			$(3,\alpha)$	B	$+--$
			$(5,\alpha)$	A	$-+-$
-31^*	-31	3	(1)	L^3	$+$
			$(2,\alpha)$	L^2	$+$
			$(2,1+\alpha)$	L	$+$
-33	$-2^2 \cdot 3 \cdot 11$	4	(1)	A^2B^2	$+++$
			$(2,1+\alpha)$	AB	$--+$
			$(3,\alpha)$	B	$-+-$
			$(6,3+\alpha)$	A	$+--$
-34	$-2^3 \cdot 17$	4	(1)	L^4	$++$
			$(5,4+\alpha)$	L^3	$--$
			$(2,\alpha)$	L^2	$++$
			$(5,1+\alpha)$	L	$--$
-35^*	$-5 \cdot 7$	2	(1)	A^2	$++$
			$(5,2+\alpha)$	A	$--$
-37	$-2^2 \cdot 37$	2	(1)	A^2	$++$
			$(2,1+\alpha)$	A	$--$
-38	$-2^3 \cdot 19$	6	(1)	L^6	$++$
			$(3,2+\alpha)$	L^5	$--$
			$(7,2+\alpha)$	L^4	$++$
			$(2,\alpha)$	L^3	$--$
			$(7,5+\alpha)$	L^2	$++$
			$(3,1+\alpha)$	L	$--$
-39^*	$-3 \cdot 13$	4	(1)	L^4	$++$
			$(2,1+\alpha)$	L^3	$--$
			$(3,1+\alpha)$	L^2	$++$
			$(2,\alpha)$	L	$--$
-41	$-2^2 \cdot 41$	8	(1)	L^8	$++$
			$(3,2+\alpha)$	L^7	$--$
			$(5,3+\alpha)$	L^6	$++$
			$(7,6+\alpha)$	L^5	$--$
			$(2,1+\alpha)$	L^4	$++$
			$(7,1+\alpha)$	L^3	$--$
			$(5,2+\alpha)$	L^2	$++$
			$(3,1+\alpha)$	L	$--$
-42	$-2^3 \cdot 3 \cdot 7$	4	(1)	A^2B^2	$+++$
			$(7,\alpha)$	AB	$-+-$
			$(3,\alpha)$	B	$--+$
			$(2,\alpha)$	A	$+--$
-43^*	-43	1	(1)	1	$+$
-46	$-2^3 \cdot 23$	4	(1)	L^4	$++$
			$(5,3+\alpha)$	L^3	$--$
			$(2,\alpha)$	L^2	$++$
			$(5,2+\alpha)$	L	$--$
-47^*	-47	5	(1)	L^5	$+$
			$(2,\alpha)$	L^4	$+$
			$(3,2+\alpha)$	L^3	$+$
			$(3,\alpha)$	L^2	$+$
			$(2,1+\alpha)$	L	$+$
-51^*	$-3 \cdot 17$	2	(1)	A^2	$++$
			$(3,1+\alpha)$	A	$--$

d	Δ	h	Clases	Relaciones	Caracteres
-53	$-2^2 \cdot 53$	6	(1)	L^6	$++$
			$(3, 2+\alpha)$	L^5	$--$
			$(9, 8+\alpha)$	L^4	$++$
			$(2, 1+\alpha)$	L^3	$--$
			$(9, 1+\alpha)$	L^2	$++$
			$(3, 1+\alpha)$	L	$--$
-55^*	$-5 \cdot 11$	4	(1)	L^4	$++$
			$(2, 1+\alpha)$	L^3	$--$
			$(5, 2+\alpha)$	L^2	$++$
			$(2, \alpha)$	L	$--$
-57	$-2^2 \cdot 3 \cdot 19$	4	(1)	A^2B^2	$+++$
			$(2, 1+\alpha)$	AB	$--+$
			$(3, 1+\alpha)$	B	$-+-$
			$(6, 3+\alpha)$	A	$+--$
-58	$-2^3 \cdot 29$	2	(1)	A^2	$++$
			$(2, \alpha)$	A	$--$
-59^*	-59	3	(1)	L^3	$+$
			$(3, 2+\alpha)$	L^2	$+$
			$(3, \alpha)$	L	$+$
-61	$-2^2 \cdot 61$	6	(1)	L^3	$++$
			$(5, 3+\alpha)$	L^2	$++$
			$(5, 2+\alpha)$	L	$++$
			$(7, 5+\alpha)$	AL^2	$--$
			$(7, 3+\alpha)$	AL	$--$
			$(2, 1+\alpha)$	A	$--$
-62	$-2^3 \cdot 31$	8	(1)	L^8	$++$
			$(3, 2+\alpha)$	L^7	$--$
			$(7, 1+\alpha)$	L^6	$++$
			$(11, 2+\alpha)$	L^5	$--$
			$(2, \alpha)$	L^4	$++$
			$(11, 9+\alpha)$	L^3	$--$
			$(7, 6+\alpha)$	L^2	$++$
			$(3, 1+\alpha)$	L	$--$
-65	$-2^2 \cdot 5 \cdot 13$	8	(1)	L^4	$+++$
			$(3, 2+\alpha)$	L^3	$-+-$
			$(9, 4+\alpha)$	L^2	$+++$
			$(3, 1+\alpha)$	L	$-+-$
			$(11, 10+\alpha)$	AL^3	$+--$
			$(2, 1+\alpha)$	AL^2	$--+$
			$(11, 1+\alpha)$	AL	$+--$
			$(5, \alpha)$	A	$--+$
-66	$-2^3 \cdot 3 \cdot 11$	8	(1)	L^4	$+++$
			$(5, 3+\alpha)$	L^3	$-+-$
			$(3, \alpha)$	L^2	$+++$
			$(5, 2+\alpha)$	L	$-+-$
			$(7, 2+\alpha)$	AL^3	$+--$
			$(11, \alpha)$	AL^2	$--+$
			$(7, 5+\alpha)$	AL	$+--$
			$(2, \alpha)$	A	$--+$
-67^*	-67	1	(1)	1	$+$

d	Δ	h	Clases	Relaciones	Caracteres
-69	$-2^2 \cdot 3 \cdot 23$	8	(1)	L^4	$+++$
			$(7, 6+\alpha)$	L^3	$+--$
			$(6, 3+\alpha)$	L^2	$+++$
			$(7, 1+\alpha)$	L	$+--$
			$(5, 1+\alpha)$	AL^3	$--+$
			$(3, \alpha)$	AL^2	$-+-$
			$(5, 4+\alpha)$	AL	$--+$
			$(2, 1+\alpha)$	A	$-+-$
-70	$-2^3 \cdot 5 \cdot 7$	4	(1)	A^2B^2	$+++$
			$(7, \alpha)$	AB	$--+$
			$(5, \alpha)$	B	$+--$
			$(2, \alpha)$	A	$-+-$
-71^*	-71	7	(1)	L^7	$+$
			$(2, 1+\alpha)$	L^6	$+$
			$(5, 3+\alpha)$	L^5	$+$
			$(3, 2+\alpha)$	L^4	$+$
			$(3, \alpha)$	L^3	$+$
			$(5, 1+\alpha)$	L^2	$+$
			$(2, \alpha)$	L	$+$
-73	$-2^2 \cdot 73$	4	(1)	L^4	$++$
			$(7, 5+\alpha)$	L^3	$--$
			$(2, 1+\alpha)$	L^2	$++$
			$(7, 2+\alpha)$	L	$--$
-74	$-2^3 \cdot 37$	10	(1)	L^5	$++$
			$(11, 6+\alpha)$	L^4	$++$
			$(3, 1+\alpha)$	L^3	$++$
			$(3, 2+\alpha)$	L^2	$++$
			$(11, 5+\alpha)$	L	$++$
			$(5, 4+\alpha)$	AL^4	$--$
			$(6, 4+\alpha)$	AL^3	$--$
			$(6, 2+\alpha)$	AL^2	$--$
			$(5, 1+\alpha)$	AL	$--$
			$(2, \alpha)$	A	$--$
-77	$-2^2 \cdot 7 \cdot 11$	8	(1)	L^4	$+++$
			$(3, 2+\alpha)$	L^3	$-+-$
			$(14, 7+\alpha)$	L^2	$+++$
			$(3, 1+\alpha)$	L	$-+-$
			$(6, 5+\alpha)$	AL^3	$--+$
			$(7, \alpha)$	AL^2	$+--$
			$(6, 1+\alpha)$	AL	$--+$
			$(2, 1+\alpha)$	A	$+--$
-78	$-2^3 \cdot 3 \cdot 13$	4	(1)	A^2B^2	$+++$
			$(2, \alpha)$	AB	$--+$
			$(13, \alpha)$	B	$+--$
			$(3, \alpha)$	A	$-+-$
-79^*	-79	5	(1)	L^5	$+$
			$(2, \alpha)$	L^4	$+$
			$(5, 4+\alpha)$	L^3	$+$
			$(5, \alpha)$	L^2	$+$
			$(2, 1+\alpha)$	L	$+$
-82	$-2^3 \cdot 41$	4	(1)	L^4	$++$
			$(7, 4+\alpha)$	L^3	$--$
			$(2, \alpha)$	L^2	$++$
			$(7, 3+\alpha)$	L	$--$

d	Δ	h	Clases	Relaciones	Caracteres
-83^*	-83	3	(1)	L^3	$+$
			$(3, 2+\alpha)$	L^2	$+$
			$(3, \alpha)$	L	$+$
-85	$-2^2 \cdot 5 \cdot 17$	4	(1)	A^2B^2	$+++$
			$(5, \alpha)$	AB	$--+$
			$(10, 5+\alpha)$	B	$+--$
			$(2, 1+\alpha)$	A	$-+-$
-86	$-2^3 \cdot 43$	10	(1)	L^{10}	$++$
			$(3, 2+\alpha)$	L^9	$--$
			$(9, 2+\alpha)$	L^8	$++$
			$(5, 2+\alpha)$	L^7	$--$
			$(17, 13+\alpha)$	L^6	$++$
			$(2, \alpha)$	L^5	$--$
			$(17, 4+\alpha)$	L^4	$++$
			$(5, 3+\alpha)$	L^3	$--$
			$(9, 7+\alpha)$	L^2	$++$
			$(3, 1+\alpha)$	L	$--$
-87^*	$-3 \cdot 29$	6	(1)	L^6	$++$
			$(2, 1+\alpha)$	L^5	$--$
			$(7, 2+\alpha)$	L^4	$++$
			$(3, 1+\alpha)$	L^3	$--$
			$(7, 4+\alpha)$	L^2	$++$
			$(2, \alpha)$	L	$--$
-89	$-2^2 \cdot 89$	12	(1)	L^{12}	$++$
			$(3, 2+\alpha)$	L^{11}	$--$
			$(17, 9+\alpha)$	L^{10}	$++$
			$(7, 3+\alpha)$	L^9	$--$
			$(5, 4+\alpha)$	L^8	$++$
			$(6, 1+\alpha)$	L^7	$--$
			$(2, 1+\alpha)$	L^6	$++$
			$(6, 5+\alpha)$	L^5	$--$
			$(5, 1+\alpha)$	L^4	$++$
			$(7, 4+\alpha)$	L^3	$--$
			$(17, 8+\alpha)$	L^2	$++$
			$(3, 1+\alpha)$	L	$--$
-91^*	$-7 \cdot 13$	2	(1)	A^2	$++$
			$(7, 3+\alpha)$	A	$--$
-93	$-2^2 \cdot 3 \cdot 31$	4	(1)	A^2B^2	$+++$
			$(6, 3+\alpha)$	AB	$--+$
			$(3, \alpha)$	B	$+--$
			$(2, 1+\alpha)$	A	$-+-$
-94	$-2^2 \cdot 47$	8	(1)	L^8	$++$
			$(5, 4+\alpha)$	L^7	$--$
			$(7, 5+\alpha)$	L^6	$++$
			$(11, 4+\alpha)$	L^5	$--$
			$(2, \alpha)$	L^4	$++$
			$(11, 7+\alpha)$	L^3	$--$
			$(7, 2+\alpha)$	L^2	$++$
			$(5, 1+\alpha)$	L	$--$

d	Δ	h	Clases	Relaciones	Caracteres
-95^*	$-5\cdot 19$	1	(1)	L^8	$++$
			$(2,\alpha)$	L^7	$--$
			$(4,\alpha)$	L^6	$++$
			$(3,2+\alpha)$	L^5	$--$
			$(5,2+\alpha)$	L^4	$++$
			$(3,\alpha)$	L^3	$--$
			$(4,3+\alpha)$	L^2	$++$
			$(2,1+\alpha)$	L	$--$
-97	$-2^2\cdot 97$	1	(1)	L^4	$++$
			$(7,6+\alpha)$	L^3	$--$
			$(2,1+\alpha)$	L^2	$++$
			$(7,1+\alpha)$	L	$--$

Tabla 7.4: Grupos de clases de cuerpos cuadráticos reales

Los valores de d marcados con un asterisco son los congruentes con 1 módulo 4. El número α es $\sqrt{d}$ o $(1+\sqrt{d})/2$. Se indica también la fracción continua de $\sqrt{\alpha}$ y una unidad fundamental ϵ.

d	Δ	h	$\sqrt{\alpha}$	ϵ	$\mathrm{N}(\epsilon)$	Clases	Caract.
2	2^3	1	$\left[1,\overline{2}\right]$	$1+\alpha$	-1	(1)	$+$
3	$2^2\cdot 3$	1	$\left[1,\overline{1,2}\right]$	$2+\alpha$	$+1$	(1)	$+$
5^*	5	1	$\left[\overline{1}\right]$	α	-1	(1)	$+$
6	$2^3\cdot 3$	1	$\left[2,\overline{2,4}\right]$	$5+2\alpha$	$+1$	(1)	$++$
7	$2^2\cdot 7$	1	$\left[2,\overline{1,1,1,4}\right]$	$8+3\alpha$	$+1$	(1)	$++$
10	$2^3\cdot 5$	2	$\left[3,\overline{6}\right]$	$3+\alpha$	-1	(1)	$++$
						$(2,\alpha)$	$--$
11	$2^2\cdot 11$	1	$\left[3,\overline{3,6}\right]$	$10+3\alpha$	$+1$	(1)	$++$
13^*	13	1	$\left[2,\overline{3}\right]$	$1+\alpha$	-1	(1)	$+$
14	$2^2\cdot 7$	1	$\left[3,\overline{1,2,1,6}\right]$	$15+4\alpha$	$+1$	(1)	$++$
15	$2^2\cdot 3\cdot 5$	2	$\left[3,\overline{1,6}\right]$	$4+\alpha$	$+1$	(1)	$+++$
						$(2,1+\alpha)$	$--+$
17^*	17	1	$\left[2,\overline{1,1,3}\right]$	$3+2\alpha$	-1	(1)	$+$
19	$2^2\cdot 19$	1	$\left[4,\overline{2,1,3,1,2,8}\right]$	$170+39\alpha$	$+1$	(1)	$++$
21^*	$3\cdot 7$	1	$\left[2,\overline{1,3}\right]$	$2+\alpha$	$+1$	(1)	$++$
22	$2^3\cdot 11$	1	$\left[4,\overline{1,2,4,2,1,8}\right]$	$197+42\alpha$	$+1$	(1)	$++$
23	$2^2\cdot 23$	1	$\left[4,\overline{1,3,1.8}\right]$	$24+5\alpha$	$+1$	(1)	$++$
26	$2^3\cdot 13$	2	$\left[5,\overline{10}\right]$	$5+\alpha$	-1	(1)	$++$
						$(2,\alpha)$	$--$
29^*	29	1	$\left[3,\overline{5}\right]$	$2+\alpha$	-1	(1)	$+$
30	$2^3\cdot 3\cdot 5$	2	$\left[5,\overline{2,10}\right]$	$11+2\alpha$	$+1$	(1)	$+++$
						$(2,\alpha)$	$+--$
31	$2^2\cdot 31$	1	$\left[5,\overline{1,1,3,5,3,1,1,10}\right]$	$1.520+273\alpha$	$+1$	(1)	$++$

d	Δ	h	$\sqrt{\alpha}$	ϵ	$\mathrm{N}(\epsilon)$	Clases	Caract.
33^*	$3\cdot 11$	1	$\left[3,\overline{2,1,2,5}\right]$	$19+8\alpha$	$+1$	(1)	$++$
34	$2^3\cdot 17$	2	$\left[5,\overline{1,4,1,10}\right]$	$35+6\alpha$	$+1$	(1)	$++$
						$(3,1+\alpha)$	$--$
35	$2^2\cdot 5\cdot 7$	2	$\left[5,\overline{1,10}\right]$	$6+\alpha$	$+1$	(1)	$+++$
						$(2,1+\alpha)$	$-+-$
37^*	37	1	$\left[3,\overline{1,1,5}\right]$	$5+2\alpha$	-1	(1)	$+$
38	$2^3\cdot 19$	1	$\left[6,\overline{6,12}\right]$	$37+6\alpha$	$+1$	(1)	$++$
39	$2^2\cdot 3\cdot 13$	2	$\left[6,\overline{4,12}\right]$	$25+4\alpha$	$+1$	(1)	$+++$
						$(2,1+\alpha)$	$--+$
41^*	41	1	$\left[3,\overline{1,2,2,1,5}\right]$	$27+10\alpha$	-1	(1)	$+$
42	$2^3\cdot 3\cdot 7$	2	$\left[6,\overline{2,12}\right]$	$13+2\alpha$	$+1$	(1)	$+++$
						$(2,\alpha)$	$+--$
43	$2^2\cdot 43$	1	$\left[6,\overline{1,1,3,1,5,1,3,1,1,12}\right]$	$3.482+531\alpha$	$+1$	(1)	$++$
46	$2^3\cdot 23$	1	$\left[6,\overline{1,3,1,1,2,6,2,1,1,3,1,12}\right]$	$24.335+3.588\alpha$	$+1$	(1)	$++$
47	$2^2\cdot 47$	1	$\left[6,\overline{1,5,1,12}\right]$	$48+7\alpha$	$+1$	(1)	$++$
51	$2^2\cdot 3\cdot 17$	2	$\left[7,\overline{7,14}\right]$	$50+7\alpha$	$+1$	(1)	$+++$
						$(3,\alpha)$	$-++$
53^*	53	1	$\left[4,\overline{7}\right]$	$3+\alpha$	-1	(1)	$+$
55	$2^2\cdot 5\cdot 11$	2	$\left[7,\overline{2,2,2,14}\right]$	$89+12\alpha$	$+1$	(1)	$+++$
						$(2,1+\alpha)$	$--+$
57^*	$3\cdot 19$	1	$\left[4,\overline{3,1,1,1,3,7}\right]$	$131+40\alpha$	$+1$	(1)	$++$
58	$2^3\cdot 29$	2	$\left[7,\overline{1,1,1,1,1,1,14}\right]$	$99+13\alpha$	-1	(1)	$++$
						$(2,\alpha)$	$--$
59	$2^2\cdot 59$	1	$\left[7,\overline{1,2,7,2,1,14}\right]$	$530+69\alpha$	$+1$	(1)	$++$
61^*	61	1	$\left[4,\overline{2,2,7}\right]$	$17+5\alpha$	-1	(1)	$+$
62	$2^3\cdot 31$	1	$\left[7,\overline{1,6,1,14}\right]$	$63+8\alpha$	$+1$	(1)	$++$
65^*	$5\cdot 13$	2	$\left[4,\overline{1,1,7}\right]$	$7+2\alpha$	-1	(1)	$++$
						$(5,2+\alpha)$	$--$
66	$2^3\cdot 3\cdot 11$	2	$\left[8,\overline{8,16}\right]$	$65+8\alpha$	$+1$	(1)	$+++$
						$(3,\alpha)$	$+--$
67	$2^2\cdot 67$	1	$\left[8,\overline{5,2,1,1,7,1,1,2,5,16}\right]$	$48.842+5.967\alpha$	$+1$	(1)	$++$
69^*	$3\cdot 23$	1	$\left[4,\overline{1,1,1,7}\right]$	$11+3\alpha$	$+1$	(1)	$++$
70	$2^3\cdot 5\cdot 7$	2	$\left[8,\overline{2,1,2,1,2,16}\right]$	$251+30\alpha$	$+1$	(1)	$++$
						$(2,\alpha)$	$--+$
71	$2^2\cdot 71$	1	$\left[8,\overline{2,2,1,7,1,2,2,16}\right]$	$3.480+413\alpha$	$+1$	(1)	$++$
73^*	73	1	$\left[4,\overline{1,3,2,1,1,2.3.1.7}\right]$	$943+250\alpha$	-1	(1)	$+$

d	Δ	h	$\sqrt{\alpha}$	ϵ	$\mathrm{N}(\epsilon)$	Clases	Caract.
74	$2^3 \cdot 37$	2	$\left[8, \overline{1,1,1,1,16}\right]$	$43 + 5\alpha$	-1	(1)	$++$
						$(2, \alpha)$	$--$
77^*	$7 \cdot 11$	1	$\left[4, \overline{1,7}\right]$	$4 + \alpha$	$+1$	(1)	$++$
78	$2^3 \cdot 3 \cdot 13$	2	$\left[8, \overline{1,4,1,16}\right]$	$53 + 6\alpha$	$+1$	(1)	$+++$
						$(2, \alpha)$	$--+$
79	$2^2 \cdot 79$	3	$\left[8, \overline{1,7,1,16}\right]$	$80 + 9\alpha$	$+1$	(1)	$++$
						$(3, 2+\alpha)$	$--$
						$(3, 1+\alpha)$	$--$
82	$2^3 \cdot 41$	4	$\left[9, \overline{18}\right]$	$9 + \alpha$	-1	(1)	$++$
						$(3, 1+\alpha)$	$--$
						$(2, \alpha)$	$++$
						$(3, 2+\alpha)$	$--$
83	$2^2 \cdot 83$	1	$\left[9, \overline{9,18}\right]$	$82 + 9\alpha$	$+1$	(1)	$++$
85^*	$5 \cdot 17$	2	$\left[5, \overline{9}\right]$	$4 + \alpha$	-1	(1)	$++$
						$(5, 2+\alpha)$	$--$
86	$2^3 \cdot 43$	1	$\left[9, \overline{3,1,1,1,8,\ 1,1,1,3,18}\right]$	$10.405 + 1.122\alpha$	$+1$	(1)	$++$
87	$2^2 \cdot 3 \cdot 29$	2	$\left[9, \overline{3,18}\right]$	$28 + 3\alpha$	$+1$	(1)	$+++$
						$(2, 1+\alpha)$	$--+$
89^*	89	1	$\left[5, \overline{4,1,1,1,\ 1,4,9}\right]$	$447 + 106\alpha$	-1	(1)	$+$
91	$2^2 \cdot 7 \cdot 13$	2	$\left[9, \overline{1,1,5,1,5,\ 1,1,18}\right]$	$1.574 + 165\alpha$	$+1$	(1)	$+++$
						$(2, 1+\alpha)$	$+--$
93^*	$3 \cdot 31$	1	$13 + 3\alpha$	$+1$	(1)	$++$	
94	$2^3 \cdot 47$	1	$\left[9, \overline{1,2,3,1,1,\ 5,1,8,1,5,1,\ 1,3,2,1,18}\right]$	$2.143.295 + 221.064\alpha$	$+1$	(1)	$++$
95	$2^2 \cdot 5 \cdot 19$	2	$\left[9, \overline{1,2,1,18}\right]$	$39 + 4\alpha$	$+1$	(1)	$+++$
						$(2, 1+\alpha)$	$--+$
97^*	97	1	$\left[5, \overline{2,2,1,4\ 4,1,2,2,9}\right]$	$5.035 + 1.138\alpha$	-1	(1)	$+$

Capítulo VIII

Primos regulares

En [Al 8.45] demostramos el teorema de Kummer según el cual el Último Teorema de Fermat es cierto para exponentes primos regulares. Sin embargo, la definición [Al 8.44] de primo regular no es fácil de comprobar. En este capítulo expondremos una caracterización muy simple de dichos primos, debida también a Kummer. Concretamente, veremos que la condición B) de [Al 8.44] es, de hecho, consecuencia de la condición A), de modo que un primo impar p es regular si y sólo si p no divide al número de clases del cuerpo ciclotómico de orden p. A su vez, encontraremos un criterio sencillo para comprobar si esto sucede.

8.1 La fórmula del número de clases

Sea p un primo impar. Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de grado p y sea $K' = K \cap \mathbb{R}$. Sea $m = (p-1)/2$ el grado de K' el subcuerpo de los números ciclotómicos reales. Partimos de las fórmulas 4.27 y 4.29 para el número de clases de estos cuerpos:

$$h = \frac{\sqrt{p}^{\,p}}{2^{m-1}\pi^m\, R} \prod_{\chi\neq 1} L(1,\chi), \qquad h' = \frac{\sqrt{p}^{\,m-1}}{2^{m-1}R'} \prod_{\substack{\chi(1)=1\\ \chi\neq 1}} L(1,\chi).$$

El teorema 3.26 nos da además la relación $R = 2^{m-1}R'$ entre los reguladores, lo que nos permite expresar h en la forma

$$h = \frac{\sqrt{p}^{\,m+2}}{2^{m-1}\pi^m} \prod_{\chi(1)=-1} L(1,\chi)\; h'.$$

Puesto que h y h' son números naturales las fórmulas no se alteran si sustituimos las funciones L por sus módulos (recordemos que en sus desarrollos aparecen sumas de Gauss, de las que sólo conocemos los módulos). Vamos usar

la notación clásica introducida por Kummer, según la cual el número de clases se descompone como $h = h_1 h_2$, donde

$$h_1 = \frac{\sqrt{p}^{\,m+2}}{2^{m-1}\pi^m} \prod_{\chi(1)=-1} |L(1,\chi)|, \qquad h_2 = \frac{\sqrt{p}^{\,m-1}}{2^{m-1}R'} \prod_{\substack{\chi(1)=1 \\ \chi\neq 1}} |L(1,\chi)|.$$

Los números h_1 y h_2 reciben el nombre de primer y segundo factor del número de clases. Vemos, pues, que el segundo factor es el número de clases de K', por lo que en particular es un número natural. Probaremos que h_1 también lo es, y así los dos factores serán divisores del número de clases.

Ahora conviene hacer unas observaciones generales sobre caracteres de grupos abelianos que nos permitirán simplificar las expresiones de ambos factores.

Sea G un grupo abeliano finito y V el conjunto de todas las aplicaciones de G en $\mathbb{C}$. Vimos en la sección 4.3 que V es un espacio vectorial que tiene por base a los caracteres de G. Para cada $g \in G$ sea $T_g : V \longrightarrow V$ la aplicación dada por $T_g(f)(t) = f(gt)$. Claramente T_g es una aplicación lineal y si χ es un carácter de G se cumple $T_g(\chi) = \chi(g)\chi$, es decir, los caracteres son vectores propios de la aplicación T_g.

Sea ahora $v \in V$ y consideremos $T = \sum_{g\in G} v(g)T_g$. La aplicación T también es lineal y tiene a los caracteres por vectores propios. En efecto,

$$T(\chi)(t) = \sum_{g\in G} v(g)T_g(\chi)(t) = \sum_{g\in G} v(g)\chi(g)\chi(t),$$

luego

$$T(\chi) = \Big(\sum_{g\in G} v(g)\chi(g)\Big)\chi.$$

Por lo tanto la matriz de T en la base formada por los caracteres es una matriz diagonal y su determinante vale

$$\det T = \prod_{\chi} \sum_{g\in G} v(g)\chi(g).$$

Calculemos por otro lado el determinante de T en la base canónica de V, esto es, en la base $\{f_s\}_{s\in G}$ formada por las funciones

$$f_s(t) = \begin{cases} 1 & \text{si } t = s \\ 0 & \text{si } t \neq s \end{cases}$$

El coeficiente (s,t) de la matriz es

$$T(f_s)(t) = \sum_{g\in G} v(g)T_g(f_s)(t) = \sum_{g\in G} v(g)f_s(tg) = v(st^{-1}).$$

Con esto hemos probado el teorema siguiente:

Teorema 8.1 *Sea G un grupo abeliano finito y $v : G \longrightarrow \mathbb{C}$. Entonces la expresión*

$$\prod_{\chi} \sum_{g\in G} v(g)\chi(g),$$

donde χ recorre los caracteres de G, es igual al determinante de $\big(v(st^{-1})\big)_{s,\,t\in G}$.

Notemos que la matriz simétrica $\big(v(st)\big)_{s,\,t\in G}$ se diferencia de la indicada en el teorema tan sólo en el orden de las columnas (alterado según la permutación $t \mapsto t^{-1}$), luego, salvo signo, los determinantes coinciden.

Fijamos ahora la notación que seguiremos en todo el análisis del número de clases. Sea ζ una raíz de la unidad de orden $p-1$ y sea g una raíz primitiva módulo p, es decir, un generador del grupo U_p. Sea χ el carácter de U_p determinado por $\chi(g) = \zeta^{-1}$. Es claro que 1, χ, $\ldots$, χ^{p-2} son todos los caracteres módulo p. Además χ^k es par si y sólo si k es par.

8.2 El primer factor del número de clases

Investigamos ahora el factor h_1 del número de clases. Hemos de probar que es un número natural, y además daremos una fórmula práctica para calcularlo.

En la fórmula de h_1 intervienen los caracteres impares. Aplicamos el teorema 4.32 evaluando la suma de Gauss mediante 4.36:

$$|L(1,\chi^{2r+1})| = \frac{\pi\sqrt{p}}{p^2}\left|\sum_{k=1}^{p-1} \bar{\chi}^{2r+1}(k)\,k\right|.$$

Llamemos g_k al menor resto positivo módulo p de g^r. Así

$$|L(1,\chi^{2r+1})| = \frac{\pi\sqrt{p}}{p^2}\left|\sum_{k=0}^{p-2} \bar{\chi}^{2r+1}(g^k)\,g_k\right| = \frac{\pi\sqrt{p}}{p^2}\left|\sum_{k=0}^{p-2} g_k\zeta^{(2r+1)k}\right|.$$

Si llamamos

$$F(x) = \sum_{k=0}^{p-2} g_k x^k,$$

tenemos que

$$|L(1,\chi^{2r+1})| = \frac{\pi\sqrt{p}}{p^2}\,|F(\zeta^{2r+1})|.$$

Recordando que en la definición de h_1 aparecen $m = (p-1)/2$ factores, concluimos que

$$h_1 = \frac{1}{(2p)^{m-1}}\,|F(\zeta)F(\zeta^3)\cdots F(\zeta^{p-2})|. \tag{8.1}$$

Observemos ahora que $\zeta^m = -1$, por lo que

$$F(\zeta^{2r+1}) = \sum_{k=0}^{m-1}(g_k - g_{m+k})\zeta^{(2r+1)k} = \sum_{k=0}^{m-1}(g_k - g_{m+k})\zeta^k\,\zeta^{2rk}.$$

Vamos a aplicar el teorema 8.1 tomando como $G = \mathbb{Z}/m\mathbb{Z}$. Sea ψ el carácter determinado por $\psi(k) = \zeta^{2k}$. Es claro que las potencias de ψ recorren todos los caracteres de G y la expresión anterior es

$$F(\zeta^{2r+1}) = \sum_{k=0}^{m-1} (g_k - g_{m+k})\zeta^k\, \psi^r(k).$$

Notemos que la función $f(k) = (g_k - g_{m+k})\zeta^k$ depende sólo del resto de k módulo m, pues

$$f(k+m) = (g_{k+m} - g_{2m+k})\zeta^{k+m} = (g_{k+m} - g_k)(-1)\zeta^k = f(k).$$

Por consiguiente la fórmula (8.1) se escribe equivale a

$$h_1 = \frac{1}{(2p)^{m-1}} \left| \prod_{r=0}^{m-1} \sum_{k\in G} f(k)\psi^r(k) \right|.$$

Aplicando el teorema 8.1 (y la observación posterior)

$$h_1 = \frac{1}{(2p)^{m-1}} \left|\det\big((g_{s+t} - g_{m+s+t})\zeta^{s+t}\big)\right|,$$

donde s, y t varían entre 0 y $m-1$. Más aún, el determinante que aparece en la fórmula anterior es, por definición,

$$\sum_{\sigma\in\Sigma_m} \operatorname{sig}\sigma \prod_{s=0}^{m-1} (g_{s+\sigma(s)} - g_{m+s+\sigma(s)})\zeta^{s+\sigma(s)}.$$

Al agrupar las potencias de ζ de cada factor obtenemos ζ elevado al exponente $2(1+2+\cdots m-1) = m(m-1)$, es decir, $(-1)^{m-1}$. Este signo sale factor común de todos los sumandos y se cancela con el valor absoluto que rodea al determinante. En definitiva hemos probado lo siguiente:

Teorema 8.2 *El primer factor del número de clases viene dado por la fórmula*

$$h_1 = \frac{1}{(2p)^{m-1}} \left|\det(g_{s+t} - g_{m+s+t})\right|,$$

donde s y t varían entre 0 y $m-1$, y g_n es el menor resto positivo módulo p de g^n.

Esta expresión involucra sólo números enteros y no presenta por tanto ningún problema para su cálculo efectivo. Por ejemplo, si $p = 23$ una raíz primitiva es $g = 5$. Hemos de calcular

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
g_n	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14
$g_n - g_{11+n}$	−21	−13	−19	−3	−15	17	−7	11	9	−1	−5	21	13	19	3	15	−17	7	−11	−9	1	5

y de aquí

$$h_1 = \frac{1}{46^{10}} \begin{vmatrix} -21 & -13 & -19 & -3 & -15 & 17 & -7 & 11 & 9 & -1 & -5 \\ -13 & -19 & -3 & -15 & 17 & -7 & 11 & 9 & -1 & -5 & 21 \\ -19 & -3 & -15 & 17 & -7 & 11 & 9 & -1 & -5 & 21 & 13 \\ -3 & -15 & 17 & -7 & 11 & 9 & -1 & -5 & 21 & 13 & 19 \\ -15 & 17 & -7 & 11 & 9 & -1 & -5 & 21 & 13 & 19 & 3 \\ 17 & -7 & 11 & 9 & -1 & -5 & 21 & 13 & 19 & 3 & 15 \\ -7 & 11 & 9 & -1 & -5 & 21 & 13 & 19 & 3 & 15 & -17 \\ 11 & 9 & -1 & -5 & 21 & 13 & 19 & 3 & 15 & -17 & 7 \\ 9 & -1 & -5 & 21 & 13 & 19 & 3 & 15 & -17 & 7 & -11 \\ -1 & -5 & 21 & 13 & 19 & 3 & 15 & -17 & 7 & -11 & -9 \\ -5 & 21 & 13 & 19 & 3 & 15 & -17 & 7 & -11 & -9 & 1 \\ 21 & 13 & 19 & 3 & 15 & -17 & 7 & -11 & -9 & 1 & 5 \end{vmatrix}$$

Un ordenador calcula este determinante en fracciones de segundo. El resultado es 127 262 242 448 329 728, de donde $h_1 = 3$. La tabla siguiente contiene el valor de h_1 para primos $p < 100$. Vemos que aumenta rápidamente. De hecho puede probarse que a partir de 23 siempre es mayor que 1, con lo que los únicos cuerpos ciclotómicos de orden primo con factorización única son los siete correspondientes a $p < 23$.

Tabla 8.1: Primer factor del número de clases de los cuerpos ciclotómicos

p	h_1	p	h_1	p	h_1
3	1	29	2^3	61	$41 \cdot 1\,861$
5	1	31	3^2	67	$67 \cdot 12\,739$
7	1	37	37	71	$7^2 \cdot 79\,241$
11	1	41	11^2	73	$89 \cdot 134\,353$
13	1	43	211	79	$5 \cdot 53 \cdot 377\,911$
17	1	47	$5 \cdot 139$	83	$3 \cdot 279\,405\,653$
19	1	53	4.889	89	$113 \cdot 118\,401\,449$
23	3	59	$3 \cdot 59 \cdot 233$	97	$577 \cdot 3\,457\,206\,209$

La tabla muestra también que los primos 37, 59 y 67 son irregulares.

Todavía no hemos probado que, como hace ver la tabla, el número h_1 es un número natural. El determinante de la expresión del teorema 8.2 es claramente un entero racional. Hay que probar que es divisible entre 2^{m-1} y entre p^{m-1}. El caso del 2 es muy simple. Notamos que

$$g_k + g_{k+m} \equiv g^k + g^{k+m} = g^k(1 + g^m) = 0 \text{ (mód } p),$$

luego $g_k + g_{k+m} = p$ y por consiguiente uno de ellos es par y el otro impar. Por lo tanto, la matriz $(g_{s+t} - g_{m+s+t})$ tiene todas sus coordenadas impares. Sumando una fila a todas las restantes obtenemos otra matriz con el mismo determinante y $m-1$ filas formadas por números pares, de donde extraemos un factor 2^{m-1}.

Falta probar que este mismo determinante es divisible entre p^{m-1}. Para ello usaremos la expresión equivalente que aparece en (8.1). Sea

$$B = F(\zeta)F(\zeta^3)\cdots F(\zeta^{p-2}).$$

El número B es, salvo el signo, el determinante del teorema 8.2, luego es un entero racional. La clave es que cada factor es una suma geométrica módulo p:

$$F(\zeta^r) = \sum_{k=0}^{p-2} g_k\zeta^{rk} \equiv \sum_{k=0}^{p-2}(g\zeta^r)^k \text{ (mód } p).$$

Para sumarla multiplicamos por la razón menos 1:

$$F(\zeta^r)(g\zeta^r - 1) \equiv (g\zeta^r)^{p-1} - 1 \equiv 0 \text{ (mód } p),$$

es decir, $p \mid F(\zeta^r)(g\zeta^r - 1)$.

Ahora hemos de estudiar la posibilidad de que divisores primos de p en $\mathbb{Q}(\zeta)$ dividan al factor de la derecha. Puesto que $p \equiv 1 \text{ (mód } p-1)$, el teorema 2.38 nos da que p se descompone en $\phi(p-1)$ factores primos de norma p.

Si $\mathfrak{p}$ es uno de estos factores, el polinomio $x^{p-1} - 1$ tiene todas sus raíces distintas módulo $\mathfrak{p}$ (es primo con su derivada), luego las potencias de ζ recorren las $p-1$ clases no nulas módulo $\mathfrak{p}$. En particular existe un r tal que $\zeta^{-r} \equiv g$ (mód $\mathfrak{p}$), luego $\mathfrak{p} \mid g\zeta^r - 1$.

Notemos que como g tiene orden $p-1$ módulo $\mathfrak{p}$, lo mismo le ha de ocurrir a ζ^{-r}, para lo cual es necesario que $(r, p-1) = 1$. Además $\mathfrak{p}$ no puede dividir a otro $g\zeta^s - 1$, pues entonces $g\zeta^s \equiv 1 \equiv g\zeta^r$ (mód $\mathfrak{p}$), luego $\zeta^s \equiv \zeta^r$ (mód $\mathfrak{p}$) y, suponiendo $0 \le r, s < p-1$, ha de ser $r = s$.

En resumen, cada uno de los $\phi(p-1)$ divisores primos de p divide exactamente a uno de los $\phi(p-1)$ números $g\zeta^r - 1$ con $(r, p-1) = 1$.

Llamamos $\mathfrak{p}_r$ al único divisor primo de p que divide a $g\zeta^r - 1$. Entonces tenemos que

$$p = \prod_{(r,p-1)=1} \mathfrak{p}_r.$$

(Convenimos en que la definición de $\mathfrak{p}_r$ vale para todo entero primo con $p-1$, de modo que $\mathfrak{p}_r = \mathfrak{p}_{r+p-1}$. Si r no es primo con $p-1$ tomamos $\mathfrak{p}_r = 1$).

Sabiendo todo esto, la relación $p \mid F(\zeta^r)(g\zeta^r - 1)$ implica que $p\,\mathfrak{p}_r^{-1} \mid F(\zeta^r)$, luego multiplicando para todos los r impares hasta $p-2$ obtenemos que

$$p^m p_1^{-1}\mathfrak{p}_3^{-1}\cdots p_{p-2}^{-1} \mid F(\zeta)F(\zeta^3)\cdots F(\zeta^{p-2}),$$

luego $p^{m-1} \mid B$, como había que probar.

Esta técnica que hemos empleado para probar que h_1 es entero puede refinarse para obtener un criterio sencillo de cuándo $p \mid h_1$, lo cual tiene interés porque una de las condiciones de la definición de primo regular es que $p \nmid h$, y en particular ha de ser $p \nmid h_1$.

En primer lugar, p dividirá a h_1 si y sólo si divide a B/p^{m-1}, y como éste es un entero racional, esto ocurrirá si y sólo si uno cualquiera de los primos $\mathfrak{p}_r$, por ejemplo p_{-1}, divide a B/p^{m-1}. Ahora bien, sabemos que

$$\frac{B}{p^{m-1}} = \frac{F(\zeta)\mathfrak{p}_1}{p}\,\frac{F(\zeta^3)\mathfrak{p}_3}{p}\cdots\frac{F(\zeta^{p-2})\mathfrak{p}_{p-2}}{p},$$

donde cada factor de la derecha es un ideal (entero). Por consiguiente $p \mid h_1$ si y sólo si $\mathfrak{p}_{-1}$ divide a uno de los ideales $F(\zeta^r)\mathfrak{p}_r\,p^{-1}$, para $r = 1, 3, \ldots, p-2$. Esto equivale a su vez a que $\mathfrak{p}_{-1}^2 \mid F(\zeta^r)\mathfrak{p}_r$ para algún r.

Ahora bien, $\mathfrak{p}_{-1}^2$ en ningún caso puede dividir a $F(\zeta^{-1})\mathfrak{p}_{-1}$. En efecto, tenemos que $g\zeta^{-1} \equiv 1 \pmod{\mathfrak{p}_1}$, de donde

$$F(\zeta^{-1}) \equiv \sum_{k=0}^{p-2}(g\zeta^{-1})^k \equiv \sum_{k=0}^{p-2} 1 \equiv -1 \pmod{\mathfrak{p}_{-1}},$$

luego, $\mathfrak{p}_{-1} \nmid F(\zeta^{-1})$. Así pues, $p \mid h_1$ si y sólo si $\mathfrak{p}_{-1}^2 \mid F(\zeta^r)\mathfrak{p}_r$ para algún $r = 1, 3, \ldots, p-4$, lo que a su vez equivale a que $\mathfrak{p}_{-1}^2 \mid F(\zeta^r)$.

Hasta aquí todo es válido para cualquier elección de la raíz primitiva g. Dada una raíz primitiva cualquiera h módulo p, podemos tomar $g = h^p$, con lo que tenemos una raíz primitiva que además cumple $g^{p-1} = h^{p(p-1)} \equiv 1 \pmod{p^2}$, pues $\phi(p^2) = p(p-1)$.

Con esta elección de g y teniendo en cuenta la factorización

$$x^{p-1} - y^{p-1} = (x-y)(x-y\zeta)\cdots(x-y\zeta^{p-2}),$$

vemos que

$$\prod_{r=0}^{p-2}(1-g\zeta^k) = 1 - g^{p-1} \equiv 0 \pmod{p^2},$$

y, dado que $\mathfrak{p}_{-1}$ no puede dividir a otro factor que no sea $1-g\zeta^{-1}$, concluimos que $\mathfrak{p}_{-1}^2 \mid 1-g\zeta^{-1}$, es decir, $\zeta \equiv g \pmod{\mathfrak{p}_{-1}^2}$.

Esto nos permite eliminar a ζ de la condición que hemos obtenido, pues

$$F(\zeta^r) = \sum_{k=0}^{p-2} g_k\zeta^{kr} \equiv \sum_{k=0}^{p-2} g_k g^{kr} \pmod{\mathfrak{p}_{-1}^2},$$

luego $\mathfrak{p}_{-1}^2 \mid F(\zeta^r)$ si y sólo si

$$\mathfrak{p}_{-1}^2 \mid \sum_{k=0}^{p-2} g_k g^{kr}, \quad \text{si y sólo si} \quad p^2 \mid \sum_{k=0}^{p-2} g_k g^{kr}.$$

Con esto tenemos ya una condición en términos de números enteros, pero se puede simplificar mucho más. El razonamiento que sigue es incorrecto, pero se puede arreglar:

$$\sum_{k=0}^{p-2} g_k g^{kr} \equiv \sum_{k=0}^{p-2} g^k g^{kr} \equiv \sum_{k=0}^{p-2} g^{k(r+1)} \equiv \sum_{k=0}^{p-2} g_k^{r+1} \equiv \sum_{n=1}^{p-1} n^{r+1} \pmod{p^2}. \tag{8.2}$$

El problema es, por supuesto, que en principio las congruencias son ciertas sólo módulo p, no p^2. Si pese a ello logramos justificarlas, habremos eliminado los g_k de la condición.

Para arreglarlo expresamos $g_k = g^k + pa_k$, para cierto entero a_k. Tomamos congruencias módulo p^2 y elevamos a $r+1$:

$$g_k^{r+1} \equiv g^{k(r+1)} + (r+1)g^{kr}pa_k \equiv g^{k(r+1)} + (r+1)g^{kr}(g_k - g^k) \pmod{p^2},$$

o sea,

$$g_k^{r+1} \equiv (r+1)g_k g^{kr} - kg^{k(r+1)} \pmod{p^2}. \tag{8.3}$$

Si no estuviera el último término y teniendo en cuenta que nos interesa $r < p-1$, esta fórmula nos aseguraría que p^2 divide al primer término de (8.2) si y sólo si divide al cuarto, con lo que el problema estaría resuelto. Afortunadamente, el sumando molesto desaparece al sumar respecto a k:

$$\sum_{k=0}^{p-2} g^{k(r+1)} = \frac{g^{(p-1)(r+1)} - 1}{g^{r+1} - 1} \equiv 0 \pmod{p^2},$$

ya que $g^{p-1} \equiv 1 \pmod{p^2}$ y $p \nmid g^{r+1} - 1$ para $r+1 < p-1$.

Por lo tanto al sumar en (8.3) obtenemos

$$\sum_{k=0}^{p-2} g_k^{r+1} \equiv (r+1)\sum_{k=0}^{p-2} g_k g^{kr} \pmod{p^2},$$

y como $p \nmid k+1$, llegamos a que

$$p^2 \mid \sum_{k=0}^{p-2} g_k g^{kr} \quad \text{si y sólo si} \quad p^2 \mid \sum_{k=0}^{p-2} g_k^{r+1} = \sum_{n=1}^{p-1} n^{r+1}.$$

Hemos demostrado el teorema siguiente:

Teorema 8.3 *Se cumple que p divide al primer factor de h si y sólo si p^2 divide a alguno de los números*

$$S_m(p) = \sum_{n=1}^{p-1} n^m, \quad \textit{para } m = 2,\ 4,\ \ldots,\ p-3.$$

Aunque esta condición puede parecer completamente satisfactoria, lo cierto es que admite una reformulación más simple, que no sólo tiene interés práctico, sino que es relevante para estudiar cuándo p divide al segundo factor de h.

La clave está en que las sumas $S_m(p)$ pueden calcularse en términos de los polinomios de Bernoulli (véase la sección 6.5 de [ITAn]):

$$S_m(p) = \frac{B_{m+1}(p) - B_{m+1}}{m+1}.$$

Aquí $B_{m+1}(x)$ es el polinomio de Bernoulli, dado por [ITAn 6.20]:

$$B_{m+1}(x) = \sum_{k=0}^{m+1} \binom{m+1}{k} B_k x^{m+1-k},$$

donde a su vez los coeficientes B_k son los números de Bernoulli [ITAn 6.17], que pueden calcularse recurrentemente como se muestra en la sección [ITAn 6.5]. Las dos relaciones precedentes nos dan:

$$S_m(p) = \frac{B_{m+1}(p) - B_{m+1}}{m+1} = \sum_{k=0}^{m} \frac{1}{m+1} \binom{m+1}{k} B_k\, p^{m+1-k}.$$

En [ITAn 6.17] se prueba que $B_1 = -1/2$, mientras que que $B_{2k+1} = 0$ para todo $k \geq 1$. Necesitamos algunas propiedades más sobre los números de Bernoulli de índice par. Ante todo, es inmediato que son números racionales. En el teorema siguiente llamamos p-enteros a los números racionales con denominador no divisible entre p, es decir, la localización de $\mathbb{Z}$ respecto de $\mathbb{Z} \setminus (p)$, o también la intersección $\mathbb{Q} \cap \mathbb{Z}_p$ de $\mathbb{Q}$ con el anillo de los enteros p-ádicos.

Teorema 8.4 (Teorema de von Staudt) *Sea m un número par y expresemos $B_m = C_m/D_m$ con $(C_m, D_m) = 1$. Entonces*

1. *D_m es libre de cuadrados.*
2. *Para cada primo p se cumple que $p \mid D_m$ si y sólo si $p - 1 \mid m$.*
3. *Si un primo p cumple que $p \mid D_m$, entonces $pB_m \equiv -1 \pmod{p}$ en el anillo de los p-enteros.*

Demostración: Probaremos el teorema por inducción sobre m. Es claro que $B_0 = 1$ cumple el teorema. Sea p un primo cualquiera. La fórmula previa al enunciado puede expresarse en la forma:

$$pB_m = S_m(p) - \sum_{k=0}^{m-1} \frac{1}{m+1} \binom{m+1}{k} p^{m-k} pB_k. \tag{8.4}$$

Vamos a probar que todos los números en el sumatorio son p-enteros múltiplos de p. Por hipótesis de inducción los números pB_k son p-enteros (porque son nulos o bien p divide al denominador de B_k con multiplicidad a lo sumo 1). Basta probar que los números

$$\frac{1}{m+1} \binom{m+1}{k} p^{m-k}$$

son p-enteros múltiplos de p.

Si $p = 2$ es inmediato, puesto que $m+1$ es impar y el número combinatorio es un entero. Supongamos que p es impar. Entonces

$$\frac{1}{m+1} \binom{m+1}{k} p^{m-k} = \frac{m(m-1)\cdots(k+1)}{(m-k+1)!} p^{m-k}.$$

Si $r = m - k + 1$, entonces el exponente de p en $r!$ es a lo sumo

$$E(r/p) + E(r/p^2) + \cdots < \frac{r}{p} + \frac{r}{p^2} + \cdots = \frac{r}{p-1} \leq \frac{r}{2} \leq r - 1 = m - k,$$

donde E denota la parte entera (observemos que $E(r/p^i)$ es el número de múltiplos de p^i menores que r). De aquí se sigue lo pedido.

Con esto hemos probado que pB_m es p-entero para todo primo p, lo que prueba que D_m es libre de cuadrados. Más aún, la fórmula (8.4) implica ahora que

$$pB_m \equiv S_m(p) \text{ (mód } p).$$

Si $p - 1 \mid m$ entonces $k^m \equiv 1$ (mód p) para $1 \leq k \leq p - 1$, luego

$$S_m(p) = \sum_{k=1}^{p-1} k^m \equiv p - 1 \equiv -1 \text{ (mód } p),$$

mientras que si $p - 1 \nmid m$, tomando una raíz primitiva g módulo p tenemos

$$S_m(p) = \sum_{k=1}^{p-1} k^m \equiv \sum_{r=0}^{p-2} g^{mr} = \frac{g^{(p-1)m} - 1}{g^m - 1} \equiv 0 \text{ (mód } p),$$

pues $p \nmid g^m - 1$ pero $p \mid g^{(p-1)m} - 1$.

Resulta, pues, que $pB_m \equiv -1, 0$ (mód p) según si $p - 1$ divide o no a m. En el primer caso $p \nmid pB_m$, luego $p \mid D_m$. En el segundo $p \mid pB_m$, luego $p \nmid D_m$. ∎

Más aún, en la prueba hemos visto que todos los términos del sumatorio que aparece en la fórmula (8.4) son p-enteros. Si además suponemos que $m \leq p - 1$ entonces $p - 1 \nmid k$, para todo $k < m$, luego $p \mid pB_k$ y todos los términos del sumatorio son múltiplos de p^2. Por lo tanto tenemos:

Teorema 8.5 *Si p es un primo, m es par y $m \leq p - 1$, entonces*

$$pB_m \equiv S_m(p) \text{ (mód } p^2).$$

Esto nos permite reformular como sigue el teorema 8.3:

Teorema 8.6 *Sea p un primo impar. Entonces p no divide al primer factor del número de clases del cuerpo ciclotómico p-ésimo si y sólo si p no divide a los numeradores de los números de Bernoulli $B_2, B_4, \ldots, B_{p-3}$.*

Demostración: La condición equivalente que proporciona el teorema 8.3 es que p^2 no ha de dividir a las sumas $S_m(p)$ para $m = 2, 4, \ldots, p - 3$. Por el teorema anterior esto equivale a que p^2 no divida a pB_m en el anillo de los p-enteros, y como p no divide a los denominadores de los B_m, esto equivale a que p no divida a los numeradores de los B_m. ∎

8.3 El segundo factor del número de clases

El segundo factor del número de clases contiene el regulador del cuerpo ciclotómico, lo que impide encontrar una expresión sencilla para calcularlo. Sin embargo su relación con las unidades a través del regulador nos dará información vital para probar que la condición A de la definición de primo regular implica la condición B.

Para desarrollarlo hemos de evaluar en 1 las funciones L correspondientes a los caracteres pares χ^{2r}, para lo que empleamos de nuevo los teoremas 4.32 y 4.36:

$$|L(1,\chi^{2r})| = \frac{|G(\chi^{2r})|}{p}\left|\sum_{k=0}^{p-2}\bar{\chi}^{2r}(g^k)\log|1-\omega^{g^k}|\right| = \frac{1}{\sqrt{p}}\left|\sum_{k=0}^{p-2}\zeta^{2rk}\log|1-\omega^{g^k}|\right|.$$

En la última serie cada sumando se repite dos veces. En efecto, para cada $0 \le k < m$ se cumple que

$$\zeta^{2r(m+k)}\log|1-\omega^{g^{m+k}}| = \zeta^{2rk}\log|1-\omega^{-g^k}| = \zeta^{2rk}\log|1-\omega^{g^s}|,$$

(el último paso es porque $1-\omega^{-g^k}$ y $1-\omega^{g^k}$ son conjugados).

Así pues,

$$|L(1,\chi^{2r})| = \frac{2}{\sqrt{p}}\left|\sum_{k=0}^{m-1}\zeta^{2rk}\log|1-\omega^{g^k}|\right|,$$

lo que nos lleva a esta expresión para el segundo factor:

$$h_2 = \frac{1}{R'}\prod_{r=1}^{m-1}\left|\sum_{k=0}^{m-1}\zeta^{2rk}\log|1-\omega^{g^k}|\right|.$$

Al igual que hemos hecho con el primer factor, vamos a aplicar el teorema 8.1 para obtener una expresión mucho más simple. Por abreviar llamaremos $a_k = \log|1-\omega^{g^k}|$. Como ya hemos comentado, $1-\omega^{g^{m+k}}$ es el conjugado de $1-\omega^{g^k}$, por lo que a_k sólo depende del resto de k módulo m.

Consideramos de nuevo $G = \mathbb{Z}/m\mathbb{Z}$ y el carácter $\psi(k) = \zeta^{2k}$, de modo que

$$h_2 = \frac{1}{R'}\left|\prod_{r=1}^{m-1}\sum_{k\in G}a_k\,\psi^r(k)\right|. \tag{8.5}$$

No podemos aplicar 8.1 porque falta el carácter principal. El factor que le correspondería sería $a_0 + \cdots + a_{m-1}$. Vamos a calcularlo. Factorizando el polinomio ciclotómico obtenemos que $p = (1-\omega)\cdots(1-\omega^{p-1})$. Tomando módulos y teniendo en cuenta que g^k recorre todas las clases de U_p cuando k varía entre 0 y $p-1$ resulta que $|1-\omega^{g^0}|\cdots|1-\omega^{g^{p-1}}| = p$. Usando una vez más que $|1-\omega^{g^{k+m}}| = |1-\omega^{g^k}|$ queda

$$\prod_{k=0}^{m-1}|1-\omega^{g^k}|^2 = p.$$

Por último, tomando logaritmos:

$$a_0 + \cdots + a_{m-1} = \log \sqrt{p}.$$

Ahora multiplicamos y dividimos por $\log \sqrt{p}$ en (8.5) de modo que ya aparecen todos los caracteres de G:

$$h_2 = \frac{1}{R' \log \sqrt{p}} \left| \prod_{r=0}^{m-1} \sum_{k \in G} a_k \, \psi^r(k) \right|.$$

El teorema 8.1 nos permite concluir que

$$h_2 = \frac{1}{R' \log \sqrt{p}} \, |\det(a_{i+j})|,$$

donde i, j varían de 0 a $m-1$.

La primera fila de la matriz (a_{i+j}) (para $i = 0$) es $(a_0, a_1, \ldots, a_{m-1})$, y las demás son permutaciones cíclicas de ésta. Si sumamos todas las columnas a una fija obtenemos una columna con todos los coeficientes iguales a $\log \sqrt{p}$. Esta constante se simplifica con la que aparece en el denominador y queda una columna de unos. Restamos la primera fila a las otras filas y desarrollamos el determinante por la columna fijada. El resultado es que

$$h_2 = \frac{|A|}{R'},$$

donde A es cualquiera de los menores de orden $m-1$ de la matriz $B = (a_{i+j} - a_j)$, donde i varía entre 1 y $m-1$ y j varía entre 0 y $m-1$.

Vamos a calcular los coeficientes $a_{i+j} - a_j$. En principio tenemos

$$a_{i+j} - a_j = \log \frac{|1 - \omega^{g^{i+j}}|}{|1 - \omega^{g^j}|}.$$

Para simplificar esta expresión consideramos el número

$$\rho = -\omega^{(p+1)/2} = \cos(\pi/p) + i \operatorname{sen}(\pi/p) \in K.$$

Entonces $\omega = \rho^2$, de donde

$$\frac{1 - \omega^k}{1 - \omega} = \frac{1 - \rho^{2k}}{1 - \rho^2} = \rho^{k-1} \, \frac{\rho^k - \rho^{-k}}{\rho - \rho^{-1}} = \rho^{k-1} \, \frac{\operatorname{sen}(k\pi/p)}{\operatorname{sen}(\pi/p)}.$$

Si $p \nmid k$ entonces $1-\omega$ y $1-\omega^k$ son asociados, luego el término de la izquierda es una unidad de K. Obviamente ρ también lo es, luego los números

$$\theta_k = \frac{\operatorname{sen}(k\pi/p)}{\operatorname{sen}(\pi/p)} = \rho^{1-k} \frac{1 - \omega^k}{1 - \omega}, \qquad \text{para } p \nmid k, \tag{8.6}$$

son también unidades de K. De hecho son reales y positivas, luego son unidades de K'.

Sea $\bar{\imath}$ el valor absoluto del menor resto módulo p de g^i situado en $[-m, m]$. Entonces

$$\frac{1-\omega^{g^i}}{1-\omega} = \rho^{g^i-1}\theta_{g^i} = \pm\rho^{g^i-1}\theta_{\bar{\imath}}.$$

Los números ω, ω^g, ..., $\omega^{g^{m-1}}$ son no conjugados dos a dos (el conjugado de ω^{g^i} es $\omega^{g^{i+m}}$). Por lo tanto los automorfismos de K dados por $\sigma_j(\omega) = \omega^{g^j}$ ($j = 0, \ldots, m-1$) son no conjugados dos a dos. Aplicamos σ_j y queda

$$\frac{1-\omega^{g^{i+j}}}{1-\omega^{g^j}} = \pm\sigma_j(\rho)^{g^i-1}\sigma_j(\theta_{\bar{\imath}}).$$

Tomando módulos y logaritmos:

$$a_{i+j} - a_j = \log|\sigma_j(\theta_{\bar{\imath}})|.$$

Ahora veamos que cuando i varía entre 1 y $m-1$, entonces $\bar{\imath}$ varía entre 2 y m. Para ello observamos que si $g^i \equiv \pm g^j$ (mód p) con $1 \le i \le j \le m-1$ entonces $g^{j-i} \equiv \pm 1$ (mód p) y $0 \le j-i \le (p-3)/2$, pero esto sólo es posible si $i = j$. Por lo tanto los valores de $\bar{\imath}$ cuando i varía entre 1 y $m-1$ son distintos dos a dos. Por definición $\bar{\imath}$ varía entre 1 y m, pero $\pm g^i \equiv 1$ (mód p) es imposible cuando i varía entre 1 y $m-1$ (± 1 se obtiene elevando g a 0 y a m). Así pues, $\bar{\imath}$ varía entre 2 y m, y como ha de tomar $m-2$ valores distintos, los toma todos.

Llamemos $C = \big(\log|\sigma_j(\theta_i)|\big)$, para $2 \le i \le m$, $0 \le j \le m-1$. Acabamos de probar que las columnas de C son salvo el orden las mismas que las de la matriz $B = (a_{i+j} - a_j)$. Por lo tanto el valor de $\det A$ que buscamos es (salvo signo, que no importa) cualquiera de los menores de orden $m-1$ de la matriz C.

Sea ahora $\epsilon_1, \ldots, \epsilon_{m-1}$ un sistema fundamental de unidades de K'. Podemos tomarlas todas positivas. Cada unidad θ_i se expresará como

$$\theta_i = \prod_{k=1}^{m-1} \epsilon_k^{c_{ik}},$$

para ciertos enteros c_{ik} (no hay que anteponer un signo negativo porque $\theta_i > 0$).

Entonces

$$\log|\sigma_j(\theta_i)| = \sum_{k=1}^{m-1} c_{ik}\log|\sigma_j(\epsilon_k)|.$$

Esto significa que C es el producto de la matriz (c_{ik}) por $(\log|\sigma_j(\epsilon_k)|)$ o, más precisamente, que cualquier menor de orden $m-1$ de C es el producto de (c_{ik}) por el menor correspondiente de $(\log|\sigma_j(\epsilon_k)|)$. Tomando determinantes queda $|\det A| = |\det(c_{ik})|R'$, luego $h_2 = |\det(c_{ik})|$.

Pero (c_{ik}) es la matriz de las coordenadas de las unidades θ_i en la base $\epsilon_1, \ldots, \epsilon_{m-1}$. Éstas últimas son una base del grupo de las unidades reales y positivas de K, luego las primeras son una base de un cierto subgrupo. Según el teorema [Al 6.15], el determinante de la matriz que relaciona ambas bases es precisamente el índice del subgrupo. En resumen, hemos probado el teorema siguiente:

Teorema 8.7 *El segundo factor del número de clases coincide con el índice en el grupo de las unidades reales y positivas de K del subgrupo generado por las unidades*

$$\theta_k = \frac{\operatorname{sen}(k\pi/p)}{\operatorname{sen}(\pi/p)}, \qquad \text{para } k = 2, \dots, m.$$

En términos equivalentes, podemos hablar del índice del grupo generado por las unidades θ_i en el grupo de las unidades de K' (con ello añadimos un factor C_2 a los dos grupos indicados en el teorema). En particular, si $h_2 = 1$ resulta que las unidades θ_i son un sistema fundamental de unidades de K.

Ejemplo Si $p = 7$ sabemos que $h = 1$ y por lo tanto también $h_2 = 1$. Esto implica que un sistema fundamental de unidades está constituido por

$$\begin{aligned} \theta_2 &= \rho^{-1}\frac{1-\omega^2}{1-\omega} = -\omega^{-4}(1+\omega) = -\omega^3 - \omega^4 = -\eta_3 = 1 + \eta_1 + \eta_2, \\ \theta_3 &= \rho^{-2}\frac{1-\omega^3}{1-\omega} = -\omega^{-1}(\omega^2 + \omega + 1) = \omega^6 + \omega + 1 = 1 + \eta_1. \end{aligned}$$

Si llamamos $\eta = \eta_1$ (y entonces $\eta_2 = \eta^2 - 2$) tenemos que $\theta_2 = \eta^2 + \eta - 1$ y $\theta_3 = 1 + \eta$. ∎

Ejercicio: En la sección 3.5 probamos que un sistema fundamental de unidades para $p = 7$ era η, $1 + \eta$. Calcular la representación logarítmica de θ_2 y deducir de ella que $\theta_2 = \eta^{-1}(1 + \eta)$.

El paso siguiente para llegar a la caracterización de los primos regulares es estudiar bajo qué condiciones podemos garantizar que p no divide a h_2. El punto de arranque será el siguiente: si $p \mid h_2$, entonces el grupo cociente determinado por los grupos de unidades considerados en el teorema anterior tiene un elemento de orden p, es decir, existe una unidad $\epsilon > 0$ en K tal que

$$\epsilon^p = \prod_{k=2}^{m} \theta_k^{c_k}, \tag{8.7}$$

para ciertos enteros c_k, pero tal que ϵ no es de esta forma.

A su vez, que ϵ no sea de esta forma equivale a que algún c_k no sea divisible entre p, pues si dos unidades positivas ϵ y δ cumplen que $\epsilon^p = \delta^p$, entonces ϵ/δ es una raíz p-ésima de la unidad positiva, lo que sólo es posible si $\epsilon = \delta$.

Si logramos probar que cuando ϵ cumple (8.7) todos los exponentes c_k son múltiplos de p, tendremos garantizado que p no divide divide a h_2. La idea de la demostración es tomar logaritmos para convertir la igualdad anterior en una ecuación lineal en $\log \theta_k$ y probar una cierta independencia lineal de estos logaritmos que nos dé las divisibilidades (algo análogo a cuando decimos que si $p \mid a + b\sqrt{2}$ entonces $p \mid a$ y $p \mid b$).

Sin embargo este argumento depende fuertemente de propiedades algebraicas y es completamente inviable usando logaritmos habituales. En su lugar

tendremos que usar logaritmos p-ádicos. Kummer no conocía los números p-ádicos cuando realizó estos cálculos, pero éstos estaban implícitos en su trabajo y fueron definidos poco después por Hensel. En realidad Kummer trabajó con derivadas logarítmicas. La idea es que el cuerpo ciclotómico se puede identificar con el cociente de $\mathbb{Q}[x]$ sobre el ideal generado por el polinomio ciclotómico. La derivada logarítmica de un polinomio $p(x)$ es $p'(x)/p(x)$.

8.4 Numeros p-ádicos ciclotómicos

Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de grado p. De acuerdo con el teorema [Al 11.13], la factorización de p en $\mathbb{Z}[\omega]$ es $p = \mathfrak{p}^{p-1}$. En particular $f(\mathfrak{p}/p) = 1$. El teorema 5.16 nos da el isomorfismo $\mathcal{O}_\mathfrak{p}/\mathfrak{p} \cong \mathbb{Z}[\omega]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. En particular todo entero $\mathfrak{p}$-ádico es congruente módulo $\mathfrak{p}$ con un entero racional. Según 5.22 tenemos que $|K_\mathfrak{p} : \mathbb{Q}_p| = p - 1$.

Teorema 8.8 *Sea π un primo de $K_\mathfrak{p}$. Entonces $\{1, \pi, \pi^2, \ldots, \pi^{p-2}\}$ es una base de $K_\mathfrak{p}$ sobre $\mathbb{Q}_p$ y también una base de $\mathcal{O}_\mathfrak{p}$ sobre $\mathbb{Z}_p$.*

Demostración: Veamos que todo $\alpha \in \mathcal{O}_\mathfrak{p}$ se expresa como combinación lineal de estos números con coeficientes en $\mathbb{Z}_p$.

Teniendo en cuenta el teorema 5.18, α se puede expresar como

$$\alpha = a_{0,0} + a_{0,1}\pi + \cdots + a_{0,p-2}\pi^{p-2} + \beta\pi^{p-1},$$

donde $0 \le a_{0,i} \le p-1$ y $\beta \in \mathcal{O}_\mathfrak{p}$.

Puesto que $p = \epsilon\pi^{p-1}$, para cierta unidad ϵ, tenemos de hecho que

$$\alpha = a_{0,0} + a_{0,1}\pi + \cdots + a_{0,p-2}\pi^{p-2} + \gamma_1 p,$$

con $\gamma_1 \in \mathcal{O}_\mathfrak{p}$.

Igualmente $\gamma_1 = a_{1,0} + a_{1,1}\pi + \cdots + a_{1,p-2}\pi^{p-2} + \gamma_2 p$, con lo que

$$\alpha = (a_{0,0} + a_{1,0}p) + (a_{0,1} + a_{1,1}p)\pi + \cdots + (a_{0,p-2} + a_{1,p-2}p)\pi^{p-2} + \gamma_2 p^2.$$

Tras $n+1$ pasos obtenemos

$$\alpha = \left(\sum_{i=0}^{n} a_{i,0}p^i\right) + \left(\sum_{i=0}^{n} a_{i,1}p^i\right)\pi + \cdots + \left(\sum_{i=0}^{n} a_{i,p-2}p^i\right)\pi^{p-2} + \gamma_n p^n.$$

Es obvio que todas las series convergen y $\gamma_n p^n$ tiende a 0, luego

$$\alpha = \left(\sum_{i=0}^{\infty} a_{i,0}p^i\right) + \left(\sum_{i=0}^{\infty} a_{i,1}p^i\right)\pi + \cdots + \left(\sum_{i=0}^{\infty} a_{i,p-2}p^i\right)\pi^{p-2}.$$

Esto prueba que $\{1, \pi, \pi^2, \ldots, \pi^{p-2}\}$ es un generador de $\mathcal{O}_\mathfrak{p}$ sobre $\mathbb{Z}_p$, de donde se sigue que también es un generador de $K_\mathfrak{p}$ sobre $\mathbb{Q}_p$, pero como el grado de la extensión es $p-1$, se trata de una base, luego el conjunto es linealmente independiente sobre $\mathbb{Q}_p$, luego también sobre $\mathbb{Z}_p$. ∎

Como $K = \mathbb{Q}(\omega)$, el teorema 5.27 nos da que $K_\mathfrak{p} = \mathbb{Q}_p(\omega)$, luego $K_\mathfrak{p}$ es la extensión ciclotómica de orden p de $\mathbb{Q}_p$. Además tiene grado $p-1$, luego el grupo de Galois es cíclico de orden $p-1$, todas las raíces de la unidad distintas de 1 son conjugadas y los $\mathbb{Q}_p$-automorfismos $K_\mathfrak{p}$ están determinados por $\sigma_i(\omega) = \omega^i$, para $i = 1, \ldots, p-1$. A su vez esto implica que los $\mathbb{Q}_p$-automorfismos de $K_\mathfrak{p}$ son extensiones de los $\mathbb{Q}$-automorfismos de K, y por consiguiente la norma y la traza de $K_\mathfrak{p}/\mathbb{Q}_p$ extienden también a las de $K/\mathbb{Q}$.

Dado un automorfismo σ y un $\alpha \in \mathcal{O}_\mathfrak{p}$, por definición $v_\mathfrak{p}\big(\sigma(\alpha)\big)$ es la multiplicidad de π en $\sigma(\alpha)$, que coincide con la multiplicidad de $\sigma(\pi)$ en $\sigma(\alpha)$ (pues $\sigma(\pi)$ también es primo y todos los primos de $K_\mathfrak{p}$ son asociados), que a su vez coincide con la multiplicidad de π en α. Es decir, $v_\mathfrak{p}\big(\sigma(\alpha)\big) = v_\mathfrak{p}(\alpha)$. De aquí se sigue esto mismo para todo $\alpha \in K_\mathfrak{p}$, luego $|\sigma(\alpha)|_\mathfrak{p} = |\alpha|_\mathfrak{p}$, es decir, que los automorfismos son isometrías. En particular son homeomorfismos.

Esto implica que un $\mathbb{Q}_p$-automorfismo de $K_\mathfrak{p}$ deja fijos los elementos de un subcuerpo L de K si y sólo si deja fijos a los elementos de la clausura de L en $K_\mathfrak{p}$. Teniendo en cuenta el teorema de Galois resulta que la aplicación que a cada subcuerpo L de K le asigna su clausura en $K_\mathfrak{p}$ es una biyección entre los subcuerpos de K y los subcuerpos de $K_\mathfrak{p}$ que contienen a $\mathbb{Q}_p$. Además esta biyección conserva los grados.

En particular el cuerpo $\overline{K'} = \overline{K \cap \mathbb{R}}$ tiene grado $m = (p-1)/2$ sobre $\mathbb{Q}_p$. A los elementos de este cuerpo los llamaremos *números $\mathfrak{p}$-ádicos reales.*

Finalmente notamos que según el teorema 5.57 tenemos definida una función logaritmo exactamente sobre los enteros $\mathfrak{p}$-ádicos de la forma $\epsilon = 1 + x$, con $v_\mathfrak{p}(x) \geq 1$, es decir, en las unidades $\epsilon \equiv 1 \pmod{\mathfrak{p}}$. A estas unidades las llamaremos *unidades principales.* Sin embargo, el logaritmo sólo es biyectivo restringido a un dominio menor, a saber, sobre el conjunto de las unidades que cumplen $\epsilon \equiv 1 \pmod{\mathfrak{p}^2}$. Si ϵ es una unidad de este tipo, entonces el teorema 5.58 garantiza además que $\log(\epsilon)$ es un entero múltiplo de $\mathfrak{p}^2$ (en efecto,con la notación de la sección anterior, tenemos $e = p-1$ y $\kappa = 2$).

Ejercicio: Probar que $\log \omega = 0$.

Recordemos que nuestra intención es tomar logaritmos en la ecuación (8.7), pero sucede que las unidades involucradas no tienen por qué ser principales. Ahora bien, puesto que $\mathcal{O}_\mathfrak{p}/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$, es claro que $\epsilon^{p-1} \equiv 1 \pmod{\mathfrak{p}}$ para toda unidad $\mathfrak{p}$-ádica ϵ, o sea ϵ^{p-1} es siempre una unidad principal. Podemos, pues, elevar la ecuación a $p-1$ y tomar logaritmos:

$$p \log \epsilon^{p-1} = \sum_{k=2}^{m} c_k \log \theta_k^{p-1}. \tag{8.8}$$

Ahora observamos que las unidades que aparecen son enteros ciclotómicos reales, luego los logaritmos son números $\mathfrak{p}$-ádicos reales (el logaritmo es una serie de potencias y cada suma parcial está en K', luego la suma está en la clausura de este cuerpo). No es evidente, pero también probaremos que son enteros.

Si demostráramos que los números $\log \theta_k^{p-1}$ forman una $\mathbb{Z}_p$-base del anillo de los enteros $\mathfrak{p}$-ádicos reales, necesariamente los números c_k/p serían enteros

p-ádicos, con lo que todos los c_k serían múltiplos de p, que es lo que queremos probar. No obstante es fácil ver que dicho anillo tiene rango m, mientras que sólo tenemos $m-1$ logaritmos $\log \theta_k^{p-1}$. Por lo tanto hemos de refinar nuestro plan.

Ahora bien, si σ es un automorfismo de $K_\mathfrak{p}$ y ϵ es una unidad principal, es obvio que $\sigma(\epsilon)$ es también una unidad principal (pues $v_\mathfrak{p}(\sigma(\epsilon)-1) = v_\mathfrak{p}\big(\epsilon-1)\big)$, y por la continuidad $\sigma(\log\epsilon) = \log\sigma(\epsilon)$, luego

$$\mathrm{Tr}(\log\epsilon) = \sum_\sigma \sigma(\log\epsilon) = \sum_\sigma \log\sigma(\epsilon) = \log\prod_\sigma \sigma(\epsilon) = \log \mathrm{N}(\epsilon).$$

Si además ϵ es una unidad de K, como es el caso, entonces $\mathrm{N}(\epsilon) = 1$, luego la traza de $\log\epsilon$ es nula. Sea V el conjunto de los números $\mathfrak{p}$-ádicos reales de traza nula. Claramente V es un espacio vectorial de dimensión $m-1$ sobre $\mathbb{Q}_p$ y si ϵ es una unidad real de K tenemos que $\log\epsilon^{p-1} \in V$.

Nuestra intención es probar que los números $\log\theta_k^{p-1}$ forman una $\mathbb{Z}_p$-base del módulo formado por los enteros de V. Para ello buscaremos una base de este módulo y estudiaremos si el determinante de la matriz de coordenadas de los logaritmos en dicha base es una unidad de $\mathbb{Z}_p$. Esta base la obtendremos a partir de la que nos proporciona el teorema 8.8, pero primero escogeremos un primo π adecuado.

Veamos que existe un único primo $\pi \in \mathcal{O}_\mathfrak{p}$ tal que

$$p = -\pi^{p-1} \quad \text{y} \quad \pi \equiv 1-\omega \ (\text{mód } \mathfrak{p}^2). \tag{8.9}$$

Factorizando el polinomio ciclotómico y evaluando en 1 tenemos que

$$p = (1-\omega)(1-\omega^2)\cdots(1-\omega^{p-1}),$$

de donde

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

Teniendo en cuenta la expresión de la izquierda, este número es un entero $\mathfrak{p}$-ádico. Tomamos congruencias módulo $\mathfrak{p}$ en $\mathcal{O}_\mathfrak{p}$.

$$\alpha = \frac{-p}{(1-\omega)^{p-1}} \equiv -2\cdot 3\cdots(p-1) \equiv 1 \ (\text{mód } \mathfrak{p}),$$

donde hemos usado el teorema de Wilson:[1] $(p-1)! \equiv -1 \ (\text{mód } p)$.

Aplicamos el teorema 5.48 al polinomio $f(x) = x^{p-1} - \alpha$. Tenemos que

$$f(1) \equiv 0 \ (\text{mód } \mathfrak{p}) \quad \text{y} \quad f'(1) = p-1 \not\equiv 0 \ (\text{mód } \mathfrak{p}).$$

Por consiguiente existe un entero $\mathfrak{p}$-ádico γ tal que $\gamma^{p-1} = -p/(1-\omega)^{p-1}$ y $\gamma \equiv 1 \ (\text{mód } \mathfrak{p})$.

[1] La prueba es elemental: el polinomio $x^{p-1}-1$ tiene por raíces a todos los elementos no nulos de $\mathbb{Z}/p\mathbb{Z}$, luego su término independiente -1 es el producto de todos ellos.

Por la segunda condición, γ es una unidad $\mathfrak{p}$-ádica, luego $\pi = \gamma(1-\omega)$ es un primo. Claramente cumple la primera condición de (8.9) y $\pi - (1-\omega) = (\gamma-1)(1-\omega)$ es divisible entre $\mathfrak{p}^2$, luego también cumple la segunda.

Para probar la unicidad observamos que si un primo ρ cumple (8.9) entonces $(\rho/\pi)^{p-1} = 1$, luego $\rho = \zeta\pi$, para una cierta raíz $(p-1)$-ésima de la unidad ζ. Puesto que $\zeta\pi \equiv \pi \pmod{\mathfrak{p}^2}$, resulta que $\zeta \equiv 1 \pmod{\mathfrak{p}}$. Si fuera $\zeta \neq 1$ entonces $x - \zeta$ dividiría al polinomio $x^{p-2} + x^{p-3} + \cdots + x + 1$, y evaluando en 1 tendríamos $1 - \zeta \mid p - 1$, luego $\mathfrak{p} \mid p - 1$, lo cual es imposible. Por consiguiente $\zeta = 1$ y $\rho = \pi$. ∎

Veamos ahora las ventajas del primo que acabamos de construir. Sea σ el automorfismo de $K_\mathfrak{p}$ de orden 2, esto es, el dado por $\sigma(\omega) = \omega^{-1}$. Puesto que π y $\sigma(\pi)$ son ambos raíces del polinomio $x^{p-1} + p$, es claro que $\sigma(\pi) = \zeta\pi$, para cierta raíz $(p-1)$-ésima de la unidad ζ.

Ahora bien, sucede que $\zeta \in \mathbb{Q}_p$, pues si $\mathfrak{P}$ es un divisor de p en el cuerpo ciclotómico $\mathbb{Q}(\zeta)$, el teorema 2.38 nos da que $e(\mathfrak{P}/p) = f(\mathfrak{P}/p) = 1$, luego los teoremas 5.22 y 5.27 implican que $|\mathbb{Q}_p(\zeta) : \mathbb{Q}_p| = 1$.

Por lo tanto, aplicando σ de nuevo queda que $\pi = \zeta^2\pi$, con lo que $\zeta^2 = 1$, o sea, $\zeta = \pm 1$. No puede ser $\zeta = 1$ porque entonces $\sigma(\pi) = \pi$ y σ sería la identidad (por 8.8). Consecuentemente $\sigma(\pi) = -\pi$.

Los números $\mathfrak{p}$-ádicos reales son precisamente los números fijados por σ, pero si expresamos un número arbitrario de $K_\mathfrak{p}$ como combinación lineal de $1, \pi, \ldots, \pi^{p-2}$, observamos que los números fijados por σ son los que tienen nulas las coordenadas asociadas a las potencias impares, luego una base del cuerpo de los números $\mathfrak{p}$-ádicos reales es $\{1, \pi^2, \pi^4, \ldots, \pi^{p-2}\}$, luego este cuerpo es $\mathbb{Q}_p(\pi^2)$.

A su vez de aquí se deriva otra consecuencia notable: Si ϵ es una unidad principal real, entonces es de la forma $\epsilon = a_0 + a_2\pi^2 + \cdots + a_{p-2}\pi^{p-2}$, donde los coeficientes son enteros p-ádicos por 8.8. Además $1 \equiv \epsilon \equiv a_0 \pmod{\mathfrak{p}}$, luego

$$1 \leq v_\mathfrak{p}(a_0 - 1) = (p-1)v_p(a_0 - 1),$$

con lo que en realidad $2 \leq p - 1 \leq v_\mathfrak{p}(a_0 - 1)$ y de aquí que $\epsilon \equiv 1 \pmod{\mathfrak{p}^2}$.

Esto significa que las unidades principales reales están en realidad en el dominio donde el logaritmo es inyectivo, y en particular el teorema 5.58 implica que el logaritmo de una unidad principal real es un entero $\mathfrak{p}$-ádico, que es uno de los resultados que necesitábamos. Recojámoslo en un teorema junto con otros hechos que hemos probado:

Teorema 8.9 *Si ϵ es una unidad ciclotómica real, entonces $\log \epsilon^{p-1}$ es un entero $\mathfrak{p}$-ádico real de traza nula. Más aún,*

$$\log \epsilon^{p-1} \equiv 0 \pmod{\mathfrak{p}^2}.$$

Ya tenemos una base para los números $\mathfrak{p}$-ádicos reales. Ahora hemos de quedarnos con los que tienen traza nula. Para ello calculamos $\mathrm{Tr}(\pi^i)$. Observar

que si ζ es una raíz de la unidad de orden $p-1$ entonces los números $\zeta^j\pi$ para $j = 0, \ldots, p-2$ son todos raíces del polinomio $x^{p-1}+p$. Por lo tanto cuando σ recorre los $\mathbb{Q}_p$-automorfismos de $K_\mathfrak{p}$ tenemos que $\sigma(\pi)$ recorre los números $\zeta^j\pi$ y $\sigma(\pi^i)$ recorre los números $\zeta^{ij}\pi^i$, es decir

$$\mathrm{Tr}(\pi^i) = \sum_{j=0}^{p-1} \zeta^{ij}\pi^i.$$

Ahora las relaciones de ortogonalidad de caracteres implican que $\mathrm{Tr}(\pi^i) = 0$ para $i = 1, \ldots, p-2$, mientras que obviamente $\mathrm{Tr}(1) = p-1$. Por consiguiente la traza de un número $\mathfrak{p}$-ádico real arbitrario es

$$\mathrm{Tr}(a_0 + a_2\pi^2 + \cdots + a_{p-2}\pi^{p-2}) = (p-1)a_0.$$

Con esto tenemos probado el teorema siguiente:

Teorema 8.10 *Si π es un primo $\mathfrak{p}$-ádico que cumple las condiciones* (8.9)*, los números $\pi^2, \pi^4, \ldots, \pi^{p-2}$ son una $\mathbb{Q}_p$-base del espacio vectorial V de los números $\mathfrak{p}$-ádicos reales de traza nula, así como una $\mathbb{Z}_p$-base del módulo de los enteros de V.*

La última afirmación es consecuencia inmediata del teorema 8.8.

8.5 La caracterización de los primos regulares

Estudiamos ahora la divisibilidad del segundo factor del número de clases entre el primo p. Por el teorema 8.9 sabemos que los números $\log\theta_k^{p-1}$ son enteros $\mathfrak{p}$-ádicos de traza nula, luego por 8.10 se pueden expresar en la forma

$$\log\theta_k^{p-1} = \sum_{i=1}^{m-1} b_{ki}\pi^{2i}, \quad 2 \le k \le m, \tag{8.10}$$

donde los coeficientes b_{ki} son enteros p-ádicos.

Según ya hemos explicado, queremos probar que estos números son una base del módulo de todos los enteros $\mathfrak{p}$-ádicos de traza nula, lo cual equivale a que el determinante de la matriz (b_{ki}) sea una unidad de $\mathbb{Z}_p$, es decir, que no sea divisible entre p.

Observemos que si $\alpha \in V$ es un entero múltiplo de p, entonces α/p es un entero $\mathfrak{p}$-ádico obviamente real y que sigue cumpliendo $\mathrm{Tr}(\alpha/p) = \mathrm{Tr}(\alpha)/p = 0$, luego $\alpha/p \in V$. Esto implica que las coordenadas de α en la base $\{\pi^{2i}\}$ serán las de α/p (que son enteras) multiplicadas por p. En resumen, los enteros de V son múltiplos de p si y sólo si sus coordenadas son múltiplos de p. A su vez de aquí deducimos que si dos enteros de V son congruentes módulo p, sus coordenadas en la base $\{\pi^{2i}\}$ también lo son.

Como consecuencia, si sustituimos cada $\log\theta_k^{p-1}$ por otro entero de V congruente con él módulo p, el determinante de la matriz de coordenadas correspondiente será congruente módulo p con el de (b_{ki}), luego nos servirá igualmente para determinar si éste es o no múltiplo de p. Esto nos permite truncar las series de potencias que definen los logaritmos.

Consideremos el polinomio

$$L(1+x) = x - \frac{x^2}{2} + \cdots + (-1)^{p-2}\frac{x^{p-1}}{p-1}.$$

Si $n \geq p$ y $v_{\mathfrak{p}}(\alpha) \geq 2$ entonces

$$\begin{aligned} v_{\mathfrak{p}}\left(\frac{\alpha^n}{n}\right) &\geq 2n - v_{\mathfrak{p}}(n) \geq 2n - (p-1)\frac{\log n}{\log p} \\ &\geq p + (n-p) + n - \frac{n(p-1)}{n-1}\frac{\log n}{\log p} \\ &\geq p + (n-p) + \frac{(p-1)n}{\log p}\left(\frac{\log p}{p-1} - \frac{\log n}{n-1}\right) \geq p, \end{aligned}$$

(donde usamos que la función $t/(t-1)$ es monótona decreciente para $t \geq 2$).

Esto significa que la diferencia entre $\log(1+\alpha)$ y $L(1+\alpha)$ es una suma de múltiplos de π^p, es decir, $\log(1+\alpha) \equiv L(1+\alpha) \pmod{\pi^p}$. Esto es aplicable a las unidades principales reales, luego

$$\log(\theta_k^{p-1}) \equiv L(\theta_k^{p-1}) \pmod{\pi^p}. \tag{8.11}$$

Comenzaremos probando que los logaritmos truncados tienen las mismas propiedades algebraicas que los logaritmos usuales si trabajamos módulo π^p. Usaremos también la exponencial truncada

$$E(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^{p-1}}{(p-1)!}. \tag{8.12}$$

Notemos que si $\epsilon \equiv 1 \pmod{\pi}$ entonces $L(\epsilon) \equiv 0 \pmod{\pi}$ y, recíprocamente, si $\alpha \equiv 0 \pmod{\pi}$ entonces $E(\alpha) \equiv 1 \pmod{\pi}$. Veamos ahora otros hechos elementales:

Teorema 8.11 *Se cumplen las propiedades siguientes:*

1. *Si* $\epsilon \equiv 1 \pmod{\pi}$ *entonces* $E(L(\epsilon)) \equiv \epsilon \pmod{\pi^p}$.
2. *Si* $\alpha \equiv 0 \pmod{\pi}$ *entonces* $L(E(\alpha)) \equiv \alpha \pmod{\pi^p}$.
3. *Si* $\alpha_1 \equiv \alpha_2 \equiv 0 \pmod{\pi}$, *entonces*

$$E(\alpha_1 + \alpha_2) \equiv E(\alpha_1)E(\alpha_2) \pmod{\pi^p}.$$

4. *Si* $\epsilon_1 \equiv \epsilon_2 \equiv 1 \pmod{\pi}$, *entonces*

$$L(\epsilon_1\epsilon_2) \equiv L(\epsilon_1) + L(\epsilon_2) \pmod{\pi^p}.$$

Demostración: Consideramos la igualdad de series de potencias formales $\exp(\log(1+x)) = 1+x$. Un examen de la definición de composición de series

formales muestra que el coeficiente de x^k en la composición depende únicamente de los coeficientes de grado menor o igual que k de las series compuestas. Por lo tanto, el polinomio $E(L(1+x))$ coincide con la serie $1+x$ hasta el término de grado $p-1$, es decir, $E(L(1+x)) = 1+x+p(x)$, donde $p(x)$ es un polinomio de grado mayor o igual que p, y ciertamente tiene coeficientes enteros p-ádicos. Por consiguiente se cumple la primera relación.

La segunda relación se prueba razonando del mismo modo con la composición de series $\log\big(1+(\exp(x)-1)\big) = x$.

Es claro que

$$\frac{(x+y)^k}{k!} = \sum_{r=0}^{k} \frac{x^r}{r!}\frac{y^{k-r}}{(k-r)!}.$$

De aquí se sigue que $E(x+y) = E(x)+E(y)+G(x,y)$, donde $G(x,y)$ es el polinomio formado por la suma de los productos de monomios de $E(x)$ y $E(y)$ al menos uno de los cuales tiene grado mayor o igual que p. Claramente los coeficientes de G son enteros p–ádicos, luego se tiene la tercera propiedad.

La cuarta propiedad la deducimos de las anteriores:

$$\begin{aligned} L(\epsilon_1\epsilon_2) &\equiv L\big(E\big(L(\epsilon_1)\big)E\big(L(\epsilon_2)\big)\big) \equiv L\big(E\big(L(\epsilon_1)+L(\epsilon_2)\big)\big) \\ &\equiv L(\epsilon_1)+L(\epsilon_2) \text{ (mód } \pi^p). \end{aligned}$$

■

Además de estas propiedades, vamos a necesitar un hecho más delicado:

Teorema 8.12 *Si el primo π cumple* (8.9) *entonces*

$$E(\pi) \equiv \omega \text{ (mód } \pi^p) \quad y \quad L(\omega) \equiv \pi \text{ (mód } \pi^p).$$

Demostración: Probemos en primer lugar que

$$E(p)^p \equiv 1 \text{ (mód } \pi^{2p-1}). \tag{8.13}$$

Sea $E(x) = 1+xg(x)$, donde $g(x)$ es un polinomio con coeficientes enteros (p-ádicos). Entonces

$$E(x)^p = 1+\binom{p}{1}xg(x)+\cdots+\binom{p}{p-1}\big(xg(x)\big)^{p-1}+x^pg(x)^p = 1+ph(x)+x^pg(x)^p,$$

donde $h(x)$ tiene coeficientes enteros (notar que p divide a los números combinatorios).

En la prueba del teorema 8.11 hemos visto que $E(x)E(y) = E(xy)+G(x,y)$, donde $G(x,y)$ es un polinomio con coeficientes enteros (p-ádicos) con todos los términos de grado $\geq p$. Inductivamente se llega a que $E(x)^p = E(px)+x^pM(x)$, donde M tiene coeficientes enteros. Así pues,

$$1+ph(x)+x^pg(x)^p = E(px)+x^pM(x),$$

luego

$$ph(x) = \frac{px}{1!} + \frac{(px)^2}{2!} + \cdots + \frac{(px)^{p-1}}{(p-1)!} + x^p H(x), \tag{8.14}$$

donde $H(x) = M(x) - g(x)^p$ tiene coeficientes enteros. Despejando $x^p H(x)$ en (8.14) vemos que los coeficientes de $H(x)$ son todos múltiplos de p. Dividimos entre p y nos queda que

$$h(x) = x + \frac{px^2}{2!} + \cdots + \frac{p^{p-2}x^{p-1}}{(p-1)!} + x^p G(x),$$

donde $G(x)$ tiene coeficientes enteros. Hacemos $x = \pi$ y así vemos que

$$h(\pi) \equiv \pi \pmod{\pi^p}.$$

(tener presente que $\pi^{p-1} \mid p$). De aquí que $ph(\pi) \equiv p\pi \pmod{\pi^{2p-1}}$.

Por otro lado $g(\pi) \equiv 1 \pmod{\pi}$, luego

$$\pi^p \mid (g(\pi)-1)^p = g(\pi)^p - 1 + \sum_{k=1}^{p-1} \binom{p}{k} (-1)^{p-k} g(\pi)^k,$$

de donde $g(\pi)^p \equiv 1 \pmod{\pi^{p-1}}$ (pues p divide a los números combinatorios) y $\pi^p g(\pi)^p \equiv \pi^p \pmod{\pi^{2p-1}}$.

Reuniendo todo esto llegamos a que

$$E(\pi)^p \equiv 1 + ph(\pi) + \pi^p g(\pi)^p \equiv 1 + p\pi + \pi^p \equiv 1 \pmod{\pi^{2p-1}},$$

pues $p\pi + \pi^p = 0$ por (8.9).

Por definición de E y por (8.9) se cumple $E(\pi) \equiv 1 + \pi \equiv \omega \pmod{\pi^2}$. Sea $\omega^{-1}E(\pi) = 1 + \pi^2\gamma$, donde γ es un entero p-ádico. Elevando a p y usando (8.13) obtenemos

$$(1 + \pi^2\gamma)^p = 1 + \gamma \sum_{k=1}^{p} \binom{p}{k} \gamma^{k-1} \pi^{2k} \equiv 1 \pmod{\pi^{2p-1}}$$

El número que multiplica a γ es divisible exactamente entre π^{p+1} (pues el primer sumando es $p\pi^2$), luego $\gamma \equiv 0 \pmod{\pi^{p-2}}$.

Así pues, $\omega^{-1}E(\pi) = 1 + \pi^2\gamma \equiv 1 \pmod{\pi^p}$, lo que nos da la primera afirmación del enunciado. La segunda es consecuencia inmediata del teorema anterior. ∎

Con esto estamos en condiciones de calcular $L(\theta_k^{p-1})$. Teniendo en cuenta (8.6) vemos que

$$\theta_k^p = (1 + \omega + \cdots + \omega^{k-1})(-1)^{1-k}.$$

Por (8.9) tenemos que $\omega \equiv 1 \pmod{\pi}$, luego $1 + \omega + \cdots + \omega^{k-1} \equiv k \pmod{\pi}$, y usando una vez más que π^{p-1} divide a los números combinatorios,

$$(1 + \omega + \cdots + \omega^{k-1})^p \equiv k^p \equiv k \pmod{\pi^{p-1}}.$$

Así pues,

$$\begin{aligned}\theta_k^{p-1} &\equiv \theta_k^{-1}\, k\,(-1)^{1-k} \equiv k\,\frac{\omega-1}{\omega^k-1}\,(-\rho)^{k-1}\\ &= \frac{\omega-1}{\pi}\left(\frac{\omega^k-1}{k\pi}\right)^{-1}\omega^{(k-1)(p+1)/2}\ (\text{mód } \pi^{p-1}).\end{aligned}$$

Notar que todos los factores del último miembro son unidades principales. Ciertamente ω lo es, de $\pi \equiv \omega - 1$ (mód π^2) se sigue que $(\omega-1)/\pi$ también lo es, y el factor central lo es también por serlo θ_k^{p-1}.

Esto nos permite aplicar L y separar los factores por el teorema 8.11:

$$L(\theta_k^{p-1}) \equiv L\left(\frac{\omega-1}{\pi}\right) - L\left(\frac{\omega^k-1}{k\pi}\right) + \frac{k-1}{2}L(\omega)\ (\text{mód } \pi^{p-1}).$$

Por el teorema anterior y 8.11, $\omega^k \equiv E(k\pi)$ (mód π^p), de donde

$$\frac{\omega^k-1}{k\pi} \equiv \frac{E(k\pi)-1}{k\pi}\ (\text{mód } \pi^{p-1}).$$

Lo mismo es válido para $(\omega-1)/\pi$, con lo que

$$L(\theta_k^{p-1}) \equiv L\left(\frac{E(\pi)-1}{\pi}\right) - \frac{\pi}{2} - L\left(\frac{E(k\pi)-1}{k\pi}\right) + \frac{k\pi}{2}\ (\text{mód } \pi^{p-1}). \quad (8.15)$$

Esta expresión nos lleva a estudiar el polinomio

$$L\left(\frac{E(x)-1}{x}\right) - \frac{x}{2}.$$

Para ello consideramos la función

$$\log\left(\frac{\exp(x)-1}{x}\right) - \frac{x}{2} = \log(\exp(x)-1) - \log x - \frac{x}{2}. \quad (8.16)$$

Si la consideramos como función de variable compleja, al derivarla se convierte en

$$\frac{e^x}{e^x-1} - \frac{1}{x} - \frac{1}{2} = \frac{1}{e^x-1} + \frac{1}{2} - \frac{1}{x} = \frac{1}{x}\,\frac{x}{e^x-1} + \frac{1}{2} - \frac{1}{x}.$$

Hemos multiplicado y dividido entre x porque así podemos aplicar la definición de los números de Bernoulli [ITAn 6.17] (así como que los de índice impar son nulos salvo $B_1 = -1/2$ y que $B_0 = 1$):

$$\frac{x}{e^x-1} = \sum_{k=0}^{\infty}\frac{B_k}{k!}x^k = 1 - \frac{x}{2} + x\sum_{i=1}^{\infty}\frac{B_{2i}}{(2i)!}x^{2i-1}.$$

Por consiguiente la derivada de 8.16 es

$$\sum_{i=1}^{\infty}\frac{B_{2i}}{(2i)!}x^{2i-1},$$

e integrando llegamos a que

$$\log\left(\frac{\exp(x)-1}{x}\right)-\frac{x}{2}=\sum_{i=1}^{\infty}\frac{B_{2i}}{(2i)(2i)!}x^{2i}$$

(notar que la función de la izquierda vale 0 en 0).

Esta igualdad sobre funciones de variable compleja implica esta misma igualdad cuando el primer término se interpreta como la composición en $\mathbb{Q}[[x]]$ de la serie de la función $(\exp(x)-1)/x-1$ con la serie de la función $\log(1+x)$. Por otra parte, en el cálculo del coeficiente de x^k de la composición de dos series, sólo usamos sus coeficientes de grado menor o igual que k, y si truncamos la exponencial según (8.12) estamos conservando los coeficientes de $(\exp(x)-1)/x-1$ hasta el de grado $p-2$, luego

$$L\left(\frac{E(x)-1}{x}\right)-\frac{x}{2}=\sum_{i=1}^{m-1}\frac{B_{2i}}{(2i)(2i)!}x^{2i}+x^{p-1}R(x),$$

donde $R(x)\in\mathbb{Q}[[x]]$ tiene coeficientes enteros p-ádicos (pues la composición de dos polinomios con coeficientes enteros tiene coeficientes enteros).

Ahora llevamos esta expresión a (8.15), que junto con (8.11) nos da

$$\log(\theta_k^{p-1})\equiv L(\theta_k^{p-1})\equiv\sum_{i=1}^{m-1}\frac{B_{2i}}{(2i)(2i)!}(1-k^{2i})\pi^{2i}\ (\text{mód }\pi^{p-1}).$$

Recordemos que, según hemos razonado al comienzo de la sección, esto implica que los coeficientes b_{ki} que aparecen en (8.10) han de cumplir

$$b_{ki}\equiv\frac{B_{2i}}{(2i)(2i)!}(1-k^{2i})\ (\text{mód }p),\quad 2\le k\le m,\ 1\le i\le m-1,$$

luego

$$\det(b_{ki})\equiv\prod_{i=1}^{m-1}\frac{(-1)^{m-1}B_{2i}}{(2i)(2i)!}\det(k^{2i}-1)\ (\text{mód }p).$$

Observemos que

$$\det(k^{2i}-1)=\begin{vmatrix}1&1&1&\cdots&1\\1&2^2&2^4&\cdots&2^{p-3}\\1&3^2&3^4&\cdots&3^{p-3}\\\vdots&\vdots&\vdots&&\vdots\\1&m^2&m^4&\cdots&m^{p-3}\end{vmatrix}$$

(restando la primera columna a todas las demás y desarrollando por la primera fila se obtiene el determinante de la izquierda).

El determinante de la derecha es de Vandermonde, por lo que en definitiva

$$\det(b_{ki})\equiv\prod_{i=1}^{m-1}\frac{(-1)^{m-1}B_{2i}}{(2i)(2i)!}\prod_{1\le r<s\le m}(s^2-r^2)\ (\text{mód }p).$$

Claramente $p \nmid s^2 - r^2 = (s+r)(s-r)$. Así mismo $p \nmid (2i)(2i)!$. Por el teorema 8.4 p tampoco divide a los denominadores de los números B_{2i}. Por lo tanto, una condición suficiente para que p no divida a $\det(b_{ki})$ es que p no divida a los numeradores de los números de bernoulli $B_2, \cdots, B_{p-3}$. Teniendo en cuenta los teoremas 8.6 y 8.10 llegamos a la conclusión siguiente:

Teorema 8.13 *Si p no divide al primer factor h_1 del número de clases del cuerpo ciclotómico p-ésimo, entonces los números $\log \theta_k^{p-1}$, $k = 2, \ldots, m$ son una $\mathbb{Z}_p$-base del módulo de los enteros p-ádicos reales de traza nula.*

Con esto llegamos finalmente al teorema que perseguíamos:

Teorema 8.14 (Kummer) *Sea p un primo impar. Las afirmaciones siguientes son equivalentes:*

1. *p es regular.*
2. *p no divide al número de clases h del cuerpo ciclotómico p-ésimo.*
3. *p no divide al primer factor h_1 del número de clases del cuerpo ciclotómico p-ésimo.*
4. *p no divide los numeradores de los números de Bernoulli $B_2, B_4, \ldots, B_{p-3}$.*

Tabla 8.2: Primos irregulares menores que 1.000.

Se indica también el menor índice $2i$ tal que p divide al numerador de B_{2i}.

p	$2i$	p	$2i$	p	$2i$	p	$2i$	p	$2i$	p	$2i$	p	$2i$
37	32	257	164	379	100	491	292	613	522	683	32	811	544
59	44	263	100	389	200	523	400	617	20	691	12	821	744
67	58	271	84	401	382	541	86	619	428	727	378	827	102
101	68	283	20	409	126	547	270	631	80	751	290	839	66
103	24	293	156	421	240	557	222	647	236	757	514	877	868
131	22	307	88	433	366	577	52	653	48	761	260	881	162
149	130	311	292	461	196	587	90	659	224	773	732	887	418
157	62	347	280	463	130	593	22	673	408	797	220	929	520
233	84	353	186	467	94	607	592	677	628	809	330	963	156
												971	166

(Hay un total de 168 primos menores que 1.000. El porcentaje de primos regulares en este intervalo es del $61,9\%$).

Demostración: La prueba de que 3) implica 2) está diseminada en los razonamientos precedentes, pero la repetimos por claridad. Hay que probar que si $p \nmid h_1$ entonces $p \nmid h_2$.

El teorema 8.7 nos da que h_2 es orden del grupo cociente de las unidades reales positivas del cuerpo ciclotómico p-ésimo sobre el subgrupo generado por las unidades θ_k, con $k = 2, \ldots, m = (p-1)/2$.

Si p divide a este orden, entonces el grupo cociente tiene un elemento de orden p, o sea, existe una unidad ciclotómica $\epsilon > 0$ tal que ϵ^p cumple (8.7) para ciertos enteros c_k, pero ϵ no es de esa forma.

Que ϵ no sea de esa forma equivale a que algún c_k no sea divisible entre p, pues en caso contrario sería $\epsilon^p = \delta^p$, para una cierta unidad δ de la forma (8.7), pero entonces ϵ/δ sería una raíz p-ésima de la unidad positiva, lo que sólo es posible si $\epsilon = \delta$.

Como $\mathcal{O}_p/\mathfrak{p}$ es el cuerpo de p elementos, se cumple que $\epsilon^{p-1} \equiv 1 \pmod p$ para toda unidad ϵ, o sea ϵ^{p-1} es una unidad principal y está definido $\log \epsilon^{p-1}$. Elevamos a $p-1$ la ecuación (8.7) y tomamos logaritmos, con lo que obtenemos (8.8).

Por el teorema 8.9 tenemos que $\log \epsilon^{p-1}$ es un entero p-ádico de traza nula, luego por el teorema 8.13 se expresa de forma única como combinación lineal de $\log \theta_k^{p-1}$ con coeficientes en $\mathbb{Z}_p$, pero por (8.8) estos coeficientes han de ser los números c_k/p, luego son enteros p-ádicos, de donde p divide a todos los c_k en $\mathbb{Z}_p$, y también en $\mathbb{Z}$.

Con esto tenemos la equivalencia entre 2), 3) y 4), y por la definición de primo regular 1) implica 2). Vamos a probar que 2) implica 1). Sólo hay que ver que si ϵ es una unidad ciclotómica congruente con un entero módulo p entonces ϵ es una potencia p-ésima.

Digamos que $\epsilon \equiv a \pmod p$. Por el lema de Kummer [Al 8.42] ha de ser $\epsilon = \omega^k \eta$, para una cierta unidad real η. Entonces η se expresa como combinación lineal con coeficientes enteros (p-ádicos) de los números $1, \pi^2, \pi^4, \ldots, \pi^{p-2}$, luego existe un entero p-ádico b (el coeficiente de 1) tal que $\eta \equiv b \pmod{\pi^2}$. Como todo entero p-ádico es congruente con un entero racional módulo p, podemos suponer que $b \in \mathbb{Z}$.

Por (8.9) tenemos que $\omega \equiv 1 + \pi \pmod{\pi^2}$, luego $\omega^k \equiv 1 + k\pi \pmod{\pi^2}$. Por lo tanto tenemos que

$$a \equiv b(1 + k\pi) \pmod{\pi^2}. \tag{8.17}$$

De aquí se sigue que $a \equiv b \pmod \pi$, y como son enteros ha de ser $a \equiv b \pmod p$, luego $a \equiv b \pmod{\pi^2}$. Entonces (8.17) implica que $bk\pi \equiv 0 \pmod{\pi^2}$ y así $\pi \mid bk$, pero $\pi \nmid b$, ya que en caso contrario tendríamos $\pi \mid \eta$. Consecuentemente $\pi \mid k$, luego $p \mid k$ y así $\omega^k = 1$, o sea, $\epsilon = \eta$ es una unidad real.

Como $(-1)^p = -1$ podemos suponer que $\epsilon > 0$ (si $-\epsilon$ es una potencia p-ésima también lo es ϵ). Por el teorema 8.9 está definido $\log \epsilon^{p-1}$. Más aún, puesto que $\epsilon^{p-1} \equiv a^{p-1} \equiv 1 \pmod p$, de la definición de logaritmo se sigue que $\log \epsilon^{p-1} \equiv 0 \pmod p$.

También por 8.9 tenemos que $\log \epsilon^{p-1}/p$ es un entero p-ádico real de traza nula, luego por 8.13 podemos expresar

$$\log \epsilon^{p-1} = \sum_{k=2}^{m} p c_k \log \theta_k^{p-1}, \tag{8.18}$$

para ciertos enteros p-ádicos c_k.

Por otra parte, el grupo generado por los números θ_k tiene índice finito (teorema 8.7) en el grupo de las unidades reales positivas. En consecuencia existe un número natural $a \neq 0$ tal que

$$\epsilon^a = \prod_{k=2}^{m} \theta_k^{d_k}, \tag{8.19}$$

para ciertos enteros d_k. Podemos suponer que los números $a, d_2, \ldots, d_m$ son primos entre sí, pues si tuvieran un factor común c, tendríamos dos unidades reales positivas α y β tales que $\alpha^c = \beta^c$, luego α/β sería una raíz de la unidad real y positiva, luego $\alpha = \beta$. Esto significa que c podría ser eliminado de ambos miembros dando lugar a una ecuación análoga.

Elevamos a $p-1$ y tomamos logaritmos:

$$a \log \epsilon^{p-1} = \sum_{k=2}^{m} d_k \log \theta_k^{p-1}.$$

Comparando con (8.18) concluimos que $d_k = pac_k$, para $k = 2, \ldots, m$, es decir, $p \mid d_k$ (en $\mathbb{Z}_p$ y por lo tanto en $\mathbb{Z}$), con lo que ha de ser $(a, p) = 1$.

Ahora (8.19) implica que ϵ^a es la potencia p-ésima de otra unidad, $\epsilon^a = \delta^p$. Sean u y v enteros tales que $au + vp = 1$. Entonces

$$\epsilon = (\epsilon^a)^u (\epsilon^v)^p = (\delta^p)^u (\epsilon^v)^p = (\delta^u \epsilon^v)^p,$$

luego efectivamente es una potencia p-ésima. ∎

Con esto tenemos el resultado de Kummer sobre el teorema de Fermat en su forma definitiva. En particular, hemos demostrado que el último teorema de Fermat es cierto para todos los exponentes menores que 100 salvo quizá para 37, 59, 67 y 74. Las estadísticas indican que la proporción de primos regulares es mayor que la de primos irregulares. Por ejemplo, de los 549 primos impares menores que 4.000 hay 334 primos regulares, lo que supone un 61% aproximadamente. Pese a ello no se sabe si el número de primos regulares es finito o infinito. Por el contrario, se puede probar que hay infinitos primos irregulares.

Capítulo IX

Ramificación

Dedicamos este último capítulo a profundizar un poco más en la aritmética de los cuerpos numéricos. Los resultados que obtendremos aquí están directa o indirectamente relacionados con la ramificación de primos. Por ejemplo, probaremos un hecho general del que hemos tenido ocasión de comprobar muchos casos particulares: los primos racionales que se ramifican en un cuerpo numérico son exactamente los divisores de su discriminante.

9.1 Extensiones no ramificadas

Nuestro estudio de la ramificación empieza por estudiar las extensiones de cuerpos métricos completos en las que no hay ramificación. Si k es un cuerpo métrico discreto completo k y D es su anillo de enteros, sabemos que D es un dominio de Dedekind con un único primo $\mathfrak{p}$. En particular D es un dominio euclídeo. Representaremos por $\overline{k}$ al cuerpo de restos $\overline{k} = D/\mathfrak{p}$.

Las extensiones finitas separables de cuerpos métricos discretos completos están descritas en el teorema 5.25: si K es una extensión separable de grado n de un cuerpo métrico discreto completo k entonces K también es un cuerpo discreto completo y sus anillos de enteros forman una extensión E/D de dominios de Dedekind.

La aritmética de E se relaciona con la de D a través del índice de ramificación $e = e(\mathfrak{P}/\mathfrak{p})$, dado por $\mathfrak{p} = \mathfrak{P}^e$, y el grado de inercia $f = f(\mathfrak{P}/\mathfrak{p}) = |\overline{K} : \overline{k}|$, donde $\overline{k}$ se identifica con un subcuerpo de $\overline{K}$ de forma natural. Sabemos que se cumple la relación $ef = n$. Recordemos, por último, que E es un D-módulo finitamente generado libre de torsión y, como D es un dominio euclídeo, por [Al 4.44] tenemos que E es de hecho un D-módulo libre, necesariamente de rango n.

Ya hemos señalado que la hipótesis de separabilidad puede eliminarse: todos los hechos que acabamos de citar son ciertos siempre que K/k es una extensión finita de cuerpos métricos discretos completos. Damos la prueba en el apéndice A. Para no añadir hipótesis superfluas, en los resultados de esta sección

y la siguiente hemos optado por enunciar los teoremas para extensiones finitas arbitrarias, con lo cual admiten una doble lectura: o bien se acepta la validez de los hechos citados para extensiones finitas, o bien se supone que las extensiones involucradas son separables.

En esta sección estudiamos con más detalle la relación entre las extensiones finitas de un cuerpo métrico discreto k y las extensiones finitas de su cuerpo de restos $\overline{k}$. Fijemos una clausura algebraica $\mathbb{K}$ de k y sea $\mathbb{E}$ la clausura entera de D en $\mathbb{K}$ (donde D es el anillo de enteros de k). Cuando hablemos de extensiones algebraicas de k entenderemos que las tomamos en $\mathbb{K}$. Para cada extensión finita K de k, su anillo de enteros E_k tiene un único ideal primo $\mathfrak{P}_k$, y es fácil ver que la unión de todos los ideales $\mathfrak{P}_K$ forma un ideal primo $\mathfrak{P}$ de $\mathbb{E}$. Dos elementos de $\mathbb{E}$ son congruentes módulo $\mathfrak{P}$ si y sólo si lo son módulo $\mathfrak{P}_K$, para cualquier extensión finita K de k que los contenga. Esto permite identificar de forma natural a cada cuerpo de restos $\overline{K}$ con un subcuerpo de $\overline{\mathbb{K}} = \mathbb{E}/\mathfrak{P}$.

También es fácil ver que $\overline{\mathbb{K}}$ es una clausura algebraica de $\overline{k}$. En efecto, cada elemento de $\overline{\mathbb{K}}$ es la clase de un elemento de $\alpha \in \mathbb{E}$, cuyo polinomio mínimo f sobre k tiene coeficientes en D, por lo que $[\alpha]$ es la raíz de la proyección natural $\overline{f}$ de f en $\overline{k}[x]$. Esto prueba que $\overline{\mathbb{K}}$ es una extensión algebraica de $\overline{k}$. Por otra parte, todo polinomio de $\overline{k}[x]$ es la proyección de un polinomio $f \in \mathbb{E}[x]$ del mismo grado. Como las raíces de un polinomio con coeficientes enteros son enteras, f se escinde en $\mathbb{E}[x]$, luego $\overline{f}$ se escinde en $\overline{\mathbb{K}}[x]$.

Así pues, cuando hablemos de extensiones algebraicas de $\overline{k}$ entenderemos que están contenidas en $\overline{\mathbb{K}}$. Es claro que la correspondencia $K \mapsto \overline{K}$ es una aplicación suprayectiva entre las extensiones finitas de k y las extensiones finitas de $\overline{k}$. Sin embargo no es inyectiva. Lo que haremos en esta sección es estudiar una familia de extensiones finitas de k que se corresponden biunívocamente con las extensiones finitas separables de $\overline{k}$.

Definición 9.1 Sea K/k una extensión de grado n de cuerpos métricos discretos completos y sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{P}$ el ideal primo de E y $\mathfrak{p}$ el ideal primo de D. Diremos que $\mathfrak{P}$ es *no ramificado* sobre $\mathfrak{p}$, o que la extensión K/k es *no ramificada* si $e = 1$ (o, equivalentemente, si $f = n$) y el cuerpo de restos $E/\mathfrak{P}$ es una extensión separable de $D/\mathfrak{p}$.

Así pues, K/k es no ramificada si $\overline{K}/\overline{k}$ es separable y $|K : k| = |\overline{K} : \overline{k}|$. Vamos a comprobar que la relación entre una extensión no ramificada y la extensión de sus cuerpos de restos es mucho más fuerte que la de tener el mismo grado. En primer lugar necesitamos un resultado técnico.

Teorema 9.2 *Sea E/D una extensión de Galois de dominios de Dedekind. Sea K/k la extensión de los cuerpos de cocientes. Sea $\mathfrak{p}$ un primo en D y supongamos que $\mathfrak{p}$ es divisible entre un único primo $\mathfrak{P}$ de E. Supongamos también que $E/\mathfrak{P}$ es separable sobre $D/\mathfrak{p}$. Consideremos un polinomio mónico irreducible $f(x) \in D[x]$ con una raíz en E. Entonces la imagen $\overline{f}$ de f en $(D/\mathfrak{p})[x]$ es potencia de un polinomio irreducible.*

DEMOSTRACIÓN: Puesto que K/k es una extensión finita de Galois, tenemos que $f(x)$ se escinde en $K[x]$ y, como E es la clausura entera de D en K, sabemos que todas las raíces de $f(x)$ están en E. Consecuentemente $f(x)$ se escinde en $E[x]$ y $\overline{f}$ se escinde en $(E/\mathfrak{P})[x]$.

Dos raíces cualesquiera de $\overline{f}$ son las clases de equivalencia de dos raíces de f, que son conjugadas en E por un k-automorfismo que fija a $\mathfrak{P}$ (por ser el único primo de $\mathfrak{P}$). Según el teorema 2.43, este automorfismo induce un $D/\mathfrak{p}$-automorfismo de $E/\mathfrak{P}$ que conjuga las raíces dadas, luego las raíces de $\overline{f}$ son todas conjugadas, con lo que $\overline{f}$ no puede ser divisible entre dos polinomios irreducibles distintos. ∎

Teorema 9.3 *Sea K/k una extensión finita de cuerpos métricos discretos completos.*

1. *Si K/k es no ramificada y $\overline{K} = \overline{k}([\alpha])$ para cierto entero $\alpha \in K$, entonces la extensión K/k es separable, $K = k(\alpha)$ y el polinomio mínimo de α en k es irreducible en $\overline{k}[x]$.*

2. *Si $K = k(\alpha)$ para un cierto entero $\alpha \in K$ cuyo polinomio mínimo no tenga raíces múltiples en $\overline{K}$, entonces K/k es no ramificada y $\overline{K} = \overline{k}([\alpha])$.*

DEMOSTRACIÓN: 1) Sea $f(x)$ el polinomio mínimo de α sobre k. Como α es entero, se cumple que $f(x)$ tiene coeficientes enteros en k, y su imagen $\overline{f}$ es un polinomio mónico con raíz $[\alpha]$. Como la extensión es no ramificada el grado de $\overline{K}$ sobre $\overline{k}$ coincide con el grado n de K/k. Claramente entonces $n \le \operatorname{grad}\overline{f} = \operatorname{grad} f \le n$, luego se da la igualdad y por lo tanto $\overline{f}$ es el polinomio mínimo de $[\alpha]$. Esto implica que $\overline{f}$ es separable, y entonces f también ha de serlo. La conclusión es ahora obvia.

2) Es obvio que $\overline{K} = \overline{k}([\alpha])$, y por hipótesis $[\alpha]$ es separable sobre $\overline{k}$. Así pues, la extensión $\overline{K}/\overline{k}$ es separable.

Pero la hipótesis implica también que el polinomio mínimo de α no tiene raíces múltiples, luego la extensión K/k es separable también. Podemos aplicar el teorema anterior a la menor extensión de Galois de k que contiene a K. Concluimos que la imagen $\overline{f}$ del polinomio mínimo de α es irreducible en $\overline{k}$. Esto prueba que $|\overline{K} : \overline{k}| \ge |K : k|$ y, como la otra desigualdad siempre es cierta, de hecho tenemos la igualdad. El teorema es ahora inmediato. ∎

Observemos que si K/k es una extensión no ramificada entonces por definición $\overline{K}/\overline{k}$ es separable, luego tiene un elemento primitivo. Por consiguiente el apartado 1) prueba que las extensiones no ramificadas son siempre separables.

El apartado 2) afirma que la condición necesaria y suficiente para que al adjuntarle a k un entero separable α obtengamos una extensión no ramificada es que las raíces de su polinomio mínimo permanezcan distintas en los cuerpos de restos.

Ahora podemos probar las propiedades básicas de las extensiones no ramificadas:

Teorema 9.4 *Sea k un cuerpo métrico discreto completo.*

1. *Si $k \subset K \subset L$ es una cadena de extensiones finitas, entonces L/k es no ramificada si y sólo si L/K y K/k son no ramificadas.*
2. *Si K/k es una extensión finita no ramificada y L/k es una extensión finita, entonces KL/L es no ramificada.*
3. *Si K/k y L/k son extensiones finitas no ramificadas entonces KL/k también lo es.*

DEMOSTRACIÓN: 1) es inmediato a partir de la definición.

2) Sea $\overline{K} = \overline{k}([\alpha])$ para cierto entero $\alpha \in K$ y sea $f(x)$ el polinomio mínimo de α sobre k. Por el teorema anterior sabemos que $K = k(\alpha)$ y que $f(x)$ es irreducible en $\overline{k}\,[x]$ (luego separable). Claramente $KL = L(\alpha)$ y el polinomio mínimo de α sobre L divide a f, luego será separable también. Por el teorema anterior la extensión KL/L es no ramificada.

3) Por 2) la extensión KL/L es no ramificada, luego por a) KL/k también lo es. ∎

Con estas propiedades ya podemos demostrar que las extensiones no ramificadas de un cuerpo k se corresponden biunívocamente con las extensiones separables del cuerpo de restos:

Teorema 9.5 *Sea k un cuerpo métrico discreto completo.*

1. *Si K y L son extensiones finitas de k tales que K/k es no ramificada y $\overline{K} = \overline{L}$, entonces $K \subset L$.*
2. *La correspondencia $K \mapsto \overline{K}$ biyecta las extensiones no ramificadas de k con las extensiones finitas separables de $\overline{k}$.*
3. *Si K/k es una extensión no ramificada entonces K/k es separable, y K/k es de Galois si y sólo si lo es $\overline{K}/\overline{k}$. En tal caso, el epimorfismo descrito en el teorema* 2.43 *es un isomorfismo entre $G(K/k)$ y $G(\overline{K}/\overline{k})$.*

DEMOSTRACIÓN: 1) Claramente $\overline{KL} = \overline{K}\,\overline{L} = \overline{L}$, y por el teorema anterior la extensión KL/L es no ramificada. Por consiguiente $|KL : L| = |\overline{KL} : \overline{L}| = 1$, es decir, $KL = L$, luego $K \subset L$.

2) Toda extensión separable de $\overline{k}$ es de la forma $\overline{k}([\alpha])$, donde α es un entero en una extensión de k. El polinomio mínimo de $[\alpha]$ en $\overline{k}$ será de la forma $\overline{f}$, donde $f \in k[x]$ es un polinomio mónico con coeficientes enteros. Descomponiéndolo en factores lineales y tomando clases, concluimos que existe una raíz β de $f(x)$ tal que $[\beta] = [\alpha]$. Equivalentemente, podemos suponer que α es raíz de $f(x)$.

Como el polinomio mínimo de α sobre k divide a f, no puede tener raíces múltiples en $\overline{\mathbb{K}}$, luego el teorema 9.3 nos da que $K = k(\alpha)$ es una extensión no ramificada de k, y ciertamente $\overline{K}$ es la extensión dada. La unicidad se sigue del apartado anterior.

3) Ya sabemos que las extensiones no ramificadas son separables. Si K/k es de Galois el teorema 2.43 nos da que $\overline{K}/\overline{k}$ también lo es, y tenemos el epimorfismo $G(K/k) \longrightarrow G(\overline{K}/\overline{k})$ descrito allí (observemos que como K tiene un único primo el grupo de descomposición es todo el grupo de Galois). Por otra parte los dos grupos de Galois tienen orden n, luego el epimorfismo es en realidad un isomorfismo.

Supongamos ahora que la extensión $\overline{K}/\overline{k}$ es de Galois. Sea $\overline{K} = \overline{k}([\alpha])$. Según el teorema 9.3 se cumple que $K = k(\alpha)$ y el polinomio mínimo f de α sobre k induce el polinomio mínimo de $[\alpha]$ sobre $\overline{k}$. Basta probar que todas las raíces de f están en K. Ahora bien, si β es una raíz de f, entonces $[\beta]$ es una raíz de $\overline{f}$ y, como $\overline{K}/\overline{k}$ es de Galois, $[\beta] \in \overline{K}$. Más aún, puesto que $[\beta]$ tiene el mismo polinomio mínimo que $[\alpha]$, se cumple $\overline{K} = \overline{k}([\beta])$.

Resulta entonces que el cuerpo $L = k(\beta)$ es una extensión no ramificada de k con el mismo cuerpo de restos, luego el apartado a) nos da que $L = K$, y por consiguiente $\beta \in K$. ∎

Como ya hemos dicho, estos teoremas vamos a aplicarlos al caso de las compleciones de los cuerpos numéricos, en las cuales los cuerpos de restos son finitos. Todas las extensiones finitas de los cuerpos finitos son de Galois, cíclicas de hecho, luego en este caso se cumple:

Teorema 9.6 *Toda extensión no ramificada de un cuerpo métrico discreto localmente compacto es finita de Galois con grupo de Galois cíclico.*

(Recordemos de 5.17 que la compacidad local en un cuerpo métrico discreto completo equivale a que el cuerpo de restos sea finito.)

9.2 Extensiones totalmente ramificadas

Estudiamos ahora las extensiones de cuerpos métricos discretos completos que están en la situación opuesta a las que hemos estudiado en la sección anterior:

Definición 9.7 Sea k un cuerpo métrico discreto completo. Una extensión K/k de grado n es *totalmente ramificada* si cumple que $e = n$ (o, equivalentemente, $f = 1$). Si $\mathfrak{p}$ es el único primo de k y $\mathfrak{P}$ es el único primo de K, también se dice que $\mathfrak{P}$ está *totalmente ramificado* sobre $\mathfrak{p}$.

Observemos que K/k es totalmente ramificada si y sólo si $\overline{K} = \overline{k}$. En general una extensión no tiene por qué ser no ramificada o totalmente ramificada, pero toda extensión (cuya extensión de cuerpos de restos sea separable) se descompone en dos extensiones de estos tipos:

Teorema 9.8 *Sea k un cuerpo métrico discreto completo y sea K una extensión finita de k tal que la extensión $\overline{K}/\overline{k}$ sea separable. Sea K_{nr} el producto de todos los cuerpos intermedios no ramificados sobre k. Entonces la extensión K_{nr}/k es no ramificada y la extensión K/K_{nr} es totalmente ramificada.*

DEMOSTRACIÓN: La extensión K_{nr}/k es no ramificada por el teorema 9.4. Según el teorema 9.5 existe una extensión no ramificada L de k tal que $\overline{L} = \overline{K}$. Por el apartado a) de este mismo teorema se cumple de hecho que $L \subset K$, luego $k \subset L \subset K_{nr}$. Consecuentemente, $\overline{K} = \overline{L} \subset \overline{K}_{nr} \subset \overline{K}$, luego $\overline{L} = \overline{K}_{nr}$ y, de nuevo por 9.5, $L = K_{nr}$. Así pues, $\overline{K}_{nr} = \overline{K}$, lo que implica que la extensión K/K_{nr} es totalmente ramificada. ∎

Recordemos que un *polinomio de Eisenstein* para un primo π en un dominio de factorización única es un polinomio mónico cuyos coeficientes sean todos divisibles entre π excepto el coeficiente director y cuyo término independiente no sea divisible entre π^2. El criterio de irreducibilidad de Eisenstein [Al 3.29] afirma que los polinomios de Eisenstein son siempre irreducibles.

Teorema 9.9 *Sea k un cuerpo métrico discreto completo y K una extensión de k de grado n.*

1. *Si K/k es totalmente ramificada y $\mathfrak{P} = (\pi)$ es el primo de K, entonces $K = k(\pi)$ y el polinomio mínimo de π en k es un polinomio de Eisenstein de grado n.*

2. *Si $K = k(\pi)$ y π es la raíz de un polinomio de Eisenstein con coeficientes en K, entonces la extensión es totalmente ramificada y π es primo en K.*

DEMOSTRACIÓN: 1) Por la nota tras 5.24 sabemos que $1, \pi, \ldots, \pi^{n-1}$ son linealmente independientes sobre k, luego $K = k(\pi)$.

Extendemos un valor absoluto de k a la clausura normal[1] de K sobre k. Como los k-automorfismos son isometrías, todos los conjugados de π tienen el mismo valor absoluto, y éste es menor que 1.

Los coeficientes distintos del director del polinomio mínimo de π se obtienen de sumas de productos de los conjugados de π, y como el valor absoluto es no arquimediano resulta que todos tienen valor absoluto menor que 1. Esto significa que todos son divisibles entre el único primo de k. El término independiente es, concretamente, el producto de todos los conjugados de π, luego su valor absoluto es $|\pi|^n$. Como el único primo de k es precisamente $\mathfrak{p} = \mathfrak{P}^n$, es claro que dicho término independiente no es divisible entre $\mathfrak{p}^2$.

2) Sea ρ un primo en k, con lo que $\mathfrak{p} = (\rho)$, y supongamos que π es una raíz de un polinomio de Eisenstein de grado n con coeficientes en k.

Entonces el valor absoluto del término independiente es $|\rho|$, y por otra parte dicho término independiente es el producto de los n conjugados de π (pues el polinomio es irreducible, luego $|\pi|^n = |\rho| < 1$

Por lo tanto, $|\pi^n/\rho| = 1$, o sea, que π^n/ρ es una unidad y, como ideal en K, se tiene $\mathfrak{p} = (\pi)^n$. De aquí se sigue que π es primo, pues el índice de ramificación no puede ser mayor que el grado de la extensión. Así pues, $\mathfrak{P} = (\pi)$ y la extensión es totalmente ramificada. ∎

Veamos una aplicación de este teorema:

[1] O bien suponemos que la extensión K/k es separable y usamos 5.25 o bien usamos A.6.

Teorema 9.10 *Sea k un cuerpo métrico localmente compacto perfecto y sea n un número natural. Entonces k tiene sólo un número finito de extensiones de grado $\leq n$.*

DEMOSTRACIÓN: Cada extensión de grado $\leq n$ de k se descompone en una extensión no ramificada de grado $\leq n$ seguida de una extensión totalmente ramificada también de grado $\leq n$. (Observemos que $\overline{k}$ es finito, luego perfecto, y por consiguiente podemos aplicar el teorema 9.8). El teorema 9.5 nos da que hay sólo un número finito de extensiones no ramificadas de k de grado $\leq n$ (porque un cuerpo finito tiene sólo un número finito de extensiones de grado $\leq n$). Basta ver que cada una de estas extensiones admite sólo un número finito de extensiones totalmente ramificadas de grado $\leq n$. Puesto que tales extensiones son localmente compactas (tienen cuerpos de restos finitos), basta probar que todo cuerpo métrico localmente compacto k tiene sólo un número finito de extensiones totalmente ramificadas de un grado fijo e.

Sea $\mathfrak{p} = (\pi)$ el primo de k. Cada extensión está determinada por un polinomio de Eisenstein de la forma

$$x^e + \alpha_{e-1}x^{e-1} + \cdots + \alpha_1 x + u_0\pi,$$

donde los coeficientes α_i están en $\mathfrak{p}$ y u_0 es una unidad de k. Si llamamos U al grupo de las unidades tenemos que cada polinomio de Eisenstein de grado e está determinado por un elemento de $\mathfrak{p} \times \overset{e-2}{\cdots} \times \mathfrak{p} \times U$. Recíprocamente, cada elemento de este espacio determina a lo sumo e extensiones de k.

El teorema 5.30 (y aquí usamos que k es perfecto) afirma que cada punto de este espacio tiene un entorno (respecto a la topología producto) cuyos puntos determinan las mismas extensiones de k. Por compacidad hay tan sólo un número finito de extensiones. ∎

La ramificación de los primos es una de las partes más delicadas de la teoría que estamos estudiando. Volveremos sobre ello más adelante, pero de momento nos conviene dar un paso más, con el cual aislaremos la situación más difícil de manejar. Para ello introducimos los conceptos siguientes:

Definición 9.11 Una extensión finita K/k de cuerpos métricos completos discretos es *dominadamente ramificada* si la extensión $\overline{K}/\overline{k}$ es separable y la característica de estos cuerpos no divide al índice de ramificación e. En caso contrario se dice que la extensión es *libremente ramificada.* Alternativamente, si $\mathfrak{p}$ es el primo de k y $\mathfrak{P}$ el de K, se dice que $\mathfrak{P}$ está dominado o libremente ramificado sobre $\mathfrak{p}$.

Observemos que las extensiones dominadamente ramificadas contienen a las no ramificadas. Si los cuerpos de restos tienen característica 0 todas las extensiones son dominadamente ramificadas y lo que diremos a continuación se vuelve trivial. Ahora necesitamos un resultado técnico.

Teorema 9.12 *Sea K/k una extensión totalmente ramificada de cuerpos métricos discretos completos cuyos cuerpos de restos tengan característica prima p.*

Sea e un número natural no divisible entre p, sea $\mathfrak{p} = (\rho)$ el ideal primo de k y sea $\pi \in K$ tal que $|\pi|^e = |\rho|$. Entonces existe una unidad ϵ en k tal que una de las raíces del polinomio $x^e - \epsilon\rho$ está contenida en $k(\pi)$.

DEMOSTRACIÓN: Sea $\delta = \pi^e/\rho$, que por hipótesis cumple $|\delta| = 1$, luego es una unidad de K. Sea $\mathfrak{P}$ el ideal primo de K. Como $\mathfrak{P}$ está totalmente ramificado sobre $\mathfrak{p}$ se cumple que $\overline{K} = \overline{k}$, luego existe una unidad $\epsilon \in k$ tal que $\delta \equiv \epsilon$ (mód $\mathfrak{P}$).

Así pues, existe un $\gamma \in \mathfrak{P}$ tal que $\delta = \epsilon + \gamma$, es decir, $\pi^e = \epsilon\rho + \gamma\rho$. Como $|\gamma| < 1$ resulta que $|\pi^e - \epsilon\rho| < |\rho|$.

Sea $f(x) = x^e - \epsilon\rho$ y sean $\alpha_1, \dots, \alpha_e$ sus raíces (que son distintas porque f es separable, ya que si K tiene característica prima, ésta ha de ser igual a p y tenemos que $p \nmid e$). Entonces

$$|f(\pi)| = |\pi - \alpha_1| \cdots |\pi - \alpha_e| = |\pi^e - \epsilon\rho| < |\rho| = |\pi|^e,$$

luego alguna de las raíces, digamos α_1, ha de cumplir $|\pi - \alpha_1| < |\pi|$.

De la ecuación $f(\alpha_i) = 0$ se sigue que $|\alpha_i|^e = |\pi|^e$, luego $|\alpha_i| = |\pi|$ y en particular tenemos $|\pi - \alpha_1| < |\alpha_1|$.

Como $p \nmid e$ podemos afirmar que $e \notin \mathfrak{p}$, luego $|e| = 1$. Teniendo esto en cuenta llegamos a que

$$|f'(\alpha_1)| = |\alpha_1|^{e-1} = |\alpha_1 - \alpha_2| \cdots |\alpha_1 - \alpha_e|,$$

pero $|\alpha_1 - \alpha_i| \le |\alpha_1|$, pues el valor absoluto es no arquimediano y $|\alpha_1| = |\alpha_i|$. Esto implica que $|\alpha_1 - \alpha_i| = |\alpha_1|$ para todo $i = 2, \dots, e$.

En resumen tenemos que $|\pi - \alpha_1| < |\alpha_1| = |\alpha_i - \alpha_1|$ para $i = 2, \dots, e$. El teorema se sigue ahora de 5.29. Notemos que según el enunciado de 5.29 haría falta que π fuera separable sobre k, pero si analizamos la prueba vemos que basta con que α sea separable y que el valor absoluto de k se extienda a una extensión que contenga a β (π en nuestro caso) y a todos los conjugados de α. ∎

El teorema siguiente mejora a 9.9 para las extensiones totalmente ramificadas con ramificación dominada. Esencialmente afirma que una extensión K/k totalmente ramificada de grado n no divisible entre la característica de $\overline{k}$ tiene ramificación dominada si y sólo si podemos tomar como primo en K a una raíz n-sima de un primo en k.

Teorema 9.13 *Sea k un cuerpo métrico discreto completo y sea K una extensión de k de grado n. Sea $\mathfrak{p}$ y $\mathfrak{P}$ los primos de k y K respectivamente. Sea p la característica de $\overline{k}$.*

1. *Si K/k es total y dominadamente ramificada entonces existen $\pi \in K$ y $\rho \in k$ de modo que $K = k(\pi)$, $\mathfrak{P} = (\pi)$, $\mathfrak{p} = (\rho)$ y el polinomio mínimo de π sobre k es $x^n - \rho$.*

2. *Si $K = k(\pi)$, donde π es una raíz de un polinomio de la forma $x^e - \rho$, con ρ entero en k y e un natural no divisible entre p, entonces la extensión K/k es dominadamente ramificada, y será totalmente ramificada si además la multiplicidad de $\mathfrak{p}$ en ρ es prima con e.*

DEMOSTRACIÓN: 1) Sea $\mathfrak{P} = (\pi)$ y $\mathfrak{p} = (\rho)$. Como la extensión es totalmente ramificada tenemos que $(\rho) = \mathfrak{p} = \mathfrak{P}^n = (\pi^n)$, y por ser dominadamente ramificada se cumple además que $p \nmid e = n$. El teorema anterior nos dice que podemos elegir ρ adecuadamente (multiplicándolo por una unidad) de manera que una raíz α del polinomio $x^n - \rho$ esté contenida en $k(\pi)$. Pero éste es un polinomio de Eisenstein, luego el teorema 9.9 nos da que α es primo en $k(\alpha) \subset k(\pi) \subset K$ y, comparando los grados, resulta que $K = k(\alpha)$, luego se cumple a) tomando π igual a este α que hemos obtenido.

2) En primer lugar observamos que $\overline{K} = \overline{k}([\pi])$, y $[\pi]$ es separable sobre $\overline{k}$, pues el polinomio $x^e - [\rho]$ es primo con su derivada. Así pues, la extensión $\overline{K}/\overline{k}$ es separable.

Sea $f(x) = x^e - \rho$. Sea $\rho = \epsilon\tau^r$, donde ϵ es una unidad en k y τ es un primo. Fijemos una raíz e-ésima primitiva de la unidad ζ y raíces e-ésimas de ϵ y τ, a las que llamaremos $\epsilon^{1/e}$ y $\tau^{1/e}$. Entonces $\epsilon^{1/e}\tau^{r/e}$ es una raíz de $f(x)$ y dos raíces cualesquiera se diferencian en una potencia de ζ. Por lo tanto $K = k(\pi) \subset k(\zeta, \epsilon^{1/e}, \tau^{1/e})$.

Los polinomios mínimos de ζ y $\epsilon^{1/e}$ dividen respectivamente a $x^e - 1$ y $x^e - \epsilon$, que son primos con sus derivadas (en K y en $\overline{K}$). Podemos aplicar dos veces el teorema 9.3 y concluir que $L = k(\zeta, \epsilon^{1/e})$ es una extensión de k no ramificada. De aquí se sigue que τ sigue siendo primo en L.

Por otra parte, el teorema 9.9 nos da que la extensión $L(\tau^{1/e})/L$ es totalmente ramificada, pues $\tau^{1/e}$ es raíz del polinomio de Eisenstein $x^e - \tau$. Además su grado es e, luego también es dominadamente ramificada.

El índice de ramificación de $L(\tau^{1/e})/k$ es igual a e (pues el de L/k vale 1), y el índice de ramificación de K/k divide a éste, luego es primo con p y por lo tanto K/k es dominadamente ramificada.

Si además la multiplicidad de $\mathfrak{p}$ en ρ (o sea, r) es prima con e, existen enteros racionales s y t tales que $se + tr = 1$. Sea $\beta = \pi^t\tau^s$. Entonces $\beta^e/\tau = \pi^{te}\tau^{se-1} = (\pi^e\tau^{-r})^t$ y, como $\pi^e = \rho = \epsilon\tau^r$ resulta que β^e/τ es una unidad. Deducimos que $v_{\mathfrak{P}}(\tau) = v_{\mathfrak{P}}(\beta^e) = e v_{\mathfrak{P}}(\beta) \geq e$ (observemos que de estas igualdades se sigue que $v_{\mathfrak{P}}(\beta) > 0$, pues $v_{\mathfrak{P}}(\tau) > 0$).

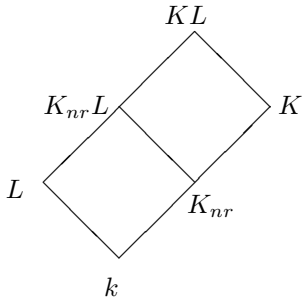
Esto implica que $e \leq e(\mathfrak{P}/\mathfrak{p}) \leq |K : k| \leq e$. En consecuencia la extensión es totalmente ramificada. ∎

La ramificación dominada se conserva en los mismos casos que la no ramificación:

Teorema 9.14 *Sea k un cuerpo métrico discreto completo.*

1. *Si $k \subset K \subset L$ es una cadena de extensiones finitas, entonces L/k es dominadamente ramificada si y sólo si L/K y K/k son dominadamente ramificadas.*
2. *Si K/k y L/k son extensiones finitas y K/k es dominadamente ramificada, entonces KL/L es dominadamente ramificada.*
3. *Si K/k y L/k son extensiones dominadamente ramificadas entonces KL/k también lo es.*

DEMOSTRACIÓN: 1) es evidente y 3) es consecuencia de 1) y 2). Para probar 2) consideremos el cuerpo K_{nr} definido en el teorema 9.8. La situación es la siguiente:



La extensión K_{nr}/k es no ramificada y por el teorema 9.4 lo mismo le ocurre a la extensión $K_{nr}L/L$. Sabemos que K/K_{nr} es total y dominadamente ramificada y usando el teorema anterior en los dos sentidos concluimos que $KL/K_{nr}L$ también es dominadamente ramificada. Como el índice de ramificación de esta extensión es el mismo que el de KL/K, tenemos 2). ∎

Como en el caso de las extensiones no ramificadas, este teorema nos permite construir una máxima extensión con ramificación dominada.

Teorema 9.15 *Sea K/k una extensión de cuerpos métricos discretos completos. Supongamos que $\overline{k}$ tiene característica prima p y que la extensión $\overline{K}/\overline{k}$ es separable. Sea K_d el producto de todos los cuerpos intermedios dominadamente ramificados sobre k. Entonces la extensión K_d/k es dominadamente ramificada y K/K_d es totalmente ramificada y el grado $|K : K_d|$ es potencia de p.*

DEMOSTRACIÓN: El teorema anterior garantiza que la extensión K_d/k es dominadamente ramificada. Claramente $K_{nr} \subset K_d$, luego la extensión K/K_d es totalmente ramificada. Sea e el índice de ramificación de K/k, que es el mismo que el de K/K_{nr}. Sea $e = mp^r$, donde $(m, p) = 1$. Sea $\mathfrak{P}$ el primo de K y $\mathfrak{p}$ el primo de K_{nr}. Entonces $\mathfrak{p} = \mathfrak{P}^e$. De aquí se sigue que si $\mathfrak{P} = (\pi)$ y $\mathfrak{p} = (\rho)$, entonces $|\pi^e| = |\rho|$ y si $\tau = \pi^{p^r}$ podemos aplicar el teorema 9.12 tomando $e = m$ y $\pi = \tau$ (y la extensión K/K_{nr}, que es totalmente ramificada). Concluimos que $K_{nr}(\tau)$ contiene una raíz α del polinomio $x^m - \rho$. Este polinomio es irreducible en $K_{nr}[x]$ por ser un polinomio de Eisenstein. Si llamamos $L = K_{nr}(\alpha)$ el teorema 9.13 nos da que L/K_{nr} es total y dominadamente ramificada, luego el índice de ramificación de L/K_{nr} es el grado de la extensión, o sea, m.

Obviamente L/k es dominadamente ramificada, también con índice de ramificación m. Por lo tanto la extensión K/L tiene índice de ramificación p^r y, como es totalmente ramificada (porque $K_{nr} \subset L$), se cumple $|K : L| = p^r$.

En consecuencia $L = K_d$, pues LK_d/L es dominadamente ramificada y tiene grado potencia de p, lo cual obliga a que $|LK_d : L| = 1$. ∎

9.3 Módulos complementarios

Ahora necesitamos estudiar un concepto que tocamos superficialmente al introducir el discriminante de un cuerpo numérico: la dualidad que la traza induce en una extensión separable de cuerpos.

Si K/k es una extensión finita de cuerpos, la aplicación $(\alpha, \beta) \mapsto \mathrm{Tr}(\alpha\beta)$ es una forma bilineal en K. Su matriz en una k-base de K dada, digamos $w_1, \ldots, w_n$, es claramente $\big(\mathrm{Tr}(w_i w_j)\big)$. En la prueba del teorema 2.17 vimos que si la extensión K/k es separable entonces esta matriz tiene determinante no nulo, por lo que la forma bilineal es regular e induce un isomorfismo entre K y su k-espacio vectorial dual (el espacio de las aplicaciones lineales de K en k). En general, cada base de un espacio vectorial de dimensión finita tiene asociada una base en su espacio dual. En nuestro caso podemos considerar su antiimagen por el isomorfismo inducido por la traza y obtenemos así otra k-base de K, a la que llamamos base dual de la base de partida.

El teorema siguiente recoge los hechos que vamos a necesitar en la práctica sobre todo lo dicho. Notemos que está probado casi en su totalidad en la demostración del teorema 2.17.

Teorema 9.16 *Sea K/k una extensión de cuerpos finita separable, consideremos la traza $\mathrm{Tr} : K \longrightarrow k$ y sea $w_1, \ldots, w_n$ una k-base de K. Entonces*

1. *La matriz $\big(\mathrm{Tr}(w_i w_j)\big)$ tiene determinante no nulo.*
2. *Existen unos únicos elementos $z_1, \ldots, z_n$ en K de modo que*

$$\mathrm{Tr}(w_i z_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Estos elementos forman una k-base de K a la que llamaremos base dual *de la base dada.*

Demostración: Tal y como indicamos en la demostración de 2.17, el apartado 1) es consecuencia inmediata de [Al 8.1], y los elementos $z_1, \ldots, z_n$ son necesariamente la base dual de $w_1, \ldots, w_n$ en el sentido de [Al 6.46]. ∎

Introducimos ahora un concepto muy relacionado con las bases duales, tal y como veremos enseguida:

Definición 9.17 Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Sea $\mathrm{Tr} : K \longrightarrow k$ la traza de la extensión. Si L es un subgrupo aditivo de K definimos el *complementario* de L como el conjunto L' de todos los elementos $\alpha \in K$ tales que $\mathrm{Tr}[\alpha L] \subset D$, o sea, $\mathrm{Tr}(\alpha\beta) \in D$ para todo $\beta \in L$.

El teorema siguiente recoge las propiedades básicas de los conjuntos complementarios. El apartado 4) describe los módulos complementarios en el único caso en que nos van a interesar:

Teorema 9.18 *Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes asociados. Sean L y M subgrupos aditivos de K. Entonces*

1. *L' es un subgrupo aditivo de K.*
2. *Si L es un D-módulo (o un E-módulo) entonces L' también lo es.*
3. *Si $L \subset M$ entonces $M' \subset L'$.*
4. *Si $w_1, \dots, w_n$ es una k-base de K y $w'_1, \dots, w'_n$ es su base dual, entonces el módulo complementario de $L = \langle w_1, \dots, w_n\rangle_D$ es $L' = \langle w'_1, \dots, w'_n\rangle_D$.*
5. *Si L es un ideal fraccional de K entonces L' también lo es.*

DEMOSTRACIÓN: 1) Si α_1, $\alpha_2 \in L'$ entonces

$$\mathrm{Tr}\big((\alpha_1 - \alpha_2)\beta\big) = \mathrm{Tr}(\alpha_1\beta) - \mathrm{Tr}(\alpha_2\beta) \in D$$

para todo $\beta \in L$.

2) Si $\alpha \in L'$ y $d \in D$ (o $d \in E$) entonces $d\beta \in L$ para todo $\beta \in L$, luego $\mathrm{Tr}(d\alpha\beta) = \mathrm{Tr}\big(\alpha(d\beta)\big) \in D$ para todo $\beta \in L$.

3) es evidente.

4) Sea $\alpha \in L'$. Entonces $\alpha = a_1w'_1 + \cdots a_nw'_n$ para ciertos elementos $a_i \in K$. Pero sucede que $a_i = \mathrm{Tr}(\alpha w_i) \in D$, luego $\alpha \in \langle w'_1, \dots, w'_n\rangle_D$.

Recíprocamente, si $\alpha = a_1w'_1 + \cdots + a_nw'_n$, para ciertos elementos $a_i \in D$, entonces $\mathrm{Tr}(\alpha w_i) = a_i \in D$, y por linealidad es claro que $\mathrm{Tr}(\alpha\beta) \in D$ para todo $\beta \in L$, luego $\alpha \in L'$.

5) Si L es un ideal fraccional de K, por b) sabemos que L' es un E-módulo. Existe un $\alpha \in K$ no nulo tal que $\alpha L \subset E$, luego $\mathrm{Tr}[\alpha L] \subset \mathrm{Tr}[E] \subset D$, luego $\alpha \in L'$ que, por consiguiente, es no nulo.

Falta probar que existe un $\alpha \in K$ no nulo tal que $\alpha L' \subset E$. En primer lugar observamos que L contiene una k-base de K. En efecto, por 2.16 existe una k-base de K formada por elementos de E. Si la multiplicamos por cualquier elemento no nulo de L obtenemos la base buscada. Sea, pues, $w_1, \dots, w_n$ una k-base de K contenida en L. Entonces $\langle w_1, \dots, w_n\rangle_D \subset L$ y, por c) y d), tenemos que $L' \subset \langle w'_1, \dots, w'_n\rangle_D$.

Como D es noetheriano, el D-módulo $\langle w'_1, \dots, w'_n\rangle_D$ también lo es, luego L' es un D-módulo finitamente generado. Digamos $L' = \langle x_1, \dots, x_r\rangle_D$. Aplicando el teorema 2.16 encontramos un elemento no nulo $\alpha \in D$ tal que $\alpha x_i \in E$ para todo i, con lo que $\alpha L' \subset E$, como había que probar. ∎

En realidad sólo nos van a interesar los complementarios de los ideales fraccionales. Para ellos probamos, en primer lugar, que conmutan con las localizaciones:

Teorema 9.19 *Sea E/D una extensión separable de dominios de Dedekind, sea S un subconjunto multiplicativo de D y sea $\mathfrak{a}$ un ideal fraccional de E. Entonces $S^{-1}(\mathfrak{a}') = (S^{-1}\mathfrak{a})'$.*

DEMOSTRACIÓN: Notemos que al localizar los cuerpos de cocientes no varían, luego la traza de la extensión $S^{-1}E/S^{-1}D$ es la misma que la de la E/D.

Si $\alpha/s \in S^{-1}(\mathfrak{a}')$ y $a/t \in S^{-1}\mathfrak{a}$, entonces $\mathrm{Tr}(\alpha a/st) = \mathrm{Tr}(\alpha a)/st \in S^{-1}D$, luego tenemos la inclusión $S^{-1}(\mathfrak{a}') \subset (S^{-1}\mathfrak{a})'$.

Por definición de ideal fraccional existe un $a \in E$ no nulo tal que $a\mathfrak{a} \subset E$. Puesto que E es un D-módulo finitamente generado y D es noetheriano, también $a\mathfrak{a}$ es finitamente generado, y de aquí que lo mismo le sucede a $\mathfrak{a}$. Sea, pues, $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle_D$. Si $\alpha \in (S^{-1}\mathfrak{a})'$ entonces se cumple $\mathrm{Tr}(\alpha a_i) \in S^{-1}D$ para $i = 1, \ldots, n$. Digamos $\mathrm{Tr}(\alpha a_i) = d_i/s_i$. Sea $s = s_1 \cdots s_n$.

Entonces $\mathrm{Tr}(s\alpha a_i) = s\,\mathrm{Tr}(\alpha a_i) \in D$, de donde por linealidad se cumple $\mathrm{Tr}(s\alpha\beta) \in D$ para todo $\beta \in \mathfrak{a}$. Esto significa que $s\alpha \in \mathfrak{a}'$ y así $\alpha \in S^{-1}(\mathfrak{a}')$. ∎

En las condiciones del teorema anterior, si $\mathfrak{p}$ es un primo en D, sus divisores primos en E son $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ y $S = D \setminus \mathfrak{p}$, el teorema 2.33 nos permite identificar a $\mathfrak{p}$ con el único primo de $D_\mathfrak{p}$ y a $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ con los únicos primos de $E_\mathfrak{p}$. Lo que afirma entonces el teorema es que el complementario local $\mathfrak{a}'_\mathfrak{p}$ está formado por las potencias de $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ que dividen al complementario global $\mathfrak{a}'$. Si identificamos cada $\mathfrak{a}_\mathfrak{p}$ con un ideal fraccional de E tenemos

$$\mathfrak{a}' = \prod_\mathfrak{p} \mathfrak{a}'_\mathfrak{p},$$

donde $\mathfrak{p}$ recorre los primos de D. De esta fórmula se desprende que todos los factores son iguales a 1 salvo a lo sumo un número finito de ellos.

Veamos un último resultado sobre complementarios de ideales fracionales:

Teorema 9.20 *Sea E/D una extensión finita de dominios de Dedekind y sea $\mathfrak{a}$ un ideal fraccional de E. Entonces $\mathfrak{a}' = E'\mathfrak{a}^{-1}$.*

DEMOSTRACIÓN: Claramente $\mathrm{Tr}[E'\mathfrak{a}^{-1}\mathfrak{a}] \subset \mathrm{Tr}[E'E] \subset D$, de donde se sigue que $E'\mathfrak{a}^{-1} \subset \mathfrak{a}'$. Además $\mathrm{Tr}[\mathfrak{a}'\mathfrak{a}E] = \mathrm{Tr}[\mathfrak{a}'\mathfrak{a}] \subset D$, con lo que $\mathfrak{a}'\mathfrak{a} \subset E'$, y de aquí que $\mathfrak{a}' \subset E'\mathfrak{a}^{-1}$. ∎

Por lo tanto el cálculo de ideales complementarios se reduce al cálculo de E'.

9.4 Diferentes

En la sección siguiente definiremos el concepto de discriminante de una extensión de dominios de Dedekind, que generalizará al concepto que conocemos de discriminante de un cuerpo numérico. Aquí vamos a presentar primero un concepto muy relacionado que enlaza mejor con la dualidad que acabamos de estudiar.

Definición 9.21 Sea E/D una extensión separable de dominios de Dedekind. Llamaremos *diferente* de la extensión a $\mathfrak{D} = (E')^{-1}$. Por la definición de complementario es obvio que $E \subset E'$, de donde $\mathfrak{D} = (E')^{-1} \subset E^{-1} = E$, es decir, $\mathfrak{D}$ es un ideal de E.

En estos términos el teorema 9.20 afirma que si $\mathfrak{a}$ es un ideal fraccional de E entonces $\mathfrak{a}' = (\mathfrak{D}\mathfrak{a})^{-1}$. Además, del teorema 9.19 se sigue que si $\mathfrak{p}$ es un ideal primo de D, entonces la localización $\mathfrak{D}_\mathfrak{p}$ del diferente es el diferente de la extensión local $E_\mathfrak{p}/D_\mathfrak{p}$. Por consiguiente podemos factorizar

$$\mathfrak{D} = \prod_\mathfrak{p} \mathfrak{D}_\mathfrak{p},$$

donde $\mathfrak{p}$ recorre los primos de D. En particular, todos los diferentes locales son unitarios salvo a lo sumo una cantidad finita de ellos.

El diferente de una extensión E/D es muy fácil de calcular cuando E es una extensión simple de D, es decir, cuando E es de la forma $D[\alpha]$. Para verlo necesitamos el resultado siguiente:

Teorema 9.22 *Sea $K = k(\alpha)$ una extensión de cuerpos separable de grado n. Sea $f \in k[x]$ el polinomio mínimo de α. Sea*

$$\frac{f(x)}{x-\alpha} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}.$$

Entonces la base dual de $1, \alpha, \ldots, \alpha^{n-1}$ es

$$\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}.$$

Demostración: Sean $\alpha_1, \ldots, \alpha_n$ las raíces de f. Si $0 \le r \le n-1$ se cumple que

$$\sum_{i=1}^{n} \frac{f(x)}{x-\alpha_i}\,\frac{\alpha_i^r}{f'(\alpha_i)} = x^r.$$

En efecto, la diferencia entre ambos miembros es un polinomio de grado menor o igual que $n-1$ y tiene por raíces a todos los α_i, luego es idénticamente nulo. Los sumandos del miembro izquierdo son todos los conjugados del polinomio

$$\frac{f(x)}{x-\alpha}\,\frac{\alpha^r}{f'(\alpha)},$$

luego la suma tiene por coeficientes a las trazas de los coeficientes de este último polinomio.

El coeficiente i-ésimo es $f'(\alpha)^{-1}b_i\alpha^r$, luego hemos obtenido que

$$\mathrm{Tr}\left(\frac{b_i}{f'(\alpha)}\,\alpha^r\right) = \begin{cases} 1 & \text{si } i = r,\\ 0 & \text{si } i \ne r. \end{cases}$$

■

Teorema 9.23 *Sea E/D una extensión separable de dominios de Dedekind, sea K/k la extensión de sus cuerpos de cocientes, sea $\mathfrak{D}$ el diferente de la extensión, sea $\alpha \in E$ tal que $K = k(\alpha)$ y sea $f(x)$ el polinomio mínimo de α sobre k. Entonces $f'(\alpha) \in \mathfrak{D}$ y si $E = D[\alpha]$ entonces $\mathfrak{D} = (f'(\alpha))$.*

DEMOSTRACIÓN: Como α es entero sobre D, tenemos que

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in D[x],$$

luego $L = D[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_D$, donde n es el grado de la extensión. Por 9.18 y el teorema anterior (con la notación de éste último),

$$L' = \left\langle \frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)} \right\rangle_D.$$

Ahora bien, la igualdad

$$f(x) = (x-\alpha)(b_0 + b_1 x + \cdots + b_{n-1}x^{n-1})$$

nos da las relaciones

$$a_i = b_{i-1} - \alpha b_i, \quad i = 1, \ldots, n-1, \qquad b_{n-1} = 1.$$

Por recurrencia resulta

$$\begin{aligned} b_{n-1} &= 1 \\ b_{n-2} &= a_{n-1} + \alpha \\ b_{n-3} &= a_{n-1} + a_{n-2}\alpha + a_{n-1}\alpha^2 \\ \cdots &\quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ b_0 &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n \end{aligned}$$

De aquí se sigue que

$$L' = \frac{1}{f'(\alpha)}\,\langle b_0, b_1, \ldots, b_{n-1}\rangle_D = \frac{1}{f'(\alpha)}\,\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_D = \frac{1}{f'(\alpha)}\,L.$$

Como $\alpha \in E$, tenemos que $L \subset E$, luego $E' \subset L' = L/f'(\alpha)$ y operando $(f'(\alpha)) = L\mathfrak{D} \subset \mathfrak{D}$, luego $f'(\alpha) \in \mathfrak{D}$.

Si $E = D[\alpha] = L$ lo que hemos probado es que $E' = E/f'(\alpha)$, luego operando $(f'(\alpha)) = \mathfrak{D}$. ∎

Este teorema nos permite calcular los diferentes de las extensiones más sencillas, como son los cuerpos cuadráticos y ciclotómicos (sobre $\mathbb{Q}$). Por ejemplo, el diferente de $\mathbb{Z}\big[\sqrt{7}\,\big]/\mathbb{Z}$ es $\mathfrak{D} = (2\sqrt{7}\,)$.

Un hecho muy importante es la transitividad de los diferentes:

Teorema 9.24 *Sea $D \subset E \subset F$ una cadena de extensiones separables de dominios de Dedekind. Entonces $\mathfrak{D}_{F/D} = \mathfrak{D}_{F/E}\mathfrak{D}_{E/D}$ (considerándolos a todos como ideales en F).*

DEMOSTRACIÓN: Hay que probar que $F'_{F/D} = F'_{F/E}E'_{E/D}$. Sean $k \subset K \subset L$ los cuerpos de cocientes correspondientes. Entonces

$$\begin{aligned} \mathrm{Tr}_k^L[F'_{F/E}E'_{E/D}F] &= \mathrm{Tr}_k^K\big[\mathrm{Tr}_K^L[F'_{F/E}E'_{E/D}F]\big] \\ &= \mathrm{Tr}_k^K\big[E'_{E/D}\,\mathrm{Tr}_K^L[F'_{F/E}F]\big] \subset \mathrm{Tr}_k^K\,[E'_{E/D}E] \subset D, \end{aligned}$$

luego $F'_{F/E}E'_{E/D} \subset F'_{F/D}$.

Sea $\alpha \in F'_{F/D}$. Entonces $\mathrm{Tr}_k^L[\alpha F] \subset D$, pero como $EF = F$ resulta que

$$\mathrm{Tr}_k^L[\alpha F] = \mathrm{Tr}_k^K\left[\mathrm{Tr}_K^L[\alpha F]\right] = \mathrm{Tr}_k^K\left[\mathrm{Tr}_K^L[\alpha EF]\right] = \mathrm{Tr}_k^K\left[E\,\mathrm{Tr}_K^L[\alpha F]\right] \subset D,$$

luego $\mathrm{Tr}_K^L[\alpha F] \subset E'_{E/D}$ y, en consecuencia, $(E'_{E/D})^{-1}\,\mathrm{Tr}_K^L[\alpha F] \subset E$. Como $(E'_{E/D})^{-1} \subset K$, esto equivale a que $\mathrm{Tr}_K^L[\alpha(E'_{E/D})^{-1}F] \subset E$, luego tenemos que $\alpha(E'_{E/D})^{-1} \subset F'_{F/E}$, y así concluimos que $\alpha \in F'_{F/E}E'_{E/D}$. ∎

Veamos ahora que los diferentes también se comportan consistentemente con las compleciones.

Teorema 9.25 *Sea K/k una extensión de cuerpos numéricos y sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{p}$ un primo en D y sea $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$. Sea $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ la extensión de las compleciones y $E_{\mathfrak{P}}/D_{\mathfrak{p}}$ la extensión de enteros correspondiente. Entonces el diferente local $\mathfrak{D}_{\mathfrak{P}} = \mathfrak{D}_{E_{\mathfrak{P}}/D_{\mathfrak{p}}}$ es la mayor potencia de $\mathfrak{P}$ que divide al diferente global $\mathfrak{D} = \mathfrak{D}_{E/D}$. Consecuentemente*

$$\mathfrak{D} = \prod_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}},$$

donde $\mathfrak{P}$ recorre los primos de E.

Demostración: Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ los primos de E que dividen a $\mathfrak{p}$. Supongamos por ejemplo que $\mathfrak{P} = \mathfrak{P}_1$. Sea $\mathrm{Tr} : K \longrightarrow k$ la traza de la extensión K/k y sean $\mathrm{Tr}_i : K_{\mathfrak{P}_i} \longrightarrow k_{\mathfrak{p}}$ las trazas locales.

Sea $S = D \setminus \mathfrak{p}$. Claramente $S^{-1}E \subset E_{\mathfrak{P}}$. Vamos a probar que $(S^{-1}E)'$ es denso en $(E_{\mathfrak{P}})'$ (el primer complementario respecto a la extensión $S^{-1}E/S^{-1}D$, el segundo respecto a $E_{\mathfrak{P}}/D_{\mathfrak{p}}$).

En primer lugar probamos que $(S^{-1}E)' \subset (E_{\mathfrak{P}})'$. Sea $x \in (S^{-1}E)'$ y sea $y \in E_{\mathfrak{P}}$. Hemos de comprobar que $\mathrm{Tr}_1(xy) \in D_{\mathfrak{p}}$, o sea, que $|\,\mathrm{Tr}_1(xy)| \le 1$.

Por densidad existe un elemento de K arbitrariamente próximo a y respecto al valor absoluto de $\mathfrak{P}_1$, y aplicándole el teorema de aproximación obtenemos un elemento $\alpha \in K$ arbitrariamente próximo a y respecto a $\mathfrak{P}_1$ y arbitrariamente próximo a 0 respecto a los otros primos.

En particular, puesto que $|y|_{\mathfrak{P}_1} \le 1$, podemos exigir que $|\alpha|_{\mathfrak{P}_i} \le 1$ para $i = 1, \ldots, r$, con lo que $\alpha \in S^{-1}E$ (pues α se expresa como una fracción de modo que los primos de $S^{-1}E$ dividen al numerador con multiplicidad mayor o igual que al denominador y, puesto que $S^{-1}E$ tiene factorización única, podemos simplificarlos hasta obtener un elemento de $S^{-1}E$). Por consiguiente tenemos que $\mathrm{Tr}(x\alpha) \in S^{-1}D \subset D_{\mathfrak{p}}$.

Por otro lado, las trazas Tr_i son continuas, luego tomando aproximaciones adecuadas podemos exigir que $|\,\mathrm{Tr}_1(xy) - \mathrm{Tr}_1(x\alpha)| \le 1$ y $|\,\mathrm{Tr}_i(x\alpha)| \le 1$ para $i = 2, \ldots, r$. Ahora aplicamos la relación (5.4):

$$\mathrm{Tr}(x\alpha) = \mathrm{Tr}_1(x\alpha) + \sum_{i=2}^{r} \mathrm{Tr}_i(x\alpha),$$

y vemos que tanto el miembro izquierdo como los términos del sumatorio están en $D_{\mathfrak{p}}$, luego también $\mathrm{Tr}_1(x\alpha) \in D_{\mathfrak{p}}$, es decir, $|\,\mathrm{Tr}_1(x\alpha)| \le 1$ y por consiguiente $|\,\mathrm{Tr}_1(xy)| \le 1$, como había que probar.

Ahora tomemos un $x \in (E_\mathfrak{P})'$ y vamos a encontrarle elementos arbitrariamente próximos en $(S^{-1}E)'$. Como K es denso en $K_\mathfrak{P}$ podemos encontrar un elemento de K arbitrariamente próximo a x y, aplicando a éste el teorema de aproximación, llegamos a un $\alpha \in K$ arbitrariamente próximo a x respecto a $\mathfrak{P}_1$ y arbitrariamente próximo a 0 respecto a los demás valores absolutos.

Veamos que $\alpha \in (S^{-1}E)'$. Para ello tomamos $y \in S^{-1}E$ y probamos que $\mathrm{Tr}(\alpha y) \in S^{-1}D$, es decir, que $|\,\mathrm{Tr}(\alpha y)| \leq 1$. Sabemos que $|\,\mathrm{Tr}_1(xy)| \leq 1$.

Con aproximaciones adecuadas podemos exigir que $|\,\mathrm{Tr}_1(xy) - \mathrm{Tr}_1(\alpha y)| \leq 1$ y $|\,\mathrm{Tr}_i(\alpha y)| \leq 1$ para $i = 2, \ldots, r$ (y, de hecho, para $i = 1$ también).

La relación entre las trazas nos da ahora que $|\,\mathrm{Tr}(\alpha y)| \leq 1$, como queríamos probar. No obstante esto no justifica que $\alpha \in (S^{-1}E)'$, porque en realidad la elección de α que hemos hecho para que se cumpla $\mathrm{Tr}_1(\alpha y) \in S^{-1}D$ depende de y. Ahora bien, podemos encontrar un mismo α que haga $\mathrm{Tr}_1(\alpha y) \in S^{-1}D$ para un conjunto finito fijo de elementos $y \in S^{-1}E$, y como $S^{-1}E$ es un $S^{-1}D$-módulo finitamente generado, basta asegurarlo para los elementos de un generador.

Tenemos, pues, que $(S^{-1}E)'$ es denso en $(E_\mathfrak{P})'$. Por otra parte es claro que $S^{-1}E$ es denso en $E_\mathfrak{P}$ (pues $E \subset S^{-1}E$ es denso en $E_\mathfrak{P}$).

El anillo $S^{-1}E$ es un dominio de Dedekind con un número finito de primos, luego es un dominio de ideales principales. En particular el diferente de la extensión $S^{-1}E/S^{-1}D$ será de la forma $\mathfrak{D}_\mathfrak{p} = (\alpha) = \alpha S^{-1}E$, luego $(S^{-1}E)' = \alpha^{-1}S^{-1}E$. Tomando clausuras queda $(E_\mathfrak{P})' = \alpha^{-1}E_\mathfrak{P} = (\alpha)^{-1}$, de donde $\mathfrak{D}_\mathfrak{P} = (\alpha) = \mathfrak{P}^n$, donde $n = v_\mathfrak{P}(\alpha)$ es el exponente de $\mathfrak{P}$ en α, o sea, en $\mathfrak{D}_\mathfrak{p}$, y por el teorema anterior también en el diferente global $\mathfrak{D}$. ∎

Como consecuencia, si K/k es una extensión de cuerpos numéricos, E/D es la extensión de sus anillos de enteros, $\mathfrak{p}$ es un primo en D, $\mathfrak{D}_\mathfrak{p}$ es el diferente de la extensión $S^{-1}E/S^{-1}D$ (donde $S = D \setminus \mathfrak{p}$) y para cada primo $\mathfrak{P}$ que divida a $\mathfrak{p}$ en E llamamos $\mathfrak{D}_\mathfrak{P}$ al diferente de la extensión de compleciones $K_\mathfrak{P}/k_\mathfrak{p}$, los teoremas anteriores prueban que

$$\mathfrak{D}_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{D}_\mathfrak{P}.$$

Así pues, una forma de calcular diferentes es calcular los diferentes locales. Una de las razones por las que este planteamiento resulta ventajoso es que los diferentes locales siempre pueden ser calculados mediante el teorema 9.23. Para demostrarlo veremos primero un resultado técnico.

Teorema 9.26 *Sea E/D una extensión finita de dominios de Dedekind. Supongamos que D tiene un único primo $\mathfrak{p}$ y que E tiene un único primo $\mathfrak{P}$. Sea $\alpha \in E$ tal que $E/\mathfrak{P} = (D/\mathfrak{p})[\alpha]$ y sea $\pi \in E$ tal que $\mathfrak{P} = (\pi)$. Entonces $E = D[\alpha, \pi]$.*

Demostración: Llamemos $F = D[\alpha, \pi]$. Basta probar que $\mathfrak{p}E + F = E$, pues entonces, considerando a E y F como D-módulos, $\mathfrak{p}(E/F) = E/F$, y el teorema 2.27 nos da que $E/F = 0$, o sea, $E = F$.

Pero $\mathfrak{p}E$ es simplemente $\mathfrak{p}$ visto como ideal en E, es decir, $\mathfrak{p}E = \mathfrak{P}^e$ para cierto natural e. Lo que hay que probar es que todo elemento de E es congruente módulo $\mathfrak{P}^e$ con uno de F. Tenemos

$$\mathfrak{P}^e \subset \mathfrak{P}^{e-1} \subset \cdots \subset \mathfrak{P}^2 \subset \mathfrak{P} \subset E.$$

Es claro que la aplicación $f : E/\mathfrak{P} \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$ definida por $f([u]) = [\pi^i u]$ es un isomorfismo de $D/\mathfrak{p}$-espacios vectoriales. Una base de $E/\mathfrak{P}$ la forman las clases de los elementos $1, \alpha, \ldots, \alpha^{f-1}$, luego una base de $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ es $\pi^i\alpha^j$, para $j = 0, \ldots, f-1$.

Es claro que la unión de estas bases, es decir, el conjunto de elementos de la forma $\pi^i\alpha^j$, para $i = 0, \ldots, e-1$, $j = 0, \ldots, f-1$, forma un generador de $E/\mathfrak{P}^e$ como $D/\mathfrak{p}$-espacio vectorial. De aquí se sigue inmediatamente lo buscado. ∎

Teorema 9.27 *Sea E/D una extensión de dominios de Dedekind. Supongamos que E tiene un único primo $\mathfrak{P}$ y que D tiene un único primo $\mathfrak{p}$ de modo que $E/\mathfrak{P}$ sea una extensión separable de $D/\mathfrak{p}$. Entonces existe un $\alpha \in E$ tal que $E = D[\alpha]$ y cualquier β suficientemente próximo a α cumple igualmente $E = D[\beta]$.*

Demostración: Sea $E/\mathfrak{P} = (D/\mathfrak{p})[\gamma]$. Sea $f(x) \in D[x]$ un polinomio mónico tal que su imagen en $(D/\mathfrak{p})[x]$ sea el polinomio mínimo de $[\gamma]$. Sea $\mathfrak{P} = (\rho)$.

Los dos primeros términos del desarrollo de Taylor de f alrededor de γ tienen coeficientes enteros, luego el resto es un polinomio con coeficientes enteros y divisible entre $(x-\gamma)^2$. Evaluando en $\gamma + \rho$ queda

$$f(\gamma + \rho) \equiv f(\gamma) + f'(\gamma)\rho \pmod{\mathfrak{P}^2}.$$

Como γ es separable (mód $\mathfrak{P}$) tenemos $f'(\gamma) \not\equiv 0 \pmod{\mathfrak{P}}$, por lo que $f'(\gamma)\rho \not\equiv 0 \pmod{\mathfrak{P}^2}$. Esto significa que o bien $f(\gamma+\rho)$ o bien $f(\gamma)$ no es congruente con 0 (mód $\mathfrak{P}^2$). Tomamos $\alpha = \gamma + \rho$ o $\alpha = \gamma$ de modo que $\pi = f(\alpha) \not\equiv 0 \pmod{\mathfrak{P}^2}$.

El cualquier caso tenemos $\alpha \equiv \gamma \pmod{\mathfrak{P}}$, luego $E/\mathfrak{P} = (D/\mathfrak{p})[\alpha]$ y así mismo $\pi \equiv f(\gamma) \equiv 0 \pmod{\mathfrak{P}}$, luego $\mathfrak{P} = (\pi)$. Además $\pi = f(\alpha) \in D[\alpha]$. Por el teorema anterior $E = D[\alpha, \pi] = D[\alpha]$.

La última afirmación de sigue de la continuidad de f en α y de que $f(\alpha) = \pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, que es un abierto. Si β está cerca de α se cumplirá que $\pi' = f(\beta)$ estará en $\mathfrak{P} \setminus \mathfrak{P}^2$, luego se cumplirá $\mathfrak{P} = (\pi')$ y podemos concluir igual que con α y π. ∎

Ahora veremos que localizando y aplicando el teorema anterior y el teorema 9.23 podemos generalizar éste último a extensiones cualesquiera.

Teorema 9.28 *Sea K/k una extensión de cuerpos numéricos y sea E/D la extensión de sus anillos de enteros. Entonces el diferente de la extensión es el máximo común divisor de todos los números $f'(\alpha)$, donde $\alpha \in E$ cumple $K = k(\alpha)$ y $f \in D[x]$ es el polinomio mínimo de α.*

DEMOSTRACIÓN: Sea $K = k(\alpha)$ con $\alpha \in E$ y sea f su polinomio mínimo. Entonces $D[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_D \subset E$. El mismo razonamiento empleado en el teorema 9.23 nos da ahora que $E' \subset E/f'(\alpha)$, luego $(f'(\alpha)) \subset \mathfrak{D}$, es decir, $\mathfrak{D} \mid f'(\alpha)$.

Para demostrar que $\mathfrak{D}$ es el máximo común divisor de todos estos elementos basta probar que para todo primo $\mathfrak{P}$ existe un α tal que el orden de multiplicidad de $\mathfrak{P}$ en $\mathfrak{D}$ es el mismo que en $f'(\alpha)$.

Sea $\mathfrak{p}$ el primo en D divisible entre $\mathfrak{P}$. Tomemos una clausura algebraica $\mathbb{K}_\mathfrak{p}$ de $k_\mathfrak{p}$ que contenga a $K_\mathfrak{P}$. De este modo, el valor absoluto de $\mathfrak{P}$ está inducido por la identidad de K en $\mathbb{K}_\mathfrak{p}$.

Por el teorema anterior existe un $\beta \in E$ tal que $E_\mathfrak{P} = D_\mathfrak{p}[\beta]$. Veamos que tomando adecuadamente $a = 0, 1$ se cumple que $|\lambda(\beta) - a| = 1$ para todo $k_\mathfrak{p}$-automorfismo λ de $\mathbb{K}_\mathfrak{p}$.

En efecto, sea L la adjunción a $K_\mathfrak{P}$ de todos los $\lambda(\beta)$. Sea $\mathfrak{Q}$ su único primo y $F_\mathfrak{Q}$ su anillo de enteros. Entonces las clases $[\lambda(\beta)]$ módulo $\mathfrak{Q}$ son conjugadas sobre $D_\mathfrak{p}/\mathfrak{p}$. Si son todas nulas entonces $|\lambda(\beta)| < 1$ para todo λ, luego sirve $a = 1$. Si ninguna es nula entonces $|\lambda(\beta)| = 1$ para todo λ, luego sirve $a = 0$.

Sea $\sigma_1, \ldots, \sigma_r : K \longrightarrow \mathbb{K}_\mathfrak{p}$ un conjunto de k-monomorfismos no equivalentes que induzcan todos los valores absolutos en K correspondientes a divisores de $\mathfrak{p}$. Podemos suponer que σ_1 es la identidad y por lo tanto induce el valor absoluto de $\mathfrak{P}$. Sea $\epsilon > 0$. Por el teorema chino del resto existe un $\alpha \in E$ tal que

$$|\alpha - \beta|_\mathfrak{P} < \epsilon, \qquad |\alpha - a|_{\mathfrak{P}'} < \epsilon,$$

para todo primo $\mathfrak{P}' \neq \mathfrak{P}$ que divida a $\mathfrak{p}$ (usamos el teorema chino del resto y no el teorema de aproximación para garantizar que $\alpha \in E$). Equivalentemente, en términos del valor absoluto de $\mathbb{K}_\mathfrak{p}$,

$$|\alpha - \beta| < \epsilon, \qquad |\sigma_i(\alpha) - a| < \epsilon, \quad \text{para } i = 2, \ldots, r. \tag{9.1}$$

Sea $K = k(\gamma)$. Sea $\pi \in \mathfrak{p}$. Entonces $K = k(\pi^m\gamma)$ para cualquier $m \geq 0$. Si tomamos m suficientemente grande como para que $|\pi^m\gamma|$ sea menor que la distancia entre dos conjugados cualesquiera de α, es claro que los números $\alpha' + \pi^m\gamma'$, cuando α' varía en los conjugados de α y γ' en los conjugados de γ, son distintos dos a dos, pero cada conjugado de $\alpha + \pi^m\gamma$ es de la forma $\alpha' + \pi^m\gamma'$, donde γ' recorre todos los conjugados de γ y α' es un conjugado de α que depende de γ'. Concluimos que $\alpha + \pi^m\gamma$ tiene tantos conjugados como γ, luego $K = k(\alpha + \pi^m\gamma)$.

Si exigimos además que $|\pi^m\gamma| < \epsilon$, tenemos que $\alpha + \pi^m$ cumple también (9.1), es decir, podemos suponer que $K = k(\alpha)$.

Si tomamos ϵ suficientemente pequeño podemos aplicar el teorema anterior y concluir que $E_\mathfrak{P} = D_\mathfrak{p}[\beta] = D_\mathfrak{p}[\alpha]$.

Notemos que, en general, si f es un polinomio mónico e irreducible con raíz α, entonces f se descompone como producto de $x - \alpha'$, donde α' recorre los conjugados de α, y al derivar se obtiene que $f'(\alpha)$ se descompone como producto de $\alpha - \alpha'$, donde α' recorre los conjugados de α distintos de él mismo.

El teorema 9.23 nos da que el diferente local $\mathfrak{D}_\mathfrak{P}$ es el producto de todos los $\alpha - \sigma(\alpha)$, donde σ recorre los k-monomorfismos $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ que se extienden a $K_\mathfrak{P}$, es decir, que son equivalentes a la identidad σ_1, pero distintos de ella.

Por otro lado, si f es el polinomio mínimo de α sobre K, tenemos también que $f'(\alpha)$ es el producto de los $\alpha - \sigma(\alpha)$, donde σ recorre los k-monomorfismos $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ distintos de la identidad.

Por el teorema 9.25 sabemos que el exponente de $\mathfrak{P}$ en el diferente global $\mathfrak{D}$ es el mismo que en $\mathfrak{D}_\mathfrak{P}$, y lo que queremos probar es que coincide con el exponente de $\mathfrak{P}$ en $f'(\alpha)$, luego basta probar que $\mathfrak{P}$ no divide a ningún factor $\alpha - \sigma(\alpha)$, donde $\sigma : K \longrightarrow K_\mathfrak{p}$ es un k-monomorfismo que no se extiende a $K_\mathfrak{P}$, es decir, que determina un primo de K distinto de $\mathfrak{P}$.

Un tal σ será equivalente a un cierto σ_i para $i = 2, \ldots, r$, o sea, existe un $k_\mathfrak{p}$-automorfismo λ de $\mathbb{K}_\mathfrak{p}$ tal que $\sigma(\alpha) = \lambda(\sigma_i(\alpha))$. Así pues

$$|\alpha - \sigma(\alpha)| = |\alpha - \lambda(\sigma_i(\alpha))| = |\lambda^{-1}(\alpha) - \sigma_i(\alpha)| = |\lambda^{-1}(\alpha) - a + a - \sigma_i(\alpha)|.$$

Como $|\lambda^{-1}(\alpha) - a| = 1$ y $|a - \sigma_i(\alpha)| < \epsilon$, concluimos que $|\alpha - \sigma(\alpha)| = 1$, luego el factor no es divisible entre $\mathfrak{P}$. ∎

Finalmente vamos a mostrar la relación que existe entre el diferente y la ramificación.

Teorema 9.29 *Sea K/k una extensión finita separable de cuerpos métricos discretos completos tal que el cuerpo de restos $\overline{k}$ sea perfecto, sea $e = e(K/k)$, sea $\mathfrak{D}$ el diferente de la extensión y $\mathfrak{P}$ el ideal primo de $\mathcal{O}_K$. Entonces:*

1. *Si $\mathfrak{P} \nmid e$, entonces $\mathfrak{D} = \mathfrak{P}^{e-1}$.*
2. *Si $\mathfrak{P} \mid e$, entonces $\mathfrak{P}^e \mid \mathfrak{D}$.*
3. *En particular $e > 1$ si y sólo si $\mathfrak{P} \mid \mathfrak{D}$.*

Demostración: Veamos en primer lugar que si $e = 1$ entonces $\mathfrak{D} = 1$ (notemos que esto es un caso particular de 1). Por el teorema del elemento primitivo, existe $\alpha \in \mathcal{O}$ tal que $\overline{K} = \overline{k}(\alpha)$. Si $e = 1$, el teorema 9.26 nos da que $\mathcal{O}_K = \langle 1, \alpha, \ldots \alpha^{n-1} \rangle_{\mathcal{O}_k}$ y 9.23 nos da entonces que $\mathfrak{D} = (f'(\alpha))$, donde $f(x) \in \mathcal{O}_k[x]$ es el polinomio mínimo de α. Puesto que $|K : k| = |\overline{K} : \overline{k}|$, la imagen de f en $\overline{k}[x]$ ha de ser el polinomio mínimo de $[\alpha]$, en particular es irreducible y, por la separabilidad, $f'(\alpha) \not\equiv 0 \pmod{\mathfrak{P}}$, es decir, $\mathfrak{P} \nmid \mathfrak{D}$, luego tiene que ser $\mathfrak{D} = 1$.

Supongamos ahora que $e > 1$. Por el teorema 9.8 podemos tomar un cuerpo intermedio $k \subset L \subset K$ de modo que $|K : L| = e(K/L) = e$ y $e(L/k) = 1$. Por la parte ya probada sabemos que $\mathfrak{D}_{L/k} = 1$, luego $\mathfrak{D} = \mathfrak{D}_{K/L}$. Así pues, basta probar el resto del teorema para la extensión K/L o, equivalentemente, podemos suponer que $|K : k| = e$. Así, podemos aplicar el teorema 9.9, según el cual $K = k(\pi)$, donde π es un primo en K cuyo polinomio mínimo en k es un polinomio de Eisenstein

$$f(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_1 x + a_0, \qquad \pi^e \mid a_i.$$

El teorema 9.26 nos da que $\mathcal{O}_K = \langle 1, \pi, \ldots, \pi^{e-1} \rangle_{\mathcal{O}_k}$, luego por 9.23 tenemos que $\mathfrak{D} = (f'(\pi))$. Ahora basta observar que

$$f'(\pi) = e\pi^{e-1} + (e-1)a_{e-1}\pi^{e-2} + \cdots + a_1.$$

Si $\mathfrak{P} \nmid e$, entonces todos los términos menos el primero son divisibles entre π^e, luego $v_{\mathfrak{P}}(f'(\pi)) = e-1$ y $\mathfrak{D} = \mathfrak{P}^{e-1}$. En cambio, si $\mathfrak{P} \mid e$, entonces todos los términos son divisibles entre π^e, luego $\mathfrak{P}^e \mid \mathfrak{D}$. Esto prueba 1) y 2), de donde 3) es inmediato. ∎

La condición $\mathfrak{p} \mid e$ puede darse exactamente en dos casos: que exista un primo $p \mid e$ tal que $\mathfrak{P} \mid p$ (lo cual no sucede con los cuerpos que nosotros estamos manejando, ya que las constantes son unidades) o bien porque K tenga característica prima p y $p \mid e$ (en cuyo caso $e = 0$ como elemento de K).

Pasamos ahora al caso de los cuerpos numéricos.

Definición 9.30 Los términos que introdujimos en el capítulo anterior para extensiones locales tienen sentido globalmente: Sea $\mathfrak{p}$ un primo en un cuerpo numérico, sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en una extensión de grado n, sea p el primo racional al cual dividen. Diremos que

1. $\mathfrak{p}$ es *no ramificado* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) = 1$,
2. $\mathfrak{p}$ es *ramificado* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) > 1$,
3. $\mathfrak{p}$ es *totalmente ramificado* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) = n$,
4. $\mathfrak{p}$ es *dominadamente ramificado* en $\mathfrak{P}$ si $p \nmid e(\mathfrak{P}/\mathfrak{p})$,
5. $\mathfrak{p}$ es *libremente ramificado* en $\mathfrak{P}$ si $p \mid e(\mathfrak{P}/\mathfrak{p})$.

También diremos que $\mathfrak{P}$ es *ramificado, totalmente ramificado, etc.* sobre $\mathfrak{p}$.

Teorema 9.31 *Sea K/k una extensión de cuerpos numéricos. Sea $\mathfrak{p}$ un primo en k, sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K, sea $e = e(\mathfrak{P}/\mathfrak{p})$ y $\mathfrak{D}$ el diferente de la extensión. Entonces:*

1. *Si el primo $\mathfrak{P}$ es dominadamente ramificado sobre $\mathfrak{p}$ entonces $\mathfrak{P}^{e-1} \mid \mathfrak{D}$, pero $\mathfrak{P}^e \nmid \mathfrak{D}$.*
2. *Si $\mathfrak{P}$ es libremente ramificado sobre $\mathfrak{p}$ entonces $\mathfrak{P}^e \mid \mathfrak{D}$.*
3. *En particular, $\mathfrak{P}$ es ramificado sobre $\mathfrak{p}$ si y sólo si $\mathfrak{P} \mid \mathfrak{D}$. El número de primos ramificados en K es finito.*

DEMOSTRACIÓN: Teniendo en cuenta que al localizar se conserva el exponente de $\mathfrak{P}$ en el diferente así como el grado de ramificación e, es claro que podemos localizar y suponer que los cuerpos K y k son completos, en cuyo caso la conclusión se sigue del teorema anterior. ∎

9.5 Discriminantes

Hemos definido el discriminante de un cuerpo numérico como el discriminante de una base entera. Si queremos extender esta definición a una extensión K/k de cuerpos numéricos nos encontramos con el problema de que el anillo de enteros de K no es necesariamente un módulo libre sobre el anillo de enteros de k, es decir, no tenemos necesariamente bases enteras (salvo que k tenga factorización única). Sin embargo, este inconveniente no afecta sustancialmente a la teoría de los discriminantes. Vamos a definir el discriminante de la extensión como un cierto ideal del cuerpo base k, de modo que si K admite una base entera sobre k, entonces el discriminante será el ideal principal generado por el discriminante de la base.

Definición 9.32 Sea K/k una extensión de cuerpos separable de grado n. Sean $\sigma_1, \dots, \sigma_n$ los k-monomorfismos de K en una clausura algebraica. Para cada conjunto de n elementos $W = \{w_1, \dots, w_n\} \subset K$ se define el *discriminante* de W como

$$\Delta[W] = \big(\det(\sigma_i(w_j))\big)^2 = \det\big((\sigma_k(w_i))(\sigma_k(w_j))\big) = \det\big(\mathrm{Tr}(w_i w_j)\big) \in k.$$

Los hechos siguientes son generalizaciones naturales de los hechos análogos que conocemos sobre los discriminantes de los cuerpos numéricos:

Es claro que $\Delta[W]$ no depende del orden de los elementos de W ni del de los monomorfismos. Si W es un sistema ligado sobre k entonces las columnas de la matriz $\big(\sigma_i(w_j)\big)$ son linealmente dependientes, luego $\Delta[W] = 0$.

Si W y W' son dos k-bases de K y $D^W_{W'}$ es la matriz del cambio de base (cuyas filas son las coordenadas de los elementos de W' en la base W) es fácil comprobar que

$$\Delta[W'] = |D^W_{W'}|^2 \Delta[W].$$

Si $K = k(\alpha)$, entonces una k-base de K es $1, \alpha, \dots, \alpha^{n-1}$, y

$$\Delta[\alpha] = \Delta[1, \alpha, \dots, \alpha^{n-1}] = \prod_{i<j} \big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2 \neq 0,$$

pues el determinante que aparece es del tipo de Vandermonde.

Uniendo todos estos hechos concluimos que $\Delta[W] = 0$ si y sólo si W es linealmente dependiente.

Otra propiedad fácil de comprobar es que

$$\Delta[\alpha w_1, \dots, \alpha w_n] = \mathrm{N}(\alpha)^2 \Delta[w_1, \dots, w_n].$$

Si E/D es una extensión separable de dominios de Dedekind y K/k es la extensión de los cuerpos de cocientes, es claro que si $W \subset E$ entonces $\Delta[W] \in D$.

Cuando $D = \mathbb{Z}$ todo D-módulo $M \subset K$ es libre y podemos definir $\Delta[M]$ como el discriminante de cualquier base de M (entendiendo que es 0 si el rango de M es menor que n). Si W y W' son dos bases de M entonces la matriz de cambio de base tiene determinante ± 1, luego $\Delta(W) = \Delta(W')$, y por lo tanto $\Delta(M)$ no depende de la elección de la base.

En el caso general no es cierto que todo D-módulo sea libre, y aún en tal caso los discriminantes de dos bases de un módulo libre no tienen por qué coincidir (se diferencian en el cuadrado de una unidad de D, que ya no tiene por qué ser igual a ± 1). Todo esto nos lleva a definir el discriminante de un D-módulo como otro D-módulo.

Definición 9.33 Sea E/D una extensión separable de grado n de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Si $M \subset K$ es un D-módulo llamaremos *discriminante* de M al D-módulo $\Delta[M]$ generado por los discriminantes $\Delta[W]$, donde W recorre los subconjuntos de M con n elementos.

Llamaremos *discriminante* de la extensión a $\Delta = \Delta[E]$. El teorema siguiente prueba entre otras cosas que Δ es un ideal no nulo de D:

Teorema 9.34 *Sea E/D una extensión separable de grado n de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Sea $M \subset K$ un D-módulo. Entonces*

1. *Si M admite una base W con n elementos, entonces $\Delta[M] = \langle \Delta[W] \rangle_D$.*
2. *Si $M \subset E$ entonces $\Delta[M]$ es un ideal de D.*
3. *Si M es un ideal no nulo (fraccional) de E entonces $\Delta[M]$ es un ideal no nulo (fraccional) de D.*
4. *Si $M \subset N \subset E$ son D-módulos libres de rango n entonces $\Delta[N] \mid \Delta[M]$ y $\Delta[M] = \Delta[N]$ si y sólo si $M = N$.*

Demostración: 1) Una inclusión es obvia. Si W' es un subconjunto de M con n elementos, entonces W y W' son dos k-bases de K y la matriz $D^W_{W'}$ de cambio de base tiene sus coeficientes en D. Por lo tanto

$$\Delta[W'] = |D^W_{W'}|^2 \Delta[W] \in \langle \Delta[W] \rangle_D \,,$$

y así tenemos la igualdad.

2) Si $M \subset E$ todos los discriminantes $\Delta[W]$ con $W \subset M$ están en D, luego $\Delta[M] \subset D$ y un D-módulo contenido en D es un ideal de D.

3) Si M es un ideal de E entonces $\Delta[M]$ es un ideal de D por el apartado 2). Sea W una k-base de K. Por el teorema 2.16 existe un $d \in D$ no nulo tal que $dW \subset E$, y dW sigue siendo una k-base de K. Si $M \neq 0$ tomamos $\alpha \in M \cap D$ no nulo, y entonces $\alpha dW \subset M$ y es una k-base, luego $0 \neq \Delta[\alpha dW] \in \Delta[M]$.

El mismo razonamiento prueba que si M es un ideal fraccional (no nulo) entonces $\Delta[M]$ es un D-módulo no nulo (y está contenido en k). Sea $\alpha \in K$ no nulo tal que $\alpha M \subset E$. Entonces $\Delta[\alpha M] = \mathrm{N}(\alpha)^2 \Delta[M] \subset D$, luego $\Delta[M]$ es un ideal fraccional de D.

4) Sea W una base de N y W' una base de M. Entonces la matriz $D^W_{W'}$ de cambio de base tiene coeficientes en D, luego $|D^W_{W'}| \in D$. Tenemos que $\Delta(W') = |D^W_{W'}|^2 \Delta(W)$ y, como $\Delta[M] = (\Delta[W'])$, $\Delta[N] = (\Delta[W])$, concluimos

que $\Delta[M] \subset \Delta[N]$ o, lo que es lo mismo, $\Delta[N] \mid \Delta[M]$, y que se da la igualdad si y sólo si $|D^W_{W'}|^2$ es una unidad en D, lo cual equivale a que la matriz $D^W_{W'}$ tenga inversa en D y a que W' sea también una base de N. ∎

Aunque tenemos un concepto de discriminante de un módulo válido en cualquier caso, el teorema anterior muestra que su comportamiento es mejor sobre los módulos libres de rango máximo. Cuando $D = \mathbb{Z}$ sabemos que todos los ideales fraccionales de E son de este tipo. Otro caso importante en el que esto sucede es cuando D tiene un único primo, pues entonces D es un dominio euclídeo (ver las observaciones tras el teorema 2.24) y los ideales fraccionales de E son D-módulos finitamente generados y libres de torsión, luego son libres. El hecho de que sus discriminantes sean no nulos prueba que tienen rango máximo. (Respecto al carácter finitamente generado de los ideales fraccionales, observemos que E es finitamente generado por el teorema 2.17 y como D es noetheriano también lo son los ideales de E, y de aquí que lo mismo vale para los ideales fraccionales).

En el caso $D = \mathbb{Z}$, la única información que se pierde al considerar los discriminantes como módulos en lugar de como números racionales es el signo, pues dos números racionales generan el mismo $\mathbb{Z}$-módulo si y sólo si se diferencian tan sólo en el signo.

Por otra parte, en virtud de la relación $\Delta[W'] = |D^W_{W'}|^2\Delta[W]$, sucede que todos los discriminantes de todos los $\mathbb{Z}$-módulos de un cuerpo numérico K tienen el mismo signo. Veamos que este signo es fácil de recuperar, con lo que en realidad trabajar con módulos no supone ningún inconveniente.

Teorema 9.35 *Sea K un cuerpo numérico y W una $\mathbb{Q}$-base de K. Entonces el signo de $\Delta[W]$ es $(-1)^t$, donde t es el número de primos infinitos complejos de K.*

Demostración: Por los comentarios anteriores basta analizar el signo del discriminante de una base concreta. Sea $K = \mathbb{Q}(\alpha)$ y consideremos

$$\Delta[\alpha] = \prod_{i<j} \big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2.$$

Dividamos los pares de índices (i, j) en tres grupos según que los monomorfismos asociados sean ambos reales, uno real y otro complejo o ambos complejos.

Es claro que si σ_i y σ_j son ambos reales entonces $\big(\sigma_j(\alpha)-\sigma_i(\alpha)\big)^2 > 0$, luego los factores del primer grupo no influyen en el signo.

Los factores del segundo tipo pueden ser agrupados en parejas formadas por un monomorfismo real acompañado por dos monomorfismos complejos conjugados. Entonces, si $\big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2$ es uno de estos factores, su pareja es $\big(\overline{\sigma_j(\alpha) - \sigma_i(\alpha)}\big)^2$, y el producto de ambos es $|\sigma_j(\alpha) - \sigma_i(\alpha)|^4 > 0$, luego los factores de este tipo tampoco contribuyen al signo.

Entre los factores del tercer tipo distingamos a su vez los formados por pares de monomorfismos conjugados y el resto. Si $\big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2$ es uno de

los factores restantes donde σ_i no es el conjugado de σ_j, entonces otro de los factores de este tipo es $\big(\overline{\sigma_j(\alpha)-\sigma_i(\alpha)}\big)^2$, y concluimos como antes.

De esta manera, los únicos factores que influyen en el signo son los de tipo $\big(\sigma_j(\alpha)-\sigma_i(\alpha)\big)^2$ donde σ_i y σ_j son conjugados. Entonces $\sigma_j(\alpha)-\sigma_i(\alpha)$ es imaginario puro y, por lo tanto, $\big(\sigma_j(\alpha)-\sigma_i(\alpha)\big)^2<0$. El número de factores de este tipo es claramente igual a t, de donde se concluye el teorema. ∎

Las propiedades básicas de los discriminantes las deduciremos de su comportamiento local, que estudiamos seguidamente.

Teorema 9.36 *Sea E/D una extensión separable de dominios de Dedekind y S un subconjunto multiplicativo de D. Sea $\mathfrak{a}$ un ideal fraccional de E. Entonces $S^{-1}\Delta[\mathfrak{a}]=\Delta[S^{-1}\mathfrak{a}]$.*

En particular si $\mathfrak{p}$ es un ideal primo de D y $\Delta_\mathfrak{p}$ es el discriminante de la extensión local $E_\mathfrak{p}/D_\mathfrak{p}$, entonces $\Delta_\mathfrak{p}$ es la mayor potencia de $\mathfrak{p}$ que divide al discriminante global Δ. Consecuentemente

$$\Delta=\prod_\mathfrak{p}\Delta_\mathfrak{p}.$$

Demostración: Si $W\subset S^{-1}\mathfrak{a}$, llamando s al producto de los denominadores (en S) de los elementos de W podemos expresar $W=W'/s$, donde $W'\subset\mathfrak{a}$. Entonces

$$\Delta[W]=\mathrm{N}(1/s)\Delta[W']=\frac{\Delta(W')}{s^n}\in S^{-1}\Delta[\mathfrak{a}],$$

luego $\Delta[S^{-1}\mathfrak{a}]\subset S^{-1}\Delta[\mathfrak{a}]$.

Por otra parte $S^{-1}\Delta[\mathfrak{a}]$ está generado como $S^{-1}D$-módulo por los elementos de la forma $\Delta[W]$, con $W\subset\mathfrak{a}\subset S^{-1}\mathfrak{a}$, pero $\Delta[W]\in\Delta[S^{-1}\mathfrak{a}]$, con lo que $S^{-1}\Delta(\mathfrak{a})\subset\Delta[S^{-1}\mathfrak{a}]$. ∎

La primera consecuencia es la versión general de un resultado que ya conocíamos para el caso $D=\mathbb{Z}$ (de hecho lo tomamos como definición de norma de un módulo 1.14):

Teorema 9.37 *Sea E/D una extensión separable de dominios de Dedekind, sea Δ su discriminante y sea $\mathfrak{a}$ un ideal fraccional de E. Entonces*

$$\Delta[\mathfrak{a}]=\mathrm{N}(\mathfrak{a})^2\Delta.$$

Demostración: Para probar esta igualdad de ideales fraccionales basta tomar un primo arbitrario $\mathfrak{p}$ de D y ver que su multiplicidad en ambos miembros es la misma. Para ello podemos localizar tomando $S=D\setminus\mathfrak{p}$ y demostrar que $\Delta[S^{-1}\mathfrak{a}]=\mathrm{N}(S^{-1}\mathfrak{a})^2\Delta[S^{-1}E]$.

En efecto, por el teorema anterior tenemos que

$$\Delta[S^{-1}\mathfrak{a}]=S^{-1}\Delta[\mathfrak{a}]\quad\text{y}\quad\Delta[S^{-1}E]=S^{-1}\Delta[E],$$

luego la multiplicidad de $\mathfrak{p}$ en $\Delta[\mathfrak{a}]$ y $\Delta[E]$ es la misma que la multiplicidad de $S^{-1}\mathfrak{p}$ en $\Delta(S^{-1}\mathfrak{a})$ y $\Delta(S^{-1}E)$.

Además, el exponente de $\mathfrak{p}$ en $\mathrm{N}(\mathfrak{a})$ es la suma de los productos de los grados de inercia de los divisores de $\mathfrak{p}$ en E por sus multiplicidades en $\mathfrak{a}$, y todo esto se conserva al localizar, luego también el exponente de $\mathfrak{p}$ en $\mathrm{N}(\mathfrak{a})^2$ es el mismo que el exponente de $S^{-1}\mathfrak{p}$ en $\mathrm{N}(S^{-1}\mathfrak{a})^2$.

Equivalentemente, podemos suponer que $\mathfrak{p}$ es el único primo de D, pero entonces D es un dominio euclídeo y E es un dominio de ideales principales (teorema 2.21).

Sea K/k la extensión de los cuerpos de cocientes. Sea $\mathfrak{a} = (\alpha) = \alpha E$, con $\alpha \in K$. Toda k-base de K contenida en $\mathfrak{a}$ es de la forma αW, donde W es una k-base contenida en E y, recíprocamente, dada W, la base αW está contenida en $\mathfrak{a}$. De la relación $\Delta[\alpha W] = \mathrm{N}(\alpha)^2\Delta[W]$ se sigue que $\Delta[\alpha E] = \mathrm{N}(\alpha)^2\Delta[E]$, o sea, $\Delta(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})^2\Delta$. ∎

Ahora estamos en condiciones de demostrar la relación ya anunciada entre el diferente y el discriminante de una extensión:

Teorema 9.38 *Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Entonces el discriminante Δ y el diferente $\mathfrak{D}$ de la extensión verifican que $\Delta = \mathrm{N}(\mathfrak{D})$.*

Demostración: El mismo argumento que en el teorema anterior nos permite suponer que D tiene un único primo. Entonces E es un D-módulo libre de rango máximo (ver las observaciones tras el teorema 9.34). Sea $W = (w_i)$ una base y sea W' la base dual. Por el teorema 9.18 sabemos que W' es base de E'.

$$\Delta[W]\Delta[W'] = \det\big(\sigma_i(w_j)\big)^2 \det(\sigma_i(w'_j))^2 = \det\big(\mathrm{Tr}(w_i w'_j)\big)^2 = 1,$$

luego $\Delta[E]\Delta[E'] = 1$. Usando esto y el teorema anterior obtenemos que

$$\Delta^{-1} = \Delta[E]^{-1} = \Delta[E'] = \Delta(\mathfrak{D}^{-1}) = \mathrm{N}(\mathfrak{D}^{-1})^2\Delta,$$

con lo que $\mathrm{N}(\mathfrak{D})^2 = \Delta^2$ y, en consecuencia, $\mathrm{N}(\mathfrak{D}) = \Delta$. ∎

De aquí se sigue una versión débil del teorema 9.31 en términos de discriminantes:

Teorema 9.39 *Sea E/D una extensión separable de dominios de Dedekind y sea $\mathfrak{p}$ un primo en D. Entonces $\mathfrak{p}$ se ramifica (sobre alguno de sus divisores) en E si y sólo si $\mathfrak{p} \mid \Delta$.*

Demostración: Si $\mathfrak{p}$ se ramifica sobre algún divisor $\mathfrak{P}$ entonces $\mathfrak{P} \mid \mathfrak{D}$, luego $\mathfrak{p} \mid \mathrm{N}(\mathfrak{P}) \mid \mathrm{N}(\mathfrak{D}) = \Delta$.

Si $\mathfrak{p} \mid \Delta = \mathrm{N}(\mathfrak{D})$, entonces algún divisor $\mathfrak{P}$ de $\mathfrak{p}$ cumple $\mathfrak{P} \mid \mathfrak{D}$, luego $\mathfrak{p}$ se ramifica sobre $\mathfrak{P}$. ∎

El teorema 3.13 afirma que el discriminante de un cuerpo numérico distinto de $\mathbb{Q}$ nunca es igual a ± 1, luego en todo cuerpo numérico existen siempre primos ramificados sobre $\mathbb{Q}$. Sin embargo el discriminante relativo de un cuerpo numérico respecto de un subcuerpo puede ser 1. Para ver un ejemplo demostraremos primero dos hechos generales de gran utilidad en la práctica. El primero es una consecuencia inmediata de los teoremas 9.24 y 9.38.

Teorema 9.40 *Sea $D \subset E \subset F$ una cadena de extensiones separables de dominios de Dedekind de grados m y n respectivamente. Entonces*

$$\Delta_{F/D} = \mathrm{N}_D^E(\Delta_{F/E})\,\Delta_{E/D}^n.$$

DEMOSTRACIÓN: Sean $k \subset K \subset L$ los cuerpos de cocientes. Tomando normas en la igualdad del teorema 9.24 queda

$$\begin{aligned}\Delta_{F/D} &= \mathrm{N}_k^L(\mathfrak{D}_{F/D}) = \mathrm{N}_k^L(\mathfrak{D}_{F/E})\,\mathrm{N}_k^L(\mathfrak{D}_{E/D}) = \mathrm{N}_k^K(\Delta_{F/E})\,\mathrm{N}_k^K(\mathfrak{D}_{E/D})^n\\ &= \mathrm{N}_D^E(\Delta_{F/E})\Delta_{E/D}^n.\end{aligned}$$

■

Teorema 9.41 *Sean K y L dos cuerpos numéricos de grados m y n respectivamente cuyos discriminantes sean primos entre sí. Entonces sus anillos de enteros cumplen $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$ y además $\Delta_{KL} = \Delta_K^n\Delta_L^m$.*

DEMOSTRACIÓN: Por la transitividad del diferente tenemos que

$$\mathfrak{D}_{KL/\mathbb{Q}} = \mathfrak{D}_{KL/K}\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{KL/L}\mathfrak{D}_{L/\mathbb{Q}}.$$

Por hipótesis $\mathfrak{D}_{K/\mathbb{Q}}$ y $\mathfrak{D}_{L/\mathbb{Q}}$ tienen normas primas entre sí, luego son primos entre sí. Vamos a probar que los dos factores restantes también son primos entre sí, con lo que podremos concluir que

$$\mathfrak{D}_{KL/K} = \mathfrak{D}_{L/\mathbb{Q}} \quad \text{y} \quad \mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{KL/L}. \tag{9.2}$$

Supongamos que existe un primo $\mathfrak{P}$ en KL tal que $\mathfrak{P} \mid \mathfrak{D}_{KL/K}$ y $\mathfrak{P} \mid \mathfrak{D}_{KL/L}$. Sean p, $\mathfrak{p}$ y $\mathfrak{p}'$ los primos en $\mathbb{Q}$, K y L respectivamente divisibles entre $\mathfrak{P}$. El teorema 9.31 nos da que $e(\mathfrak{P}/\mathfrak{p})$ y $e(\mathfrak{P}/\mathfrak{p}')$ son ambos mayores que 1. Si consideramos las compleciones respecto a estos primos resulta que $KL_{\mathfrak{P}}/K_{\mathfrak{p}}$ y $KL_{\mathfrak{P}}/L_{\mathfrak{p}'}$ son ambas ramificadas, luego por el teorema 9.4 b) llegamos a que $K_{\mathfrak{p}}/\mathbb{Q}_p$ y $L_{\mathfrak{p}'}/\mathbb{Q}_p$ también son ramificadas, pero entonces el teorema 9.31 nos da que $\mathfrak{p} \mid \mathfrak{D}_{K/\mathbb{Q}}$ y $\mathfrak{p}' \mid \mathfrak{D}_{L/\mathbb{Q}}$, luego $p \mid \Delta_K$ y $p \mid \Delta_L$, contradicción.

Sea W una $\mathbb{Z}$-base de $\mathcal{O}_K$. Sea W' la base dual. Entonces W' es una $\mathbb{Z}$-base de $(\mathfrak{D}_{K/\mathbb{Q}})^{-1}$, luego es también un generador como $\mathcal{O}_L$-módulo del ideal fraccional generado por $(\mathfrak{D}_{K/\mathbb{Q}})^{-1}$ en KL, que por (9.2) es $(\mathfrak{D}_{KL/L})^{-1}$. Dualizando de nuevo concluimos que W es un generador de $\mathcal{O}_{KL}$ como $\mathcal{O}_L$-módulo. Así pues, $\mathcal{O}_{KL} = \mathcal{O}_L[W] = \mathcal{O}_L\mathbb{Z}[W] = \mathcal{O}_L\mathcal{O}_K$.

La relación entre los discriminantes se obtiene tomando normas en

$$\mathfrak{D}_{KL/\mathbb{Q}} = \mathfrak{D}_{KL/K}\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{L/\mathbb{Q}}\mathfrak{D}_{K/\mathbb{Q}}.$$

En principio así obtenemos la igualdad como ideales, pero el signo es también correcto. Para probarlo observamos que $K \cap L = \mathbb{Q}$, ya que el discriminante de $K \cap L$ da lugar a un factor común en los discriminantes de K y L (por el teorema 9.40), luego ha de ser 1 y, en consecuencia (por [4.13]), $K \cap L = \mathbb{Q}$. De

aquí que los monomorfismos de KL se expresen de forma única como producto de los monomorfismos de K por los monomorfismos de L (una base de KL es el producto de una base de K por una base de L). Si K y L tienen t y t' primos complejos respectivamente, entonces tienen $2t$ y $2t'$ monomorfismos complejos, y KL tiene $2tn+2t'm-4tt'$ monomorfismos complejos (un producto de monomorfismos es complejo si y sólo si lo es al menos uno de los factores), luego KL tiene $tn+t'm-2tt'$ primos complejos, y el teorema 9.35 nos da que el signo es correcto. ∎

9.6 Ejemplos y aplicaciones

Vamos a dar algunos ejemplos que ilustren la potencia de la teoría que hemos desarrollado hasta aquí. Comenzamos con dos ejemplos de discriminante relativo igual a 1.

Ejemplo Consideremos el cuerpo $K = \mathbb{Q}(\sqrt{5},\sqrt{-5})$. Como $\mathbb{Q}(\sqrt{5})$ es un cuerpo real y por lo tanto no contiene a $\sqrt{-5}$, es claro que K es un cuerpo numérico de grado 4. Además K es el cuerpo de escisión de $(x^2+5)(x^2-5)$, luego K es una extensión de Galois de $\mathbb{Q}$.

Es claro que el grupo de Galois es producto de dos grupos cíclicos, y sus tres subgrupos propios se corresponden con los cuerpos intermedios $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$ y $\mathbb{Q}(i)$.

Los discriminantes de estos cuerpos son respectivamente 5, -20 y -4, luego podemos aplicar el teorema 9.41 a $\mathbb{Q}(\sqrt{5})$ y a $\mathbb{Q}(i)$ para concluir que el discriminante de K es $\Delta = 400$. El teorema 9.40 nos da entonces que el discriminante de K relativo a $\mathbb{Q}(\sqrt{-5})$ es 1. ∎

Ejemplo (Artin) Sea $K_5 = \mathbb{Q}(\alpha)$, donde α es una raíz del polinomio $f(x) = x^5 - x + 1$. Es fácil ver que $f(x)$ es irreducible módulo 3, luego es irreducible en $\mathbb{Q}[x]$ y por consiguiente K_5 tiene grado 5 sobre $\mathbb{Q}$. Se cumple que $\Delta[\alpha] = 19\cdot 151$ (ver el ejemplo y el ejercicio siguiente tras el teorema [2.8]). Como es libre de cuadrados podemos afirmar que el discriminante de K_5 es $\Delta = 19\cdot 151$.

Sea K el cuerpo de escisión de $f(x)$ sobre $\mathbb{Q}$. Vamos a probar que tiene grado 120 o, equivalentemente, que $G \cong \Sigma_5$, donde $G = G(K/\mathbb{Q})$ y Σ_5 es el grupo de permutaciones de 5 elementos. Si identificamos estos 5 elementos con las cinco raíces de f, entonces $G \le \Sigma_5$. Ahora consideramos las factorizaciones

$$\begin{aligned} f(x) &\equiv (x-6)^2(x^3+12x^2+13x+9) \text{ (mód 19)},\\ f(x) &\equiv (x-9)(x^4+9x^3+12x^2+16x+15) \text{ (mód 23)}. \end{aligned}$$

Según el teorema 2.35, el 19 tiene un divisor en K_5 con grado de inercia 3, y el 23 tiene un divisor con grado de inercia 4. Por lo tanto $60 = 5\cdot 4\cdot 3 \mid |G|$. Esto nos deja únicamente dos posibilidades para G: o bien $G = A_5$ o bien $G = \Sigma_5$. De la definición de discriminante se sigue que $\sqrt{\Delta} \in K$, luego $k = \mathbb{Q}\big(\sqrt{\Delta}\,\big) \subset K$. Así pues, G contiene a $G(K/k)$ como subgrupo normal de índice 2, lo que implica que $G = \Sigma_5$ y $G(K/k) = A_5$.

Vamos a probar que ningún primo de k se ramifica en K. En primer lugar probaremos que los primos de $\mathbb{Q}$ que se ramifican en K son a lo sumo 19 y 151. Para ello acotaremos el diferente de la extensión. Notemos que al adjuntar una a una las raíces de $f(x)$ obtenemos una cadena de cuerpos

$$\mathbb{Q} \subset K_5 \subset K_{20} \subset K_{60} \subset K.$$

Basta probar que el diferente de cada paso es divisible a lo sumo entre divisores primos de 19 y 151. Ahora bien, si K_i/K_j es uno de los pasos intermedios, tenemos que $K_i = K_j(\alpha)$, donde α es una raíz de $f(x)$. Si llamamos $g(x)$ al polinomio mínimo de α sobre K_j, entonces $g(x) \mid f(x)$, por lo que $g'(\alpha) \mid f'(\alpha)$. Por el teorema 9.28 sabemos que el diferente de K_i/K_j divide a $f'(\alpha)$ y, por otra parte, considerando las extensiones $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K_i$, podemos calcular

$$\mathrm{N}_{\mathbb{Q}}^{K_i}\big(f'(\alpha)\big) = \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}\big(f'(\alpha)\big)^{|K_i:\mathbb{Q}(\alpha)|} = \Delta^{|K_i:\mathbb{Q}(\alpha)|},$$

ya que $f'(\alpha)$ es el diferente de $\mathbb{Q}(\alpha)/\mathbb{Q}$ por el teorema 9.23 (notemos que todo lo dicho antes para K_5 vale $\mathbb{Q}(\alpha)$, que es uno de sus conjugados).

Así pues, todo primo que divide al diferente de K_i/K_j divide a Δ, es decir, a 19 o a 151 y éstos son, pues, los únicos primos de $\mathbb{Q}$ que pueden ramificarse en K. Vamos a ver que su índice de ramificación vale exactamente 2.

La factorización de $f(x)$ módulo 19 que hemos calculado antes nos muestra que 19 se descompone en K_5 como producto de un primo al cuadrado con grado de inercia 1 por otro primo con grado de inercia 3. Las compleciones de K_5 respecto a estos primos dan lugar a dos extensiones de $\mathbb{Q}_{19}$, una de grado 2 y otra de grado 3. Llamémoslas L_2 y L_3. Ambas son de Galois: la primera por ser de grado 2 y la segunda por ser no ramificada (teorema 9.6). Cada una de ellas se obtiene adjuntando a $\mathbb{Q}_{19}$ una raíz de $f(x)$, luego L_2 contiene a dos raíces y L_3 a las otras tres.

Sea ahora $\mathfrak{P}$ un divisor de 19 en K. La compleción $K_{\mathfrak{P}}$ se obtiene adjuntando a $\mathbb{Q}_{19}$ las raíces de $f(x)$, luego $K_{\mathfrak{P}} = L_2L_3$. Por consiguiente $|K_{\mathfrak{P}} : \mathbb{Q}_{19}| = 6$ y, claramente, $e = 2$, $f = 3$.

En definitiva, la factorización de 19 en K consta de 20 primos al cuadrado con grado de inercia 3.

El 151 se trata de forma similar, a partir de la factorización

$$f(x) \equiv (x-9)(x-39)^2(x^2+87x+61) \text{ (mód 151)}.$$

Ahora vemos que $f(x)$ tiene ya una raíz en $\mathbb{Q}_{151}$, mientras que las otras cuatro dan lugar a dos extensiones cuadráticas, una con $e = 2$ y otra con $f = 2$. La conclusión es que 151 se descompone en 30 factores primos al cuadrado con grado de inercia 2.

Evidentemente 19 y 151 se ramifican en k, es decir, $19 = \mathfrak{p}^2$ y $151 = \mathfrak{q}^2$. Es claro entonces que $\mathfrak{p}$ y $\mathfrak{q}$ son no ramificados en K. El primero se descompone en 20 primos distintos con grado de inercia 3 y el segundo en 30 primos distintos con grado de inercia 2. Ningún otro primo puede ramificarse, luego no hay primos ramificados y el diferente es trivial: $\mathfrak{D}_{K/k} = 1$. ∎

Ejercicio: Probar que el cuerpo K_5 del ejemplo anterior tiene factorización única.

Ahora vamos a calcular el discriminante y el anillo de enteros de los cuerpos ciclotómicos de orden potencia de primo. Para ello necesitamos el hecho siguiente:

Teorema 9.42 *Sea p un número primo, r un número natural no nulo y ζ una raíz p^r-ésima primitiva de la unidad sobre $\mathbb{Q}$. Entonces $\zeta - 1$ es primo en el anillo de enteros de $\mathbb{Q}(\zeta)$ y $p = (\zeta - 1)^{\phi(p^r)}$.*

Demostración: Las raíces p^r-ésimas primitivas de la unidad son las raíces de $x^{p^r} - 1$ que no son raíces de $x^{p^{r-1}} - 1$, luego el polinomio ciclotómico p^r-ésimo es

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

Evaluando en 1 queda que

$$p = \prod_i (1 - \zeta^i),$$

donde i recorre los números menores que p^r no divisibles entre p.

Ahora notamos que $(1-\zeta^i)/(1-\zeta) = 1+\zeta+\cdots+\zeta^{i-1}$ es entero, pero ζ y ζ^i son dos raíces primitivas cualesquiera, luego $(1-\zeta)/(1-\zeta^i)$ también es entero, es decir, que $1 - \zeta^i$ es un asociado de $1 - \zeta$ para todo i, luego podemos poner

$$p = \epsilon(1 - \zeta)^{\phi(p^r)},$$

para cierta unidad ciclotómica ϵ. Como p no puede descomponerse en más de $\phi(p^r)$ factores podemos afirmar que $1 - \zeta$ es primo. Es claro entonces que la factorización de p en ideales es la indicada en el enunciado. ∎

Teorema 9.43 *Sea p un número primo, r un número natural no nulo y ζ una raíz p^r-ésima primitiva de la unidad sobre $\mathbb{Q}$. Entonces el anillo de enteros del cuerpo ciclotómico $\mathbb{Q}(\zeta)$ es $\mathbb{Z}[\zeta]$ y el discriminante es*

$$\Delta = (-1)^{\phi(p^r)/2} \frac{p^{r\phi(p^r)}}{p^{\phi(p^r)/(p-1)}}.$$

Demostración: El signo es consecuencia del teorema 9.35. Ocupémonos del valor absoluto. Si llamamos $f(x)$ al polinomio ciclotómico tenemos que $x^{p^r} - 1 = f(x)(x^{p^{r-1}} - 1)$, luego derivando y sustituyendo en ζ queda

$$p^r \zeta^{p^r - 1} = f'(\zeta)(\zeta^{p^{r-1}} - 1),$$

luego $f'(\zeta) \mid p^r$. Por el teorema 9.28 podemos afirmar que $\mathfrak{D} \mid f'(\zeta) \mid p^r$, y al tomar normas queda que el discriminante Δ es potencia de p. Así pues, $\Delta = \Delta_p$.

Si llamamos E al anillo de enteros ciclotómicos, al localizar en p el teorema anterior nos da que E_p tiene un único primo (salvo asociados), que es $\zeta - 1$. Más aún, $\zeta - 1$ es totalmente ramificado sobre p, luego el grado de inercia es 1 y el teorema 9.26 nos da que

$$E_p = \mathbb{Z}_p[1, \zeta - 1] = \mathbb{Z}_p[\zeta - 1] = \mathbb{Z}_p[\zeta].$$

Por lo tanto $\Delta_p = \Delta[\zeta]$, y este discriminante no depende de si se calcula en la extensión local o en la global (pues los cuerpos de cocientes son los mismos, y los monomorfismos también). Así pues, $\Delta = \Delta(\mathbb{Z}[\zeta])$ y por el teorema 9.34 4) concluimos que $E = \mathbb{Z}[\zeta]$.

Por el teorema 9.23 resulta que $\mathfrak{D} = (f'(\zeta))$ y $\Delta = \pm \mathrm{N}(f'(\zeta))$. Concretamente tenemos que $f'(\zeta) = p^r\zeta^{p^{r-1}}/(\zeta^{p^{r-1}} - 1)$.

Es claro que $\mathrm{N}(p^r) = p^{r\phi(p^r)}$, $\mathrm{N}(\zeta) = 1$ y sólo queda calcular $\mathrm{N}(\zeta^{p^{r-1}} - 1)$. Ahora bien, $\omega = \zeta^{p^{r-1}}$ es una raíz p-ésima primitiva de la unidad, luego el teorema 26 nos da que $\omega - 1$ es primo en $\mathbb{Q}(\omega)$ y $p = (\omega - 1)^{p-1}$. De aquí se sigue que $\mathrm{N}(\omega - 1) = p$, donde N es ahora la norma de $\mathbb{Q}(\omega)$.

La norma de $\omega - 1$ en $\mathbb{Q}(\zeta)$ se obtiene por la transitividad elevando la anterior al grado de $\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)$, es decir, $\mathrm{N}(\zeta^{p^{r-1}} - 1) = p^{\phi(p^r)/(p-1)}$. ∎

Ahora podemos aplicar el teorema 9.41 para extender el teorema anterior a cuerpos ciclotómicos arbitrarios.

Teorema 9.44 *Sea m un número natural no nulo y ζ una raíz m-sima primitiva de la unidad sobre $\mathbb{Q}$. Entonces el anillo de enteros del cuerpo ciclotómico $\mathbb{Q}(\zeta)$ es $\mathbb{Z}[\zeta]$ y el discriminante es*

$$\Delta = (-1)^{\phi(m)/2}\,\frac{m^{\phi(m)}}{\prod\limits_{p|m} p^{\phi(m)/(p-1)}}$$

Demostración: Basta observar que si $(m, n) = 1$, ζ es una raíz m-sima primitiva de la unidad y ω es una raíz n-sima primitiva de la unidad entonces $\zeta\omega$ es una raíz mn-ésima primitiva de la unidad y $\mathbb{Q}(\zeta\omega) = \mathbb{Q}(\zeta)\mathbb{Q}(\omega)$. Después se aplica inductivamente el teorema 9.41. ∎

En particular tenemos caracterizados los primos que ramifican en un cuerpo ciclotómico:

Teorema 9.45 *Sea $m > 1$ un número natural y K el cuerpo ciclotómico de orden m. Entonces un primo impar p se ramifica en K si y sólo si $p \mid m$. El 2 se ramifica en K si y sólo si $4 \mid m$.*

El teorema 9.39, junto con el teorema de Minkowski 3.13 implica que todo cuerpo numérico (distinto de $\mathbb{Q}$) tiene primos ramificados (sobre $\mathbb{Q}$). Esto nos da el teorema siguiente:

Teorema 9.46 *Si K es un cuerpo numérico normal, el grupo de Galois $G(K/\mathbb{Q})$ está generado por los grupos de inercia $T_\mathfrak{P}$ de los primos $\mathfrak{P}$ de K ramificados sobre $\mathbb{Q}$.*

Demostración: Sea $G = G(K/\mathbb{Q})$ y sea $H \leq G$ el subgrupo generado por los grupos de inercia $T_\mathfrak{P}$. Basta probar que la extensión $L/\mathbb{Q}$ no tiene primos ramificados, pues la observación previa al teorema implica que $L = \mathbb{Q}$, con lo que $G = H$.

Supongamos que $\mathfrak{p}$ es un primo de L ramificado sobre $\mathbb{Q}$. Sea $\mathfrak{P} \mid \mathfrak{p} \mid p$, de modo que p es el primo racional divisible entre $\mathfrak{p}$ y $\mathfrak{P}$ es cualquier divisor primo de $\mathfrak{p}$ en K. Entonces $\mathfrak{P}$ está ramificado sobre $\mathbb{Q}$, luego $T_\mathfrak{P} \leq H$. Si llamamos Z al cuerpo fijado por $T_\mathfrak{P}$, tenemos que $\mathbb{Q} \subset L \subset Z \subset K$. Sea $\mathfrak{P}'$ el primo de Z divisible entre $\mathfrak{P}$.

El teorema 2.45 nos da que $e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{P}')$, pero por otra parte

$$e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{P}')e(\mathfrak{P}'/\mathfrak{p})e(\mathfrak{p}/p),$$

luego tiene que ser $e(\mathfrak{p}/p) = 1$, en contra de lo supuesto. Así pues, no hay primos ramificados en L. ∎

Esto nos permite probar que el polinomio $x^n - x - 1$ es un ejemplo de polinomio con grupo de Galois Σ_n, lo que nos da una prueba explícita mucho más directa del teorema [Al 9.8].

Teorema 9.47 *Si $n \geq 2$, el grupo de Galois de $x^n - x - 1$ es isomorfo a Σ_n.*

Demostración: En uno de los ejemplos de la sección [Al 3.5] probamos que el polinomio $x^n - x - 1$ es irreducible en $\mathbb{Q}[x]$. Si K es su cuerpo de escisión y $G = G(K/\mathbb{Q})$, podemos ver a G considerar a G como grupo de permutaciones de las n raíces del polinomio, con lo que $G \leq \Sigma_n$. La acción de G es claramente transitiva, luego, en virtud del teorema [TG 2.14], basta probar que G está generado por transposiciones para concluir que $G = \Sigma_n$.

Por el teorema anterior G está generado por los grupos de inercia $T_\mathfrak{P}$, donde $\mathfrak{P}$ recorre los primos de K ramificados sobre $\mathbb{Q}$. Vamos a probar que cualquier grupo de inercia (de primos ramificados o no) es trivial o está generado por una única transposición, con lo que ciertamente G está generado por transposiciones.

Sea, pues, $\mathfrak{P}$ un primo en K, sea p el primo racional al cual divide y supongamos que existe $\sigma \in T_\mathfrak{P}$ no trivial. Entonces existe una raíz α del polinomio tal que $\sigma(\alpha) \neq \alpha$. Notemos que el polinomio $x^n - x - 1$ es mónico y tiene coeficientes enteros, luego sus raíces están en el anillo de enteros $\mathcal{O}_K$ de K.

Que σ esté en el grupo de inercia significa que induce el automorfismo trivial en el cuerpo de restos $K_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$ o, explícitamente, que $\sigma(\beta) \equiv \beta \pmod{\mathfrak{P}}$ para todo $\beta \in \mathcal{O}_K$.

Si $x^n - x - 1 = (x - \alpha_1)\cdots(x - \alpha_n) \in K[x]$, al tomar clases módulo $\mathfrak{P}$ resulta que dos de las raíces (α y $\sigma(\alpha)$) determinan la misma clase, luego $[\alpha]$ es una raíz doble de $x^n - x - 1$ en $K_\mathfrak{p}$ visto como polinomio en $\mathbb{Z}_p[x]$.

Vamos a probar que si el polinomio $x^n - x - 1 \in \mathbb{Z}_p[x]$ tiene una raíz doble en una extensión, dicha raíz es única (es decir, que las demás raíces son simples) y tiene multiplicidad exactamente igual a 2. Admitiendo esto, si $\beta \in \mathcal{O}_K$ es una raíz de $x^n - x - 1$ distinta de α y de $\sigma(\alpha)$, su clase $[\beta] \in K_\mathfrak{P}$ tiene que ser una raíz simple, pero $[\sigma(\beta)] = [\beta]$ también es raíz, luego tiene que ser $\sigma(\beta) = \beta$ o, de lo contrario, $[\beta]$ aparecería dos veces en la factorización de $x^n - x - 1$. Por lo tanto, σ fija a todas las raíces del polinomio distintas de α y $\sigma(\alpha)$, luego $\sigma = (\alpha, \sigma(\alpha))$ es una transposición, y α está determinado como la única raíz del polinomio que es raíz múltiple módulo $\mathfrak{P}$, luego $T_\mathfrak{P} = \{1, \sigma\}$.

Supongamos, pues que γ es una raíz múltiple de $x^n - x - 1 \in \mathbb{Z}_p[x]$ en una extensión. Esto significa que γ es raíz del polinomio y de su derivada, luego

$$\gamma^n - \gamma - 1 = 0, \qquad n\gamma^{n-1} - 1 = 0.$$

La segunda ecuación implica que $n \not\equiv 0 \pmod{p}$ y que $\gamma^{n-1} = 1/n \in \mathbb{Z}_p$. La primera ecuación implica entonces que $\gamma/n = \gamma + 1$, de donde $(1-n)\gamma = n$, lo cual a su vez implica que $1 - n \not\equiv 0 \pmod{p}$, y a su vez $\gamma = n/(1-n) \in \mathbb{Z}_p$, luego éste es el único valor que puede tomar γ. Para probar que la multiplicidad es 2 basta ver que γ no es raíz de la segunda derivada, pero esto significa que $n(n-1)\gamma^{n-1} \neq 0$, lo cual es cierto. ∎

9.7 Grupos y cuerpos de ramificación

Hemos probado que el diferente y el discriminante de una extensión de cuerpos numéricos son divisibles exactamente entre los primos ramificados, pero no sabemos nada sobre los exponentes con que aparecen dichos primos. Sucede que estos exponentes también están relacionados con el modo en que los primos se ramifican en una extensión, por lo que ahora estudiaremos más a fondo este proceso de ramificación. De este estudio no sólo obtendremos consecuencias de gran interés teórico, sino también resultados valiosísimos para el cálculo de diferentes y discriminantes en casos concretos.

En el capítulo II obtuvimos los primeros resultados en torno a la descomposición de un primo $\mathfrak{p}$ en una extensión de Galois K/k. Concretamente, en el teorema 2.45 vimos que si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, la factorización de $\mathfrak{p}$ puede descomponerse en tres pasos, correspondientes a los cuerpos F y Z fijados por los grupos de descomposición y de inercia de $\mathfrak{P}$ respectivamente. En el primer paso el primo $\mathfrak{p}$ se escinde de sus conjugados sin aumentar el grado de inercia ni el índice de ramificación, en el segundo paso aumenta únicamente el grado de inercia y en el tercero se produce la ramificación. Es este último tramo el que ahora vamos a estudiar con más detalle, descomponiéndolo en más pasos intermedios.

Los nuevos pasos intermedios que vamos a considerar entre Z y K los obtendremos definiendo una cadena de subgrupos del grupo de inercia. Recordemos que si E/D es una extensión finita de Galois de dominios de Dedekind, $\mathfrak{P}$ es un primo en E, $\mathfrak{p}$ es su divisor en D y la extensión $\overline{E}/\overline{D}$ de los cuerpos de restos determinados por $\mathfrak{P}$ y $\mathfrak{p}$ es separable, entonces el grupo de inercia $T_\mathfrak{P}$ es el núcleo del epimorfismo $G_\mathfrak{P} \longrightarrow G(\overline{E}/\overline{D})$ dado por $\overline{\sigma}([\alpha]) = [\sigma(\alpha)]$, luego

$$T_\mathfrak{P} = \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ para todo } \alpha \in E\}.$$

Éste será nuestro punto de partida.

Definición 9.48 Sea E/D una extensión finita de Galois de dominios de Dedekind, sea K/k la extensión de sus cuerpos de cocientes, sea $\mathfrak{P}$ un ideal primo en E y sea $\mathfrak{p}$ el primo de D divisible entre $\mathfrak{P}$. Supongamos que la extensión

$\overline{E}/\overline{D}$ de los cuerpos de restos determinados por $\mathfrak{P}$ y $\mathfrak{p}$ es separable. Para cada número natural $i \geq 0$ definimos el i-ésimo *grupo de ramificación* de $\mathfrak{P}$ como

$$G^i_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\alpha) \equiv \alpha \ (\text{mód } \mathfrak{P}^{i+1}) \ \text{ para todo } \alpha \in E\},$$

donde $G_{\mathfrak{P}} = \{\sigma \in G(E/D) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ es el grupo de descomposición de $\mathfrak{P}$.

Claramente tenemos las inclusiones

$$\cdots \ G^{i+1}_{\mathfrak{P}} \ \leq \ G^i_{\mathfrak{P}} \ \leq \ \cdots \ \leq \ G^0_{\mathfrak{P}} \ \leq \ G_{\mathfrak{P}}.$$

Además, según los comentarios precedentes, el grupo $G^0_{\mathfrak{P}}$ no es sino el grupo de inercia de $\mathfrak{P}$. A veces conviene adoptar el convenio de que $G_{\mathfrak{P}} = G^{-1}_{\mathfrak{P}}$. Cuando no haya confusión suprimiremos el subíndice $\mathfrak{P}$.

A la hora de calcular explícitamente los grupos de ramificación de una extensión E/D resulta útil la observación siguiente: si $E = D[\alpha_1, \ldots, \alpha_n]$, entonces

$$G^i_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\alpha_j) \equiv \alpha_j \ (\text{mód } \mathfrak{p}^{i+1}) \text{ para } j = 1, \ldots, n\}.$$

Así reducimos a un número finito las condiciones para que un automorfismo pertenezca a un grupo de ramificación.

El i-ésimo *cuerpo de ramificación* de $\mathfrak{P}$ será el cuerpo K_i fijado por G_i. Entonces K_0 es el cuerpo de inercia y, llamando F al cuerpo de descomposición, tenemos las inclusiones

$$k \subset F \subset K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K$$

Si K/k es una extensión de Galois de cuerpos numéricos, $\mathfrak{P}$ es un primo en K y $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$, sabemos que el grupo de descomposición $G_{\mathfrak{P}}$ es isomorfo al grupo local $G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ y es inmediato comprobar que este isomorfismo hace corresponder los grupos de ramificación locales y globales (usando que los automorfismos locales son continuos, que el anillo de enteros globales es denso en el anillo de enteros locales y que el ideal global es denso en el local). En consecuencia los cuerpos de descomposición globales se corresponden también con los locales. Los resultados probados en el caso local y que se refieran únicamente a propiedades algebraicas de los grupos de ramificación serán válidos también para cuerpos globales.

El teorema siguiente nos proporcionará otra reducción importante en el estudio de los grupos de ramificación. La demostración es inmediata.

Teorema 9.49 *Consideremos una cadena de extensiones de dominios de Dedekind $D \subset E \subset F$ de modo que F/D sea de Galois. Sea $k \subset L \subset K$ la cadena de cuerpos de cocientes. Sea $\mathfrak{P}$ un ideal primo en L, sea $\mathfrak{p}$ el primo de D al cual divide y supongamos que la extensión de cuerpos de restos $\overline{F}/\overline{D}$ es separable. Entonces, para todo índice $i \geq -1$ se cumple*

$$\begin{aligned} G^i_{K/L} &= G^i_{K/k} \cap G(K/L), \\ K^i_{K/L} &= K^i_{K/k} L. \end{aligned}$$

De este modo, si partimos de una extensión de Galois K/k de cuerpos numéricos y $\mathfrak{P}$ es un primo en K, el teorema anterior nos da que los grupos de ramificación de $\mathfrak{P}$ en la extensión K/k son los mismos que en la extensión K/F, donde F es el cuerpo de inercia. Por lo tanto, para estudiar estos grupos podemos suponer que $k = F$ y así, si $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$, se cumple $\mathfrak{p} = \mathfrak{P}^e$ y el grado de inercia es $f = 1$.

Por consiguiente, la extensión local $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ es totalmente ramificada y, según hemos comentado, los grupos de ramificación de $\mathfrak{P}$ en esta extensión son isomorfos a los de la extensión K/k, con la ventaja de que ahora $\mathfrak{P}$ es el único primo de $K_{\mathfrak{P}}$. Además ahora es principal, es decir, $\mathfrak{P} = (\pi)$ para cierto entero π. Si llamamos E/D a los anillos de enteros, el teorema 9.26 nos da que $E = D[\pi]$ (notemos que como $f = 1$ se cumple $E/\mathfrak{P} = D/\mathfrak{p}$). Más aún, observemos que podemos elegir como π a cualquier elemento del cuerpo de partida K que sea divisible entre $\mathfrak{P}$ pero no entre $\mathfrak{P}^2$.

Estas consideraciones nos llevan a una expresión más sencilla para los grupos de ramificación:

Teorema 9.50 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K y sea π un elemento de $\mathfrak{P}$ no divisible entre $\mathfrak{P}^2$. Entonces, para cada $i \geq 0$,*

$$G^i_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\pi) \equiv \pi \ (\text{mód } \mathfrak{P}^{i+1})\}.$$

DEMOSTRACIÓN: Supongamos que los cuerpos son numéricos (el caso p-ádico es más sencillo). Por las observaciones previas al teorema podemos suponer que k es el grupo de inercia de $\mathfrak{P}$, y entonces tenemos $E = D[\pi]$, donde E/D es la extensión de enteros de $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Por lo tanto

$$G^i = \{\sigma \in G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \mid \sigma(\pi) \equiv \pi \ (\text{mód } \mathfrak{P}^{i+1})\}.$$

Ahora basta restringir a K. ∎

Otra aplicación de la reducción al caso local completamente ramificado es el apartado 3) del teorema siguiente, que enunciamos junto con otros hechos elementales:

Teorema 9.51 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos, sea $\mathfrak{P}$ un ideal primo en K. Entonces*

1. *Para todo $\sigma \in G(K/k)$ y todo $i \geq 0$ se cumple $(G^i_{\mathfrak{P}})^\sigma = G^i_{\sigma(\mathfrak{P})}$.*
2. *En particular $G^i_{\mathfrak{P}} \trianglelefteq G_{\mathfrak{P}}$.*
3. *Existe un índice i tal que $G^i_{\mathfrak{P}} = 1$ (y por lo tanto $K_i = K$).*

DEMOSTRACIÓN: 1) Si $\tau \in G^i_{\mathfrak{P}}$ entonces, todo entero α de K cumple $\tau(\sigma^{-1}(\alpha)) \equiv \sigma^{-1}(\alpha)$ (mód $\mathfrak{P}^{i+1}$), luego

$$(\sigma^{-1}\tau\sigma)(\alpha) = \sigma(\tau(\sigma^{-1}(\alpha)) \equiv \alpha \ (\text{mód } \sigma(\mathfrak{P})^{i+1}),$$

con lo que $\sigma^{-1}\tau\sigma \in G^i_{\sigma(\mathfrak{P})}$. Así pues, $(G^i_{\mathfrak{P}})^\sigma \leq G^i_{\sigma(\mathfrak{P})}$. Como σ^{-1} cumple esto mismo, también es cierta la otra inclusión.

2) Es consecuencia inmediata de 1).

3) Según las observaciones previas al teorema 9.50 podemos suponer que K/k es una extensión de cuerpos p-ádicos completamente ramificada y, si π es un generador de $\mathfrak{P}$, entonces $K = k(\pi)$. En consecuencia, los valores $\sigma(\pi)$ para $\sigma \in G_\mathfrak{P} = G(K/k)$ son todos distintos dos a dos. Así, si $\sigma \neq 1$, se cumple $\sigma(\pi) - \pi \neq 0$, y basta tomar i suficientemente grande para que $\pi^{i+1} \nmid \sigma(\pi) - \pi$ para ningún $\sigma \in G_\mathfrak{P} \setminus 1$. El teorema anterior nos da entonces que $G^i_\mathfrak{P} = 1$. ∎

Ahora caracterizamos completamente el primer grupo de ramificación y parcialmente los grupos siguientes.

Teorema 9.52 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un primo en K, sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$, sea e el grado de ramificación y p la característica de sus cuerpos de restos (en el caso numérico p es el primo racional al cual dividen). Sea $e = p^s e_0$, con $(p, e_0) = 1$. Entonces:*

1. *G^0/G^1 es cíclico de orden e_0.*
2. *Para $i \geq 1$ se cumple que G^i/G^{i+1} es producto de grupos cíclicos de orden p (sin excluir la posibilidad de que sea trivial).*

Demostración: Basta demostrarlo en el caso p-ádico. Sea $\mathfrak{P} = (\pi)$. Si $\sigma \in G(K/k)$ entonces $\sigma(\pi)$ es primo en K, luego $\sigma(\pi) = \epsilon_\sigma \pi$ para una cierta unidad ϵ_σ. Si $\sigma, \tau \in G^0$ entonces

$$(\sigma\tau)(\pi) = \epsilon_{\sigma\tau}\pi = \tau(\sigma(\pi)) = \tau(\epsilon_\sigma \pi) = \tau(\epsilon_\sigma)\tau(\pi) = \tau(\epsilon_\sigma)\epsilon_\tau \pi,$$

luego $\epsilon_{\sigma\tau} = \tau(\epsilon_\sigma)\epsilon_\tau \equiv \epsilon_\sigma \epsilon_\tau \pmod{\mathfrak{P}}$.

Por lo tanto, si llamamos $\overline{K}$ al cuerpo de restos de K, podemos definir el homomorfismo $G^0 \longrightarrow \overline{K}^*$, dado por $\sigma \mapsto [\epsilon_\sigma]$.

Su núcleo es claramente G^1, luego G^0/G^1 es isomorfo a un subgrupo de $\overline{K}^*$, que es un grupo cíclico, luego G^0/G^1 es cíclico también. Más aún, $E/\mathfrak{P}$ es un cuerpo finito de orden potencia de p, luego $\overline{K}^*$ tiene orden primo con p y G^0/G^1 también.

Ahora probaremos 2), con lo que el orden de G^1 será potencia de p y, en consecuencia, el orden de G^0/G^1 tendrá que ser exactamente e_0.

Sea $\sigma \in G^i$. Entonces $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$, luego $\sigma(\pi) = \pi + \eta_\sigma \pi^{i+1}$ para un cierto $\eta_\sigma \in E$. Si ahora tomamos $\sigma, \tau \in G^i$, tenemos

$$\begin{aligned}(\sigma\tau)(\pi) &= \pi + \eta_{\sigma\tau}\pi^{i+1} = \tau(\pi + \eta_\sigma \pi^{i+1}) = \tau(\pi) + \tau(\eta_\sigma)\tau(\pi)^{i+1} \\ &= \pi + \eta_\tau \pi^{i+1} + \tau(\eta_\sigma)\tau(\pi)^{i+1} = \pi + \eta_\tau \pi^{i+1} + \tau(\eta_\sigma)\epsilon_\tau^{i+1}\pi^{i+1},\end{aligned}$$

luego $\eta_{\sigma\tau} = \eta_\tau + \tau(\eta_\sigma)\epsilon_\tau^{i+1} \equiv \eta_\tau + \eta_\sigma \pmod{\mathfrak{P}}$ pues, como $\tau \in G^i$, se cumple $\epsilon_\tau \equiv 1 \pmod{\mathfrak{P}}$.

Con esto tenemos otro homomorfismo $G^i \longrightarrow \overline{K}$ dado por $\sigma \mapsto [\eta_\sigma]$, cuyo núcleo es claramente G^{i+1}. Por lo tanto G^i/G^{i+1} es isomorfo a un subgrupo del grupo aditivo de $\overline{K}$, pero esto es lo mismo que un subespacio vectorial de $\overline{K}$ considerado como espacio vectorial sobre el cuerpo de p elementos. Claramente entonces G^i/G^{i+1} es producto de grupos cíclicos de orden p. ∎

En las condiciones del teorema anterior, si $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$ y su norma absoluta (el número de clases módulo $\mathfrak{p}$) es n, entonces el cuerpo $\overline{K}$ tiene n^f elementos, donde $f = f(\mathfrak{P}/\mathfrak{p})$, y tenemos que $e_0 \mid n^f - 1$, así como que $|G^i : G^{i+1}| \,\big|\, n^f$.

En términos de la teoría de grupos el teorema nos dice que G^1 es un p-subgrupo de Sylow de G^0. El hecho de que sea normal implica que es, de hecho, el único p-subgrupo de Sylow de G^0, luego en la práctica es fácil de identificar. Esto explica los términos "ramificación dominada" y "ramificación libre": cuando la ramificación es dominada la serie de los grupos de ramificación termina en $G^1 = 1$, luego la ramificación está "controlada" gracias al teorema anterior, pero si la ramificación es libre no disponemos de ningún resultado general para determinar el modo en que descienden los grupos G^i, y para saberlo hay que analizar separadamente cada caso.

Del teorema anterior se deduce un hecho interesante sobre las extensiones de cuerpos p-ádicos:

Teorema 9.53 *Si K/k es una extensión de Galois de cuerpos p-ádicos, entonces el grupo de Galois $G(K/k)$ es resoluble.*

Demostración: Sea $G = G(K/k) = G^{-1}$ y consideremos la sucesión de subgrupos

$$1 = G^r \trianglelefteq \cdots \trianglelefteq G^1 \trianglelefteq G^0 \trianglelefteq G.$$

La extensión K_0/k es no ramificada y, de acuerdo con 9.6, su grupo de Galois G/G^0 es cíclico. Por el teorema anterior G^0/G^1 también es cíclico y los demás cocientes son abelianos, luego G es resoluble. ∎

Los teoremas anteriores están relacionados con los resultados que hemos obtenido en las dos primeras secciones: Si K/k es una extensión de Galois de cuerpos p-ádicos, tenemos la sucesión de cuerpos $k \subset K_0 \subset K_1 \subset K$.

La extensión K_0/k es no ramificada y K/K_0 es totalmente ramificada. Es fácil ver que K_0 es precisamente el cuerpo K_{nr} descrito en 9.8. El teorema 9.52 prueba que K_1/K_0 es también cíclica de grado primo con p, luego es total y dominadamente ramificada. Es claro que K_1 es el cuerpo K_d descrito en 9.15, que nos anticipaba también que el grado $|K : K_1|$ es potencia de p, tal y como hemos probado.

Del teorema siguiente deduciremos resultados más precisos sobre la estructura de los grupos de ramificación:

Teorema 9.54 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K, sea $\tau \in G^0$ y $\sigma \in G^i$ para $i \geq 1$. Entonces $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$ si y sólo si $\sigma \in G^{i+1}$ o $\tau^i \in G^1$.*

Demostración: Basta probarlo en el caso p-ádico. Sea $\mathfrak{P} = (\pi)$. Sea $\tau(\pi) = \epsilon\pi$, donde ϵ es una unidad de K. Como por hipótesis $\tau \in G^0$, tenemos que $\tau(\epsilon) \equiv \epsilon \pmod{\mathfrak{P}}$, luego $\tau^i(\pi) \equiv \epsilon^i\pi \pmod{\mathfrak{P}^2}$ (por ejemplo, $\tau(\epsilon)\pi \equiv \epsilon\pi \pmod{\mathfrak{P}^2}$, luego $\tau^2(\pi) = \tau(\epsilon)\epsilon\pi \equiv \epsilon^2\pi \pmod{\mathfrak{P}^2}$, etc.).

De aquí que la afirmación $\tau^i \in G^1$ equivale a que $\epsilon^i \equiv 1 \pmod{\mathfrak{P}}$. Así mismo, si $\sigma(\pi) = \pi + \eta\pi^{i+1}$, donde η es un entero en K, la afirmación $\sigma \in G^{i+1}$ equivale a que $\mathfrak{P} \mid \eta$.

Hemos de probar, pues, que $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$ si y sólo si $\epsilon^i \equiv 1 \pmod{\mathfrak{P}}$ o bien $\mathfrak{P} \mid \eta$.

Calculamos

$$(\tau\sigma)(\pi) = \sigma(\tau(\pi)) = \sigma(\epsilon\pi) = \sigma(\epsilon)\pi + \sigma(\epsilon)\eta\pi^{i+1}.$$

Como $\sigma(\epsilon) \equiv \epsilon \pmod{\mathfrak{P}^{i+1}}$ tenemos que $\sigma(\epsilon)\pi \equiv \epsilon\pi \pmod{\mathfrak{P}^{i+2}}$, luego

$$(\tau\sigma)(\pi) \equiv \epsilon\pi + \epsilon\eta\pi^{i+1} \pmod{\mathfrak{P}^{i+2}} \tag{9.3}$$

Por otro lado

$$(\sigma\tau)(\pi) = \tau(\sigma(\pi)) = \tau(\pi + \eta\pi^{i+1}) = \tau(\pi) + \tau(\eta)\tau(\pi)^{i+1} = \epsilon\pi + \tau(\eta)\epsilon^{i+1}\pi^{i+1}$$

y, como $\tau(\eta) \equiv \eta \pmod{\mathfrak{P}}$, se cumple $\tau(\eta)\pi^{i+1} \equiv \eta\pi^{i+1} \pmod{\mathfrak{P}^{i+2}}$, y así

$$(\sigma\tau)(\pi) \equiv \epsilon\pi + \eta\epsilon^{i+1}\pi^{i+1} \pmod{\mathfrak{P}^{i+2}}. \tag{9.4}$$

Restando (9.3) y (9.4) queda

$$(\tau\sigma - \sigma\tau)(\pi) \equiv (\epsilon\pi)^{i+1}\eta(\epsilon^{-i} - 1) \pmod{\mathfrak{P}^{i+2}}.$$

Llamemos $\pi' = (\tau\sigma)(\pi)$, con lo que $\pi = (\sigma^{-1}\tau^{-1})(\pi')$. Sustituyendo llegamos a que

$$\pi' - (\sigma^{-1}\tau^{-1}\sigma\tau)(\pi') \equiv (\epsilon\pi)^{i+1}\eta(\epsilon^{-i} - 1) \pmod{\mathfrak{P}^{i+2}}.$$

Puesto que también se cumple $\mathfrak{P} = (\pi')$, el teorema 9.50 nos permite concluir que $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$ si y sólo si $\mathfrak{P} \mid \eta(\epsilon^{-i} - 1)$. ∎

Como primera consecuencia inmediata obtenemos un resultado general sobre la sucesión de grupos de ramificación. Recordemos que el centro de un grupo G es el subgrupo

$$Z(G) = \{g \in G \mid gh = hg \text{ para todo } h \in G\}.$$

Teorema 9.55 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K. Sea $i \geq 1$. Entonces*

$$G^i/G^{i+1} \leq Z(G^1/G^{i+1}).$$

Demostración: Si tomamos $\tau \in G^1$ se cumple $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$, luego $[\sigma] \in Z(G^1/G^{i+1})$. ∎

En términos de la teoría de grupos esto significa que la sucesión de grupos de ramificación es una serie central del p-grupo G^1.

Ahora veamos una consecuencia del teorema 9.54 mucho más importante.

Teorema 9.56 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K tal que G^0 sea abeliano. Si $G^i \neq G^{i+1}$ entonces $e_0 \mid i$.*

DEMOSTRACIÓN: Sea $[\tau]$ un generador de G^0/G^1. Por hipótesis podemos tomar $\sigma \in G^i \setminus G^{i+1}$, con lo que el teorema 9.54 nos da que $[\tau]^i = 1$, luego $e_0 \mid i$. ∎

Definición 9.57 Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K. Los índices $i \geq 0$ tales que $G^i \neq G^{i+1}$ se llaman *números de ramificación* de $\mathfrak{P}$. Los representaremos por $v_1, \ldots, v_t$. Así, la serie de grupos de ramificación puede abreviarse a

$$1 = G^{v_t+1} \lhd \cdots \lhd G^{v_1+1} \lhd G^0 \trianglelefteq G_{\mathfrak{P}}.$$

El teorema anterior afirma que si $G_{\mathfrak{P}}$ es abeliano entonces los números v_i han de ser múltiplos de e_0.

Con los grupos de ramificación podemos mejorar el teorema 9.31 y calcular exactamente los exponentes de los primos en el diferente de una extensión.

Teorema 9.58 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos y sea $\mathfrak{P}$ un ideal primo en K. Entonces el exponente de $\mathfrak{P}$ en el diferente de K/k es*

$$E = \sum_{i=0}^{\infty} (|G^i| - 1).$$

DEMOSTRACIÓN: Por el teorema 9.25 podemos suponer que la extensión es p-ádica. Si Z es el cuerpo de inercia de $\mathfrak{P}$, la extensión Z/k es no ramificada, luego su diferente es 1. Por el teorema 9.24 podemos suponer que $Z = k$. Entonces $G(K/k) = G^0$ y, si llamamos E/D a la extensión de los anillos de enteros, tenemos que $E = D[\alpha]$, para un cierto $\alpha \in E$ (por 9.27).

Sea $f(x)$ el polinomio mínimo de α. El teorema 9.23 nos da que el diferente de la extensión es

$$\mathfrak{D} = \big(f'(\alpha)\big) = \prod_{\sigma \in G^0 \setminus 1} (\sigma(\alpha) - \alpha).$$

Pero $G^0 \setminus 1 = \bigcup_{i=0}^{\infty} (G^i \setminus G^{i+1})$, la unión es disjunta y, si $\sigma \in G^i \setminus G^{i+1}$, esto significa por definición que $(\sigma(\alpha) - \alpha) = \mathfrak{P}^{i+1}$. Por lo tanto

$$E = \sum_{i=0}^{\infty} (i+1)\big(|G^i| - |G^{i+1}|\big).$$

Supongamos que G^t es el primer grupo de ramificación trivial. Entonces

$$\begin{aligned} E &= |G^0| - |G^1| + 2(|G^1| - |G^2|) + 3(|G^2| - |G^3|) + \cdots + t(|G^{t-1}| - 1) \\ &= |G^0| + |G^1| + |G^2| + \cdots + |G^{t-1}| - t = \sum_{i=0}^{t-1} (|G^i| - 1) = \sum_{i=0}^{\infty} (|G^i| - 1). \end{aligned}$$

∎

9.8 Cálculo de grupos de ramificación

Terminamos examinando algunos ejemplos concretos:

Cuerpos cuadráticos Sea K un cuerpo cuadrático de discriminante Δ y consideremos la extensión $K/\mathbb{Q}$. Sea $\mathfrak{p}$ un primo de K y sea p el primo racional al cual divide. La tabla siguiente indica el cuerpo de descomposición F de $\mathfrak{p}$ junto con los cuerpos de ramificación en cada uno de los casos posibles:

		F	K_0	K_1	K_2	K_3
	$(\Delta/p) = 1$	K	K	K	K	K
p impar	$(\Delta/p) = -1$	$\mathbb{Q}$	K	K	K	K
	$p \mid \Delta$	$\mathbb{Q}$	$\mathbb{Q}$	K	K	K
$p = 2$	$\Delta = 4m$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K	K
	$\Delta = 8m$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K

Las tres primeras columnas se calculan inmediatamente a partir de los valores r, f, e y e_0. Con esto se completan las tres primeras filas.

Para calcular las restantes observamos que una base entera de K es en cualquier caso la formada por 1 y $\omega = \big(\Delta + \sqrt{\Delta}\,\big)/2$. El grupo de ramificación i-ésimo será trivial o no según si contiene a la conjugación σ, y esto a su vez equivale a que $\mathfrak{p}^{i+1} \mid \omega - \sigma(\omega) = \sqrt{\Delta}$.

Si $p = 2$ y el discriminante es de tipo $\Delta = 4m$, con m impar, entonces el exponente de $\mathfrak{p}$ en $\sqrt{\Delta}$ es 2, luego $G^1 \neq 1$ y $G^2 = 1$.

Si $\Delta = 8m$ entonces el exponente de $\mathfrak{p}$ en $\sqrt{\Delta}$ es 3 y concluimos que $G^2 \neq 1$ y $G^3 = 1$. ∎

Cuerpos ciclotómicos Para calcular los grupos de ramificación de los cuerpos ciclotómicos probamos en primer lugar un resultado que reduce el problema al caso de extensiones de orden potencia de primo.

Teorema 9.59 *Sea K el cuerpo ciclotómico de orden $n = p^r m$, donde p es primo y $(m, p) = 1$. Sean k y k' los cuerpos ciclotómicos de orden p^r y m respectivamente. Sea $\mathfrak{P}$ un divisor primo de p en K y sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$. Entonces*

1. *Los grupos de ramificación de $\mathfrak{P}$ respecto a la extensión $K/\mathbb{Q}$ (a partir de $i = 0$) coinciden con los de la extensión K/k'.*
2. *El isomorfismo natural $G(K/k') \cong G(k/\mathbb{Q})$ hace corresponder los grupos de ramificación de $\mathfrak{P}$ con los correspondientes de $\mathfrak{p}$.*

Demostración: Es claro que podemos sustituir cada cuerpo por su compleción respecto al primo adecuado, de modo que K será ahora $K_{\mathfrak{P}}$, k será $k_{\mathfrak{p}}$, etc.

Según el teorema 2.38, el índice de ramificación de $\mathfrak{P}$ sobre $\mathbb{Q}_p$ es el mismo que sobre k' y a su vez coincide con el de $\mathfrak{p}$ sobre $\mathbb{Q}_p$ (todos ellos valen $e = \phi(p^r)$).

Según el teorema 9.49, el grupo de inercia G^0 para la extensión K/k' es un subgrupo del correspondiente a $K/\mathbb{Q}_p$, pero como ambos tienen orden e, son el mismo.

La extensión K/k es no ramificada, luego podemos identificar $\mathfrak{p} = \mathfrak{P}$. Más precisamente, $\mathfrak{p}$ y $\mathfrak{P}$ dividen a los enteros de k con la misma multiplicidad, luego las congruencias de enteros de k módulo $\mathfrak{p}$ son las mismas que módulo $\mathfrak{P}$. Si fijamos $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ entonces el teorema 9.50 nos da que el i-ésimo grupo de ramificación tanto para la extensión K/k' como para $K/\mathbb{Q}_p$ viene dado por

$$G^i = \{\sigma \in G^0 \mid \sigma(\pi) \equiv \pi \ (\text{mód } \mathfrak{P}^{i+1})\},$$

luego ambas extensiones tienen los mismos grupos de ramificación. También es inmediato que los grupos respecto a $k/\mathbb{Q}_p$ se corresponden con éstos a través del isomorfismo natural (inducido por la restricción a k). ∎

Para las extensiones de orden potencia de primo tenemos:

Teorema 9.60 *Sea p un número primo, ζ una raíz p^r-ésima primitiva de la unidad y $K = \mathbb{Q}(\zeta)$. Sea $\mathfrak{p}$ el único primo que divide a p en K. Identificamos $G(K/\mathbb{Q})$ con el grupo U_{p^r} de las unidades módulo p^r. Entonces $G^0 = U_{p^r}$ y, si $p^k \le i < p^{k+1}$, se cumple*

$$G^i = \big\{[n] \in U_{p^r} \mid n \equiv 1 \ (\text{mód } p^{k+1})\big\}.$$

Demostración: Llamemos $H_k = \big\{[n] \in U_{p^r} \mid n \equiv 1 \ (\text{mód } p^k)\big\}$ y veamos que si $k \ge 1$ entonces $H_k \le G^{p^k-1}$.

Si σ es el automorfismo identificado con una clase $[n]$ tal que $n \equiv 1 \ (\text{mód } p^k)$, para probar que $\sigma \in G^{p^k-1}$ basta ver que $\mathfrak{p}^{p^k} \mid \sigma(\zeta) - \zeta = \zeta^n - \zeta$. Pero ζ es una unidad y $\mathfrak{p} = (\zeta - 1)$, luego esto equivale a que $(\zeta-1)^{p^k} \mid \zeta^{n-1} - 1$. Tomamos clases módulo $(\zeta-1)^{p^k}$, con lo que trabajamos en un anillo de característica p. Se cumple que $[0] = [\zeta - 1]^{p^k} = ([\zeta] - [1])^{p^k} = [\zeta]^{p^k} - [1]$, o sea, $[\zeta]^{p^k} = [1]$ y, como por hipótesis $p^k \mid n-1$, también $[\zeta]^{n-1} = [1]$, luego $[\zeta^{n-1} - 1] = [0]$, como queríamos probar.

Cambiando k por $k+1$ queda que $H_{k+1} \le G^{p^{k+1}-1}$, para todo $k \ge 0$, luego también $H_{k+1} \le G^i$ para $p^k \le i < p^{k+1}$.

Considerando el epimorfismo natural $U_{p^r} \longrightarrow U_{p^{k+1}}$ para $0 \le k < r$ vemos que $|H_{k+1}| = p^{r-(k+1)}$. Por lo tanto tenemos que si $p^k \le i < p^{k+1}$ se cumple $|G^i| \ge p^{r-(k+1)}$.

Vamos a calcular la fórmula del teorema 9.58 usando estas cotas inferiores. Si vemos que el resultado E es exactamente el exponente de $\mathfrak{p}$ en el diferente de la extensión, entonces todas las desigualdades tendrán que ser igualdades y tendremos el teorema.

Según el teorema 9.43, el exponente de p en el discriminante de la extensión es $E = r(p-1)p^{r-1} - p^{r-1} = p^{r-1}(pr - r - 1)$. Como el discriminante es la norma del diferente y $\mathrm{N}(\mathfrak{p}) = p$, este número E es también el exponente de $\mathfrak{p}$ en el diferente. Veamos qué obtenemos con las cotas.

Las cotas valen 1 a partir del término $i = p^{r-1}$, luego tenemos p^{r-1} sumandos no nulos del tipo $C_i - 1$ (para $i = 0, \dots, p^{r-1} - 1$). Agrupando todos los unos, hemos de sumar todas las cotas C_i y restar p^{r-1} al resultado.

En primer lugar $C_0 = |U_{p^r}| = (p-1)p^{r-1}$, para $i = 1, \dots, p-1$ tenemos $p-1$ sumandos iguales a p^{r-1}, para $i = p, \dots, p^2-1$ tenemos $p(p-1)$ sumandos iguales a p^{r-2}, para $i = p^2, \dots, p^3 - 1$ tenemos $p^2(p-1)$ sumandos iguales a p^{r-3}, etc.

Así pues, tenemos r bloques que suman $(p-1)p^{r-1}$ cada uno. El total, después de restar p^{r-1}, es

$$r(p-1)p^{r-1} - p^{r-1} = p^{r-1}(pr - r - 1) = E.$$

■

En particular los números de ramificación son 0, $p-1$, p^2-1, …, $p^{r-1}-1$, excepto cuando $p = 2$, en cuyo caso 0 no es un número de ramificación (tanto G^0 como G^1 tienen 2^{r-1} elementos). El grado entre dos cuerpos de ramificación sucesivos es igual a p.

Cuerpos cúbicos puros Por último estudiamos la clausura normal de un cuerpo cúbico puro $\mathbb{Q}\big(\sqrt[3]{m}\,\big)$, es decir, un cuerpo de la forma $K = \mathbb{Q}\big(\sqrt[3]{m}, \sqrt{-3}\,\big)$. Para mayor comodidad del lector reproducimos la tabla .2II con el tipo de factorización de cada primo:

Casos		$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt[3]{m})$	K	e	f
$p \nmid ab$	$p \equiv \quad 1(3) \quad x^3 \equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$	1	1
	$\qquad\qquad\quad x^3 \not\equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	p	$\mathfrak{p}_1\mathfrak{p}_2$	1	3
	$p \equiv -1(3)$	p	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	2
$p \mid ab$	$p \equiv \quad 1(3)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}^3$	$(\mathfrak{p}_1\mathfrak{p}_2)^3$	3	1
	$p \equiv -1(3)$	p	$\mathfrak{p}^3$	$\mathfrak{p}^3$	3	2
$p = 3$	Tipo I	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^6$	6	1
	Tipo II	$\mathfrak{p}^2$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$	2	1

La tabla siguiente indica los cuerpos de ramificación en cada caso. Como de costumbre, F es el cuerpo de descomposición. Llamaremos $L_3 = \mathbb{Q}\big(\sqrt[3]{m}\,\big)$ y $L_2 = \mathbb{Q}\big(\sqrt{-3}\,\big)$.

Casos		F	K_0	K_1	K_2	K_3	K_4
$p \nmid ab$	$p \equiv \quad 1(3) \quad x^3 \equiv ab^2(p)$	K	K	K	K	K	K
	$\qquad\qquad\quad x^3 \not\equiv ab^2(p)$	L_2	K	K	K	K	K
	$p \equiv -1(3)$	L_3	K	K	K	K	K
$p \mid ab$	$p \equiv \quad 1(3)$	L_2	L_2	K	K	K	K
	$p \equiv -1(3)$	$\mathbb{Q}$	L_2	K	K	K	K
$p = 3$	Tipo I $\quad 3 \nmid ab$	$\mathbb{Q}$	$\mathbb{Q}$	L_2	K	K	K
	Tipo I $\quad 3 \mid ab$	$\mathbb{Q}$	$\mathbb{Q}$	L_2	L_2	L_2	K
	Tipo II	L_3	L_3	K	K	K	K

Notemos que la extensión $K/\mathbb{Q}$ contiene tres cuerpos intermedios conjugados de grado 3. Cuando en la tabla aparece L_3 hay que entender que los cada uno de los tres divisores de p en K tiene como cuerpo de ramificación a uno de estos tres cuerpos.

Observemos también que el penúltimo caso de la primera tabla se ha desdoblado en dos en la segunda. Excepto estos dos casos, todos los demás se razonan fácilmente.

Por ejemplo, tomemos la última fila: el número de factores en que se descompone p es $r = 3 = |F : \mathbb{Q}|$, luego $F = L_3$. Ahora, $f = 1 = |K_0 : F|$, con lo que $K_0 = L_3$. Finalmente tenemos $|K_1 : K_0| = e_0 = 2$, luego $K_1 = K$.

El único caso que tenemos que analizar es $p = 3$ cuando el cuerpo cúbico es de tipo I, que se corresponde con las filas penúltima y antepenúltima de la tabla. En ambos casos es claro que $K_1 = L_2$. Para determinar los cuerpos siguientes usaremos el teorema 9.58, para lo cual hemos de calcular el diferente de la extensión. En realidad nos bastaría calcular el diferente local correspondiente al divisor 3, pero por completitud calcularemos el diferente global tanto para cuerpos de tipo I como de tipo II. La idea es que si consideramos la cadena $\mathbb{Q} \subset L_2 \subset K$ tenemos problemas con K/L_2 debido a la ramificación libre, pero si consideramos $\mathbb{Q} \subset L_3 \subset K$ la ramificación libre está en el tramo $L_3/\mathbb{Q}$, pero aquí podemos calcular el diferente a partir del discriminante, que es conocido.

Llamemos $\mathfrak{f} = 3ab$ si L_3 es de tipo I y $\mathfrak{f} = ab$ si L_3 es de tipo II. Según el teorema 1.20, el discriminante de L_3 es $3\mathfrak{f}^2$ (consideramos a $\mathfrak{f}$ como ideal, por lo que prescindimos del signo).

Fijemos notación para la factorización del 3: Si L_3 es de tipo II tenemos que $3 = \mathfrak{p}_1\mathfrak{p}_2^2$ en L_3, $3 = \mathfrak{q}^2$ en L_2, $\mathfrak{p}_1 = \mathfrak{P}_1^2$, $\mathfrak{p}_2 = \mathfrak{P}_2\mathfrak{P}_3$, $\mathfrak{q} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ en K.

El tipo I también se ajusta a este esquema si convenimos que $\mathfrak{p}_1 = \mathfrak{p}_2$, $\mathfrak{P}_1 = \mathfrak{P}_2 = \mathfrak{P}_3$.

Cada divisor primo (racional) de $\mathfrak{f}$ tiene un único divisor en L_3, que lo divide con multiplicidad 3, luego podemos escribir $\mathfrak{f}^{1/3}$ para referirnos al ideal de L_3 que resulta de dividir entre tres los exponentes de los primos de L_3 que aparecen en $\mathfrak{f}$.

De los divisores de 3, el único que se ramifica en L_3 es $\mathfrak{p}_2$, luego es el único que puede aparecer en el diferente de $L_3/\mathbb{Q}$. Teniendo esto en cuenta, es claro que dicho diferente ha de ser $\mathfrak{D}_{3/1} = \mathfrak{p}_2\mathfrak{f}^{2/3}$.

Respecto a la extensión K/L_3, el único primo ramificado es $\mathfrak{P}_1$, con índice 2, luego la ramificación es dominada, los grupos de ramificación son $G^0 \cong C_2$, $G^1 = 1$, y el teorema 9.58 nos da que el diferente es exactamente $\mathfrak{D}_{6/3} = \mathfrak{P}_1$.

Con esto tenemos el diferente de toda la extensión $K/\mathbb{Q}$, que resulta ser

$$\mathfrak{D}_{6/1} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{f}^{2/3} = 3^{1/2}\mathfrak{f}^{2/3}.$$

Por otro lado, el diferente de la extensión $L_2/\mathbb{Q}$ se calcula inmediatamente a partir del discriminante, que es -3. Evidentemente $\mathfrak{D}_{2/1} = \mathfrak{q} = 3^{1/2}$. Así llegamos al diferente que nos interesaba, el de la extensión K/L_2, que es

$$\mathfrak{D}_{6/2} = \mathfrak{f}^{2/3}. \tag{9.5}$$

Necesitábamos el exponente de $\mathfrak{P} = \mathfrak{P}_1 = \mathfrak{P}_2 = \mathfrak{P}_3$ en $\mathfrak{D}_{6/2}$ cuando L_3 es de tipo I. Como $\mathfrak{f} = 3ab$, dicho exponente será $E = 4$ si $p \nmid ab$ o bien $E = 8$ si $p \mid ab$.

Los grupos G_i para K/L_2 tienen orden 3 o son triviales, luego aportan sumandos iguales a 2 en el teorema 9.58. Así pues, si $p \nmid ab$ hay 2 grupos no triviales (los correspondientes a $i = 0, 1$) y si $p \mid ab$ hay 4 grupos no triviales ($i = 0, 1, 2, 3$). Esto es lo que refleja la tabla anterior.

Apéndice A

El lema de Hensel

En este apéndice probaremos un resultado importante sobre cuerpos completos no arquimedianos, del cual deduciremos entre otras cosas que la hipótesis de separabilidad del teorema 5.25 (y de sus consecuencias) puede eliminarse.

En primer lugar observamos que si K es un cuerpo métrico no arquimediano (no necesariamente discreto), podemos definir su *anillo de enteros* como

$$E = \{\alpha \in K \mid |\alpha| \leq 1\}.$$

Claramente se trata de un anillo y K es su cuerpo de cocientes. Las unidades de E son los elementos de K con valor absoluto 1. También es claro que E tiene un único ideal maximal, a saber,

$$\mathfrak{p} = \{\alpha \in K \mid |\alpha| < 1\}.$$

(Notemos que $\mathfrak{p}$ está formado por los elementos no unitarios de E.) También tenemos definido el *cuerpo de restos* $\overline{K} = E/\mathfrak{p}$.

Teorema A.1 *Sea K un cuerpo métrico no arquimediano. Entonces cualquier valor absoluto de K se extiende a un valor absoluto no arquimediano sobre el cuerpo de fracciones algebraicas $K(x)$ de manera que para cada polinomio $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ se cumple $|f(x)| = \max\limits_{0\leq i\leq n} \{|a_i|\}$.*

Demostración: Consideremos la aplicación definida sobre el anillo de polinomios $K[x]$ como indica el enunciado y vamos a probar que verifica los axiomas de un valor absoluto no arquimediano.

El único que no es inmediato es que esta aplicación conserva los productos. Si tenemos dos polinomios f y g con coeficientes $\{a_i\}$ y $\{b_j\}$ entonces un coeficiente de su producto es de la forma $\sum\limits_{i=0}^{k} a_i b_{k-i}$, y ciertamente

$$\Big|\sum_{i=0}^{k} a_i b_{k-i}\Big| \leq \max_i |a_i b_{k-i}| \leq \max_i |a_i| \max_j |b_j|,$$

de donde $|f(x)g(x)| \leq |f(x)|\,|g(x)|$. Hemos de probar la igualdad.

Llamemos $f_1(x)$ a la suma de los monomios $a_i x^i$ tales que $|a_i| = |f(x)|$ y $f_2(x)$ a la suma de los monomios restantes. Así $f(x) = f_1(x) + f_2(x)$. Descomponemos igualmente $g(x) = g_1(x) + g_2(x)$. Notemos que $|f_2(x)| < |f_1(x)|$ y $|g_2(x)| < |g_1(x)|$. Así

$$f(x)g(x) = f_1(x)g_1(x) + f_1(x)g_2(x) + f_2(x)g_1(x) + f_2(x)g_2(x).$$

Es fácil ver que el valor absoluto de los tres últimos factores es estrictamente menor que el del primero, luego por la desigualdad triangular no arquimediana (que ya hemos dicho que se cumple) concluimos que $|f(x)g(x)| = |f_1(x)g_1(x)|$.

Por la desigualdad ya probada $|f_1(x)g_1(x)| \le |f_1(x)|\,|g_1(x)|$ y, considerando el coeficiente director, vemos que de hecho se tiene la igualdad. Así pues $|f(x)g(x)| = |f_1(x)|\,|g_1(x)| = |f(x)||g(x)|$.

Esta propiedad justifica que $|f(x)/g(x)| = |f(x)|/|g(x)|$ no depende del representante elegido para la fracción algebraica y claramente es un valor absoluto en $K(x)$ (conviene probar la desigualdad triangular usual, y el hecho de que la restricción a K sea el valor absoluto no arquimediano de partida implica que la extensión es no arquimediana). ∎

Observemos que los distintos valores absolutos de K inducen valores absolutos equivalentes en $K(x)$, por lo que, en definitiva, cada cuerpo métrico no arquimediano K induce una única estructura de cuerpo métrico no arquimediano en $K(x)$. Veamos ahora un resultado técnico previo al lema de Hensel.

Teorema A.2 *Sea K un cuerpo métrico no arquimediano, sean dos polinomios $g(x)$, $g_0(x) \in K[x]$ de modo que $g_0(x)$ es mónico y $|g_0(x)| \le 1$. Consideremos la división euclídea*

$$g(x) = g_0(x)c(x) + r(x), \qquad \operatorname{grad} r(x) < \operatorname{grad} g_0(x), \qquad c(x), r(x) \in K[x].$$

Entonces $|r(x)| \le |g(x)|$.

Demostración: Sean

$$g(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad g_0(x) = x^m + \cdots + b_1 x + b_0.$$

Entonces

$$|g_0(x)a_n x^{n-m}| = |g_0(x)|\,|a_n| \le |a_n| \le |g(x)|,$$

luego $|g(x) - g_0(x)a_n x^{n-m}| \le |g(x)|$. Continuando el proceso de la división llegamos a que $|r(x)| \le |g(x)|$. ∎

Si K es un cuerpo métrico no arquimediano, E es su anillo de enteros y

$$\mathfrak{p} = \{f(x) \in E[x] \mid |f(x)| < 1\},$$

es claro que $\mathfrak{p}$ es un ideal primo de $E[x]$ y que el cociente $E[x]/\mathfrak{p}$ es isomorfo de forma natural al anillo de polinomios $\overline{K}[x]$. Representaremos por $\bar{f}(x)$ la clase de $f(x)$ en el cociente.

Teorema A.3 (Lema de Hensel) *Sea K un cuerpo métrico completo no arquimediano y sea E su anillo de enteros. Supongamos que un polinomio de $E[x]$ factoriza módulo $\mathfrak{p}$ como $\bar{f}(x) = \bar{g}_0(x)\bar{h}_0(x)$, donde $g_0(x)$ es mónico y $\bar{g}_0(x)$ y $\bar{h}_0(x)$ son primos entre sí. Entonces existen polinomios $g(x)$, $h(x) \in E[x]$ tales que $f(x) = g(x)h(x)$, $g(x)$ es mónico, tiene el mismo grado que $g_0(x)$ y $\bar{g}(x) = \bar{g}_0(x)$, $\bar{h}(x) = \bar{h}_0(x)$.*

DEMOSTRACIÓN: Por hipótesis existe un polinomio $p(x) \in E[x]$ tal que

$$f(x) = g_0(x)h_0(x) + p(x) \qquad \text{y} \qquad |p(x)| < 1. \tag{A.1}$$

El hecho de que $\bar{g}_0(x)$ y $\bar{h}_0(x)$ sean primos entre sí se traduce en que existen polinomios $a(x)$, $b(x)$, $c(x) \in E[x]$ de modo que

$$a(x)g_0(x) + b(x)h_0(x) = 1 + c(x) \qquad \text{y} \qquad |c(x)| < 1. \tag{A.2}$$

Multiplicamos por $p(x)$:

$$a(x)p(x)g_0(x) + b(x)p(x)h_0(x) = p(x) + c(x)p(x). \tag{A.3}$$

Dividimos $b(x)p(x)$ y $c(x)p(x)$ entre $g_0(x)$:

$$b(x)p(x) = g_0(x)q(x) + u_1(x), \qquad \operatorname{grad} u_1(x) < \operatorname{grad} g_0(x), \tag{A.4}$$
$$c(x)p(x) = g_0(x)q_1(x) + r(x), \qquad \operatorname{grad} r(x) < \operatorname{grad} g_0(x). \tag{A.5}$$

El teorema anterior nos da

$$|u_1(x)| \leq |b(x)p(x)| = |b(x)|\,|p(x)| \leq |p(x)| < 1, \tag{A.6}$$
$$|r(x)| \leq |c(x)p(x)| = |c(x)||p(x)| \leq |p(x)| < 1. \tag{A.7}$$

Sustituyendo (A.4) y (A.5) en (A.3) obtenemos:

$$\big(a(x)p(x) + q(x)h_0(x) - q_1(x)\big)g_0(x) + u_1(x)h_0(x) = p(x) + r(x).$$

Llamamos $v_1(x)$ a la expresión entre paréntesis, y así queda

$$v_1(x)g_0(x) + u_1(x)h_0(x) = p(x) + r(x). \tag{A.8}$$

La desigualdad triangular junto con (A.6), (A.7) y (A.8) nos da que

$$|v_1(x)g_0(x)| \leq \text{máx}\{|u_1(x)h_0(x)|, |p(x)|, |r(x)|\} = |p(x)|$$

y, como $|g_0(x)| = 1$, concluimos que

$$|v_1(x)| \leq |p(x)| < 1. \tag{A.9}$$

Definimos

$$g_1(x) = g_0(x) + u_1(x), \tag{A.10}$$
$$h_1(x) = h_0(x) + v_1(x). \tag{A.11}$$

Así $g_1(x)$ es mónico y del mismo grado que $g_0(x)$. Por (A.6) y (A.9) resulta

$$|g_1(x)| = |g_0(x)| = 1, \quad |h_1(x)| \leq 1, \quad \bar{g}_1(x) = \bar{g}_0(x), \quad \bar{h}_1(x) = \bar{h}_0(x).$$

Sea

$$p_1(x) = f(x) - g_1(x)h_1(x). \tag{A.12}$$

Usando (A.1) y (A.8) tenemos

$$\begin{aligned} p_1(x) &= f(x) - g_0(x)h_0(x) - g_0(x)v_1(x) - u_1(x)h_0(x) - u_1(x)v_1(x) \\ &= p(x) - p(x) - r(x) - u_1(x)v_1(x) = -r(x) - u_1(x)v_1(x), \end{aligned}$$

luego por (A.6), (A.7) y (A.9)

$$\begin{aligned} |p_1(x)| &\leq \text{máx}\big\{|r(x)|, |u_1(x)v_1(x)|\big\} \leq \text{máx}\big\{|c(x)|\,|p(x)|, |p(x)|\,|p(x)|\big\} \\ &\leq \text{máx}\big\{|c(x)|, |p(x)|\big\}|p(x)| = k|p(x)|, \end{aligned} \tag{A.13}$$

donde $k = \text{máx}\big\{|c(x)|, |p(x)|\big\} < 1$. Más aún, (A.2), (A.10) y (A.11) implican

$$\begin{aligned} a(x)g_1(x) + b(x)h_1(x) &= a(x)g_0(x) + a(x)u_1(x) + b(x)h_0(x) + b(x)v_1(x) \\ &= 1 + c(x) + a(x)u_1(x) + b(x)v_1(x) = 1 + c_1(x), \end{aligned}$$

con $c_1(x) = c(x) + a(x)u_1(x) + b(x)v_1(x)$ y, en virtud de (A.6), (A.9) y (A.13),

$$|c_1(x)| < 1, \quad \text{máx}\big\{|c_1(x)|, |p_1(x)|\big\} \leq \text{máx}\big\{|c(x)|, |p(x)|\big\} = k.$$

Por otro lado,

$$\begin{aligned} &\text{grad}(g_1(x)h_1(x)) = \text{grad}(g_0(x)h_1(x)) \\ &\quad\leq [(A.11)]\,\text{máx}\big\{\text{grad}(g_0(x)h_0(x)), \text{grad}(g_0(x)v_1(x))\big\} \\ &\quad\leq [(A.1), (A.8)]\,\text{máx}\big\{\text{grad}\, f(x), \text{grad}\, p(x), \text{grad}(u_1(x)h_0(x)), \text{grad}\, r(x)\big\} \\ &\quad\leq [(A.1), (A.4), (A.5)]\,\text{máx}\big\{\text{grad}\, f(x), \text{grad}\, p(x)\big\} = m. \end{aligned}$$

En resumen tenemos dos polinomios $g_1(x)$, $h_1(x)$ que cumplen las hipótesis del teorema en lugar de $g_0(x)$ y $h_0(x)$ y además

$$|p_1(x)| \leq k|p(x)|, \qquad \text{grad}(g_1(x)h_1(x)) \leq m.$$

Podemos repetir el proceso indefinidamente, y así obtenemos polinomios $g_n(x)$, $h_n(x)$, $p_n(x)$, $u_n(x)$, $v_n(x)$ tales que

$$\begin{aligned} g_n(x) &= g_0(x) + \sum_{i=1}^{n} u_i(x), \quad |u_i(x)| \leq |p_{i-1}(x)| \leq k^i, \\ h_n(x) &= h_0(x) + \sum_{i=1}^{n} v_i(x), \quad |v_i(x)| \leq |p_{i-1}(x)| \leq k^i, \\ f(x) &= g_n(x)h_n(x) + p_n(x), \quad |p_n(x)| \leq k^{n+1}. \end{aligned}$$

Además los polinomios $g_n(x)$ son mónicos, todos del mismo grado y

$$\operatorname{grad} h_n(x) \leq m - \operatorname{grad} g_0(x).$$

Definimos

$$g(x) = g_0(x) + \sum_{i=1}^{\infty} u_i(x), \qquad h(x) = h_0(x) + \sum_{i=1}^{\infty} v_i(x).$$

Notemos que la convergencia de las series no se sigue simplemente de que las sucesiones $|u_i(x)|$ y $|v_i(x)|$ tiendan a 0, pues $K(x)$ no es completo, pero el grado de los sumandos está acotado y, al intercambiar formalmente las series con las sumas de cada polinomio, obtenemos un polinomio cuyos coeficientes son series convergentes (pues K sí que es completo) y es fácil ver que tales polinomios son realmente las sumas de las series.

Por otro lado es claro que la sucesión $p_n(x)$ tiende a 0, luego $f(x) = g(x)h(x)$. Claramente

$$|g(x) - g_0(x)| \leq \max_i\{|u_i(x)|\} < 1, \qquad |h(x) - h_0(x)| \leq \max_i\{|v_i(x)|\} < 1$$

y además $g(x)$ es mónico y tiene el mismo grado que $g_0(x)$. ∎

Veamos dos casos particulares:

Teorema A.4 *Sea K un cuerpo completo no arquimediano y*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

un polinomio con coeficientes enteros (en K), $a_n \neq 0$. Si $|a_n| < 1$ y $|a_i| = 1$ para un $i \neq 0$ entonces f es reducible.

Demostración: Sea $0 < i < n$ el mayor índice tal que $|a_i| = 1$. Definimos

$$g_0(x) = \frac{1}{a_i}(a_i x^i + \cdots + a_1 x + a_0), \qquad h_0(x) = a_i.$$

Claramente ambos polinomios tienen coeficientes enteros, son primos entre sí, $g_0(x)$ es mónico y

$$|f(x) - g_0(x)h_0(x)| = |a_n x_n + \cdots + a_{i+1}x^{i+1}| < 1.$$

También es obvio que $\bar{g}_0(x)$ y $\bar{h}_0(x)$ son primos entre sí. El lema de Hensel implica que f se descompone en producto de dos polinomios, uno de grado i y otro de grado $n - i$, luego es reducible. ∎

Teorema A.5 *Sea K un cuerpo completo no arquimediano y $f(x)$ un polinomio mónico irreducible en $K[x]$. Si el término independiente de $f(x)$ es entero, entonces los coeficientes restantes también lo son.*

DEMOSTRACIÓN: Sea c el coeficiente de $f(x)$ con mayor valor absoluto. Hemos de probar que $|c| \leq 1$. En caso contrario $f(x)/c$ tiene todos sus coeficientes enteros y uno de ellos igual a 1. Su coeficiente director es $1/c$, y se cumple $|1/c| < 1$, luego por el teorema anterior $f(x)$ sería reducible, en contra de lo supuesto. ∎

Ahora podemos probar que la aplicación definida en el teorema 5.23 es siempre un valor absoluto:

Teorema A.6 *Sea k un cuerpo métrico completo. Sea K/k una extensión finita de grado n. Entonces cada valor absoluto de k se extiende de forma única a un valor absoluto de K que viene dado por $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$.*

DEMOSTRACIÓN: La única extensión no trivial de un cuerpo arquimediano completo es $\mathbb{C}/\mathbb{R}$ con la topología usual, y en tal caso el resultado es evidente (ver la sección 5.7). Podemos suponer, pues, que k es no arquimediano.

Es obvio que la aplicación $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$ extiende al valor absoluto de k, así como que satisface los axiomas de valor absoluto salvo quizá la desigualdad triangular.

Hemos de probar que si $|\alpha| \leq |\beta|$ entonces $|\alpha+\beta| \leq |\beta|$ o, equivalentemente, que $|\alpha/\beta + 1| \leq 1$, para todo α, $\beta \in K$, $\beta \neq 0$. Alternativamente, basta ver que si $|\alpha| \leq 1$ entonces $|\alpha + 1| \leq 1$. En nuestro caso concreto esto equivale a que si $|\,\mathrm{N}(\alpha)| \leq 1$ entonces $|\,\mathrm{N}(\alpha + 1)| \leq 1$. Como $\mathrm{N}_{K/k}(\alpha) = (\mathrm{N}_{k(\alpha)/k}(\alpha))^{|K:k(\alpha)|}$, podemos suponer que $K = k(\alpha)$.

Sea $f(x)$ el polinomio mínimo de α en $k[x]$. Su término independiente es, salvo el signo, $\mathrm{N}_{K/k}(\alpha)$, luego es entero en k. El teorema A.5 implica que todos sus coeficientes son enteros. El polinomio mínimo de $\alpha + 1$ es $f(x - 1)$, que también tiene sus coeficientes enteros, en particular su término independiente, luego $|\,\mathrm{N}(\alpha + 1)| \leq 1$. ∎

Notemos que dos valores absolutos de k se diferencian en un exponente, luego lo mismo les sucede a sus extensiones. Así pues, la estructura métrica que obtenemos en K no depende del valor absoluto de k del que partamos, y así K se convierte en un cuerpo métrico completo de modo que sus valores absolutos están en biyección con los de k (la completitud la garantiza 5.23).

Combinando los teoremas A.1 y A.6 tenemos lo siguiente:

Teorema A.7 *Sea K/k una extensión finitamente generada. Entonces todo valor absoluto en k se extiende a K.*

DEMOSTRACIÓN: Por [Al 9.26], podemos tomar una base de trascendencia $x_1, \ldots, x_n$ de K sobre k. Entonces, cada x_i es trascendente sobre $\mathbb{Q}(x_1, \ldots, x_{i-1})$ y aplicando sucesivamente el teorema A.1 tenemos que cualquier valor absoluto prefijado en $\mathbb{Q}$ se extiende a $K_0 = k(x_1, \ldots, x_n)$. Además, la extensión K/K_0 es algebraica y finitamente generada, luego es finita.

Sea $\bar{K}_0$ la compleción de K_0 respecto de la extensión del valor absoluto dado. Podemos identificar a K con un subcuerpo de una extensión de $\bar{K}_0$ (basta expresar $K = K_0(\alpha)$ y adjuntar a $\bar{K}_0$ una raíz del polinomio mínimo de

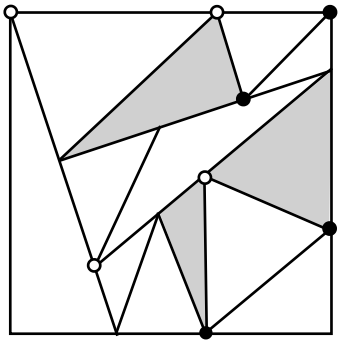
α sobre K_0). Así la extensión $\bar{K}_0K/\bar{K}_0$ es finita, luego por A.6 el valor absoluto de $\bar{K}_0$ tiene una extensión a $\bar{K}_0K$ y la restricción de ésta a K es una extensión del valor absoluto dado. ∎

Usando esto podemos demostrar el resultado geométrico que citábamos en la introducción:

Teorema A.8 *No es posible dividir un cuadrado en un número impar de triángulos de la misma área.*

Demostración: Supongamos que hemos dividido un polígono Q en un número finito de triángulos disjuntos (en el sentido geométrico de que la intersección de dos cualesquiera de ellos conste a lo sumo de puntos comunes de sus fronteras). Diremos que dos vértices de los triángulos son adyacentes si están situados sobre el lado de un mismo triángulo y el segmento que los une no contiene otros vértices. Llamaremos segmentos a los segmentos que unen dos vértices adyacentes.

Así, por ejemplo, la hipotenusa del triángulo rectángulo que hay a la izquierda de la figura es un lado que se divide en tres segmentos, mientras que los catetos son lados y segmentos a la vez. El lector puede buscar en la figura el único segmento que no es el lado de ningún triángulo.



Supongamos que divisimos los vértices de los triángulos en tres clases disjuntas A, B, C, como las marcadas en la figura con círculos blancos (A), negros (B) o sin círculos (C).

Diremos que un lado o un segmento es de tipo AB si tiene un extremo de tipo A y otro de tipo B. Por ejemplo, el cuadrado de la figura tiene un único lado de tipo AB. Vamos a probar lo siguiente:

> *Si el polígono Q tiene un número impar de lados de tipo AB y ningún lado de ningún triángulo tiene vértices de los tres tipos, entonces al menos uno de los triángulos tiene vértices de los tres tipos.*

Observemos que la figura cumple las hipótesis y, ciertamente, los tres triángulos sombreados cumplen la conclusión.

Supongamos que no hay triángulos con vértices de los tres tipos. Dividimos la prueba en varios pasos:

1. *Un lado de un triángulo de tipo AB contiene un número impar de segmentos de tipo AB.*

   En efecto, como no puede contener vértices de los tres tipos, todos los vértices que contenga tienen que ser de tipo A o B. Si nos movemos desde el vértice A hasta el vértice B, el tipo de vértice tiene que cambiar un número impar de veces, luego tenemos que pasar por un número impar de segmentos de tipo AB.

2. *Un lado de un triángulo que no sea de tipo AB contiene un número par de segmentos de tipo AB.*

   Si el lado no contiene vértices de tipo A o B, entonces tiene 0 segmentos de tipo AB, y si sus vértices son de tipo A y B, sus extremos serán ambos del mismo tipo, luego si nos movemos de uno al otro el tipo de vértice tiene que cambiar un número par de veces, luego tenemos que pasar por un número par de segmentos de tipo AB.

3. *Cada triángulo tiene 0 o 2 lados de tipo AB.*

   Si tiene al menos un lado de tipo AB, como sus vértices no pueden ser de los tres tipos, el tercer vértice tiene que ser también de tipo A o B, lo que hace que haya exactamente 2 lados de tipo AB.

4. *Cada triángulo consta de un número par de segmentos de tipo AB.*

   El número de lados de tipo AB es par, y cada uno de ellos contiene un número impar de segmentos de tipo AB, luego entre todos los lados de tipo AB hay un número par de tales segmentos, y a ellos hay que sumar los segmentos contenidos en los lados que no son de tipo AB, que también son un número par, luego el número total es par.

5. *El polígono Q consta de un número impar de segmentos de tipo AB.*

   Por hipótesis Q consta de un número impar de lados de tipo AB, cada uno de los cuales consta de un número impar de segmentos de tipo AB, luego dichos lados contienen en total un número impar de segmentos de tipo AB. A ellos hay que sumarles los contenidos en los lados que no son de tipo AB, pero cada lado contiene un número par de ellos, luego el total es impar.

Ahora observamos que las dos últimas afirmaciones que hemos probado no pueden darse a la vez. En efecto, si contamos los segmentos de tipo AB que hay en cada triángulo, el total es un número par, pero hemos contado dos veces cada segmento que no esté en Q, luego si al resultado le restamos dos veces el número de segmentos interiores de tipo AB, seguimos teniendo un número par, que es el número de segmentos de tipo AB que están en Q, en contradicción con lo que hemos probado.

Pasamos ya a demostrar el teorema. No perdemos generalidad si suponemos que el cuadrado es el cuadrado unidad $Q = [0,1]^2$. Lo suponemos dividido en m triángulos de área $1/m$ y vamos a probar que m es par.

Sea K el cuerpo que resulta de adjuntarle a $\mathbb{Q}$ las coordenadas de los vértices de los triángulos. Se trata de una extensión de $\mathbb{Q}$ finitamente generada, luego por el teorema anterior el valor absoluto diádico de $\mathbb{Q}$ se extiende a K. De este modo tenemos un valor absoluto no arquimediano en K con la propiedad de que $|2| < 1$. Dividimos los puntos $(x, y) \in K^2$ en tres tipos mediante el criterio siguiente:

- (x, y) es de tipo A si $|x| < 1$ y $|y| < 1$.
- (x, y) es de tipo B si $|x| \geq 1$ y $|y| \leq |x|$.
- (x, y) es de tipo C si $|y| \geq 1$ y $|x| < |y|$.

Es obvio que los tres conjuntos de puntos son disjuntos dos a dos. Además, todo punto es de uno de los tres tipos, pues si no es de tipo A, o bien $|x| \geq 1$ o bien $|y| \geq 1$. Si sólo es $|x| \geq 1$, es que $|y| < 1 \leq |x|$ y el punto es de tipo B. Si sólo es $|y| \geq 1$, entonces $|x| < 1 \leq |y|$ y el punto es de tipo C. Por último, si $|x| \geq 1$ y $|y| \geq 1$, el punto será claramente de tipo B o C.

En particular, el punto $(0, 0)$ es de tipo A, los puntos $(1, 0)$ y $(1, 1)$ son de tipo B y el punto $(0, 1)$ es de tipo C. Por lo tanto, Q tiene un único lado de tipo AB.

1. *Si $P = (x, y)$ y $P' = (x', y')$ cumplen que $P - P'$ es de tipo A, es decir, que $|x - x'| < 1$ y $|y - y'| < 1$. Entonces P y P' tienen que ser del mismo tipo.*

   En efecto, si P es de tipo A es inmediato, pues

   $$|x'| = |x' - x + x| \leq \text{máx}\{|x' - x|, |x|\} < 1,$$

   e igualmente con y', luego P' es de tipo A.

   Si P es de tipo B, entonces

   $$1 \leq |x| = |x - x' + x'| \leq \text{máx}\{|x - x'|, |x'|\} = |x'|,$$

   $$|y'| = |y' - y + y| \leq \text{máx}\{|y' - y|, |y|\} \leq |x| \leq |x'|,$$

   luego P' también es de tipo B. Si P es de tipo C razonamos como antes que $1 \leq |y| \leq |y'|$ y

   $$|x'| = |x' - x + x| \leq \text{máx}\{|x' - x|, |x|\} < |y| \leq |y'|,$$

   luego P' también es de tipo C.

2. *Tres puntos alineados no pueden ser de tres tipos distintos.*

   En efecto, si así fuera, lo mismo sucedería con los tres puntos que resultan de restar a los tres puntos el que es de tipo A, con lo que tendríamos tres puntos alineados de tres tipos distintos uno de los cuales (el de tipo A) sería $(0, 0)$. Sean $P = (x, y)$ el punto de tipo B y $P' = (x', y')$ el punto de tipo C.

   Entonces $|y| \leq |x|$, $|x'| < |y'|$, luego $|x'y| < |xy'|$, pero el hecho de que ambos estén alineados con 0 se traduce en que son linealmente dependientes, luego $xy' = x'y$, y tenemos una contradicción.

En particular, los lados de los triángulos en los que suponemos dividido Q no pueden tener vértices de los tres tipos, luego, según hemos probado antes, existe al menos un triángulo T con vértices de los tres tipos. Restando a sus vértices el de tipo A, podemos suponer que el vértice de tipo A es $(0,0)$. Llamemos $P=(x,y)$ al vértice de tipo B y $P'=(x',y')$ al vértice de tipo C. Como en la prueba de 2) esto implica que $|x'y|<|xy'|$, pero el área de T es

$$\pm\frac{1}{2}(xy'-x'y)=\frac{1}{m},$$

luego

$$|1/m|=|1/2||xy'-x'y|\le|1/2|\,\text{máx}\{|xy'|,|x'y|\}=|1/2||x||y'|>1,$$

pues $|1/2|>1$, $|x|\ge 1$, $|y'|\ge 1$, luego $|m|<1$, y esto implica que m es par. ∎

Terminamos este apéndice con una aplicación interesante del lema de Hensel. Vamos a demostrar que los únicos cuerpos métricos localmente compactos de característica prima son los cuerpos de series formales de potencias sobre cuerpos finitos.

Teorema A.9 *Sea K un cuerpo métrico localmente compacto de característica prima p. Sea π un primo en K. Entonces K contiene un cuerpo k isomorfo a su cuerpo de restos de modo que la aplicación $k((x))\longrightarrow K$ dada por $f(x)\mapsto f(\pi)$ es un isomorfismo topológico.*

Demostración: Por el teorema 5.17 el cuerpo de restos $\overline{K}$ de K es finito. Digamos que tiene p^n elementos. El polinomio $q(x)=x^{p^n}-x$ se escinde en factores lineales distintos en $\overline{K}$ luego aplicando varias veces el lema de Hensel vemos que lo mismo le ocurre en K. Más aún, las raíces de $q(x)$ en K recorren todas las clases de $\overline{K}$. La adjunción al cuerpo primo de K de estas raíces es un cuerpo finito k de p^n elementos.

El teorema 5.18 implica que la aplicación descrita en el enunciado es biyectiva. Es fácil ver que es un homomorfismo y por lo tanto un isomorfismo. También es claro $v\big(f(x)\big)=v\big(f(\pi)\big)$ para todo $f(x)\in k((x))$, por lo que el isomorfismo es topológico. ∎

Índice de Tablas

Índice de Materias