Carlos Ivorra Castillo

TEORÍA 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

Prefacio

Este libro pretende servir de introducción a la teoría algebraica de números a un lector con una cierta base de álgebra moderna (un poco de álgebra lineal, un poco de teoría de anillos, un poco de teoría de cuerpos y un poco de teoría de grupos). Además del interés que por sí misma puede despertar en cualquier matemático, el algebrista puede ver en ella el origen histórico de muchos de los conceptos que maneja y un campo inmenso donde aplicarlos. Es fácil caer en la falsa opinión de que la teoría de números es una colección de resultados anecdóticos e intrascendentes sobre los números naturales o enteros, y es difícil mostrar en pocas palabras lo erróneo de esta creencia. Por ello hemos dedicado el primer capítulo a presentar una panorámica de la teoría de números en general y del contenido de este libro en particular. A partir de ahí el lector puede hacerse una primera estimación de si realmente le interesa la teoría, aunque lo cierto es que su auténtico encanto y su magnificencia no caben en el primer capítulo de ningún libro.

Capítulo I

Introducción a la teoría algebraica de números

El interés del hombre por los números es tan antiguo como la civilización. Son muchos los pueblos antiguos que se interesaron por los números bien por razones prácticas inmediatas, bien por su relación con la astronomía y el cómputo del tiempo o incluso asociados a la adivinación y el esoterismo. Entre todos ellos destacan los griegos, que llegaron a desarrollar una teoría de números pura guiada por criterios estrictamente matemáticos en el sentido moderno de la palabra. Los griegos descubrieron las leyes básicas de la aritmética. Conocían la división euclídea, los números primos, el cálculo del máximo común divisor y el mínimo común múltiplo, etc. Quizá el lector crea que esto significa dominar completamente los números naturales, pero no es así ni mucho menos. Lo que hicieron los griegos al desarrollar la aritmética elemental fue simplemente descubrir el lenguaje de los números, lo cual no equivale a entender lo que se lee en ese lenguaje. Para entender lo que queremos decir consideraremos un ejemplo tomado de la Aritmética de Diofanto.

1.1 Ternas pitagóricas

En el siglo III, Diofanto trató en su Aritmética el problema de encontrar ternas de números naturales no nulos x, y, z tales que $x^2 + y^2 = z^2$. Estas ternas se llaman *ternas pitagóricas,* pues según el teorema de Pitágoras permiten construir triángulos rectángulos con lados enteros. Los egipcios las usaban para construir ángulos rectos en arquitectura. Entre los ejemplos más conocidos están $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$. ¿Cómo encontrarlas todas?

En primer lugar notamos que si (x, y, z) es una terna pitagórica, también lo es (mx, my, mz) para cualquier número m y, recíprocamente, dada una terna pitagórica (x, y, z), podemos dividir sus componentes por su m.c.d. para obtener otra que cumpla además $(x, y, z) = 1$. Una terna cuyos elementos no tengan divisores comunes se llama *primitiva.* Si encontramos un método para

hallar todas las ternas primitivas, las restantes se obtienen multiplicándolas por números arbitrarios, luego el problema está resuelto. Las ternas anteriores son todas primitivas.

Ante todo observemos que un divisor primo de dos de las componentes de una terna pitagórica, divide a la tercera. Por ejemplo, si $p \mid x$ y $p \mid z$, entonces $p \mid z^2 - x^2$, con lo que $p \mid y^2$ y por lo tanto $p \mid y$. Esto significa que, en realidad, las componentes de una terna pitagórica primitiva son primas entre sí dos a dos. En particular no puede haber más de una componente par. Un número es par o impar si y sólo si lo es su cuadrado, y la suma y la diferencia de números impares es par. Como consecuencia si dos de las componentes son impares, la restante ha de ser par, es decir, en una terna primitiva hay siempre dos componentes impares y una par.

Ahora veamos que z ha de ser impar. En otro caso lo son x e y, es decir, $x = 2m+1$, $y = 2n+1$, luego $x^2 = 4m^2+4m+1$, $y^2 = 4n^2+4n+1$. Al tomar clases módulo 4 resulta que $[z]^2 = [x]^2 + [y]^2 = [1] + [1] = [2]$. Sin embargo ninguna clase módulo 4 tiene a [2] por cuadrado: $[0]^2 = [0]$, $[1]^2 = [1]$, $[2]^2 = [0]$, $[3]^2 = [1]$.

Como la situación de x e y es simétrica, podemos suponer que x es par e y impar. Según lo visto z es también impar. Consecuentemente $z+y$, $z-y$ son ambos pares. Digamos que $x = 2u$, $z+y = 2v$, $z-y = 2w$.

Ahora $x^2 = z^2 - y^2 = (z+y)(z-y)$, luego $u^2 = vw$, $v > 0$, $w > 0$.

Por otro lado $(v, w) = 1$, ya que si un primo p divide a ambos, entonces

$$\begin{aligned} p &\mid (v+w) = \frac{1}{2}(z+y) + \frac{1}{2}(z-y) = \frac{1}{2}\,2z = z, \\ p &\mid (v-w) = \frac{1}{2}(z+y) - \frac{1}{2}(z-y) = y, \end{aligned}$$

y como $(y, z) = 1$, esto es contradictorio.

Por la factorización única, es claro que si $vw = u^2$ con $(v, w) = 1$, $v > 0$, $w > 0$, entonces tanto v como w han de ser cuadrados (cada uno ha de contener cada primo un número par de veces porque así le ocurre a u). Pongamos $v = p^2$ y $w = q^2$. Obviamente $(p, q) = 1$.

Así tenemos que $z = v + w = p^2 + q^2$, $y = v - w = p^2 - q^2$. En particular $q < p$.

Como z e y son impares, p y q deben tener paridad opuesta. Sustituyendo en las fórmulas anteriores queda

$$x^2 = z^2 - y^2 = p^4 + 2p^2q^2 + q^4 - p^4 + 2p^2q^2 - q^4 = 4p^2q^2 = (2pq)^2,$$

luego $x = 2pq$. En consecuencia la terna original queda de la forma

$$(x, y, z) = (2pq, p^2 - q^2, p^2 + q^2),$$

donde p, q son números naturales primos entre sí, $q < p$ y de paridad opuesta.

Recíprocamente, es fácil comprobar que cualquier terna en estas condiciones es una terna pitagórica primitiva. Por lo tanto ya sabemos enumerarlas todas. La tabla 1.1 contiene las correspondientes a los valores de $p \leq 7$.

Tabla 1.1: Ternas pitagóricas

p	q	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85

En una tablilla cuneiforme aproximadamente del año 1.500 a.C. se ha encontrado una enumeración de ternas pitagóricas, entre las cuales se encontraba $(4.961, 6.480, 8.161)$. Se obtiene con $p = 81$ y $q = 40$.

La clasificación de las ternas pitagóricas es un ejemplo típico de lo que fue la teoría de números desde los griegos hasta mediados del siglo XVII. Hay una infinidad de resultados similares que describen el comportamiento de los números enteros. Problemas fáciles de enunciar y comprender y a menudo con soluciones fáciles de enunciar y comprender, pero tales que el argumento que lleva desde el planteamiento hasta la solución puede llegar a ser increíblemente ingenioso y laborioso. Esto iba a cambiar en los siglos posteriores. En la sección siguiente presentamos uno de los problemas que contribuyó más a dicho cambio.

1.2 El Último Teorema de Fermat

En el siglo XVII los matemáticos estaban más interesados por explorar ideas nuevas, como el recién descubierto cálculo diferencial, que por los viejos problemas sobre números enteros que se estudiaba en los libros de Euclides, Diofanto, etc. Se tenía la impresión de que no había mucho que descubrir en este campo. Uno de los principales responsables de que se renovara el interés por la teoría de números fue Pierre de Fermat, quien, según era habitual en la época, retaba a otros matemáticos a resolver problemas que él mismo había resuelto o al menos conjeturado. Éstos eran del estilo de determinar qué números naturales pueden expresarse como suma de dos cuadrados, o de tres, o de cuatro, etc., o qué números coinciden con la suma de sus divisores propios, o hallar las soluciones enteras de determinadas ecuaciones ...

La facilidad para formular conjeturas sencillas mediante cálculos directos hacía a los problemas mucho más intrigantes. Por ejemplo, fueron muchos los matemáticos que intentaron sin éxito probar algo tan simple (de enunciar y de

constatar empíricamente) como que todo número natural es suma de cuatro cuadrados. La primera prueba es de Lagrange. Entre los muchos resultados que probó Fermat se encuentra el siguiente:

Teorema 1.1 *La ecuación, $x^4 + y^4 = z^2$ no tiene soluciones enteras positivas.*

DEMOSTRACIÓN: Si existen soluciones positivas de la ecuación $x^4+y^4 = z^2$, entonces (x^2, y^2, z) es una terna pitagórica. Notar que si dividimos x, y, z por su m.c.d. obtenemos números primos entre sí que siguen cumpliendo la ecuación, luego podemos suponer que $(x, y, z) = 1$, y claramente esto implica que en realidad son primos entre sí dos a dos y que la terna (x^2, y^2, z) es primitiva.

Según los resultados de la sección anterior, $x^2 = 2pq$, $y^2 = p^2-q^2$, $z = p^2+q^2$, donde p y q son números enteros primos entre sí, de distinta paridad y $p > q > 0$ (intercambiamos x con y si es necesario para que x^2 sea el par).

Ahora, $p^2 = y^2 + q^2$, luego (q, y, p) es otra terna pitagórica, lo que obliga a que p sea impar, luego q ha de ser par, y así $q = 2ab$, $y = a^2 - b^2$, $p = a^2 + b^2$, para ciertos enteros a y b primos entre sí, de paridad opuesta, $a > b > 0$ (notar que se trata de una terna primitiva porque $(p, q) = 1$).

Por lo tanto $x^2 = 4ab(a^2 + b^2)$ y en consecuencia $ab(a^2 + b^2) = (x/2)^2$. Por otra parte $(a, b) = 1$ implica fácilmente que $(ab, a^2 + b^2) = 1$.

Ahora usamos un argumento muy simple pero importante: si el producto de dos números naturales primos entre sí es un cuadrado, entonces ambos son cuadrados, pues cada uno de ellos debe tener cada factor primo con exponente par.

Concluimos que ab y $a^2 + b^2$ son cuadrados y, por el mismo argumento, también lo son a y b. Digamos $a = u^2$, $b = v^2$, $a^2 + b^2 = w^2$.

Entonces $u^4 + v^4 = a^2 + b^2 = w^2 = p < p^2 + q^2 = z < z^2$.

En resumen, si existe una terna de números positivos (x, y, z) de manera que $x^4 + y^4 = z^2$, existe otra (u, v, w) que cumple lo mismo pero con $w^2 < z^2$. Si existieran tales ternas debería haber una con z mínimo, lo cual es falso según lo visto, por lo que la ecuación no tiene solución. ∎

En particular el teorema anterior implica que la ecuación $x^4 + y^4 = z^4$ no tiene soluciones positivas. Es conocido que Fermat creyó en cierta ocasión haber probado que esto mismo es cierto para cualquier exponente distinto de 2. Es prácticamente seguro que cometió un error y que se dio cuenta de ello, pues jamás afirmó públicamente tener tal prueba y el problema ha resistido el ataque de los mejores matemáticos de los últimos doscientos años. Simplemente, Fermat anotó su presunto hallazgo en un margen de su ejemplar de la Aritmética de Diofanto y después olvidó, o no consideró necesario, tachar la nota. Tras su muerte, uno de sus hijos hizo públicas las notas de su padre, entre las cuales figuraba esa pequeña declaración de haber probado lo que desde entonces se conoce como Último Teorema de Fermat, esto es, la afirmación:

> *La ecuación $x^n + y^n = z^n$ no tiene soluciones enteras positivas para exponentes $n > 2$.*

El nombre no hace referencia a que fuera el último resultado que Fermat hubiera demostrado, sino a que a principios del siglo XIX todas las afirmaciones que Fermat había dejado enunciadas sin demostración habían sido demostradas o refutadas salvo ésta, que era, pues, el último 'teorema' de Fermat cuya prueba faltaba encontrar.

El teorema anterior muestra que Fermat sí había probado (y comunicado) la prueba para exponente $n = 4$. Más aún, esto implica de hecho que el teorema de Fermat es cierto para cualquier exponente de la forma $n = 4k$. En efecto, si existieran números positivos (x, y, z) tales que $x^{4k} + y^{4k} = z^{4k}$, entonces (x^k, y^k, z^k) sería una solución a la ecuación $x^4 + y^4 = z^4$, lo cual es imposible. En particular el Último Teorema de Fermat es cierto para las potencias de dos.

De aquí se sigue ahora que si el Último teorema de Fermat es cierto para exponentes primos impares, entonces es cierto para todo exponente. En efecto, si existen soluciones positivas a una ecuación $x^n + y^n = z^n$, entonces n no puede ser potencia de 2, luego existe un primo impar p tal que $p \mid n$, o sea, $n = pk$, para cierto entero k, luego (x^k, y^k, z^k) es una solución positiva a la ecuación $x^p + y^p = z^p$.

Observemos que si p es impar el Último Teorema de Fermat equivale a la no existencia de soluciones enteras no triviales (o sea, con $xyz \neq 0$) de la ecuación

$$x^p + y^p + z^p = 0,$$

lo que muestra que en realidad el papel de las tres variables es simétrico. Esto simplifica algunos argumentos.

Euler demostró el teorema de Fermat para $p = 3$, ya en el siglo XIX, el joven Dirichlet y el anciano Legendre demostraron independientemente el caso $p = 5$, pero Dirichlet fracasó al abordar el caso $p = 7$, y sólo consiguió una prueba para exponente 14. La complejidad de los argumentos aumentaba tan rápidamente que $p = 7$ era prácticamente intratable. Más adelante Kummer llegó a probar el teorema de Fermat para todos los exponentes menores que 100. Evidentemente esto no fue el resultado de cálculos más prolijos todavía, sino de nuevas ideas. Lo explicaremos con más detalle en la sección siguiente.

1.3 Factorización única

La clasificación de las ternas pitagóricas, así como el teorema 1.1, descansan sobre la aritmética elemental. Sin embargo, la potencia de estos métodos pronto se ve superada por la dificultad de los problemas que surgen de forma natural. El Último Teorema de Fermat es un caso extremo, pero hay ejemplos más simples. El resultado siguiente es uno de los problemas planteados por Fermat:

Teorema 1.2 *Las únicas soluciones enteras de la ecuación*

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

son $y = \pm 5$, $x = 3$.

DEMOSTRACIÓN: En primer lugar, y ha de ser impar, pues si fuera par, y^2+2 sería divisible entre 2, pero no entre 4, mientras que x^3 sería divisible entre 2, luego entre 8.

Ahora consideramos el anillo $\mathbb{Z}[\sqrt{-2}\,] = \{a+b\sqrt{-2} \mid a,b \in \mathbb{Z}\}$. En este anillo la ecuación factoriza en la forma

$$\big(y+\sqrt{-2}\,\big)\big(y-\sqrt{-2}\,\big) = x^3. \tag{1.1}$$

Consideramos la norma $\mathrm{N} : \mathbb{Z}[\sqrt{-2}\,] \longrightarrow \mathbb{N}$ dada por

$$\mathrm{N}\big(a+b\sqrt{-2}\,\big) = \big(a+b\sqrt{-2}\,\big)\big(a-b\sqrt{-2}\,\big) = a^2+2b^2.$$

Es fácil ver que esta norma es multiplicativa (se trata de la norma de la extensión $\mathbb{Q}\big(\sqrt{-2}\,\big)/\mathbb{Q}$ en el sentido de la teoría de cuerpos). Si x, y cumplen la ecuación, entonces un divisor común $c+d\sqrt{-2}$ de $y+\sqrt{-2}$ y de $y-\sqrt{-2}$ en $\mathbb{Z}[\sqrt{-2}\,]$ dividiría también a su suma $2y$ y a su diferencia $2\sqrt{-2}$. Tomando normas, $c^2+2d^2 \mid 4y^2$, $c^2+2d^2 \mid 8$. Por lo tanto $c^2+2d^2 \mid 4$.

Las únicas posibilidades son $c=\pm1$, $d=0$ o bien $c=0$, $d=\pm1$ o bien $c=\pm2$, $d=0$. En los dos primeros casos obtenemos una unidad y en los otros obtenemos un elemento de norma 2 o 4, que no puede dividir a $y+\sqrt{-2}$, cuya norma es y^2+2, impar.

Así pues, $y+\sqrt{-2}$, $y-\sqrt{-2}$ son primos entre sí. Ahora bien, si dos números primos entre sí son un cubo, tal y como afirma (1.1), entonces cada uno de ellos lo es, es decir, $y+\sqrt{-2} = \big(a+b\sqrt{-2}\,\big)^3$ para ciertos enteros a y b.

Igualando los coeficientes de obtenemos que $1 = b(3a^2-2b^2)$, lo que sólo es posible si $b=1$ y $a=\pm1$, de donde $y=\pm5$ y por lo tanto $x=3$. ∎

En realidad la prueba anterior tiene una laguna: si un producto de números primos entre sí es un cubo perfecto, cada factor será también un cubo perfecto siempre y cuando se trate de elementos de un anillo con factorización única, es decir, donde todo elemento se descomponga de forma única (salvo orden y asociación) en producto de primos, y además cada unidad sea un cubo. Lo cierto es que el anillo $\mathbb{Z}[\sqrt{-2}\,]$ tiene estas propiedades, pero no lo hemos justificado.

Ejercicio: Probar que las únicas unidades del anillo $\mathbb{Z}[\sqrt{-2}\,]$ son ±1.

Ejemplo En el anillo $\mathbb{Z}[\sqrt{-5}\,]$ tenemos las factorizaciones

$$6 = 2\cdot3 = \big(1+\sqrt{-5}\,\big)\big(1-\sqrt{-5}\,\big). \tag{1.2}$$

Si consideramos la norma $\mathrm{N}\big(x+y\sqrt{-5}\,\big) = x^2+5y^2$ vemos que, al igual que en el caso de $\mathbb{Z}[\sqrt{-2}\,]$, conserva productos, y los únicos elementos de norma 1 son ±1. Además no hay elementos de norma 2 o 3. De todo esto se sigue que los cuatro factores de (1.2) son irreducibles y no asociados, pues tienen norma 4, 9 y 6, luego un factor propio de cualquiera de ellos habría de tener norma 2 o 3. Por consiguiente nos encontramos ante una doble factorización en irreducibles no primos. ∎

La clave de la prueba del teorema 1.2 ha sido sin duda la factorización (1.1) en el anillo $\mathbb{Z}\big[\sqrt{-2}\,\big]$. Paulatinamente los matemáticos fueron comprendiendo que estructuras algebraicas abstractas como $\mathbb{Z}\big[\sqrt{-2}\,\big]$ o, más en general, anillos, módulos, ideales, grupos, etc. proporcionaban herramientas poderosas para obtener resultados sobre los números enteros. Muchas pruebas basadas en largos e ingeniosos cálculos de carácter elemental podían ser sustituidas por pruebas cortas, conceptuales y claras basadas en estructuras algebraicas cada vez más abstractas. En la mayoría de los casos, la posibilidad de dar una prueba elemental resultaba prácticamente inconcebible.

En la prueba del caso $p = 3$ del teorema de Fermat, Euler partió de la descomposición

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2),$$

mientras que Dirichlet y Legendre, en sus pruebas para $p = 5$, consideraron

$$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4).$$

El eje de los argumentos respectivos era el mismo argumento que hemos empleado en la prueba de 1.2, es decir, determinar cuándo los factores son primos entre sí, en tal caso argumentar que si el producto es un cubo o una potencia quinta, lo mismo le ha de suceder a cada factor y después analizar las implicaciones de este hecho. Es fácil comprender que el aumento de la complejidad del segundo factor volvía los argumentos cada vez más enrevesados.

Un paso importante fue dado por Lamé cuando pensó en considerar el anillo de los enteros ciclotómicos

$$\mathbb{Z}[\omega] = \{a_{p-1}\omega^{p-1} + \cdots a_1\omega + a_0 \mid a_{p-1}, \ldots, a_0 \in \mathbb{Z}\},$$

donde ω es una raíz p-ésima primitiva de la unidad. En efecto, si en la factorización

$$x^p - 1 = (x - 1)(x - \omega) \cdots (x - \omega^{p-1})$$

sustituimos x por x/y y multiplicamos por $-y^p$ obtenemos

$$x^p + y^p = (x + y)(x + \omega y) \cdots (x + \omega^{p-1}y). \tag{1.3}$$

Lamé conjeturó que si $\mathbb{Z}[\omega]$ tuviera factorización única tal vez sería posible generalizar los argumentos de los casos que hemos comentado para obtener una prueba completa del teorema de Fermat, con la ventaja de trabajar con factores lineales. Por ello muchos matemáticos de principios del siglo XIX investigaron la factorización de enteros ciclotómicos. Cauchy trato sin éxito de encontrar un algoritmo de división euclídea. Fue en este contexto, estudiando los enteros ciclotómicos, en el que Kummer pudo obtener el resultado que citábamos antes, en virtud del cual el teorema de Fermat es cierto para exponentes menores que 100. Kummer descubrió que los anillos de enteros ciclotómicos no siempre tienen factorización única, pero que la conjetura de Lamé era correcta.

1.4 La ley de reciprocidad cuadrática

La lógica matemática nos enseña que no puede existir una teoría de números completa, en el sentido de que existen propiedades de los números naturales que son ciertas sin que exista ningún motivo por el cual lo sean, es decir, sin que existan argumentos que lo prueben, ni mucho menos que lo expliquen. En un término medio tenemos una amplia familia de resultados que podemos probar, pero que en el fondo no comprendemos, en el sentido de que la prueba sólo es una comprobación de que todo encaja más o menos sorprendentemente. Pero en el extremo opuesto tenemos una importante clase de resultados que no sólo sabemos demostrar, sino que podemos considerarlos bien comprendidos en el sentido de que sabemos explicarlos a partir de principios generales conceptualmente simples. Si comparamos la teoría de números con la física, estos tres tipos de situaciones se corresponden respectivamente con 1) hechos puntuales, como que un determinado día ha llovido en determinado sitio, cosa cuya necesidad no cabe esperar que se pueda demostrar elegantemente a partir de ninguna teoría física, 2) leyes basadas directamente en la experiencia, como el comportamiento químico de los distintos átomos, que la química física sólo justifica con precisión en muy pocos casos particulares, y 3) leyes como las que rigen los fenómenos eléctricos, que, además de haber sido obtenidas empíricamente, todas ellas pueden explicarse perfectamente a partir de las ecuaciones de Maxwell.

Del mismo modo que las leyes fundamentales de la física sólo pueden enunciarse en el contexto de teorías abstractas que involucran conceptos muy distantes de la experiencia cotidiana, el gran descubrimiento de la teoría de números del siglo XIX fue que las leyes fundamentales sobre los números involucran esencialmente conceptos algebraicos abstractos, de forma que las propiedades que se observan sobre los números enteros son reflejos más o menos lejanos de estas leyes generales. En este sentido, la auténtica teoría sobre los números enteros es la teoría sobre los objetos algebraicos (o analíticos) donde se pueden enunciar dichas leyes generales.

Las *Disquisitiones Arithmericae* de Gauss, publicadas a principios del siglo XIX, constituyeron el primer paso por el que la teoría de números pasó de ser una colección de resultados dispersos con pruebas técnicas superficiales, a ser la profunda y potente teoría que es en la actualidad. La parte mas importante de las *Disquisitiones* es la teoría sobre formas cuadráticas binarias, con la que se pueden hallar todas las soluciones enteras de cualquier ecuación de la forma $p(x, y) = 0$, donde $p(x, y)$ es un polinomio de segundo grado con coeficientes enteros. Aunque no es éste el momento de entrar en detalles, es importante dejar claro que no estamos hablando un algoritmo ingenioso para manipular ecuaciones, sino de una teoría algebraica que, en lenguaje moderno, emplea grupos finitos, congruencias módulo subgrupos, caracteres, matrices, determinantes, módulos, etc.

Gauss probó que los resultados fundamentales concernientes a las formas cuadráticas sobre los números enteros podían deducirse de un principio general, un resultado descubierto por Euler, pero del que éste no fue capaz de probar más que una mínima porción. Gauss lo redescubrió y lo demostró en el contexto

de su teoría de formas cuadráticas. Se trata de la famosa Ley de Reciprocidad Cuadrática. Para enunciarla debemos introducir algunos conceptos.

Definición 1.3 Sea p un primo impar. Diremos que un número natural n primo con p es un *resto cuadrático* módulo p si $n \equiv x^2 \pmod{p}$, para cierto entero x. En caso contrario (siempre suponiendo que n es primo con p) diremos que n es un *resto no cuadrático* módulo p. Definimos el *símbolo de Legendre* como

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ es un resto cuadrático módulo } p \\ -1 & \text{si } n \text{ es un resto no cuadrático módulo } p \\ 0 & \text{si } p \mid n \end{cases}$$

Es obvio que si $a \equiv b \pmod{p}$ entonces $(a/p) = (b/p)$.

Conviene pensar en el símbolo de Legendre desde el siguiente punto de vista algebraico: Sea U_p el grupo de las unidades de $\mathbb{Z}/p\mathbb{Z}$. La aplicación $U_p \longrightarrow U_p^2$ dada por $x \mapsto x^2$ tiene por imagen al grupo de las clases de restos cuadráticos módulo p, y su núcleo es $\pm[1]$ (pues el polinomio $x^2 - 1$ sólo puede tener dos raíces). Por lo tanto $U_p/U_p^2 \cong \{\pm 1\}$, y el símbolo de Legendre (cuando $p \nmid n$) es la composición de la aplicación $n \mapsto [n]$ con este isomorfismo.

Ahora es claro que para todo a, b,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Ley de reciprocidad cuadrática

1. *Sean p y q primos impares distintos entonces*

   (a) *Si $p \equiv 1 \pmod{4}$ o $q \equiv 1 \pmod{4}$ entonces*

   $$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

   (b) *Si $p \not\equiv 1 \pmod{4}$ y $q \not\equiv 1 \pmod{4}$ entonces*

   $$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

2. *(Primera Ley Suplementaria) Si p es un primo impar*

   $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

3. *(Segunda Ley Suplementaria) Si p es un primo impar*

   $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8} \\ -1 & \text{si } p \not\equiv \pm 1 \pmod{8} \end{cases}$$

Sería difícil explicar aquí en poco espacio la importancia teórica de estos hechos, pero la tienen. Lo que sí podemos mostrar fácilmente (aunque no sea lo más importante) es que la ley de reciprocidad permite calcular fácilmente cualquier símbolo de Legendre. Por ejemplo,

$$\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{5}{71}\right) = -\left(\frac{71}{3}\right)\left(\frac{71}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = 1,$$

donde alternativamente hemos aplicado la ley de reciprocidad para invertir los símbolos y hemos reducido los 'numeradores' módulo los 'denominadores'.

Pero destaquemos ante todo que la Ley de Reciprocidad es lo más opuesto a un resultado elemental. Si el lector reflexiona sobre lo que significa que un primo p sea un resto cuadrático módulo q y que q sea un resto cuadrático módulo p, seguro que no encuentra ninguna conexión, por mínima que sea, que le pueda sugerir un intento de prueba (a no ser que ya esté familiarizado con la teoría de números). Pese a ello ahí tenemos una relación que además resulta ser sorprendentemente simple en cuanto a su enunciado. Hoy se conoce casi un centenar de pruebas distintas de la Ley de Reciprocidad Cuadrática. La primera demostración que encontró Gauss era muy técnica, hasta el punto de desalentar a sus mejores alumnos. Poco después encontró otra basada en lo más sutil de su teoría de formas cuadráticas, esta vez de estructura mucho más simple. Más tarde encontró otra basada en técnicas analíticas. Se conocen otras debidas a Dirichlet (que usa análisis de Fourier), a Kronecker (basada en las propiedades de los enteros ciclotómicos), hay otra de carácter elemental mucho más corta (basada en argumentos de Gauss), pero la prueba que más ha penetrado en el contenido de la ley de reciprocidad se debe a Artin, data de mediados del siglo XX y en esencia la explica en términos de cohomología de grupos.

El camino que lleva desde la ley de reciprocidad de Gauss a la de Artin fue iniciado por el propio Gauss, quien conjeturó una ley de reciprocidad cúbica y una bicuadrática, aunque no pudo probarlas. Gauss comprendió que el símbolo de Legendre no es simplemente una notación cómoda para enunciar la ley de reciprocidad, sino que el asociar las clases módulo p con las potencias de -1 juega un papel importante. La razón por la que los números enteros satisfacen una ley de reciprocidad cuadrática es que $\mathbb{Z}$ contiene una raíz cuadrada primitiva de la unidad, por lo que una ley de reciprocidad cúbica había de buscarse en el cuerpo $\mathbb{Q}\big(\sqrt{-3}\,\big)$, es decir, el cuerpo ciclotómico tercero, y una ley de reciprocidad bicuadrática había de buscarse en el cuerpo $\mathbb{Q}\big(\sqrt{-1}\,\big)$, el cuerpo ciclotómico cuarto. Así lo hizo y las encontró. Precisamente, el anillo $\mathbb{Z}[i]$ se conoce como anillo de los enteros de Gauss a raíz de sus investigaciones sobre la reciprocidad bicuadrática.

Las primeras demostraciones de las leyes de reciprocidad cúbica y bicuadrática se deben a Eisenstein, quien encontró además un fragmento de una ley de reciprocidad p-ésima, estudiando, por supuesto, el anillo de enteros ciclotómicos de orden p. Kummer compaginó sus investigaciones sobre el Último Teorema de Fermat con la búsqueda de una ley de reciprocidad general. Ambos problemas apuntaban hacia los cuerpos ciclotómicos. Sus investigaciones fueron continua-

das por Kronecker y sus discípulos, en una línea que llevó hasta la ya citada Ley de Reciprocidad de Artin, una de las cumbres de la teoría de números moderna.

1.5 El teorema de Dirichlet

Hay un problema más que llevó al estudio de los enteros ciclotómicos. Antes que Gauss, Legendre había abordado también el problema de demostrar la Ley de Reciprocidad Cuadrática, y consiguió demostrarla aceptando sin demostración un hecho muy sencillo de enunciar y que los datos empíricos corroboraban: Para todo natural n no nulo, cada una de las clases del grupo U_n de las unidades módulo n contiene al menos un número primo. Gauss no consiguió demostrar este hecho, pero se las arregló para evitarlo. Dirichlet vislumbró una posible conexión con los cuerpos ciclotómicos que efectivamente le llevó hasta una demostración de lo que hoy se conoce como Teorema de Dirichlet sobre Primos en Progresiones Aritméticas, pues admite el siguiente enunciado elemental.

Teorema de Dirichlet *Si a, b son números enteros primos entre sí, entonces la progresión aritmética $an + b$, para $n = 1, 2, \ldots$ contiene infinitos primos.*

Aunque no estamos en condiciones de explicar la idea que guió a Dirichlet, digamos al menos que está relacionada con que el grupo de Galois de la extensión ciclotómica n-sima de $\mathbb{Q}$ es isomorfo a U_n. El teorema de Dirichlet es una herramienta importante en la teoría de números y, aunque en ocasiones puede ser evitado (como hizo Gauss para probar la Ley de Reciprocidad) ello suele llevar a caminos torcidos que restan naturalidad a las demostraciones. Por este motivo la prueba de Dirichlet fue muy celebrada, además de porque fue uno de los primeros éxitos importantes de la teoría analítica de números.

1.6 Ecuaciones diofánticas

Una ecuación diofántica es simplemente una ecuación polinómica de la que se buscan las soluciones enteras. Se llaman así en honor al matemático griego Diofanto, aunque en todos los libros que se conservan no hay ningún resultado sobre ecuaciones diofánticas en este sentido moderno. Él buscaba siempre soluciones racionales en lugar de enteras.

Todos los resultados que hemos probado en este capítulo son soluciones de ecuaciones diofánticas. Del mismo modo que el estudio de los sistemas de ecuaciones lineales dio lugar al álgebra lineal, las ecuaciones diofánticas están en la base de las distintas ramas de la teoría de números. Sabemos que no puede existir una teoría general de ecuaciones diofánticas en el mismo sentido que la hay para los sistemas de ecuaciones lineales, pero hay muchos resultados aplicables a familias concretas de ecuaciones. Ya hemos comentado que Gauss dedicó gran parte de sus *Disquisitiones arithmeticae* a encontrar un método para resolver cualquier ecuación diofántica de segundo grado con dos variables.

Observar que las ecuaciones diofánticas con una variable son triviales, pues resolverlas se reduce a aproximar analíticamente las raíces del polinomio que determina la ecuación y comprobar si son enteras. Si pasamos a ecuaciones con dos variables, las de grado 1 también son sencillas.

Ejercicio: Dar un método para determinar todas las soluciones enteras de una ecuación de la forma $ax + by = c$, donde a, b, $c \in \mathbb{Z}$.

Así pues, el primer caso no trivial es el de las ecuaciones de segundo grado con dos variables (el caso estudiado por Gauss). Puede probarse que mediante cambios de variable adecuados el problema puede reducirse a estudiar ecuaciones definidas por formas cuadráticas, es decir, ecuaciones de la forma

$$ax^2 + bxy + cy^2 = d. \tag{1.4}$$

Notemos que si $a = 0$ o $c = 0$ el problema es trivial, pues una de las incógnitas ha de ser un divisor de d y hay un número finito de soluciones. Supongamos, pues, $a \neq 0 \neq c$. Veamos hasta dónde podemos llegar mediante razonamientos elementales para encontrar así el núcleo del problema.

Factorizamos el polinomio $ax^2 + bx + c = a(x - \alpha)(x - \beta)$, y entonces la ecuación se convierte en

$$a(x - \alpha y)(x - \beta y) = d.$$

Los números α y β son $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Sea $D = b^2 - 4ac$. El número D se llama *discriminante* de la forma cuadrática $ax^2 + bxy + cy^2$.

Si $D = 0$ entonces $\alpha = \beta = -b/2a$. Multiplicando por $4a$ obtenemos la ecuación $(2ax + by)^2 = 4ad$, cuyas soluciones enteras son fáciles de hallar.

Si $D = k^2 \neq 0$, entonces multiplicando por $4a$ queda

$$(2ax + (b + k)y)(2ax + (b - k)y) = 4ad,$$

que a su vez se reduce a un número finito de sistemas de ecuaciones de la forma

$$2ax + (b + k)y = u, \qquad 2ax + (b - k)y = v,$$

donde u y v recorren las factorizaciones de $4ad$. Si $d \neq 0$ el número de soluciones es finito. Si $d = 0$ la ecuación se reduce a $2ax + (b \pm k)y = 0$, cuya solución es sencilla.

Nos queda el caso en que D no es un cuadrado perfecto. Entonces 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

$$\mathrm{N}(x - \alpha y) = d/a. \tag{1.5}$$

Por lo tanto, la solución de una ecuación diofántica de la forma (1.4) 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 $x = 1.766.319.049$, $y = 226.153.980$.

Lo que hemos ganado es que ahora podemos dar un tratamiento sistemático al problema. Es prácticamente imposible trabajar en general con una ecuación con coeficientes indeterminados, pero es muy cómodo teorizar sobre extensiones de Galois. Más aún, un estudio directo de una ecuación de grado 2 sería difícilmente generalizable a ecuaciones de grados superiores, mientras que en lugar de trabajar concretamente con ecuaciones del tipo (1.5), podemos considerar ecuaciones similares definidas por normas de extensiones arbitrarias de $\mathbb{Q}$, sin que ello suponga apenas ningún esfuerzo adicional. Ello nos llevará a un método para resolver una familia de ecuaciones diofánticas que incluye todas las del tipo (1.4), pero también muchas otras de grados arbitrariamente grandes. Vamos a plantear el problema en toda su generalidad:

Sea K una extensión finita de $\mathbb{Q}$, es decir, K es un cuerpo tal que $\mathbb{Q} \subset K \subset \mathbb{C}$ y como espacio vectorial sobre $\mathbb{Q}$ tiene dimensión finita (en el caso anterior sería $K = \mathbb{Q}\big(\sqrt{D}\,\big)$, que tiene dimensión 2 sobre $\mathbb{Q}$). Un cuerpo en estas condiciones se denomina *cuerpo numérico*.

La teoría de Galois nos da que la extensión tiene un *elemento primitivo,* es decir, existe un $\zeta \in K$ tal que $K = \mathbb{Q}(\zeta)$ (en el caso anterior $\zeta = \sqrt{D}\,$). Todo elemento de K es *algebraico* sobre $\mathbb{Q}$, es decir, para cada $\alpha \in K$ existe un único polinomio mónico irreducible $p(x) \in \mathbb{Q}[x]$ tal que $p(a) = 0$. Además $p(x)$ divide a cualquier polinomio de $\mathbb{Q}[x]$ que tenga a α por raíz. A este polinomio lo llamaremos *polinomio mínimo* de α y lo abreviaremos por $\operatorname{pol\,mín}\alpha$.

En particular el grado de $\operatorname{pol\,mín}\zeta$ es el *grado* de K, es decir, la dimensión de K como $\mathbb{Q}$-espacio vectorial. Llamémoslo n.

La teoría de Galois nos da también que $\operatorname{pol\,mín}\zeta$ tiene n raíces distintas en $\mathbb{C}$, llamémoslas $\zeta_1, \ldots, \zeta_n$ (con $\zeta = \zeta_1$), así como que para $i = 1, \ldots, n$ existe un isomorfismo $\sigma_i : K \longrightarrow \mathbb{Q}(\zeta_i)$ tal que $\sigma_i(\zeta) = \zeta_i$. Es fácil ver que $\sigma_1, \ldots, \sigma_n$ son los únicos monomorfismos de K en $\mathbb{C}$, luego no dependen de la elección de ζ.

(En el caso anterior los conjugados de $\sqrt{D}$ son $\pm\sqrt{D}$ y los monomorfismos son la identidad y la conjugación que envía $\sqrt{D}$ a $-\sqrt{D}$. De hecho son isomorfismos, aunque si K no es una extensión de Galois puede ocurrir que $\mathbb{Q}(\zeta_i)$ no esté contenido en K).

El cuerpo $L = \mathbb{Q}(\zeta_1, \ldots, \zeta_n)$ es la *clausura normal* de K, es decir, la menor extensión de Galois sobre $\mathbb{Q}$ que contiene a K. Los monomorfismos σ_i son las restricciones a K de los automorfismos de L.

Si σ es un automorfismo de L, entonces $\sigma_i \circ \sigma$ es un monomorfismo de K, luego se trata de uno de los σ_j. Además si $i \neq j$, entonces $\sigma_i \circ \sigma \neq \sigma_j \circ \sigma$ (pues difieren sobre ζ). Por lo tanto la composición con σ permuta los monomorfismos σ_i. El cuerpo K tiene asociada una *norma* $\mathrm{N} : K \longrightarrow \mathbb{Q}$ definida por

$$\mathrm{N}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

La norma de un número α es ciertamente un número racional, debido a que cualquier automorfismo σ de L permuta los factores de $\mathrm{N}(\alpha)$, y por consiguiente

$\sigma\big(\mathrm{N}(\alpha)\big) = \mathrm{N}(\alpha)$. Si $\alpha_1, \ldots, \alpha_r$ son elementos no nulos de K definimos

$$\mathrm{N}(x_1\alpha_1+\cdots+x_r\alpha_r) = \big(x_1\sigma_1(\alpha_1)+\cdots+x_r\sigma_1(\alpha_r)\big)\cdots\big(x_1\sigma_n(\alpha_1)+\cdots+x_r\sigma_n(\alpha_r)\big)$$

Es claro que se trata de una forma de grado n (una *forma* es un polinomio cuyos monomios tienen todos el mismo grado). Tener en cuenta que el producto de formas es una forma y que los factores que definen $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$ son formas.

Al igual que ocurre con $\mathrm{N}(\alpha)$, todo automorfismo σ de L permuta los factores de $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$, luego

$$\sigma\big(\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)\big) = \mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r).$$

La teoría de Galois nos da entonces que $\mathrm{N}(x_1\alpha_1+\cdots+x_r\alpha_r) \in \mathbb{Q}[x_1, \ldots, x_r]$.

Si $x_1, \ldots, x_r \in \mathbb{Q}$, entonces $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$ es simplemente la norma de $x_1\alpha_1 + \cdots + x_r\alpha_r$.

Un *módulo* M de K será un subgrupo de $(K, +)$ generado por un conjunto finito $\alpha_1, \ldots, \alpha_r$ de elementos de K, es decir,

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

Hemos visto que hallar las soluciones de una ecuación diofántica definida por una forma cuadrática (1.4) con discriminante no cuadrado perfecto equivale a encontrar las soluciones de (1.5), lo que a su vez equivale a encontrar los elementos del módulo $M = \langle 1, \alpha \rangle$ de norma d/a. En general, uno de los problemas que resolveremos en este libro será el de determinar las soluciones enteras de una ecuación del tipo

$$\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r) = m,$$

lo cual equivale a su vez a encontrar los elementos del módulo $M = \langle \alpha_1, \ldots, \alpha_r \rangle_{\mathbb{Z}}$ de norma m. El método que daremos puede considerarse una generalización de la teoría de Gauss sobre formas cuadráticas binarias. En la sección siguiente damos algunos resultados adicionales que terminan de perfilar el planteamiento del problema.

1.7 Ecuaciones definidas por formas

Cada forma $F(x_1, \ldots, x_r)$ con coeficientes enteros plantea dos problemas básicos:

1. Determinar las soluciones de la ecuación diofántica $F(x_1, \ldots, x_r) = m$, para cada entero m.

2. Determinar qué enteros m están *representados* por F, es decir, admiten una expresión del tipo $F(x_1, \ldots, x_r) = m$ para ciertos enteros $x_1, \ldots, x_r$.

La teoría que vamos a desarrollar resolverá estos problemas para una familia bastante amplia de formas. Para empezar, éstas habrán de admitir una representación del tipo $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$, y entonces los problemas indicados se pueden reformular, tal y como vimos en la sección anterior, en términos del módulo generado por los números algebraicos $\alpha_1, \ldots, \alpha_r$.

Una técnica básica en la resolución de ecuaciones es transformarlas en otras equivalentes, es decir, con las mismas soluciones, pero cada vez más sencillas. Aunque esto no basta para resolver ecuaciones diofánticas, al menos nos da cierta libertad para simplificar el problema lo más posible. En primer lugar notemos que al multiplicar una ecuación por una constante (racional) no nula, las soluciones (enteras) no varían, por lo que en muchos casos podremos considerar que una forma y uno cualquiera de sus múltiplos son 'la misma forma', en el sentido de que podremos reemplazar una por otra. Esto supone que admitimos trabajar con formas con coeficientes racionales, no necesariamente enteros.

Hay otro sentido en el que dos formas pueden ser mutuamente reemplazables:

Definición 1.4 Diremos que dos formas $F(x_1, \ldots, x_r)$, $G(y_1, \ldots, y_s)$ del mismo grado son *equivalentes* (en sentido amplio) si cada una puede obtenerse de la otra a partir de un cambio de variables lineal con coeficientes enteros. Diremos que son *equivalentes* si $r = s$ y la matriz del cambio de variables tiene determinante ± 1 (con lo que tenemos dos cambios de variables mutuamente inversos).

Por ejemplo, las formas

$$x^2 + 7y^2 + z^2 - 6xy + 6yz - 2xz \qquad \text{y} \qquad 2u^2 - v^2$$

son equivalentes (en sentido amplio), pues los cambios de variables

$$\begin{array}{rcrcrcl} x &=& & & 3v & \qquad u &=& -x + 2y + z \\ y &=& u + & & v & \qquad v &=& x - \ y - z \\ z &=& -u + & & v & & & \end{array}$$

convierten una en otra.

Es claro que en esta situación una solución entera de una de las formas da lugar a una solución entera de la otra mediante las fórmulas de cambio de variables, luego sabemos resolver una si y sólo si sabemos resolver la otra.

Ejercicio: Probar que si los números algebraicos $\alpha_1, \ldots, \alpha_r$ y $\beta_1, \ldots, \beta_s$ generan un mismo módulo de un cuerpo numérico K entonces las formas $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$ y $\mathrm{N}(x_1\beta_1 + \cdots + x_s\beta_s)$ son equivalentes en sentido amplio, y si ambos son bases del mismo módulo entonces son equivalentes.

Este ejercicio muestra que a cada módulo le podemos asociar una única clase de equivalencia (en sentido amplio) de formas, así como que toda forma es equivalente en sentido amplio a una forma $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$, donde $\alpha_1, \ldots, \alpha_r$ forman una base de un cierto módulo. (Notemos que todo módulo es un $\mathbb{Z}$-módulo finitamente generado y libre de torsión, luego es libre.)

El teorema siguiente muestra cómo la equivalencia de formas nos permite pasar a formas con propiedades adicionales de interés:

Teorema 1.5 *Toda forma de grado n es equivalente a otra en la que la potencia n-sima de una de las variables tiene coeficiente no nulo.*

DEMOSTRACIÓN: Sea $F(x_1,\dots,x_r)$ una forma de grado n. Probamos primero que existen enteros $a_2,\dots,a_r$ tales que $F(1,a_2,\dots,a_r)\neq 0$. Lo haremos por inducción sobre r.

Si $r=1$ entonces es $F(x_1)=Ax_1^n$ con $A\neq 0$, luego $F(1)\neq 0$.

Si es cierto para formas con $r-1$ variables, escribimos F como

$$F = G_0x_r^n + G_1x_r^{n-1} + \cdots + G_n,$$

donde cada G_i es 0 o una forma de grado i con $r-1$ variables, pero no pueden ser todas nulas, pues F tiene grado n. Por hipótesis de inducción existen enteros $a_2,\dots,a_{r-1}$ tales que $G_i(1,a_2,\dots,a_{r-1})\neq 0$ para algún i.

El polinomio $F(1,a_2,\dots,a_{r-1},x_r)$ no es nulo, luego existe un entero a_r tal que $F(1,a_2,\dots,a_{r-1},a_r)\neq 0$.

Ahora hacemos el siguiente cambio de variables:

$$\begin{aligned} x_1 &= y_1\\ x_2 &= a_2y_1+y_2\\ \dots &\quad \dots\dots\dots\\ x_r &= a_ry_1+y_r. \end{aligned}$$

Con ello F se convierte en $G(y_1,\dots,y_r)=F(y_1,a_2y_1+y_2,\dots,a_ry_1+y_r)$, que es una forma equivalente (el cambio tiene determinante 1) y el coeficiente de y_1^n es $G(1,0,\dots,0)=F(1,a_2,\dots,a_r)\neq 0$. ∎

Ahora podemos dar una caracterización sencilla de las formas que admiten una representación de tipo $\mathrm{N}(x_1\alpha_1+\cdots+x_r\alpha_r)$.

Definición 1.6 Una forma $F(x_1,\dots,x_r)\in\mathbb{Q}[x_1,\dots,x_r]$ es *factorizable* si existe un cuerpo K (extensión de $\mathbb{Q}$) tal que F se escinde en producto de factores lineales de $K[x_1,\dots,x_r]$.

Por definición, las formas $\mathrm{N}(x_1\alpha_1+\cdots+x_r\alpha_r)$ son factorizables. También es evidente que si dos formas son equivalentes, una es factorizable si y sólo si lo es la otra.

Ejercicio: Comprobar que la forma $x^2+y^2+z^2$ no es factorizable (si lo fuera se descompondría en dos factores lineales).

Los razonamientos con formas cuadráticas binarias vistos en la sección anterior justifican que todas ellas son factorizables.

En general, una condición necesaria para poder abordar una ecuación diofántica definida por una forma expresándola como norma en un módulo es que la forma ha de ser factorizable. De hecho las formas $N(x_1\alpha_1+\cdots+x_r\alpha_r)$ factorizan en cuerpos numéricos, pero esto no es una restricción adicional:

Teorema 1.7 *Toda forma factorizable factoriza en un cuerpo numérico.*

DEMOSTRACIÓN: Sea $F = (\alpha_{11}x_1 + \cdots + \alpha_{1r}x_r)\cdots(\alpha_{n1}x_1 + \cdots + \alpha_{nr}x_r)$ una forma factorizable, donde los coeficientes α_{ij} están en un cierto cuerpo K. Es obvio que si una forma factoriza en un cuerpo K, también lo hacen sus equivalentes, luego podemos exigir que el coeficiente A de x_1^n sea no nulo. Entonces todos los coeficientes a_{i1} son no nulos (su producto es A), luego podemos extraerlos y escribir

$$F = A(x_1 + \beta_{12}x_2 + \cdots + \beta_{1r}x_r)\cdots(x_1 + \beta_{n2}x_2 + \cdots + \beta_{nr}x_r).$$

Para $2 \le j \le r$ hacemos $x_j = 1$ y las demás variables 0, con lo que queda

$$F(x_1, 0, \ldots, 1, \ldots, 0) = A(x_1 + \beta_{1j})\ldots(x_1 + \beta_{nj}),$$

y así tenemos un polinomio mónico con coeficientes racionales cuyas raíces son los elementos $-\beta_{ij}$, luego son algebraicos.

El cuerpo $\mathbb{Q}\big(\{\beta_{ij}\}\big)$ es una extensión finita de $\mathbb{Q}$, luego podemos identificarlo con un subcuerpo de $\mathbb{C}$, es decir, con un cuerpo numérico, y F factoriza en él. ∎

Una forma de tipo $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$ no tiene por qué ser irreducible en el anillo $\mathbb{Q}[x_1, \ldots, x_r]$. Por ejemplo, en el cuerpo $K = \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ se tiene que $\mathrm{N}\big(x\sqrt{2} + y\sqrt{3}\big) = (2x^2 - 3y^2)^2$. Desgraciadamente poco podemos decir en general sobre formas reducibles, pues sus factores se comportan independientemente y la teoría de cuerpos no es de gran ayuda. Por ejemplo, de nuestro análisis de las formas cuadráticas binarias en la sección anterior se deduce que una forma cuadrática es reducible en $\mathbb{Q}[x, y]$ si y sólo si su discriminante es cuadrado perfecto, y ese caso tuvo que ser estudiado aparte.

Nuestra teoría se aplicará satisfactoriamente a formas factorizables irreducibles, caracterizadas por estar definidas por generadores de K.

Teorema 1.8 *Sea un cuerpo numérico $K = \mathbb{Q}(\alpha_2, \ldots, \alpha_r)$. Entonces la forma $F(x_1, \ldots, x_r) = \mathrm{N}(x_1 + x_2\alpha_2 + \cdots + x_r\alpha_r)$ es irreducible en $\mathbb{Q}[x_1, \ldots, x_r]$ y toda forma factorizable irreducible en $\mathbb{Q}[x_1, \ldots, x_r]$ es equivalente a un múltiplo por una constante de una forma de este tipo.*

DEMOSTRACIÓN: Supongamos que $F = GH$, donde $G, H \in \mathbb{Q}[x_1, \ldots, x_r]$. Por definición

$$F = \big(x_1 + x_2\sigma_1(\alpha_2) + \cdots + x_r\sigma_1(\alpha_r)\big)\cdots\big(x_1 + x_2\sigma_n(\alpha_2) + \cdots + x_r\sigma_n(\alpha_r)\big).$$

Cada forma $L_i = x_1 + x_2\sigma_i(\alpha_2) + \cdots + x_r\sigma_i(\alpha_r)$ divide a G o a H. Digamos que L_1 divide a G, o sea, $G = L_1M$. Aplicando el monomorfismo σ_i y teniendo en cuenta que G tiene los coeficientes racionales llegamos a que $G = L_i\sigma_i(M)$, o sea, todas las formas L_i dividen al polinomio G.

Como $\alpha_2, \ldots, \alpha_r$ generan K, si dos monomorfismos coinciden sobre ellos es que son iguales. De aquí se sigue que las formas L_i son distintas dos a dos, y como el coeficiente de x_1 es 1 en todas ellas, no pueden diferenciarse en una unidad, es decir, son primas entre sí. Consecuentemente su producto, o sea, F, divide a G. Esto implica que H es una constante, luego F es irreducible.

Si $F^*(x_1,\dots,x_r)$ es una forma irreducible factorizable de grado n, por el teorema 1.5 podemos suponer que el coeficiente de x_1^n es no nulo, y entonces F^* factoriza como

$$F^* = A(x_1 + \beta_{12}x_2 + \cdots + \beta_{1r}x_r)\cdots(x_1 + \beta_{n2}x_2 + \cdots + \beta_{nr}x_r).$$

Consideremos el cuerpo $K = \mathbb{Q}(\beta_{12},\dots,\beta_{1r})$ y la forma irreducible $F = \mathrm{N}(x_1 + \beta_{12}x_2 + \cdots + \beta_{1r}x_r)$.

Tenemos que la forma $(x_1+\beta_{12}x_2+\cdots+\beta_{1r}x_r)$ divide a F y a F^*. Aplicando los monomorfismos de K obtenemos que todos los factores de F dividen a F^* y en la prueba de la parte anterior hemos visto que son primos entre sí, luego F divide a F^*. Como F^* es irreducible ha de ser un múltiplo de F por una constante. ∎

1.8 Conclusión

El resto de este libro está dedicado a desarrollar las técnicas algebraicas y analíticas que permiten abordar los distintos problemas que hemos citado en este breve recorrido por la teoría de números del siglo XIX. Encontraremos un método para resolver las ecuaciones diofánticas del tipo estudiado en las secciones anteriores, conoceremos la teoría de Gauss sobre formas cuadráticas, incluyendo la ley de reciprocidad, determinaremos los enteros que son sumas de dos, tres y cuatro cuadrados, probaremos los resultados más importantes de Kummer sobre el teorema de Fermat, así como el teorema de Dirichlet sobre primos en progresiones aritméticas. Todo ello lo obtendremos desde el marco de la teoría general de cuerpos numéricos, que fue desarrollada por Dedekind a finales del siglo XIX generalizando y unificando los razonamientos de sus antecesores. Excepcionalmente haremos una incursión en la teoría moderna. Demostraremos el teorema de Hasse Minkowski sobre clasificación de formas cuadráticas, con el que obtendremos, si no la última palabra, sí una visión bastante profunda de la ley de reciprocidad cuadrática.

El último capítulo contiene algunos resultados de la teoría de números trascendentes. Concretamente probamos el teorema de Lindemann–Weierstrass, que generaliza las pruebas de trascendencia de e y π, y el teorema de Gelfond–Schneider, que resuelve una parte del séptimo problema de Hilbert. La teoría de números trascendentes es mucho más ardua que la de números algebraicos, y en muchas ocasiones requiere a ésta como herramienta a un nivel mucho más elevado que el de este libro. Sirvan los ejemplos presentados como una pequeña y parcial muestra de sus técnicas.

Capítulo II

Cuerpos numéricos

El estudio de los cuerpos numéricos está en la base de la teoría algebraica de números. Toda la teoría que vamos a desarrollar resulta especialmente sencilla y elegante cuando se aplica al caso de los *cuerpos cuadráticos,* es decir, los cuerpos numéricos de grado 2. Comencemos describiendo estos cuerpos.

Si K es un cuerpo cuadrático, la teoría de Galois nos da que tiene un elemento primitivo, es decir, existe un $\zeta \in K$ tal que $K = \mathbb{Q}(\zeta)$. Entonces $\operatorname{pol\,mín}\zeta$ tiene grado 2. Multiplicándolo por una constante obtenemos un polinomio ax^2+bx+c con coeficientes enteros con raíz ζ y tal que $a \neq 0$. Si llamamos $D = b^2 - 4ac$, entonces $\zeta = \frac{-b\pm\sqrt{D}}{2a}$, y es claro que $K = \mathbb{Q}\big(\sqrt{D}\,\big)$.

El número D no puede ser un cuadrado perfecto, o de lo contrario $K = \mathbb{Q}$ y su grado sería 1. Digamos que $D = m^2d$, donde d es libre de cuadrados (quizá $d = -1$). Entonces $\sqrt{D} = m\sqrt{d}$ y es evidente que $K = \mathbb{Q}\big(\sqrt{d}\,\big)$.

En resumen, todo cuerpo cuadrático es de la forma $\mathbb{Q}\big(\sqrt{d}\,\big)$ para un entero d libre de cuadrados. Sus elementos son de la forma $\mathbb{Q}\big(\sqrt{d}\,\big) = \{a+b\sqrt{d} \mid a, b \in \mathbb{Q}\}$.

Pronto veremos que si $d \neq d'$ en estas condiciones, entonces los cuerpos que determinan son distintos.

En lo sucesivo, cuando digamos que $\mathbb{Q}\big(\sqrt{d}\,\big)$ es un cuerpo cuadrático se sobrentenderá que d es un entero libre de cuadrados. Si $d < 0$ se entiende que $\sqrt{d}$ es el número complejo $\sqrt{-d}\,i$.

2.1 Enteros algebraicos

Puede considerarse que el primer paso en la construcción de la teoría algebraica de números moderna lo dio Dedekind al definir los enteros algebraicos. Éstos permiten desarrollar una teoría general que recoja como casos particulares los resultados clásicos sobre enteros cuadráticos (como son los enteros de Gauss) o enteros ciclotómicos. En general, los enteros algebraicos juegan el mismo papel respecto a los números algebraicos que los enteros ordinarios respecto a los números racionales.

Definición 2.1 Un número complejo es un *entero algebraico* si y sólo si es la raíz de un polinomio mónico con coeficientes enteros.

Llamaremos $\mathbb{A}$ al cuerpo de todos los números algebraicos y $\mathbb{E}$ al conjunto de todos los enteros algebraicos (que, como pronto veremos, es un anillo). Claramente $\mathbb{E} \subset \mathbb{A}$.

Teorema 2.2 *Un número algebraico a es un entero algebraico si y sólo si* $\operatorname{pol\,mín} a \in \mathbb{Z}[x]$.

Demostración: Una implicación es obvia. Supongamos que a es un entero algebraico y sea $p(x) \in \mathbb{Z}[x]$ un polinomio mónico tal que $p(a) = 0$. Sea $q(x)$ un factor irreducible de $p(x)$ en $\mathbb{Z}[x]$ tal que $q(a) = 0$. Existe un polinomio $r(x) \in \mathbb{Z}[x]$ tal que $p(x) = q(x)r(x)$. Como el producto de los coeficientes directores de $q(x)$ y $r(x)$ debe ser igual al coeficiente director de $p(x)$ que es 1, el coeficiente director de $q(x)$ debe ser ± 1. Podemos exigir que sea 1 y así $q(x)$ es un polinomio mónico irreducible en $\mathbb{Z}[x]$ del que a es raíz. Por el criterio de irreducibilidad de Gauss, $q(x)$ también es irreducible en $\mathbb{Q}[x]$, luego $q(x) = \operatorname{pol\,mín} a \in \mathbb{Z}[x]$. ∎

Como el polinomio mínimo de un número racional r es $x - r$, es obvio ahora que un número racional es un entero algebraico si y sólo si es un entero. Las propiedades básicas de los enteros algebraicos se deducen del teorema siguiente.

Teorema 2.3 *Un número complejo c es un entero algebraico si y sólo si el anillo $\mathbb{Z}[c] = \{q(c) \mid q(x) \in \mathbb{Z}[x]\}$ es un $\mathbb{Z}$-módulo finitamente generado. En tal caso dicho módulo es libre de rango $|\mathbb{Q}(c) : \mathbb{Q}|$.*

Demostración: Supongamos que c es un entero algebraico. Entonces $p(c) = 0$, donde $p(x)$ es un polinomio mónico con coeficientes enteros y de grado n. Veamos que

$$\mathbb{Z}[c] = \langle c^m \mid m = 1, \ldots, n-1 \rangle . \tag{2.1}$$

Un elemento arbitrario de $\mathbb{Z}[c]$ es de la forma $q(c)$, donde $q(x)$ es un polinomio con coeficientes enteros. Dividimos $q(x) = p(x)u(x) + r(x)$, donde u y r tienen ambos coeficientes enteros y el grado de r es menor que n. Entonces resulta que $q(c) = r(c)$, luego pertenece al miembro derecho de (2.1), y la otra inclusión es obvia. De hecho el generador $(1, c, \ldots, c^{n-1})$ es una base, pues una combinación lineal nula es de la forma $r(c) = 0$, con $r(x) \in \mathbb{Z}[x]$ de grado menor que n, luego concluimos que $r = 0$.

Supongamos ahora que $\mathbb{Z}[c]$ es finitamente generado. Digamos que admite n generadores $v_1, \ldots, v_n$. Cada v_i es un polinomio en c con coeficientes enteros. Sea m mayor que el grado de cualquiera de dichos polinomios.

Entonces c^m se expresa como combinación lineal con coeficientes enteros de los v_i, luego en definitiva $c^m = q(c)$, con $q(x) \in \mathbb{Z}[x]$ de grado menor que m. La ecuación $c^m - q(c) = 0$ justifica que c es un entero algebraico. ∎

Con esto estamos en condiciones de probar lo que habíamos anunciado:

Teorema 2.4 *El conjunto $\mathbb{E}$ de los enteros algebraicos es un subanillo de $\mathbb{A}$.*

DEMOSTRACIÓN: Sean c, $d \in \mathbb{E}$. Hay que probar que $c+d$ y cd están en $\mathbb{E}$. Sea $\{v_1, \ldots, v_n\}$ un generador de $\mathbb{Z}[c]$ y sea $\{w_1, \ldots, w_m\}$ un generador de $\mathbb{Z}[d]$. Sea M el $\mathbb{Z}$-módulo generado por los todos los productos $v_i w_j$.

Todo c^r se expresa como combinación lineal con coeficientes enteros de los v_i y todo d^s se expresa como combinación lineal con coeficientes enteros de los w_j. Al multiplicar estas expresiones obtenemos una expresión de $c^r d^s$ como combinación lineal con coeficientes enteros de los generadores de M, luego cada $c^r d^s \in M$.

En particular, $\mathbb{Z}[cd] \subset M$, luego es un $\mathbb{Z}$-módulo finitamente generado (todo submódulo de un $\mathbb{Z}$-módulo finitamente generado es finitamente generado). Por el teorema anterior $cd \in \mathbb{E}$.

Al desarrollar $(c+d)^k$ obtenemos una combinación lineal con coeficientes enteros de elementos de la forma $c^r d^s$, que están en M, luego $\mathbb{Z}[c+d] \subset M$ y también se cumple que $c+d \in \mathbb{E}$. ∎

Del mismo modo que todo número racional es cociente de dos números enteros, todo número algebraico es cociente de dos enteros algebraicos. En efecto:

Teorema 2.5 *Para cada $c \in \mathbb{A}$ existe un entero no nulo m tal que $mc \in \mathbb{E}$.*

DEMOSTRACIÓN: Sea $\operatorname{pol\,mín}\, c = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Sea m el producto de los denominadores de todos los coeficientes no nulos de $p(x)$.

Entonces $m^n(c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0) = 0$, luego

$$(mc)^n + a_{n-1}m(mc)^{n-1} + \cdots + a_1 m^{n-1}(mc) + a_0 = 0.$$

Por lo tanto, $x^n + a_{n-1}mx^{n-1} + \cdots + a_1 m^{n-1}x + a_0$ es un polinomio mónico con coeficientes enteros del cual es raíz mc. ∎

Desde el punto de vista de la teoría algebraica de números, los enteros usuales son sólo un caso particular de los enteros algebraicos. Por ello es costumbre reservar la palabra "entero" para referirse a los enteros algebraicos. Nosotros seguiremos esta costumbre en lo sucesivo y por ello a los elementos de $\mathbb{Z}$ los llamaremos "enteros racionales", pues ciertamente son los enteros (algebraicos) que además son números racionales.

Ejemplo 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 $\text{pol mín}(2+\alpha^2) = x^3+2x^2-4x-9$. 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 igual para calcular normas, trazas, etc.

2.2 Discriminantes

Completamos los requisitos algebraicos de nuestra teoría estudiando los discriminantes de bases de cuerpos numéricos. En general, si K es un cuerpo numérico, la traza $\text{Tr} : K \longrightarrow \mathbb{Q}$ determina una forma bilineal simétrica

$$\begin{array}{ccc} K\times K & \longrightarrow & \mathbb{Q} \\ (\alpha,\beta) & \mapsto & \text{Tr}(\alpha\beta) \end{array}$$

Dada una base $\{\beta_1,\dots,\beta_n\}$ de K, la matriz de la forma en esta base es $A = \big(\text{Tr}(\beta_i\beta_j)\big)$. Si llamamos $\sigma_1,\dots,\sigma_n$ a los *monomorfismos* de K, es decir, los monomorfismos $\sigma : K \longrightarrow \mathbb{C}$, esta matriz puede descomponerse como producto $A = \big(\sigma_k(\beta_i)\big)_{ik}\big(\sigma_k(\beta_j)\big)_{kj}$.

Definición 2.6 Llamaremos *discriminante* de una base $B = \{\beta_1,\dots,\beta_n\}$ de un cuerpo numérico K al número

$$\Delta[B] = \Delta[\beta_1,\dots,\beta_n] = \det\big(\text{Tr}(\beta_i\beta_j)\big) = \Big(\det\big(\sigma_i(\beta_j)\big)\Big)^2.$$

Notar que el cuadrado hace que el valor del discriminante no dependa del orden de los elementos de la base o del de los monomorfismos.

En particular, si ζ es un elemento primitivo de K, las potencias $1,\zeta,\dots,\zeta^{n-1}$ forman una base de K. Por brevedad escribiremos $\Delta[\zeta] = \Delta[1,\zeta,\dots,\zeta^{n-1}]$.

Los discriminantes constituyen una herramienta muy poderosa para trabajar con cuerpos numéricos. El teorema siguiente recoge sus propiedades más importantes.

Teorema 2.7 *Sean B y C dos bases de un cuerpo numérico K.*

1. *$\Delta[B] \in \mathbb{Q}$ y $\Delta[B] \neq 0$.*
2. *Si D_B^C es la matriz cuyas filas son las coordenadas de los elementos de B respecto de la base C, entonces $\Delta[B] = |D_B^C|^2\Delta[C]$.*
3. *Si los elementos de B son enteros, $\Delta[B] \in \mathbb{Z}$ y $\Delta[B] \equiv 0,1 \pmod 4$.*

DEMOSTRACIÓN: La propiedad 2) es un hecho general sobre formas bilineales. Es obvio que los discriminantes son números racionales. Para probar que son no nulos basta verlo para una base en particular (con esto probamos que la forma bilineal determinada por la traza es regular). Consideremos concretamente $\{1, \zeta, \dots, \zeta^{n-1}\}$, donde ζ es un elemento primitivo de K. Para esta base el determinante que aparece es un determinante de Vandermonde

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

y como los n conjugados de ζ son distintos, el determinante es no nulo.

Es obvio que los conjugados de enteros son enteros, luego las trazas de los enteros son enteros racionales, y así la primera parte de 3) es clara.

Sea $B = \{\beta_1, \dots, \beta_n\}$. Sea ρ uno de los monomorfismos de K. Llamemos $A = \big(\sigma_i(\beta_j)\big)$. El determinante de A es una suma de productos de la forma

$$\pm\sigma_{\tau(1)}(\beta_1)\cdots\sigma_{\tau(n)}(\beta_n),$$

donde $\tau \in \Sigma_n$, el grupo de las permutaciones de n elementos. Si le aplicamos ρ obtenemos un término de la forma

$$\pm\rho\big(\sigma_{\tau(1)}(\beta_1)\big)\cdots\rho\big(\sigma_{\tau(n)}(\beta_n)\big).$$

Ahora bien, cada monomorfismo $\sigma_i\rho$ ha de ser un $\sigma_{\rho(i)}$, para cierto índice $\rho(i)$ (y ahora estamos llamando ρ a una permutación de $\{1, \dots, n\}$ inducida por el automorfismo ρ). Por lo tanto la imagen por ρ del producto es

$$\pm\sigma_{\rho(\tau(1))}(\beta_1)\cdots\sigma_{\rho(\tau(n))}(\beta_n),$$

es decir, el sumando del determinante correspondiente a la permutación $\tau\rho$.

Si (la permutación inducida por) ρ es una permutación par entonces ρ envía sumandos con signo positivo a sumandos con signo positivo y sumandos con signo negativo a sumandos con signo negativo, mientras que si ρ es impar entonces intercambia los sumandos positivos con los negativos. En otras palabras, si llamamos respectivamente P y N a la suma de términos positivos y negativos (sin el signo) del determinante de A, tenemos que $\det A = P - N$ y o bien $\rho(P) = P$ y $\rho(N) = N$, o bien $\rho(P) = N$ y $\rho(N) = P$.

En cualquier caso $\rho(P + N) = P + N$ y $\rho(PN) = PN$, para todo automorfismo ρ, luego concluimos que $P+N$, $PN \in \mathbb{Q}$. Además son enteros algebraicos, luego están en $\mathbb{Z}$. Finalmente,

$$\Delta[B] = (P - N)^2 = (P + N)^2 - 4PN \equiv (P + N)^2 \equiv 0, 1 \text{ (mód 4)},$$

pues todo cuadrado es 0 o 1 módulo 4. ∎

En la prueba anterior hemos visto que los discriminantes asociados a elementos primitivos son especialmente simples de manejar debido a que son el cuadrado de un determinante de Vandermonde. Este hecho también simplifica enormemente su cálculo práctico.

Teorema 2.8 *Sea $K = \mathbb{Q}(\zeta)$ un cuerpo numérico y $p(x) = \operatorname{pol}\operatorname{mín}\zeta$. Entonces*

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

donde $p'(x)$ es la derivada formal de $p(x)$ y n es el grado de K.

DEMOSTRACIÓN: Según hemos visto en la prueba del teorema anterior

$$\Delta[\zeta] = \prod_{1\le i<j\le n} \big(\sigma_j(\zeta) - \sigma_i(\zeta)\big)^2. \tag{2.2}$$

Por otro lado, $p(x) = \prod_{i=1}^n \big(x - \sigma_i(\zeta)\big)$, y se demuestra fácilmente (por inducción sobre n) que

$$p'(x) = \sum_{j=1}^n \prod_{\substack{i=1\\ i\ne j}}^n \big(x - \sigma_i(\zeta)\big),$$

luego

$$p'\big(\sigma_j(\zeta)\big) = \prod_{\substack{i=1\\ i\ne j}}^n \big(\sigma_j(\zeta) - \sigma_i(\zeta)\big) \qquad \text{para } j = 1,\dots,n.$$

Multiplicando todas estas ecuaciones obtenemos

$$\mathrm{N}\big(p'(\zeta)\big) = \prod_{j=1}^n \sigma_j\big(p'(\zeta)\big) = \prod_{j=1}^n p'\big(\sigma_j(\zeta)\big) = \prod_{\substack{i,j=1\\ i\ne j}}^n \big(\sigma_j(\zeta) - \sigma_i(\zeta)\big).$$

Agrupamos los pares $\big(\sigma_j(\zeta)-\sigma_i(\zeta)\big)\big(\sigma_i(\zeta)-\sigma_j(\zeta)\big) = -\big(\sigma_j(\zeta)-\sigma_i(\zeta)\big)^2$. El número de factores (-1) que aparecen es $n(n-1)/2$, luego teniendo en cuenta (2.2) queda $\mathrm{N}\big(p'(\zeta)\big) = (-1)^{n(n-1)/2}\Delta[\zeta]$, y de aquí se sigue el teorema. ∎

Ejercicio: Sea $K = \mathbb{Q}\big(\sqrt{d}\big)$ un cuerpo cuadrático. Calcular $\Delta\big[1,\sqrt{d}\big]$ directamente y mediante el teorema anterior.

Ejercicio: Sea ω una raíz p-ésima primitiva de la unidad para un primo impar p. Probar que $\Delta[\omega] = (-1)^{(p-1)/2}p^{p-2}$.

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,

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

Desde aquí se llega a la fórmula indicada sin más que operar. (Hemos supuesto $a \ne 0$, 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 $\Delta[\alpha] = 5^4b^4 + 2^8a^5$.

Definición 2.9 En el teorema 2.7 hemos visto que la forma bilineal asociada a la traza de un cuerpo numérico K es regular, por lo que induce un isomorfismo entre K y su espacio vectorial dual. Concretamente, cada $\alpha \in K$ se corresponde con la aplicación lineal $K \longrightarrow \mathbb{Q}$ dada por $\beta \mapsto \mathrm{Tr}(\alpha\beta)$. Si $B = \{\alpha_1, \ldots, \alpha_n\}$ es una base de K, podemos considerar su base asociada en el espacio dual de K, que a través del isomorfismo citado se corresponde con una nueva base $\{\alpha_1^*, \ldots, \alpha_n^*\}$ de K. Esta base se llama *base dual* de B, y está caracterizada por que

$$\mathrm{Tr}(\alpha_i\alpha_j^*) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Ejemplo Sea α una raíz del polinomio $x^3 + 4x + 1$. Una base del cuerpo $\mathbb{Q}(\alpha)$ la forman obviamente los números $\{1, \alpha, \alpha^2\}$. Vamos a calcular la matriz en dicha base de la forma bilineal asociada a la traza. En la página 22 tenemos los conjugados de α. Si por ejemplo queremos calcular $\mathrm{Tr}(\alpha \cdot \alpha)$ calculamos

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

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

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

Es fácil ver entonces que la base dual de la dada es

$$\frac{265}{283} + \frac{24}{283}\alpha + \frac{64}{383}\alpha^2,$$
$$\frac{24}{283} - \frac{32}{283}\alpha + \frac{9}{383}\alpha^2,$$
$$\frac{64}{283} + \frac{9}{283}\alpha + \frac{24}{383}\alpha^2.$$

■

2.3 Módulos y órdenes

Finalmente estamos en condiciones de estudiar de forma sistemática algunos conceptos que nos surgieron en el capítulo anterior, en relación con el estudio de las ecuaciones definidas mediante formas. Recordemos la definición de módulo:

Definición 2.10 Un *módulo* de un cuerpo numérico K es un subgrupo aditivo de K finitamente generado.

Vimos en el capítulo anterior que los módulos están asociados a clases de equivalencia de formas: Si $\alpha_1, \ldots, \alpha_r$ generan un módulo M, entonces la ecuación diofántica

$$\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r) = c \tag{2.3}$$

tiene por soluciones a (las coordenadas de) los elementos de M de norma c. Un generador distinto da lugar a una forma equivalente.

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, y los $\mathbb{Z}$-módulos finitamente generados libres de torsión son libres, o sea, tienen base, y todas las bases tienen el mismo número de elementos, llamado rango de M ($\operatorname{rang} M$).

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 de K, $\operatorname{rang} M \le n$ (el grado de K).

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.

Si B y B' son dos bases de M, entonces la matriz de cambio de base tiene coeficientes enteros, al igual que su inversa, luego su determinante ha de ser ± 1. El teorema 2.7 nos da entonces que $\Delta[B] = \Delta[B']$, luego podemos definir el *discriminante* de M como el discriminante $\Delta[M]$ de cualquiera de sus bases.

Definición 2.11 Si M es un módulo de 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 $\alpha \in K$, $\alpha \neq 0$ tal que $N = \alpha M$.

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

Ejercicio: Comprobar que si F es una forma asociada a un módulo de la forma αM, entonces $F = \mathrm{N}(\alpha)F'$, donde F' es una forma asociada al módulo M.

Este ejercicio justifica que si estudiamos un módulo para resolver una determinada ecuación diofántica de tipo (2.3) podemos sustituirlo por otro similar.

Observar que si $\alpha_1, \ldots, \alpha_r$ son no nulos y generan un módulo completo M, entonces los números $1, \alpha_2/\alpha_1, \ldots, \alpha_r/\alpha_1$ generan el módulo similar $(1/\alpha_1)M$ y, en particular,

$$K = \mathbb{Q}(\alpha_2/\alpha_1, \ldots, \alpha_r/\alpha_1).$$

Por el teorema 1.8, la forma asociada a este último generador es irreducible, luego también lo es la forma $\mathrm{N}(x_1\alpha_1 + \cdots + x_r\alpha_r)$, pues se diferencia de la anterior en una constante. En resumen, las formas asociadas a módulos completos son irreducibles. Llamaremos *formas completas* a las formas asociadas a módulos completos. Éstas son exactamente las formas a las que la teoría que vamos a desarrollar se aplica con éxito.

Ejemplo Consideremos la ecuación $x^2 + 5xy + 2y^2 = 2$. Siguiendo la técnica del capítulo anterior podemos factorizarla como

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

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.

Con esto no hemos hecho sino reformular el problema. Veamos una mínima muestra de las ventajas del nuevo enfoque. Consideremos el número

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

Sencillos cálculos nos dan que $\mathrm{N}(\epsilon) = 1$ y que $\epsilon M \subset M$. Parte de la teoría que tenemos por delante dará cuenta de cómo se puede llegar a un número con estas propiedades. De momento veamos el interés de estos hechos. Ahora es claro que los números

$$\epsilon^n \frac{5+\sqrt{17}}{2}, \quad \text{para } n = 1, 2, 3, \ldots$$

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. Esto es un fragmento de la técnica que usaremos para resolver el caso general: veremos que todas las soluciones pueden encontrarse de este modo a partir de un número finito de soluciones básicas.

Planteando esto en general, una solución de (2.3) esta determinada por un elemento m en un módulo M tal que $\mathrm{N}(m) = c$. Si ϵ es un elemento de K tal que $\epsilon m \in M$ y $\mathrm{N}(\epsilon) = 1$, entonces $\mathrm{N}(\epsilon m) = c$, luego ϵm es otra solución. Esto nos lleva a la definición de coeficiente de un módulo.

Definición 2.12 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.

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

En estos términos, los elementos de $\mathcal{O}_M$ de norma 1 satisfacen las propiedades que pedíamos a ϵ en el ejemplo anterior. Para localizarlos probaremos que las unidades de $\mathcal{O}_M$ son precisamente los elementos de norma ± 1 y así el problema se reducirá parcialmente al problema algebraico de determinar las unidades de un anillo. Primero necesitamos el siguiente hecho básico sobre $\mathcal{O}_M$.

Teorema 2.13 *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 2.14 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 es el anillo de coeficientes de un módulo completo (al menos de sí mismo).

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. Recogemos éste y otros hechos importantes en el próximo teorema.

Teorema 2.15 *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 luego $\mathbb{Z}[\alpha]$ es finitamente generado (porque $\mathcal{O}$ es un módulo), luego por el teorema 2.3 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 2.16 *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 2.17 *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 $\mathcal{O}$. Claramente I es un módulo (todo $\mathbb{Z}$-submódulo de un $\mathbb{Z}$-módulo finitamente generado es 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. ∎

Volvamos al problema de las ecuaciones diofánticas definidas por formas completas. Ya sabemos que es equivalente a encontrar todos los elementos de una norma dada c en un módulo completo M. También hemos visto que si tenemos un $m \in M$ con $\mathrm{N}(m) = c$, entonces obtenemos nuevas soluciones considerando números de la forma ϵm, donde, en los términos que hemos introducido, ϵ es una unidad de $\mathcal{O}_M$ de norma 1. Conviene introducir una definición:

Definición 2.18 Dos elementos x e y de un módulo completo M son *asociados* si existe una unidad $\epsilon \in \mathcal{O}_M$ tal que $x = \epsilon y$.

Teniendo en cuenta que un orden es su propio anillo de coeficientes, resulta que cuando M es un orden este concepto de asociación se corresponde con el usual en teoría de anillos: dos elementos de un anillo son asociados si se diferencian en una unidad.

Así, resolver una ecuación diofántica asociada a una forma completa se reduce a encontrar un conjunto maximal de elementos no asociados de una norma dada junto con todas las unidades de norma $+1$. El planteamiento es razonable porque ahora probamos que tal conjunto maximal es siempre finito, es decir, 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 2.19 *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 2.15, 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.

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. ∎

Es importante señalar que la prueba del teorema anterior no es constructiva, es decir, no nos da un método para encontrar un conjunto maximal de elementos no asociados de una norma dada. Más adelante daremos una versión efectiva de este resultado. Por el momento hemos conseguido perfilar nuestro objetivo:

> Para resolver el problema de las ecuaciones diofánticas determinadas por formas completas hemos de dar un algoritmo para determinar un conjunto maximal (finito) de elementos no asociados de una norma dada en un módulo completo y otro para calcular un generador del grupo de las unidades de norma $+1$ de un orden numérico (que también veremos que es finito).

Terminamos la sección con un resultado fundamental a la hora de trabajar con órdenes numéricos. Partimos de unas consecuencias elementales de 2.7.

Teorema 2.20 *Sea K un cuerpo numérico.*

1. *Si $\mathcal{O}$ es un orden de K, entonces $\Delta[\mathcal{O}] \in \mathbb{Z}$.*
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 2.7.

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 2.7 concluimos 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 último apartado del teorema anterior implica que no es posible formar cadenas ascendentes de órdenes en un cuerpo numérico (esto es falso para módulos: basta pensar en $M \subset (1/2)M \subset (1/4)M \subset (1/8)M \subset \cdots$).

Así pues, cada orden está contenido en un orden maximal por encima del cual no hay más órdenes. Vamos a probar que de hecho todos los órdenes de K están contenidos en un mismo orden maximal. El teorema anterior nos dice también que dicho orden tendrá un discriminante menor que el de cualquier otro orden, y éste va a ser el criterio con el que lo encontraremos.

Definición 2.21 Llamaremos *orden* (maximal) de un cuerpo numérico K al conjunto $\mathcal{O}_K = K \cap \mathbb{E}$. Claramente es un anillo que contiene a todos los demás órdenes de K.

No es evidente que $\mathcal{O}_K$ sea él mismo un orden. Para probarlo notemos primero que del teorema 2.5 se sigue inmediatamente que K es el cuerpo de cocientes de $\mathcal{O}_K$, así como que existe un $\zeta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\zeta)$, es decir, que siempre podemos tomar un elemento primitivo que sea entero. Las n primeras potencias de este elemento primitivo constituyen una base de K formada por enteros.

Teorema 2.22 *Si K es un cuerpo numérico, entonces $\mathcal{O}_K$ es un orden de K que contiene a todos los órdenes.*

DEMOSTRACIÓN: Según acabamos de comentar, K tiene una base B formada por enteros. Los discriminantes de estas bases son enteros racionales, luego podemos tomar una base de K formada por enteros tal que el número natural $\big|\Delta[B]\big|$ sea mínimo. Digamos $B = \{b_1, \ldots, b_n\}$. Vamos a probar que entonces B es una base de $\mathcal{O}_K$ como módulo. Obviamente sus elementos son linealmente independientes sobre $\mathbb{Z}$, pues lo son sobre $\mathbb{Q}$. Basta probar que generan $\mathcal{O}_K$.

Supongamos, por el contrario, que existe un elemento $d \in \mathcal{O}_K$ que no pertenezca al submódulo generado por $\{b_1, \ldots, b_n\}$. Como en cualquier caso $\{b_1, \ldots, b_n\}$ es una base de K, se cumplirá que

$$d = a_1 b_1 + \cdots + a_n b_n, \tag{2.4}$$

para ciertos números racionales $a_1, \ldots, a_n$ no todos enteros. Podemos suponer que $a_1 \notin \mathbb{Z}$. Sea $a_1 = a + r$, donde $a \in \mathbb{Z}$ y $0 < r < 1$. Sustituyendo en (2.4) obtenemos que

$$r b_1 + a_2 b_2 + \cdots + a_n b_n = d - a b_1 \in \mathcal{O}_K.$$

Si llamamos c_1 a este elemento y $c_i = b_i$ para $i = 2, \ldots, n$ obtenemos una nueva base C de K formada por enteros tal que la matriz de cambio de base es

$$D_C^B = \begin{pmatrix} r & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Claramente $\big|D_C^B\big| = r$ y en consecuencia

$$\big|\Delta[C]\big| = r^2 \big|\Delta[B]\big| < \big|\Delta[B]\big|,$$

en contra de la elección de B. Por lo tanto B es una base de $\mathcal{O}_K$ como $\mathbb{Z}$-módulo. ∎

Definición 2.23 Llamaremos *discriminante* de K a $\Delta_K = \Delta[\mathcal{O}_K] \in \mathbb{Z}$. Una *base entera* de K es una base de $\mathcal{O}_K$ como módulo.

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 cuyas coordenadas son enteras.

Es importante tener claro que una base de un cuerpo K formada por enteros no es necesariamente una base entera. Basta pensar que si $v_1, \ldots, v_n$ es una base entera de K, entonces $2v_1, \ldots, v_n$ sigue siendo una base de K formada por enteros, pero ya no es una base entera, pues v_1 es un entero algebraico y no tiene coordenadas enteras respecto a esta segunda base.

En general, si C es una base de K formada por enteros y B es una base entera, entonces los mismos argumentos empleados en el teorema 2.20 nos dan que $\Delta[C] = m^2\Delta[B]$, para cierto número natural m, de manera que C es una base entera si y sólo si $m = 1$. Esto nos da de nuevo que una base entera es simplemente una base formada por enteros con discriminante mínimo, como de hecho hemos visto en la prueba del teorema 2.22.

2.4 Determinación de bases enteras

Para encontrar una base entera de un cuerpo numérico K basta dar un procedimiento para obtener a partir de una base formada por enteros otra base formada por enteros con discriminante menor, siempre que exista, pues así, partiendo de la base formada por las potencias de un elemento primitivo entero, tras un número finito de pasos llegaremos a una base de discriminante mínimo, que será una base entera según las últimas consideraciones de la sección anterior.

Antes de abordar el asunto en general veamos lo que ocurre con los cuerpos cuadráticos.

Enteros cuadráticos En $K = \mathbb{Q}(\sqrt{d}\,)$ 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 2.20 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 2.7 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

$$\alpha = \frac{1 + \sqrt{d}}{2}$$

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

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

$$\alpha = \begin{cases} \sqrt{d} & \text{si } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4 \end{cases} \tag{2.5}$$

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 $0 \leq r < m$. 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 $\mathcal{O}_1$.

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

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

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 i-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 $0 \leq g_i \leq p-1$ 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 (después 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 determinante de K.

Partimos del orden $\mathbb{Z}[\xi]$, cuyo discriminante vale, según el teorema 2.8, $\Delta[\xi] = -\mathrm{N}(\alpha)$, 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 2.26 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. Por ejemplo el cuerpo que acabamos de estudiar.

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 $\sigma_1\big(\sqrt[3]{m}\,\big) = \omega\sqrt[3]{m}$, $\sigma_2\big(\sqrt[3]{m}\,\big) = \omega^2\sqrt[3]{m}$. Observar 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.

Notar 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 2.27 *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 2.25 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 $\alpha = (u + \theta_1)/2$, 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 2.25 hemos de comprobar los siguientes números (para aprovechar la simetría ordenamos la base en la forma $\theta_1, \theta_2, 1$):

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

Hemos tomado como representantes de las clases módulo 3 los números -1, 0, 1 en lugar de 0, 1, 2 (ver el comentario tras el teorema 2.25).

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

$$3 \mid (1-ab), \tag{2.6}$$
$$27 \mid (1+ab^2+a^2b-3ab). \tag{2.7}$$

De (2.6) se sigue que

$$a \equiv b \equiv \pm 1 \pmod 3. \tag{2.8}$$

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 $a \equiv \pm b \pmod 9$ pero que cumplen (2.8) son $(1,4)$, $(1,7)$, $(2,5)$, $(2,8)$, $(4,7)$, $(5,8)$. En ninguno de estos casos se cumple (2.7). ∎

La tabla siguiente resume el teorema:

Tabla 2.1: Tipos de cuerpos cúbicos puros

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

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 $M = \big\langle 4, \sqrt[3]{2}, \sqrt[3]{4}\,\big\rangle$ es igual a $\big\langle 1, 2\sqrt[3]{2}, 2\sqrt[3]{4}\,\big\rangle$.

Enteros ciclotómicos En el capítulo anterior vimos algunos problemas importantes relacionados con los cuerpos ciclotómicos y sus anillos de enteros. Ciertamente hay muchas razones por las que estos anillos juegan un papel relevante en la teoría algebraica de números. Comenzamos a estudiarlos probando que los que en el capítulo anterior llamamos 'enteros ciclotómicos' son realmente los enteros ciclotómicos en el sentido general, es decir, probaremos que si ω es una raíz p-ésima primitiva de la unidad, donde p es primo, entonces el orden de $K = \mathbb{Q}(\omega)$ es $\mathbb{Z}[\omega]$. El resultado es cierto también si p no es primo, pero no estamos en condiciones de probarlo. Comenzamos con algunas consideraciones previas sobre trazas y normas:

Si $p \nmid i$, entonces $\mathrm{Tr}(\omega^i)$ es la suma de los $p-1$ conjugados de ω^i, es decir,

$$\mathrm{Tr}(\omega^i) = \omega + \omega^2 + \cdots + \omega^{p-1} = -1.$$

Si $a \in \mathbb{Q}$ entonces $\mathrm{Tr}(a) = a + a + \cdots + a = (p-1)a$. En resumen,

$$\mathrm{Tr}(\omega^i) = \begin{cases} -1 & \text{si } p \nmid i \\ p-1 & \text{si } p \mid i \end{cases}$$

En general, si $\sum_{i=0}^{p-1} a_i\omega^i$ es un elemento cualquiera de $\mathbb{Q}(\omega)$, entonces

$$\begin{aligned} \mathrm{Tr}\left(\sum_{i=0}^{p-1} a_i\omega^i\right) &= \sum_{i=0}^{p-1} a_i \,\mathrm{Tr}(\omega^i) = a_0\,\mathrm{Tr}(1) - \sum_{i=1}^{p-1} a_i \\ &= (p-1)a_0 - \sum_{i=1}^{p-1} a_i = pa_0 - \sum_{i=0}^{p-1} a_i. \end{aligned}$$

Respecto a las normas, nos basta observar que si $\pi = 1-\omega$, entonces $\mathrm{N}(\pi) = p$. En efecto, basta evaluar en 1 el polinomio

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

Teorema 2.28 *Sea p un número primo impar y $K = \mathbb{Q}(\omega)$, donde ω es una raíz p-ésima primitiva de la unidad. Entonces $\mathcal{O}_K = \mathbb{Z}[\omega]$.*

Demostración: Sea $\alpha = \sum_{i=0}^{p-2} a_i\omega^i$ un entero ciclotómico de orden p. Hemos de probar que todos los coeficientes son enteros racionales. En principio sabemos que la traza es un entero. Más aún, para cada $0 \le k \le p-2$ tenemos que $\mathrm{Tr}(\alpha\omega^{-k}) \in \mathbb{Z}$. Así tenemos la misma información sobre todos los coeficientes:

$$\begin{aligned} \mathrm{Tr}(\alpha\omega^{-k}) &= pa_k - \sum_{i=0}^{p-2} a_i \in \mathbb{Z}, \qquad \text{para } k \ne p-1 \\ \mathrm{Tr}(\alpha\omega) &= -\sum_{i=0}^{p-2} a_i \in \mathbb{Z}. \end{aligned}$$

Por lo tanto $pa_k \in \mathbb{Z}$ para todo $k = 0, \ldots, p-1$. Llamemos $b_k = pa_k$. Hemos de probar que $p \mid b_k$ para todo k, con lo que los a_k serán también

enteros. Consideremos $\pi = 1 - \omega$. Sustituyendo $\omega = 1 - \pi$ y desarrollando obtenemos

$$p\alpha = \sum_{i=0}^{p-2} b_i \omega^i = \sum_{i=0}^{p-2} c_i \pi^i,$$

donde

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} b_j \in \mathbb{Z},$$

para $i = 0, \ldots, p-2$. Como $\pi = 1 - \omega$, por simetría se cumple también

$$b_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} c_j,$$

para $i = 0, \ldots, p-2$.

Por lo tanto basta probar que $p \mid c_j$ para todo j, pues entonces estas fórmulas implican que p también divide a los b_i.

Lo probaremos por inducción. Suponemos que $p \mid c_i$ para cada $i \leq k-1$ y vamos a probar que $p \mid c_k$, donde $0 \leq k \leq p-2$.

La razón por la que hemos hecho el cambio de variable es que ω es una unidad de $\mathcal{O}_K$, mientras que π cumple $\mathrm{N}(\pi) = p$ (veremos que esto implica que π es primo en $\mathcal{O}_K$). Tenemos que

$$p = \mathrm{N}(1-\omega) = \prod_{i=1}^{p-1} (1 - \omega^i) = (1-\omega)^{p-1} \prod_{i=1}^{p-1} (1 + \omega + \cdots + \omega^{i-1}) = \pi^{p-1}\delta,$$

para cierto $\delta \in \mathcal{O}_K$.

En consecuencia $p \equiv 0 \pmod{\pi^{k+1}}$, es decir, módulo el ideal generado por π^{k+1} en $\mathcal{O}_K$.

Por otro lado,

$$0 \equiv p\alpha = \sum_{i=0}^{p-2} c_i \pi^i \equiv c_k \pi^k \pmod{\pi^{k+1}},$$

pues los términos anteriores a $c_k\pi^k$ son múltiplos de p por hipótesis de inducción y los posteriores son múltiplos de π^{k+1} directamente.

Esto equivale a que $c_k \pi^k = \eta \pi^{k+1}$ para un cierto $\eta \in \mathcal{O}_K$, luego $c_k = \eta\pi$.

Finalmente tomamos normas: $c_k^{p-1} = \mathrm{N}(c_k) = \mathrm{N}(\eta)\,\mathrm{N}(\pi) = p\,\mathrm{N}(\eta)$, luego en efecto $p \mid c_k$. ∎

El teorema 2.8 nos da ahora los discriminantes:

Teorema 2.29 *Sea p un primo impar. El discriminante del cuerpo ciclotómico de orden p es igual a $(-1)^{(p-1)/2} p^{p-2}$.*

DEMOSTRACIÓN: Sea ω una raíz p-ésima primitiva de la unidad. Como los enteros ciclotómicos son el anillo $\mathbb{Z}[\omega]$, una base entera de $\mathbb{Q}(\omega)$ está formada por $1, \omega, \ldots, \omega^{p-1}$. El polinomio mínimo de ω es $p(x) = \frac{x^p-1}{x-1}$ y su derivada vale

$$p'(x) = \frac{px^{p-1}(x-1) - (x^p-1)}{(x-1)^2},$$

luego $p'(\omega) = \frac{p\omega^{p-1}}{\omega-1}$. Así pues,

$$\mathrm{N}\big(p'(\omega)\big) = \frac{p^{p-1}\cdot 1^{p-1}}{p} = p^{p-2}.$$

Como p es impar, $(-1)^{p(p-1)/2} = (-1)^{(p-1)/2}$ y por 2.8

$$\Delta[\omega] = (-1)^{(p-1)/2}p^{p-2}.$$

∎

Respecto a los cuerpos ciclotómicos de orden arbitrario, nos conformaremos con el hecho siguiente:

Teorema 2.30 *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 en la prueba del teorema 2.7, se cumple que

$$\Delta[\omega] = \prod_{1\le i<j\le n} \big(\sigma_i(\omega) - \sigma_j(\omega)\big)^2, \tag{2.9}$$

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 (2.9) 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 $p \nmid \Delta$. ∎

Para terminar con el caso de los cuerpos ciclotómicos, estudiemos el cuerpo ciclotómico octavo $\mathbb{Q}(\omega)$. Su grado es 4 y, de hecho, $\operatorname{pol\,mín}\omega = x^4 + 1$. El teorema 2.8 nos da que el discriminante del orden $\mathbb{Z}[\omega]$ es 256. Hemos de probar que no es posible eliminar ningún 2.

Según el teorema 2.25, 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

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

Notar 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 $\omega, \ldots, \omega^{p-1}$. 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 $\mathbb{Z}[\eta_1, \ldots, \eta_m]$.

Vamos a calcular el discriminante $\Delta_{K'} = \Delta[\eta_1, \ldots, \eta_m] = \det\big(\operatorname{Tr}(\eta_i\eta_j)\big)$. 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 $(1, p, \ldots, p)$. 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 $\{1, \eta, \eta^2 - 2\}$. (Notar 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

$$\begin{aligned} \eta_1 &= 1,246979604, \\ \eta_2 &= -0,4450418670, \\ \eta_3 &= -1,801937736. \end{aligned}$$

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:

Teorema 2.31 *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. Observar 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 $\sqrt{\Delta} \notin \mathbb{Q}$. ∎

2.5 Normas e Índices

Veamos ahora un par de conceptos adicionales de utilidad en el estudio de los cuerpos numéricos.

Definición 2.32 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 2.7 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

$$\Delta[M] = \mathrm{N}(M)^2 \Delta[\mathcal{O}]. \tag{2.10}$$

Observar 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 (2.10) son enteros racionales. En este caso la norma tiene una interpretación algebraica importante.

Teorema 2.33 *Sea M un módulo completo contenido en su anillo de coeficientes $\mathcal{O}$. Entonces $\mathrm{N}(M) = |\mathcal{O} : M|$.*

DEMOSTRACIÓN: Es un hecho conocido (se ve al probar que todo submódulo de un $\mathbb{Z}$-módulo libre es libre) que 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 $\{e_1,\dots,e_n\}$ de $\mathbb{Z}^n$, envía la base B a la base $\{a_1e_1,\dots,a_ne_n\}$, 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 $|\mathcal{O}:M| = |(\mathbb{Z}/a_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/a_n\mathbb{Z})| = |a_1|\cdots|a_n| = \mathrm{N}(M)$. ∎

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

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

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

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 $\mathcal{O}$.

Si las normas nos relacionan los módulos completos con sus anillos de coeficientes, los índices, que definimos seguidamente, relacionan los órdenes con el orden maximal.

Definición 2.35 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 $\mathrm{índ}\,\mathcal{O}$ tal que

$$\Delta[\mathcal{O}] = (\mathrm{índ}\,\mathcal{O})^2\Delta_K. \tag{2.11}$$

Concretamente $\mathrm{índ}\,\mathcal{O}$ 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 2.33 nos da que

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

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

Vamos a calcular los índices de los elementos de algunos cuerpos numéricos. Para un cuerpo cuadrático $\mathbb{Q}\bigl(\sqrt{d}\,\bigr)$, cuando $d\not\equiv 1\ (\mathrm{mód}\ 4)$ tenemos que una base del anillo $\mathbb{Z}\bigl[a+b\sqrt{d}\,\bigr]$ 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 $d\equiv 1$ (mód 4) los enteros son de la forma $\big(a+b\sqrt{d}\,\big)/2$, con $a\equiv b$ (mód 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, $a\not\equiv b$ (mód 9). Usamos la notación del teorema 2.27. 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 $x\equiv y\equiv z$ (mód 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 $3y^3-7z^3=\pm1$, 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 2.4. 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.

Capítulo III

Factorización ideal

Vimos en el capítulo I que la factorización única en un anillo puede tener muchas consecuencias sobre los números enteros. Kummer investigó la factorización única en los anillos de enteros ciclotómicos de orden primo en relación con el último teorema de Fermat, y su trabajo le llevó a un descubrimiento importantísimo. En primer lugar observó que todo primo ciclotómico debía dividir a un primo racional, por lo que la factorización única se reducía a probar que todo primo racional se descompone en producto de primos, y se dedicó a buscar factorizaciones explícitas en casos concretos para ratificar o refutar la conjetura sobre la unicidad. Para cada primo racional, Kummer encontró argumentos que le permitían predecir en cuántos primos ciclotómicos debía factorizar y con qué multiplicidad y, para cada uno de los factores, encontró a su vez criterios explícitos que le determinaban a qué enteros ciclotómicos debía dividir. Sólo le faltaba encontrar los primos mismos. Con la ayuda de estos criterios le fue relativamente fácil encontrarlos hasta que se enfrentó con la factorización del 43 en el anillo de enteros ciclotómicos correspondientes a $p = 23$. Para este caso probó que la existencia de los factores primos que su teoría predecía conducía a una contradicción. Sin embargo, en el tiempo que tardó en encontrar este ejemplo de factorización no única, su teoría había mostrado tal grado de coherencia y de capacidad de predicción que Kummer confió más en sus razonamientos que en la evidencia a la que había llegado. Reforzando sus razonamientos para no basarse en la hipotética factorización única, demostró que su teoría sobre factores primos era consistente con independencia de que los primos en cuestión existieran o no, es decir, que podía asignar a cada entero ciclotómico una descomposición en factores primos que satisfacía las propiedades formales que se cumplen en todo dominio de factorización única, aunque a veces, tales factores resultaran ser, en sus propios términos, 'factores ideales'. Más tarde, Dedekind simplificó la teoría de divisores ideales de Kummer sustituyendo la construcción formal axiomática por una construcción algebraica, en la que cada divisor ideal era identificado con el conjunto de todos sus múltiplos 'reales'. A su vez estos conjuntos de múltiplos podían ser determinados mediante unas propiedades muy simples: las que definen los ideales en el sentido moderno de la palabra. El

enfoque de Dedekind tenía la ventaja de que se podía aplicar sin ningún cambio al orden maximal de cualquier cuerpo numérico. Comenzamos el capítulo con una exposición de la teoría de Dedekind en términos del álgebra abstracta.

3.1 Dominios de Dedekind

Recordemos que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de un anillo D, su producto es

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} p_i q_i \;\middle|\; n \in \mathbb{N} \text{ y } p_i \in \mathfrak{a}, q_i \in \mathfrak{b} \text{ para } i = 1, \ldots, n \right\}. \tag{3.1}$$

En otras palabras, $\mathfrak{ab}$ es el menor ideal que contiene a todos los productos ab tales que $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$. Como $\mathfrak{a}$ y $\mathfrak{b}$ son ideales, estos productos están contenidos en ambos, luego se cumple que $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.

Definición 3.1 Un dominio íntegro D es un *dominio de Dedekind* si todo ideal propio de D (o sea, distinto de 0 y D) se descompone de forma única salvo el orden en producto de ideales primos.

Vamos a probar que la factorización ideal es formalmente análoga a la factorización real de los dominios de factorización única. Sin embargo tenemos un obstáculo justo al principio, y es que hay un hecho obvio en todo dominio íntegro cuyo análogo ideal no es evidente: los elementos no nulos son simplificables. Para probar que los ideales no nulos son simplificables demostraremos que el conjunto de los ideales de un dominio de Dedekind se puede sumergir en un grupo, con lo que para simplificar un ideal en ambos miembros de una igualdad bastará con multiplicar por su inverso en dicho grupo.

Definición 3.2 Sea D un dominio íntegro y K su cuerpo de cocientes. Un *ideal fraccional* de D es un D-submódulo no nulo $\mathfrak{a}$ de K tal que existe un $c \in D$ no nulo de manera que $c\mathfrak{a} \subset D$ (donde $c\mathfrak{a} = \{ca \mid a \in \mathfrak{a}\}$).

Si $\mathfrak{a}$ es un ideal fraccional de D, entonces $c\mathfrak{a}$ es D-submódulo de K contenido en D, luego es un D-submódulo de D, o también, $\mathfrak{b} = c\mathfrak{a}$ es un ideal no nulo de D y $\mathfrak{a} = c^{-1}\mathfrak{b}$.

El recíproco se prueba igualmente, luego, en definitiva, los ideales fraccionales de D son los conjuntos de la forma $c^{-1}\mathfrak{b}$, donde $\mathfrak{b}$ es un ideal no nulo de D y $c \in D$ es un elemento no nulo.

Tomando $c = 1$ deducimos que todos los ideales no nulos de D son ideales fraccionales. Recíprocamente, un ideal fraccional $\mathfrak{a}$ es un ideal si y sólo si $\mathfrak{a} \subset D$ (por la propia definición).

Podemos definir el producto de dos ideales fraccionales por la misma fórmula (3.1) que para ideales. Es fácil comprobar que efectivamente el producto de ideales fraccionales es un ideal fraccional, así como que cumple la propiedad asociativa.

Si $c \in K$ es no nulo, llamaremos ideal fraccional *principal* generado por c al ideal fraccional $(c) = cD$. Es fácil ver que $(c)\mathfrak{a} = c\mathfrak{a}$. En particular $(c)(d) = (cd)$.

Llamaremos $1 = (1) = D$. Es claro que $\mathfrak{a}\,1 = \mathfrak{a}$ para todo ideal fraccional $\mathfrak{a}$.

Diremos que un ideal fraccional $\mathfrak{a}$ es *inversible* si existe otro ideal fraccional $\mathfrak{b}$ tal que $\mathfrak{ab} = 1$. Es claro que si existe tal $\mathfrak{b}$ entonces es único, y lo representaremos por $\mathfrak{a}^{-1}$.

Todo ideal fraccional principal es inversible, pues $(c)^{-1} = (c^{-1})$.

Antes hemos visto que todo ideal fraccional es de la forma $c^{-1}\mathfrak{b}$, para cierto ideal $\mathfrak{b}$ y cierto $c \in D$. En términos del producto de ideales fraccionales tenemos que todo ideal fraccional es de la forma $(c)^{-1}\mathfrak{b}$, o sea, una fracción de dos ideales. Para probar que los ideales fraccionales de un dominio de Dedekind forman un grupo necesitamos unos hechos sencillos válidos en cualquier dominio íntegro.

Teorema 3.3 *Sea D un dominio íntegro.*

1. *Todo ideal fraccional principal de D es inversible.*
2. *Un producto de ideales no nulos de D es inversible si y sólo si lo es cada factor.*
3. *Si un ideal inversible de D factoriza como producto de ideales primos, entonces la descomposición es única salvo el orden.*

DEMOSTRACIÓN: 1) Ya hemos comentado que $(c)^{-1} = (c^{-1})$.

2) Es obvio que si cada factor es inversible el producto también lo es (su inverso es el producto de los inversos). Si el producto es inversible entonces el inverso de un factor es el inverso del producto multiplicado por los factores restantes.

3) Supongamos que un mismo ideal no nulo se expresa de dos formas

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

como producto de ideales primos (necesariamente no nulos) . Podemos suponer que $r \leq s$.

Tomamos un factor (digamos $\mathfrak{p}_1$) que no contenga estrictamente a ninguno de los restantes. Por definición de ideal primo, y puesto que $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1$, ha de existir un índice i de modo que $\mathfrak{q}_i \subset \mathfrak{p}_1$. Reordenando podemos suponer que $\mathfrak{q}_1 \subset \mathfrak{p}_1$. Igualmente ha de existir un índice j tal que $\mathfrak{p}_j \subset \mathfrak{q}_1 \subset \mathfrak{p}_1$. Por la elección de $\mathfrak{p}_1$ ha de ser $\mathfrak{p}_j = \mathfrak{q}_1 = \mathfrak{p}_1$. Tomando inversos podemos eliminarlos de la factorización, hasta llegar a que $D = \mathfrak{q}_{s-r} \cdots \mathfrak{q}_s \subset \mathfrak{q}_s$, lo que contradice la definición de ideal primo a no ser que $r = s$. Es claro que con esto el teorema queda demostrado. ∎

Teorema 3.4 *Si D es un dominio de Dedekind, entonces los ideales fraccionales de D forman un grupo. Además los ideales primos coinciden con los maximales.*

DEMOSTRACIÓN: Basta probar que todo ideal primo (no nulo) tiene un inverso y es maximal, pues entonces todo ideal no nulo será inversible por ser producto de ideales primos (inversibles) y todo ideal fraccional será inversible porque es de la forma $(c)^{-1}\mathfrak{b}$, donde $(c)^{-1}$ es ciertamente inversible y $\mathfrak{b}$ es un ideal, luego inversible también.

Vemos primero que todo ideal primo inversible es maximal. Sea $\mathfrak{p}$ un ideal primo. Hay que demostrar que si $d \in D \setminus \mathfrak{p}$ entonces $\mathfrak{p} + (d) = D$. En caso contrario existen ideales primos tales que $\mathfrak{p}+(d) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ y $\mathfrak{p}+(d^2) = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Es fácil ver que

$$\big(\mathfrak{p} + (d)\big)/\mathfrak{p} = \big(\mathfrak{p}_1/\mathfrak{p}\big) \cdots \big(\mathfrak{p}_r/\mathfrak{p}\big) \quad \text{y} \quad \big(\mathfrak{p} + (d^2)\big)/\mathfrak{p} = \big(\mathfrak{q}_1/\mathfrak{p}\big) \cdots \big(\mathfrak{q}_s/\mathfrak{p}\big).$$

El ideal $\big(\mathfrak{p} + (d)\big)/\mathfrak{p} = \big([d]\big)$ es principal y $D/\mathfrak{p}$ es un dominio íntegro, luego tiene inverso por el teorema anterior, el cual nos da también que todos los ideales primos $\mathfrak{p}_1/\mathfrak{p}$, ... , $\mathfrak{p}_r/\mathfrak{p}$ tienen inverso como ideales de $D/\mathfrak{p}$.

Lo mismo ocurre con $\mathfrak{q}_1/\mathfrak{p}$, ... , $\mathfrak{q}_s/\mathfrak{p}$. Igualamos:

$$\big(\mathfrak{q}_1/\mathfrak{p}\big) \cdots \big(\mathfrak{q}_r/\mathfrak{p}\big) = \big([d^2]\big) = \big([d]\big)^2 = \big(\mathfrak{p}_1/\mathfrak{p}\big)^2 \cdots \big(\mathfrak{p}_s/\mathfrak{p}\big)^2.$$

Otra aplicación del teorema anterior nos da que $s = 2r$ y que, ordenando adecuadamente, $\mathfrak{p}_i/\mathfrak{p} = \mathfrak{q}_{2i}/\mathfrak{p} = \mathfrak{q}_{2i-1}/\mathfrak{p}$. De aquí se sigue que $\mathfrak{p}_i = \mathfrak{q}_{2i} = \mathfrak{q}_{2i-1}$, y de aquí a su vez obtenemos que $\mathfrak{p} + (d^2) = \big(\mathfrak{p} + (d)\big)^2$. Consecuentemente

$$\mathfrak{p} \subset \mathfrak{p} + (d^2) = \big(\mathfrak{p} + (d)\big)^2 \subset \mathfrak{p}^2 + (d).$$

Todo elemento de $\mathfrak{p}$ es, pues, de la forma $c + ad$, con $c \in \mathfrak{p}^2$ y $a \in D$, pero como $\mathfrak{p}$ es primo y $d \notin \mathfrak{p}$, ha de ser $a \in \mathfrak{p}$, lo que prueba que $\mathfrak{p} \subset \mathfrak{p}^2 + \mathfrak{p}(d) \subset \mathfrak{p}$, es decir, $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}(d)$, y como $\mathfrak{p}$ tiene inverso, $1 = \mathfrak{p} + (d)$, contradicción.

Finalmente, si $\mathfrak{p}$ es cualquier ideal primo no nulo, sea $c \in \mathfrak{p}$, $c \neq 0$. Como D es un dominio de Dedekind podemos factorizar $(c) = \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p}$, donde los ideales primos $\mathfrak{p}_i$ son todos inversibles (por el teorema anterior, ya que (c) lo es) y en consecuencia maximales (por lo ya probado). Por definición de ideal primo, algún ideal $\mathfrak{p}_i$ está contenido en $\mathfrak{p}$, luego por maximalidad $\mathfrak{p} = \mathfrak{p}_i$ es maximal y tiene inverso. ∎

Ahora ya podemos trabajar con dominios de Dedekind como si fueran dominios de factorización única.

Definición 3.5 Sea D un dominio de Dedekind. Diremos que un ideal $\mathfrak{b}$ *divide* a un ideal $\mathfrak{a}$ si existe un ideal $\mathfrak{c}$ tal que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Lo representaremos $\mathfrak{b} \mid \mathfrak{a}$. Notar que en tal caso $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$. Claramente $\mathfrak{b} \mid \mathfrak{a}$ si y sólo si $\mathfrak{a}\mathfrak{b}^{-1}$ es un ideal.

Observar que $\mathfrak{b} \mid \mathfrak{a}$ si y sólo si $\mathfrak{a} \subset \mathfrak{b}$. En efecto, si $\mathfrak{b} \mid \mathfrak{a}$ entonces $\mathfrak{a} = \mathfrak{b}\mathfrak{c} \subset \mathfrak{b}$ y si $\mathfrak{a} \subset \mathfrak{b}$ la propia definición de producto nos da que $\mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{b}\mathfrak{b}^{-1} = 1 = D$, luego el ideal fraccional $\mathfrak{a}\mathfrak{b}^{-1}$ es de hecho un ideal y por lo tanto $\mathfrak{b} \mid \mathfrak{a}$.

Así un ideal $\mathfrak{p}$ es primo si y sólo si $\mathfrak{p} \neq 1$ y cuando $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ entonces $\mathfrak{p} \mid \mathfrak{a}$ o $\mathfrak{p} \mid \mathfrak{b}$, es decir, el concepto de ideal primo en un dominio de Dedekind es formalmente análogo al de primo real en un dominio de factorización única.

Similarmente, un ideal $\mathfrak{p}$ es maximal si y solo si $\mathfrak{p} \neq 1$ y cuando $\mathfrak{a} \mid \mathfrak{p}$ entonces $\mathfrak{a} = 1$ o $\mathfrak{a} = \mathfrak{p}$, es decir, el concepto de ideal maximal en un dominio de Dedekind es formalmente análogo al de elemento irreducible en un dominio de factorización única (notar que en términos de ideales no hay ni unidades ni asociados). Hemos probado que en un dominio de Dedekind 'maximal' equivale a 'primo', lo cual es análogo al hecho de que en un dominio de factorización única 'irreducible' equivale a 'primo'.

Si $c \in D$ escribiremos $\mathfrak{a} \mid c$ o $c = \mathfrak{ab}$ en lugar de $\mathfrak{a} \mid (c)$ o $(c) = \mathfrak{ab}$. De este modo los divisores ideales pueden dividir a elementos reales. Concretamente, tenemos $\mathfrak{a} \mid c$ si y sólo si $(c) \subset \mathfrak{a}$, si y sólo si $c \in \mathfrak{a}$, es decir, un ideal, como conjunto, es el conjunto de todos sus múltiplos reales. Notar también que $a \mid b$ si y sólo si $(a) \mid (b)$.

La factorización única ideal nos permite hablar de la multiplicidad de un ideal primo en otro ideal (o en un elemento real) exactamente en el mismo sentido que en un dominio de factorización única. Toda familia finita de ideales tiene un máximo común divisor y un mínimo común múltiplo que se pueden calcular del modo usual, aunque en realidad hay una caracterización más simple: Teniendo en cuenta que $\mathfrak{a} \mid \mathfrak{b}$ es lo mismo que $\mathfrak{b} \subset \mathfrak{a}$, resulta que el máximo común divisor de una familia de ideales es el mayor ideal que los contiene, y el mínimo común múltiplo es el mayor ideal contenido en ellos, o sea:

$$\begin{aligned} \operatorname{mcd}(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) &= \mathfrak{a}_1 + \cdots + \mathfrak{a}_r, \\ \operatorname{mcm}(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) &= \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r. \end{aligned}$$

En particular $(a, b) = (a) + (b)$ puede entenderse como el ideal generado por a y b o como el máximo común divisor de (a) y (b). Es equivalente. Podemos hablar de ideales primos entre sí, etc. con las propiedades usuales. Como ilustración de la aritmética ideal vamos a probar el teorema chino del resto:

Teorema 3.6 (Teorema chino del resto) *Sea D un dominio de Dedekind y sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ ideales de D primos entre sí dos a dos. Si $\mathfrak{m} = \mathfrak{m}_1 \cdots \mathfrak{m}_n$ se cumple*

$$D/\mathfrak{m} \cong (D/\mathfrak{m}_1) \times \cdots \times (D/\mathfrak{m}_n)$$

y el isomorfismo viene dado por la aplicación $[\alpha] \mapsto \big([\alpha], \ldots, [\alpha]\big)$.

Demostración: Es claro que la aplicación indicada es un monomorfismo de anillos. Sólo hay que probar que es suprayectiva, es decir, que dados $\alpha_1, \ldots, \alpha_n$ en D existe un $\alpha \in D$ tal que $\alpha \equiv \alpha_i \pmod{\mathfrak{m}_i}$ para $i = 1, \ldots, n$. Llamemos $\mathfrak{m}_i^* = \mathfrak{m}/\mathfrak{m}_i$. Entonces $\mathfrak{m}_i$ y $\mathfrak{m}_i^*$ son primos entre sí, es decir, $\mathfrak{m}_i + \mathfrak{m}_i^* = 1 = D$. Por consiguiente $\alpha_i = \beta_i + \gamma_i$, donde $\beta_i \in \mathfrak{m}_i$ y $\gamma_i \in \mathfrak{m}_i^*$. Equivalentemente, $\gamma_i \equiv \alpha_i \pmod{\mathfrak{m}_i}$ y $\gamma_i \equiv 0 \pmod{\mathfrak{m}_j}$ para $j \neq i$. Es claro que $\alpha = \gamma_1 + \cdots + \gamma_n$ es el buscado. ∎

De aquí deducimos un hecho técnico sobre dominios de Dedekind que es fácil usar inadvertidamente, pues en los dominios de factorización única es trivial.

Teorema 3.7 *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 $\mathfrak{p}_i$. Por el teorema chino del resto 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 $\mathfrak{p}_i$. Por hipótesis $\beta \mid \alpha\delta$, es decir, existe un $\gamma \in D$ tal que $\alpha\delta = \beta\gamma$ ∎

Es fácil encontrar dominios de factorización única que no sean dominios de Dedekind. Por ejemplo $\mathbb{Z}[x]$ no es un dominio de Dedekind ya que (x) es un ideal primo no maximal. Recíprocamente veremos que los órdenes maximales de todos los cuerpos numéricos son dominios de Dedekind y muchos de ellos no tienen factorización única. Por lo tanto la divisibilidad ideal no es una generalización de la real, sino que ambas son paralelas. Las dos pueden darse simultáneamente. Esto ocurre exactamente en los dominios de ideales principales:

Teorema 3.8 *Un dominio íntegro D es un dominio de ideales principales si y sólo si es un dominio de Dedekind y un dominio de factorización única.*

DEMOSTRACIÓN: Es sabido que si D es dominio de ideales principales entonces tiene factorización única, y todo ideal propio de D es de la forma (c), donde c no es 0 ni una unidad. Entonces c se descompone en producto de primos $c = p_1 \cdots p_n$, con lo que $(c) = (p_1) \cdots (p_n)$ también es producto de ideales primos. Recíprocamente, una descomposición de (c) en ideales primos da lugar a una factorización de c, de donde se sigue la unicidad.

Si D es a la vez un dominio de Dedekind y un dominio de factorización única entonces dado un ideal primo $\mathfrak{p}$ tomamos un $c \in \mathfrak{p}$ no nulo y lo factorizamos $c = p_1 \cdots p_n$ en producto de primos. Tenemos que $\mathfrak{p} \mid c$, luego $\mathfrak{p} \mid p_i$ para algún i, luego $(p_i) \subset \mathfrak{p}$ y, como los ideales primos son maximales, $\mathfrak{p} = (p_i)$ es principal, y todo ideal propio de D es principal por ser producto de ideales primos principales. ∎

El concepto de dominio de factorización única es muy útil en cuanto que proporciona un gran control sobre los anillos que tienen esta propiedad, pero está el inconveniente de que no es fácil determinar cuándo se da el caso. En cambio, el concepto de dominio de Dedekind admite una caracterización algebraica muy fácil de verificar en la práctica. Veámosla.

Teorema 3.9 *(Teorema de Dedekind) Sea D un dominio íntegro y K su cuerpo de cocientes. Entonces D es un dominio de Dedekind si y sólo si cumple las tres propiedades siguientes:*

1. *D es noetheriano.*
2. *Los ideales primos no nulos de D son maximales.*

3. *Si $a \in K$ es raíz de un polinomio mónico con coeficientes en D, entonces $a \in D$.*

DEMOSTRACIÓN: Todo dominio de Dedekind es noetheriano, pues una cadena de ideales estrictamente creciente significaría una cadena decreciente de divisores, lo cual es imposible. La propiedad 2) está probada en el teorema 3.4. Es interesante notar que la prueba de 3) vale indistintamente para dominios de Dedekind o para dominios de factorización única. En efecto:

Sea $c = \frac{a}{b}$, con $a, b \in D$. Si $c \notin D$ entonces $b \nmid a$, luego existe un primo $\mathfrak{p}$ (ideal o real) tal que el exponente de $\mathfrak{p}$ en a sea estrictamente menor que en b. Sea $p(x) = \sum_{i=0}^{n} d_i x^i$, donde $d_n = 1$. Entonces

$$\frac{a^n}{b^n} + d_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + d_1\frac{a}{b} + d_0 = 0.$$

Multiplicando por b^n queda:

$$a^n = -d_{n-1}ba^{n-1} - \cdots - d_1 b^{n-1}a - d_0 b.$$

Ahora bien, el exponente de $\mathfrak{p}$ en el miembro izquierdo es exactamente n veces el exponente en a, mientras que en el miembro derecho es estrictamente mayor, con lo que tenemos una contradicción.

Supongamos ahora que un dominio íntegro D cumple las tres propiedades del enunciado y veamos que es un dominio de Dedekind. Dividimos la prueba en varios pasos.

(i) *Sea $\mathfrak{a} \neq 0$ un ideal de D. Entonces existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ de manera que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}$.*

En caso contrario existe un ideal $\mathfrak{a}$ tal que no existen ideales primos en las condiciones pedidas y que es maximal entre los ideales para los que esto ocurre.

En particular $\mathfrak{a}$ no puede ser primo, o cumpliría (i) trivialmente. Tampoco puede ser que $\mathfrak{a} = D$. Por lo tanto existen dos ideales $\mathfrak{b}$ y $\mathfrak{c}$ tales que $\mathfrak{bc} \subset \mathfrak{a}$, pero no $\mathfrak{b} \subset \mathfrak{a}$ o $\mathfrak{c} \subset \mathfrak{a}$.

Por la maximalidad de $\mathfrak{a}$, existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ y $\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ tales que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subset \mathfrak{a} + \mathfrak{b}, \qquad \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \subset \mathfrak{a} + \mathfrak{c},$$

de donde $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subset \mathfrak{aa} + \mathfrak{ab} + \mathfrak{ac} + \mathfrak{bc} \subset \mathfrak{a}$, contradicción.

(ii) *Si $\mathfrak{a}$ es un ideal no nulo de D, llamaremos $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset D\}$.*

Es claro que $\mathfrak{a}^{-1}$ es un D-submódulo de K, y para cualquier $c \in \mathfrak{a}$ no nulo se cumple que $c\mathfrak{a}^{-1} \subset D$, luego $\mathfrak{a}^{-1}$ es un ideal fraccional de D.

También es inmediato que $D \subset \mathfrak{a}^{-1}$, luego $\mathfrak{a} = \mathfrak{a}D \subset \mathfrak{aa}^{-1}$.

De la definición de $\mathfrak{a}^{-1}$ se sigue que $\mathfrak{aa}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subset D$. Esto significa que el ideal fraccional $\mathfrak{a}^{-1}\mathfrak{a}$ es de hecho un ideal de D.

Notar también que si $\mathfrak{a} \subset \mathfrak{b}$ son dos ideales de D, entonces $D \subset \mathfrak{b}^{-1} \subset \mathfrak{a}^{-1}$.

(iii) *Si $\mathfrak{a}$ es un ideal propio, entonces $D \subsetneq \mathfrak{a}^{-1}$.*

Sea $\mathfrak{p}$ un ideal maximal de D tal que $\mathfrak{a} \subset \mathfrak{p}$. Entonces $\mathfrak{p}^{-1} \subset \mathfrak{a}^{-1}$. Basta probar que $\mathfrak{p}^{-1}$ contiene estrictamente a D. Sea $a \in \mathfrak{p}$ no nulo. Por (i), sea r el menor natural tal que existen ideales primos para los que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)$. Como $(a) \subset \mathfrak{p}$ y $\mathfrak{p}$ es primo, existe un índice i tal que $\mathfrak{p}_i \subset \mathfrak{p}$. Reordenando podemos suponer que $\mathfrak{p}_1 \subset \mathfrak{p}$. Como $\mathfrak{p}_1$ es maximal ha de ser $\mathfrak{p}_1 = \mathfrak{p}$, y por la minimalidad de r tenemos que $\mathfrak{p}_2 \cdots \mathfrak{p}_r$ no está contenido en (a). Tomamos, pues, un elemento $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$.

Claramente $b\mathfrak{p} \subset (a)$, luego $ba^{-1}\mathfrak{p} \subset a^{-1}(a) = D$ y $ba^{-1} \in \mathfrak{p}^{-1}$, pero por otra parte $b \notin (a) = aD$, luego $ba^{-1} \notin D$. Así pues, $\mathfrak{p}^{-1} \neq D$.

(iv) *Si $\mathfrak{a}$ es un ideal no nulo de D y S es un subconjunto de K tal que $\mathfrak{a}S \subset \mathfrak{a}$, entonces $S \subset D$.*

Sea $s \in S$. Como D es noetheriano tenemos que $\mathfrak{a} = (a_1, \ldots, a_m)$ para ciertos $a_1, \ldots, a_m \in D$. Por hipótesis $a_i s \in \mathfrak{a}$ para $i = 1, \ldots, m$, luego existen elementos $b_{ij} \in D$ de manera que

$$a_i s = \sum_{j=1}^{m} b_{ij} a_j \qquad \text{para } i = 1, \ldots, m.$$

Esto puede expresarse matricialmente mediante la ecuación $s(a_j)^t = B(a_j)^t$, donde llamamos $B = (b_{ij})$. Equivalentemente, $(B - sI_m)(a_j)^t = 0$. Por consiguiente la matriz $B - sI_m$ no puede ser regular, pues entonces multiplicando por su inversa concluiríamos que $(a_j) = 0$, lo cual es imposible. Por lo tanto $|B - sI_m| = 0$ y el polinomio $p(x) = |B - xI_m| \in D[x]$ es mónico, no nulo y tiene por raíz a s. Por la hipótesis 3) tenemos que $s \in D$.

(v) *Si $\mathfrak{p}$ es un ideal maximal de D, entonces $\mathfrak{p}\mathfrak{p}^{-1} = D$.*

Por (ii) sabemos que $\mathfrak{p}\mathfrak{p}^{-1}$ es un ideal de D tal que $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset D$. Puesto que $\mathfrak{p}$ es maximal, ha de ser $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ o bien $\mathfrak{p}\mathfrak{p}^{-1} = D$. Si se diera el primer caso, por (iv) tendríamos que $\mathfrak{p}^{-1} \subset D$, lo que contradice a (iii).

(vi) *Si $\mathfrak{a} \neq 0$ es un ideal, entonces $\mathfrak{a}\mathfrak{a}^{-1} = D$.*

Supongamos lo contrario. Como D es noetheriano existe un ideal $\mathfrak{a}$ maximal entre los que incumplen (vi). Obviamente $\mathfrak{a} \neq D$. Sea $\mathfrak{p}$ un ideal maximal tal que $\mathfrak{a} \subset \mathfrak{p}$.

Por (ii) $D \subset \mathfrak{p}^{-1} \subset \mathfrak{a}^{-1}$, luego $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset D$. En particular el ideal fraccional $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal de D. No puede ocurrir que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, pues entonces (iv) implicaría que $\mathfrak{p}^{-1} \subset D$ en contradicción con (iii). Así pues, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, luego la maximalidad de $\mathfrak{a}$ implica que $\mathfrak{a}\mathfrak{p}^{-1}$ cumple (vi), es decir, $\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = D$. Por definición de $\mathfrak{a}^{-1}$ esto significa que $\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subset \mathfrak{a}^{-1}$. Por consiguiente $D = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset D$, de donde $\mathfrak{a}\mathfrak{a}^{-1} = D$, en contradicción con nuestra hipótesis.

(vii) *Todo ideal propio de D es producto de ideales primos.*

En caso contrario sea $\mathfrak{a}$ un ideal propio maximal entre los que no pueden expresarse como producto de ideales primos. En particular $\mathfrak{a}$ no es primo. Sea $\mathfrak{p}$ un ideal maximal tal que $\mathfrak{a} \subset \mathfrak{p}$. Como en (vi) concluimos que $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset D$ y de nuevo por (iv) y (iii), la primera inclusión es estricta.

Por la maximalidad de $\mathfrak{a}$ tenemos que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ para ciertos ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Por lo tanto $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, en contra de la elección de $\mathfrak{a}$.

(viii) *La descomposición de un ideal en primos es única salvo el orden.*

Supongamos que un mismo ideal propio se expresa de dos formas

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

como producto de ideales primos (necesariamente no nulos) . Podemos suponer que $r \leq s$.

Entonces, puesto que $\mathfrak{p}_1$ es primo y $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1$, ha de existir un índice i tal que $\mathfrak{q}_i \subset \mathfrak{p}_1$. Reordenando podemos suponer que $\mathfrak{q}_1 \subset \mathfrak{p}_1$ y, por maximalidad, de hecho $\mathfrak{q}_1 = \mathfrak{p}_1$. Multiplicando por el inverso tenemos $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Repitiendo el proceso llegamos a que $\mathfrak{p}_i = \mathfrak{q}_i$ para $i = 1, \ldots, r$ y (si $r < s$) a que $D = \mathfrak{q}_{s-r} \cdots \mathfrak{q}_s$, pero entonces $D \subset \mathfrak{q}_s$, lo cual es imposible. Por lo tanto ha de ser $r = s$. ∎

Observar que la prueba del teorema anterior nos ha dado una expresión explícita para el inverso de un ideal en un dominio de Dedekind:

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

Terminamos nuestro estudio de los dominios de Dedekind en general con un resultado técnico que en ocasiones es útil. Si $\mathfrak{a}$ es un ideal no principal de un dominio de Dedekind, entonces ningún múltiplo real de $\mathfrak{a}$ es exactamente igual a $\mathfrak{a}$, es decir, para cualquier $\alpha \in \mathfrak{a}$ se cumple que α divide estrictamente a $\mathfrak{a}$ o, lo que es lo mismo, que $\alpha\mathfrak{a}^{-1} \neq 1$. Vamos a probar que α puede tomarse de modo que en este 'exceso de divisores' no aparezca un conjunto de primos prefijado.

Teorema 3.10 *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 $\alpha \notin \mathfrak{a}\mathfrak{p}$ 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 $\alpha \in \mathfrak{a} - \mathfrak{a}\mathfrak{p}_1$. Para $r > 1$ sea $\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_i^{-1}\mathfrak{b}$. Si $\mathfrak{a}\mathfrak{p}_i \subset \mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_i^{-1}\mathfrak{b}$ 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 $\alpha_i \in \mathfrak{a}_i\mathfrak{p}_i$, en contradicción con la elección que hemos hecho. ∎

Una aplicación de este resultado nos permite probar que todo ideal de un dominio de Dedekind está generado por a lo sumo dos elementos.

Teorema 3.11 *Sea D un dominio de Dedekind y $\mathfrak{a}$ un ideal no nulo de D. 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 $\mathfrak{a} = (\alpha) + (\beta) = (\alpha, \beta)$. ∎

3.2 Divisibilidad ideal en órdenes numéricos

El teorema de Dedekind probado en la sección anterior nos permite probar fácilmente que los órdenes maximales de los cuerpos numéricos tienen factorización única ideal. La única propiedad que en estos momentos no es evidente es la tercera condición. La probamos en un teorema aparte porque tiene interés por sí misma.

Teorema 3.12 *Si $c \in \mathbb{A}$ es raíz de un polinomio mónico $p(x) \in \mathbb{E}[x]$, entonces $c \in \mathbb{E}$.*

Demostración: Sea $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, donde cada $a_i \in \mathbb{E}$.

Sea $B = \mathbb{Z}[a_0, \ldots, a_{n-1}]$. Entonces B es un submódulo del orden maximal de $\mathbb{Q}(a_0, \ldots, a_{n-1})$, luego es un $\mathbb{Z}$-módulo finitamente generado. Digamos que $B = \langle v_1, \ldots, v_r\rangle$. El mismo argumento empleado en el teorema 2.3 prueba ahora que $B[c] = \langle 1, c, \ldots, c^{n-1}\rangle_B$ (como B-módulo).

Sea N el $\mathbb{Z}$-módulo generado por los elementos $v_i \cdot c^k$, donde $1 \le i \le r$, $0 \le k \le n-1$.

Así, un elemento de $B[c]$ es una combinación lineal con coeficientes en B de los c^k y cada coeficiente es una combinación lineal con coeficientes enteros de los v_i.

Por lo tanto $B \subset N$ y es, en consecuencia, un $\mathbb{Z}$-módulo finitamente generado. Por el teorema 2.3 concluimos que c es un entero algebraico. ∎

En particular, si K es un cuerpo numérico, $\mathcal{O}$ es su orden maximal y $\alpha \in K$ es raíz de un polinomio mónico de $\mathcal{O}[x]$, entonces α es entero, luego $\alpha \in \mathcal{O}$. Ahora es fácil probar:

Teorema 3.13 *Si $\mathcal{O}$ es el orden maximal de un cuerpo numérico K, entonces $\mathcal{O}$ es un dominio de Dedekind.*

Demostración: Acabamos de probar que $\mathcal{O}$ cumple la propiedad 3) del teorema de Dedekind. Los ideales no nulos de $\mathcal{O}$ son módulos completos (teorema 2.17. Por lo tanto son finitamente generados (como $\mathbb{Z}$-módulos, luego también como ideales). Esto significa que $\mathcal{O}$ es noetheriano y así tenemos 1).

Por otra parte, los ideales tienen cocientes finitos (por 2.33, notar que su anillo de coeficientes es necesariamente $\mathcal{O}$), y los dominios íntegros finitos son cuerpos, luego los ideales primos son maximales (propiedad 2). ∎

Ejercicio: Probar que un orden de un cuerpo numérico distinto del orden maximal no puede tener factorización única, sea real o ideal.

Es costumbre hablar de ideales, unidades, etc. de un cuerpo numérico K refiriéndose a los conceptos correspondientes de su orden maximal (todos estos conceptos serían triviales aplicados a K, por lo que no hay confusión posible). En estos términos, los ideales fraccionales de K son simplemente los módulos completos cuyo anillo de coeficientes es $\mathcal{O}_K$. En el capítulo anterior definimos una norma sobre estos ideales, y en éste hemos definido un producto. Vamos a probar que la norma conserva los productos. Esto nos permitirá usar la norma en el estudio de la divisibilidad ideal del mismo modo en que empleamos la norma del cuerpo en el estudio de la divisibilidad real.

Teorema 3.14 *Si $\mathfrak{a}$, $\mathfrak{b}$ son ideales fraccionales de un cuerpo numérico K, entonces* $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$.

Demostración: Todo ideal fraccional es de la forma $\mathfrak{a} = \alpha^{-1}\mathfrak{b}$, donde $\alpha \in \mathcal{O}_K$ y $\mathfrak{b}$ es un ideal. Por el teorema 2.34 tenemos que $\mathrm{N}(\mathfrak{a}) = |\,\mathrm{N}(\alpha^{-1})|\,\mathrm{N}(\mathfrak{b})$, luego basta probar que la norma es multiplicativa sobre ideales no nulos.

Por la unicidad de la factorización en primos e inducción sobre el número de factores, basta probar que $\mathrm{N}(\mathfrak{ap}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{p})$ cuando $\mathfrak{p}$ es un ideal primo (el caso en que uno de los factores es 1 es obvio).

Consideremos los grupos abelianos finitos $\mathfrak{a}/\mathfrak{ap} \le \mathcal{O}_K/\mathfrak{ap}$. El tercer teorema de isomorfía implica que $|\mathcal{O}_K/\mathfrak{ap}| = |\mathcal{O}_K/\mathfrak{a}|\,|\mathfrak{a}/\mathfrak{ap}|$, o sea, $\mathrm{N}(\mathfrak{ap}) = \mathrm{N}(\mathfrak{a})\,|\mathfrak{a}/\mathfrak{ap}|$. Basta probar que $|\mathfrak{a}/\mathfrak{ap}| = |\mathcal{O}_K/\mathfrak{p}|$. Notemos que por la factorización única $\mathfrak{ap}$ no puede ser igual a $\mathfrak{p}$, luego $\mathfrak{ap} \subsetneq \mathfrak{a}$, es decir, $|\mathfrak{a}/\mathfrak{ap}| > 1$.

Por el mismo motivo no pueden existir ideales $\mathfrak{b}$ de $\mathcal{O}_K$ tales que $\mathfrak{ap} \subsetneq \mathfrak{b} \subsetneq \mathfrak{a}$, pues entonces $\mathfrak{a} \mid \mathfrak{b} \mid \mathfrak{ap}$, luego la descomposición en factores de $\mathfrak{b}$ debe contener a la de $\mathfrak{a}$ y estar contenida en la de $\mathfrak{ap}$, luego $\mathfrak{b}$ será igual a $\mathfrak{ap}$ o a $\mathfrak{a}$ según que la multiplicidad de $\mathfrak{p}$ en $\mathfrak{b}$ sea la de $\mathfrak{ap}$ o la de $\mathfrak{a}$.

Por lo tanto, si $a \in \mathfrak{a} \setminus \mathfrak{ap}$, entonces $\mathfrak{a} = \mathfrak{ap} + (a)$ y a su vez esto implica que la aplicación $f : \mathcal{O}_K \longrightarrow \mathfrak{a}/\mathfrak{ap}$ dada por $f(x) = [xa]$ es un epimorfismo de $\mathcal{O}_K$-módulos con la propiedad de que $\mathfrak{p} \subset \mathrm{N}(f)$. Ahora, $\mathrm{N}(f)$ es un $\mathcal{O}_K$-submódulo de $\mathcal{O}_K$, o sea, un ideal. Como $\mathfrak{p}$ es maximal, ha de ser $\mathrm{N}(f) = \mathfrak{p}$ o $\mathrm{N}(f) = \mathcal{O}_K$, pero el segundo caso implicaría que $\mathfrak{a}/\mathfrak{ap} \cong \mathcal{O}_K/\mathcal{O}_K$, con lo que $|\mathfrak{a}/\mathfrak{ap}| = 1$, contradicción. Lo correcto es $\mathfrak{a}/\mathfrak{ap} \cong \mathcal{O}_K/\mathfrak{p}$, y así $|\mathcal{O}_K/\mathfrak{p}| = |\mathfrak{a}/\mathfrak{ap}|$. ∎

He aquí los hechos más importantes en relación con normas y divisibilidad:

Teorema 3.15 *Sean $\mathfrak{a}$, $\mathfrak{b}$ ideales de un cuerpo numérico K.*

1. *Si $\mathfrak{a} \mid \mathfrak{b}$ entonces $\mathrm{N}(\mathfrak{a}) \mid \mathrm{N}(\mathfrak{b})$.*
2. *$\mathfrak{a} \mid \mathrm{N}(\mathfrak{a})$. En particular si $\mathrm{N}(\mathfrak{a}) = 1$ entonces $\mathfrak{a} = 1$.*

3. *Si* $\mathrm{N}(\mathfrak{a})$ *es un número primo, entonces* $\mathfrak{a}$ *es un ideal primo.*

4. *Si* $\mathfrak{a}$ *es un ideal primo no nulo, entonces* $\mathfrak{a}$ *divide a un único primo racional* p *y se cumple que* $\mathrm{N}(\mathfrak{a}) = p^m$ *para cierto natural* m *menor o igual que el grado de* K*.*

5. *Si* $\alpha \in \mathcal{O}_K$ *entonces* $\mathrm{N}\big((\alpha)\big) = |\,\mathrm{N}(\alpha)|$*.*

6. *Sólo un número finito de ideales pueden tener una misma norma.*

Demostración: 1) es consecuencia inmediata del teorema 3.14.

2) Por definición, $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. El anillo $\mathcal{O}/\mathfrak{a}$ es en particular un grupo finito (con la suma) y el orden de cualquier elemento es divisible entre $\mathrm{N}(\mathfrak{a})$. Por lo tanto $\mathrm{N}(\mathfrak{a})[1] = [0]$, lo que equivale a que $\mathrm{N}(\mathfrak{a}) \in \mathfrak{a}$.

3) Un ideal de norma prima no puede descomponerse en primos (por 1 y 2), luego ha de ser primo.

4) Como $\mathfrak{a} \mid \mathrm{N}(\mathfrak{a})$ y $\mathfrak{a}$ es primo, $\mathfrak{a}$ debe dividir a uno de los primos racionales que dividen a $\mathrm{N}(\mathfrak{a})$. Digamos que $\mathfrak{a} \mid p$. Entonces $\mathrm{N}(\mathfrak{a}) \mid \mathrm{N}(p) = p^n$, donde n es el grado de K. Consecuentemente, $\mathrm{N}(\mathfrak{a}) = p^m$ para un cierto $m \leq n$.

Si $\mathfrak{a}$ dividiera a otro primo q, el mismo argumento nos daría que $\mathrm{N}(\mathfrak{a})$ habría de ser potencia de q, lo cual es imposible salvo si $q = p$.

5) Por el teorema 2.34.

6) Por 2), los ideales de norma m dividen a m y el conjunto de divisores de m es finito. ∎

Este teorema contiene información relevante a la hora de estudiar los ideales propios de un anillo de enteros. El apartado 4) nos dice que todo ideal primo divide a un primo racional, por lo que factorizando los primos racionales se encuentran todos los ideales primos. La unicidad de 4) implica que los primos racionales (no asociados) son primos entre sí, de donde se sigue la existencia de infinitos ideales primos en cada anillo de enteros (al menos uno distinto para cada primo racional). El apartado 5) muestra que la norma ideal extiende consistentemente a la norma real.

Ejemplo Consideremos de nuevo el caso de factorización no única (1.2) que encontramos en el anillo $\mathbb{Z}\big[\sqrt{-5}\,\big]$:

$$6 = 2 \cdot 3 = \big(1 + \sqrt{-5}\,\big)\big(1 + \sqrt{-5}\,\big).$$

Los cuatro factores son irreducibles, pero no son primos. Como $\mathrm{N}(2) = 4$, el ideal (2) sólo puede descomponerse en producto de dos ideales primos de norma 2, o sea, $2 = \mathfrak{p}_1\mathfrak{p}_2$. Igualmente 3 ha de ser producto de dos ideales de norma 3, digamos $3 = \mathfrak{q}\mathfrak{r}$. Por otra parte, los factores de la derecha tienen los dos norma 6, luego han de descomponerse en producto de un ideal de norma 2 por otro de

norma 3. La unicidad de la factorización obliga a que sea $\big(1+\sqrt{-5}\,\big)=\mathfrak{p}_1\mathfrak{q}$ y $\big(1-\sqrt{-5}\,\big)=\mathfrak{p}_2\mathfrak{r}$, de modo que la factorización única de 6 es

$$6=2\cdot 3=(\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{q}\mathfrak{r})=(\mathfrak{p}_1\mathfrak{q})(\mathfrak{p}_2\mathfrak{r})=\big(1+\sqrt{-5}\,\big)\big(1-\sqrt{-5}\,\big).$$

Más aún, evidentemente $\mathfrak{p}_1$ es el máximo común divisor de 2 y $1+\sqrt{-5}$, es decir, que $\mathfrak{p}_1=\big(2,1+\sqrt{-5}\,\big)$.

Similarmente $\mathfrak{p}_2=\big(2,1-\sqrt{-5}\,\big)$, $\mathfrak{q}=\big(3,1+\sqrt{-5}\,\big)$ y $\mathfrak{r}=\big(3,1-\sqrt{-5}\,\big)$.

Finalmente observamos que $\mathfrak{p}_1=\mathfrak{p}_2$, pues $1-\sqrt{-5}=2-\big(1+\sqrt{-5}\,\big)$. Por el contrario $\mathfrak{q}\neq\mathfrak{r}$, pues en otro caso $1=3-\big(1+\sqrt{-5}+1-\sqrt{-5}\,\big)\in\mathfrak{q}$, o sea, $\mathfrak{q}=1$.

Si llamamos $\mathfrak{p}=\mathfrak{p}_1=\mathfrak{p}_2$, la factorización de 6 es, en definitiva, $6=\mathfrak{p}^2\mathfrak{q}\mathfrak{r}$. Los factores son 'ideales' porque no están en el anillo $\mathbb{Z}\big[\sqrt{-5}\,\big]$, pero se comportan como si lo estuviesen. ∎

Veamos ahora cómo encontrar sistemáticamente factorizaciones como la del ejemplo anterior. Nuestro teorema básico es el siguiente.

Teorema 3.16 *Sea $K=\mathbb{Q}(\zeta)$ un cuerpo numérico, donde ζ es entero y p un primo racional tal que $p\nmid \text{índ}\,\zeta$. Sea $g(x)=\text{pol mín}\,\zeta$ 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 $\mathrm{N}(\mathfrak{p}_i)=p^{\text{grad}\,g_i}$.*

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 $\bar{g}_i=\text{pol mín}(\zeta_i,\mathbb{Z}/p\mathbb{Z})$.

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 $k=\text{índ}\,\zeta=\big|\mathcal{O}_K:\mathbb{Z}[\zeta]\big|$. 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 $kx\equiv 1\ (\text{mód}\ p)$. Dado cualquier $\beta\in\mathcal{O}_K$, sea $\gamma=kx\beta$. Entonces $\gamma\in\mathbb{Z}[\zeta]$ y $\gamma\equiv\beta\ (\text{mód}\ \mathfrak{p}_i)$. 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

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

Notar 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.

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

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

donde n es el grado de K. Así pues $\mathrm{N}(\mathfrak{p}_1^{e_1}\cdots p_r^{e_r}) = \mathrm{N}(p)$, 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. En la sección siguiente hallaremos la factorización del 2 para el caso particular del ejemplo de Dedekind.

Ejemplo Volvamos a obtener las factorizaciones de 2 y 3 en el anillo $\mathbb{Z}\big[\sqrt{-5}\,\big]$.

En primer lugar, $\operatorname{pol\,mín}\sqrt{-5} = x^2+5$. Su imagen en el cuerpo $(\mathbb{Z}/2\mathbb{Z})[x]$ es $x^2+1 = (x+1)^2$, luego 2 factoriza como $2 = \big(2, 1+\sqrt{-5}\,\big)^2$.

La imagen en $(\mathbb{Z}/3\mathbb{Z})[x]$ es $x^2+2 = x^2-1 = (x+1)(x-1)$, lo que nos da la factorización $3 = \big(3, 1+\sqrt{-5}\,\big)\big(3, -1+\sqrt{-5}\,\big) = \big(3, 1+\sqrt{-5}\,\big)\big(3, 1-\sqrt{-5}\,\big)$. ∎

El teorema 3.16 puede refinarse cuando se aplica a extensiones de Galois de $\mathbb{Q}$. Ello se debe esencialmente a que los automorfismos obligan a que las factorizaciones presenten un alto grado de simetría. En efecto, ante todo, si K

es una extensión finita de Galois de $\mathbb{Q}$ y $\sigma \in G(K/\mathbb{Q})$, es claro que la imagen $\sigma[\mathfrak{a}]$ de un ideal fraccional cualquiera de K es de nuevo un ideal fraccional, que será un ideal (entero) si y sólo si lo es $\mathfrak{a}$. Así pues, podemos extender a σ a un automorfismo del grupo de los ideales fraccionales de K dado por $\sigma(\mathfrak{a}) = \sigma[\mathfrak{a}]$. Decimos 'extender' porque la acción sobre los ideales es consistente con la acción sobre elementos reales en el sentido de que $\sigma\big((\alpha)\big) = \big(\sigma(\alpha)\big)$, para todo $\alpha \in K$ no nulo.

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

Teorema 3.17 *Sea K una extensión de Galois de grado n sobre $\mathbb{Q}$ y sea p un primo racional. Entonces la factorización de p en K es de la forma*

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e, \tag{3.2}$$

donde los ideales $\mathfrak{p}_i$ son primos distintos, forman una clase de conjugación y todos tienen la misma norma $\mathrm{N}(\mathfrak{p}_i) = p^f$, para un cierto f tal que $efr = n$.

Demostración: Es obvio que si $\mathfrak{p} \mid p$, entonces todo conjugado de $\mathfrak{p}$ cumple lo mismo. Veamos que cualquier otro divisor $\mathfrak{q}$ de p es un conjugado de $\mathfrak{p}$. Supongamos, por reducción al absurdo, que $\sigma(\mathfrak{p}) \neq \mathfrak{q}$ para todo automorfismo σ. Por el teorema chino del resto existe un $\alpha \in \mathcal{O}_K$ tal que

$$\begin{aligned} \alpha &\equiv 0 \ (\text{mód } \mathfrak{q}), \\ \alpha &\equiv 1 \ (\text{mód } \sigma(\mathfrak{p})) \ \text{ para todo } \sigma \in G(K/\mathbb{Q}). \end{aligned}$$

Pero entonces $\mathfrak{q} \mid \alpha \mid \mathrm{N}(\alpha)$, luego $p \mid \mathrm{N}(\alpha)$, luego $\mathfrak{p} \mid \mathrm{N}(\alpha)$ y por consiguiente $\mathfrak{p} \mid \sigma(\alpha)$ para algún $\sigma \in G(K/\mathbb{Q})$, de donde $\sigma^{-1}(\mathfrak{p}) \mid \alpha$, contradicción.

Es claro que el exponente de un primo $\mathfrak{p}$ en la descomposición en primos de p debe ser el mismo que el de todos sus conjugados. Como todos los divisores primos de p son conjugados, de hecho todos tienen el mismo exponente e, luego la factorización es del tipo (3.2). También es obvio que primos conjugados tienen la misma norma, necesariamente potencia de p. La igualdad $n = efr$ se sigue de tomar normas en ambos miembros de (3.2). ∎

En particular, el teorema anterior afirma que dos primos de un cuerpo numérico normal son conjugados si y sólo si dividen al mismo primo racional, si y sólo si tienen la misma norma. Otra consecuencia interesante es el teorema siguiente:

Teorema 3.18 *Sea K una extensión finita de Galois de $\mathbb{Q}$ y $\mathfrak{a}$ un ideal fraccional de K. Entonces*

$$\mathrm{N}(\mathfrak{a}) = \prod_{\sigma} \sigma(\mathfrak{a}), \tag{3.3}$$

donde σ recorre los automorfismos de K.

DEMOSTRACIÓN: Los dos miembros de (3.3) son multiplicativos, luego basta probarlo para un ideal primo $\mathfrak{p}$. Sea $\mathrm{N}(\mathfrak{p}) = p^f$. La factorización de p es de la forma (3.2), digamos que con $\mathfrak{p} = \mathfrak{p}_1$.

Sea $G = G(K/\mathbb{Q})$ y $H = \{\sigma \in G \mid \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\}$. Es claro que H es un subgrupo de G, así como que los automorfismos que envían $\mathfrak{p}_1$ a $\mathfrak{p}_i$ son exactamente los de $H\sigma$, donde σ es un automorfismo fijo que cumpla esta propiedad. Por lo tanto, en el miembro izquierdo de (3.3) (con $\mathfrak{p}$ en lugar de $\mathfrak{a}$) cada conjugado de $\mathfrak{p}$ aparece el mismo número de veces, concretamente, $|H| = n/r = ef$ veces. Así pues,

$$\prod_\sigma \sigma(\mathfrak{p}) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{ef} = p^f = \mathrm{N}(\mathfrak{p}).$$

■

3.3 Ejemplos de factorizaciones ideales

Estudiemos ahora las descomposiciones de los primos racionales en algunos de los cuerpos que venimos estudiando.

Cuerpos cuadráticos Sea $K = \mathbb{Q}\big(\sqrt{d}\big)$ un cuerpo cuadrático. Sabemos que su orden maximal es $\mathbb{Z}[\zeta]$, donde ζ 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 ζ será $x^2 - d$ o bien $x^2 - x + \frac{1-d}{4}$. Según el teorema 3.16, 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 3.16.

Tabla 3.1: Factorización en cuerpos cuadráticos

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

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

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 3.19 *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 $p^n \leq p^r$, o sea, $n \leq \mathrm{o}_m(p)$, y así tenemos la igualdad. ∎

Teorema 3.20 *Sea $K = \mathbb{Q}(\omega)$ el cuerpo ciclotómico de orden m y p un primo racional. Sea $m = p^i m'$, donde $p \nmid m'$. Entonces la factorización de p en K es de la forma* (3.2)*, donde $f = \mathrm{o}_{m'}(p)$, $e = \phi(p^i)$ y $r = \phi(m)/ef$.*

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

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

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

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 de hecho 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 $p = \epsilon(1 - \omega_p)^{\phi(p^i)}$, 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 $e \geq \phi(p^i)$.

Supongamos ahora que $m' \neq 1$. Por el teorema 2.30 $p \nmid \Delta[\omega_{m'}]$, luego en particular $p \nmid \mathrm{índ}\, \omega_{m'}$. Podemos aplicar el teorema 3.16 al orden $\mathbb{Z}[\omega_{m'}]$. El polinomio $x^{m'} - 1$ tiene raíces simples módulo p, luego p se descompondrá en primos distintos. Veamos que si $\mathfrak{p}$ es uno de los divisores de p y $\mathrm{N}(\mathfrak{p}) = p^t$, entonces $t = \mathrm{o}_{m'}(p)$.

Por 3.16 sabemos que t es el grado de uno de los factores irreducibles de $\mathrm{pol\,mín}\, \omega_{m'}$ módulo p, que a su vez es el grado de la extensión ciclotómica p-ésima de $\mathbb{Z}/p\mathbb{Z}$. Según el teorema anterior, t tiene el valor indicado.

Comparando las normas concluimos que p se descompone en $\phi(m')/t$ factores primos distintos de norma p^t.

Sea $\mathcal{O}$ el orden maximal de $\mathbb{Q}(\omega)$, sea $\mathcal{O}_{m'}$ el orden maximal de $\mathbb{Q}(\omega_{m'})$, sea $\mathfrak{P}$ un factor primo de p en $\mathbb{Q}(\omega)$ y $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{m'}$. Es claro que $\mathfrak{p}$ es un divisor primo de p en $\mathcal{O}_{m'}$, así como que la aplicación natural $\mathcal{O}_{m'}/\mathfrak{p} \longrightarrow \mathcal{O}/\mathfrak{P}$ es un monomorfismo de cuerpos. El cardinal del primero es p^t, y el del segundo p^f, luego concluimos que $f \geq \mathrm{o}_{m'}(p)$.

Sea $g = \phi(m')/t$. Veamos que p tiene al menos g factores distintos en $\mathbb{Q}(\omega)$. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ los divisores primos distintos de p en $\mathbb{Q}(\omega_{m'})$. Para cada j sea

$$\pi_j \in \mathfrak{p}_j \setminus \prod_{l \neq j} \mathfrak{p}_l.$$

Entonces $p \mid \mathrm{N}(\pi_j)$ (para la norma de $\mathbb{Q}(\omega_{m'})/\mathbb{Q}$, luego también para la norma de $\mathbb{Q}(\omega)/\mathbb{Q}$). Sea $\mathfrak{P}_j$ un divisor primo de p en $\mathbb{Q}(\omega)$ que divida a π_j. Veamos que estos ideales son distintos dos a dos. En caso contrario uno de ellos, digamos $\mathfrak{P}$ dividiría a dos números π_j y $\pi_{j'}$. Por lo tanto el ideal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{m'}$ contiene a p, π_j, $\pi_{j'}$. Pero entonces $\mathfrak{p}_j = \mathfrak{p} = \mathfrak{p}_{j'}$, contradicción.

Esto prueba que $r \geq \phi(m')/t$. Finalmente observamos que

$$\phi(m) = efr \geq \phi(p^i)\, t\, \phi(m')/t = \phi(m),$$

luego las tres desigualdades han de ser igualdades. ∎

Ejemplo Vamos a considerar el caso $m = 23$ y $p = 47$ en el teorema anterior. Como $p \equiv 1$ (mód m), tenemos que $f = \mathrm{o}_m(p) = 1$, luego 47 factoriza en 22 primos distintos de norma 47. Vamos a probar que en $\mathbb{Z}[\omega]$ no hay elementos de norma ± 47, con lo que los factores primos de 47 serán ideales no principales, y habremos probado que $\mathbb{Z}[\omega]$ no tiene factorización única.

El discriminante del cuerpo es $\Delta = -23^{21}$. Si llamamos $\sigma_1, \ldots, \sigma_{22}$ a los monomorfismos de $\mathbb{Q}(\omega)$, como $\mathbb{Q}(\omega)/\mathbb{Q}$ es normal concluimos que todos los conjugados $\sigma_i(\omega^j)$ están en $\mathbb{Q}(\omega)$, luego $\sqrt{\Delta} = 23^{10}\sqrt{-23} = \det\big(\sigma_i(\omega_j)\big) \in \mathbb{Q}(\omega)$, y de aquí concluimos que $\mathbb{Q}\big(\sqrt{-23}\,\big) \subset \mathbb{Q}(\omega)$.

Si en $\mathbb{Q}(\omega)$ hubiera un entero de norma ± 47, la norma de dicho entero respecto a la extensión $\mathbb{Q}(\omega)/\mathbb{Q}\big(\sqrt{-23}\,\big)$ sería un entero cuadrático de norma ± 47 (necesariamente $+47$). Basta ver, pues, que en $\mathbb{Q}\big(\sqrt{-23}\,\big)$ no hay enteros de norma 47.

Ahora bien, un entero de $\mathbb{Q}\big(\sqrt{-23}\,\big)$ es de la forma $a + b\frac{1+\sqrt{-23}}{2}$, con a, b enteros racionales, y su norma es

$$\begin{aligned} \mathrm{N}\left(a + b\frac{1+\sqrt{-23}}{2}\right) &= \left(\frac{2a+b}{2} + b\frac{\sqrt{-23}}{2}\right)\left(\frac{2a+b}{2} - b\frac{\sqrt{-23}}{2}\right) \\ &= \frac{1}{4}\big((2a-b)^2 + 23b^2\big). \end{aligned}$$

Si hubiera un elemento de norma 47 tendríamos

$$188 = 47 \cdot 4 = (2a - b)^2 + 23b^2,$$

pero 188 no es un cuadrado perfecto, ni $188 - 23 = 165$, ni $188 - 23 \cdot 4 = 96$, luego b no puede tomar los valores $0, \pm 1, \pm 2$, y para valores mayores resulta que $(2a - b)^2 + 23b^2 > 188$. ∎

Éste fue el primer ejemplo de factorización no única en anillos de enteros ciclotómicos que encontró Kummer.

Ejercicio: Probar que todo cuerpo cuadrático está contenido en uno ciclotómico.

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 2.27.

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 3.16 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 $p \equiv -1 \pmod 3$ 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 $p \equiv 1 \pmod 3$ 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 $p \equiv -1 \pmod 3$ el polinomio $x^3 - ab^2$ tiene una única raíz módulo p, luego se descompone en un factor de grado 1 y otro de

Tabla 3.2: Factorización en cuerpos cúbicos puros

Casos		Factorización	e	f
$p \nmid 3ab$	$x^3 \equiv ab^2 \pmod p$ resoluble	$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1
$p \equiv 1 \pmod 3$	$x^3 \equiv ab^2 \pmod p$ no resoluble	$p = p$	1	3
$p \nmid 3ab$	$p \equiv -1 \pmod 3$	$p = \mathfrak{p}_1\mathfrak{p}_2$	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

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 $p \equiv 1 \pmod 3$ hay dos casos, según que la congruencia $x^3 \equiv ab^2 \pmod p$ 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 $x^3 - ab^2 \equiv x^3 \pmod p$, 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 $x^3 - ab^2 \equiv x^3 \pm 1 \equiv (x \pm 1)^3 \pmod 3$, 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 $\operatorname{índ}\theta_0 = |b - a|/9$, luego si $27 \nmid b - a$ podemos usar θ_0. En caso contrario

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

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 2.27 vimos que

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

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,

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

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 $3 = \mathfrak{p}_1\mathfrak{p}_2^2$.

Notar que hemos probado que los cuerpos cúbicos puros no tienen divisores esenciales. La tabla 3.2 resume los resultados que hemos obtenido.

Ejercicio: Sean K_1, K_2 y K_3 los cuerpos definidos en la página 36. Considerar las factorizaciones de 5 y 11 en cada uno de ellos para concluir que se trata efectivamente de tres cuerpos distintos.

El ejemplo de Dedekind Ya hemos comentado que el ejemplo de Dedekind $\mathbb{Q}(\xi)$, donde ξ es una raíz del polinomio $x^3 + x^2 - 2x + 8$, tiene a 2 como divisor esencial, luego el teorema 3.16 no nos permite factorizar el 2. 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 nos faltaba. ∎

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

Teorema 3.21 *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 $p \nmid \text{índ}\,\alpha$. Si $f(x) = \text{pol mín}\,\alpha$ el teorema 3.16 implica que f se descompone en n factores distintos módulo p, lo cual es absurdo, pues los factores habrían de ser lineales y $p < n$. ∎

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

Teorema 3.22 *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: Sabemos que $p = \epsilon(\omega-1)^{p-1}$, donde ϵ es una unidad ciclotómica y $\mathrm{N}(\omega-1) = p$. Ahora tomamos normas respecto a la extensión K/K^*, con lo que $p^2 = \epsilon'\pi^{p-1}$, donde $\epsilon' = \mathrm{N}(\epsilon)$ es una unidad de K^* y $\pi = \mathrm{N}(\omega-1)$ sigue teniendo norma p, luego es primo. En consecuencia $p = \epsilon''\pi^{(p-1)/2}$, y el resultado es claro.

Supongamos ahora que $q \neq p$. En general, sabemos que q factoriza en la forma descrita en el teorema 3.17. Hemos de probar que $e = 1$ y que f es el indicado. Supongamos en primer lugar que $e > 1$. Tomemos un primo $\mathfrak{Q}$ que divida a p en K y sea $\mathfrak{q} = \mathfrak{Q} \cap K^*$. Es claro que $\mathfrak{q}$ es un ideal primo en K^* que divide a q. Sea $\pi \in \mathfrak{q} \setminus \mathfrak{q}^2$ tal que no sea divisible entre ningún otro divisor primo de q (existe por 3.10). Entonces $\pi = \mathfrak{q}\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal primo con q. Sea $\alpha \in \mathfrak{a}^e \setminus (q)$. Entonces $\pi^e \mid q\alpha$ en K^*, luego también en K, pero $\pi \in \mathfrak{q} \subset \mathfrak{Q}$, luego $\mathfrak{Q}^e \mid p\alpha$, y como $p \nmid \mathrm{N}(\alpha)$, ha de ser $\mathfrak{Q}^e \mid p$, lo que contradice a 3.20.

Sean $\mathfrak{Q}$ y $\mathfrak{q}$ como antes. Según el teorema 3.20 sabemos que $\mathrm{N}(\mathfrak{Q}) = q^f$. Sea $\mathrm{N}(\mathfrak{q}) = f'$. Sea $\mathcal{O}$ el anillo de enteros ciclotómicos y $\mathcal{O}'$ el anillo de enteros de K^*. La aplicación $\mathcal{O}'/\mathfrak{q} \longrightarrow \mathcal{O}/\mathfrak{Q}$ dada por $[\alpha] \mapsto [\alpha]$ es claramente un monomorfismo de cuerpos, que nos permite identificar a $\mathcal{O}'/\mathfrak{q}$ con el conjunto de clases de $\mathcal{O}/\mathfrak{Q}$ con un representante en $\mathcal{O}'$, es decir, con un representante real. Por definición de norma de un ideal tenemos que el grado de esta extensión es precisamente f/f'.

Es evidente que $\mathcal{O}/\mathfrak{Q} = \big(\mathcal{O}'/\mathfrak{q}\big)\big([\omega]\big)$, y $[\omega]$ es raíz de un polinomio de grado 2 con coeficientes en $\mathcal{O}'/\mathfrak{q}$ (el polinomio mínimo de ω sobre K' módulo $\mathfrak{q}$), luego el grado de esta extensión de cuerpos de restos es a lo sumo 2. En particular, si f es impar ha de ser $f' = f$. Supongamos ahora que f es par. Bastará probar

que $f \neq f'$, o equivalentemente, que la extensión de cuerpos de restos no es trivial.

El grupo de Galois de $\mathcal{O}/\mathfrak{Q}$ tiene orden f, luego contiene un automorfismo de orden 2, digamos σ. Puesto que $[\omega]$ es raíz del polinomio ciclotómico módulo $\mathfrak{Q}$, ha de ser $\sigma\big([\omega]\big) = [\omega]^r$, para cierto r primo con p. Como tiene orden 2, ha de ser $\omega^{r^2} \equiv \omega$ (mód $\mathfrak{Q}$), luego $\mathfrak{Q} \mid \omega^{r^2} - \omega$ y de aquí que $\mathfrak{Q} \mid \omega^{r^2-1} - 1$. Ahora bien, este número es primo y divide a p salvo que $p \mid r^2 - 1$. Ésta es la única posibilidad, luego $r \equiv \pm 1$ (mód p), y en consecuencia $\sigma\big([\omega]\big) = [\omega]^{\pm 1}$. Como σ tiene orden 2 el signo ha de ser negativo, y en general $\sigma\big([\omega^i]\big) = [\omega^{-i}]$. Si llamamos $\eta_i = \omega^i + \omega^{-i}$ las clases de estos números generan $\mathcal{O}'/\mathfrak{q}$ y todas son fijadas por σ, luego σ es la identidad en $\mathcal{O}'/\mathfrak{q}$ y no en $\mathcal{O}/\mathfrak{Q}$. Los dos cuerpos son distintos. ∎

La demostración de este teorema se simplifica considerablemente en un contexto más adecuado. La hemos incluido aquí porque estos cuerpos nos proporcionarán ejemplos interesantes y éste era el único hecho cuya justificación a nuestro nivel presentaba inconvenientes.

3.4 La función de Euler generalizada

Completamos nuestro estudio de los ideales de los cuerpos numéricos generalizando la función de Euler que nos permite calcular el número de unidades módulo un ideal.

Definición 3.23 Sea K un cuerpo numérico. Llamaremos *función de Euler generalizada* de K a la función que a cada ideal $\mathfrak{a}$ de K le hace corresponder el orden $\Phi(\mathfrak{a})$ del grupo $(\mathcal{O}_K/\mathfrak{a})^*$ de las unidades módulo $\mathfrak{a}$.

Es evidente que $(\mathcal{O}_K/\mathfrak{a})^*$ está formado por las clases de los enteros α que cumplen $\mathfrak{a} + (\alpha) = 1$. El teorema siguiente nos permite calcular fácilmente la función de Euler:

Teorema 3.24 *Sea K un cuerpo numérico.*

1. *si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de K 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 K, entonces $\Phi(\mathfrak{p}^e) = \big(\mathrm{N}(\mathfrak{p}) - 1\big)\,\mathrm{N}\big(\mathfrak{p}\big)^{e-1}$.*

Demostración: 1) es consecuencia inmediata del teorema chino del resto.

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 $(\alpha + \pi^e\beta, \pi) = 1$ si y sólo si $(\alpha, \pi) = 1$.

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. ∎

3.5 Factorización ideal en órdenes no maximales

Los órdenes no maximales de los cuerpos numéricos cumplen las propiedades 1 y 2 del teorema de Dedekind (por los mismos argumentos que los maximales), pero incumplen la 3, lo que impide que tengan factorización única real o ideal. Sin embargo los fallos de la factorización ideal son mínimos y pueden ser 'acotados', como vamos a ver aquí.

Definición 3.25 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 3.26 *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 la propiedad 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 3.27 *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

$$\mathcal{O}'/(\mathcal{O}' \cap \mathfrak{a}) \cong \mathcal{O}/\mathfrak{a}. \tag{3.4}$$

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 $I_\mathfrak{f}(\mathcal{O}')$. Así mismo podemos simplificar ideales no nulos, etc.

No podemos interpretar el isomorfismo (3.4) 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 3.28 *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 (3.4) 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 3.29 *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* 2.24 *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 3.27 y 3.28 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.

3.6 El problema de la factorización única real

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 3.16 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 $\mathrm{o}_7(2) = 3$, el teorema 3.20 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

$$2 = (2, \omega^3+\omega+1)(2, \omega^3+\omega^2+1). \tag{3.5}$$

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. Observar 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 (3.5) 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.

Una forma rápida de resolver estos problemas en casos muy particulares es probar que el orden considerado es un dominio euclídeo. Una posible norma euclídea es el valor absoluto de la norma. La siguiente caracterización resulta útil:

Teorema 3.30 *Sea $\mathcal{O}$ el orden maximal de un cuerpo numérico K. Entonces $\mathcal{O}$ es un dominio euclídeo con norma euclídea $|\mathrm{N}(x)|$ si y sólo si para todo $\alpha \in K$ existe un $\beta \in \mathcal{O}$ tal que $|\mathrm{N}(\alpha-\beta)| < 1$.*

DEMOSTRACIÓN: La norma de un dominio euclídeo ha de cumplir que $|\,\mathrm{N}(\alpha)| \le |\,\mathrm{N}(\alpha\beta)|$, para todo par de enteros no nulos α y β. Esto es evidente.

Por otra parte, dados Δ y δ en $\mathcal{O}$ con $\delta \neq 0$, existe un $\beta \in \mathcal{O}$ tal que $\rho = \frac{\Delta}{\delta} - \beta$ tiene norma menor que 1, luego $\Delta = \delta\beta + \delta\rho$ y $|\,\mathrm{N}(\delta\rho)| < |\,\mathrm{N}(\delta)|$, tal y como exige el algoritmo euclídeo. El recíproco es similar. ∎

Una muestra de la limitada aplicación de este hecho es el teorema siguiente:

Teorema 3.31 *Si $\mathbb{Q}\big(\sqrt{d}\,\big)$ es un cuerpo cuadrático con $d < -11$ entonces $\mathbb{Q}\big(\sqrt{d}\,\big)$ no es euclídeo.*

DEMOSTRACIÓN: Como d ha de ser libre de cuadrados, de hecho $d \le -13$. Sea $\mathcal{O}$ el anillo de enteros. Observemos que si $\delta = (a/2) + (b/2)\sqrt{d}$, donde a y b son enteros, cumple $|\,\mathrm{N}(\delta)| \le 3$, entonces $a^2 - db^2 \le 12$, y como $d \le -13$, necesariamente $b = 0$ y $|a| \le 3$, pero entonces $\delta = a/2$ es entero y no puede ser más que $\delta = 0, 1, -1$. En particular las únicas unidades de $\mathcal{O}$ son ± 1.

Si $\mathcal{O}$ fuera euclídeo podríamos tomar un $\delta \in \mathcal{O}$ de norma euclídea mínima entre los enteros no nulos ni unitarios, con lo que todo $\Delta \in \mathcal{O}$ se expresa como $\Delta = \delta c + r$, donde $r = 0, 1, -1$, por la elección de δ.

Esto significa que $\mathcal{O}/(\delta) = \big\{[0], [1], [-1]\big\}$, luego $|\,\mathrm{N}(\delta)| \le 3$ y, según hemos visto, δ es nulo o unitario, en contra de la elección que hemos hecho. ∎

Ejercicio: Probar que los únicos cuerpos euclídeos $\mathbb{Q}\big(\sqrt{d}\,\big)$ con $d \le -1$ son los correspondientes a $d = -1, -2, -3, -7, -11$.

Capítulo IV

Métodos geométricos

En este capítulo desarrollaremos las técnicas adecuadas para resolver los problemas que hemos venido planteando en los capítulos anteriores. Todos 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 $\mathbb{R}$.

4.1 La representación geométrica

Definición 4.1 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 la representación geométrica cumple el objetivo que nos habíamos propuesto:

Teorema 4.2 *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, $\sqrt{\big|\Delta[\alpha_1,\dots,\alpha_n]\big|}/2^t \neq 0$. ∎

4.2 Retículos

El último teorema que acabamos de obtener nos lleva a la definición siguiente:

Definición 4.3 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

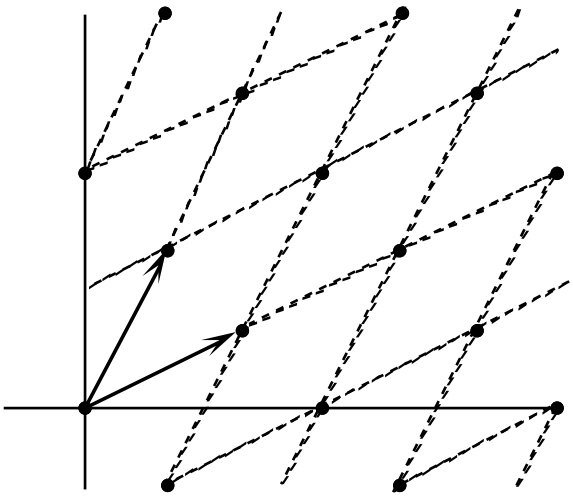
$$\mathcal{M} = \langle v_1,\dots,v_m\rangle_{\mathbb{Z}} = \{a_1v_1+\cdots+a_mv_m \mid a_1,\dots,a_m\in\mathbb{Z}\},$$

donde $v_1,\dots,v_m$ son vectores linealmente independientes en $\mathbb{R}^n$.

Obviamente los vectores $v_1,\dots,v_m$ 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 4.2 implica que la imagen de un módulo a través de la representación geométrica es un retículo, que será completo si el módulo lo es.

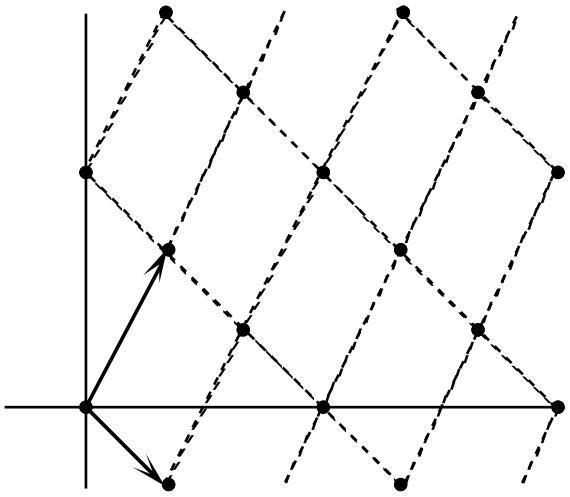
Por ejemplo, he aquí una imagen del retículo en $\mathbb{R}^2$ generado por los vectores $(1,2)$ y $(2,1)$:



A la vista de la figura resulta natural definir el *paralelepípedo fundamental* de una base $v_1,\dots,v_m$ 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 4.4 *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 las propiedades de la medida de Lebesgue $\mu(T) = |\det(a_{ij})|\mu\big([0,1[^n\big) = |\det(a_{ij})|$.

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 4.2 contiene el cálculo del volumen de su paralelepípedo fundamental:

Teorema 4.5 *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

$$c_M = \frac{\sqrt{|\Delta[M]|}}{2^t} = \frac{\sqrt{|\Delta[\mathcal{O}]|}}{2^t}\,\mathrm{N}(M).$$

Para demostrar las propiedades elementales de los paralelepípedos necesitaremos algunos conceptos topológicos:

Consideraremos en $\mathbb{R}^n$ el producto escalar euclídeo dado por

$$xy = x_1y_1 + \cdots + x_ny_n.$$

Así mismo consideraremos la norma euclídea $\|x\| = \sqrt{xx}$. Llamaremos B_n a la bola unitaria (de centro 0 y radio 1) en $\mathbb{R}^n$, y así rB_n será la bola de centro 0 y radio r. Cuando no haya confusión suprimiremos el subíndice n.

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 4.6 *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 $0 \le r_i < 1$. 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 $0 \le s_i < 1$ 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 $v_1, \dots, v_m$ 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 $\|u\| \le a_1\|v_1\| + \cdots + a_m\|v_m\| < d$.

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 $\|x\| \le \|x + u\| + \| - u\| < r + d$, y como $\mathcal{M}$ es discreto hay sólo un número finito de vectores $x \in \mathcal{M}$ tales que $\|x\| \le r + d$. ∎

El resultado siguiente es importante porque da una caracterización topológica del concepto de retículo, que nosotros hemos introducido algebraicamente.

Teorema 4.7 *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 generado por $\mathcal{M}$ en $\mathbb{R}^n$. Sea m su dimensión. Sean $v_1, \dots, v_m \in \mathcal{M}$ linealmente independientes. Sea $\mathcal{M}_0 \subset \mathcal{M}$ el retículo que generan. Sea T el paralelepípedo fundamental de $\mathcal{M}_0$ asociado a $\{v_1, \dots, v_m\}$.

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 $w_1, \dots, w_r$ que generan $\mathcal{M}$, y $r \le m$. Pero como $\mathcal{M}_0 \subset \mathcal{M}$, los vectores linealmente independientes $v_1, \dots, v_m$ son combinación lineal de $w_1, \dots, w_r$, 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 4.8 *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 4.6 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, tenemos que $rww = uw$, y aplicando la desigualdad de Cauchy–Schwarz llegamos a una contradicción: $r \leq \|u\| \, \|w\| = \|u\|$. ∎

Ejercicio: Probar que un retículo $\mathcal{M}$ es completo si y sólo si el grupo topológico $\mathbb{R}^n/\mathcal{M}$ es compacto (es topológicamente isomorfo a un producto de n veces la circunferencia unidad).

4.3 El teorema de Minkowski

Demostramos ahora el teorema central de este capítulo. Necesitamos un par de conceptos geométricos adicionales: Un subconjunto A de $\mathbb{R}^n$ es *convexo* si cuando $a, b \in A$ y $0 \leq \lambda \leq 1$, entonces $\lambda a + (1-\lambda)b \in A$. El conjunto X es *absolutamente convexo* si es convexo y cuando $a \in A$, también $-a \in A$.

Teorema 4.9 (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

$$\mu(Y) = \sum_{x \in \mathcal{M}} \mu(Y \cap T_{-x})$$

(notar 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

$$\big(x + \frac{1}{2}A\big) \cap \big(x' + \frac{1}{2}A\big) \neq \varnothing.$$

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 4.10 *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. Recordar la notación $n = s + 2t$ introducida en 4.1.

Teorema 4.11 *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 4.12 *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 4.5 vale $k = \sqrt{|\Delta[M]|}/2^t$.

En definitiva, se ha de cumplir que $\mu\big(X_{st}(c)\big) > 2^{s+t}\sqrt{|\Delta[M]|}$. Por el teorema anterior esto es

$$\frac{(2c)^n}{n!}\left(\frac{\pi}{8}\right)^t > 2^{s+t}\sqrt{|\Delta[M]|},$$

o sea, $c^n > \left(\frac{4}{\pi}\right)^t\sqrt{|\Delta[M]|}\,n!$. 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

$$\begin{aligned}\sqrt[n]{|\mathrm{N}(\alpha)|} &= \sqrt[n]{|\sigma_1(\alpha)\cdots\sigma_s(\alpha)\sigma_{s+1}(\alpha)^2\cdots\sigma_{s+t}(\alpha)^2|}\\ &\le \frac{|\sigma_1(\alpha)|+\cdots+|\sigma_s(\alpha)|+2|\sigma_{s+1}(\alpha)|+\cdots+2|\sigma_{s+t}(\alpha)|}{n} < \frac{c}{n}.\end{aligned}$$

Así pues, $|\,\mathrm{N}(\alpha)| < c^n/n^n$.

Dado $0 < \epsilon < 1$, existe un $c_\epsilon > 0$ tal que $c_\epsilon^n = \left(\frac{4}{\pi}\right)^t n!\sqrt{\left|\Delta[M]\right|} + \epsilon$, a partir del cual obtenemos un $\alpha_\epsilon \in \mathcal{M}$ no nulo tal que

$$|\,\mathrm{N}(\alpha_\epsilon)| < \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\left|\Delta[M]\right|} + \frac{\epsilon}{n^n}.$$

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, $|\,\mathrm{N}(\alpha)| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\left|\Delta[M]\right|}$. ∎

He aquí una aplicación sencilla:

Teorema 4.13 (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

$$1 \le \left|\mathrm{N}(\alpha)\right| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n},$$

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:

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, \qquad 0 < \theta < 1,$$

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

$$A = \Big\{x \in \mathcal{R}^{st} \;\Big|\; |x_1| < \sqrt{|\Delta|},\ |x_i| < 1\ (2 \le i \le s+t)\Big\} \quad \text{si } s \neq 0$$

$$A = \Big\{x \in \mathcal{R}^{0t} \;\Big|\; |\operatorname{Re} x_1| < \frac{1}{2},\ |\operatorname{Im} x_1| < \sqrt{|\Delta|}, |x_i| < 1\ (2 \le i \le t)\Big\} \quad \text{si } s = 0$$

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). Observar que este argumento nos permite obtener explícitamente tales cuerpos.

El teorema 4.12 tiene una consecuencia más importante que las que acabamos de obtener:

Teorema 4.14 *Sea K un cuerpo numérico de grado $n = s+2t$ y discriminante Δ. Entonces todo ideal de K es similar a otro ideal $\mathfrak{a}$ 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 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

$$\big|\mathrm{N}(\gamma)\big| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\big|\Delta[\mathfrak{c}]\big|},$$

según el teorema 4.12.

Según la definición de norma de un módulo, tenemos $\sqrt{\big|\Delta[\mathfrak{c}]\big|} = \mathrm{N}(\mathfrak{c})\sqrt{|\Delta|}$. 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

$$\mathrm{N}(\mathfrak{a}) = \frac{\mathrm{N}\big((\gamma)\big)}{\mathrm{N}(\mathfrak{c})} = \frac{\big|\mathrm{N}(\gamma)\big|\sqrt{|\Delta|}}{\sqrt{\big|\Delta[\mathfrak{c}]\big|}} \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

∎

El interés de esto reside en que, según el teorema 3.15, sólo hay un número finito de ideales de una norma dada, luego hemos probado el conjunto de las clases de similitud de ideales del orden maximal de un cuerpo dado es finito. Dedicamos la próxima sección a analizar las implicaciones de este hecho.

4.4 El grupo de clases

Dado un cuerpo numérico K, consideremos el grupo abeliano de los ideales fraccionales de K. Recordemos que los ideales fraccionales no son sino los módulos completos cuyo anillo de coeficientes es el orden maximal de K. Entre

estos módulos tenemos definida la relación de similitud: Dos ideales fraccionales $\mathfrak{a}$ y $\mathfrak{b}$ son similares si y sólo si existe un $\alpha \in K$ no nulo tal que $\mathfrak{b} = \alpha\mathfrak{a}$. Podemos expresar $\alpha = \beta/\gamma$ con β y γ enteros. Así, $\mathfrak{a}$ y $\mathfrak{b}$ son similares si y sólo si existen dos enteros β y γ no nulos tales que $\beta\mathfrak{a} = \gamma\mathfrak{b}$. Esta última ecuación puede expresarse equivalentemente en términos de ideales como $(\beta)\mathfrak{a} = (\gamma)\mathfrak{b}$.

Los ideales principales generan un grupo en el grupo de todos los ideales fraccionales. Sus elementos son de la forma $(\beta)(\gamma)^{-1}$, y es evidente que la similitud de módulos coincide con la congruencia módulo este subgrupo. Usaremos la notación $\mathfrak{a} \approx \mathfrak{b}$ para representar la similitud de ideales fraccionales.

Definición 4.15 Llamaremos *grupo de clases* de K al cociente del grupo de ideales fraccionales de K sobre el subgrupo generado por los ideales principales no nulos de K. Dos ideales fraccionales determinan la misma clase si y sólo si son similares.

Todo ideal fraccional es de la forma $\alpha^{-1}\mathfrak{a}$, donde α es un entero no nulo y $\mathfrak{a}$ es un ideal K. Evidentemente $\alpha^{-1}\mathfrak{a}$ es similar a $\mathfrak{a}$, luego concluimos que toda clase del grupo de clases se puede expresar como la clase $[\mathfrak{a}]$ de un ideal. Más aún, el teorema 4.14 afirma que toda clase de ideales tiene un representante de norma menor o igual que cierta cota, y ya hemos observado que sólo hay un número finito de ideales en tales condiciones. Por lo tanto el grupo de clases es finito, y a su número de elementos h se le llama *número de clases* del cuerpo numérico K.

Ahora observamos que si dos ideales son similares, entonces uno es principal si y sólo si lo es el otro: En efecto, si $\mathfrak{b} = \alpha\mathfrak{a}$ y $\mathfrak{a} = (\gamma)$, entonces $\alpha\gamma \in \mathfrak{b}$, luego es un entero y de hecho $\mathfrak{b} = (\alpha\gamma)$.

Esto significa que la clase $[1] = [(1)]$ no contiene más ideales que los principales, luego el grupo de clases es trivial ($h = 1$) si y sólo si todos los ideales de K son principales, si y sólo si K tiene factorización única.

Más en general, si $\mathfrak{a}$ es cualquier ideal de K, se cumple que $[\mathfrak{a}]^h = 1$, es decir, $\mathfrak{a}^h$ es siempre un ideal principal.

Para aplicar el teorema 4.14 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 4.14 afirma que todo ideal de K es similar a otro de norma a lo sumo $M_{st}\sqrt{|\Delta|}$. La tabla 4.1 contiene las primeras constantes de Minkowski redondeadas hacia arriba en la última cifra para que las cotas que proporcionan sean correctas.

Ejemplo 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.

Tabla 4.1: 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	$0,15199$

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 $M_{03}\sqrt{7^5} < 4,2$. Observar 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 el teorema 3.16 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). Ya sabemos que para $p = 23$ no hay factorización única. ∎

Enteros ciclotómicos reales Veremos en el capítulo XIII 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 del correspondiente cuerpo $K' = K \cap \mathbb{R}$. 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. La prueba del teorema 3.22 muestra que el divisor de 19 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, $\sqrt[3]{122} < 4,96$, 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 $\mathfrak{q} = (37, \omega^2 + \omega + 1)$ en K, tenemos que $\omega^2 \equiv -1 - 3\omega$ (mód $\mathfrak{q}$). Despejando, $\omega^{-1} \equiv -3 - \omega$ (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.

$\mathrm{N}(1 + \eta_1 - \eta_3) = 47$
$\mathrm{N}(1 + \eta_1 + \eta_7) = 137$
$\mathrm{N}(1 - \eta_1 + \eta_3) = 139$
$\mathrm{N}(1 - \eta_2 + \eta_4 + \eta_5 + \eta_6) = 229$
$\mathrm{N}(1 - \eta_1 - \eta_2) = -277$
$\mathrm{N}(1 + \eta_5 + \eta_7 - \eta_{10} + \eta_{11}) = 367$
$\mathrm{N}(1 - \eta_2 - \eta_3 - \eta_5) = 461$
$\mathrm{N}(1 + \eta_3 + \eta_5 + \eta_7 - \eta_8 + \eta_{11}) = -599$
$\mathrm{N}(1 - \eta_5 + \eta_7 - \eta_8 + \eta_{10} + \eta_{11}) = 643$
$\mathrm{N}(1 - \eta_1 - \eta_4 + \eta_5 + \eta_6 + \eta_9) = -827$
$\mathrm{N}(1 - \eta_5 + \eta_7 - \eta_8 - \eta_{10} + \eta_1 1) = 829$

$$\mathrm{N}(1 - \eta_1 - \eta_2 - \eta_3 - \eta_4 - \eta_5 - \eta_6 - \eta_7 - \eta_8 - \eta_{10}) = 691$$

Esto prueba que el anillo de enteros ciclotómicos reales de orden 23 tiene factorización única. ∎

Ejercicio: Probar que $\mathbb{Q}\big(\sqrt[3]{2}\big)$ tiene factorización única.

Ejemplo Para el ejemplo de Dedekind $\mathbb{Q}(\xi)$, tenemos $s = t = 1$ 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 69) que 2 se descompone en tres ideales primos principales. Como $\text{índ}\,\xi = 2$, 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. ∎

De momento aún no disponemos de las herramientas necesarias para calcular números de clases en general. Ello supone ser capaz de decidir si dos ideales dados son similares o no, lo que a su vez exige ser capaz de decidir si un ideal dado es principal o no, y a su vez hemos visto que esto equivale a resolver las ecuaciones diofánticas asociadas a los ideales. Ahora vamos a generalizar el concepto de grupo de clases a órdenes numéricos arbitrarios.

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 3.27 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 4.16 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 3.27, 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

$$\begin{aligned} P_{\mathfrak{f}}(\mathcal{O}') &= \{\alpha \in \mathcal{O}' \mid \alpha\mathcal{O} + \mathfrak{f} = 1\}, \\ P_{\mathfrak{f}}^*(\mathcal{O}') &= \{\alpha\mathcal{O}\beta^{-1}\mathcal{O} \mid \alpha, \beta \in P_{\mathfrak{f}}(\mathcal{O}')\}. \end{aligned}$$

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 $\mathfrak{ab} = (\alpha)$. 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 $I_\mathfrak{f}(\mathcal{O}')$.

Así mismo, 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. Ahora vamos a probar que es finito, a la vez que calculamos su orden.

Teorema 4.17 *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 3.10 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 $\alpha \equiv \beta$ (mód $\mathfrak{f}$) y por ser unidades existe un $\gamma \in \mathcal{O}$ tal que $\alpha\gamma \equiv \beta\gamma \equiv 1$ (mód $\mathfrak{f}$). 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 4.18 *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 $\mathcal{O}_m/(m) \cong \mathbb{Z}/m\mathbb{Z}$. ∎

Ejemplo Consideremos el orden $\mathbb{Z}\big[\sqrt{-3}\,\big]$, de índice 2 en el orden maximal de $\mathbb{Q}\big(\sqrt{-3}\,\big)$. Es fácil ver que el número de clases de este cuerpo es 1, así como que su grupo de unidades consta exactamente de las 6 raíces sextas de la unidad (en la sección siguiente obtendremos este hecho como consecuencia de resultados generales), mientras que el grupo de unidades de $\mathbb{Z}\big[\sqrt{-3}\,\big]$ consta sólo de $\{\pm 1\}$. Por consiguiente, y según la notación del teorema anterior, $e = 3$.

Por otra parte, el 2 se conserva primo en $\mathbb{Q}\big(\sqrt{-3}\,\big)$, luego $\Phi(2) = \mathrm{N}(2) - 1 = 3$. En total concluimos que el número de clases de $\mathbb{Z}\big[\sqrt{-3}\,\big]$ es $h_2 = 1$. Como ya sabemos, esto no significa que el anillo tenga factorización única. Un ejemplo de factorización no única es el siguiente:

$$2 \cdot 2 = \big(1 + \sqrt{-3}\,\big)\big(1 - \sqrt{-3}\,\big). \tag{4.1}$$

Vamos a probar que éste es en realidad el único caso posible. Consideremos un número cualquiera $a + b\sqrt{-3} \in \mathbb{Z}\big[\sqrt{-3}\,\big]$.

Supongamos que $2 \mid \mathrm{N}\big(a + b\sqrt{-3}\,\big) = a^2 + 3b^2$. Entonces a y b son ambos pares o ambos impares. En el primer caso $a + b\sqrt{-3} = 2\big(u + v\sqrt{-3}\,\big)$, en el segundo tenemos que a y b son ambos de la forma $4n \pm 1$. Por lo tanto bien $a+b$ o bien $a-b$ es múltiplo de 4, es decir, $4 \mid a \pm b$, para una elección adecuada del signo.

Trabajando en el orden maximal vemos que 2 es primo y $2 \mid \mathrm{N}\big(a + b\sqrt{-3}\,\big)$, luego divide a $a \pm b\sqrt{-3}$. Como es invariante por conjugación, de hecho tenemos que $2 \mid a+b\sqrt{-3}$. Por otra parte $\frac{1\pm\sqrt{-3}}{2}$ es una unidad, luego $1\pm\sqrt{-3}$ es asociado a 2 y también divide a $a + b\sqrt{-3}$. Digamos que

$$a + b\sqrt{-3} = \big(1 \pm \sqrt{-3}\,\big)\big(u + v\sqrt{-3}\,\big),$$

donde u y v son enteros o semienteros. Entonces

$$u + v\sqrt{-3} = \frac{a \pm 3b + (a \mp b)\sqrt{-3}}{4},$$

luego eligiendo el signo podemos hacer que u y v sean ambos enteros.

Así en ambos casos (tanto si a y b son pares o impares) hemos llegado a una factorización de la forma $a+b\sqrt{-3} = \tau\beta$, donde τ es 2 o $1\pm\sqrt{-3}$ y $\beta \in \mathbb{Z}\big[\sqrt{-3}\,\big]$. Repitiendo el proceso podemos llegar a una factorización $a+b\sqrt{-3} = \tau_1 \cdots \tau_r\beta$, donde ahora $\mathrm{N}(\beta)$ es impar. Como el número de clases es 1, β se descompone en producto de primos en $\mathbb{Z}\big[\sqrt{-3}\,\big]$, digamos

$$a + b\sqrt{-3} = \tau_1 \cdots \tau_r\pi_1 \cdots \pi_s. \tag{4.2}$$

Los factores τ_i son irreducibles de norma 4 y los factores π_i son primos de norma impar. Todos ellos son primos en el orden maximal.

Ejercicio: Probar que la descomposición (4.2) es única salvo signos y salvo las transformaciones entre los τ_i que pueden hacerse a partir de (4.1). La factorización es única salvo signos si exigimos que en la descomposición no aparezcan factores $1 \pm \sqrt{-3}$ con signos opuestos.

Terminamos la sección con un último resultado de finitud:

Teorema 4.19 *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 4.12 (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'. ∎

4.5 La representación logarítmica

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 4.20 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

$$\log\big|\mathrm{N}(x)\big| = l_1(x) + \cdots + l_{s+t}(x). \tag{4.3}$$

Si K es un cuerpo numérico llamaremos *representación logarítmica* de K a la aplicación $l : K \setminus \{0\} \longrightarrow \mathbb{R}^{s+t}$ dada por $l(\alpha) = l\big(x(\alpha)\big)$, donde x es la representación geométrica de K.

Así pues,

$$l(\alpha) = \big(\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_s(\alpha)|, \log|\sigma_{s+1}(\alpha)|^2, \ldots, \log|\sigma_{s+t}(\alpha)|^2\big).$$

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 4.21 *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 $k = 1, \dots, s+t$. Esto implica que el conjunto $\{x(\alpha) \mid \alpha \in W\}$ 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 4.22 *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 4.7, 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 $k = 1, \dots, s$ y $\big|\sigma_k(\epsilon)\big|^2 < e^r$ si $k = s+1, \dots, t$. 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 $0 = \log\big|\mathrm{N}(\epsilon)\big| = l_1(\epsilon) + \cdots + l_{s+t}(\epsilon)$.

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 4.8 o bien aplicando el teorema 4.8 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 (4.3) 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 (observar 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 2.19 existe sólo un número finito de elementos α no asociados y de $\mathcal{O}$ con norma menor que Q en módulo. Sean, pues, $\alpha_1, \ldots, \alpha_m \in \mathcal{O}$ no nulos tales que $|\,\mathrm{N}(\alpha_i)| < Q$ y de modo que cualquier otro entero en estas condiciones sea asociado en $\mathcal{O}$ a uno de ellos. Notar 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 4.23 (Teorema de Dirichlet) *Sea $\mathcal{O}$ un orden de un cuerpo numérico de grado $n = s + 2t$. Entonces existen unidades $\epsilon_1, \dots, \epsilon_r$ 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 $m_1, \dots, m_r$ son enteros racionales.*

Demostración: Sea U el grupo de las unidades de $\mathcal{O}$. Basta tomar unidades $\epsilon_1, \dots, \epsilon_r \in U$ tales que $l(\epsilon_1), \dots, l(\epsilon_r)$ sean una base de $l[U]$. ∎

Definición 4.24 Un conjunto de unidades $\epsilon_1, \dots, \epsilon_r$ 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 $\omega = \big(-1 + \sqrt{-3}\,\big)/2$.

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 $\epsilon_1, \dots, \epsilon_r$ un sistema fundamental de unidades de un orden $\mathcal{O}$ de un cuerpo numérico. Entonces $l(\epsilon_1), \dots, l(\epsilon_r)$ forman una base del retículo $l[U]$,

donde U es el grupo de las unidades de $\mathcal{O}$. El vector $l_0 = \frac{1}{\sqrt{s+t}}(1,\dots,1)$ es unitario y ortogonal al subespacio V formado por los vectores cuyas coordenadas suman 0.

Los vectores $l_0, l(\epsilon_1),\dots,l(\epsilon_r)$ 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 $l_0, l(\epsilon_1),\dots,l(\epsilon_r)$. Si sumamos todas las columnas a la columna i-ésima y tenemos en cuenta que las componentes de $l(\epsilon_1),\dots,l(\epsilon_r)$ 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 $l(\epsilon_1),\dots,l(\epsilon_r)$.

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 $R = 1$.

4.6 Cálculo de sistemas fundamentales de unidades

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. En esta sección probaremos 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 4.25 *Sea M un módulo completo de un cuerpo numérico K de grado n. Sea $\{\alpha_1,\dots,\alpha_n\}$ una base de M. Entonces existe una constante A tal que todos los elementos $\alpha \in M$ que cumplen $|\sigma_1(\alpha)| < c_1,\dots,|\sigma_n(\alpha)| < c_n$, para ciertos números reales positivos $c_1,\dots,c_n$ tienen sus coordenadas (en la base dada) acotadas en módulo por $A\sum_{j=1}^n c_j$.*

Demostración: 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 $\{\beta_1,\dots,\beta_n\}$ definida en 2.9.

Sea $A > 0$ tal que $|\sigma_i(\beta_j)| \le A$ 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

$$|a_i| = \big|\mathrm{Tr}(\alpha\beta_i)\big| = \Big|\sum_{j=1}^{n} \sigma_j(\alpha)\sigma_j(\beta_i)\Big| \le A\sum_{j=1}^{n}\big|\sigma_j(\alpha)\big| < A\sum_{j=1}^{n} c_j.$$

■

El próximo teorema contiene las ideas centrales del algoritmo para obtener sistemas fundamentales de unidades de cuerpos numéricos.

Teorema 4.26 *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 $u_2, \ldots, u_r \in \mathcal{M}$ y sus proyecciones en V son una base de $\mathcal{N}$, entonces $u, u_2, \ldots, u_r$ son una base de $\mathcal{M}$.*
3. *Todo elemento $x' \in \mathcal{N}$ es la proyección de un $x \in \mathcal{M}$ tal que*

$$\|x\| \le \sqrt{\frac{\|u\|^2}{4} + \|x'\|^2}.$$

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 $u_i = a_i u + u_i'$, 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 $v' = \sum_{i=2}^{r} b_i u_i'$, para ciertos enteros racionales b_i. Consecuentemente:

$$v = \left(a - \sum_{i=2}^{r} a_i b_i\right) u + \sum_{i=2}^{r} b_i u_i.$$

De aquí se sigue que el primer sumando del segundo miembro está en $\mathcal{M}$ y por la hipótesis sobre u el coeficiente $b_1 = a - \sum_{i=2}^{r} a_i b_i$ 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 $|\alpha| \le 1/2$. Entonces

$$\|x\|^2 = |\alpha|^2\|u\|^2 + \|x'\|^2 \le \|u\|^2/4 + \|x'\|^2.$$

■

Veamos ahora cómo podemos calcular en la práctica 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 4.25 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. Así mismo, sea $\mathcal{M}_1$ la imagen del grupo de unidades por la representación logarítmica, sea $\mathcal{M}_2$ la proyección de $\mathcal{M}_1$ en V_2 y sea $\mathcal{M}_3$ 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 4.25 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.

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 $\mathbb{Q}\big(\sqrt[3]{6}\big)$.

Ejemplo Vamos a calcular un sistema fundamental de unidades del cuerpo ciclotómico séptimo. Para este cuerpo se cumple $s = 0$, $t = 3$, luego el sistema consta de dos unidades.

En primer lugar probaremos un resultado general nos reducirá a la mitad el grado del cuerpo a estudiar.

Teorema 4.27 (Lema de Kummer) *Si $\mathbb{Q}(\omega)$ es el cuerpo ciclotómico de orden p, entonces toda unidad de $\mathbb{Z}[\omega]$ es el producto de una unidad real por una potencia de ω.*

Demostración: Sea $\epsilon = r(\omega)$ una unidad de $\mathbb{Z}[\omega]$. Su conjugado complejo es $\bar\epsilon = r(\omega^{-1}) = r(\omega^{p-1})$, que también es una unidad. Consideremos la unidad $\mu = \epsilon/\bar\epsilon \in \mathbb{Z}[\omega]$.

Todo conjugado de μ es de la forma $\sigma(\mu) = r(\omega^k)/r(\omega^{-k})$. Como el denominador es el conjugado (complejo) del numerador, concluimos que $|\sigma(\mu)| = 1$.

Esto significa que μ está en el núcleo de la representación logarítmica, y según el teorema 4.21 es una raíz de la unidad.

El grupo de las raíces de la unidad de $\mathbb{Q}(\omega)$ es cíclico de orden un cierto natural m. Sea ζ un generador. Puesto que ω está en dicho grupo, ha de ser $p \mid m$. Digamos $m = p^i x$ con $i \geq 1$.

El cuerpo $\mathbb{Q}(\zeta)$ es un cuerpo ciclotómico de grado $\phi(m)$, donde ϕ es la función de Euler. Así pues, $\phi(m) = (p-1)p^{i-1}\phi(x) \mid p-1$. Esto implica que $i = 1$ y que $\phi(x) = 1$, de donde $x = 2$ (ha de ser par), y así el grupo de las raíces de la unidad de $\mathbb{Q}(\omega)$ tiene orden $2p$, luego está formado por las unidades $\pm\omega^i$.

Continuando nuestro razonamiento, $\mu = \pm\omega^i$ para un entero racional i.

Supongamos que el signo fuera negativo. Entonces $\epsilon = -\omega^i\bar{\epsilon}$. Tomamos congruencias en $\mathbb{Z}[\omega]$ módulo el primo $\pi = 1-\omega$. Observar que $\omega \equiv 1$ (mód π). Así, $\epsilon \equiv -\bar{\epsilon}$ (mód π). Por otra parte, tomando congruencias en $\epsilon = r(\omega)$ y $\bar{\epsilon} = r(\omega^{-1})$ llegamos a que tanto ϵ como $\bar{\epsilon}$ son congruentes módulo π con la suma de los coeficientes de $r(x)$, luego $\epsilon \equiv -\epsilon$ (mód π), lo que implica que $\epsilon \equiv 0$ (mód π), es decir, $\pi \mid \epsilon$, lo cual es imposible porque π es un primo y ϵ una unidad. En consecuencia ha de ser $\epsilon = \omega^i\bar{\epsilon}$.

Sea j un entero racional tal que $2j \equiv i$ (mód p). Entonces $\epsilon = \omega^{2j}\bar{\epsilon}$, luego $\epsilon/\omega^j = \bar{\epsilon}/\omega^{-j} = \overline{\epsilon/\omega^{-j}} \in \mathbb{R}$. ∎

Observar que hemos demostrado que las únicas raíces de la unidad de $\mathbb{Q}(\omega)$ son las potencias de ω y sus opuestas. Teniendo en cuenta que las únicas raíces de la unidad reales son ± 1, esto está contenido en el enunciado del teorema anterior.

Teorema 4.28 *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 teorema anterior $\epsilon = \omega^i\eta$ 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 así $\epsilon_1^{m_1}\cdots\epsilon_r^{m_r} = \pm\epsilon_1^{k_1}\cdots\epsilon_r^{k_r}$.

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, $R = 2^{m-1}R'$. ∎

Volvamos, pues, al problema de hallar un sistema fundamental de unidades de $\mathbb{Q}(\omega)$, donde $\omega^7 = 1$. Sea $\eta = \omega + \omega^6$. Podemos trabajar en el cuerpo $\mathbb{Q}(\eta)$. En el capítulo II (página 44) 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:

$$\mathrm{N}\big(a+b\eta+c(\eta^2-2)\big) = a^3+b^3+c^3-a^2b-2ab^2-a^2c+3b^2c-2ac^2-4bc^2+3abc.$$

Así mismo podemos calcular la constante $A = 0'68$ del teorema 4.25.

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 $R = 4R' = 2'12$. ∎

Tenemos, pues, resuelto el problema de encontrar las unidades de un cuerpo numérico. Sin embargo para obtener nuevas soluciones de una ecuación diofántica a partir de una dada necesitamos las unidades de norma $+1$. Vamos a ver que un pequeño retoque nos permite obtener una expresión que genere exclusivamente 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). ∎

4.7 Cálculo del número 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 (4.3) tenemos 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 25 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 4.14, 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 3.16.

$\mathfrak{p} = (p,\eta)$	$\lvert\,\mathrm{N}(\eta)\rvert$	$\mathfrak{p} = (p,\eta)$	$\lvert\,\mathrm{N}(\eta)\rvert$	$\mathfrak{p} = (p,\eta)$	$\lvert\,\mathrm{N}(\eta)\rvert$
$(2, 1+\alpha)$	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 $2 = \mathfrak{p}\mathfrak{q}$, 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 4.25 es menor que $A = 1$.

Es fácil ver que α es una unidad fundamental de K: 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 $|\beta| \le 1/2$, 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 4.25, 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 $M_3=M\cap(0\times0\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})$, 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

$$\{\omega^5 + \omega^4 + 1,\ \ \omega^4 + \omega^3 + \omega^2 + 1,\ \ \omega^3 + 2\omega^2 + \omega + 1,\ \ 2\omega^2 + 2\omega + 2,\ \ 2\omega + 2,\ \ 2\}$$

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, de acuerdo con las observaciones que hicimos en la página 31, en este capítulo hemos resuelto el problema de determinar las soluciones de una ecuación diofántica definida por una forma completa.

Capítulo V

Fracciones continuas

Entre los métodos conocidos a finales del siglo XVII para resolver ciertas ecuaciones diofánticas se encuentran ciertos algoritmos que en términos modernos lo que hacen es calcular unidades fundamentales de cuerpos cuadráticos, de forma mucho más sencilla y rápida que con los métodos generales que explicamos en el capítulo anterior. La forma más elegante y refinada de estos algoritmos se expresa en términos de fracciones continuas. En este capítulo expondremos los resultados básicos entorno a ellas y su aplicación al cálculo de unidades fundamentales cuadráticas. En el siguiente veremos que también simplifican considerablemente la determinación de si dos módulos (y en particular dos ideales) son o no similares, con la consiguiente ventaja a la hora de calcular los números de clases.

5.1 Propiedades básicas

Definición 5.1 Partamos de una sucesión de enteros racionales $a_0, a_1, a_2, \ldots$ todos positivos salvo quizá el primero. Llamaremos

$$\begin{aligned}
[a_0] &= a_0,\\
[a_0, a_1] &= a_0 + \frac{1}{a_1},\\
[a_0, a_1, a_2] &= a_0 + \frac{1}{a_1 + \frac{1}{a_2}},\\
[a_0, a_1, a_2, a_3] &= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}},
\end{aligned}$$

En general tenemos definido el número racional $[a_0, \ldots, a_n]$ para todo n, que es no nulo si $n \geq 1$. Una definición formal se da por recurrencia de derecha a izquierda, es decir: $x_0 = a_n$, $x_{i+1} = a_{n-1-i} + 1/x_i$, $[a_0, \ldots, a_n] = x_n$.

Llamaremos $r_n = [a_0, \ldots, a_n] = p_n/q_n$, donde p_n y q_n son enteros racionales primos entre sí $q_n > 0$ (convenimos que si $a_0 = 0$, entonces $p_0 = 0$, $q_0 = 1$).

La sucesión r_n se llama *fracción continua* determinada por la sucesión a_n. Los números racionales r_n se llaman *convergentes* de la fracción continua.

Demostraremos que los convergentes realmente convergen a un cierto número real. Para ello comenzamos obteniendo una relación recurrente para los numeradores y los denominadores p_n y q_n.

Teorema 5.2 *Con la notación anterior:*

$$p_0 = a_0, \quad q_0 = 1, \quad p_1 = a_0a_1 + 1, \quad q_1 = a_1,$$

$$p_n = a_np_{n-1} + p_{n-2}, \qquad q_n = a_nq_{n-1} + q_{n-2}.$$

DEMOSTRACIÓN: Los casos $n = 0, 1, 2$ se comprueban directamente. Hay que probar que los valores dados por las fórmulas (en estos tres casos) son realmente primos entre sí, pero esto se ve fácilmente por los métodos usuales.

Supongámoslo cierto para $n - 1 \geq 2$ y probémoslo para n. Definimos los enteros racionales primos entre sí

$$\frac{p'_j}{q'_j} = [a_1, \ldots, a_{j+1}], \quad j = 0, 1, 2, \ldots$$

Por la hipótesis de inducción aplicada a $n - 1$ se cumplen las fórmulas

$$p'_{n-1} = a_np'_{n-2} + p'_{n-3}, \qquad q'_{n-1} = a_nq'_{n-2} + q'_{n-3}. \tag{5.1}$$

Por otra parte $\dfrac{p_j}{q_j} = a_0 + \dfrac{q'_{j-1}}{p'_{j-1}}$, luego

$$p_j = a_0p'_{j-1} + q'_{j-1}, \qquad q_j = p'_{j-1}, \tag{5.2}$$

donde se ha usado que si $(p'_{j-1}, q'_{j-1}) = 1$, los valores que dan estas fórmulas también son primos entre sí.

Haciendo $j = n$ en (5.2) y usando (5.1) obtenemos

$$\begin{aligned} p_n &= a_0(a_np'_{n-2} + p'_{n-3}) + (a_nq'_{n-2} + q'_{n-3}) \\ &= a_n(a_0p'_{n-2} + q'_{n-2}) + a_0p'_{n-3} + q'_{n-3}, \\ q_n &= a_nq'_{n-2} + q'_{n-3}. \end{aligned}$$

Aplicando (5.2) con $j = n - 1$ y $n - 2$ se deduce

$$p_n = a_np_{n-1} + p_{n-2}, \qquad q_n = a_nq_{n-1} + q_{n-2}.$$

■

De estas relaciones se sigue en particular que la sucesión q_n es creciente, y si $a_0 > 0$ entonces p_n también lo es. Veamos otra consecuencia sencilla:

Teorema 5.3 *Con la notación anterior,* $p_nq_{n+1} - p_{n+1}q_n = (-1)^{n+1}$ *o, lo que es lo mismo:* $r_n - r_{n+1} = (-1)^{n+1}/q_nq_{n+1}$.

DEMOSTRACIÓN: Claramente

$$\begin{aligned} p_nq_{n+1} - p_{n+1}q_n &= p_n(a_{n+1}q_n + q_{n-1}) - (a_{n+1}p_n + p_{n-1})q_n \\ &= p_nq_{n-1} - p_{n-1}q_n = -(p_{n-1}q_n - p_nq_{n-1}), \end{aligned}$$

y como $p_0q_1 - p_1q_0 = a_0a_1 - (a_0a_1 + 1) = -1$, se cumple el teorema. ∎

Con esto estamos en condiciones de demostrar la convergencia de las fracciones continuas.

Teorema 5.4 *Con la notación anterior, existe un único número real α tal que*

$$r_0 < r_2 < r_4 < r_6 < \cdots \alpha \cdots < r_7 < r_5 < r_3 < r_1.$$

Escribiremos $\alpha = [a_0, a_1, a_2, a_3, \dots\ ]$.

DEMOSTRACIÓN: Los convergentes están ordenados como se indica, pues

$$r_{n+2} - r_n = r_{n+2} - r_{n+1} + r_{n+1} - r_n = (-1)^{n+1}/q_{n+1}q_{n+2} + (-1)^{n+1}/q_nq_{n+1},$$

luego la sucesión de los convergentes pares es creciente y la de los impares decreciente. El teorema anterior nos da que cualquier convergente par es menor que cualquier convergente impar, así como que sus distancias tienden a 0 (la sucesión q_nq_{n+1} tiende a infinito), luego r_n converge a un número α, que es el supremo de los convergentes pares y el ínfimo de los impares. ∎

Teorema 5.5 *Las fracciones continuas son números irracionales.*

DEMOSTRACIÓN: Con la notación anterior, supongamos que $\alpha = p/q$ es un número racional (con p y q primos entre sí).

Como la sucesión q_n es creciente, existe un n tal que $q < q_{n+1}$. Puesto que α está entre r_n y r_{n+1}, se cumple que $|\alpha - r_n| \le |r_n - r_{n+1}| = 1/q_nq_{n+1} < 1/q_nq$.

Pero por otro lado $|\alpha - r_n| = |p/q - p_n/q_n| = |pq_n - qp_n|/q_nq \ge 1/q_nq$, puesto que $p/q \ne p_n/q_n$, luego $|pq_n - qp_n| \ge 1$, contradicción. ∎

El resultado que da importancia a las fracciones continuas es el que garantiza que todo número irracional positivo admite un único desarrollo en fracción continua. En efecto:

Teorema 5.6 *Sea α un número real cualquiera.*

1. *Si α es racional entonces $\alpha = [a_0, \dots, a_n]$ para ciertos enteros racionales.*
2. *Si α es irracional entonces $\alpha = [a_0, a_1, a_2, a_3, \dots\ ]$ para ciertos enteros racionales.*

Además si α es irracional el desarrollo es único.

DEMOSTRACIÓN: Definimos $a_0 = E(\alpha)$ (la parte entera de α). Si $\alpha \neq [a_0]$, entonces podemos escribir $\alpha = a_0 + 1/\alpha_1$ para un cierto número real positivo α_1. Tomamos $a_1 = E(\alpha_1)$. Si $a_1 = \alpha_1$ entonces $\alpha = [a_0, a_1]$. En otro caso $\alpha_1 = a_1 + 1/\alpha_2$ para cierto número real positivo α_2.

Si el proceso termina es que α es un número racional. Veamos que si no termina obtenemos una fracción continua que converge a α.

Por construcción se tiene que $\alpha = [a_0, \ldots, a_n, \alpha_{n+1}]$ (notar que el último término no es un número natural, pero la definición vale igualmente).

Es fácil ver que la función $[a_0, \ldots, a_n, x]$ es monótona creciente cuando n es impar y monótona decreciente cuando n es par. Como $a_{n+1} = E(\alpha_{n+1}) < \alpha_{n+1}$, se cumple que α es mayor que todos los convergentes pares y menor que todos los impares. Esto prueba que la fracción continua converge a α.

Para probar la unicidad supongamos que tenemos dos fracciones continuas infinitas, tales que $[a_0, a_1, \ldots\ ] = [b_0, b_1, \ldots\ ]$. Entonces $a_0 \leq [a_0, a_1, \ldots\ ] \leq a_0 + 1$ e igualmente con la otra fracción. Como el límite es irracional no se dan las igualdades, luego $a_0 = E\big([a_0, a_1, \ldots\ ]\big) = E\big([b_0, b_1, \ldots\ ]\big) = b_0$.

Restando a_0 de ambas y tomando inversos resulta $[a_1, a_2, \ldots\ ] = [b_1, b_2, \ldots\ ]$. Siguiendo así llegamos a que todos los coeficientes coinciden. ∎

Los números racionales admiten dos desarrollos en fracción continua, por ejemplo, $[2, 3, 1] = [2, 4]$.

El teorema 5.3 afirma que $|r_n - r_{n+1}| = 1/q_n q_{n+1}$ para cualquier par de convergentes consecutivos de una fracción continua. Puesto que su límite α se halla entre ambos, tenemos que

$$|\alpha - r_n| < 1/q_n a_{n+1} < 1/q_n^2.$$

Esto significa que los convergentes son buenas aproximaciones de sus límites. Podemos mejorar ligeramente este hecho observando que

$$|\alpha - r_n| + |\alpha - r_{n+1}| = |r_n - r_{n+1}| = 1/q_n q_{n+1}.$$

Cualquier par de números reales distintos cumple $xy < (x^2 + y^2)/2$, concluimos que

$$|\alpha - r_n| + |\alpha - r_{n+1}| < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}.$$

Esto prueba que de cada dos convergentes consecutivos de un número irracional α, uno de ellos, p/q cumple $|\alpha - p/q| < 1/2q^2$. El resultado principal que necesitamos es el recíproco de este hecho.

Teorema 5.7 *Si p, q son números naturales primos entre sí y $|\alpha - p/q| < 1/2q^2$, entonces p/q es un convergente de α.*

DEMOSTRACIÓN: Vamos a probar que si p y q son enteros cualesquiera tales que $0 < q < q_{n+1}$, entonces $|q\alpha - p| \geq |q_n\alpha - p_n|$. Esto significa que el convergente n-simo es la mejor aproximación racional de α con denominador menor que q_{n+1}.

En efecto, la matriz de los coeficientes del sistema de ecuaciones

$$\begin{aligned} p &= up_n + vp_{n+1} \\ q &= uq_n + vq_{n+1} \end{aligned}$$

tiene determinante ± 1, luego tiene una solución entera (u, v). Por la hipótesis se ha de cumplir $u \neq 0$ y en el caso en que $v \neq 0$ entonces u y v tienen signos opuestos, y así

$$\begin{aligned} |q\alpha - p| &= |(uq_n + vq_{n+1})\alpha - (up_n + vp_{n+1})| \\ &= |u(q_n\alpha - p_n) + v(q_{n+1}\alpha - p_{n+1})| \geq |q_n\alpha - p_n|. \end{aligned}$$

Ahora, en las hipótesis del teorema, tomamos un n tal que $q_n \leq q < q_{n+1}$. Entonces

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{p}{q}\right| + \left|\alpha - \frac{p_n}{q_n}\right| = \frac{|\alpha q - p|}{q} + \frac{|\alpha q_n - p_n|}{q_n} \leq \left(\frac{1}{q} + \frac{1}{q_n}\right)|\alpha q - p|.$$

Como $q \geq q_n$ y $|\alpha q - p| < 1/2q$, concluimos que

$$\frac{|pq_n - qp_n|}{qq_n} < \frac{1}{qq_n},$$

y como el numerador es entero, ha de ser 0, o sea, p/q es el convergente n-simo.

∎

Probamos ahora un resultado sencillo pero útil en la manipulación de fracciones continuas.

Teorema 5.8 *Sea $\alpha = [a_0, a_1, a_2, \dots\ ]$ y sea $\beta = [a_{n+1}, a_{n+2}, a_{n+3}, \dots\ ]$, para $n \geq 1$. Entonces se cumple que*

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}.$$

DEMOSTRACIÓN: La prueba consiste simplemente en observar que en la demostración del teorema 5.2 no se ha usado que los coeficientes a_n sean enteros salvo para probar que $(p_n, q_n) = 1$. Por lo tanto podemos aplicarlo a $\alpha = [a_0, \dots, a_n, \beta]$ y concluir que, aunque ahora p_{n+1} y q_{n+1} no sean números racionales,

$$\alpha = \frac{p_{n+1}}{q_{n+1}} = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}$$

∎

Ejercicio: Probar que las fracciones continuas determinan un homeomorfismo entre $[0, 1] \setminus \mathbb{Q}$ y el producto de una cantidad numerable de copias de $\mathbb{N}$ (el espacio de Baire). Deducir de aquí que el espacio de Baire es homeomorfo a $\mathbb{R} \setminus \mathbb{Q}$.

5.2 Desarrollos de irracionales cuadráticos

La relación de las fracciones continuas con los cuerpos cuadráticos se basa en que los desarrollos de los irracionales cuadráticos son periódicos, tal y como probamos a continuación.

Teorema 5.9 *Un número irracional α es cuadrático si y sólo si los coeficientes de su fracción continua se repiten periódicamente a partir de un cierto término.*

DEMOSTRACIÓN: Supongamos que los coeficientes de la fracción continua de α se repiten a partir de un cierto término.

Puesto que $[a_0, a_1, a_2, \dots\ ] = a_0 + 1/[a_1, a_2, \dots\ ]$, es claro que uno es cuadrático si y sólo si lo es el otro, luego podemos suponer que los coeficientes de α se repiten desde el primero (sin anteperíodo), o sea,

$$\alpha = [a_0, \dots a_n, a_0, \dots a_n, a_0, \dots a_n, \dots\ ].$$

El teorema anterior nos da entonces que

$$\alpha = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}.$$

Operando obtenemos un polinomio de segundo grado del cual es raíz α.

Observar que la fórmula anterior no vale si el período tiene longitud 1, pero en tal caso también podemos considerar que el período tiene longitud 2.

Supongamos ahora que α es un irracional cuadrático. Digamos que α es raíz del polinomio $ax^2 + bx + c$, donde a, b, c son enteros racionales, $a > 0$ y $d = b^2 - 4ac > 0$.

Consideremos la forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$. Así $f(\alpha, 1) = 0$. El cambio de variables

$$\begin{aligned} x &= p_n x' + p_{n-1} y', \\ y &= q_n x' + q_{n-1} y' \end{aligned}$$

tiene determinante ± 1, luego f es equivalente a la forma

$$f_n(x, y) = f(p_n x + p_{n-1} y, q_n x + q_{n-1} y) = a_n x^2 + b_n xy + c_n y^2.$$

Así, si llamamos $\alpha_n = [a_n, a_{n+1}, \dots\ ]$, el teorema 5.8 nos da que

$$\alpha = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}},$$

luego

$$\begin{aligned} 0 &= f(\alpha, 1) = \frac{1}{(q_n \alpha_{n+1} + q_{n-1})^2} f(p_n \alpha_{n+1} + p_{n-1}, q_n \alpha_{n+1} + q_{n-1}) \\ &= \frac{1}{(q_n \alpha_{n+1} + q_{n-1})^2}\ f_n(\alpha_{n+1}, 1), \end{aligned}$$

o sea, $f_n(\alpha_{n+1}, 1) = 0$. También se cumple que $a_n = f_n(1,0) = f(p_n, q_n)$, $c_n = f_n(0,1) = f(p_{n-1}, q_{n-1}) = a_{n-1}$ y $b_n^2 - 4a_n c_n = d$.

De $f(\alpha, 1) = 0$ se sigue

$$\frac{a_n}{q_n^2} = f\left(\frac{p_n}{q_n}, \frac{q_n}{q_n}\right) - f(\alpha, 1) = a\left(\left(\frac{p_n}{q_n}\right)^2 - \alpha^2\right) + b\left(\frac{p_n}{q_n} - \alpha\right).$$

Sabemos que $|\alpha - p_n/q_n| < 1/q_n^2$, luego

$$|\alpha^2 - (p_n/q_n)^2| < \frac{|\alpha + p_n/q_n|}{q_n^2} < \frac{2|\alpha| + 1}{q_n^2}.$$

Todo esto implica que $|a_n| < |a|(2|\alpha| + 1) + |b|$, o sea, $|a_n|$ satisface una cota independiente de n. Las relaciones que hemos obtenido prueban que $|b_n|$ y $|c_n|$ también están acotadas.

Por lo tanto los polinomios $f_n(x, 1)$ varían en un conjunto finito, al igual que sus raíces, entre las que se encuentran los números α_n. En consecuencia existen naturales n y k tales que $\alpha_n = \alpha_{n+k}$, y es claro que esto implica que $a_{m+k} = a_m$ para todo $m \geq n$, o sea, los coeficientes de α se repiten periódicamente. ∎

Ejemplo Consideremos el número $\alpha = \big(1 + \sqrt{5}\big)/2$, que es raíz del polinomio $x^2 - x - 1$. Puesto que $\alpha^2 = \alpha + 1$, resulta que $\alpha = 1 + 1/\alpha$, lo que implica claramente que

$$\frac{1 + \sqrt{5}}{2} = [1, 1, 1, \dots\ ].$$

∎

En general, para calcular el desarrollo de un irracional cuadrático α vamos calculando sus coeficientes a_n al mismo tiempo que los restos α_n. Concretamente a_n es la parte entera de α_n y $\alpha_{n+1} = 1/(\alpha_n - a_n)$. Si tenemos la precaución de expresar siempre α_n en forma canónica, $a + b\sqrt{d}$, detectaremos cuándo α_n coincide con otro resto anterior, con lo que terminará el período.

Ejemplo Desarrollemos $\sqrt{19}$:

$$\begin{array}{llllllll}
\alpha_0 = \sqrt{19}, & a_0 = 4, & \alpha_1 = \frac{4+\sqrt{19}}{3}, & a_1 = 2, & \alpha_2 = \frac{2+\sqrt{19}}{5}, & a_2 = 1, \\
\alpha_3 = \frac{3+\sqrt{19}}{2}, & a_3 = 3, & \alpha_4 = \frac{3+\sqrt{19}}{5}, & a_4 = 1, & \alpha_5 = \frac{2+\sqrt{19}}{2}, & a_5 = 2, \\
\alpha_6 = 4 + \sqrt{19}, & a_6 = 8, & \alpha_7 = \frac{4+\sqrt{19}}{3}, & a_7 = 2. &&&&
\end{array}$$

Así pues, $\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$, donde la barra indica el período que se repite. Este número tiene un anteperíodo de longitud 1. Enseguida veremos que esto no es casual. ∎

Una fracción continua es *periódica pura* si no tiene anteperíodo.

Teorema 5.10 *Un irracional cuadrático α tiene fracción continua periódica pura si y sólo si $\alpha > 1$ y su conjugado $\bar{\alpha}$ (es decir, la otra raíz de* pol mín α*) cumple $-1 < \bar{\alpha} < 0$.*

DEMOSTRACIÓN: Recordemos que el desarrollo en fracción continua se calcula partiendo de $\alpha_0 = \alpha$ y de aquí $a_n = E(\alpha_n), \alpha_{n+1} = 1/(\alpha_n - a_n)$.

Por inducción es claro que $-1 < \bar{\alpha}_n < 0$. En efecto, $\bar{\alpha}_{n+1} = 1/(\bar{\alpha}_n - a_n)$ y admitiendo $-1 < \bar{\alpha}_n < 0$, tenemos $-1 - a_n < \bar{\alpha}_n - a_n < -a_n$, con lo que $-1 < -1/(a_n + 1) < \bar{\alpha}_{n+1} < -1/a_n < 0$.

Ahora, despejando en $\alpha_{n+1} = 1/(\alpha_n - a_n)$, tenemos que $-1/\bar{\alpha}_{n+1} = a_n - \bar{\alpha}_n$, y como $0 < -\bar{\alpha}_n < 1$, concluimos que $a_n = E(a_n - \bar{\alpha}_n) = E(-1/\bar{\alpha}_{n+1})$.

Por el teorema anterior sabemos que $\alpha_m = \alpha_n$ para ciertos $m < n$, luego también $1/\bar{\alpha}_m = 1/\bar{\alpha}_n$, y así $a_{m-1} = a_{n-1}$. Por lo tanto

$$\alpha_{m-1} = a_{m-1} + 1/\alpha_m = a_{n-1} + 1/\alpha_n = \alpha_{n-1}.$$

Repitiendo el argumento llegamos a que $\alpha_0 = \alpha_{n-m}$, luego la fracción es periódica pura.

Ahora supongamos que la fracción es periódica pura. Entonces a_0 coincide con un coeficiente posterior, luego $\alpha \geq a_0 \geq 1$. Por el teorema 5.8 resulta que

$$\alpha = \frac{p_n\alpha + p_{n-1}}{q_n\alpha + q_{n-1}},$$

luego α es raíz del polinomio $f(x) = q_n x^2 + (q_{n-1} - p_n)x - p_{n-1}$.

Ahora bien, $\bar{\alpha}$ también es raíz de este polinomio, y $f(0) = -p_{n-1} < 0$, $f(-1) = p_n - p_{n-1} + q_n - q_{n-1} > 0$, por el teorema 5.2, luego $-1 < \bar{\alpha} < 0$. ∎

Si d no es un cuadrado perfecto, entonces el conjugado de $E\big(\sqrt{d}\big) + \sqrt{d}$ es $E\big(\sqrt{d}\big) - \sqrt{d}$, que claramente está entre -1 y 0, luego $E\big(\sqrt{d}\big) + \sqrt{d}$ tiene un desarrollo periódico puro. Por lo tanto el desarrollo de $\sqrt{d}$ tiene exactamente una cifra de anteperíodo.

5.3 Transformaciones modulares

Seguidamente investigamos cuándo dos irracionales tienen fracciones continuas finalmente iguales. Veremos que esto sucede cuando son equivalentes en el sentido siguiente:

Definición 5.11 Dos números α y β son *equivalentes* si existen enteros racionales a, b, c, d tales que

$$\alpha = \frac{a\beta + b}{c\beta + d}, \qquad ad - bc = \pm 1. \tag{5.3}$$

Se comprueba enseguida que dos números racionales cualesquiera son equivalentes, y que un número racional nunca es equivalente a uno irracional, por lo que podemos limitarnos a considerar números irracionales.

También es fácil ver que la fórmula anterior define una biyección sobre los números irracionales. Las biyecciones de este tipo se llaman *transformaciones*

modulares. Las inversas y la composición de transformaciones modulares son de nuevo transformaciones modulares, por lo que la equivalencia de números irracionales (y en general la de números reales) es una relación de equivalencia.

Los teoremas 5.3 y 5.8 nos dan que la transformación $\alpha = [a_0, \ldots, a_n, \beta]$ es modular, dada concretamente por

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}.$$

El teorema siguiente caracteriza las transformaciones modulares que se pueden expresar de esta forma.

Teorema 5.12 *Si una transformación modular (5.3) cumple $c > d > 0$ entonces se puede expresar de la forma $\alpha = [a_0, \ldots, a_n, \beta]$ para ciertos enteros racionales $a_0, \ldots, a_n$, todos positivos salvo quizá el primero.*

DEMOSTRACIÓN: Hay que probar que existen $a_0, \ldots, a_n$ tales que

$$p_n = a, \quad p_{n-1} = b, \quad q_n = c, \quad q_{n-1} = d. \tag{5.4}$$

Lo probaremos por inducción sobre d.

Si $d = 1$ tenemos que $a = bc \pm 1$. En el caso $a = bc + 1$ sirve $\alpha = [b, c, \beta]$. Si se cumple $a = bc - 1$, entonces $\alpha = [b - 1, 1, c - 1, \beta]$.

Supongamos ahora que $d > 1$. Aplicando el teorema 5.2, las ecuaciones (5.4) equivalen a

$$p_{n-1} = b, \quad p_{n-2} = a - a_n b, \quad q_{n-1} = d, \quad q_{n-2} = c - a_n d. \tag{5.5}$$

Se sigue cumpliendo $b(c - a_n d) - (a - a_n b)d = \pm 1$ para cualquier a_n, y por hipótesis de inducción (5.5) tendrá solución si garantizamos $d > c - a_n d > 0$, o equivalentemente, si $c/d > a_n > (c - d)/d$.

Notemos que c/d no puede ser entero, pues si $c = kd$ entonces $d \mid 1$. Como $c/d - (c - d)/d = 1$, podemos tomar un número natural a_n en estas condiciones y así se cumple el teorema. ∎

Teorema 5.13 *Dos números irracionales α y β son equivalentes si y sólo si sus desarrollos en fracción continua son finalmente iguales, es decir, si*

$$\alpha = [a_0, \ldots, a_m, c_0, c_1, \ldots\ ], \qquad \beta = [b_0, \ldots, b_n, c_0, c_1, \ldots\ ].$$

DEMOSTRACIÓN: El teorema 5.8 nos da que en estas condiciones tanto α como β son equivalentes al número $[c_0, c_1, \ldots\ ]$, luego son equivalentes entre sí.

Supongamos ahora que α y β son equivalentes. Digamos que

$$\alpha = \frac{a\beta + b}{c\beta + d}, \qquad ad - bc = \pm 1.$$

Podemos suponer que $c\beta + d > 0$. Sea $\beta = [b_0, \ldots, b_{k-1}, \beta_k]$, donde $\beta_k = [b_k, b_{k+1}, \ldots\ ]$. Entonces:

$$\beta = \frac{\beta'_k p_{k-1} + p_{k-2}}{\beta'_k q_{k-1} + q_{k-2}}.$$

Componiendo las transformaciones modulares obtenemos que

$$\alpha = \frac{P\beta'_k + R}{Q\beta'_k + S},$$

donde

$$\begin{aligned} P &= ap_{k-1} + bq_{k-1}, \\ R &= ap_{k-2} + bq_{k-2}, \\ Q &= cp_{k-1} + dq_{k-1}, \\ S &= cp_{k-2} + dq_{k-2}, \end{aligned}$$

que son enteros racionales y cumplen $PS - QR = \pm 1$.

Por el teorema 5.3 y puesto que β se encuentra entre dos convergentes consecutivos cualesquiera, $|p_{k-1}/q_{k-1} - \beta| < 1/q_{k-1}q_k$, o sea, $|p_{k-1} - \beta q_{k-1}| < 1/q_k$. Por lo tanto $p_{k-1} = \beta q_{k-1} + \delta/q_{k-1}$, e igualmente $p_{k-2} = \beta q_{k-2} + \delta'/q_{k-2}$, con $|\delta|, |\delta'| < 1$.

De aquí resulta que

$$Q = (c\beta + d)q_{k-1} + \frac{c\delta}{q_{k-1}}, \qquad S = (c\beta + d)q_{k-2} + \frac{c\delta'}{q_{k-2}}.$$

Teniendo en cuenta que $c\beta + d > 0$, es claro que haciendo k suficientemente grande podemos conseguir $Q > S > 0$. Aplicando el teorema anterior resulta que $\alpha = [a_0, \ldots, a_m, \beta_k]$, de donde se sigue el teorema. ∎

5.4 Unidades de cuerpos cuadráticos

Recordemos que según el teorema 2.24 los órdenes de los cuerpos cuadráticos $\mathbb{Q}\big(\sqrt{d}\,\big)$ son los de la forma $\mathcal{O}_m = \mathbb{Z}[m\omega] = \{a + bm\omega \mid a, b \in \mathbb{Z}\}$, donde $\omega = \sqrt{d}$ o bien $\omega = \big(1 + \sqrt{d}\,\big)/2$ según el resto de d módulo 4.

Sabemos también que si $d > 0$, un sistema fundamental de unidades de $\mathcal{O}_m$ consta de una sola unidad ϵ, y es obvio que si ϵ es una unidad fundamental, las unidades fundamentales son exactamente $\pm\epsilon$ y $\pm 1/\epsilon$. Por lo tanto hay una única unidad fundamental $\epsilon > 1$. En lo sucesivo, cuando hablemos de la unidad fundamental de $\mathcal{O}_m$ nos referiremos siempre a la unidad mayor que 1.

Si $\epsilon = x + ym\omega > 1$ es cualquier unidad de $\mathcal{O}_m$, como $\mathrm{N}(\epsilon) = \epsilon\bar{\epsilon} = \pm 1$, tenemos que $\bar{\epsilon} = \pm 1/\epsilon$, y en cualquier caso $\epsilon - \bar{\epsilon} > 0$, o sea, $ym(\omega - \bar{\omega}) > 0$, y como $\omega - \bar{\omega} > 0$, resulta que $y > 0$.

Por otro lado, $\bar{\omega} < -1$ excepto en el caso $d = 5$. En efecto, en el caso $d \not\equiv 1 \pmod 4$ es $\bar{\omega} = -\sqrt{d} < -1$, mientras que si $d \equiv 1 \pmod 4$, entonces $\bar{\omega} = \big(1 - \sqrt{d}\,\big)/2 < -1$ si y sólo si $\sqrt{d} > 3$, si y sólo si $d > 9$, o sea, si y sólo si $d \neq 5$.

Claramente $m\bar{\omega} < -1$ excepto si $m = 1, d = 5$. Como $|\bar{\epsilon}| = |x + ym\bar{\omega}| < 1$, salvo en el caso exceptuado ha de ser $x > 0$.

Hemos concluido que la unidad fundamental de $\mathcal{O}_m$ es $\epsilon = x + ym\omega$ con $x, y > 0$ salvo si $d = 5$, $m = 1$. En tal caso no es difícil comprobar que la unidad fundamental es ω (o sea, $x = 0$, $y = 1$).

Ahora es fácil ver que $\epsilon^n = x' + y'm\omega$, con $x' > x$ e $y' > y$. Por lo tanto la unidad fundamental está caracterizada por que es de la forma $\epsilon = x + ym\omega$ con $x, y > 0$ mínimos entre los coeficientes de las unidades (salvo el caso exceptuado).

Puesto que $\mathrm{N}(\epsilon) = (x + ym\omega)(x + ym\bar{\omega}) = \pm 1$, resulta

$$\left|\frac{x}{y} + m\bar{\omega}\right| = \frac{1}{y(x + ym\omega)}.$$

En el caso $d \equiv 1 \pmod 4$ (salvo el caso exceptuado)

$$\left|\frac{x}{y} - m\frac{\sqrt{d}-1}{2}\right| = \left(y^2\left(\frac{x}{y} + m\frac{\sqrt{d}+1}{2}\right)\right)^{-1} < \frac{1}{2y^2},$$

pues $m\frac{\sqrt{d}+1}{2} > 2$. En el caso restante,

$$\left|\frac{x}{y} - m\sqrt{d}\right| = \frac{1}{y\big(x + ym\sqrt{d}\,\big)} \leq \frac{1}{y^2\big(\sqrt{d-1} + \sqrt{d}\,\big)} < \frac{1}{2y^2},$$

donde hemos usado que $\mathrm{N}(\epsilon) = x^2 - y^2m^2d = \pm 1$, luego $x^2 \geq dy^2 - 1 \geq y^2(d-1)$, y en consecuencia $x \geq y\sqrt{d-1}$.

En cualquier caso (salvo el exceptuado) llegamos a que

$$\left|\frac{x}{y} - (-m\bar{\omega})\right| < \frac{1}{2y^2},$$

lo que por el teorema 5.7 significa que x/y es uno de los convergentes de $-m\bar{\omega}$ (notemos que $(x, y) = 1$, o de lo contrario ϵ no podría tener norma unitaria).

Como el numerador y el denominador de los convergentes crece, tenemos que el convergente x/y correspondiente a la unidad fundamental será el primero que cumpla que la norma del entero asociado sea ± 1.

Ejemplo Vamos a calcular la unidad fundamental del orden $\mathbb{Z}\big[\sqrt{54}\,\big]$, es decir, el orden $\mathcal{O}_3$ de $\mathbb{Q}\big(\sqrt{6}\,\big)$. Hemos de calcular los convergentes de $\sqrt{54}$. Para ello hallamos el desarrollo $\sqrt{54} = [7, \overline{2, 1, 6, 1, 2, 1, 4}]$ y mediante las fórmulas del teorema 5.2 calculamos

a_n	7	2	1	6	1	2	1
p_n	7	15	22	147	169	485	$\cdots$
q_n	1	2	3	20	23	66	$\cdots$
$p_n^2 - 54q_n^2$	-8	9	-2	9	-5	1	$\cdots$

Con lo que la unidad fundamental buscada es $485 + 66\sqrt{54}$. ∎

Este método tiene su origen en un algoritmo para resolver la llamada *ecuación de Pell*, que no es sino la ecuación diofántica $x^2 - dy^2 = 1$. Si d no

es un cuadrado perfecto, una solución entera (x, y) de la ecuación de Pell se corresponde con una unidad $x + y\sqrt{d}$ del orden $\mathbb{Z}\big[\sqrt{d}\,\big]$.

En el caso en que $d < 0$ el número de unidades (de soluciones) es finito, y es igual a 2 (las correspondientes a ± 1, esto es $(\pm 1, 0)$) salvo si $d = -1, -3$, en cuyo caso hay 4 y 6 soluciones respectivamente.

Si $d > 0$ entonces hay infinitas soluciones (x, y), que son de la forma

$$x + y\sqrt{d} = \pm\big(u + v\sqrt{d}\,\big)^n, \quad \text{para } n \in \mathbb{Z},$$

donde $u + v\sqrt{d}$ es la unidad fundamental del orden $\mathbb{Z}\big[\sqrt{d}\,\big]$. La solución (u, v) se llama *solución fundamental.*

Finalmente si $d = k^2$ entonces la ecuación factoriza como $(x+ky)(x-ky) = 1$, lo que implica $x + ky = x - ky = 1$, o bien $x + ky = x - ky = -1$, lo que lleva a las soluciones triviales $(\pm 1, 0)$ (salvo si $d = 0$, en cuyo caso $(\pm 1, y)$ es siempre solución).

Según los cálculos anteriores, la solución fundamental, o sea, la mínima solución no trivial, de la ecuación $x^2 - 54y^2 = 1$ es $(485, 66)$.

Si $\mathcal{O}$ es el orden maximal de un cuerpo cuadrático real K y ϵ es su unidad fundamental, es fácil comprobar que la unidad fundamental de un orden cualquiera $\mathcal{O}_m$ es ϵ^k, donde k es el menor número natural no nulo tal que $\epsilon^k \in \mathcal{O}_m$. De aquí se deduce que el índice e_m del grupo de unidades de $\mathcal{O}_m$ en el grupo de unidades de $\mathcal{O}$ es precisamente k. Recordemos que dicho índice interviene en la fórmula del teorema 4.18 para el cálculo del número de clases de los órdenes no maximales.

Ejemplo Sea $K = \mathbb{Q}\big(\sqrt{2}\,\big)$. Es fácil comprobar que la unidad fundamental de K es $\epsilon = 1 + \sqrt{2}$ y que su número de clases es $h = 1$. Si $m = 2^s t$, donde t es impar y $\epsilon^m = a + b\sqrt{2}$, entonces la potencia de 2 que divide a b es exactamente 2^s (se prueba sin dificultad por inducción sobre s). Consecuentemente, $e_{2^s} = 2^s$.

Por otra parte, $2 = \mathfrak{p}^2$ en K, donde $\mathfrak{p}$ es un ideal de norma 2. Por lo tanto, la fórmula de 4.18 nos da que el número de clases de $\mathcal{O}_{2^s}$ es

$$h_{2^s} = \frac{\Phi(\mathfrak{p}^{2k})}{\phi(2^k)e_{2^s}}\, h = \frac{2^{2k-1}}{2^{k-1}2^k} = 1.$$

■

Ejercicio: Sea $K = \mathbb{Q}\big(\sqrt{5}\,\big)$. Probar que el número de clases de $\mathcal{O}_{5^k}$ es 1 y el número de clases de $\mathcal{O}_{2^k}$ es 2, para $k \geq 3$.

5.5 La fracción continua de e

Ya que hemos desarrollado la teoría básica sobre fracciones continuas, dedicamos esta sección a ilustrar algunos resultados más avanzados. Nuestro objetivo será obtener el desarrollo en fracción continua del número e, que es

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots\ ]$$

Ninguno de los resultados de esta sección será necesario en los capítulos siguientes.

Fijemos un número natural m no nulo y para cada $n \geq 0$ definamos

$$\psi_n = \sum_{r=0}^{\infty} \frac{2r+2n+1}{1\cdot 3\cdot 5\cdots(2r+2n+1)} \ \frac{2r+2}{2\cdot 4\cdot 6\cdots(2r+2)} \ \frac{1}{m^{2r}}.$$

En primer lugar observamos que

$$\begin{aligned} \psi_0 &= \sum_{r=0}^{\infty} \frac{1}{(2r)!} \ \frac{1}{m^{2r}} = \frac{1}{2}\big(e^{1/m} + e^{-1/m}\big), \\ \psi_1 &= \sum_{r=0}^{\infty} \frac{1}{(2r+1)!} \ \frac{1}{m^{2r}} = \frac{m}{2}\big(e^{1/m} - e^{-1/m}\big). \end{aligned}$$

Comprobemos además que se cumple la relación

$$m^2\psi_n = (2n+1)m^2\psi_{n+1} + \psi_{n+2}, \qquad n = 0, 1, 2, \ldots \tag{5.6}$$

de donde se sigue en particular que todas las series convergen.

En efecto:

$$m^2\psi_n - (2n+1)m^2\psi_{n+1} = \sum_{r=0}^{\infty} \frac{(2r+2n+3)m^2 2r}{1\cdot 3\cdot 5\cdots(2r+2n+3)} \ \frac{2r+2}{2\cdot 4\cdot 6\cdots(2r+2)} \ \frac{1}{m^{2r}}.$$

Si eliminamos el primer sumando, que es nulo, y cambiamos el índice r por $r+1$ obtenemos la expresión que define a ψ_{n+2}.

Es claro que $\psi_n > 0$ para todo número natural n. Por lo tanto podemos definir

$$\omega_n = \frac{m\psi_n}{\psi_{n+1}}, \qquad n = 0, 1, 2, \ldots$$

Dividiendo entre $m\psi_{n+1}$ en (5.6) llegamos a la fórmula siguiente:

$$\omega_n = (2n+1)m + \frac{1}{\omega_{n+1}}, \qquad n = 0, 1, 2, \ldots$$

de donde se sigue que $\omega_n > 1$ para todo n, y que el desarrollo en fracción continua de ω_0 es

$$\omega_0 = [m, 3m, 5m, \ldots\ ].$$

Ahora bien,

$$\omega_0 = \frac{m\psi_0}{\psi_1} = \frac{e^{1/m} + e^{-1/m}}{e^{1/m} - e^{-1/m}} = \frac{e^{2/m}+1}{e^{2/m}-1},$$

con lo cual obtenemos en particular que

$$\frac{e+1}{e-1} = [2, 6, 10, 14, \ldots\ ].$$

Puesto que las fracciones continuas (infinitas) representan números irracionales, esto prueba que el número e no es racional. Más aún, que no es un irracional cuadrático, pues la fracción continua que nos ha aparecido no es periódica.

Sea ahora

$$\xi = \frac{e^{2/m}+1}{2} = 1 + \frac{1}{\omega_0 - 1}.$$

Es inmediato que $\xi = [1, m-1, 3m, 5m, \dots\ ]$.

Para obtener el desarrollo en fracción continua de e necesitamos eliminar el 2 del denominador de ξ. Llamemos $\eta = e^{2/m} = 2\xi - 1$. Vamos a exponer un método general que permite calcular en muchos casos la fracción continua de un número η a partir de la fracción continua de un número ξ cuando entre ellos se da una relación del tipo

$$\eta = \frac{u\xi + v}{w},$$

donde u y w son números naturales no nulos y v es un número entero.

Antes de enunciar el resultado principal hemos de observar que si $a > 1$ entonces

$$[\dots, a] = [\dots, a-1, 1],$$

por lo que un número racional admite siempre un desarrollo en fracción continua de longitud par y otro de longitud impar.

También es útil notar que las fórmulas del teorema 5.2 son válidas para $n = 0, 1$ si convenimos en que $p_{-1} = 1$, $q_{-1} = 0$, $p_{-2} = 0$, $q_{-2} = 1$.

Teorema 5.14 *Sea $\xi = [a_0, a_1, a_2, \dots\ ]$ el desarrollo en fracción continua de un irracional ξ. Sea p_n/q_n el convergente n-simo y $\xi_n = [a_n, a_{n+1}, a_{n+2}, \dots\ ]$. Sea $\eta = (u\xi+v)/w$, donde u, v, w son números enteros, $u > 0$, $w > 0$, $uw = D > 1$. Para un índice cualquiera $n \geq 1$ desarrollamos el número racional*

$$\frac{u[a_0, a_1, \dots, a_{n-1}] + v}{w} = \frac{up_{n-1} + vq_{n-1}}{wq_{n-1}} = [b_0, b_1, \dots, b_{m-1}]$$

eligiendo el final de modo que $m \equiv n$ (mód 2). Sea r_j/s_j el convergente j-ésimo de este desarrollo, de modo que en particular se tiene

$$\frac{up_{n-1} + vq_{n-1}}{wq_{n-1}} = \frac{r_{m-1}}{s_{m-1}}. \tag{5.7}$$

Entonces existen números enteros u', v', w' tales que

$$\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} = \begin{pmatrix} r_{m-1} & r_{m-2} \\ s_{m-1} & r_{m-2} \end{pmatrix} \begin{pmatrix} u' & v' \\ 0 & w' \end{pmatrix},$$

$u' > 0$, $w' > 0$, $u'w' = D$, $-w' \leq v' \leq u'$, y $\eta = [b_0, b_1, \dots, b_{m-1}, \eta_m]$, donde $\eta_m = (u'\xi_n + v')/w'$.

DEMOSTRACIÓN: La ecuación matricial equivale al siguiente sistema de ecuaciones:

$$\begin{aligned} up_{n-1} + vq_{n-1} &= r_{m-1}u', && (5.8)\\ wq_{n-1} &= s_{m-1}u', && (5.9)\\ up_{n-2} + vq_{n-2} &= r_{m-1}v' + r_{m-2}w', && (5.10)\\ wq_{n-2} &= s_{m-1}v' + s_{m-2}w'. && (5.11) \end{aligned}$$

Como r_{m-1} y s_{m-1} son enteros primos entre sí, de (5.7) se sigue que los cocientes

$$\frac{up_{n-1} + vq_{n-1}}{r_{m-1}} = \frac{wq_{n-1}}{s_{m-1}}$$

son un mismo número entero u' que satisface (5.8) y (5.9). Considerando el segundo cociente concluimos que $u' > 0$.

Las ecuaciones (5.10) y (5.11) forman un sistema de ecuaciones lineales de determinante ± 1, luego tiene solución entera v', w'.

Tomando determinantes en la ecuación matricial llegamos a que

$$uw(-1)^{n-1} = (-1)^{m-1}u'w',$$

y puesto que $m \equiv n$ (mód 2), podemos concluir que $D = uw = u'w'$. De aquí se deduce además que $w' > 0$. De (5.11) se sigue que

$$v' = \frac{wq_{n-1} - s_{m-2}w'}{sm-1} \geq -\frac{s_{m-2}}{s_{m-1}}w' \geq -w',$$

y usando además (5.9)

$$v' = \frac{wq_{n-2} - s_{m-2}w'}{s_{m-1}} \leq \frac{w}{s_{m-1}}\ q_{n-2} = \frac{u'}{q_{n-1}}\ q_{n-2} \leq u'.$$

Por el teorema 5.8 tenemos

$$\xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}.$$

Haciendo uso de esto y de las ecuaciones que definen a u', v', w' llegamos a que

$$\begin{aligned} \eta &= \frac{u\xi + v}{w} = \frac{(up_{n-1} + vq_{n-1})\xi_n + (up_{n-2} + vq_{n-2})}{w(q_{n-1}\xi_n + q_{n-2})}\\ &= \frac{r_{m-1}u'\xi_n + r_{m-1}v' + r_{m-2}w'}{s_{m-1}u'\xi_n + s_{m-1}v's_{m-2}w'}, \end{aligned}$$

de donde, de acuerdo con la definición $\eta_m = (u'\xi_n + v')/w'$, se concluye

$$\eta = \frac{r_{m-1}\eta_m + r_{m-2}}{s_{m-1}\eta_m + s_{m-2}}.$$

Consecuentemente $\eta = [b_0, b_1, \ldots, b_{m-1}, \eta_m]$. ∎

Ahora observamos que en las hipótesis del teorema anterior se cumple

$$\eta_m = (u'\xi_n + v')/w' > v'/w' \geq -1.$$

Más aún, si $a_n \geq D$, teniendo en cuenta que a_n es la parte entera de ξ_n, de hecho

$$\eta_m = (u'\xi_n + v')/w' > (u'D + v')/w' \geq (u'^2 w' - w')/w' = u'^2 - 1 \geq 0,$$

y si $a_n \geq 2D$ entonces

$$\eta_m = (u'\xi_n + v')/w' > (u'2D + v')/w' \geq 2u'^2 - 1 \geq 1.$$

Esto es importante porque cuando $\eta_m > 1$, la relación

$$\eta = [b_0, b_1, \ldots, b_{m-1}, \eta_m]$$

indica que los coeficientes de la fracción continua de η_m son la prolongación del desarrollo de η en fracción continua, que comienza con $[b_0, b_1, \ldots, b_{m-1}, \ldots\ ]$.

Es fácil ver que esto sigue siendo cierto cuando $\eta_m \geq 0$ si convenimos en que

$$[\ \ldots, a, 0, b, c, \ldots\ ] = [\ \ldots, a + b, c, \ldots\ ].$$

Nuestra intención es partir de un número irracional ξ_0 y dividir su fracción continua en secciones

$$\xi_0 = [a_0, \ldots, a_{n_1-1} \mid a_{n_1}, \ldots, a_{n_2-1} \mid a_{n_2}, \ldots, a_{n_3-1} \mid a_{n_3}, \ldots\ ],$$

a las que aplicar sucesivamente el teorema anterior.

Dado $\eta_0 = (u_0\xi_0 + v_0)/w_0$ tal que $u_0, w_0 > 0$ y $D = u_0 w_0 > 1$, el teorema nos da números u_1, v_1, w_1 en las mismas condiciones (con el mismo D) y $b_0, \ldots, b_{m_1-1}$ tales que

$$\eta_0 = [b_0, \ldots, b_{m_1-1}, \eta_{m_1}] \quad \text{con} \quad \eta_{m_1} = (u_1\xi_{n_1} + v_1)/w_1.$$

Ahora aplicamos el teorema a $\xi_{n_1} = [a_{n_1}, \ldots, a_{n_2} - 1 \mid a_{n_2}, \ldots, a_{n_3-1} \mid a_{n_3}, \ldots\ ]$ y obtenemos números u_2, v_2, w_2 con el mismo D y $b_{m_1}, \ldots, b_{m_2-1}$ tales que

$$\eta_{m_1} = [b_{m_1}, \ldots, b_{m_2-1}, h_{m_2}] \quad \text{con} \quad \eta_{m_2} = (u_2\xi_{n_1} + v_2)/w_2.$$

Suponiendo que $b_{m_1} \geq 0$ podemos enlazar ambos pasos y escribir

$$\eta_0 = [b_0, \ldots, b_{m_1-1}, \eta_{m_1}] = [b_0, \ldots, b_{m_1-1} \mid b_{m_1}, \ldots, b_{m_2-1}, \eta_{m_2}].$$

A continuación aplicamos el teorema a ξ_{n_2}, y así sucesivamente. De este modo vamos obteniendo el desarrollo en fracción continua de η_0, suponiendo que los sucesivos b_{m_i} que vamos obteniendo no sean negativos. Una forma de garantizarlo es partir la fracción original de modo que cada $a_{n_i} \geq D$, aunque no es necesario.

Con la ayuda del teorema siguiente podremos garantizar que, con las hipótesis adecuadas, al cabo de un número finito de pasos entraremos en un ciclo que nos dará una fórmula general para el desarrollo completo de η_0. Al mismo tiempo nos dará una técnica útil para simplificar los cálculos.

Teorema 5.15 *En las hipótesis del teorema 5.14, si sustituimos a_0 por otro número congruente módulo D, digamos $a_0 + Dg$ (pero mantenemos los mismos $a_1, \dots, a_{n-1}$) entonces se obtienen los mismos números u', v', w', así como los mismos m y $b_1, \dots, b_{m-1}$. El número b_0 se transforma en $b_0 + u^2 g$.*

DEMOSTRACIÓN: Claramente

$$\begin{aligned}\frac{u[a_0 + Dg, a_1, \dots, a_{n-1}] + v}{w} &= \frac{u[a_0, a_1, \dots, a_{n-1}] + v}{w} + \frac{uDg}{w}\\ &= \frac{u[a_0, a_1, \dots, a_{n-1}] + v}{w} + u^2 g.\end{aligned}$$

Según el teorema 5.14 el desarrollo de este número es $[b_0, b_1, \dots, b_{m-1}]$, luego es inmediato que con el cambio todos los coeficientes quedan igual salvo el primero que se incrementa en $u^2 g$.

Las relaciones recurrentes que determinan los denominadores de los convergentes no dependen del primer término de la fracción continua, luego los números q_i y s_i permanecen invariantes.

La fórmula (5.9) nos da que u' tampoco varía. Como $u'w' = D$, también w' permanece inalterado. Por último, la ecuación (5.11) garantiza la conservación de v'. ∎

Con esto tenemos en realidad un método general para calcular las fracciones continuas de números η_0 a partir de números ξ_0, pero explicaremos mejor este método aplicándolo al caso que nos interesa. Digamos sólo en general que si aplicamos sucesivamente el teorema 5.14, las ternas (u_i, v_i, w_i) que vamos obteniendo varían en un conjunto finito (a causa de las restricciones que impone el teorema), luego después de un número finito de pasos volveremos a la misma terna.

Recordemos que si $\xi_0 = (e^{2/m} + 1)/2$ habíamos calculado

$$\xi_0 = [1, m - 1, 3m, 5m, \dots\ ]$$

y que $\eta_0 = e^{2/m} = 2\xi_0 - 1$. En este caso $u = 2$, $v = -1$, $w = 1$. Como $D = 2$, para obtener congruencias módulo 2 haremos $m = 2t$ (y después estudiaremos el caso $m = 2t + 1$). Dividimos la fracción de este modo:

$$\xi_0 = [1 \mid 2t - 1 \mid 6t \mid 10t \mid 14t \mid \dots\ ].$$

Vamos a aplicar el teorema 5.14 a cada segmento. El teorema 5.15 nos dice que podemos sustituir cada coeficiente por otro congruente módulo 2. Por ejemplo podemos considerar

$$\xi_0^* = [1 \mid 1 \mid 0 \mid 0 \mid 0 \mid \dots\ ].$$

Ciertamente esto no tiene sentido como fracción continua, pero los cálculos a realizar sí lo tienen porque cada uno de ellos sólo involucra a un segmento, es decir a una fracción [1] o [0] que sí es correcta. Al hacer los cálculos obtendremos para cada segmento unos coeficientes $\mid b_{m_i}, \dots, b_{m_{i+1}} - 1 \mid$, que serán

los que buscamos salvo el primero. A estos primeros coeficientes tendremos que sumarles las cantidades 0, $u_1^2(t-1)$, $u_2^2\,3t$, $u_3^2\,5t$, ...

Aplicamos el teorema 5.14 al primer segmento:

$$\frac{1[1]-1}{1} = 1 = [1] = [b_0], \quad m = 1.$$

$$\begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} r_0 & r_{-1} \\ s_0 & s_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} u_0 & v_0 \\ 0 & w_0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}.$$

La ecuación matricial es

$$\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} u_1 & v_1 \\ 0 & w_1 \end{pmatrix},$$

y la solución:

$$\begin{pmatrix} u_1 & v_1 \\ 0 & w_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Ahora aplicamos el teorema al segundo segmento [1]:

$$\frac{1[1]+0}{1} = \frac{1}{2} = [0,1,1] = [b_2, b_3, b_4],$$

donde hemos tomado el desarrollo con tres cifras para que la longitud sea impar, como la de [1]. Ahora

$$\begin{pmatrix} r_2 & r_1 \\ s_2 & s_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} u_2 & v_2 \\ 0 & w_2 \end{pmatrix},$$

de donde

$$\begin{pmatrix} u_2 & v_2 \\ 0 & w_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$$

Sólo hay que rectificar el valor de b_2, que en realidad es $u_1^2(t-1) = t-1 \geq 0$, luego por ahora tenemos que $\eta_0 = [1 \mid t-1, 1, 1 \mid \ldots\ ]$.

La siguiente aplicación del teorema es al segmento [0]:

$$\frac{1[0]-1}{2} = -\frac{1}{2} = [-1,1,1] = [b_5, b_6, b_7].$$

$$\begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} u_3 & v_3 \\ 0 & w_3 \end{pmatrix},$$

y esta vez llegamos a que

$$\begin{pmatrix} u_3 & v_3 \\ 0 & w_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} u_2 & v_2 \\ 0 & w_2 \end{pmatrix},$$

El valor corregido de b_5 es $b_5 = -1 + u_2^2\, 3t = 3t - 1 \geq 0$.

Tenemos, pues, que $\eta_0 = [1 \mid t-1, 1, 1 \mid 3t-1, 1, 1 \mid \dots\ ]$.

Ahora bien, para los cálculos relativos al cuarto segmento partimos exactamente de los mismos datos que para el tercero (la fracción [0] y la terna $(u_3, v_3, w_3) = (1, -1, 2)$), luego llegaremos exactamente a los mismos coeficientes $[-1, 1, 1]$, y otra vez a la misma terna. Lo único que cambiará será la corrección del primer coeficiente, que ahora será $5t$, y después $7t$, etc., dando lugar siempre a coeficientes mayores que 0.

Consecuentemente tenemos la fracción continua de η_0, que no es sino

$$\eta_0 = [1, t-1, 1, 1, 3t-1, 1, 1, 5t-1, 1, 1, 7t-1, 1, 1, \dots\ ],$$

o más brevemente:

$$\sqrt[t]{e} = \eta_0 = [\overline{1, (2k+1)t-1, 1}]_{k=0}^{\infty}.$$

En el caso $t = 1$ aparece un cero que debe ser cancelado:

$$e = [1, 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, \dots\ ] = [2, 1, 2, 1, 1, 4, 1, 1, 6, \dots\ ],$$

así, $e = [2, \overline{1, 2k, 1}]_{k=0}^{\infty}$.

En general, este método puede ser aplicado siempre que la fracción continua de ξ_0 pueda ser dividida en segmentos que (por lo menos desde uno dado en adelante) tengan todos la misma longitud y los mismos términos, salvo quizá el primero, y de modo que los primeros términos de cada segmento sean mayores o iguales que D (para que los coeficientes que obtenemos puedan ser enlazados) y congruentes módulo D (para que podamos reducirlos a constantes por el teorema 5.15 y así llegar a un ciclo como ha ocurrido en el ejemplo).

Otra aplicación la tenemos cuando hacemos $m = 2t + 1$ en la expresión original. Entonces queda

$$\xi_0 = [1 \mid 2t \mid 6t+3 \mid 10t+5 \mid 14t+7 \mid \dots\ ],$$

y con este método podemos calcular la fracción continua de $e^{2/(2t+1)}$. Para ello reducimos módulo 2 a la fracción $\xi_0^* = [1 \mid 0 \mid 1 \mid 1 \mid 1 \mid \dots\ ]$.

Esta vez se obtienen las ternas

$$(2, -1, 1), \quad (1, 0, 2), \quad (2, 0, 1), \quad (1, 0, 2), \quad (1, -1, 2), \quad (2, 0, 1).$$

La primera repetición $(u_1, v_1, w_1) = (u_3, v_3, w_3)$ no es significativa, pues los primeros (y únicos) coeficientes de los segmentos primero y tercero son [0] y [1] respectivamente, luego no son congruentes y por lo tanto no podemos garantizar que comience un ciclo (y de hecho no comienza).

En cambio la repetición $(u_5, v_5, w_5) = (u_2, v_2, w_2)$ sí cierra el proceso. La fracción que se obtiene es

$$\eta_0^* = [1 \mid 0 \mid 2 \mid 0, 1, 1 \mid 0 \mid 2 \mid 0, 1, 1 \mid 0 \mid 2 \mid 0, 1, 1 \mid 0 \mid 2 \mid 0, 1, 1 \mid \dots\ ]$$

Para corregir los primeros coeficientes observamos que al pasar de ξ_0 a ξ_0^* hemos restado $2\cdot 0$, $2t$, $2(t+1)$, $2(5t+2)$, $2(7t+3)$, ... así como que los valores de u_i son $2,1,2,1,1,2,1,1,2,1,1,2,\ldots$

Por lo tanto ahora hemos de sumar

$$0,\ t,\ 4(t+1),\ 5t+2,\ 7t+3,\ 4(9t+5),\ 11t+7,\ 13t+9,\ 4(15t+11),\ \ldots$$

Omitimos los detalles, pero no es difícil llegar a que la expresión final es

$$\begin{aligned} e^{2/(2t+1)} &= [1, \overline{(1+6k)t+3k, (12+24k)t+6+12k, (5+6k)t+2+3k, 1, 1}] \\ &= \overline{[1, (1+6k)t+3k, (12+24k)t+6+12k, (5+6k)t+2+3k, 1]}_{k=0}^{\infty}. \end{aligned}$$

La fórmula se simplifica bastante en el caso $t=0$, que nos da

$$\begin{aligned} e^2 &= \overline{[1, 3k, 6+12k, 2+3k, 1]}_{k=0}^{\infty} = [1, 0, 6, \overline{2+3k, 1, 1, 3+3k, 18+12k}]_{k=0}^{\infty} \\ &= [7, \overline{2+3k, 1, 1, 3+3k, 18+12k}]_{k=0}^{\infty} \end{aligned}$$

Explícitamente:

$$e^2 = [7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, 1, 1, 9, 42, 11, 1, 1, 12, 54, \ldots\ ].$$

■

Capítulo VI

Cuerpos cuadráticos

En los cuerpos cuadráticos, toda la sutileza de la teoría algebraica de números se muestra de la forma más simple posible. Esto los convierte en los modelos idóneos para formular conjeturas y obtener primeras pruebas. Ciertamente, los resultados más importantes de la teoría algebraica de números han seguido este proceso: primero fueron probados para cuerpos cuadráticos y sólo en una segunda etapa fueron generalizados. Este proceso de generalización es a menudo complicado y suele requerir ideas esencialmente nuevas. Tanto es así que aún hoy existen hechos sobre cuerpos cuadráticos que plausiblemente deberían corresponderse con hechos generales sin que tan siquiera se sepa cómo abordar el problema de formularlos adecuadamente.

Los resultados fundamentales que hemos probado hasta ahora (finitud del número de clases, cálculo de unidades fundamentales, etc) fueron obtenidos por Gauss en el caso cuadrático, aunque en términos muy diferentes a los que nosotros hemos empleado. La teoría de Gauss trata sobre formas cuadráticas binarias, pero es equivalente a la teoría de cuerpos cuadráticos debido a que la relación entre módulos y formas que hemos estudiado puede refinarse en el caso cuadrático hasta tal punto que permite traducir fielmente cualquier hecho sobre formas a un hecho análogo sobre módulos y viceversa.

Sin embargo, hay un sentido en el que ambos enfoques no son equivalentes, y es que mientras la mayor parte de la teoría resulta más natural en términos de módulos, lo cierto es que hay algunos conceptos de gran importancia teórica que resultan completamente naturales en términos de formas y sin embargo hace falta profundizar mucho en la teoría para comprender completamente su sentido en términos de módulos. Por ello resulta enriquecedor conocer ambos planteamientos y la relación entre ambos. En este capítulo nos limitaremos a exponer la parte de la teoría de Gauss sobre formas cuadráticas que se corresponde con la teoría que ya conocemos, a la vez que mostraremos las simplificaciones de la teoría general aplicada al caso cuadrático. Esto nos servirá de preparativo para desarrollar en capítulos posteriores el resto de dicha teoría, cuya generalización ha constituido uno de los problemas centrales de la teoría desde la época de Gauss hasta mediados del presente siglo.

6.1 Formas cuadráticas binarias

Definición 6.1 Una *forma cuadrática* (binaria) es un polinomio de la forma $f(x,y) = ax^2 + bxy + cy^2$, donde a, b, c son enteros racionales no todos nulos.

En lo sucesivo, y mientras no se indique lo contrario, cuando hablemos de una forma $f(x,y)$ entenderemos que a, b, c son sus coeficientes de acuerdo con la fórmula anterior. Vamos a introducir algunos conceptos básicos sobre formas cuadráticas.

En primer lugar recordemos de 1.4 que dos formas cuadráticas $f(x,y)$ y $g(x,y)$ son *equivalentes* si $f(x,y) = g(px+qy, rx+sy)$, donde p, q, r, s son enteros racionales tales que $ps-qr = \pm 1$. En tal caso las soluciones enteras de la ecuación $f(x,y) = t$ están en correspondencia biunívoca con las de la ecuación $g(x,y) = t$.

Esto se expresa mejor con notación matricial. La forma $f(x,y)$ se puede representar matricialmente como

$$f(x,y) = (x,y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

de modo que si una forma f tiene matriz A y otra forma g tiene matriz B, entonces f y g son equivalentes si y sólo si existe una matriz C con coeficientes enteros racionales y determinante ± 1 tal que $A = CBC^t$.

Determinante y discriminante En particular notamos que el *determinante* de f, esto es, el número $|B| = ac - b^2/4$ es invariante por equivalencia. El *discriminante* de f se define como el entero racional $b^2 - 4ac$. Puesto que no es más que -4 veces el determinante, también es invariante por equivalencia.

Formas completas Todas las formas cuadráticas se descomponen en producto de dos formas lineales. Dada una forma $f(x,y)$, si se cumple $a = c = 0$ la factorización es obvia. Supongamos ahora que $a \neq 0$. Entonces consideramos el polinomio $f(x,1) = ax^2+bx+c = a(x+\alpha)(x+\beta)$ y encontramos la factorización

$$f(x,y) = a(x+\alpha y)(x+\beta y).$$

Observar que α y β son $\big(b \pm \sqrt{D}\,\big)/2a$, donde D es el discriminante de f. Si D es cuadrado perfecto, el polinomio ax^2+bx+c es se descompone en factores lineales en $\mathbb{Q}[x]$, luego también en $\mathbb{Z}[x]$, y así la forma $f(x,y)$ se descompone en factores lineales en $\mathbb{Z}[x,y]$. Por el contrario, si D no es cuadrado perfecto, entonces $D = m^2 d$ para ciertos enteros racionales m, d, con d libre de cuadrados, luego α y β son elementos conjugados del cuerpo $\mathbb{Q}\big(\sqrt{d}\,\big)$, y la factorización puede expresarse como $f(x,y) = a\,\mathrm{N}(x+\alpha y)$. En los términos del capítulo II esto significa que la forma $f(x,y)$ es (salvo una constante) una forma completa.

En el caso $a = c = 0$ se cumple que $D = b^2$ es cuadrado perfecto y por otro lado la forma también factoriza en $\mathbb{Z}[x,y]$, luego concluimos que una forma cuadrática factoriza en $\mathbb{Z}[x,y]$ si y sólo si su discriminante es cuadrado perfecto

y, puesto que las formas completas son irreducibles en $\mathbb{Q}[x,y]$, una forma es completa (salvo una constante) si y sólo si su discriminante no es cuadrado perfecto. En lo sucesivo sólo consideraremos formas cuadráticas completas.

Signo El discriminante de una forma cuadrática determina su signo en el sentido siguiente: Si $f(x,y)$ tiene determinante D, entonces

$$4af(x,y) = (2ax+by)^2 - Dy^2,$$

luego si $D<0$ el signo de $f(x,y)$ es igual al signo de a para todos los valores de x e y, mientras que si $D>0$ la forma toma valores tanto positivos como negativos.

De acuerdo con esto, diremos que $f(x,y)$ es *definida positiva* si $f(x,y)>0$ para todo par $(x,y)\neq(0,0)$, lo cual ocurre cuando $D<0$, $a>0$.

Diremos que $f(x,y)$ es *definida negativa* si $f(x,y)<0$ cuando $(x,y)\neq(0,0)$, lo cual ocurre si $D<0$, $a<0$.

Y en otro caso, es decir, si $D>0$, diremos que la forma es *indefinida.*

Observar que si $D<0$, una forma definida negativa se transforma en definida positiva (con el mismo discriminante) cambiando el signo a sus coeficientes, por lo cual en la mayoría de los casos no será restricción el trabajar sólo con formas definidas positivas.

Por otro lado es obvio que si dos formas están relacionadas por un cambio de variables entonces una toma sólo valores positivos si y sólo si lo mismo le ocurre a la otra, es decir, dos formas equivalentes son ambas definidas positivas, ambas definidas negativas o ambas indefinidas.

Formas principales El discriminante $D=b^2-4ac$ de una forma cuadrática no puede ser cualquier número, sino que cumple $D\equiv 0 \pmod 4$ si b es par y $D\equiv 1 \pmod 4$ si b es impar.

Si un entero racional D cumple estas condiciones siempre existen formas cuadráticas de discriminante D. La más sencilla de todas recibe el nombre de *forma principal* de discriminante D, definida como $x^2-\frac{D}{4}y^2$ si $D\equiv 0 \pmod 4$ y $x^2+xy+\frac{1-D}{4}y^2$ si $D\equiv 1 \pmod 4$. Las formas principales están determinadas por las condiciones $a=1$ y $b=0$ o 1, según sea el resto de D.

Módulos A continuación vamos a refinar la relación que ya conocemos en general entre formas y módulos. Según vimos en el capítulo II, a cada base de un módulo completo le sabemos asociar una forma con coeficientes racionales. Como ahora estamos trabajando con coeficientes enteros, multiplicaremos la forma por el entero adecuado para que los coeficientes resulten enteros. La forma resultante será única si exigimos que sus coeficientes a,b,c sean primos entre sí.

Las formas cuadráticas con coeficientes primos entre sí se llaman formas *primitivas.*

La forma explícita de asignar a cada base de un módulo completo su forma primitiva resulta ser muy sencilla. Para obtenerla probamos primero un resultado auxiliar:

Teorema 6.2 *Sea γ una raíz irracional de un polinomio ax^2+bx+c con coeficientes enteros racionales primos entre sí, $a>0$. Entonces el anillo de coeficientes del módulo $\langle 1,\gamma\rangle$ es $\langle 1, a\gamma\rangle$, el discriminante de este orden es b^2-4ac y la norma del módulo es $1/a$.*

Demostración: El número γ pertenecerá a un cuerpo cuadrático $\mathbb{Q}\big(\sqrt{d}\,\big)$. Todo elemento de $\mathbb{Q}\big(\sqrt{d}\,\big)$ es de la forma $\delta = x+y\gamma$, donde x e y son números racionales. Se cumplirá $\delta\,\langle 1,\gamma\rangle \subset \langle 1,\gamma\rangle$ si y sólo si $\delta \in \langle 1,\gamma\rangle$ y

$$\delta\gamma = x\gamma + y\gamma^2 = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\gamma \in \langle 1,\gamma\rangle\,.$$

O sea, δ es un coeficiente de $\langle 1,\gamma\rangle$ si y sólo si x, y, cy/a, by/a son enteros. Puesto que $(a,b,c)=1$, esto ocurre si y sólo si x e y son enteros y $a \mid y$.

Ahora es fácil calcular la matriz de cambio de base de $(1,\gamma)$ a $(1,a\gamma)$, y concluir que la norma de $\langle 1,\gamma\rangle$ es $1/a$.

El discriminante del orden es

$$\begin{vmatrix} 1 & a\gamma \\ 1 & a\bar\gamma \end{vmatrix}^2 = a(a\gamma^2 + a\bar\gamma^2 - 2a\gamma\bar\gamma) = a(-b\gamma - c) + a(-b\bar\gamma - c) - 2ac$$

$$= -ab(\gamma+\bar\gamma) - 2ac - 2ac = b^2 - 4ac.$$

■

Sea ahora (α,β) una base (ordenada) de un módulo M de un cierto cuerpo cuadrático $\mathbb{Q}\big(\sqrt{d}\,\big)$. A esta base le asociamos la forma cuadrática

$$f(x,y) = \frac{\mathrm{N}(\alpha x+\beta y)}{\mathrm{N}(M)} = ax^2+bxy+cy^2. \tag{6.1}$$

Vamos a probar que los coeficientes a, b, c son enteros primos entre sí. Llamemos $\gamma = -\beta/\alpha$. Entonces γ es raíz de un único polinomio Ax^2+Bx+C con coeficientes enteros racionales tales que $(A,B,C)=1$ y $A>0$. Así

$$A\left(x+\frac{\beta}{\alpha}\right)\left(x+\frac{\bar\beta}{\bar\alpha}\right) = Ax^2+Bx+C,$$

luego

$$\frac{A}{\mathrm{N}(\alpha)}(x\alpha+\beta)(x\bar\alpha+\bar\beta) = Ax^2+Bx+C,$$

de donde

$$\mathrm{N}(\alpha x+\beta y) = \frac{\mathrm{N}(\alpha)}{A}(Ax^2+Bxy+Cy^2).$$

Por el teorema anterior, la norma de $M = \langle \alpha, \beta \rangle = \alpha \langle 1, \gamma \rangle$ es $|\,\mathrm{N}(\alpha)|/A$, y por consiguiente

$$ax^2 + bxy + cy^2 = \mathrm{N}(\alpha x + \beta y)/\,\mathrm{N}(M) = \pm(Ax^2 + Bxy + Cy^2),$$

luego la forma que le hemos asignado a la base (α, β) según (6.1) es primitiva.

Más aún, el anillo de coeficientes de $M = \langle \alpha, \beta \rangle$ es el mismo que el de $\langle 1, \gamma \rangle$, es decir, el orden $\langle 1, A\gamma \rangle$, y, por el teorema anterior, su discriminante es $B^2 - 4AC = b^2 - 4ac$. Esto significa que el discriminante del anillo de coeficientes de M es el mismo que el de la forma cuadrática asociada.

Observamos además que $a = \mathrm{N}(\alpha)/\,\mathrm{N}(M)$, y por lo tanto si el discriminante es negativo, o sea, si el cuerpo es imaginario, entonces $a > 0$, luego la forma es definida positiva. En resumen:

Teorema 6.3 *Para cada base ordenada (α, β) del módulo M, la forma cuadrática $f(x, y) = \mathrm{N}(\alpha x + \beta y)/\,\mathrm{N}(M)$ tiene coeficientes enteros, es primitiva, tiene el mismo discriminante que el anillo de coeficientes de M y es definida positiva cuando dicho discriminante es negativo.*

Es fácil comprobar que, como ya observamos en el capítulo II las formas asociadas a dos bases de un módulo M son equivalentes, y los coeficientes del cambio de variables son los mismos que los del cambio de base. En particular el determinante del cambio de variables es el mismo que el determinante del cambio de base. Esto significa que a cada módulo M le asignamos una clase de equivalencia de formas. Al variar la base de M recorremos todas las formas de la clase.

También comentamos en el capítulo II que si M tiene asociada una forma f, entonces un módulo similar γM tiene asociada la forma $\mathrm{N}(\gamma)f$. Sin embargo, como ahora hemos modificado la correspondencia para trabajar sólo con formas primitivas, la relación se simplifica:

Si $\gamma \neq 0$, y f es la forma asociada a la base (α, β) de M, la forma asociada a la base $(\gamma\alpha, \gamma\beta)$ de γM es

$$\frac{\mathrm{N}(\gamma\alpha x + \gamma\beta y)}{\mathrm{N}(\gamma M)} = \frac{\mathrm{N}(\gamma)\,\mathrm{N}(\alpha x + \beta y)}{|\,\mathrm{N}(\gamma)|\,\mathrm{N}(M)} = \pm f(x, y),$$

donde el signo es el de $\mathrm{N}(\gamma)$.

Así, si la clase asociada a M es $[f]$, la clase asociada a γM es $[\pm f]$. Cuando $\mathrm{N}(\gamma) > 0$ ambas clases son la misma, pero si $\mathrm{N}(\gamma) < 0$ las formas f y $-f$ no son necesariamente equivalentes. En los cuerpos imaginarios, donde la norma siempre es positiva, esto nos permite asociar a cada clase de similitud de módulos una clase de equivalencia de formas, pero en los cuerpos reales puede haber clases de similitud a las que correspondan dos clases de equivalencia.

Por otra parte, la correspondencia de módulos a clases de formas (primitivas no definidas negativas) es siempre suprayectiva. En efecto, hemos visto que toda forma factoriza como $f(x, y) = a\,\mathrm{N}(x + \alpha y)$, luego la forma asociada al módulo $M = \langle 1, \alpha \rangle$ se diferencia de f en el factor $a\,\mathrm{N}(M)$. Como ambas formas

son primitivas el factor ha de ser ± 1, concretamente el signo de a. Si $a > 0$ nos sirve el módulo M. Si $a < 0$ el discriminante ha de ser positivo (o la forma sería definida negativa), luego existe un número γ de norma negativa y nos sirve el módulo γM.

La correspondencia de módulos a clases de formas no es inyectiva por razones obvias, desde el momento en que módulos similares M y γM con $\mathrm{N}(\gamma) > 0$ tienen asociada la misma clase, pero la situación es peor, en el sentido de que puede haber también módulos no similares cuya clase asociada sea la misma. Veamos en qué condiciones esto es posible:

Supongamos que a dos módulos M y M' les corresponde la misma clase de formas. Escogiendo oportunamente las bases podemos suponer que $M = \langle \alpha, \beta \rangle$, $M' = \langle \alpha', \beta' \rangle$ y que la forma asociada a ambas bases es la misma. En la prueba del teorema 6.3 hemos visto que $\gamma = -\beta/\alpha$ y $\gamma' = -\beta'/\alpha'$ son raíces del mismo polinomio, luego son iguales o conjugados. Puesto que M y M' son similares, respectivamente, a $\langle 1, \gamma \rangle$ y $\langle 1, \gamma' \rangle$, concluimos que M es similar a M' o bien a su conjugado.

Esto es todo lo que podemos decir: si dos módulos son conjugados, la forma que les asignamos es la misma, y más adelante veremos ejemplos de módulos no similares a sus conjugados, con lo que una misma clase de formas se corresponde a veces con módulos no similares. En cualquier caso, una clase de formas nunca se corresponde con más de dos clases de módulos similares.

En resumen tenemos que una clase de módulos similares puede corresponderse con dos clases de formas y que una clase de formas puede corresponderse con dos clases de módulos similares. Esta situación tan poco satisfactoria se puede arreglar completamente si refinamos las relaciones de equivalencia que estamos considerando. Nos ocupamos de ello seguidamente.

6.2 Equivalencia y similitud estricta

Definición 6.4 Dos formas cuadráticas son *estrictamente equivalentes* si son equivalentes mediante un cambio de variables de determinante $+1$. Dos módulos M y N de un cuerpo cuadrático son *estrictamente similares* si $M = \alpha N$ para un cierto número α de norma positiva.

Observar que dos formas que se diferencien en un cambio de variables de discriminante negativo pueden ser pese a ello estrictamente equivalentes. Por ejemplo, si una forma cumple $a = c$, entonces el cambio $x = y$, $y = x$ produce el mismo efecto (ninguno) que el cambio $x = x$, $y = y$.

También puede que dos formas sean equivalentes pero no estrictamente equivalentes, en cuyo caso su clase de equivalencia se parte en dos clases de equivalencia estricta.

Lo mismo sucede con la similitud estricta de módulos, aunque aquí podemos precisar un poco más:

Si el discriminante de un orden es negativo (el cuerpo es imaginario) todas las normas son positivas, luego la similitud coincide con la similitud estricta sobre los módulos de dicho orden.

Si el discriminante es positivo, entonces la similitud coincide con la similitud estricta en los módulos del orden si y sólo si su unidad fundamental tiene norma negativa.

En efecto, si ϵ es una unidad de norma negativa y tenemos $M = \alpha N$ con $\mathrm{N}(\alpha) < 0$, entonces también $M = \epsilon M = \epsilon\alpha N$, luego la similitud coincide con la similitud estricta.

Recíprocamente, si α es cualquier número que cumpla $\mathrm{N}(\alpha) < 0$ y M es cualquier módulo del orden considerado, los módulos M y αM han de ser estrictamente similares, luego existe un β de norma positiva de manera que $\beta M = \alpha M$, luego $(\alpha/\beta)M = M$ y por lo tanto $\mathrm{N}(M) = |\mathrm{N}(\alpha/\beta)|\,\mathrm{N}(M)$, de donde $|\mathrm{N}(\alpha/\beta)| = 1$ y, dados los signos de las normas de α y β, ha de ser $\mathrm{N}(\alpha/\beta) = -1$. Claramente α/β es una unidad del orden de M y si una unidad tiene norma -1 la unidad fundamental también.

Así pues, la similitud y la similitud estricta sólo difieren en los módulos cuyos órdenes tienen unidades fundamentales de norma 1, y en este caso todas las clases de similitud de módulos se dividen en dos clases de similitud estricta.

Finalmente vamos a refinar la correspondencia entre módulos y formas que hemos descrito en la sección anterior de manera que induzca una biyección entre clases de equivalencia y similitud estrictas.

Definición 6.5 Una base (α, β) de un módulo M de un cuerpo cuadrático $\mathbb{Q}(\sqrt{d}\,)$ está *orientada* si el determinante

$$\Delta = \begin{vmatrix} \bar{\alpha} & \bar{\beta} \\ \alpha & \beta \end{vmatrix},$$

cumple $\Delta > 0$ para $d > 0$ y $\Delta/i > 0$ para $d < 0$ (la barra indica la conjugación compleja).

Más explícitamente, si $\alpha = p + q\sqrt{d}$ y $\beta = r + s\sqrt{d}$, entonces

$$\Delta = 2(ps - qr)\sqrt{d},$$

luego la orientación de la base (α, β) según la definición anterior equivale a que su orientación es la misma que la de la base $(1, \sqrt{d})$ en el sentido usual en espacios vectoriales. Los siguientes hechos se comprueban sin dificultad:

1. Si (α, β) no está orientada, entonces (β, α) sí lo está.
2. Si (α, β) está orientada, entonces $(\bar{\beta}, \bar{\alpha})$ también lo está.
3. Si (α, β) está orientada, entonces $(\gamma\alpha, \gamma\beta)$ lo está si y sólo si $\mathrm{N}(\gamma) > 0$.
4. Un cambio de base conserva la orientación si y sólo si su determinante es positivo.

Como consecuencia, si recorremos las bases orientadas de un módulo M, las formas asociadas recorren una clase de equivalencia estricta. A módulos estrictamente similares les corresponde la misma clase de equivalencia estricta de formas.

Tenemos, pues, una correspondencia que a cada clase de equivalencia estricta de módulos le asigna una clase de equivalencia estricta de formas (las asociadas a las bases orientadas de los módulos de la clase). Esta correspondencia sigue siendo suprayectiva (considerando sólo formas primitivas no definidas negativas), pues si a una forma $f(x,y)$ le corresponde una base (α,β) y ésta no está orientada, podemos tomar la base $(\bar\alpha,\bar\beta)$, que da la misma forma y sí está orientada.

Vamos a ver que también es inyectiva. Sean M y M' dos módulos que tengan asignada la misma clase de formas. Escogiendo adecuadamente las bases podemos suponer que $M=\langle\alpha,\beta\rangle$, $M'=\langle\alpha',\beta'\rangle$ y que la forma asociada a ambas bases es la misma.

En la prueba del teorema 6.3 hemos visto que $\mathrm{N}(\alpha)$ tiene el mismo signo que el coeficiente de x^2 y lo mismo vale para la otra, luego $\mathrm{N}(\alpha)$ y $\mathrm{N}(\alpha')$ tienen el mismo signo. Por consiguiente las bases $(1,\beta/\alpha)$ y $(1,\beta'/\alpha')$ están ambas orientadas o ninguna lo está, según el signo de $\mathrm{N}(\alpha)$. Pero sabemos que β/α y β'/α' son iguales o conjugados, y no pueden ser conjugados porque la conjugación invierte la orientación, así que son iguales. De aquí se sigue que $M=\alpha\,\langle 1,\beta/\alpha\rangle=\alpha\,\langle 1,\beta'/\alpha'\rangle\,(\alpha/\alpha')M'$, luego M y M' son estrictamente similares.

Vamos a reflexionar sobre cómo las relaciones estrictas resuelven los problemas que nos aparecían con las relaciones no estrictas. Consideremos primeramente el caso de los cuerpo reales, donde la situación era peor. Dado un módulo M podemos considerar las clases estrictas $[M]$, $[\overline{M}]$, $[-M]$ y $-[\overline{M}]$, donde $\overline{M}$ es el módulo conjugado de M y $-[M]$ representa a la clase de similitud estricta de los módulos γM con $\mathrm{N}(\gamma)<0$.

Estas clases no son necesariamente distintas. Puede ocurrir que $M=\overline{M}$ (por ejemplo si en un cuerpo cuadrático un primo factoriza como $p=\mathfrak{p}^2$, entonces $M=\mathfrak{p}$ es su propio conjugado) y puede ocurrir $[M]=-[M]$ (esto ocurre exactamente cuando hay unidades de norma negativa). Por lo tanto tenemos una, dos o cuatro clases estrictas.

Si a M le corresponde la forma $f(x,y)=ax^2+bxy+cy^2$, entonces a $\overline{M}$ le corresponde $f(y,x)$ (porque al conjugar se invierte la orientación y hay que cambiar el orden de la base), mientras que, según hemos probado, a $-M$ le corresponde la forma $-f(x,y)$. Por simple estética podemos transformar $f(y,x)$ mediante el cambio $x=-y$, $y=x$ y considerar la forma estrictamente equivalente $ax^2-bxy+cy^2$. Así, la biyección entre clases actúa como sigue:

$$\begin{aligned}
[M] &\longleftrightarrow [ax^2+bxy+cy^2]\\
[\overline{M}] &\longleftrightarrow [ax^2-bxy+cy^2]\\
-[M] &\longleftrightarrow [-ax^2-bxy-cy^2]\\
-[\overline{M}] &\longleftrightarrow [-ax^2+bxy-cy^2].
\end{aligned}$$

Al considerar relaciones no estrictas la biyección se estropea, porque M es similar a $-M$ y $\overline{M}$ es similar a $-\overline{M}$, mientras que $ax^2+bxy+cy^2$ es equivalente a $ax^2-bxy+cy^2$ (mediante el cambio $x=x$, $y=-y$) y $-ax^2-bxy-cy^2$ es equivalente a $-ax^2+bxy-cy^2$.

En los cuerpos imaginarios sólo tenemos las clases $[M]$ y $[\overline{M}]$ (que pueden ser la misma o no) y las clases de formas $[ax^2+bxy+cy^2]$, $[ax^2-bxy+cy^2]$ (las dos restantes las eliminamos por definición). Aquí el problema es más simple: las clases de formas se convierten en la misma al considerar la equivalencia no estricta, mientras que las clases de módulos pueden seguir siendo distintas.

Es importante recordar, pues, que módulos estrictamente similares se corresponden con formas estrictamente equivalentes y viceversa, pero que esto es falso si consideramos relaciones no estrictas.

6.3 Grupos de clases

Vamos a definir un producto de módulos que induzca una estructura de grupo en los conjuntos de clases de similitud estricta y no estricta de los módulos de un orden cuadrático dado. En el caso de la similitud no estricta veremos que el grupo así obtenido es el mismo grupo de clases que definimos en 4.16.

Definición 6.6 Sean M y M' dos módulos completos de un cuerpo cuadrático. Elijamos dos bases $M=\langle\alpha,\beta\rangle$, $M'=\langle\alpha',\beta'\rangle$. Llamaremos *módulo producto* al módulo

$$MM'=\langle\alpha\alpha',\alpha\beta',\beta\alpha',\beta\beta'\rangle\,.$$

La definición no depende de la elección de las bases, pues MM' es, de hecho, el módulo generado por los productos mm' con $m\in M$ y $m'\in M'$ (es fácil ver que el producto es un módulo completo). Observemos que el producto de ideales es un caso particular del producto de módulos. El producto de módulos es conmutativo y asociativo. Los hechos más importantes en torno a este producto se deducen del teorema siguiente:

Teorema 6.7 *Si M es un módulo completo con anillo de coeficientes $\mathcal{O}$ y $\overline{M}$ es su conjugado, entonces $M\overline{M}=\mathrm{N}(M)\mathcal{O}$.*

Demostración: Supongamos primero que $M=\langle1,\gamma\rangle$. Entonces, con la notación del teorema 6.2, tenemos que

$$M\overline{M}=\langle1,\gamma,\bar\gamma,\gamma\bar\gamma\rangle=\left\langle1,\gamma,-\gamma-\frac{b}{a},-\frac{c}{a}\right\rangle=\left\langle1,\gamma,\frac{b}{a},\frac{c}{a}\right\rangle=\frac{1}{a}\,\langle a,b,c,a\gamma\rangle\,.$$

Puesto que $(a,b,c)=1$, todo entero racional es combinación lineal entera de ellos, luego $M\overline{M}=(1/a)\,\langle1,a\gamma\rangle=\mathrm{N}(M)\mathcal{O}$.

Si M es un módulo arbitrario, $M=\alpha M'$, donde M' tiene la forma anterior, luego $M\overline{M}=\alpha\bar\alpha M'\overline{M}'=\mathrm{N}(\alpha)\,\mathrm{N}(M')\mathcal{O}=|\,\mathrm{N}(\alpha)|\,\mathrm{N}(M')\mathcal{O}=\mathrm{N}(M)\mathcal{O}$. ∎

De aquí se siguen varias consecuencias. En primer lugar, si M y M' son módulos de un mismo orden $\mathcal{O}$ y llamamos $\mathcal{O}'$ al anillo de coeficientes del producto MM', tenemos que

$$\mathrm{N}(MM')\mathcal{O}' = MM'\overline{MM}' = \mathrm{N}(M)\mathcal{O}\,\mathrm{N}(M')\mathcal{O} = \mathrm{N}(M)\,\mathrm{N}(M')\mathcal{O}.$$

Como dos órdenes distintos no pueden ser similares, resulta que $\mathcal{O} = \mathcal{O}'$, es decir, el producto de módulos de un orden vuelve a ser un módulo del mismo orden. Tomando ahora normas en $\mathrm{N}(MM')\mathcal{O} = \mathrm{N}(M)\,\mathrm{N}(M')\mathcal{O}$ concluimos también que $\mathrm{N}(MM') = \mathrm{N}(M)\,\mathrm{N}(M')$.

Más aún, dado un módulo cualquiera M de un orden $\mathcal{O}$, se cumple $M\mathcal{O} = M$ y el módulo $M' = \overline{M}/\,\mathrm{N}(M)$ tiene la propiedad de que $MM' = \mathcal{O}$. En resumen:

Teorema 6.8 *El conjunto de todos los módulos completos con anillo de coeficientes igual a un orden cuadrático $\mathcal{O}$ es un grupo abeliano con el producto definido en* 6.6.

Ejercicio: Probar que en un cuerpo cuadrático se cumple que $\mathcal{O}_m\mathcal{O}_{m'} = \mathcal{O}_{(m,m')}$, para todo par de números naturales no nulos m, m'.

Ejercicio: Sea $M = \langle 4, \sqrt[3]{2}, \sqrt[3]{4}\rangle$ un módulo de $\mathbb{Q}\big(\sqrt[3]{2}\big)$. Probar que su anillo de coeficientes es $\langle 1, 2\sqrt[3]{2}, 2\sqrt[3]{4}\rangle$ mientras que el de $M^2 = \langle 2, 2\sqrt[3]{2}, \sqrt[3]{4}\rangle$ es el orden maximal $\langle 1, \sqrt[3]{2}, \sqrt[3]{4}\rangle$ (donde el producto se define análogamente a 6.6).

Si $\mathcal{O}$ es un orden cuadrático, la clase de similitud (estricta) de $\mathcal{O}$ está formada por los módulos $\alpha\mathcal{O}$, donde $\alpha \neq 0$ ($\mathrm{N}(\alpha) > 0$). Claramente se trata de un subgrupo del grupo de todos los módulos de $\mathcal{O}$, y la similitud (estricta) es precisamente la congruencia módulo este subgrupo, por lo que el conjunto de clases de similitud es el grupo cociente. Estos grupos cociente se llaman *grupo de clases estrictas* y *grupo de clases no estrictas* del orden considerado.

Vamos a probar que el grupo de clases no estrictas de un orden cuadrático es el mismo definido en 4.16. Como la definición dada allí se basa en ideales, necesitaremos el teorema siguiente, que caracteriza los módulos que son ideales de su anillo de coeficientes.

Teorema 6.9 *Sea $K = \mathbb{Q}\big(\sqrt{d}\big)$ un cuerpo cuadrático. Sea $\omega = \sqrt{d}$ o bien $\omega = \big(1 + \sqrt{d}\big)/2$ según el resto de d módulo* 4. *Entonces*

1. *Si $\mathfrak{a}$ es un módulo de la forma $\mathfrak{a} = k\,\langle a, b + m\omega\rangle$, con a, b, k enteros racionales, entonces $\mathfrak{a}$ es un ideal de $\mathcal{O}_m$ si y sólo si $a \mid \mathrm{N}(b + m\omega)$.*

2. *Todo ideal de $\mathcal{O}_m$ puede expresarse de esta forma.*

3. *Si $\mathfrak{a}$ es un ideal en estas condiciones y su anillo de coeficientes es $\mathcal{O}_m$, entonces se cumple $\mathrm{N}(\mathfrak{a}) = k^2|a|$.*

DEMOSTRACIÓN: Sea $\mathfrak{a}$ un módulo completo contenido en $\mathcal{O}_m$. Sea k el mayor número natural que divida (en $\mathcal{O}_m$) a todos los elementos de $\mathfrak{a}$. Entonces $\mathfrak{a} = kM$, donde M es un módulo completo contenido en $\mathcal{O}_m$ tal que no hay ningún natural mayor que 1 que divida a todos sus elementos. Obviamente $\mathfrak{a}$ será un ideal de $\mathcal{O}_m$ si y sólo si lo es M.

Es fácil ver que M tiene una base de la forma $M = \langle a, b + cm\omega\rangle$, donde a, b, c son enteros racionales, $a > 0$. En efecto, dada una base de M, podemos sustituir una de sus componentes por la suma o resta de ambas, de manera que el coeficiente de $m\omega$ disminuya en valor absoluto. Tras un número finito de pasos deberá hacerse nulo. El número a es el menor natural no nulo contenido en M. Puesto que (a, b, c) divide a todos los elementos de M, se cumple que a, b, c son primos entre sí.

Es claro que M será un ideal de $\mathcal{O}_m$ si y sólo si $am\omega, m\omega(b + cm\omega) \in M$.

La condición $am\omega \in M$ equivale a que existan enteros racionales u y v tales que $am\omega = ua + v(b + cm\omega)$.

Operando se llega a que $v = a/c$ y a que $u = -b/c$. Consecuentemente, $am\omega \in M$ cuando y sólo cuando $c \mid a$ y $c \mid b$, pero como $(a, b, c) = 1$, esto equivale a que $c = 1$.

Admitiendo $c = 1$, la segunda condición se convierte en $m\omega(b + m\omega) \in M$, que a su vez equivale a $(m\,\mathrm{Tr}(\omega) - m\bar{\omega})(b + m\omega) \in M$ (puesto que $\mathrm{Tr}(\omega) = \omega + \bar{\omega}$).

Sumamos y restamos $-b$ y la condición equivale a

$$(-b - m\bar{\omega})(b + m\omega) + (m\,\mathrm{Tr}(\omega) + b)(b + m\omega) \in M.$$

Como el segundo sumando es un múltiplo entero de un elemento de M, está seguro en M, luego la condición se reduce a que $(b + m\bar{\omega})(b + m\omega) \in M$, o sea, $\mathrm{N}(b + m\omega) \in M$ y en definitiva a que $a \mid \mathrm{N}(b + m\omega)$.

Para probar la última afirmación podemos suponer que $\mathfrak{a} = \langle a, b + m\omega\rangle$. Notamos que $m\omega \equiv -b \pmod{\mathfrak{a}}$, luego todo elemento de $\mathcal{O}_m$ es congruente con un entero módulo $\mathfrak{a}$. Por otra parte a es el menor número natural no nulo contenido en $\mathfrak{a}$, luego $|\mathcal{O}_m/\mathfrak{a}| = a$. Si el anillo de coeficientes de $\mathfrak{a}$ es $\mathcal{O}_m$, entonces esta cantidad es precisamente $\mathrm{N}(\mathfrak{a})$. ∎

Ejercicio: Probar que si $\mathfrak{a} = k\,\langle a, b + \omega\rangle$ es un ideal del orden maximal de K en las condiciones del teorema anterior y su norma es prima con m, entonces se cumple $\mathfrak{a} \cap \mathcal{O}_m = k\,\langle a, mb + m\omega\rangle$.

Ahora probamos un resultado técnico:

Teorema 6.10 *Si $ax^2 + bxy + cy^2$ es una forma cuadrática primitiva y m es un entero racional, existe una forma cuadrática $a'x^2 + b'xy + c'y^2$ estrictamente equivalente a la dada y tal que $(a', m) = 1$.*

DEMOSTRACIÓN: Sea r el producto de los primos que dividen a m pero no a c. Sea t el producto de los primos que dividen a m y a c pero no a a (se entiende que valen 1 si no hay tales primos).

Entonces $(r, t) = 1$, luego existe un entero u tal que $ur \equiv 1 \pmod{t}$. Sea finalmente $s = (ur - 1)/t$. Así $ru - ts = 1$, luego el cambio de variables

$x = rx' + sy'$, $y = tx' + uy'$ transforma la forma cuadrática dada en otra propiamente equivalente en la que $a' = ar^2 + brt + ct^2$.

Veamos que $(a', m) = 1$. Sea p un divisor primo de m. Si $p \nmid c$, entonces $p \mid r$ y $p \nmid t$, luego $p \nmid a'$.

Si $p \mid c$ distinguimos dos casos: si $p \nmid a$ entonces $p \mid t$ pero $p \nmid r$, luego $p \nmid a'$. Si $p \mid c$ y $p \mid a$, como $(a, b, c) = 1$ tenemos que $p \nmid b$, $p \nmid r$ y $p \nmid t$, luego $p \nmid a'$. ∎

Con esto podemos probar el resultado que necesitamos para relacionar las dos definiciones que hemos dado del grupo de clases.

Teorema 6.11 *Todo módulo completo M con anillo de coeficientes $\mathfrak{O}_m$ es estrictamente similar a un ideal de $\mathfrak{O}_m$ de norma prima con cualquier entero prefijado n.*

Demostración: Consideremos un módulo M cuyo anillo de coeficientes sea $\mathfrak{O}_m$. Éste tendrá asociada una forma cuadrática primitiva, y por el teorema anterior podemos obtener otra propiamente equivalente $ax^2 + bxy + cy^2$ con $(a, n) = 1$. Esta forma cuadrática puede expresarse como $a(x + \gamma y)(x + \bar{\gamma} y)$, donde $-\gamma$ es una raíz del polinomio $ax^2 + bx + c$, y por lo tanto la forma está asociada al módulo $\langle 1, \gamma \rangle$, o también al módulo estrictamente similar

$$\langle a, a\gamma \rangle = \left\langle a, \frac{b - t\sqrt{d}}{2} \right\rangle,$$

donde $b^2 - 4ac = t^2 d$ con d libre de cuadrados. Cambiando γ por su conjugado si es preciso podemos suponer que las bases están orientadas.

Como formas equivalentes están asociadas a módulos similares, en realidad este módulo es similar al módulo original M y en particular su anillo de coeficientes sigue siendo $\mathfrak{O}_m$.

Así mismo el discriminante de la forma ha de ser el de $\mathfrak{O}_m$, es decir, o bien $t^2 d = m^2 d$ o bien $t^2 d = m^2 4d$, según el resto de d módulo 4. Por lo tanto $t = m$ o bien $t = 2m$.

Observar que

$$\mathrm{N}\left(\frac{b - t\sqrt{d}}{2}\right) = ac \quad \text{y} \quad \mathrm{Tr}\left(\frac{b - t\sqrt{d}}{2}\right) = b,$$

luego se trata de un entero. En el caso $d \not\equiv 1 \pmod 4$, el coeficiente b ha de ser par, digamos $b = 2b'$, y $t = 2m$, y el módulo es $\left\langle a, b' + m\sqrt{d} \right\rangle$, que por el teorema 6.9 es un ideal de $\mathfrak{O}_m$ de norma prima con n.

En el caso $d \equiv 1 \pmod 4$ llegamos a lo mismo. En efecto, entonces el módulo que hemos obtenido es

$$\left\langle a, \frac{b + t}{2} - t\omega \right\rangle,$$

pero $t = m$ y el ideal tiene la misma forma que en el caso anterior. ∎

Recordemos que, si $\mathcal{O}_m$ es un orden cuadrático, el grupo de clases que habíamos definido en 4.16 (teniendo en cuenta las observaciones tras 3.29) es $I_m^*(\mathcal{O})/P_m^*(\mathcal{O}_m)$, donde $I_m^*(\mathcal{O})$ es el grupo de los ideales fraccionales del orden maximal $\mathcal{O}_1$ que se expresan como cocientes de ideales primos con m. El teorema 3.27 nos da un isomorfismo entre $I_m^*(\mathcal{O})$ y un subgrupo del grupo de los módulos con anillo de coeficientes $\mathcal{O}_m$ (los que se expresan como cociente de ideales de norma prima con m). Al componerlo con la proyección en el grupo de clases de similitud (que hemos definido en esta sección) obtenemos un homomorfismo que es suprayectivo por el teorema anterior. Su núcleo está formado por los cocientes de ideales $\mathfrak{a}/\mathfrak{b}$ primos con m que, vistos como módulos de $\mathcal{O}_m$, son (estrictamente) similares a $\mathcal{O}_m$, es decir, tales que existe un $\gamma \in K^*$ (de norma positiva) de modo que $\alpha/\beta = \gamma\mathcal{O}_m$ o, equivalentemente $\alpha = \gamma\beta$. El teorema siguiente prueba que (para la similitud no estricta) este núcleo es precisamente $P_m^*(\mathcal{O}_m)$:

Teorema 6.12 *Sea K un cuerpo cuadrático y $\mathfrak{a}$, $\mathfrak{b}$ dos ideales de $I_m(\mathcal{O}_m)$ tales que existe un $\gamma \in K^*$ (de norma positiva) de modo que $\mathfrak{a} = \gamma\mathfrak{b}$. Entonces $\gamma = \beta/\alpha$, para ciertos α, $\beta \in \mathcal{O}_m$ de norma (positiva) prima con m.*

Demostración: Recordemos del capítulo III (ver las observaciones tras el teorema 3.29) que $I_m(\mathcal{O}_m)$ es el conjunto de los ideales de norma prima con m.

Expresemos $\gamma = \beta/\alpha$, para ciertos α, $\beta \in \mathcal{O}_1$, el orden maximal de K. Tenemos que $\alpha\mathfrak{a} = \beta\mathfrak{b}$, en principio considerando a $\mathfrak{a}$ y $\mathfrak{b}$ como ideales de $\mathcal{O}_m$, pero multiplicando por $\mathcal{O}_1$ podemos verlos como ideales de $\mathcal{O}_1$. Entonces, en virtud de 3.27, los ideales $\mathfrak{a}$ y $\mathfrak{b}$ son primos con m, luego los primos que dividen a m han de dividir a α y a β con la misma multiplicidad. Aplicando el teorema 3.7 podemos suponer que ninguno de ellos divide a β (y, por consiguiente, tampoco a α).

En particular $(\alpha)+(m) = 1$, luego existen $\alpha', \xi \in K$ tales que $\alpha\alpha' = 1+\xi m$. Cambiando α y β por $\alpha\alpha'$ y $\beta\alpha'$ se sigue cumpliendo que $(\alpha)+(m) = 1$ (es decir, α es primo con m luego β también), pero además ahora $\alpha \in 1 + (m) \subset \mathcal{O}_m$. Más aún $(\alpha) \in I_m(\mathcal{O}_m)$ (pues su norma es prima con m).

Falta probar que también $\beta \in \mathcal{O}_m$. Por el teorema 3.27 podemos escribir $(\alpha)\mathfrak{a} = \big((\beta) \cap \mathcal{O}_m\big)\mathfrak{b}$, lo que prueba que $(\alpha)\mathfrak{a} \subset \mathfrak{b}$ (vistos como ideales en $\mathcal{O}_m$). Ahora la relación $\alpha\mathfrak{a} = \beta\mathfrak{b}$ muestra que $\beta\mathfrak{b} \subset \mathfrak{b}$, es decir, que β es un coeficiente de $\mathfrak{b}$, luego por 3.28 tenemos que $\beta \in \mathcal{O}_m$ y, al igual que sucedía con α, también $(\beta) \in I_m(\mathcal{O}_m)$.

Por último, si γ tiene norma positiva podemos exigir que α y β también la tengan (cambiándolos si es preciso por $\alpha\alpha$ y $\beta\alpha$). ∎

Así pues, tenemos que el grupo de clases de similitud no estricta de los módulos cuyo anillo de coeficientes es el orden cuadrático $\mathcal{O}_m$ es isomorfo al grupo de clases $\mathcal{H}(\mathcal{O}_m) = I_m^*(\mathcal{O})/P_m^*(\mathcal{O}_m)$. En particular su orden viene dado por el teorema 4.17.

Más aún, también podemos representar el grupo de clases de similitud estricta de $\mathcal{O}_m$ como un grupo de clases de ideales del orden maximal. Basta

definir

$$P_m^+(\mathcal{O}_m) = \big\{(\alpha\mathcal{O}_1)(\beta\mathcal{O}_1)^{-1} \mid \alpha,\beta \in P_m(\mathcal{O}_m),\ \mathrm{N}(\alpha)>0,\ \mathrm{N}(\beta)>0\big\}.$$

(Observemos que $P_m(\mathcal{O}_m)$ es simplemente el conjunto de los elementos de $\mathcal{O}_m$ de norma prima con m).

Hemos probado que el grupo de clases de similitud estricta es isomorfo a $I_m^*(\mathcal{O})/P_m^+(\mathcal{O}_m)$.

La biyección entre el grupo de clases estrictas y el conjunto de clases de equivalencia estricta de formas determina en éste una estructura de grupo. Gauss probó que esta estructura está inducida por una operación entre formas cuadráticas que él describió y denominó *composición de formas.* No vamos a describir esta composición, pero sí es importante observar qué clase de formas es el elemento neutro del grupo.

Teorema 6.13 *Las formas asociadas a los órdenes cuadráticos son las formas principales.*

Demostración: Dado un entero libre de cuadrados d, los órdenes de $\mathbb{Q}\big(\sqrt{d}\,\big)$ son, según el teorema 2.24, los módulos $\mathcal{O}_k = \langle 1, k\omega\rangle$, donde ω es $\sqrt{d}$ o $\big(1+\sqrt{d}\,\big)/2$, según el resto de d módulo 4.

Si $d \not\equiv 1$ (mód 4) la forma asociada a $\mathcal{O}_k$ es $\mathrm{N}(x+k\sqrt{d}\,y) = x^2 - k^2dy^2$, la forma principal de discriminante $4k^2d$.

Si $d \equiv 1$ (mód 4) y $k = 2k'$ es par entonces $\mathcal{O}_k = \Big\langle 1, k'\sqrt{d}\Big\rangle$, y la forma asociada es, como antes la forma principal de discriminante k^2d. Si k es impar

$$\mathcal{O}_k = \left\langle 1, \frac{k+k\sqrt{d}}{2}\right\rangle = \left\langle 1, \frac{1+k\sqrt{d}}{2}\right\rangle,$$

y en esta base

$$\mathrm{N}\left(x + y\,\frac{1+k\sqrt{d}}{2}\right) = x^2 + xy + \frac{1-k^2d}{4}y^2,$$

que también es la forma principal de discriminante k^2d. Observar que todas las bases que hemos considerado están orientadas. ∎

Gauss llamó *clase principal* (estricta) de un discriminante dado D a la clase de equivalencia (estricta) de la forma principal de discriminante D. Acabamos de probar que los módulos asociados a las formas de la clase principal (estricta) son exactamente los de la clase de similitud (estricta) del orden de discriminante D. Por ello esta clase de similitud recibe también el nombre de clase principal (estricta). En términos de ideales, la clase principal (estricta) está formada por los ideales principales (generados por elementos de norma positiva). Éste es el motivo por la que en la teoría general de anillos los ideales generados por un solo elemento reciben el nombre de 'ideales principales'.

Terminamos esta sección con unos breves comentarios sobre los grupos de clases estrictas. Sabemos que éstos coinciden con los grupos de clases no estrictas en los órdenes de cuerpos imaginarios, por lo que podemos restringirnos a cuerpos reales.

Si $\mathcal{O}$ es un orden cuadrático de discriminante $D > 0$, definimos $-1 = \big[\sqrt{D}\,\big]$. Se trata de la clase estricta que contiene a todos los ideales principales de $\mathcal{O}$ generados por números de norma negativa. Si llamamos $1 = [D]$ a la clase principal, tenemos que $1 = -1$ si y sólo si la unidad fundamental de $\mathcal{O}$ tiene norma negativa. En cualquier caso se cumple que $(-1)^2 = \big[\sqrt{D}\,\big]^2 = [D] = 1$.

Ahora, si $\big\{[M_1], \ldots, [M_h]\big\}$ es el grupo de clases no estrictas, eso significa que todo módulo es similar a uno de los módulos $M_1, \ldots, M_h$, luego todo módulo es estrictamente similar a uno de los módulos $\pm M_1, \ldots, \pm M_h$, donde $-M = \sqrt{D}M$, y el grupo de clases estrictas es $\big\{\pm[M_1], \ldots, \pm[M_h]\big\}$.

Esto implica que el grupo de clases no estrictas es isomorfo al cociente del grupo de clases estrictas sobre el subgrupo $\{\pm 1\}$, ahora bien, es importante dejar claro que la estructura del grupo de clases estrictas no se deduce de la estructura del grupo de clases no estrictas. Por ejemplo, si sabemos que tres clases no estrictas cumplen $[M][N] = [R]$, no podemos concluir que esto siga siendo cierto si interpretamos las clases como clases estrictas. Entonces tendremos que $[M][N] = [\pm R]$, pero el signo concreto tendrá que ser verificado calculando explícitamente el coeficiente que hace similar a R con MN. En términos de la teoría de grupos, no es cierto en general que el grupo de clases estrictas sea producto directo de $\{\pm 1\}$ por un grupo isomorfo al de clases no estrictas.

6.4 Ecuaciones diofánticas cuadráticas

Consideremos una forma cuadrática completa primitiva $f(x, y)$ de discriminante D y que factorice en el cuerpo $\mathbb{Q}\big(\sqrt{d}\,\big)$. Vamos a aplicar la teoría que hemos expuesto para determinar las soluciones enteras de la ecuación $f(x, y) = m$.

Podemos suponer que $m > 0$ y que f no es definida negativa, o de lo contrario cambiamos el signo a los dos miembros y obtenemos una ecuación equivalente.

Según hemos visto, la forma admite una representación del tipo

$$f(x, y) = \frac{\mathrm{N}(\alpha x + \beta y)}{\mathrm{N}(M)},$$

donde (α, β) es una base orientada del módulo M. Las soluciones (x, y) de la ecuación están en correspondencia biunívoca con los elementos $\xi = \alpha x + \beta y \in M$ de norma $m\,\mathrm{N}(M)$.

Sea $\mathcal{O}$ el anillo de coeficientes de M. Sea C la clase de equivalencia estricta de M. La clase C está unívocamente determinada por f.

Si $\xi \in M$ tiene norma $m\,\mathrm{N}(M)$, entonces el módulo $\mathfrak{a} = \xi M^{-1}$ cumple $\mathfrak{a}M = \xi\mathcal{O} \subset M$, luego $\mathfrak{a} \subset \mathcal{O}$, es decir, $\mathfrak{a}$ es un ideal de $\mathcal{O}$. Su norma es $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\xi)\,\mathrm{N}(M)^{-1} = m$ y se cumple $\mathfrak{a} \in C^{-1}$.

Recíprocamente, si $\mathfrak{a}$ es un ideal de $\mathcal{O}$ contenido en la clase C^{-1} y de norma m, existe un ξ de norma positiva tal que $\mathfrak{a} = \xi M^{-1}$, luego $\xi \in \mathfrak{a}M \subset M$ y $\mathrm{N}(\xi) = m\,\mathrm{N}(M)$.

Tenemos, pues, una correspondencia entre los elementos $\xi \in M$ de norma $m\,\mathrm{N}(M)$ y los ideales en C^{-1} de norma m. Más aún, si tenemos dos parejas $(\xi, \mathfrak{a})$, $(\psi, \mathfrak{b})$, entonces $\mathfrak{a} = \xi M^{-1}$, $\mathfrak{b} = \psi M^{-1}$, y por consiguiente $\mathfrak{a} = \xi\psi^{-1}\mathfrak{b}$, $\mathrm{N}(\xi\psi^{-1}) = 1$. Consecuentemente $\mathfrak{a} = \mathfrak{b}$ si y sólo si $\xi\psi^{-1}$ es una unidad de $\mathcal{O}$ (de norma positiva), si y sólo si ξ y ψ son asociados.

Diremos que dos soluciones (x, y) son asociadas si sus números correspondientes son asociados en el sentido de 2.18. Resumimos en un teorema lo que hemos obtenido:

Teorema 6.14 *Sea $\mathcal{O}$ un orden cuadrático de discriminante D. Sea f una forma cuadrática de discriminante D y sea C la clase de similitud estricta de ideales de $\mathcal{O}$ asociada a f. Entonces la ecuación $f(x, y) = m$ tiene solución entera, para un $m > 0$ si y sólo si la clase C^{-1} contiene ideales de norma m.*

Ahora probaremos que es fácil encontrar los ideales de norma m. Nos faltará un método para seleccionar los que están en C^{-1}, o sea, los que son estrictamente similares a M^{-1} (o equivalentemente a $\overline{M}$).

Sea $\mathfrak{a}$ un ideal del orden $\mathcal{O}$ de norma m (con anillo de coeficientes $\mathcal{O}$). Sea k el menor número natural no nulo contenido en $\mathfrak{a}$. Entonces $\mathfrak{a} = \langle k, k\gamma\rangle = k\,\langle 1, \gamma\rangle$. El número γ está determinado salvo signo y adición de enteros racionales. Será único si lo elegimos de forma que $\gamma = x + y\sqrt{d}$ con $y > 0$, $-1/2 < x \le 1/2$. Con la notación de 6.2 se cumple $\gamma = \big(-b + \sqrt{D}\,\big)/2a$ con $-a \le b < a$.

Puesto que $\mathcal{O} = \langle 1, a\gamma\rangle$ y $\mathfrak{a} \subset \mathcal{O}$, concluimos que $a \mid k$, o sea, $k = as$ para un entero racional $s > 0$.

Por otro lado $m = \mathrm{N}(\mathfrak{a}) = k^2(1/a) = as^2$ y tenemos $\mathfrak{a} = as\,\langle 1, \gamma\rangle$.

Vamos a probar que la representación $\mathfrak{a} = as\,\langle 1, \gamma\rangle$ es única si exigimos que a, s y γ cumplan las propiedades siguientes:

1. La parte imaginaria (o irracional) de γ es positiva.
2. La parte racional de γ está en $]-1/2, 1/2]$.
3. $m = as^2$, a, $s > 0$.

En efecto, si a', s', γ' determinan el mismo ideal $\mathfrak{a}$, o sea, si se cumple $as\,\langle 1, \gamma\rangle = a's'\,\langle 1, \gamma'\rangle$, entonces $as = a's'$, pues ambos son el mínimo natural contenido en $\mathfrak{a}$ (usando 1). De aquí que $\langle 1, \gamma\rangle = \langle 1, \gamma'\rangle$ y por 1) y 2) $\gamma = \gamma'$.

Por 3) y usando $as = a's'$ deducimos que $s = s'$, luego $a = a'$.

Ahora, dado m, tomemos a y s de modo que $m = as^2$ (hay un número finito de posibilidades). Con ellos buscamos b y c tales que $b^2 - 4ac = D$, $(a, b, c) = 1$, $-a \le b < a$ y construimos $\gamma = \big(-b + \sqrt{D}\,\big)/2a$.

Es claro que $\mathfrak{a} = as\,\langle 1, \gamma\rangle$ es un ideal de norma m de su anillo de coeficientes $\mathcal{O} = \langle 1, a\gamma\rangle$, de discriminante D (sólo hay que notar que $\mathfrak{a} \subset \mathcal{O}$). De este modo los encontramos todos.

En los órdenes maximales (o en órdenes cualesquiera cuando buscamos ideales de norma prima con el índice) es más fácil plantear todas las factorizaciones posibles en ideales primos y encontrar tales primos factorizando los primos racionales.

Después hemos de plantear la igualdad $\mathfrak{a} = \xi M^{-1}$, descartar los ideales para los que no hay solución y encontrar los valores de ξ cuando la hay. Esto es precisamente lo que nos falta resolver.

Ejemplo Consideremos la ecuación $17x^2+32xy+14y^2 = 9$. Su discriminante es $D = 72 = 4 \cdot 9 \cdot 2$, luego está asociada a un módulo del orden $\mathcal{O}_3$ de $\mathbb{Q}(\sqrt{2}\,)$.

Para calcular este módulo factorizamos la forma cuadrática:

$$17x^2 + 32xy + 14y^2 = \left(x + \frac{16+3\sqrt{2}}{17}\,y\right)\left(x + \frac{16-3\sqrt{2}}{17}y\right)$$

$$= \frac{1}{17}\big(17x + \big(16+3\sqrt{2}\,\big)y\big)\big(17x + \big(16-3\sqrt{2}\,\big)y\big).$$

Por lo tanto podemos tomar $M = \big\langle 17, 16+3\sqrt{2}\,\big\rangle$, de norma 17. Claramente entonces

$$M^{-1} = \frac{1}{17}\left\langle 17, 16-3\sqrt{2}\right\rangle = \left\langle 1, \frac{16-2\sqrt{2}}{17}\right\rangle.$$

Ahora buscamos todos los ideales de $\mathcal{O}_3$ de norma 9. Esto significa buscar los números (a,b,c) que cumplen $9 = as^2$, $b^2-4ac = 72$, $(a,b,c) = 1$, $-a \le b < a$.

Las posibilidades para a son $a = 1, 9$. Si $a = 1$ ha de ser $b = -1, 0$. Vemos que la ecuación $1 - 4c = 72$ es imposible, mientras que $b = 0$ da $(1, 0, -18)$.

Si $a = 9$, de la ecuación $b^2 - 36c = 72$ se sigue $6 \mid b$, luego $b = 6k$ con $k^2 - c = 2$, y $k = -1, 0, 1$.

En total obtenemos las soluciones $(9, -6, -1)$, $(9, 0, -2)$, $(9, 6, -1)$.

Las soluciones halladas corresponden a los cuatro ideales

$$3\left\langle 1, 3\sqrt{2}\right\rangle, \quad 9\left\langle 1, \frac{\pm 1+\sqrt{2}}{3}\right\rangle, \quad 9\left\langle 1, \frac{\sqrt{2}}{3}\right\rangle.$$

Sabemos, pues, que las soluciones (x, y) de la ecuación (salvo asociación) se corresponden con los números

$$\xi = 17x + \big(16+3\sqrt{2}\,\big)y \tag{6.2}$$

tales que $\mathfrak{a} = \xi M^{-1}$, donde $\mathfrak{a}$ recorre los cuatro ideales que hemos obtenido.

Calcular los valores de ξ presupone decidir si existen, es decir, presupone un algoritmo para determinar si dos módulos ($\mathfrak{a}$ y M^{-1} en este caso) son estrictamente similares.

En esta dirección probamos el teorema siguiente:

Teorema 6.15 *Los módulos $\langle 1,\gamma\rangle$ y $\langle 1,\gamma'\rangle$ (correspondientes a un mismo orden cuadrático real) son similares si y sólo si γ y γ' son equivalentes en el sentido de* 5.11.

DEMOSTRACIÓN: Si existe un número ξ tal que $\langle 1,\gamma\rangle = \xi\,\langle 1,\gamma'\rangle$, entonces $\xi\gamma' = p\gamma + q$, $\xi = r\gamma + s$, donde p, q, r, s son enteros racionales tales que $ps - qr = \pm 1$. Dividiendo ambas ecuaciones obtenemos

$$\gamma' = \frac{p\gamma + q}{r\gamma + s},$$

con $ps - qr = \pm 1$.

Recíprocamente, si se cumple esto

$$\langle 1,\gamma'\rangle = \frac{1}{r\gamma+s}\,\langle r\gamma + s,\ p\gamma + q\rangle = \frac{1}{r\gamma+s}\,\langle 1,\gamma\rangle\,.$$

∎

En el capítulo anterior vimos que dos números reales son equivalentes si y sólo si sus fracciones continuas son finalmente iguales, lo que resuelve completamente el problema de la similitud de ideales y módulos de un cuerpo real. Notemos que el teorema no nos dice si los módulos son estrictamente similares, pero esto se comprueba calculando explícitamente el número que da la similitud (si no hay unidades de norma negativa y éste tiene norma negativa, entonces los módulos no son estrictamente similares). Lo ilustramos continuando con nuestro ejemplo:

Calculamos la unidad fundamental del orden $\mathcal{O}_3 = \mathbb{Z}\big[3\sqrt{2}\,\big]$. Para ello desarrollamos $3\sqrt{2} = \big[4,\overline{4,8}\,\big]$ y la unidad fundamental resulta ser $\epsilon = 17 + 12\sqrt{2}$, de norma 1. Por lo tanto la similitud estricta no coincide con la no estricta.

Veamos ahora si los módulos $3\,\langle 1, 3\sqrt{2}\rangle$ y $\left\langle 1, \frac{16-3\sqrt{2}}{17}\right\rangle$ son similares. Calculamos:

$$3\sqrt{2} = \big[4,\overline{4,8}\,\big], \qquad \frac{16-3\sqrt{2}}{17} = \big[0,1,2,\overline{4,8}\,\big].$$

Como las fracciones son finalmente idénticas los números son equivalentes, concretamente, si llamamos $\alpha = \big[\,\overline{4,8}\,\big]$ tenemos que $3\sqrt{2} = [4,\alpha] = 4 + 1/\alpha$ mientras

$$\frac{16-3\sqrt{2}}{17} = [0,1,2,\alpha] = \cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\alpha}}}.$$

A partir de aquí se obtiene enseguida que

$$\frac{16-3\sqrt{2}}{17} = \frac{3\sqrt{2}-2}{3\sqrt{2}-1},$$

y el teorema anterior nos da entonces que

$$\left\langle 1, \frac{16-3\sqrt{2}}{17}\right\rangle = \frac{1}{3\sqrt{2}-1}\left\langle 1, 3\sqrt{2}\right\rangle,$$

luego $3\langle 1, 3\sqrt{2}\rangle = (9\sqrt{2}-3)M^{-1}$, pero el número $\xi = 9\sqrt{2}-3$ tiene norma negativa, luego no da una solución.

Consideramos ahora el ideal $9\left\langle 1, \frac{1+\sqrt{2}}{3}\right\rangle$. En primer lugar calculamos

$$\gamma = \frac{1+\sqrt{2}}{3} = \big[0, 1, \overline{4, 8}\,\big].$$

De aquí se sigue fácilmente que

$$\frac{16-3\sqrt{2}}{17} = \frac{\gamma+1}{2\gamma+1},$$

luego

$$9\left\langle 1, \frac{1+\sqrt{2}}{3}\right\rangle = 9\left(2\,\frac{1+\sqrt{2}}{3}+1\right)M^{-1} = \big(15+6\sqrt{2}\,\big)M^{-1}.$$

El número $\xi = 15+6\sqrt{2}$ tiene norma 153, luego es válido y, según (6.2) proporciona la solución $(-1, 2)$.

Con el ideal $9\left\langle 1, \frac{1-\sqrt{2}}{3}\right\rangle$ llegamos a $\xi = 21-12\sqrt{2}$, también de norma 153 y que proporciona la solución $(5, -4)$. El último ideal se descarta igual que el primero.

Con esto concluimos que las soluciones de la ecuación dada son de la forma (x_n, y_n), de modo que

$$\pm\big(15+6\sqrt{2}\,\big)\big(17+12\sqrt{2}\,\big)^n = 17x_n + \big(16+3\sqrt{2}\,\big)y_n,$$

o bien

$$\pm\big(21-12\sqrt{2}\,\big)\big(17+12\sqrt{2}\,\big)^n = 17x_n + \big(16+3\sqrt{2}\,\big)y_n,$$

para cada entero racional n.

Dado que los dos valores de ξ que hemos hallado tienen la misma norma, resulta razonable investigar su cociente. Es fácil ver que

$$21-12\sqrt{2} = \big(3+2\sqrt{2}\,\big)\big(15+6\sqrt{2}\,\big).$$

El número $3+2\sqrt{2}$ es una unidad, pero no del orden $\mathcal{O}_3$, por lo que las dos soluciones que hemos hallado no son asociadas.

Si observamos que $17+12\sqrt{2} = \big(3+2\sqrt{2}\,\big)^2$ resulta que podemos expresar las soluciones de la ecuación como

$$\pm\big(15+6\sqrt{2}\,\big)\big(3+2\sqrt{2}\,\big)^{2n} = 17x_n + \big(16+3\sqrt{2}\,\big)y_n,$$

y

$$\pm\big(15+6\sqrt{2}\,\big)\big(3+2\sqrt{2}\,\big)^{2n+1} = 17x_n + \big(16+3\sqrt{2}\,\big)y_n,$$

o más sencillamente,

$$\pm\big(15+6\sqrt{2}\,\big)\big(3+2\sqrt{2}\,\big)^{n} = 17x_n + \big(16+3\sqrt{2}\,\big)y_n,$$

■

Nos falta resolver el problema de la similitud de módulos en cuerpos imaginarios. Una forma sencilla de abordarlo es en términos de formas cuadráticas. Las formas que nos interesan son las definidas positivas. Sea, pues, $ax^2+bxy+cy^2$ una forma definida positiva. Esto significa que $a, c > 0$ y $D = b^2 - 4ac < 0$.

El cambio de variables $x = y'$, $y = -x'$ intercambia los coeficientes a y c mientras que cambia b por $-b$, luego nos permite pasar a una forma equivalente en la que $a \le c$.

Por otra parte, el cambio $x = x' \pm y'$, $y = y'$ la convierte en

$$ax^2 + (b \pm 2a)xy + (a \pm b + c)y^2,$$

con lo que aplicando varias veces este cambio podemos pasar a una forma equivalente en la que $|b| \le a$. Con ello podemos perder la condición $a \le c$, pero podemos repetir el proceso nuevamente, y tras un número finito de pasos (puesto que cada vez el valor de a se hace menor) llegamos a una forma equivalente a la primera que cumple simultáneamente $|b| \le a \le c$. Más aún, si $b = -a$ el segundo cambio nos permite hacer $b = a$ sin cambiar c, y si $a = c$ entonces el primer cambio nos permite obtener $b \ge 0$. La definición y el teorema siguientes recogen lo que hemos obtenido:

Definición 6.16 Una forma cuadrática definida positiva $ax^2+bxy+cy^2$ está *reducida* si cumple $-a < b \le a < c$ o bien $0 \le b \le a = c$.

Teorema 6.17 *Toda forma cuadrática definida positiva es estrictamente equivalente a una forma reducida.*

Más aún, tenemos un algoritmo para encontrar dicha forma. Observar que las formas principales están reducidas. El teorema siguiente resuelve el problema de la similitud de módulos en cuerpos imaginarios:

Teorema 6.18 *Dos formas reducidas son estrictamente equivalentes si y sólo si son iguales.*

Demostración: Sea $f(x,y) = ax^2+bxy+cy^2$ una forma reducida. Si $0 < |y| \le |x|$ entonces

$$\begin{aligned} f(x,y) &\ge ax^2 - |bxy| + cy^2 = |x|(a|x| - |by|) + c|y|^2 \\ &\ge |x|^2(a - |b|) + c|y|^2 \ge a - |b| + c. \end{aligned}$$

Se obtiene el mismo resultado si suponemos $0 < |x| \le |y|$.

Puesto que $a - |b| + c$ se alcanza en $(1, \pm 1)$, tenemos que esta cantidad es el mínimo de f sobre pares (x,y) donde $x \ne 0$, $y \ne 0$.

Si consideramos tan sólo pares (x,y) de enteros primos entre sí, los únicos que falta por considerar aparte de los que tienen componentes no nulas son $(1,0)$ y $(0,1)$, donde f toma los valores a y c. Por lo tanto, el conjunto de las imágenes que toma f sobre tales pares comienza con $a \le c \le a - |b| + c, \ldots$

Es fácil ver que un cambio de variables de determinante 1 biyecta los pares de números enteros primos entre sí, luego si dos formas cuadráticas reducidas de

coeficientes (a,b,c) y (a',b',c') son estrictamente equivalentes, ambas alcanzan el mismo mínimo sobre tales pares, es decir, $a = a'$.

Si $a = b = c$, entonces la primera forma toma el valor a al menos sobre tres pares de enteros primos entre sí. Si $a = c \neq b$ (y entonces $c < a - |b| + c$) lo toma sólo dos veces y si $a < c$ lo toma sólo una vez. Lo mismo le ocurre a la segunda forma, luego si $a = b = c$ tenemos que $a' = b' = c'$ y ambas son la misma forma, si $a = c \neq b$ tenemos $a' = c' \neq b'$, y si $a < c$ entonces también $a' < c'$, y en este último caso c y c' son ambos iguales al mínimo valor distinto de a que toman ambas formas sobre pares de enteros primos entre sí. En cualquier caso tenemos $c = c'$.

Finalmente, si $a = c \neq b$ o bien $a < c$, concluimos por el mismo argumento que también $a - |b| + c = a' - |b'| + c'$, y así en cualquier caso $b = \pm b'$.

Vamos a probar que si $b = -b'$ entonces $b = 0$. En el caso $a = c$ es inmediato por la definición de forma reducida (sería, $b \geq 0$, $b' \geq 0$), luego suponemos $a < c$.

No puede ser $b = a$ porque entonces $b' = -a'$, en contra de la definición de forma reducida. Así pues, $-a < b < a < c$. Llamemos f a la primera forma y f' a la segunda. Digamos que $f(x,y) = f'(px + qy, rx + sy)$. Entonces $a = f(1,0) = f'(p,r)$, pero f' sólo toma el valor a en $(\pm 1, 0)$, luego $p = \pm 1$ y $r = 0$. Como $ps - qr = 1$, ha de ser $s = \pm 1$. Igualmente $c = f(0,1) = f'(q,s)$, luego $q = 0$. En definitiva, $f(x,y) = f'(\pm x, \pm y)$, de donde $b = b' = 0$. ∎

De este modo, para comprobar si dos módulos son similares basta reducir sus formas cuadráticas asociadas y ver si coinciden. En la sección siguiente veremos un ejemplo.

6.5 Cálculo de grupos de clases

Las técnicas que acabamos de desarrollar nos permiten calcular fácilmente los grupos de clases cuadráticos. Veamos algunos casos:

Ejemplo Calculemos el grupo de clases no estrictas del orden maximal del cuerpo $\mathbb{Q}(\sqrt{82})$. Como se trata de un orden maximal podemos aplicar el teorema 4.14 y concluir que todo ideal es semejante a otro de norma a lo sumo 9. Hemos de buscar todos los ideales de norma menor o igual que 9.

Buscaremos primero los ideales primos. Puesto que $x^2 - 82 \equiv x^2$ (mód 2), el teorema 3.16 nos da la factorización $2 = \big(2, \sqrt{82}\big)^2$, luego hay un único ideal de norma 2.

Por otra parte, $x^2 - 82 \equiv x^2 - 1 \equiv (x+1)(x-1)$ (mód 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 $x^2 - 82 \equiv x^2 - 2$ (mód 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

$$1, \quad \mathfrak{p}, \quad \mathfrak{q}, \quad \mathfrak{q}^2, \quad \mathfrak{r}, \quad \mathfrak{r}^2, \quad \mathfrak{pq}, \quad \mathfrak{pr}.$$

Para estudiar las relaciones de similitud entre ellos necesitamos conocer bases. El teorema 6.9 nos da que

$$\mathfrak{p} = \left\langle 2, \sqrt{82}\right\rangle \quad \mathfrak{q} = \left\langle 3, 1-\sqrt{82}\right\rangle, \quad \mathfrak{r} = \left\langle 3, 1+\sqrt{82}\right\rangle.$$

(estos ideales están contenidos en $\mathfrak{p}$, $\mathfrak{q}$ y $\mathfrak{r}$ y tienen la misma norma).

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

$$\begin{aligned}
\sqrt{82} &= \left[9, \overline{18}\,\right],\\
\frac{\sqrt{82}}{2} &= \left[4, \overline{1,1,8}\,\right],\\
\frac{1-\sqrt{82}}{3} &= \left[-3, 3, \overline{5,1,2}\,\right],\\
\frac{1+\sqrt{82}}{3} &= \left[3, \overline{2,1,5}\,\right].
\end{aligned}$$

Vemos, pues, que ningún par es similar. Estudiemos ahora $\mathfrak{q}^2$, que es similar a

$$\left\langle 1, \frac{1-\sqrt{82}}{3}, \frac{83-2\sqrt{82}}{3}\right\rangle = \left\langle 1, \frac{1-\sqrt{82}}{9}\right\rangle.$$

Calculamos

$$\frac{1-\sqrt{82}}{9} = \left[-1, 9, \overline{1,1,8}\,\right],$$

luego $[\mathfrak{q}^2] = [\mathfrak{p}]$.

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 $h \le 7$, 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. La unidad fundamental del orden tiene norma negativa, luego el grupo de clases estrictas es el mismo. ∎

Ejemplo Calculamos el número de clases del cuerpo $\mathbb{Q}(\sqrt{-17})$. Éste coincide con el número de formas reducidas de discriminante $D = -56$. Para hallarlas todas notamos en general que $-D = 4ac - b^2 \geq 3ac$, luego $a, |b|, c \leq -D/3$.

En este caso buscamos coeficientes menores o iguales que 18. Los únicos valores posibles son $(3, \pm 2, 5)$, $(2, 0, 7)$, $(1, 0, 14)$, luego el número de clases es 4. ∎

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 6.9, 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 4.14 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.

Ejemplo Consideremos ahora $K = \mathbb{Q}(\sqrt{-14}\,)$. Vamos a calcular los grupos de clases de los órdenes $\mathcal{O}_1$ y $\mathcal{O}_3$ de K, así como el epimorfismo del primero en el segundo. Puesto que la mayor parte de las comprobaciones son mecánicas, nos limitaremos a exponer los resultados y esbozar cómo pueden obtenerse.

$x^2 + 126y^2$ $9x^2 + 14y^2$	1 $(23, 9 + 3\sqrt{-14}\,)$	1 $(23, 3 - \sqrt{-14}\,)$	$x^2 + 14y^2$
$7x^2 + 18y^2$ $2x^2 + 63y^2$	$(7, 3\sqrt{-14}\,)$ $(2, 3\sqrt{-14}\,)$	$(7, \sqrt{-14}\,)$ $(2, \sqrt{-14}\,)$	$2x^2 + 7y^2$
$5x^2 - 4xy + 26y^2$ $10x^2 - 4xy + 13y^2$	$(5, 3 + 3\sqrt{-14}\,)$ $(13, 2 - 3\sqrt{-14}\,)$	$(5, 1 + \sqrt{-14}\,)$ $(13, 5 - \sqrt{-14}\,)$	$3x^2 + 2xy + 5y^2$
$5x^2 + 4xy + 26y^2$ $10x^2 + 4xy + 13y^2$	$(5, 3 - 3\sqrt{-14}\,)$ $(13, 2 + 3\sqrt{-14}\,)$	$(5, 1 - \sqrt{-14}\,)$ $(13, 5 + \sqrt{-14}\,)$	$3x^2 - 2xy + 5y^2$

Es fácil obtener todas las formas cuadráticas reducidas de discriminante $-4 \cdot 14$. Resultan ser las cuatro que aparecen en la última columna de la tabla. Esto nos dice que el número de clases de $\mathbb{Q}(\sqrt{-14}\,)$ es $h = 4$. El teorema 4.18 nos da entonces que el número de clases de $\mathcal{O}_3$ es $h_3 = 8$.

Seguidamente vamos factorizando primos. Consideremos el caso del 2:

- Claramente $2 = \mathfrak{p}^2$, donde $\mathfrak{p} = (2, \sqrt{-14}\,) = \langle 2, \sqrt{-14}\rangle$.
- La forma cuadrática asociada es $2x^2 + 7y^2$, que ya está reducida, luego situamos el ideal en la tercera columna, al lado de esta forma.
- Calculamos $\mathfrak{p} \cap \mathcal{O}_3 = \langle 2, 3\sqrt{-14}\rangle$ y lo situamos en la segunda columna.
- Calculamos la forma cuadrática asociada a este ideal, que ya está reducida y es $2x^2 + 63y^2$. La situamos en la primera columna.

Nos saltamos el 3, pues no podemos bajarlo a $\mathcal{O}_3$. Repetimos el proceso con el 5, el 7 y el 13 (el 11 se conserva primo). Con ello completamos toda la tabla salvo la segunda fila. Los primos siguientes nos dan formas ya calculadas en la primera fila. Podemos seguir tanteando hasta encontrar el 23 o bien observar

que necesitamos un ideal similar a 1, por lo que queremos un primo representable por la forma $x^2 + 14y^2$. Entonces no es difícil pensar en 23.

Con esto hemos encontrado ocho ideales de $\mathcal{O}_3$ cuyas formas reducidas son todas distintas, luego representan las ocho clases posibles. Cada uno se corresponde con el ideal de $\mathcal{O}_1$ que está a su lado en la tercera columna. Éstos últimos son similares por parejas y representan las cuatro clases de ideales de $\mathcal{O}_1$. ∎

Ejercicio: Comprobar que el grupo de clases de $\mathcal{O}_1$ en el ejemplo anterior es cíclico y está generado por cualquiera de los divisores de 5. Así mismo, el grupo de clases de $\mathcal{O}_3$ es de tipo $C_4 \times C_2$, y dos generadores son un divisor de 5 y el divisor de 2.

Ejercicio: Comprobar que existen tres clases de equivalencia no estricta de formas cuadráticas de discriminante -56.

Capítulo VII

Números p-ádicos

En su trabajo sobre el último teorema de Fermat, en un momento dado Kummer se encontró con una ecuación entre enteros ciclotómicos donde las incógnitas estaban en los exponentes. Si se hubiera tratado de una ecuación ordinaria, lo natural hubiera sido tomar logaritmos, de forma que se volviera lineal, pero esto no tenía sentido en el caso que le ocupaba. Sin embargo Kummer encontró un artificio de cálculo que le dio un resultado similar. Básicamente se trataba de considerar las derivadas logarítmicas de ciertos polinomios mínimos. En ésta y otras ocasiones, Kummer había estado rozando un concepto muy profundo. Todos sus cálculos se expresan de forma clara y natural en términos de los números p-ádicos, descubiertos más tarde por Kurt Hensel. A partir del trabajo de Helmut Hasse, alumno de Hensel, los números p-ádicos se situaron en el núcleo de la teoría algebraica de números del siglo XX. Nosotros no entraremos a explicar el porqué de su importancia a niveles más avanzados. Puesto que los vamos a necesitar más adelante para exponer razonablemente los resultados de Kummer sobre el último teorema de Fermat, los introducimos ahora y así aprovechamos la ocasión para dar un enfoque moderno y elegante de la parte de la teoría de Gauss sobre formas cuadráticas que todavía nos queda por estudiar.

Los números p-ádicos presentan características comunes con los números reales y los números racionales. 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:

$$\begin{array}{l} 1 \\ 1,4 \\ 1,41 \\ 1,414 \\ \ldots\ldots \end{array}$$

Ahora fijamos un número primo, por ejemplo $p = 7$, y vamos a buscar aproximaciones enteras "módulo 7". Las soluciones de $x^2 \equiv 2 \,(\text{mód } 7)$ 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 $x^2 \equiv 2 \,(\text{mód } 7^2)$. 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

$$\begin{aligned}(3+7t)^2 &\equiv 2 \,(\text{mód } 7^2),\\ 9 + 6\cdot 7t + 7^2t^2 &\equiv 2 \,(\text{mód } 7^2),\\ 7(1+6t) &\equiv 0 \,(\text{mód } 7^2),\\ (1+6t) &\equiv 0 \,(\text{mód } 7)\\ t &\equiv 1 \,(\text{mód } 7).\end{aligned}$$

Así pues, $x_1 = 3 + 1\cdot 7$ es una mejor aproximación a $\sqrt{2}$ módulo 7 en el sentido de que su cuadrado es congruente con 2 módulo 7 y 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 congruentes con 2 módulo más potencias de 7 cada vez.

En términos topológicos, la idea subyacente es que queremos considerar "próximos" dos números enteros si su diferencia es divisible entre muchas potencias de 7.

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.

Para tratar estas ideas en el contexto adecuado debemos introducir algunos conceptos básicos.

7.1 Valores absolutos

Definición 7.1 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

$$|\alpha|_0 = \begin{cases} 0 & \text{si } \alpha = 0\\ 1 & \text{si } \alpha \neq 0\end{cases}$$

Veamos ahora los hechos y conceptos básicos en torno a los valores absolutos:

Propiedades elementales Las propiedades 1) y 3) de la definición 7.1 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, $|-\alpha| = |\alpha|$. El mismo argumento empleado en $\mathbb{R}$ con el valor absoluto usual prueba en general que $|\alpha - \beta| \geq \big||\alpha| - |\beta|\big|$.

Ejercicio: Probar que un cuerpo finito no admite más valor absoluto que el trivial.

Cuerpos métricos Todo valor absoluto en un cuerpo induce en éste una distancia (en el sentido topológico) dada por $d(\alpha,\beta) = |\alpha - \beta|$. Un *cuerpo métrico* es un par $(K,\mathcal{T})$, donde K es un cuerpo y $\mathcal{T}$ es una topología en K determinada por un valor absoluto.

Quizá el lector hubiera esperado que hubiéramos definido un cuerpo métrico como un par formado por un cuerpo y un valor absoluto. Efectivamente, ésta es la definición que adoptan muchos textos, pero preferimos la que hemos dado porque enfatiza un hecho importante, y es que todos los conceptos que vamos a introducir dependen exclusivamente de la topología, y no del valor absoluto que la induce. Dado un cuerpo métrico K, llamaremos valores absolutos de K a los valores absolutos que inducen la topología de K.

Los mismos argumentos que se emplean en el caso de los números reales y complejos sirven para demostrar que la suma y el producto son aplicaciones continuas en un cuerpo métrico, así como cualquiera de sus valores absolutos, los polinomios, la función $1/x$ (salvo en 0), etc.

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, lo que explica por qué nunca necesitamos fijar un valor absoluto concreto.

Teorema 7.2 *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 K 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 7.3 *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

$$\begin{aligned} |\alpha+\beta|^\rho &= |\alpha|^\rho\,|1+\beta/\alpha|^\rho \leq |\alpha|^\rho\,\big(1+|\beta/\alpha|\big)^\rho \\ &\leq |\alpha|^\rho\,\big(1+|\beta/\alpha|\big) \leq |\alpha|^\rho\,\big(1+|\beta/\alpha|^\rho\big) = |\alpha|^\rho + |\beta|^\rho. \end{aligned}$$

∎

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 7.4 *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 su trabajo. 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 7.2 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.

Puede probarse 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 7.5 *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 $|\alpha + \beta| \leq \max\big\{|\alpha|, |\beta|\big\}$.*
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 $|a+b| \le \sqrt[n]{n+1}\,\text{máx}\big\{|\alpha|,|\beta|\big\}$, 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 $|\alpha+\beta| = \text{máx}\big\{|\alpha|,|\beta|\big\}$.

Compleciones De acuerdo con la topología general, 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 $|\alpha_m - \alpha_n| < \epsilon$. Notar que por el apartado 4) del teorema 7.2 esta propiedad no depende del valor absoluto considerado.

Es fácil ver que toda sucesión convergente es de Cauchy. Un cuerpo métrico K es *completo* si todas sus sucesiones de Cauchy son convergentes. Es bien sabido que $\mathbb{R}$ y $\mathbb{C}$ son cuerpos métricos completos, mientras que $\mathbb{Q}$ no lo es.

Las sucesiones de Cauchy tienen una caracterización sencilla en los cuerpos no arquimedianos:

Teorema 7.6 *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 7.7 *En un cuerpo métrico completo no arquimediano, la serie* $\sum_{n=1}^{\infty} x_n$ *es convergente si y sólo si* $\lim_n x_n = 0$.

El resultado fundamental sobre completitud es el siguiente:

Teorema 7.8 *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.*

DEMOSTRACIÓN: La prueba es formalmente idéntica a la conocida construcción de $\mathbb{R}$ mediante sucesiones de Cauchy. Por ello nos limitaremos a esbozarla. Sea A el conjunto de todas las sucesiones de Cauchy de k. Claramente A es un anillo con la suma y el producto definidos término a término. El conjunto I formado por las sucesiones convergentes a 0 es un ideal de A (se comprueba que las sucesiones de Cauchy están acotadas y de aquí que el producto de una sucesión de Cauchy por una convergente a 0 converge a 0).

Sea K el anillo cociente A/I. Se cumple que K es un cuerpo, pues si $[x_n] \in K$ no es nulo, entonces la sucesión (x_n) no converge a 0. Más aún, no tiene a 0 como punto de acumulación, pues una sucesión de Cauchy converge a cualquiera de sus puntos de acumulación. En particular, (x_n) es finalmente no nula, y modificando sus primeros términos podemos tomar otra equivalente (congruente módulo I) de modo que todos sus términos sean no nulos. Entonces $[1/x_n]$ es la inversa de $[x_n]$ (se comprueba fácilmente que la sucesión $(1/x_n)$ es de Cauchy).

Si $[x_n] \in K$, se comprueba que la sucesión $|x_n|$ es una sucesión de Cauchy en $\mathbb{R}$, luego converge a un número $\big|[x_n]\big|$ que depende exclusivamente de la clase de equivalencia y no del representante. Es inmediato comprobar que esto define un valor absoluto en K.

La aplicación que a cada $x \in k$ le asigna la clase $\big[(x)\big] \in K$ (la clase de la sucesión constantemente igual a x) es claramente un monomorfismo de cuerpos. Si identificamos a k con su imagen, es claro que k es un subcuerpo de K y que el valor absoluto que hemos definido en K extiende al dado en k.

Ahora, si $[x_n] \in K$, la sucesión (x_n), considerada como sucesión en K, converge precisamente a $[x_n]$. En efecto, dado $\epsilon > 0$, existe un natural r tal

que si $m, n \geq r$ entonces $|x_n - x_m| < \epsilon$, luego $\lim_n |x_n - x_m| \leq \epsilon$, luego por la definición del valor absoluto de K tenemos que $\big|[(x_n - x_m)_n]\big| \leq \epsilon$, o sea, $\big|[x_n] - x_m\big| \leq \epsilon$, para todo $m \geq r$, luego la sucesión (x_m) converge a $[x_n]$.

Esto implica que k es denso en K. Además K es completo, pues dada una sucesión de Cauchy (y_n) en K, para cada n existe un elemento $x_n \in k$ tal que $|y_n - x_n| < 1/n$, de donde se sigue fácilmente que la sucesión (x_n) es de Cauchy en k, luego converge a un $x \in K$. Es inmediato que x es un punto de acumulación de (y_n), luego (y_n) es convergente.

Falta probar la unicidad. Si K y K' son dos cuerpos completos que contienen a k como conjunto denso, entonces cada $x \in K$ es el límite de una sucesión (x_n) en k, que será de Cauchy en K', luego convergerá a un elemento $\phi(x) \in K'$ independiente de la sucesión elegida.

Esto define una aplicación $\phi : K \longrightarrow K'$ y se comprueba sin dificultad que se trata de una isometría que fija a los elementos de k. ∎

El cuerpo métrico K construido en el teorema anterior se llama *compleción* del cuerpo k. Hemos probado que cada valor absoluto se k se extiende a su compleción (de forma única por densidad).

Por ejemplo, $\mathbb{R}$ es la compleción de $\mathbb{Q}$ respecto al valor absoluto usual.

7.2 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 7.9 Sea K un cuerpo numérico y $\mathcal{O}$ su orden maximal. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}$. Para cada $\alpha \in \mathcal{O}$ definimos el *valor* $\mathfrak{p}$*-ádico* de α como el exponente de $\mathfrak{p}$ en la factorización ideal de α. Lo representaremos por $v_\mathfrak{p}(\alpha)$. Todo elemento no nulo de K se expresa como cociente de enteros, $\gamma = \alpha/\beta$. Definimos su valor $\mathfrak{p}$-ádico como $v_\mathfrak{p}(\gamma) = v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta)$. Es claro que esta definición depende sólo de γ y no de su representación como fracción.

De este modo tenemos definida una aplicación de $K^* = K \setminus \{0\}$ en $\mathbb{Z}$. Conviene recoger sus propiedades básicas en una definición general:

Definición 7.10 Una *valoración* es una aplicación $v : K \setminus \{0\} \longrightarrow \mathbb{Z}$, donde K es un cuerpo, tal que:

1. v es suprayectiva,
2. $v(\alpha\beta) = v(\alpha) + v(\beta)$, para $\alpha, \beta \in K \setminus \{0\}$
3. $v(\alpha + \beta) \geq \min\big\{v(\alpha), v(\beta)\big\}$, para $\alpha, \beta \in K \setminus \{0\}$, $\alpha \neq -\beta$.

Es fácil comprobar que las valoraciones $\mathfrak{p}$-ádicas que hemos definido antes cumplen realmente estas propiedades. Las propiedades 2) y 3) se comprueban primero sobre enteros y después sobre números 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 acordamos las identidades $n + \infty = +\infty + \infty = +\infty$, entonces 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 $v(\alpha + \beta) = \min\{v(\alpha), v(\beta)\}$.

En estos términos, queremos considerar que dos enteros algebraicos α y β están más próximos respecto a un primo $\mathfrak{p}$ 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. 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 de $\mathbb{R}^*$.

Ejercicio: Probar que los valores absolutos de un cuerpo métrico discreto están inducidos por una única valoración (probar que ρ es necesariamente el mayor valor absoluto menor que 1).

Notar 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, concluimos que $v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$ también es continua.

Sea k un cuerpo métrico discreto y K su compleción. 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 los valores absolutos de éste. Esto prueba que la compleción de un cuerpo métrico discreto es discreta.

Como caso particular tenemos que cada ideal primo $\mathfrak{p}$ en un cuerpo numérico k dota a éste de una estructura de cuerpo métrico discreto. Representaremos por $|\ |_\mathfrak{p}$ a cualquiera de los valores absolutos inducidos por la valoración $\mathfrak{p}$-ádica (y lo llamaremos *valor absoluto* $\mathfrak{p}$*-ádico).*

Definición 7.11 Sea K un cuerpo numérico y $\mathfrak{p}$ un ideal primo de K. Llamaremos *cuerpo de los números* $\mathfrak{p}$*-ádicos* $K_\mathfrak{p}$ a la compleción de K respecto al valor absoluto $\mathfrak{p}$-ádico. 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.

Tenemos, pues, que $K_\mathfrak{p}$ es un cuerpo métrico discreto completo.

Ejercicio: Probar que la sucesión (p^n) converge a 0 en $\mathbb{Q}_p$, y que $\displaystyle\sum_{n=0}^{\infty} p^n = 1/(1-p)$.

Las propiedades básicas de las compleciones que acabamos de definir pueden probarse en general sobre cuerpos métricos discretos: 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.

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 $v(\epsilon) = 1$, 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 7.12 *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 7.13 *Sea K un cuerpo métrico discreto. Entonces su anillo de enteros es un dominio euclídeo, y sus ideales son exactamente*

$$0 \subset \ldots \subset \mathfrak{p}^3 \subset \mathfrak{p}^2 \subset \mathfrak{p} \subset 1.$$

Ahora nos ocupamos mostrar la fuerte relación entre la aritmética de un cuerpo numérico y la de sus compleciones.

Teorema 7.14 *Sea K un cuerpo numérico y $\mathfrak{p}$ un primo de K. Sea $\mathcal{O}$ el anillo de enteros de K y $\mathcal{O}_\mathfrak{p}$ el de $K_\mathfrak{p}$. Sea $\mathfrak{p}_*$ el único primo de $\mathcal{O}_\mathfrak{p}$. Entonces:*

1. *$\mathcal{O}_\mathfrak{p}$ es la clausura de $\mathcal{O}$.*
2. *$\mathfrak{p}_*^n$ es la clausura de $\mathfrak{p}^n$.*
3. *La aplicación $[\alpha] \mapsto [\alpha]$ determina un isomorfismo $\mathcal{O}/\mathfrak{p}^n \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}_*^n$.*

DEMOSTRACIÓN: 1) Como $\mathcal{O} \subset \mathcal{O}_\mathfrak{p}$ y $\mathcal{O}_\mathfrak{p}$ es cerrado en $K_\mathfrak{p}$, tenemos que la clausura de $\mathcal{O}$ está contenida en $\mathcal{O}_\mathfrak{p}$.

Tomemos ahora $\alpha \in \mathcal{O}_\mathfrak{p}$ 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

$$|\beta|_\mathfrak{p} = |\alpha + (\beta - \alpha)|_\mathfrak{p} \le \max\{|\alpha|_\mathfrak{p}, |\beta - \alpha|_\mathfrak{p}\} \le 1.$$

Sea $\beta = a/b$, donde $a, b \in \mathcal{O}$. Por el teorema 3.7 podemos exigir que $\mathfrak{p} \nmid b$. Si $x \in \mathcal{O}$, 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

$$|\alpha - x|_\mathfrak{p} \le \max\{|\alpha - \beta|_\mathfrak{p}, |\beta - x|_\mathfrak{p}\} < \epsilon.$$

Esto prueba que α está en la clausura de $\mathcal{O}$.

2) Por el apartado anterior, todo elemento de $\mathcal{O}_\mathfrak{p}$ es de la forma $\alpha = \lim_n \alpha_n$, con $\alpha_n \in \mathcal{O}$. Por la continuidad de la valoración, $v_\mathfrak{p}(\alpha) = \lim_n v_\mathfrak{p}(\alpha_n)$, luego $\alpha \in \mathfrak{p}_*^n$ si y sólo si $\alpha_n \in \mathfrak{p}^n$ para todo n suficientemente grande.

3) Es claro que la aplicación está bien definida y es un homomorfismo. Observemos que $\alpha \equiv \beta \pmod{\mathfrak{p}^n}$ equivale a $v_\mathfrak{p}(\alpha - \beta) \geq n$, y lo mismo es válido para $\mathfrak{p}_*$, luego la aplicación es inyectiva. Por último el apartado 1) implica que para todo $\alpha \in \mathcal{O}_\mathfrak{p}$ existe un $\beta \in \mathcal{O}$ tal que $v_\mathfrak{p}(\alpha - \beta) \geq n$, lo que se traduce en que todo elemento de $\mathcal{O}_\mathfrak{p}$ es congruente módulo $\mathfrak{p}_*^n$ con un elemento de $\mathcal{O}$, es decir, que la aplicación es suprayectiva. ∎

Según el teorema anterior, la congruencia de dos enteros de K módulo $\mathfrak{p}_*^n$ es equivalente a la congruencia módulo $\mathfrak{p}^n$. Por ello en lo sucesivo suprimiremos el asterisco, y ya no distinguiremos entre $\mathfrak{p}$ y $\mathfrak{p}_*$.

Ejercicio: Sea K un cuerpo numérico y $\mathfrak{p}$ un ideal primo de K. Determinar la clausura en $K_\mathfrak{p}$ de un ideal cualquiera de K.

Pasamos ahora a estudiar la topología de los cuerpos discretos. En el caso concreto de los cuerpos $\mathfrak{p}$-ádicos, la finitud de los cuerpos de restos se traduce en una propiedad de compacidad análoga a la de los números reales y complejos.

Teorema 7.15 *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 $\alpha_n^1 \equiv x_0 \pmod{\pi}$. 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 anterior, 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 7.16 *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*

$$\alpha = \sum_{n=k}^{\infty} x_n\,\pi^n, \tag{7.1}$$

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 (7.1) para $\pi^{-k}\,\alpha$, y multiplicando por π^k obtenemos otro para α.

Observar que si en (7.1) 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 (7.1), 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, el 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 considerar en el cuerpo $\mathbb{Q}_p$ las representaciones de la forma (7.1) con $\pi = p$ y $0 \leq x_n < p$. 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.

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, es decir, 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: un entero m es un resto cuadrático módulo p^r, donde p es un primo impar, si y sólo si m es un resto cuadrático módulo p. Esto puede probarse estudiando con detalle los grupos de unidades módulo p^r. Nosotros lo deduciremos de las propiedades de los números p-ádicos. Dedicamos la sección siguiente a esta clase de resultados de existencia.

7.3 Criterios de existencia de raíces

Los teoremas siguientes garantizan en la existencia de raíces de ciertos polinomios en cuerpos métricos discretos y completos.

Teorema 7.17 *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 $\delta_j \equiv \gamma_j \pmod{\mathfrak{p}^{k+1}}$.

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 7.6 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 7.18 *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 7.19 *Sea* K *un cuerpo métrico discreto completo. Sea* D *su anillo de enteros y* $\mathfrak{p}$ *su ideal primo. Sea* $F(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$. *Entonces la ecuación* $F(x_1, \ldots, x_n) = 0$ *tiene solución en* D *si y sólo si las congruencias* $F(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}^m}$ *tienen solución para todo* m.

Notar que si F es un polinomio mónico con una sola variable, la propiedad 3) del teorema 3.9 nos da que la existencia de una raíz en D es de hecho equivalente a la existencia de una raíz en K.

Por otro lado, el criterio de irreducibilidad de Eisenstein es aplicable a los cuerpos métricos discretos, lo que nos da polinomios irreducibles de grado arbitrariamente grande. En particular la clausura algebraica de cualquiera de estos cuerpos tiene grado infinito.

Ejercicio: Sea p un primo impar y c un resto cuadrático módulo p. Probar que existe $\sqrt{c} \in \mathbb{Q}_p$. En particular c es un resto cuadrático módulo p^m para todo m.

Ejercicio: Sea c un número impar. Probar que $\sqrt{c} \in \mathbb{Q}_2$ si y sólo si $c \equiv 1 \pmod 8$.

Si p y q son primos impares, sea a un resto cuadrático módulo p y b un resto no cuadrático módulo q. 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 $\mathbb{Q}_q$. Más en general:

Ejercicio: Sean p y q dos números primos. Probar que los cuerpos $\mathbb{Q}_p$ y $\mathbb{Q}_q$ no son isomorfos.

Terminamos con un caso particular sobre existencia de raíces de la unidad.

Teorema 7.20 *El cuerpo* $\mathbb{Q}_p$ *contiene una raíz de la unidad de orden* $p-1$.

Demostración: Consideremos un entero racional c no divisible entre p. La sucesión $\{c^{p^n}\}$ converge en $\mathbb{Z}_p$, pues

$$c^{p^{n+1}} - c^{p^n} = c^{p^n}(c^{(p-1)p^n} - 1) = c^{p^n}(c^{\phi(p^{n+1})} - 1) \quad \text{y} \quad p^{n+1} \mid c^{\phi(p^{n+1})} - 1.$$

Esto prueba que $c^{p^{n+1}} - c^{p^n}$ tiende a 0, luego c^{p^n} es de Cauchy y por lo tanto convergente a un número $\zeta \in \mathbb{Z}_p$.

Ahora bien, en realidad hemos probado que $c^{(p-1)p^n} - 1$ tiende a 0, y por otra parte esta sucesión converge a $\zeta^{p-1} - 1$, es decir, $\zeta^{p-1} = 1$.

Así mismo $c^{p^n} - c$ converge a $\zeta - c$ y $p \mid c^{p^n} - c$, o sea, $v_p(c^{p^n} - c) \geq 1$. Por continuidad $v_p(\zeta - c) \geq 1$, o sea, $\zeta \equiv c \pmod p$.

Hemos probado que si $1 \leq c < p-1$ existe un $\zeta \in \mathbb{Z}_p$ tal que $\zeta^{p-1} = 1$ y $\zeta \equiv c \pmod p$. Por lo tanto hay al menos $p-1$ raíces $p-1$-ésimas de la unidad en $\mathbb{Z}_p$, luego tiene que haber raíces primitivas. ∎

Ejercicio: Probar que si p es un primo impar el polinomio ciclotómico p-ésimo es irreducible en $\mathbb{Q}_p$.

7.4 Series en cuerpos no arquimedianos

Para terminar con las propiedades generales de los cuerpos no arquimedianos dedicamos esta sección al estudio de las series infinitas. El notable teorema 7.7 hace que éstas presenten un comportamiento especialmente simple, análogo al de las series absolutamente convergentes en $\mathbb{R}$ o en $\mathbb{C}$. El teorema siguiente es un buen ejemplo de ello.

Teorema 7.21 *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 7.7, 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 $\{\alpha_1, \ldots, \alpha_k\} \subset \{\beta_1, \ldots, \beta_{k'}\}$. 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 $\{\beta_1, \ldots, \beta_{k'}\} \setminus \{\alpha_1, \ldots, \alpha_k\}$, 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.

Observar 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.

También se cumple la asociatividad infinita:

Teorema 7.22 *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 $\sum_{i\in I} \alpha_i = \sum_{n=0}^{\infty} \sum_{i\in I_n} \alpha_i$.*

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,

$$\sum_{(i,j)\in I\times J}\alpha_i\beta_j=\sum_{i\in I}\Big(\sum_{j\in J}\alpha_i\beta_j\Big)=\sum_{i\in I}\Big(\alpha_i\Big(\sum_{j\in J}\beta_j\Big)\Big)=\Big(\sum_{i\in I}\alpha_i\Big)\Big(\sum_{j\in J}\beta_j\Big).$$

Definición 7.23 Si A es un anillo, se llama $A[[x]]$ al anillo de las *series formales de potencias* sobre A, es decir, de las series de la forma

$$\sum_{n=0}^{\infty}a_nx^n\qquad a_n\in A.$$

Las operaciones en $A[[x]]$ son

$$\begin{aligned}\sum_{n=0}^{\infty}a_nx^n+\sum_{n=0}^{\infty}b_nx^n &= \sum_{n=0}^{\infty}(a_n+b_n)x^n,\\ \Big(\sum_{n=0}^{\infty}a_nx^n\Big)\Big(\sum_{n=0}^{\infty}b_nx^n\Big) &= \sum_{n=0}^{\infty}\Big(\sum_{k=0}^{n}a_kb_{n-k}\Big)x^n.\end{aligned}$$

De este modo, si K es un cuerpo completo no arquimediano y dos series de potencias convergen en un $x\in K$, entonces las series suma y producto en $K[[x]]$ convergen a la suma y el producto de los límites respectivamente. Es conocido que lo mismo es cierto para $K=\mathbb{C}$.

Ejercicio: Probar que una serie de potencias en un cuerpo completo no arquimediano K converge en todo K, o bien en un disco $|x|<r$ o bien sólo en 0.

Ejercicio: Sea K un cuerpo y $K((x))$ el cuerpo de cocientes de $K[[x]]$. Para cada serie formal de potencias no nula $s=\sum_{n=0}^{\infty}a_nx^n$, sea $v(s)$ el mínimo n tal que $a_n\neq 0$. Probar que v se extiende a una valoración en $K((x))$ con la que éste se convierte en un cuerpo métrico discreto completo cuyo anillo de enteros es $K[[x]]$. Probar que todo $s\in K((x))$ no nulo se expresa de forma única como $s=\sum_{n=m}^{+\infty}a_nx^n$, con $m\in\mathbb{Z}$, $a_n\in K$ y $a_m\neq 0$, donde la serie ha de entenderse como límite en $K((x))$ de la sucesión de sumas parciales. Además entonces $v(s)=m$.

Podemos definir como sigue una sustitución en $A[[x]]$: Sean dos series

$$f(x)=\sum_{n=0}^{\infty}a_nx^n\quad\text{y}\quad g(x)=\sum_{n=1}^{\infty}b_nx^n,$$

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 7.24 *Sea K un cuerpo métrico discreto completo. Sean f y g dos series de potencias en K tales que $f(x)$ converja para $v(x)\geq r$, $g(y)$ 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

$$(g \circ f)(y) = \sum_{n=0}^{\infty} \sum_{k=n}^{\infty} c_{nk} y^k = \sum_{n=0}^{\infty} a_n \big(g(y)\big)^n = f\big(g(y)\big).$$

■

Ahora aplicamos los resultados que hemos obtenido al estudio de dos series concretas muy importantes. Partamos de un cuerpo numérico K y $\mathfrak{p}$ 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 $\mathfrak{p}$. Es claro entonces que se cumple 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 (observar 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 $v_\mathfrak{p}(x) \le 0$ es claro que el término general de $\log(1+x)$ no converge a 0. Si $v_\mathfrak{p}(x) \ge 1$ entonces para cada natural $n = p^a m$ se cumple que $p^a \le n$ y $v_\mathfrak{p}(n) = ea \le e(\log n/\log p)$. Por lo tanto

$$v_\mathfrak{p}\left(\frac{x^n}{n}\right) = nv_\mathfrak{p}(x) - v_\mathfrak{p}(n) \ge nv_\mathfrak{p}(x) - e\,\frac{\log n}{\log p},$$

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 $v_\mathfrak{p}(x) \ge 1$ 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 $v_\mathfrak{p}(y) \ge v_\mathfrak{p}(x)$, de modo que $y = tx$, con $v_\mathfrak{p}(t) \ge 0$ (suponemos $x \ne 0$, 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 $v_\mathfrak{p}(x) \ge 1$, el teorema 7.24 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 7.25 *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 7.26 *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 7.24, 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 $\kappa = 1$. Observar 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: $\log 1 = \log(-1) = 0$.

Capítulo VIII

El teorema de Hasse-Minkowski

En este capítulo probaremos el teorema de Hasse-Minkowski, en el cual se basará el tratamiento que daremos en el capítulo siguiente a la teoría de Gauss sobre géneros de formas cuadráticas. Históricamente, este teorema fue la primera muestra relevante de la importancia de los números p-ádicos en la teoría algebraica de números. Para alcanzar nuestro objetivo conviene que expongamos los hechos básicos sobre formas cuadráticas en un cuerpo arbitrario K.

8.1 Formas cuadráticas

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 8.1 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. En el capítulo VI considerábamos tan sólo formas cuadráticas binarias sobre el anillo $\mathbb{Z}$. Observar 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 en general toda forma cuadrática se puede expresar de la forma

$$f(x_1, \ldots, x_n) = (x_1, \ldots, x_n) A (x_1, \ldots, x_n)^t,$$

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. 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 $B = CAC^t$.

Observar que si A es una matriz simétrica, una matriz del tipo CAC^t siempre es simétrica. Notar también que si dos formas cuadráticas son equivalentes, una es regular si y sólo si lo es la otra. En el capítulo VI 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 8.2 *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 $e_1 CAC^t = vAC^t$, y el coeficiente i-ésimo de este vector es $vAC^t e_i^t = vAv_i^t = 0$ 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 8.3 *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. Observar 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. El teorema anterior simplifica muchas demostraciones, por ejemplo la siguiente:

Teorema 8.4 *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 8.5 *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 8.6 *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 8.4 también representa a 1, luego por el teorema 8.2 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 8.7 *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 8.8 *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 8.2 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. ∎

8.2 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.

Nos interesa 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 8.9 *Sea p un primo impar. Entonces una unidad $\epsilon = \sum_{n=0}^{\infty} c_n p^n$ (con $0 \le c_n < p$) es un cuadrado si y sólo si c_0 es un resto cuadrático módulo p.*

Demostración: Si $\epsilon = \eta^2$, para una cierta unidad η, entonces existe un entero racional $0 < d < p$ tal que $\eta \equiv d \pmod p$ (d es el término independiente del desarrollo de η en serie de potencias, y no es 0 porque η es una unidad). Entonces $c_0 \equiv \epsilon \equiv d^2 \pmod p$.

Recíprocamente, si $c_0 \equiv d^2 \pmod p$ para un cierto d (no divisible entre p), consideremos 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 7.18 nos da que existe un $\eta \in \mathbb{Z}_p$ tal que $\epsilon = \eta^2$. ∎

Definición 8.10 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 (que con la notación del teorema es c_0), 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 8.11 *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 8.12 *Una unidad diádica ϵ es un cuadrado en $\mathbb{Q}_2$ si y sólo si se cumple que $\epsilon \equiv 1 \pmod 8$.*

Demostración: Si $\epsilon = \eta^2$, entonces $\eta \equiv 1 \pmod 2$ y por otro lado existe un entero racional k tal que $\eta \equiv k \pmod 8$. Por la condición anterior k es impar y además $\epsilon \equiv k^2 \pmod 8$.

Es fácil probar que el cuadrado de un número impar siempre es congruente con 1 módulo 8 (basta verlo para 1, 3, 5, 7).

Supongamos ahora que $\epsilon \equiv 1 \pmod 8$. Tomamos $F(x) = x^2 - \epsilon$ y vemos que $F(1) \equiv 0 \pmod 8$, $F'(1) = 2 \equiv 0 \pmod 2$ y $F'(1) = 2 \not\equiv 0 \pmod 4$. El teorema 7.17 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 $\epsilon u^{-1} \equiv 1 \pmod 8$, 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 8.13 *Se cumple que $|\mathbb{Q}_2^* : \mathbb{Q}_2^{*2}| = 8$.*

Demostración: Razonando como en el teorema 8.11 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

$$F = F_0 + pF_1 = (\epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2) + p(\epsilon_{r+1} x_{r+1}^2 + \cdots + \epsilon_n x_n^2), \tag{8.1}$$

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 8.14 *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,

$$(\epsilon_1 a_1^2 + \cdots + \epsilon_r a_r^2) + p(\epsilon_{r+1} a_{r+1}^2 + \cdots + \epsilon_n a_n^2) = 0 \tag{8.2}$$

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 7.18 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 (8.2) 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 (8.2), 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 8.15 *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 8.14 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 7.18 como lo hemos hecho en el teorema 8.14 obtenemos el criterio siguiente para este tipo de formas:

Teorema 8.16 *Sean $\epsilon_1, \ldots, \epsilon_r$ unidades p-ádicas. 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.*

Notar 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 8.17 *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 valor impar.*

Demostración: De nuevo, una implicación es obvia. Supongamos que $F(a_1, \ldots, a_n) \equiv 0 \pmod{16}$ donde alguno de los enteros a_i es impar. Si esto sucede para $i \leq r$, entonces tenemos que

$$F(a_1, \ldots, a_n) \equiv 0 \pmod{8}, \qquad F_i'(a_1, \ldots, a_n) = 2\epsilon_i a_i \not\equiv 0 \pmod{4},$$

luego el teorema 7.17 nos da que F representa 0.

Si los números $a_1, \ldots, a_r$ 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 8.18 *Con la notación anterior, si $F \equiv 0 \pmod{8}$ tiene una solución en la que alguna variable $x_1, \ldots, x_r$ 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 8.19 *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 8.20 *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 (8.1), y de acuerdo con la observación posterior a (8.1) 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 8.16 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 8.18 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 8.5 nos da la siguiente consecuencia inmediata:

Teorema 8.21 *Toda forma cuadrática regular con cuatro o más variables representa a todos los números p-ádicos no nulos.*

Otra consecuencia importante del teorema 8.19 (junto con el teorema 8.16) es la siguiente:

Teorema 8.22 *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 $\mathbb{Q}_p$.*

8.3 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 8.5

$$\beta \in N_\alpha \quad \Leftrightarrow \quad x^2 - \alpha y^2 \text{ representa } \beta \quad \Leftrightarrow \quad \alpha x^2 + \beta y^2 - z^2 \text{ representa 0.}$$

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 8.11 y 8.13 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 8.23 *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 8.5 esta forma representa a toda unidad ϵ (incluyendo a las que no son cuadrados), pues según el teorema 8.22 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 8.11). Ahora bien, si $\alpha = \epsilon$ y $\beta = p$ o si $\alpha = p$, $p\epsilon$ y $\beta = \epsilon$, el teorema 8.14 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 8.18 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 8.24 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 8.5, 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 8.25 *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 8.14, 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 8.22, la forma $\epsilon x^2 + \eta y^2 - z^2$ siempre representa 0.

6) En la tabla construida en la prueba del teorema 8.23 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 $\eta \equiv 1 \pmod 4$. ∎

Notar 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 8.9 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 8.26 *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 8.27 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 8.28 *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 8.7 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 8.8. ∎

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 7.17, 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 8.29 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.

En la definición anterior hemos introducido por primera vez un convenio que tiene su explicación en el desarrollo posterior de la teoría, y que aquí no podríamos justificar debidamente. Se trata del uso del subíndice ∞ para hacer

referencia a los números reales. En esta misma línea, llamaremos $\mathbb{Q}_\infty = \mathbb{R}$ y representaremos por $|\ |_\infty$ al valor absoluto usual en $\mathbb{R}$. En la práctica esto nos permitirá englobar a $\mathbb{R}$ y los cuerpos p-ádicos bajo la expresión común $\mathbb{Q}_p$, si entendemos que p recorre los números primos incluyendo $p = \infty$. Como acabamos de decir, existe una base teórica para hablar de un 'primo infinito' en $\mathbb{Q}$ en estrecha analogía con los primos finitos usuales, pero no estamos en condiciones de entrar en ello.

8.4 El teorema de Hasse-Minkowski

Por fin estamos en condiciones de abordar el teorema central de este capítulo:

Teorema 8.30 (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 8.5 tenemos la siguiente consecuencia inmediata:

Teorema 8.31 *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 cualquier cuerpo numérico pueden descomponerse en resultados análogos 'locales' en torno a las compleciones del cuerpo respecto todos sus primos (y aquí hay que incluir ciertos '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.

En esta sección demostraremos el teorema de Hasse-Minkowski para formas de hasta tres variables, con lo que el teorema 8.31 estará probado para formas binarias. El resto de la prueba requerirá consideraciones adicionales que incluyen la ley de reciprocidad cuadrática (que probaremos en el capítulo siguiente) y el teorema de Dirichlet sobre primos en progresiones aritméticas, que probaremos en el capítulo XI. Por otra parte, en lo sucesivo sólo necesitaremos los casos que vamos a probar aquí.

DEMOSTRACIÓN: (del Tª 8.30 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 8.7, 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 $\mathbb{Q}$.

Observar 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).

Observar que para aquellos primos p que no dividan a abc los coeficientes son unidades p-ádicas, y por el teorema 8.22 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 8.14 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:

$$ax^2+by^2-cz^2 \equiv (ax+by-cz)^2 \pmod p.$$

Si para cada primo $p \mid abc$ tomamos $r_p \in \mathbb{Z}$ de modo que $r_p \equiv 1 \pmod p$, $r_p \equiv 0 \pmod{abc/p}$ y sumamos las formas $r_pL^p(x,y,z)$, por una parte y por otra las formas $r_pM^p(x,y,z)$, obtenemos formas lineales $L(x,y,z)$, $M(x,y,z)$ con coeficientes enteros tales que

$$L(x,y,z) \equiv L^p(x,y,z) \pmod p, \qquad M(x,y,z) \equiv M^p(x,y,z) \pmod p$$

para todos los divisores primos de abc. Claramente entonces

$$ax^2+by^2-cz^2 \equiv L(x,y,z)M(x,y,z) \pmod{abc}$$

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

$$0 \le x < \sqrt{bc}, \quad 0 \le y < \sqrt{ac}, \quad 0 \le z < \sqrt{ab}. \tag{8.3}$$

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 8.3 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

$$L(x_1,y_1,z_1) \equiv L(x_2,y_2,z_2) \pmod{abc}.$$

Llamando (x_0,y_0,z_0) a la diferencia de ambas ternas, la linealidad de L implica que $L(x_0,y_0,z_0) \equiv 0 \pmod{abc}$. Así,

$$ax_0^2+by_0^2-cz_0^2 \equiv L(x_0,y_0,z_0)M(x_0,y_0,z_0) \equiv 0 \pmod{abc}.$$

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 8.7), luego $ax^2+by^2-cz^2$ también. ∎

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 8.32 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 8.33 (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

$$\begin{aligned} \gamma^2 a + T'AT &= a, \\ \gamma aS + T'AQ &= 0, \\ S'aS + Q'AQ &= B. \end{aligned}$$

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

$$M'AM = (Q'+kS'T')A(Q+kTS) = Q'AQ+kS'T'AQ+kQ'ATS+k^2S'T'ATS$$

$$= Q'AQ-k\gamma aS'S-k\gamma aS'S+k^2(a-\gamma^2 a)S'S = Q'AQ+a\big((1-\gamma^2)k^2-2k\gamma\big)S'S.$$

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 8.34 *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 8.30 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 8.31 resulta que g representa a r en $\mathbb{Q}$.

Por el teorema 8.2 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. ∎

Observar 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 8.27.

Definición 8.35 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, 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 8.27).

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 8.28 y 8.34 (junto con sus versiones para ∞) obtenemos:

Teorema 8.36 *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 8.22 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.

8.5 La ley de reciprocidad cuadrática

Observemos que en la demostración del teorema 8.30 para formas de tres variables no se ha 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, que enunciamos en el capítulo I (sección 1.4). Ahora vamos a presentarla en una versión equivalente que muestra con elegancia su conexión con la teoría de formas cuadráticas.

Teorema 8.37 *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: Observar 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 y con ella tendremos probada la ley de reciprocidad cuadrática. Observar que esta fórmula explica por qué en el teorema 8.30 no era necesaria la hipótesis de que la forma cuadrática representara 0 en $\mathbb{Q}_2$: 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 implica que si esto sucede para todos los primos salvo quizá uno (incluido $p=\infty$) también ha de cumplirse para éste último.

8.6 Conclusión de la prueba

Para completar la prueba del teorema 8.30 necesitaremos el siguiente hecho auxiliar:

Teorema 8.38 *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 8.30:

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

$$t \equiv b_2 \pmod{16},$$

$$\begin{aligned} t &\equiv b_{p_1} \ (\text{mód } p_1^2), \\ &\vdots \qquad \vdots \\ t &\equiv b_{p_s} \ (\text{mód } p_s^2). \end{aligned} \tag{8.4}$$

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 $b_{p_i}t^{-1} \equiv 1$ (mód p_i). Por el teorema 8.9 tenemos que $b_{p_i}t^{-1}$ es un cuadrado en $\mathbb{Q}_{p_i}$. Igualmente, b_2t^{-1} es una unidad y $b_2t^{-1} \equiv 1$ (mód 8), luego por el teorema 8.12 también es un cuadrado.

Así pues, para $p = 2, p_1, \ldots, p_s$ se cumple que b_pt^{-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 8.22 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 8.37 (aún no demostrada) resulta que también representan 0 en el caso exceptuado (ver la observación tras el teorema). Por el teorema 8.30 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 8.5 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 (8.4). 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 (ver el capítulo I), 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 8.22 representa 0 en $\mathbb{Q}_q$, luego por el teorema 8.4 también representa a t. Con esto concluimos que g y h representan a t en $\mathbb{Q}$ y la prueba termina.

Observar que por el teorema 8.20 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. ∎

Vamos a acabar el capítulo con una aplicación interesante del teorema de Hasse-Minkowski. Nos apoyaremos en el teorema siguiente.

Teorema 8.39 *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,

$$\begin{aligned} g(x',x') &= a^2\, g(x,x) + 2ab\, g(x,y) + b^2\, g(y,y) \\ &= a^2t^2n + ab(2nt-b) + b^2(n+a) = n(a^2t^2+2abt+b^2) = t'^2n, \end{aligned}$$

lo que contradice la minimalidad de t ∎

Teorema 8.40 (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 $f(x-x',y-y',z-z') \le 1/4+1/4+1/4 = 3/4 < 1$. 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 8.31 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 8.22 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 8.5) 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 8.5 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 $1,5,2,10$ (observar que -1 es congruente con 7 y considerar la tabla calculada en la prueba de 8.23). 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 $a \equiv 7$ (mód $\mathbb{Q}_2^{*2}$).

Por lo tanto los números naturales n representados por f son todos excepto los que cumplen $a \equiv 7$ (mód $\mathbb{Q}_2^{*2}$), o equivalentemente, $-a \equiv 1$ (mód $\mathbb{Q}_2^{*2}$), o sea, excepto los que cumplen que $-a$ es un cuadrado en $\mathbb{Q}_2$.

Por el teorema 8.12 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 8.41 (Legendre) *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 $m \equiv 7$ (mód 8) y por lo tanto $m - 1 \equiv 6$ (mód 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 IX

La teoría de los géneros

Finalmente estamos en condiciones de abordar, desde el punto de vista que pretendíamos, la parte más profunda e interesante de la teoría de Gauss sobre formas cuadráticas binarias, la teoría de los géneros. Como es habitual, nosotros la trataremos tanto en términos de formas cuadráticas como en términos de módulos e ideales de órdenes cuadráticos. En este capítulo, y mientras no se indique lo contrario, la expresión 'forma cuadrática' tendrá el sentido que le dábamos en el capítulo VI, es decir, el de forma cuadrática binaria con coeficientes enteros, regular y primitiva (y definida positiva si su discriminante es negativo).

Ya conocemos un método para determinar si una forma cuadrática dada representa o no a un entero dado. Sin embargo el método es demasiado complejo, en el sentido de que se trata de una serie de cálculos que nos dan la respuesta en cada caso particular, pero no nos dicen nada sobre qué enteros son representables en general por una forma dada. Por ejemplo, con las técnicas del capítulo anterior es fácil ver que la forma $x^2 + y^2$ representa a un primo impar p si y sólo si $p \equiv 1$ (mód 4). Las técnicas del capítulo VI nos permiten probar que 5 está representado por dicha forma, así como que 7 no lo está, pero no nos son de ninguna ayuda para llegar hasta esta sencilla caracterización. Por otra parte, resultados de este tipo eran conocidos desde la época de Fermat, aunque las pruebas requerían argumentos específicos en cada caso particular.

La teoría de los géneros sí proporciona esta clase de resultados. Gauss descubrió que existen condiciones necesarias, muy sencillas de enunciar y de manejar, para que un número esté representado por una forma cuadrática. En ocasiones estas condiciones son también suficientes, con lo que el problema de determinar los números representados por la forma considerada tiene una respuesta particularmente simple. Cuando no son suficientes, al menos proporcionan información relevante sobre el problema. Una parte de la teoría era ya conocida por Legendre, con anterioridad al trabajo de Gauss.

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. Dedicamos la primera sección a estudiar este problema.

9.1 Equivalencia modular

Del mismo modo que en el estudio de la representabilidad de números por formas cuadráticas es imprescindible el concepto de equivalencia, para estudiar la representabilidad módulo un natural n hemos de introducir la equivalencia módulo n:

Definición 9.1 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 nos indica que es suficiente estudiar la equivalencia módulo potencias de primos.

Teorema 9.2 *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.*

Demostración: Si tenemos que $f(x,y) \equiv g(a_1x+a_2y, a_3x+a_4y) \pmod{m}$ y $f(x,y) \equiv g(b_1x+b_2y, b_3x+b_4y) \pmod{n}$, donde los determinantes de los cambios son primos con m y n respectivamente, por el teorema chino del resto podemos encontrar enteros c_i tales que $c_i \equiv a_i \pmod{m}$ y $c_i \equiv b_i \pmod{n}$. Entonces $f(x,y)$ es congruente con $g(c_1x+c_2y, c_3x+c_4y)$ módulo m y módulo n, luego también módulo mn, y es fácil ver que el determinante de este cambio es también primo con mn, luego f y g son equivalentes módulo mn. El recíproco es obvio. ∎

Para estudiar la equivalencia módulo una potencia de primo p^n vamos a buscar formas equivalentes a una dada lo más sencillas posibles. Supongamos primero $p \neq 2$. Dada una forma $f(x,y)$ de discriminante D, el teorema 6.10 nos da otra forma equivalente $ax^2+bxy+cy^2$ tal que $p \nmid a$. El cambio de variables

$$\begin{aligned} x &= x' - by' \\ y &= 2ay' \end{aligned}$$

la transforma en

$$a(x^2 - Dy^2). \tag{9.1}$$

Para simplificar aún más la expresión, notemos que si U_{p^n} representa al grupo de las unidades de $\mathbb{Z}/p^n\mathbb{Z}$ y $U_{p^n}^2$ al subgrupo de los cuadrados, entonces $|U_{p^n} : U_{p^n}^2| = 2$. En efecto, basta ver que la aplicación $x \mapsto x^2$ tiene núcleo $\{\pm 1\}$, pero si $x^2 \equiv 1 \pmod{p^n}$, entonces $p^n \mid x^2 - 1 = (x+1)(x-1)$, y no puede ocurrir simultáneamente que $p \mid x+1$ y $p \mid x-1$, pues restando saldría que $p \mid 2$. Por lo tanto $p^n \mid x+1$ o $p^n \mid x-1$, con lo que $x \equiv \pm 1 \pmod{p^n}$.

Tomemos un resto no cuadrático cualquiera módulo p, digamos r. Obviamente r tampoco es un cuadrado módulo p^n, con lo que $U_{p^n} = U_{p^n}^2 \cup rU_{p^n}^2$. En particular, el número a de (9.1) se escribirá módulo p^n como $a = u^2$ o bien $a = ru^2$, para un cierto entero u (primo con p). El cambio $x' = ux$, $y' = uy$ nos transforma (9.1) en una de las dos formas

$$x^2 - Dy^2 \qquad \text{o} \qquad r(x^2 - Dy^2), \tag{9.2}$$

donde, recordemos, r es cualquier resto no cuadrático módulo p que fijemos de antemano. Ahora distinguimos dos casos:

Si $p \mid D$, entonces las formas (9.2) son congruentes módulo p con x^2 y rx^2 respectivamente, que se caracterizan por que una representa sólo restos cuadráticos módulo p y la otra sólo restos no cuadráticos módulo p. En resumen:

Teorema 9.3 *Si $p \mid D$, toda forma cuadrática f de discriminante D es equivalente módulo p^n con una de las formas* (9.2) *y sólo con una. Concretamente, f es equivalente a la primera si y sólo si representa restos cuadráticos módulo p y es equivalente a la segunda en caso contrario.*

De acuerdo con esto, Gauss dio la definición siguiente

Definición 9.4 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.

Las consideraciones anteriores prueban que $\chi_p(f)$ no depende de la elección de a, así como que formas equivalentes módulo p^n tienen el mismo carácter módulo p. 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. También hemos probado que dos formas f y g de discriminante D son equivalentes módulo p^n si y sólo si tienen el mismo carácter módulo p.

Examinemos ahora el segundo caso, es decir, $p \nmid D$. Entonces es claro que los polinomios x^2 y $r - Dy^2$ toman cada uno $(p+1)/2$ valores distintos módulo p, luego ha de haber enteros u e v que den la misma imagen, es decir, tales que

$r \equiv u^2 - Dv^2 \pmod{p}$. Entonces, $u^2 - Dv^2$ es un resto no cuadrático módulo p, y si elegimos a éste precisamente como r, tenemos la igualdad $r = u^2 - Dv^2$. El cambio de variables

$$\begin{aligned} x &= ux' + Dvy' \\ y &= vx' + uy' \end{aligned}$$

transforma la forma de la izquierda de (9.2) en la forma de la derecha, luego ambas son equivalentes módulo p^n y, en definitiva, todas las formas cuadráticas de discriminante D son equivalentes módulo p^n. Para extender a este caso las conclusiones anteriores definimos el *carácter* módulo p de una forma f (cuando p es impar y no divide al discriminante) como $\chi_p(f) = 1$. Definimos igualmente el carácter de una clase de fórmulas.

De este modo sigue siendo cierto que dos formas cuadráticas de discriminante D son equivalentes módulo p^n, con p impar, si y sólo si tienen el mismo carácter módulo p, lo cual se cumple siempre si $p \nmid D$.

Nos falta estudiar el caso $p = 2$. Si una forma cuadrática tiene discriminante $D = b^2 - 4ac$, entonces D es impar si y sólo si b lo es, y entonces $D \equiv 1 \pmod 8$ si y sólo si $2 \mid ac$. Ocupémonos primero del caso impar.

Teorema 9.5 *Toda forma cuadrática de discriminante impar D es equivalente módulo 2^n a una de las dos formas*

$$xy \qquad o \qquad x^2 + xy + y^2.$$

Concretamente, una forma es equivalente a la primera si y sólo si $D \equiv 1 \pmod 8$ y es equivalente a la segunda en caso contrario.

Demostración: Toda forma con discriminante $D \equiv 1 \pmod 8$ es equivalente a una forma $ax^2 + bxy + 2cy^2$ con a impar. Con el cambio $y' = by$ podemos hacer $b = 1$. Por otra parte, si aplicamos a xy el cambio de variables $x = x' + 2uy$, $y = ax' + vy$ (con v impar) obtenemos la forma

$$ax^2 + (v + 2au)xy + 2uvy^2.$$

Para que ésta sea congruente con la dada se han de cumplir las congruencias

$$v + 2au \equiv 1 \pmod{2^n} \tag{9.3}$$

$$uv \equiv c \pmod{2^n}. \tag{9.4}$$

Como v es una unidad módulo 2^n, podemos despejar u en (9.4) y sustituirlo en (9.3). Así obtenemos $v + 2acv^{-1} \equiv 1 \pmod{2^n}$, o equivalentemente:

$$v(v-1) \equiv -2ac \pmod{2^n}$$

Si demostramos que esta congruencia tiene solución v impar, entonces (9.3) nos permitirá calcular u, y tendremos probado que xy es equivalente a cualquier

forma con discriminante $D \equiv 1 \pmod 8$. Ahora bien, es fácil ver que la congruencia $v^2 - v - 2k \equiv 0 \pmod 8$ tiene solución para todo k, y el teorema 7.17 implica que existe un entero diádico v tal que $v^2 - v - 2k = 0$. Tomando clases módulo 2^n obtenemos la solución buscada.

Consideremos ahora el caso $D \not\equiv 1 \pmod 8$. En primer lugar probamos que si a, b, c y r son impares entonces la congruencia

$$ax^2 + bxy + cy^2 \equiv r \pmod{2^n} \tag{9.5}$$

tiene solución. Dividiendo entre r podemos suponer $a = 1$. Así nos queda la forma $f(x, y) = x^2 + bxy + (2k + 1)y^2$. Observamos que

$$f(1,0) = 1, \quad f(1,2) = 2b + 5, \quad f(-1,2) = -2b + 5 \ \text{ y } \ f(1,4) = 1 + 4b$$

son cuatro impares distintos módulo 8, luego uno de ellos es congruente con r módulo 8, es decir, se cumple (9.5) módulo 8. Además en cualquiera de los cuatro casos la derivada $f'_y(x, y) \equiv \pm b \pmod 4$, luego el teorema 7.17 nos da que (9.5) tiene solución en $\mathbb{Z}_2$ y por consiguiente también módulo 2^n.

En particular existen enteros u y v tales que $au^2 + buv + cv^2 \equiv 1 \pmod{2^n}$. Uno de los dos ha de ser impar. Supongamos que es u. El cambio de variables $x = ux'$, $y = vx' + y$ nos convierte la forma de partida en otra equivalente con $a = 1$. El cambio $y' = by$ nos hace $b = 1$, luego toda forma en el caso que estamos estudiando es equivalente módulo 2^n a una de la forma $x^2 + xy + (2k + 1)y^2$.

Vamos a probar que la forma $x^2 + xy + y^2$ se puede transformar en ésta mediante un cambio adecuado. Concretamente hacemos $x = x' + uy'$, $y = vy'$, (con v impar) con lo que llegamos a $x^2 + (2u + v)xy + (u^2 + uv + v^2)y^2$. Hemos de conseguir

$$\begin{aligned} 2u + v &\equiv 1 \pmod{2^n} \\ u^2 + uv + v^2 &\equiv 2k + 1 \pmod{2^n} \end{aligned}$$

Al despejar v en la primera congruencia y sustituir en la segunda llegamos a la misma congruencia que antes, a saber: $u^2 - u \equiv \text{impar} \pmod{2^n}$, que ya sabemos que tiene solución.

Por último notamos que las dos formas del enunciado no son equivalentes módulo 2^n, pues evidentemente xy representa a todos los enteros, mientras que $x^2 + xy + y^2 \not\equiv 2 \pmod 4$. ∎

En particular el teorema anterior prueba que todas las formas cuadráticas con discriminante impar son equivalentes módulo 2^n. Al igual que hemos hecho con los primos impares, definimos el *carácter* módulo 2 de una forma f con discriminante impar como $\chi_2(f) = 1$. Así sigue siendo cierto en este caso que dos formas con el mismo discriminante son equivalentes módulo p^n si y sólo si tienen el mismo carácter módulo p.

Ya sólo nos queda el caso en que 2 divide al discriminante. Este caso presenta diferencias relevantes respecto al de los primos impares, debidas esencialmente

a que el índice del subgrupo de los cuadrados en U_{2^n} no es 2, sino 4. En efecto, dado un entero impar a, del teorema 8.12 se sigue que a se expresa como $a = r\epsilon^2$, donde $r = \pm 1, \pm 5$ y ϵ es una unidad diádica. Tomando restos módulo 2^n obtenemos que $a \equiv rk^2 \pmod{2^n}$ para cierto entero impar k.

Teniendo esto en cuenta, procedemos como en el caso de los primos impares. Dada una forma cuadrática $ax^2+2bxy+cy^2$, pasando a otra equivalente podemos suponer que a es impar. El cambio $x = x' - by$, $y = ay'$ la transforma en $a(x^2 - D'y^2)$, donde $D' = D/4$. Por último, expresando $a \equiv rk^2 \pmod{2^n}$ y haciendo el cambio $x' = kx$, $y' = ky$ llegamos a una forma equivalente a una de las cuatro formas

$$r(x^2 - D'y^2), \qquad r = \pm 1, \pm 5. \tag{9.6}$$

Ahora vamos a ver que si $x^2 - D'y^2$ representa r módulo 8, entonces es equivalente con la correspondiente forma de (9.6) módulo 2^n. En efecto, suponemos que existen enteros u, v tales que $A = u^2 - D'v^2 \equiv r \pmod 8$. El cambio $x = ux' + D'vy'$, $y = vx' + uy'$ nos transforma $x^2 - D'y^2$ en $A(x^2 - D'y^2)$. Ahora expresamos $A \equiv r'k^2 \pmod{2^n}$, donde $r' = \pm 1, \pm 5$, y al tomar restos módulo 8 queda que $r' = r$, con lo que el cambio $x' = kx$, $y' = ky$ nos lleva a una forma equivalente a (9.6) para el r considerado.

En vista de esto estudiamos los impares representados módulo 8 por la forma $x^2 - D'y^2$. Son los indicados en la tabla siguiente, en función del resto de D' módulo 8:

D'	0	1	2	3	4	5	6	7
r	1	± 1	± 1	1	1	± 1	1	1
		± 5		5	5	± 5	-5	5

La tabla se interpreta como sigue:

- Si $D/4 \equiv 1, 5 \pmod 8$ entonces $x^2 - D'y^2$ representa todos los impares módulo 8, luego es equivalente a todas las formas (9.6) y así, todas las formas de discriminante D son equivalentes módulo 2^n.

- Si $D/4 \equiv 3, 4, 7 \pmod 8$ entonces las formas $x^2 - D'y^2$ y $5(x^2 - D'y^2)$ son equivalentes, de donde se sigue que $-(x^2 - D'y^2)$ y $-5(x^2 - D'y^2)$ también lo son. Por lo tanto toda forma de discriminante D es equivalente a $\pm(x^2 - D'y^2)$, y estas dos no son equivalentes entre sí, pues una representa sólo los impares congruentes con $1, 5$ módulo 8, y obviamente, la otra sólo representa los congruentes con $-1, -5$ módulo 8.

- Si $D/4 \equiv 2 \pmod 8$ tenemos que $\pm(x^2 - D'y^2)$ son equivalentes, y por lo tanto $\pm 5(x^2 - D'y^2)$ también lo son. Toda forma de discriminante D es equivalente a $x^2 - D'y^2$ si los impares que representa son congruentes con ± 1 módulo 8 y es equivalente a $5(x^2 - D'y^2)$ si los impares que representa son congruentes con $\pm 5 \pmod 8$.

- Si $D/4 \equiv 6 \pmod 8$ llegamos a una conclusión similar.

- Si $D/4 \equiv 0$ (mód 8) entonces cada forma de (9.6) sólo representa a los impares congruentes con r módulo 8, luego determinan cuatro clases de formas diferentes.

Estas conclusiones se pueden expresar también en términos de caracteres, sólo que ahora hemos de distinguir entre cuatro clases módulo los cuadrados y no entre dos. El análogo al símbolo de Legendre serán ahora las funciones siguientes:

Definición 9.6 Las funciones δ y ϵ, definidas sobre los enteros impares, son las dadas por

$$\delta(k) = (-1)^{(k-1)/2} = \begin{cases} 1 & \text{si } k \equiv \ \ 1 \text{ (mód 4)} \\ -1 & \text{si } k \equiv -1 \text{ (mód 4)} \end{cases}$$

$$\epsilon(k) = (-1)^{(k^2-1)/8} = \begin{cases} 1 & \text{si } k \equiv \pm 1 \text{ (mód 8)} \\ -1 & \text{si } k \equiv \pm 5 \text{ (mód 8)} \end{cases}$$

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

$$\chi_2(f) = \begin{cases} 1 & \text{si } \ D/4 \equiv 1,5 \text{ (mód 8)} \\ \epsilon(a) & \text{si } \ D/4 \equiv 2 \text{ (mód 8)} \\ \delta(a) & \text{si } \ D/4 \equiv 3,4,7 \text{ (mód 8)} \\ \delta(a)\epsilon(a) & \text{si } \ D/4 \equiv 6 \text{ (mód 8)} \end{cases}$$

Si $D/4 \equiv 0$ (mód 8) definimos tres caracteres de f módulo 2, dados por

$$\chi_{21}(f) = \delta(a), \quad \chi_{22}(f) = \epsilon(a), \quad \chi_{23}(f) = \delta(a)\epsilon(a).$$

Hemos demostrado que estos caracteres no dependen de la elección de a así como que formas equivalentes módulo p^n tienen el mismo carácter (o los mismos caracteres [1]) módulo p, para todo primo p, por lo que tiene sentido hablar del carácter de una clase de equivalencia de formas. Además tenemos el resultado siguiente:

Teorema 9.7 *Si p es primo, dos formas cuadráticas de discriminante D son equivalentes módulo p^n si y sólo si tienen el mismo carácter módulo p. Esto ocurre siempre que $p \nmid D$.*

Para tratar unificadamente todos los casos en la medida de lo posible, conviene observar que para cada discriminante D y para cada primo p tenemos definida una función $\chi_p^* : U_p \longrightarrow \{\pm 1\}$ si p es impar, o $\chi_2^* : U_8 \longrightarrow \{\pm 1\}$ si

[1] En lo sucesivo, cuando hablemos del carácter de una forma módulo un primo p habremos de recordar que si $p = 2$ puede haber en realidad tres caracteres, si bien no lo indicaremos explícitamente en cada ocasión para evitar constantes y monótonas salvedades como ésta.

$p = 2$, 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.

La función 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 $1, \delta, \epsilon, \epsilon\delta$ si $p = 2$. Es importante notar que cualquiera de ellas es multiplicativa, es decir, $\chi_p^*(xy) = \chi_p^*(x)\chi_p^*(y)$, así como que $\chi_p^*(x)$ sólo depende del resto de x módulo D (si D es par pero $8 \nmid D$, entonces $\chi_2^* = 1, \delta$, y en realidad depende del resto de x módulo 4).

9.2 Géneros de formas y módulos

Definición 9.8 Diremos que dos formas cuadráticas de un mismo discriminante D son del mismo *género* si tienen los mismos caracteres.

Esto completa la clasificación de las formas cuadráticas binarias: éstas se dividen en órdenes según su discriminante, las formas de cada orden se dividen a su vez en géneros según sus caracteres, y las formas de un mismo género se distribuyen en clases de equivalencia (en $\mathbb{Z}$). Por último cada clase de equivalencia puede dividirse en dos clases de equivalencia estricta.

Según los teoremas 9.2 y 9.7, dos formas son del mismo género si y sólo si representan los mismos enteros módulo cualquier número natural $n > 1$.

Ejemplo En el capítulo VI calculamos las formas cuadráticas reducidas de discriminante $D = -504 = -2^3 \cdot 3^2 \cdot 7$. Para este discriminante tenemos tres caracteres no triviales, χ_2, χ_3 y χ_7. El carácter módulo 2 viene inducido por $\chi_2^* = \epsilon$. La tabla siguiente contiene todas las formas reducidas de discriminante D junto con su sistema de caracteres. Vemos que las ocho clases de equivalencia se reparten en cuatro géneros, a dos clases por género.

Forma	χ_2	χ_3	χ_7
$x^2 + 126y^2$	$+$	$+$	$+$
$7x^2 + 18y^2$	$+$	$+$	$+$
$9x^2 + 14y^2$	$+$	$-$	$+$
$2x^2 + 63y^2$	$+$	$-$	$+$
$10x^2 + 4xy + 13y^2$	$-$	$+$	$-$
$10x^2 - 4xy + 13y^2$	$-$	$+$	$-$
$5x^2 + 4xy + 26y^2$	$-$	$-$	$-$
$5x^2 - 4xy + 26y^2$	$-$	$-$	$-$

En particular notamos que, aunque tres caracteres podrían definir ocho géneros, de hecho sólo aparecen cuatro. Concretamente sucede que $\chi_2 = \chi_7$. ∎

Todas las regularidades que se aprecian en este ejemplo pueden ser explicadas teóricamente. Para ello conviene reformular la teoría de los géneros en términos de ideales, donde tenemos una estructura de grupo.

En el capítulo VI definimos una correspondencia biunívoca entre las clases de equivalencia estricta de formas cuadráticas de discriminante D y las clases de similitud estricta de los módulos cuyo anillo de coeficientes es el orden cuadrático de discriminante D. A través de esta correspondencia podemos definir 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. Así mismo definimos los *caracteres* y el *género* de un módulo en particular como los de su clase de similitud estricta.

Conviene tener presente que dos módulos similares no son necesariamente del mismo género. Para ver ejemplos de esta situación consideramos un orden numérico de discriminante $D > 0$. Siguiendo la notación que introdujimos en el capítulo VI, llamamos 1 y -1 a las clases de similitud estricta de los ideales principales generados respectivamente por números de norma positiva o negativa. Sabemos que una forma asociada a 1 es la forma principal, que representa a 1, y por lo tanto todos sus caracteres son positivos. Al estudiar la relación entre módulos y formas vimos también que a -1 le corresponde la forma principal cambiada de signo, que representa a -1. Si, por ejemplo, D es divisible entre un primo impar p tal que $(-1/p) = -1$, entonces, dado cualquier módulo M del orden considerado, el módulo $\sqrt{D}\,M$ es similar a M pero tiene carácter distinto módulo p.

Notemos que hemos probado lo siguiente:

Teorema 9.9 *En un orden cuadrático real, $\chi_p(-1) = \chi_p^*(-1)$, para número primo p.*

Recordemos ahora el teorema 6.11, 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. Los resultados del capítulo 3 nos garantizan que estos ideales heredan el buen comportamiento de los de los órdenes maximales a través de la correspondencia descrita en el teorema 3.27. Teniendo esto en cuenta, el teorema siguiente nos permite calcular los caracteres de una clase sin necesidad de pasar por la clase de formas asociada.

Teorema 9.10 *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 $\chi_p(\mathfrak{a}) = \chi_p^*\big(\mathrm{N}(\mathfrak{a})\big)$.*

Demostración: Hemos de calcular el carácter de cualquier forma cuadrática asociada a $\mathfrak{a}$. Según el capítulo VI, tomamos una base orientada de $\mathfrak{a}$, digamos (α, β), y una tal forma es la dada por $f(x, y) = \mathrm{N}(\alpha x + \beta y)/\mathrm{N}(\mathfrak{a})$.

Ahora bien, sabemos que $\mathfrak{a} \mid \mathrm{N}(\mathfrak{a})$, es decir, $\mathrm{N}(\mathfrak{a}) \in \mathfrak{a}$, luego existen enteros racionales u, v tales que $\mathrm{N}(\mathfrak{a}) = \alpha u + \beta v$. Entonces

$$f(u, v) = \mathrm{N}\big(\mathrm{N}(\mathfrak{a})\big)/\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}),$$

luego efectivamente, $\chi_p(\mathfrak{a}) = \chi_p(f) = \chi_p^*\big(\mathrm{N}(\mathfrak{a})\big)$. ∎

Este teorema tiene muchas consecuencias. La más importante es que, en términos de módulos, los caracteres son homomorfismos de grupos:

Teorema 9.11 *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 $\{\pm 1\}$.*

DEMOSTRACIÓN: Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}$ estrictamente similares a M y N respectivamente y con normas primas con p. Entonces

$$\begin{aligned}\chi_p(MN) &= \chi_p(\mathfrak{ab}) = \chi_p^*\big(\mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})\big) = \chi_p^*\big(\mathrm{N}(\mathfrak{a})\big)\chi_p^*\big(\mathrm{N}(\mathfrak{b})\big)\\ &= \chi_p(\mathfrak{a})\chi_p(\mathfrak{b}) = \chi_p(M)\chi_p(N).\end{aligned}$$

■

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.

Ejemplo En el capítulo VI calculamos el grupo de clases de $\mathbb{Q}\big(\sqrt{-161}\big)$. Vimos que tiene orden 16, y está generado por las clases $\sigma = [3_1]$, de orden 8, y $\tau = [7_0]$, de orden 2. Sus formas cuadráticas asociadas son $3x^2 + 2xy + 54y^2$ y $7x^2 + 23y^2$, respectivamente. Por otro lado, el discriminante es $\Delta = -4 \cdot 7 \cdot 23$ y los caracteres a considerar son χ_2 (que se calcula con $\chi_2^* = \delta$), χ_7 y χ_{23}. De aquí obtenemos inmediatamente que los caracteres de σ son $(--+)$ y los de τ son $(-+-)$. Los restantes se calculan mediante el teorema 9.11:

1	$+++$	σ^4	$+++$	τ	$-+-$	$\tau\sigma^4$	$-+-$
σ	$--+$	σ^5	$--+$	$\tau\sigma$	$+--$	$\tau\sigma^5$	$+--$
σ^2	$+++$	σ^6	$+++$	$\tau\sigma^2$	$-+-$	$\tau\sigma^6$	$-+-$
σ^3	$--+$	σ^7	$--+$	$\tau\sigma^3$	$+--$	$\tau\sigma^7$	$+--$

Vemos que aparecen cuatro géneros: $(+++), (--+), (-+-), (+--)$ y que hay exactamente cuatro clases de cada género. ■

La única propiedad que observamos y que todavía no sabemos justificar es por qué el número de géneros siempre es la mitad del número máximo posible.

La explicación hay que buscarla en los géneros del orden maximal de un cuerpo cuadrático y en su relación con los géneros de sus otros órdenes. Conviene introducir algunas definiciones.

Definición 9.12 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.

En el caso en que haya tres caracteres módulo 2, sólo consideraremos fundamental a uno de ellos, al único que cumple el teorema siguiente:

Teorema 9.13 *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 8.27.

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 8.25)

$$\chi_p(f) = \left(\frac{a}{p}\right) = (a, p)_p = (a, D)_p.$$

Si $p = 2$ (y a es impar) distinguimos casos según el resto de $D/4$ módulo 8. Observar 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 8.26 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 $\mathcal{O}$, entonces 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.

Ejemplo En el capítulo VI calculamos el epimorfismo entre el grupo de clases del orden de discriminante $D = -504 = -8 \cdot 9 \cdot 7$ y el de su orden maximal, de discriminante $D_0 = -56 = -8 \cdot 7$. La tabla siguiente muestra los géneros de ambos grupos de clases:

$x^2 + 126y^2$	$+\,+\,+$	$x^2 + 14y^2$	$+\,+$
$9x^2 + 14y^2$	$+\,-\,+$		
$7x^2 + 18y^2$	$+\,+\,+$	$2x^2 + 7y^2$	$+\,+$
$2x^2 + 63y^2$	$+\,-\,+$		
$5x^2 - 4xy + 26y^2$	$-\,-\,-$	$3x^2 + 2xy + 5y^2$	$-\,-$
$10x^2 - 4xy + 13y^2$	$-\,+\,-$		
$5x^2 + 4xy + 26y^2$	$-\,-\,-$	$3x^2 - 2xy + 5y^2$	$-\,-$
$10x^2 + 4xy + 13y^2$	$-\,+\,-$		

Los caracteres fundamentales son χ_2 y χ_7. Por ello los caracteres del orden maximal se obtienen eliminando el signo central. ∎

Para órdenes maximales el teorema 9.13 puede mejorarse.

Teorema 9.14 *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 9.13 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 9.13. ∎

Ahora podemos comprender por qué el número de géneros es siempre la mitad del que *a priori* podría ser. En un orden maximal, el número de caracteres negativos de un género ha de ser par, como consecuencia del teorema 8.37 (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 9.15 *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 9.9 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 $p \equiv 1$ (mód 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 9.13 y 9.14.

El teorema siguiente es inmediato si tenemos en cuenta 8.36.

Teorema 9.16 *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 9.14 es que en un orden maximal, el género de un módulo depende sólo de su norma. Más exactamente, la situación es ésta:

Teorema 9.17 *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 8.8, 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).

9.3 El número de géneros

En esta sección demostraremos la ley de reciprocidad cuadrática contando el número de géneros. De acuerdo con el teorema 9.15 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 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 9.18 *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 $p_1, \ldots, p_r$ 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

$$\begin{aligned} \zeta &\equiv \pi_i^{c_i} \pmod{\mathfrak{p}_i^{c_i+1}}, \\ \zeta &\equiv 1 \pmod{\mathfrak{q}_i^{c_i+1}}. \end{aligned}$$

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 —ver la tabla 3.1— se sigue inmediatamente de la hipótesis). Podemos aplicar el teorema 3.7 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 9.19 (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 6.11 podemos suponer que $\mathfrak{a}$ es un ideal de norma prima con m. El teorema 9.17 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

$$[\mathfrak{a}] = \prod_i [\mathfrak{p}_i]^{a_i-u_i+v_i-b_i} = \prod_i [\mathfrak{p}_i]^{2(a_i-u_i)} = \Big[\prod_i \mathfrak{p}_i^{a_i-u_i}\Big]^2.$$

■

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

$$H = \langle c_1\rangle \times \cdots \times \langle c_r\rangle \times \langle d_1\rangle \times \cdots \times \langle d_s\rangle\,, \tag{9.7}$$

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 (9.7), 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 9.20 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 III (ver tabla 3.1) 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 3.17), 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 9.21 *Sea $K = \mathbb{Q}\big(\sqrt{d}\,\big)$ un cuerpo cuadrático y $\mathfrak{O}$ su orden maximal. Si $\alpha \in K$ cumple que $\mathrm{N}(\alpha) = 1$, entonces existe un $\rho \in \mathfrak{O}$ 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 $\mathfrak{O}$, 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 9.22 *Cada clase ambigua de un orden cuadrático maximal $\mathfrak{O}$ contiene exactamente dos ideales ambiguos. Por lo tanto $\mathfrak{O}$ tiene exactamente 2^{m-1} clases ambiguas, luego también 2^{m-1} géneros, donde m es el número de divisores primos del discriminante de $\mathfrak{O}$.*

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.

Notar 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 9.19, 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.

9.4 El carácter de un cuerpo cuadrático

La ley de reciprocidad cuadrática tiene muchas repercusiones sobre los cuerpos cuadráticos. En esta sección veremos que determina unas reglas muy sencillas sobre el tipo de factorización de los primos racionales. Ya hemos usado en varias ocasiones que un primo racional p puede factorizar de tres formas distintas en un cuerpo cuadrático:

Definición 9.23 Sea K un cuerpo cuadrático y p un primo racional. Diremos que p se *escinde* en K si $p = \mathfrak{pq}$, donde $\mathfrak{p}$ y $\mathfrak{q}$ son dos primos distintos de K.

Diremos que p se *ramifica* en K si $p = \mathfrak{p}^2$, para un cierto primo $\mathfrak{p}$ de K. Diremos que p *se conserva* en K si p es primo en K.

Llamaremos carácter de K a la aplicación $\chi_K : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ dada por

$$\chi_K(a) = \begin{cases} \prod_{p|\Delta_K} (a, \Delta_K)_p & \text{si } (a, \Delta_K) = 1 \\ 0 & \text{si } (a, \Delta_K) \neq 1 \end{cases}$$

Seguidamente probamos que χ_K determina el carácter de los primos respecto a K (si se ramifican, se escinden o se conservan):

Teorema 9.24 *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 $\chi_K(q) = \prod_{p|\Delta_K} (q, \Delta_K)_p = 1$. El teorema 8.37 nos da que

$$\prod_p (q, \Delta_K)_p = 1, \tag{9.8}$$

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 9.8 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. ∎

Esto tiene interés porque las propiedades del símbolo de Hilbert prueban que χ_K tiene un comportamiento muy satisfactorio:

Teorema 9.25 *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 $r \equiv 1 \pmod{8m}$. 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 $r \equiv 1 \pmod 8$. 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 $(-1, \Delta)_p = (-1, p)_p = (-1/p) \equiv p \pmod 4$.

Por otra parte $(-1, \Delta)_2 = (-1, 2)_2^i\, (-1, m)_2 = (-1, m)_2 \equiv m \pmod 4$.

Al multiplicar todas las congruencias queda $\chi_K(-1) \equiv m\,|m| \pmod 4$. Notar que si Δ es impar hemos incluido un factor de más, pero no importa, pues en tal caso $(-1, \Delta)_2 \equiv m \equiv 1 \pmod 4$.

Claramente entonces $\chi_K(-1) = m/|m| = \Delta/|\Delta|$. ∎

Definición 9.26 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 $\chi_K : U_\Delta \longrightarrow \{\pm 1\}$, y vista así es un epimorfismo de grupos.

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 9.24, 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). Notar 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.

Ejemplo Vamos a calcular el carácter de $\mathbb{Q}(\sqrt{15})$, o sea, $\Delta = 60$. El grupo U_{60} es

$$\big\{[1],[7],[11],[13],[17],[19],[23],[29],[31],[37],[41],[43],[47],[49],[53],[59]\big\}$$

Comenzamos con $\chi(59) = \chi(-1) = \chi(1) = 1$.

$\chi(7) = (60/7) = (4/7) = (2/7)^2 = 1$, luego $\chi(49) = 1$, $\chi(53) = \chi(-7) = 1$, $\chi(11) = \chi(-49) = 1$.

$\chi(13) = (60/13) = (8/13) = (2/13) = -1$, luego $\chi(47) = -1$.

$\chi(17) = (60/17) = (9/17) = 1$, luego $\chi(43) = 1$.

Como ya tenemos ocho clases de escisión, las hemos encontrado todas, a saber:

$$\big\{[1],[7],[11],[17],[43],[49],[53],[59]\big\}.$$

■

Ahora podemos probar calcular el número de géneros de los órdenes no maximales.

Teorema 9.27 *Sea $\mathcal{O}$ un orden cuadrático con m caracteres. Entonces una combinación de caracteres 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 (que probaremos en el capítulo XI). 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 1, 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 ∎

El carácter de un cuerpo cuadrático nos da una expresión sencilla para el número de ideales de una norma dada:

Teorema 9.28 *Sea K un cuerpo cuadrático. El número de ideales de K de norma k es igual a $\sum_{r|k} \chi_K(r)$.*

DEMOSTRACIÓN: Descompongamos $k = p_1^{s_1} \cdots p_t^{s_t}$ como producto de factores primos. Teniendo en cuenta la propiedad multiplicativa de χ_K se cumple que

$$\sum_{r|k} \chi_K(r) = \sum_{i=0}^{s_1} \chi_K(p_1)^i \cdots \sum_{i=0}^{s_t} \chi_K(p_t)^i.$$

Si $\chi_K(p_j) = 0$ entonces $\sum_{i=0}^{s_j} \chi_K(p_j)^i = 1$, luego estos factores no influyen.

Si $\chi_K(p_j) = -1$ entonces $\sum_{i=0}^{s_j} \chi_K(p_j)^i$ vale 1 si s_j es par y 0 si es impar. Por lo tanto la suma total es igual a 0 cuando alguno de los exponentes s_j correspondientes a primos que se conservan es impar. Ciertamente, cuando esto ocurre no hay ideales de norma k.

Si todos estos exponentes son pares entonces el sumatorio se reduce a los factores correspondientes a los primos que se escinden. Supongamos que son $p_1, \ldots, p_a$. Entonces

$$\sum_{r|k} \chi_K(r) = (s_1 + 1) \cdots (s_a + 1). \tag{9.9}$$

Hay que probar que éste es el número de ideales de norma k. Ahora bien, si $\mathfrak{a}$ es un ideal de norma k y $\mathfrak{p}$ es un primo que divide a un p_j que se ramifica o se conserva, entonces el exponente de $\mathfrak{p}$ en $\mathfrak{a}$ ha de ser $2s_j$ si p_j se ramifica o s_j si p_j se conserva.

La única variación puede darse en los exponentes de los ideales que dividen a primos racionales que se escinden $p_j = \mathfrak{pq}$, donde los exponentes de $\mathfrak{p}$ y $\mathfrak{q}$ han de cumplir únicamente que su suma sea s_j. Por lo tanto el exponente de $\mathfrak{p}$ puede ser cualquiera entre 0 y s_j, y éste determina el exponente de $\mathfrak{q}$. Así pues, cada primo p_j que se escinde da lugar a s_{j+1} variaciones en la factorización de $\mathfrak{a}$, luego el número de ideales de norma k es el dado por (9.9). ∎

Terminamos esta sección con una variante de la fórmula del teorema 4.18 en la que sustituimos la función de Euler por el carácter del cuerpo cuadrático.

Teorema 9.29 *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 4.18 obtenemos la expresión buscada. ∎

Ejercicio: Usar la fórmula del teorema anterior para calcular el número de clases del orden $\mathcal{O}_3$ de $\mathbb{Q}\left(\sqrt{-2}\right)$.

9.5 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 6.14, 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 9.30 *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. ∎

Notar 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. Así mismo, 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.

Ejemplos ¿Qué números naturales se pueden expresar como suma de dos cuadrados?

La forma $x^2 + y^2$ es la forma principal de discriminante -4 y el cuerpo asociado tiene una sola clase de similitud. El grupo U_4 está formado por las clases $\{\pm[1]\}$, y como $\chi_K(1) = 1$, ha de ser $\chi_K(-1) = -1$.

Concluimos que los números de la forma x^2+y^2 son aquellos cuya parte libre de cuadrados no contiene primos congruentes con -1 módulo 4 (o equivalentemente, está formada por primos congruentes con 1 módulo 4 más el 2). ∎

El mismo análisis vale para los números de la forma x^2+2y^2. Ahora $D=-8$ y $U_8=\{[1],[3],[5],[7]\}$. Como $(-8/3)=(1/3)=1$, tenemos $\chi_K(3)=1$, luego $\chi_K(5)=\chi_K(7)=-1$.

Los números de la forma x^2+2y^2 son aquellos cuya parte libre de cuadrados no contiene más primos que 2 y los congruentes con 1 o 3 módulo 8. ∎

Para x^2+3y^2 el discriminante es $D=-2^2\cdot 3$, luego la forma está asociada al orden $\mathcal{O}_2$ de $\mathbb{Q}(\sqrt{-3})$. El teorema anterior nos da que los números impares de la forma x^2+3y^2 son aquellos cuya parte libre de cuadrados no contiene más primos que 3 y los congruentes con 1 módulo 3. Es claro que todo número en estas condiciones es de la forma x^2+3y^2 aunque sea par. Por otra parte, 2 es primo en $\mathbb{Q}(\sqrt{-3})$ y debe dividir a los dos conjugados $x\pm y\sqrt{-3}$ con la misma multiplicidad, luego la multiplicidad de 2 en $x^2+3y^2=(x+y\sqrt{-3})(x-y\sqrt{-3})$ ha de ser par. Así, si un primo p divide a la parte libre de cuadrados de x^2+3y^2, necesariamente p es impar y se corresponde con un primo de norma p en la factorización de x^2+3y^2, luego es 3 o congruente con 1 módulo 3, es decir, la condición vale en realidad para todos los números, pares o impares. ∎

La forma x^2+4y^2 tiene discriminante -16, y está asociada al orden $\mathcal{O}_2$ de $\mathbb{Q}(i)$. El teorema anterior nos da que si k es impar entonces esta forma representa a k si y sólo si su parte libre de cuadrados consta de primos congruentes con 1 módulo 4. Si k es par entonces $x^2+4y^2=2r$ implica que x es par, luego $k=4x^2+4y^2$, luego un número par está representado por esta forma si y sólo si es múltiplo de 4 y al dividirlo entre 4 está representado por x^2+y^2.

En resumen: Los números representados por x^2+4y^2 son aquellos cuya parte libre de cuadrados consta de primos congruentes con 1 módulo 4 y el 2, pero con la condición de que si aparece el 2 su multiplicidad en k sea mayor que 1. ∎

Muy diferente es el caso de la forma x^2+5y^2. Se trata de la forma principal de discriminante -20, asociada a $\mathbb{Q}(\sqrt{-5})$, 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, el cuerpo 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 9.31 *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 9.30 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. ∎

Notar 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 9.30 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

$$(k,-20)_5 = (5,5)_5^i(5,-4)_5^i(r,5)_5 = (5,-1)_5^i(5,-1)_5^i(r,5)_5 = (r/5) = 1.$$

Así, si k es representado por una de las formas f o g, será representado 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. ∎

Ejemplos Veamos ahora un par de ejemplos de discriminante positivo. Consideremos la forma $x^2 - 2y^2$. Observar que en los casos anteriores, en último extremo, decidir si una de las formas consideradas representaba a un número dado podía resolverse en un número finito de pasos dando valores a x e y, pues los valores posibles estaban acotados. Con esta forma hay infinitas posibilidades.

El discriminante es 8 y el número de clases estrictas es 1 (porque la unidad fundamental tiene norma negativa). $U_8 = \big\{[1],[3],[5],[7]\big\}$.

Se cumple $\chi_K(1) = \chi_K(7) = 1$ (porque $\Delta > 0$), luego un número natural k es de la forma $x^2 - 2y^2$ si y sólo si su parte libre de cuadrados consta de los primos 2 y los congruentes con ± 1 módulo 8.

En realidad ésta es la condición para que cualquier número natural k esté representado por cualquier forma de discriminante 8, en particular para que k esté representado por la forma $-x^2 + 2y^2$, o sea, para que $-k$ esté representado por $x^2 - 2y^2$. Por lo tanto la condición vale para números enteros no necesariamente positivos. ∎

Vamos a calcular los primos de la forma $p = x^2 - 3y^2$. El discriminante es 12 y corresponde al orden maximal de $\mathbb{Q}\big(\sqrt{3}\big)$ (es la forma principal). Ahora la unidad fundamental tiene norma positiva, por lo que hay dos clases de formas cuadráticas no equivalentes. Un representante de la otra clase es $3x^2 - y^2$ (si una forma representa un primo p no puede representar a $-p$, o habría una unidad de norma negativa). Además hay dos géneros, luego buscamos las condiciones para que un entero p esté representado por el género principal.

La condición del teorema 9.30 es que $p = 2, 3$ o $p \equiv \pm 1$ (mód 12). Para que p esté representado por una forma del género principal hace falta además que $(p, 12)_3 = (p, 3)_3 = 1$. Esto lo cumplen sólo los primos $p \equiv 1$ (mód 12). ∎

Ejercicio: Determinar los primos de la forma $p = 3x^2 + 2xy + 5y^2$. ¿Qué podemos decir de los primos de la forma $p = x^2 + 14y^2$?

En vista de los resultados que hemos obtenido, la teoría de los géneros es especialmente útil al estudiar formas asociadas a órdenes en los que cada género contiene una única clase de similitud de ideales. La tabla 9.1 contiene los primeros discriminantes negativos con esta propiedad junto con los coeficientes (a, b, c) de formas cuadráticas representantes de cada clase.

El teorema 9.28 nos da el número de representaciones que admite un entero por formas de un discriminante dado:

Teorema 9.32 *Sea $\mathcal{O}$ un orden cuadrático y k un número natural primo con el índice de $\mathcal{O}$. Sea F un conjunto completo de representantes de las clases de similitud estricta de formas cuadráticas con anillo de coeficientes $\mathcal{O}$. Entonces el número de representaciones no asociadas de k por formas cuadráticas de F es exactamente $\sum_{r|k} \chi_K(r)$, donde K es el cuerpo cuadrático asociado a $\mathcal{O}$.*

En particular, si el orden es imaginario, el número total de soluciones de las ecuaciones $f(x, y) = k$ cuando f recorre F es $u\sum_{r|k} \chi_K(r)$, donde u es el número de unidades de $\mathcal{O}$.

Tabla 9.1: 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	$1,0,28$		$5,0,9$		$7,0,10$		
	$3,3,5$		$4,0,7$		$7,4,7$				

Este teorema es especialmente útil cuando se aplica a los órdenes en los que cada género contiene una sola clase de similitud de ideales. Entonces dos formas cuadráticas representan a un mismo entero si y sólo si son equivalentes. Así, en los términos del teorema anterior, si una forma f de F representa a k, ninguna otra forma de F lo representa, por lo que la fórmula da el número de soluciones no asociadas de una ecuación $f(x,y) = k$ para una forma fija f cuando k es primo con el índice del orden asociado y supuesto que la ecuación tenga al menos una solución.

De aquí se deduce un criterio de primalidad:

Teorema 9.33 *Sea $f(x,y)$ una forma cuadrática asociada a un orden de discriminante $\Delta < -4$ en el que cada género contenga una única clase de similitud*

estricta de ideales. Sea p un número natural primo con Δ que se expresa exactamente de cuatro formas distintas como $p = f(x,y)$ con $(x,y) = 1$. Entonces p es primo.

DEMOSTRACIÓN: El orden de f tendrá exactamente dos unidades, luego el teorema anterior junto con 9.28 nos da que su cuerpo cuadrático tiene exactamente dos ideales de norma p. Más aún, en la demostración de 9.28 se ve que el número de ideales de norma p viene dado por la fórmula 9.9, de donde se sigue que p es divisible entre un único primo que se escinde y además con multiplicidad 1. Basta ver que p no es divisible entre primos que se conservan o se ramifican. Ciertamente, p no es divisible entre primos que se ramifican, pues por hipótesis es primo con el discriminante del cuerpo. Supongamos que q es un primo que se conserva y divide a p.

Consideremos un módulo asociado a la forma f. Podemos exigir que sea un ideal de norma prima con q. Más aún, según el teorema 6.9 podemos tomarlo de la forma $\mathfrak{a} = \langle a, b + m\omega\rangle$, donde $\mathrm{N}(\mathfrak{a}) = a$. Cambiando f por una forma estrictamente equivalente, podemos suponer que

$$p = f(x,y) = \frac{\mathrm{N}(ax + (b+m\omega)y)}{a}.$$

Notar que si $(x,y) = 1$ y aplicamos un cambio de variables lineal de determinante 1, las imágenes siguen cumpliendo lo mismo. El numerador es un entero racional, luego tenemos que $q \mid \mathrm{N}(ax + (b + m\omega)y)$, y como q es primo en el orden cuadrático, también $q \mid ax + (b + m\omega)y$. Esto implica que $q \mid ax + by$, $q \mid my$, con lo que $q \mid y$ y $q \mid ax$, lo cual es imposible. ∎

Un caso particular de este teorema era ya conocido por Euler, quien lo usó para encontrar primos grandes. Concretamente, Euler definió un *número idóneo* (o conveniente) como un número natural n tal que —en nuestros términos— el orden de discriminante $-4n$ tiene una sola clase de similitud estricta de ideales en cada género. Entonces se cumple:

> Si n es un número idóneo y p es un número impar que se expresa de forma única como $p = x^2 + ny^2$, para ciertos números naturales x, y tales que $(x, ny) = 1$, entonces p es primo.

Las cuatro representaciones de las que habla el teorema anterior son entonces $(\pm x, \pm y)$. Euler encontró los siguientes números idóneos:

Tabla 9.2: Los números idóneos de Euler

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40,$$
$$42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165,$$
$$168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462,$$
$$520, 760, 840, 1.320, 1.365, 1.848.$$

No se conoce ninguno más, y de hecho se conjetura que no los hay.

Ejercicio: Probar que $3.049 = 7^2 + 120 \cdot 5^2$ es primo.

Ejemplo El mayor número primo que encontró Euler con ayuda de los números convenientes es $p = 18.518.809 = 197^2 + 1.848 \cdot 100^2$. Vamos a esbozar un argumento (debido a Gauss) que lo demuestra. Un cálculo directo obligaría a comprobar que p no es divisible entre los primeros 590 primos.

Hemos de probar que la única solución de la ecuación

$$p = x^2 + 1.848\, y^2 \tag{9.10}$$

es $x = 197$, $y = 100$. Una tal solución cumple $x^2 \equiv 1$ (mód 1.848). Como $1.848 = 8 \cdot 3 \cdot 7 \cdot 11$, esto es equivalente a que $x^2 \equiv 1$ (mód 8), $x^2 \equiv 1$ (mód 3), $x^2 \equiv 1$ (mód 7), $x^2 \equiv 1$ (mód 11), o a que $x \equiv 1$ (mód 2), $x \equiv \pm 1$ (mód $3, 7, 11$).

Por el teorema chino del resto, $x \equiv \pm 1, \pm 43, \pm 155 \pm 197$ (mód 462) (notar que $462 = 2 \cdot 3 \cdot 7 \cdot 11$). Puesto que $x < \sqrt{p}$, esto nos da 76 posibilidades para x:

$$\begin{aligned}
1 + 462k &\qquad 0 \le k \le 9,\\
-1 + 462k &\qquad 1 \le k \le 9,\\
43 + 462k &\qquad 0 \le k \le 9,\\
-43 + 462k &\qquad 1 \le k \le 9,\\
155 + 462k &\qquad 0 \le k \le 9,\\
-155 + 462k &\qquad 1 \le k \le 9,\\
197 + 462k &\qquad 0 \le k \le 9,\\
-197 + 462k &\qquad 1 \le k \le 9.
\end{aligned}$$

Hay que descartarlas todas menos $x = 197$. La mayoría de ellas se eliminan tomando congruencias. Por ejemplo, consideremos el primo 5. Al tomar congruencias módulo 5 en la ecuación (9.10) queda $x^2 + 3y^2 \equiv 4$ (mód 5). Como $y^2 \equiv 0, 1, 4$ (mód 5), resulta $x^2 \equiv 1, 2, 4$ (mód 5), pero 2 no es un resto cuadrático módulo 5, y por consiguiente $x^2 \equiv 1, 4$ (mód 5). Esto equivale a que $x \not\equiv 0$ (mód 5).

Si consideramos, por ejemplo $x = 1 + 462k \equiv 1 + 2k$ (mód 5), la condición es $2k \not\equiv -1$ (mód 5), o también $k \not\equiv 2$ (mód 5), lo que nos elimina los casos $k = 2, 7$. Del mismo modo eliminamos un par de casos de cada una de las ocho sucesiones.

Repitiendo el proceso con el primo 13 eliminamos los valores $k = 0, 4, 5, 9$ de la primera sucesión.

Cuando el primo que usamos divide a 1.848 hemos de tomar congruencias módulo una potencia, para evitar identidades triviales. Por ejemplo, si usamos el 3 hemos de plantear $x^2 + 3y^2 \equiv 4$ (mód 9). Como $y^2 \equiv 0, 1$ (mód 3), ha de ser $3y^2 \equiv 0, 3$ (mód 9), luego $x^2 \equiv 1, 4$ (mód 9). Si lo aplicamos a la primera sucesión obtenemos

$$(1 + 462k)^2 \equiv (1 + 3k)^2 \equiv 1 + 6k \equiv 1, 4 \text{ (mód 9)},$$

de donde $6k \equiv 0, 3$ (mód 9), $2k \equiv 0, 1$ (mód 3), $k \equiv 0, 2$ (mód 3), lo cual nos descarta el valor $k = 3$.

Tomando congruencias módulo 9, 5, 49, 121, 13, 17, 19 y 23 descartamos todos los casos excepto $-43 + 3 \cdot 462$, $-155 + 6 \cdot 462$ y 197. Los dos primeros pueden descartarse directamente, despejando y^2 de (9.10) y comprobando que el número que obtenemos no es realmente un cuadrado. ∎

9.6 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 9.34 *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 el teorema 9.9, $\chi_p(-1) = (-1/p) = -1$, 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. Según vimos en el capítulo VI, la similitud estricta difiere de la no estricta sólo si la unidad fundamental tiene norma positiva. ∎

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 9.3: 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 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 9.35 *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 9.19 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 9.34 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 9.34 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. Notar que no requiere teoría de géneros.

Teorema 9.36 *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 $\mathbb{Q}(\sqrt{d})$.*

DEMOSTRACIÓN: Notar que $d \equiv 1$ (mód 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:

$$-15 = 1^2 - 4\cdot 2^2, \quad -23 = 3^2 - 4\cdot 2^3, \quad -31 = 1^2 - 4\cdot 2^3,$$

$$-47 = 9^2 - 4\cdot 2^5, \quad -71 = 21^2 - 4\cdot 2^7, \quad -79 = 7^2 - 4\cdot 2^5,$$

$$-271 = 89^2 - 4\cdot 2^{11}.$$

Tabla 9.4: 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 el indicado en 2.5.

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 9.5: 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 el indicado en 2.5. 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)	$++$
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)	$++$
						$(3,1+\alpha)$	$--$

d	Δ	h	$\sqrt{\alpha}$	ϵ	$\mathrm{N}(\epsilon)$	Clases	Caract.
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)	$+$
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)	$+++$
						$(2, \alpha)$	$--+$

d	Δ	h	$\sqrt{\alpha}$	ϵ	$\mathrm{N}(\epsilon)$	Clases	Caract.
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 X

El Último Teorema de Fermat

En los capítulos anteriores hemos aplicado la teoría de los cuerpos numéricos al estudio de la teoría de Gauss, que éste desarrolló enteramente en términos de formas cuadráticas. El lector se hará idea, sin duda, de la enorme ventaja que supone sustituir las formas por ideales en los resultados principales. Sin embargo, hemos de recordar que la teoría de ideales no surgió de aquí, sino del trabajo de Kummer en torno al último teorema de Fermat, por lo que es ilustrativo ahondar en su relación con este problema. En el capítulo I vimos ya los precedentes. Según dijimos, el primer resultado al respecto, después del teorema 1.1, es la prueba de Euler para el caso $p = 3$. Conviene que nos detengamos en ella.

10.1 El caso $p = 3$

Teorema 10.1 *No existen enteros no nulos x, y, z tales que $x^3 + y^3 = z^3$.*

DEMOSTRACIÓN: Vamos a seguir la prueba del teorema 1.1. Para empezar suponemos que existen números (x, y, z) que cumplen $x^3 + y^3 = z^3$. Dividiéndolos entre su m.c.d. podemos suponer que son primos entre sí y, al cumplir la ecuación, han de ser primos entre sí dos a dos. Es obvio que a lo sumo uno de los tres números puede ser par, pero si x, y son impares entonces z es par, luego exactamente uno de ellos es par.

Por simetría podemos suponer que x e y son impares. Entonces $x+y$, $x-y$ son pares, digamos $x + y = 2p$, $x - y = 2q$. Así $x = p + q$, $y = p - q$.

Ahora consideramos la factorización siguiente:

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2).$$

Sustituyendo obtenemos

$$x^3 + y^3 = 2p\left((p + q)^2 - (p + q)(p - q) + (p - q)^2\right) = 2p(p^2 + 3q^2).$$

Además podemos afirmar que p y q son primos entre sí (un factor común lo sería de x e y) y tienen paridades opuestas (porque $x = p + q$ es impar). Cambiando el signo de x, y, z si es necesario podemos suponer que $x + y > 0$, luego $p > 0$ e, intercambiando x con y si es necesario, también $q > 0$ (no puede ser que $x = y$, pues q sería 0, y como $(x, y) = 1$ habría de ser $x = y = 1$, y entonces $z^3 = 2$, lo cual es imposible).

En resumen, si existe una solución (x, y, z) con x e y impares, entonces existen números naturales no nulos p y q de paridad opuesta, primos entre sí tales que el número $2p(p^2 + 3q^2)$ es un cubo.

El análogo en la prueba del teorema 1.1 era la factorización $x^2 = 4ab(a^2+b^2)$, que nos daba que $ab(a^2+b^2)$ debía ser un cuadrado. Igualmente nosotros hemos de justificar que los números $2p$ y $p^2 + 3q^2$ son primos entre sí, con lo que cada uno de ellos será un cubo.

En realidad esto no tiene por qué ser cierto, pero poco falta. Notemos primero que, como p y q tienen paridad opuesta, $p^2 + 3q^2$ es impar, de donde se sigue claramente que $(2p, p^2 + 3q^2) = (p, p^2 + 3q^2) = (p, 3q^2)$ y como $(p, q) = 1$ el único factor común de p y $3q^2$ es 3. En otras palabras, si $3 \nmid p$, entonces $(2p, p^2 + 3q^2) = 1$. Supongamos que es así.

Entonces, según lo dicho, $2p$ y $p^2 + 3q^2$ son cubos. Ahora necesitamos un resultado que juegue el papel de la clasificación de las ternas pitagóricas en la prueba de 1.1. Se trata del hecho siguiente que demostraremos después:

> (∗) *Si los enteros p, q, r cumplen $p^2 + 3q^2 = r^3$, $(p, q) = 1$ y r es impar, entonces existen enteros a y b tales que $p = a^3 - 9ab^2$, $q = 3a^2b - 3b^3$, $r = a^2 + 3b^2$.*

Admitiendo esto, $p = a(a - 3b)(a + 3b)$, $q = 3b(a - b)(a + b)$. Claramente a y b son primos entre sí y tienen paridades opuestas (o si no p y q serían pares).

Por otra parte $2p = 2a(a - 3b)(a + 3b)$ es un cubo. Veamos de nuevo que los factores $2a$, $a - 3b$ y $a + 3b$ son primos entre sí dos a dos, con lo que los tres serán cubos.

Como a y b tienen paridades opuestas, $a - 3b$ y $a + 3b$ son impares, luego un factor común de $2a$ y $a \pm 3b$ es un factor de a y $a \pm 3b$, luego también un factor común de a y $3b$. Igualmente un factor común de $a + 3b$ y $a - 3b$ lo es de a y $3b$, luego basta probar que $(a, 3b) = 1$. Puesto que $(a, b) = 1$, lo contrario obligaría a que $3 \mid a$, pero entonces $p \mid 3$ y estamos suponiendo lo contrario.

Así pues, $2a = u^3$, $a-3b = v^3$, $a+3b = w^3$, luego $v^3+w^3 = 2a = u^3$. Nuestro objetivo es encontrar una solución de la ecuación de Fermat con z^3 par y menor (en valor absoluto) que el valor del que hemos partido. Así podremos concluir que no pueden existir tales soluciones ya que no puede haber una mínima. Hemos de reordenar la terna (u, v, w) para dejar en tercer lugar la componente par. Como $u^3v^3w^3 = 2a(a-3b)(a+3b) = 2p \mid z^3$, lo cierto es que la componente par, sea cual sea, es menor en módulo que z^3.

Falta llegar a la misma conclusión si $3 \mid p$. Supongamos que $p = 3s$ y que $3 \nmid q$. Entonces nuestro cubo es $2p(p^2 + 3q^2) = 3^2 \cdot 2s\,(3s^2 + q^2)$ y los números $3^2 \cdot 2s$ y $3s^2 + q^2$ son primos entre sí, pues $(s, q) = 1$ obliga a que los únicos

divisores comunes posibles sean 2 y 3, pero $3s^2+q^2$ es impar (luego 2 no sirve) y $3 \nmid q$, (luego tampoco sirve).

Consecuentemente $3^2 \cdot 2s = u^3$ y $3s^2+q^2 = v^3$. Aplicando $(*)$ llegamos a que $q = a(a-3b)(a+3b)$, $s = 3b(a-b)(a+b)$.

Por otro lado $3^2 \cdot 2s = 3^3 \cdot 2b(a-b)(a+b)$ es un cubo, luego $2b(a-b)(a+b)$ también lo es. El resto es prácticamente igual al caso anterior. ∎

Nos falta demostrar $(*)$. Euler supuso la factorización única en el anillo $\mathbb{Z}\big[\sqrt{-3}\,\big]$. Aunque esto es falso, en el capítulo IV probamos que su número de clases es 1, lo que se traduce en que sus elementos de norma impar sí se descomponen de forma única como producto de primos, y esto basta. En efecto, como $(p,q) = 1$ el número $p+q\sqrt{-3}$ no es divisible entre enteros no unitarios, es decir, no es divisible entre primos que se conservan, y si un primo $p = \pi_1\pi_2$ se escinde y $\pi_1 \mid p+q\sqrt{-3}$, entonces $\pi_2 \nmid p+q\sqrt{-3}$. Por lo tanto la descomposición en primos es

$$p+q\sqrt{-3} = \pi_1^{n_1}\cdots\pi_r^{n_r},$$

donde $\mathrm{N}(\pi_i) = p_i$ son primos distintos dos a dos. Tomando normas queda que

$$r^3 = p_1^{2n_1}\cdots p_r^{2n_r},$$

luego $3 \mid n_i$ para todo i, lo que implica que $p+q\sqrt{-3}$ es un cubo en $\mathbb{Z}\big[\sqrt{-3}\,\big]$. Por consiguiente

$$p+q\sqrt{-3} = \big(a+b\sqrt{-3}\,\big)^3 = a^3-9ab^2+(3a^2b-3b^3)\sqrt{-3},$$

y esto prueba $(*)$. ∎

Ejercicio: Probar que, aunque $4^2+3\cdot 4^2 = 8^3$, no es cierto que $p = q = 4$ tengan la forma indicada en $(*)$.

Ejercicio: Probar $(*)$ sin suponer que r sea impar.

10.2 El teorema de Kummer

Según explicamos en el capítulo I, Kummer siguió la idea de Lamé de considerar la factorización

$$x^p+y^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y), \tag{10.1}$$

donde ω es una raíz p–ésima de la unidad. Kummer creyó haber probado el teorema de Fermat completo hasta que Dirichlet le hizo notar que su prueba suponía la factorización única de los anillos de enteros ciclotómicos. Ello le llevó a investigar si dicha factorización única era cierta, para completar así su prueba. Como ya sabemos, la conclusión fue que en general es falsa, pero al mismo tiempo descubrió la factorización única en ideales. El paso siguiente era determinar si el argumento que probaba el teorema de Fermat suponiendo la factorización única real seguía siendo válido usando únicamente la factorización

única ideal. El resultado fue que hacían falta algunas hipótesis adicionales. Vamos a describir el problema con más detalle. Según lo dicho, partimos de la factorización 10.1. Siguiendo el esquema de la prueba de Euler, hemos de estudiar si los monomios $x + \omega^i y$ son primos entre sí.

Como en el caso $p = 3$, si la ecuación $x^p + y^p = z^p$ tiene solución, podemos suponer que x, y, z son primos entre sí dos a dos.

Si dos monomios $x + \omega^i y$, $x + \omega^j y$ (digamos con $i < j$) tienen un factor en común, entonces este factor divide a

$$(x + \omega^j y) - (x + \omega^i y) = \omega^{j-i}(\omega^i - 1)y = \text{unidad } (\omega - 1)y, \tag{10.2}$$

así como a

$$(x + \omega^j y) - \omega^{j-i}(x + \omega^i y) = \text{unidad } (\omega - 1)x.$$

(En la prueba de 3.20 vimos que los números $\omega^i - 1$, donde $p \nmid i$ son conjugados.)

Como x e y son primos entre sí, el único factor común que pueden tener dos de los monomios es $\omega - 1$. De hecho, las ecuaciones anteriores muestran que si $\omega - 1$ divide a uno de los monomios, en realidad los divide a todos. Esto sucede si y sólo si $\omega - 1 \mid z$, lo que equivale a que $p \mid z$.

Observar que como p es impar y no exigimos que x, y, z sean positivos, los tres son intercambiables, es decir, la ecuación $x^p + y^p = z^p$ puede expresarse también como $(-z)^p + y^p = (-x)^p$, etc. Por lo tanto si p divide a uno de los tres números x, y, z podemos exigir que divida a z, y el caso contrario es que p no divida a ninguno de ellos. Ésta es la distinción tradicional en el teorema de Fermat:

Caso I $x^p + y^p = z^p$ donde x, y, z son enteros no nulos primos entre sí dos a dos y primos con p.

Caso II $x^p + y^p = z^p$ donde x, y, z son enteros no nulos primos entre sí dos a dos y además $p \mid z$.

Notar que en la prueba de Euler también hemos tratado por separado los casos I y II.

En la prueba del caso I para $p = 3$ hemos usado que como los dos factores eran primos entre sí y su producto era un cubo, ambos tenían que ser cubos. Lo que tenemos ahora es que si α y β son enteros ciclotómicos primos entre sí tales que $\alpha\beta = \gamma^p$ para un tercer entero ciclotómico γ, entonces los ideales (α) y (β) son potencias p-ésimas. Digamos que $(\alpha) = \mathfrak{a}^p$. Sin embargo, para que el argumento de Kummer funcione es necesario que $\alpha = \delta^p$, para cierto entero δ. Esto nos lleva al problema siguiente:

> Si α es un entero ciclotómico tal que $(\alpha) = \mathfrak{a}^p$ para un cierto ideal $\mathfrak{a}$, ¿bajo qué condiciones podemos garantizar que α es una potencia p-ésima?

En primer lugar es necesario que el ideal $\mathfrak{a}$ sea principal. Esto puede garantizarse a partir de un resultado sencillo sobre grupos: supongamos que p no divide al número de clases h del cuerpo ciclotómico. Entonces al tomar clases se

cumple que $[\mathfrak{a}]^p = \big[(\alpha)\big] = 1$, luego el orden de $[\mathfrak{a}]$ divide a p, pero dicho orden ha de dividir también al orden h del grupo de clases, luego ha de ser 1, es decir, $[\mathfrak{a}] = 1$ y el ideal $\mathfrak{a}$ ha de ser principal, digamos $\mathfrak{a} = (\delta)$.

Así pues $(\alpha) = (\delta^p)$, pero esto no garantiza que α sea una potencia p-ésima, sino tan sólo que $\alpha = \epsilon\delta^p$ para una cierta unidad ciclotómica ϵ. Nos falta justificar de algún modo que ϵ es también una potencia p-ésima. Observemos que una condición necesaria para que un entero ciclotómico cualquiera sea una potencia p-ésima es que sea congruente con un entero racional módulo p. En efecto, si $\epsilon = \eta^p$ y $\eta = a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1}$, al tomar clases módulo p queda que $[\epsilon] = [a_0]^p + [a_1]^p + \cdots + [a_{p-1}]^p$.

Esta condición no es en general suficiente, y el recíproco completa las hipótesis de Kummer:

Definición 10.2 Un primo impar p es *regular* si cumple:

A) p no divide al número de clases del cuerpo ciclotómico de orden p.

B) Si ϵ es una unidad ciclotómica, entonces ϵ es una potencia p-ésima si y sólo si ϵ es congruente con un entero racional módulo p.

Con esto podemos demostrar el resultado de Kummer:

Teorema 10.3 (Kummer) *El último teorema de Fermat es cierto para exponentes regulares.*

Demostración: Según las observaciones anteriores, si p es un primo regular y suponemos que existen enteros no nulos tales que $x^p + y^p = z^p$, de hecho podemos suponer que x, y, z son primos entre sí dos a dos y que o bien p no divide a ninguno de ellos (caso I) o bien p divide a z (caso II). En cualquier caso tenemos la factorización

$$z^p = x^p + y^p = (x + y)(x + \omega y)\cdots(x + \omega^{p-1}y),$$

En el caso I los factores son primos entre sí. En el caso II su único factor común es el primo $\omega - 1$.

Consideremos en primer lugar el caso I. Por la factorización única en ideales, cada ideal $(x + \omega^i y)$ es una potencia p-ésima, luego por la propiedad A) de la definición de primo regular podemos concluir que $x + \omega y = \epsilon\beta^p$, para una cierta unidad ϵ y un entero ciclotómico β (ver las explicaciones previas a la definición).

Vamos a llegar a una contradicción tan sólo a partir de aquí, sin necesidad de usar la condición B). Para ello aplicamos la conjugación que envía ω a ω^{-1} (que no es sino la conjugación compleja). Así obtenemos que $x + \omega^{-1}y = \bar{\epsilon}\bar{\beta}^p$.

Del teorema 4.27 se sigue que $\epsilon/\bar{\epsilon} = \omega^r$, donde $0 \le r < p$. Por otra parte hemos visto que toda potencia p-ésima es congruente módulo p con un entero racional, luego $\bar{\beta}^p \equiv m \pmod p$, de donde se sigue que $\beta^p \equiv \bar{\beta}^p \pmod p$. Reuniendo todo esto vemos que

$$x + \omega^{-1}y = \bar{\epsilon}\bar{\beta}^p = \omega^{-r}\epsilon\bar{\beta}^p \equiv \omega^{-r}\epsilon\beta^p = \omega^{-r}(x + \omega y) \pmod p.$$

Equivalentemente:

$$x\omega^r + y\omega^{r-1} - y\omega - x \equiv 0 \text{ (mód } p). \tag{10.3}$$

Notemos que si p divide a un entero ciclotómico α y tenemos una expresión de α como combinación lineal entera de $p-1$ potencias de ω, como éstas son una base entera, es necesario que p divida a cada uno de los coeficientes. Usaremos esto para probar que $r = 1$ descartando cualquier otra posibilidad (notar también que podemos suponer $p \geq 5$, ya que el caso $p = 3$ está probado).

Si $r = 0$ la congruencia (10.3) se convierte en $y\omega^{-1} - y\omega \equiv 0$ (mód p), luego $p \mid y$, contradicción.

Si $r = 2$ queda $x\omega^2 - x \equiv 0$ (mód p), luego $p \mid x$, contradicción.

Si $r > 2$ todas las potencias de ω que aparecen en (10.3) son distintas, y como sólo hay $4 < p-1$, concluimos igualmente que $p \mid x$.

Así pues, ha de ser $r = 1$, y entonces (10.3) es $(x-y)\omega + y - x \equiv 0$ (mód p), con lo que concluimos que $x \equiv y$ (mód p).

Ahora bien, si escribimos la ecuación de Fermat como $x^p + y^p + z^p = 0$, el caso I es simétrico respecto a tres variables x, y, z luego intercambiando los papeles podemos llegar igualmente a que $x \equiv y \equiv z$ (mód p).

Pero $0 = x^p + y^p + z^p \equiv x + y + x \equiv 3x$ (mód p), y como $p > 3$, llegamos una vez más a la contradicción $p \mid x$.

Supongamos ahora que $p \mid z$ (caso II). Sustituyamos z por $p^k z$, donde ahora z es primo con p. Tenemos entonces que $x^p + y^p = p^{kp} z^p$, donde x, y, z son enteros primos con p.

En el anillo de enteros ciclotómicos, p factoriza como $p = \eta(\omega-1)^{p-1}$, donde η es una unidad. La ecuación se convierte en

$$x^p + y^p = \epsilon(\omega-1)^{pm} z^p, \tag{10.4}$$

donde ϵ es una unidad y $m = k(p-1) > 0$.

Hemos de probar que esta ecuación no tiene soluciones enteras primas con $\omega - 1$. Para ello probaremos más en general que no existen enteros ciclotómicos x, y, z primos con $\omega - 1$ que satisfagan (10.4). Supongamos por reducción al absurdo que existen enteros ciclotómicos que cumplan (10.4) con el menor valor posible para m. Factorizando el miembro izquierdo de (10.4) tenemos

$$(x+y)(x+\omega y)\cdots(x+\omega^{p-1}y) = \epsilon(\omega-1)^{pm} z^p. \tag{10.5}$$

Sabemos que en el caso II el primo $\omega - 1$ divide de hecho a todos los factores de la izquierda. Más aún, la ecuación (10.2) implica que $(\omega-1)^2$ no divide a la diferencia de dos cualesquiera de estos factores. Equivalentemente, los números

$$\frac{x+\omega^i y}{1-\omega}, \quad i = 0, \ldots, p-1,$$

son no congruentes dos a dos módulo $\omega - 1$.

Como $\mathrm{N}(\omega-1)=p$, estos números forman un conjunto completo de representantes de las clases de congruencia módulo $\omega-1$.

En particular existe un único i entre 0 y $p-1$ tal que $(\omega-1)^2 \mid x+\omega^i y$. Si llamamos y a $\omega^i y$, se sigue cumpliendo (10.4) y ahora $(\omega-1)^2 \mid x+y$, mientras que los factores restantes $x+\omega^i y$ son divisibles entre $\omega-1$ pero no entre $(\omega-1)^2$.

En consecuencia el miembro izquierdo de (10.5) es divisible entre $(\omega-1)^{p+1}$, y en particular ha de ser $m>1$.

Sea $\mathfrak{m}=(x,y)$. Como x e y son primos con $\omega-1$, lo mismo le ocurre a $\mathfrak{m}$. Por lo tanto si $i\neq 0$ tenemos que $(x+\omega^i y)=(\omega-1)\mathfrak{m}\mathfrak{c}_i$, mientras que $x+y$ ha de ser divisible entre los $p(m-1)+1$ factores $\omega-1$ restantes que dividen el miembro derecho de (10.5), es decir,

$$(x+y)=(\omega-1)^{p(m-1)+1}\mathfrak{m}\mathfrak{c}_0.$$

Los ideales $\mathfrak{c}_i$, para $i=0,\dots,p-1$, son primos entre sí dos a dos, pues si un primo $\mathfrak{p}$ divide a dos de ellos, entonces $\mathfrak{m}\mathfrak{p}$ divide a dos números $x+\omega^i y$, $x+\omega^j y$, luego también divide a su suma y a su diferencia, es decir, a $(\omega-1)y$, $(\omega-1)x$, luego a $\mathfrak{m}=(x,y)$, pero esto es imposible.

La ecuación dada queda ahora del modo siguiente:

$$\mathfrak{m}^p(\omega-1)^{pm}\mathfrak{c}_0\mathfrak{c}_1\cdots\mathfrak{c}_{p-1}=(\omega-1)^{pm}(z)^p.$$

Puesto que los $\mathfrak{c}_i$ son primos entre sí, todos han de ser potencias p-ésimas. Digamos que $\mathfrak{c}_i=\mathfrak{b}_i^p$, con lo que

$$\begin{aligned}(x+y) &= (\omega-1)^{p(m-1)+1}\mathfrak{m}\mathfrak{b}_0^p,\\ (x+\omega^i y) &= (\omega-1)\mathfrak{m}\mathfrak{b}_i^p, \qquad i=1,\dots,p-1.\end{aligned}$$

Despejamos $\mathfrak{m}$ en la primera ecuación y lo sustituimos en la segunda:

$$(\omega-1)^{p(m-1)}\mathfrak{b}_0^p(x+\omega^i y)=(x+y)\mathfrak{b}_i^p, \quad i=1,\dots,p-1. \tag{10.6}$$

Esto implica que los ideales $\mathfrak{b}_0^p$ y $\mathfrak{b}_i^p$ son similares, luego $(\mathfrak{b}_i\bar{\mathfrak{b}}_0)^p$ es principal, donde $\bar{\mathfrak{b}}_0=\mathrm{N}(\mathfrak{b}_0)/\mathfrak{b}_0$. Por la propiedad A de la definición de primo regular concluimos que el ideal $\mathfrak{b}_i\bar{\mathfrak{b}}_0$ también es principal, digamos $\mathfrak{b}_i\bar{\mathfrak{b}}_0=(\alpha_i)$. Multiplicando por $\mathfrak{b}_0$ queda $\mathrm{N}(\mathfrak{b}_0)\mathfrak{b}_i=(\alpha_i)\mathfrak{b}_0$. Notar que tanto $\mathrm{N}(\mathfrak{b}_0)$ como (α_i) son primos con $\omega-1$. Elevamos a p y sustituimos en (10.6):

$$(\omega-1)^{p(m-1)}\,\mathrm{N}(\mathfrak{b}_0)^p(x+\omega^i y)=(x+y)(\alpha_i)^p, \quad i=1,\dots,p-1.$$

Eliminando los ideales queda

$$(\omega-1)^{p(m-1)}\,\mathrm{N}(\mathfrak{b}_0)^p(x+\omega^i y)=\epsilon_i(x+y)\alpha_i^p,$$

donde ϵ_i es una unidad, o equivalentemente

$$(\omega-1)^{p(m-1)}(x+\omega^i y)=\epsilon_i(x+y)\gamma_i^p, \tag{10.7}$$

donde $\gamma_i=\alpha_i/\,\mathrm{N}(\mathfrak{b}_0)$.

Nuestro objetivo es combinar estas ecuaciones para llegar a una ecuación similar a (10.4) pero con un valor menor para m. Una forma rápida de hacerlo es partir de la identidad

$$(x+\omega y)(1+\omega)-(x+\omega^2 y)=\omega(x+y).$$

Si la multiplicamos por $(\omega-1)^{p(m-1)}$ y usamos (10.7) para $i=1,2$ obtenemos

$$(x+y)\gamma_1^p\epsilon_1(1+\omega)-(x+y)\gamma_2^p\epsilon_2=(x+y)\omega(\omega-1)^{p(m-1)}.$$

Como $1+\omega$ es una unidad, esta ecuación se puede poner en la forma

$$\gamma_1^p+\gamma_2^p\epsilon=\eta(\omega-1)^{p(m-1)},$$

donde ϵ y η son unidades. Multiplicando por $\mathrm{N}(\mathfrak{b}_0)^p$ queda una ecuación de tipo

$$\alpha^p+\epsilon\beta^p=\eta(\omega-1)^{p(m-1)}\gamma^p,$$

donde α, β y γ son enteros ciclotómicos primos con $\omega-1$. Esta ecuación será de tipo (10.4) si ϵ es una potencia p-ésima. Lo probaremos usando la propiedad B de la definición de primo regular.

En efecto, basta observar que $p(m-1)\geq p$, pues hemos probado que $m>1$, luego

$$\alpha^p+\epsilon\beta^p\equiv 0 \ (\text{mód } p).$$

Despejando ϵ (lo cual es posible porque β es primo con p) vemos que es congruente con una potencia p-ésima módulo p, luego es congruente con un entero racional módulo p, luego es una potencia p-ésima (por la propiedad B). ∎

Este teorema no aporta información alguna en ausencia de un criterio para reconocer qué primos son regulares. Kummer formuló dos conjeturas sobre los primos regulares:

1. La propiedad A implica la propiedad B, de modo que un primo p es regular si y sólo si $p\nmid h$, donde h es el número de clases del cuerpo ciclotómico de orden p.

2. Existen infinitos primos regulares.

Admitiendo la primera conjetura, el problema de decidir si un primo es regular se reduce al cálculo del número de clases del cuerpo ciclotómico correspondiente, lo cual no es cosa fácil, pues h aumenta muy rápidamente con p. Pocos meses después de probar el teorema anterior, Kummer demostró la conjetura 1 y halló un método sorprendentemente simple de decidir si se cumple la propiedad A sin necesidad de calcular explícitamente el número de clases h. Ambos resultados se obtienen a partir de una técnica común que desarrollaremos en los próximos capítulos. Respecto a la segunda conjetura, nunca ha sido demostrada ni refutada, pero Kummer se retractó de ella cuando dispuso de más datos. En realidad no hay evidencias de que sea falsa.

Capítulo XI

La función dseta de Dedekind

Según comentábamos en el capítulo anterior, Kummer buscaba una caracterización práctica de los primos regulares, lo que supone ser capaz de decidir si un primo p divide o no al número de clases del cuerpo ciclotómico de orden p. Al abordar el problema se dio cuenta de que podía aprovechar el trabajo de Dirichlet sobre los primos en progresiones aritméticas, que a su vez se basaban en su propia teoría de factorización ideal en los cuerpos ciclotómicos. Los resultados de Dirichlet y Kummer sobre cuerpos ciclotómicos fueron generalizados por Dedekind a cuerpos numéricos arbitrarios, y es en este contexto general en el que los expondremos aquí. El punto de partida es el siguiente resultado de Euler:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}},$$

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:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{para } s > 1.$$

Su convergencia es fácil de probar. Sólo hay que observar que

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s},$$

para $n \geq 1$ en la desigualdad de la izquierda y $n \geq 2$ en la desigualdad de la derecha. De aquí

$$\int_1^{N+1} \frac{dx}{x^s} < \sum_{n=1}^{N} \frac{1}{x^s} < 1 + \int_1^N \frac{dx}{x^s},$$

para todo número natural $N > 1$. Integrando y tomando límites en N queda

$$\frac{1}{s-1} \leq \zeta(s) \leq 1 + \frac{1}{s-1}, \quad s > 1.$$

Más aún, multiplicando por $s-1$ y tomando límites en s obtenemos

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1. \tag{11.1}$$

Euler notó que esto implica la existencia de infinitos números primos. En efecto, (11.1) 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.

Dirichlet conocía los resultados de Kummer, en particular el teorema 3.20, según el cual el tipo de factorización de un primo p en un cuerpo ciclotómico de orden m depende del resto de p módulo m, y por lo tanto de la clase de p en U_m. Dirichlet conjeturó que una fórmula similar a la de Euler donde la suma se haga sobre los ideales del cuerpo ciclotómico m-simo y el producto sobre los correspondientes primos ciclotómicos, tal vez podría utilizarse para probar que toda progresión $mx + n$ con $[n] \in U_m$ contiene números primos.

Ejercicio: Probar que la función dseta de Riemann converge uniformemente en los subconjuntos compactos de $]1, +\infty[$. Deducir que es continua en dicho intervalo.

Resultados básicos sobre series y productos infinitos Para comodidad del lector, enunciamos aquí los resultados analíticos más importantes que vamos a utilizar.

Criterio de mayoración de Weierstrass *Si $\{f_n\}$ es una sucesión de funciones definidas en $A \subset \mathbb{C}$ y $\{a_n\}$ es una sucesión en $\mathbb{R}$ de modo que $|f_n(z)| \leq a_n$ para todo $z \in A$ y $\sum_n a_n < +\infty$, entonces la serie funcional $\sum_n f_n(z)$ converge uniformemente en su dominio.*

Criterio de comparación *Si $\{a_n\}$ y $\{b_n\}$ son dos sucesiones en $\mathbb{C}$ tales que existe $\lim_n |a_n|/|b_n|$ entonces la serie $\sum_n a_n$ converge absolutamente si y sólo si lo hace $\sum_n b_n$.*

Productos infinitos *Un producto infinito $\prod_n (1+a_n)$ de números complejos converge (absolutamente) si y sólo si la serie $\sum_n a_n$ converge (absolutamente). En tal caso la serie $\sum_n \log(1+a_n)$ converge a un logaritmo del producto.*

11.1 Convergencia de la función dseta

Definición 11.1 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.

Observar que la función dseta de $\mathbb{Q}$ es precisamente la función dseta de Riemann.

Nuestro primer problema es demostrar que esta serie converge para $s > 1$. Si llamamos h al número de clases de K podemos descomponerla en suma de h series como sigue:

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

donde C recorre las clases de similitud de ideales de K.

Para probar la convergencia de la serie completa es suficiente probar la de las series

$$\zeta_C(s) = \sum_{\mathfrak{a}\in C} \frac{1}{\mathrm{N}(\mathfrak{a})^s}.$$

En primer lugar las reescribimos para que el conjunto de índices sea el de los números naturales, como es habitual. Para ello llamamos $f_C(n)$ al número de ideales de C de norma n, con lo que

$$\zeta_C(s) = \sum_{n=1}^{\infty} \frac{f_C(n)}{n^s}.$$

La convergencia la obtendremos a partir de una estimación de la sucesión de coeficientes. En realidad 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 IV. Conservamos

la notación que introdujimos allí. Concretamente $\sigma_1,\dots,\sigma_s$ serán los monomorfismos reales de K, mientras que $\sigma_{s+1},\bar\sigma_{s+1},\dots,\sigma_{s+t},\bar\sigma_{s+t}$ serán los monomorfismos complejos. Así, el grado de K será $n = s+2t$. La representación geométrica de un número $\alpha\in K$ es

$$x(\alpha) = \big(\sigma_1(\alpha),\dots,\sigma_{s+t}(\alpha)\big) \in \mathcal{R}^{st}.$$

En $\mathcal{R}^{st}$ se define la norma $\mathrm{N}(x_1,\dots,x_{s+t}) = x_1\cdots x_s|x_{s+1}|^2\cdots|x_{s+t}|^2$, 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 $\mathrm{N}(x)\neq 0$ tienen asignada la representación logarítmica dada por $l(x) = \big(l_1(x),\dots,l_{s+t}(x)\big)$, donde

$$l_k(x) = \begin{cases} \log|x_k| & \text{para } k=1,\dots,s,\\ \log|x_k|^2 & \text{para } k=s+1,\dots,s+t.\end{cases}$$

Sea $\epsilon_1,\dots,\epsilon_r$ un sistema fundamental de unidades de K. Sabemos que los vectores $l(\epsilon_1),\dots,l(\epsilon_r)$ 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 $l^* = (1,\overset{s)}{\dots},1,2,\overset{t)}{\dots},2)$ 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 $\xi,\xi_1,\dots,\xi_r$ son números reales.

Por último, sea m el número de raíces de la unidad contenidas en K.

Definición 11.2 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 $0\le\xi_i<1$.

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, 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 11.3 *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 11.4 *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 11.3): 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 observamos 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

$$\begin{aligned} l_k(\xi x) &= \log|\xi x_k| = \log\xi + l_k(x), \quad \text{para } 1 \leq k \leq s, \\ l_j(\xi x) &= \log|\xi x_j|^2 = 2\log\xi + l_k(x), \quad \text{para } 1 \leq j \leq t. \end{aligned}$$

En consecuencia, $l(\xi x) = \log\xi\, l^* + l(x)$ y las coordenadas $\xi_1, \ldots, \xi_r$ de los vectores $l(\xi x)$ y $l(x)$ en la base $l^*, l(\epsilon_1), \ldots, l(\epsilon_r)$ 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 $|\,\mathrm{N}(\alpha)| \leq r\,\mathrm{N}(\mathfrak{b})$. 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 $|\,\mathrm{N}(x)| \leq r\,\mathrm{N}(\mathfrak{b})$.

Llamemos $T = \{x \in X \mid |\,\mathrm{N}(x)| \leq 1\}$. 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

$$\{x \in X \mid |\,\mathrm{N}(x)| \leq r\} = \left\{ \sqrt[n]{r}\left(\frac{x}{\sqrt[n]{r}}\right) \in X \mid \left|\mathrm{N}\left(\frac{x}{\sqrt[n]{r}}\right)\right| \leq 1 \right\} = \sqrt[n]{r}\,T,$$

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 11.5 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 $\|\phi(x)-\phi(y)\| \le C\|x-y\|$.

Usando el teorema del valor medio es fácil ver que toda función de clase C^1 tiene la propiedad de Lipschitz en compactos.

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.

Teorema 11.6 *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.

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

$$j_C(r) = \frac{n\big(\sqrt[n]{r\,\mathrm{N}(\mathfrak{b})}\big)}{m}. \tag{11.2}$$

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

$$l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r), \tag{11.3}$$

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 4.22 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 (4.3), las componentes de $l(x)$ suman $\log\big|\mathrm{N}(x)\big|$, pero sumando en el miembro derecho de (11.3) y teniendo en cuenta que las componentes de $l(\epsilon_i)$ suman $\log 1 = 0$, tenemos que $\log\big|\mathrm{N}(x)\big| = \xi(s+2t) = n\xi$.

Por lo tanto (11.3) se convierte en

$$l(x) = \frac{1}{n}\log\big|\mathrm{N}(x)\big|l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r). \tag{11.4}$$

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 (11.4) equivale al sistema de ecuaciones

$$\log \rho_j^{e_j} = \frac{e_j}{n}\log\prod_{i=1}^{s+t}\rho_i^{e_i} + \sum_{k=1}^{r}\xi_k l_j(\epsilon_k). \tag{11.5}$$

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 (11.5) 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

$$\log \rho_j^{e_j} = \frac{e_j}{n} \log \xi + \sum_{k=1}^{r} \xi_k l_j(\epsilon_k). \tag{11.6}$$

definen un cambio de variables

$$(\rho_1, \dots, \rho_{s+t}, \theta_1, \dots, \theta_t) \mapsto (\xi, \xi_1, \dots, \xi_r, \theta_1, \dots, \theta_t)$$

y, respecto a éstas últimas, el conjunto F' está definido por las condiciones

$$0 < \xi \leq 1, \quad 0 \leq \xi_k < 1, \quad 0 \leq \theta_j < 2\pi. \tag{11.7}$$

En efecto, las ecuaciones (11.6) pueden escribirse también como

$$\log \rho_j = \frac{1}{n} \log \xi + \sum_{k=1}^{r} \xi_k \log |\sigma_j(\epsilon_k)|, \qquad j = 1, \dots, s+t,$$

o también

$$\rho_j = \xi^{1/n} \exp\left(\sum_{k=1}^{r} \xi_k \log |\sigma_j(\epsilon_k)| \right), \qquad j = 1, \dots, s+t. \tag{11.8}$$

Esto nos da $(\rho_1, \dots, \rho_{s+t}, \theta_1, \dots, \theta_t)$ a partir de $(\xi, \xi_1, \dots, \xi_r, \theta_1, \dots, \theta_t)$. Para la transformación inversa notamos que al sumar las ecuaciones (11.6) 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 (notar 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 el capítulo 4 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 (11.8) 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 11.6, y las constantes que aparecen son

$$v = \mu(T) = 2^s \pi^t R$$

y, según el teorema 4.5, 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 (11.2) hemos probado el teorema siguiente:

Teorema 11.7 *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*

$$j_C(r) = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}}\, r + O(r^{1-1/n}).$$

Observar 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. Veámoslo.

Teorema 11.8 *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*
$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}}\, h, \tag{11.9}$$
donde h es el número de clases de K.

Demostración: El segundo apartado es consecuencia clara del primero. Para probar éste consideremos la sucesión $\{x_n\}$ 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

$$\zeta_C(s) = \sum_{\mathfrak{a}\in C} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{1}{x_n^s}.$$

Claramente, $j_C(x_n)$ es el número de términos de la sucesión menores o iguales que x_n, luego claramente $j_C(x_n-1) < n \le j_C(x_n)$. Por lo tanto:

$$\left(\frac{x_n-1}{x_n}\right)\frac{j_C(x_n-1)}{x_n-1} < \frac{n}{x_n} \le \frac{j_C(x_n)}{x_n}.$$

Es obvio que x_n tiende a infinito, luego al tomar límites en n queda

$$\lim_n \frac{n}{x_n} = \frac{2^s(2\pi)^t R}{m\sqrt{|\Delta_K|}}.$$

Llamemos L a este límite. Entonces, dado $\epsilon > 0$, existe un n_0 tal que si $n \geq n_0$ entonces

$$L - \epsilon < \frac{n}{x_n} < L + \epsilon,$$

luego

$$(L-\epsilon)^s \frac{1}{n^s} < \frac{1}{x_n^s} < (L+\epsilon)^s \frac{1}{n^s}.$$

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

$$\sum_{n=n_0}^{\infty} (L+\epsilon)^{s_1} \frac{1}{n^{s_0}},$$

luego converge uniformemente. Más aún,

$$(L-\epsilon)^s \sum_{n=n_0}^{\infty} \frac{1}{n^s} \leq \sum_{n=n_0}^{\infty} \frac{1}{x_n^s} \leq (L+\epsilon)^s \sum_{n=n_0}^{\infty} \frac{1}{n^s}.$$

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. Aunque no entraremos en ello, puede probarse que ζ_K se extiende a una función holomorfa con un polo simple en 1, por lo que el miembro derecho de (11.9) es precisamente el residuo en 1 de ζ_K.

11.2 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 11.9 *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 entonces 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).

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

$$\prod_{\mathrm{N}(\mathfrak{p}) \le N} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}} = \sum_{k_1, \ldots, k_r = 0}^{\infty} \frac{1}{\mathrm{N}(\mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r})^s} = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{a}$ recorre los ideales no divisibles entre primos de norma mayor que N.

Así pues,

$$\left| \prod_{\mathrm{N}(\mathfrak{p}) \le N} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}} - \zeta_K(s) \right| < \sum_{\mathrm{N}(\mathfrak{a}) > N} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

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 juega 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, 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 11.10 *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 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

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{1}{m\,\mathrm{N}(\mathfrak{p})^{ms}} \tag{11.10}$$

(notar 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 (11.10), 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 algunos conceptos nuevos. Sin embargo, sí estamos en condiciones de exponer los resultados análogos para cuerpos cuadráticos, lo que nos servirá de orientación para el caso ciclotómico, un poco más complicado.

Consideremos la fórmula de Euler generalizada para un cuerpo cuadrático K y en ella agrupemos 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:

$$\frac{1}{1-\frac{1}{p^{2s}}} = \begin{cases} \dfrac{1}{1-\frac{1}{p^s}}\dfrac{1}{1-\frac{1}{p^s}} & \text{si } p \text{ se escinde,}\\[2ex] \dfrac{1}{1-\frac{1}{p^s}}\dfrac{1}{1+\frac{1}{p^s}} & \text{si } p \text{ se conserva,}\\[2ex] \dfrac{1}{1-\frac{1}{p^s}} & \text{si } p \text{ se ramifica.}\end{cases}$$

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

$$\zeta_K(s) = \prod_p\frac{1}{1-\frac{1}{p^s}}\prod_p\frac{1}{1-\frac{\chi_K(p)}{p^s}} = \zeta(s)\prod_p\frac{1}{1-\frac{\chi_K(p)}{p^s}},$$

donde hemos usado la fórmula de Euler para la función dseta de Riemann (la función dseta de $\mathbb{Q}$). Llamemos

$$L(s,\chi_K)=\sum_{n=1}^{\infty}\frac{\chi_K(n)}{n^s},\quad \text{para } s>1. \tag{11.11}$$

Es claro que la serie converge absolutamente (está mayorada por la función dseta) y el mismo argumento que prueba la fórmula de Euler para $\mathbb{Q}$ permite probar la relación

$$L(s,\chi_K)=\prod_p \frac{1}{1-\frac{\chi_K(p)}{p^s}},$$

sin más que sustituir la función constante 1 por la función χ_K (notar que ya tenemos garantizada la convergencia absoluta del producto). En definitiva hemos factorizado la función dseta de K como

$$\zeta_K(s)=\zeta(s)L(s,\chi_K).$$

Multiplicamos ambos miembros por $(s-1)$ y tomamos límites cuando s tiende a 1. El teorema 11.8 nos da que existe

$$\lim_{s\to 1^+} L(s,\chi_K)=\frac{2^{s+t}\pi^t R}{m\sqrt{|\Delta_K|}}\,h.$$

Por lo tanto podemos definir $L(1,\chi_K)$ como este límite y así la función L es continua en $[1,+\infty[$. Puesto que estamos considerando un cuerpo cuadrático, la expresión de $L(1,\chi_K)$ se simplifica considerablemente:

Teorema 11.11 *Sea K un cuerpo cuadrático de discriminante Δ. Entonces el número de clases de K viene dado por*

$$h=\begin{cases}\dfrac{\sqrt{\Delta}}{2\log\epsilon}\,L(1,\chi_K) & \text{si } \Delta>0 \text{ y } \epsilon>1 \text{ es la unidad fundamental de } K,\\[2ex] \dfrac{m\sqrt{-\Delta}}{2\pi}\,L(1,\chi_K) & \text{si } \Delta<0 \text{ y } m \text{ es el número de unidades de } K.\end{cases}$$

El análisis de las funciones L se puede llevar más lejos hasta obtener resultados más operativos. Por ejemplo, la serie (11.11) converge en realidad para $s>0$, lo que permite calcular $L(1,\chi_K)$ sumando la serie directamente (sin necesidad de tomar límites). No obstante, antes de entrar en ello conviene generalizar los conceptos que estamos manejando, para que los resultados sean aplicables a cuerpos numéricos no necesariamente cuadráticos, especialmente a los ciclotómicos.

Terminamos esta sección demostrando una versión débil del teorema de Dirichlet. La 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 11.10 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 11.10 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 $]1,2]$.

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.

Notemos que en la prueba anterior no interviene la función dseta de K, sino tan sólo las funciones ζ y L, que sólo involucran números enteros y el carácter χ_K. Esto puede hacer pensar que la prueba no depende de la teoría de cuerpos cuadráticos. En efecto, la mayor parte de la prueba anterior (así como la del teorema de Dirichlet) puede basarse en argumentos sobre series de carácter elemental. El único punto no trivial, que nosotros hemos justificado con ayuda de la función ζ_K, es que $L(1,\chi_K)\neq 0$. Esto también puede probarse mediante técnicas analíticas, pero ya no es trivial. Es necesario usar la teoría de funciones holomorfas. Aún así, la prueba analítica del teorema de Dirichlet es más elemental que la que nosotros daremos, pero ésta es la original de Dirichlet

y en la que se ven más claramente las ideas subyacentes. Además se generaliza más fácilmente a otros resultados de gran importancia en el desarrollo de la teoría algebraica de números.

11.3 Caracteres de grupos abelianos

En su estudio de la función dseta de los cuerpos ciclotómicos, Dirichlet se encontró con unas funciones que juegan el mismo papel que el carácter de un cuerpo cuadrático. Introducimos el concepto en el contexto general de los grupos abelianos finitos:

Definición 11.12 Sea G un grupo abeliano finito. Un *carácter* de G es un homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$.

Los caracteres de ideales o de formas cuadráticas en el sentido de Gauss son esencialmente caracteres del grupo de clases estrictas, o también del grupo de géneros, en el sentido de esta definición. El carácter de un cuerpo cuadrático K es un carácter del grupo $U_{|\Delta|}$ de las unidades módulo $|\Delta|$, donde Δ es el discriminante de K. Las funciones δ, ϵ, $\delta\epsilon$ definidas en 9.6 inducen caracteres en el grupo U_8.

En todos estos casos los caracteres tomaban tan sólo los valores ± 1, ahora admitimos que tomen valores complejos cualesquiera. De todos modos un carácter no puede tomar cualquier valor: Si g es un elemento de un grupo abeliano G de 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, 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 concluimos que 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 11.13 *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 11.14 *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. ∎

Observar 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 11.15 *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 11.16 (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.

11.4 Caracteres modulares

Estudiamos ahora con más detalle los caracteres de los grupos de unidades módulo un número natural m. Tal y como hemos hecho hasta ahora en los casos particulares que hemos manejado, conviene considerar a estos caracteres definidos sobre $\mathbb{Z}$.

Definición 11.17 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.

Notar 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. Observar 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 $a' \equiv a$ (mód m) y $a' \equiv 1$ (mód 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 11.18 *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,

$$N_1 = \big\{[a] \in U_{m'} \mid a \equiv 1 \pmod{m_1}\big\} \quad \text{y} \quad N_2 = \big\{[a] \in U_{m'} \mid a \equiv 1 \pmod{m_2}\big\}.$$

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 $N = \big\{[a] \in U_{m'} \mid a \equiv 1 \pmod{d}\big\}$ 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 $N_1N_2 \le N$, 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 $a \equiv 1 \pmod{d}$. De aquí se sigue que si $a \equiv a' \pmod{d}$ entonces $\chi'(a) = \chi'(a')$.

Dado $[a] \in U_d$ existe un $[a'] \in U_{m'}$ tal que $a' \equiv a \pmod{d}$ (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 11.19 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 11.20 *Un carácter χ módulo m es primitivo si y sólo si para todo divisor propio d de m existe un entero x tal que $(x, m) = 1$, $x \equiv 1 \pmod{d}$ 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. ∎

Para terminar vamos a caracterizar 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 11.21 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.

El teorema 9.25 afirma que los caracteres de los cuerpos cuadráticos reales son pares, mientras que los de los cuerpos imaginarios son impares.

Teorema 11.22 *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 $K = \mathbb{Q}(\sqrt{d}\,)$. Si $d \equiv -1$ (mód 4) entonces $\Delta = 4d$ y basta tomar x tal que $x \equiv -1$ (mód 4), $x \equiv 1$ (mód $|d|$), con lo que $\chi(x) = -1$. Observar que de hecho se cumple $x \equiv 1$ (mód $2|d|$), tal y como se requiere.

Si $d = 2d'$, entonces $\Delta = 8d'$ y tomamos $x \equiv 5$ (mód 8), $x \equiv 1$ (mód $|d'|$). Entonces $x \equiv 1$ (mód $4|d'|$) 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, 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 es cuando $n = 1$. De hecho el carácter en cuestión es 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 $\delta(a) = (-1)^{(a-1)/2}$.

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. De hecho se trata de los caracteres ϵ y $\delta\epsilon$ definidos en 9.6.

En general, el grupo U_{2^n} es el producto de un grupo cíclico de orden 2 por un grupo cíclico de orden 2^{n-2}. Sea a un elemento de 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 el grupo U_m factoriza en el producto de los grupos de unidades correspondientes a dichas potencias y, por el teorema 11.13, 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, 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 $d \equiv 1 \pmod 4$ y $K = \mathbb{Q}\big(\sqrt{d}\big)$ si $d \equiv -1 \pmod 4$, con lo que la situación es análoga.

Finalmente, si $m = 8d$ entonces 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. ∎

11.5 La función dseta en cuerpos ciclotómicos

La teoría de caracteres nos permitirá desarrollar la función dseta de los cuerpos ciclotómicos de manera análoga a como hemos hecho con los cuerpos cuadráticos. Sea, pues, $\mathbb{Q}(\omega)$ el cuerpo ciclotómico de orden m. En la fórmula de Euler agrupamos los factores que dividen a un mismo primo racional p:

$$\zeta_K(s) = \prod_p \prod_{\mathfrak{p}\mid p} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}},$$

donde p recorre los primos racionales.

Si p es un primo y $m = p^i m'$, el teorema 3.20 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

$$\zeta_K(s) = \prod_p \left(1 - \frac{1}{p^{f_p s}}\right)^{-\phi(m)/f_p}. \tag{11.12}$$

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 $p^{f_p s}$,

$$1 - \frac{1}{p^{f_p s}} = \prod_{k=0}^{f_p-1} \left(1 - \frac{\omega_p^k}{p^s}\right). \tag{11.13}$$

Entonces el producto

$$\prod_{k=0}^{f_p-1} \left(1 - \frac{\omega_p^k}{p^s}\right)^{\phi(m)/f_p} = \left(1 - \frac{1}{p^{f_p s}}\right)^{\phi(m)/f_p}$$

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 11.15, 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 11.15 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 (11.12) 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 11.23 *Sea K el cuerpo ciclotómico de orden m. Entonces*

$$\zeta_K(s) = \prod_\chi L(s,\chi), \quad \text{para todo } s > 1$$

donde,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi_0(p)}{p^s}}. \tag{11.14}$$

La función $L(s,\chi)$ se conoce como la *función L de Dirichlet* asociada a χ.

Demostración: Sólo queda justificar la convergencia de los dos miembros de (11.14), la igualdad entre la serie y el producto se demuestra por el mismo argumento empleado en el teorema 11.9.

La serie converge absolutamente (y uniformemente en los compactos) para $s > 1$, porque está mayorada por la función dseta de Riemann. El producto converge como consecuencia de la convergencia de $\zeta_K(s)$, pero de hecho conviene observar que la convergencia es absoluta. En efecto, podemos expresarlo como

$$\prod_p \left(1 + \frac{\chi_0(p)}{p^s - \chi_0(p)}\right),$$

y la convergencia absoluta del producto es, por definición, la de la serie

$$\sum_p \frac{\chi_0(p)}{p^s - \chi_0(p)}.$$

Ésta se comprueba fácilmente comparando los módulos con $1/p^s$. ∎

De ahora en adelante, para simplificar la notación, siempre que χ sea un carácter modular sobrentenderemos que $\chi(n)$ representa en realidad a $\chi_0(n)$. Por ejemplo, si 1 es el carácter principal módulo m, entonces 1_0 es el carácter principal módulo 1, por lo que entenderemos que $1(n) = 1$ incluso cuando $(n,m) \neq 1$. Esto implica que

$$L(s,1) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \zeta(s).$$

En particular $L(s,1)$ tiende a infinito en 1. Para los caracteres no principales la situación es muy diferente, como se deduce del teorema que sigue.

Teorema 11.24 *Sea $\{a_n\}$ una sucesión de números complejos tal que las sumas $A_k = \sum_{n=1}^{k} a_n$ estén acotadas. Entonces la serie*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

converge para todo número real $s > 0$. Para todo $\delta > 0$ la convergencia es uniforme en el intervalo $[\delta, +\infty[$, luego la suma es continua en $]0, +\infty[$.

DEMOSTRACIÓN: Dado $\epsilon > 0$, sea n_0 tal que $1/n^\delta < \epsilon$ para $n \geq n_0$. Así $1/n^s < \epsilon$ para todo $s \geq \delta$ y todo $n \geq n_0$. Sea $M > N > n_0$. Entonces

$$\begin{aligned}\sum_{k=N}^{M} \frac{a_k}{k^s} &= \sum_{k=N}^{M} \frac{A_k - A_{k-1}}{k^s} = \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N-1}^{M-1} \frac{A_k}{(k+1)^s} \\ &= -\frac{A_{N-1}}{N^s} + \sum_{k=N}^{M-1} \left(\frac{A_k}{k^s} - \frac{A_k}{(k+1)^s} \right) + \frac{A_M}{M^s},\end{aligned}$$

luego si, según la hipótesis, se cumple que $|A_k| \leq C$ para todo k, entonces

$$\left| \sum_{k=N}^{M} \frac{a_k}{k^s} \right| \leq \frac{C}{N^s} + C \sum_{k=N}^{M-1} \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{C}{M^s} = \frac{2C}{N^s} < 2C\epsilon$$

para todo s en el intervalo $[\delta, +\infty[$. ∎

Teorema 11.25 *Si χ es un carácter modular no principal la serie*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

converge para todo número real $s > 0$ y la convergencia es uniforme en cada intervalo $[\delta, +\infty[$. En particular la función $L(s, \chi)$ es continua en $]0, +\infty[$.

DEMOSTRACIÓN: Es una consecuencia inmediata del teorema anterior pues, si m es el conductor de χ, el teorema 11.16 nos da que $\sum_n \chi(n) = 0$ cada vez que n recorre un conjunto completo de representantes de las clases módulo m. De aquí se sigue inmediatamente que todas las sumas finitas están acotadas. ∎

Es importante tener presente que la expresión de $L(s, \chi)$ como producto sólo es válida en $]1, +\infty[$ y que la convergencia de la serie no es absoluta en $]0, 1]$.

En particular tenemos que

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}, \qquad \text{para } \chi \neq 1 \tag{11.15}$$

Ahora que sabemos que $L(s, \chi)$ converge en 1 podemos llevar más lejos el teorema 11.23 y obtener de la fórmula que necesitaba Kummer para caracterizar los primos regulares.

Teorema 11.26 *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: Notar que si m es impar, entonces el cuerpo ciclotómico de orden m es el mismo que el de orden $2m$. En cualquier caso, el cuerpo ciclotómico de orden $2m$ tiene $2m$ raíces de la unidad.

Por el teorema 11.23 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 11.8. ∎

Una consecuencia inmediata del teorema anterior 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 11.27 (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 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 $s>1$. La convergencia absoluta del producto (11.14) 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 $s>1$. Observar 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

$$|R(s,\chi)| \leq \sum_p\sum_{n=2}^{\infty}\frac{1}{p^{ns}} = \sum_p\frac{1}{p^s(p^s-1)} \leq \sum_p\frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty}\frac{1}{n(n-1)} = 1$$

(la última serie es telescópica).

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

$$\sum_\chi \chi(A^{-1}) \log L(s,\chi) = \phi(m) \sum_{p\in A} \frac{1}{p^s} + R_A(s). \tag{11.16}$$

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, es conocido que 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 (11.16) 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. ∎

11.6 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 11.11 y 11.26 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 11.26 interviene también el regulador del cuerpo, cuyo cálculo involucra determinar un sistema fundamental de unidades, y esto no es sencillo. Pese a ello, dicha fórmula nos permitirá obtener resultados cualitativos sobre h que serán suficientes para caracterizar de forma efectiva a los primos regulares.

La única expresión con que contamos para calcular $L(1,\chi)$ es (11.15), 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

$$L(1,\chi_K) = \frac{1}{1} - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \frac{1}{11} - \frac{1}{12} - \frac{1}{13} + \frac{1}{14} + \cdots \tag{11.17}$$

Para ello observamos que

$$L(1,\chi_K) = \int_0^1 (1 - x - x^2 + x^3 + x^5 - x^6 - x^7 + x^8 + \cdots)\, dx. \tag{11.18}$$

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 (11.17), luego el límite es el mismo. De (11.18) 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 11.11 nos da que el número de clases de $\mathbb{Q}\big(\sqrt{5}\big)$ 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 11.11 porque sabemos que el resultado ha de ser entero).[1]

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 11.26.

Sea ω una raíz octava primitiva de la unidad. En el capítulo II 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.

[1] 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.

Según lo dicho, esto prueba que una unidad fundamental es $\epsilon = 1+\sqrt{2}$, luego el regulador es

$$R = \log\bigl(1+\sqrt{2}\bigr)^2 = 2\log\bigl(1+\sqrt{2}\bigr).$$

Por último, los caracteres no principales módulo 8 son los tres caracteres cuadráticos δ, ϵ, $\delta\epsilon$ definidos en 9.6, y que se corresponden respectivamente con los cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}\bigl(\sqrt{2}\bigr)$ y $\mathbb{Q}\bigl(\sqrt{-2}\bigr)$. Según 11.26, el número de clases que buscamos es

$$h = \frac{8\cdot 16}{(2\pi)^2\cdot 2\log\bigl(1+\sqrt{2}\bigr)} L(1,\delta)L(1,\epsilon)L(1,\delta\epsilon).$$

Por otra parte, la fórmula del teorema 11.11 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 IV.

Veamos ahora una técnica mucho más eficiente para el cálculo de funciones L en 1. 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 $\mathbb{Z}/nZ$ 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 11.28 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

$$L(s,\chi) = \frac{1}{m}\sum_{k=1}^{m-1} G_k(\chi)\sum_{n=1}^{\infty}\frac{\omega^{-nk}}{n^s}. \tag{11.19}$$

Dedicaremos el capítulo siguiente al estudio de estas sumas. Aquí probaremos el único resultado en torno a ellas que nos hace falta de momento:

Teorema 11.29 *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 11.20 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. ∎

Sabiendo esto, la fórmula (11.19) 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 las sumas $\sum_{n=1}^{N} \omega^{-nk}$ se anulan cada vez que $m \mid N$ por las relaciones de ortogonalidad) y en consecuencia toman un número finito de valores. Podemos aplicar el teorema 11.24 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 la serie de Taylor

$$-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$$

converge en realidad siempre que $|z| \leq 1$, excepto en $z = 1$. Con ello tenemos probado el teorema siguiente:

Teorema 11.30 *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 $\epsilon(n) = (-1)^{(m^2-1)/8}$.

Para calcular la suma de Gauss hemos de considerar 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

$$\begin{aligned} L(1,\epsilon) &= \frac{-1}{\sqrt{8}} \left(\log(1-\omega^{-1}) - \log(1-\omega^{-3}) - \log(1-\omega^{-5}) + \log(1-\omega^{-7})\right) \\ &= \frac{-1}{\sqrt{8}} \log \frac{|1-\omega\ |^2}{|1-\omega^3|^2} = \frac{1}{\sqrt{8}} \log \frac{2+\sqrt{2}}{2-\sqrt{2}} \\ &= \frac{1}{\sqrt{8}} \log\left(1+\sqrt{2}\right)^2 = \frac{\log\left(1+\sqrt{2}\right)}{\sqrt{2}}. \end{aligned}$$

■

Ejercicio: Comprobar que las sumas $G_a(\epsilon)$ cumplen el teorema 11.29.

Ejercicio: Calcular las sumas de Gauss correspondientes al carácter $\delta\epsilon$.

Los cálculos del ejemplo y el ejercicio anterior se pueden seguir fácilmente en general. En las condiciones del teorema 11.30 tenemos que

$$1-\omega^{-k} = 2\operatorname{sen}\frac{k\pi}{m}\left(\cos\left(\frac{\pi}{2}-\frac{k\pi}{m}\right)+i\operatorname{sen}\left(\frac{\pi}{2}-\frac{k\pi}{m}\right)\right).$$

(basta desarrollar el miembro derecho usando la trigonometría).

Si $0<k<m$ entonces $-\pi/2<\pi/2-k\pi/m<\pi/2$, luego

$$\log(1-\omega^{-k}) = \log|1-\omega^{-k}| + i\pi\left(\frac{1}{2}-\frac{k}{m}\right),$$

(recordar 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 11.30

$$\begin{aligned} L(1,\chi) &= -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log(1-\omega^{-k}),\\ L(1,\chi) &= -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log(1-\omega^{-k}). \end{aligned}$$

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 11.31 *Sea χ un carácter primitivo módulo m.*

1. *Si χ es par entonces*

$$L(1,\chi) = -\frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log|1-\omega^k| = \frac{G(\chi)}{m}\sum_k \overline{\chi(k)}\log\operatorname{sen}\frac{k\pi}{m}.$$

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.

El estudio de las sumas de Gauss que llevaremos a cabo en el capítulo siguiente nos permitirá simplificar aún más estas fórmulas, especialmente en el caso de los caracteres cuadráticos.

11.7 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 3.22, 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 $\omega_q = \cos(2\pi/f_q)+i\operatorname{sen}(2\pi/f_q)$ y usamos la fórmula (11.13), 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

$$\zeta_{K^*}(s) = \frac{1}{1-\frac{1}{p^s}} \prod_{q\neq p} \prod_{\chi(1)=1} \frac{1}{1-\frac{\chi(q)}{q^s}}.$$

Si entendemos, como siempre, que el carácter principal toma el valor 1 incluso sobre p, vemos 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 11.32 *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*

$$h^* = \frac{\sqrt{p}^{\,m-1}}{2^{m-1}R^*} \prod_{\substack{\chi(1)=1\\ \chi\neq 1}} L(1,\chi).$$

Capítulo XII

Sumas de Gauss

Las sumas de Gauss nos han aparecido en el capítulo anterior al evaluar las funciones L, pero lo cierto es que estas sumas ya habían sido estudiadas mucho antes de que Kummer y Dirichlet se las encontraran como nosotros nos las hemos encontrado. Como su nombre indica, estas sumas fueron introducidas por Gauss, quien obtuvo importantes resultados sobre y mediante ellas.

En este capítulo trataremos de explicar el motivo de su interés y así mismo obtendremos los resultados que necesitamos para acabar de perfilar el análisis de las funciones L.

12.1 Propiedades básicas

En primer lugar recordamos la definición de las sumas de Gauss:

Definición 12.1 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.

En el capítulo anterior probamos además que si χ es un carácter primitivo entonces

$$G_a(\chi) = \overline{\chi(a)}G(\chi), \tag{12.1}$$

donde $G(\chi) = G_1(\chi)$, luego podemos limitarnos a estudiar esta suma, que recibe el nombre de *suma principal*.

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

$$\omega = \cos\frac{2\pi}{5} + i\ \text{sen}\,\frac{2\pi}{5}.$$

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

$$G(\chi) = \omega + i\omega^2 - i\omega^3 - \omega^4 = -\sqrt{\frac{5-\sqrt{5}}{2}} + \sqrt{\frac{5+\sqrt{5}}{2}}\,i.$$

Observar 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. Lo calculamos en el teorema siguiente, cuya prueba contiene una interesante interpretación algebraica de las sumas de Gauss

Teorema 12.2 *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 $|G(\chi)|^2 = m$. ∎

12.2 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 el hecho siguiente:

Teorema 12.3 *Sea p un primo impar y a un entero primo con p. Entonces*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

DEMOSTRACIÓN: Si $(a/p) = 1$ entonces $a \equiv r^2 \pmod{p}$, de donde se sigue que $a^{(p-1)/2} \equiv r^{p-1} \equiv 1 \pmod{p}$. Por otro lado, el polinomio $x^{(p-1)/2} - 1$ no puede tener más de $(p-1)/2$ raíces módulo p, luego sus raíces son exactamente los $(p-1)/2$ restos cuadráticos módulo p.

Si $(a/p) = -1$, entonces $(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \pmod{p}$, luego ha de ser $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$, y como no es congruente con 1, ha de serlo con -1 ∎

Haciendo $a = -1$ 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. 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

$$\begin{aligned} &\omega^p + \omega^{-p} = \omega + \omega^{-1} = \gamma && \text{si } p \equiv \pm 1 \pmod 8,\\ &\omega^p + \omega^{-p} = \omega^3 + \omega^{-3} = -(\omega + \omega^{-1}) = -\gamma && \text{si } p \equiv \pm 3 \pmod 8. \end{aligned}$$

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 el teorema 12.3:

$$\gamma^{p-1} = (\gamma^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \text{ (mód } p).$$

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 12.4 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 $G(p) = G_1(p)$.

La relación (12.1) implica que si $p \nmid a$ entonces $G_a(p) = (a/p)G(p)$.

En realidad Gauss definió

$$G_a(p) = \sum_{x=0}^{p-1} \omega^{ax^2}. \tag{12.2}$$

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 (12.2), 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. De todos modos la sumas asociadas a primos son las únicas relevantes en el problema que nos ocupa.

Como consecuencia del teorema 12.2 sabemos que $|G(p)| = \sqrt{p}$, pero Gauss probó algo más fuerte:

Teorema 12.5 *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 12.2 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 12.2 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 11.30 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 12.3.

$$G(p)^{q-1} = (G(p)^2)^{(q-1)/2} = p'^{(q-1)/2} \equiv \left(\frac{p'}{q}\right) \pmod{q}.$$

Por otra parte, si consideramos la definición de $G(p)$ tenemos

$$G(p)^q = \left(\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\omega^r\right)^q \equiv \sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\omega^{qr} = G_q(p) = \left(\frac{q}{p}\right)G(p) \text{ (mód } q).$$

Combinando las dos congruencias queda

$$\left(\frac{p'}{q}\right)G(p) \equiv G(p)^q \equiv \left(\frac{q}{p}\right)G(p) \text{ (mód } q).$$

Multiplicamos por $G(p)$ y así $(p'/q)p' \equiv (q/p)p'$ (mód 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. Para esta prueba necesitamos la versión del teorema 12.5 en cuerpos finitos. De hecho el argumento que presentamos es válido en cualquier cuerpo, lo que prueba que se trata de una relación puramente algebraica.

Sean p y q primos impares distintos y sea ω una raíz p-ésima primitiva de la unidad en una extensión de $\mathbb{Z}/q\mathbb{Z}$. Definimos la suma de Gauss

$$\gamma = \sum_{x=1}^{p}\omega^{x^2}.$$

Veamos que $\gamma^2 = (-1)^{(p-1)/2}p$. En principio tenemos

$$\gamma^2 = \sum_{x\,y=1}^{p}\omega^{x^2+y^2}. \tag{12.3}$$

Es fácil ver que la forma cuadrática $x^2 + y^2$ representa todas las clases módulo p. Esto se sigue de los resultados vistos en capítulos anteriores, pero un argumento elemental es el siguiente: dado, r, los polinomios x^2 e $r - y^2$ toman $(p + 1)/2$ valores distintos módulo p, luego ha de haber un x y un y tales que $x^2 = r - y^2$. Sea

$$G = \big\{(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \;\big|\; x^2 + y^2 \neq 0\big\}.$$

Es claro que G es un grupo con el producto dado por

$$(x, y)(x', y') = (xx' - yy', xy' + x'y).$$

El inverso de un par se calcula por la misma fórmula que el de un número complejo. Además la aplicación $(x, y) \mapsto x^2 + y^2$ es un epimorfismo de G en U_p.

De aquí concluimos que la forma x^2+y^2 representa el mismo número de veces cada clase no nula módulo p.

Si $(-1/p) = -1$, entonces $x^2+y^2 = 0$ sólo sucede cuando $x = y = 0$. Por lo tanto, de los p^2 sumandos de (12.3), hay uno igual a $\omega^0 = 1$ y los p^2-1 restantes se reparten entre las $p-1$ potencias no triviales de ω, de modo que cada una aparece $p+1$ veces. Por consiguiente

$$\gamma^2 = 1 + (p+1)\sum_{r=1}^{p-1}\omega^r = 1 + (p-1)(-1) = -p = \left(\frac{-1}{p}\right)p.$$

Si $(-1/p) = 1$ entonces para cada clase $x \in U_p$, la ecuación $x^2+y^2 = 0$ tiene exactamente dos soluciones, luego en total hay $2(p-1)+1$ representaciones del 0, que se corresponden con otros tantos sumandos iguales a 1 en (12.3). Queda un total de $p^2-2p+1 = (p-1)^2$ sumandos, con lo que cada potencia de ω no trivial aparece $p-1$ veces. Así pues,

$$\gamma^2 = 2p-1+(p-1)\sum_{r=1}^{p-1}\omega^r = 2p-1+(p-1)(-1) = p = \left(\frac{-1}{p}\right)p.$$

Por otra parte,

$$\gamma^q = \sum_{x=0}^{p}\omega^{qx^2} = \left(\frac{q}{p}\right)\gamma,$$

pues si $(q/p) = 1$ entonces $q \equiv u^2 \pmod p$, luego $qx^2 \equiv (ux)^2 \pmod p$ y cuando x recorre las clases módulo p lo mismo vale para ux. Por lo tanto en este caso $\gamma^q = \gamma$. En cambio, si $(q/p) = -1$ los exponentes de γ^q recorren dos veces los restos no cuadráticos módulo p (más el cero), mientras que los de γ recorren dos veces los restos cuadráticos (más el cero). Claramente entonces $\gamma+\gamma^q = 0$, pues es dos veces la suma de todas las potencias de ω.

Con esto tenemos que $\gamma^{q-1} = (q/p)$. Ahora bien, $\gamma^2 \in \mathbb{Z}/q\mathbb{Z}$ y será un resto cuadrático módulo q si y sólo si $\gamma \in \mathbb{Z}/q\mathbb{Z}$, si y sólo si $\gamma^{q-1} = \gamma$. Por consiguiente

$$\left(\frac{q}{p}\right) = \left(\frac{\gamma^2}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

■

12.3 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 12.5 era suficiente para demostrar la ley de reciprocidad cuadrática, quedaba planteado el problema de calcular el valor exacto de $G(p)$.

Por 12.5 podemos afirmar que

$$G(p) = \begin{cases} \pm\sqrt{p} & \text{si } p \equiv \ \ 1 \text{ (mód 4)} \\ \pm\sqrt{p}\,i & \text{si } p \equiv -1 \text{ (mód 4)} \end{cases} \tag{12.4}$$

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.*". Vamos a dar una prueba debida a Shur.

Teorema 12.6 *Sea p un primo impar. Entonces*

$$G(p) = \begin{cases} \sqrt{p} & \textit{si } p \equiv \ \ 1 \text{ (mód 4)} \\ \sqrt{p}\,i & \textit{si } p \equiv -1 \text{ (mód 4)} \end{cases}$$

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 (12.2) 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

$$a + b = (p+1)/2, \qquad c + d = (p-1)/2. \tag{12.5}$$

Además tenemos

$$G(p) = \big(a - b + (c - d)i\big)\sqrt{p}. \tag{12.6}$$

Comparando con (12.4) concluimos que

$$\begin{aligned} &a - b = \pm 1, \quad c = d \qquad \text{cuando } p \equiv \ \ 1 \ (\text{mód } 4), \\ &c - d = \pm 1, \quad a = b \qquad \text{cuando } p \equiv -1 \ (\text{mód } 4). \end{aligned} \tag{12.7}$$

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 [1]

$$\sum_{0\le r<s\le p-1} (r+s) = \sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s) = \sum_{r=1}^{p-1} \left(r^2 + \frac{r(r-1)}{2}\right) = 2p\left(\frac{p-1}{2}\right)^2.$$

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 $2b + c - d \equiv p(p-1)/2$ (mód 4). Uniendo esto a (12.5) y (12.7) resulta que si $p \equiv 1$ (mód 4) entonces $c = d$, y

$$a - b = a + b - 2b = \frac{p+1}{2} - 2b \equiv \frac{p+1}{2} - \frac{p-1}{2} \equiv p \equiv 1 \ (\text{mód } 4),$$

luego $a - b = 1$, y si $p \equiv -1$ (mód 4) entonces $a = b$ y

$$c - d \equiv -(p-1)/2 - 2b = -\frac{p-1}{2} - \frac{p+1}{2} \equiv -p \equiv 1 \ (\text{mód } 4),$$

luego $c - d = 1$. En ambos casos (12.6) nos da el resultado. ∎

[1] Usamos aquí la fórmula de Bernoulli: $\sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1)}{6}$. La probaremos en el capítulo siguiente, p. 323.

Las sumas de Gauss tienen aplicaciones muy diversas en teoría de números. Entre otras cosas, permiten calcular el número de soluciones de ciertas congruencias, permiten obtener generalizaciones de la ley de reciprocidad cuadrática y tienen importancia en el estudio de los cuerpos ciclotómicos. Ahora nos dedicaremos a obtener los resultados adicionales que nos hacen falta para completar nuestra evaluación de las funciones L. Para el caso cuadrático debemos extender el teorema anterior a sumas de caracteres de módulo no necesariamente primo. Todas las dificultades de cálculo las hemos superado ya. Lo que queda es fácil. La clave es el teorema siguiente:

Teorema 12.7 *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 $m = m_1 \times m_n$. 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,

$$G_a(\chi_1)G_a(\chi_2)\,\chi_1(m_2)\chi_2(m_1) = \Big(\sum_{u,v} \chi_1(u)\chi_2(v)\omega^{m_2 a u + m_1 a v}\Big)\chi_1(m_2)\chi_2(m_1)$$

$$= \sum_{u,v} \chi_1(m_2 u)\chi_2(m_1 v)\omega^{a(m_2 u + m_1 v)}$$

$$= \sum_{u,v} \chi_1(m_2u + m_1v)\chi_2(m_2u + m_1v)\omega^{a(m_2u+m_1v)} = \sum_r \chi_1(r)\chi_2(r)\omega^{ar}$$

$$= \sum_r \chi(r)\omega^{ar} = G_a(\chi),$$

donde u varía en U_{m_1}, v varía en U_{m_2} y r en U_m. ∎

Con esto podemos probar:

Teorema 12.8 *Sea χ un carácter cuadrático primitivo módulo m. Entonces*

$$G(\chi) = \begin{cases} \sqrt{m} & \text{si } \chi(-1) = 1 \\ i\sqrt{m} & \text{si } \chi(-1) = -1 \end{cases}$$

DEMOSTRACIÓN: Por el teorema 11.22 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 12.6 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 $\delta\epsilon$. ∎

12.4 El número de clases en cuerpos cuadráticos

Si en las fórmulas del teorema 11.11 evaluamos la función L mediante las fórmulas del teorema 11.31 y en éstas evaluamos la suma de Gauss, obtenemos el teorema siguiente:

Teorema 12.9 *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 $0 < k < |\Delta|$, $(k, \Delta) = 1$.

Notar 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 $h = 1$.

La fórmula para cuerpos 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 del teorema 12.8 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

$$\begin{aligned} hm &= -\sum_k \chi_K(k)k = -\sum_{k=1}^{m/2}\chi_K(k)k - \sum_{k=1}^{m/2}\chi_K(m-k)(m-k) \\ &= -\sum_{k=1}^{m/2}\chi_K(k)k + \sum_{k=1}^{m/2}\chi_K(k)(m-k) \\ &= -2\sum_{k=1}^{m/2}\chi_K(k)k + m\sum_{k=1}^{m/2}\chi_K(k). \end{aligned} \tag{12.8}$$

Por otra parte separamos los sumandos pares de los impares:

$$hm = -\sum_k \chi_K(k)k = -\sum_{k=1}^{m/2}\chi_K(2k)2k - \sum_{k=1}^{m/2}\chi_K(m-2k)(m-2k)$$

$$\begin{aligned} &= -2\chi_K(2)\sum_{k=1}^{m/2}\chi_K(k)k + \sum_{k=1}^{m/2}\chi_K(2k)(m-2k) \\ &= -4\chi_K(2)\sum_{k=1}^{m/2}\chi_K(k)k + m\,\chi_K(2)\sum_{k=1}^{m/2}\chi_K(k). \end{aligned}$$

Por lo tanto

$$hm\,\chi_K(2) = -4\sum_{k=1}^{m/2}\chi_K(k)k + m\sum_{k=1}^{m/2}\chi_K(k). \tag{12.9}$$

Multiplicamos (12.8) por 2 y le restamos (12.9):

$$hm\big(2-\chi_K(2)\big) = m\sum_{k=1}^{m/2}\chi_K(k).$$

Finalmente observamos que la ecuación obtenida en el caso m par es ésta misma, puesto que entonces $\chi_K(2) = 0$. En resumen:

Teorema 12.10 *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. El enunciado es claramente:

Teorema 12.11 *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. (Esto lo sabíamos ya como consecuencia de la teoría de géneros.)

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.

Ejemplo Vamos a calcular el número de clases de $\mathbb{Q}(\sqrt{-23})$. La tabla siguiente indica el símbolo de Legendre de los números necesarios:

1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	−1	1	−1	1	1	−1	−1

(Notar que sólo hace falta calcular los valores para 2, 3, 5, 7 y 11. Los restantes se deducen de éstos.)

Por consiguiente $h = 7 - 4 = 3$. ∎

En el caso real no hay fórmulas tan simple, pero vamos a encontrar una variante interesante de la fórmula del teorema 12.9.

Consideremos

$$\theta = \frac{\prod_b \operatorname{sen}(\pi b/\Delta)}{\prod_a \operatorname{sen}(\pi a/\Delta)},$$

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 12.9 es

$$h = \frac{1}{\log \epsilon} \log \theta,$$

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 $\theta > 0$.

Los resultados que hemos obtenido se aplican también a los cuerpos ciclotómicos, pero nos ocuparemos de ello en el próximo tema.

Capítulo XIII

Cuerpos ciclotómicos

En este capítulo obtendremos la fórmula analítica para el número de clases de los cuerpos ciclotómicos de orden primo y de su análisis obtendremos la caracterización de Kummer de los primos regulares.

13.1 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^*. Partimos de las fórmulas que obtuvimos en el capítulo XI para el número de clases de ambos cuerpos (teoremas 11.26 y 11.32):

$$h = \frac{\sqrt{p}^{\,p}}{2^{m-1}\pi^m\, R} \prod_{\chi\neq 1} L(1,\chi), \qquad h^* = \frac{\sqrt{p}^{\,m-1}}{2^{m-1}R^*} \prod_{\substack{\chi(1)=1\\ \chi\neq 1}} L(1,\chi).$$

El teorema 4.28 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 $h = h_1h_2$, 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 el capítulo XI 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 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 13.1 *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.

13.2 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 11.31 evaluando la suma de Gauss mediante 12.2:

$$|L(1,\chi^{2r+1})| = \frac{\pi\sqrt{p}}{p^2}\left|\sum_{k=1}^{p-1}\bar{\chi}^{2r+1}(k)\,k\right|.$$

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

$$h_1 = \frac{1}{(2p)^{m-1}}\,|F(\zeta)F(\zeta^3)\cdots F(\zeta^{p-2})|. \tag{13.1}$$

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 13.1 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 (13.1) 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 13.1 (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 13.2 *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 13.1: 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 13.2 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 (13.1). Sea

$$B = F(\zeta)F(\zeta^3)\cdots F(\zeta^{p-2}).$$

El número B es, salvo el signo, el determinante del teorema 13.2, 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 $p \equiv 1 \pmod{p-1}$, el teorema 3.20 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 $\zeta^{-r} \equiv g \pmod{\mathfrak{p}}$, 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 $g\zeta^s \equiv 1 \equiv g\zeta^r \pmod{\mathfrak{p}}$, luego $\zeta^s \equiv \zeta^r \pmod{\mathfrak{p}}$ 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:

$$\sum_{k=0}^{p-2} g_k g^{kr} \equiv \sum_{k=0}^{p-2} g^k g^{kr} \equiv \sum_{k=0}^{p-2} g^{k(r+1)} \equiv \sum_{k=0}^{p-2} g_k^{r+1} \equiv \sum_{n=1}^{p-1} n^{r+1} \pmod{p^2}. \quad (13.2)$$

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,

$$g_k^{r+1} \equiv (r+1)g_k g^{kr} - kg^{k(r+1)} \pmod{p^2}. \quad (13.3)$$

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 (13.2) 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 (13.3) 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 13.3 *Se cumple que p divide al primer factor de h si y sólo si p^2 divide a alguno de los números*

$$S_r = \sum_{n=1}^{p-1} n^r, \quad \textit{para } r = 2,\ 4,\ \ldots,\ p-3.$$

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. Nos ocupamos de ella en la sección siguiente.

13.3 Los números de Bernoulli

Hay fórmulas para calcular las sumas de potencias $1^k + 2^k + \cdots + m^k$. La correspondiente a $k = 1$ es sobradamente conocida:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Fue Jacques Bernoulli quien obtuvo la generalización de esta fórmula a exponentes superiores, y sus resultados eran bien conocidos en la época de Kummer. Básicamente Bernoulli demostró que existe un único polinomio de grado n, hoy llamado polinomio de Bernoulli, $B_n(x)$, tal que

$$x^n = \int_x^{x+1} B_n(x)\, dx.$$

Por ejemplo, si planteamos

$$\begin{aligned} x^2 &= \int_x^{x+1} (ax^2+bx+c)\,dx = \left[\frac{ax^3}{3}+\frac{bx^2}{2}+cx\right]_x^{x+1} \\ &= ax^2+(a+b)x+\frac{1}{3}\,a+\frac{1}{2}\,b+c, \end{aligned}$$

al igualar los coeficientes llegamos a que $B_2(x) = x^2 - x + 1/6$, de donde

$$\sum_{k=1}^{m} k^2 = \int_1^{m+1} B_2(x)\,dx = \frac{m(m+1)(2m+1)}{6}.$$

Para obtener los resultados generales sobre los polinomios de Bernoulli que vamos a necesitar conviene introducirlos desde un contexto diferente, relacionado con las investigaciones de Euler sobre las series

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}.$$

Definición 13.4 Llamaremos *polinomios de Bernoulli* a las funciones $B_k(x)$ determinadas por

$$\frac{ze^{xz}}{e^z-1} = \sum_{k=0}^{\infty} \frac{B_k(x)}{k!} z^k.$$

Observar que la función de la izquierda tiene una singularidad evitable en 0, por lo que se trata de una función entera y la serie de potencias de la derecha converge en todo el plano complejo.

Se llama *números de Bernoulli* a los números $B_k = B_k(0)$.

El teorema siguiente demuestra que las funciones $B_k(x)$ son efectivamente polinomios, así como que están determinados por los números de Bernoulli.

Teorema 13.5 *Se cumple que* $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k\, x^{n-k}$.

Demostración: En efecto:

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n &= \frac{z}{e^z-1} e^{xz} = \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n\right)\left(\sum_{n=0}^{\infty} \frac{x^n}{n!} z^n\right) \\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{B_k}{k!}\frac{x^{n-k}}{(n-k)!} z^n. \end{aligned}$$

Comparando coeficientes queda

$$B_n(x) = \sum_{k=0}^{n} n!\frac{B_k}{k!}\frac{x^{n-k}}{(n-k)!} = \sum_{k=0}^{n} \binom{n}{k} B_k\, x^{n-k}.$$

■

Una regla para recordar esta fórmula es

$$B_n(x) = (B + x)^n,$$

donde las "potencias" B^k que aparecen al aplicar el teorema del binomio han de entenderse como los números de Bernoulli B_k.

Ahora veremos que los polinomios que hemos definido se corresponden con los polinomios estudiados por Bernoulli. Ello es consecuencia del teorema que sigue.

Teorema 13.6 *Para todo $n \geq 1$ se cumple*

$$\frac{d\,B_{n+1}(x)}{dx} = (n+1)B_n(x).$$

DEMOSTRACIÓN: Por el teorema anterior $B_{n+1}(x) = \sum_{k=0}^{n+1} \binom{n+1}{k} B_k x^{n+1-k}$. Por lo tanto

$$\begin{aligned}\frac{d\,B_{n+1}(x)}{dx} &= \sum_{k=0}^{n} \frac{(n+1)!}{k!(n+1-k)!} B_k(n+1-k)x^{n-k} \\ &= (n+1)\sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k} = (n+1)B_n(x).\end{aligned}$$

■

El teorema siguiente recoge las propiedades más importantes de los números y polinomios de Bernoulli:

Teorema 13.7 *Para todo $n \geq 0$ se cumple:*

1. *$B_{n+1}(x+1) - B_{n+1}(x) = (n+1)x^n$. En particular, para $n \geq 2$ tenemos que $B_n(0) = B_n(1)$.*
2. *Como consecuencia,*

$$x^n = \frac{B_{n+1}(x+1) - B_{n+1}(x)}{n+1} = \int_x^{x+1} B_n(x)\,dx.$$

3. *Esto a su vez implica*

$$\sum_{k=1}^{m} k^n = \int_1^{m+1} B_n(x)\,dx = \frac{B_{n+1}(m+1) - B_{n+1}}{n+1}.$$

DEMOSTRACIÓN: La identidad siguiente se comprueba sin esfuerzo:

$$z\frac{e^{(x+1)z}}{e^z - 1} - z\frac{e^{xz}}{e^z - 1} = ze^{xz}.$$

Desarrollando en serie ambos miembros queda

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

Igualando los coeficientes obtenemos el resultado. ∎

Teniendo en cuenta que $B_n = B_n(0) = B_n(1)$, el teorema 13.5 nos da la relación siguiente.

Teorema 13.8 *Para $n \geq 2$ se cumple que $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$.*

Podemos expresar esta fórmula como $B_n = (B+1)^n$. Observar que B_n figura en ambos miembros de la igualdad, por lo que se simplifica. Esta fórmula aplicada a $n+1$ expresa a B_n en función de los números anteriores y en particular demuestra que los números de Bernoulli son números racionales. Teniendo en cuenta que $B_0 = 1$ podemos calcular fácilmente los restantes. Por ejemplo:

$$\begin{array}{ll} B_2 = B_0 + 2B_1 + B_2, & \text{luego } B_1 = -1/2. \\ B_3 = B_0 + 3B_1 + 3B_2 + B_3, & \text{luego } B_2 = 1/6. \end{array}$$

Los números de Bernoulli de índice impar distinto de 1 son todos nulos. Lo demostraremos enseguida. Los siguientes números de índice par son

$$B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2.730},$$

$$B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3.617}{510}, \quad B_{18} = \frac{43.867}{798}, \quad B_{20} = -\frac{174.611}{330}, \quad \ldots$$

Los numeradores y denominadores de los números B_{2n} crecen muy rápidamente. Por ejemplo, Euler calculó hasta

$$B_{30} = \frac{8.615.841.276.005}{14.322}.$$

Los primeros polinomios de Bernoulli son

$$\begin{aligned} B_0(x) &= 1, \\ B_1(x) &= x - \frac{1}{2}, \\ B_2(x) &= x^2 - x + \frac{1}{6}, \\ B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x, \\ B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30}, \\ B_5(x) &= x^5 - \frac{4}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x. \end{aligned}$$

Del teorema 13.7 se siguen ahora fácilmente los casos particulares

$$\sum_{k=1}^{m} k = \frac{m(m+1)}{2}, \quad \sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1}{6}, \quad \sum_{k=1}^{m} k^3 = \frac{m^2(m+1)^2}{4}.$$

Respecto a los números de Bernoulli de índice impar, observemos que, por la definición y teniendo en cuenta que $B_0 = 1$, $B_1 = -1/2$,

$$f(z) = \frac{z}{e^z - 1} - 1 + \frac{z}{2} = \sum_{k=2}^{\infty} \frac{B_k}{k!} z^k,$$

y $f(z)$ es par, pues

$$f(z) - f(-z) = \frac{z}{e^z - 1} + \frac{z}{2} + \frac{z}{e^{-z} - 1} + \frac{z}{2} = z\left(1 + \frac{-2 + e^z + e^{-z}}{2 - e^z - e^{-z}}\right) = 0.$$

Esto implica que $B_{2k+1} = 0$, para $k \geq 1$, tal y como habíamos afirmado.

Nuestro interés en los números de Bernoulli se debe a que proporcionan fórmulas para calcular las sumas S_r que aparecen en el teorema 13.3. El teorema siguiente nos permitirá reformular la condición de dicho teorema en términos de los números B_{2n}. Para enunciarlo definamos un p-entero como un número racional r tal que p no divide al denominador de su fracción irreducible. Es claro que el conjunto de los p-enteros es un anillo cuyo único primo es p (de hecho es precisamente $\mathbb{Q} \cap \mathbb{Z}_p$).

Teorema 13.9 (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. Sea p un primo cualquiera. Llamemos $S_m(p) = \sum_{k=1}^{p-1} k^m$. Entonces los teoremas 13.5 y 13.7 nos dan que

$$(m+1)S_m(p) = B_{m+1}(p) - B_{m+1} = \sum_{k=0}^{m} \binom{m+1}{k} B_k\, p^{m+1-k}.$$

Equivalentemente

$$pB_m = S_m(p) - \sum_{k=0}^{m-1} \frac{1}{m+1} \binom{m+1}{k} p^{m-k} pB_k. \tag{13.4}$$

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

$$E(r/p) + E(r/p^2) + \cdots < \frac{r}{p} + \frac{r}{p^2} + \cdots = \frac{r}{p-1} \le \frac{r}{2} \le r-1 = m-k,$$

donde E denota la parte entera (observar 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 (13.4) implica ahora que

$$pB_m \equiv S_m(p) \pmod{p}.$$

Si $p-1 \mid m$ entonces $k^m \equiv 1 \pmod{p}$ para $1 \le k \le p-1$, luego

$$S_m(p) = \sum_{k=1}^{p-1} k^m \equiv p-1 \equiv -1 \pmod{p},$$

mientras que si $p-1 \nmid m$, tomando una raíz primitiva g módulo p tenemos

$$S_m(p) = \sum_{k=1}^{p-1} k^m \equiv \sum_{r=0}^{p-2} g^{mr} = \frac{g^{(p-1)m}-1}{g^m-1} \equiv 0 \pmod{p},$$

pues $p \nmid g^m - 1$ pero $p \mid g^{(p-1)m} - 1$.

Resulta, pues, que $pB_m \equiv -1, 0 \pmod{p}$ 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 (13.4) son p-enteros. Si además suponemos que $m \le p-1$ 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 13.10 *Si p es un primo, m es par y $m \le p-1$, entonces*

$$pB_m \equiv S_m(p) \pmod{p^2}.$$

Esto nos permite reformular como sigue el teorema 13.3:

Teorema 13.11 *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 13.3 es que p^2 no ha de dividir a las sumas $S_k(p)$ para $k = 2, 4, \ldots, p-3$. Por el teorema anterior esto equivale a que p^2 no divida a pB_k en el anillo de los p-enteros, y como p no divide a los denominadores de los B_k, esto equivale a que p no divida a los numeradores de los B_k. ∎

13.4 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 11.31 y 12.2:

$$|L(1,\chi^{2r})| = \frac{|G(\chi^{2r})|}{p}\left|\sum_{k=0}^{p-2}\bar{\chi}^{2r}(g^k)\log|1-\omega^{g^k}|\right| = \frac{1}{\sqrt{p}}\left|\sum_{k=0}^{p-2}\zeta^{2rk}\log|1-\omega^{g^k}|\right|.$$

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 13.1 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

$$h_2 = \frac{1}{R^*}\left|\prod_{r=1}^{m-1}\sum_{k\in G} a_k\,\psi^r(k)\right|. \tag{13.5}$$

No podemos aplicar 13.1 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 (13.5) 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 13.1 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 filas restantes 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

$$\rho = -\omega^{(p+1)/2} = \cos(\pi/p) + i\,\mathrm{sen}(\pi/p) \in K.$$

Entonces $\omega = \rho^2$, de donde

$$\frac{1-\omega^k}{1-\omega} = \frac{1-\rho^{2k}}{1-\rho^2} = \rho^{k-1}\,\frac{\rho^k - \rho^{-k}}{\rho - \rho^{-1}} = \rho^{k-1}\,\frac{\mathrm{sen}(k\pi/p)}{\mathrm{sen}(\pi/p)}.$$

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

$$\theta_k = \frac{\mathrm{sen}(k\pi/p)}{\mathrm{sen}(\pi/p)} = \rho^{1-k}\frac{1-\omega^k}{1-\omega}, \qquad \text{para } p \nmid k, \tag{13.6}$$

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 $g^i \equiv \pm g^j \pmod p$ con $1 \le i \le j \le m-1$ entonces $g^{j-i} \equiv \pm 1 \pmod p$ 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 $\pm g^i \equiv 1 \pmod p$ 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 $\epsilon_1,\dots,\epsilon_{m-1}$. 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. Es conocido que el determinante de la matriz que relaciona ambas bases es precisamente el índice del subgrupo. En resumen, hemos probado el teorema siguiente:

Teorema 13.12 *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 el capítulo IV 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

$$\epsilon^p = \prod_{k=2}^{m}\theta_k^{c_k}, \tag{13.7}$$

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 (13.7) 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 habremos de 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 $p'(x)/p(x)$.

13.5 Numeros p-ádicos ciclotómicos

Sea $\mathfrak{p}$ el único divisor primo de p en el cuerpo ciclotómico K. Consideramos la valoración $\mathfrak{p}$-ádica $v_\mathfrak{p}$ según la definición 7.9, la cual induce a su vez el valor absoluto

$$|\alpha|_\mathfrak{p} = \rho^{v_\mathfrak{p}(\alpha)}, \qquad 0 < \rho < 1.$$

Llamaremos $K_\mathfrak{p}$ al cuerpo de los números $\mathfrak{p}$-ádicos, es decir, a la compleción de K respecto a este valor absoluto (teorema 7.8) Claramente $\mathbb{Q} \subset K \subset K_\mathfrak{p}$. Llamaremos $\mathcal{O}_\mathfrak{p}$ al anillo de los enteros de $\mathfrak{p}$-ádicos, que según 7.14 es la clausura en $K_\mathfrak{p}$ de $\mathbb{Z}[\omega]$. Según dicho teorema tenemos también que $\mathcal{O}_\mathfrak{p}/\mathfrak{p} \cong \mathbb{Z}[\omega]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. En particular todo entero $\mathfrak{p}$-ádico es congruente módulo $\mathfrak{p}$ con un entero racional.

Puesto que $p = \mathfrak{p}^{p-1}$, se cumple $v_p(r) = (p-1)v_\mathfrak{p}(r)$, para todo $r \in \mathbb{Q}$ no nulo. Por consiguiente

$$|r|_\mathfrak{p} = \rho^{v_p(r)/(p-1)} = |r|_p,$$

donde definimos el valor absoluto p-ádico tomando como base $\rho^{1/(p-1)}$. Esto significa que el valor absoluto $\mathfrak{p}$-ádico extiende al valor absoluto p–ádico. Por consiguiente, la clausura de $\mathbb{Q}$ en $K_\mathfrak{p}$ es una compleción de $\mathbb{Q}$ respecto al valor absoluto p-ádico, y según el teorema 7.8 es topológicamente isomorfa a $\mathbb{Q}_p$. En vista de esto podemos considerar $\mathbb{Q}_p \subset K_\mathfrak{p}$. En particular $\mathbb{Z}_p \subset \mathcal{O}_\mathfrak{p}$.

El teorema siguiente nos da la relación fundamental entre $K_\mathfrak{p}$ y $\mathbb{Q}_p$.

Teorema 13.13 *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 en primer lugar que $1, \pi, \pi^2, \ldots, \pi^{p-2}$ son linealmente independientes sobre $\mathbb{Q}_p$ (con lo que también lo serán sobre $\mathbb{Z}_p$). Consideremos una combinación lineal nula

$$\alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \cdots + \alpha_{p-2}\pi^{p-2} = 0.$$

Si no todos los coeficientes son nulos, multiplicando por una potencia adecuada de p podemos conseguir otra combinación con no todos los coeficientes nulos y tal que todos son enteros p-ádicos y al menos uno de ellos es una unidad. Sea i el menor índice tal que α_i sea una unidad. Para todo $j < i$ tenemos que

$$v_{\mathfrak{p}}(\alpha_j\pi^j) = j + v_{\mathfrak{p}}(\alpha_j) = j + (p-1)v_p(\alpha_j) \geq p - 1 \geq i + 1.$$

Si $j > i$ concluimos igualmente que

$$v_{\mathfrak{p}}(\alpha_j\pi^j) = j + v_{\mathfrak{p}}(\alpha_j) \geq j \geq i + 1,$$

es decir, $\mathfrak{p}^{i+1}$ divide a todos los términos de la combinación lineal salvo quizá a $\alpha_i\pi^i$, pero esto implica que también divide a éste, luego $\mathfrak{p} \mid \alpha_i$, y esto es contradictorio, pues $v_{\mathfrak{p}}(\alpha_i) = (p-1)v_p(\alpha_i) = 0$.

Ahora basta probar 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 7.16, 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 $0 \leq a_{0,i} \leq p-1$ 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

$$\alpha = \left(\sum_{i=0}^{\infty} a_{i,0}p^i\right) + \left(\sum_{i=0}^{\infty} a_{i,1}p^i\right)\pi + \cdots + \left(\sum_{i=0}^{\infty} a_{i,p-2}p^i\right)\pi^{p-2}.$$

Finalmente, todo elemento de $K_{\mathfrak{p}}$ puede expresarse como $p^n\alpha$, con $\alpha \in \mathcal{O}_{\mathfrak{p}}$ y $n \in \mathbb{Z}$. De aquí se sigue inmediatamente que $1, \pi, \pi^2, \ldots, \pi^{p-2}$ es un generador de $K_{\mathfrak{p}}$ sobre $\mathbb{Q}_p$. ∎

Si aplicamos el teorema anterior al primo $\pi = \omega - 1$ concluimos que

$$K_\mathfrak{p} = \mathbb{Q}_p(1, \pi, \pi^2, \dots \pi^{p-2}) = \mathbb{Q}_p(\pi) = \mathbb{Q}_p(\omega),$$

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 $i = 1, \dots, p-1$. 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 7.25 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 7.26 garantiza además que $\log(\epsilon)$ es un entero múltiplo de $\mathfrak{p}^2$ (en efecto,con la notación del capítulo VII tenemos $e = p-1$ y $\kappa = 2$).

Ejercicio: Probar que $\log \omega = 0$.

Recordemos que nuestra intención es tomar logaritmos en la ecuación (13.7), 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:

$$p \log \epsilon^{p-1} = \sum_{k=2}^{m} c_k \log \theta_k^{p-1}. \tag{13.8}$$

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 13.13, pero primero escogeremos un primo π adecuado.

Veamos que existe un único primo $\pi \in \mathcal{O}_\mathfrak{p}$ tal que

$$p = -\pi^{p-1} \quad \text{y} \quad \pi \equiv 1-\omega \ (\text{mód } \mathfrak{p}^2). \tag{13.9}$$

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: $(p-1)! \equiv -1 \ (\text{mód } p)$ (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).

Aplicamos el teorema 7.18 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 $\gamma \equiv 1 \pmod{\mathfrak{p}}$.

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 (13.9) 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 (13.9) 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. Según el teorema 7.20 tenemos que $\zeta \in \mathbb{Q}_p$, luego 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 13.13). 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 $\{1, \pi^2, \pi^4, \ldots, \pi^{p-2}\}$, o sea, 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 ϵ 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 13.13. 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 7.26 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 13.14 *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 13.15 *Si π es un primo $\mathfrak{p}$-ádico que cumple las condiciones* (13.9)*, 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 13.13.

13.6 La caracterización de los primos regulares

Con los resultados de la sección anterior estamos en condiciones de estudiar la divisibilidad del segundo factor del número de clases entre el primo p. Por el teorema 13.14 sabemos que los números $\log \theta_k^{p-1}$ son enteros $\mathfrak{p}$-ádicos de traza nula, luego por 13.15 se pueden expresar en la forma

$$\log \theta_k^{p-1} = \sum_{i=1}^{m-1} b_{ki}\pi^{2i}, \quad 2 \le k \le m, \tag{13.10}$$

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

$$\log(\theta_k^{p-1}) \equiv L(\theta_k^{p-1}) \pmod{\pi^p}. \tag{13.11}$$

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

$$E(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^{p-1}}{(p-1)!}. \tag{13.12}$$

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 13.16 *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 13.17 *Si el primo π cumple* (13.9) *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

$$E(p)^p \equiv 1 \text{ (mód } \pi^{2p-1}). \tag{13.13}$$

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 13.16 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

$$ph(x) = \frac{px}{1!} + \frac{(px)^2}{2!} + \cdots + \frac{(px)^{p-1}}{(p-1)!} + x^p H(x), \tag{13.14}$$

donde $H(x) = M(x) - g(x)^p$ tiene coeficientes enteros. Despejando $x^p H(x)$ en (13.14) 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 (13.9).

Por definición de E y por (13.9) 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 (13.13) 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 (13.6) vemos que

$$\theta_k^p = (1 + \omega + \cdots + \omega^{k-1})(-1)^{1-k}.$$

Por (13.9) 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,

$$\begin{aligned}\theta_k^{p-1} &\equiv \theta_k^{-1}\, k\,(-1)^{1-k} \equiv k\,\frac{\omega-1}{\omega^k-1}\,(-\rho)^{k-1}\\ &= \frac{\omega-1}{\pi}\left(\frac{\omega^k-1}{k\pi}\right)^{-1}\omega^{(k-1)(p+1)/2} \pmod{\pi^{p-1}}.\end{aligned}$$

Notar que todos los factores del último miembro son unidades principales. Ciertamente ω lo es, de $\pi \equiv \omega - 1 \pmod{\pi^2}$ 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 13.16:

$$L(\theta_k^{p-1}) \equiv L\left(\frac{\omega-1}{\pi}\right) - L\left(\frac{\omega^k-1}{k\pi}\right) + \frac{k-1}{2}L(\omega) \pmod{\pi^{p-1}}.$$

Por el teorema anterior y 13.16, $\omega^k \equiv E(k\pi) \pmod{\pi^p}$, de donde

$$\frac{\omega^k-1}{k\pi} \equiv \frac{E(k\pi)-1}{k\pi} \pmod{\pi^{p-1}}.$$

Lo mismo es válido para $(\omega-1)/\pi$, con lo que

$$L(\theta_k^{p-1}) \equiv L\left(\frac{E(\pi)-1}{\pi}\right) - \frac{\pi}{2} - L\left(\frac{E(k\pi)-1}{k\pi}\right) + \frac{k\pi}{2} \pmod{\pi^{p-1}}. \quad (13.15)$$

Esta expresión nos lleva a estudiar el polinomio

$$L\left(\frac{E(x)-1}{x}\right) - \frac{x}{2}.$$

Para ello consideramos la función

$$\log\left(\frac{\exp(x)-1}{x}\right) - \frac{x}{2} = \log(\exp(x)-1) - \log x - \frac{x}{2}. \quad (13.16)$$

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 13.4 (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 13.16 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 (13.12) 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 (13.15), que junto con (13.11) 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 (13.10) 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 13.9 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 13.11 y 13.15 llegamos a la conclusión siguiente:

Teorema 13.18 *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 13.19 (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 $B_2, B_4, \ldots, B_{p-3}$.*

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 13.12 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 (13.7) 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 (13.7), 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 $\epsilon^{p-1} \equiv 1$ (mód 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 (13.7) y tomamos logaritmos, con lo que obtenemos (13.8).

Por el teorema 13.14 tenemos que $\log \epsilon^{p-1}$ es un entero p-ádico de traza nula, luego por el teorema 13.18 se expresa de forma única como combinación lineal de $\log \theta_k^{p-1}$ con coeficientes en $\mathbb{Z}_p$, pero por (13.8) 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 teorema 4.27 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 (13.9) tenemos que $\omega \equiv 1 + \pi \pmod{\pi^2}$, luego $\omega^k \equiv 1 + k\pi \pmod{\pi^2}$. Por lo tanto tenemos que

$$a \equiv b(1 + k\pi) \pmod{\pi^2}. \tag{13.17}$$

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 (13.17) 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 13.14 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 13.14 tenemos que $\log \epsilon^{p-1}/p$ es un entero p-ádico real de traza nula, luego por 13.18 podemos expresar

$$\log \epsilon^{p-1} = \sum_{k=2}^{m} pc_k \log \theta_k^{p-1}, \tag{13.18}$$

para ciertos enteros p-ádicos c_k.

Por otra parte, el grupo generado por los números θ_k tiene índice finito (teorema 13.12) en el grupo de las unidades reales positivas. En consecuencia existe un número natural $a \neq 0$ tal que

$$\epsilon^a = \prod_{k=2}^{m} \theta_k^{d_k}, \tag{13.19}$$

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 (13.18) 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 (13.19) 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 hemos llegado al 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.

Tabla 13.2: 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 $61,9\%$).

Capítulo XIV

Números trascendentes

Dedicamos este último capítulo a dar una pequeña muestra de las aplicaciones de la teoría algebraica de números a las pruebas de trascendencia. Éstas son esencialmente analíticas, pero requieren conceptos algebraicos elementales, como la teoría de Galois (o al menos la teoría sobre polinomios simétricos) y los enteros algebraicos. En realidad, los últimos avances en la teoría de números trascendentes hacen uso de un aparato algebraico mucho más sofisticado, pero no vamos a entrar en ello. Aquí probaremos dos resultados clásicos, el teorema de Lindemann-Weierstrass, que data del siglo pasado, y el teorema de Gelfond-Schneider, de 1934.

14.1 El teorema de Lindemann-Weierstrass

En 1873 Hermite demostró la trascendencia del número e. Anteriormente ya se había probado que e no era racional. De hecho era conocido su desarrollo en fracción continua, visto en el tema anterior. En 1882 Lindemann consiguió generalizar el argumento de Hermite y demostró la trascendencia de π. Lindemann afirmó que sus técnicas permitían probar de hecho un resultado mucho más general. La primera prueba detallada de este resultado fue publicada por Weierstrass y constituirá el contenido de esta sección junto con sus consecuencias inmediatas. Necesitaremos dos resultados auxiliares.

Teorema 14.1 *Sean $f_i(x) \in \mathbb{Z}[x]$, $i = 1, \ldots, r$ polinomios no constantes de grado k_i y para cada i sean $\beta_{1i}, \ldots, \beta_{k_i i}$ las raíces de $f_i(x)$. Supongamos que son no nulas. Sean $a_i \in \mathbb{Z}$ para $i = 0, \ldots, r$ tales que $a_0 \neq 0$. Entonces*

$$a_0 + \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} e^{\beta_{ki}} \neq 0.$$

Demostración: Supongamos que se cumple la igualdad. Vamos a expresar cada $e^{\beta_{ki}}$ como

$$e^{\beta_{ki}} = \frac{M_{ki} + \epsilon_{ki}}{M_0}, \quad k = 1, \ldots, k_i, \quad i = 1, \ldots, r,$$

donde $M_0 \in \mathbb{Z}$, $M_0 \neq 0$. Entonces, sustituyendo en la igualdad obtendremos que

$$a_0 M_0 + \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki} + \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} \epsilon_{ki} = 0, \tag{14.1}$$

con $a_0 M_0 \neq 0$.

Vamos a encontrar un primo p tal que $a_0 M_0$ no sea divisible entre p, mientras que la suma

$$\sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki}$$

será un número entero múltiplo de p. Por otra parte se cumplirá que

$$\left| \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} \epsilon_{ki} \right| < 1, \tag{14.2}$$

con lo que tendremos una contradicción, pues en (14.1) los dos primeros sumandos son un entero no divisible entre p, luego no nulo, mientras que el tercero tiene módulo menor que 1.

Para conseguir todo esto definimos primeramente

$$f(z) = \prod_{i=1}^{r} f_i(z) = b_0 + b_1 z + \cdots + b_N z^N = b_N \prod_{i=1}^{r} \prod_{k=1}^{k_i} (z - \beta_{ki}),$$

donde $N = \sum_{i=1}^{r} k_i$ y $b_0 \neq 0$, ya que las raíces son no nulas. Podemos suponer que $b_N > 0$. Sea

$$M_0 = \int_0^{+\infty} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z}}{(p-1)!}\, dz,$$

donde p es un número primo y la integración se realiza sobre el semieje real positivo.

Vamos a probar que la integral es finita y que, si p es suficientemente grande, se trata de un número entero no divisible entre p. Notar que

$$b_N^{(N-1)p-1} z^{p-1} f^p(z) = b_N^{(N-1)p-1} b_0^p z^{p-1} + \sum_{s=p+1}^{(N+1)p} c_{s-1} z^{s-1},$$

para ciertos coeficientes $c_s \in \mathbb{Z}$, y $b_N b_0 \neq 0$. Por lo tanto

$$\begin{aligned} M_0 &= \frac{b_N^{(N-1)p-1} b_0^p}{(p-1)!} \int_0^{+\infty} z^{p-1} e^{-z}\, dz + \sum_{s=p+1}^{(N+1)p} \frac{c_{s-1}}{(p-1)!} \int_0^{+\infty} z^{s-1} e^{-z}\, dz \\ &= b_N^{(N-1)p-1} b_0^p + \sum_{s=p+1}^{(N+1)p} \frac{(s-1)!}{(p-1)!} c_{s-1} = b_N^{(N-1)p-1} b_0^p + pC, \end{aligned}$$

para un cierto $C \in \mathbb{Z}$. Hemos hecho uso de la conocida identidad de Euler

$$n! = \int_0^{+\infty} z^n e^{-z}\, dz,$$

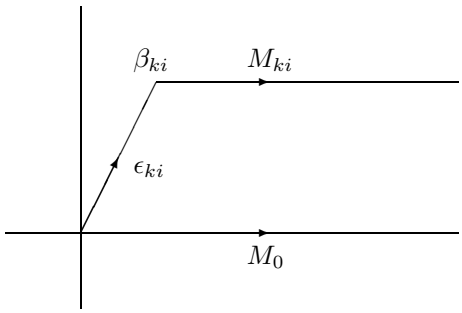
que se demuestra sin dificultad por inducción sobre n integrando por partes.

Así, cualquier primo p mayor que $|a_0|$, b_N, $|b_0|$ hace que M_0 sea un entero racional y que $p \nmid a_0 M_0$.

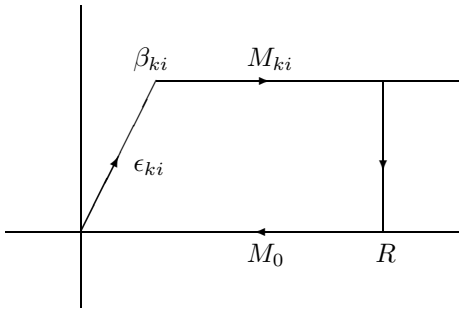
Ahora definimos

$$\begin{aligned} M_{ki} &= e^{\beta_{ki}} \int_{\beta_{ki}}^{+\infty} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z}}{(p-1)!}\, dz, \quad k = 1, \dots, k_i, \quad i = 1, \dots, r, \\ \epsilon_{ki} &= e^{\beta_{ki}} \int_0^{\beta_{ki}} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z}}{(p-1)!}\, dz, \quad k = 1, \dots, k_i, \quad i = 1, \dots, r, \end{aligned}$$

donde los caminos de integración son los indicados en la figura siguiente:



La finitud de M_{ki} se debe a que, puesto que el integrando es una función entera, por el teorema de Cauchy sabemos que la integral a lo largo de una trayectoria como la de la figura siguiente es nula para todo R suficientemente grande:



Ahora bien, es fácil ver que la integral sobre el segmento vertical tiende a 0 con R, luego la integral que define M_{ki} es finita y al sumarle la integral que define a ϵ_{ki} da exactamente M_0. Así pues, $M_{ki} + \epsilon_{ki} = e^{\beta_{ki}} M_0$, y tenemos la descomposición buscada.

Si en la definición de M_{ki} descomponemos en factores el polinomio $f(z)$ obtenemos

$$M_{ki} = \int_{\beta_{ki}}^{+\infty} \frac{b_N^{Np-1} z^{p-1} \prod_{j=1}^{r} \prod_{t=1}^{k_j} (z-\beta_{tj})^p e^{-z+\beta_{ki}}}{(p-1)!}\, dz.$$

El camino de integración es $z = u + \beta_{ki}$, luego $dz = du$. Al hacer el cambio la integral se convierte en

$$M_{ki} = \int_0^{+\infty} \frac{b_N^{Np-1} (u+\beta_{ki})^{p-1} u^p e^{-u} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (u+\beta_{ki}-\beta_{tj})^p}{(p-1)!}\, du,$$

donde el asterisco en el producto indica que falta el factor $(t,j) = (k,i)$, que hemos extraído como u^p. Podemos redistribuir los coeficientes b^N:

$$M_{ki} = \int_0^{+\infty} \frac{(b_N u + b_N\beta_{ki})^{p-1} u^p e^{-u} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (b_N u + b_N\beta_{ki} - b_N\beta_{tj})^p}{(p-1)!}\, du.$$

Es fácil ver que, puesto que b_N es el coeficiente director de un polinomio cuyas raíces son los β_{ij}, los números $\alpha_{ij} = b_N\beta_{ij}$ son enteros algebraicos. Con esta notación:

$$M_{ki} = \int_0^{+\infty} \frac{(b_N u + \alpha_{ki})^{p-1} u^p e^{-u} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (b_N u + \alpha_{ki} - \alpha_{tj})^p}{(p-1)!}\, du.$$

Sumando obtenemos que

$$\sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki} = \int_0^{+\infty} \frac{u^p \Phi(u) e^{-u}}{(p-1)!}\, du,$$

donde

$$\Phi(u) = \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} (b_N u + \alpha_{ki})^{p-1} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (b_N u + \alpha_{ki} - \alpha_{tj})^p.$$

Si consideramos una extensión finita de Galois K de $\mathbb{Q}$ que contenga a todos los α_{ij}, resulta que un automorfismo de K permuta los números $\alpha_{1i}, \ldots, \alpha_{k_i i}$, y se ve claramente que entonces deja invariante a $\Phi(u)$. Esto significa que $\Phi(u) \in \mathbb{Q}[u]$, y como los α_{ij} son enteros, en realidad $\Phi(u) \in \mathbb{Z}[u]$. Digamos que

$$u^p \Phi(u) = \sum_{s=p+1}^{(N+1)p} d_{s-1} u^{s-1}.$$

Entonces

$$\sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki} = \sum_{s=p+1}^{(N+1)p} \frac{d_{s-1}}{(p-1)!} \int_0^{+\infty} u^{s-1} e^{-u}\, du = \sum_{s=p+1}^{(N+1)p} d_{s-1} \frac{(s-1)!}{(p-1)!} = pC,$$

para un $C \in \mathbb{Z}$. Sólo queda demostrar (14.2).

Sea R tal que todos los números β_{ij} estén contenidos en el disco de centro 0 y radio R. Llamemos

$$g_{ki} = \max_{|z|\leq R} |b_N^{N-2} f(z) e^{-z+\beta_{ki}}|, \quad g = \max_{|z|\leq R} |b_N^{N-1} z f(z)|,$$

y sea g_0 el máximo de todos los números g_{ki}. Entonces

$$\begin{aligned} |\epsilon_{ki}| &= \left| \int_0^{\beta_{ki}} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z+\beta_{ki}}}{(p-1)!}\, dz \right| \\ &\leq \frac{1}{(p-1)!} |\beta_{ki}|\, |b_N^{N-2} f(z) e^{-z+\beta_{ki}}|\, |b_N^{N-1} z f(z)|^{p-1} \leq g_0 R \frac{g^{p-1}}{(p-1)!}. \end{aligned}$$

Puesto que la última expresión tiende a 0 con p, eligiendo p suficientemente grande podemos garantizar que se cumple (14.2). ∎

Teorema 14.2 *Consideremos números* $\sum_{k=1}^{k_i} A_{ki} e^{\alpha_{ki}}$*, donde* $k_i \geq 1$*,* $i = 1, \ldots, r$*,* $r \geq 2$*,* $A_{ki} \in \mathbb{C} \setminus \{0\}$ *y* $\alpha_{1i}, \ldots, \alpha_{k_i i}$ *son números complejos distintos para cada* i*. Si operamos el producto*

$$\prod_{i=1}^{r} \sum_{k=1}^{k_i} A_{ki} e^{\alpha_{ki}} = \sum_{i=1}^{N} B_i e^{\beta_i},$$

donde $\beta_1, \ldots, \beta_N$ *son distintos dos a dos (es decir, los coeficientes* B_i *se obtienen multiplicando un* A_{ki} *para cada* i *y después sumando todos los productos que acompañan a un mismo exponente), se cumple que alguno de los coeficientes* B_i *es no nulo.*

Demostración: Ordenemos los números $\alpha_{1i}, \ldots, \alpha_{k_i i}$ según el crecimiento de sus partes reales y, en caso de igualdad, según el crecimiento de sus partes imaginarias. Entonces el número $\alpha_{11} + \cdots + \alpha_{1r}$ no puede alcanzarse mediante otra combinación $\alpha_{j_1 1} + \cdots + \alpha_{j_r r}$, pues la parte real de una cualquiera de estas sumas será mayor o igual que la de la primera, y en caso de igualdad la parte imaginaria será mayor. Consecuentemente existe un i de modo que $\beta_i = \alpha_{11} + \cdots + \alpha_{1r}$ y el coeficiente B_i será exactamente $A_{11} \cdots A_{1r} \neq 0$. ∎

Teorema 14.3 (Teorema de Lindemann-Weierstrass) *Si* $\alpha_1, \ldots, \alpha_n$ *son números algebraicos distintos (*$n \geq 2$*) y* $c_1, \ldots, c_n$ *son números algebraicos no todos nulos, entonces*

$$c_1 e^{\alpha_1} + \cdots + c_n e^{\alpha_n} \neq 0.$$

DEMOSTRACIÓN: Supongamos, por el contrario, que

$$c_1 e^{\alpha_1} + \cdots + c_n e^{\alpha_n} = 0. \tag{14.3}$$

Podemos suponer que todos los coeficientes c_i son no nulos. Multiplicando la ecuación por un número natural suficientemente grande podemos suponer que de hecho son enteros algebraicos. Veremos en primer lugar que podemos suponer también que son enteros racionales.

Sean $c_{i1}, \ldots, c_{ik_i}$ los conjugados de cada c_i. Entonces

$$\prod_{i_1=1}^{k_1} \cdots \prod_{i_n=1}^{k_n} (c_{1i_1} e^{\alpha_1} + \cdots + c_{ni_n} e^{\alpha_n}) = 0,$$

pues entre los factores se encuentra (14.3). Operemos el polinomio

$$\prod_{i_1=1}^{k_1} \cdots \prod_{i_n=1}^{k_n} (c_{1i_1} z_1 + \cdots + c_{ni_n} z_n) = \sum c_{h_1,\ldots,h_n} z_1^{h_1} \cdots z_n^{h_n},$$

donde el último sumatorio se extiende sobre todas las n-tuplas $(h_1, \ldots, h_n)$ de números naturales tales que $h_1 + \cdots + h_n = N = k_1 + \cdots + k_n$.

Si consideramos una extensión finita de Galois K de $\mathbb{Q}$ que contenga a todos los números c_{ij}, resulta que todo automorfismo de K permuta los números $c_{i1}, \ldots, c_{ik_i}$, luego deja invariante a este polinomio, lo que implica que sus coeficientes $c_{h_1,\ldots,h_n}$ son números racionales. Como además son enteros, tenemos que $c_{h_1,\ldots,h_n} \in \mathbb{Z}$.

Sustituimos $z_i = e^{\alpha_i}$ y nos queda

$$\prod_{i_1=1}^{k_1} \cdots \prod_{i_n=1}^{k_n} (c_{1i_1} e^{\alpha_1} + \cdots + c_{ni_n} e^{\alpha_n}) = \sum c_{h_1,\ldots,h_n} e^{h_1\alpha_1+\cdots+h_n\alpha_n} = \sum_{i=1}^{M} b_i e^{\beta_i},$$

donde los coeficientes b_i son enteros racionales obtenidos sumando los $c_{h_1,\ldots,h_n}$ que acompañan a un mismo exponente, es decir, según las hipótesis del teorema anterior, por lo que alguno de ellos es no nulo (y claramente ha de haber al menos dos no nulos). Los números b_i son números algebraicos distintos, luego tenemos una expresión como la original pero con coeficientes enteros.

A partir de ahora suponemos (14.3) con $c_i \in Z$ y donde $\alpha_1, \ldots, \alpha_n$ son números algebraicos distintos.

Sea $f(x) \in \mathbb{Q}[x]$ el producto de los polinomios mínimos de los números α_i (sin repetir dos veces el mismo factor). Sea $m \geq n$ el grado de f, sean $\gamma_1, \ldots, \gamma_m$ todas las raíces de f. Llamemos $\mu = m(m-1)\ldots(m-n+1)$, al número de n-tuplas posibles $(i_1, \ldots, i_n)$ de números distintos comprendidos entre 1 y m. Entonces

$$\prod (c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) = 0,$$

donde el producto recorre las μ citadas n-tuplas. El producto es 0 porque entre sus factores se encuentra (14.3).

Consideremos el polinomio

$$\prod(c_1 z_{i_1} + \cdots + c_n z_{i_n}) = \sum B_{h_1,\ldots,h_m} z_1^{h_1} \cdots z_m^{h_m},$$

donde la suma se extiende sobre las m-tuplas $(h_1, \ldots, h_m)$ de números naturales que suman μ y los coeficientes $B_{h_1,\ldots,h_m}$ son enteros racionales.

La expresión de la izquierda es claramente invariante por permutaciones de las indeterminadas $z_1, \ldots, z_m$, luego los coeficientes $B_{h_1,\ldots,h_m}$ son invariantes por permutaciones de $h_1, \ldots, h_m$. Consecuentemente podemos agrupar así los sumandos:

$$\prod(c_1 z_{i_1} + \cdots + c_n z_{i_n}) = \sum_{k=1}^{r} B_k \sum z_{k_1}^{h_{k1}} \ldots z_{k_m}^{h_{km}},$$

donde r es el número de elementos de un conjunto de m-tuplas $(h_{k1}, \ldots, h_{km})$ de números naturales que suman μ sin que haya dos que se diferencien sólo en el orden, y el segundo sumatorio varía en un conjunto P_k de permutaciones $(k_1, \ldots, k_m)$ de $(1, \ldots, m)$ que dan lugar, sin repeticiones, a todos los monomios posibles $z_{k_1}^{h_{k1}} \ldots z_{k_m}^{h_{km}}$. Sustituimos las indeterminadas por exponenciales y queda

$$\prod(c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) = \sum_{k=1}^{r} B_k \sum e^{h_{k1}\gamma_{k_1} + \cdots + h_{km}\gamma_{k_m}} = 0.$$

La definición del conjunto P_k hace que el polinomio

$$\prod\big(x - (h_{k1} z_{k_1} + \cdots + h_{km} z_{k_m})\big)$$

sea invariante por permutaciones de $z_1, \ldots, z_m$, luego

$$F_k(x) = \prod\big(x - (h_{k1}\gamma_{k_1} + \cdots + h_{km}\gamma_{k_m})\big) \in \mathbb{Q}[x].$$

Si llamamos $\gamma_{1k}, \ldots, \gamma_{t_k k}$ a las raíces de $F_k(x)$ (repetidas con su multiplicidad), nuestra ecuación puede escribirse como

$$\prod(c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) = \sum_{k=1}^{r} B_k (e^{\gamma_{1k}} + \cdots + e^{\gamma_{t_k k}}) = 0.$$

Sean $s_i(x) \in \mathbb{Q}[x]$, $i = 1, \ldots, q$ los distintos factores mónicos irreducibles de los polinomios $F_k(x)$. Así cada $F_k(x)$ se expresa como

$$F_k(x) = \prod_{i=1}^{q} s_i^{p_{ik}}(x),$$

para ciertos números naturales p_{ik}.

Sean $\beta_{1i}, \ldots, \beta_{t_i i}$ las raíces de $s_i(x)$ (todas son simples, porque el polinomio es irreducible). Entonces el polinomio $F_k(x)$ tiene p_{ik} veces cada raíz β_{ji}, luego

$$B_k(e^{\gamma_{1k}} + \cdots + e^{\gamma_{t_k k}}) = \sum_{i=1}^{q} p_{ik} B_k (e^{\beta_{1i}} + \cdots + e^{\beta_{t_i i}}).$$

Sumando resulta

$$\begin{aligned}\prod(c_1e^{\gamma_{i_1}}+\cdots+c_ne^{\gamma_{i_n}}) &= \sum_{k=1}^{r} B_k(e^{\gamma_{1k}}+\cdots+e^{\gamma_{t_kk}})\\ &= \sum_{i=1}^{q} A_i(e^{\beta_{1i}}+\cdots+e^{\beta_{t_ii}})=0,\end{aligned}$$

donde

$$A_i=\sum_{k=1}^{r} p_{ik}B_k\in\mathbb{Z}.$$

Notemos que todos los números β_{ij} son distintos, pues son raíces de polinomios irreducibles distintos. Por construcción, los exponentes β_{ij} son todas las sumas distintas de exponentes γ_{ij} que aparecen al efectuar el producto de la izquierda de la ecuación. Podemos aplicar el teorema anterior y concluir que alguno de los coeficientes A_i es no nulo. Eliminando los nulos podemos suponer que ninguno lo es. En resumen tenemos

$$\sum_{i=1}^{q} A_i(e^{\beta_{1i}}+\cdots+e^{\beta_{t_ii}})=0,$$

donde los coeficientes son enteros racionales no nulos y los exponentes de cada sumando son familias de números conjugados correspondientes a polinomios irreducibles distintos $s_i(x)$ de grado t_i. Distinguimos dos casos:

1) Algún $\beta_{ki}=0$. Pongamos por ejemplo $i=1$. Esto significa que $s_1(x)=x$, luego además $t_1=1$ y la ecuación se reduce a

$$A_1+\sum_{i=2}^{q} A_i(e^{\beta_{1i}}+\cdots+e^{\beta_{t_ii}})=0,$$

donde los exponentes son todos no nulos, y esto contradice al teorema 14.1.

2) Todos los β_{ki} son distintos de 0. Dividimos la ecuación entre $e^{\beta_{k1}}$ para $k=1,\ldots,t_1$, con lo que obtenemos las ecuaciones

$$\sum_{i=1}^{q} A_i\sum_{t=1}^{t_i} e^{\beta_{ti}-\beta_{k1}}=0,\quad k=1,\ldots,t_1.$$

Las sumamos y queda

$$\sum_{i=1}^{q} A_i\sum_{k=1}^{t_1}\sum_{t=1}^{t_i} e^{\beta_{ti}-\beta_{k1}}=0.$$

En el sumando $i=1$, los sumandos con $k=t$ valen todos 1. Los separamos:

$$t_1A_1+A_1\sum_{k\neq t} e^{\beta_{ti}-\beta_{k1}}+\sum_{i=2}^{q} A_i\sum_{k=1}^{t_1}\sum_{t=1}^{t_i} e^{\beta_{ti}-\beta_{k1}}=0,$$

donde en el primer sumatorio k y t varían entre 1 y t_1.

El polinomio

$$g_1(x) = \prod_{k\neq t}\big(x - (\beta_{t1} - \beta_{k1})\big)$$

es invariante por permutaciones de los conjugados β_{k1}, luego sus coeficientes son racionales. Igualmente ocurre con los polinomios

$$g_i(x) = \prod_{k=1}^{t_1}\prod_{t=1}^{t_i}\big(x - (\beta_{ti} - \beta_{k1})\big)$$

para $i = 2, \ldots, q$. Además todos tienen las raíces no nulas.

Llamando $A_0 = t_1A_1 \neq 0$, $k_1 = t_1(t_1 - 1)$, $k_i = t_1t_i$ para $i = 2, \ldots, q$ y $\alpha_{1i}, \ldots, \alpha_{k_ii}$ a las raíces de $g_i(x)$, la ecuación se convierte en

$$A_0 + \sum_{i=1}^{q} A_i \sum_{k=1}^{k_i} e^{\alpha_{ki}} = 0,$$

que contradice al teorema 14.1. ∎

Ejercicio: Probar que si $\alpha_1, \ldots, \alpha_n$ son números algebraicos linealmente independientes sobre $\mathbb{Q}$ entonces $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son algebraicamente independientes sobre $\mathbb{Q}$, es decir, no son raíces de ningún polinomio $P(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ no nulo.

Algunas consecuencias inmediatas son las siguientes:

1. *Si $\alpha \neq 0$ es un número algebraico, entonces e^α es un número trascendente. En particular el número e es trascendente.*

   En efecto, si $c = e^\alpha$ fuera algebraico, tendríamos $e^\alpha - ce^0 = 0$, en contradicción con el teorema de Lindemann-Weierstrass.

2. *El número π es trascendente.*

   Si π fuera algebraico también lo sería $i\pi$, y el número $e^{i\pi} = -1$ sería trascendente.

3. *Si $\alpha \neq 1$ es un número algebraico, entonces $\log\alpha$ es trascendente.*

   Si $\beta = \log\alpha \neq 0$ fuera algebraico, entonces $\alpha = e^\beta$ sería trascendente.

4. *Si $\alpha \neq 0$ es un número algebraico, entonces $\operatorname{sen}\alpha$, $\cos\alpha$, $\tan\alpha$ son números trascendentes.*

   Si $\beta = \operatorname{sen}\alpha = (e^{i\alpha} - e^{-i\alpha})/2i$ fuera algebraico, entonces

   $$e^{i\alpha} - e^{-i\alpha} - 2i\beta e^0 = 0,$$

   en contradicción con el teorema de Lindemann-Weierstrass. Igualmente con el coseno.

   Si $\beta = \tan\alpha = (e^{i\alpha} - e^{-i\alpha})/(e^{i\alpha} + e^{-i\alpha})$ fuera algebraico, entonces

   $$(\beta - 1)e^{i\alpha} + (\beta + 1)e^{-i\alpha} = 0,$$

   en contradicción con el teorema de Lindemann-Weierstrass.

Ejercicio: Probar que las funciones arcsen, arccos y arctan toman valores trascendentes sobre números algebraicos (salvo casos triviales).

14.2 El teorema de Gelfond-Schneider

Entre los famosos problemas planteados por Hilbert a principios de siglo, el séptimo consistía en determinar el carácter algebraico o trascendente de ciertos números concretos, tales como la constante de Euler. Entre otras cosas Hilbert preguntaba si en general α^β es un número trascendente cuando α y β son números algebraicos, $\alpha \neq 0$, 1 y β es irracional (en los casos exceptuados α^β es obviamente algebraico). Por α^β se entiende $e^{\beta \log \alpha}$, donde $\log \alpha$ es *cualquier* logaritmo complejo de α. Esta parte del séptimo problema fue demostrada independientemente por Gelfond y Schneider en 1934. De este hecho se sigue en particular que los números $2^{\sqrt{2}}$ o $e^\pi = (-1)^{-i}$ son trascendentes.

Sea K un cuerpo numérico de grado h y $\beta_1, \ldots, \beta_h$ una base entera de K. Si $\alpha \in K$ llamaremos $\alpha^{(i)}$, para $i = 1, \ldots, h$, a los conjugados de α en un cierto orden. Llamaremos $\overline{|\alpha|} = \max\limits_{1\le i\le h} |\alpha^{(i)}|$.

Si $\gamma_1, \ldots, \gamma_h$ es la base dual de $\beta_1, \ldots, \beta_h$ entonces, todo entero α de K se expresa en forma única como $\alpha = a_1\beta_1 + \cdots + a_h\beta_h$, para ciertos enteros racionales a_i tales que

$$|a_i| = |\operatorname{Tr}(\alpha\gamma_i)| = |\alpha^{(1)}\gamma_i^{(1)} + \cdots + \alpha^{(h)}\gamma_i^{(h)}| \le \max_{1\le i\le h} |\gamma^{(i)}|\,\overline{|\alpha|}.$$

Así pues, existe una constante c que depende sólo de K y de la base $\beta_1, \ldots, \beta_h$ tal que para todo entero $\alpha \in K$ se cumple

$$\alpha = a_1\beta_1 + \cdots + a_h\beta_h \quad \text{con } |a_i| \le c,\ i = 1, \ldots, h.$$

Probamos dos teoremas previos:

Teorema 14.4 *Sea (a_{jk}) una matriz $M \times N$ con coeficientes enteros racionales tal que $M < N$ y de modo que todos los coeficientes estén acotados por $A \ge 1$. Entonces el sistema de ecuaciones lineales*

$$a_{j1}x_1 + \cdots + a_{jN}x_N = 0, \quad 1 \le j \le M,$$

tiene una solución entera no trivial tal que $|x_k| \le E\big((NA)^{M/(N-M)}\big)$, para $1 \le k \le N$ (donde E denota la parte entera).

Demostración: Para cada N-tupla de enteros racionales $(x_1, \ldots, x_N)$ consideremos la M-tupla de enteros racionales $(y_1, \ldots, y_M)$ dada por

$$y_j = a_{j1}x_1 + \cdots + a_{jN}x_N, \quad 1 \le j \le M.$$

Sea $H = E\big((NA)^{M/(N-M)}\big)$. De este modo, $(NA)^{M/(N-M)} < H + 1$, luego $NA < (H+1)^{(N-M)/M}$, $NAH + 1 \le NA(H+1) < (H+1)^{N/M}$, luego tenemos que $(NAH + 1)^M < (H + 1)^N$.

Sea $(x_1, \ldots, x_N)$ tal que $0 \le x_k \le H$ para $1 \le k \le N$. Sea $-B_j$ la suma de los a_{jk} negativos y C_j la suma de los a_{jk} positivos. Entonces

$$B_j + C_j = |a_{j1}| + \cdots + |a_{jN}| \le NA,$$

y claramente $-B_j H \le y_j \le C_j H$.

Ahora bien, el número de N-tuplas $(x_1, \ldots, x_N)$ tales que $0 \le x_k \le H$ es $(H+1)N$, mientras que sus M-tuplas asociadas $(y_1, \ldots, y_M)$ varían en un conjunto de a lo sumo $(C_j H + B_j H + 1)M \le (NAH + 1)^M$ elementos. Como $(NAH+1)^M < (H+1)^N$, ha de haber dos N-tuplas distintas con la misma imagen. Su diferencia cumple el teorema. ∎

Teorema 14.5 *Sea (α_{kl}) una matriz $p \times q$ con coeficientes enteros en K tal que $p < q$ y de modo que $\overline{|\alpha_{kl}|} \le A$. Entonces el sistema de ecuaciones lineales*

$$\alpha_{k1}\xi_1 + \cdots + \alpha_{kq}\xi_q = 0, \quad 1 \le k \le p,$$

tiene una solución entera (en K) no trivial tal que $\overline{|\xi_l|} \le c(1 + (cqA)^{p/(q-p)})$, para $1 \le l \le q$, donde c es una constante que depende de K y de la base $\beta_1, \ldots, \beta_h$, pero no de la matriz.

DEMOSTRACIÓN: : Para cualquier q-tupla $(x_1, \ldots, x_q)$ de enteros de K consideremos sus coordenadas

$$\xi_l = x_{l1}\beta_1 + \cdots + x_{lh}\beta_h, \quad 1 \le l \le q,$$

donde $x_{l1}, \ldots, x_{lh}$ son enteros racionales. Así mismo sea

$$\alpha_{kl}\beta_r = a_{klr1}\beta_1 + \cdots + a_{klrh}\beta_h, \quad 1 \le k \le p,\ 1 \le l \le q,\ 1 \le r \le h.$$

Entonces

$$\begin{aligned}\sum_{l=1}^{q} \alpha_{kl}\xi_l &= \sum_{l=1}^{q} \alpha_{kl} \sum_{r=1}^{h} x_{lr}\beta_r = \sum_{r=1}^{h}\sum_{l=1}^{q} x_{lr} \sum_{u=1}^{h} a_{klru}\beta_u \\ &= \sum_{u=1}^{h}\left(\sum_{r=1}^{h}\sum_{l=1}^{q} a_{klru}x_{lr}\right)\beta_u,\end{aligned}$$

luego $(\xi_1, \ldots, \xi_q)$ será solución del sistema de ecuaciones si y sólo si las coordenadas $(x_{l1}, \ldots, x_{lh})$ son solución del sistema de $M = hp$ ecuaciones con $N = hq$ incógnitas

$$\sum_{r=1}^{h}\sum_{l=1}^{q} a_{klru}x_{lr} = 0, \quad 1 \le u \le h, \ \ 1 \le k \le p.$$

Según hemos observado al comienzo de la sección, existe una constante c' tal que

$$|a_{klru}| \le c' \overline{|\alpha_{kl}\beta_r|} \le c' \max_{1 \le i \le h} \overline{|\beta_i|} A = c'' A.$$

Por el teorema anterior este sistema de ecuaciones tiene una solución entera no trivial tal que

$$|x_{lr}| \le E\big((hqc''A)^{p/(q-p)}\big) \le 1 + (hqc''A)^{p/(q-p)}, \quad 1 \le l \le q, \;\; 1 \le r \le h.$$

Los $(\xi_1, \dots, \xi_q)$ con estas coordenadas son enteros de K no todos nulos que cumplen el sistema de ecuaciones y además

$$\begin{aligned} \overline{|\xi_l|} &\le |x_{l1}|\,\overline{|\beta_1|} + \cdots + |x_{lh}|\,\overline{|\beta_h|} \le \max_{1\le i\le h} \overline{|\beta_i|}(|x_{l1}| + \cdots + |x_{lh}|) \\ &\le hc''(1 + (hqc''A)^{p/(q-p)}) = c(1 + (cqA)^{p/(q-p)}). \end{aligned}$$

■

Teorema 14.6 (Gelfond-Schneider) *Si α y β son números algebraicos tales que $\alpha \ne 0$, 1 y β es irracional, entonces el número α^β es trascendente.*

Demostración: Fijemos un valor para $\log\alpha$ y supongamos que $\gamma = e^{\beta\log\alpha}$ es algebraico. Sea K un cuerpo numérico de grado h que contenga a α, β y γ. Sean $m = 2h+2$ y $n = q^2/(2m)$, donde $t = q^2$ es un múltiplo de $2m$.

Observar que podemos tomar valores para n arbitrariamente grandes en estas condiciones. En lo sucesivo las letras c, c_1, c_2, ... representarán constantes que dependerán de K, de una base entera de K prefijada y de α, β, γ, pero nunca de n.

Sean $\rho_1, \dots, \rho_t$ los números $(a+b\beta)\log\alpha$, con $1 \le a \le q$, $1 \le b \le q$. Observar que como β es irracional, los números 1 y β son linealmente independientes, luego los números $\rho_1, \dots, \rho_t$ son distintos dos a dos.

Sean $\eta_1, \dots, \eta_t$ números complejos en K arbitrarios. Consideremos la función holomorfa en $\mathbb{C}$ dada por $R(z) = \eta_1 e^{\rho_1 z} + \cdots + \eta_t e^{\rho_t z}$. Consideremos las mn ecuaciones lineales con $t = 2mn$ incógnitas $(\eta_1, \dots, \eta_t)$

$$(\log\alpha)^{-k} R^{k)}(l) = 0, \quad 0 \le k \le n-1, \;\; 1 \le l \le m.$$

Los coeficientes de la ecuación (k,l) son los números

$$(\log\alpha)^{-k}\rho_i^k e^{\rho_i l} = (\log\alpha)^{-k}\big((a+b\beta)\log\alpha\big)^k e^{l(a+b\beta)\log\alpha} = (a+b\beta)^k \alpha^{al}\gamma^{bl} \in K,$$

con $1 \le l \le m$, $1 \le a, b \le q$, $0 \le k \le n-1$.

Sea c_1 un número natural no nulo tal que $c_1\alpha$, $c_1\beta$ y $c_1\gamma$ sean enteros en K. En cada coeficiente, al desarrollar el binomio $(a+b\beta)^k$ aparecen monomios de α, β y γ con grado a lo sumo

$$k + al + bl \le n - 1 + mq + mq \le n + 4m^2 n = (4m^2+1)n,$$

luego si multiplicamos cualquiera de los coeficientes por $c_1^{4(m^2+1)n} = c_2^n$ obtenemos un entero de K.

El módulo de los conjugados de los coeficientes multiplicados por c_2^n es a lo sumo

$$|c_2^n(a+b\beta^{(i)})^k(\alpha^{(i)})^{al}(\gamma^{(i)})^{bl}| \le c_2^n(a+b\overline{|\beta|})^k\,\overline{|\alpha|}^{al}\,\overline{|\gamma|}^{bl}$$

$$\le c_2^n(q+q\overline{|\beta|})^{n-1}\,\overline{|\alpha|}^{mq}\,\overline{|\gamma|}^{mq} \le c_2^n\big(\sqrt{2m}\sqrt{n}+\sqrt{2m}\sqrt{n}\,\overline{|\beta|}\big)^{n-1}\overline{|\alpha|}^{2m^2n}\,\overline{|\gamma|}^{2m^2n}$$

$$\le c_2^n\big(\sqrt{2m}+\sqrt{2m}\,\overline{|\beta|}\big)^n\overline{|\alpha|}^{2m^2n}\,\overline{|\gamma|}^{2m^2n}\sqrt{n}^{\,n-1} = c_3^n\,n^{(n-1)/2}.$$

Podemos aplicar el teorema anterior, que nos garantiza que $\eta_1,\dots,\eta_t$ pueden elegirse de modo que sean enteros en K, no todos nulos, satisfagan las $2t$ ecuaciones (multiplicadas o no por c_2^n, da igual) y además

$$\begin{aligned}\overline{|\eta_k|} &\le c\big(1+(c\,2t\,c_3^n\,n^{(n-1)/2})\big) \le 4ct\,c_3^n\,n^{(n-1)/2}\\ &\le 8m\,c\,n\,c_3^n\,n^{(n-1)/2} \le c_4^n\,n^{(n+1)/2},\end{aligned} \tag{14.4}$$

para $1\le k\le t$.

A partir de ahora consideramos la función $R(z)$ para estos $\eta_1,\dots,\eta_t$. En primer lugar, $R(z)$ no puede ser idénticamente nula, pues desarrollándola en serie de Taylor en el origen resultaría entonces que

$$\eta_1\rho_1^k+\cdots+\eta_t\rho_t^k=0, \quad \text{para } k=0,1,2,3,\dots$$

pero las t primeras ecuaciones son un sistema de ecuaciones lineales en $\eta_1,\dots,\eta_t$ cuyo determinante es de Vandermonde, luego es no nulo, puesto que $\rho_1,\dots,\rho_t$ son distintos dos a dos. Esto implica que $\eta_1=\cdots=\eta_t=0$, lo cual es falso.

En resumen tenemos que la función entera $R(z)$ es no nula pero tiene sus $n-1$ primeras derivadas nulas en los puntos $l=1,\dots,m$.

Existe, pues, un natural $r\ge n$ tal que $R^{k)}(l)=0$ para $0\le k\le r-1$, $1\le l\le m$ y $R^{r)}(l_0)\ne 0$ para un cierto l_0 tal que $1\le l_0\le m$.

Llamemos $\rho=(\log\alpha)^{-r}R^{r)}(l_0)\ne 0$. El mismo análisis que hemos realizado antes sobre los coeficientes del sistema nos da ahora que $\rho\in K$ y que $c_1^{r+2mq}\rho$ es un entero en K.

Así pues, $1\le|\,\mathrm{N}(c_1^{r+2mq}\rho)|=|\,\mathrm{N}(\rho)|$, luego

$$|\,\mathrm{N}(\rho)|\ge c_1^{-h(r+2mq)}>c_5^{-r}. \tag{14.5}$$

Por otro lado tenemos que ρ es una suma de t términos, cada uno de los cuales es el producto de un η_k, para el que tenemos la cota (14.4), y de un coeficiente de la forma $(a+b\beta)^r\alpha^{al_0}\gamma^{bl_0}$, cuyos conjugados están acotados por

$$(a+b\overline{|\beta|})^r\,\overline{|\alpha|}^{al_0}\,\overline{|\gamma|}bl_0 \le (q+q\overline{|\beta|})^r\,\overline{|\alpha|}^{mq}\,\overline{|\gamma|}^{mq} \le (c_6q)^rc_7^q.$$

Consecuentemente $\overline{|\rho|}\le t\,c_4^n\,n^{(n+1)/2}(c_6q)^rc_7^q$.

Ahora acotamos $t=q^2=2mn\le 2mr$, $n\le r$, $q\le\sqrt{2m}\sqrt{n}\le\sqrt{2m}\,r^{1/2}$ y llegamos a

$$\overline{|\rho|}\le 2mr\,c_4^r\,r^{(r+1)/2}\,c_6^r\big(\sqrt{2m}\big)^r r^{r/2}c_7^{2mr}\le c_8^r\,r^{r+3/2}. \tag{14.6}$$

Vamos a obtener una cota más fina para $|\rho|$. Para ello aplicaremos la fórmula integral de Cauchy a la función

$$S(z) = r!\frac{R(z)}{(z-l_0)^r}\prod_{\substack{k=1\\k\neq l_0}}^{m}\left(\frac{l_0-k}{z-k}\right)^r.$$

Puesto que las derivadas anteriores al orden r son nulas en $1,\ldots,m$, la función S es entera. Además

$$\rho = (\log\alpha)^{-r}R^{r)}(l_0) = (\log\alpha)^{-r}S(l_0) = (\log\alpha)^{-r}\frac{1}{2\pi i}\int_C \frac{S(z)}{z-l_0}\,dz,$$

donde C es la circunferencia $|z| = m(1+r/q)$, que contiene a los números $1,\ldots,m$, en particular a l_0. Para los puntos $z\in C$ tenemos las cotas

$$\begin{aligned}
|R(z)| &\leq t\,c_4^n\,n^{(n+1)/2}\exp\big((q+q|\beta|)\,|\log\alpha|\,m(1+r/q)\big)\\
&\leq t\,c_4^n\,n^{(n+1)/2}\,c_9^{r+q} \leq c_{10}^r\,r^{(r+3)/2},\\
|z-k| &\geq |z|-|k| \geq m(1+r/q)-m = mr/q, \quad \text{para } k=1,\ldots,m,
\end{aligned}$$

$$\left|(z-l_0)^{-r}\prod_{\substack{k=1\\k\neq l_0}}^{m}\left(\frac{l_0-k}{z-k}\right)^r\right| \leq \left(\frac{q}{mr}\right)^r\prod_{\substack{k=1\\k\neq l_0}}^{m} m^r\left(\frac{q}{mr}\right)^r = c_{11}\left(\frac{q}{r}\right)^{mr},$$

$$\begin{aligned}
|S(x)| &\leq r!\,c_{10}^r\,r^{(r+3)/2}\,c_{11}^r\left(\frac{q}{r}\right)^{mr}\\
&\leq r^r c_{10}^r\,r^{(r+3)/2}c_{11}^r\big(\sqrt{2m}\big)^{mr}r^{-mr/2} = c_{12}^r\,r^{(3r+3-mr)/2}.
\end{aligned}$$

Acotando la integral llegamos a que

$$\begin{aligned}
|\rho| &\leq \frac{1}{2\pi}|(\log\alpha)^{-r}|2\pi\left(1+\frac{r}{q}\right)c_{12}^r\,r^{(3r+3-mr)/2}\left(\frac{q}{mr}\right)\\
&= |\log\alpha|^{-r}\left(\frac{q}{mr}+\frac{1}{m}\right)c_{12}^r\,r^{(3r+3-mr)/2}\\
&\leq |\log\alpha|^{-r}(q+1)^r c_{12}^r\,r^{(3r+3-mr)/2} = c_{13}^r\,r^{(3r+3-mr)/2}.
\end{aligned}$$

Ahora vamos a acotar $|\,\mathrm{N}(\rho)|$, que es el producto de los módulos de los conjugados de ρ, usando la cota anterior para $|\rho|$ y la cota (14.6) para los $h-1$ conjugados restantes. Concretamente

$$|\,\mathrm{N}(\rho)| \leq c_{13}^r r^{(3r+3-mr)/2}(c_8^r r^{r+3/2})^{h-1} = c_{14}^r\,r^{(3r+3-mr)/2+(h-1)(r+3/2)}.$$

Si sustituimos $m = 2h+2$ la expresión se simplifica hasta

$$|\,\mathrm{N}(\rho)| \leq r^{(3h-r)/2}.$$

Pero combinando esto con (14.5) resulta $c_5^{-r} < c_{14}^r\, r^{(3h-r)/2}$, o lo que es lo mismo, $r^{(r-3h)/2} < c_{14}^r\, c_5^r = c_{15}^r$. Tomando logaritmos es fácil llegar a que

$$\left(\frac{1}{2} - \frac{3h}{2r}\right) \log r < \log c_{15}.$$

Hemos probado que esto se cumple para una constante c_{15} y para valores de r arbitrariamente grandes (pues $r \geq n$), pero esto es claramente contradictorio, pues el miembro de la izquierda tiende a $+\infty$ cuando r tiende a $+\infty$. ∎

Bibliografía

[1] Baker, A. *Breve introducción a la teoría de números.* Alianza Ed., Madrid, 1986.

[2] Bastida, J.R. *Field extensions and Galois theory.* Addison-Wesley P.C., California, 1984.

[3] Borevich, Z.I., Shafarevich, I.R. *Number Theory.* Academic Press, New York, 1967.

[4] Cohn, H. *Advanced Number Theory* Dover, New York, 1962

[5] Cohn, H. *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer, New York, 1978.

[6] Edwards, H. M. *Fermat's last theorem.* Springer, New York, 1977.

[7] Hua, L.K. *Introduction to Number Theory.* Springer, Berlin, 1982.

[8] Hungerford, T.W. *Algebra.* Springer, New York, 1974.

[9] Ireland, K. y Rosen, M. *A Classical Introduction to Modern Number Theory.* Springer, New York 1982.

[10] Perron, O. *Die Lehre von den Kettenbrüchen.* Teubner, Stuttgart, 1954

[11] Phost y Zassenhauss *Algorithmic Algebraic Number Theory.* Cambridge University Press, 1989.

[12] Serre, J. P. *A Course in Arithmetic.* Springer, New York, 1973.

[13] Shidlovski, A.B. *Aproximaciones diofánticas y números trascendentes.* Servicio editorial Universidad del País Vasco (1989).

[14] Stewart, I. y Tall, D. *Algebraic number theory.* Chapman and Hall, Londres, 1979.

Índice de Tablas

Índice de Materias