Teoría de Números

Miguel Martínez González, Saúl Rodríguez Martín

Apuntes basados en las clases de Juan Ramón Delgado Pérez de la asignatura Teoría de Números del grado en Matemáticas de la Universidad Complutense de Madrid.

Agradecimientos a Ignacio Caamaño por señalar numerosas erratas.

Índice

Capítulo 1

Reciprocidad Cuadrática

1.1 Cuerpos finitos

1.1.1 Característica de un cuerpo. $(x+y)^p = x^p + y^p$

Sea $\mathbb{F}$ un cuerpo finito. Llamamos *característica* de $\mathbb{F}$, $\chi(\mathbb{F})$, al mínimo número natural tal que $n \cdot 1_{\mathbb{F}} := 1_{\mathbb{F}} + \overset{n}{\ldots} + 1_{\mathbb{F}} = 0$. Si tal número no existe decimos que $\chi(\mathbb{F}) = 0$, y si existe será un número primo, ya que si fuera un número compuesto $n = n_1 n_2$, con $n_1, n_2 > 1$, entonces $(n_1 1_{\mathbb{F}})(n_2 1_{\mathbb{F}}) = (n_1 n_2)1_{\mathbb{F}} = 0$, por tanto o bien $n_1 1 = 0$ o $n_2 1 = 0$, contradiciendo que $n = \chi(\mathbb{F})$.

Ahora, si $\mathbb{F}$ tiene característica prima p, entonces se cumplirá la igualdad $(a+b)^p = a^p + b^p$. Esto pasa porque, desarrollando el binomio de Newton, y usando que $\binom{p}{i}$ es múltiplo de p si $1 \leq i \leq p-1$, tenemos que:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

También se cumplirá para cada n que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Podemos probar esto por inducción: ya hemos visto que el caso $n = 1$ se cumple, y si se cumple para $n-1$, tenemos que $(a+b)^{p^n} = \left((a+b)^{p^{n-1}}\right)^p = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = (a^{p^{n-1}})^p + (b^{p^{n-1}})^p = a^{p^n} + b^{p^n}$.

1.1.2 Clasificación de cuerpos finitos

El cuerpo $\mathbb{F} = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, tiene p elementos, $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$, y tiene característica p. De hecho, bajo isomorfismo será el único cuerpo con p elementos: Dado otro cuerpo de p elementos, $\mathbb{F}_p$, el subgrupo aditivo generado por 1 en $\mathbb{F}_p$ tiene que tener p elementos, por tanto es todo $\mathbb{F}_p$, y podemos definir el isomorfismo $\mathbb{F}_p \to \mathbb{Z}_p; a1_{\mathbb{F}} \mapsto \overline{a}$.

Sea ahora $\mathbb{F}$ un cuerpo finito cualquiera, con $p = \chi(\mathbb{F})$. Llamamos $P = \{0, 1_{\mathbb{F}}, \ldots, (p-1)1_{\mathbb{F}}\}$. Entonces P es un subcuerpo de $\mathbb{F}$. Esto pasa porque $1_{\mathbb{F}} \in P$ y P es un cuerpo, ya que la función $f : \mathbb{Z} \to \mathbb{F}; a \to a1_{\mathbb{F}}$ cumple $\ker(f) = p\mathbb{Z}$, y por tanto induce un isomorfismo de $\mathbb{Z}_p$ en P. Al ser P subcuerpo de $\mathbb{F}$, podemos considerar $\mathbb{F}$ como un espacio vectorial sobre P. Como $\mathbb{F}$ tiene finitos elementos, tendrá dimensión finita n sobre P, por tanto $\mathbb{F}$ tiene p^n elementos. Con esto hemos deducido que todo cuerpo finito tendrá p^n elementos, para cierto p primo y n entero positivo (n no puede ser 0 ya que todo cuerpo tiene al menos dos elementos distintos, 0 y 1).

De hecho, para cada p primo y $n \geq 1$ podemos encontrar un cuerpo de p^n elementos. Para ello consideramos el polinomio $x^{p^n} - x \in \mathbb{F}_p$. Sea ahora F un cuerpo de descomposición de $x^{p^n} - x$, y consideramos el conjunto A de raíces de F. Entonces 1_F y -1_F están en A (el caso -1_F se puede comprobar por separado si $p = 2$ y si p es impar), y si $x, y \in A$, $x^{p^n} = x$ e $y^{p^n} = y$, tenemos que $x+y, xy$ y $\frac{1}{x} \in A$, ya que $(x+y)^{p^n} = x^{p^n} + y^{p^n} = x+y$, $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$, y $\left(\frac{1}{x}\right)^{p^n} = \frac{1}{x^{p^n}} = \frac{1}{x}$. Por tanto A es un subcuerpo de $\mathbb{F}$ que contiene a $\mathbb{F}_p$, y de hecho tiene p^n elementos distintos. Para comprobar esto, es decir, que $q(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ tiene p^n raíces distintas,

basta comprobar que $q(x)$ y su derivada no tienen factores comunes. Su derivada es $q'(x) = p^n x^{p^n-1} - 1 = -1$, por tanto no comparte factores con $q(x)$. Así que A es un cuerpo de p^n elementos, como queríamos.

Además, dado un cuerpo $\mathbb{F}$ de p^n elementos, su grupo multiplicativo tiene $p^n - 1$ elementos, por tanto todo $x \in \mathbb{F}$ cumple que $x^{p^n-1} = 1$, y por tanto $x^{p^n} = x$. Es decir, todos los elementos de $\mathbb{F}$ son raíces del polinomio $x^{p^n} - x$. De aquí se puede deducir que todo par de cuerpos $\mathbb{F}$ y $\mathbb{F}'$ de p^n elementos son isomorfos, ya que ambos son cuerpos de descomposición del polinomio $x^{p^n} - x$ sobre sus subcuerpos de p elementos formados por los múltiplos de $1_{\mathbb{F}}$ y $1_{\mathbb{F}'}$ respectivamente. Resumiendo la anterior discusión:

Teorema 1.1. Si $\mathbb{F}$ es un cuerpo finito, entonces $\mathbb{F}$ tiene p^n elementos, para ciertos p primo y $n \geq 1$. De hecho, dados p, n fijos, hay un único cuerpo $\mathbb{F}_{p^n}$ de p^n elementos bajo isomorfismo, y sus elementos son todos raíces de $x^{p^n} - x$.

1.1.3 Automorfismo de Frobenius

Ahora, en un cuerpo $\mathbb{F}$ de p^n elementos consideramos la función $\phi_p : \mathbb{F} \to \mathbb{F}; \phi(x) = x^p$. Entonces ϕ es un homomorfismo, ya que $\phi(1) = 1, \phi(xy) = \phi(x)\phi(y), \phi_p(x+y) = \phi_p(x) + \phi_p(y)$ y $\phi(-x) = -\phi(x)$. Además, $\phi_p^n(x) = x^{p^n} = x$ para todo x, es decir, ϕ_p^n es la identidad en $\mathbb{F}$. Como ϕ_p^n es una biyección, ϕ_p es una biyección, es decir, es un automorfismo de $\mathbb{F}$, conocido como el *automorfismo de Frobenius* de $\mathbb{F}$. De hecho se puede comprobar que este automorfismo tiene orden n y es el generador del grupo de Galois (cíclico) de $\mathbb{F}/\mathbb{F}_p$.

1.1.4 Grupos aditivo y multiplicativo de un cuerpo finito

Veamos la estructura de los grupos aditivo y multiplicativo de un cuerpo $\mathbb{F}_{p^n}$ de p^n elementos. Respecto al grupo aditivo, $\mathbb{F}_{p^n}^+$, todo elemento tiene orden p, por tanto por el teorema de clasificación de grupos abelianos finitamente generados, el grupo será isomorfo a $\mathbb{Z}_p^n$.

El grupo multiplicativo, $\mathbb{F}_{p^n}^\times$, tiene $p^n - 1$ elementos, y de hecho vamos a comprobar que es cíclico. Es decir, queremos ver que hay elementos de orden $p^n - 1$. Pero el teorema de clasificación de grupos abelianos finitamente generados nos dice que hay un elemento x_0 de orden máximo n_0 de forma que el orden del resto de elementos de $\mathbb{F}_{p^n}$ divide a n_0, es decir, $x^{n_0} = 1\ \forall x \in \mathbb{F}_{p^n}$. Es decir, todos los elementos de $\mathbb{F}_{p^n}$ son raíces de $x^{n_0} - 1$. Pero $x^{n_0} - 1$ tiene que tener grado mayor o igual a su número de raíces, que es $p^n - 1$. Es decir, $n_0 \geq p^n - 1$. Además, $n_0 \leq p^n - 1$, ya que el orden de x_0 divide al orden del grupo $\mathbb{F}_{p^n}^\times$. Por tanto $n_0 = p^n - 1$, y ya tenemos un elemento x_0 de orden $p^n - 1$. Enunciamos este importante resultado:

Teorema 1.2. El grupo multiplicativo de un cuerpo finito es cíclico.

1.2 Ecuaciones diofánticas. El principio local-global

Buscamos resolver ecuaciones diofánticas, es decir, encontrar soluciones enteras o racionales a una ecuación de la forma $P(x_1, \ldots, x_n) = 0$, donde P es un polinomio. Queremos saber tanto si hay soluciones como formas de calcularlas.

1.2.1 Ecuaciones lineales en 2 variables

El caso más simple es el de una ecuación lineal.
Por ejemplo: $ax + by = c,\ a, b, c \in \mathbb{Z}$. Tiene solución si y solo si $\text{mcd}(a, b)|c$.
Esto es fácil de ver, si existe solución denotamos $d := \text{mcd}(a, b)$ y entonces habrán $a', b' \in \mathbb{Z} :\ a = da',\ b = db'$, por tanto $c = d(a'x + b'y)$.
Por otro lado, $d|c \ \Rightarrow\ \exists c' \in \mathbb{Z} : c = dc'$, y como $0 \neq d|a, b$ tenemos

$$a' + b' = c',\ \text{mcd}(a', b') = 1;$$

esta ecuación tiene solución por la identidad de Bézout, es decir, existen $m, n \in \mathbb{Z}$ tales que:

$$a'm + b'n = 1\ \Rightarrow a'mc' + b'nc' = c' \Rightarrow\ x = mc',\ y = nc'.$$

Fijémonos en que si ya tenemos soluciones $x_0, y_0 \in \mathbb{Z}$ podemos definir para cada $\lambda \in \mathbb{Z}$: $x := x_0 - \lambda b'$, $y := y_0 + \lambda a' \Rightarrow$

$$ax + by = a(x_0 - \lambda b') + b(y_0 + \lambda a') = ax_0 + by_0 = c.$$

Sacamos así infinitas soluciones. De hecho, toda solución es de esta forma, veamos por qué:
Sea $x_0, y_0 \in \mathbb{Z}$ una solución y sea $x, y \in \mathbb{Z}$ otra distinta. Veamos si tiene sentido expresar $x = x_0 + \lambda b'$. Como λ puede ser cualquier entero, tenemos que ver que $x \equiv x_0 \mod b'$. Recordemos que $xa' + yb' = c'$ con $\mathrm{mcd}(a, b) = 1$, luego $xa' = c' \mod b'$ y por tanto $x \equiv x_0 \equiv c'a'^{-1} \mod b'$.

En conclusión, sabemos cuándo las ecuaciones diofánticas lineales en dos variables tienen solución y podemos calcularlas usando el algoritmo de Euclides para sacar el máximo común divisor.

1.2.2 El principio Local-Global

Sea $f \in \mathbb{Z}[X_1, \ldots, X_n]$, consideremos la ecuación $f(x_1, \ldots, x_n) = 0$, entonces cualquier solución $(a_1, \ldots, a_n)$ suya cumplirá que:

$$f(a_1, \ldots, a_n) \equiv 0 \mod m \ \forall m.$$

Así obtenemos condiciones necesarias que tendrá que cumplir cualquier solución de la ecuación diofántica. Además, estas ecuaciones serán más fáciles de estudiar porque $\mathbb{Z}_m$ tiene finitos elementos. Debido al teorema chino del resto, el caso que más nos interesará estudiar será el caso en que m es primo o potencia de primo.

Intentaremos ver cuándo se da la siguiente implicación:

$$\forall m \ \exists x_1, \ldots, x_n \in \mathbb{Z}_m : f(x_1, \ldots, x_n) \equiv 0 \mod m \implies \exists x_1, \ldots, x_n \in \mathbb{Z} : f(x_1, \ldots, x_n) = 0$$

Esto es lo que se llama principio de Hasse o local-global y ha sido uno de los motivos para el desarrollo de la teoría de números.
Demostraremos más adelante que en el caso cuadrático la implicación es cierta.
Sin embargo, ya en el caso cúbico el principio no tiene por qué ser cierto. La siguiente ecuación,

$$3x^3 + 4y^3 + 5z^3 = 0,$$

fue estudiada por Selmer en los 50, y vamos a ver durante las prácticas que tiene solución en congruencias pero no tiene solución no trivial en los enteros.

Otro ejemplo Sea $y^2 = x^3 + 7$, esta es una curva elíptica. Si existiesen $x, y \in \mathbb{Z}$ solución, entonces x debe ser impar:

$$y^2 \equiv x^3 + 3 \mod 4,$$

Si x es par entonces $x^3 \equiv 0 \mod 4$, pero 3 no es un resto cuadrático módulo 4 (1.3) .
Por otro lado, sumando 1 :

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4) = (x + 2)((x - 1)^2 + 3).$$

Como x es impar, $(x - 1)^2 + 3 \equiv 3 \mod 4$ Si descomponemos $(x - 1)^2 + 3$ en producto de primos, al menos uno debe ser $3 \mod 4$ pues si no el producto sería $1 \mod 4$.
Por tanto $\exists p$ primo tal que $p \equiv 3 \mod 4$ y $p|(x - 1)^2 + 3$.
Además, $y^2 + 1 = pm$ donde m es un entero. Luego

$$y^2 + 1 \equiv 0 \mod p$$

Más adelante veremos que los primos para los que algún y puede cumplir esa identidad son precisamente los congruentes con 1 módulo 4, llegando así a un absurdo.

Observemos que si homogeneizamos el polinomio y replanteamos el problema, es como pedirle a $y^2 = x^3 + 7$ soluciones racionales en vez de enteras. Recalcamos que es un problema distinto que podemos abordar con teoría más general de curvas y grupos.

1.3 Símbolos de Legendre. El criterio de Euler

Euler descubrió que, dados dos primos impares p y q, la solubilidad de $x^2 \equiv q \mod p$ y $x^2 \equiv p \mod q$ estaba relacionada.
Es más, si $p, q \equiv 3 \mod 4$ entonces una y solamente una de las ecuaciones tendrá solución.
En el resto de casos veremos que ninguna o ambas ecuaciones tienen solución. A esta relación entre la solubilidad de las ecuaciones se le llama ley de reciprocidad. Euler no logró probarla. Legendre lo intentó e introdujo un símbolo para simplificar la notación

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si} \quad \exists b \in \mathbb{Z} : \ a \equiv b^2 \mod p \\ -1 & \text{si} \quad \forall b \in \mathbb{Z} : \ a \not\equiv b^2 \mod p \end{cases}$$

La ley de reciprocidad obedece a la siguiente ecuación

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$$

Legendre da una demostración. No obstante, supone la infinitud de infinitos primos en una sucesión aritmética pero sin demostrarlo.
Gauss en 1801 publica *Disquisitiones arithmeticae* donde se da la primera demostración completa. No se queda conforme con dar una y a lo largo de su vida publica hasta 8 demostraciones distintas, con la idea de poder generalizar la ley a otros exponentes. A día de hoy se conocen más de 200 demostraciones distintas.

Definición 1.3. Se dice que $a \in \mathbb{Z}$ es un resto cuadrático módulo n si $\exists x \in \mathbb{Z} : \ x^2 \equiv a \mod n$.

Vamos a estudiar los residuos cuadráticos módulo p, con p primo. Si $p = 2$, 1 y 0 son restos cuadráticos. Podemos suponer entonces que p es impar.
Dados $a \in \mathbb{Z}, b \in \mathbb{Z}^+$ se define el símbolo de Legendre como

$$\left(\frac{a}{b}\right) := \begin{cases} 1 & \text{si} \quad \exists c \in \mathbb{Z} : a \equiv c^2 \mod b \\ -1 & \text{si} \quad \forall c \in \mathbb{Z} : a \not\equiv c^2 \mod b \end{cases}$$

Veamos una primera identidad.

Proposición 1.4. Sean $a, b \in \mathbb{Z}$ y p un primo impar: $p \nmid a, b$, entonces la siguiente identidad es cierta:

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

Demostración. Al pedir que $p \nmid a, b$ estamos trabajando dentro del grupo multiplicativo $\mathbb{Z}_p^*$ de $p-1$ elementos, nos fijamos en que $a^2 \equiv (-a)^2 \mod p$ así que la aplicación $\varphi : x \in \mathbb{Z}_p^* \mapsto x^2$ cumple que $|\varphi(\mathbb{Z}_p^*)| \leq \dfrac{p-1}{2}$.
Como $\mathbb{Z}_p^*$ es cíclico, tomamos a de orden $p-1$, entonces a^2 tiene orden $\dfrac{p-1}{2}$ y genera los residuos cuadráticos, que son $\dfrac{p-1}{2}$.

Así que tenemos en $\mathbb{Z}_p^*$ tenemos $\dfrac{p-1}{2}$ residuos cudráticos en $\mathbb{Z}_p$ mientras que $\dfrac{p-1}{2}$ elementos de $\mathbb{Z}_p$ no son residuos cuadráticos.

Si a, b son residuos entonces $\exists c, d \in \mathbb{Z}: \ a \equiv c^2 \mod p, \ b \equiv d^2 \mod$ luego $ab = (cd)^2 \mod p$. Es decir, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1 \Rightarrow \left(\frac{ab}{p}\right) = 1$.
Si $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1$, suponemos sin pérdida de generalidad que $\left(\frac{a}{p}\right) = 1$. Si se diese el caso de que $\left(\frac{ab}{p}\right) = 1$ se tiene que existen $c, d \in \mathbb{Z}: \ a \equiv c^2 \mod p, \ ab \equiv d^2 \mod p$. Luego $(c^{-1}d)^2 \equiv b \mod p$ llegando a un absurdo.

Por último, si $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Consideremos la aplicación $\psi : x \in \mathbb{Z}_p^* \mapsto ax$, se trata de una biyección. Denotemos por $R := \{x \in \mathbb{Z}_p^* : \exists c \in \mathbb{Z}, \ x \equiv c^2 \mod p\}$, sabemos que, como $\psi(R) = \mathbb{Z}_p^* \setminus R$ llegamos a que $\psi(\mathbb{Z}_p^* \setminus R) = R$ luego como $b \in \mathbb{Z}_p^* \setminus R$, $\left(\frac{ab}{p}\right) = 1$. □

Dado p primo, la función $a \to \left(\frac{a}{p}\right)$ solamente depende de la clase de equivalencia de a, es decir, si $a \equiv_p b$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Esto, junto a la propiedad 1.4, hace al símbolo de Legendre sobre p lo que se llama un *carácter* de Dirichlet, de los cuales veremos más ejemplos más adelante. Vamos a ver una forma que dio Euler de calcular símbolos de Legendre sobre un primo impar.

Teorema 1.5 (Criterio de Euler)**.** Sean $a \in \mathbb{Z}$ y p primo impar. Entonces se cumple que

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$$

Demostración. Si $a \equiv_p 0$ es obvio. Supongamos que no, es decir, a es un elemento de $\mathbb{Z}_p^\times = \{1, g, g^2, \ldots, g^{p-2}\}$, siendo g un generador de $\mathbb{Z}_p^\times$.

Al elevar los elementos de $\mathbb{Z}_p^\times$ al cuadrado, obtenemos todos los residuos cuadráticos distintos de 0, que serán $\{1, g^2, g^4, \ldots, g^{2(p-2)}\} = \{1, g^2, g^4, \ldots, g^{p-3}\}$ (ya que $g^{p-1} = 1$ y a partir de ahí todos los elementos se repiten). Por tanto los residuos cuadráticos son los elementos g^k, con k par entre 0 y $p-3$, y los demás elementos de $\mathbb{Z}_p^\times$, es decir, $\{g, g^3, \ldots, g^{p-2}\}$, no son residuos cuadráticos.

Ahora, si a es residuo cuadrático, $\left(\frac{a}{p}\right) = 1$, es de la forma g^{2k} para cierto k. Por tanto $a^{\frac{p-1}{2}} = g^{k(p-1)} = 1^k = 1$.

Si a no es residuo cuadrático, $\left(\frac{a}{p}\right) = -1$, es de forma g^{2k+1}. Por tanto

$$a^{\frac{p-1}{2}} = g^{k(p-1)+\frac{p-1}{2}} = a^{\frac{p-1}{2}} = \left(g^{(p-1)}\right)^k g^{\frac{p-1}{2}} = 1^k g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}}.$$

$g^{\frac{p-1}{2}}$ es -1 porque $0 = g^{p-1} - 1 = \left(g^{\frac{p-1}{2}}\right)^2 - 1 = \left(g^{\frac{p-1}{2}} + 1\right)\left(g^{\frac{p-1}{2}} - 1\right)$, y $g^{\frac{p-1}{2}} - 1$ no es 0, ya que g tiene orden $p-1$. □

1.4 Leyes suplementarias. Criterio de Gauss

Teorema 1.6 (1ª ley suplementaria)**.** Dado p primo impar,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Es decir, -1 es residuo cuadrático módulo un primo p impar sii $p \equiv_4 1$.

Demostración. Si $p \equiv 1 \mod 4$ entonces $\frac{p-1}{2}$ es par, ergo $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, ergo $\exists c \in \mathbb{Z} : c^2 + 1 = 0 \mod p$.
Mientras que si $p \equiv 3 \mod 4$, $\frac{p-1}{2}$ es par, ergo $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$, así que$\forall c \in \mathbb{Z} : c^2 + 1 \not\equiv 0 \mod p$. □

Antes de enunciar la segunda ley suplementaria, conviene comprobar que para todo n impar, $n^2 - 1$ es múltiplo de 8. Como esto solo depende de la clase módulo 8 de n, basta comprobar que se cumple para $1, 3, 5$ y 7.

Teorema 1.7 ($2^{\underline{a}}$ ley suplementaria)**.** Dado p primo impar,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Es decir, 2 es residuo cuadrático módulo p sii $p \equiv_8 \pm 1$.

Demostración. Consideramos la inclusión $\mathbb{Z}_p \equiv \mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2}$. Entonces, el grupo múltiplicativo $\mathbb{F}_{p^2}^{\times}$ tiene $p^2 - 1$[1] (múltiplo de 8) elementos, y es cíclico. Por tanto tiene algún elemento ω de orden 8. Es decir, $\omega^8 = 1$, pero $\omega^4 \neq 1$: ω es una raíz octava primitiva de la unidad. Entonces, ω^4 será -1, por ser su cuadrado 1 y no ser 1. Entonces, $\omega^{-4} = \frac{1}{\omega^4} = -1$. De ahí deducimos $(\omega^2 + \omega^{-2})^2 = \omega^4 + \omega^{-4} + 2 = -1 - 1 + 2 = 0$. Ergo, $\omega^2 + \omega^{-2} = 0$. Ahora calculamos $(\omega + \omega^{-1})^2 = \omega^2 + \omega^{-2} + 2 = 0 + 2 = 2$.

Es decir, si $\omega + \omega^{-1}$ estuviera en $\mathbb{F}_p$, ya tendríamos un elemento cuyo cuadrado es 2. Recíprocamente, si hay un elemento de $\mathbb{F}_p$ cuyo cuadrado es 2, ese será $\omega + \omega^{-1}$ ó $-\omega - \omega^{-1}$. Por tanto,

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow \omega + \omega^{-1} \in \mathbb{F}_p.$$

Pero a su vez, los elementos de $\mathbb{F}_p$ son exactamente las raíces de $x^p - x$, osea que $\omega + \omega^{-1}$ estará en $\mathbb{F}_p$ si y solo si $\omega + \omega^{-1} = (\omega + \omega^{-1})^p$. Es decir, $\omega + \omega^{-1} = \omega^p + \omega^{-p}$. Ahora bien, como $\omega^8 \equiv 1$, tenemos que $\omega^p = \omega^q$, donde $q \equiv_8 p$ y q está entre -3 y 3. Veamos ahora que se cumple el enunciado por casos:

- Si $p \equiv_8 \pm 1$, entonces $\omega^p = \omega^{\pm 1}$, por tanto es obvio que $\omega + \omega^{-1} = \omega^p + \omega^{-p}$.
- Si, por el contrario, $p \equiv_8 \pm 3$, entonces $\omega^p = \omega^{\pm 3}$. En este caso no pasará que $\omega + \omega^{-1} = \omega^p + \omega^{-p}$, ya que la ecuación $x + \frac{1}{x} + 1 = 0$, o equivalentemente, $x^2 + x + 1 = 0$[2], solo tiene 2 soluciones, que son ω y ω^{-1}, no ω^3 ni ω^{-3}.

Y bueno, como p es impar q también luego solo tenemos que mirar estos 4 casos.
Ahora nos fijamos en los valores módulo 8 de $(p-1)$ y $(p+1)$. Al meter ± 1 se obtiene $0, 2$ y $-2, 0$. Luego al dividir entre ocho obtenemos que $\frac{p^2-1}{8}$ es par. En cambio para ± 3 se tienen $2, 4$ y $-4, -2$ así que $\frac{p^2-1}{8}$ es impar.Por tanto la segunda ley suplementaria es cierta. □

Gauss dio otro criterio, que enunciamos sin demostración, para calcular el símbolo de legendre de un entero sobre un primo impar. Para verlo necesitamos la siguiente definición:

Definición 1.8. Sea p primo impar, n entero. Entonces el *resto mínimo* de n entre p es el entero m entre $-\frac{p-1}{2}$ y $\frac{p-1}{2}$ tal que $n \equiv_p m$.

Teorema 1.9 (Criterio de Gauss)**.** Sea p primo impar, n natural no múltiplo de p. Entonces,

$$\left(\frac{n}{p}\right) = (-1)^m,$$

donde m es el número de enteros k con $1 \leq k \leq \frac{p-1}{2}$ de forma que kn tiene resto mínimo negativo entre p. □

[1] $p^2 - 1 = (p-1)(p+1)$, p es impar luego al menos un de los dos factores es divisible por 4.
[2] $(x^2 + x + 1)(x - 1) = x^3 - 2$.

Este criterio permite demostrar las leyes suplementarias. La primera es directa: si $n = -1$, usando la notación del enunciado, los números kn serían $-1, -2, \ldots, -\frac{p-1}{2}$. Como todos tienen resto mínimo negativo, tenemos que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. La segunda ley requiere algunas cuentas pero no es mucho más difícil de demostrar con este criterio. De hecho, este criterio se puede usar para probar la reciprocidad cuadrática.

1.5 Ley de Reciprocidad Cuadrática

Teorema 1.10. Si $p, q > 2$ son primos distintos, entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Demostración. Llamamos $\overline{p}$ a la clase de p módulo q. Sea n el orden de $\overline{p}$ en $\mathbb{Z}_q^\times$. Entonces, $n|q-1$, y como $\overline{p}^n = 1$, tenemos que $p^n \equiv_q 1$, por tanto $q|p^n - 1$. Como $p^n - 1$ es a su vez el orden del grupo multiplicativo cíclico de $\mathbb{F}_{p^n}$, habrá un elemento $\omega \in \mathbb{F}_{p^n}^\times$ de orden q, es decir, una raíz primitiva q-ésima de la unidad en $\mathbb{F}_{p^n}$. Consideremos ahora la siguiente matriz cuadrada simétrica de orden q:

$$A = (\omega^{(i-1)(j-1)})_{i=1,\ldots,q}^{j=1,\ldots,q} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{q-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(q-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{q-1} & \omega^{2(q-1)} & \ldots & \omega^{(q-1)^2} \end{pmatrix}$$

Es una matriz de Vandermonde, por tanto, si llamamos δ a su determinante, tenemos que

$$\delta = \prod_{0 \le i < j \le q-1} (\omega^j - \omega^i)$$

Afirmamos entonces:

$$\delta^2 = \overline{q}^{q-1} \cdot \overline{q^*}, \tag{1.1}$$

donde $q^* = (-1)^{\frac{q-1}{2}} q$. Vamos a demostrarlo.

δ^2 es el determinante de $(A^2)_i^j = \sum_k a_i^k a_k^j = \sum_k \omega^{(i-1)(k-1)} \omega^{(k-1)(j-1)} = \sum_k \omega^{(i+j-2)(k-1)} = \sum_k (\omega^{i+j-2})^{k-1}$. Si $i + j - 2$ es múltiplo de q, $\omega^{i+j-2} = 1$, ergo $A_{i,j}^2 = \overline{q}$. Si, por el contrario, $i + j - 2$ no es múltiplo de q, ω^{i+j-2} es una raíz primitiva q-ésima de la unidad, por tanto $A_{i,j}^2$ vale la suma de las raíces q-ésimas de la unidad, es decir, 0. Resumiendo:

$$A^2 = \begin{pmatrix} \overline{q} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \overline{q} \\ 0 & 0 & 0 & \cdots & \overline{q} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \overline{q} & \cdots & 0 & 0 \\ 0 & \overline{q} & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Mediante $\frac{q-1}{2}$ transposiciones de columnas, podemos transformar A^2 en $\overline{q}I$, por tanto, como queríamos, $\delta^2 = \left|A^2\right| = \overline{q}^q (-1)^{\frac{q-1}{2}} = \overline{q}^{q-1} \cdot \overline{q^*}$.

Pasamos a hacer una segunda afirmación:

$$\delta^p = (-1)^{\frac{q-1}{n}} \delta \tag{1.2}$$

Para comprobarla, recordemos que en $\mathbb{F}_{p^n}$ se cumple que $(xy)^p = x^p y^p$ y que $(x+y)^p = x^p + y^p$. Ahora bien, como al evaluar un polinomio $f \in \mathbb{F}_{p^n}[x_1, \ldots, x_n]$ solo estamos haciendo sumas de produc-

tos de las variables, tendremos usando las propiedades anteriores que para cualesquiera $a_1, \ldots, a_n \in \mathbb{F}_{p^n}$, $f(a_1, \ldots, a_n)^p = f(a_1^p, \ldots, a_n^p)$. Por tanto, como el determinante de una matriz es un polinomio en función de sus entradas, tenemos que $\det(A)^p$ será el determinante de la matriz obtenida al elevar las entradas de A a p. Es decir:

$$\delta^p = |A^p| = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^p & \omega^{2p} & \cdots & \omega^{(q-1)p} \\ 1 & \omega^{2p} & \omega^{4p} & \cdots & \omega^{2(q-1)p} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(q-1)p} & \omega^{2(q-1)p} & \cdots & \omega^{(q-1)^2 p} \end{vmatrix}. \text{ Llamamos } A_p \text{ a esta nueva matriz.}$$

Como w^p es otra raíz q-ésima de la unidad, $\omega^p, \omega^{2p}, \ldots, \omega^{(q-1)p}$ son las raíces q-ésimas de la unidad. Por tanto las filas de nuestra matriz son de la forma $(1, \alpha, \ldots, \alpha^{q-1})$, donde α es una raíz q-ésima de la unidad. Es decir, las filas de la matriz A_p son las mismas que las filas de la matriz A, salvo una permutación. Por tanto el determinante de A y el de A_p serán iguales salvo por el signo. Para comprobar cómo cambia el signo, tendremos que estudiar cómo se permutan exactamente las filas.

Para esto, nombraremos a las filas según su segundo elemento, es decir, para cada raíz α, la fila α será $(1, \alpha, \alpha^2, \ldots, \alpha^{q-1})$. Entonces, si la i-ésima fila de A es la fila α, entonces la i-ésima fila de A_p será la fila α^p. Por tanto, la permutación que hay entre las filas es esencialmente la permutación $\Phi : \alpha \mapsto \alpha^p$ entre las raíces q-ésimas de la unidad. ¿Qué signo tiene esta permutación? Para comprobarlo podemos escribirla como composición de ciclos disjuntos. Dada una raíz $\alpha \neq 1$, α tiene orden q. Por tanto, como $p^n \equiv_q 1$, $\alpha^{p^n} = \alpha$. Además, este n es el menor que cumple esa propiedad. Por tanto un ciclo disjunto de n elementos de Φ será $(\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}})$. Como no hemos especificado α, esto pasa para todas las raíces. Como hay $q-1$ raíces en los ciclos (el 1 queda fijo bajo la permutación, osea que no está en ningún ciclo), tenemos que Φ factoriza como $\frac{q-1}{n}$ ciclos de n elementos cada uno. Como un ciclo de orden n tiene signo $(-1)^{n-1}$, nuestra permutación tendrá signo $(-1)^{(n-1)\frac{q-1}{n}}$.

Por tanto, tendremos que $|A_p| = (-1)^{(n-1)\frac{q-1}{n}}|A|$. Es decir, $\delta^p = (-1)^{(n-1)\frac{q-1}{n}}\delta$. Para comprobar que eso equivale a nuestra fórmula basta comprobar que $(-1)^{(n-1)\frac{q-1}{n}} = (-1)^{\frac{q-1}{n}}$. Es decir, como $(-1)^{\frac{q-1}{n}} = (-1)^{-\frac{q-1}{n}}$, esto equivale a probar que $(-1)^{(n-1)\frac{q-1}{n}} = (-1)^{-\frac{q-1}{n}}$, osea, $(-1)^{n\frac{q-1}{n}} = 1$, lo cual es obvio ya que $q-1$ es par.

Ya estamos en la recta final. Recapitulando, nuestras dos afirmaciones nos dicen que:

$$\begin{cases} \delta^2 = \overline{q}^{q-1} \cdot \overline{q^*} & (1) \\ \delta^p = (-1)^{\frac{q-1}{n}}\delta & (2) \end{cases}$$

Ahora, primero demostramos que $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$. Haremos esto probando que $\left(\frac{q^*}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{q}\right) = 1$ mediante una sucesión de dobles implicaciones.

$\left(\frac{q^*}{p}\right)$ será 1 cuando q^* sea un residuo cuadrático $\mod p$. Pero, en la igualdad (1), $\overline{q}^{q-1}$ es un cuadrado en $\mathbb{Z}_p$ (por ser $q-1$ par). Por tanto, q^* será un cuadrado en $\mathbb{Z}_p$ si y solo si δ^2 es un cuadrado no nulo en $\mathbb{Z}_p$. Además, que δ^2 sea un cuadrado en $\mathbb{Z}_p$ equivale a decir que $\delta \in \mathbb{Z}_p$: en efecto, si $\delta \in \mathbb{Z}_p$ es obvio que δ^2 es un cuadrado en $\mathbb{Z}_p$, y recíprocamente, si δ^2 es un cuadrado en $\mathbb{Z}_p$, sea $x \in \mathbb{Z}_p$ con $x^2 = \delta^2$, entonces $(x+\delta)(x-\delta) = 0$, ergo x es δ o $-\delta$, por tanto $\delta \in \mathbb{Z}_p$. A su vez, ya sabemos que $\delta \in \mathbb{Z}_p$ si y solo si $\delta = \delta^p$. Esto equivale por la igualdad (2) a $(-1)^{\frac{q-1}{n}} = 1$, es decir, $\frac{q-1}{n}$ es par, es decir, $2 \left| \frac{q-1}{n} \right.$, es decir, $2n \,|\, q-1$, es decir, $n \left| \frac{q-1}{2} \right.$, lo cual, usando que n es el orden de p en $\mathbb{Z}_q^\times$, quiere decir que $p^{\frac{q-1}{2}} = 1$, es decir, $\left(\frac{p}{q}\right) = 1$.

Solo quedan unos cálculos, usando lo que ya sabemos:

$$1 = \left(\frac{p}{q}\right)\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Dividiendo en ambos lados por $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, obtenemos la ley de reciprocidad cuadrática.

□

Veamos algunos ejemplos de uso de la ley de reciprocidad cuadrática.

Determinar residuos cuadráticos Veamos si 383 es resto cuadrático módulo 443. Ambos son primos. Se tiene que

$$\left(\frac{383}{443}\right) = (-1)^{\frac{283-1}{2}\frac{443-1}{2}}\left(\frac{443}{383}\right) = -\left(\frac{60}{383}\right) = -\left(\frac{2}{383}\right)^2\left(\frac{3}{383}\right)\left(\frac{5}{383}\right) = -\left(\frac{3}{383}\right)\left(\frac{5}{383}\right) =$$

$$(-1)^{\frac{3-1}{2}}\left(\frac{383}{3}\right)(-1)^{\frac{5-1}{2}}\left(\frac{383}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = 1$$

Así que 383 es resto cuadrático módulo 443. Otro asunto es saber cuáles son sus raíces.

Cuando queremos saber qué restos cuadráticos hay módulo p con $p > 2$ primo pequeño, es necesario solo revisar los números hasta $\frac{p-1}{2}$.

Primos de Fermat. Decimos que un primo es de fermat si es de la forma $p = 2^{2^n} + 1$ para cierto $n \geq 0$. Veamos que si p es un primo de Fermat, 7 es raíz primitiva módulo p, salvo en el caso $p = 3$.
Esto quiere decir que 7 es un generador del grupo multiplicativo de $\mathbb{F}_p$.
Veámoslo, el orden del grupo multiplicativo es 2^{2^n} luego queremos ver que el orden de 7 es 2^{2^n}. En un grupo cíclico de orden 2^k, todos los elementos tienen orden potencia de 2, y es fácil ver que un elemento x tiene orden 2^k sii $x^{2^{k-1}}$ no es 1. En nuestro caso, $k = 2^n$, tendremos que 7 tiene orden 2^{2^n} si y solo si $7^{2^{2^n-1}}$ no es 1, es decir, $7^{\frac{p-1}{2}} \neq 1$.
Por el criterio de Euler, equivale a decir que $\left(\frac{7}{p}\right) = -1$ y haciendo uso de la ley de reciprocidad cuadrática:

$$\left(\frac{2^{2^n}}{7}\right) = \left(\frac{p}{7}\right) = (-1)^{(\frac{p-1}{2})(\frac{7-1}{2})}\left(\frac{7}{p}\right) = \left(\frac{7}{p}\right)$$

Así que tratamos de ver que $\left(\frac{2^{2^n}}{7}\right) = -1$.
Calculemos 2^{2^n} módulo 7. Los residuos cuadráticos módulo 7 son $1, 4, 2$ luego nos interesa que $2^{2^n} + 1$ sea $3, 5$ ó 6. Es decir, queremos que 2^{2^n} es $2, 4$ ó 5 si $n \geq 1$.
Sabemos que $2^6 = 1 \mod 7$, así que el valor de 2^k en módulo 7 solo depende del valor de k en módulo 6. A su vez, es directo ver por inducción que $2^n \equiv_6 2$ si n es impar y $2^n \equiv_6 4$ si n es par. Por tanto, $2^{2^n} \equiv_7 2^{2^1} \equiv_7 4$ si n es impar y $2^{2^n} \equiv_7 2^{2^2} \equiv_7 2$ si n es par, por tanto $2^{2^n} + 1$ no es residuo cuadrático, como queríamos.

1.5.1 Primos p con un residuo cuadrático dado

Dado $a \in \mathbb{Z}$, consideremos la siguiente ecuación de incógnita p:

$$\exists x |\ x^2 \equiv a \mod p,\ p \nmid a$$

donde $p > 2$ es primo.

Veamos qué tiene que ocurrir para que $a = -1$ sea resto cuadrático, como

$$1 = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \Leftrightarrow p \equiv 1 \mod 4$$

Los primos $p = 4m + 1$ cumplen que -1 es resto cuadrático módulo p.

Si $a = 2$, la segunda ley suplementaria:

$$1 = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

tomando p módulo 8 : $p = 1 + 2k + 8m$ luego $p^2 = 1 + 4k + 4k^2 + 16m(1 + 2k) + 64m^2$,

$$\frac{p^2-1}{8} = \frac{k(k+1)}{2} + 2m(1+2k) + 8m^2 \equiv \frac{k(k+1)}{2} \mod 2,$$

k puede ser $0, 1, 2, 3$, $\frac{k(k+1)}{2} \equiv 0 \mod 2$ si y solo si $k = 0, 3$ esto quiere decir que $p = \pm 1 \mod 8$ luego $p = 8m+1$ ó $p = 8m + 7$.

Si $a = -2$:

$$1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$$

Tenemos dos casos, ambos factores valen 1 o ambos valen -1. El primer caso se da solo cuando $p \equiv 1 \mod 8$. En cambio el segundo cuando $p \equiv 3 \mod 8$. Luego son los primos de la forma $p = 8m + 1$ ó $p = 8m + 3$.

Si $a = 3$:

$$1 = \left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

Si $p \equiv 1 \mod 4$ y $\left(\frac{p}{3}\right) = 1$, entonces, si suponemos $p > 3$ se tiene lo siguiente

$$\begin{cases} p \equiv 1 \mod 4 \\ p \equiv 1 \mod 3 \end{cases}$$

Este sistema tiene como solución $p \equiv 1 \mod 12$. Si $p \equiv 3 \mod 4$ y $\left(\frac{p}{3}\right) = -1$:

$$\begin{cases} p \equiv 3 \mod 4 \\ p \equiv 2 \mod 3 \end{cases}$$

Como $3 \equiv_4 -1$, $2 \equiv_3 -1$. Deducimos inmediatamente que $p \equiv -1 \mod 12$.
Así que $p \equiv \pm 1 \mod 12$. Son los primos de la forma $p = 12m + 1$ ó $p = 12m + 11$.

Si ponemos a más grande la situación se puede complicar. Para usar estos problemas se puede utilizar el teorema de los restos:

Teorema 1.11. TEOREMA DE LOS RESTOS
Sea una cantidad finita de congruencias lineales

$$\begin{cases} x \equiv a_1 \mod m_1 \\ \cdots \\ x \equiv a_t \mod m_t \end{cases}$$

tales que $\text{mcd}(m_i, m_j) = 1 \ \forall i, j = 1, \ldots, t$ con $i \neq j$.
Entonces $\exists a \in \mathbb{Z}$ único módulo $\prod_{1 \leq i \leq t} a_i$ tal que $a \equiv a_i \mod m_i \ \forall i = 1, \ldots, t$.

Demostración práctica y sencilla. Sea $M_i := \prod_{j \neq i} m_j$, entonces $\prod_j m_j = m_i M_i \ \forall i = 1, \ldots, t$.

Se tiene que $\text{mcd}(M_i, m_i) = 1$, luego $\exists M_i^* \in \mathbb{Z} : \ M_i^* M_i \equiv 1 \mod m_i$. Sea

$$a_0 := \sum_j a_j M_j^* M_j \equiv_{m_i} a_i M_i^* M_i \equiv_{m_i} a_i \ \forall i = 1, \ldots, t$$

a_0 es solución, sea a otra solución se tiene $\forall i = 1, \ldots, t$ que $m_i | a_0 - a$. Luego $\prod_j m_j | a - a_0$ y

$$a \equiv a_0 \mod \prod_j m_j$$

□

Capítulo 2

Dominios euclídeos

2.1 Dominios euclídeos

Sea R dominio de integridad, entonces R es dominio euclídeo si hay una función $\varphi : R \setminus \{0\} \to \mathbb{N}$ tal que si $a, b \in R$:

1) $ab \neq 0 \Rightarrow \ \varphi(a) \leq \varphi(ab)$

2) $b \neq 0 \Rightarrow a = qb + r,\ q, r \in R,\ r = 0$ ó $\varphi(r) < \varphi(b)$.

Recordemos que en dominios de integridad, se cumple la cadena de implicaciones DE $\implies$ DIP $\implies$ DFU, es decir, todo dominio euclídeo es un dominio de ideales principales, y todo dominio de ideales principales es un DFU. De modo que solo con encontrar una función ϕ como la de arriba, ya tendremos que los elementos de nuestro anillo tienen una factorización esencialmente única como producto de irreducibles.

Lema 2.1. Sea R dominio de integridad, sea K el cuerpo de fracciones de R. Si existe $\varphi : K \setminus \{0\} \to \mathbb{Q}$ tal que

1) $\varphi(\alpha) \in \mathbb{N}\ \forall \alpha \in R$.

2) $\forall x, y \in K,\ \varphi(xy) = \varphi(x)\varphi(y)$.

3) $\forall x \in K \setminus R,\ \exists \gamma \in R :\ \varphi(x - \gamma) < 1$.

Entonces R es dominio euclídeo.

Demostración. Veamos que la restricción de φ a R, que es una función de $R \setminus \{0\}$ en $\mathbb{N}$ por 1), cumple las propiedades 1 y 2 de la definición de dominio euclídeo.

1 es fácil de ver, ya que si $ab \neq 0$ y $a, b \in R$, entonces $\varphi(a), \varphi(b) \in \mathbb{N}$, por tanto $\varphi(ab) = \varphi(a)\varphi(b) \geq \varphi(a)$.

Para ver 2, sean $a, b \in R$ con $b \neq 0$. Entonces tenemos dos opciones:

• $\frac{a}{b} \in R$. Entonces hay $c \in R$ con $a = bc$, y se cumple 2.

• $\frac{a}{b} \notin R$. Entonces por la propiedad 3) hay cierto $q \in R$ con $\varphi(\frac{a}{b} - q) < 1$. Es decir, $\varphi(\frac{a-bq}{b}) < 1$. Es decir, $\frac{\varphi(a-bq)}{\varphi(b)} < 1$. Es decir, como $\varphi(b)$ es natural, $\varphi(a - bq) < \varphi(b)$. Llamando $r = a - bq$ tenemos que $a = bq + r$ y $\varphi(r) < \varphi(b)$, y se cumple 2. □

Ejemplos

•$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$, los enteros Gaussianos. El cuerpo de fracciones de $\mathbb{Z}[i]$ es $\mathbb{Q}[i] = \mathbb{Q}(i)$. Para comprobar que $\mathbb{Z}[i]$ es un DE, usamos el lema 2.1 con la función $\varphi(r + si) = r^2 + s^2$, es decir, $\varphi(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$.
Tenemos que ver que se dan las tres propiedades de 2.1. Dados $a, b \in \mathbb{Z}$, se tiene que $\varphi(a + bi) = a^2 + b^2 \in \mathbb{N}$. Dados $\alpha, \beta :\ \varphi(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \varphi(\alpha)\varphi(\beta)$.

Para la propiedad 3, si nos dan un punto $a + bi$ con $a, b \in \mathbb{Q}$, está claro que podemos encontrar un punto con coordenadas enteras a distancia < 1: basta coger c, d enteros a distancia $\leq \frac{1}{2}$ de a y b respectivamente, y entonces tenemos que $c + di \in \mathbb{Z}_i$ y $\varphi((a+bi)-(c+di)) = |(a-c)+(b-d)i| = (a-b)^2+(c-d)^2 \leq \frac{1}{4}+\frac{1}{4} < 1$.

•$\mathbb{Z}[\sqrt{-2}]$. El cuerpo de fracciones en este caso es $\mathbb{Q}[\sqrt{-2}]$. La función φ que usaremos será la misma: $\varphi(\alpha) = |\alpha|^2$, siendo $|\cdot|$ el módulo complejo. Es decir, $\varphi(a+b\sqrt{-2}) = a^2+2b^2$. Las dos primeras propiedades se cumplen igual que en el ejemplo anterior, y la tercera también: en este caso si tenemos el número $a+b\sqrt{-2}$ cogeremos c y d a distancia $\leq \frac{1}{2}$ de a y b respectivamente, y entonces $\varphi((a+b\sqrt{-2})-(c+d\sqrt{-2})) = |(a-c)+(b-d)\sqrt{-2}| = (a-b)^2+2(c-d)^2 \leq \frac{1}{4}+\frac{2}{4} < 1$.

•$\mathbb{Z}[\sqrt{-3}]$. Este anillo **no** va a ser un dominio euclideo. Veamos primero por qué la función $\varphi(\alpha) = |\alpha|^2$ no hace a $\mathbb{Z}[\sqrt{-3}]$ un dominio euclideo. Fijémonos en que en $\mathbb{Z}[\sqrt{-1}]$, para probar que es un DE hemos usado la desigualdad $\frac{1}{4}+\frac{1}{4} < 1$, y en $\mathbb{Z}[\sqrt{-2}]$ hemos usado la desigualdad $\frac{1}{4}+\frac{2}{4} < 1$. Si intentamos repetir el argumento de antes, necesitaríamos la desigualdad $\frac{1}{4}+\frac{3}{4} < 1$, que es falsa. De hecho, se puede ver que cogiendo el número $\frac{1}{2}+\frac{\sqrt{-3}}{2}$, este número no tiene ningún elemento de $\mathbb{Z}[\sqrt{-3}]$ a distancia < 1. Por tanto la función módulo no funciona en este caso.

De hecho, $\mathbb{Z}[\sqrt{-3}]$ no será dominio euclideo por la siguiente igualdad: $2 \cdot 2 = (1-\sqrt{3})(1+\sqrt{-3})$. En esta igualdad, tanto 2 como $1-\sqrt{-3}$ y $1+\sqrt{-3}$ son irreducibles. Lo comprobaremos en el caso 2, los otros son similares. Si tuviéramos $2 = (a_1+b_1\sqrt{-3})(a_2+b_2\sqrt{-3})$, tomando módulo al cuadrado tendríamos que $4 = (a_1^2+3b_1^2)(a_2^2+3b_2^2)$. Como a^2+3b^2 no puede ser 2 si $a,b \in \mathbb{Z}$, tendremos que o bien $a_1^2+3b_1^2$ o $a_2^2+3b_2^2$ tendrá que ser 1, por tanto $a_1+b_1\sqrt{-3}$ o $a_2+b_2\sqrt{-3}$ es una unidad. Por tanto 2 es irreducible.

Ahora, en la igualdad $2 \cdot 2 = (1-\sqrt{-3})(1+\sqrt{-3})$, todos los números son irreducibles, por tanto tenemos dos factorizaciones distintas del 4. Estas factorizaciones son de verdad distintas porque al multiplicar 2 por una unidad (solo hay dos unidades, 1 y -1) no obtenemos ni $1+\sqrt{-3}$ ni $1-\sqrt{-3}$. Por tanto $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única luego tampoco es dominio euclídeo.

2.2 $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{-2}]$

2.2.1 $\mathbb{Z}[i]$

Vamos a estudiar más en detalle $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{-2}]$: Las unidades en $\mathbb{Z}[i]$ son $1,-1,i,-i$. Pues dado $a+bi \in \mathbb{Z}[i]$: $\exists c+di \in \mathbb{Z}[i]$ con $1 = (a+bi)(c+di)$, entonces $1 = |a+bi|^2|c+di|^2$, el producto de las normas debe ser 1 luego son no negativas. Como $|a+bi| = a^2+b^2$ la única opción es que $|a+bi| = |c+di| = 1$, dándonos las unidades mencionadas anteriormente. Como estamos en un DFU, un elemento es primo si y solo si es irreducible. Veamos quiénes son los primos.

Dado un elemento $\pi \in \mathbb{Z}[i]$ irreducible, $N(\pi) = \pi\overline{\pi} \in \mathbb{Z}$. $\pi\overline{\pi}$ se descompone como producto de primos de $\mathbb{Z}$, luego π debe dividir a algún p primo en $\mathbb{Z}$. Así que si queremos encontrar los elementos π irreducibles en $\mathbb{Z}[i]$, podemos suponer que $\pi|p$ siendo p primo en $\mathbb{Z}$.

Veamos qué pasa si $p = 2$:

$$2 = 1^2+1^2 = (1+i)(1-i) = -i(1+i)^2,\ N(1+i) = N(1-i) = 2.$$

Es un cuadrado módulo unidad (es decir, es un producto de un cuadrado y una unidad). Además, es fácil ver que $1+i$ y $1-i$ son irreducibles asociados.

Veamos ahora el caso de p primo impar:

• Si $p \equiv 1 \mod 4$, vimos en el ejercicio 1 que $p = a^2+b^2$, con $a,b \in \mathbb{Z}$, por tanto $p = N(a+bi) = N(a-bi)$, y tenemos 2 nuevos primos, $a+bi$ y $a-bi$. Si intentamos que p sea cuadrado módulo unidad tendríamos $a-bi = \mu(a+bi)$ siendo μ unidad. Haciendo casos podemos ver que p no sería primo. Por tanto p no es cuadrado módulo unidad. Además, $a+bi$ y $a-bi$ son salvo unidad los únicos primos de módulo p, ya que si hubiera otro $c+di$ tendríamos $p = (c+di)(c-di)$, y por factorización única $c+di$ sería asociado a $a+bi$ o a $a-bi$.

• Si $p \equiv 3 \mod 4$, p es irreducible en $\mathbb{Z}[i]$, ya que si $p = ab$, tomando módulos tenemos que $|a|^2|b|^2 = p^2$, ergo $|a|^2 = p$, y como a no puede estar en $\mathbb{Z}$ esto contradice el ejercicio 1.

Con esto hemos hallado todos los ideales primos (o equivalentemente, maximales) de $\mathbb{Z}[i]$. Veamos cuántos elementos tienen los cuerpos residuales. Dado $n \in \mathbb{Z}$, $\frac{\mathbb{Z}[i]}{(n)}$ tiene n^2 elementos, ya que cada clase tiene un único

representante con parte real e imaginaria entre 0 y $n-1$. Por tanto si $p \equiv_4 3$, $\frac{\mathbb{Z}[i]}{(p)}$ es isomorfo a $\mathbb{F}_{p^2}$. Sea ahora $\pi \notin \mathbb{Z}$ irreducible en $\mathbb{Z}[i]$, con $|\pi|^2 = p \equiv_4 1$, y consideremos $\frac{\mathbb{Z}[i]}{(\pi)}$. Tiene característica p pues $p \cdot \overline{1} = \overline{\pi}(\pi\overline{1}) = \overline{0}$.

Como $p = \pi\overline{\pi}$ y $(\pi, \overline{\pi}) = 1$, se puede aplicar el teorema chino del resto:

$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[i]}{(\pi)} \times \frac{\mathbb{Z}[i]}{(\overline{\pi})}$$

Así que, como $\frac{\mathbb{Z}[i]}{(p)}$ tiene p^2 elementos y $\frac{\mathbb{Z}[i]}{(\pi)}$, $\frac{\mathbb{Z}[i]}{(\overline{\pi})}$ no son triviales, $\frac{\mathbb{Z}[i]}{(\pi)}$ tiene p elementos.

Si tomamos $\frac{\mathbb{Z}[i]}{(1+i)}$ se tienen 2 elementos, los $a+bi$ con $a+b$ impar y los que tienen $a+b$ par.

2.2.2 $\mathbb{Z}[\sqrt{-2}]$

De forma similar al caso de $\mathbb{Z}[i]$, (donde antes usábamos el ejercicio 1, ahora usamos el ejercicio 3) se puede comprobar que hay dos tipos de primos en $\mathbb{Z}[\sqrt{-2}]$: Los p primos en $\mathbb{Z}$ con $p \equiv_8 5$ ó 7, y los elementos de la forma $a+bi$, con a^2+2b^2 un primo p de $\mathbb{Z}$ que es 2 o que es 1 ó 3 módulo 8. En concreto, para cada p de esta forma hay 2 primos conjugados que lo dividen, y no son asociados (en $\mathbb{Z}[\sqrt{-2}]$, dos números son asociados si son iguales u opuestos).

2.3 Descenso infinito. Caso $n = 4$ del Último Teorema de Fermat

Recordemos el Último Teorema de Fermat, que dice que no hay soluciones enteras no nulas a la siguiente ecuación si $n > 2$:

$$x^n + y^n = z^n$$

Este archiconocido teorema fue conjeturado por Fermat en 1637, y nadie lo consiguió demostrar hasta Andrew Wiles en 1995. Sin embargo, el caso $n = 4$, que es el más sencillo, sí que fue probado por Fermat. A continuación probamos una versión más general del caso $n = 4$, usando el método de descenso infinito:

Proposición 2.2. La ecuación $x^4 + y^4 = z^2$ no tiene soluciones enteras con $xyz \neq 0$.

Demostración. Vamos a usar para probar esto el método de descenso infinito. En este caso, probaremos que para cada solución (x, y, z) de la ecuación, hay una solución (c, d, a) con $cda \neq 0$ 'más pequeña que (x, y, z)', en concreto, con $|a| < |z|$. Esto implica que no hay soluciones, ya que si hubiera una solución (x_0, y_0, z_0), podríamos crear a partir de ella una sucesión de soluciones (x_n, y_n, z_n) con z_n no nula de forma que $|z_{n+1}| < |z_n|$. Esto es absurdo, ya que $|z_n|$ sería una sucesión decreciente de enteros positivos no nulos, lo cual no puede existir.

Sea entonces (x, y, z) una solución. Podemos suponer $x, y, z > 0$, cambiándolos por sus opuestos si no. Si hay un primo p que divide a x, y y z, entonces p^4 divide a z^2, ergo p^2 divide a z y entonces $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ es una solución más pequeña. Supongamos entonces $(x, y, z) = 1$.

x, y no pueden ser impares, ya que entonces, tomando módulo 4, $z^2 \equiv_4 2$. Por tanto podemos suponer que x es impar e y es par. Ahora bien, como tenemos la terna pitagórica $(x^2)^2 + (y^2)^2 = z^2$, con x impar, por lo visto en el ejercicio 5 podemos encontrar m, n enteros tales que:

$$x^2 = m^2 - n^2, y^2 = 2mn, z = m^2 + n^2.$$

m, n tendrán que ser coprimos, y no pueden ser ambos impares. Pero entonces, como tenemos $x^2 + n^2 = m^2$, tenemos otra terna pitagórica, de modo que hay r, s enteros tales que:

$$x = r^2 - s^2, n = 2rs, m = r^2 + s^2$$

Como m, n son coprimos, r, s serán coprimos, y como $m = r^2 + s^2$, m también será coprimo con ellos. De modo que, como r, s, m son coprimos y $y^2 = 2mn = 4mrs$, m, r, s tendrán que ser cuadrados. Ergo, la ecuación $m = r^2 + s^2$ se transforma en una nueva solución de la ecuación inicial, con $|\sqrt{m}| \leq |m| < |z|$, como queríamos. □

Pasamos a intentar demostrar el caso $n = 3$ del último teorema de Fermat. Obviamente, la existencia de soluciones a $x^3+y^3 = z^3$ equivale a la existencia de soluciones a $x^3+y^3+z^3 = 0$. Para estudiar esta ecuación, hacemos un breve estudio de $\mathbb{Z}[\omega]$.

2.4 $\mathbb{Z}[\omega]$. El caso $n = 3$ del Último Teorema de Fermat

2.4.1 $\mathbb{Z}[\omega]$

Llamamos $\omega = \frac{-1+i\sqrt{3}}{2}$, una raíz cúbica primitiva de la unidad. Es raíz del polinomio $x^3 - 1$ y su polinomio mínimo sobre $\mathbb{Z}[x]$ es $\frac{x^3-1}{x-1} = x^2 + x + 1 = (x - \omega)(x - \overline{\omega})$. Por tanto por las fórmulas de Cardano-Vieta tenemos que $\omega\overline{\omega} = -(\omega + \overline{\omega}) = 1$.

Proposición 2.3. $\mathbb{Z}[\omega]$ es un dominio euclídeo con la función $\varphi(z) = |z|^2$.

Demostración. El cuerpo de fracciones de $\mathbb{Z}[\omega]$ es $\mathbb{Q}(\omega)$. Ahora, usando la proposición 2.1 vamos a ver que la función $\varphi(z) = |z|^2$ hace a $\mathbb{Z}[\omega]$ un dominio euclideo. Para esto primero vemos que si $a + b\omega \in \mathbb{Q}[\omega]$ (con $a, b \in \mathbb{Q}$), entonces $|a+b\omega|^2 = (a+b\omega)(a+b\overline{\omega}) = a^2-ab+b^2$ es racional .Si $a+b\omega \in \mathbb{Z}[\omega]$, entonces a^2-ab+b^2 es entero, y de hecho si a, b no son ambos nulos, es entero positivo, ya que $a^2 - ab + b^2 = \frac{3(a-b)^2+(a+b)^2}{4} > 0$. Además, está claro que la función φ es multiplicativa, así que solo queda la última propiedad de 2.1.

Dado $a + b\omega \in \mathbb{Q}[\omega]$, cogemos c, d a distancia $< \frac{1}{2}$ de a, b, y entonces, $\varphi((c + d\omega) - (a + b\omega)) = \varphi((c - a) + (d - b)\omega) = (c - a)^2 - (c - a)(d - b) + (d - b)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1$. □

Las unidades en $\mathbb{Z}[\omega]$ serán $1, -1, \omega, -\omega, \omega^2, -\omega^2$. No puede haber más porque estos son los únicos elementos de módulo 1 de $\mathbb{Z}[\omega]$, y la igualdad $\omega \cdot \omega^2 = 1$ prueba que todos ellos son unidades. Forman un grupo multiplicativo cíclico de orden 6, generado por $-\omega$ (de hecho, son las raíces sextas de la unidad en $\mathbb{C}$).

Ahora, sea $\lambda = 1 - \omega$. Necesitaremos algunas propiedades de este número. Primero, $\lambda^2 = 1 + \omega^2 - 2\omega = 1 + \omega + \omega^2 - 3\omega = -3\omega$. Es decir, λ^2 es 3 salvo unidades. Además, $|\lambda| = 3$, así que λ es irreducible. Por lo dicho, tenemos que $(3) \subsetneq (\lambda) \subsetneq \mathbb{Z}[\omega]$, ergo el orden del cuerpo $\mathbb{Z}[\omega]/(\lambda)$ será un divisor propio del orden de $\mathbb{Z}[\omega]/(3)$, que es 9. Por tanto, el orden de $\mathbb{Z}[\omega]/(\lambda)$ es 3, es decir, ese cuerpo es isomorfo a $\mathbb{F}_3$. 0, 1 y -1 son representantes de los 3 elementos de este cuerpo.

2.4.2 El caso $n = 3$

La ecuación $x^3+y^3+z^3 = 0$ equivale a $-z^3 = (x^3+y^3)$. x^3+y^3 factoriza como $(x+y)(x+\omega y)(x+\omega^2 y)$. Para ver esto, vemos que $x^3 + y^3 = y^3\left(\frac{x^3}{y^3} + 1\right)$, y como $s^3 + 1 = (s + 1)(s + \omega)(s + \omega^2)$, tenemos $y^3\left(\frac{x^3}{y^3} + 1\right) = y^3\left(\frac{x}{y} + 1\right)\left(\frac{x}{y} + \omega\right)\left(\frac{x}{y} + \omega^2\right) = (x + y)(x + \omega y)(x + \omega^2 y)$. Por tanto, nuestra ecuación es:

$$-z^3 = (x + y)(x + \omega y)(x + \omega^2 y)$$

Para seguir necesitamos un lema:

Lema 2.4. Sea $\lambda = 1 - \omega$. Entonces, si $\alpha \equiv 1 \mod \lambda$, entonces $\alpha^3 \equiv 1 \mod \lambda^4$. También, si $\alpha \equiv -1 \mod \lambda$, $\alpha^3 \equiv -1 \mod \lambda^4$.

Demostración. Primero supongamos $\alpha \equiv 1 \mod \lambda$. Sea β tal que $\lambda\beta = \alpha - 1$. Entonces, $\alpha^3 - 1 = (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2) = (\alpha-1)(\alpha-1+(1-\omega))(\alpha-1+(1-\omega^2)) = (\lambda\beta)(\lambda(\beta+1))(\lambda(\beta+(1+\omega))) = \lambda^3\beta(\beta+1)(\beta+1+\omega)$. Basta entonces ver que $\beta(\beta + 1)(\beta + 1 + \omega)$ es múltiplo de λ. Pero, como $1, \omega$ y $1 + \omega$ no están en (λ) por ser unidades, los números $\beta, \beta + 1, \beta + 1 + \omega$ son representantes de clases distintas de $\mathbb{Z}[\omega]/(\lambda)$. Como este cuerpo solo tiene tres clases, uno de esos tres números estará en (λ), por tanto $\beta(\beta + 1)(\beta + 1 + \omega)$ es múltiplo de λ.

Para la segunda parte, si $\alpha \equiv -1 \mod \lambda$, entonces en módulo λ^4, usando la primera parte del lema tenemos que $\alpha^3 \equiv -(-\alpha)^3 \equiv -1$. □

Teorema 2.5. Dados $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ tales que

$$\alpha^3 + \beta^3 + \gamma^3 = 0,$$

se tiene que $\alpha\beta\gamma = 0$.

Demostración. Como la ecuación cúbica es homogénea, podemos suponer $(\alpha, \beta, \gamma) = 1$, y por tanto $(\alpha, \beta) = (\beta, \gamma) = (\gamma, \alpha) = 1$. Esto es porque toda solución es un múltiplo de una solución de este tipo (reducida en $\mathbb{Z}$), ya que si en una solución, (α, β, γ) es d no unidad, entonces $\left(\frac{\alpha}{d}, \frac{\beta}{d}, \frac{\gamma}{d}\right)$ es una solución reducida. los elementos del ideal generado por esta también son soluciones y si suponemos que $\text{mcd}(\alpha, \beta) \neq 1$, entonces $\text{mcd}(\alpha, \beta)|\gamma$.
Se divide la demostración en dos casos. Sea $\lambda := 1 - \omega$ y supongamos que $\lambda \nmid \alpha\beta\gamma$:
Entonces $\alpha, \beta, \gamma \equiv \pm 1 \mod \lambda \Rightarrow \alpha^3, \beta^3, \gamma^3 \equiv \pm 1 \mod \lambda^4$ por el lema. Sustituimos arriba para obtener

$$0 \equiv_{\lambda^4} \pm 1 \pm 1 \pm 1 = \pm 3, \pm 1$$

Pero $\pm 1, \pm 3$ no son 0 módulo λ^4, ya que no son múltiplos en $\mathbb{Z}[\omega]$ de 9, que es asociado de λ^4. Por tanto, $\lambda \nmid \alpha\beta\gamma$ no puede darse.

Supongamos entonces que $\lambda|\alpha\beta\gamma$. Como seguimos suponiendo que α, β, γ sean coprimos dos a dos, suponemos sin pérdida de generalidad que $\lambda|\gamma,\ \lambda \nmid \alpha,\ \lambda \nmid \beta$.
Sea $n \in \mathbb{N}$ y $\delta \in \mathbb{Z}[\omega]$ tales que $\gamma = \lambda^n \delta$ y $\lambda \nmid \delta$.
Reescribimos la ecuación:

$$\alpha^3 + \beta^3 + \lambda^{3n}\delta^3 = 0$$

con $\lambda \nmid \alpha\beta\delta$ y

$$\text{mcd}(\alpha, \beta) = \text{mcd}(\beta, \delta) = \text{mcd}(\delta, \alpha) = 1.$$

De esta forma, (α, β, δ) es solución reducida en $\mathbb{Z}[\omega]$ de la ecuación

$$x^3 + y^3 + \lambda^{3n} z^3 = 0,\ n \in \mathbb{N}.$$

Esta ecuación es un caso particular de

$$E_{\varepsilon,n} :\ x^3 + y^3 + \varepsilon\lambda^{3n} z^3 = 0,\ \varepsilon \in \mathbb{Z}[\omega]^\times,\ n \in \mathbb{N}$$

con $\varepsilon = 1$, veamos qué sucede con este tipo de ecuaciones. A continuación vamos a comprobar dos cosas:
En primer lugar, si $E_{\varepsilon,n}$ tiene una solución reducida, entonces $n \geq 2$.
En segundo lugar, si $E_{\varepsilon,n}$ tiene una solución reducida, entonces $\exists \varepsilon_1 \in \mathbb{Z}[\omega]^\times$ tal que $E_{\varepsilon_1,n-1}$ tiene solución reducida.
Conocidos estos dos hechos, un argumento de descenso nos dice que las $E_{\varepsilon,n}$ no tendrán soluciones.

Veamos que $n \geq 2$, supongamos que tenemos α, β, γ solución reducida en $\mathbb{Z}[\omega]$ de $E_{\varepsilon,n}$:

$$-\varepsilon\lambda^{3n}\delta^3 = \alpha^3 + \beta^3 \equiv_{\lambda^4} \pm 1 \pm 1 = 0, \pm 2.$$

Como $n \geq 1$ se tiene que $\varepsilon\lambda^{3n}\delta^3 \equiv_{\lambda^3} 0$. Como $\pm 2 \not\equiv 0 \mod \lambda$ la única opción es que $\alpha^3 + \beta^3 \equiv_{\lambda^4} = 0$. Como ε es unidad, no lo divide λ. Por hipótesis $\lambda \nmid \delta$ luego $\lambda^4|\lambda^{3n} \Rightarrow\ n \geq 2$.

Sea α, β, γ solución reducida en $\mathbb{Z}[\omega]$ de $E_{\varepsilon,n}$:

$$\alpha^3 + \beta^3 + \varepsilon\lambda^{3n}\delta^3 = 0.$$

Nos fijamos en que $1 \equiv_\lambda \omega \equiv_\lambda \omega^2$, ergo:

$$\alpha + \beta \equiv_\lambda \alpha + \omega\beta \equiv_\lambda \alpha + \omega^2\beta \Rightarrow\ -\varepsilon\lambda^{3n}\delta^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega^2\beta) \equiv_\lambda (\alpha + \beta)^3$$

Como λ divide a $-\varepsilon\lambda^{3n}\delta^3$, debe dividir a alguno de los factores $\alpha+\beta, \alpha+\omega\beta, \alpha+\omega^2\beta$. Como son congruentes módulo λ divide a los tres, luego

$$\frac{\alpha+\beta}{\lambda}, \frac{\alpha+\omega\beta}{\lambda}, \frac{\alpha+\omega^2\beta}{\lambda} \in \mathbb{Z}[\omega]$$

Veamos que estos tres elementos son coprimos dos a dos.
Sea $\pi \in \mathbb{Z}[\omega]$ irreducible y supongamos que $\pi|\frac{\alpha+\beta}{\lambda}, \frac{\alpha+\omega\beta}{\lambda}$. Entonces $\lambda\pi|\alpha+\beta, \alpha+\omega\beta$ luego $\lambda\pi|\alpha+\beta-(\alpha+\omega\beta) = \lambda\beta$ y $\lambda\pi|\omega(\alpha+\beta)-(\alpha+\omega\beta) = -\lambda\alpha$. Se tiene que $\pi|\alpha, \beta$ pero $\text{mcd}(\alpha,\beta) = 1$. Absurdo. El razonamiento para ver que

$$\text{mcd}\left(\frac{\alpha+\omega\beta}{\lambda}, \frac{\alpha+\omega^2\beta}{\lambda}\right) = \text{mcd}\left(\frac{\alpha+\omega^2\beta}{\lambda}, \frac{\alpha+\omega\beta}{\lambda}\right) = 1$$

es igual. Resumiendo, tenemos que $\alpha+\beta, \alpha+\omega\beta, \alpha+\omega^2\beta$ no tienen factores primos aparte de λ y su producto es $-\varepsilon\lambda^{3n}\delta^3$. Supongamos que λ divide a $\frac{\alpha+\beta}{\lambda}$, y por tanto no a $\frac{\alpha+\omega\beta}{\lambda}, \frac{\alpha+\omega^2\beta}{\lambda}$ (podemos suponerlo porque si no cambiamos β por $\omega\beta$ o $\omega^2\beta$ en la ecuación). Entonces, por lo dicho, tendremos $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}[\omega]$ no múltiplos de λ y u_1, u_2, u_3 unidades tales que

$$\alpha+\beta = u_1\lambda^{3n-2}\alpha_1^3, \quad \alpha+\omega\beta = u_2\lambda\alpha_2^3 \quad \alpha+\omega^2\beta = u_3\lambda\alpha_3^3$$

$$-\varepsilon\lambda^{3n}\delta^3 = (\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta) = u_1\lambda^{3n-2}\alpha_1^3 u_2\lambda\alpha_2^3 u_3\lambda\alpha_3^3$$

y tendremos que $\text{mcd}(\alpha_1,\alpha_2) = \text{mcd}(\alpha_2,\alpha_3) = \text{mcd}(\alpha_3,\alpha_1) = 1$, por ser $\frac{\alpha+\beta}{\lambda}, \frac{\alpha+\omega\beta}{\lambda}, \frac{\alpha+\omega^2\beta}{\lambda}$ coprimos.
Ahora nos fijamos en que

$$0 = (\alpha+\beta) + \omega(\alpha+\omega\beta) + \omega^2(\alpha+\omega^2\beta) =$$

$$u_1\lambda^{3n-2}\alpha_1^3 + \omega u_2\lambda\alpha_2^3 + \omega^2 u_3\lambda\alpha_3^3 = \lambda(u_1\alpha_1^3\lambda^{3(n-1)} + \omega u_2\alpha_2^3 + \omega^2 u_3\alpha_3^3).$$

$\lambda \neq 0$ y $\omega u_2 \in \mathbb{Z}[\omega]^\times$ así que multiplicamos por su inverso:

$$0 = \omega^2 u_2^{-1}u_1\alpha_1^3\lambda^{3(n-1)} + \alpha_2^3 + \omega u_2^{-1}u_3\alpha_3^3 = \varepsilon_1\alpha_1^3\lambda^{3(n-1)} + \alpha_2^3 + u_4\alpha_3^3.$$

Donde hemos denotado $\varepsilon_1 := \omega^2 u_2^{-1}u_1,\ u_4 := \omega u_2^{-1}u_3$.

$$0 = \varepsilon_1\alpha_1^3\lambda^{3(n-1)} + \alpha_2^3 + u_4\alpha_3^3 \equiv_{\lambda^3} \alpha_2^3 + u_4\alpha_3^3 \equiv_{\lambda^3} \pm 1 + u_4 \cdot (\pm 1)$$

Donde hemos usado el lema 2.4 y que $\alpha_1, \alpha_2 \equiv_\lambda \pm 1$. Esto obliga a que u_4 sea ± 1 pues si no, $\pm 1 \pm u_4 \not\equiv_{\lambda^2} 0$. Suponemos que u_4 es 1 pues si fuese -1 cambiamos α_3 por $-\alpha_3$ y ya es $u_4 = 1$. Entonces se tiene que

$$0 = \varepsilon_1\alpha_1^3\lambda^{3(n-1)} + \alpha_2^3 + \alpha_3^3$$

es una solución de $E_{\varepsilon_1,n-1}$, como queríamos.

□

Intentar generalizar este argumento a exponentes primos superiores no es viable pues estamos haciendo un uso excesivo de las unidades, que en este caso son pocas.

Ejercicios Ver soluciones de $x^3+y^3 = 2z^3$. (Las triviales son con $x = \pm y$). Una solución se puede encontrar en [2], página 79.
Ver soluciones de $x^3+y^3 = 3z^3$. (Las triviales son $\alpha^3+\beta^3 = \gamma^3 = 0$.). Una solución se puede encontrar en el apartado 13.5 de [3].

2.5 Algunos problemas resueltos

Problema 2.1. Dado p primo, ver que $p = a^2+b^2$ si y solo si $p = 1, 2 \mod 4$.

Solución. Si $p = a^2+b^2$, tomamos módulo 4. Entonces, como solo 0 y 1 son residuos cuadráticos módulo 4. a^2 y b^2 pueden ser 0 o 1 luego p podría ser $0, 1$ o 2. No obstante, si fuese 0 no sería primo.
Ahora supongamos que $p \equiv 1, 2 \mod 4$.

Si $p \equiv 2 \mod 4$, p es primo luego debe ser 2.
Así que $a = b = 1$ cumplen que $a^2 + b^2 \equiv 2 \mod 4$.
Por otro lado, si $p \equiv 1 \mod 4$, entonces $(-1)^{\frac{p-1}{2}} = 1$ así que $\left(\frac{-1}{p}\right) = 1$.
Es decir, existe $a \in \mathbb{Z} : \ p|a^2 + 1 = (a+i)(a-i) \in \mathbb{Z}[i]$.
p no divide a $a+i$ ni a $a-i$ así que p no es primo. Como estamos en un DFU tampoco es irreducible, así que $\exists (a_1 + b_1 i), (a_2 + b_2 i) \in \mathbb{Z}[i]$ no unidades tales que

$$p = (a_1 + b_1 i)(a_2 + b_2 i) \Rightarrow \ p^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2).$$

Como no son unidades sus módulos no son uno así que $a_1^2 + b_1^2 = p$. □

Problema 2.2. Sea $p \in \mathbb{N}$ primo impar, demostrar que $-4 \equiv_p x^4$ para algún x si y solo si $p \equiv_4 1$.

Solución. $\Longrightarrow$: Si $-4 \equiv_p x^4$ para algún x, entonces $-4 \equiv_p (x^2)^2$, es decir, -4 es un residuo cuadrático módulo p, por tanto $p \equiv_4 1$.

$\Longleftarrow$: Suponemos $p \equiv_4 1$. Vamos a usar el siguiente lema:

Sea $p \equiv_1 4$, entonces $a \equiv_p x^4$ para algún x si y solo si $a^{\frac{p-1}{4}} \equiv_p 1$.

Para probar el lema trabajaremos en $\mathbb{Z}_p$. Entonces, si $\overline{a} = x^4$ para cierto x, entonces $\overline{a}^{\frac{p-1}{4}} = x^{p-1} = 1$. Recíprocamente, supongamos que $\overline{a}^{\frac{p-1}{4}} = 1$. Sea g un generador del grupo cíclico de $\mathbb{Z}_p$ y $m \in \mathbb{Z}$ tal que a es de la forma g^m. Entonces $a^{\frac{p-1}{4}} = g^{m\frac{p-1}{4}} = 1$, por tanto como el orden de g es $p-1$, tenemos que $p-1 | m\frac{p-1}{4}$. Es decir, m es múltiplo de 4, es decir, hay m_1 con $m = 4m_1$. Por tanto $a = (g^{m_1})^4$, como queríamos.

Ahora, usando el lema con $a = -4$, solo tenemos que comprobar que $(-4)^{\frac{p-1}{4}} = 1$. Pero $(-4)^{\frac{p-1}{4}} = 2^{\frac{p-1}{2}}(-1)^{\frac{p-1}{4}} = \left(\frac{2}{p}\right)(-1)^{\frac{p-1}{4}}$. Para comprobar que esto es 1, dividimos en casos en módulo 8. Como $p \equiv_4 1$, solo hay dos casos:

- $p \equiv_8 1$. En este caso, $\frac{p-1}{4}$ es par, y usando la segunda ley suplementaria, $\left(\frac{2}{p}\right)(-1)^{\frac{p-1}{4}} = 1 \cdot 1 = 1$.
- $p \equiv_8 5$. En este caso, $\frac{p-1}{4}$ es impar, y por la $2^{\underline{a}}$ ley suplementaria, $\left(\frac{2}{p}\right)(-1)^{\frac{p-1}{4}} = (-1) \cdot (-1) = 1$.

□

Problema 2.3. Sea $p \in \mathbb{N}$ primo impar, demostrar que -2 es residuo cuadrático módulo p si y solo si p se puede expresar como $a^2 + 2b^2$, con $a, b \in \mathbb{Z}$.

Solución. $\Longleftarrow$: Si $a^2 + 2b^2 = p$, b no puede ser múltiplo de p, ya que entonces o bien $b = 0$, y $a^2 = p$, lo cual es imposible, o bien $|b| \geq p$, ergo $a^2 + 2b^2 > p$.

Ahora, pasando a $\mathbb{Z}_p$, tenemos que $\overline{a}^2 = -2\overline{b}^2$. Por tanto $-2 = \frac{\overline{a}^2}{\overline{b}^2} = \left(\frac{\overline{a}}{\overline{b}}\right)$, es decir, -2 es residuo cuadrático.

$\Longrightarrow$: Para esta implicación usaremos algo que veremos en breve: que $\mathbb{Z}[\sqrt{-2}]$ es un DFU. Si -2 es residuo cuadrático módulo p, existe $a \in \mathbb{Z}$ con $p|a^2 + 2$. Es decir, en $\mathbb{Z}[\sqrt{-2}]$, $p|(a + \sqrt{-2})(a - \sqrt{-2})$. Sin embargo, en $Z[\sqrt{-2}]$, p no divide a $a + \sqrt{-2}$ ni a $a - \sqrt{-2}$, ya que los múltiplos de p son de la forma $k_1 p + k_2 p\sqrt{-2}$, con $k_1, k_2 \in \mathbb{Z}$. Ergo, p no puede ser un primo en $\mathbb{Z}[\sqrt{-2}]$. Como $\mathbb{Z}[\sqrt{-2}]$ es un DFU, p no es irreducible en $\mathbb{Z}[\sqrt{-2}]$. Ergo, podemos escribir $p = (a_1 + b_1\sqrt{-2})(a_2 + b_2\sqrt{-2})$. Tomando módulos al cuadrado en la igualdad anterior, tenemos que $p^2 = (a_1^2 + 2b_1^2)(a_2^2 + 2b_2^2)$. Como $a_1 + b_1\sqrt{-2}$ y $a_2 + b_2\sqrt{-2}$ no son unidades, tenemos que $a_1^2 + 2b_1^2$ y $a_2^2 + 2b_2^2$ son enteros > 1, por tanto serán p. Es decir, $a_1^2 + 2b_1^2 = p$.

Con las herramientas que tenemos, no es difícil comprobar que -2 será residuo cuadrático módulo p cuando p sea 1 ó 3 módulo 8. Por tanto será entonces cuando p se pueda escribir como $a^2 + 2b^2$.

□

Generalización de los problemas 1 y 3

Sea p primo y sea $k \in \mathbb{N}$ tal que $\mathbb{Z}[\sqrt{-k}]$ es DFU. Entonces existen $x, y \in \mathbb{Z} :\ p = x^2 + ky^2 \Leftrightarrow \left(\frac{-2}{p}\right) = 1$.

Para la implicación de izquierda a derecha tomamos módulo p y dividimos por y^2 (que no es múltiplo de p).
Para la de derecha a izquierda:
Sabemos que $\exists a \in \mathbb{Z} :\ p | a^2 + k = (a + \sqrt{-k})(a - \sqrt{-k})$.
Como $p \nmid a + \sqrt{-k}, a - \sqrt{-k}$ no es primo en $\mathbb{Z}\sqrt{-k}$, tampoco es irreducible así que existen $(a_1 + b_1\sqrt{-k}), (a_2 + b_2\sqrt{-k})$ no unidades tales que

$$p = (a_1 + b_1\sqrt{-k})(a_2 + b_2\sqrt{-k}) \Rightarrow p^2 = (a_1^2 + kb_1^2)(a_2^2 + kb_2^2)$$

Luego $p = a_1^2 + kb_1^2$, ya que si un número $\alpha \in \mathbb{Z}[\sqrt{-k}]$, con $k \geq 2$, cumple $|\alpha| = 1$, el número es 1 o -1, ergo es una unidad.

Problema 2.4. Estudiar la solubilidad en enteros de

$$x^2 + y^2 = z^2,$$

usando a ser posible los enteros de Gauss.

Solución. Nos comenzamos fijando en que si $a^2 + b^2 = c^2$ se cumple para ciertos valores $a, b, c \in \mathbb{Z}$ entonces ak, bk, ck es también solución con $k \in \mathbb{Z}$. Supongamos entonces que no hay primos que dividan a a, b, c a la vez. No obstante, si un primo dividiese a 2 de ellos tiene que dividir al tercero luego suponemos sin pérdida de generalidad que

$$\text{mcd}(x, y) = \text{mcd}(y, z) = \text{mcd}(z, x) = 1$$

Si tomamos módulo 4 vemos, sin pérdida de generalidad, que $a \equiv_4 c \equiv_4 1,\ b \equiv_4 0$. Escribimos $z = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, sabemos que un primo $p > 2$ es irreducible en $\mathbb{Z}[i]$ si y solo si $p \equiv 3 \mod 4$. Se tiene por otro lado que

$$z^2 = x^2 + y^2 = (x + iy)(x - iy)$$

Si $\exists j = 1, \dots r$ tal que $p_j \equiv_4 3$, entonces p_j divide a $x + iy$ o a $x - iy$, en cualquier caso p_j divide a x y a y luego la hipótesis de que x, y, z son coprimos entre sí no se daría.
Así que $\forall j = 1, \dots r$ se tiene que $p_j \equiv_4 1$, pero entonces $\exists a_j, b_j \in \mathbb{Z} :\ p_j = (a_j + ib_j)(a_j - ib_j)$:

$$(x + iy)(x - iy) = \prod_{j=1}^{r} (a_j + ib_j)^{2\alpha_j} (a_j - ib_j)^{2\alpha_j}$$

Si $a_j + ib_j | x + iy$ entonces $a_j - ib_j | x - iy$. Con esta idea y tomando el signo de los b_j de tal forma que

$$x + iy = \prod_{j=1}^{r} (a_j + ib_j)^{2\alpha_j}.$$

Luego $x + iy$ es un cuadrado, $x - iy$ también.
Existen $u, v \in \mathbb{Z} :\ x + iy = (u + iv)^2 = u^2 - v^2 + 2iuv$.
$x = u^2 - v^2$ e $y = 2uv$. Nos fijamos en que

$$u^2 + v^2 = |z|^2 = |u + iv|^2 = \left|(u + iv)^2\right| = |u^2 - v^2 + 2iuv| = (u^2 - v^2)^2 + (2uv)^2.$$

Así que $z = u^2 + v^2$. Dada una terna "reducida" siempre podremos encontrar $u, v \in \mathbb{Z}$ que nos permita generarla. Además, dados u, v cualqesquiera siempre generan una terna.
Mencionar que hemos supuesto que y es par y que también están las no reducidas:

$$x = k(u^2 - v^2), \quad y = 4kuv, \quad z = k(u^2 + v^2)$$

□

Problema 2.5. Sacar todas las soluciones enteras de

$$x^3 - 1 = y^2$$

Como pista usar el dominio euclídeo $\mathbb{Z}[i]$.

Solución. En primer lugar escribimos

$$x^3 = y^2 + 1 = (y+i)(y-i)$$

Si $p = 4k+3$ primo, es primo en los enteros de Gauss y $p \nmid 1$.
Si $p = 4k+1$ primo, entonces $p = (a+bi)(a-bi)$, si divide a ambos factores, $a+bi|y+i \Rightarrow a-bi|y-i$ luego $p = (a-bi)(a+bi)|y-1$ y $p \nmid 1$.
Para el caso $p = 2$ tomamos módulo 8 y hacemos casos.
Deducimos que $y+i, y-i$ son coprimos así que ambos deben ser cubos, en particular el primero:

$$y + i = (\alpha + \beta i)^3 = \alpha^3 - 3\alpha\beta^2 + (3\alpha^2\beta - \beta^3)i \Rightarrow \ 1 = 3\alpha^2\beta - \beta^3 = \beta(3\alpha^2 - \beta^2)$$

Como trabajamos en enteros, se tienen dos casos: $\beta = 3\alpha^2 - \beta^2 = 1$ ó $\beta = 3\alpha^2 - \beta^2 = -1$.
En el primero llegamos a un absurdo mientras que en el segundo se tiene que $\alpha = 0$. Esto nos lleva a que $y + i = (-i)^3 = i \Rightarrow y = 0, x = 1$.

□

Problema 2.6. Sacar todas las soluciones enteras de

$$x^3 - 2 = y^2$$

usando el dominio $\mathbb{Z}[\sqrt{-2}]$.

Solución. La ecuación equivale a $x^3 = (y+\sqrt{-2})(y-\sqrt{-2})$. Vamos a ver ahora que $y+\sqrt{-2}$ e $y-\sqrt{-2}$ son coprimos. Si no lo fueran, tendríamos un primo p que dividiría a ambos, y por tanto a su diferencia, $2\sqrt{-2}$. Pero $\sqrt{-2}$ es primo, y es el único que divide a $2\sqrt{-2}$. Por tanto, podemos suponer $p = \sqrt{-2}$. Ahora bien, si $\sqrt{-2}$ divide a $y+\sqrt{-2}$ y a $y+\sqrt{-2}$, entonces $2|x^3$. Esto es absurdo, ya que entonces, $8|x^3$, y tomando módulo 4 en la ecuación del enunciado, tendríamos $y^2 \equiv 2$.

Ergo, $y+\sqrt{-2}$ e $y-\sqrt{-2}$ son coprimos. Pero en la igualdad $x^3 = (y+\sqrt{-2})(y-\sqrt{-2})$, al factorizar en primos, todos los primos tienen que aparecer con exponente múltiplo de 3. Por tanto, en la factorización de $y+\sqrt{-2}$ los primos aparecerán con exponente múltiplo de 3, es decir, $y+\sqrt{-2}$ es un cubo salvo unidades (± 1). Como el opuesto de un cubo es un cubo, $y+\sqrt{-2}$ es un cubo: $y+\sqrt{-2} = (a+b\sqrt{-2})^3$, para ciertos $a, b \in \mathbb{Z}$. Igualando partes imaginarias, $3a^2b - 2b^3 = 1$. Por tanto b es 1 o -1. Si $b = 1$, queda $3a^2 = 3$, es decir, $a = \pm 1$, en cuyo caso $y = a^3 - 6ab^2 = \pm 5$, y despejamos $x = 3$. Si $b = -1$, queda $-3a^2 = -1$, que no tiene soluciones enteras.

Ergo, las únicas soluciones a esta ecuación son $x = 3, y = \pm 5$. □

Problema 2.7. Sacar todas las soluciones enteras de $x^3 - 4 = y^2$ usando el dominio $\mathbb{Z}[i]$.

Solución. La ecuación equivale a $x^3 = (y+2i)(y-2i)$. Igual que en el ejercicio anterior, veamos qué factores comparten $y+2i$ e $y-2i$. Si un primo p divide a $y+2i$ y a $y-2i$, entonces divide a su diferencia, 4, ergo el único primo que dividirá a ambos será $1+i$. Podemos escribir entonces $y+2i = (1+i)^\gamma \prod p_i^{\alpha_i}$, y tendremos que $y-2i = (1-i)^\gamma \prod_i \overline{p_i}^{\alpha_i} = i^{-\gamma}(1+i)^\gamma \prod_i \overline{p_i}^{\alpha_i}$. Por tanto, x^3 es, salvo unidades, $(1+i)^{2\gamma} \prod_i p_i^{\alpha_i} \overline{p_i}^{\alpha_i}$. Ergo, α_i y γ son todos múltiplos de 3, al ser todos los p_i y $\overline{p_i}$ distintos.

Por tanto $y+2i$ es un cubo o un cubo por una unidad. Como toda unidad es un cubo en $\mathbb{Z}[i]$, tenemos que $y+2i$ es un cubo, $y+2i = (a+bi)^3$, con $a, b \in \mathbb{Z}$. Igualando partes imaginarias, $2 = 3a^2b - b^3$. Hay cuatro casos posibles para b, $1, -1, 2, -2$. Las soluciones para (a, b) que obtenemos son $(\pm 1, 1)$, $(\pm 1, -2)$. Esto da lugar, usando $y = a^3 - 3ab^2$ a los valores de y $\pm 2, \pm 11$. Obtenemos así las soluciones $(2, \pm 2)$ y $(5, \pm 11)$. □

Capítulo 3

Reciprocidad cúbica

3.1 $\mathbb{Z}[\omega]$ revisitado

Irreducibles en $\mathbb{Z}[\omega]$ Sea $\pi \in \mathbb{Z}[\omega]$ irreducible, entonces $N(\pi) = \pi\overline{\pi} = p_1 \dots p_t \in \mathbb{Z}$, luego π divide a algún p primo en $\mathbb{Z}$:

$$\pi | p \Rightarrow \ N(\pi) | N(p) = p^2.$$

Tenemos dos posibilidades, que $N(\pi) = p$ ó que $N(\pi) = p^2$.
En el primer caso se tiene que $p = \pi\overline{\pi}$ y $\pi, \overline{\pi}$ no son asociados. Esto se ve tomando $\pi = a + b\omega$, tomando $\overline{\pi} = \pm 1, \pm\omega, \pm\omega^2 \cdot \pi$, y sustituyendo en $p = \pi\overline{\pi}$.
En el segundo caso, $\pi | p$ luego $p = \pi\alpha$ así que $p^2 = N(\pi)N(\alpha) = p^2 N(\alpha)$ luego $N(\alpha) = 1$ y es unidad. En este caso p y π son asociados y p irreducible en $\mathbb{Z}[\omega]$. El 3 cumple que $3 = (-\omega^2)\lambda^2$.

Al igual que vimos en $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{-2}]$, vamos a ver quiénes primos de $\mathbb{Z}[\omega]$. Para ello valdrá ver los divisores primos de todos los primos enteros distintos de 3.

Proposición 3.1. Sea $p \in \mathbb{Z}$ primo. Entonces, si $p \equiv_3 2$, es primo en $\mathbb{Z}[\omega]$. Si $p \equiv_3 1$, p es producto de dos primos no asociados en $\mathbb{Z}[\omega]$.

Demostración. Si $p \equiv_3 2$, entonces no puede haber ningún primo de norma p. Esto pasa porque dado cualquier $a + b\omega$, su norma será $a^2 - ab + b^2 \equiv_3 (a + b)^2 \not\equiv_3 2$, ergo no puede haber números de norma p en $\mathbb{Z}[\omega]$. Por tanto, por la anterior discusión, p es irreducible.

Si $p \equiv_3 1$, entonces podemos comprobar usando reciprocidad que $\left(\dfrac{-3}{p}\right) = 1$,[1] ergo hay $a \in \mathbb{Z}$ con $p | a^2 + 3 = (a + \sqrt{-3})(a - \sqrt{-3}) = ((a+1) + 2\omega)((a-1) - 2\omega)$, que no son múltiplos de p por tener coordenadas no múltiplo de p en la base $(1, \omega)$. Por tanto p no es primo, ergo no es irreducible, y por la discusión anterior p será producto de dos primos conjugados $\pi\overline{\pi}$. □

Ejemplo En el caso $p = 7$, sabemos que no va ser irreducible en $\mathbb{Z}[\omega]$. Queremos $(a, b) \in \mathbb{Z}$ tales que $7 = a^2 - ab + b^2 = (a - b)^2 + ab = |a + b\omega|$ Vemos que $(1, 3)$ y $(2, 3)$ son soluciones. Si multiplicamos $a + b\omega$ por unidades obtenemos más hasta un total de 12.
Esto tiene una interpretación geométrica curiosa, cuando trabajamos con los enteros de Eisenstein, estamos creando una malla triangular en el plano. La idea ahora es que si tomamos una circunfencia de centro 0 y radio $\sqrt{p}$, $p \equiv_3 1$ primo, cortará a 12 puntos de la malla. $\mathbb{Z}[\omega]$ es DFU y como p es producto de 2 primos no asociados salen 12 puntos en total.

Se les suele llamar primos inertes a los primos de $\mathbb{Z}$ que no descomponen como producto de 2 irreducibles.

Así pues, todo número de $\mathbb{Z}[\omega]$ se podrá expresar de la forma:

[1] $\left(\dfrac{-3}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\dfrac{p}{3}\right)(-1)^{\frac{p-1}{2}} = 1.$

$$\alpha = (-\omega)^{\varepsilon}\lambda^{a}\prod_{i=1}^{s} q_i^{a_i}\prod_{j=1}^{r}\pi_j^{b_j}$$

con $\varepsilon, a, a_i, b_j \in \mathbb{N}\cup\{0\}$ (ε se puede tomar entre 0 y 5 de forma única), $q_i \equiv_3 2$, $|\pi_j|^2 = p_j \equiv_3 1$ (π_j y $\overline{\pi_j}$ pueden aparecer por separado).

La norma de λ es 3, la de q_i es q_i^2 y la de π_j es p_i luego

$$a^2 - ab + b^2 = N(\alpha) = 3^a\prod_{i=1}^{s} q_i^{2a_i}\prod_{j=1}^{r} p_j^{b_j}$$

Así que los enteros de la forma $a^2 - ab + b^2$ deben cumplir que en su descomposición factorial, los primos de la forma $p \equiv_3 2$ deben tener exponente par.

Cuerpos residuales en $\mathbb{Z}[\omega]$

Sea π irreducible en $\mathbb{Z}[\omega]$. Veamos qué podemos decir del cuerpo $\frac{\mathbb{Z}[\omega]}{(\pi)}$. Primero veremos el caso de primos q enteros con $q \equiv_3 2$.

Tomemos $0 \neq m \in \mathbb{Z}$, entonces $\frac{\mathbb{Z}[\omega]}{(m)}$ tiene m^2 elementos, ya que cualquier $a + b\omega \in \mathbb{Z}[\omega]$ tiene un único representante de forma $mr' + s'\omega$, con r', s' entre 0 y $m-1$:

$$a + b\omega = (a'm + r') + (b'm + s')\omega = m(a' + b'\omega) + (r' + s'\omega) \equiv_m r' + s'\omega$$

Así que si tomamos $m = q$ primo con $q \equiv_3 2$ se tiene que

$$\frac{\mathbb{Z}[\omega]}{(q)} \approx \mathbb{F}_{q^2}.$$

Vamos al caso π irreducible en $\mathbb{Z}[\omega]$ con $N(\pi) = p \in \mathbb{Z}$ primo. Se tiene por el teorema chino del resto que:

$$\frac{\mathbb{Z}[\omega]}{(p)} \approx \frac{\mathbb{Z}[\omega]}{(\pi)} \times \frac{\mathbb{Z}[\omega]}{(\overline{\pi})}$$

El miembro izquierdo es un anillo y los de la derecha son cuerpos de al menos dos elementos. Por tanto cada cuerpo tiene p elementos:

$$\frac{\mathbb{Z}[\omega]}{(\pi)} \approx \frac{\mathbb{Z}[\omega]}{(\overline{\pi})} \approx \mathbb{F}_p$$

Podemos recordar que $\frac{\mathbb{Z}[\omega]}{(\lambda)} \approx \mathbb{F}_3$.

Dado $\pi \in \mathbb{Z}[\omega]$ irreducible con $\pi \neq \lambda$:

- Si $N(\pi)$ es primo en $\mathbb{Z}$, la norma es 1 módulo 3.
- Si $\pi \in \mathbb{Z}$ primo, entonces $\pi \equiv 2 \mod 3$ y $N(\pi) = \pi^2 \equiv 1 \mod 3$.

En general, $3|N(\pi) - 1$. Además, $N(\pi)$ es el cardinal del cuerpo que creamos al cocientar. Por tanto, 3 divide al orden del grupo multiplicativo:

$$3|N(\pi) - 1 = \left|\left(\frac{\mathbb{Z}[\omega]}{(\pi)}\right)^{\times}\right|$$

Así que dado $\alpha \in \mathbb{Z}[\omega],\ \pi \nmid \alpha$:

$$\alpha^{N(\pi)-1} \equiv 1 \mod \pi \Rightarrow\ \pi|\alpha^{N(\pi)-1} - 1 = \left(\alpha^{\frac{N(\pi)-1}{3}}\right)^3 - 1 =$$

$$\left(\alpha^{\frac{N(\pi)-1}{3}} - 1\right)\left(\alpha^{\frac{N(\pi)-1}{3}} - \omega\right)\left(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2\right)$$

Como $\pi \neq \lambda$, π solo puede dividir a uno de los factores pues si dividiese a dos, dividiría a la resta y llegaríamos a que divide a λ.

3.2 Símbolo cúbico

El último comentario de la sección anterior nos dice que en módulo π, cualquier $\alpha^{\frac{N(\pi)-1}{3}} \in \mathbb{Z}[\omega]$ será $1, \omega$ o ω^2 (pero no dos de ellos). Por tanto podemos dar la siguiente definición:

Definición 3.2.

$$\left(\frac{\alpha}{\pi}\right)_3 := \omega^m, \qquad \text{si} \quad \pi | \alpha^{\frac{N(\pi)-1}{3}} - \omega^m, \ m = 0, 1, 2$$

De esta forma

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \ \text{mód}\, \pi$$

Lo hemos definido de forma similar al criterio de Euler de reciprocidad cuadrática.

Propiedades

1. Si $\alpha \equiv_\pi \beta \Rightarrow$

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$$

2. Dados $\alpha, \beta \in \mathbb{Z}[\omega]$ se tiene que

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3.$$

3. Dado $\alpha \in \mathbb{Z}[\omega]$:

$$\exists \beta \in \mathbb{Z}[\omega] : \ \beta^3 \equiv \alpha \ \text{mód}\, \pi \quad \Leftrightarrow \quad \left(\frac{\alpha}{\pi}\right)_3 = 1.$$

Demostración. Las primeras dos leyes son inmediatas pasando a $\alpha^{\frac{N(\pi)-1}{3}} \ \text{mód}\, \pi$. Veamos la tercera.

Si β existe se tiene

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \ \text{mód}\, \pi = \beta^{N(\pi)-1} \ \text{mód}\, \pi = 1.$$

Por otro lado, si $\left(\frac{\alpha}{\pi}\right)_3 = 1$, por definición $\alpha^{\frac{N(\pi)-1}{3}} = 1$. Tomamos un generador $\overline{g}$ de $\left(\frac{\mathbb{Z}[\omega]}{(\pi)}\right)^\times$ y $k \in \mathbb{N}$ tal que $\overline{g}^k \equiv \alpha \ \text{mód}\, \pi$ luego

$$1 \equiv \alpha^{\frac{N(\pi)-1}{3}} \equiv (\overline{g}^k)^{\frac{N(\pi)-1}{3}}$$

Así que $N(\pi) - 1 | k\frac{N(\pi)-1}{3}$, es decir, existe $b \in \mathbb{Z}$:

$$(N(\pi) - 1)b = k\frac{N(\pi) - 1}{3} \Rightarrow \ 3b = k \Rightarrow \ 3|k$$

Luego $k/3 \in \mathbb{Z}$ y $\overline{g}^{k/3}$ es raíz cúbica de α módulo π. □

Dado $\pi \nmid \alpha$ con π irreducible en $\mathbb{Z}[\omega]$ con $N(\pi) \neq 3$, la aplicación

$$\left(\frac{\cdot}{\pi}\right)_3 : \left(\frac{\mathbb{Z}[\omega]}{(\pi)}\right)^\times \Rightarrow \mathbb{C}^\times$$

es un homomorfismo de grupos (a homomorfismos de este tipo se les llama carácteres).
Si π asociado a primo $q \equiv_3 2$ en $\mathbb{Z}$ tratamos con $\mathbb{F}_q^2$. Si $N(\pi) = p$ primo en $\mathbb{Z}$ tratamos con $\mathbb{F}_p, \ p \equiv_3 1$.

Tenemos ya que que

$$\exists \beta \in \mathbb{Z}[\omega] : \ \beta^3 \equiv \alpha \ \text{mód}\, \pi \quad \Leftrightarrow \quad \left(\frac{\alpha}{\pi}\right)_3 = 1$$

El problema es que estas raíces están en los enteros de Eisenstein y queremos encontrarlas en $\mathbb{Z}$. Veamos la relación entre ambas cosas.

Proposición 3.3. Sea $q \equiv_3 2$ primo entero, entonces todo elemento de $\mathbb{Z}[q]^\times$ será residuo cúbico módulo q.

Demostración. Sea $\overline{g}$ generador de $\mathbb{Z}_q^\times$. El orden de $\overline{g}$ es $q-1$ luego $3 \nmid q-1$ así que g^3 sigue teniendo orden $q-1$:

$$\mathbb{Z}_q^\times = \langle \overline{g} \rangle = \langle \overline{g}^3 \rangle, \text{ por tanto } \mathbb{Z}_q^\times = \left(\mathbb{Z}_q^\times\right)^3$$

□

Proposición 3.4. Dados p, a en $\mathbb{Z}$, con $p \equiv_3 1$ primo, $p = \pi\overline{pi}$, la ecuación $x^3 \equiv_p a$ es soluble en $\mathbb{Z}$ sii $\left(\frac{a}{\pi}\right)_3 = 1$.

Demostración. $\Longrightarrow$: Obvio, ya que $x^3 \equiv_p a$ implica $x^3 \equiv_\pi a$. $\Longleftarrow$: Si $\left(\frac{a}{\pi}\right)_3 = 1$, entonces hay β con $\beta^3 \equiv_\pi a$. Pero habrá $\beta' \equiv_\pi \beta$ con $\beta' \in \mathbb{Z}$: esto pasa porque $\mathbb{Z}[\omega]/(\pi)$ tiene p elementos y característica p, por tanto sus clases son de hecho $\overline{0}, \overline{1}, \ldots, \overline{p-1}$, que obviamente tienen representantes enteros. Así pues, $\beta'^3 \equiv_\pi a$, es decir, $\pi | \beta'^3 - a$. Tomando módulos al cuadrado, $p|(\beta'^3 - a)^2$. Ergo, $p|\beta'^3 - a$, como queríamos.

□

Ejemplo 3.5. Con $q = 2$:
Calculemos $\left(\frac{\alpha}{2}\right)_3$. Estamos trabajando en $\mathbb{F}_4$, tenemos los elementos $\{0, 1, \omega, 1+\omega\}$. Claramente $\left(\frac{1}{2}\right)_3 = 1$ pues $1^3 = 1$.
- $\left(\frac{\omega}{2}\right)_3 \equiv_2 \omega^{\frac{4-1}{3}} = \omega$.
- $\left(\frac{1+\omega}{2}\right)_3 \equiv_2 \omega^2$ por descarte.

Con $q = 5$: Tenemos 24 elementos en el grupo multiplicativo de $\mathbb{F}_{25}$. Tienen la forma $a + b\omega$ con $a, b \in \{0, 1, 2, 3, 4\}$. Ir elemento por elemento es tedioso. Busquemos generadores y veamos qué sucede.
ω tiene orden 3 y $(\omega\lambda)^2 = \omega^2(1 - 2\omega + 2\omega^2) = -3\omega^3 = -3$ está en $\mathbb{F}_5 \subset \mathbb{F}_{25}$, $(\omega\lambda)^4 \equiv 9 \equiv -1 \mod 5$ luego $\omega\lambda$ tiene orden 8.
Por tanto $\mathbb{F}_{25} = \langle \overline{\omega^2\lambda} \rangle$.[2] (en el grupo cíclico de 24 elementos, al multiplicar uno de orden 3 y uno de orden 8 obtenemos un generador).
Así que dado $a \in \mathbb{F}_{25}^\times$, $\exists k \in \mathbb{N} :\ (\overline{\omega^2\lambda})^k = a$ luego

$$\left(\frac{a}{5}\right)_3 = \left(\frac{\omega^2\lambda}{5}\right)_3^k = \left(\frac{\omega}{5}\right)_3^{2k} \left(\frac{\lambda}{5}\right)_3^k; \quad \left(\frac{\omega}{5}\right)_3 \equiv_5 \omega^{\frac{25-1}{3}} = \omega^8 = \omega^2$$

$$\left(\frac{\lambda}{5}\right)_3^2 = \left(\frac{\lambda^2}{5}\right)_3 = \left(\frac{-3\omega}{5}\right)_3 = \left(\frac{-3}{5}\right)_3 \left(\frac{\omega}{5}\right)_3 = \omega^2 \Rightarrow \left(\frac{\lambda}{5}\right)_3 = \omega.$$

Así que $\left(\frac{a}{5}\right)_3 = (\omega^2)^{2k}\omega^k = \omega^k\omega^k = \omega^{2k}$. Vamos probando casos para sacar los residuos cúbicos:

$$k = 0 :\Rightarrow\ 1, \qquad k = 3 :\Rightarrow\ \lambda^3 = (1-\omega)^3 = 1 - 3\omega + 3\omega^2 - 1 = -3\omega - 3(\omega+1) \equiv_5 2 + 4\omega$$

$$k = 6 :\Rightarrow\ (2+4\omega)^2 = 4 + 16\omega + 16\omega^2 \equiv_5 4 + \omega + \omega^2 = 3$$

$$k = 9 :\Rightarrow\ 3(2+4\omega) = 6 + 12\omega \equiv_5 1 + 2\omega, \quad k = 12 :\Rightarrow\ 3^2 \equiv_5 4$$

$$k = 15 :\Rightarrow\ 4(2+4\omega) \equiv_5 3 + \omega, \qquad k = 18 :\Rightarrow\ 3 \cdot 4 \equiv_5 2$$

$$k = 21 :\Rightarrow\ 2(2+4\omega) \equiv_5 4 + 3\omega$$

Dada una unidad $u \in \mathbb{Z}[\omega]^\times$ se tiene que $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha}{u\pi}\right)_3$ pues si π divide a algo $u\pi$ también y viceversa. Lo mismo no sucede si tomamos un asociado de α, básicamente porque no todas las unidades son residuos cúbicos.

[2]Esta barra es para señalar que es la clase de equivalencia, no tiene nada que ver con el conjugado.

3.2.1 Irreducibles primarios. Leyes suplementarias

Dados irreducibles $\pi_1, \pi_2 \in \mathbb{Z}[\omega]$ no asociados y tales que $N(\pi_1), N(\pi_2) \neq 3$, queremos relacionar $\left(\frac{\pi_1}{\pi_2}\right)_3$ con $\left(\frac{\pi_2}{\pi_1}\right)_3$.

Definición 3.6. Sea $\pi \in \mathbb{Z}[\omega]$ un irreducible. Diremos que π es primario si $\pi \equiv 2 \mod 3$.

Esta definición se puede dar sobre cualquier elemento, no necesariamente irreducible: $\exists c + d\omega \in \mathbb{Z}[\omega]$ tal que $\pi = 2 + 3(c + d\omega)$.
Un irreducible primario se puede escribir como $\pi = (3m - 1) + 3n\omega \ m, n \in \mathbb{Z}$.

Proposición 3.7. Sea $\pi \in \mathbb{Z}[\omega]$ irreducible, con $N(\pi) \neq 3$. Entonces exactamente uno de sus asociados es primario.

Demostración. En $\mathbb{Z}[\omega]/(3)$, que tiene 9 elementos, las seis unidades, $1, -1, \omega, -\omega, \omega^2, -\omega^2$, son todas distintas (ya que sus diferencias no son múltiplo de 3). Además tenemos los otros 3 elementos, también distintos, $1 - \omega, 1 - \omega^2, 0$, que no son unidades (ya que $(1 - \omega)(1 - \omega^2) = 0$ en $\mathbb{Z}[\omega]/(3)$).

Ahora, sea $\pi \in \mathbb{Z}[\omega]$ irreducible, con $N(\pi) \neq 3$. Entonces π es coprimo con 3, por tanto π, será una unidad en $\mathbb{Z}[\omega]/(3)$. Si buscamos un elemento a de $\mathbb{Z}[\omega]/(3)$ tal que $a\pi = -1$, habrá uno único, que es $\frac{-1}{\pi}$. Este elemento es una unidad en $\mathbb{Z}[\omega]/(3)$, y por tanto por lo que hemos visto en el anterior párrafo le corresponde una única unidad de $\mathbb{Z}[\omega]$. □

Ejemplo de primario asociado a un irreducible. $7 = (3+\omega)(3+\overline{\omega})$, ninguno de los factores irreducibles es primario. Veamos que un irreducible asociado sí que lo es:
- $\pm(3 + \omega) = \pm 3 \pm \omega$
- $\pm\omega(3 + \omega) = \pm 3\omega \pm \omega^2 = \pm 3\omega \mp \omega \mp 1 = \mp 1 \pm 2\omega$
- $\pm\omega^2(3 + \omega) = \pm 3\omega^2 \pm 1 = \mp 3(\omega + 1) \pm 1 = \mp 2 \mp 3\omega$.

Así que $-\omega^2(3 + \omega) = 2 + 3\omega$ es irreducible, primario y cumple que $(2 + 3\omega)(2 + 3\overline{\omega}) = 4 + 9 - 6 = 7$.

Ejercicio Dado un irreducible $\pi \in \mathbb{Z}[\omega]$, tal que $\pi\overline{\pi} = p$ primo. Con $p \equiv_3 1$. Entonces uno y solamente uno de los asociados de π es primario.

Nos comenzamos fijando en que tomando módulo 3 salen 9 posibilidades: $\alpha + \beta\omega$, donde $\alpha, \beta \in \{-1, 0, 1\}$. Nos fijamos en que si $\alpha + \beta \equiv_3 0$ no se cumple que $p \equiv_3 1$ pues

$$1 \equiv_3 p = a^2 + b^2 - ab \equiv_3 a^2 + a^2 + a^2 \equiv_3 0.$$

La ecuación $\alpha + \beta \equiv_3 0$ la cumplen 3 posibilidades de las 9. Quedan 6 y hay 6 asociados. Si calculamos la clase de cada unidad vemos que son precisamente estas 6 posibilidades restantes. Como el producto de unidades es unidad, el producto de clases es clase.
Dado π irreducible como en el enunciado. Su clase módulo 3 será alguna de las 6 posibles, de estas 6 solo una caracteriza a los primarios. El producto de unidades es un grupo, el producto de la clase de π por cada unidad: $L_\pi : \mathbb{Z}[\omega]^\times \to \mathbb{Z}[\omega]$ que manda u unidad a la clase de $u\pi$ genera 6 elementos cada uno con una clase distinta pues, aunque π no es inversible, sí que hay una unidad con la misma clase que π y podemos multiplicar por su inverso para ver que se trata de una biyección. Así que exactamente uno de los asociados es primario.

Teorema 3.8 (Primera ley suplementaria)**.** $\pi \in \mathbb{Z}[\omega]$ irreducible:

$$\left(\frac{-1}{\pi}\right)_3 = 1, \qquad \left(\frac{\omega}{\pi}\right)_3 = \begin{cases} 1 & \text{si} \quad N(\pi) \equiv 1 \mod 9 \\ \omega & \text{si} \quad N(\pi) \equiv 4 \mod 9 \\ \omega^2 & \text{si} \quad N(\pi) \equiv 7 \mod 9 \end{cases}$$

Demostración.

$$-1^3 \equiv -1 \mod \pi$$

Supongamos que $N(\pi) = p \in \mathbb{Z}$ primo con $p \equiv_3 1$. Encribimos entonces $N(\pi) = 9k + r$ donde r puede ser $1, 4, 7$:

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{\frac{N(\pi)-1}{3}} = \omega^{\frac{9k+r-1}{3}} = \omega^{\frac{r-1}{3}} = \begin{cases} 1 & \text{si } r = 1 \\ \omega & \text{si } r = 4 \\ \omega^2 & \text{si } r = 7 \end{cases}$$

Por otro lado, si $\pi = q \in \mathbb{Z}$ primo con $q \equiv_3 2$, $N(\pi) - 1 = q^2 - 1 = (3k+2)^2 - 1 = 9k^2 + 12k + 3 \Rightarrow$

$$\left(\frac{\omega}{q}\right)_3 \equiv_q \omega^{3k^2+4k+1} = \omega^{4k+1} = \omega^{k+1} = \begin{cases} 1 & \text{si } k = -1 \\ \omega & \text{si } k = 0 \\ \omega^2 & \text{si } k = 1 \end{cases}$$

Calculamos $N(\pi) \equiv_9 3k + 4 = \begin{cases} 1 & \text{si } k = -1 \\ 4 & \text{si } k = 0 \\ 7 & \text{si } k = 1 \end{cases}$ □

Teorema 3.9 (Segunda ley suplementaria)**.** $\pi \in \mathbb{Z}[\omega]$ irreducible primario tal que $\pi \nmid \lambda$ sean $m, n \in \mathbb{Z}$: $\pi = (3m-1) + 3n\omega$. Entonces:

$$\left(\frac{\lambda}{\pi}\right)_3 = \omega^{2m}$$

Demostración. Tenemos $\pi = (3m-1) + 3n\omega$ primo primario y queremos ver que $\left(\frac{\lambda}{\pi}\right)_3 = \omega^{2m}$.
Si $\pi \in \mathbb{Z}$:

$$\left(\frac{\lambda}{\pi}\right)_3^2 = \left(\frac{\lambda^2}{\pi}\right)_3 = \left(\frac{-3\omega}{\pi}\right)_3 = \left(\frac{-3}{\pi}\right)_3 \left(\frac{\omega}{\pi}\right)_3 = \left(\frac{\omega}{\pi}\right)_3 \equiv_\pi \omega^{\frac{(3m-1)^2-1}{3}} = \omega^{-2m} = \omega^m \Rightarrow \left(\frac{\lambda}{\pi}\right)_3 \equiv_\pi \omega^{2m}$$

Si $\pi \notin \mathbb{Z}$, $N(\pi) = (3m-1)^2 + 9n^2 - 3n(3m-1) \in \mathbb{Z}$ primo.

El caso de $\pi \notin \mathbb{Z}$ no es nada obvio, y de hecho fue publicado por Eisenstein después de la propia ley de reciprocidad cúbica. Una prueba se puede encontrar en [1]. Usa la ley de reciprocidad cúbica pero esto no será problema ya que no usaremos el suplemento para probar la ley. □

3.3 Sumas de Gauss y Jacobi

Para demostrar la reciprocidad cúbica vamos a generalizar una de los 8 demostraciones que dio Gauss de la cuadrática. Antes necesitaremos desarrollar algunas herramientas.

Consideremos $\hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$, el conjunto de homomorfismos $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$, donde $p \equiv_3 1$.[3]
Llamaremos caracteres a estos homomorfismos de grupos. Es directo ver que si $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ es un caracter:

1. $\chi(1) = 1$
2. $\forall a$, $\chi(a)$ es raíz $p-1$-ésima de la unidad.
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

Proposición 3.10. $\hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$ tiene una estructura de grupo con el producto definido por $(\chi_1 \cdot \chi_2)(a) := \chi_1(a)\chi_2(a)$. Llamaremos ε al elemento neutro, dado por $\varepsilon(a) = 1\ \forall a$.

Demostración. Es directo comprobar que $\chi_1 \cdot \chi_2$ está en $\hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$, y el resto de propiedades de grupo. El caracter inverso vendrá dado por $\chi^{-1}(a) := \chi(a)^{-1}$. □

Además, dado un generador g de $\mathbb{F}_p^\times$ determinamos el homomorfismo según dónde mandemos g. De esta forma, al haber $p-1$ raíces $p-1$-ésimas de la unidad tenemos $p-1$ caracteres. Si consideramos el generador

[3]Gran parte de los conceptos se pueden definir para todo primo aunque aquí pidamos que sea 1 módulo 3.

λ que manda g a $\omega_{p-1} := e^{\frac{2\pi i}{p-1}}$ dado cualquier otro caracter χ, mandará g a un elemento $a \in \mathbb{C}$ luego

$$\exists k \in \mathbb{Z} : \ a = \omega_{p-1}^k \Rightarrow \chi(g) = a = \omega_{p-1}^k = \lambda(g)^k = \lambda^k(g).$$

Luego el grupo de caracteres también es cíclico así que es isomorfo a $\mathbb{F}_p^\times$, el grupo cíclico de orden $p-1$. Este isomorfismo, $\hom(\mathbb{F}_{p^n}^\times, \mathbb{C}^\times) \equiv \mathbb{F}_{p^n}^\times$, es cierto en general para cuerpos finitos.

De momento usaremos λ para referirnos a un caracter que manda un generador a ω_{p-1}. $\lambda(a) \neq 1$ si $a \neq 1$.

Nos será conveniente extender los caracteres a funciones $\chi : \mathbb{F}_p \to \mathbb{C}$ de la siguiente forma:

$\chi(0) = \begin{cases} 1 & \text{si } \chi = \varepsilon \\ 0 & \text{si } \chi \neq \varepsilon \end{cases}$

Proposición 3.11.

$$1) \ \sum_{a \in \mathbb{F}_p} \chi(a) = \begin{cases} p & \text{si } \chi = \varepsilon \\ 0 & \text{si } \chi \neq \varepsilon \end{cases}$$

$$2) \ \sum_{\chi} \chi(a) = \begin{cases} 1 & \text{si } a = 0 \\ p & \text{si } a = 1 \\ 0 & \text{si } a \neq 0, 1 \end{cases}$$

Demostración. Para la primera propiedad, si $\chi = \varepsilon$:

$$\sum_{a \in \mathbb{F}_p} \varepsilon(a) = \sum_{a \in \mathbb{F}_p} 1 = p$$

Si $\chi \neq \varepsilon, \exists b \in \mathbb{F}_p^\times : \ \chi(b) \neq 1$, por tanto:

$$\chi(b) \sum_{a \in \mathbb{F}_p} \chi(a) = \sum_{a \in \mathbb{F}_p} \chi(ba) = \sum_{a \in \mathbb{F}_p} \chi(a) \Rightarrow \ (\chi(b) - 1) \sum_{a \in \mathbb{F}_p} \chi(a) = 0$$

Como $\chi(b) \neq 1$ deducimos que $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$.
Vamos a la segunda propiedad:
Si $a = 0$ usamos el convenio y es directo.
Si $a = 1$ $\chi(a) = 1$ para todo caracter χ.
Si $a \neq 0, 1$ se tiene que $\lambda(a) \neq 1$ luego

$$\lambda(a) \sum_{\chi} \chi(a) = \sum_{\chi} (\lambda\chi)(a) = \sum_{\chi} \chi(a) \Rightarrow \ (\lambda(a) - 1) \sum_{\chi} \chi(a) = 0$$

Igual que antes, como $\lambda(a) \neq 1$ deducimos que $\sum_{\chi} \chi(a) = 0$. □

Definición 3.12 (Suma de Gauss)**.** Dado $a \in \mathbb{F}_p$ se define, una suma de Gauss es $g_a : \hom(\mathbb{F}_p^\times, \mathbb{C}) \to \mathbb{C}$ definida por

$$g_a(\chi) := \sum_t \chi(t) \xi^{at}$$

donde $\xi := \omega_p = e^{\frac{2\pi i}{p}}$.

Denotamos por $g := g_1$.
Si $\chi = \varepsilon$ entonces

$$g_a(\chi) = \sum_t \xi^{at} = \sum_t (\xi^a)^t = \begin{cases} 0, & a \neq 0 \\ p. & a = 0 \end{cases}$$

Si tomamos $\chi = \left(\frac{\cdot}{p}\right)$ la imagen de $\mathbb{F}_p^\times$ es $\{-1, 1\}$.

$$g_a(\chi) = \sum_t \left(\frac{t}{p}\right) \xi^{at}$$

Esto es lo que Gauss usó para demostrar la reciprocidad cuadrática.

Veamos qué pasa si tomamos $\chi = \left(\frac{\cdot}{\pi}\right)_3 \in \hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$ con $N(\pi) = p$ primo en $\mathbb{Z}$, $p \equiv_3 1$. Sabemos que hay $N(\pi) - 1$ caracteres distintos. Pero 3 divide a $N(\pi) - 1$. Tomamos módulo 3 en la imagen de χ. De esta forma podemos trabajar con 3 caracteres: $\varepsilon, \chi, \chi^2$.

Veamos que $\chi^2 = \left(\frac{\cdot}{\overline{\pi}}\right)_3$:

$$\left(\frac{a}{\overline{\pi}}\right)_3 \equiv_{\overline{\pi}} a^{\frac{N(\overline{\pi})-1}{3}} \Leftrightarrow \overline{a^{\frac{p-1}{3}}} \equiv_\pi \overline{a}^{-\frac{p-1}{3}} \equiv_\pi \overline{a}^{2\frac{p-1}{3}} \equiv_\pi \left(\frac{a}{\pi}\right)_3^2 = \chi^2(a)$$

Ya nos centraremos en usar las propiedades de los caracteres con el símbolo cúbico. De momento sigamos trabajando con sumas de Gauss.

Proposición 3.13. Propiedades con la suma de Gauss:
1) $g_a(\chi) = \chi(a^{-1})g(\chi), \quad a \neq 0.$
2) $g_a(\varepsilon) = 0, \quad a \neq 0.$
3) $g_0(\chi) = 0, \quad \chi \neq \varepsilon.$
4) $g_0(\varepsilon) = p.$

Demostración. No sé por qué las demostramos al revés.
4) $g_0(\varepsilon) = \sum_t \varepsilon(t)\xi^{0t} = \sum_t \varepsilon(t) = p$
3) $g_0(\chi) = \sum_t \chi(t)\xi^{0t} = \sum_t \chi(t) = 0$, pues $\chi \neq \varepsilon$.
2) $g_a(\varepsilon) = \sum_t \varepsilon(t)\xi^{at} = \sum_t \xi^{at} = \sum_t \xi^t = 0$ pues $a \neq 0$.
1) $\chi(a)g_a(\chi) = \chi(a)\sum_t \chi(t)\xi^{at} = \sum_t \chi(at)\xi^{at} = \sum_t \chi(t)\xi^t = g(\chi)$ pues $a \neq 0$. Ahora, como $\chi(a)^{-1} = \chi^{-1}(a)$ pasamos al otro lado $\chi(a)$ y se tiene $g_a(\chi) = \chi(a^{-1})g(\chi)$. □

Proposición 3.14. Si $\chi \neq \varepsilon$, entonces

$$|g(\chi)| = \sqrt{p}.$$

Demostración. Esto es equivalente a ver que $g(\chi)\overline{g(\chi)} = p$. Calculemos la siguiente suma de dos formas distintas:

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_{a\neq 0} \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)} = \sum_{a\neq 0} \chi(1)g(\chi)\overline{g(\chi)} = \sum_{a\neq 0} g(\chi)\overline{g(\chi)} = (p-1)|g(\chi)|^2$$

Ahora la calculamos:

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_a \left(\sum_t \chi(t)\xi^{at}\right)\left(\sum_t \overline{\chi(t)}\xi^{-at}\right) = \sum_{a,x,y} \chi(x)\overline{\chi(y)}\xi^{a(x-y)} = \sum_{x,y} \chi(x)\overline{\chi(y)}\left(\sum_a \xi^{a(x-y)}\right)$$

Si $x \not\equiv_p y$, ξ^{x-y} es una raíz de la unidad distinta de 1, así que al variar a y sumar obtendremos 0. Por tanto

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_{x,y} \chi(x)\overline{\chi(y)}\left(\sum_a \xi^{a(x-y)}\right) = \sum_{x\equiv y} \chi(x)\overline{\chi(y)}\left(\sum_a \xi^{a(x-y)}\right) = p\sum_{x\equiv y} \chi(x)\overline{\chi(y)} =$$

$$p\sum_x \chi(x)\overline{\chi(x)} = p\sum_{x\not\equiv 0} \chi(x)\overline{\chi(x)} + p(\chi(0)\overline{\chi(0)}) = p\sum_{x\not\equiv 0} \chi(x)\chi(x)^{-1} = p(p-1)$$

Igualamos ambas expresiones:

$$(p-1)|g(\chi)|^2 = p(p-1) \Leftrightarrow |g(\chi)|^2 = p.$$

□

Se define $\overline{\chi}(a) := \overline{\chi(a)} = \chi(a)^{-1} = \chi(a^{-1}) = \chi^{-1}(a)$. Las últimas igualdades se dan si $a \neq 0$. $\overline{\varepsilon} = \varepsilon$.

Proposición 3.15. Se cumple que:

$$\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$$

Demostración.

$$\overline{g(\chi)} = \overline{\sum_t \chi(t)\xi^t} = \sum_t \overline{\chi(t)}\xi^{-t} = \sum_t \chi(-1)\overline{\chi(-1)\chi(t)}\xi^{-t} =$$

$$\chi(-1)\sum_t \overline{\chi}(-t)\xi^{-t} = \chi(-1)\sum_t \overline{\chi}(t)\xi^t = \chi(-1)g(\overline{\chi})$$

□

Corolario 3.16.

$$g(\chi)g(\overline{\chi}) = \chi(-1)p$$

Demostración. Como $p = g(\chi)\overline{g(\chi)} = g(\chi)\chi(-1)g(\overline{\chi})$ luego $\chi(-1)\chi(-1) = 1 \rightarrow\ \chi(-1)p = g(\chi)g(\overline{\chi})$ □

Definición 3.17 (Sumas de Jacobi)**.** Sean $\chi, \lambda \in \hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$, se define una suma de Jacobi $J : \hom(\mathbb{F}_p^\times, \mathbb{C}^\times)^2 \rightarrow \mathbb{C}$ tal que

$$J(\chi, \lambda) := \sum_{a+b=1} \chi(a)\lambda(b) \in \mathbb{C}$$

Proposición 3.18. Sean $\chi, \lambda \in \hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$ caracteres $\neq \varepsilon$ y supongamos que $\chi\lambda \neq \varepsilon$. Entonces:
1) $J(\varepsilon, \varepsilon) = p$
2) $J(\varepsilon, \chi) = 0$,
3) $J(\chi, \chi^{-1}) = -\chi(-1)$,
4) $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$

Demostración.

1. $J(\varepsilon, \varepsilon) = \sum\limits_{a+b=1} \varepsilon(a)\varepsilon(b) = \sum\limits_{a+b=1} 1 = p$
2. $J(\varepsilon, \chi) = \sum\limits_{a+b=1} \chi(b) = 0$ pues $\chi \neq \varepsilon$.
3. $J(\chi, \chi^{-1}) = \sum\limits_{a+b=1} \chi(a)\chi^{-1}(b) = \sum\limits_{\substack{a+b=1 \\ b\neq 0}} \chi(a)\chi(b^{-1}) = \sum\limits_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum\limits_{a\neq 1} \chi\left(\frac{a}{1-a}\right)$ Sea $c = \frac{a}{1-a}$. Se tiene entonces que
$$c = \frac{a}{1-a} \ \Leftrightarrow\ (1-a)c = a \ \Leftrightarrow\ \frac{c}{c+1} = a$$
Es decir, a y c están en una correspondencia biyectiva ya que c no está definida para $a = 1$ y si intentamos obtener 1 a partir de c llegamos a un absurdo: $1 = \frac{c}{c+1} \ \Leftrightarrow\ c+1 = c \ \Leftrightarrow\ 1 = 0$. De esta forma podemos poner que
$$J(\chi, \chi^{-1}) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right) = \sum_{c\neq -1} \chi(c) = -\chi(-1)$$
Esta última igualdad se debe a que $\sum\limits_c \chi(c) = 0$ luego
$$\sum_{c\neq -1} \chi(c) = \sum_c \chi(c) - \chi(-1) = -\chi(-1).$$
4. Desarrollamos el numerador
$$g(\chi)g(\lambda) = \sum_{x,y} \chi(x)\lambda(y)\xi^{x+y} = \sum_t \sum_{x+y=t} \chi(x)\lambda(y)\xi^t$$
Si $t = 0$ tenemos que $\sum\limits_{x+y=0} \chi(x)\lambda(y) = \sum\limits_x \chi(x)\lambda(-x) = \lambda(-1)\sum\limits_x \chi(x)\lambda(x) = \lambda(-1)\sum\limits_x (\chi\lambda)(x) = 0$.

Sea ahora t fijo no nulo, entonces $\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x/t+y/t=1} \chi(x)\lambda(y) = (\chi\lambda)(t) \sum_{x/t+y/t=1} \chi(x/t)\lambda(y/t) = (\chi\lambda)(t)J(\chi,\lambda)$ Así que

$$g(\chi)g(\lambda) = \sum_t \sum_{x+y=t} \chi(x)\lambda(y)\xi^t = J(\chi,\lambda)\sum_{t\neq 0}(\chi\lambda)(t)\xi^t$$

Como $\chi\lambda \neq \varepsilon$ se tiene

$$g(\chi)g(\lambda) = J(\chi,\lambda)\sum_{t\neq 0}(\chi\lambda)(t)\xi^t = J(\chi,\lambda)\sum_t(\chi\lambda)(t)\xi^t = J(\chi,\lambda)g(\lambda\chi).$$

y por 3.14 podemos pasar $g(\lambda\chi)$ dividiendo.

□

Corolario 3.19. Con χ, λ caracteres y $\chi, \lambda, \chi\lambda \neq \varepsilon$:

$$|J(\chi,\lambda)| = \sqrt{p}$$

Demostración. Es consecuencia directa de 3.14 y de 3.18. □

Proposición 3.20. Sea $\chi \in \hom(\mathbb{F}_p^\times, \mathbb{C}^\times)$ caracter con $|\chi| = 3$ (ergo, $\chi^2 = \chi^{-1}$) y $p \equiv_3 1$. Entonces

$$g(\chi)^3 = pJ(\chi,\chi)$$

Demostración.

$$g(\chi)^3 = g(\chi)^2 g(\chi) = J(\chi,\chi)g(\chi^2)g(\chi) = J(\chi,\chi)g(\overline{\chi})g(\chi) = J(\chi,\chi)\chi(-1)p.$$

Además, $\chi(-1) = \chi((-1)^3) = (\chi^3)(-1) = \varepsilon(-1) = 1$, por tanto tenemos el resultado. □

3.4 La ley de reciprocidad cúbica

Dedicaremos esta sección a probar la ley de reciprocidad cúbica:

Teorema 3.21 (Ley de reciprocidad cúbica)**.** Sean $\pi, \pi' \in \mathbb{Z}[\omega]$ irreducibles primarios distintos de λ. Entonces:

$$\left(\frac{\pi}{\pi'}\right)_3 = \left(\frac{\pi'}{\pi}\right)_3.$$

Podemos ignorar el caso $\pi = \pi'$, que es trivial.
Sea $\chi_\pi = \left(\frac{\cdot}{\pi}\right)_3$, $p = \pi\overline{\pi}$ siendo $\pi, \overline{\pi}$ primos primarios en $\mathbb{Z}[\omega]$.

Lema 3.22. $J(\chi_\pi, \chi_\pi) = \pi$

Demostración.

$$J(\chi_\pi,\chi_\pi) = \sum_{a+b=1} \chi_\pi(a)\chi_\pi(b) \in \mathbb{Z}[\omega]$$

Así que existen enteros a, b tales que $J(\chi_\pi, \chi_\pi) = a + b\omega$.
Sabemos también que $J(\chi_\pi,\chi_\pi)\overline{J(\chi_\pi,\chi_\pi)} = N(J(\chi_\pi,\chi_\pi)) = \sqrt{p}^2 = p = \pi\overline{\pi}$. Veamos que estos primos son primarios:

$$J(\chi_\pi,\chi_\pi) \equiv_3 pJ(\chi_\pi,\chi_\pi) = g(\chi_\pi)^3 = \left(\sum_t \chi_\pi(t)\xi^t\right)^3 \equiv_3 \sum_t \chi_\pi(t)^3\xi^{3t} = \sum_{t\neq 0}(\xi^3)^t = -1 \equiv_3 2.$$

Por tanto, como $J(\chi_\pi,\chi_\pi)\overline{J(\chi_\pi,\chi_\pi)} = \pi\overline{\pi}$ y todos los primos que aparecen ahí son primarios, tenemos que o bien $J(\chi_\pi,\chi_\pi) = \pi$ o bien $J(\chi_\pi,\chi_\pi) = \overline{\pi}$. Para ver que el caso que se cumple es el primero, basta ver que $J(\chi_\pi,\chi_\pi)|\pi$. Pero

$$J(\chi_\pi,\chi_\pi) = \sum_{a+b=1} \chi_\pi(a)\chi_\pi(b) = \sum_t \chi_\pi(t)\chi_\pi(1-t) \equiv_\pi \sum_t t^{\frac{p-1}{3}}(1-t)^{\frac{p-1}{3}} = \sum_t a_m t^m + \ldots + a_{2m}t^{2m} =$$

$$a_m \sum_t t^m + \ldots + a_{2m}\sum_t t^{2m}, \text{ siendo } m = \frac{p-1}{3}.$$

Veamos que si j está entre m y $2m$ (en concreto $1 < j < p$), entonces $\sum_{t\neq 0} t^j \equiv_p 0$.
Recordemos que los elementos en $\mathbb{F}_p^\times$ no nulos se expresan como g_p^k con $0 \leq k \leq p-2$ donde g_p es un generador. Así que

$$\sum_{t\neq 0} t^j = \sum_{k=0}^{p-2} (g_p^j)^k \equiv_p 0.$$

Así que $\overline{\pi}$ sería congruente con 0 módulo π, luego $\pi|\overline{\pi}$ y esto no tiene sentido.

□

Por el lema anterior y 3.20:

Corolario 3.23.

$$g(\chi_\pi)^3 = p\pi \quad \square$$

Demostración de la ley de reciprocidad cúbica. Se tienen varios casos, si $q_1, q_2 \in \mathbb{Z}$ con $q_1 \equiv_3 q_2 \equiv_3 2$ es trivial pues todo entero es residuo cúbico módulo p primo con $p \equiv_3 2$. Ahora veamos qué pasa si tenemos $p \equiv_3 1$ y $q \equiv_3 2$ primos en $\mathbb{Z}$

Calculemos

$$g(\chi_\pi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}} \equiv_q \chi_q(p\pi) = \chi_q(\pi)$$

Luego $g(\chi_\pi)^{q^2} \equiv_q \chi_q(\pi)g(\chi_\pi)$. A su vez,

$$g(\chi_\pi)^{q^2} = \left(\sum_t \chi_\pi(t)\xi^t\right)^{q^2} \equiv_q \sum_t \chi_\pi(t)^{q^2}\xi^{q^2 t}$$

. Además, como $\chi_\pi(t)^3 = 1$ y $q^2 \equiv_3 1$, tenemos que $\chi_\pi(t)^{q^2} = \chi_\pi(t)$, ergo por la ecuación anterior:

$$g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi).$$

Usando 3.13, tenemos que $g(\chi_\pi)^{q^2} = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$, donde $\chi_\pi(q^{-2}) = \chi_\pi(q)$ ya que $\frac{q^{-2}}{q}$ es un cubo. Usando esta última igualdad y la segunda que deducimos, tenemos que

$$\chi_\pi(q)g(\chi_\pi) \equiv_q \chi_q(\pi)g(\chi_\pi).$$

Como $g(\chi_\pi)$ tiene módulo $\sqrt{p}$, es coprimo con q, por tanto es una unidad en $\mathbb{Z}[\omega]/(q)$, y podemos cancelarlo en la anterior igualdad:

$$\chi_\pi(q) \equiv_q \chi_q(\pi).$$

Por tanto $\chi_\pi(q) = \chi_q(\pi)$, como queríamos.

Vamos al caso, $\pi_1, \pi_2 \in \mathbb{Z}$ con $|\pi_1| = p_1, |\pi_2| = p_2$ con $p_1 \equiv_3 p_2 \equiv_3 1$. El objetivo es obtener las 3 siguientes igualdades:

$$\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\pi_2}(p_1\overline{\pi}_1) \tag{3.1}$$

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2) \tag{3.2}$$

$$\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\pi_1}(p_2). \tag{3.3}$$

La primera igualdad se puede obtener partiendo de la igualdad $g(\chi_{\gamma_1^3})^3 = p_1\gamma_1$, elevando ambos lados a $\frac{N\pi_2-1}{2} = \frac{p_2-1}{3}$ y tomando congruencias módulo π_2, luego se puede obtener la igualdad con un desarrollo similar al del caso anterior. La segunda igualdad también se puede obtener de esa forma. La tercera igualdad se obtiene de que

$$\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\overline{\pi_1}}(p_2)^2 = \overline{\chi_{\overline{\pi_1}}(p_2)} = \chi_{\pi_1}(p_2),$$

donde la última igualdad se obtiene de que la igualdad $p_2^{(N\pi_1-1)/3} \equiv_{\pi_1} \chi_{\pi_1}(p_2)$ da lugar, tomando conjugados, a la igualdad $p_2^{(N\pi_1-1)/3} \equiv_{\overline{\pi_1}} \overline{\chi_{\pi_1}(p_2)}$, por tanto $\chi_{\overline{\pi_1}}(p_2) \equiv_{\overline{\pi_1}} p_2^{(N\overline{\pi_1}-1)/3} \equiv_{\pi_1} p_2^{(N\pi_1-1)/3} \equiv_{\overline{\pi_1}} \overline{\chi_{\pi_1}(p_2)}$, ergo $\chi_{\overline{\pi_1}}(p_2) = \overline{\chi_{\pi_1}(p_2)}$.

Teniendo las tres igualdades en cuenta podemos construir la siguiente cadena:

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi_1}) =^1 \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi_1}}(p_2^2) =^3 \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(\pi_2 p_2) =^2 \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\overline{\pi_1}) = \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\pi_1)$$

Podemos tachar y nos queda $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$, como queríamos.

□

3.5 Algunos problemas resueltos

Problema 3.1. Ver que $x^3 \equiv 2 \mod p$, con $p \equiv_3 1$, tiene solución $\Leftrightarrow$ $\exists \pi \equiv 5 \mod 6$ y $p = \pi\overline{\pi}$.

Solución. Si $\pi \equiv 5 \mod 6$, π será primario, por tanto podemos asumir que π es un divisor irreducible primario de p. Además, la ecuación $x^3 \equiv 2 \mod p$ tiene soluciones en x sii $\left(\frac{2}{\pi}\right)_3 = 1$ por 3.4, por tanto basta demostrar lo siguiente:

Sea $\pi \notin \mathbb{Z}$ irreducible primario, entonces $\left(\frac{2}{\pi}\right)_3 = 1$ sii $\pi \equiv 5 \mod 6$.

Pero esto es directo, porque por reciprocidad cúbica $\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv_2 \pi$, ergo $\left(\frac{2}{\pi}\right)_3 = 1$ sii $\pi \equiv_2 1$. Y, como sabemos que $\pi \equiv_3 2$, $\pi \equiv_2 1$ equivale a $\pi \equiv 5 \mod 6$ (esto se ve expresando $\pi = a + b\omega$ y viendo que ambas cosas equivalen a $a \equiv_6 5$ y $b \equiv_6 0$). □

Problema 3.2. Ver que si $p \equiv_3 1$, $x^3 \equiv 2 \mod p$ tiene solución $\Leftrightarrow$ $p = c^2 + 27d^2$.

Solución. $\Rightarrow$ Si $x^3 \equiv 2 \mod p$, por el ejercicio anterior $\pi \equiv 5 \mod 6$, siendo π primario con $N\pi = p$. Entonces, $\pi = a + b\omega$, con $a \equiv_6 5, b \equiv_6 0$. Ergo, llamando $c = \frac{2a-b}{2}$ y $d = \frac{b}{6}$:

$$p = N\pi = \frac{(2a-b)^2 + 3b^2}{4} = \frac{(2c)^2 + 3(6d)^2}{4} = c^2 + 27d^2,$$

como queríamos.

$\Leftarrow$ $p = c^2 + 27d^2 = N(c + 3d\sqrt{-3}) = N((c+3d) + \omega(6d))$. De modo que, por el ejercicio anterior, nos vale con que haya un asociado de $(c+3d) + \omega(6d)$ de la forma $a + b\omega$, con $a \equiv_6 5, b \equiv_6 0$. Pensando ahora en la ecuación módulo 6

$$p \equiv_6 c^2 + 27d^2$$

es fácil ver mirando resíduos cuadráticos que hay dos tipos de soluciones: d es par y c es ± 1, y d es impar, c es ± 2. Es directo comprobar que en cada uno de estos cuatro casos, o bien el propio $(c+3d) + \omega(6d)$ o su opuesto $-(c+3d) - \omega(6d)$ son de la forma $a + b\omega$, con $a \equiv_6 5, b \equiv_6 0$, por tanto hemos acabado. □

Cap 5 Ejercicios 1-28 buena selección del Ireland Rosen.

Capítulo 4

Anillos de enteros

4.1 Números algebraicos y enteros algebraicos

En teoría algebraica de números trabajaremos con cuerpos de números:

Definición 4.1. Se dice que K es un cuerpo de números si K es cuerpo y:
1) $\mathbb{Q} \subset K \subset \mathbb{C}$.
2) $\dim_{\mathbb{Q}} K$ es finita.

Recordemos algo de notación sobre teoría de Galois.

Dada una extensión de cuerpos $K \subseteq L$, llamamos $[L : K]$ a la dimensión de L como espacio vectorial sobre K, y llamamos $K(\alpha)$ al menor subcuerpo de L que contiene a K y α. En concreto, si $\alpha \in \mathbb{C}$, $\mathbb{Q}(\alpha)$ será el conjunto de elementos de la forma $\frac{p(\alpha)}{q(\alpha)}$, donde $p, q \in \mathbb{Q}[x]$ con $q(\alpha) \neq 0$.

Llamaremos $\overline{\mathbb{Q}}$ al cierre algebraico de $\mathbb{Q}$ en $\mathbb{C}$, es decir, los elementos de $\mathbb{C}$ que son raíces de algún polinomio de $\mathbb{Q}[x]$. $\overline{\mathbb{Q}}$ es un cuerpo numerable (ya que hay numerables polinomios en $\mathbb{Q}[x]$ y cada uno tiene finitas raíces). $\overline{\mathbb{Q}}$ contiene a todas las extensiones algebraicas de $\mathbb{Q}$ en $\mathbb{C}$.

Si α es algebraico sobre K, llamamos $\min_K(\alpha)$ al polinomio mónico de $K[x]$ de grado mínimo que se anula en α.

Teorema 4.2 (Teorema del elemento primitivo)**.** Si K es un cuerpo de números, entonces $K = \mathbb{Q}(\alpha)$ para cierto $\alpha \in K$.

Demostración. En Teoría de Galois se estudia que toda extensión finita separable de cuerpos está generada por un solo elemento, esto es un caso concreto. □

Definición 4.3. Definimos el conjunto de enteros algebraicos, $\mathbb{A}$, como el conjunto de números complejos que son raíz de algún polinomio mónico con coeficientes en $\mathbb{Z}$:

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \ h(a) = 0, \ h \in \mathbb{Z}[X], \ h \text{ mónico}\}.$$

Lema 4.4. Sea $\alpha \in \mathbb{C}$. Entonces $\alpha \in \mathbb{A}$ si y solo si existe $0 \neq W <_+ \mathbb{C}$ (es decir, W subgrupo aditivo de $\mathbb{C}$) finitamente generado tal que $\alpha W \subseteq W$.

Demostración. $\Leftarrow$ Llamamos $\alpha_1, \ldots, \alpha_n$ a un conjunto de generadores de W. Ahora, como $\alpha W \subseteq W$, existen a_{ij} coeficientes enteros tales que $\alpha\alpha_i = \sum_{i=1}^{n} a_{ij}\alpha_j$. Llamando M a la matriz (a_{ij}) de coeficientes enteros, y, si dado un vector v de n coeficientes enteros llamamos $k(v)$ al entero $\sum_{i=1}^{n} v_i\alpha_i$, entonces por cómo hemos definido a_{ij} tendremos que, dado un vector v,

$$\alpha k(v) = k(Mv).$$

Y así, por inducción sobre n, vemos que $\alpha^n k(v) = k(M^n v)$. De aquí es directo deducir que para cualquier polinomio $p \in \mathbb{Z}[x]$, tendremos que $p(\alpha)k(v) = k(p(M)v)$.

Ya casi hemos acabado, porque, llamando p al polinomio característico de la matriz M, tenemos que $p(M) = 0$ y p es mónico de coeficientes enteros. Por tanto, $p(\alpha)k(v) = k(p(M)v) = k(0) = 0$. Esto se cumple para todo v, por tanto $p(\alpha)W = 0$, es decir, $p(\alpha) = 0$, y hemos acabado.

$\Rightarrow$ Si $\alpha \in \mathbb{A}$, hay $p \in \mathbb{Z}[x]$ mónico con $p(\alpha) = 0$, de grado n. En este caso, cogemos W como el conjunto de elementos de la forma $q(\alpha)$, con $q \in \mathbb{Z}[x]$. Está claro que es un subgrupo aditivo. Además, estará generado por $1, \alpha, \ldots, \alpha^{n-1}$, ya que dado cualquier $q \in \mathbb{Z}[x]$, al ser p mónico podemos hacer división euclidea y habrá c y q' tales que $q = rp + q'$, con q' de grado $< n$. Así que $q(\alpha) = q'(\alpha)$, y $q'(\alpha)$ está en el subgrupo generado por $1, \alpha, \ldots, \alpha^{n-1}$. O sea que todo W está generado por $1, \alpha, \ldots, \alpha^{n-1}$. Por último, es obvio que $\alpha W \subseteq W$. □

Proposición 4.5. $\mathbb{A}$ es un dominio de integridad, con cuerpo de fracciones $\overline{\mathbb{Q}}$.

Demostración. Sean w_1, w_2 en $\mathbb{A}$, cogemos W_1, W_2 subgrupos aditivos finitamente generados tales que $w_1W_1 \subseteq W_1$ y $w_2W_2 \subseteq W_2$.

Si W_1 generado por $a_1, \ldots, a_n$ y W_2 generado por $b_1, \ldots, b_m$, cogemos W subgrupo aditivo generado por a_ib_j, con $i = 1, \ldots, n; j = 1, \ldots, m$. Entonces es fácil ver que $w_1W \subseteq W$ y $w_2W \subseteq W$, por tanto $(w_1 + w_2)W \subseteq w_1W + w_2W \subseteq W$ (por ser W subgrupo aditivo) y $w_1w_2W = w_1(w_2W) \subseteq w_1W \subseteq W$. Por tanto, $w_1 + w_2$ y $w_1w_2 \in \mathbb{A}$. Como $-1 \in \mathbb{A}$, tenemos que $-w_1 \in A$, ergo $\mathbb{A}$ es un anillo. Obviamente es un dominio de integridad, ya que es un subanillo de $\mathbb{C}$, y su cuerpo de fracciones está contenido en $\overline{\mathbb{Q}}$ ya que $\mathbb{A} \subseteq \overline{\mathbb{Q}}$.

Para ver que su cuerpo de fracciones es de hecho $\overline{\mathbb{Q}}$, veamos que cualquier elemento de $\overline{\mathbb{Q}}$ se puede expresar como $\frac{a}{b}$, siendo $a \in \mathbb{A}$ y $b \in \mathbb{Z}$. Ya que si $a \in \overline{\mathbb{Q}}$, entonces hay un polinomio $p(x) = \sum_{i=1}^{n} k_i x^i \in \mathbb{Z}[x]$ que se anula en a. Pero entonces, $q(x) = \sum_{i=1}^{n} k_i (k_n)^{n-i} x^i$ se anula en $k_n a$. Todos los coeficientes de este polinomio son múltiplos de k_n, por tanto $\frac{q(x)}{k_n}$ es un polinomio mónico en coeficientes enteros que se anula en $k_n a$. Es decir, ak_n es entero algebraico, y ya tenemos a como cociente de un entero algebraico y un entero. □

Definición 4.6. Dado un cuerpo de números K, llamamos $O_K = \mathbb{A} \cap K$, los elementos de K que son enteros algebraicos.

Teorema 4.7. $\alpha \in \mathbb{A}$ si y solo si $\min_{\mathbb{Q}}(\alpha)$ tiene coeficientes enteros.

Demostración. $\Leftarrow$ es obvia. Si $\alpha \in \mathbb{A}$ y p es mónico en $\mathbb{Z}[x]$ tal que $p(\alpha) = 0$, entonces los divisores irreducibles de p en $\mathbb{Z}[x]$ son mónicos, y alguno de ellos, que llamamos q, cumple que $q(\alpha) = 0$. Ahora bien, como q es irreducible en $\mathbb{Z}[x]$, por el lema de Gauss también es irreducible en $\mathbb{Q}[x]$, por tanto de hecho q es $\min_{\mathbb{Q}}(\alpha)$, y tiene coeficientes enteros. □

Ejemplo 4.8. $O_{\mathbb{Q}} = \mathbb{Z}$. Esto está claro ya que, por la proposición anterior, cualquier elemento de $O_{\mathbb{Q}}$ es raíz de un polinomio mónico de $\mathbb{Z}[x]$ de grado 1, $x - a$, por tanto es el entero a.

Ejemplo 4.9. $O_{\mathbb{Q}[i]} = \mathbb{Z}[i]$. Veamos por qué. Tenemos una extensión de $\mathbb{Q}$ de grado 2, por tanto todo elemento de $\mathbb{Q}[i]$ tiene polinomio mínimo de grado ≤ 2. En concreto, todo elemento de $O_{\mathbb{Q}}$ se anula en un polinomio mónico de grado ≤ 2. Es decir, dado un elemento $r + si \in O_{\mathbb{Q}}$, tendremos que

$$(r + si)^2 + a_1(r + si) + a_0 = 0, \text{ con } a_0, a_1 \in \mathbb{Z}.$$

Es decir, $r^2 - s^2 + a_1r + a_0 = 0$ y $2rs + a_1s = s(2r + a_1) = 0$. De la segunda ecuación hay dos opciones:

- $s = 0$. Entonces de la primera ecuación, $r^2 + a_1r + a_0 = 0$, y como $r \in \mathbb{Q}$, r es entero por ser raíz de un polinomio mónico.
- $s \neq 0$. Entonces, $r = \frac{-a_1}{2}$. Operando la primera ecuación, queda que $-4s^2 - a_1^2 + 4a_0 = 0$. Por tanto $4s^2 \in \mathbb{Z}$, así que s será de la forma $\frac{b}{2}$, con b entero. Entonces la ecuación $-4s^2 - a_1^2 + 4a_0 = 0$ se transforma en $-b^2 - a_1^2 + 4a_0 = 0$, y módulo 4 vemos que b y a_1 tienen que ser pares pues 0 es el único residuo cuadrático a módulo 4 tal que $-a$ es residuo cuadrático. por tanto s es entero. De modo que, como r es racional cumple la ecuación $r^2 - s^2 + a_1r + a_0 = 0$, mónica en r y de coeficientes enteros, r es entero.

Ejemplo 4.10. Sea K un cuerpo cuadrático (extensión de grado 2), $K = \mathbb{Q}(\alpha)$, donde $\alpha^2 \in \mathbb{Q}$ y $\alpha \notin \mathbb{Q}$. Podemos suponer que α^2 entero libre de cuadrados, multiplicando α si no por un racional adecuado (esto no cambia $\mathbb{Q}[\alpha]$) Veamos quién es O_K. Un elemento de K, $a_0 + a_1\alpha$, tendrá polinomio mínimo $(x - a_0)^2 - a_1^2\alpha^2$, es decir, $x^2 - 2a_0x + a_0^2 - a_1^2\alpha^2$. Necesitamos que este polinomio tenga coeficientes enteros, es decir, que $-2a_0$ y $a_0^2 - a_1^2\alpha^2$ sean enteros. Esto implica que $2a_0$ y $4a_1^2\alpha^2$ son enteros. Llamamos $a_0 = \frac{b_0}{2}$, con b entero. Como $4a_1^2\alpha^2$ es entero y α es libre de cuadrados, el único entero que puede dividir al denominador de a_1 es 2, ya que si no $4a_1^2\alpha^2$ tendría denominador > 1 en su forma irreducible. Por tanto también podemos llamar $a_1 = \frac{b_1}{2}$. Ahora, como $a_0^2 - a_1^2\alpha^2$ es entero, tendremos que $b_0^2 - b_1^2\alpha^2$ es múltiplo de 4. Esto da lugar a varios casos:

- b_0 y b_1 son pares, y a_0, a_1 enteros.
- b_0 y b_1 son impares, en cuyo caso módulo 4 vemos que $\alpha^2 \equiv_4 1$.
- b_0 par y b_1 impar, pero en este caso el numerador de α^2 no sería libre de cuadrados, ya que sería $\equiv_4 0$. Por tanto este caso es descartable. b_1 impar, b_0 par se descarta directamente usando módulo 4.

Es fácil comprobar que los dos casos posibles (b_0 y b_1 tienen la misma paridad) dan lugar de hecho a enteros algebraicos, ya que su polinomio mínimo tiene coeficientes enteros, por tanto hemos deducido la siguiente proposición:

Proposición 4.11. Sea el cuerpo cuadrático $K = \mathbb{Q}[\sqrt{d}]$, con $d \in \mathbb{Z}$ libre de cuadrados. Entonces O_K será:

- $\{a + b\sqrt{d}; a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}]$, si $d \not\equiv_4 1$.
- $\mathbb{Z}[\sqrt{d}] \cup \{\frac{a+b\sqrt{d}}{2};\ a, b \text{ impares}\} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, si $d \equiv_4 1$.

En el primer caso, $\{1, \sqrt{d}\}$ es una base de $\mathbb{Z}[\sqrt{d}]$ como $\mathbb{Z}$-módulo, y en el segundo caso, $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ es base de $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ como $\mathbb{Z}$-módulo. □

Ejemplo 4.12. El ejemplo 4.9 es un corolario de este teorema en el caso $d = -1$. Poniendo $d = -3$, tenemos que $O_{\mathbb{Q}[\sqrt{-3}]} = \mathbb{Z}[-\omega^2] = \mathbb{Z}[\omega]$.

En el caso de cuerpos cúbicos (dimensión 3) sobre $\mathbb{Q}$, la cosa se complica. Incluso en el ejemplo sencillo $K = \mathbb{Q}[\sqrt[3]{2}]$, donde se cumplirá que $O_K = \mathbb{Z}[\sqrt[3]{2}]$, si lo intentamos comprobar de forma similar al ejemplo 4.9 los cálculos se vuelven muy complicados. De modo que nos será útil desarrollar herramientas más generales.

4.2 Normas y trazas

Sea K un cuerpo de números, sea $\alpha \in K$. Entonces, recordemos que K tiene estructura de espacio vectorial sobre $\mathbb{Q}$, por tanto α induce una aplicación $\mathbb{Q}$-lineal, $\lambda_\alpha : K \to K; x \to \alpha x$. λ_α es un endomorfismo de K como $\mathbb{Q}$-espacio vectorial, y si $\lambda \neq 0$ es un automorfismo.

Definición 4.13.
Llamamos *norma* de α a $N_{K/\mathbb{Q}}(\alpha) = \det(\lambda_\alpha)$.
Llamamos *traza* de α a $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{tr}(\lambda_\alpha)$.

Estos conceptos están bien definidos, ya que recordemos que la traza y determinante son características de una aplicación que no dependen de en qué base la expresemos. Nuestras aplicaciones $N_{K/\mathbb{Q}}$ y $\mathrm{Tr}_{K/\mathbb{Q}}$ van de K en $\mathbb{Q}$. Se cumplen estas propiedades:

Proposición 4.14. *(Propiedades de norma y traza)* Sean $\alpha_1, \alpha_2 \in K$, $a \in \mathbb{Q}$.

1) $N_{K/\mathbb{Q}}(a) = a^n$, donde n es el grado de la extensión $\mathbb{Q} \subseteq K$.
2) $N_{K/\mathbb{Q}}(\alpha_1\alpha_2) = N_{K/\mathbb{Q}}(\alpha_1)N_{K/\mathbb{Q}}(\alpha_2)$.
3) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1 + \alpha_2) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1) + \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_2)$.
4) $\mathrm{Tr}_{K/\mathbb{Q}}(a\alpha_1) = a\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1)$.

5) $N_{K/\mathbb{Q}}(a\alpha_1) = a^n N_{K/\mathbb{Q}}(\alpha_1)$.

Demostración.

1. Se cumple ya que λ_a tiene por matriz aI, donde I es la identidad.
2. Se cumple ya que $\lambda_{\alpha_1\alpha_2} = \lambda_{\alpha_1} \circ \lambda_{\alpha_2}$, por tanto el determinante de $\lambda_{\alpha_1\alpha_2}$ es el producto de los determinantes de λ_{α_1} y λ_{α_2}.
3. Traza de la suma de dos matrices es la suma de las trazas.
4. Es directo teniendo en cuenta que si λ_{α_1} tiene asociada una matriz M en cierta base, $\lambda_{a\alpha_1}$ tiene matriz aM.
5. Se sigue de 1 y 2.

□

Un resumen de lo anterior es que $N_{K/\mathbb{Q}} \in \hom(K^\times, \mathbb{Q}^\times)$ y $\mathrm{Tr}_{K/\mathbb{Q}} \in \hom_K(K, \mathbb{Q})$.

Pasamos a estudiar formas de calcular la norma de un elemento $\alpha \in K$. Sea β tal que $K = \mathbb{Q}[\beta]$. Llamamos n al grado de K sobre $\mathbb{Q}$ y m al grado de $\mathbb{Q}[\alpha]$ sobre $\mathbb{Q}$ y d al grado de K sobre $\mathbb{Q}[\alpha]$, de forma que $n = md$. Entonces, tenemos que:

- $(1, \alpha, \ldots, \alpha^{m-1})$ es una base de $\mathbb{Q}[\alpha]$ como $\mathbb{Q}$-espacio vectorial.
- $(1, \beta, \ldots, \beta^{d-1})$ es una base de K como $\mathbb{Q}[\alpha]$-espacio vectorial.

Por tanto, los productos dos a dos de los elementos de dichas bases, es decir, $B = (\alpha^i\beta^j)_{i=0,\ldots,m-1;j=1,\ldots,d-1}$, es una base de K como $\mathbb{Q}$-espacio vectorial. En concreto, ordenamos B de la siguiente forma:

$$B = (\overbrace{1, \alpha, \ldots, \alpha^{m-1}}^{B_0}, \overbrace{\beta, \beta\alpha, \ldots, \beta\alpha^{m-1}}^{B_1}, \ldots, \overbrace{\beta^{d-1}, \beta^{d-1}\alpha, \ldots, \beta^{d-1}\alpha^{m-1}}^{B_{d-1}})$$

Aquí, para cada elemento a de B_j se cumple que αa es combinación de los elementos de B_j, por tanto la matriz M de λ_α será una matriz diagonal por bloques, cada bloque M_j correspondiente a un B_j:

$$M = \begin{pmatrix} M_0 & 0 & \cdots & 0 & 0 \\ 0 & M_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & M_{d-2} & 0 \\ 0 & 0 & \cdots & 0 & M_{d-1} \end{pmatrix} \tag{4.1}$$

Esto va a hacer más fácil el cálculo del determinante. Veamos cómo exactamente será cada M_j.

Llamamos $f = a_0 + a_1 x + \cdots + a_m x^m$ al polinomio mínimo de α. Entonces, como los elementos de B_j son de forma $\beta^j\alpha^i$, tendremos que, si i está entre 0 y $m-2$, $\alpha(\beta^j\alpha^i) = \beta^j\alpha^{i+1}$, y si $i = m-1$, $\alpha(\beta^j\alpha^m - 1) = \beta^j\alpha^m = \sum_{i=0}^{m-1} -a_i\beta^j\alpha^i$. Resumiendo:

$$M_j = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}$$

Es decir, su determinante es $(-1)^m a_0$. Pero, a su vez, llamando $\alpha_1, \ldots, \alpha_m$ a las raíces de f, tenemos que a_0, el término independiente de f, es $(-1)^m \prod_{i=1}^m \alpha_i$. Por tanto, el determinante del bloque asociado a B_j será $\prod_{i=1}^m \alpha_i$. Multiplicando el determinante de todos los bloques, tenemos que:

Proposición 4.15. Sea $\alpha \in K$, con K cuerpo de números. Sea m el grado de la extensión $\mathbb{Q}[\alpha]/\mathbb{Q}$, d el grado de la extensión $K/\mathbb{Q}[\alpha]$ y sean $\alpha_1, \ldots, \alpha_m$ las raíces (en $\mathbb{C}$) de $\min_{\mathbb{Q}}(\alpha)$. Entonces,

$$N_{K/\mathbb{Q}}(\alpha) = \left(\prod_{i=1}^{m} \alpha_i\right)^d,$$

Equivalentemente, $N_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0^d$, donde $\min_{\mathbb{Q}}(\alpha) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$. En concreto, si $K = \mathbb{Q}[\alpha]$, $N_{\mathbb{Q}[\alpha]/\mathbb{Q}}(\alpha) = (-1)^m a_0$. □

Para dar otra versión del teorema, repasamos algo más de teoría de Galois. Dado $\alpha \in K$, con K cuerpo de números y $\mathbb{Q}[\alpha]/\mathbb{Q}$ de grado m, tenemos que cualquier homomorfismo de anillos $\sigma : \mathbb{Q}[\alpha] \to \mathbb{C}$ cumplirá que $\varphi|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$, y entonces σ solo depende de la imagen de α. Las posibles imágenes de α son las raíces del polinomio mínimo de α, es decir, $\alpha_1, \ldots, \alpha_m$, por tanto hay exactamente m homomorfismos $\sigma : \mathbb{Q}[\alpha] \to \mathbb{C}$. Los llamamos $\sigma_i : \mathbb{Q}[\alpha] \to \mathbb{C}$, con $\sigma_i(\alpha) = \alpha_i$. De forma similar, si llamamos n a $[K : \mathbb{Q}]$ (el grado de K sobre $\mathbb{Q}$), habrá n inmersiones (homomorfismos inyectivos) $\tau_j : K \to \mathbb{C}$, y de hecho se cumplirá que para cada $\sigma_i : \mathbb{Q}[\alpha] \to \mathbb{C}$ hay $d = \frac{n}{m}$ homomorfismos τ con $\tau|_{\mathbb{Q}[\alpha]} = \sigma_i$. Por tanto, si τ_j son los homomorfismos de K en $\mathbb{C}$, en $\prod_j \tau_j(\alpha)$ aparece d veces cada una de las raíces $\alpha_1, \ldots, \alpha_n$.

Teniendo en cuenta esta discusión podemos dar una reformulación del teorema anterior:

Proposición 4.16. Sea $\alpha \in K$, con K cuerpo de números de dimensión n sobre $\mathbb{Q}$. Sean $\tau_j : K \to \mathbb{C}$ los homomorfismos de K en $\mathbb{C}$. Entonces,

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{j=1}^{n} \tau_j(\alpha),$$

□

Para calcular la traza de un elemento $\alpha \in K$, hacemos lo mismo: Volviendo a la matriz M de 4.1, tenemos que $\mathrm{Tr}(\alpha) = \mathrm{Tr}(M) = \sum_{j=0}^{d-1} \mathrm{Tr}(M_j) = -da_{m-1}$. A su vez, a_{m-1} es el segundo coeficiente de mayor grado de $\min_{\mathbb{Q}}(\alpha) = \prod_{i=1}^{m}(x - \alpha_i)$, por tanto $a_{m-1} = -\sum_{i=1}^{m} \alpha_i$. Por tanto, $\mathrm{Tr}(\alpha) = d\left(\sum_{i=1}^{m} \alpha_i\right)$. Podemos reformular el teorema como antes, ya que cada α_i aparece d veces como $\tau_j(\alpha)$, donde los τ_j son los homomorfismos de K en $\mathbb{C}$. Enunciamos las dos formulaciones:

Proposición 4.17. Sea $\alpha \in K$, con K cuerpo de números. Sea m el grado de la extensión $\mathbb{Q}[\alpha]/\mathbb{Q}$, d el grado de la extensión $K/\mathbb{Q}[\alpha]$ y sean $\alpha_1, \ldots, \alpha_m$ las raíces (en $\mathbb{C}$) de $\min_{\mathbb{Q}}(\alpha)$. Entonces,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = d\left(\sum_{i=1}^{m} \alpha_i\right) = -da_{m-1},$$

$\min_{\mathbb{Q}}(\alpha) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$. En concreto, si $K = \mathbb{Q}[\alpha]$, $\mathrm{Tr}_{\mathbb{Q}[\alpha]/\mathbb{Q}}(\alpha) = -a_{m-1}$.
Equivalentemente, sean $\tau_j : K \to \mathbb{C}$ los homomorfismos de K en $\mathbb{C}$. Entonces,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{j=1}^{n} \tau_j(\alpha),$$

□

Corolario 4.18. Si $\alpha \in K$ es un entero algebraico, entonces $N_{K/\mathbb{Q}}(\alpha)$ y $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ son enteros.

Demostración. Si α es entero algebraico, $\min_{\mathbb{Q}}(\alpha) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ tiene coeficientes enteros. Por tanto, en la notación de los teoremas anteriores, $N_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0^d$ y $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -da_{m-1}$ son números enteros. □

El recíproco del anterior teorema es falso. Por ejemplo, si α es una raíz de $x^3 + x^2 + \frac{x}{2} + 1$, entonces α tiene traza y norma enteras, pero su polinomio mínimo no tiene coeficientes enteros, o sea que no es un entero algebraico.

Cuando hablemos de la norma o traza de un elemento α $(N(\alpha), \mathrm{Tr}(\alpha))$ sin especificar el cuerpo, normalmente nos referiremos a en el cuerpo $K = \mathbb{Q}[\alpha]$. Es un buen ejercicio calcular con todos los criterios de las proposiciones anteriores la norma y traza de ω $(N(\omega) = 1, \mathrm{Tr}(\omega) = -1)$, veremos una generalización de ello en breve. En $\mathbb{Q}[\omega]$ y $\mathbb{Q}[i]$, y en general en cualquier cuerpo cuadrático no contenido en $\mathbb{R}$, los únicos dos homomorfismos de K sobre $\mathbb{C}$ serán la identidad y la conjugación. Por tanto, por 4.16 tendremos que $N(x) = x\overline{x}$, es decir, en esos cuerpos la norma coincide con la norma habitual de $\mathbb{C}$. También tendremos en esos cuerpos que $\mathrm{Tr}(x) = x + \overline{x} = 2\mathrm{Re}(x)$.

Ejemplo 4.19. Sea $K = \mathbb{Q}[\sqrt{d}]$ con $\sqrt{d} \notin \mathbb{Q}$. Calculemos $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$. Pues tenemos dos inmersiones, la identidad y mandar $\sqrt{d}$ a $-\sqrt{d}$.
Si $d < 0$ la se tiene que $N(\alpha) = |\alpha|^2$, es decir, la norma como la hemos definido en este capítulo hace a K un dominio euclídeo. Sin embargo, si $d > 0$, $a^2 - db^2$ puede no ser positivo, o sea que no tenemos por qué tener un dominio euclídeo. Podemos intentar tomar el valor absoluto de la norma, $|N(\alpha)|$, a ver si eso sirve para tener un dominio euclídeo, pero veremos más adelante que esto da problemas.

Ejemplo 4.20. Consideremos la norma $N(a+b\alpha+c\alpha^2)$, $a, b, c \in \mathbb{Q}$ con $\alpha^3 = 2$ y $\mathbb{Q}(\alpha)/\mathbb{Q}$. Visto como espacio vectorial tenemos por ejemplo la base $B = \{1, \alpha, \alpha^2\}$. Construimos la matriz poniendo en la primera columna las coordenadas respecto de la base. En el resto de elementos a_i^j ponemos αa_i^{j-1}. De esta forma se tiene que:

$$x = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} \Rightarrow N(x) = \begin{vmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{vmatrix} = a^3 + 2b^3 + 4c^3 - 6abc, \quad T(x) = 3a$$

También podemos ver la traza teniendo en cuenta que $\min_{\mathbb{Q}}(\alpha) = x^3 - 2$, $\min_{\mathbb{Q}}(\alpha^2) = x^3 - 3$ no tienen elemento cuadrático y, por defecto, la traza de un número a será 1 :

$$T(x) = aT(1) + bT(\alpha) + cT(\alpha^2) = 3a + b0 + c0 = 3a \in \mathbb{Z}$$

4.3 Enteros algebraicos de los cuerpos ciclotómicos

Calcularemos todos los enteros algebraicos en estos cuerpos. Sea $\omega = \omega_p := e^{\frac{2\pi i}{p}}$ con $p \in \mathbb{Z}$ primo. Consideremos $K := \mathbb{Q}(\omega)$. $\min_{\mathbb{Q}}(\omega) = x^{p-1} + \cdots + x + 1$, cuyas raíces son las raíces p-ésimas primitivas de la unidad, $\omega, \omega^2, \ldots, \omega^{p-1}$. Llamamos a este polinomio Φ_p, el *polinomio ciclotómico de orden p*:

$$\Phi_p = \prod_{k=1}^{p-1}(x - \omega^k)$$

Como Φ_p tiene grado $p - 1$, $[K : \mathbb{Q}] = p - 1$ y tenemos que $\{1, \omega, \ldots, \omega^{p-2}\}$ es una base de K como espacio vectorial sobre $\mathbb{Q}$. Como todas las raíces de $\min_{\mathbb{Q}}(\omega)$ están en $\mathbb{Q}[\omega]$, tenemos que $\mathbb{Q}[\omega]$ es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^{p-1} + \cdots + x + 1$, por tanto es una extensión de Galois sobre $\mathbb{Q}$.

A continuación queremos probar que $O_K = \mathbb{Z}[\omega]$. Primero introducimos algo de notación y hechos de $\mathbb{Z}[\omega]$.

Proposición 4.21. Sea ω raíz primitiva p-ésima de la unidad, con p primo impar, y sea $\lambda = 1 - \omega$. Entonces, λ es un entero algebraico, y en $\mathbb{Q}(\omega)/\mathbb{Q}$:

1. $N(\omega) = 1$
2. $\mathrm{Tr}(\omega) = -1$
3. $\mathrm{Tr}(\lambda) = N(\lambda) = p$
4. $\lambda\mathbb{A} \cap \mathbb{Z} = p\mathbb{Z}$

Demostración. Por un lado $N(\omega) = \ldots = N(\omega^{p-1}) = (-1)^{p-1}a_0 = 1$. Para la traza $T(\omega) = \ldots = T(\omega^{p-1}) = -a_{p-2} = -1$. Calculamos ahora $T(\lambda) = T(1) - T(\omega) = p - 1 - (-1) = p$. $N(\lambda) = N(1-\omega) = (-1)^{p-1}N(\omega - 1) = N(\omega - 1)$. Denotemos por $y := \omega - 1$, se tiene

$$(y + 1)^{p-1} + \ldots + (y + 1) + 1 = 0$$

El polinomio anterior es irreducible (ya que el ciclotómico lo es), está en $\mathbb{Z}[x]$, por tanto λ es algebraico, y su término independiente es $b_0 = p$ luego $N(\lambda) = p = \sigma_1(\lambda)\dots\sigma_{p-1}(\lambda)$ donde cada σ_k es una inmersión de K en $\mathbb{C}^\times$. Es decir, $p = \lambda\lambda_2\dots\lambda_{p-1}$, donde $\lambda_i = 1-\omega^k = \lambda\beta_k$, con $\beta_k = \sum_{j=0}^{k-1}\omega^j \in R$.

Vamos a ver que se cumplirá que $\lambda\mathbb{A}\cap\mathbb{Z} = p\mathbb{Z}$. El contenido $\supseteq$ es directo: $p \in \lambda\mathbb{A}$ ya que $p = \lambda\lambda_2\dots\lambda_{p-1}$, y λ_i son enteros algebraicos. El otro contenido se da porque el ideal $p\mathbb{Z}$ es maximal y si suponemos que $\lambda\mathbb{A}\cap\mathbb{Z} = \mathbb{Z}$ tendríamos que $1 \in \lambda\mathbb{A} \Rightarrow 1 = \lambda\beta$ con $\beta \in \mathbb{A} \Rightarrow\ 1 = N(\lambda)N(\beta) = pm,\ m \in \mathbb{Z}$ lo cual es imposible. □

Proposición 4.22. Sea ω raíz primitiva p-ésima de la unidad, sean $K = \mathbb{Q}[\omega]$ y $\alpha = a_0+a_1\omega+\dots+a_{p-2}\omega^{p-2} \in \mathbb{Q}(\omega),\ a_k \in \mathbb{Q}$. Entonces $\alpha \in O_K \ \Leftrightarrow\ a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}$. Es decir,

$$O_K = \mathbb{Z}[\omega].$$

Demostración. $\Leftarrow$) es inmediata al estar $\omega \in O_K$. Veamos $\Rightarrow$) :
Como α es entero algebraico se tiene que $T(\lambda\alpha) \in \mathbb{Z}$. Calculemos la traza

$$T(\lambda\alpha) = T(a_0\lambda + a_1\lambda\omega + \dots + a_{p-2}\lambda\omega^{p-2}) = a_0T(\lambda) + a_1T(\lambda\omega) + \dots + a_{p-2}T(\lambda\omega^{p-2}) =$$

$$= a_0T(1-\omega) + a_1T(\omega-\omega^2) + \dots + a_{p-2}T(\omega^{p-2}-\omega^{p-1})$$

Todas las $\omega^k,\ 1 \le k \le p-1$ tienen la misma traza por 4.21 luego

$$T(\lambda\alpha) = a_0T(1-\omega) = pa_0$$

Ahora calculamos la traza con inmersiones

$$T(\lambda\alpha) = \sigma_1(\lambda\alpha)+\dots+\sigma_{p-1}(\lambda\alpha) = \lambda\alpha+\lambda_2\alpha_2+\dots+\lambda_{p-1}\alpha_{p-1} = \lambda\alpha+\lambda\beta_2\alpha_2+\dots+\lambda\beta_{p-1}\alpha_{p-1} = \lambda\beta,\ \beta \in O_K.$$

Pero, por 4.21 4, como $T(\lambda\alpha) = \lambda\beta$ es entero tenemos que es múltiplo de p, por tanto pa_0 es múltiplo de p, por tanto $a_0 \in \mathbb{Z}$.

Ahora, como $a_0 \in \mathbb{Z},\ \alpha \in O_K \ \Rightarrow\ \alpha - a_0 \in O_K$. Pero $\alpha - a_0 = \omega(a_1 + a_2\omega + \dots + a_{p-2}\omega^{p-3}),\ \omega$ es unidad, de hecho:

$$\omega^{p-1}(\alpha - a_0) = \omega^{p-1}\omega(a_1 + a_2\omega + \dots + a_{p-2}\omega^{p-3}) = (a_1 + a_2\omega + \dots + a_{p-2}\omega^{p-3}) \in O_K$$

Repetimos el argumento para ver que $a_1 \in \mathbb{Z}$ y así sucesivamente. □

4.4 Discriminantes

Sea K cuerpo de números y consideremos la aplicación

$$\begin{array}{rccc} B: & K\times K: & \longrightarrow & \mathbb{Q} \\ & (\alpha,\beta) & \longmapsto & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) \end{array}$$

B es una forma bilineal. Por tanto, fijada una base de K como e.v. sobre $\mathbb{Q}$, la aplicación define una matriz A, de forma que si tomamos α como vector horizontal y β como vector vertical,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = \alpha A\beta.$$

Llamaremos a su determinante discriminante de la base.
Es decir, dada $R = (\alpha_1, \dots, \alpha_n)$ $\mathbb{Q}$-base de K se tiene

$$\Delta(\alpha_1, \dots, \alpha_n) = |\mathrm{Tr}(\alpha_i, \alpha_j)| \in \mathbb{Q}$$

Proposición 4.23. *(Cambio de base)* Sea $R' = \{\alpha'_1, \dots, \alpha'_n\}$ otra $\mathbb{Q}$-base de K. Sea P a la matriz de cambio

de base de R' a R y sea A la matriz de B en la base R y A' en la base R'. Entonces

$$A' = P^t AP, \text{ por tanto } \Delta' = |A'| = |P|^2|A| = |P|^2\Delta. \quad \square$$

Corolario 4.24. Si tenemos dos bases $(\alpha_1, \ldots, \alpha_n)$ y $(\alpha'_1, \ldots, \alpha'_n)$, con $\alpha'_i = \sum_{j=1}^n k_{i,j}\alpha_j$ y los $k_{i,j}$ son enteros, entonces la matriz P tiene entradas enteras, por tanto $|P|$ es entero ($\neq 0$) y por tanto $|A'|$ es el producto de un cuadrado perfecto y $|A|$. $\square$

Proposición 4.25. Si K es un cuerpo de números con base $(\alpha_1, \ldots, \alpha_n)$, la aplicación $B : K \times K :\to \mathbb{Q}$ es no degenerada, es decir, su matriz tiene determinante no nulo. Sin embargo, si $\alpha_1, \ldots, \alpha_n$ son $\mathbb{Q}$-linealmente dependientes, el determinante $|\mathrm{Tr}(\alpha_i, \alpha_j)|$ será 0.

Demostración. Para la primera parte, llamando A a la matriz, basta ver que para cada vector b hay un vector a con $aAb \neq 0$. Cogiendo $a = b^{-1}$, $aAb = \mathrm{Tr}(b^{-1}b) = \mathrm{Tr}(1) \neq 0$.

Para la segunda parte, si $\alpha_1, \ldots, \alpha_n$ son linealmente dependientes, cumplen una relación tipo $\sum_i a_i\alpha_i = 0$, con los a_i no todos nulos. Multiplicando esa igualdad por cierto α_j y tomando trazas, tenemos que $\sum_i a_i Tr(\alpha_i\alpha_j) = 0$. Como aquí las a_i no dependen de j, hemos encontrado una dependencia lineal entre las columnas de la matriz $(\mathrm{Tr}(\alpha_i, \alpha_j))$, por tanto su determinante es 0. $\square$

Vamos a ver algunos ejemplos antes de seguir.

Ejemplo 4.26. Sea $K = \mathbb{Q}[\sqrt{d}]$ con $\sqrt{d} \notin \mathbb{Q}$. Tomemos como base $(1, \sqrt{d})$, entonces

$$A = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{pmatrix}$$

$\min_{\mathbb{Q}} \sqrt{d} = x^2 - d$ luego

$$\Delta = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d$$

Si tomamos por ejemplo $d \equiv 1 \pmod 4$ se tiene que $\left(1, \frac{1+\sqrt{d}}{2}\right)$ sigue siendo una base formada por enteros. Calculemos el determinante en esta base, $\mathrm{Tr}((1+\sqrt{d})/2) = 2/2 + 0/2 = 1$, $\mathrm{Tr}((1+\sqrt{d})^2/4) = \mathrm{Tr}(1/4 + \sqrt{d}/2 + d/4) = 1/2 + d/2 = (1+d)/2$

$$\Delta = \begin{vmatrix} 2 & 1 \\ 1 & (1+d)/2 \end{vmatrix} = d$$

Es decir, en la misma extensión, esta base nos da un discriminante más bajo que la anterior. En general, buscamos bases que nos den un discriminante mínimo. Ya veremos después por qué es importante.

Ejemplo 4.27. Calculemos el discriminante en $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ de la base $(1, \alpha, \alpha^2)$ donde $\alpha = \sqrt[3]{2}$.

$$A = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix}$$

$\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\alpha) = 0$, $\mathrm{Tr}(\alpha^2) = 0$, $\mathrm{Tr}(\alpha^3) = 6$, $\mathrm{Tr}(\alpha^4) = 2\mathrm{Tr}(\alpha) = 0$ luego

$$\Delta = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{vmatrix} = -108$$

Así que $\Delta = -2^2 \cdot 3^3$

Ejemplo 4.28. Sea ahora $K = \mathbb{Q}(\alpha)$, $\alpha^3 = \alpha + 1$. $\min_{\mathbb{Q}}(\alpha) = x^3 - x - 1 \in \mathbb{Q}[x]$. El polinomio es irreducible

pues si no, sería reducible en $\mathbb{Z}[x]$, y no tiene raíces en $\mathbb{Z}$.

$$A = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix}$$

Calculamos $\min_{\mathbb{Q}}(\alpha^2) = x^3 - 2x^2 + x - 1$ pues si $x = \alpha^2 \Rightarrow$

$$x^2 = \alpha^4 = \alpha(\alpha+1) = \alpha^2 + \alpha, \quad x^3 = \alpha^2(\alpha^2+\alpha) = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1$$

Así que

$$0 = x^3 + \lambda_2 x^2 + \lambda_1 x + \lambda_0 = \alpha^2 + 2\alpha + 1 + \lambda_2(\alpha^2+\alpha) + \lambda_1\alpha^2 + \lambda_0 = (1+\lambda_2+\lambda_1)\alpha^2 + (2+\lambda_2)\alpha + 1 + \lambda_0 \Rightarrow$$

$$\lambda_0 = -1,\ \lambda_1 = 1,\ \lambda_2 = -2.$$

Así que $\mathrm{Tr}(1) = 3,\ \mathrm{Tr}(\alpha) = 0,\ \mathrm{Tr}(\alpha^2) = 2,\ \mathrm{Tr}(\alpha^3) = \mathrm{Tr}(\alpha+1) = 3,\ \mathrm{Tr}(\alpha^4) = \mathrm{Tr}(\alpha^2+\alpha) = 2$

$$A = \begin{vmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{vmatrix} = -23$$

$$\Delta(1, \alpha, \alpha^2) = -23$$

4.5 Bases de enteros y bases enteras

Definición 4.29. Decimos que $(\alpha_1, \ldots, \alpha_n)$ es una base de enteros de K sobre $\mathbb{Q}$ si es una base de K como espacio vectorial sobre $\mathbb{Q}$ formada por enteros algebraicos.

Proposición 4.30. Todo cuerpo de números K se puede expresar como $\mathbb{Q}[\alpha]$, para α entero algebraico. Por tanto, todo cuerpo de números K tiene una base de enteros.

Demostración. Para la primera parte, sea a tal que $K = \mathbb{Q}[a]$, y sea $f(x) = x^n + \sum_{i=0}^{n-1} \frac{a_i}{b_i} x^i$, con $a_i, b_i \in \mathbb{Z}$, su polinomio mínimo sobre $\mathbb{Q}$. Entonces, llamando $\alpha = a\prod_{i=0}^{n-1} b_i$, el polinomio mínimo de α será $f\left(\frac{x}{\prod_{i=0}^{n-1} b_i}\right) \cdot \left(\prod_{i=1}^{n-1} b_i\right)^n$, que es directo comprobar que tiene coeficientes enteros. Por tanto, α es entero algebraico y $K = \mathbb{Q}[a] = \mathbb{Q}[\alpha]$.

Para la segunda parte, basta coger base $1, \alpha, \ldots, \alpha^{n-1}$. □

Proposición 4.31. Dada una base de enteros $(\alpha_1, \ldots, \alpha_n)$, $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z} \setminus \{0\}$.

Demostración. Es directo ya que para todos i, j, $\alpha_i\alpha_j$ es entero, por tanto $\mathrm{Tr}(\alpha_i, \alpha_j)$ es entero. Además, no es 0 por 4.25. □

Es decir, toda base de enteros tiene discriminante entero. Podemos preguntarnos por aquellas bases de enteros cuyo discriminante es lo más pequeño posible:

Definición 4.32. Dada una base de enteros $(\alpha_1, \ldots, \alpha_n)$, decimos que es una base entera si para cualquier otra base de enteros $(\beta_1, \ldots, \beta_n)$, $|\Delta(\alpha_1, \ldots, \alpha_n)| \leq |\Delta(\beta_1, \ldots, \beta_n)|$.

Por 4.30 habrá alguna base entera para todo cuerpo de números K. Además, todas las bases de $K/\mathbb{Q}$ tienen discriminante del mismo signo por 4.23, por tanto todas las bases enteras tendrán el mismo discriminante. Así que tiene sentido definir el siguiente concepto:

Definición 4.33. Denotamos $d_K = \Delta(\alpha_1, \ldots, \alpha_n)$ siendo $\{\alpha_1, \ldots, \alpha_n\}$ cualquier base entera.

Vamos a ver una caracterización importante de las bases enteras: son exactamente las bases de enteros de $K/\mathbb{Q}$ que generan O_K como $\mathbb{Z}$-módulo.

Proposición 4.34. Una base de enteros $(\alpha_1, \ldots, \alpha_n)$ es base entera de K si y solo si todo elemento de O_K es de la forma $\sum_{i=1}^n a_i\alpha_i$, con $a_i \in \mathbb{Z}$.

Demostración. Si todo elemento de O_K es de forma $\sum_{i=1}^n a_i\alpha_i$, entonces para cada base $(\beta_1, \ldots, \beta_n)$ de enteros, la matriz de cambio de (β_i) a (α_i) tiene coeficientes enteros, por tanto por 4.24 el discriminante de la base (β_i) será un entero por el discriminante de la base (α_i). O sea que, en efecto, la base (α_i) tiene mínimo valor absoluto del discriminante.

Recíprocamente, sea $(\alpha_1, \ldots, \alpha_n)$ una base de enteros K. Supongamos que hay un elemento $\alpha \in O_K$ que tal que en su expresión $a_1\alpha_1 + \cdots + a_n\alpha_n$, con $a_n \in \mathbb{Q}$, no todos los a_n son enteros. Entonces podemos expresar $\alpha = \frac{a_1'\alpha_1 + \cdots + a_n'\alpha_n}{m}$, con a_i' y m enteros y el menor $m > 1$ posible. Sea ahora p un primo que divide a m, $m = p^k m^*$, con $p \nmid m^*$. Entonces hay cierto a_i con $p \nmid a_i'$ (ya que si no podríamos simplificar y m no sería mínimo). Suponemos que $p \nmid a_1$, por ejemplo (el resto de casos son similares). Multiplicando por $m^* p^{k-1}$, tenemos que:

$$m^* p^{k-1}\alpha = \frac{a_1'\alpha_1 + \cdots + a_n'\alpha_n}{p}, \text{ con } a_i' \text{ enteros.}$$

Ahora, como a_1' no es múltiplo de p, habrá a_1^* y λ enteros con $a_1'a_1^* = 1 + \lambda p$. Multiplicando ahora por a_1^*, tenemos:

$$a_1^* m^* p^{k-1}\alpha = \frac{(1+\lambda p)\alpha_1 + \cdots + a_1^* a_n''\alpha_n}{p} = \frac{\alpha_1 + \cdots + a_1^* a_n'\alpha_n}{p} + \lambda\alpha_1.$$

Por tanto, como tanto $a_1^* m^* p^{k-1}\alpha$ como $\lambda\alpha_1$ son enteros algebraicos, su diferencia, $\frac{\alpha_1 + \cdots + a_1^* a_n'\alpha_n}{p}$, será un entero algebraico. Ahora consideramos la base de enteros $\left(\frac{\alpha_1 + \cdots + a_1^* a_n'\alpha_n}{p}, \alpha_2, \ldots, \alpha_n\right)$. Su matriz de cambio a la base $(\alpha_1, \ldots, \alpha_n)$ es la siguiente:

$$M = \begin{pmatrix} \frac{1}{p} & 0 & \cdots & 0 & 0 \\ \frac{a_1^* a_2'}{p} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{a_1^* a_{n-1}'}{p} & 0 & \cdots & 1 & 0 \\ \frac{a_1^* a_n'}{p} & 0 & \cdots & 0 & 1 \end{pmatrix} \tag{4.2}$$

es decir, tiene determinante < 1. Por tanto por 4.23 esta nueva base tiene discriminante menor que $(\alpha_1, \ldots, \alpha_n)$. Por tanto, α_n no era una base entera, como queríamos. □

Corolario 4.35. Si $(\alpha_1, \ldots, \alpha_n)$ es una base entera y $(\beta_1, \ldots, \beta_n)$ es otra base de enteros, entonces hay k entero tal que $\Delta(\beta_1, \ldots, \beta_n) = k^2\Delta(\alpha_1, \ldots, \alpha_n)$. Además, $(\beta_1, \ldots, \beta_n)$ es base entera sii $k^2 = 1$.

Demostración. Se deduce de la proposición anterior y 4.24. □

Ejemplo 4.36. Retomando el ejemplo 4.28, tenemos que $\Delta(1, \alpha, \alpha^2) = -23$. Por tanto esta será una base entera. Ya que si no, habría una base entera $(\beta_1, \ldots, \beta_n)$ con $-23 = k^2\Delta(\beta_1, \ldots, \beta_n)$, siendo k y $\Delta(1, \alpha, \alpha^2)$ enteros, con $k > 1$. Esto es imposible, por ser 23 primo.

El mismo razonamiento de este ejemplo se generaliza de forma directa:

Proposición 4.37. Si $(\alpha_1, \ldots, \alpha_n)$ es una base de enteros de un cuerpo de números K y $\Delta(\alpha_1, \ldots, \alpha_n)$ es libre de cuadrados, entonces $(\alpha_1, \ldots, \alpha_n)$ es una base entera.

Y, si observamos la segunda parte de la demostración de 4.34, hemos descubierto un método para obtener bases enteras a partir de una base de enteros cualquiera:

Lema 4.38. *(Kummer)* Dada una base de enteros $(\alpha_1, \ldots, \alpha_n)$ de un cuerpo de números K, o bien es una base entera o existen $p \in \mathbb{Z}$ primo con $p^2|\Delta(\alpha_1, \ldots, \alpha_n)$, i entre 1 y n y enteros $0 \leq s_1, \ldots, s_{i-1} < p$ tales que

$$\alpha_i^* = \frac{s_1\alpha_1 + \cdots + s_{i-1}\alpha_{i-1} + \alpha_i}{p} \in O_K.$$

En este último caso, $\Delta(\alpha_1,\dots,\alpha_{i-1},\alpha_i^*,\alpha_{i+1},\dots,\alpha_n)=\frac{1}{p^2}\Delta(\alpha_1,\dots,\alpha_n)$.

Demostración. En la prueba de 4.34, nuestro p será el mismo p de la prueba, y el i será el mayor de los índices tales que $p\nmid a_i$ (en la demostración cogimos $i=1$, pero esto puede no ser así). Podemos suponer que $a_j=0$ para $j>i$ restando si no el entero algebraico $\frac{a_j}{p}$. Los números s_j serán los $a_i^*a_j'$ de la prueba, solo que podemos asegurarnos de que estén entre 0 y $p-1$ restándoles un múltiplo de p adecuado, ya que eso no afectará a que α_i^* sea entero. □

Ejemplo 4.39. Retomando el ejemplo 4.27, podemos usar el lema de Kummer para comprobar que, aunque $\Delta(1,\alpha,\alpha^2)$ no es libre de cuadrados, es base entera. Para ello basta comprobar que los elementos α_i^* del lema no son enteros algebraicos. En el caso $p=2$, tales elementos serían $\frac{1}{2},\frac{\alpha}{2},\frac{1+\alpha}{2},\frac{\alpha^2}{2},\frac{1+\alpha^2}{2},\frac{\alpha+\alpha^2}{2},\frac{1+\alpha+\alpha^2}{2}$. Se puede comprobar que ninguno de estos números es entero simplemente calculando sus normas y trazas. Con $p=3$, tendremos otros 12 casos y se puede comprobar también que no son enteros (se puede comprobar mirando las normas de los elementos, usando que $N(a+b\alpha+c\alpha^2)=a^3+2b^2+4c^3-6abc$), por tanto $\Delta(1,\alpha,\alpha^2)$ es una base entera, y la extensión tiene discriminante -2^23^3.

Definición 4.40. Se dice que un anillo de enteros R es monogénico cuando tiene una base entera de forma $(1,\alpha,\dots,\alpha^{n-1})$, para cierto α. Esto equivale a que exista α con $R=\mathbb{Z}[\alpha]$.

4.6 Cálculo de discriminantes. Aplicaciones

Proposición 4.41. Sea K cuerpo de números con $[K:\mathbb{Q}]=n$, sean $\alpha_1,\dots,\alpha_n\in K$ y sean $\sigma_1,\dots,\sigma_n$ las inmersiones de K en $\mathbb{C}$. Entonces,

$$\Delta(\alpha_1,\dots,\alpha_n)=\det(\sigma_i(\alpha_j))^2$$

Demostración. Llamando $A=(t(\alpha_i\alpha_j))$ y $B=(\sigma_k(\alpha_i))$, entonces $A=BB^t$, ya que $t(\alpha_i\alpha_j)=\sum_{k=1}^n\sigma_k(\alpha_i\alpha_j)$ para todos i,j. Por tanto $\Delta(\alpha_1,\dots,\alpha_n)=\det(A)=\det(B)^2=\det(\sigma_i(\alpha_j))^2$. □

Teorema 4.42. *(Stickelberger)* Sea K un cuerpo de números. Entonces d_K es 0 ó 1 módulo 4.

Demostración. Denotamos por A_n al subgrupo alternado del grupo simétrico S_n. Calculamos el determinante como suma de productos de permutaciones:

$$\sqrt{d_K}=|\sigma_i(a_j)|=\sum_{\tau\in A_n}\prod_{i=1}^n\sigma_i(a_{\tau(i)})-\sum_{\tau\in S_n\setminus A_n}\prod_{i=1}^n\sigma_i(a_{\tau(i)})$$

Denotemos por P a la primera suma y por N a la segunda.
Resulta que, dada cualquier σ_k inmersión se tiene que:

$$\begin{aligned}
\sigma_k(P+N) &= \sigma_k\left(\sum_{\tau\in A_n}\prod_{i=1}^n\sigma_i(a_{\tau(i)})+\sum_{\tau\in S_n\setminus A_n}\prod_{i=1}^n\sigma_i(a_{\tau(i)})\right)\\
&= \sum_{\tau\in A_n}\prod_{i=1}^n(\sigma_k\circ\sigma_i)(a_{\tau(i)})+\sum_{\tau\in S_n\setminus A_n}\prod_{i=1}^n(\sigma_k\circ\sigma_i)(a_{\tau(i)})\\
&= \sum_{\tau\in A_n}\prod_{i=1}^n\sigma_i(a_{\tau(i)})+\sum_{\tau\in S_n\setminus A_n}\prod_{i=1}^n\sigma_i(a_{\tau(i)})\quad\text{(Cambia el orden de las sumas si } \sigma_k\in S_n\setminus A_n)\\
&= P+N
\end{aligned}$$

Con PN vemos de forma similar que $\sigma_k(PN)=PN$.
Como $P+N$ y PN son invariantes bajo toda inmersión están en $\mathbb{Q}$. Además por su definición son enteros algebraicos (ya que son polinomios en las a_i, que son enteros algebraicos) luego están en $\mathbb{Z}$. Ahora usemos la identidad

$$d_K=(P-N)^2=(P+N)^2-4PN\in\mathbb{Z}$$

Módulo 4 solo son residuos cuadráticos 0 y 1 así que $d_k\equiv 0,1 \mod 4$. □

Proposición 4.43. Sea $K = \mathbb{Q}[\alpha]$ cuerpo de números, con $(1, \alpha, \ldots, \alpha^{n-1})$ base de $K/\mathbb{Q}$. Entonces

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)), \text{ donde } f = \min_{\mathbb{Q}}(\alpha).$$

Otra forma de calcularlo: si $\alpha_1, \ldots, \alpha_n$ son las raíces de $\min_{\mathbb{Q}}(\alpha)$ en $\mathbb{C}$,

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j}(\alpha_j - \alpha_i)^2, \text{ es decir, el discriminante de } \min_{\mathbb{Q}}(\alpha).$$

Demostración.

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = |\sigma_i(\alpha^j)|^2 = |\sigma_i(\alpha)^j|^2 = |(\alpha_i)^j|^2$$

Esto es un determinante de Vandermonde así que

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = |(\alpha_i)^j|^2 = \prod_{i<j}(\alpha_j - \alpha_i)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_j - \alpha_i)$$

Fijémonos en que $f = \min_{\mathbb{Q}}(\alpha) = \prod_{i=1}^{n}(x - \alpha_i)$ luego

$$f'(x) = \sum_{k=1}^{n} \prod_{\substack{i=1 \\ i \neq k}}^{n}(x - \alpha_i) \Rightarrow \ f'(\alpha_k) = \prod_{\substack{i=1 \\ i \neq k}}^{n}(\alpha_k - \alpha_i)$$

De esta forma

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_j - \alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} f'(\alpha_j) =$$

$$(-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} f'(\sigma_j(\alpha)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} \sigma_j(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha))$$

La penúltima identidad se da porque los coeficientes de f' son racionales y $\sigma_j(q) = q \ \forall q \in \mathbb{Q}$. □

La segunda fórmula que hemos dado para el discriminante de la base entera de potencias es el discriminante del polinomio mínimo de α. Por tanto se puede expresar como polinomio en función de los coeficientes de $\min_{\mathbb{Q}}(\alpha)$ (ya que el discriminante de un polinomio tiene una expresión como determinante en función de los coeficientes del polinomio).

Ejemplo 4.44. Sea $f = x^2 + bx + c$. Dependiendo del signo del discriminante $b^2 - 4c$ tenemos 2 raíces imaginarias, una raíz real doble o dos raíces reales.

$$f = x^2 + bx + c = (x - \alpha_1)(x - \alpha_2) \Rightarrow \ (\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b^2) - 4ac = b^2 - 4ac$$

Luego

$$(\alpha_1 - \alpha_2)^2 = \delta_1^2 - 4\delta_2,$$

donde $\delta_1 = \alpha_1 + \alpha_2$ y $\delta_2 = \alpha_1\alpha_2$ son los polinomios simétricos elementales evaluados en α_1 y α_2, que a su vez, al evaluarlos, coinciden (salvo quizá por el signo) con los coeficientes del polinomio mínimo.

Esto será generalizable a extensiones de cualquier grado, ya que el discriminante es $\Delta(\alpha_1, \ldots, \alpha_n) = \prod_{i<j}(\alpha_j - \alpha_i)^2$, un polinomio simétrico en las α_i, por tanto por el teorema fundamental de los polinomios simétricos, tendremos que $\Delta(\alpha_1, \ldots, \alpha_n)$ será un polinomio en función de $\delta_1, \ldots, \delta_n$, los polinomios simétricos elementales en $\alpha_1, \ldots, \alpha_n$ (que a su vez son, salvo signo, los coeficientes de $\min_{\mathbb{Q}}(\alpha)$).

Ejemplo 4.45. Sea ahora $f = x^3 + ax^2 + bx + c$. En este caso el polinomio simétrico en 3 variables es

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = F(s_1, s_2, s_3)$$

donde $(s_1, s_2, s_3) = (x_1 + x_2 + x_3, x_1x_2 + x_2x_3 + x_3x_1, x_1x_2x_3)$. Pues salen 27 sumandos y hay que aplicar el algoritmo del Teorema Fundamental de los polinomios simétricos para encontrar F.

Jjaj, lo ha dejado como ejercicio lol.

Apliquemos la fórmula que hemos visto antes al caso ciclotómico y cúbico.

Ejemplo 4.46. Sea $\omega = \omega_p := e^{\frac{2\pi i}{p}}$ con $p \in \mathbb{Z}$ primo impar. Entonces, por 4.22 y 4.34, $(1, \omega, \dots, \omega^{p-2})$ es base entera de $O_K = O_{\mathbb{Q}(\omega)}$. Así que

$$d_{\mathbb{Q}(\omega)} = \Delta(1, \omega, \dots, \omega^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = (-1)^{\frac{p-1}{2}} N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega))$$

El signo depende de si p es 1 ó 3 módulo 4.
Calculemos la norma de $\Phi_p'(\omega)$:

$$x^p - 1 = (x-1)\Phi_p(x) \Rightarrow\ px^{p-1} = \Phi_p(x) + (x-1)\Phi_p'(x) \Rightarrow\ p\omega^{p-1} = \Phi_p(\omega) + (\omega-1)\Phi_p'(\omega) = (\omega-1)\Phi_p'(\omega) = -\lambda\Phi_p'(\omega) \Rightarrow$$

$$N(\Phi_p'(\omega)) = N\left(-\frac{p\omega^{p-1}}{\lambda}\right) = N(p)N(\omega)^{p-1}/N(-\lambda)$$

La norma de p es p^{p-1}, la de ω es 1 y la de λ y $-\lambda$ coincide pues p es impar. Así que la norma de $-\lambda$ es p. Luego

$$d_{\mathbb{Q}(\omega)} = (-1)^{\frac{p-1}{2}} N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = (-1)^{\frac{p-1}{2}} \frac{p^{p-1}}{p} = (-1)^{\frac{p-1}{2}} p^{p-2}$$

En primer lugar, el único primo que divide al discriminante es p.
En segundo lugar, el exponente $p-2$ es impar. De esta forma aunque consigamos bases de números con una norma más pequeña siempre quedará una p en el discriminante y por tanto

$$\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}(\omega).$$

Así que $(-1)^{\frac{p-1}{2}} p$ es un cuadrado en $\mathbb{Q}(\omega)$. De esta forma, $\mathbb{Q}(\omega)$ contiene al cuerpo cuadrático $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.
En tercer lugar, el grupo de Galois de $\mathbb{Q}(\omega)/\mathbb{Q}$ es isomorfo a $\mathbb{Z}_p^\times$, que es cíclico. Además, la extensión es normal y separable luego de Galois. $\mathcal{G}\mathrm{al}(\mathbb{Q}(\omega)/\mathbb{Q})$ solo tiene un subgrupo de índice 2 al que le corresponde una única subextensión de dimensión 2. Así que ese único cuerpo cuadrático es precisamente $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.

Ejemplo 4.47. Sea $f = x^3 + ax + b$ irreducible. Vamos a calcular su discriminante. Sea $\alpha :\ f(\alpha) = 0$, entonces

$$\Delta(1, \alpha, \alpha^2) = -N_{K/\mathbb{Q}}(f'(\alpha)) =$$

Tenemos que $f'(\alpha) = 3\alpha^2 + a$, saquemos su polinomio mínimo:

$$x = 3\alpha^2 + a = 3(-a - b\alpha^{-1}) + a \Rightarrow\ \alpha = \frac{-3b}{x + 2a} \Rightarrow$$

$$0 = \alpha^3 + a\alpha + b = \left(\frac{-3b}{x+2a}\right)^3 + a\left(\frac{-3b}{x+2a}\right) + b \Rightarrow$$

$$(-3b)^3 + a(x+2a)^2(-3b) + b(x+2a)^3 = 0 \Rightarrow\ \min_{\mathbb{Q}}(f'(\alpha)) = (x+2a)^3 - 3a(x+2a)^2 - 27b^2$$

El término independiente es $8a^3 - 12a^3 - 27b^2 = -4a^3 - 27b^2$ luego

$$\Delta(1, \alpha, \alpha^2) = -4a^3 - 27b^2.$$

Si ahora tomamos por ejemplo $f = x^3 - 2$, su discriminante es

$$d(f) = -4a^3 - 27b^2 = -27 \cdot 4 = -3^3 \cdot 2^2.$$

Ejemplo 4.48. Sacar el discriminante $\Delta(1, \alpha, \dots, \alpha^{n-1})$ para α raíz de $x^n + ax + b$, de $x^n + ax^{n-1} + b,\ b \neq 0$

y de $x^n + ax^m + b$.[1]

Sea $f = x^n + ax + b$ y sea $\alpha :\ f(\alpha) = 0$, entonces

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)) =$$

Tenemos que $f'(\alpha) = n\alpha^{n-1} + a$, para sacar su polinomio mínimo se tiene en cuenta que $\alpha^{n-1} + a + b\alpha^{-1} = 0 \Rightarrow$

$$x = n\alpha^{n-1} + a = n(-a - b\alpha^{-1}) + a \Rightarrow\ \alpha^{-1} = \frac{a - x - na}{nb}.$$

Seguimos operando para obtener un candidato a polinomio mínimo:

$$x = n\alpha^{n-1} + a = n\left(\frac{nb}{a - x - na}\right)^{n-1} + a = n\left(\frac{-nb}{x + na - a}\right)^{n-1} + a \Rightarrow\ x(x+na-a)^{n-1} = n(-nb)^{n-1} + a(x+na-a)^{n-1}$$

Para comprobar que $\min_{\mathbb{Q}}(n\alpha^{n-1} + a) = x(x + na - a)^{n-1} - n(-nb)^{n-1} - a(x + na - a)^{n-1}$, sustituimos $x = n\alpha^{n-1} + a$. En primer lugar $\alpha(x + na - a) = \alpha(n\alpha^n n - 1 + na) = n(\alpha^n + a\alpha) = -nb$. Como $\alpha \neq 0$, mutiplicamos por α^{n-1} :

$$\alpha^{n-1}(x(x+na-a)^{n-1} - n(-nb)^{n-1} - a(x+na-a)^{n-1}) = (n\alpha^{n-1} + a)(-nb)^{n-1} - n(nb)^{n-1}\alpha^{n-1} - a(-nb)^{n-1} =$$

$$(-nb)^{n-1}((n\alpha^{n-1} + a) - n\alpha^{n-1} - a) = 0$$

El término independiente de $\min_{\mathbb{Q}}(n\alpha^{n-1} + a)$ es $-n(-nb)^{n-1} + a(na - a)^{n-1}$ luego

$$N(f'(\alpha)) = -n(-nb)^{n-1} + a(na-a)^{n-1} = b^{n-1}(-n)^n + (n-1)^{n-1}a^n \Rightarrow\ d(f) = (-1)^{\frac{n(n-1)}{2}}(b^{n-1}(-n)^n + (n-1)^{n-1}a^n)$$

Ejemplo 4.49. Ahora calculemos el discriminante de $f = x^n + ax^{n-1} + b$. En primer lugar

$$f'(\alpha) = n\alpha^{n-1} + (n-1)a\alpha^{n-2} = \alpha^{n-2}(n\alpha + (n-1)a)$$

Luego $N(f'(\alpha)) = N(\alpha)^{n-2}N(n\alpha + (n-1)a)$. La norma de α es b, ahora hay que calcular $N(n\alpha + (n-1)a)$:

$$x = n\alpha + (n-1)a \Rightarrow\ \alpha = \frac{x - (n-1)a}{n} \Rightarrow\ 0 = \left(\frac{x - (n-1)a}{n}\right)^n + a\left(\frac{x - (n-1)a}{n}\right)^{n-1} + b \Rightarrow$$

$$\min_{\mathbb{Q}}(n\alpha + (n-1)a) = (x - (n-1)a)^n + an(x - (n-1)a)^{n-1} + bn^n$$

Su término independiente es $(-(n-1)a)^n + an(-(n-1)a)^{n-1} + bn^n \Rightarrow$

$$N(f'(\alpha)) = b^{n-2}((-(n-1)a)^n + an(-(n-1)a)^{n-1} + bn^n) =$$

$$(-1)^n b^{n-2}a^n((n-1)^n - n(n-1)^{n-1}) + b^{n-1}n^n = (-1)^{n+1}b^{n-2}a^n(n-1)^{n-1} + b^{n-1}n^n$$

Así que

$$\Delta(1, \alpha, \ldots, \alpha^n) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}}((-1)^{n+1}b^{n-2}a^n(n-1)^{n-1} + b^{n-1}n^n)$$

Ejemplo 4.50. El caso $x^n + ax^m + b$ con $m < n$ es más complicado.

Recordemos que con $\alpha^3 - \alpha - 1 = 0$ y considerando $K = \mathbb{Q}(\alpha)$ se tiene que $\Delta(1, \alpha, \alpha^2) = -23$. Como es primo deducimos que es base entera y por tanto $d(1, \alpha, \alpha^2) = -23$.
Consideremos ahora $\beta^3 + \beta - 1$ y $F = \mathbb{Q}(\beta)$:

$$\Delta(1, \beta, \beta^2) = -4(1)^3 - 27(-1)^2 = -4 - 27 = -31.$$

Así que el discriminante es -31 por ser primo en $\mathbb{Z}$.

[1] Justificar que es irreducible creo.

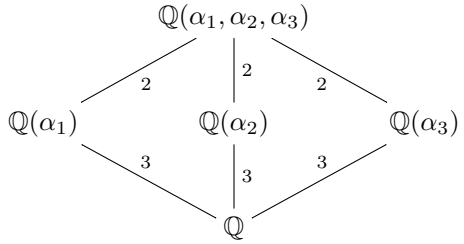
Una propiedad sobre K y F muy difícil de demostrar pero que obtenemos de forma automática es que ni son el mismo cuerpo ni son isomorfos. Esto se debe a que el discriminante es distinto.
Hay que tener cuidado porque si dos cuerpos tiene la misma dimensión e igual discriminante no tienen por qué ser isomorfos.

Ejemplo 4.51. Sea $K = \mathbb{Q}(\alpha)$ con $f = \min_{\mathbb{Q}}(\alpha) = x^3 - 3x - 1$. Usando la fórmula $d(f) = \Delta(1, \alpha, \alpha^2) = -4b^3 - 27a^2 = -4(-3)^3 - 27(-1)^2 = 4(3^3) - 3^3 = 3^4 = 81$.

Pequeño inciso teoría de Galois si eso meter en anexo. La característica de $\mathbb{Q}$ es 0, $f = x^3 - 3x - 1$ es irreducible en $\mathbb{Q}$ pues la única posible raíz es 1 y no anula el polinomio. Al considerar el grupo de Galois de $\mathbb{Q}(f)/\mathbb{Q}$ sabemos 3 divide a su orden y que es subgrupo de S_3.
Por tanto se tienen dos opciones, el grupo de Galois es S_3 o es el cíclico de 3 elementos. Se tiene

$$d(f) = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 \in \mathbb{Z}, \text{ donde } \alpha_1, \alpha_2, \alpha_3 \text{ son las raíces de } f.$$

Podemos determinar de qué grupo se trata en función de si $d(f)$ es cuadrado exacto o no. Si lo es tenemos el cíclico de 3 elementos mientras que si no lo es se trata de S_3.
De esta forma, como tenemos que $d(x^3-3x-1) = 81$ sabemos que el grupo de Galois es el cíclico de 3 elementos y por tanto $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha)$ con $\alpha_1 = \alpha$. Luego $\mathbb{Q}(f) = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3)$ con $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$.
En los casos anteriores $f = x^3 - x - 1$ ó $g = x^3 + x - 1$ el grupo de Galois es S_6 y por tanto:



Ejercicio 4.52. Comprobar que $\{1, \alpha, \alpha^2\}$ es base entera con $K = \mathbb{Q}(\alpha)$ y $\alpha^3 - 3\alpha - 1 = 0$. Como $d(f) = 81$ tenemos que probar el primo 3. Las opciones son

$$\frac{s_0 + \alpha}{3}, \qquad \frac{s_0 + s_1\alpha + \alpha^2}{3}.$$

En primer lugar calculamos

$$N(a + b\alpha + c\alpha^2) = \det(\lambda_{a+b\alpha+c\alpha^2}) = \begin{vmatrix} a & c & b \\ b & a+3c & c+3b \\ c & b & a+3c \end{vmatrix}.$$

Pues $\alpha(a+b\alpha+c\alpha^2) = a\alpha+b\alpha^2+(3\alpha+1)c = c+(a+3c)\alpha+b\alpha^2$ y $\alpha^2(a+b\alpha+c\alpha^2) = \alpha(c+(a+3c)\alpha+b\alpha^2) = c\alpha + (a+3c)\alpha^2 + b(3\alpha+1) = b + (c+3b)\alpha + (a+3c)\alpha^2$.
Luego

$$N\left(\frac{s_0+\alpha}{3}\right) = \frac{1}{27}N(s_0+\alpha) = \frac{1}{27}\begin{vmatrix} s_0 & 0 & 1 \\ 1 & s_0 & 3 \\ 0 & 1 & s_0 \end{vmatrix} = \frac{1}{27}(s_0^3 - 3s_0 + 1)$$

Módulo 3 el numerador solo se anula si $s_0 \equiv_3 -1$. En ese caso tomamos módulo 9 :

$$(3k-1)^3 \equiv_9 -1 \Rightarrow (3k-1)^3 - 3(3k-1) + 1 \equiv_9 -3(3k-1) \equiv_9 3 \not\equiv_9 0.$$

Luego $N\left(\frac{s_0+\alpha}{3}\right) \notin \mathbb{Z}$. Ahora vamos con

$$N(\frac{s_0+s_1\alpha+\alpha^2}{3}) = \frac{1}{27}\begin{vmatrix} s_0 & 1 & s_1 \\ s_1 & s_0+3 & 1+3s_1 \\ 1 & s_1 & s_0+3 \end{vmatrix} = \frac{1}{27}\left(s_0(s_0+3)^2+1+3s_1+s_1^3-2s_1(s_0+3)-s_0s_1(1+3s_1)\right)$$

Tomando módulo 3 se tiene

$$s_0(s_0+3)^2+1+3s_1+s_1^3-2s_1(s_0+3)-s_0s_1(1+3s_1) \equiv_3 s_0^3+1+s_1^3-2s_1s_0-s_0s_1 \equiv_3 s_0+1+s_1$$

Así que para cancelar el numerador se necesita que $s_1 \equiv_3 -s_0-1$. Tomando módulo 27 e introduciendo $s_1 = 3k-s_0-1$ en Symbolab:

$$s_0(s_0+3)^2+1+3s_1+s_1^3-2s_1(s_0+3)-s_0s_1(1+3s_1) = -3s_0^3+27ks_0^2+27ks_0+9s_0-54k^2x+27k^3+3-27k^2 \equiv_{27} -3s_0^3+9s_0+3$$

Esta última expresión es 0 si y solo si

$$-s_0^3+3s_0+1 \equiv_9 0.$$

Si $s_0 \equiv_3 0$ entonces $-s_0^3+3s_0+1 \equiv_9 1 \not\equiv_9 0$.
Si $s_0 \equiv_3 1$ entonces $-s_0^3+3s_0+1 \equiv_9 3s_0 \not\equiv_9 0$.
Si $s_0 \equiv_3 -1$ entonces $-s_0^3+3s_0+1 \equiv_9 2+3s_0 \equiv_3 2+3(3k-1) \equiv_9 2-3 \equiv_9 -1 \not\equiv_9 0$.
Luego efectivamente $\{1,\alpha,\alpha^2\}$ es base entera. □

Ejercicio 4.53. Ahora que sabemos que $\{1,\alpha,\alpha^2\}$ es base entera con $K=\mathbb{Q}(\alpha)$ y $\alpha^3-3\alpha-1=0$. Encontrar coeficientes $a_0,a_1,a_2 \in \mathbb{Z}$ tales que $\alpha' = a_0+a_1\alpha+a_2\alpha^2$ siendo $\alpha' \neq \alpha$ raíz de $\min_{\mathbb{Q}}(\alpha)$.
Busquemos $\beta \in K$ tal que $\alpha\beta = \sigma(\alpha)$. Para ello, supongamos que existe, entonces

$$0 = \sigma(\alpha)^3-3\sigma(\alpha)-1 = (\alpha\beta)^3-3\alpha\beta-1 = \beta^3(3\alpha+1)-3\beta\alpha-1 = 3\alpha(\beta^3-\beta)+\beta^3-1 = (\beta-1)(3\alpha\beta(\beta+1)+\beta^2+\beta+1) =$$

$\beta \neq 1$ pues suponemos que σ es una inmersión no trivial. Entonces

$$0 = 3\alpha\beta(\beta+1)+\beta^2+\beta+1 = (3\alpha+1)\beta^2+(3\alpha+1)\beta+1$$

Si sacamos el discriminante como polinomio en β vemos que necesitamos encontrar, si es que existe, un elemento $\gamma = a+b\alpha+c\alpha^2,\ a,b,c \in \mathbb{Z}$ tal que $\gamma^2 = (3\alpha+1)(3\alpha-3) = 9\alpha^2-6\alpha-3$. Haciendo algunos cálculos podemos hayar que $\gamma = 1+\alpha-2\alpha^2$ funciona. De esta forma

$$\beta = \frac{-(3\alpha+1)\pm\sqrt{(3\alpha+1)(3\alpha-3)}}{2(3\alpha+1)} = \frac{-(3\alpha+1)\pm(1+\alpha-2\alpha^2)}{2(3\alpha+1)} = \frac{1}{2}(-(3\alpha+1)\pm(1+\alpha-2\alpha^2))(9\alpha^2-3\alpha-26) =$$

Hemos invertido el elemento resolviendo un sistema de ecuaciones lineales.
Entendemos que dependiendo de qué signo tomemos trataremos con σ ó σ^{-1}. Como no la hemos especificado tomamos el + para que se nos simplifique un poco todo:

$$\beta = \frac{1}{2}(-(3\alpha+1)+(1+\alpha-2\alpha^2))(9\alpha^2-3\alpha-26) = (-\alpha-\alpha^2)(9\alpha^2-3\alpha-26) = -6-\alpha+2\alpha^2$$

Si hubiésemos tomado el $-$ nos habría quedado $\beta = 5+\alpha-2\alpha^2$.
Volviendo a tomar $\beta = -6-\alpha+2\alpha^2$ se tiene que

$$\sigma(\alpha) = \alpha\beta = \alpha(-6-\alpha+2\alpha^2) = -\alpha^2+2.$$

Ejemplo 4.54. *Cuerpo de números sin base entera de potencias, se le atribuye a Dedekind* Sea el cuerpo $\mathbb{Q}[\alpha]$, con $\min_{\mathbb{Q}}(\alpha) = x^3-x^2-2x-8$.

1. $\min_{\mathbb{Q}}(\alpha)$ es irreducible. Esto pasa porque si no, $\min_{\mathbb{Q}}(\alpha)$ tendría raíces enteras, y es directo comprobar que esto no pasa.
2. $\Delta(1,\alpha,\alpha^2) = -4\cdot 503$. Para comprobar esto, usamos la fórmula $\Delta(1,\alpha,\alpha^2) = -N(f'(\alpha)) = -N(3\alpha^2-$

$2\alpha - 2$). Operando vemos que la matriz de $\lambda_{3\alpha^2-2\alpha-2}$ en base $(1, \alpha, \alpha^2)$ es

$$\begin{pmatrix} -2 & 24 & 8 \\ -2 & 4 & 26 \\ 3 & 1 & 5 \end{pmatrix}$$

y su determinante es $2012 = 4 \cdot 503$, así que el enunciado es cierto.

3. $\beta = \frac{4}{\alpha}$ es entero algebraico, y $\Delta(1, \alpha, \beta) = -503$. Para ver esto, vemos que como $\alpha = \frac{4}{\beta}$, sustituyendo $\frac{4}{\beta}$ en $\min_{\mathbb{Q}}(\alpha)$ y multiplicando por β^3 vemos que el polinomio mínimo de β es $x^3 + x^2 + 2x - 8$, que está en $\mathbb{Z}[x]$. Para ver que el discriminante es -503, basta ver que $\beta = -1 - \frac{\alpha}{2} + \frac{\alpha^2}{2}$, por tanto la matriz de cambio de base de $(1, \alpha, \beta)$ a $(1, \alpha, \alpha^2)$ tiene determinante $\frac{1}{2}$ y por tanto $\Delta(1, \alpha, \beta) = \frac{1}{4}\Delta(1, \alpha, \alpha^2) = -503$.

4. No hay ninguna base entera de potencias, es decir, de forma $(1, \gamma, \gamma^2)$. Como 503 es primo, está claro que $(1, \alpha, \beta)$ es una base entera.

   Supongamos que existe tal γ. Entonces tendríamos que tener que $-503 = \Delta(1, \gamma, \gamma^2)$. Consideremos la matriz de paso P de la base $\{1, \gamma, \gamma^2\}$ en la base $\{1, \alpha, \beta\}$. El determinante de P debe ser ± 1. Escribamos

   $$\gamma = a + b\alpha + c\beta, \quad a, b, c \in \mathbb{Z} \Rightarrow \ \gamma^2 = a^2 + b^2\alpha^2 + c^2\beta^2 + 2ab\alpha + 2ac\beta + 2bc\alpha\beta$$

   En primer lugar $\alpha\beta = 4$, los únicos elementos que no están expresados en la base $\{1, \alpha, \beta\}$ son $b^2\alpha^2$ y $c^2\beta^2$ así que toca calcularlos.

   $$0 = \alpha^3 - \alpha^2 - 2\alpha - 8 \Rightarrow \ \beta = \frac{4}{\alpha} = \frac{\alpha^2 - \alpha - 2}{2} \Rightarrow \ \alpha^2 = 2\beta + \alpha + 2$$

   Haciendo cálculos llegamos también a que

   $$\beta^2 = \frac{(\alpha^2 - \alpha - 2)^2}{4} = \frac{-4\beta + 8\alpha + 8}{4} - \beta + 2\alpha + 2.$$

   Así que

   $$\gamma^2 = a^2 + b^2(2\beta + \alpha + 2) + c^2(-\beta + 2\alpha + 2) + 2ab\alpha + 2ac\beta + 8bc = a^2 + 8bc + 2b^2 + 2c^2 + (b^2 + 2c^2 + 2ab)\alpha + (2b^2 - c^2 + 2ac)\beta$$

   Ya podemos escribir la matriz de paso P :

   $$P = \begin{pmatrix} 1 & a & a^2 + 8bc + 2b^2 + 2c^2 \\ 0 & b & b^2 + 2c^2 + 2ab \\ 0 & c & 2b^2 - c^2 + 2ac \end{pmatrix} \Rightarrow \ |P| = \begin{vmatrix} 1 & a & a^2 + 8bc + 2b^2 + 2c^2 \\ 0 & b & b^2 + 2c^2 + 2ab \\ 0 & c & 2b^2 - c^2 + 2ac \end{vmatrix} =$$

   $$\begin{vmatrix} b & b^2 + 2c^2 + 2ab \\ c & 2b^2 - c^2 + 2ac \end{vmatrix} = 2b^3 - c^2b - b^2c - 2c^3 = 2(b^3 - c^3) - bc(b + c)$$

   Ahora, tomando módulo 2 vemos que $|P| \equiv_2 bc(b + c)$, si $bc \not\equiv_2 0$ entonces $b \equiv_2 c$ y por tanto $b + c \equiv_2 0$. Es decir, $|P|$ siempre es par luego no puede ser ± 1.

Volvemos un poco a ciclotómicos. Tomamos $\Phi_9 = x^6 + x^3 + 1$, es irreducible[2] y tiene como raíces $\omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^8$ donde $\omega := e^{\frac{2\pi i}{9}}$.
El grupo de Galois de $\mathbb{Q}(\omega)/\mathbb{Q}$ es isomorfo a $\mathbb{Z}_9^\times$.

Proposición 4.55 (Gauss)**.** El grupo $\mathbb{Z}_n^\times$ es cíclico si y solo si n es 2,4, p^m o $2p^m$ con $p > 2$ primo y $m \in \mathbb{N}$. □

Proposición 4.56. Sea $a \in \mathbb{Z}$ tal que $\overline{a}$ es generador de $\mathbb{Z}_p^\times$. Entonces, o bien $\overline{a}$ o bien $\overline{a + p}$ son generadores de $\mathbb{Z}_{p^2}^\times$. Además, dado $a \in \mathbb{Z}$ tal que $\overline{a}$ es generador de $\mathbb{Z}_{p^2}^\times$, $\overline{a}$ es generador de $\mathbb{Z}_{p^n}^\times$ para toda $n \in \mathbb{N}$.

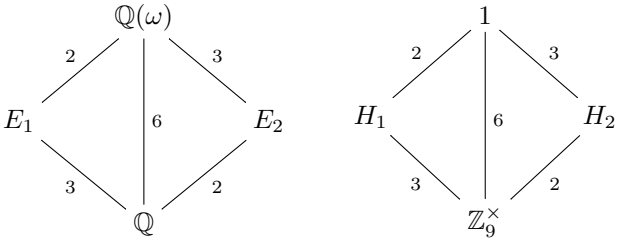
Demostración. Para la primera parte, si $\overline{a}$ tiene orden $p - 1$ en $\mathbb{Z}_p^\times$, tendrá orden múltiplo de $p - 1$ en $\mathbb{Z}_{p^2}^\times$,

[2] En el apéndice B veremos este caso particular. Si hay tiempo se meterá el general.

y lo mismo se puede decir de $\overline{a+p}$. Además, $(a+p)^{p-1} \equiv_{p^2} a^{p-1} + p(p-1)a \not\equiv_{p^2} a^{p-1}$. Por tanto, a^{p-1} y $(a+p)^{p-1}$ son distintos módulo p^2. Sea $g \in \{a, a+p\}$ tal que $\overline{g^{p-1}} \neq 1$ en $\mathbb{Z}_{p^2}^\times$. Entonces, por lo que hemos visto antes $\overline{g}$ tiene orden múltiplo de $p-1$, mayor que $p-1$ y divisor de $p(p-1)$, que es el orden de $\mathbb{Z}_{p^2}^\times$. Así que $o(g) = p(p-1)$, es decir, g es generador de $\mathbb{Z}_{p^2}^\times$.

Para la segunda parte, usamos inducción. Basta darse cuenta de que hay $\Phi(p^{n-1}(p-1)) = p^{n-2}(p-1)\Phi(p-1)$ generadores de $\mathbb{Z}_{p^n}^\times$ y hay $\Phi(p^n(p-1)) = p^{n-1}(p-1)\Phi(p-1)$ generadores de $\mathbb{Z}_{p^{n+1}}^\times$. Además, a cada generador de $\mathbb{Z}_{p^{n+1}}^\times$, su clase en $\mathbb{Z}_{p^n}^\times$ será también un generador de $\mathbb{Z}_{p^n}^\times$. Osea, que cualquier generador de $\mathbb{Z}_{p^{n+1}}^\times$ es congruente módulo p^n a alguna de las $p^{n-2}(p-1)\Phi(p-1)$ clases que generan $\mathbb{Z}_{p^n}^\times$. Esto solo nos deja $p \cdot p^{n-2}(p-1)\Phi(p-1) = p^{n-1}(p-1)\Phi(p-1)$ posibles clases que generan $\mathbb{Z}_{p^{n+1}}^\times$ (ya que cada clase de $\mathbb{Z}_{p^n}^\times$ corresponde a p clases de $\mathbb{Z}_{p^{n+1}}^\times$). Pero sabemos que hay exactamente $p^{n-1}(p-1)\Phi(p-1)$ generadores de $\mathbb{Z}_{p^{n+1}}^\times$, así que las clases que generan $\mathbb{Z}_{p^{n+1}}^\times$ son exactamente las asociadas a las clases de $\mathbb{Z}_{p^2}^\times$ que generan $\mathbb{Z}_{p^2}^\times$, que es esencialmente lo que pide el enunciado. □

Ejemplo 4.57. Ahora usamos el teorema de la correspondencia de Galois para describir las subsextensiones de $\mathbb{Q}(x^6+x^3+1)/\mathbb{Q}$:



Como todos los subgrupos son normales tanto $E_1/\mathbb{Q}$ como $E_2/\mathbb{Q}$ son extensiones de Galois. Centrémonos en $E_1/\mathbb{Q}$, necesitamos un automorfismo en $\mathbb{Q}(\omega)$ de orden 2 que deje fijo a los racionales, probemos con la conjugación $\omega \mapsto \overline{\omega}$. Deja fijos a los reales luego:

$$\omega^k + \omega^{-k} = \omega^k + \overline{\omega}^k = 2\,\mathrm{Re}(\omega) \in \mathbb{R},\ k = 1, 2, 4$$

Podemos generar estos 3 elementos con $k = 1$: $\omega + \overline{\omega}$ pues

$$(\omega + \overline{\omega})^2 = \omega^2 + \overline{\omega}^2 + 2; \quad (\omega^2 + \overline{\omega}^2)^2 = \omega^4 + \overline{\omega}^4 + 2.$$

De esta forma $E_1 = \mathbb{Q}(\omega + \overline{\omega})$. Calculemos el polinomio mínimo de $\omega + \overline{\omega}$:

$$(\omega + \overline{\omega})^3 = \omega^3 + \overline{\omega}^3 + 3(\omega + \overline{\omega}) \Rightarrow\ x^3 = \omega^3 + \omega^6 + 3x = 3x - 1.$$

Ahora, esto nos permite deducir también que $\min_{\mathbb{Q}}(-\omega - \overline{\omega}) = x^3 - 3x - 1$.

Ejercicio 4.58. Encontrar otra extensión cúbica cíclica de dimensión 3 a partir de $\mathbb{Q}(\omega)$ donde $\omega = \omega_7 := e^{\frac{2\pi i}{7}}$ y estudiar si el cuerpo extensión cúbica es isomorfo ó igual al anterior.

La idea es la misma. Buscamos $K = \mathbb{Q}(\omega_7 + \omega_7^{-1})$.

$$\min_{\mathbb{Q}}(\omega_7) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \Rightarrow\ \omega^{-1} + \omega^{-2} + \omega^{-3} + \omega^3 + \omega^2 + \omega + 1 = 0.$$

Hacemos $x = \omega + \omega^{-1},\ x^2 = \omega^2 + \omega^{-2} + 2,\ x^3 = \omega^3 + \omega^{-3} + 3x$ luego

$$0 = 1 + (\omega + \omega^{-1}) + (\omega^2 + \omega^{-2}) + (\omega^3 + \omega^{-3}) = 1 + x + (x^2 - 2) + (x^3 - 3x) \Rightarrow \min_{\mathbb{Q}}(\omega_7 + \omega_7^{-1}) = x^3 + x^2 - 2x - 1$$

Si trasladamos el polinomio, es decir, $y = x + \frac{1}{3}$ el discriminante no varía pues es el producto de restas de raíces así que 1/3 desaparece. De esta forma:

$$(y-1/3)^3+(y-1/3)^2-2(y-1/3)-1 = (y^3-y^2+y/3-1/27)+(y^2-2y/3+1/9)+(-2y+2/3)-1 = y^3+ay+b.$$

Donde $a = -7/3$ y $b = -7/27$. Usando la fórmula que ya calculamos:

$$-4a^3 - 27b^2 = 4(7^3/3^3) - 27(7^2/27^2) = \frac{4 \cdot 7^3 - 7^2}{27} = 49\frac{4 \cdot 7 - 1}{27} = 49$$

El discriminante es distinto de 81 así que toda esperanza de establecer un isomorfismo de cuerpos se esfuma.

En el ejemplo 4.57 hemos visto que el grupo de Galois del cuerpo de descomposición de $x^3 - 3x - 1$ es abeliano, y que de hecho dicho cuerpo está contenido en $\mathbb{Q}[\omega_9]$, siendo ω_9 raíz novena de la unidad. Esto no es una casualidad, de hecho se tiene el siguiente teorema que enunciamos sin demostrar:

Teorema 4.59. Sea K un cuerpo de números tal que $K/\mathbb{Q}$ es una extensión de Galois con grupo de Galois abeliano (se dice en ese caso que la extensión $K/\mathbb{Q}$ es abeliana). Entonces K está contenida para algún m en el cuerpo ciclotómico $\mathbb{Q}[\omega_m]$. □

Mediante un procedimiento similar al ejemplo 4.57 podemos encontrar infinitos cuerpos cúbicos de números no isomorfos dos a dos. Para ello, sea p un primo con $p \equiv_3 1$. Entonces, la extensión $\mathbb{Q}[\omega_p]/\mathbb{Q}$ es de Galois, con grupo de Galois $\mathbb{Z}_p^\times$. Es decir, su grupo de Galois es cíclico de orden múltiplo de 3. Por ello podemos encontrar un único cuerpo K_p con $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}[\omega_p]$ de forma que $[K_p : \mathbb{Q}] = 3$. Además, $K_p/\mathbb{Q}$ será una extensión de Galois, ya que $\mathbb{Q}[\omega_p]$ es una extensión de Galois con grupo de Galois abeliano, por tanto todos los subgrupos de $\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ son normales. Mediante técnicas que vamos a desarrollar en la asignatura veremos además que para dos primos p, q, las extensiones K_p y K_q no serán isomorfas, ya que no tendrán el mismo discriminante.

Capítulo 5

Dominios de Dedekind

5.1 Ideales de los cuerpos de números

Recordemos que O_K son los elementos del cuerpo K que son enteros algebraicos. Ya vimos en el capítulo que si $[K : \mathbb{Q}]$ tiene grado n, entonces O_K es un grupo abeliano libre de dimensión n (ya que O_K tiene alguna base entera que lo genera libremente como $\mathbb{Z}$-módulo).

Proposición 5.1. Sea K cuerpo de números con $[K : \mathbb{Q}] = n$, y sea I un ideal no nulo de O_K. Entonces I, al igual que O_K, es un grupo abeliano libre de rango n.

Demostración. Recordemos que un subgrupo de un grupo abeliano libre de n elementos será también un grupo libre, con rango $\leq n$. Esto implica que I es un grupo abeliano libre de rango $\leq n$. Ahora, como I no es el ideal 0, sea $\alpha \subseteq I$ no nulo. Tenemos las inclusiones de subgrupos:

$$(\alpha) \subseteq I \subseteq O_K$$

ahora bien, es fácil comprobar que si O_K es el grupo libre generado por unos elementos $a_1, \ldots, a_n$, entonces (α) es el grupo libre generado por $\alpha a_1, \ldots, \alpha a_n$. Por tanto (α) es un grupo libre de rango n. Al ser un subgrupo de I, el rango de I tendrá que ser $\geq n$, y por tanto I es un grupo abeliano libre de rango n. □

Enunciamos por conveniencia el resultado usado:

Corolario 5.2. Dada cualquier base de enteros de O_k : $\alpha_1, \ldots \alpha_n$ se tiene que $\alpha\alpha_1, \ldots, \alpha\alpha_n$ es base de enteros de (α).

Corolario 5.3. Todo ideal de O_K es finitamente generado. Es decir, O_K es un anillo noetheriano.

Demostración. Dado I ideal de O_K, está generado como grupo por un conjunto finito $i_1, \ldots, i_n$ de generadores. Por tanto $i_1, \ldots, i_n$ también generan a I como ideal. □

Vamos a ver estudiar cómo se comportan las cadenas de ideales en O_K.

Definición 5.4. Sean $p_0 \subsetneq p_1 \subsetneq p_2 \cdots \subsetneq p_n$ una cadena de ideales primos, decimos que tiene longitud n. Llamamos dimensión de Krull de un anillo R al supremo de las longitudes de cadenas de ideales de R.

Ejemplo 5.5. $\mathbb{Z}$ tiene dimensión de Krull 1, ya que las cadenas que pueden formarse son de forma $0 \subsetneq (p)$, con p primo en $\mathbb{Z}$, y no se puede formar ninguna cadena de dimensión 2.

Ejemplo 5.6. Se puede comprobar que la dimensión de Krull de $\mathbb{Z}[x]$ es 2. Un ejemplo de cadena de longitud 2 sería $0 \subsetneq (x) \subsetneq (2, x)$.

Proposición 5.7. Un anillo R tiene dimensión de Krull 1 sii tiene ideales primos no nulos, y todos ellos son maximales.

Demostración. Está claro que R tendrá dimensión ≥ 1 si tiene ideales primos no nulos. Si sus ideales primos son todos maximales, no puede haber cadenas de longitud 2, ya que tendríamos $0 \subsetneq p_1 \subsetneq p_2$, con p_1 maximal. Recíprocamente, si hay un ideal primo no maximal p, entonces hay uno maximal m que lo contiene, y $0 \subseteq p \subseteq m$ es una cadena de longitud 2. □

Vamos a intentar demostrar que O_K tiene dimensión 1, es decir, que todos sus ideales primos son maximales.

Lema 5.8. Sea I ideal no nulo de O_K. Entonces $I \cap \mathbb{Z} \neq \{0\}$.

Demostración. Sea $0 \neq \alpha \in I$. Como α es entero algebraico, su polinomio mínimo sobre $\mathbb{Q}$ será $x^n + \cdots + a_1 x + a_0$, con $a_0 \neq 0$. De la ecuación $\alpha^n + \cdots + a_1\alpha + a_0 = 0$, despejamos $a_0 = -\alpha(\alpha^{n-1} + \cdots + a_1)$. Ergo, como $a_n\alpha^{n-1} + \cdots + a_1 \in O_K$, tenemos que $a_0 \in (\alpha) \subseteq I$. Como a_0 es entero, hemos acabado. □

Lema 5.9. Todo dominio de integridad finito es un cuerpo.

Demostración. Sea R dominio de integridad finito, sea $a \in X$ no nulo. Entonces, por ser dominio de integridad, la función $R \xrightarrow{f} R; x \to ax$ es inyectiva. Al ser R finito, si $f : R \to R$ es inyectiva también será sobreyectiva, ergo hay b con $ab = 1$. Es decir, a tiene inverso. Como a es un elemento cualquiera no nulo, R es cuerpo. □

Teorema 5.10. Sea K cuerpo de números, O_K su anillo de enteros asociado. Todo ideal primo no nulo de O_K es maximal.

Demostración. Sea I ideal de O_K. Sea $m \in I \cap \mathbb{Z}$, con $m \neq 0$. Entonces, veamos que el cociente $\frac{O_K}{(m)}$ es finito. Sea $a_1, \ldots, a_n$ base entera de O_K. Es decir, $a_1, \ldots, a_n$ generan O_K como $\mathbb{Z}$-módulo libre. Por tanto, $O_K = a_1\mathbb{Z} \oplus \cdots \oplus a_n\mathbb{Z}$. A su vez, $(m) = mO_K = a_1(m\mathbb{Z}) \oplus \cdots \oplus a_n(m\mathbb{Z})$. Tomando cocientes (y abusando de notación xd),

$$\frac{O_K}{(m)} = \frac{a_1\mathbb{Z} \oplus \cdots \oplus a_n\mathbb{Z}}{a_1(m\mathbb{Z}) \oplus \cdots \oplus a_n(m\mathbb{Z})} \simeq a_1\frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \cdots \oplus a_n\frac{\mathbb{Z}}{m\mathbb{Z}},$$

de modo que el cociente $\frac{O_K}{mO_K}$ tiene finitos elementos, en concreto m^n. Por tanto, como $\frac{O_K}{I} \simeq \frac{O_K/(m)}{I/(m)}$, $\frac{O_K}{I}$ también tendrá finitos elementos.

En el caso concreto de que I sea un ideal primo, $\frac{O_K}{I}$ es un dominio de integridad que además tiene finitos elementos. Por tanto es un cuerpo, es decir, I es maximal. □

Hemos visto que O_K es noetheriano y de dimensión de Krull 1. Nos hará falta una última propiedad:

Definiciones 5.11. Sea R dominio de integridad, sea K cuerpo de fracciones de R. Decimos que $a \in K$ es entero sobre R si hay un polinomio $f \in R[x]$ mónico y no nulo con $f(a) = 0$.

Decimos que R es íntegramente cerrado si cada elemento de K que es entero sobre R está en R.

Proposición 5.12. Sea K cuerpo de números, O_K su anillo de enteros asociado. Entonces O_K es íntegramente cerrado.

Demostración. K es el cuerpo de fracciones de O_K. Queremos ver que si hay $\alpha \in K$ y $f(x) = x^m + \beta_{m-1}x^{m-1} + \cdots + \beta_0 \in O_K[x]$ tal que $f(\alpha) = 0$, entonces $\alpha \in O_K$. Como sabemos que $\alpha \in K$, basta ver que α es entero algebraico. Para ello usaremos el lema 4.4, encontrando un W subgrupo abeliano finitamente generado de $\mathbb{C}$ de forma que $\alpha W \subseteq W$. Definiremos W a partir de un conjunto finito S que lo genera como subgrupo. Ponemos entonces

$$S = \left\{ \alpha^i \prod_{j=0}^{m-1} \beta_j^{i_j}; i = 0, 1, \ldots, m-1; i_j = 0, 1, \ldots, \deg(\beta_j) - 1 \right\},$$

donde $\deg(\beta_j)$ es el grado de $\mathbb{Q}[\beta_j] : \mathbb{Q}$. Está claro que el conjunto S así definido es finito. Para comprobar que $\alpha W \subseteq W$, basta comprobar que $\alpha s \in W$ para todo $s \in S$.

Sea $s = \alpha^i\beta_0^{i_0} \ldots \beta_{m-1}^{m-1}$. Si $i < m-1$, $\alpha s \in S$, por tanto $\alpha s \in W$. Si $i = m-1$, $\alpha s = \alpha^m\beta_0^{i_0} \ldots \beta_{m-1}^{m-1} = (-b_{m-1}\alpha^{m-1} + \cdots + \beta_0)\beta_0^{i_0} \ldots \beta_{m-1}^{m-1}$. Tenemos una suma de m términos de forma $-\alpha^j\beta_0^{i_0} \ldots \beta_{j-1}^{i_{j-1}}\beta_j^{i_j+1}\beta_{j+1}^{i_{j+1}} \ldots \beta_0^{i_0}$.

Si $i_j < \deg \beta_j - 1$, de nuevo tenemos (el opuesto de) un elemento de s. Si $i_j = \deg(\beta_j) - 1$, el elemento es de forma $-\alpha^j \beta_0^{i_0} \dots \beta_{j-1}^{i_{j-1}} \beta_j^{\deg(\beta_j)} \beta_{j+1}^{i_{j+1}} \dots \beta_0^{i_0} = (-\sum_{l=0}^{\deg(\beta_j)-1} k_l \beta_j^l)(-\alpha^j \beta_0^{i_0} \dots \beta_{j-1}^{i_{j-1}} \beta_{j+1}^{i_{j+1}} \dots \beta_0^{i_0})$, donde los enteros k_l son los coeficientes del polinomio mínimo de β_j. Por tanto esto es una suma de enteros por elementos de S, ergo está en W. □

5.2 Dominios de Dedekind. Factorización única de ideales

En la sección anterior hemos visto que los anillos de enteros O_K cumplen estas tres proposiciones:

(I) O_K es un dominio noetheriano.

(II) $\dim(O_K) = 1$.

(III) O_K es íntegramente cerrado.

Definición 5.13. Decimos que un dominio íntegro R es un dominio de Dedekind si cumple (I), (II) y (III).

Recordemos que dados ideales I, J de un anillo, el conjunto $IJ := \{\sum_{i=1}^n a_i b_i : \ a_i \in I, \ b_i \in J, \ n \in \mathbb{N}\}$ es un ideal que llamamos IJ, el *producto* de I y J. Esta sección se dedicará a probar que en un dominio de Dedekind (lo probaremos en cuerpos de números, aunque la demostración general es la misma), todo ideal $I \neq 0$ se podrá expresar de forma única (salvo orden) como $P_1 \dots P_n$, donde P_i son ideales primos (por tanto, maximales). Es decir, una especie de teorema de factorización única pero con ideales en vez de elementos. De modo que vamos a estudiar los ideales en los dominios de Dedekind.

Definición 5.14. Dados ideales I, J de un anillo R, decimos que I divide a J, $I|J$, si hay un ideal I' con $J = II'$.

Veamos algunas propiedades del producto de ideales. Estudiemos $I_K := \{I \subset O_K : \ I \text{ es ideal no nulo de } O_k\}$. El par $(I_K, \cdot)$ donde $\cdot$ denota al producto entre ideales es:

1. Asociativo.
2. Conmutativo.
3. Tiene elemento neutro, el propio ideal O_K.

Sin embargo en general no tiene elemento inverso.

K tiene estructura de O_K-módulo, consideremos el conjunto $\{O_K\text{-submódulos de } K \text{ finitamente generados}\}$. A sus elementos los llamaremos ideales fraccionarios. Podemos definir el mismo producto sobre ellos y esta vez sí que encontraremos inversos.
De esta forma, podemos definir el cociente

$$\frac{\{O_K\text{-submódulos de } K \text{ finitamente generados}\}}{\{(x) : \ x \in K\}}$$

Aquí construiremos el cociente construyendo la relación de equivalencia en vez de tomar los ideales principales.

Proposición 5.15. Sea $\omega \in O_K$ y sean I, J ideales de O_K. Entonces

$$(\omega)J = IJ \Rightarrow \ (\omega) = I.$$

Demostración. Recordemos que dado $\alpha \in K$, si $\alpha I \subset I \Rightarrow \ \alpha \in O_K$ (1). Veamos antes de demostrar la proposición que $IJ = I \Rightarrow J = O_K$ (2).
Como I es ideal no nulo, está generado por n elementos

$$I = \alpha_1 \mathbb{Z} + \dots + \alpha_n \mathbb{Z}, \ \alpha_1, \dots, \alpha_n \in I$$

Pero cada α_i está en IJ luego se puede expresar como $\alpha_i = \alpha_1 \beta_{i1} + \dots + \alpha_n \beta_{in}$, con $i = 1, \dots, n$ y $\beta_{ij} \in J$.

Por tanto

$$Id_n \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = (\beta_{ij}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \Rightarrow \ (Id_n - (\beta_{ij})) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

El vector es no nulo luego $|Id_n - (\beta_{ij})| = 0$. Si desarrollamos el determinante vemos que existe $\beta \in J$ tal que

$$0 = |Id_n - (\beta_{ij})| = 1 + \beta \Rightarrow \ 1 = -\beta \in J.$$

Tenemos el 1 en el ideal luego el ideal J es todo O_K.

Pasamos a demostrar el enunciado. Dado $i \in I, iJ \subseteq IJ = \omega J$, por tanto $\omega^{-1} iJ \subseteq J$. Usando esto y 4.4 (ya que J es un $\mathbb{Z}$-módulo finitamente generado) tenemos que $\omega^{-1} i$ es entero, algebraico, es decir, $\omega^{-1} i \in O_K$. Como $\omega^{-1} i \in O_K$ para todo $i \in I$, tenemos que $I \subseteq (\omega)$. De modo que $\omega^{-1} I$ es un ideal de O_K. Como $\omega^{-1} IJ = J$, $w^{-1} I$ será todo O_K por lo que hemos visto. Por tanto $I = (\omega)$.

□

Definición 5.16. Sean ideales I, J en I_K. Diremos que

$$I \sim J \ \Leftrightarrow \ \exists 0 \neq \alpha, \beta \in O_K : \ (\alpha) I = (\beta) J.$$

Proposición 5.17. La relación introducida en la definición anterior es de equivalencia.

Demostración. Las propiedades reflexiva y simétrica son inmediatas. Para la transitividad, sean ideales I, J, K tales que $I \sim J, \ J \sim K$. Entonces existen $0 \neq \alpha, \beta, \gamma, \delta \in O_K$ tales que

$$(\alpha) I = (\beta) J, \quad (\gamma) J = (\delta) K \Rightarrow \ (\alpha\gamma) I = (\beta\gamma) J = (\beta\gamma) J = (\beta\delta) K.$$

Claramente $\alpha\gamma, \beta\delta \in O_K$. □

Definición 5.18. Denotaremos por

$$C_K := \frac{I_K}{\sim},$$

al conjunto cociente definido por la relación de equivalencia $\sim$.

Proposición 5.19. Si $I \sim J$ e $I' \sim J'$, entonces $II' \sim JJ'$.

Demostración. Sean $\alpha, \beta, \alpha', \beta' \in O_K$ tales que

$$(\alpha) I = (\beta) J, \quad (\alpha') I' = (\beta') J' \Rightarrow \ (\alpha\alpha') II' = (\alpha I)(\alpha' I') = (\beta J)(\beta' J') = (\beta\beta') JJ' \Rightarrow \ II' \sim JJ'$$

□

La clase de O_K, a la que denotamos por $\overline{O}_K$, es el elemento neutro de C_K. Veamos cómo son los elementos relacionados con O_K :

$$I \sim O_K \ \Leftrightarrow \ \exists \alpha, \beta \in O_K : \ (\alpha) I = (\beta) O_K.$$

Proposición 5.20. Los elementos relacionados con O_K son los ideales principales de O_K.

Demostración. Si tenemos $(\alpha) I = (\beta) O_K$, tenemos que $I = \alpha^{-1} \beta O_K$, por tanto $\alpha^{-1} \beta \in O_K$ (si no no podría ser que $I \subseteq O_K$). Así que tenemos que $I = \alpha^{-1} \beta O_K$ es el ideal principal $(\alpha^{-1} \beta)$ de O_K. La implicación recíproca es obvia. □

Fijémonos en que si $|C_K| = 1$ es que todos los ideales de O_K son principales.

Lema 5.21 (Hurwitz)**.** Sea K un cuerpo de números, entonces existe un entero M_K tal que $\forall x \in K \ \exists 1 \leq t \leq M_K, \ \exists \omega \in O_K : \ |N_{K/\mathbb{Q}}(tx - \omega)| < 1$.

Demostración. Sea $x \in K,\ x = \sum_{i=1}^{n} x_i\alpha_i,\ \{\alpha_1, \ldots, \alpha_n\}$ es base entera de O_K y $x_i \in \mathbb{Q}$. Entonces

$$|N_{K/\mathbb{Q}}(x)| = \left|\prod_j \sigma_j\left(\sum_i x_i\alpha_i\right)\right| = \prod_j \left|\sum_i x_i\sigma_j(\alpha_i)\right| \leq \max_i\{|x_i|\}^n \prod_j \sum_i |\sigma_j(\alpha_i)|$$

Si fijamos la base entera se tiene que $\prod_j \sum_i |\sigma_j(\alpha_i)|$ es constante, llamémosla $C < m^n =: M$, para algún $m \in \mathbb{Z}$.

$$|N_{K/\mathbb{Q}}(x)| < \max_i\{|x_i|\}^n m^n$$

Definimos $\phi : K \to \mathbb{R}^n$ como $\phi(x) = (x_1, \ldots, x_n)\ \forall x \in K$. Denotemos por $\lfloor x \rfloor := \sum \lfloor x_i \rfloor \alpha_i$ parte entera y por $\{x\} = \sum \{x_i\}\alpha_i$ parte fraccionaria. Entonces

$$\phi(\{x\}) \in [0, 1)^n$$

Dividimos el cubo unidad en m^n regiones dividiendo cada lado en m partes de lado $1/m$. Por el principio del palomar, existen $h, k \in \mathbb{Z} :\ 1 \leq h < k \leq M + 1 :\ \phi(\{hx\})$ y $\phi(\{kx\})$ están en la misma celda.
Definimos $t := k - h$. Luego $tx = kx - hx = \lfloor kx \rfloor x - \lfloor hx \rfloor + \{kx\} - \{hx\},\ \omega := \lfloor kx \rfloor x - \lfloor hx \rfloor \in O_K \Rightarrow$

$$|N_{K/\mathbb{Q}}(tx - \omega)| = |N_{K/\mathbb{Q}}(\{kx\} - \{hx\})| < \max_i\{1/m\}^n m^n = 1.$$

□

Proposición 5.22. El cardinal de C_K es finito. Lo llamaremos $h_K := |C_K|$.

Demostración. Sea I un ideal no nulo de O_K. Si tomamos $\alpha \in I$ no nulo su norma es no nula. Entonces, como la norma es entera en O_K, podemos coger $\beta \in I$ tal que $|N_{K/\mathbb{Q}}(\beta)| = \min\{|N_{K/\mathbb{Q}}(\alpha)| :\ \alpha \in I,\ \alpha \neq 0\}$.

Sea ahora $\alpha \in I,\ \alpha \neq 0$. Definimos $x := \frac{\alpha}{\beta} \in K$. Ahora, podemos coger por 5.21 un entero $t < M$ y un $\omega \in O_K$ tal que

$$1 > |N_{K/\mathbb{Q}}(tx - \omega)| = |N_{K/\mathbb{Q}}(t\frac{\alpha}{\beta} - \omega)| \Rightarrow\ |N_{K/\mathbb{Q}}(\beta)| > |N_{K/\mathbb{Q}}(t\alpha - \omega\beta)|.$$

Ahora bien, $t\alpha - \omega\beta \in I$ y $|N_{K/\mathbb{Q}}(\beta)| > |N_{K/\mathbb{Q}}(t\alpha - \omega\beta)|$, ergo $t\alpha - \omega\beta = 0$. En concreto esto implica que $t\alpha \in (\beta)$. Como $t|M!$ sin importar que x tomemos, se cumplirá que $M!\alpha \in (\beta)$ para cualquier $\alpha \in I$, ergo $M!I \subset (\beta)$.

$J := \beta^{-1}M!I$ es ideal de O_K, con $(\beta)J = M!I \Rightarrow I \sim J$. Como $\beta \in I$, $M!\beta \in (\beta)J$, ergo $M! \in J$.

En particular, $(M!) \subseteq J \subseteq O_K$. Además, como vimos en 5.10:

$$\left|\frac{O_K}{(M!)}\right| = (M!)^n < \infty.$$

Por tanto, como cada ideal J conteniendo a $(M!)$ está asociado a un ideal de $\frac{O_K}{(M!)}$, y solo hay finitos ideales en $\frac{O_K}{(M!)}$, solo habrá finitos J posibles. Como a su vez $I \sim J$, ya que $J = \beta^{-1}M!I$, ya tenemos que solo hay finitas clases de equivalencia. □

Proposición 5.23. Si $A \subseteq O_K$ es un ideal, hay un entero k, $1 \leq k \leq h_K$, tal que A^k es principal.

Demostración. Consideramos los ideales $A, A^2, \ldots, A^{h_K+1}$. Entonces dos de ellos estarán relacionados por $\sim$, digamos $A^i \sim A^j$, con $i < j$. En ese caso, hay a, b con $(a)A^i = (b)A^j = (b)A^{j-i}A^i$. Por tanto por 5.15 tenemos que $(a) = (b)A^{j-i}$. Es decir, $(a)O_K = (b)A^{j-i}$, por tanto $O_K \sim A^{j-i}$. Así que por 5.20, A^{j-i} es principal. □

Proposición 5.24. C_K es un grupo con el producto dado por $\overline{I} \cdot \overline{J} = \overline{IJ}$.

Demostración. Este producto está bien definido por 5.19. Además es asociativo (y conmutativo) y tiene elemento neutro, O_K. Por el lema anterior tiene elemento inverso, ya que dado A ideal, hay n con A^n principal, por tanto $\overline{A} \cdot \overline{A^{n-1}} = \overline{A^n} = \overline{O_K}$. □

De modo que C_K es un grupo, y solo será el grupo trivial cuando O_K sea un dominio de ideales principales.

Ejercicio 5.25. Ver los casos $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-5})$. Sin usar que sabemos que $\mathbb{Q}(i)$ es dominio eucídeo.
Sacar la M y después intentar sacar ideales intermedios.
Para el primer caso saldrá $h = 1$ y para el segundo $h > 1$. Todo esto con bastante esfuerzo XDddd.

Ya podemos generalizar 5.15:

Proposición 5.26. Si I, J, J' son ideales en O_K y $IJ = IJ'$, entonces $J = J'$.

Demostración. Llamamos $(\alpha) = I^n$, para ciertos $n \in \mathbb{N}, \alpha \in O_K$. Entonces, multiplicando la igualdad $IJ = IJ'$ por I^{n-1}, tenemos que $\alpha J = \alpha J'$. Multiplicando ambos subconjuntos de K por $\frac{1}{\alpha}$, tenemos que $J = J'$. □

Proposición 5.27. Dados I, J ideales de O_K, $I|J \iff J \subseteq I$.

Demostración. $\Longrightarrow$ es obvio. Si $J \subseteq I$, sean a, n tales que $(a) = I^n$. Entonces $I^{n-1}J \subseteq I^n = (a)$. Por tanto $I' = a^{-1}I^{n-1}J$ (es decir, el resultado de multiplicar por a^{-1} los elementos de $I^{n-1}J$) es un ideal de O_K. Y tenemos que $II' = a^{-1}I^nJ = J$, por tanto $I|J$. □

Por fin llegamos a nuestro objetivo: la factorización única de ideales en dominios de Dedekind (aunque lo enunciamos para cuerpos de números).

Teorema 5.28. Sea I ideal propio de O_K, existen ideales primos $P_1, \dots, P_n$, únicos salvo el orden, tales que

$$I = P_1 \dots P_n.$$

Los P_i serán maximales por 5.10.

Demostración. Comenzamos viendo que todo ideal de O_K se puede expresar como producto de ideales primos. Sea I ideal propio de O_K. Hay un ideal P_1 maximal en O_K que contiene a I. Como $I \subseteq P_1$, por 5.27 habrá un ideal I_1 con $I = P_1I_1$. Esto obviamente implica que $I \subseteq I_1$. Además, $I \neq I_1$, ya que si tuviéramos que $I = I_1$, entonces de $O_KI = I = P_1I_1 = P_1I$ y 5.26 se deduce que $O_K = P_1$, lo cual es falso. Por tanto $I \subsetneq I_1$.

Si $I_1 = O_K$, tenemos que $I = P_1$, por tanto I es producto de ideales. Si no, I_1 es ideal propio de O_K, y repitiendo el mismo proceso encontramos P_2 primo e $I_2 \subsetneq I_1$ con $I_1 = P_2I_2$. Podemos repetir este proceso recursivo tantas veces como queramos: si I_{n-1} no es propio, podemos encontrar ideales P_n primo e I_n tales que $I_{n-1} = I_nP_n$ y $I_n \subsetneq I_{n-1}$. Al repetir este proceso pueden pasar dos cosas:

- Para cierto n se cumple que $I_n = O_K$. Entonces el proceso acaba, y tenemos que $I = I_1P_1 = I_2P_1P_2 = \dots = I_nP_1 \dots P_n = P_1 \dots P_n$, y ya tenemos I expresado como producto de primos.
- I_n es propio para todo n. Esto es imposible, ya que en ese caso tendríamos una cadena ascendente infinita de ideales $I_1 \subsetneq I_2 \subsetneq I_3 \dots$, lo cual no puede pasar ya que O_K es un anillo noetheriano, así que no tiene cadenas infinitas ascendentes de ideales.

Por tanto ya tenemos que todo ideal de O_K se puede factorizar como producto finito de ideales primos. Veamos ahora que la factorización es esencialmente única.

Supongamos que un ideal tiene dos factorizaciones distintas,

$$P_1 \dots P_t = Q_1 \dots Q_s, \text{ con } t \leq s$$

Entonces se cumple que $P_1|Q_1 \dots Q_s$, por tanto $Q_1 \dots Q_s \subseteq P_1$. Pero, si un producto finito de ideales está contenido en un ideal primo, entonces alguno de ellos está contenido en dicho ideal primo, por tanto hay cierto Q_i, que podemos suponer que es Q_1, con $Q_1 \subseteq P_1$. Como P_1 y Q_1 son maximales por 5.10, esto implica que $P_1 = Q_1$. Por tanto tenemos que

$$P_1(P_2 \dots P_t) = P_1(Q_2 \dots Q_s).$$

Esto, por 5.26, implica que:

$$P_2 \dots P_t = Q_2 \dots Q_s.$$

De la misma forma podemos deducir que $P_2 = Q_2$ (salvo orden) y entonces $P_3 \dots P_t = Q_3 \dots Q_s$. Repitiendo este proceso, obtenemos que $P_i = Q_i$ para $i = 1, \dots, t-1$, y que:

$$P_t = Q_t \dots Q_s$$

entonces, igual que antes deducimos que $P_t = Q_t$, y expresando la igualdad como

$$P_t(O_K) = Q_t(Q_{t+1} \dots Q_s)$$

y usando 5.26, tenemos que $O_K = Q_{t+1} \dots Q_s$. Esto solo puede pasar si $t = s$, ya que si no $Q_{t+1} \dots Q_s$ no sería el anillo total. Por tanto $t = s$, y $P_i = Q_i$ para $i = 1, \dots, t$, así que hemos acabado. □

5.3 Ejemplos del grupo de clases C_K

Recordemos que el espectro de un anillo se define como el conjunto de sus ideales primos. Lo que nos dice este último teorema de factorización es que podremos construir el conjunto de ideales de O_K a partir de su espectro, ya que todo ideal es un producto finito de primos. Y de hecho, en cuerpos de números, podremos obtener todos los ideales primos a partir de los primos de $\mathbb{Z}$ como se explica a continuación.

Dado un ideal primo P de O_K, $P \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ (ya que $P \cap \mathbb{Z}$ es la contracción de P bajo la inclusión $\mathbb{Z} \hookrightarrow O_K$). Además, por 5.8, $P \cap \mathbb{Z}$ no es $\{0\}$. Por tanto $P \cap \mathbb{Z} = p\mathbb{Z}$, para un primo p de $\mathbb{Z}$. Como $p \in P$, tenemos que $pO_K \subseteq P$. Por tanto P es un elemento de la factorización de pO_K como producto de ideales primos de O_K.

De modo que para encontrar los ideales primos de O_K (su espectro), nos vale con encontrar los factores primos de todos los ideales pO_K, con p primo en $\mathbb{Z}$.

Ejemplo 5.29. En $\mathbb{Z}[i]$ podemos encontrar los ideales de esta forma. Dado un primo entero p, ya hemos visto que $p\mathbb{Z}[i]$ es primo si $p \equiv_4 3$, y si $p \equiv_4 1$ entonces $p = p_1 p_2$ con p_1, p_2 primos en $\mathbb{Z}[i]$, por tanto $p\mathbb{Z}[i]$ factoriza como $(p_1\mathbb{Z}[i])(p_2 Z[i])$. Por último, $2\mathbb{Z}[i] = ((1+i)\mathbb{Z}[i])^2$.

En general, si R es un DIP, los ideales primos de R son los que están generados por un elemento primo de R, por tanto si ya sabemos los elementos primos de R también conocemos los ideales primos.

El grupo $C_{\mathbb{Q}[i]}$ es el grupo trivial, ya que $\mathbb{Z}[i]$ es un DIP.

Ejemplo 5.30. Volvemos a $\mathbb{Z}[i]$, pero vamos a intentar ver que $C_{\mathbb{Q}[i]}$ es el grupo trivial sin usar que $\mathbb{Z}[i]$ es un dominio euclídeo, es decir, de forma constructiva usando las pruebas de 5.21 y 5.22.

Comenzamos encontrando el M de la prueba de 5.22, es decir, $M = m^2$, con $m \in \mathbb{Z}$ y $M \geq \prod_j \sum_i |\sigma_j(\alpha_i)|$. En este caso σ_1 es la identidad, y σ_2 es la conjugación, podemos tomar base entera $\{\alpha_1, \alpha_2\}$, con $\alpha_1 = 1$ y $\alpha_2 = i$. Así, un cálculo directo nos da que $\prod_j \sum_i |\sigma_j(\alpha_i)| = 4$, por tanto podemos tomar $M = 2^2 = 4$.

Ahora vamos a la prueba de 5.22, que nos dice que cualquier ideal I de O_K es equivalente a algún ideal J, con $M! \in J$. En este caso, $M! = 24$, por tanto tenemos que ver los ideales J tales que $24 \in J$. De hecho vamos a ver las clases de ideales primos P con $24 \in P$, y una vez que los tengamos podremos construir el resto de ideales con sus productos.

Sea P primo con $24 \in P$. Como $24 = i \cdot 3 \cdot (1+i)^6$, o bien $1+i \in P$ o $3 \in P$:

- $1+i \in P$. En este caso, $(1+i) \subseteq P$, y tenemos que $\frac{P}{2}$ es un ideal de $\frac{\mathbb{Z}[i]}{(1+i)}$. Pero $1+i$ tiene dos elementos, y solo tiene dos ideales: $\{0\}$ y el total. A su vez, estos ideales corresponden en $\mathbb{Z}[i]$ a los ideales $(1+i)$ y $\mathbb{Z}[i]$. De ellos, el único primo es $(1+i)$. Así que en este caso, el único P posible es $(1+i)$.
- $3 \in P$. En este caso, $(3) \subseteq P$. Si (3) es primo, es maximal o sea que P tiene que ser (3). Si (3) no fuera primo, tendría que darse que $(3) \subsetneq P$, sea entonces $\alpha = a+bi \in P \setminus (3)$. La norma de α, $N(\alpha) = a^2 + b^2$,

no es múltiplo de 3 ya que módulo 3 vemos que si $3|a^2+b^2$ entonces $a|3$ y $b|3$, lo cual no puede ser porque $\alpha \notin (3)$. Pero a su vez $N(\alpha)$ es múltiplo de α, por tanto $N(\alpha) \in P$. Por tanto 3 y $N(\alpha)$ están en P, y como por Bezout 1 es una combinación entera de 3 y $N(\alpha)$, $1 \in P$, es decir, $P = \mathbb{Z}[i]$, absurdo. Por tanto no puede haber ningún primo P estrictamente contenido en (3).

Ya podemos ver entonces quién es $C_{\mathbb{Q}[i]}$. Dado un ideal I en $C_{\mathbb{Q}[i]}$, se cumple que $I \sim J$, con $24 \in J$. Factorizando J como producto de primos (que contienen a 24, por tanto son o bien $(1+i)$ o (3)), tenemos que $J = (1+i)^n(3)^m$, por tanto $\overline{I} = \overline{J} = (\overline{1+i})^n(\overline{3})^m = \overline{O}_K^n \overline{O}_K^m = \overline{O}_K$. Es decir, $C_{\mathbb{Q}[i]}$ es trivial.

Ejemplo 5.31. Vamos ahora los ideales primos en un anillo que no es un DIP, de forma análoga a 5.30. Cogemos el cuerpo de números $K = \mathbb{Q}[\sqrt{-5}]$. Vimos en 4.10 que su anillo de enteros es $\mathbb{Z}[\sqrt{-5}]$. Por tanto una base de enteros viene dada por $\{1, \sqrt{-5}\}$. De nuevo usaremos el procedimiento de 5.21 y 5.22. Nuestra base de enteros es $\{1, \sqrt{-5}\}$ y nuestros automorfismos son la identidad y la conjugación. De modo que calculamos que $\prod_j \sum_i |\sigma_j(\alpha_i)| = (1+\sqrt{-5})^2 < 4^2 = 16$, por tanto $M_K = 16$.

Así que en este caso tendríamos que buscar los ideales primos P con $16! \in P$. Podemos expresar $16! = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$. Por tanto en este caso tendríamos que estudiar 6 casos posibles: $2 \in P, 3 \in P, 5 \in P, 7 \in P, 11 \in P, 13 \in P$.

- $2 \in P$, es decir, $P|(2)$. Veamos que (2) factoriza como $(2, 1+\sqrt{-5})^2$. Para ver esto, comprobamos que $2 \in (2, 1+\sqrt{-5})^2$ ya que $2 = (1+\sqrt{-5})(2-(1+\sqrt{-5})) - 2 \cdot 2$, y además $(2, 1+\sqrt{-5})^2 \subseteq (2)$ ya que los productos de los generadores, $2 \cdot 2, 2 \cdot (1+\sqrt{-5})$ y $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$ están todos en (2).

  Además, $(2, 1+\sqrt{-5})$ y $(2, 1-\sqrt{-5})$ son maximales. Esto pasa porque $\frac{\mathbb{Z}[\sqrt{-5}]}{(2,1+\sqrt{-5})} \equiv \frac{\frac{\mathbb{Z}[\sqrt{-5}]}{(2)}}{\frac{(2,1+\sqrt{-5})}{(2)}}$, y $\frac{(2,1+\sqrt{-5})}{(2)}$ contiene 2 de los 4 elementos de $\frac{\mathbb{Z}[\sqrt{-5}]}{(2)}$, por tanto $\frac{\mathbb{Z}[\sqrt{-5}]}{(2,1+\sqrt{-5})}$ tiene dos elementos, es decir, es un cuerpo. Por tanto $(2, 1+\sqrt{-5})$ es maximal. Igual pasa con $(2, 1-\sqrt{-5})$.

- $3 \in P$. En este caso se puede comprobar que $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.

- $5 \in P$. En este caso claramente $(5) = (\sqrt{-5})^2$, y $(\sqrt{-5})$ es maximal ya que es un ideal que contiene estrictamente a (5), y $\frac{\mathbb{Z}[\sqrt{-5}]}{(5)}$ tiene 25 elementos, por tanto $\frac{\mathbb{Z}[\sqrt{-5}]}{(1+\sqrt{-5})}$ tiene 5 elementos, es decir, es un cuerpo.

- $7 \in P$. En este caso se puede comprobar que $(7) = (7, 3+\sqrt{-5})(7, 3-\sqrt{-5})$.

- $11 \in P$. Se puede comprobar que (11) es primo.

- $13 \in P$. Se puede comprobar que (13) también es primo.

Si todos los ideales primos que hemos encontrado fueran principales, tendríamos que como en el caso de $\mathbb{Z}[i]$, C_K tendría 1 elemento. Sin embargo, este no es el caso: el ideal $(2, 1+\sqrt{-5})$ no es principal. Ya que si g fuera su generador, $g|2$, por tanto $N(g) \leq N(2) = 4$, por tanto g sería $1, -1, 2$ o -2, y no puede darse ninguno de estos casos ya que $(2) \subsetneq (2, 1+\sqrt{-5}) \subsetneq \mathbb{Z}[\sqrt{-5}]$.

Por poner otro ejemplo, veamos que $(3, 1+\sqrt{-5})$ tampoco es principal: si llamamos a g a un hipotético elemento con $(g) = (3, 1+\sqrt{5})$, entonces como $g|3$ y $g|\sqrt{-5}$, tenemos que $N(g)|N(3)$ y $N(g)|N(1+\sqrt{-5})$, es decir, $N(g)|9$ y $N(g)|6$, ergo $N(g)|3$. Como $N(g) = a^2 + 5b^2$, donde $g = a + b\sqrt{-5}$, si $N(g) = 3$ solo puede ser $g = \pm 1$, así que $(3, 1+\sqrt{-5})$ sería O_K. Pero este no es el caso, ya que si hubiera elementos $a, b \in \mathbb{Z}[\sqrt{-5}]$ con $1 = 3a + (1+\sqrt{-5})b$, tendríamos que $1 - \sqrt{5} = 3(1-\sqrt{-5})a + 6$, lo cual no pasa porque el primer miembro no tiene coeficientes real e imaginario múltiplo de 3. Un método similar puede usarse para comprobar que $(7, 3+\sqrt{-5})$ no es principal.

Además, $(3, 1+\sqrt{-5}) \neq (3, 1-\sqrt{-5})$, ya que si tuviéramos que $1 - \sqrt{-5} \in (3, 1+\sqrt{-5})$, entonces $1 = 3 - (1+\sqrt{-5}) - (1-\sqrt{-5}) \in (3, 1+\sqrt{-5})$, y ya hemos visto que eso no es cierto.

Sabiendo que $(3, 1+\sqrt{-5})$ no es principal, podemos usar la estructura de grupo de C_K para ver que $(3, 1-\sqrt{-5})$ no es principal. Ya que, como $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, tenemos que $\overline{(3)} = \overline{(3, 1+\sqrt{-5})}\,\overline{(3, 1-\sqrt{-5})}$.

Si $(3, 1-\sqrt{-5})$ fuera principal, tendríamos que $\overline{(3,1-\sqrt{-5})} = 1$, por tanto $1 = \overline{(3,1+\sqrt{-5})} \cdot 1$, es decir, $\overline{(3,1+\sqrt{-5})}$ sería principal, y hemos visto que no lo es.

Vamos a estudiar entonces los elementos del grupo conmutativo C_K. Por lo dicho al principio de la sección, un conjunto de generadores del grupo vendrá dado por las clases de $2_1 := (2, 1+\sqrt{-5}), 3_1 = (3, 1+\sqrt{-5}), 3_2 = (3, 1-\sqrt{-5}), 5_1 = (\sqrt{-5}), 7_1 = (7, 3+\sqrt{-5}), 7_2 = (7, 3-\sqrt{-5}), 11_1 = (11)$ y $13_1 = 13$. Además no es difícil comprobar que todos estos ideales son distintos dos a dos, comprobando que el ideal generado por cualesquiera dos de ellos es 1. $5_1, 11_1$ y 13_1 son principales, osea que sus clases son el elemento 1 de C_K.

Por tanto C_K está generado por $\overline{2_1}, \overline{3_1}, \overline{3_2}, \overline{7_1}, \overline{7_2}$. Para estudiar la estructura del grupo habrá que intentar estudiar la relación entre sus elementos. Por las igualdades de ideales que hemos visto $((2) = 2_1^2, (3) = 3_1 3_2, \dots)$, tenemos que:

- $\overline{2_1}^2 = 1$
- $\overline{3_1} \cdot \overline{3_2} = 1$
- $\overline{7_1} \cdot \overline{7_2} = 1$

Vamos a buscar más relaciones. Por lo visto, el ideal (6) factoriza como $2_1^2 3_1 3_2$. Además, $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$, por tanto los factores $2_1^2 3_1 3_2$ se reparten entre $(1+\sqrt{-5})(1-\sqrt{-5})$. Como además está claro por sus definiciones que $2_1 | (1+\sqrt{-5})$, $3_1 | (1-\sqrt{-5})$, $2_1 | (1-\sqrt{-5})$, $3_2 | (1-\sqrt{-5})$, se dará que $(1+\sqrt{-5}) = 2_1 3_1$ y $(1-\sqrt{5}) = 2_1 3_2$. Por tanto:

- $\overline{2_1} \cdot \overline{3_1} = 1$
- $\overline{2_1} \cdot \overline{3_2} = 1$

Un planteamiento similar usando el ideal $(14) = (3+\sqrt{-5})(3-\sqrt{-5})$ en vez de $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$ nos lleva a que:

- $\overline{2_1} \cdot \overline{7_1} = 1$
- $\overline{2_1} \cdot \overline{7_2} = 1$

Ya tenemos suficiente para concluir que el grupo C_K tiene de hecho 2 elementos: basta ver que $\overline{2_1}, \overline{3_1}, \overline{3_2}, \overline{7_1}, \overline{7_2}$ son todos iguales. Esto se deduce de las relaciones que hemos ido deduciendo: como $1 = \overline{2_1}^2 = \overline{2_1} \cdot \overline{3_1} = \overline{2_1} \cdot \overline{3_2} = \overline{2_1} \cdot \overline{7_1} = \overline{2_1} \cdot \overline{7_2}$, dividiendo entre $\overline{2_1}$ en las igualdades tenemos que $\overline{2_1} = \overline{3_1} = \overline{3_2} = \overline{7_1} = \overline{7_2}$. Así que C_K está generado por $\overline{2_1}$. Como $\overline{2_1}$ tiene orden 2, al no ser principal y cumplir $\overline{2_1}^2 = 1$, ya lo tenemos:

El grupo $C_{\mathbb{Q}[\sqrt{-5}]}$ tiene dos elementos. Por tanto $\mathbb{Z}[\sqrt{-5}]$ no es un DIP, y de hecho es directo comprobar que no es un DFU, ya que $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$ son dos factorizaciones distintas de 6 como producto de irreducibles.

En el ejemplo anterior, ambas factorizaciones de 6 tienen 2 factores. Esto se puede generalizar:

Teorema 5.32 (Carlitz)**.** Si $h_K = |C_K| = 2$, entonces para cualquier $\alpha \in O_K$, cualquier factorización de α como producto de irreducibles tiene el mismo número de elementos.

Demostración. Consideramos la factorización de (α) (única) en ideales primos,

$$(\alpha) = p_1 \dots p_s \pi_1 \dots \pi_t,$$

donde los p_i son principales y los π_i no lo son.

Ahora, sea $\alpha = \alpha_1 \dots \alpha_n$ una factorización de α como producto de irreducibles. Los ideales (α_i) tendrán en su factorización como producto de ideales primos algunos de los p_i y los π_i. En concreto:

- Si (α_i) es maximal, entonces $(\alpha_i) = (p_i)$ para algún i, ya que no puede ser ningún π_j al no ser principales estos ideales.

- Si (α_i) no es maximal, (α_i) será un producto de los π_j, ya que ningún p_j puede dividir a (α_i): en ese caso tendríamos que $(\alpha_i) \subsetneq (p_j)$ al ser (α_i) no maximal, por tanto α_i sería el producto de el generador de p_j y un elemento no unidad.

  De hecho, (α_i) es producto de exactamente dos de los π_j: (α_i) no puede ser ningún π_j al ser principal, y si (α_i) fuera producto de 3 o más de los π_j, tendríamos que $(\alpha_i) = \pi_{i_1}\pi_{i_2}I$, para ciertos i_1, i_2 e I ideal propio de O_K. Sin embargo, como $|C_K| = 2$ y π_{i_1}, π_{i_2} no son principales, su producto es principal, generado por cierto elemento g. De modo que (α_i) es g por un elemento de I, es decir, no es irreducible: contradicción. De modo que (α_i) es producto de exactamente dos de los π_j.

Concluimos entonces que para cualquier factorización $\alpha = \alpha_1 \dots \alpha_n$, y su correspondiente factorización de ideales $(\alpha) = (\alpha_1)\dots(\alpha_n)$, habrá algunos α_i tales que (α_i) es uno de los p_j (en concreto, hay s de ellos) y otros α_i tales que (α_i) es de forma $\pi_{i_1}\pi_{i_2}$ (en concreto, habrá $\frac{t}{2}$ de ellos). De modo que cualquier factorización de α como producto de irreducibles tiene el mismo número de elementos, $s + \frac{t}{2}$. □

Esta demostración del teorema y una de su recíproco, que también es cierto, puede encontrarse en [4].

Es conocido que todo dominio euclídeo es un DIP. Sin embargo la implicación recíproca es falsa: hay DIPs que no son dominios euclídeos. El siguiente ejemplo es uno de ellos.

Ejemplo 5.33. Vamos a calcular C_K, con $K = \mathbb{Q}[\sqrt{-19}]$. Por lo visto en 4.10, O_K es $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Una base entera de este anillo es $\left\{1, \frac{1+\sqrt{-19}}{2}\right\}$. Llamamos $\alpha = \frac{1+\sqrt{-19}}{2}$. Como en los ejemplos anteriores obtenemos M_K, en este caso resulta que $M_K = 16$, igual que en $K = \mathbb{Q}[\sqrt{-5}]$.

De modo que de nuevo, buscamos ideales primos P con $16! \in P$, así que igual que antes, tendremos que $p \in P$, para algún primo entero $p < 16$. Se puede comprobar que los ideales maximales (distintos) que obtendremos mediante este procedimiento son:

- $2_1 = (2)$
- $3_1 = (3)$
- $5_1 = (5, \alpha), 5_2 = (5, \alpha - 1)$
- $7_1 = (7, \alpha - 2), 7_2 = (7, \alpha + 1)$
- $11_1 = (11)$
- $13_1 = (13)$

Es instructivo ver una forma de comprobar que (13) es ideal maximal. Si no lo fuera, estaría contenido en algún maximal P, y podríamos coger cierto $\beta \in P \setminus (13)$. $N(\beta)$ es un entero, y está en P por ser múltiplo de β. Por tanto $13|N(\beta)$, ya que si no 1 sería combinación entera de 13 y $N(\beta)$, y sabemos que $1 \notin P$. Expresando $\beta = a + b\alpha$, podemos calcular que $N(\beta) = \frac{(2a-b)^2+19b^2}{4}$. Por tanto como $13|N(\beta)$, tendremos que $13|(2a-b)^2 + 19b^2$. Si $b \equiv_{13} 0$, por la ecuación anterior tendríamos $a \equiv_{13} 0$, por tanto β sería múltiplo de 13, lo cual no es cierto. Por tanto $b \neq 0$. Así que en módulo 13 tenemos la ecuación $-19 = \frac{(2a-b)^2}{b^2}$. Es decir, $-19 \equiv 7$ sería un residuo cuadrático módulo 13. Esto no se cumple, por tanto tenemos una contradicción y (13) es maximal. Se puede ver que $(2), (3), (11)$ son maximales de forma similar.

Si comprobamos que los ideales $(5, \alpha), (5, \alpha - 1), (7, \alpha - 2)$ y $(7, \alpha + 1)$ son principales, ya tendremos que todos nuestros ideales P maximales con $16! \in P$ son principales, por tanto el grupo C_K será trivial, y tendremos que $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ es un DIP.

Empezamos por $(5, \alpha)$. Este ideal es principal, ya que $|\alpha| = \alpha\overline{\alpha} = 5$, por tanto $5 \in (\alpha)$, por tanto $(5, \alpha) = (\alpha)$. Visto esto, está claro que $(5, \alpha - 1)$ es principal, ya que el producto de las clases de $(5, \alpha)$ y $(5, \alpha - 1)$ es la clase de (5), que es la identidad en C_K.

De igual forma vemos que $(7, \alpha+1) = (\alpha+1)$ ya que $|\alpha+1| = 7$, y también como antes, como $(7, \alpha+1)$ es principal y $(7, \alpha+1)(7, \alpha-2) = (7)$ es principal tenemos que $(7, \alpha-2)$ es principal.

De modo que hemos demostrado que $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ es un DIP. Además no va a ser difícil ver que este anillo no es un dominio euclídeo: Supongamos que φ es una norma euclídea en R, y sea $x \in R - \{-1, 0, 1\}$ con $\varphi(x)$ mínimo. Es decir, x no es una unidad pero cualquier elemento con norma menor que la de x es una unidad. Por tanto por definición de norma euclídea podemos expresar cualquier elemento de R como $ax + r$, con $r \in \{-1, 0, 1\}$. Esto quiere decir que $\frac{R}{(x)}$ tiene como máximo 3 elementos. Esto implica que alguno de los números $1, 2, 3$ tiene que estar en (x), ya que si $1, 2, 3$ no estuvieran en el ideal, sus diferencias (que son $\pm 1, \pm 2$) tampoco estarían en el ideal y por tanto tendríamos, junto con el 0, 4 elementos distintos de $\frac{R}{(x)}$. Obviamente 1 no está en x, y como $2, 3$ son primos en R solo tendríamos las opciones $(x) = (2)$ y $(x) = (3)$, las cuales descartamos ya que $\frac{R}{(x)}$ tiene 4 y 9 elementos respectivamente en esos casos. Por tanto $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ es un DIP que no es un dominio euclídeo.

Introducimos sin demostración otro teorema que nos permite ahorrar muchos cálculos al trabajar con el grupo de clases para estudiar si un anillo de números es DIP. Usando la definición 5.35:

Teorema 5.34. Todo ideal de O_K es equivalente a un ideal J tal que

$$N(J) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_k|},$$

donde r_2 se define así: si n es el orden de $K/\mathbb{Q}$, habrá un número r_1 de inmersiones σ tales que $\sigma(K) \subseteq \mathbb{R}$, y un número par $2r_2$ de inmersiones complejas, tales que $\sigma(K) \not\subseteq \mathbb{R}$. Este número es par ya que si σ es una inmersión con $\sigma(K) \not\subseteq \mathbb{R}$, el conjugado de sigma, $\overline{\sigma}(x) = \overline{\sigma(x)}$, también lo es, y es distinto a σ.

5.4 Normas de ideales

Definición 5.35. Definimos la norma de un ideal no nulo $I \subseteq O_K$ como $N(I) = \left|\frac{O_K}{I}\right|$.

En cuerpos de enteros, la norma de un ideal siempre será un número natural.
Vamos a ver propiedades que cumple la norma. Este concepto será importante:

Definición 5.36. Decimos que dos ideales I, J son comaximales si $I + J = (1)$.

Proposición 5.37. Si $I + J = (1)$, entonces $I^i + J^j = (1)$ para todos i, j.

Demostración. Tenemos que $1 = a + b$ para ciertos $a \in I, b \in J$. Elevando a $i + j$, tenemos que:

$$1 = (a+b)^{i+j} = \sum_{k=0}^{i+j} \binom{i+j}{k} a^k b^{i+j-k} = \sum_{k=0}^{i} \binom{i+j}{k} a^k b^{i+j-k} + \sum_{k=i+1}^{i+j} \binom{i+j}{k} a^k b^{i+j-k}.$$

En la anterior suma, el primer sumando es múltiplo de b^j, por tanto está en J^j, y el segundo sumando es múltiplo de a^i, por tanto está en I^i. Por tanto $1 \in I^i + J^j$. □

Proposición 5.38. Si $I + J = (1)$, entonces $I \cap J = IJ$.

Demostración. $IJ \subseteq I \cap J$ siempre se cumple para I, J ideales cualesquiera, ya que $IJ \subseteq IO_K = I$, y $IJ \subseteq O_K J = J$. Además, si $I + J = (1)$, hay $i \in I, j \in J$ con $i + j = 1$, por tanto para cualquier $x \in I \cap J$, $x = x1 = xi + xj \in IJ$. □

Proposición 5.39. Si $I + J = O_K$, entonces $N(I)N(J) = N(IJ)$.

Demostración. Por la definición de norma, nos basta ver que $\frac{O_K}{IJ}$ y $\frac{O_K}{I} \times \frac{O_K}{J}$ tienen el mismo número de elementos. Consideremos la siguiente función:

$$\begin{array}{ccc} O_K & \to & \frac{O_K}{I} \times \frac{O_K}{J}; \\ x & \to & (x + I, x + J) \end{array}$$

esta función es un homomorfismo de anillos, y su núcleo es claramente $I \cap J$. Además será sobreyectiva: dado un elemento $(y+I, z+J)$ de $\frac{O_K}{I} \times \frac{O_K}{J}$, existe x con $(x+I, x+J) = (y+I, z+J)$. Para comprobarlo basta coger $x = a_1 z + a_2 y$, donde $a_1 \in I, a_2 \in J$ y $a_1 + a_2 = 1$. En este caso, $x + I = a_1 z + a_2 y + I = a_2 y + I = y + I$, donde la última igualdad viene de que $y - a_2 y = a_1 y \in I$.

Por tanto el homomorfismo induce un isomorfismo $\frac{O_K}{I \cap J} \equiv \frac{O_K}{I} \times \frac{O_K}{J}$. Así que por la proposición anterior, $I \cap J = IJ$. □

Vamos ahora a centrarnos en la factorización de ideales de forma pO_K, con $p \in \mathbb{Z}$ entero.

Definición 5.40. Sea P ideal maximal, I ideal en O_K. Llamamos $e(P|I)$ al mayor número entero e tal que $P^e | I$ (en caso de que $P \nmid I$, $e(P|I) = 0$).

Llamamos $e(P|\mathbb{Z}) = e(P|P \cap \mathbb{Z})$.

Ahora, sea P un ideal primo de O_K. Llamamos p al primo entero con $P \cap \mathbb{Z} = p\mathbb{Z}$. Sabemos que $O_K/(p)$ es un cuerpo finito. Podemos considerar el homomorfismo de anillos $\mathbb{Z} \to \frac{O_K}{P}$ dado por $m \to m + P$. Su núcleo será $p\mathbb{Z}$, por tanto el homomorfismo induce una inclusión

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \hookrightarrow \frac{O_K}{P}; \overline{n} \mapsto n + P$$

en concreto, como $\frac{\mathbb{Z}}{p\mathbb{Z}}$ es un cuerpo, esto da a $\frac{O_K}{P}$ una estructura de espacio vectorial sobre $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (con producto escalar $\overline{n}(a+P) = na + P$).

Definición 5.41. Llamamos grado de inercia de P sobre $\mathbb{Z}$, $f(P/\mathbb{Z})$ o $f(P/p)$ al grado de la extensión $[\frac{O_K}{P} : \frac{\mathbb{Z}}{p\mathbb{Z}}]$.

Nuestro próximo objetivo será probar que, dados p primo entero y K cuerpo de números, con $[K : \mathbb{Q}] = n$ y (p) factorizando como $(p) = \prod_{i=1}^{r} P_i^{e_i}$, entonces se cumple que $n = \sum_{i=1}^{r} e_i f_i$, siendo $f_i = f(P_i|p)$.

Proposición 5.42. Si P es un ideal primo de O_K, entonces $N(P) = p^{f(P|p)}$.

Demostración. O_K/P es un espacio vectorial de dimensión f sobre $\mathbb{Z}/p\mathbb{Z}$, así que tiene p^f elementos. Por tanto $N(P) = |O_K/P| = p^f$. □

Proposición 5.43. Si P es un ideal primo de O_K y $m \in \mathbb{Z}$, $N(P^m) = N(P)^m$.

Demostración. Usamos inducción. El caso $m = 1$ es la proposición anterior.
Suponemos entonces que $N(P^{m-1}) = N(P)^{m-1}$. En primer lugar $P^m \subsetneq P^{m-1}$ siendo P^{m-1} ideal de O_K (por haber factorización única de ideales). Tomemos $\alpha \in P^{m-1} \setminus P^m$, de modo que $P^m \subsetneq P^m + (\alpha) \subset P^{m-1}$, y veamos que entonces se cumple que $P^m + (\alpha) = P^{m-1}$.
Esto pasa por que como $P^{m-1} | P^m + (\alpha)$ y $P^m + (\alpha) | P^m$, habrá ideales I, J con $P^m = I(P^m + (\alpha))$ y $P^m + (\alpha) = JP^{m-1}$. Por tanto $P^m = IJP^{m-1}$, es decir, $P = IJ$, por tanto al ser I no trivial y P primo, $J = O_K$, así que en efecto $P^m + (\alpha) = P^{m-1}$.

Ahora, P^{m-1}/P^m es ideal de O^k/P^m luego, usando los teoremas de isomorfía:

$$\frac{O_K/P^m}{P^{m-1}/P^m} \approx \frac{O_K}{P^{m-1}} \Rightarrow N(P^m) = N(P^{m-1}) \left| \frac{P^{m-1}}{P^m} \right| \overset{(*)}{=} N(p)^{m-1} N(p) = N(p)^m$$

En la igualdad $(*)$ hemos usado la definición de norma, la hipótesis de inducción y que $\left| \frac{P^{m-1}}{P^m} \right| = N(p)$, demostrémoslo:
Definimos la aplicación $\phi : O_K \to \frac{P^m + (\alpha)}{P^m}$ tal que $\phi(\beta) = \beta\alpha + P^m \ \forall \alpha \in O_K$. Conserva sumas pues

$$\phi(\beta_1 + \beta_2) = (\beta_1 + \beta_2)\alpha + P^m = \beta_1\alpha + P^m + \beta_2\alpha + P^m = \phi(\beta_1) + \phi(\beta_2).$$

Es sobreyectiva, un elemento en $P^m + (\alpha)$ es $\beta\alpha + \gamma$ con $\gamma \in P^m$ luego al cocientar nos queda $\beta\alpha$.
Además, $\beta \in \ker \phi \Leftrightarrow \beta\alpha \in P^m \Leftrightarrow (\beta)(\alpha) \subset P^m \Leftrightarrow P^m | (\alpha)(\beta)$. Recordemos que $\alpha \in P^{m-1} \setminus P^m$ luego

$P|(\beta)$, que sucede cuando $\beta \in P$ luego $\ker \phi = P$.
Por tanto

$$\frac{O_K}{P} \approx \frac{P^{m-1}}{P^m}$$

Así que $\left|\frac{P^{m-1}}{P^m}\right| = \left|\frac{O_K}{P}\right| = N(p)$, □

Teorema 5.44. Si tenemos un ideal $I \subseteq O_K$ con factorización en primos $P_1^{m_1} \cdot \ldots \cdot P_r^{m_r}$, entonces $N(I) = N(P_1^{m_1}) \cdot \ldots \cdot N(P_r^{m_r})$.

Demostración. Tenemos que $N(I) = N(P_1^{m_1}) \cdot \ldots \cdot N(P_r^{m_r})$ por 5.39, ya que por 5.37 los $P_i^{m_i}$ son comaximales dos a dos. Además, por la proposición anterior $N(P_i^{m_i}) = N(P_i)^{m_i}$, y hemos acabado. □

Corolario 5.45. Si I, I' son ideales en O_K, $N(II') = N(I)N(I')$. □

Corolario 5.46. Si P es primo en O_K y con la notación anterior, $N(P^m) = p^{fm}$.

Proposición 5.47. Sea $\alpha \in O_K,\ K = \mathbb{Q}(\gamma)$ con $K/\mathbb{Q}$ de Galois.[1] Entonces

$$N((\alpha)) = \left|N_{K/\mathbb{Q}}(\alpha)\right|$$

Demostración. Recordemos que $N_{K/\mathbb{Q}}(\alpha) = \prod \sigma_i(\alpha)$ donde las σ_i son las inmersiones.
Así que

$$|N_{K/\mathbb{Q}}(\alpha)|^n = \left|\frac{O_K}{(|N_{K/\mathbb{Q}}(\alpha)|)}\right| = \left|\frac{O_K}{(|\sigma_1(\alpha) \cdot \ldots \cdot \sigma_n(\alpha)|)}\right| =$$

$$\left|\frac{O_K}{(|\sigma_1(\alpha)|)}\right| \cdot \ldots \cdot \left|\frac{O_K}{(|\sigma_n(\alpha)|)}\right| = N((\sigma_1(\alpha))) \cdot \ldots \cdot N((\sigma_n(\alpha)))$$

Veamos ahora que $N((\sigma_i(\alpha))) = N((\alpha))$. Como las aplicaciones σ_i son automorfismos $\sigma_i : K \to K$, con $\sigma_i((\alpha)) = (\sigma_i(\alpha))$, σ_i induce un isomorfismo entre cocientes $\frac{K}{(\alpha)} \to \frac{K}{(\sigma_i(\alpha))}$, por tanto $\left|\frac{K}{(\alpha)}\right| = \left|\frac{K}{(\sigma_i(\alpha))}\right|$, es decir, $N((\sigma_1(\alpha))) = N((\alpha))$.

que restringida a $\sigma_i : K \to K$ también lo es luego $(\alpha) \mapsto (\sigma_i(\alpha))$ y entonces $\frac{O_K}{(\alpha)}$ es isomorfo a $\frac{O_K}{(\sigma_i(\alpha))}$ luego tienen el mismo número de elementos y sus normas coinciden. En consecuencia:

$$|N_{K/\mathbb{Q}}(\alpha)|^n = N((\sigma_1(\alpha))) \cdot \ldots \cdot N((\sigma_n(\alpha))) = N((\alpha))^n,$$

y se cumple el enunciado. □

Teorema 5.48. Sea n la dimensión del cuerpo de números sobre $\mathbb{Q}$. Entonces $n = \sum_{i=1}^r e_i f_i$, $\quad pO_K = P_1^{e_1} \ldots P_r^{e_r}$.

Demostración. Tenemos que

$$p^n = N(pO_K) = N(P_1^{e_1} \ldots P_r^{e_r}) = N(P_1^{e_1}) \ldots N(P_r^{e_r}) = p^{f_1 e_1} \ldots p^{f_r e_r} = p^{\sum_{i=1}^r e_i f_i} \Rightarrow\ n = \sum_{i=1}^r e_i f_i.$$

□

Ejemplo 5.49. Sea $n = 2$, cuerpo cuadrático. Entonces cada primo p puede descomponer de dos modos:

$$pO_K = \begin{cases} P_1^2 & r = 1,\ e_1 = 2,\ f_1 = 1, & N(P_1) = p^1 = p, & \frac{O_K}{P_1} \approx \frac{\mathbb{Z}}{p\mathbb{Z}} \\ P_1 P_2 & r = 2,\ e_1 = e_2 = f_1 = f_2 = 1, & N(P_i) = p, & \frac{O_K}{P_i} \approx \frac{\mathbb{Z}}{p\mathbb{Z}} \\ P_1 & r = 1,\ e_1 = 1,\ f_1 = 2 & N(P_1) = p^2 & \frac{O_K}{P_1} \approx \mathbb{F}_{p^2} \end{cases}$$

[1] Este último requisito es para que la demostración sea más presentable. Realmente la igualdad se da aunque la extensión no sea de Galois. Por tanto, dado un ideal maximal de norma $p \in \mathbb{Z}$ primo. Si encontramos $\alpha \in K$ de norma p, sabemos que el ideal es principal y está generado por α.

Ejercicio 5.50. $K = \mathbb{Q}(\sqrt{d}),\ d \equiv_4 3$. Clasificar los ideales pO_K.

Demostración. Si $d \equiv_4 3$, podemos coger de base entera $\{1, \alpha = \sqrt{d}\}$, con discriminante $d_K = 4d$.
$2O_K = 2_1^2,\ 2_1 = (2, \alpha+1)$. Pues $2 = (1+\alpha)((1+\alpha)-2) + \frac{3-d}{4} \cdot 4$ y $(2, 1+\alpha)^2 | (2)$ pues $2|2^2, 2(1+\alpha), (1+\alpha)^2 = 1 + d + 2\alpha$.
Sea ahora $p > 2$. Si $p|d_k = 4d$ entonces $p|d$. Entonces

$$pO_K = P_1^2,\ P_1 = (p, \alpha),$$

ya que obviamente $P_1^2 \subseteq pO_K$ y además $p \in P_1^2$, ya que $p = mcd(p^2, d)$ por ser d libre de cuadrados, por tanto p es una combinación entera de p^2 y d, que están en P_1^2.
En el caso de que $p \nmid d$ y que $\left(\frac{d}{p}\right) = 1$ tendremos que

$$pO_K = P_1P_2,\ P_1 = (p, \alpha + a),\ P_2 = (p, \alpha - a)$$

donde $a^2 \equiv d \mod p$. Veámoslo, existe $k_a : d - a^2 = pk_a$. Entonces

$$P_1P_2 = (p, \alpha+a)(p, \alpha-a) = (p^2, p(\alpha+a), p(\alpha-a), d-a^2) = (p^2, 2p\alpha, 2pa, k_ap) = (p)(p, 2\alpha, 2a, k_a)$$

Sabemos $1 \in (p, 2\alpha, 2a, k)$ pues $p \nmid 2a$ ya que si lo hiciese se tendría que $p^2|4a^2 = 4(d - pk_a)$. Además $(p, \alpha+a) \neq (p, \alpha-a)$, si los ideales fuesen iguales $\alpha + a$ y $\alpha - a$ se encontrarían en el mismo ideal maximal y $2a$ también. Al ser p impar 2 no estaría en el ideal luego a tendría que estar en (p) pero $a^2 \equiv d \mod p$ luego $d \equiv_p 0$ y p dividiría a d.

Por último, si $p \nmid d$ y que $\left(\frac{d}{p}\right) = -1$ se tendrá que $pO_K = P_1$, veremos este caso generalizado en 5.52. □

Ejemplo 5.51. Fijémonos en que la cantidad de primos que dividen a d es finita. Para los que no dividen a d vemos que podemos determinar pO_K según la ley de reciprocidad cuadrática:

$$\left(\frac{d}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{d_k}{p}\right).$$

Si $d = 3 \Rightarrow\ d_K = 12$:

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow 1 = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} \Leftrightarrow\ p \equiv_{12} 1, 9, 11$$

5.5 Lema de Kummer. Ejemplos

Lema 5.52 (Kummer)**.** Sea $K = \mathbb{Q}(\alpha),\ \alpha \in O_K$ cuerpo de números, y sea p primo entero que no divide a $m := [O_K : \mathbb{Z}[\alpha]]$. Denotemos por $g := \min_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Sea $\overline{g} \in \mathbb{Z}_p[x]$ el polinomio g módulo p.
Escribimos $\overline{g} = \overline{g}_1^{e_1} \dots \overline{g}_r^{e_r}$ descomposición en polinomios irreducibles en $\mathbb{Z}_p[x]$, con $g_i \in \mathbb{Z}[x]$ mónico y tal que g_i módulo p es $\overline{g}_i$. Se cumplen:

- *i)* $P_i := (p, g_i(\alpha))$ es ideal maximal de $O_K\ \forall i = 1, \dots, r$.
- *ii)* $P_i \neq P_j\ \forall i \neq j$.
- *iii)* $pO_K = P_1^{e_1} \dots P_r^{e_r}$, y el grado de inercia $f(P_i/p)$ es de hecho $f_i := \operatorname{gr} g_i$.

Demostración de 5.52. Haremos 3 afirmaciones, demostraremos el lema a partir de ellas y luego las demostraremos:

- *a)* $P_i = O_K$ ó $O_K/P_i \approx \mathbb{F}_{p^{f_i}},\ f_i = \operatorname{gr}(g_i)$.
- *b)* $P_i + P_j = O_K\ \forall i \neq j$.
- *c)* $pO_K | P_1^{e_1} \dots P_r^{e_r}$.

$a)+b)+c) \Rightarrow$ **Lema** Usando $a)$ y reordenando los P_i si fuese necesario sabemos que

$$P_1, \ldots, P_s \text{ son maximales mientras que } P_{s+1} = \ldots = P_r = O_K.$$

Como $P_i = (p, g_i(\alpha)) \supset p\mathbb{Z}$ tiene sentido calcular $f(P_i/p) = f_i = \text{gr}(g_i)$ pues $O_K/P_i \approx \mathbb{F}_{p^{f_i}}$ para $i = 1, \ldots, s$.
Para $i > s$ no tenemos ideales maximales, no tiene sentido considerar el grado de inercia así que los vamos a ignorar.
Por $b)$ sabemos que P_i y P_j son comaximales para $i \neq j$. Aplicando $c)$:

$$pO_K | P_1^{e_1} \ldots P_r^{e_r} = P_1^{e_1} \ldots P_r^{e_r} O_K \ldots O_K | P_1^{e_1} \ldots P_s^{e_s}.$$

Así que si factorizamos pO_K, queda

$$pO_K = P_1^{e_1'} \ldots P_s^{e_s'}, \quad e_i' \leq e_i.$$

Observemos ahora $c)$:

$$P_1^{e_1} \ldots P_r^{e_r} = pO_K I$$

Veamos que $e_i' = e_i$.
En primer lugar, $n = e_1' f_1 + \ldots + e_s' f_s$.
Por otra parte, $n = \text{gr}(\overline{g}) = e_1 f_1 + \ldots e_r f_r \Rightarrow$

$$0 = (e_1 - e_1')f_1 + \ldots (e_s - e_s')f_s + e_{s+1} f_{s+1} + \ldots e_r f_r.$$

En la igualdad anterior todos los sumandos de la derecha son ≥ 0, por tanto todos son 0. Es decir, $r = s$ y $e_i = e_i' \ \forall i = 1, \ldots, s$, (ya que los f_i son > 0). De $r = s$ y que son comaximales se deduce $ii)$, y por lo que acabamos de ver ya tenemos $iii)$, por tanto ya hemos demostrado el teorema a partir de las 3 afirmaciones. Vamos ahora a probarlas.

$a)$ Consideremos $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]/(\overline{g}_i)$ tal que $\phi(h) = \overline{h} + (\overline{g}_i)$.
Es homomorfismo de anillos unitarios suprayectivo. Además $\mathbb{Z}_p[x]/(\overline{g}_i) \approx \mathbb{F}_{p^{f_i}}$ pues un elemento de $\mathbb{Z}_p[x]/(\overline{g}_i)$ es de la forma

$$\overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_m x^m + (\overline{g}_i)$$

donde $m + 1 = \text{gr}(\overline{g}_i)$, luego tenemos $p^m = p^{f_i}$ elementos.
Por otro lado, $\mathbb{Z}_p[x]$ es dominio de ideales principales, $(\overline{g}_i)$ es ideal principal y $\overline{g}_i$ irreducible. $(\overline{g}_i)$ es ideal maximal luego $\mathbb{Z}_p[x]/(\overline{g}_i)$ es cuerpo.
Calculemos ahora $\ker \phi$. Tanto p como g_i están en el núcleo de ϕ. Por tanto

$$(p, g_i) \subset \ker \phi.$$

Sea ahora $h \in \ker \phi$, entonces $\overline{h} \in (\overline{g}_i) \Rightarrow$

$$\exists k_1 \in \mathbb{Z}[x] : \ \overline{h} = \overline{k}_1 \overline{g}_i \Rightarrow \ \exists k_2 \in \mathbb{Z}[x] : \ h - k_1 g_i = p k_2 \Rightarrow \ h = k_1 g_i + p k_2 \in (p, g_i)$$

Así que $\ker \phi = (p, g_i)$ luego por el teorema de isomorfía

$$\frac{\mathbb{Z}[x]}{\ker \phi} \approx \mathbb{F}_{p^{f_i}} \Rightarrow \ \ker \phi \text{ es ideal maximal.}$$

Ahora definimos $\psi : \mathbb{Z}[x] \to O_K/P_i$ como $\psi(h) = h(\alpha) + P_i$ homomorfismo de anillos.
Ahora, $(p, g_i) \subset \ker \psi$ pues

$$\psi(p) = p + P_i = P_i, \qquad \psi(g_i) = g_i(\alpha) + P_i = P_i.$$

Pero entonces $(p, g_i) \subset \ker \psi \subset \mathbb{Z}_p[x]$ con (p, g_i) ideal maximal así que

$$(p, g_i) = \ker \psi \qquad \text{ó} \qquad \ker \psi = \mathbb{Z}[x]$$

ahora veamos que ψ es sobreyectiva, para ello tenemos que ver que $O_K = \mathbb{Z}[\alpha] + P_i$, es decir, que todo $\beta \in O_K$ puede expresarse como $h(\alpha) + \gamma$, con $h \in \mathbb{Z}[x]$, $\gamma \in P_i$

Veamos de hecho algo un poco más general: que $\mathbb{Z}[\alpha] + pO_K \overset{(*)}{=} O_K$. Si demostramos eso tendremos que

$$O_K = \mathbb{Z}[\alpha] + pO_K \subset \mathbb{Z}[\alpha] + P_i \subset O_K, \text{ por tanto } O_K = \mathbb{Z}[\alpha] + P_i.$$

Demostremos entonces $(*)$. Claramente

$$\mathbb{Z}[\alpha], pO_K \subset \mathbb{Z}[\alpha] + pO_K \subset O_K$$

El cociente $\frac{O_K}{pO_K}$ tiene p^n elementos. Además, $p \nmid m = [O_K : [\alpha]]$. Sea $s = [O_K : \mathbb{Z}[\alpha] + pO_K],\ s|p^n, m$ así que $s = 1$. Es decir: $\mathbb{Z}[\alpha] + pO_K = O_K$ y por tanto ψ es sobreyectiva.

Seguimos con $(p, g_i) = \ker\psi$ ó $\ker\psi = \mathbb{Z}[x]$.

- Si $\ker\psi = \mathbb{Z}[x] \Rightarrow\ \frac{\mathbb{Z}[x]}{\mathbb{Z}[x]} \approx \frac{O_K}{P_i} \Rightarrow O_K = P_i$.
- Si $\ker\psi = (p, g_i) \Rightarrow\ \frac{\mathbb{Z}[x]}{(p,g_i)} \approx \frac{O_K}{P_i}$. Pero $\frac{\mathbb{Z}[x]}{(p,g_i)} \approx \mathbb{F}_{p^{f_i}}$.

b) Tenemos que ver que $1 \in P_i + P_j,\ i \neq j$:

$$P_i + P_j = (p, g_i(\alpha), g_j(\alpha)).$$

Sabemos que $\overline{g}_i, \overline{g}_j \in \mathbb{Z}_p[x]$ irreducibles distintos. Como $\mathbb{Z}[x]$ es un DIP, la identidad de Bezout nos dice que

$$\overline{1} = \overline{h}_i\overline{g_i} + \overline{h}_j\overline{g}_j \Rightarrow\ 1 = h_ig_i + h_jg_j + ph_{ij},$$

para ciertos $h_i, h_j, h_{ij} \in \mathbb{Z}[x]$. Ahora sustituímos α :

$$1 = h_i(\alpha)g_i(\alpha) + h_j(\alpha)g_j(\alpha) + ph_{ij}(\alpha) \in (p, g_i(\alpha), g_j(\alpha)) = P_i + P_j.$$

Luego $P_i + P_j = O_K$.

c) El objetivo es ver que $pO_K | P_1^{e_1} \dots P_r^{e_r}$. En primer lugar:

$$P_1^{e_1} \dots P_r^{e_r} = (p, g_1(\alpha))^{e_1} \dots (p, g_r(\alpha))^{e_r} = \left(p\beta_1, \dots, p\beta_k, \prod_{i=1}^{r} g_i^{e_i}\right) \text{(Para algunos } \beta_1, \dots, \beta_k)$$

Es decir, si escribimos el producto como lista de generadores, todos ellos serán de la forma p por algo menos uno: $\prod_{i=1}^{r} g_i^{e_i}$:

$$\overline{g} = \overline{g}_1^{e_1} \dots \overline{g}_r^{e_r} \Rightarrow\ g = g_1^{e_1} \dots g_r^{e_r} + ph,\ h \in \mathbb{Z}[x].$$

Sustituyendo α :

$$0 = g(\alpha) = g_1^{e_1}(\alpha) \dots g_r^{e_r}(\alpha) + ph(\alpha) \Rightarrow\ g_1^{e_1}(\alpha) \dots g_r^{e_r}(\alpha) = -ph(\alpha).$$

Luego

$$P_1^{e_1} \dots P_r^{e_r} = \left(p\beta_1, \dots, p\beta_k, \prod_{i=1}^{r} g_i^{e_i}\right) = (p\beta_1, \dots, p\beta_k, -ph(\alpha)) = (p)(\beta_1, \dots, \beta_k, -h) \subset (p) \Rightarrow$$

$$pO_K | (p)(\beta_1, \dots, \beta_k, -h) = P_1^{e_1} \dots P_r^{e_r}.$$

□

El primer ejemplo de uso que veremos son algunos cuerpos cuadráticos.

Ejemplo 5.53. Tenemos $\alpha := \sqrt{d},\ d \equiv 3 \mod 4,\ d_K = 4d,\ \{1, \alpha\}$ base entera por 4.11.
Al ser base entera tenemos que $[O_K : \mathbb{Z}[\alpha]] = 1$ así que con este α y con $g = x^2 - d$ podremos trabajar con todo p primo.
Si $p = 2$:

$$\overline{g} \equiv_2 x^2 + 1 \equiv_2 (x+1)^2 \Rightarrow\ 2O_K = (2, \alpha + 1)^2,\ f = 1,\ e = 2.$$

Si $2 < p$:
En el caso de que $p|d$ se tiene que

$$\overline{g} \equiv_p x^2 \Rightarrow pO_K = (p, \alpha).$$

Ahora, si $p \nmid d$ tenemos dos opciones. Supongamos que d es residuo cuadrático módulo p, luego $\exists a \in \mathbb{Z}$:

$$\overline{g} \equiv_2 (x-a)(x+a) \Rightarrow pO_K = (p, \alpha + a)(p, \alpha - a),\ (p, \alpha + a) \neq (p, \alpha - a)$$

Por último, si $p \nmid d$ y d no es residuo cuadrático se tiene que $\overline{g}$ es irreducible luego $pO_K = (p, 0) = (p)$ maximal, $f = 2$.

Ejemplo 5.54. Sea $d \equiv 2 \mod 4,\ K := \mathbb{Q}(\sqrt{d}),\ d_K = 4d,\ \{1, \sqrt{d}\}$ es base entera luego $O_K = \mathbb{Z}[\sqrt{d}]$.

$$\min_{\mathbb{Q}}(\sqrt{d}) = x^2 - d$$

Sea ahora $p \in \mathbb{Z}$ un primo:

- Si $p = 2 \Rightarrow\ x^2 - d \equiv_2 x^2 \Rightarrow 2O_K = 2_1^2, \quad 2_1 = (2, \sqrt{d})$.
- Si $p > 2,\ p|d \Rightarrow\ x^2 - d \equiv_p x^2 \Rightarrow\ pO_K = p_1^2, \quad p_1 = (p, \sqrt{d})$.
- Si $p \nmid d,\ \left(\frac{d}{p}\right) = 1 \Rightarrow\ x^2 - d \equiv_p (x-a)(x+a),\ a^2 \equiv_p d \Rightarrow\ pO_K = p_1 p_2, \quad p_1 = (p, x-a),\ p_2 = (p, x+a)$.
  Supongamos que $p_1 = p_2 \Rightarrow p|2a$, como p es impar $p|a \Rightarrow p|d$ llegando a un absurdo. Así que $p_1 \neq p_2$.
- Si $p \nmid d,\ \left(\frac{d}{p}\right) = -1 \Rightarrow\ x^2 - d \in \mathbb{Z}_p[x]$ es irreducible luego: (p) es maximal ya que $pO_K = (p, \sqrt{d}^2 - d) = (p)$.

Calcular los grados de inercia es inmediato. Y mediante la ley de reciprocidad cuadrática podemos clasificar los primos en series aritméticas, por ejemplo con $d = 6$ veamos qué pasa con $p \neq 2, 3$ primo:

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p^2-1}{8}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

Estudiemos cuándo $\left(\frac{6}{p}\right) = 1$:

- $2|\frac{p^2-1}{8} + \frac{p-1}{2}$ y $p \equiv_3 0, 1$. Nos fijamos en que

  $$2|\frac{p^2-1}{8} + \frac{p-1}{2} = \frac{p-1}{2}\left(\frac{p+1}{4} + 1\right) \Leftrightarrow\ 16|(p-1)(p+5).$$

  p es impar, así que $2|p-1, p+5$ luego necesitamos que $4|\frac{p-1}{2}\frac{p+5}{2}$. 2 no puede dividir a ambos factores pues $\frac{p+5}{2} - \frac{p-1}{2} = 3$, así que si divide a uno de ellos no puede dividir al otro. Por tanto, si $4|\frac{p-1}{2} \Rightarrow\ p \equiv_8 1$ y si $4|\frac{p+5}{2} \Rightarrow\ p \equiv_8 -5$.
  De esta forma tenemos las opciones $p \equiv 1, 3, 9, 19 \mod 24$.
- $2 \nmid \frac{p^2-1}{8} + \frac{p-1}{2}$ y $p \equiv_3 2$. Ahora buscamos que $4 \nmid \frac{p-1}{2}\frac{p+5}{2}$ así que $p \equiv_8 5, 7$. Por tanto se tiene que $p \equiv_{24} 5, 7$.

De esta forma $\left(\frac{6}{p}\right) = 1 \Leftrightarrow\ p \equiv_{24} 1,3,5,7,9,19.$

Ejemplo 5.55. Ahora sea $d \equiv 1 \mod 4,\ d_K = d,\ \left\{1, \frac{1+\sqrt{d}}{2}\right\}$ es base entera. Para calcular el polinomio mínimo:

$$x = \frac{1+\sqrt{d}}{2} \Rightarrow\ 2x-1 = \sqrt{d} \Rightarrow 4x^4 - 4x + 1 = d \Rightarrow$$

$$\min_{\mathbb{Q}}\left(\frac{1+\sqrt{d}}{2}\right) = x^2 - x + \frac{1-d}{4}.$$

Este polinomio no es cómodo para trabajar así que seguiremos otra estrategia.
Sabemos que $\{1, \sqrt{d}\}$ no es base entera, calculemos $[O_K : \mathbb{Z}[\sqrt{d}]]$.
Para hacerlo tomamos $\{1, \alpha\}$ base de O_K con $\alpha := \frac{1+\sqrt{d}}{2}$. Queremos obtener con ella una base de $\mathbb{Z}[\sqrt{d}]$:

$$\{1, 2\alpha\} = \{1, 1+\sqrt{d}\} \text{ base de } \mathbb{Z}[\sqrt{d}].$$

De esto deducimos que:

$$\frac{O_K}{\mathbb{Z}[\sqrt{d}]} = \frac{\mathbb{Z} \oplus \alpha\mathbb{Z}}{\mathbb{Z} \oplus 2\alpha\mathbb{Z}} \approx \frac{\mathbb{Z}}{\mathbb{Z}} \oplus \frac{\alpha\mathbb{Z}}{2\alpha\mathbb{Z}} \approx \mathbb{Z}_2.$$

Así que $[O_K : \mathbb{Z}[\sqrt{d}]] = 2$.
Fijándonos en la enunciación del lema de Kummer, podremos usar $g = x^2 - d$ para todo primo $p \neq 2$ pues p no debe dividir a $[O_K : \mathbb{Z}[\sqrt{d}]]$ con $g = \min_{\mathbb{Q}}(\sqrt{d})$. De modo que este caso se resuelve como en el ejemplo anterior. Por tanto la clasificación para $p \neq 2$ es exactamente igual que antes. Veamos ahora qué sucede si $p = 2$:
Tenemos

$$x^2 - x + \frac{1-d}{4} \equiv_2 \begin{cases} x^2+x+1 & \text{si} \quad d \equiv_5 \mod 8 \\ x(x-1) & \text{si} \quad d \equiv_1 \mod 8 \end{cases}$$

$x^2 + x + 1$ es irreducible luego

$$2O_K = \begin{cases} 2_1,\ f_1 = 2 & \text{si} \quad d \equiv_5 \mod 8 \\ 2_1 2_2, \quad 2_1 = \left(2, \frac{1+\sqrt{d}}{2}\right),\ 2_2 = \left(2, \frac{-1+\sqrt{d}}{2}\right) & \text{si} \quad d \equiv_1 \mod 8 \end{cases}$$

Hemos estudiado las extensiones cuadráticas. Veamos alguna cúbica ya que la cosa se va a complicar.

Ejercicio 5.56. Sea $K = \mathbb{Q}(\alpha)$ con $\alpha^3 - \alpha - 1 = 0$ y $\alpha \in \mathbb{R}$. Aquí $n = 3,\ \Delta(1, \alpha, \alpha^2) = -23 = d_K$.
Sabemos que $O_K = \mathbb{Z}[\alpha]$, veamos cómo descompone $23O_K$. Para ello factorizamos módulo 23 :

$$x^3 - x - 1 \equiv_{23} (x-3)(x^2+3x+8) \equiv_{23} (x-3)(x-10)^2.^2$$

Así que

$$23O_K = 23_1 23_2^2 \qquad \text{donde} \quad 23_1 = (23, \alpha - 3), \quad 23_2 = (23, \alpha - 10).$$

Además, $e_1 = 1,\ e_2 = 2,\ f_1 = 1,\ f_2 = 1$.
La extensión no era de Galois pues solo estamos metiendo una raíz real mientras que $x^3 - x - 1$ tiene también dos raíces complejas pues el discriminante es negativo.

Ejemplo 5.57. Ahora veamos $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. Vimos que $\Delta(1, \alpha, \alpha^2) = -2^2 \cdot 3^3,\ O_K = \mathbb{Z}[\alpha]$ tomemos $g = x^3 - 2 \in \mathbb{Z}[x]$:

- $2O_K = 2_1^3, \quad 2_1 = (2, \alpha)$.
- $3O_K = 3_1^3, \quad 3_1 = (3, \alpha + 1)$.

[2] El 3 se saca a ojo, después se resuelve la ecuación cuadrática, en el discriminante queda 0 y acabamos con $x \equiv -\frac{3}{2} \equiv -3 \cdot 12 \equiv 3 \cdot 11 \equiv 33 \equiv 10$.

- $p \neq 2,3 \Rightarrow pO_K = \begin{cases} p_1p_2p_3 & e_1=e_2=e_3=f_1=f_2=f_3=1 \quad \text{si} \quad p \equiv_3 1,\ p = C^2+27D^2,\ C,D \in \mathbb{Z}(\text{ver 3.2}). \\ p_1 & e_1=1,\ f_1=3 \quad \text{si} \quad p \equiv_3 1,\ p \neq C^2+27D^2,\ \forall C,D \in \mathbb{Z}. \\ p_1p_2 & e_1=e_2=1,\ f_1=1,\ f_2=2 \quad \text{si} \quad p \equiv_3 2. \end{cases}$

5.6 Ramificación. Ejemplos

Definición 5.58. Decimos que un primo entero p ramifica en K si en la factorización como producto de primos, $(p) = P_1^{e_1} \dots P_r^{e_r}$, hay algún $e_i > 1$.

Teorema 5.59. Sea K cuerpo de números con $K/\mathbb{Q}$ de Galois, sea p primo entero. Entonces, si pO_K factoriza como $pO_K = P_1^{e_1} \dots P_r^{e_r}$, entonces $e_1 = \dots = e_r$ y $f_1 = \dots = f_r$. Llamando e y f a estos valores comunes, tenemos que $n = ref$.

Demostración. Denotemos por $G = \mathcal{G}\text{al}(K/\mathbb{Q}) = \text{Aut}_{\mathbb{Q}} K = \{\sigma_1, \dots, \sigma_n\}$ donde $n = \dim(K/\mathbb{Q})$. Queremos ver que G actúa transitivamente sobre $\{P_1, \dots, P_r\}$. Es decir, queremos ver que los P_i son 'iguales salvo automorfismo'. Desde ahí no será difícil probar que $e_1 = \dots = e_r$ y que $f_1 = \dots = f_r$.

Primero veamos que G actúa sobre $\{P_1, \dots, P_r\}$. Dado cierto P_i y $\sigma \in G$, $\sigma(P_i)$ será un ideal maximal (por serlo P_i y por ser σ un automorfismo) y además, de nuevo por ser σ automorfismo y cumplirse que $P_i|(p)$, tenemos que $\sigma(P_i)|\sigma((p))$, y como $\sigma((p)) = (p)$ (ya que σ fija los racionales), tenemos que $\sigma(P_i)|(p)$. Por tanto $\sigma(P_i)$ es maximal y divide a (p), de modo que es uno de los P_i. Por tanto tiene sentido definir la aplicación

$$\begin{array}{rccc} \varphi: & G \times \{P_1, \dots, P_r\} & \longrightarrow & \{P_1, \dots, P_r\} \\ & (\sigma, P) & \longmapsto & \sigma(P) \end{array}$$

Veamos que efectivamente se trata de una acción de G sobre el conjunto de ideales P :

- $\varphi(\text{id}_K, P) = \text{id}_K(P) = P$.
- $\varphi(\sigma_1 \circ \sigma_2, P) = (\sigma_1 \circ \sigma_2)(P) = \sigma_1(\sigma_2(P)) = \varphi(\sigma_1, \varphi(\sigma_2, P))$.

Así que G actúa sobre $\{P_1, \dots, P_r\}$.

Ahora queremos ver que se trata de una acción transitiva, es decir, dados $P, P' \in \{P_1, \dots, P_r\}$ $\exists \sigma \in G$: $P' = \sigma(P)$. Usaremos reducción al absurdo.
Supongamos que existen $P, P' \in \{P_1, \dots, P_r\}$ tales que para toda $\sigma \in G$: $P' \neq \sigma(P)$. Consideremos ahora el conjunto $\{P', \sigma(P) : \sigma \in G\}$. Por el teorema de los restos:

$$\exists \alpha \in O_K : \begin{cases} \alpha \equiv 0 & \text{mód } P' \\ \alpha \equiv 1 & \text{mód } \sigma(P)\ \forall \sigma \in G \end{cases}$$

En primer lugar, $\alpha \in P'$, en segundo lugar $\alpha \notin \sigma(P)$ ya que si $\alpha \in \sigma(P) \Rightarrow 1 \in \sigma(P) \Rightarrow \sigma(P)$ no sería maximal. Así que, al ser σ automorfismo:

$$\sigma^{-1}(\alpha) \notin \sigma^{-1} \circ \sigma(P) = P\ \forall \sigma \in G, \text{ por tanto } \sigma(\alpha) \notin P\ \forall \sigma \in G.$$

Llegaremos ahora a la contradicción. En primer lugar

$$N_{K/\mathbb{Q}}(\alpha) \in (\alpha) \subset P' \Rightarrow N_{K/\mathbb{Q}}(\alpha) \in P' \cap \mathbb{Z} \overset{(*)}{=} p\mathbb{Z} \subset P.$$

$(*)$ se cumple porque $P' \cap \mathbb{Z}$ es ideal primo de $\mathbb{Z}$ y $P'|pO_K$, ergo $p \in P'$, ergo $p \in P' \cap \mathbb{Z}$, ergo $P' \cap \mathbb{Z} = (p)$. Ahora, sabiendo que $N_{K/\mathbb{Q}}(\alpha) \in P$:

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \Rightarrow \exists \sigma \in G : \sigma(\alpha) \in P$$

Pero habíamos dicho que $\sigma(\alpha) \notin P\ \forall \sigma \in G$. Hemos llegado a una contradicción y por tanto φ es transitiva.

Sean ahora P_i, P_j con $i, j = 1, \ldots, r$ y consideremos $\sigma \in G$ tal que $P_j = \sigma(P_i)$. Entonces, σ es automorfismo en K pero también en O_K y como $p \in \mathbb{Z} \subset \mathbb{Q}$ se tiene que $\sigma(p) = p$ luego:

$$\sigma(pO_K) = pO_K = P_1^{e_1} \ldots P_r^{e_r}.$$

Pero también:

$$\sigma(pO_K) = \sigma\left(P_1^{e_1} \ldots P_r^{e_r}\right) = \sigma(P_1)^{e_1} \ldots \sigma(P_r)^{e_r}.$$

Ahora, $\sigma : \{P_1, \ldots, P_r\} \to \{P_1, \ldots, P_r\}$ es inyectiva luego, al tener O_K descomposición única en ideales primos llegamos a que

$$P_j^{e_j} = \sigma(P_i)^{e_i} = P_j^{e_i}.$$

Fijamos por ejemplo i y vemos que $e_i = e_j \ \forall j = 1, \ldots, r$ luego $e := e_1 = \ldots = e_r$.
Ahora, $f_i = \dim_{\mathbb{Z}_p}\left(\frac{O_K}{P_i}\right)$ luego

$$f_j = \dim_{\mathbb{Z}_p}\left(\frac{O_K}{P_j}\right) = \dim_{\mathbb{Z}_p}\left(\frac{O_K}{\sigma(P_i)}\right) \overset{(**)}{=} \dim_{\mathbb{Z}_p}\left(\frac{O_K}{P_i}\right) = f_i.$$

Con el mismo argumento de antes llegamos a que $f := f_1 = \ldots = f_r$. Veamos $(**)$:
La aplicación $\sigma : O_K \to O_K$ lleva el ideal maximal P_i en el ideal maximal P_j. Entonces la aplicación $\overline{\sigma} : \frac{O_K}{P_i} \to \frac{O_K}{P_j}$ tal que $\beta + P_i \mapsto \sigma(\beta) + P_j$ es isomorfismo:
Hay que ver que está bien definida y directamente tomamos $\overline{\sigma}^{-1}$ para terminar antes.

Ahora, usando 5.48 se tiene que

$$n = \sum_{i=1}^{n} e_i f_i = \sum_{i=1}^{n} ef = ref.$$

□

Proposición 5.60. Si p ramifica en O_K, entonces $p | d_K$.

Demostración. Si p ramifica podemos escribir, para cierto primo P divisor de pO_K que tiene índice de ramificación > 1, $pO_K = PI$, donde cualquier primo Q cumple que $Q | pO_K \ \Leftrightarrow \ Q | I$. Además $PI \subsetneq I$ pues si se tuviese $PI = I \Rightarrow \ P = O_K$ tachando I.
Sea $\alpha \in I \setminus PI = I \setminus pO_K$. Tomemos una base entera de $O_K : \{\alpha_1, \ldots, \alpha_n\}$ y expresamos α en esa base: $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n, \ a_i \in \mathbb{Z}$. Entonces, reordenando si fuese necesario $p \nmid a_1$. Definimos $\alpha_1^* := \alpha$:

$$\Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n) = a_1^2 \Delta(\alpha_1, \ldots, \alpha_n) = a_1^2 d_K.$$

Supongamos ahora que $p | \Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n)$. Entonces $p | a_1^2 d_K$, por tanto $p | d_K$. Así que veamos que $p | \Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n)$. Por 4.41:

$$\Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n) = \begin{vmatrix} \sigma_1(\alpha) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2$$

Pasamos a considerar K^*, el cierre de Galois de K. Los σ_i tienen una extensión a automorfismos K^* por ser K^* extensión de Galois, por tanto podemos considerarlos como automorfismos de K^*. Consideramos ahora un ideal primo Q^* de O_{K^*} que contiene a (p), por tanto $(p) = \mathbb{Q} \cap Q^*$ y definimos $Q = O_K \cap Q^*$, que es un ideal primo de O_K. Tenemos las siguientes inclusiones:

$$\begin{array}{ccccc} \mathbb{Q} & \subseteq & K & \subseteq & K^* \\ (p) & \subseteq & Q & \subseteq & Q^* \end{array}$$

Además, como $\alpha \in I$, α está en todos los primos que dividen a (p), por tanto $\alpha \in Q \subseteq Q^*$. Es decir, $\alpha \in Q^*$ para cualquier Q^* primo de O_{K^*} sobre p. Por tanto, si σ es un automorfismo de K^*, $\alpha \in \sigma(Q^*)$ (ya que $\sigma(Q^*)$ es primo de O_{K^*} sobre p). En concreto, $\alpha \in \sigma_i^{-1}(Q^*)$ para los σ_i, o equivalentemente:

$$\sigma_i(\alpha) \in Q^* \text{ para todo } i \text{ y para todo } Q^* \text{ primo de } O_{K^*} \text{ sobre } p.$$

Ahora, atendiendo a la expresión que hemos dado de $\Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n)$ como determinante, vemos que los elementos de la primera columna están en Q^* y el resto son elementos de O_{K^*}. Por tanto, desarrollando el determinante por la primera columna, tenemos que $\Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n) \in Q^*$, para todo Q^* primo de O_{K^*} sobre p. Pero además, $\Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n)$ es entero, por tanto $\Delta(\alpha_1^*, \alpha_2, \ldots, \alpha_n) \in Q^* \cap \mathbb{Z} = (p)$. Es decir, es múltiplo de p, como queríamos. □

Corolario 5.61. El número de primos que ramifican sobre un cuerpo de números O_K es finito.

Demostración. Ya sabemos que el discriminante es un entero no nulo, por tanto finitos primos lo dividen. □

De hecho, enunciamos sin demostración el recíproco del teorema anterior, que también se cumple:

Proposición 5.62. Si $p|d_K$, entonces p ramifica en O_K.

También sin demostración enunciamos el siguiente resultado de Dedekind:

Proposición 5.63. Si $K \neq \mathbb{Q}$ es un cuerpo de números sobre $\mathbb{Q}$, $|d_K| \neq 1$.

Por tanto todo cuerpo de números distinto de $\mathbb{Q}$ tendrá primos que ramifiquen.

Ejemplo 5.64. Veamos cómo descomponen los primos en las extensiones ciclotómicas.

Sea q primo y $\omega = \omega_q$ raíz q-ésima de la unidad. Sabemos que una base entera de $K = \mathbb{Q}[\omega]$ sobre $\mathbb{Q}$ viene dada por $(1, \omega, \ldots, \omega^{q-2})$, y que $d_K = (-1)^{\frac{q-1}{2}} q^{q-2}$. Como $[O_K : \mathbb{Z}[\omega]] = 1$, para usar 5.52 podremos usar siempre el polinomio mínimo de ω, $x^{q-1} + \cdots + x + 1$. Vamos a ver cómo ramifica q.

Tenemos que en $\mathbb{Z}_q$, $x^{q-1} + \cdots + x + 1 = \frac{x^q - 1}{x-1} = (x-1)^{q-1}$. Por tanto

$$qO_K = q_1^{q-1}, \text{ donde } q_1 = (q, \omega - 1).$$

Como hemos visto que la norma de $\lambda = 1 - \omega$ es q, tenemos que $q_1 = (q, 1 - \omega) = (1 - \omega)$.

Pasamos a los primos $p \neq q$. Estos primos no ramifican, ya que no dividen a d_K, por tanto descompondrán como $pO_K = P_1 \ldots P_r$, con los P_i distintos, y de forma que $rf = q - 1$, siendo f el grado de inercia común a los P_i (ya que $K/\mathbb{Q}$ es de Galois). Así que vamos a intentar averiguar quién es f. En concreto vamos a ver que f es el orden de $\overline{p} \in \mathbb{Z}_q^*$. Es decir, f será el menor natural tal que $p^f \equiv_q 1$.

Llamamos $P = P_1$, por ejemplo. Recordemos que f está definido como la dimensión sobre $\mathbb{Z}_p$ de $\frac{\mathbb{Z}[\omega]}{P}$. Por tanto, f será el número tal que $\frac{\mathbb{Z}[\omega]}{P}$ tiene p^f elementos, es decir, $\frac{\mathbb{Z}[\omega]}{P}$ será F_{p^f}. La extensión finita $\frac{\mathbb{Z}[\omega]}{P} : \mathbb{Z}_p$ es de Galois (es separable y es el cuerpo de descomposición del polinomio $x^{p^f} - x$).

Además, tenemos el Automorfismo de Frobenius (definido en la primera sección de estos apuntes),

$$\phi_p : \frac{\mathbb{Z}[\omega]}{P} \to \frac{\mathbb{Z}[\omega]}{P}; \alpha + P \mapsto \alpha^p + P.$$

Este automorfismo es generador del grupo de Galois de $\frac{\mathbb{Z}[\omega]}{P} : \mathbb{Z}_p$, por tanto su orden es el orden de la extensión, que es f. Osea que como queremos comprobar que $f = |\overline{p}|$, nos basta ver que $|\phi_p| = |\overline{p}|$.

Por otra parte, sabemos que el grupo de Galois de $\mathbb{Q}[\omega]/\mathbb{Q}$ es cíclico isomorfo a $\mathbb{Z}_q^*$. En concreto, los elementos del grupo serán aplicaciones $\sigma_a : \mathbb{Q}[\omega] \to \mathbb{Q}[\omega]$ con $\sigma_a(\omega) = \omega^a$, con $a \in \{1, \ldots, q-1\} = \mathbb{Z}_q^*$. Por tanto, como $\overline{a} \mapsto \sigma_a$ es un isomorfismo de grupos, el orden $|\sigma_p|$ en $Gal(\mathbb{Q}[\omega] : \mathbb{Q})$ será el mismo que $|\overline{p}|$ en $\mathbb{Z}_p^*$.

De modo que el resultado que buscamos se reduce a ver que $|\sigma_p| = |\phi_p|$. Para ver esto bastará comprobar que dado k entero, σ_p^k es la identidad sii ϕ_p^k es la identidad. Veámoslo:

$$\phi_p^k = 1_{\frac{\mathbb{Z}[\omega]}{P}} : \mathbb{Z}_p \iff \omega^{p^k} + P = \omega + P \iff \omega^{p^k} \equiv_P \omega$$

$$\sigma_p^k = 1_{\mathbb{Q}[\omega]} \iff \omega^{p^k} = \omega.$$

Por tanto basta ver que si $\omega^{p^k} \equiv_P \omega$, entonces $\omega^{p^k} = \omega$. Pero, si $\omega^{p^k} \equiv_P \omega$, entonces $\omega^{p^k} - \omega \in P$, y multiplicando por ω^{-1}, $\omega^{p^k - 1} - 1 \in P$. Pero, esto implica que $\omega^{p^k - 1} = 1$, ya que si no $\omega^{p^k - 1}$ sería raíz primitiva de la unidad, y vimos antes al factorizar (q) que entonces $(\omega^{p^k} - 1)$ es un divisor primo de (q). Por tanto no puede ser también un divisor primo de (p), ya que (p) y (q) son comaximales. De modo que $\omega^{p^k - 1} = 1$, por tanto $\omega^{p^k} = \omega$ y hemos acabado.

Ejemplo 5.65. Un ejemplo concreto del ejemplo anterior: $\omega = \omega_7$ raíz séptima de la unidad.

Entonces, $7O_K = 7_1^6$, con $7_1 = (\lambda) = (\omega - 1)$.

Para $p \neq 7$, tenemos $pO_K = P_1 \dots P_r$, con $6 = rf$. f será el orden de $\overline{p}$ en $\mathbb{Z}_7^*$, por tanto tenemos los casos:

- Si $p \equiv_7 1$, $f = 1$, ergo $r = 6$, y $pO_K = P_1P_2P_3P_4P_5P_6$.
- Si $p \equiv_7 6$, $f = 2, r = 3$, ergo $pO_K = P_1P_2P_3$.
- Si $p \equiv_7 2, 4$, $f = 3, r = 2$, ergo $pO_K = P_1P_2$.
- Si $p \equiv_7 3, 5$, $f = 6, r = 1$, ergo pO_K es primo.

Ejemplo 5.66. Consideramos la ecuación $x^3 = y^2 + 13$, vamos a buscar soluciones enteras. Trabajaremos en $K = \mathbb{Q}[\sqrt{-13}]$, que recordemos que tiene anillo de enteros $O_K = \mathbb{Z}[\sqrt{-13}]$, por ser $13 \equiv_4 1$, con base de enteros $(1, \sqrt{-13})$ y discriminante $-4 \cdot 13 = -52$. De modo que en el lema de Kummer, podemos usar el polinomio $x^2 - 13$ para cualquier primo.

Usando el lema con $p = 2$ no es difícil ver que $(2) = 2_1^2$, con $2_1 = (2, 1 + \sqrt{-13})^2$. Esto sirve para demostrar que $\mathbb{Z}[\sqrt{-13}]$ no es un DIP, ya que 2_1 no es un ideal principal, pues por tener $2_1^2 = (2)$ tenemos que $N(2_1)^2 = N(2)$, ergo $N(2_1) = 2$, y no hay ningún elemento de norma 2 en O_K. Como ser DIP y DFU son equivalentes en anillos de enteros, $\mathbb{Z}[\sqrt{-13}]$ no es DFU. Esto indica que no podemos resolver esta ecuación igual que resolvimos la ecuación $x^3 = y^2 + 1$ usando $\mathbb{Z}[i]$. Veamos cómo nos las apañamos.

En $\mathbb{Z}[\sqrt{-13}]$, la ecuación factoriza como $x^3 = (y + \sqrt{-13})(y - \sqrt{-13})$. Esto se puede tomar como una igualdad de ideales:

$$(x)^3 = (y + \sqrt{-13})(y - \sqrt{-13}).$$

Pero $(y + \sqrt{-13})$ y $(y - \sqrt{-13})$ son comaximales (es decir, primos entre sí), ya que si llamo I a su suma, tenemos que $2\sqrt{13} = y + \sqrt{-13} - (y - \sqrt{-13}) \in I$, por tanto $26 \in I$, $2y = (y + \sqrt{-13}) + (y - \sqrt{-13}) \in I$ y $y^2 + 13 = (y + \sqrt{-13})(y - \sqrt{-13}) \in I$. Pero y no puede ser múltiplo de 13 en la ecuación, ya que entonces x^3 sería múltiplo de 13 pero no de 13^2, y entonces, si y es par, 26 e $y^2 + 13$ son coprimos y $1 \in I$. y no puede ser par porque entonces tendríamos $x^3 \equiv_4 2$, lo cual es imposible. Por tanto $1 \in I$ y $(y + \sqrt{-13})$ y $(y - \sqrt{-13})$ son comaximales.

De modo que como $(x)^3 = (y + \sqrt{-13})(y - \sqrt{-13})$ y $(y + \sqrt{-13}), (y - \sqrt{-13})$ son coprimos, ambos son cubos. Sea J el ideal tal que $(y + \sqrt{-13}) = J^3$. En principio J no tendría por qué ser principal, pero vamos a ver que de hecho va a serlo.

En general vamos a estudiar el grupo de clases C_K. Para ello hacemos uso del oh tan poderoso teorema 5.34, que en este caso nos dice que J es equivalente a un ideal J' con

$$N(J') \leq \left(\frac{4}{\pi}\right) \frac{2}{4} \sqrt{52} = 2\frac{\sqrt{52}}{\pi} < 5.$$

Es decir, $N(J') \leq 4$. Por tanto C_K estará generado por ideales primos de normas $2, 3$ y 4. Los ideales de norma 2 dividen a (2), por tanto solo tenemos el ideal 2_1 de antes. Los ideales primos de norma 4 dividen a (4), por tanto dividen a (2), y de nuevo solo tenemos 2_1. Por último tenemos los ideales de norma 3, que dividen a (3). Como $x^2 + 13 \equiv_3 x^2 + 1$ es irreducible módulo 3, $(3) = 3_1$ es primo. Por tanto C_K está generado por 2_1 y 3_1. Como 3_1 es principal, C_K está generado por 2_1, que tiene orden 2 por ser $2_1^2 = (2)$. Por tanto C_K es un grupo de 2 elementos, que llamamos 0 y 1, como en $\mathbb{Z}[2]$.

Por tanto como J^3 es principal, la clase de J en C_K tendrá que ser 0, ya que si fuera 1, la clase de J^3 sería $3 \cdot 1 = 1$. Por tanto J es principal.

De modo que tendrá que haber $a, b \in \mathbb{Z}$ tales que $(a + b\sqrt{-13})^3 = \pm(y + \sqrt{-13})$. Podemos quitar el $\pm$ ya que -1 es un cubo. Desarrollando,

$$y + \sqrt{-13} = (a^3 - 39ab^2) + \sqrt{-13}(3a^2b - 13b^3)$$

Por tanto $3a^2b - 13b^3 = 1$, ergo $b = \pm 1$. Si $b = 1$, $3a^2 - 13 = 1$, no hay solución. Si $b = -1$, $-3a^2 + 13 = 1$, hay solución $a = \pm 2$. De modo que nuestros posibles valores de y son $a^3 - 39ab^2 = a(a^2 - 39b^2) = \pm 2(-35) = \pm 70$, con $x = 17$.

Problemitas. 1. Ver que O_K es $DFU \Leftrightarrow DIP$.
2. $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$ sin cuadrados. Ver que son equivalentes:

- $d = 1, 2, 3, 7, 11$.
- O_K es norma euclídea, es decir, el módulo al cuadrado es norma euclídea.
- O_K es euclídeo.

3. Probar que si $d = 19, 43, 67, 163$, entonces O_K es DIP.
4. Hallar soluciones enteras de $x^3 = y^2 + 41$.
5. Sea $F = \mathbb{Q}[\sqrt{-14}]$, $K = F[\sqrt{-7}]$. Entonces, O_K no es O_F-módulo libre (esto no pasa en cuerpos de números sobre $\mathbb{Q}$!).
6.Sea $K_i = \mathbb{Q}[\alpha_i], i = 1, 2, 3$, con:

$$\begin{array}{rcl} \min_{\mathbb{Q}}(\alpha_1) & = & x^3 - 18x - 6 \\ \min_{\mathbb{Q}}(\alpha_1) & = & x^3 - 36x - 78 \\ \min_{\mathbb{Q}}(\alpha_1) & = & x^3 - 54x - 150 \end{array}$$

Comprobar que los K_i son irreducibles, que $d_1 = d_2 = d_3$, con $d_i = d_{K_i}$ y que K_1, K_2, K_3 son no isomorfos dos a dos. Es decir, las extensiones tienen el mismo discriminante pero no son isomorfas.

7. Sea $\alpha = \sqrt[3]{6}$ real, y sea $K = \mathbb{Q}[\alpha]$.

1. Probar que $\{1, \alpha, \alpha^2\}$ es base entera de O_K.
2. $h_K = 1$.
3. Descomponer (?) pO_K con $p \geq 2$, obteniendo generadores de los ideales en $p = 2, 3, 5$.
4. Probar que $U_K = \{\pm(1 - 6\alpha + 3\alpha^2); i \in \mathbb{Z}\}$.
5. Probar que $\forall x, y, z$, $x^3 + 6y^3 = 10z^3 \implies x, y, z = 0$.
6. *(Selmer)* Probar que $3x^3 + 4y^3 + 5z^3 = 0$ no tiene soluciones no triviales enteras. (Ver explicación, tiene que ver con curvas planas y cosas. No se puede definir una adición por no tener puntos racionales, o algo así)[3].

8. Probar que $x^3 + 22y^3 + 3z^3 = 0$ tiene soluciones mód m $\forall m$ (nah eso no hace falta xdd) pero no tiene soluciones enteras no $(0, 0, 0)$ (esa parte sí). Trabajar en $\mathbb{Q}[\sqrt[3]{22}]$ o $\mathbb{Q}[\sqrt[3]{3}]$. (spoiler: es $\mathbb{Q}[\sqrt[3]{22}]$)

9.

1. Encontrar los m que se pueden escribir de forma $m = x^2 - xy + y^2$. Y el número de representaciones de cada m.
2. Encontrar los m que se pueden escribir de forma $m = a^3 + 2b^3 + 4c^3 - 6abc$ y obtener todas las representaciones de $m = 50$. (spoiler: hay infinitas).

10. *(Euler)* $p \in \mathbb{Z}$. Ver que son equivalentes:

1. $n^2 + n + p$ es primo si $0 \leq n \leq p - 2$.
2. $O_{\mathbb{Q}(\sqrt{1-4p})}$ es un DIP. (caso 41! jaja, el mítico)

11. (sencillo) Si q es primo, entonces $mq+1$ es primo para infinitos valores de m. (Usar cuerpos ciclotómicos)

12. (Samuel pg 102 creo) Sea $\alpha \in \mathbb{R}$ con $\min_{\mathbb{Q}}(\alpha) = x^3 - x + 1$. Sea $K = \mathbb{Q}[\alpha]$. Sea F el cuerpo de descomposición de $x^3 - x + 1$ sobre $\mathbb{Q}$.$\mathbb{Q} \subsetneq K \subsetneq F$.

1. Comprobar que $\mathbb{Q}[\sqrt{-23}] \subseteq F$.

[3]En los apuntes de Arrondo de curvas se habla muy por encima del asunto, definen el grupo y tal.

2. Obtener todos los cuerpos intermedios. (T^a fundamental Galois).
3. $h_K = 1$.
4. Descomponer $2O_F$ en F y comprobar que 2 es el único primo ramificado en F.
5. Comprobar que la extensión $[F/\mathbb{Q}[\sqrt{-23}]]$ no es ramificada. Ningún primo de $O_{\mathbb{Q}[\sqrt{-23}]}$ ramifica en F. Ver explicación. El ideal del discriminante es todo O_K (esto no pasa en $\mathbb{Q}$).
6. Ahora repite lo mismo con el polinomio $x^3 + x + 1$.

Capítulo 6

Grupos de unidades en cuerpos de números

6.1 Grupos de unidades

Vamos a estudiar grupos de unidades en cuerpos de números. En los casos $\mathbb{Z}[\sqrt{-d}]$ que hemos visto, estos grupos de unidades eran finitos, sin embargo en general la situación va a ser complicada: de hecho este caso que hemos mencionado es el único en que el grupo es finito. Pero primero recordamos un par de teoremas sobre grupos abelianos.

Teorema 6.1. Sea F grupo abeliano libre de rango n, sea G subgrupo no trivial de F, entonces existen $x_1, \ldots, x_n$ base de F y $0 < d_1|d_2| \ldots d_{r-1}|d_r$ enteros tales que $\{d_1x_1, \ldots, d_rx_r\}$ es base de G.

Demostración. Inducción sobre n. El caso $n = 1$ es directo: tenemos F generado por cierto x_1, y entonces G subgrupo de F estará generado por d_1x_1, para cierto d_1 entero.

Ahora supongamos que el teorema se cumple en los grupos abelianos libres de rango $< n$, y sea F libre y una base suya cualquiera $(y_1, \ldots, y_n)$. Considero también las combinaciones enteras de la base que están en G, $\sum_{i=1}^n a_iy_i \in G$, con $a_i \in \mathbb{Z}$.

Ahora, defino d_1 como el menor coeficiente (en valor absoluto) no nulo que aparece en alguna expresión $\sum_{i=1}^n a_iy_i \in G$, con y_i alguna base de F y $a_i \in \mathbb{Z}$. Podemos expresar entonces $0 \neq d_1y_1 + a_2y_2 + \cdots + a_ny_n \in G$. Ahora expresamos $a_i = q_id_1 + r_i$, con $q_i, r_i \in \mathbb{Z}, 0 \leq r_i < d_1$. Entonces tenemos

$$0 \neq d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n \in G.$$

Pero, llamando $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$, está claro que $(x_1, y_2, \ldots, y_n)$ es una base de F, ya que y_j es combinación entera de ellos para todo j, y es directo comprobar que cualquier combinación entera de ellos es 0 sii los coeficientes son todos 0.

Pero entonces, al ser $x_1, y_2 \ldots, y_n$ base de F y $r_i < d_1$ para todo i, tenemos por definición de d_1 que $r_i = 0 \forall i$, es decir,

$$0 \neq d_1(y_1 + q_2y_2 + \cdots + q_ny_n) \in G.$$

Ahora, como $x_1, y_2, \ldots, y_n$ es base de F, tenemos que $F =< x_1 > \oplus H$, con $H =< y_2, \ldots, y_n >$. Aquí, H es libre generado por $n-1$ elementos, por tanto, como $G \cap H$ es un subgrupo de H, o bien $G \cap H$ es trivial, en cuyo caso está claro que el enunciado se cumple ya que $G =< d_1x_1 >$, o bien por hipótesis de inducción hay una base $x_2, \ldots, x_n$ de H y enteros $d_2, \ldots, d_r$ tales que $d_2x_2, \ldots, d_rx_r$ es base de $G \cap H$ y $0 < d_2|d_3| \ldots d_{r-1}|d_r$. Para obtener el enunciado empezaremos comprobando que $G =< d_1x_1 > \oplus (G \cap H)$, ya que en ese caso $d_1x_1, d_2x_2, \ldots, d_rx_r$ serán base de G, y después veremos que $d_1|d_2$ para concluir.

Vamos a probar entonces que $G =< d_1x_1 > \oplus (G \cap H)$. Sea un elemento de G,

$$v = a_1x_1 + a_2y_2 + \cdots + a_ny_n, \text{ con } a_1 = qd_1 + r, \, q, r \text{ enteros con } 0 \leq r < d_1.$$

Entonces $v - q(d_1x_1) = r_1x_1 + a_2y_2 + \cdots + a_ny_n$, y como $v - q(d_1x_1)$ está en G tenemos por definición de d_1 que $r_1 = 0$. Por tanto v se puede expresar como

$$v = q(d_1x_1) + (a_2y_2 + \cdots + a_ny_n),$$

es decir, un elemento de $< d_1x_1 >$ más otro de $G \cap H$. Obviamente esta forma de expresarlo es única, ya que $< d_1x_1 > \cap (G \cap H) = \{0\}$. Por tanto efectivamente $G =< d_1x_1 > \oplus (G \cap H)$.

Solo nos queda comprobar que $d_1|d_2$. Pero $d_1x_1, d_2x_2, \ldots, d_rx_r$ son base de G, con $x_1, x_2, \ldots, x_n$ base de F. Escribiendo $d_2 = qd_1 + r$ (división euclídea), tenemos que $d_1x_1 + d_2x_2 = d_1(x_1 + qx_2) + rx_2$ es un elemento de G, y además es fácil comprobar que $x_1 + qx_2, x_2, \ldots, x_n$ es base de F, por tanto por definición de d_1 tenemos que $r = 0$, es decir, d_2 es múltiplo de d_1. □

Recordemos que todo grupo abeliano finitamente generado es un cociente de un grupo libre finitamente generado: en efecto, dado G generado por unos elementos $g_1, \ldots, g_m$, podemos definir el homomorfismo sobreyectivo

$$\begin{array}{rccl} \phi: & \mathbb{Z}^m & \to & G; \\ & (x_1, \ldots, x_m) & \to & x_1g_1 + \cdots + x_ng_n \end{array}$$

y, por el primer teorema de isomorfía, tendremos que $G \simeq \frac{\mathbb{Z}^m}{\ker \phi}$.

Ahora bien, $K := \ker \phi$ es un subgrupo de un grupo abeliano libre generado por m elementos. Si K es trivial, entonces $G \simeq \mathbb{Z}^m$ es libre. Si no, por el teorema anterior, tenemos una base $x_1, \ldots, x_m$ de $\mathbb{Z}^m$ y enteros $0 < d_1| \ldots |d_r$ tales que K está generado por $d_1x_1, \ldots, d_rx_r$. De modo que tendremos que

$$G \simeq \frac{\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_m}{d_1\mathbb{Z}x_1 \oplus \cdots \oplus d_r\mathbb{Z}x_r \oplus \{0\} \oplus \cdots \oplus \{0\}} \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

Acabamos de deducir el teorema de clasificación de grupos abelianos finitamente generados:

Teorema 6.2. Sea A grupo abeliano finitamente generado, entonces existen enteros $0 < d_1| \ldots |d_r$ y m de forma que $A \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^m$. □

Llamamos subgrupo de torsión de A, $t(A)$, a su conjunto de elementos de orden finito (elementos de torsión), es decir, en el teorema de arriba sería el subgrupo de A correspondiente a $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \{0\}$.

Vamos, ahora sí, a centrarnos en los grupos de unidades.

Definición 6.3. Dado K cuerpo de números, llamamos U_K a $O_K^\times$, es decir, el grupo de unidades de O_K.

El próximo objetivo será estudiar U_K y su subgrupo de torsión. El resultado importante que vamos a probar durante las próximas secciones es este:

Teorema 6.4. Dado K cuerpo de números, U_K es finitamente generado. $t(U_K)$ será un grupo cíclico finito generado por una raíz de la unidad ω, y tendremos que

$$U_K \simeq < \omega > \oplus \mathbb{Z}^{r_1+r_2-1} =< \omega > \oplus \mathbb{Z}^r,$$

donde r_1 es el número de inmersiones f de K en $\mathbb{C}$ con $f(K) \subseteq \mathbb{R}$, y $2r_2$ es el número de inmersiones g de K en $\mathbb{C}$ con $g(K) \not\subseteq \mathbb{R}$.

Por el modo en que hemos definido r_1 y r_2, si llamamos n al orden de K sobre $\mathbb{Q}$ entonces $n = r_1 + 2r_2$, ya que el número de inmersiones de K en $\mathbb{C}$ es el grado de la extensión $K/\mathbb{Q}$. r_1 se puede ver como el número de raíces reales de $\min_{\mathbb{Q}}(\alpha)$, donde α es un complejo con $K = \mathbb{Q}[\alpha]$, y r_2 será la mitad del número de raíces no reales de $\min_{\mathbb{Q}}(\alpha)$.

Ejemplo 6.5. Veamos el caso de cuerpos cuadráticos $K = \mathbb{Q}[\sqrt{d}]$, con d entero libre de cuadrados.

Si $d < 0$ tenemos que $r_1 = 0$ y $r_2 = 1$ (ya que las inmersiones de K en $\mathbb{C}$ son la identidad y la conjugación), por tanto $r = r_1 + r_2 - 1 = 1$ y $U_K = (\omega)$, con ω una raíz de la unidad. Los elementos de U_K serán los elementos de norma 1, es decir, de la forma $a + b\sqrt{-d}$, con $a^2 - db^2 = 1$. Usando ahora 4.11, no es difícil comprobar que si

$d = -1$ ($\mathbb{Z}[i]$) hay 4 unidades, si $d = -3$ ($\mathbb{Z}[\omega]$) hay 6 unidades, y en el resto de casos hay solo 2 unidades, 1 y -1.

De hecho estos cuerpos $\mathbb{Q}[\sqrt{d}]$ con $d < 0$ son los únicos con grupo de unidades finito: Si $r = r_1 + r_2 - 1 = 0$, entonces $r_1 + r_2 = 1$. Si $r_1 = 1$, entonces el grado de la extensión será $n = r_1 + 2r_2 = 1$, o sea que no hay extensiones no triviales que lo cumplan. Si por el contrario $r_2 = 1$, $n = r_1 + 2r_2 = 2$, y tenemos extensiones cuadráticas, es decir, de la forma $\mathbb{Q}[\sqrt{d}]$ con d libre de cuadrados. Además d tendrá que ser negativo porque las extensiones no pueden estar contenidas en $\mathbb{R}$ al ser $r_1 = 0$.

Pasamos a ver el caso $d > 0$. En este caso $r_1 = 2$ y $r_2 = 0$, ya que habrá dos inmersiones reales (que mandarán $\sqrt{d}$ a $\sqrt{d}$ y $-\sqrt{d}$ respectivamente). Por tanto $r = 1$. Además todas las raíces de la unidad en esta extensión son 1 y -1, ya que son reales. Por tanto el teorema nos dice que todas las raíces serán expresables como $\pm u^k$, para cierta unidad u y k entero.

Empezamos por el caso $d \equiv_4 1$. En este caso, $(1, \sqrt{d})$ es una base entera. Las unidades serán los elementos de norma 1, es decir, $a + b\sqrt{d}$ con

$$a^2 - db^2 = \pm 1 \qquad \textit{(Ecuaciones de Pell)}$$

De modo que U_K nos dará las soluciones a las ecuaciones de Pell. Llamamos a u, la unidad tal que $U_K = \{\pm u^k; k \in \mathbb{Z}\}$, la **unidad fundamental.** Entonces, si $N(u) = 1$, entonces $N(\pm u^k) = N(\pm 1)N(u^k) = 1N(u)^k = 1$. Es decir, todas las unidades tienen norma 1. Esto quiere decir que la ecuación de Pell $a^2 - db^2 = -1$ no va a tener soluciones, ya que esas soluciones corresponderían a elementos de norma -1. Si, por el contrario, la ecuación de Pell con -1 tiene solución, entonces u tendrá norma -1.

Se puede comprobar que si la ecuación de Pell con -1 tiene solución, entonces una unidad fundamental vendrá dada por la menor solución (a, b) de la ecuación de Pell $a^2 - db^2 = -1$, en el sentido de que a sea lo menor posible en valor absoluto. De forma similar, si no hay solución a $a^2 - db^2 = -1$ entonces una unidad fundamental vendrá dada por la menor solución a $a^2 - db^2 = 1$.

Ejemplo 6.6. Si tenemos una extensión cúbica $\mathbb{Q}[\alpha]$ se nos presentan 2 casos:

- Si $\min_{\mathbb{Q}}(\alpha)$ tiene una raíz real, entonces $r_1 = 1, r_2 = 1$, por tanto $r = 1$. Por tanto las unidades serán de forma $\omega^k \omega_1^{k_1}$, donde ω es una raíz m-ésima de la unidad para cierto m (así que podemos tomar k entre 0 y $m - 1$) y ω_1 es otra unidad. De hecho ω solo podrá ser 1 o -1: esto es obvio si $\alpha \in \mathbb{R}$, ya que entonces ω será una raíz real de la unidad, y si $\alpha \notin \mathbb{R}$ entonces $\mathbb{Q}[\alpha] \sim \mathbb{Q}[\alpha']$ donde α' es la raíz real de $\min_{\mathbb{Q}}(\alpha)$, por tanto las raíces de unidad que haya en $\mathbb{Q}[\alpha]$ tendrán el mismo orden que las que haya en $\mathbb{Q}[\alpha']$, es decir, también serán 1 o -1.
- Si $\min_{\mathbb{Q}}(\alpha)$ tiene tres raíces reales, entonces $r_1 = 3, r_2 = 0$, por tanto $r = 2$. De modo que en este caso podremos encontrar raíces ω_1, ω_2 de forma que cualquier raíz se pueda expresar de forma $\omega^k \omega_1^{k_1} \omega_2^{k_2}$, con k, k_1, k_2 enteros y $\omega^m = 1$ para cierto $m > 0$. En este caso como ω es una raíz de la unidad real solo puede ser ± 1, o sea que las unidades serán de forma $\pm \omega_1^{k_1} \omega_2^{k_2}$.

6.2 Retículos

El primer paso para demostrar 6.4 será estudiar algunos subgrupos aditivos de $\mathbb{R}^n$. El próximo desarrollo está basado en el capítulo 4 de [5].

Definición 6.7. Decimos que un subgrupo H de R^n es discreto si para cualquier $K \subseteq \mathbb{R}^n$ compacto, $H \cap K$ es finito.

Decimos que un subgrupo H de R^n es un retículo si está generado libremente por r elementos linealmente independientes sobre $\mathbb{R}$, con $r \leq n$.

Proposición 6.8. Todo retículo es discreto.

Demostración. Supongamos que un retículo H está generado por $e_1, \ldots, e_r$ linealmente independientes. Sea $d_i > 0$ la distancia desde e_i al subespacio generado por los e_j con $j \neq i$.

Ahora supongamos que tenemos $K \subseteq \mathbb{R}^n$ compacto, y sea n tal que $K \subseteq B(0,n)$. Ahora, si tenemos que un elemento $x = \sum k_i e_i \in K$, con $k_i \in \mathbb{Z}$, entonces $|x| < n$, por tanto para cada i $|k_i e_i + \sum_{j \neq i} k_j e_j| < n$. Es decir, $d(-k_i e_i, \sum_{j \neq i} k_j e_j) < n$. Pero la distancia desde $-k_i e_i$ al subespacio generado por los e_j es $|k_i| d_i$, por tanto tenemos que $|k_i| < \frac{n}{d_i}$.

De modo que los elementos de H en K serán todos de forma $\sum k_i e_i$, con $|k_i| < \frac{n}{d_i}$. Es decir, solo hay finitos elementos de H en K, como queríamos. □

La implicación recíproca también es cierta, pero nos va a costar más probarla.

Proposición 6.9. Todo subgrupo discreto de $\mathbb{R}^n$ es un retículo.

Demostración. Sea $H \subseteq \mathbb{R}^n$ subgrupo discreto. Sea r el máximo número de vectores linealmente independientes que podemos encontrar en H ($r \leq n$), y sean $\{e_1, \ldots, e_r\}$ en H linealmente independientes. Sea

$$P = \left\{ \sum_{i=1}^{r} k_i e_i ; 0 \leq k_i \leq 1 \right\}.$$

P es compacto (por ser la imagen del compacto $[0,1]^r$ bajo la aplicación contínua $(k_1, \ldots, k_r) \mapsto \sum k_i e_i$. Por tanto por ser H discreto, $P \cap H$ es finito.

Ahora, dado x cualquiera de H, por maximalidad de r tenemos que x será una combinación lineal de $e_1, \ldots, e_r$, $x = \sum k_i e_i$. De hecho vamos a ver que estos k_i son racionales. Recordemos que dado $k \in \mathbb{R}$, $\lfloor k \rfloor$ es la parte entera de k, y llamamos $\{k\} \in [0,1]$ a $k - \lfloor k \rfloor$. Entonces, si llamamos x_j a $jx \in H$ para cada x, tenemos que:

$$x_j = \sum j k_i e_i = \sum \lfloor j k_i \rfloor e_i + \sum \{j k_i\} e_i.$$

El primero de los sumandos, $\sum \lfloor j k_i \rfloor e_i$, está en H, y el segundo, $\sum \{j k_i\} e_i$, está en P. También está en H por estar x_j y $\sum \lfloor j k_i \rfloor e_i$ en H.

Por tanto para todo j, $\sum \{j k_i\} e_i$ está en $P \cap H$. Como $P \cap H$ es finito, tendrá que haber dos enteros $j_1 \neq j_2$ con $\sum \{j_1 k_i\} e_i = \sum \{j_2 k_i\} e_i$. Es decir, $x_{j_1} - \sum \lfloor j_1 k_i \rfloor e_i = x_{j_2} - \sum \lfloor j_2 k_i \rfloor e_i$. Es decir, $\sum (j_2 - j_1) k_i e_i = \sum (\lfloor j_1 k_i \rfloor - \lfloor j_2 k_i \rfloor) e_i$. Por tanto para cada i tenemos que $(j_2 - j_1) k_i = \lfloor j_1 k_i \rfloor - \lfloor j_2 k_i \rfloor$. Es decir,

$$k_i = \frac{\lfloor j_1 k_i \rfloor - \lfloor j_2 k_i \rfloor}{j_2 - j_1}.$$

Por tanto k_i son números racionales, ya que numerador y denominador de la anterior expresión son enteros.

De modo que hemos visto que: Todo elemento $x \in H$ es suma de una combinación entera de los e_i y un elemento v de $P \cap H$ de forma $v = \sum \{k_i\} e_i$, con $\{k_i\}$ racionales.

Llamando $v_j = \sum \{k_{i,j}\} e_i$ a esos finitos elementos de $P \cap H$, podemos tomar d denominador común de todos los $\{k_{i,j}\}$, de modo que $d k_{i,j}$ es entero para todos i, j. Por tanto $d v_j \in H_1$, donde H_1 es el subgrupo (libre) de H generado por $e_1, \ldots, e_r$. Por tanto todo $x \in H$ es suma de un elemento de H_1 y un $v_j \in \frac{H_1}{d}$. Por tanto $H \subseteq \frac{H_1}{d}$.

Ahora bien, $\frac{H_1}{d}$ es un grupo isomorfo a H_1 (el isomorfismo es $x \mapsto dx$), por tanto tenemos que como H es un subgrupo de $\frac{H_1}{d}$, por 6.1 H es libre de rango $\leq r$, al ser r el rango de $\frac{H_1}{d}$.

Además, como H_1 es subgrupo de H y H_1 es libre de rango r, H no puede ser libre de rango $< r$. Por tanto H es libre de rango exactamente r.

Ahora, sea $x_1, \ldots, x_r$ una base de H. Entonces H está contenido en el subespacio lineal de $\mathbb{R}^n$ generado por $x_1, \ldots, x_r$, que llamaremos W. Por tanto $e_1, \ldots, e_r$, que eran linealmente independientes, están todos en W, así que W tiene dimensión $\geq r$. Esto implica que $x_1, \ldots, x_r$ son linealmente independientes, y hemos acabado ya que $x_1, \ldots, x_r$ cumplen la definición de que H es un retículo. □

Definiciones 6.10. Decimos que un retículo $H \subseteq \mathbb{R}^n$ es completo si está generado por n vectores linealmente independientes.

Dada una base $e = (e_1, \ldots, e_n)$ de $\mathbb{R}^n$, definimos

$$P_e = \left\{ \sum_{i=1}^{n} \lambda_i e_i ; 0 \leq \lambda_i < 1 \right\}$$

Si H es el retículo generado por una base e de $\mathbb{R}^n$, decimos que P_e es la región fundamental de H.

Dada una base e de $\mathbb{R}^n$ que genera un retículo H, todo elemento $x \in \mathbb{R}^n$ podrá expresarse como $\sum_{i=1}^n k_i e_i = (\sum_{i=1}^n \lfloor k_i \rfloor e_i) + (\sum_{i=1}^n \{k_i\} e_i)$, es decir, un elemento de H más un elemento de P_e. Esto nos lleva a la siguiente proposición:

Proposición 6.11.

$$\mathbb{R}^n = \bigcup_{h \in H} (h + P_e),$$

donde la anterior unión es disjunta.

Demostración. La discusión anterior muestra que la unión es $\mathbb{R}^n$. Además si la unión no fuera disjunta, habría elementos de H $h_1 \neq h_2$ con $(h_1 + P_e) \cap (h_2 + P_e) \neq \varnothing$. De modo que habría $p_1, p_2 \in P$ con $h_2 - h_1 = p_1 - p_2$, de modo que $h_2 - h_1 \in H \cap P_e$. Pero es fácil ver que $H \cap P_e = \{0\}$, así que $h_1 = h_2$ y $p_1 = p_2$. □

Es decir, los $h + P_e$ serán 'paralelepípedos' que formen una partición de $\mathbb{R}^n$.

Definición 6.12. Sea e una base que genera un retículo H, definimos el volumen de H, $\mathrm{vol}(H)$, como $\mu(P_e)$, siendo μ la medida Lebesgue en $\mathbb{R}^n$.

Para comprobar que este volumen está bien definido deducimos a continuación la proposición 6.14.

Proposición 6.13. Dada una base e de $\mathbb{R}^n$,

$$\mu(P_e) = |\det(M)|,$$

donde M es la matriz de columnas $e_1, \ldots, e_n$.

Demostración. P_e es la imagen del cubo $[0,1)^n$ por la aplicación $f : \mathbb{R}^n \to \mathbb{R}^n; (k_1, \ldots, k_n) \to \sum k_i e_i$. Esta aplicación tiene derivada M en todo punto, por tanto el teorema de cambio de variables:

$$\mu(P_e) = \int_{P_e} 1 d\mu = \int_{[0,1)^n} |\det(M)| d\mu = \mu([0,1)^n) |\det(M)| = |\det(M)|.$$

□

Proposición 6.14. Si e_1 y e_2 generan el mismo retículo H entonces $\mu(P_{e_1}) = \mu(P_{e_2})$.

Demostración. Sea $M_{1,2}$ la matriz de cambio de base de e_1 a e_2. Como los vectores de e_2 son elementos de H, son combinaciones enteras de elementos de los vectores de e_1, por tanto $M_{1,2}$ tiene entradas enteras. Por tanto el determinante de $M_{1,2}$ es entero. Por la misma razón, si $M_{2,1}$ es la matriz de cambio de e_2 a e_1, el determinante de $M_{2,1}$ es entero. Además, $M_{1,2}M_{2,1}$ es la identidad por cómo están definidas, por tanto $\det(M_1)\det(M_2) = 1$. Por tanto $\det(M_1)$ y $\det(M_2)$ tendrán que ser ± 1, y por la proposición anterior hemos acabado. □

Proposición 6.15. Sea H un retículo de R^n, y sea $S \subseteq \mathbb{R}^n$ medible con $\mu(S) > \mathrm{vol}(H)$. Entonces hay elementos $s_1 \neq s_2$ de S con $s_1 - s_2 \in H$.

Demostración. Sea e base de H y supongamos que el enunciado no es cierto. Entonces los conjuntos $A_h := ((h + P_e) \cap S) - h$, con $h \in H$, serían disjuntos dos a dos, ya que si no habría h_1, h_2 tales que $((h_1 + P_e) \cap S) - h_1$ y $((h_2 + P_e) \cap S) - h_2$ intersecan, por tanto $h_1 - h_2$ estaría en $((h_1 + P_e) \cap S) - ((h_2 + P_e) \cap S)$, es decir, habría $p_1, p_2 \in P_e$ con $h_1 + p_1, h_2 + p_2 \in S$ y $h_1 - h_2 = h_1 + p_1 - h_2 - p_2$, es decir, $h_1 + p_1$ y $h_2 + p_2$ serían elementos de S con diferencia en H.

Pero ahora, si los conjuntos A_h son disjuntos, usando 6.11 y que H es numerable llegamos al siguiente absurdo:

$$\mu(S) = \mu\left(\bigcup_{h \in H} S \cap (h + P_e) \cap S\right) = \sum_{h \in H} \mu((h + P_e) \cap S) = \sum_{h \in H} \mu(A_h) = \mu\left(\bigcup_{h \in H} A_h\right) \leq \mu(P_e) = \mathrm{vol}(H),$$

donde en la penúltima igualdad hemos usado que la unión de los A_h está contenida en P_e. □

Corolario 6.16. Minkowski
Sea H retículo, sea $S \subseteq \mathbb{R}^n$ medible convexo y con $S = -S$, es decir, $x \in S \implies -x \in S$.
Entonces, si $\mu(S) > 2^n \text{vol}(H)$, $S \cap H \neq \{0\}$.

Demostración. Consideramos el conjunto $\frac{S}{2}$, que tiene medida $> \text{vol}(H)$. Por tanto hay $s_1 \neq s_2 \in \frac{S}{2}$ con $s_1 - s_2 \in H$. Pero como $s_1, s_2 \in \frac{S}{2}$, $2s_1, 2s_2 \in S$, ergo $-2s_2 \in S$ por ser $-S = S$, ergo $\frac{1}{2}(2s_1 - 2s_2) = s_1 - s_2$ estará en S por ser S convexo. O sea que tenemos $s_1 - s_2 \neq 0$ en $S \cap H$. □

6.3 Primos como sumas de cuadrados

En esta sección vemos formas de usar los retículos para expresar enteros como sumas de cuadrados. Vamos a seguir [6] para este tema, aunque un libro más sencillo de seguir es [7]

El procedimiento clásico para ver que si un primo $p \equiv 1 \pmod 4$ entonces se puede expresar como $p = a^2 + b^2,\ a, b \in \mathbb{Z}$ es el siguiente:

- En primer lugar, el grupo multiplicativo $\mathbb{F}_p^\times$ es cíclico y su orden es divisible por 4 luego $\exists u \in \mathbb{F}_p :\ u^2 = -1 \in \mathbb{F}_p$.
- Esto quiere decir que $\exists u, m \in Z :\ u^2 + 1 = mp,\ m \geq 1$.
- Si $m = 1$ hemos acabado, si $m > 1$ buscamos $v, w, m' \in \mathbb{Z} :\ v^2 + w^2 = m'p,\ 1 \leq m' < m$.

La parte final, el argumento de descenso, requiere algo de tiempo. Veamos cómo la teoría que hemos desarrollado de retículos nos ayuda a evitar el argumento de descenso.
Consideramos $H := \{(a, b) \in \mathbb{Z}^2 :\ b \equiv ua \pmod p\}$ donde $u^2 \equiv -1 \pmod p$.
H es un retículo de $\mathbb{R}^2$ pues sus elementos se escriben de la forma

$$(a, b) = (a, ua + mp) = a(1, u) + m(0, p),$$

pues está claro que $(1, u)$ y $(0, p)$ son linealmente independientes.

$$\text{vol}(H) = \begin{vmatrix} 1 & 0 \\ u & p \end{vmatrix} = p.$$

Tomamos la bola $\overline{B}(0, r)$ con $r > 0$ lo suficientemente grande como para que

$$\mu(\overline{B}(0, r)) = \pi r^2 > 2^2 \,\text{vol}(H) = 4p.$$

Por ejemplo tomamos $r > 0 :\ r^2 = \frac{3}{2}p$. Comprobamos que funciona:

$$\pi \frac{3}{2} p > 4p \Leftrightarrow\ 3\pi > 8.$$

Entonces por el último corolario sabemos que existe $0 \neq (a, b) \in B(0, r) \cap H$. Luego

$$0 \neq a^2 + b^2 \equiv_p a^2 + u^2 a^2 \equiv_p a^2 - a^2 = 0.$$

Por tanto $a^2 + b^2 = mp$ con $m \geq 1$. Sin embargo, $r^2 = \frac{3}{2}p$ y $a^2 + b^2 \leq r^2$ luego

$$mp = a^2 + b^2 \leq \frac{3}{2} p \Rightarrow\ m \leq \frac{3}{2} \Rightarrow\ m = 1.$$

Así que $a^2 + b^2 = p$ para ciertos $a, b \in \mathbb{Z}$.

Obsérvese que dados dos números representables como suma suma de dos cuadrados, su producto también lo será. Sean $x, y \in \mathbb{Z}$ tales que existan $a, b, c, d :\quad x = a^2 + b^2,\ y = c^2 + d^2$. Entonces $x = (a + bi)(a - bi) = N(a + bi),\ y = N(c + di)$ luego

$$xy = N(a + bi)N(c + di) = N((a + bi)(c + di)).$$

Esto último es una suma de cuadrados.
También podemos preguntarnos, para cada n entero, cuántas formas hay de expresar n como suma de dos cuadrados. Esto es sencillo usando lo que conocemos de $\mathbb{Z}[i]$: factorizando n en $\mathbb{Z}[i]$,

$$n = \varepsilon(1+i)^{\gamma}\pi_1^{\gamma_1}\overline{\pi_1}^{\gamma_1}\dots\pi_k^{\gamma_k}\overline{\pi_k}^{\gamma_k}q_1^{\tau_1}\dots q_m^{\tau_m},$$

donde ε es una unidad, los q_i son primos enteros que son $\equiv_4 3$, y $\pi_i\overline{\pi_i}$ son primos enteros $\equiv_4 1$. Entonces, si n es expresable como suma de cuadrados, $n = a^2+b^2 = (a+bi)(a-bi)$, entonces los factores primos de n se repartirán entre $a+bi$ y $a-bi$. Vamos a ver cuántos posibles números $a+bi$ hay de esta forma, es decir, cuántos pares (a,b) hay con $a^2+b^2 = n$.

Si factorizamos $a+bi$, tendrá que ser de la forma

$$a+bi = \varepsilon'(1+i)^{\alpha}\pi_1^{\alpha_1}\overline{\pi_1}^{\alpha_1'}\dots\pi_k^{\alpha_k}\overline{\pi_k}^{\alpha_k'}q_1^{\beta_1}\dots q_m^{\beta_m}.$$

Pero entonces, $n = (a+bi)(a-bi)$ será (usando que $a-bi$ es $a+bi$ conjugado)

$$n = (-i)^{\alpha}(1+i)^{2\alpha}\pi_1^{\alpha_1+\alpha_1'}\overline{\pi_1}^{\alpha_1+\alpha_1'}\dots\pi_k^{\alpha_k+\alpha_k'}\overline{\pi_k}^{\alpha_k+\alpha_k'}q_1^{2\beta_1}\dots q_m^{2\beta_m}$$

Por tanto, ya sabemos que $\alpha = \frac{\gamma}{2}$, $\beta_k = \frac{\tau_k}{2}$. ε se puede elegir como queramos, ya que al multiplicar teníamos que $\varepsilon\overline{\varepsilon} = 1$ o sea que no importa. De modo que hay 4 formas de cogerlo. Por último, tenemos que $\alpha_i+\alpha_i' = \gamma_i$, por tanto α_i puede tomar cualquier valor entre 0 y γ_i, es decir, un total de γ_i+1 valores. Por tanto hay un total de $4\prod_{i=1}^{k}(\gamma_i+1)$ posibles $a+bi$, y por tanto hay ese número de (a,b) tales que $a^2+b^2 = n$.

Los primos suma de 3 cuadrados están caracterizados. No obstante el producto de dos números de este estilo no es necesariamente suma de tres cuadrados. Saber el número de representaciones es todavía peor.

Teorema 6.17. Sea $n \in \mathbb{N}$, entonces existen enteros $a,b,c,d \in \mathbb{Z}$ tales que:

$$n = a^2+b^2+c^2+d^2.$$

Demostración. Comencemos con $n = p$ primo, en particular con $n = 2$. En este caso $2 = 1^2+1^2+0^2+0^2$.
Si $n = p > 2$ veamos qué sucede. En primer lugar veamos que existen $u,v \in \mathbb{Z}$:

$$-1 \equiv_p u^2+v^2.$$

En $\mathbb{F}_p$ hay $\frac{p-1}{2}+1$ cuadrados perfectos luego, si consideramos la igualdad siguiente con u,v arbitrarios:

$$-1-u^2 \equiv_p v^2.$$

Al ir cambiando u,v en ambos miembros de la igualdad se tienen $\frac{p-1}{2}+1$ elementos distintos luego tiene que haber u,v tales que las expresiones de ambos lados coincidan (si no tendríamos $(\frac{p-1}{2}+1)+(\frac{p-1}{2}+1) > p$ elementos distintos en $\mathbb{F}_p$).

Tomamos entonces valores $u,v \in \mathbb{Z}:\ -1 \equiv_p u^2+v^2$ y volvemos a usar el argumento del retículo:

$$H := \{(a,b,c,d) \in \mathbb{Z}^4 :\ c \equiv_p ua+vb,\ d \equiv_p -va+ub\},$$

H es retículo pues sus elementos vienen dados de la forma

$$(a,b,c,d) = (a,b,ua+vb+mp,-va+ub+np) = a(1,0,u,-v)+b(0,1,v,u)+m(0,0,p,0)+n(0,0,0,p)$$

Son claramente linealmente independientes con

$$\mathrm{vol}(H) = \begin{vmatrix} 1 & 0 & u & -v \\ 0 & 1 & v & u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{vmatrix} = p^2.$$

Tomamos bolas $\overline{B}(0,r) \subset \mathbb{R}^4$ con $r > 0$ lo suficientemente grande como para que

$$\mu(\overline{B}(0,r)) = \frac{1}{2}\pi^2 r^4 > 2^4 \operatorname{vol}(H) = 16p^2.$$

En este caso tomaremos $r > 0 :\ r^2 = \frac{19}{10}p$, efectivamente

$$\frac{1}{2}\pi^2 \left(\frac{19}{10}p\right)^2 > 2^4 \operatorname{vol}(H) = 16p^2 \Leftrightarrow\ \pi^2 \frac{19^2}{2 \cdot 10^2} > 16 \Leftrightarrow\ \pi^2 > \frac{2^7 \cdot 5^2}{19^2}.$$

Fijémonos en que $3200 = 2^7 \cdot 5^2 < 19^2 \cdot 3^2 = 3249$ luego

$$\pi^2 > 3^2 > \frac{2^7 \cdot 5^2}{19^2}.$$

Así que podemos usar el último corolario asegurando que existe $0 \neq (a,b,c,d) \in \overline{B}(0,r) \cap H$ luego

$a^2+b^2+c^2+d^2 \equiv_p a^2+b^2+(ua+vb)^2+(-va+ub)^2 = a^2+b^2+u^2a^2+v^2b^2+v^2a^2+u^2b^2 = a^2(1+u^2+v^2)+b^2(1+u^2+v^2) \equiv_p 0$

Luego $\exists m \in Z$ con $m \geq 1$:

$$a^2 + b^2 + c^2 + d^2 = mp.$$

Pero al mismo tiempo

$$a^2 + b^2 + c^2 + d^2 < r^2 = \frac{19}{10}p \Rightarrow m = 1.$$

Por tanto todos los primos son suma de cuatro cuadrados. Veamos ahora que si dos números son expresables como suma de cuatro cuadrados su producto también:
Sean $\alpha, \beta \in \mathbb{C}$ y consideremos la matriz

$$\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$$

si tomamos el determinante de la matriz nos da $N(\alpha) + N(\beta)$ así que metiendo $\alpha, \beta \in \mathbb{Z}[i]$ se tiene la suma de 4 cuadrados.
Ahora vemos que dados además $\gamma, \delta \in \mathbb{Z}[i]$ definimos $\xi := \alpha\gamma - \overline{\beta}\delta,\ \eta := \beta\gamma + \overline{\alpha}\delta, \quad \xi, \eta \in \mathbb{Z}[i]$ y

$$\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & -\overline{\delta} \\ \delta & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \xi & -\overline{\eta} \\ \eta & \overline{\xi} \end{pmatrix}.$$

Sabemos que el determinante del producto de matrices es el producto de determinantes así que ya estaría, dado n lo ponemos como producto de primos, sabemos que para cada primo p existe una matriz de esta forma tal que su determinante es p luego tomamos el producto de esas matrices, su determinante es n y suma de 4 cuadrados. □

6.4 El teorema de las unidades

Teorema 6.18 (Teorema de las unidades de Dirichlet)**.** Sea $K/\mathbb{Q}$ un cuerpo de números y $n = r_1 + 2r_2 = [K : \mathbb{Q}]$ donde r_1 son las inmersiones reales y $2r_2$ las complejas y $r := r_1 + r_2 - 1$.
Entonces $U_K := O_K^\times$ es abeliano finitamente generado. De hecho, existen $\omega, u_1, \ldots, u_r \in U_K$ y existe $m \in \mathbb{N}$ tales que:

1. $m = |\omega|$, aquí $|\cdot|$ denota al orden en U_K.
2. $u_1, \ldots, u_r$ son $\mathbb{Z}$-independientes.
3. $\forall u \in U_K\ \exists!\ 0 \leq i < m,\ i_1, \ldots, i_r \in \mathbb{Z} :\ u = \omega^i u_1^{i_1} \ldots u_r^{i_r}$.

Al decir que $u_1, \ldots, u_r$ son $\mathbb{Z}$-independientes nos referimos a que dados $i_1, \ldots, i_r$ se tiene que que $u_1^{i_1} \ldots u_r^{i_r} = 1 \Rightarrow\ i_1 = \ldots = i_r = 0$. Las $u_1, \ldots, u_r$ que cumplen este enunciado suelen llamarse 'sistema fundamental de

unidades'. La propiedad 3 (que implica la 2) nos permite representar cualquier unidad como producto de ω y los u_i.

Este teorema indica la estructura de los grupos de unidades, y nos permite expresar todas las unidades de O_K como productos de unas pocas unidades. Vamos a demostrar el teorema usando retículos.

Demostración. Sean $\sigma_1, \dots, \sigma_{r_1} : K \to \mathbb{R}$ las inmersiones reales y sean $\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2} : K \to \mathbb{C}$ las complejas, de forma que $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ para $i = 1, \dots, r_2$.

Representamos K por un elemento primitivo, es decir, $K = \mathbb{Q}(\gamma)$ con $\min_{\mathbb{Q}}(\gamma) = (x-\gamma_1)\dots(x-\gamma_n), \quad \gamma_i \in \mathbb{C}$. Cada inmersión σ_i viene determinada por el valor al que le asigna $\gamma_1 := \gamma$ así que supongamos que $\sigma_i(\gamma) = \gamma_i$ para cada $i = 1, \dots n$.
De esta forma $\gamma = \gamma_1, \dots, \gamma_{r_1} \in \mathbb{R}$ y $\gamma_{r_1+1}, \dots, \gamma_{r_1+r_2} \in \mathbb{C} \setminus \mathbb{R}$ y $\gamma_{r_1+r_2+i} = \overline{\gamma_{r_1+i}},\ i = 1, \dots r_2$.

Definamos ahora una aplicación $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tal que

$$\sigma(\alpha) := (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)).$$

Identificamos $\mathbb{C}$ con $\mathbb{R}^2$ haciendo $(a+bi) \sim (a,b)$ luego podemos reinterpretar $\sigma : K \to \mathbb{R}^n$ tal que

$$\sigma(\alpha) = (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \operatorname{Re}\sigma_{r_1+1}(\alpha), \operatorname{Im}\sigma_{r_1+1}(\alpha) \dots, \operatorname{Re}\sigma_{r_1+r_2}(\alpha), \operatorname{Im}\sigma_{r_1+r_2}(\alpha)).$$

Todo esto es para poder usar un retículo en $\mathbb{R}^n$.

σ es homomorfismo de grupos aditivos, es decir, $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$. Además, es inyectivo, lo vemos viendo que si $\sigma(\alpha) = 0$ es que todas las inmersiones sobre α son 0, cada una de ellas es inyectiva luego $\alpha = 0$. Es decir, $\ker\sigma = \{0\}$.
Veamos ahora que $\sigma(O_K)$ es un retículo completo de $\mathbb{R}^n$ y además calcularemos su volumen.

Tomemos $\{\alpha_1, \dots, \alpha_n\}$ base entera de O_K. Al ser inyectiva σ, será biyectiva sobre la imagen de O_K y por tanto O_K es isomorfo a $\sigma(O_K)$ por σ.
Por tanto $\sigma(O_K)$ es grupo abeliano libre de rango n con base $\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$. Para ver que son $\mathbb{R}$-independientes podemos calcular el volumen:

El volumen En primer lugar pondremos una de las expresiones que hemos visto para d_K, tengamos en cuenta que como es un cuadrado podemos intercambiar las filas del determinante a placer. Además, $d_K \neq 0$ por ser el discriminante de O_K:

$$d_K = \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_n) \\ \overline{\sigma}_{r_1+1}(\alpha_1) & \cdots & \overline{\sigma}_{r_1+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \overline{\sigma}_{r_1+r_2}(\alpha_1) & \cdots & \overline{\sigma}_{r_1+r_2}(\alpha_n) \end{vmatrix}^2 = \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+1}(\alpha_n) \\ \overline{\sigma}_{r_1+1}(\alpha_1) & \cdots & \overline{\sigma}_{r_1+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_n) \\ \overline{\sigma}_{r_1+r_2}(\alpha_1) & \cdots & \overline{\sigma}_{r_1+r_2}(\alpha_n) \end{vmatrix}^2 \overset{(*)}{=}$$

$$2^{2r_2}(-i)^{2r_2}\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_n) \\ \operatorname{Re}\sigma_{r_1+1}(\alpha_1) & \cdots & \operatorname{Re}\sigma_{r_1+1}(\alpha_n) \\ \operatorname{Im}\sigma_{r_1+1}(\alpha_1) & \cdots & \operatorname{Im}\sigma_{r_1+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \operatorname{Re}\sigma_{r_1+r_2}(\alpha_1) & \cdots & \operatorname{Re}\sigma_{r_1+r_2}(\alpha_n) \\ \operatorname{Im}\sigma_{r_1+r_2}(\alpha_1) & \cdots & \operatorname{Im}\sigma_{r_1+r_2}(\alpha_n) \end{vmatrix}^2 = 4^{r_2}(-1)^{r_2}\operatorname{vol}(\sigma(O_K))^2.$$

La igualdad $(*)$ se debe a: $\binom{a+bi}{a-bi} \mapsto \binom{a+bi}{-2bi} \mapsto \binom{a}{-2bi} \mapsto 2(-i)\binom{a}{b}$, hacemos esto en r_2 pares de filas y el determinante está al cuadrado. Por tanto nos hemos quedado con:

$$|d_K| = 4^{r_2}\operatorname{vol}(\sigma(O_K))^2 \Rightarrow \quad \operatorname{vol}(\sigma(O_K)) = 2^{-r_2}\sqrt{|d_K|} \neq 0.$$

Volvemos a las unidades Definamos una función $L : K \setminus \{0\} \to \mathbb{R}^{r_1+r_2}$ como

$$L(\alpha) := (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1}(\alpha)|, \log|\sigma_{r_1+1}(\alpha)|, \ldots, \log|\sigma_{r_1+r_2}(\alpha)|).$$

Recordemos que las σ_i son en particular inyectivas así que L está definida correctamente.
Fijémonos en que $L(\alpha\beta) = L(\alpha) + L(\beta)$, luego si nos restringimos a las unidades $L : U_K \to \mathbb{R}^{r_1+r_2}$ tenemos que L es homomorfismo de grupos. En primer lugar $L(U_K) <_+ \mathbb{R}^{r_1+r_2}$. Veremos que $L(U_K)$ es retículo comprobando que:
$\forall C \subset \mathbb{R}^{r_1+r_2}$ compacto se tiene que $L(U_K) \cap C$ es finito.

Para demostrarlo comprobaremos algo más fuerte:

$$J := \{\alpha \in O_K : \ L(\alpha) \in C\} \quad \text{es finito.}$$

C es compacto en el espacio euclídeo luego está contenido en una bola $B(0, \varepsilon')$ con $\varepsilon' > 0$ lo suficientemente grande. Ahora tomamos $\varepsilon := e^{\varepsilon'}$ de tal forma que dado $\alpha \in J$ se tiene:

$$\log|\sigma_1(\alpha)| = L(\alpha)_i \leq |L(\alpha)| \leq \varepsilon' \Rightarrow |\sigma_1(\alpha)| \leq e^{\varepsilon'} = \varepsilon.$$

Es decir, $\exists \varepsilon > 0 : \ \forall \alpha \in J$ se tiene que $|\sigma_i(\alpha)| \leq \varepsilon$.
Tomamos $\min_{\mathbb{Q}}(\alpha)$ de grado $n'|n$ y lo elevamos a n/n' :

$$(\min_{\mathbb{Q}}(\alpha))^{n/n'} = x^n + a_1x^{n-1} + \ldots + a_n, \quad a_i \in \mathbb{Z}.$$

Ahora, se tiene que

$$\begin{cases} a_1 &= -(\sigma_1(\alpha) + \ldots + \sigma_n(\alpha)) \\ \vdots & \vdots \\ a_n &= (-1)^n\sigma_1(\alpha)\ldots\sigma_n(\alpha) \end{cases} \Rightarrow \begin{cases} |a_1| &\leq n\varepsilon \\ \vdots & \vdots \\ |a_n| &\leq \varepsilon^n \end{cases}$$

De hecho $|a_k| \leq \binom{n}{k}\varepsilon^k$. Recordemos que los a_k son enteros acotados luego la cantidad de polinomios que podemos construir con ellos es finita. Por tanto la cantidad de elementos de J también es finita.

Ya sabemos que $L(U_K)$ es un retículo luego es isomorfo a $\mathbb{Z}^s$ con $s \leq r_1 + r_2$.
Fijémonos ahora en $\ker L|_{U_K}$. Este subgrupo es $\{\alpha \in U_K : \ L(\alpha) \in \{0\}\}$, por tanto al ser $\{0\}$ compacto, $\ker L|_{U_K}$ es finito. Además sus elementos son unidades de O_K, por tanto en concreto están en $\mathbb{C}$.

Así que $\ker L_{|U_K}$ es un subgrupo finito del grupo multiplicativo de un cuerpo, por tanto es cíclico. Luego $\exists \omega \in U_K : \ \ker L_{|U_K} = \langle\omega\rangle$. Denotemos por $m := |\omega|$ al orden de ω. Como $U_K \subset O_K \subset K \subset \mathbb{C}$ sabemos que ω es una raíz m-ésima primitiva de la unidad. en conclusión podemos tomar $\omega = \omega_m$.

Recordemos que L restringido a U_K es homomorfismo de grupos luego por el primer teorema de isomorfía,

$$\frac{U_K}{\langle\omega\rangle} \approx L(U_K) \approx \mathbb{Z}^s.$$

Tomemos $u_1, \ldots, u_s \in U_K :\ \overline{u}_1, \ldots, \overline{u}_s \in U_K/\langle\omega\rangle$ es $\mathbb{Z}$-base. Es decir, dado $u \in U_K$, su clase en $U_K/\langle\omega\rangle$ se representa de forma **única** como

$$\overline{u} = \overline{u}_1^{i_1} \ldots \overline{u}_s^{i_s}, \quad \text{para ciertos valores } i_1, \ldots, i_s \in \mathbb{Z}.$$

Por tanto $\exists!\ i \in \mathbb{Z}$ con $0 \leq i < m$ tal que $u = \omega^i u_1^{i_1} \ldots u_s^{i_s}$.
Veamos esto, sea $a, b \in U_K$ tales que $\overline{a} = \overline{b}$. Supongamos que existen $i, j \in \mathbb{Z}$ tales que $0 \leq i < j < m$ con $a = \omega^i a = \omega^j b \Rightarrow 1 = \omega^{j-i}$ y ω tendría orden menor que m.

Para terminar de demostrar el teorema tenemos que ver que $s = r := r_1 + r_2 - 1$. De momento tenemos que $s \leq r_1 + r_2$.
La norma manda las unidades de O_K en las unidades de $\mathbb{Z}$ luego:

$$\begin{array}{rcl} \alpha \in U_K & \Leftrightarrow & \pm 1 = N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha) \\ & \Leftrightarrow & 1 = |\sigma_1(\alpha)| \ldots |\sigma_n(\alpha)| \\ & \Leftrightarrow & 0 = \log|\sigma_1(\alpha)| + \ldots + \log|\sigma_n(\alpha)| \\ & \Leftrightarrow & 0 = \log|\sigma_1(\alpha)| + \ldots + \log|\sigma_{r_1}(\alpha)| + 2\log|\sigma_{r_1+1}(\alpha)| + \ldots + \log|\sigma_2 r_1 + r_2(\alpha)| \end{array}$$

Por tanto, si definimos el hiperplano de $\mathbb{R}^{r_1+r_2}$:

$$\pi := \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : x_1 + \ldots + x_{r_1} + 2x_{r_1+1} + \ldots + 2x_{r_1+r_2} = 0\},$$

sabemos que $L(U_K) \subset \pi$ y que $\dim(\pi) = r_1 + r_2 - 1 =: r \Rightarrow\ s \leq r$.

Supongamos ahora que $s < r$. Entonces existe $f : \pi \to \mathbb{R}$ forma no nula con $f(L(U_K)) = 0$ pues $\dim(\pi) = \dim(\ker f) + \dim(f(\pi))$, así que como f es una forma no nula, $\dim(f(\pi)) = 1 \Rightarrow \dim(\ker f) = r - 1$ y si la dimensión de $f(L(U_K))$ es menor que r en principio podremos contenerlo en $\ker f$. Veámoslo:
Comenzamos tomando una base de $f(L(U_K)) :\ e_1, \ldots, e_s$ y la extendemos en $\pi :\ e_{s+1}, \ldots, e_r$. Ahora definimos f como $f(e_k) = \begin{cases} 0 & \text{si} \quad k \leq s \\ 1 & \text{si} \quad k > s \end{cases}$
Veamos ahora que nunca podremos encontrar esta forma, es decir:
Para toda forma no nula $f : \pi \to \mathbb{R}$ existe $\alpha \in U_K :\ f(L(\alpha)) \neq 0$.

Para ello buscaremos un conjunto S tal que $\mu(S) > 2^n \operatorname{vol}(\sigma(O_K))$. Construiremos el conjunto en función de cierto $\lambda = (\lambda_1, \ldots, \lambda_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2}$:

$$S_\lambda = [-\lambda_1, \lambda_1] \times \ldots \times [-\lambda_{r_1}, \lambda_{r_1}] \times \overline{D}(0, \lambda_{r_1+1}) \times \ldots \times \overline{D}(0, \lambda_{r_1+r_2}) \subset \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}.$$

Con $\overline{D}(0, r)$ nos referimos a la bola plana de centro 0 y radio $r > 0$. Al haber construido S de esta manera es fácil calcular su medida:

$$\mu(S) = \prod_{k=1}^{r_1} 2\lambda_k \prod_{k=r_1+1}^{r_1+r_2} \pi\lambda_k^2 = 2^{r_1}\pi^{r_2} \prod_{k=1}^{r_1} \lambda_k \prod_{k=r_1+1}^{r_1+r_2} \lambda_k^2.$$

Si fijamos $\mu(S)$ podemos poner $\lambda_{r_1+r_2}$ en función de las otras coordenadas de λ.
Entonces, fijados todos los λ_k menos $\lambda_{r_1+r_2}$, podemos elegir $\lambda_{r_1+r_2}$ para que se cumpla:

$$\varepsilon := \prod_{k=1}^{r_1} \lambda_k \prod_{k=r_1+1}^{r_2} \lambda_k^2 > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_k|}.$$

Entonces se tiene que:

$$\mu(S) = 2^{r_1}\pi^{r_2}\varepsilon > 2^{r_1}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_k|} = 2^{r_1+r_2}\sqrt{|d_k|} = 2^{r_1+2r_2}\,\mathrm{vol}(\sigma(O_K)) \Rightarrow \quad \mu(S) > 2^n\,\mathrm{vol}(\sigma(O_K)).$$

Por tanto $\sigma(O_K)\cap S_\lambda \neq \{0\}$, luego existe $\alpha_\lambda \in O_K$, con $\alpha_\lambda \neq 0$ pues σ es inyectiva, tal que $\sigma(\alpha_\lambda) \in S_\lambda \setminus \{0\}$. Ahora, definimos $\lambda_{r_1+r_2+i} := \lambda_{r_1+i}$, para $i = 1, \ldots, r_2$ y se tiene que como $\sigma(\alpha_\lambda) \in S_\lambda : \quad |\sigma_i(\alpha_\lambda)| \leq \lambda_i \ \forall i = 1, \ldots, n$. Como $\alpha \in O_K \setminus \{0\}$ sabemos que $N_{K/\mathbb{Q}}(\alpha_\lambda) \in \mathbb{Z} \setminus \{0\}$ luego

$$1 \leq |N_{K/\mathbb{Q}}(\alpha_\lambda)| = \left|\prod_i \sigma_i(\alpha_\lambda)\right| = \prod_i |\sigma_i(\alpha_\lambda)| \leq \prod_i \lambda_i = \prod_{i=1}^{r_1}\lambda_i \prod_{i=r_1+1}^{r_1+r_2}\lambda_i^2 = \varepsilon \Rightarrow \quad 1 \leq |N_{K/\mathbb{Q}}(\alpha_\lambda)| \leq \varepsilon \Rightarrow$$

$$|\sigma_i(\alpha_\lambda)| = \frac{|N_{K/\mathbb{Q}}(\alpha_\lambda)|}{\prod\limits_{j\neq i}|\sigma_j(\alpha_\lambda)|} \geq 1 \cdot \prod_{j\neq i}\lambda_j^{-1} = \lambda_i\varepsilon^{-1} \Rightarrow \quad \lambda_i\varepsilon^{-1} \leq |\sigma_i(\alpha_\lambda)| \leq \lambda_i \ \forall i = 1, \ldots, n.$$

Como $\lambda_i\varepsilon^{-1} > 0 \ \forall i = 1, \ldots, n$ tomamos logaritmos:

$$\log\lambda_i - \log\varepsilon = \log(\lambda_i\varepsilon^{-1}) \leq \log|\sigma_i(\alpha_\lambda)| \leq \log\lambda_i \Rightarrow \quad 0 \leq \log\lambda_i - \log|\sigma(\alpha_\lambda)| \leq \log\varepsilon.$$

Tomamos ahora $0 \neq f \in \pi^*$ con $f(x_1, \ldots, x_{r+1}) = \sum\limits_{i=1}^{r} c_i x_i, \ c_i \in \mathbb{R}, \ \forall (x_1, \ldots, x_{r+1}) \in \pi$.
Evaluamos $L(\alpha_\lambda)$ en f :

$$\left|f(L(\alpha_\lambda)) - \sum_{i=1}^{r} c_i \log\lambda_i\right| = \sum_{i=1}^{r}|c_i|\,|\log|\sigma_i(\alpha_\lambda)| - \log\lambda_i| \leq \left(\sum_{i=1}^{r}|c_i|\right)\log\varepsilon$$

Recapitulemos, hemos definido $\varepsilon > \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_k|}$ en función de los $\lambda_i, \ i = 1, \ldots, r_1 + r_2$.
Después hemos visto las siguientes desigualdades:

- $1 \leq |N_{K/\mathbb{Q}}(\alpha_\lambda)| \leq \varepsilon$.
- $\lambda_i\varepsilon^{-1} \leq |\sigma_i(\alpha_\lambda)| \leq \lambda_i \ \forall i = 1, \ldots, n$.
- $0 \leq \log\lambda_i - \log|\sigma(\alpha_\lambda)| \leq \log\varepsilon$.
- $\left|f(L(\alpha_\lambda)) - \sum\limits_{i=1}^{r} c_i \log\lambda_i\right| =\leq \left(\sum\limits_{i=1}^{r}|c_i|\right)\log\varepsilon$.

Donde los c_i vienen dados por una forma $f \in \pi^*$ y queremos ver que hay al menos un elemento $\alpha \in O_K$ tal que $f(L(\alpha)) \neq 0$.
Tomemos entonces $\delta \in \mathbb{R}$ con $\sum_{i=1}^{r}|c_i|\log\varepsilon < \delta$. Para cada $h \in \mathbb{N}$ tomamos λ_i^h, con $1 \leq i \leq r$ de tal forma que

$$\sum_{i=1}^{r} c_i \log\lambda_i^h = 2h\delta$$

El valor $\lambda_{r+1} = \lambda_{r_1+r_2}$ viene determinado por ε y los otros λ_i con $i = 1, \ldots, r$.
Además existe $\alpha_{\lambda^h} \in O_K : \quad \alpha_{\lambda^h} \in S_{\lambda^h}$ luego $|\sigma_i(\alpha_{\lambda^h})| \leq \lambda_i^h \ \forall i = 1, \ldots, n$. Recordemos que $\lambda^h_{r_1+r_2+i} := \lambda^h_{r_1+i}$ para $i = 1, \ldots, r_2$. Ahora, tenemos que:

$$\delta > \left(\sum_{i=1}^{r}|c_i|\right)\log\varepsilon \geq \left|f(L(\alpha_{\lambda^h})) - \sum_{i=1}^{r} c_i\log\lambda_i^h\right| = |f(L(\alpha_{\lambda^h})) - 2h\delta| \Rightarrow$$

$$-\delta < f(L(\alpha_{\lambda^h})) - 2h\delta < \delta \Rightarrow \quad \delta(2h-1) < f(L(\alpha_{\lambda^h})) < \delta(2h+1).$$

Denotemos por $I_h := (\delta(2h-1), \delta(2h+1))$ intervalo abierto, como h es un entero positivo, nos fijamos en que estos intervalos son disjuntos. Luego como $f(L(\alpha_{\lambda^h})) \in I_h$ sabemos que si $h, k \in \mathbb{N}$ con $h \neq k$ se tiene

que $f(L(\alpha_{\lambda^h})) \neq f(L(\alpha_{\lambda^k}))$ pues están en intervalos disjuntos. Lo importante aquí es que $f(L(\alpha_{\lambda^h}))$ toma infinitos valores distintos.
Ahora, $N(\alpha_{\lambda^h}O_K) = |N_{K/\mathbb{Q}}(\alpha_{\lambda^h})| \leq \varepsilon$. La cantidad de ideales en O_K con norma menor o igual que ε es finita pues todo ideal descompone de forma única como producto de primos. Por tanto el conjunto $\{\alpha_{\lambda^h}O_K : h \in \mathbb{N}\}$ es finito luego existen $h, k \in \mathbb{N}$ con $h \neq k$ tales que

$$\alpha_{\lambda^h}O_K = \alpha_{\lambda^k}O_K.$$

Como generan el mismo ideal principal, son asociados, luego $\exists u \in U_K : \quad \alpha_{\lambda^h} = u\alpha_{\lambda^k}$. Por tanto:

$$L(\alpha_{\lambda^h}) = L(u\alpha_{\lambda^k}) = L(u) + L(\alpha_{\lambda^k}) \Rightarrow \quad f(L(\alpha_{\lambda^h})) = f(L(u)) + f(L(\alpha_{\lambda^k})) \Rightarrow$$

$$f(L(u))) = f(L(\alpha_{\lambda^h})) - f(L(\alpha_{\lambda^k})) \neq 0.$$

Luego no podemos encontrar una forma no nula en π que anule $L(U_K)$ y por tanto la dimensión de $L(U_K)$ debe ser precisamente r. □

Resultados random que veremos (???? no no? xd)

- Si K es un cuerpo de números distinto de $\mathbb{Q}$, $d_K \neq \pm 1$.
- Sea $d \in \mathbb{Z}$, la cantidad de cuerpos de números con discriminante d es finita salvo isomorfía.

6.5 La ecuación de Pell

Recordemos que la ecuación de Pell se refiere a la ecuación

$$x^2 - ny^2 = 1,$$

donde nos dan n entero y buscamos soluciones para x, y enteros. Podemos suponer que n es libre de cuadrados, ya que si no, escribiendo $n = k^2m$ con m libre de cuadrados, entonces si (x, y) es solución de $x^2 - ny^2 = 1$, entonces (x, ky) es solución de $x^2 - my^2 = 1$, por tanto el caso n se puede resolver a partir del caso m.

Para estudiarla vamos a analizar las unidades de los cuerpos cuadráticos reales, $K = \mathbb{Q}[\sqrt{d}]$, con $d > 0$ entero libre de cuadrados. Empezamos con el caso $d \not\equiv_4 1$, con $O_K = \mathbb{Z}[\sqrt{d}]$.

En este caso $r_1 = 2, r_2 = 0$, por tanto $r = r_1 + r_2 - 1 = 1$. Además, como $K \subseteq \mathbb{R}$, las únicas raíces de la unidad (es decir, el subgrupo de torsión de U_K) son 1 y -1. De modo que el grupo de unidades será de la forma

$$U_K = \{\pm u^i; i \in \mathbb{Z}\},$$

para cierta unidad fundamental $u \neq 1, -1$. Al ser u una unidad, tiene norma 1, es decir, si llamamos $u = a+b\sqrt{d}$ entonces $N(u) = a^2 - db^2 = 1$. Entonces, por la estructura del grupo de unidades, las únicas cuatro posibles unidades fundamentales son $u, -u, u^{-1}$ y $-u^{-1}$, ya que son las únicas unidades v con $U_K = \{\pm v^i; i \in \mathbb{Z}\}$. Como solo una de las cuatro unidades es > 1, podemos suponer $u > 1$, es decir, u es la mayor de las 4 unidades. Como las posibles 4 unidades fundamentales son de la forma $\pm a \pm b\sqrt{d}$ (ya que $u^{-1} = \pm(a - b\sqrt{d})$) y hemos cogido u como la mayor de ellas, u será de forma $a + b\sqrt{d}$ con $a, b > 0$.

Escribiendo $u_k := u^k = (a + b\sqrt{d})^k$, llamamos a_k y b_k a los enteros tales que $u_k = a_k + b_k\sqrt{d}$. a_k y b_k con $k > 0$ se pueden obtener en función de una recurrencia, ya que:

$$u_{k+1} = u_k u = (a_k + b_k\sqrt{d})(a + b\sqrt{d}) = (a_k a + db_k b) + \sqrt{d}(a_k b + b_k a).$$

Por tanto,

$$\begin{array}{rcl} a_{k+1} & = & a_k a + db_k b \\ b_{k+1} & = & a_k b + b_k a. \end{array} \tag{6.1}$$

Esto implica, en concreto, que $a_{k+1} > a_k$ y $b_{k+1} > b_k$.

Además, para $k > 0$, $u^{-k} = u_k^{-1}$ es $a_k - b_k\sqrt{d}$ (ya que $N(u_k) = 1$). Por tanto, como las unidades de U_K son los elementos de forma $\pm u_k$ y $\pm u^{-k}$, tenemos que:

$$U_K = \{\pm 1\}\{\pm a_k \pm b_k\sqrt{d}\}.$$

Por tanto todas las unidades salvo 1 y -1 serán de forma $\pm n \pm m\sqrt{d}$, donde $n \geq a, m \geq b$. Por tanto para encontrar la solución fundamental basta encontrar la solución con el menor $a > 0$ posible (y el menor $b > 0$ posible) de alguna de las ecuaciones $a^2 - db^2 = \pm 1$.

Un método para hacerlo es encontrar el menor b tal que $db^2 \pm 1$ es un cuadrado perfecto. Encontrar esta solución no tiene por qué ser fácil: por ejemplo, con $n = 313$ una unidad fundamental es $126862368 + 7170685\sqrt{313}$. Resumiendo la discusión anterior:

Proposición 6.19. Si $d > 0$, $d \not\equiv_4 1$, es libre de cuadrados, la ecuación $a^2 - db^2 = \pm 1$ tiene soluciones no triviales. De hecho, si (a, b) es la solución entera con menores a, b positivos, entonces las soluciones serán de forma $(\pm a_k, \pm b_k)$, donde a_k y b_k vienen dadas por la recurrencia 6.1. □

Ejemplo 6.20. En el caso $d = 3$, $K = \mathbb{Q}[\sqrt{3}]$, tenemos la ecuación $a^2 - 3b^2 = \pm 1$. La solución más pequeña en este caso es $a = 2, b = 1$, o sea que una unidad fundamental es $2 + \sqrt{3}$. Así que las unidades en este cuerpo son todas de la forma $\pm(2 \pm \sqrt{3})^i$, con $i \in \mathbb{Z}$.

En este caso no puede haber unidades de norma -1, ya que la unidad fundamental u tiene norma 1, por tanto $N(\pm u^k) = N(\pm 1)N(u)^k = 1$. De hecho estaba claro desde un principio que no puede haber unidades de norma -1, ya que mirando en módulo 3 está claro que no hay soluciones a la ecuación $x^2 - 3y^2 = -1$

Esto se puede generalizar:

Proposición 6.21. Si $d \in \mathbb{Z}^+$ es libre de cuadrados y hay un primo p con $p|d$ y $\left(\dfrac{-1}{p}\right) = -1$, entonces la ecuación $a^2 - db^2 = -1$ no tiene soluciones enteras.

Demostración. Módulo p la ecuación se transforma en $a^2 \equiv_p -1$, que no tiene solución. □

Si $d \equiv_4 1$, entonces $O_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. O sea que en este caso la ecuación a tener en cuenta será de forma

$$\pm 1 = N(u) = \frac{(2a+b)^2 - db^2}{4}, \text{ es decir, } \pm 4 = a'^2 - db'^2,$$

con $a' = 2a + b$ y $b' = b$. No lo vamos a ver en detalle, pero como en el caso anterior resolver la ecuación se reduce a encontrar el menor valor de b' tal que $d(b')^2 \pm 4$ es un cuadrado perfecto, y se pueden obtener el resto de soluciones mediante una recurrencia.

Ejemplo 6.22. Vamos a ver qué soluciones enteras tiene la ecuación $3x^2 - 4y^2 = 11$. Es decir, encontrar los puntos con coordenadas enteras en la hipérbola dada por $3x^2 - 4y^2 = 11$.

Para ello trabajamos en el cuerpo $\mathbb{Q}[\sqrt{3}]$. Aquí, la ecuación se traduce a $(2y)^2 - 3x^2 = -11$. Es decir, buscamos elementos $2y + x\sqrt{3}$ que tienen norma 11. Esto implica que el ideal $(2y + x\sqrt{3})$ divide a (11). De modo que vamos a factorizar el ideal (11) usando el lema de Kummer. Podemos usar el polinomio $x^2 - 3$, ya que $O_K = \mathbb{Z}[\sqrt{3}]$. En $\mathbb{Z}_{11}$, $x^2 - 3 = (x - 5)(x + 5)$, así que $(11) = 11_1 11_2$, con $11_1 = (11, 5 - \sqrt{3})$ y $11_2 = (11, -5 - \sqrt{3})$.

Por tanto el ideal $(2y + x\sqrt{3})$, que tiene norma ± 11, es o bien 11_1 u 11_2. Si es 11_1, 11_1 será principal, y en efecto podemos ver que $11_1 = (1 + 2\sqrt{3})$, y ahí tenemos un elemento de norma -11. Ahora, como $(2y + x\sqrt{3}) = (1 + 2\sqrt{3})$, tenemos que $2y + x\sqrt{3}$ es $1 + 2\sqrt{3}$ por una unidad. Si el ideal es 11_2, lo mismo pero cambiando $1 + 2\sqrt{3}$ por el generador de 11_2, $1 - 2\sqrt{3}$. De modo que hemos reducido el problema a encontrar las unidades de $\mathbb{Z}[\sqrt{3}]$.

Como una unidad fundamental en $\mathbb{Z}[\sqrt{3}]$ es $2 + \sqrt{3}$, ya tenemos que las soluciones $x + y\sqrt{3}$ serán de la forma $\pm(1 + 2\sqrt{3})(2 + \sqrt{3})^i$, con $i \in \mathbb{Z}$, o bien $\pm(1 + 2\sqrt{3})(2 + \sqrt{3})^i$, con $i \in \mathbb{Z}$. Equivalentemente, las soluciones son de forma $(1 \pm 2\sqrt{3})(\pm 2 \pm \sqrt{3})^i$, con $i \geq 0$. De nuevo, se pueden encontrar sin mucha dificultad recurrencias que describan estas soluciones.

Más ejercicios Encontrar las soluciones enteras de $x^2 - 10y^2 = 10$ y $2x^2 + xy + 3y^2 = 78$ (en la última aparece un cuerpo cuadrático imaginario).

6.6 El caso cúbico con $r = 1$

En esta sección pondremos $K = \mathbb{Q}[\alpha]$, donde $\min_{\mathbb{Q}}(\alpha)$ es cúbico y tiene una raíz real que es precisamente α.

Recordemos que el discriminante de un polinomio de raíces $\alpha_1, \ldots, \alpha_n$ es $\prod_{i<j}(\alpha_i - \alpha_j)^2$. Usando esto, no es difícil ver que si un polinomio p cúbico tiene 1 raíz real α_1 y dos conjugadas $\alpha_2, \overline{\alpha_2}$, entonces el discriminante de p es $(\alpha_1 - \alpha_2)^2(\alpha_1 - \overline{\alpha_2})^2(\alpha_2 - \overline{\alpha_2})^2 = |\alpha_1 - \alpha_2|^2 \cdot (2i\,\mathrm{Im}(\alpha_2))^2$, por tanto es un entero negativo.

Como $\min_{\mathbb{Q}}(\alpha)$ tiene una raíz real, tenemos $r_1 = 1, r_2 = 1$, así que $r = 1$. Como además nuestro cuerpo tiene una inmersión real, las únicas posibles raíces de la unidad son 1 y -1, de modo que de nuevo,

$$U_K = \pm u^i; i \in \mathbb{Z}$$

para cierta u unidad fundamental. De nuevo, las 4 posibles unidades fundamentales son $u, -u, u^{-1}, -u^{-1}$, y una de ellas es > 1, por tanto cogemos como u la que es > 1. Se va a dar el siguiente resultado:

Teorema 6.23. Artin
Si $K = \mathbb{Q}[\alpha]$, con $\min_{\mathbb{Q}}(\alpha)$ cúbico con única raíz real α, y hay $u \in U_K$ con $u > 1$ y

$$4u^{\frac{3}{2}} + 24 \leq |d_K|,$$

entonces u es unidad fundamental.
Además, para cualquier unidad $u > 1$ de U_K se cumple que $4u^3 + 24 > |d_K|$.

Antes de probarlo, veamos cómo se aplica a algunos ejemplos.

Ejemplo 6.24. Si $\alpha^3 = 2$, ya hemos visto que el discriminante de $\mathbb{Q}(\alpha)$ es $-108 = -2^3 3^3$. Si consideramos el elemento $\alpha - 1$, su polinomio mínimo es $(x+1)^3 - 2 = x^3 + 3x^3 + 3x - 1$, por tanto $N(\alpha - 1) = 1$. Es una unidad. De hecho, su inverso es $\alpha^2 + \alpha + 1$, ya que el producto de ambos es $\alpha^3 - 1 = 1$. Además, $\alpha^2 + \alpha + 1 > 1$. Llamando $u = \alpha^2 + \alpha + 1$, si tuviéramos que $4u^{\frac{3}{2}} + 24 < 108$, tendríamos que u es unidad fundamental. Pero $\alpha^2 + \alpha + 1 < 5$, por tanto $4u^{\frac{3}{2}} + 24 < 4 \cdot 15 + 24 < 108$, así que u es unidad fundamental.

Ejercicio Encontrar una unidad fundamental en $\mathbb{Q}[\alpha]$, con $\min_{\mathbb{Q}}(\alpha) = x^3 - x + 2$. (Base entera: $(1, \alpha, \alpha^2)$, $d_K = -104$).

Demostración de 6.23. Tenemos $[K : \mathbb{Q}] = 3$, $r_1 = r_2 = 1$ y $K \subset \mathbb{R}$. Dada $u \in U_K$ con $u > 1$, al ser mayor que 1 se tiene $[\mathbb{Q}(u) : \mathbb{Q}] > 1$ luego debe darse $K = \mathbb{Q}(u)$. Consideramos el polinomio mínimo de u de grado 3. Tiene 3 raíces: $u = u_1$, $v = u_2$, $\overline{v} = u_3$, $v, \overline{v} \in U_K$, $v, \overline{v} \notin \mathbb{R}$. Nuestro primer objetivo es ver que dada $u \in U_K$: $u > 1$ se tiene que

$$|d_K| < 4u^3 + 24.$$

Por ser u unidad, su norma debe ser ± 1 luego:

$$\pm 1 = N(u) = uv\overline{v} = u|v|^2 > 0 \Rightarrow \quad N(u) = 1.$$

Tomamos $\{1, u, u^2\}$ como base de enteros luego

$$|d_K| \leq |\Delta(1, u, u^2)| = \mathrm{abs}\begin{vmatrix} \sigma_1(1) & \sigma_1(u) & \sigma_1(u^2) \\ \sigma_2(1) & \sigma_2(u) & \sigma_2(u^2) \\ \sigma_3(1) & \sigma_3(u) & \sigma_3(u^2) \end{vmatrix}^2 = \mathrm{abs}\begin{vmatrix} 1 & u & u^2 \\ 1 & v & v^2 \\ 1 & \overline{v} & \overline{v}^2 \end{vmatrix}^2$$

Escribimos $u = r^2$ para cierto $r > 0$ y para que $1 = uv\overline{v}$ ponemos $v = r^{-1}e^{i\theta}$, $\overline{v} = r^{-1}e^{-i\theta}$ luego, nos ha quedado el valor absoluto de un determinante de Vandermonde:

$$|d_K| \leq |\Delta(1,u,u^2)| = \text{abs}\begin{vmatrix} 1 & r^2 & r^4 \\ 1 & r^{-1}e^{i\theta} & r^{-2}e^{2i\theta} \\ 1 & r^{-1}e^{-i\theta} & r^{-2}e^{-2i\theta} \end{vmatrix}^2 = \text{abs}[(r^{-1}e^{i\theta}-r^2)^2(r^{-1}e^{-i\theta}-r^2)^2(r^{-1}e^{-i\theta}-r^{-1}e^{-i\theta})^2] =$$

$$\text{abs}[(r^{-2}+r^4-r(e^{i\theta}+e^{-i\theta}))^2(r^{-1}2(-i)\,\text{sen}\,\theta)^2] = 4(r^{-2}+r^4-r(2\cos\theta))^2(r^{-1}\,\text{sen}\,\theta)^2 =$$

$$4(r^{-3}+r^3-2\cos\theta)^2(\text{sen}\,\theta)^2 = 4((r^{-3}+r^3)\,\text{sen}\,\theta - \text{sen}\,2\theta)^2 =$$

Busquemos ahora $\max_\theta\{[(r^3+r^{-3})\,\text{sen}\,\theta - \text{sen}\,2\theta]^2\}$, denotamos por $2t := (r^3+r^{-3})$ y definimos $f(x) := 2t\,\text{sen}\,\theta - \text{sen}\,2\theta$, luego

$$0 = f'(x) = 2t\cos\theta - 2\cos 2\theta \Leftrightarrow\ 0 = t\cos\theta - \cos 2\theta = t\cos\theta + \text{sen}^2\,\theta - \cos^2\theta = t\cos\theta + 1 - 2\cos^2\theta.$$

Ahora definimos $g(x) = 2x^2 - tx - 1$. Queremos encontrar una raíz real de este polinomio cuyo valor absoluto sea menor o igual que 1 para asegurar la existencia de $\theta_0 \in \mathbb{R} :\ \cos\theta_0 = \alpha_0$ donde α_0 es raíz de g.
g se trata de una parábola convexa, luego si existe $x \in \mathbb{R} :\ g(x) < 0$ tendrá raíces reales. Además, como el término independiente de g es -1 sabemos que el producto de las raíces v_1, v_2 de g es -1 luego $|v_1||v_2| = 1$ luego alguna de ellas será menor o igual que -1. Veamos que $g(1) < 0$ y $g\left(-\frac{1}{2r^3}\right) < 0$ asegurando la existencia de esta raíz e indicándonos que está en el intervalo $[-1, -\frac{1}{2r^3})$:

- Supongamos que $0 \leq g(1) = 1 - t \Rightarrow\ r^3(1-t) = r^3\left(1 - \frac{r^3+r^{-3}}{2}\right) = \frac{2r^3-r^6-1}{2} = -\frac{(r^3-1)^2}{2}$. Por tanto $g(1) < 0$.
- Ahora evaluamos $g\left(-\frac{1}{2r^3}\right) = 2\frac{1}{4r^6} + t\frac{1}{2r^3} - 1 = \frac{1+tr^3-2r^6}{2r^6} = \frac{1+(r^3+r^{-3})r^3/2-2r^6}{2r^6} = \frac{1+(r^6+1)/2-2r^6}{2r^6} = \frac{2+r^6+1-4r^6}{4r^6} = \frac{3-3r^6}{4r^6} = 3\frac{1-r^6}{4r^6}$. Como $r^2 = u > 1$ con $r > 0$ se tiene que $r > 1$ luego $g\left(-\frac{1}{2r^3}\right) = 3\frac{1-r^6}{4r^6} < 0$.

Tomemos entonces $\alpha_0 \in [-1, -\frac{1}{2r^3})$ raíz de g y $\theta_0 \in \mathbb{R} :\ \cos\theta_0 = \alpha_0$. La otra raíz de g debe ser mayor que 1, la derivada de g en α_0 es menor que 0 y por tanto f tiene un máximo en α_0. Sustituyamos:

$$|d_K| \leq 4((x^3+x^{-3})\,\text{sen}\,\theta - \text{sen}\,2\theta)^2 = 4(2t\,\text{sen}\,\theta_0 - 2\,\text{sen}\,\theta_0\cos\theta_0)^2 = 16\,\text{sen}^2\,\theta_0(t-\cos\theta_0)^2 = 16(1-\alpha_0^2)(t-\alpha_0)^2.$$

Vamos a desarrollar esta expresión, para ello tendremos en cuenta:

- $t\alpha_0 = 2\alpha_0^2 - 1$.
- $t^2\alpha_0^2 = 4\alpha_0^4 - 4\alpha_0^2 + 1$

Por tanto

$$16(1-\alpha_0^2)(t-\alpha_0)^2 = 16(1-\alpha_0^2)(t^2 - 2t\alpha_0 + \alpha_0^2) = 16(1-\alpha_0^2)(t^2 - 2(2\alpha_0^2-1) + \alpha_0^2) =$$

$$16t^2(1-\alpha_0^2) + 16(2-3\alpha_0^2)(1-\alpha_0^2) = 4(r^3+r^{-3})^2 - 16(4\alpha_0^4 - 4\alpha_0^2 + 1) + 16(2-3\alpha_0^2)(1-\alpha_0^2) =$$

$$4(r^6+2+r^{-6}) + 16(1-\alpha_0^2-\alpha_0^4) = 4(r^6+6) + 4(r^{-6} - 4\alpha_0^2 - 4\alpha_0^4) = 4(u^3+6) + 4(r^{-6} - 4\alpha_0^2 - 4\alpha_0^4).$$

Nuestro primer objetivo es llegar a que $|d_K| < 4(u^3+6)$. Por tanto debemos ver que $4(r^{-6} - 4\alpha_0^2 - 4\alpha_0^4) < 0$ lo cual se da si por ejemplo $r^{-6} - 4\alpha_0^2 < 0$.
Recordemos que $\alpha_0 \in [-1, -\frac{1}{2r^3})$. Es decir:

$$\alpha_0 < -\frac{1}{2r^3} < 0 \Rightarrow\ \alpha_0^2 > \frac{1}{4r^6} \Rightarrow\ 0 > \frac{1}{r^6} - 4\alpha_0^2.$$

Conclusión Tenemos una unidad $u > 1$ que cumple que $4u^{3/2} + 24 \leq |d_K|$ y tomamos una unidad fundamental $v > 1$, esto se puede hacer pues dada v unidad fundamental se tiene $v \neq \pm 1$ y que $\pm v^{\pm 1}$ es unidad fundamental luego al menos una de las cuatro opciones es mayor que 1.

Para esta v se tiene que $|d_K| < 4u^3 + 24$. Ahora, por ser v unidad fundamental y al mismo tiempo ser $u, v > 1$ se tiene que

$$\exists i \in \mathbb{N} : \ u = v^i.$$

Si $i = 1$ hemos acabado pues u es unidad fundamental.
Si $i \geq 2$ se tiene tenemos $v = u^{1/i}$ luego:

$$|d_K| < 4v^3 + 24 = 4u^{3/i} + 24 \leq 4u^{3/2} + 24 \leq |d_K|.$$

Así que llegamos a un absurdo y la única posibilidad es que $i = 1, \ u = v$. □

Anexo A

El determinante de Vandermonde

Dados $x_1, \ldots, x_n \in \mathbb{K}$, se dice que la siguiente matriz de orden n es de Vandermonde:

$$A = (x_i^{j-1})_i^j. \qquad \text{Mirar}^1$$

La matriz luce así:

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ 1 & x_3 & x_3^2 & \cdots & x_3^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix}$$

Calculemos su determinante:

$$|A_k| = |(x_i^{j-1})_i^j|$$

Dejamos la primera columna igual y al resto le restamos x_n por la columna anterior. Luego:

$$(B)_i^j = \begin{cases} 1 & \text{si} \quad j = 1 \\ x_i^{j-1} - x_n x_i^{j-2} & \text{si} \quad j \neq 1 \end{cases}$$

Esta matriz B tendrá el mismo determinante, nos fijamos en que para $j > 1$, $i = n$ se tienen ceros. Por tanto, definiendo la matriz de orden $n-1$: $(C)_i^j := x_i^j - x_n x_i^{j-1} = x_i^{j-1}(x_i - x_n)$:

$$|A| = |B| = (-1)^{n-1}|C|,$$

en cada fila se tiene $(x_i - x_n)$ como factor común luego, si denotamos por A_k a la matriz de Vandermonde determinada por $x_1, \ldots x_k$:

$$|A_n| = (-1)^{n-1}|C| = (-1)^{n-1}|A_{n-1}| \prod_{i<n}(x_i - x_n),$$

la idea es aplicar este proceso las veces que sean necesarias hasta llegar a A_1, que es la matriz (1), luego

$$|A| = \prod_{1<j\leq n} \prod_{i<j} (-1)^{j-1}(x_i - x_n) = \prod_{1\leq i<j\leq n} (-1)(x_i - x_j) = \prod_{1\leq i<j\leq n} (x_j - x_i).$$

[1] Esto es notación wachi que me apetecía poner, básicamente en la posición (i, j) de la matriz aparece el x_i elevado a $j-1$.

Anexo B

Cuerpos ciclotómicos

Si consideramos $m \in \mathbb{Z}$, la ecuación $x^m - 1 = 0$ tiene exactamente m soluciones distintas, entre las que se encuentra el 1.
De esta forma $(x^m - 1) = (x-1)(x^{m-1} + \ldots + 1)$.

Proposición B.1. Sea p primo, entonces el polinomio en $\mathbb{Q}[x]$:

$$x^{p-1} + \ldots + 1$$

es irreducible.

Demostración. Trasladamos el polinomio haciendo $x = t + 1$:

$$\sum_{k=0}^{p-1} x^k = \sum_{k=0}^{p-1} (t+1)^k = \sum_{k=0}^{p-1} \sum_{j=0}^{k} \binom{k}{j} t^j$$

En primer lugar:
Nos fijamos en el coeficiente $p-1$-ésimo, en ese caso $k = p-1$ y $j = k = p-1$ luego el binomio es 1 y el coeficiente también.
Ahora nos fijamos en el término independiente, así que fijado k, se necesita que $j = 0$ y en ese caso el binomio es 1. Luego $\sum_{k=0}^{p-1} 1t^0 = p$.
Por último sea otro término j-ésimo cualquiera, su coeficiente será

$$\sum_{k \geq j}^{p-1} \binom{k}{j} = \sum_{k=0}^{p-j-1} \binom{j+k}{j} = \binom{p}{j+1}.^1$$

Como $p | \binom{p}{j+1}$ aplicamos el criterio de Eisenstein y deducimos que efectivamente el polinomio es irreducible en $\mathbb{Z}[x]$. □

Definición B.2. Se define el p-ésimo polinomio ciclotómico (p primo) como $\Phi_p(x) = x^{p-1} + \ldots + 1 \in \mathbb{Z}[x]$.
Definimos el primer polinomio ciclotómico como $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$.

Proposición B.3. Sea $m \in \mathbb{N}$, entonces el polinomio $x^m - 1 \in \mathbb{Z}[x]$ descompone como

$$x^m - 1 = \prod_{k|m} \Phi_k(x)$$

[1] Hemos usado que $\sum_{k=0}^{m} \binom{j+k}{j} = \binom{j+m+1}{j+1}$,se demuestra aplicando inducción sobre m.

Así podemos definir el m-ésimo polinomio ciclotómico recursivamente como

$$\Phi_m(x) = \frac{x^m - 1}{\prod\limits_{\substack{k|m \\ k \neq m}} \Phi_k(x)}$$

Existe un isomorfismo entre $\mathbb{Z}_m$ y las raíces de $x^m - 1$ con el producto complejo, ambos son grupos cíclicos de p elementos así que tomemos $\omega = \omega_m := e^{\frac{2\pi i}{n}}$ como generador. La idea es que el orden de los elementos de $\mathbb{Z}_m$ divide a m, así que podemos tomar cada $k|m$.

- El elemento de orden 1 es el $1 \in \mathbb{C}$, cuyo polinomio mínimo es $x - 1$.
- Los elementos ω^k de orden $p \in \mathbb{Z}$ primo con $p|m$ junto con el 1 forman un grupo cíclico de orden p. Además el polinomio mínimo de ω^k es Φ_p.
- Recordemos la función φ de Euler. $\varphi(m) \geq 2$ si $m \geq 2$ luego hay al menos dos raíces elementos ω^k tal que $k \not| m$. Si tomamos $\prod\limits_{k \not| m} (x - \omega^k)$ obtenemos $\Phi_m(x)$.

Ejemplo B.4. Veamos $x^{p^2} - 1$:

$$x^{p^2} - 1 = \Phi_1 \Phi_p \Phi_{p^2} = (x-1)(x^{p-1} + \ldots + 1)\frac{x^{p^2} - 1}{x^p - 1} \Rightarrow \ \Phi_{p^2} = x^{p(p-1)} + \ldots + 1$$

Ahora con $x^{12} - 1$:

$$x^{12} - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_4 \Phi_6 \Phi_{12}$$

$$\Phi_1 = x - 1, \quad \Phi_2 = x + 1, \quad \Phi_3 = x^2 + x + 1, \quad \Phi_4 = x^2 + 1$$

$$\Phi_6 = x^2 - x + 1, \quad \Phi_{12} = \frac{x^{12} - 1}{(x^6 - 1)(x^2 + 1)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1$$

El próximo paso es ver que Φ_m es irreducible en $\mathbb{Z}$ para toda $m \in \mathbb{Z}$. Adjuntamos dos enlaces con demostraciones de Gauss y Kronecker.
`https://www.lehigh.edu/~shw2/c-poly/several_proofs.pdf`
`https://paramanands.blogspot.com/2009/12/gauss-and-regular-polygons-cyclotomic-polynomials.html#.YGZTW68zaUk`

Caso particular $m = 9$ Veamos este caso, $x^9 - 1 = \Phi_1 \Phi_3 \Phi_9 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$.
Pasamos a módulo 2, si no fuese irreducible se tendría que

$$\phi_9(x) = h(x)g(x)$$

donde h es irreducible en $\mathbb{Z}_2[x]$ de grado $1, 2$ ó 3.
h no puede ser de grado 1 pues ni 0 ni 1 son raíces de $\phi_9(x) = x^6 + x^3 + 1$. Existen 4 polinomios mónicos de grado 2 en $\mathbb{Z}_2[x]$ de los cuales solo 1 es irreducible: $x^2 + x + 1$.
Dividimos:

$$\frac{x^6 + x^3 + 1}{x^2 + x + 1} = x^4 + x^3 + \frac{1}{x^2 + x + 1}$$

Existen 8 polinomios mónicos de grado 3 en $\mathbb{Z}_2[x]$ de los cuales solo 2 son irreducibles: $x^3 + x^2 + 1$, $x^3 + x + 1$.
Dividimos igual que antes:

$$\frac{x^6 + x^3 + 1}{x^3 + x^2 + 1} = x^3 + x^2 + x + 1 + \frac{x}{x^3 + x^2 + 1}, \qquad \frac{x^6 + x^3 + 1}{x^3 + x + 1} = x^3 + x + \frac{x^2 + x + 1}{x^3 + x + 1}$$

Así que Φ_9 es irreducible en $\mathbb{Z}_2[x]$ y por tanto en $\mathbb{Z}[x]$.

Bibliografía

[1] Kenneth S. Williams. *On Eisenstein´s supplement to the law of cubic reciprocity.* Bull. Cal. Math. Soc, 69, 311-314 (1977).

[2] W. Sierpinski. *Elementary Theory of Numbers.* Elsevier Science Ltd (1988).

[3] Hardy & Wright. *An introduction to the theory of numbers. Fourth edition.* Oxford University Press, 1959.

[4] L. Carlitz. *A characterization of Algebraic Number Fields of Class Number Two.* Proc. Amer. Math. Soc.11, 391–392 (1960).

[5] Pierre Samuel. *Algebraic Theory of Numbers.* Herrmann, Paris, 1970.

[6] Emil Grosswald. *Representations of Integers as Sums of Squares.* Sprenger Verlag, 1985.

[7] Ian Stewart, David Tall. *Algebraic Number Theory and Fermat´s Last Theorem,* 3^{rd} *edition.* A K Peters, 2002.