Teoría Algebraica de Números

Miguel González
mgonzalez.contacto@gmail.com

Enero de 2022

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

Revisado en 2022

Acerca de este documento

Estos apuntes son una versión revisada de los de la asignatura Teoría Algebraica de Números del grado en matemáticas, tomados en Enero de 2022 por Miguel González. A los apuntes originales se les ha añadido esta página, una imagen de portada, y breves párrafos explicativos en las zonas menos completas. Asimismo se han revisado las erratas y completado los contenidos faltantes.

Este documento es:

- Una recopilación ordenada y directa de las definiciones y resultados más importantes del tema en cuestión, al nivel de los estudios de grado.
- Una colección de demostraciones completas de dichos resultados (salvo en los casos más básicos).
- Una *guía* para revisar de manera rápida las ideas que se han adquirido previamente, o para consultar enunciados puntuales que puedan no haberse comprendido en su totalidad.

Este documento NO es:

- Un libro de texto de la asignatura.
- Una colección de ejercicios para practicar los conceptos adquiridos.
- Un listado de ejemplos para ilustrar las ideas tratadas. A pesar de ello, en ocasiones se incluyen ejemplos puntuales que puedan ser de especial interés o curiosidad, pero se intentan reducir al mínimo en virtud del primer punto de la lista anterior.

Sobre Teoría Algebraica de Números

Esta asignatura es una introducción a la teoría algebraica de números, cuyo objetivo es dar respuesta a preguntas de teoría de números utilizando para ello herramientas algebraicas como la teoría de anillos, dominios de Dedekind o grupos de clases, entre otros.

Se establecen con estas herramientas resultados como la ley de reciprocidad cuadrática o el teorema de navidad de Fermat.

Requisitos previos

1. Conocimientos de aritmética (factorización y congruencias, entre otros).
2. Conocimientos de álgebra (grupos, anillos, cuerpos).

Índice

1. Introducción

1.1. Ternas pitagóricas y enteros gaussianos

El objetivo que se plantea es resolver la ecuación $x^2+y^2=z^2$ en los racionales positivos. Multiplicando y dividiendo por los factores adecuados, esto se reduce a encontrar soluciones a la ecuación en los enteros, en las que x, y, z son coprimos dos a dos.

Definición 1. Una **terna pitagórica** es una 3-tupla $(x, y, z) \in \mathbb{Z}_+^3$ con $(x, y, z) = 1$.

Obsérvese que por motivos de paridad, y eliminando el caso $x \equiv y \equiv z \equiv 0 \mod 2$ por coprimalidad, ha de ser que tanto z como uno de x o y sean impares (para ver que z no puede ser par ha de hacerse módulo 4), así que sin perder generalidad podemos asumir que el único par es y.

Proposición 1. *Se tiene que (x, y, z) es una terna pitagórica (con y par) si y solo si $x = m^2 - n^2$, $y = 2mn$ y $z = m^2 + n^2$ para $m > n > 0$ coprimos y de distinta paridad.*

Demostración. La implicación $\Longleftarrow$ se verifica inmediatamente. Para la contraria, obsérvese que $y^2 = z^2 - x^2 = (x+z)(z-x)$. Estos dos factores sabemos que son pares, es decir $x+z = 2A$ y $z-x = 2B$. En caso de que $p|A, B$ para cierto primo p, se tendría $p|(A + B) = z$ y por tanto, como también $p|x + z$ se tendría $p|x$, contradiciendo la coprimalidad. Entonces, A y B deben ser coprimos, y como $y^2 = 4AB$ se sigue que de hecho $A = m^2$ y $B = n^2$ para ciertos números m, n coprimos. Operando $z + x = 2m^2$ y $z - x = 2n^2$ se obtienen las expresiones deseadas. □

Ahora consideramos el problema de resolver $a^2 = x^2 + y^2$ donde $a \in \mathbb{Z}$ es fijo y $x, y \in \mathbb{Q}^+$. Un método de resolución es poner $y = rx - a$, donde $r \in \mathbb{Q}$. En ese caso, la ecuación queda reducida a una cuadrática en x cuyas soluciones son racionales: $x = \frac{2ra}{r^2+1}$, $y = \frac{(r^2-1)a}{r^2+1}$. Es decir, intersecando estas rectas de pendiente racional y ordenada en el origen $-a$ con la circunferencia de radio a, los puntos tienen coordenadas racionales. Además, si se pone $r = \frac{m}{n}$ y $a = 1$ se recupera el caso de las ternas pitagóricas.

Esto es así porque resolver $x^2 + y^2 = z^2$ en los enteros es lo mismo que $X^2 + Y^2 = 1$ en los racionales. Es decir, buscamos los puntos de coordenadas racionales de la circunferencia unidad. Este conjunto se denota por $C(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\}$. La construcción a continuación permite obtener todo el conjunto a partir de un punto conocido del mismo (en este caso, el $(1, 0)$):

Proposición 2. *Existe una biyección entre $\mathbb{Q}$ y $C(\mathbb{Q}) \setminus P$, donde $P = (1, 0)$.*

Demostración. La biyección consiste en enviar el $r \in \mathbb{Q}$ al punto de intersección de la recta que une $(0, r)$ con P. Este punto, dado que la recta es $Y = (1 - X) \cdot r$, debe verificar $X^2 + (1 - X)^2 \cdot r^2 = 1$, y por tanto se trata del $(\frac{r^2-1}{r^2+1}, \frac{2r}{r^2+1})$. Se comprueba inmediatamente (invirtiendo el proceso) que todo punto de $C(\mathbb{Q}) \setminus P$ proviene de esta construcción. □

Observación 1. En el argumento anterior, $\mathbb{Q}$ se puede reemplazar por cualquier cuerpo K de característica distinta de 2, y cualquier punto $P \in C(K)$. Esto es así porque el polinomio de grado 2 que aparece en la demostración tiene como una de las raíces P, y coeficientes en K, luego la otra raíz también tiene coeficientes en K. De hecho, puede sustituirse C por cualquier cónica irreducible.

En particular, si una cónica irreducible tiene un punto de coordenadas racionales, tiene infinitos.

El problema de las ternas se puede resolver asimismo considerando el anillo de los enteros gaussianos $\mathbb{Z}[i] \subset \mathbb{C}$, donde $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Proposición 3. *El anillo $\mathbb{Z}[i]$ es un dominio euclídeo, siendo la función de grado la norma: $d : \mathbb{Z}[i]\setminus\{0\} \mapsto \mathbb{N}$, dada por $d(a+ib) = a^2+b^2 = (a+ib)(a-ib)$. En particular, es de ideales principales y de factorización única.*

Demostración. Pongamos $\alpha = a + bi$ y $\beta = c + di$. El número $\frac{\alpha}{\beta} \in \mathbb{Q}(i)$ puede expresarse redondeando las partes real e imaginaria al entero más cercano, es decir, poniendo: $\frac{\alpha}{\beta} = (n_1 + s_1) + (n_2 + s_2)i$, donde $n_1, n_2 \in \mathbb{Z}$, $s_1, s_2 \in \mathbb{Q}$ y $|s_i| \leq \frac{1}{2}$. Sea $n = n_1 + in_2$ y $s = s_1 + is_2$. Entonces, la división euclídea viene dada por $\alpha = n\beta + s\beta$, y efectivamente el resto, si $s \neq 0$, cumple $d(s\beta) = d(s)d(\beta) \leq \frac{1}{2}d(\beta) < d(\beta)$. □

Con esto, es fácil resolver el problema pitagórico en este anillo. En primer lugar, se factoriza $z^2 = (x + iy)(x - iy)$. Los elementos $(x + iy)$ y $(x - iy)$ no tienen factores irreducibles comunes, dado que si $\pi|(x + iy)$ y $\pi|(x - iy)$, se tiene $\pi|2x$, y además como $\pi|z^2$ entonces $\pi|z$. Como $2x$ y z son coprimos, se tiene que $2xa + bz = 1$ para ciertos enteros a, b, lo que indicaría que $\pi|1$ y por lo tanto debería ser una unidad, no siendo irreducible entonces.

De ello se deduce que $(x + iy) = u(m + ni)^2$, con $u \in \mathcal{U}(\mathbb{Z}[i])$, es decir, que es un cuadrado perfecto salvo a lo sumo una unidad que se cancele al elevar al cuadrado. De cualquiera de las posibles elecciones de u ($\{1, -1, i, -i\}$) se recuperan las expresiones $x = m^2 - n^2$, $y = 2mn$ y $z = m^2 + n^2$ ya conocidas.

1.2. Último teorema de Fermat y descenso infinito

Este es el último teorema de Fermat:

Teorema 1. *Sea $n \in \mathbb{N}$, $n \geq 3$. No existen soluciones enteras $x, y, z \in \mathbb{Z} \setminus \{0\}$ para $x^n + y^n = z^n$.*

Factorizando n, es fácil ver que basta con probarlo si $n = 4$ o bien $n = p$ primo impar. Demostrar el teorema en su totalidad es muy complicado, pero podemos resolver algún caso sencillo con la técnica del *descenso infinito*. Por ejemplo, el caso $n = 4$ sigue inmediatamente del siguiente resultado:

Proposición 4. *La ecuación $x^4 = y^4 + z^2$ no tiene soluciones enteras no triviales o, equivalentemente, no existen triángulos rectángulos de lados enteros cuya área sea un cuadrado.*

Demostración. Para establecer la equivalencia entre los dos enunciados, consideramos un triángulo pitagórico de lados a, b, c con $(a, b, c) = 1$ (en caso de no ser primitivo, como el área es $A = \frac{ab}{2}$ podría seguir dividiéndose por el factor común y el área seguiría siendo un cuadrado). Ya sabemos que entonces $a = m^2 - n^2$, $b = 2mn$ y $c = m^2 + n^2$ con $m > n > 0$, $(m, n) = 1$, y $m - n$ impar. Entonces, $A = (m^2 - n^2)mn = (m - n)(m + n)mn$, de donde sigue que cada uno de los 4 factores es cuadrado perfecto al ser todos coprimos (esto se comprueba fácilmente usando las propiedades de m y n). Escribimos $m = x^2$, $n = y^2$, $m + n = u^2$, $m - n = v^2$, donde u, v son impares y coprimos. Si definimos $z = uv$, entonces se satisface:

$$z^2 + y^4 = x^4$$

y, recíprocamente, toda solución de esa ecuación permite poner $a = x^4 - y^4$, $b = 2x^2y^2$ y $c = x^4 + y^4$ para obtener un triángulo pitagórico de área cuadrada.

Ahora resta ver que esto no puede darse. Para ello, véase que $2y^2 = y^2 + y^2 = (x^2 - v^2) + (u^2 - x^2) = (u + v)(u - v)$. Como u, v son impares, debe darse $(u + v, u - v) = 2$ (dado que u,v no tiene factores en común, y $u + v$, $u - v$ son pares pero no pueden tener como factores más potencias de 2 dado que entonces su suma, u, sería par). De esa expresión ($2y^2 = (u + v)(u - v)$) se sigue que y ha de ser par y que $\{u + v, u - v\} = \{2r^2, 4s^2\}$. De aquí, $u = r^2 + 2s^2$ y $|v| = r^2 - 2s^2$, y por lo tanto:

$$x^2 = \frac{u^2 + v^2}{2} = (r^2)^2 + (2s^2)^2$$

lo que indica que el triángulo de lados $(r^2, 2s^2, x)$ es pitagórico, y además tiene área: $A = r^2s^2$, cuadrada. No obstante, su hipotenusa es $x < x^4 + y^4 = z$. Iterando el proceso, se obtiene una infinidad de triángulos solución de hipotenusas estrictamente decrecientes, cosa que es imposible que exista dado que las hipotenusas son números enteros. □

1.3. El teorema de Navidad

Lema 1. *Sea p un primo impar. Entonces, $\exists a \in \mathbb{Z}$ con $a^2 \equiv -1 \mod p \iff p \equiv 1 \mod 4$.*

Demostración. Para $\implies$, sabemos del pequeño teorema de Fermat que $1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$, luego $\frac{p-1}{2}$ es par, como se quería. Para $\impliedby$, obsérvese que dado un $b \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, se tiene que o bien $b^{\frac{p-1}{2}} \equiv -1 \mod p$, o bien $b^{\frac{p-1}{2}} \equiv 1 \mod p$, dado que su cuadrado es 1 y $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Además, como los polinomios $X^{\frac{p-1}{2}} \pm 1$ en $\mathbb{Z}/p\mathbb{Z}[X]$ pueden tener a lo sumo $\frac{p-1}{2}$ raíces, sigue que de hecho la mitad de los elementos de $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ verifican la primera congruencia, y la otra mitad la segunda. En cualquier caso, tomando b de tal modo que $b^{\frac{p-1}{2}} \equiv -1 \mod p$, se pone $a = b^k$, donde k es el valor tal que $\frac{p-1}{2} = 2k$, y verifica lo deseado. □

Teorema 2 (De Navidad)**.** *Sea p un primo. Entonces, $\exists a, b \in \mathbb{Z}$ con $a^2 + b^2 = p \iff p = 2$ o bien $p \equiv 1 \mod 4$.*

Demostración. $p = 2$ es inmediato. Ahora, para $\implies$ basta con darse cuenta de que si $p \equiv 3 \mod 4$, entonces $a^2 + b^2 \equiv 0, 1, 2 \mod 4$ así que no puede ser p. Para $\impliedby$, tenemos del lema previo un a con $a^2 \equiv -1 \mod p$, de donde $a^2 + 1 = mp$ para cierto m con $0 < m < p$. A continuación aplicamos descenso para reducir el m hasta 1. Para ello, notamos que $(a, b = 1)$ es solución de $x^2 + y^2 = mp$. Si $m > 1$, elegimos $u \equiv a \mod m$ y $v \equiv b \mod m$, de tal modo que $|u|, |v| \leq \frac{m}{2}$. Esto es posible porque $m > 1$, considerando los representantes módulo m centrados en 0.

Como $a^2 + b^2 = mp$, sigue que $m|a^2 + b^2$, pero también $m|au + bv$, $m|av - bu$ y $m|u^2 + v^2$ (por como se han elegido u y v módulo m). Ahora consideramos la ecuación:

$$(u^2 + v^2)(a^2 + b^2) = (au + bv)^2 + (av - bu)^2.$$

Como se ha explicado, es divisible enteramente por m^2:

$$\left(\frac{u^2 + v^2}{m}\right)\left(\frac{a^2 + b^2}{m}\right) = \left(\frac{au + bv}{m}\right)^2 + \left(\frac{av - bu}{m}\right)^2,$$

pero $\frac{a^2+b^2}{m} = p$. Por tanto, la ecuación se lee como: $kp = a_1^2 + b_1^2$, donde además $k = \frac{u^2+v^2}{m} \leq \frac{m}{2} < m$ por como se escogieron los u, v. Esto decrementa el m y permite iterar hasta que $m = 1$. □

Obsérvese que la prueba es constructiva, es decir, proporciona un algoritmo para obtener la descomposición de p. Este algoritmo primero requiere de encontrar una raíz de -1 en módulo p (para lo cual el lema previo provee otro algoritmo, que consiste en hallar una raíz $\frac{p-1}{2}$-ésima de -1, que la mitad de los elementos lo son, y elevarla al k adecuado). Después, se escribe $a^2 + 1 = mp$ y se toman los u, v del siguiente paso, que además decrecen el valor de m rápidamente.

1.4. Cuerpos ciclotómicos para el último teorema de Fermat

Tras haber demostrado el último teorema de Fermat para $n = 4$, falta demostrarlo para los primos p impares. En concreto vamos a centrarnos en el caso más sencillo en el que $p \nmid x, y, z$, es decir, p no divide a ninguno de los elementos de la terna primitiva.

Observación 2. Si $x^3 + y^3 = z^3$ es una solución primitiva, entonces $3 \mid xyz$.

Demostración. Obsérvese que si $3 \nmid a$, entonces $a^3 \equiv \pm 1 \mod 9$. Entonces, si $3 \nmid xyz$, lo que sucede es que módulo 9 la ecuación toma la forma $\pm 1 + \pm 1 = \pm 1$ lo cual es imposible. □

Esto nos deja el caso en que $p \geq 5$ un primo impar, y que vamos a intentar resolver en los enteros ciclotómicos.

Definición 2. Fijado $p \geq 5$ se denota $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ la p-ésima raíz de la unidad. Recordemos que el polinomio mínimo en $\mathbb{Q}$ es el ciclotómico $\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}$.

Cuando esté claro, se prescindirá del subíndice p.

Observación 3. Si $x^p + y^p = z^p$, se tiene en $\mathbb{Z}[\zeta]$ la factorización:

$$z^p = (x+y)(x+\zeta y)\dots(x+\zeta^{p-1}y).$$

Demostración. Esto sigue de que $X^p - 1 = \Pi_{k=0}^{p-1}(X-\zeta^k)$, poniendo $X = \frac{x}{-y}$ y multiplicando por $(-y)^p$ a ambos lados. □

Proposición 5. *Consideramos la factorización anterior de $x^p + y^p = z^p$. Si $p \nmid xyz$, entonces $(x+\zeta y)$ no comparte factores irreducibles con $(x+\zeta^k y)$ para $k \neq 1$, $0 \leq k \leq p-1$.*

Demostración. Tomamos $\pi \in \mathbb{Z}[\zeta]$ un irreducible que cumpla $\pi | x+\zeta y$, y por tanto $\pi | z^p$. Si se tuviera $\pi | x+\zeta^k y$, entonces, restando, $\pi | y\zeta(1-\zeta^{k-1})$. Como ζ es una unidad (tiene el inverso ζ^{p-1}), entonces asimismo $\pi | y(1-\zeta^{k-1})$, de donde sigue que $\pi | y\Pi_{j=0}^{p-1}(1-\zeta^j) = y\Phi_p(1) = yp$.

No obstante, en $\mathbb{Z}$ se tiene que $(z^p, yp) = 1$ porque $p \nmid z$, luego podemos escribir $az^p + byp = 1$ lo que implicaría $\pi | 1$ contradiciendo irreducibilidad. □

De donde sigue el importante resultado:

Proposición 6. *Consideramos la factorización anterior de $x^p + y^p = z^p$. Si $p \geq 5$ es un primo* ***tal que*** *$\mathbb{Z}[\zeta_p]$* ***es un dominio de factorización única****, así como $p \nmid xyz$, entonces $x + y\zeta = u\alpha^p$ para cierta unidad $u \in \mathcal{U}(\mathbb{Z}[\zeta])$ y $\alpha \in \mathbb{Z}[\zeta]$.*

Demostración. Descomponiendo z^p en factores irreducibles, todos ellos aparecen elevados a p. **Por factorización única**, todos estos factores han de dividir a uno de los elementos de $(x+y)(x+\zeta y)\dots(x+\zeta^{p-1}y)$ (dado que también son primos). En cuanto uno de esos factores π divida a $(x+\zeta y)$, toda la potencia π^p lo divide porque no pueden compartirse factores por la proposición previa. □

Con este resultado ya es posible avanzar en el último teorema de Fermat. Introducimos unas definiciones necesarias:

Definición 3. Dados $\alpha, \beta \in \mathbb{Z}[\zeta]$, se dice que $\alpha \equiv \beta \mod p$ si $\alpha - \beta \in p\mathbb{Z}[\zeta]$.

Obsérvese que esta relación es compatible con la conjugación compleja. Vamos a caracterizar la relación y a mostrar que si $\alpha, \beta \in \mathbb{Z} \subset \mathbb{Z}[\zeta]$, esta coincide con la habitual.

Observación 4. En $\mathbb{Z}[\zeta]$, todo elemento α se escribe de manera única como $a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$, para coeficientes a_j enteros. Con esta escritura, $p|\alpha \iff p|a_j$, $0 \leq j \leq p-2$.

Razón. Esto es porque el grado de la extensión es $p-1$, dicho de otro modo, $\zeta^{p-1} = -1-\zeta-\dots-\zeta^{p-2}$, lo que permite reducir las potencias superiores a $p-2$. La segunda afirmación sigue de que si $\alpha = p\beta$ entonces $a_j = pb_j$ donde (b_j) son los coeficientes de β, dado que $p \in \mathbb{Z}$.

Observación 5. Si (a_j) y (b_j) son los coeficientes de α y β respectivamente en la descomposición anterior, entonces $\alpha \equiv \beta \mod p \iff a_j \equiv b_j \mod p$. En particular, la relación de equivalencia extiende a la de $\mathbb{Z}$.

Razón. Sigue directamente de la segunda afirmación de la observación previa.

Ya solo resta el siguiente resultado para poder demostrar el caso deseado del último teorema de Fermat:

Proposición 7. *Dado $\alpha \in \mathbb{Z}[\zeta]$, se tiene que $\alpha^p \equiv n \mod p$ para un $n \in \mathbb{Z}$.*

Demostración. Como módulo p se cumple que elevar a la p es un homeomorfismo, entonces, si $\alpha = \sum \alpha_k \zeta^k$, se tiene que $\alpha^p = \sum \alpha_k^p \zeta^{kp} = \sum \alpha_k^p$. □

Proposición 8 (Primer caso del último teorema de Fermat)**.** *Sea $p \geq 5$ un primo* ***tal que*** *$\mathbb{Z}[\zeta_p]$* ***es un dominio de factorización única****, y (x,y,z) una solución primitiva de $x^p + y^p = z^p$. Entonces, $p \mid xyz$.*

Demostración. De un resultado previo sabemos que $x+y\zeta = u\alpha^p$, luego, del lema previo, $x+y\zeta \equiv un$ mód p con $n \in \mathbb{Z}$, de donde, conjugando, $x + y\zeta^{p-1} \equiv \bar{u}n \mod p$. Un resultado de Kummer afirma que las unidades de $\mathbb{Z}[\zeta]$ verifican $\frac{u}{\bar{u}} = \zeta^k$ para cierto k, luego podemos escribir

$$x + y\zeta \equiv un \equiv \zeta^k \bar{u}n \equiv (x + y\zeta^{p-1})\zeta^k \equiv x\zeta^k + y\zeta^{k-1},$$

de donde se sigue que $p|[(x + y\zeta) - (x\zeta^k + y\zeta^{k-1})]$.

Continuamos el estudio por casos según el valor de k. Si $k = p$, entonces la igualdad se lee $p|y(\zeta - \zeta^{p-1}) = y(\zeta + 1 + \zeta + \cdots + \zeta^{p-2})$, de donde $p|y + 2y\zeta + y\zeta^2 + \cdots + y\zeta^{p-2}$, que ya está escrita en la *base* de potencias de ζ y por tanto p divide a todos los coeficientes, en particular $p|y$.

Si $k = p-1$, entonces la ecuación pasa a ser $p|x + y\zeta - y\zeta^{p-2} - x(-1 - \zeta - \cdots - \zeta^{p-2})$. Como $p \geq 5$, el término ζ^{p-3} aparece de manera no nula con coeficiente x, luego $p|x$.

Para $1 \leq k \leq p-2$, la ecuación $p|[(x + y\zeta) - (x\zeta^k + y\zeta^{k-1})]$ ya está escrita en la base, y el término constante es, si $k \neq 1$, x, luego $p|x$, y si $k = 1$, es $x - y$, luego $p|x - y$ y por tanto $x \equiv y \mod p$. Pero, en este caso, reaplicando el argumento a $z^p + (-x)^p = y^p$, sigue que $z \equiv -x \mod p$, de donde $2x^p \equiv x^p + y^p \equiv z^p \equiv -x^p \mod p$, luego $p|3x^p$ de donde $p|x$. □

Obsérvese que solo funciona si $\mathbb{Z}[\zeta]$ es un dominio de factorización única, cosa que no siempre ocurre, como en $\mathbb{Z}[\zeta_2 3]$. Esta condición puede relajarse ligeramente atendiendo a los ideales en $\mathbb{Z}[\zeta]$ en lugar de a los elementos en sí, basándose en el siguiente resultado de Dedekind:

Teorema 3 (Dedekind)**.** *Sea $I \subset \mathbb{Z}[\zeta]$ un ideal no vacío. Entonces $I = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r$ de manera única, donde los $\mathfrak{p}_k$ son ideales primos.*

Aquí el producto de ideales denota el ideal formado por sumas finitas de productos de elementos de los ideales. Es decir, $AB = \{\sum_{j\in J, |J|<\infty} a_j b_j : a_j \in A, b_j \in B\}$.

Definición 4. Dados ideales $I, J \subset \mathbb{Z}[\zeta]$, se dice que son equivalentes, $I \sim J$, si $\alpha I = \beta J$ para $\alpha, \beta \in \mathbb{Z}[\zeta]$. El conjunto cociente $\mathfrak{I}/\sim$, donde $\mathfrak{I}$ son todos los ideales, resulta ser un grupo abeliano finito con el producto, donde el neutro es la clase formada por todos los ideales principales.

Definición 5. Se define el **número de clase** de p como $h_p = |\mathfrak{I}/\sim| < \infty$.

Definición 6. Un primo impar p es **regular** si $p \nmid h_p$.

Lo que relaja un poco las condiciones del primer caso del teorema de Fermat que se ha demostrado anteriormente:

Proposición 9. *Sea $p \geq 5$ un primo regular, y (x, y, z) una solución primitiva de $x^p + y^p = z^p$. Entonces, $p \mid xyz$.*

Demostración. Lo único que necesitamos es que $x + y\zeta = u\alpha^p$, que es el único paso que dependía del dominio de factorización única. Partimos de la igualdad de ideales principales: $(z)^p = (x + y)(x + \zeta y) \ldots (x + \zeta^{p-1}y)$, y supongamos que hay un ideal primo $\mathfrak{p}$ que divide a $(x + y\zeta)$ y a otro $(x + y\zeta^k)$ con $k \neq 1$. Entonces, $(x + y\zeta) \subset \mathfrak{p}$ y $(x + y\zeta^k) \subset \mathfrak{p}$, de donde, restando, $y\zeta(1 - \zeta^{k-1}) \in \mathfrak{p}$, y, por ser ζ unidad, entonces $y(1 - \zeta^{k-1}) \in \mathfrak{p}$, de donde $y\Pi_{j=0}^{p-1}(1 - \zeta^j) \in \mathfrak{p}$ y por tanto $y\Phi_p(1) = yp \in \mathfrak{p}$. Como también se tenía que $\mathfrak{p}|(z)^p$, y hay factorización única en los ideales primos (por el resultado anterior de Dedekind), entonces $\mathfrak{p}|(z)$ luego $z \in \mathfrak{p}$ y como además $(py, z) = 1$, entonces $myp + bz = 1 \in \mathfrak{p}$, contradiciendo que $\mathfrak{p}$ sea primo.

Por lo tanto, se tiene que $(x + y\zeta) = I^p$ para cierto ideal I (repitiendo el argumento de la Proposición 6 y usando el teorema de Dedekind para la unicidad). Por tanto, como I^p es principal, en el grupo de clases sigue que $o(I)|p$, pero además $o(I)|h_p$, y como p es regular, entonces forzosamente $o(I) = 1$ así que I es principal, luego $(x + y\zeta) = (\alpha)^p$ y por tanto $x + y\zeta = u\alpha^p$. □

2. Cuerpos de números y anillos de enteros

2.1. Cuerpos de números y números algebraicos

Definición 7. Un **cuerpo de números** es un subcuerpo $K \subset \mathbb{C}$ (por lo tanto, $\mathbb{Q} \subset K$), que verifica $[K : \mathbb{Q}] < \infty$.

Un resultado conocido de la teoría de extensiones de cuerpos es:

Teorema 4 (del elemento primitivo)**.** *Dado un cuerpo de números K, se tiene un $\alpha \in \mathbb{C}$ con $K = \mathbb{Q}(\alpha)$.*

Como veremos posteriormente, los cuerpos de números se relacionan estrechamente con los conocidos como números algebraicos, cuya definición se presenta a continuación.

Definición 8. Se dice que $\alpha \in \mathbb{C}$ es **algebraico** si $\exists P \in \mathbb{Q}[X] \setminus \{0\}$ tal que $P(\alpha) = 0$.

Observación 6. Puede suponerse que P es mónico, dividiendo por su coeficiente principal. Asimismo, si de todos los polinomios mónicos que se anulan en α tomamos uno de grado mínimo, que denotaremos $P_\alpha(X)$, se tiene que este es irreducible.

De lo contrario, escribiríamos $P_\alpha = Q_1 \cdot Q_2$, ambos no constantes, y alguno de ellos debería verificar $Q_i(\alpha) = 0$ por regularidad de $\mathbb{Q}$, de donde se contradice la minimalidad del grado.

Proposición 10. *Dado $\alpha \in \mathbb{C}$ algebraico, se tiene que $P \in \mathbb{Q}[X] \setminus \{0\}$ anula a $\alpha \iff P_\alpha | P$.*

Demostración. $\impliedby$ es evidente, y para $\implies$ basta con poner $P = QP_\alpha + R$ por división euclídea, de donde sigue que $R(\alpha) = 0$ y por minimalidad del grado de P_α debe ser $R = 0$. □

Por tanto, P_α es único y se denomina **polinomio mínimo**.

El siguiente teorema relaciona los cuerpos de números con los números algebraicos:

Proposición 11. *Dado $\alpha \in \mathbb{C}$, equivalen:*

1. *α es algebraico.*
2. *$\mathbb{Q}(\alpha)$ es un cuerpo de números.*
3. *Se tiene un cuerpo de números K con $\alpha \in K$.*

Demostración. Para $1 \implies 2$, sea P el polinomio mínimo de α. Consideremos el cuerpo $K = \frac{\mathbb{Q}[X]}{\langle P \rangle}$, que es un cuerpo por irreducibilidad de P. Se tiene que la aplicación $\overline{x} \mapsto \alpha$ es un isomorfismo de cuerpos con $\mathbb{Q}(\alpha)$ (está bien definido porque envía el $\overline{P(X)}$ al 0 dado que $P(\alpha) = 0$, es inyectivo dado que como P es mínimo, el único elemento que se anula es el ideal generado por P, es decir, el neutro, y es sobreyectivo porque tanto α como $\mathbb{Q}$ están en su imagen).

Para $2 \implies 3$, basta tomar $K = \mathbb{Q}(\alpha)$.

Para $3 \implies 1$, si $\dim K = n$ entonces se tiene que $\{1, \alpha, \ldots, \alpha^n\}$ son linealmente dependientes, de donde $\sum_{j=0}^{n} a_j \alpha^j = 0$ y entonces α anula al polinomio $\sum_{j=0}^{n} a_j X^j$. □

Definición 9. Se define el **cuerpo de los números algebraicos** $\overline{\mathbb{Q}}$ como el conjunto de todos los números algebraicos.

Proposición 12. *Se tiene que $\overline{\mathbb{Q}}$ es un cuerpo algebraicamente cerrado.*

Demostración. Para ver que es un cuerpo, si $\alpha \in \overline{\mathbb{Q}}$, por el resultado previo se tiene $\mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}$ luego en particular $-\alpha$, α^{-1} son algebraicos. Asimismo, dado otro $\beta \in \overline{\mathbb{Q}}$ se tiene que $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \beta)$ es finita (por el resultado previo) y entonces $\alpha + \beta$ y $\alpha\beta$ son algebraicos al pertenecer al cuerpo de números $\mathbb{Q}(\alpha, \beta)$.

Ahora veremos que es algebraicamente cerrado. Sea $P(X) = \sum_j a_j X^j$ un polinomio con $a_j \in \overline{\mathbb{Q}}$. Dado $\gamma \in \mathbb{C}$ con $P(\gamma) = 0$, se tienen las extensiones:

$$\mathbb{Q} \subset \mathbb{Q}(a_0) \subset \mathbb{Q}(a_0, a_1) \subset \cdots \subset \mathbb{Q}(a_0, \ldots, a_n) \subset \mathbb{Q}(a_0, \ldots, a_n, \gamma),$$

todas ellas claramente finitas, de donde $\gamma \in \overline{\mathbb{Q}}$. □

Ahora nos preguntamos si el polinomio mínimo de un número algebraico puede escribirse con sus coeficientes en $\mathbb{Z}$, dado que, si bien puede obtenerse un polinomio con coeficientes en $\mathbb{Z}$ satisfecho por cualquier número algebraico, no está garantizado que este sea mónico, o irreducible. Comenzamos con la siguiente definición:

Definición 10. Dado $\alpha \in \overline{\mathbb{Q}}$, si existe un polinomio mónico (irreducible o no) $P(X) \in \mathbb{Z}[X]$ que verifica $P(\alpha) = 0$, se dice que α es un **entero algebraico**.

Por ejemplo, los enteros, las raíces cuadradas de enteros o las raíces de la unidad son enteros algebraicos. La definición puede cambiarse por una equivalente en virtud del siguiente lema:

Lema 2 (Gauss)**.** *Sea $f \in \mathbb{Z}[X]$ un polinomio mónico que descompone como $f = gh$ con $g, h \in \mathbb{Q}[X]$, ambos mónicos. Se tiene entonces que $g, h \in \mathbb{Z}[X]$.*

Demostración. Sean $m_0 = \text{mín}\{m \in \mathbb{N} : mg \in \mathbb{Z}[X]\}$ y $n_0 = \text{mín}\{n \in \mathbb{N} : nh \in \mathbb{Z}[X]\}$. Se afirma que $m = n = 1$. En caso contrario, suponemos que $m_0 > 1$ y $p | m_0$ es un divisor suyo. La observación clave es que $[m_0 g], [n_0 h] \neq 0$ en $\mathbb{Z}/p\mathbb{Z}$. Esto es así porque, por un lado, si p dividiera todos los coeficientes de $m_0 g$, entonces $\frac{m_0}{p} g \in \mathbb{Z}[X]$ y $\frac{m_0}{p}$ es un entero menor que m_0, contradiciendo su minimalidad. Por otro lado, si p dividiera todos los coeficientes de $n_0 h$, entonces $\frac{n_0}{p} h \in \mathbb{Z}[X]$ y $\frac{n_0}{p}$ es un entero menor que n_0, dado que como g era mónico, n_0 es el coeficiente de mayor grado (luego p lo divide), y esto contradice la minimalidad de n_0. Sigue entonces la igualdad absurda en $\mathbb{Z}/p\mathbb{Z}[X]$: $0 = [m_0 n_0 f] = [m_0 g][n_0 h] \neq 0$. □

Del lema se obtienen este corolario relevante:

Observación 7. El número algebraico $\alpha \in \overline{\mathbb{Q}}$ es un entero algebraico si y solo si su polinomio mínimo, $P_\alpha(X)$, tiene coeficientes enteros. En particular, los únicos enteros algebraicos que hay en $\mathbb{Q}$ son los elementos de $\mathbb{Z}$.

Razón. Esto es así porque si α es un entero algebraico, anula a un polinomio $P \in \mathbb{Z}[X]$, y se puede poner $P = Q \cdot P_\alpha(X)$ y aplicar el lema previo.

Es posible caracterizar los enteros algebraicos de una manera similar a la conocida para números algebraicos:

Teorema 5. *Dado $\alpha \in \mathbb{C}$, son equivalentes:*

1. *α es un entero algebraico.*
2. *El anillo $\mathbb{Z}[\alpha]$ verifica que $(\mathbb{Z}[\alpha], +)$ es un grupo abeliano finitamente generado.*
3. *Hay un anillo $R \subset \mathbb{C}$ con $\alpha \in R$ que verifica que $(R, +)$ es un grupo abeliano finitamente generado.*
4. *Hay un subgrupo $G < (\mathbb{C}, +)$ que es abeliano y finitamente generado, que cumple $\alpha G \subset G$.*

Demostración. Para $1 \implies 2$, se tiene que $\sum_{j=0}^{n} a_j \alpha^j = 0$, donde $\alpha_j \in \mathbb{Z}$ y $\alpha_n = 1$, de donde se tiene que $\alpha^n = -\sum_{j=0}^{n-1} a_j \alpha^j$ y por lo tanto $(\mathbb{Z}[\alpha], +) = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$. Para $2 \implies 3$ basta con tomar $R = \mathbb{Z}[\alpha]$. Para $3 \implies 4$ basta con tomar $G = (R, +)$.

Para $4 \implies 1$, escribimos $G = \langle a_1, \ldots, a_n \rangle$. Como $\alpha G \subset G$, se tiene que $\alpha a_j = \sum_{i=1}^{n} n_{ij} a_i$, donde $n_{ij} \in \mathbb{Z}$. Así, la matriz $A = \alpha \cdot I_n - (n_{ij})_{i,j}$ verifica que $A \cdot (a_1, \ldots, a_n)^t = 0$, por lo que, al tener núcleo no trivial, fuerza que $0 = \det A = P(\alpha)$, donde $P(X) = \det(X \cdot I_n - (n_{ij})_{i,j}) \in \mathbb{Z}[X]$, como se quería. □

Teorema 6. *Sea $A \subset \mathbb{C}$ el conjunto de los enteros algebraicos. Se tiene que A es un anillo.*

Demostración. Como $\mathbb{Z} \subset A$, solo hace falta probar que si $\alpha, \beta \in A$, entonces $\alpha\beta$ y $\alpha + \beta \in A$. Por el teorema previo, podemos escribir $\mathbb{Z}[\alpha] = \langle 1 = \gamma_0, \gamma_1, \ldots, \gamma_n \rangle_+$, donde el subíndice + enfatiza que está siendo considerado como grupo abeliano con la suma. Del mismo modo, $\mathbb{Z}[\beta] = \langle 1 = \delta_0, \ldots, \delta_m \rangle_+$, pero entonces sigue que $\mathbb{Z}[\alpha, \beta] = \langle \{\Pi \gamma_i \delta_j\} \rangle_+$, y por el punto 3 del teorema previo, se tiene lo que se quería. □

Definición 11. Sea K un cuerpo de números. Se define el **anillo de enteros de** K como $\mathcal{O}_K = K \cap A$, donde A es el anillo de enteros algebraicos.

Por ejemplo, en virtud de la observación 7, sigue que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Proposición 13. *Sea K un cuerpo tal que $[K : \mathbb{Q}] = 2$ y, por lo tanto, $K = \mathbb{Q}(\sqrt{d})$ donde d es un entero libre de cuadrados. Se tiene entonces:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, & d \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\}, & d \equiv 1 \mod 4 \end{cases}$$

Demostración. Sea $\alpha = r + s\sqrt{d}$ un elemento arbitrario de $\mathbb{Q}(\sqrt{d})$. Encontraremos su polinomio mínimo para ver cuándo es de coeficientes enteros. Tenemos que $(\alpha - r)^2 = s^2 d$, de donde se tiene que el mínimo es $X^2 - 2rX + r^2 - s^2 d$. Por tanto, hace falta que $2r, r^2 - s^2 d \in \mathbb{Z}$. Esto fuerza que $r = \frac{n}{2}$, con $n \in \mathbb{Z}$, luego $\frac{n^2}{4} - s^2 d \in \mathbb{Z}$, lo que implica que $s^2 d = \frac{n^2 - 4K}{4}$ con $K \in \mathbb{Z}$. Como d es libre de cuadrados, es necesario entonces (para que aparezca el denominador 4), que $s = \frac{m}{2}$ con $m \in \mathbb{Z}$.

Por tanto, $\alpha = \frac{m+n\sqrt{d}}{2}$ con $\frac{m^2}{4} d = \frac{n^2 - 4K}{4}$. Reordenando, se llega a que $m^2 d - n^2 \equiv 0 \mod 4$. De este modo, si m es par, hace falta $n^2 \equiv 0 \mod 4$ luego n es par, y si m es impar, hace falta que $d \equiv n^2 \mod 4$. En este caso, n no puede ser par, o $d \equiv 0 \mod 4$ contradiciendo que sea libre de cuadrados, por tanto debe ser $d \equiv 1 \mod 4$ y n impar. Estos pasos son reversibles, es decir, que si n, m son pares entonces los coeficientes del mínimo son enteros, y si n, m son impares y $d \equiv 1 \mod 4$ también (esto es verificable de inmediato en la expresión encontrada previamente para el mínimo), luego hemos acabado. □

Definición 12. Sea $\alpha \in \overline{\mathbb{Q}}$. Las raíces de su polinomio mínimo, $P_{\alpha,\mathbb{Q}}(X)$, se denominan **conjugados de** α.

Observación 8. Hay exactamente $\deg P_{\alpha,\mathbb{Q}}$ conjugados de α distintos.

Esto es así porque si $P_{\alpha,\mathbb{Q}} := P$ tuviera una raíz doble β, entonces $P'(\beta) = 0$, de donde $P | P'$, lo cual no es posible porque $\deg P' < \deg P$ y $P' \neq 0$. (Nótese que en otros cuerpos de característica no nula es posible que $P' = 0$, y esto no sería cierto).

Proposición 14. *Sea K un cuerpo de números con $[K : \mathbb{Q}] = n$. Entonces existen n inmersiones distintas, $\sigma_1, \ldots, \sigma_n$, donde $\sigma_j : K \mapsto \mathbb{C}$ son homomorfismos de cuerpos.*

Demostración. Escribimos $K = \mathbb{Q}(\alpha)$, por el teorema del elemento primitivo. Como $K \simeq \mathbb{Q}[X] / \langle P_{\alpha,\mathbb{Q}} \rangle$ mediante el único homomorfismo definido por $\alpha \mapsto \overline{X}$, para definir morfismos de K en $\mathbb{C}$ es necesario y suficiente escoger la imagen de $\overline{X}$ como un β que verifique $P_{\alpha,\mathbb{Q}}(\beta) = 0$, es decir, cada uno de los conjugados da lugar a un homomorfismo distinto. □

Observación 9. En el caso del resultado anterior, si escogemos un $\alpha \in K$ con $\mathbb{Q}(\alpha) \subsetneq K$, se tiene entonces la cadena $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$, donde la primera extensión es de grado $d | n$ y la segunda de grado $\frac{n}{d}$. De este modo, existen d inmersiones $\{\sigma_i\}_{i=1}^d$ de $\mathbb{Q}(\alpha)$ en $\mathbb{C}$.

Tras esto, es posible escribir $K = \mathbb{Q}(\alpha)(\beta)$, con β de grado $\frac{n}{d}$ sobre $\mathbb{Q}(\alpha)$, dando lugar a $\frac{n}{d}$ inmersiones de K en $\mathbb{C}$ que extienden a σ_i para i fijo (mediante conjugados de β), para recuperar las $d \cdot \frac{n}{d} = n$ inmersiones únicas.

Definición 13. Las inmersiones $\sigma : K \mapsto \mathbb{C}$ con $\sigma(K) \subset \mathbb{R}$ se denominan **inmersiones reales**. En caso contrario, son **inmersiones imaginarias**.

El número de inmersiones reales de una extensión K con $[K : \mathbb{Q}] = n$ se suele denotar por r, y el número de inmersiones imaginarias por $2s$ (véase que ha de ser par dado que es posible postcomponer la conjugación con cualquiera de ellas para obtener otra). Evidentemente, $2s + r = n$.

Definición 14. Sea K un cuerpo de números de grado $[K : \mathbb{Q}] = n$. Se define la **traza de la extensión** como la aplicación $T : K \mapsto \mathbb{Q}$ dada por $T(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$, y la **norma de la extensión** como la aplicación $N : K \mapsto \mathbb{Q}$ dada por $N(\alpha) = \sigma_1(\alpha) \cdot \cdots \cdot \sigma_n(\alpha)$.

En ambos casos, $\{\sigma_j\}_{j=1}^n$ son las únicas n inmersiones de K en $\mathbb{C}$.

Nótese que la definición depende fuertemente del cuerpo K y el cuerpo base $\mathbb{Q}$, es decir, no está bien definido hablar de *la norma de un elemento* sin establecer estos cuerpos.

Proposición 15. *Se tiene en el contexto anterior que:*

1. $T(\alpha + \beta) = T(\alpha) + T(\beta)$
2. $N(\alpha\beta) = N(\alpha)N(\beta)$
3. $T(q) = nq$ *y* $N(q) = q^n$ *para* $q \in \mathbb{Q}$.

Demostración. 1 y 2 son inmediatas de la definición. Para 3 basta con observar que los σ_j fijan los racionales al ser homomorfismos de cuerpos. □

Proposición 16. *Se tiene efectivamente que* $T(\alpha), N(\alpha) \in \mathbb{Q}$*, y si* $\alpha \in \mathcal{O}_K$*, entonces* $T(\alpha), N(\alpha) \in \mathbb{Z}$.

Demostración. Si α es de grado n, es decir, $K = \mathbb{Q}(\alpha)$, entonces su polinomio mínimo tiene grado n y es $P(X) = \Pi_{j=1}^n (X - \sigma_i(\alpha))$, luego la norma y la traza aparecen en los coeficientes de grado 0 y $n - 1$ de P, respectivamente, garantizando lo que se quiere probar. Si no, entonces se tiene la cadena $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$, de grados d y $\frac{n}{d}$. Por la discusión realizada en la observación 9, si $\{\tau_i\}$ son las d inmersiones de $\mathbb{Q}(\alpha)$, los valores $\tau_i(\alpha)$ aparecen cada uno $\frac{n}{d}$ veces en el listado de los $\sigma_i(\alpha)$. Por tanto, sigue que $T_K(\alpha) = \frac{n}{d} T_{\mathbb{Q}(\alpha)}(\alpha)$, y $N_K(\alpha) = (N_{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}$, y puede aplicarse el caso anterior. □

2.2. Cuerpos ciclotómicos

Definición 15. El **cuerpo ciclotómico** de orden n es $\mathbb{Q}(\zeta_n)$, con $\zeta_n = e^{\frac{2\pi i}{n}}$. El polinomio mínimo de ζ_n se denomina **polinomio ciclotómico de orden** n y se denota $\Phi_n(X)$.

Ya sabemos que $\Phi_p(X) = \frac{X^p - 1}{X - 1}$. El siguiente resultado caracteriza el resto:

Proposición 17. *Se tiene que* $X^m - 1 = \Pi_{d|m} \Phi_d(X)$*, de donde* $\Phi_m(X) = \frac{X^m - 1}{\Pi_{d|m, d<m} \Phi_d(X)}$*. En particular, el grado de la extensión ciclotómica de grado* m *es* $\varphi(m)$.

Demostración. Por inducción en m. Si $m = 1$ o $m = p$ primo, el resultado es inmediato. Ahora, por hipótesis de inducción se tiene que $\deg \frac{X^m - 1}{\Pi_{d|m, d<m} \Phi_d(X)} = m - \Pi_{d|m, d<m} \Phi_d(X) = \varphi(m)$, para lo que se ha usado también el hecho de que $m = \sum_{d|m} \varphi(d)$. Para acabar la prueba, mostraremos que ζ_m tiene $\varphi(m)$ conjugados, lo que garantiza que ese sea su mínimo.

En concreto, se afirma que ζ_m^k es conjugado de ζ_m en el m-ésimo cuerpo ciclotómico si y solo si $(m, k) = 1$. En efecto, si $(m, k) = d > 1$, entonces $(\zeta_m^k)^{\frac{m}{d}} = 1$, luego ζ_m^k es una raíz de $X^{\frac{m}{d}} - 1$, no satisfecho por ζ_m luego no es conjugado. Ahora queda ver que si $(m, k) = 1$, ζ^k sí es conjugado. Para ello, mostraremos que $\Phi_m(\zeta_m^k) = 0$, para lo que basta mostrar que si $p \nmid m$, entonces $\Phi_m(\theta) = 0 \implies \Phi_m(\theta^p) = 0$, e iterar en los divisores de k.

Para esto último, escribimos $X^m - 1 = \Phi_m \cdot g$, ambos en $\mathbb{Z}[X]$ y mónicos por el lema de Gauss. Como $\theta^m - 1 = \Phi_m(\theta)g(\theta) = 0 \cdot g(\theta) = 0$, se tiene $\theta^m = 1$, y por tanto: $0 = \theta^{pm} - 1 = \Phi_m(\theta^p)g(\theta^p)$. Para acabar solo hay que ver que $g(\theta^p) \neq 0$. Si lo fuese, entonces $\Phi_m | g(X^p)$ (porque este último anula a θ), y entonces, módulo p, se tiene $\overline{\Phi_m}|\overline{g}(X)^p$, donde se usa que elevar a p es un homomorfismo módulo p. De ahí sigue que $\overline{\Phi_m}$ y $\overline{g}$ tienen un factor común h, luego $h^2|\overline{\Phi_m}\overline{g} = \overline{X^m - 1}$. Esto supone que $\overline{X^m - 1}$ tiene una raíz doble, es decir compartida con su derivada $\overline{mX^{m-1}}$. Como $p \nmid m$, entonces $\overline{m} \neq 0$ luego la única tal raíz es 0, que no anula $X^m - 1$, contradicción. □

2.3. Discriminantes

Definición 16. Sea K un cuerpo de números con $|K : \mathbb{Q}| = n$ y sean $\sigma_1, \ldots, \sigma_n : K \mapsto \mathbb{C}$ las n inmersiones correspondientes. Dados $\alpha_1, \ldots, \alpha_n \in K$, se define como sigue su **discriminante:**

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i(\alpha_j))_{i,j})^2$$

Proposición 18. *Se tiene en el contexto de la definición previa que, si T es la traza de K sobre $\mathbb{Q}$, entonces* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det((T(\alpha_i\alpha_j))_{i,j})$.

Demostración. Calculamos el discriminante como $\det((\sigma_j)(\alpha_i) \cdot (\sigma_i(\alpha_j)))$, pero esa matriz tiene como entrada r, s el valor: $\sum_{k=1}^n \sigma_k(\alpha_r)\sigma_k(\alpha_s) = \sum_{k=1}^n \sigma_k(\alpha_r\alpha_s) = T(\alpha_r\alpha_s)$. □

Teorema 7. *Se tiene que* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0 \iff \{\alpha_1, \ldots, \alpha_n\}$ *son linealmente independientes sobre* $\mathbb{Q}$.

Demostración. Para $\Longleftarrow$, pongamos que $\sum_j q_j\alpha_j = 0$ para $q_j \in \mathbb{Q}$ no todos nulos. Entonces $0 = \sigma_i(\sum_j q_j\alpha_j) = \sum_j q_j\sigma_i(\alpha_j)$, de donde sigue que $(\sigma_i(\alpha_j)_{i,j}) \cdot (q_j)_j = 0$, por tanto la matriz tiene núcleo no trivial y determinante 0, como se quería.

Para $\Longrightarrow$, se razona por contradicción. Supongamos que $\alpha_1, \ldots, \alpha_n$ son linealmente independientes con discriminante nulo. Entonces, hay racionales no todos nulos $q = (q_1, \ldots, q_n)^t$ tales que $q \cdot (T(\alpha_i\alpha_j))_{i,j} = 0$ (dada la proposición anterior). Si llamamos F_i a las filas de la matriz $(T(\alpha_i\alpha_j))_{i,j}$, eso quiere decir que $\sum_i F_i q_i = 0$, luego, como T es $\mathbb{Q}$-lineal, sigue que $0 = T(\sum_i q_i\alpha_i)\alpha_j$. Llamando $\alpha = (\sum_i q_i\alpha_i)$, que es no nulo por independencia lineal de los α_i, sigue entonces que $0 = T(\alpha\alpha_j)$ para todos los j. Como los $\{\alpha_j\}_j$ forman base de K sobre $\mathbb{Q}$ por ser linealmente independientes, también lo hacen $\{\alpha\alpha_j\}_j$, y como T es $\mathbb{Q}$-lineal esto implica que $T \equiv 0$, contradiciendo que $T(1) = n$. □

Proposición 19. *Supongamos que $K = \mathbb{Q}(\alpha)$ con grado n sobre $\mathbb{Q}$. Sea $f = P_{\alpha,\mathbb{Q}}$ el polinomio mínimo. Sean $\{\alpha_1, \ldots, \alpha_n\}$ los conjugados de α. Se tiene la siguiente expresión para el discriminante de las potencias de α:*

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{r<s}(\alpha_r - \alpha_s)^2 = \pm N(f'(\alpha)),$$

donde el signo final es positivo si y solo si $n \equiv 0, 1 \mod 4$.

Demostración. $\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2 = \det(\sigma_i(\alpha)^j)^2 = \prod_{r<s}(\alpha_r - \alpha_s)^2$ usando la identidad de Vandermonde. Por otro lado, sabemos que $f(X) = \prod(X - \alpha_j)$, luego $f'(X) = \sum_{k=1}^n \prod_{s\neq k}(X - \alpha_s)$. Evaluando, $f'(\alpha_r) = \prod_{s\neq r}(\alpha_r - \alpha_s)$. Por tanto, $N(f'(\alpha)) = \prod_{r=1}^n \prod_{s\neq r}(\alpha_r - \alpha_s) = \pm\prod_{r<s}(\alpha_r - \alpha_s)^2$.

El signo aparece porque, si $r < s$, en el producto inicial se tienen $(\alpha_r - \alpha_s)$ y $(\alpha_s - \alpha_r)$, es decir, hay que revertir por cada elección de r y s uno de los dos términos de la pareja. Hay $\binom{n}{2}$ tales emparejamientos, es decir, $\frac{n(n-1)}{2}$, que es par precisamente cuando $n \equiv 0, 1 \mod 4$. □

Observación 10. En el caso del cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$ para p un primo impar, se tiene $\operatorname{disc}(1, \zeta, \ldots, \zeta^{p-2}) = \pm p^{p-2}$ con las mismas reglas para el signo que en la proposición previa. Esto se puede observar utilizando $\frac{X^p-1}{X-1}$ como polinomio mínimo en lo anterior.

En adelante, cuando $K = \mathbb{Q}(\alpha)$, con grado n, denotaremos $\text{disc}(\alpha) = \text{disc}(1, \alpha, \ldots, \alpha^{n-1})$.

Proposición 20. *Se tiene que* $\text{disc}(\zeta_m) | m^{\varphi(m)}$ *para cualquier* $m \in \mathbb{Z}$.

Demostración. Sea $f(X) = \Phi_m(X)$ el mínimo de ζ_m. Sabemos que hay un polinomio mónico de coeficientes enteros g que cumple $X^m - 1 = fg$, de tal manera que, derivando, $mX^{m-1} = f'g + gf'$. Evaluando, se tiene que $m\zeta_m^{m-1} = f'(\zeta_m)g(\zeta_m)$, es decir, que $m = f'(\zeta_m)g(\zeta_m)\zeta_m$. Tomando normas, sigue que $m^{\varphi(m)} = \pm \text{disc}(\zeta_m) \cdot N(g(\zeta_m)\zeta_m)$, donde esa norma es un entero por tomarse a un elemento de $\mathbb{Z}[\zeta_m]$, luego hemos acabado. □

2.4. Estructura aditiva de los enteros

El objetivo es estudiar el grupo $(\mathcal{O}_K, +)$.

Definición 17. El grupo abeliano G es un grupo **abeliano libre con** n **generadores** si se tienen elementos $\{a_1, \ldots, a_n\} \subset G$ tales que $G = \{\sum m_i a_i : m_i \in \mathbb{Z}\}$. Es decir, $G = \bigoplus a_i\mathbb{Z} \simeq \mathbb{Z}^n$. En este contexto, los elementos $\{a_1, \ldots, a_n\}$ se conocen como *base* del grupo abeliano libre.

Se tiene el siguiente resultado de teoría de grupos:

Proposición 21. *Si* G *es abeliano libre en* n *generadores y* $H < G$ *es un subgrupo, entonces* H *es abeliano libre en* $r \leq n$ *generadores.*

Puede darse el caso de que $r = n$ incluso aunque $H \subsetneq G$.

Proposición 22. *Si* $A \subset B \subset C$ *son grupos abelianos y* A, C *son libres con* n *generadores, entonces* B *también.*

Demostración. Ya sabemos que B es libre con $r \leq n$ generadores aplicando el resultado previo a $B \subset C$. Si se aplica ahora a $A \subset B$, sigue que $r \geq n$ luego $r = n$. □

Proposición 23. *Sea* $\alpha \in \overline{\mathbb{Q}}$ *un número algebraico. Entonces,* $\exists d \in \mathbb{Z}$ *que verifica que* $d\alpha \in \mathcal{O}_{\overline{\mathbb{Q}}}$*, es decir, es un entero algebraico.*

Demostración. Sea $X^n + \sum_j^{n-1} q_j X^j$ el mínimo de α. Si d es el mínimo común denominador de los q_j, entonces se tiene, multiplicando por d^n, que $(dX)^n + \sum_j^{n-1} q_j (dX)^j d^{n-j}$ es un polinomio mónico en dX con coeficientes en $\mathbb{Z}$, que se satisface cuando $X = \alpha$ y por tanto $d\alpha$ es un entero algebraico. □

Observación 11. Por tanto, dada una base $\{\alpha_1, \ldots, \alpha_n\}$ de $K/\mathbb{Q}$ una extensión de grado n, puede suponerse de enteros algebraicos dado que, si no, es posible obtener otra $\{d_1\alpha_1, \ldots, d_n\alpha_n\}$ por la proposición previa.

Suponiendo ahora que $\{\alpha_1, \ldots, \alpha_n\}$ es de enteros algebraicos, entonces en particular todas las sumas finitas realizadas con esos elementos son enteros algebraicos de K (porque $\mathcal{O}_K$ es un anillo), y por tanto $\bigoplus \alpha_j\mathbb{Z} \subset \mathcal{O}_K$.

Ahora se quiere encontrar otro grupo abeliano libre de n generadores que contenga a $\mathcal{O}_K$, para poder afirmar asimismo que $\mathcal{O}_K$ es abeliano libre en n generadores.

Proposición 24. *Sea* $\{\alpha_1, \ldots, \alpha_n\}$ *una base de* $K/\mathbb{Q}$ *compuesta por enteros algebraicos. Entonces, cualquier entero algebraico* $\alpha \in \mathcal{O}_K$ *admite la expresión:*

$$\alpha = \frac{\sum_{j=1}^n m_j \alpha_j}{d},$$

donde $d = \text{disc}(\alpha_1, \ldots, \alpha_n)$ *y además* $d \mid m_i^2$.

Por tanto, $\mathcal{O}_K \subset \bigoplus \frac{\alpha_j}{d}\mathbb{Z}$*, deduciéndose así (junto con la observación previa) que* $\mathcal{O}_K$ *es un grupo abeliano libre en* n *generadores.*

Demostración. Escribimos $\alpha = \sum x_j \alpha_j$ donde cada $x_j \in \mathbb{Q}$. Si $\sigma_1, \dots, \sigma_n$ son las inmersiones de K, entonces $\sigma_i(\alpha) = \sum x_j \sigma_i(\alpha_j)$, es decir:

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

donde $M = (\sigma_i(\alpha_j))_{i,j}$. Sabemos de un resultado de Cramer que $x_j = \frac{y_j}{\delta}$, donde $\delta = \det M$ y $y_j = \det M_j$, donde M_j surge de sustituir la j-ésima columna de M por $\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}$.

Entonces, sigue que $x_j = \frac{\delta y_j}{\delta^2} = \frac{\delta y_j}{d}$, luego basta con ver que $\delta y_j \in \mathbb{Z}$. Pero como $d \in \mathbb{Z}$ por ser enteros algebraicos los α_j, se tiene que $\delta y_j = d \cdot x_j \in \mathbb{Q}$, y además tanto δ como y_j son enteros algebraicos por ser determinantes de matrices en enteros algebraicos. Se sigue entonces que $\delta y_j \in \mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

Finalmente, para ver que d divide al cuadrado, basta con ver que $(y_j \delta)^2 = y_j^2 d$, y $y_j^2 \in \mathbb{Z}$ (al ser el discriminante de $\{\alpha_1, \dots, \alpha_{j-1}, \alpha, \alpha_{j+1}, \dots, \alpha_n\}$), luego se tiene lo que se quería. □

Definición 18. Una **base entera** de K son $\{\alpha_1, \dots, \alpha_n\} \subset \mathcal{O}_K$ que forman base del grupo abeliano libre $\mathcal{O}_K$.

Observación 12. Si $\{\alpha_1, \dots, \alpha_n\}$ es una base entera de K, es asimismo una base de K como $\mathbb{Q}$-espacio. Esto es así porque si $\beta \in K$, entonces sabemos que hay un entero con $d\beta \in \mathcal{O}_K$, luego $d\beta = \sum m_j \alpha_j$ y por tanto $\beta = \sum \frac{m_j}{d} \alpha_j$.

El recíproco en general es falso, como se puede comprobar con $K = \mathbb{Q}(\sqrt{d})$ con $d \equiv 1 \mod 4$, cuyo anillo de enteros es $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Este conjunto con la suma resulta ser un grupo abeliano libre para la base $\{1, \frac{1+\sqrt{d}}{2}\}$, y se tiene que el conjunto $\{1, \sqrt{d}\}$ es una base de enteros algebraicos de K que por el contrario no es una base entera (porque el grupo abeliano libre en esa base es $\mathbb{Z}[\sqrt{d}]$).

Definición 19. Dado un cuerpo K con $|K : \mathbb{Q}| = n$, se define $\operatorname{disc}(K) = \operatorname{disc}(\alpha_1, \dots, \alpha_n) := \Delta_K$, donde $\{\alpha_1, \dots, \alpha_n\}$ es una de las bases enteras de K.

Vamos a ver que está bien definido. Para ello:

Proposición 25. *Sea $\{\alpha_1, \dots, \alpha_n\} \subset K$ una base como $\mathbb{Q}$-espacio vectorial de K. Sean $\{\beta_1, \dots, \beta_n\} \subset K$. Es posible escribir, entonces, $\begin{pmatrix} \beta_1 \\ \dots \\ \beta_n \end{pmatrix} = M \cdot \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix}$ con M una matriz $n \times n$ de entradas en $\mathbb{Q}$. Se tiene:*

$$\operatorname{disc}(\beta_1, \beta_2, \dots, \beta_n) = (\det M)^2 \operatorname{disc}(\alpha_1, \alpha_2, \dots, \alpha_n)$$

Demostración. Se debe a que las inmersiones σ_i son $\mathbb{Q}$-lineales y, por tanto, también se tiene $\begin{pmatrix} \sigma_i(\beta_1) \\ \dots \\ \sigma_i(\beta_n) \end{pmatrix} = M \cdot \begin{pmatrix} \sigma_i(\alpha_1) \\ \dots \\ \sigma_i(\alpha_n) \end{pmatrix}$. Entonces, si M_β y M_α son las respectivas matrices cuyo determinante cuadrado es el discriminante, sigue que $M_\beta = M \cdot M_\alpha$ y el resultado es inmediato. □

Proposición 26. *Sea $A = \{\alpha_1, \dots, \alpha_n\} \subset K$ una base entera de K. Sean $B = \{\beta_1, \dots, \beta_n\} \subset \mathcal{O}_K$. Es posible escribir, entonces, $\begin{pmatrix} \beta_1 \\ \dots \\ \beta_n \end{pmatrix} = M \cdot \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix}$, con M una matriz $n \times n$ de entradas en $\mathbb{Z}$. Equivalen:*

1. *B es base entera.*
2. *M es invertible en $\mathbb{Z}$.*
3. $\det(M) = \pm 1$.
4. $\operatorname{disc}(B) = \operatorname{disc}(A)$.

Asimismo, equivalen:

5. *B es $\mathbb{Q}$-base de K.*
6. $\det(M) \neq 0$.
7. $|\operatorname{disc}(B)| \geq |\operatorname{disc}(A)|$.

Demostración. Para 1 $\implies$ 2, si B es base entera entonces se puede poner también $\begin{pmatrix}\alpha_1\\ \dots \\ \alpha_n\end{pmatrix} = M_2 \cdot \begin{pmatrix}\beta_1\\ \dots \\ \beta_n\end{pmatrix}$, con M_2 una matriz cuyas entradas son enteras, y por lo tanto $M_2 \cdot M = I$. Ahora, 2 $\implies$ 3 sigue de un resultado conocido en teoría de anillos que afirma que M en el anillo de matrices $\mathcal{M}_n(R)$, con R un dominio, es invertible si y solo si $\det(M) \in \mathcal{U}(R)$. Para 3 $\implies$ 4 basta con usar la proposición previa. Por otra parte, para 4 $\implies$ 1, basta con ver que por el resultado previo, sigue que $\det(M) = \pm 1$, dado que además es entero, luego M es invertible y se puede poner $\begin{pmatrix}\alpha_1\\ \dots \\ \alpha_n\end{pmatrix} = M^{-1} \cdot \begin{pmatrix}\beta_1\\ \dots \\ \beta_n\end{pmatrix}$ así que B es base entera (porque A lo era y M^{-1} tiene coeficientes en $\mathbb{Z}$.

Para 5 $\implies$ 6, se tiene de la proposición previa que $\operatorname{disc}(B) \neq 0$ y ya hemos establecido que esto implica la independencia lineal de B. Para 6 $\implies$ 7, basta con usar la proposición previa. Finalmente, para 7 $\implies$ 5 basta con ver que, por la proposición previa, $\det(M) \neq 0$ luego $\operatorname{disc}(B) \neq 0$. □

De este resultado sigue que el discriminante está bien definido. Una observación:

Observación 13. Si, en el contexto de la proposición anterior, $\operatorname{disc}(B)$ es libre de cuadrados, entonces es base entera.

Esto es así porque entonces, como $\operatorname{disc}(B) = \det(M)^2 \operatorname{disc}(A)$, sigue que $\operatorname{disc}(M) = \pm 1$, o si no no sería libre de cuadrados.

A continuación vamos a calcular el anillo de enteros de $\mathbb{Q}(\zeta)$ donde ζ es una raíz m-ésima de la unidad. En concreto, lo demostraremos para $m = p^l$ una potencia de primo. Para ello son necesarios algunos resultados:

Lema 3. *Se tiene, si ζ es una raíz p^l-ésima de la unidad primitiva con p primo, que en $\mathbb{Q}(\zeta)$ se cumple $N(1-\zeta) = p$*

Demostración. $N(1-\zeta) = \prod_{p \nmid k}(1-\zeta^k) = \Phi_{p^l}(1)$. No obstante, sabemos que $\Phi_{p^l}(X) = \frac{X^{p^l}-1}{X^{p^{l-1}}-1} = (X^{p^{l-1}})^{p-1} + (X^{p^{l-1}})^{p-2} + \cdots + 1$, luego $\Phi_{p^l}(1) = p$. □

Lema 4. *Se tiene, si ζ es una raíz p^l-ésima de la unidad primitiva con p primo, que $\frac{p}{(1-\zeta)^i} \in \mathbb{Z}[\zeta]$, para cualquier i con $0 \leq i \leq [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p^l)$.*

Demostración. En $\mathbb{Z}[\zeta]$ se cumple $(1-\zeta)|(1-\zeta^k)$ para cualquier $k \geq 1$, dado que $(1-\zeta^k) = (1-\zeta)(1+\zeta+\cdots+\zeta^{k-1})$. Por tanto: $\frac{p}{(1-\zeta)^{\varphi(p^l)}} = \frac{N(1-\zeta)}{(1-\zeta)^{\varphi(p^l)}} = \prod_{p\nmid k} \frac{1-\zeta^k}{1-\zeta} = \prod_{p\nmid k}(1+\zeta+\cdots+\zeta^{k-1}) \in \mathbb{Z}[\zeta]$, como se quería. □

Con esto, podemos pasar a demostrar el resultado principal:

Teorema 8. *Sea $\zeta = e^{\frac{2\pi i}{m}}$ la raíz m-ésima primitiva de la unidad. Entonces el anillo de enteros de $K = \mathbb{Q}(\zeta)$ es $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Demostración. La demostración se da para el caso $m = p^l$ potencia de primo p. Se denota por $n = [K:\mathbb{Q}] = \varphi(m)$. Obsérvese que $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$ (porque $\zeta = 1-(1-\zeta)$), hecho que se usará a lo largo de toda la demostración.

El cuerpo K tiene una base formada por enteros: $\{1, (1-\zeta), \ldots, (1-\zeta)^{n-1}\}$. Entonces, si $d = \operatorname{disc}(1, (1-\zeta), \ldots, (1-\zeta)^{n-1})$, dado $\alpha \in \mathcal{O}_K$ sabemos que $\alpha = \frac{\sum m_j(1-\zeta)^j}{d}$. Si fuese $\mathbb{Z}[\zeta] \subsetneq \mathcal{O}_K$, entonces alguno de los $\alpha \in \mathcal{O}_K$ tendría un j_0 tal que $\frac{m_{j_0}}{d} \notin \mathbb{Z}$.

Observando que también coincide que $d = \operatorname{disc}(1, \zeta, \ldots, \zeta^{n-1})$ (esto sigue rápidamente de la proposición 19), se tiene que $d|m^{\varphi(m)}$ y por tanto $d = p^s$ para cierto s. Multiplicando al α anterior adecuadamente:

$$\beta = p^{s-1}\alpha = \frac{\sum m_j(1-\zeta)^j}{p}$$

donde $p \nmid m_{j_0}$. Si j_0 es el primer índice donde eso ocurre, entonces restando todos los enteros algebraicos $\frac{m_j}{p}(1-\zeta)^j$ para $j < j_0$, se tiene finalmente el entero algebraico:

$$\gamma = \frac{\sum_{j\geq j_0} m_j(1-\zeta)^j}{p}.$$

Es posible obtener, en virtud del lema previo, otro entero algebraico:

$$\frac{p}{(1-\zeta)^{j_0+1}}\gamma = \frac{m_{j_0}}{1-\zeta} + \sum_{j>j_0} m_j(1-\zeta)^{j-j_0-1}$$

y como el último sumando está formado por enteros algebraicos (en concreto, por elementos de $\mathbb{Z}[\zeta]$ dado que $j - j_0 - 1 \geq 0$), esto permite concluir, finalmente, que $\frac{m_{j_0}}{1-\zeta}$ es un entero algebraico. Tomando normas sigue que $\frac{m_{j_0}^n}{p} \in \mathbb{Z}$, contradiciendo que $p \nmid m_{j_0}$. □

3. Residuos cuadráticos

El objetivo es determinar cuando, dado un $n \in \mathbb{Z}$, se tiene que $n \equiv a^2 \mod p$ para cierto a. Evidentemente, si $p|n$, entonces $n \equiv 0^2 \mod p$. Asimismo, si $p = 2$ es inmediato que todos los números son cuadrados. Con el fin de estudiar el resto de casos, se introduce la siguiente notación:

Definición 20. Dado p un primo y $n \in \mathbb{Z}$, se define el **símbolo de Legendre**:

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & p \mid n \\ 1, & p \nmid n, \exists a \in \mathbb{Z}, n \equiv a^2 \mod p \\ -1, & p \nmid n, \nexists a \in \mathbb{Z}, n \equiv a^2 \mod p \end{cases}$$

Puesto que se define en términos de clases módulo p, se tiene que $\left(\frac{\cdot}{p}\right) : \mathbb{Z}/p\mathbb{Z} \mapsto \{0, 1, -1\}$. Una primera pregunta es, fijado el p, obtener los n símbolos de Legendre para saber qué numeros son residuos cuadráticos módulo p:

Teorema 9 (Criterio de Euler)**.** *Sea $n \in \mathbb{Z}$ y p un primo impar. Se tiene que $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \mod p$.*

Demostración. Si $p|n$, entonces ambos lados son 0 evidentemente. Si no, si $n \equiv a^2 \mod p$, entonces $n^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \mod p$, como se quería, usando el pequeño teorema de Fermat, así como que $p \nmid a$ porque $p \nmid n$. Finalmente, hay que observar esta factorización en $\mathbb{Z}/p\mathbb{Z}[X]$: $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$. Como hay exactamente $\frac{p-1}{2}$ cuadrados no nulos módulo p, dado que elevar al cuadrado es una función sobreyectiva 2 a 1 en $\mathbb{Z}/p\mathbb{Z}^*$, sigue que los elementos que no son cuadrados deben ser raíces de $X^{\frac{p-1}{2}} + 1$, porque todos los elementos no nulos son raíces de $X^{p-1} - 1$ por el pequeño teorema de Fermat. Por tanto, si n no es un cuadrado módulo p, entonces $n^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$, como se quería. □

Una pregunta más complicada es, fijado el n, para qué primos es un residuo cuadrático. Dado que hay infinitos primos, no se pueden comprobar uno a uno con el criterio previo, es necesario establecer resultados al respecto.

Observación 14. Del criterio previo sigue que, si p es un primo, se tiene que $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$ para cualesquiera $m, n \in \mathbb{Z}$.

Esto es así porque $(mn)^{\frac{p-1}{2}} = m^{\frac{p-1}{2}} n^{\frac{p-1}{2}}$. Para $p = 2$, que no cubre el teorema previo, se puede verificar fácilmente.

Lema 5. *Sea p un primo impar y $\zeta = e^{\frac{2\pi i}{p}}$. Sea $\tau = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a$. Entonces, se tiene que $\tau^2 = \left(\frac{-1}{p}\right) \cdot p$.*

Demostración. $\tau^2 = (\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a)(\sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta^b) = \sum_{a,b} \left(\frac{ab}{p}\right) \zeta^{a+b}$. Aprovechando que, como $a \neq 0$, $x \mapsto ax$ es un isomorfismo, podemos escribir $b = ac$ y entonces $\tau^2 = \sum_{a,c} \left(\frac{a^2 c}{p}\right) \zeta^{a+ac} = \sum_c \left(\frac{c}{p}\right) \sum_a (\zeta^{1+c})^a$, donde el último paso utiliza que $\left(\frac{a^2}{p}\right) = 1$ al ser a^2 un cuadrado.

Ahora, se tiene que $\sum_a (\zeta^{1+c})^a = \begin{cases} p-1, & c = p-1 \\ -1 & 1 \leq c \leq p-2 \end{cases}$, donde el segundo resultado se obtiene de que $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$ dado que sabemos que exactamente la mitad de números son cuadrados módulo p. Entonces, $\tau^2 = \sum_c \left(\frac{c}{p}\right) \sum_a (\zeta^{1+c})^a = \sum_{c=1}^{p-2} -\left(\frac{c}{p}\right) + (p-1)\left(\frac{-1}{p-1}\right) = p\left(\frac{-1}{p}\right)$, donde de nuevo se utiliza el mismo hecho que antes para que $\sum_{c=1}^{p-2} -\left(\frac{c}{p}\right) = \left(\frac{-1}{p}\right)$. □

El siguiente teorema establece algunas propiedades útiles que, junto a la observación previa, permiten en multitud de ocasiones calcular los símbolos de Legendre de manera rápida:

Teorema 10 (Ley de Reciprocidad Cuadrática)**.** *Sean p, q dos primos impares distintos. Entonces:*

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

Demostración. El punto 2 ya se ha probado en el lema 1. Para el punto 1, vamos a denotar $p^* = \left(\frac{-1}{p}\right) p$. En ese caso, el teorema se reescribe como que $\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right) = 1$, puesto que es fácil comprobar, deshaciendo las definiciones, que $\left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$. Definimos $\tau(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^a$, y $\zeta = \zeta_p = e^{\frac{2\pi}{p}}$.

Por un lado, se tiene que $\left(\frac{q}{p}\right) \tau(\zeta^q) = \sum_{a=1}^{p-1} \left(\frac{qa}{p}\right) \zeta^{qa} = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \zeta^c = \tau(\zeta)$, donde usamos de nuevo que $x \to qx$ es un isomorfismo de $\mathbb{Z}/p\mathbb{Z}$.

Por otro lado, trabajando módulo q en $\mathbb{Z}[\zeta]$, sigue que $\tau(\zeta) \equiv \left(\frac{q}{p}\right)\tau(\zeta^q) \equiv \left(\frac{q}{p}\right)\tau(\zeta)^q \equiv \left(\frac{q}{p}\right)(\tau^2(\zeta))^{\frac{q-1}{2}}\tau(\zeta) \equiv \left(\frac{q}{p}\right)(p^*)^{\frac{q-1}{2}}\tau(\zeta) \equiv \left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right)\tau(\zeta) \mod q$, donde se ha usado el lema previo y el criterio de Euler.

Es decir, que $(1-\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right))\tau(\zeta) \equiv 0 \mod q$. Para terminar de establecer que $\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right) = 1$, veamos que, si fuese -1, se tendría que $2\tau(\zeta) \equiv 0 \mod q$, luego $4\tau^2(\zeta) \equiv 0 \mod q$, es decir que $4\tau^2(\zeta) = q\alpha$ con $\alpha \in \mathbb{Z}[\zeta]$. Esto implicaría que $\alpha = \frac{4p^*}{q}$, es decir, sería racional además de entero algebraico, luego $\alpha \in \mathbb{Z}$, contradiciendo que p y q sean primos impares distintos.

Finalmente, vamos a demostrar el punto 3. Analizamos la ecuación $x^2 + y^2 \equiv 2 \mod p$, donde p es un primo impar. Solo hay 4 soluciones con $x = \pm y$, dado que entonces la ecuación es $2x^2 \equiv 2 \mod p \implies x^2 \equiv 1 \mod p$. Ahora, si $x \neq \pm y$ y además ambos son no nulos, cada ecuación (a, b) viene acompañada de todas las siguientes: $(\pm a, \pm b), (\pm b, \pm a)$, luego hay un múltiplo de 8 de soluciones de este tipo. Finalmente, si uno de los dos es cero, la ecuación tiene la forma $x^2 \equiv 2 \mod p$, que tiene 4 soluciones $((\pm a, 0), (0, \pm a))$ si $\left(\frac{2}{p}\right) = 1$ y 0 en caso contrario.

Es decir, si $\left(\frac{2}{p}\right) = 1$ hay $8k + 4 + 4 \equiv 0 \mod 8$ soluciones, y si no, hay $8k + 4 \equiv 4 \mod 8$ soluciones. Ahora vamos a contar exactamente las soluciones. Puesto que $(1, 1)$ es una solución, basta con intersecar con la recta $y = t \cdot (x-1)+1$ para extraer las demás, además de $(1, -1)$ que se obtiene con la recta $x = 1$. Al calcular la intersección, se obtiene el punto $x = \frac{t^2-2t-1}{1+t^2}$ cuando $1 + t^2 \neq 0$, que además es distinto del propio $x = 1$ si $t \neq -1$. Es decir:

- Si -1 no es un cuadrado módulo p, es decir, si $p \equiv 3 \mod 4$, entonces se tienen precisamente $p + 1$ soluciones (una por cada valor de t, aquella que no es $(1, 1)$ o bien $(1, 1)$ si $t = -1$, más $(1, -1)$), y por tanto se tiene, del análisis anterior, que $\left(\frac{2}{p}\right) = 1 \iff p + 1 \equiv 0 \mod 8 \iff p \equiv -1 \mod 8$, que es compatible con $p \equiv 3 \mod 4$.
- Si -1 es un cuadrado módulo p, es decir, si $p \equiv 1 \mod 4$, entonces se tienen dos soluciones de menos, es decir $p - 1$, y ahora $\left(\frac{2}{p}\right) = 1 \iff p \equiv 1 \mod 8$, que de nuevo es compatible.

□

4. Factorización en dominios de Dedekind

Teorema 11. *Sea R un anillo (conmutativo y con unidad). Son equivalentes:*

1. *Todo ideal $I \subset R$ es finitamente generado.*
2. *Si $I_1 \subset I_2 \subset \dots$ es una cadena ascendente de ideales de R, entonces se estabiliza, es decir, $\exists N$ tal que $I_N = I_{N+k}$, $\forall k \geq 0$.*
3. *Si $S \neq \emptyset$ es un conjunto de ideales de R, tiene un elemento maximal (para el orden de inclusión).*

Demostración. Para $1 \implies 2$, dada una tal cadena, consideramos el ideal $I = \bigcup I_k$, que es tal a causa de las inclusiones (en general, la unión de ideales no tiene por qué serlo), y escribimos $I = (a_1, \dots, a_n)$. Por construcción, $\exists k_j$ tal que $a_j \in I_{k_j}$. Sea $K = \text{máx}\{k_j\}$, entonces se tiene que $I_K = I$, y por tanto $I_{K'} = I$, $\forall K' > K$. Para $2 \implies 3$, si no hubiera maximales en un conjunto de ideales S, se puede formar una cadena $I_1 \subsetneq I_2 \subsetneq \dots$, de ideales de S, en contradicción con 2. Para $3 \implies 1$, sea I un ideal y $S = \{J \subset I : J \text{ es finitamente generado}\}$. Como $0 \in S$, es no vacío, así que tiene un maximal M. Ha de ser $M = I$, porque, si no, poniendo $M = (a_1, \dots, a_n)$, y escogiendo $b \in I \setminus M$, se tendría $M \subsetneq (a_1, \dots, a_n, b) \in S$. Así, I es finitamente generado. □

Definición 21. Un anillo R es **noetheriano** si cumple alguna de las condiciones del teorema previo.

Por ejemplo, todo dominio de ideales principales es noetheriano (como $K[X]$ para K cuerpo). El dominio $K[X_1, X_2, \dots]$ de polinomios en un conjunto numerable de indeterminadas con coeficientes en K no es noetheriano, porque la cadena $(X_1) \subset (X_1, X_2) \subset \dots$ no estabiliza. Sin embargo, el dominio $K[X_1, \dots, X_n]$ sí que es noetheriano si K es un cuerpo, en virtud del teorema siguiente:

Teorema 12 (Base de Hilbert)**.** *Si A es noetheriano, entonces $A[X]$ también.*

Demostración. Supongamos que $I \subset A[X]$ no fuera finitamente generado. Entonces, podemos escoger $f_1 \in I \setminus \{0\}$ de grado mínimo y definir $I_1 = (f_1) \subsetneq I$. Ahora, podemos escoger $f_2 \in I \setminus I_1$ de grado mínimo (por tanto, $\deg f_1 \leq \deg f_2$), y definir $I_2 = (f_1, f_2) \subsetneq I$. Iterativamente, se consiguen los polinomios $\{f_n\}_n$ tales que $\{\deg f_n\}_n$ es creciente y cada $I_k = (f_1, \dots, f_k) \subsetneq I$.

Sea ahora $J = (a_1, a_2, \dots)$ el ideal generado por los coeficientes principales de los polinomios, es decir, $f_j = a_j X^{\deg f_j} + \tilde{f}_j$, con $\deg \tilde{f}_j < \deg f_j$. Como A es noetheriano, debe ser $J = (a_1, \dots, a_N)$. Es decir, $a_{N+1} = \sum_1^N b_j a_j$ para ciertos $b_j \in A$. Definimos ahora el polinomio $g = f_{N+1} - \sum_1^N b_i X^{\deg f_{N+1} - \deg f_i} f_i$. Por construcción se tiene $g \in I_{N+1}$, y además $g \notin I_N$ o si no se tendría $f_{N+1} \in I_N$. No obstante, su grado cumple $\deg g < \deg f_{N+1}$, dado que el coeficiente del término de grado $\deg f_{N+1}$ es $a_{N+1} - \sum_1^N b_j a_j = 0$. Esto es una contradicción y se tiene lo que se quería. □

Proposición 27. *Sea R un dominio noetheriano. Todo $a \in R$ no nulo se descompone como producto: $a = u \prod_{i=1}^r b_i$, donde $u \in \mathcal{U}(R)$ y los b_i son irreducibles (no necesariamente de manera única).*

Demostración. Supongamos que no fuese así. Sea S el conjunto de los ideales (a), donde a es un elemento no unidad que no se descompone como tal producto (en particular, a_0 no es irreducible). Sea $(a_0) \in S$ el maximal de S. Escribiendo $a_0 = \alpha\beta$, con $\alpha, \beta \notin \mathcal{U}(R)$, se tiene entonces que $(\alpha), (\beta) \notin S$, puesto que $(a_0) \subsetneq (\alpha), (\beta)$. Entonces se podría poner α y β como producto de irreducibles, luego también se podría a_0. □

Definición 22. Un dominio R se dice **dominio de Dedekind** si verifica:

1. R es noetheriano.

2. R es íntegramente cerrado, es decir, si K es el cuerpo de fracciones de R, entonces $\mathcal{O}_K^R = R$, siendo $\mathcal{O}^R$ el conjunto de raíces de polinomios mónicos con coeficientes en R (en analogía con los enteros algebraicos usuales, donde $R = \mathbb{Z}$).

3. Todo ideal primo no nulo es maximal, es decir, no existen cadenas $(0) \subsetneq P_1 \subsetneq P_2$ donde P_1, P_2 son primos. Dicho de otro modo, $\dim R \leq 1$.

A lo largo de esta sección consideraremos dominios de Dedekind que no son cuerpos, es decir, $\dim R = 1$. Por ejemplo, todos los dominios de ideales principales son de Dedekind. Un ejemplo de dominio de factorización única noetheriano que no es de Dedekind es $K[X, Y]$ con K cuerpo, dado que se tiene la cadena de ideales primos $(0) \subsetneq (X) \subsetneq (X, Y)$.

El objetivo, a continuación, es, dado un cuerpo de números $K \subset \mathbb{C}$, comprobar que el anillo de enteros de K es de Dedekind. Para ello, unos lemas previos:

Lema 6. *Si A es noetheriano y $\varphi : A \mapsto B$ es un homomorfismo de anillos sobreyectivo, entonces B es noetheriano (equivalentemente, todos los cocientes A/J son noetherianos).*

Demostración. Los ideales de A/J son de la forma I/J, donde $J \subset I \subset A$ es una cadena de ideales de A. Así, como I es finitamente generado, también lo es I/J (tomando clases). □

Lema 7. *Sea K un cuerpo de números. Si I es un ideal con $0 \subsetneq I \subsetneq \mathcal{O}_K$, entonces $\mathcal{O}_K/I$ es finito.*

Demostración. Dado $\alpha \in I$, la aplicación $\mathcal{O}_K/(\alpha) \mapsto \mathcal{O}_K/I \simeq \frac{\mathcal{O}_K/(\alpha)}{I/(\alpha)}$ es sobreyectiva, luego basta probarlo para $I = (\alpha)$. Del mismo modo, si tomamos $m = N(\alpha) \in \mathbb{Z}$ su norma, resulta que $m \in \alpha \cdot \mathcal{O}_K$, puesto que $\frac{m}{\alpha} \in K$, y además es un entero algebraico al ser el producto de todos los conjugados de α (salvo este último), que lo son. De esa relación se deduce que $m \in (\alpha)$, así que de nuevo es posible establecer la aplicación sobreyectiva $\mathcal{O}_K/(m) \mapsto \mathcal{O}_K/(\alpha)$, luego basta verlo para $I = (m)$.

Ahora, dada una base entera $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$, se tiene que $(\mathcal{O}_K, +) \simeq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, luego $(m) \simeq m\mathbb{Z}\alpha_1 \oplus \cdots \oplus m\mathbb{Z}\alpha_n$, así que $\mathcal{O}_K/(m) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}$, luego es finito. □

Con esto, es muy fácil probar el resultado buscado:

Teorema 13. *Si K es un cuerpo de números, $\mathcal{O}_K$ es un dominio de Dedekind.*

Demostración. Es noetheriano porque, dada una base entera $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$, se tiene la aplicación sobreyectiva $\mathbb{Z}[X_1, \ldots, X_n] \mapsto \mathcal{O}_K$ dada por $X_j \mapsto \alpha_j$, y como $\mathbb{Z}[X_1, \ldots, X_n]$ es noetheriano, uno de los lemas previos muestran que $\mathcal{O}_K$ es noetheriano.

Es íntegramente cerrado porque, si $P(X) = X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathcal{O}_K[X]$, y $\alpha \in K$ verifica $P(\alpha) = 0$, sucede entonces que $\alpha^n = -\sum_{i=0}^{r-1} a_i \alpha^i$, de donde se deduce que $\alpha^j \in \mathcal{O}_K + \alpha\mathcal{O}_K + \cdots + \alpha^{r-1}\mathcal{O}_K$, para cualquier j (reduciendo las potencias mediante el polinomio). Ahora solo basta poner $\mathcal{O}_K = \bigoplus \alpha_k\mathbb{Z}$, para la base entera $\{\alpha_k\}_k$, de donde sigue entonces que $\mathbb{Z}[\alpha] \subset \bigoplus_{k,1\leq j\leq r-1} \alpha_k\alpha^j\mathbb{Z}$. De aquí sigue que $R = \alpha_k\alpha^j\mathbb{Z}$ es un anillo finitamente generado que contiene a $\mathbb{Z}[\alpha]$, y por lo tanto α es algebraico (y como pertenecía a K, se tiene que $\alpha \in \mathcal{O}_K$).

Finalmente, dado un ideal primo $I \subset \mathcal{O}_K$, como $\mathcal{O}_K/I$ es un dominio y además es finito (en virtud del lema previo), debe ser un cuerpo, siendo I maximal. □

A continuación veremos algunos resultados de ideales en dominios de Dedekind.

Lema 8. *Todo ideal $I \subset R$ no nulo en un dominio de Dedekind R contiene un producto de ideales primos no nulos.*

Demostración. Supongamos que no fuese así, y sea $S \neq \emptyset$ el conjunto de ideales que violan la propiedad del lema. Sea $M \in S$ su elemento maximal. Como no es primo, se tienen $r, s \in R \setminus M$ con $rs \in M$. Por tanto, $M + (r)$ y $M + (s)$ contienen estrictamente a M, luego contienen productos de ideales primos: $P_1 \ldots P_k \subset M + (r)$, $Q_1 \ldots Q_l \subset M + (s)$. Así, $P_1 \ldots P_k Q_1 \ldots Q_l \subset (M + (r))(M + (s)) = M \cdot M + (r) \cdot M + (s) \cdot M + (r)(s) \subset M + M + M + (rs) \subset M + (rs) = M$, lo que es una contradicción. □

Lema 9. *Sea $I \subsetneq R$ un ideal propio no nulo de un dominio de Dedekind R que no es un cuerpo. Sea K su cuerpo de fracciones. Entonces, $\exists \gamma \in K \setminus R$ con $\gamma R \subset R$.*

Demostración. Sea $a \in I$ un elemento no nulo. Por el lema previo, hay ideales primos $P_1 \dots P_r \subset (a)$, que tomamos con r mínimo. Como I no es el total, hay un ideal maximal (por tanto, primo) P, que cumple $I \subset P$. Es decir, $P_1 \dots P_r \subset (a) \subset I \subset P$. De $P_1 \dots P_r \subset P$ se deduce que uno de ellos, sin perder en generalidad P_1, cumple $P_1 \subset P$. Esto es así porque, si no, habría $a_j \in P_j \setminus P$ para cada j, pero $\prod_j a_j \in P$, contradiciendo P primo. Como, por ser R de Dedekind, se tiene que P_1 es también maximal, ha de ser $P_1 = P$, es decir, $P_1 \dots P_r \subset (a) \subset I \subset P_1$. Como $P_2 \dots P_r \subsetneq (a)$ por minimalidad del r, debe haber $b \in P_2 \dots P_r \setminus (a)$.

Se afirma que $\gamma = \frac{b}{a}$. Como $b \notin (a)$, se tiene $\gamma \notin R$. Asimismo, $\gamma I = \frac{b}{a} I \subset \frac{b}{a} P_1 \subset \frac{1}{a} P_1 \cdot (P_2 \dots P_r) \subset \frac{(a)}{a} = R$. □

Teorema 14. *Si R es un dominio de Dedekind, e $I \subset R$ es un ideal no nulo, entonces $\exists J \subset R$ otro ideal nulo tal que $IJ = (a)$, con $a \in R$.*

Demostración. Sea $a \in I$ no nulo. Sea $J := \{\gamma \in R : \gamma I \subset (a)\}$. Es fácil comprobar que es un ideal, y además no nulo porque $a \in J$. Por la definición de J, se tiene $JI \subset (a)$. Sea $A := \frac{1}{a} JI$, que verifica $A \subset \frac{1}{a}(a) = R$, y es otro ideal.

Ahora vamos a ver que $A = R$, de donde seguiría que $(a) = (a)R = (a)A = JI$. Si fuese $A \subsetneq R$, podríamos escoger un $\gamma \in K \setminus R$, donde K es el cuerpo de fracciones de R, por el lema previo, tal que $\gamma A \subset R$. Como $\gamma A = \gamma \frac{1}{a} JI$, lo que se tiene entonces es que $\gamma JI \subset R(a) = (a)$, es decir, los elementos de γJ multiplicados por I están en (a), de tal modo que $\gamma J \subset J$ por la definición de J.

Ahora, si $J = (a_1, \dots, a_n)$, se tendrá $\gamma a_j = \sum_i r_{ij} a_i$, para cierta matriz $(r_{ij})_{i,j}$ de elementos de R. Esto quiere decir que la matriz $\gamma I_n - (r_{ij})_{i,j}$ tiene núcleo no trivial (el vector $(a_1, \dots, a_n)$ por lo menos), luego el polinomio $\det(XI_n - (r_{ij}))$, que es mónico y de coeficientes en R, se anula en γ, de donde sigue que γ es un R-entero de K, así que como R es de Dedekind y por tanto íntegramente cerrado, sigue $\gamma \in R$, lo que es una contradicción. □

De este teorema siguen ciertos corolarios:

Proposición 28. *Sea R un dominio de Dedekind y $\mathcal{H} = \{$ideales de R no nulos$\}/\sim$, donde $I \sim J \iff aI = bJ \iff (a)I = (b)J$ (para ciertos $a, b \in R$). Entonces, $\mathcal{H}$ es un grupo con la operación $[I]\cdot[J] = [IJ]$.*

Demostración. Todas las propiedades de grupo, así como que la operación está bien definida, pueden comprobarse con teoría de ideales básica (sin tener en cuenta que R sea un dominio de Dedekind) siendo el neutro la clase de los ideales principales, salvo la existencia de inversos. Esta se demuestra con el teorema previo: si $I \subset R$ es un ideal no nulo, entonces el J tal que $IJ = (a)$ hace que $[IJ] = [(a)]$, que es el neutro. □

Proposición 29 (Propiedad cancelativa)**.** *Sea R un dominio de Dedekind. Dados ideales no nulos $A, B, C \subset R$ con $AB = AC$, se tiene que $B = C$.*

Demostración. Sabemos del teorema que habrá un J tal que $AJ = (a)$, luego, multiplicando por ese J, sigue $(a)B = (a)C$, es decir $aB = aC$, luego $B = C$ al estar en un dominio. □

Proposición 30. *Sea R un dominio. Si $A, B \subset R$ son ideales tal que $AC = B$ para cierto C, se dice que A **divide a** B, y se denota $A|B$. Obsérvese que, en ese caso, $B = AC \subset A$. Se tiene que, si R es un dominio de Dedekind, entonces $A|B \iff B \subset A$.*

Demostración. $\implies$ ya está explicada en el enunciado. Para $\impliedby$, escogemos el J que hace $AJ = (a)$. Se afirma que el ideal $C = \frac{1}{a} JB$ es el buscado. En primer lugar, como $B \subset A$, entonces $C \subset \frac{1}{a} JA = \frac{1}{a}(a) = R$, así que efectivamente es un ideal de R. Por otro lado, $AC = \frac{1}{a} AJB = \frac{(a)}{a} B = B$. □

El siguiente resultado es un teorema de gran importancia. Recordemos que los elementos de un dominio de Dedekind descomponían como producto de primos, pero quizás de manera no única. En los ideales esto último mejora:

Teorema 15. *Sea R un dominio de Dedekind e $I \subset R$ un ideal no nulo. Entonces I se escribe de manera única como producto de ideales primos.*

Demostración. Para ver la descomposición, si hubiese ideales que no descompusieran, el conjunto S de tales ideales sería no vacío. Sea $M \in S$ un elemento maximal. Entonces $M \subsetneq R$, dado que R es producto de un conjunto vacío de ideales primos. Por tanto, hay un ideal maximal (y primo) P con $M \subset P$, y por el lema previo, $P|M$ luego $M = PJ$ para cierto J. Véase que se tiene $M = PJ \subset J$. Si fuese $PJ = J$, se tendría entonces $PJ = J = RJ$, luego, como se tiene cancelación, sería $P = R$ contradiciendo que P sea primo. Por tanto, $PJ = M \subsetneq J$ así que J es producto de ideales primos: $J = P_1 \dots P_r$, contradiciendo que M no lo sea, dado que $M = PJ = PP_1 \dots P_r$.

Para la unicidad, supongamos que $P_1 \dots P_r = Q_1 \dots Q_s$ con todos ellos primos. Como $Q_1 \dots Q_s \subset P_1$, se tiene que uno de los $Q_j \subset P_1$ por primalidad de P_1. Sin perder generalidad, sea $j = 1$. Entonces $Q_1 \subset P_1$ y al tratarse de un dominio de Dedekind vale la igualdad, así que pueden cancelarse y ahora se tendría $Q_2 \dots Q_s = P_2 \dots P_r$. Inductivamente se tiene la igualdad de todos ellos, así como que $r = s$ puesto que si no alguno de los P_j o Q_j sería todo R (en el paso en el que uno de los dos lados de la igualdad sea el producto vacío). □

Teorema 16. *Si R es un Dominio de Dedekind que es dominio de factorización única, entonces es dominio de ideales principales.*

Demostración. Sea $I \subset R$ un ideal no nulo. Ponemos $IJ = (a)$ para cierto J y $a \in R$, por uno de los lemas previos. Al tratarse de un dominio de factorización única, $a = u\pi_1 \dots \pi_r$ con $u \in \mathcal{U}(R)$ y los $\pi_j \in R$ irreducibles (y, equivalentemente en un DFU, primos), de manera única. Entonces, $IJ = (a) = (\pi_1 \dots \pi_r) = (\pi_1) \dots (\pi_r)$. Por el teorema previo, factorizando I y J en sus ideales primos y por unicidad, ha de seguir que $I = (\pi_{i_1}) \dots (\pi_{i_k})$ luego $I = (\pi_{i_1} \dots \pi_{i_k})$, como se quería. □