UNIVERSIDAD NACIONAL DE CÓRDOBA

FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

SERIE "B"

TRABAJOS DE MATEMÁTICA

N° 67/2019

Una introducción a la teoría algebraica de números

Emilio A. Lauret
CIEM–FaMAF, Universidad Nacional de Córdoba, Argentina.
elauret@famaf.unc.edu.ar

Editor: Jorge G. Adrover

CIUDAD UNIVERSITARIA – (5000) CÓRDOBA
REPÚBLICA ARGENTINA

Prefacio

Estas notas están basadas en dos cursos que dicté en la Facultad de Matemática, Astronomía, Física y Computación (FaMAF) de la Universidad Nacional de Córdoba (UNC), Argentina. El primero de ellos fue durante el primer cuatrimestre (Marzo–Junio) de 2016 mientras que el segundo fue en el segundo cuatrimestre de 2018 (Agosto–Noviembre). Ambos consistieron en 15 semanas de dos clases semanales de 120 minutos.

Los contenidos son más o menos los mismos que algunos de los cursos dictados por el Profesor Roberto Miatello también en FaMAF en años anteriores. La inclusión de extensiones algebraicas de cuerpos y la Teoría de Galois durante las primeras semanas se debe a que estos temas no están incluidos en ninguna materia obligatoria en esta universidad.

Durante el texto aparecerán diferentes ejercicios, los cuales usualmente piden completar alguna demostración o realizar un cálculo omitido. Además, la mayoría de las secciones finaliza con problemas. Éstos nunca son muchos, aunque ninguno es de obvia resolución.

La referencia principal para la primera parte (extensiones algebraicas y teoría de Galois) son Capítulos V y VI de [**Lang**]. Para la segunda parte (Capítulos 3, 4 y 5) seguiremos Capítulos 2–5 de [**Marcus**]. A pesar que estas notas pueden ser vistas como una mera transcripción de estos excelentes libros, espero que sean útiles para los estudiantes del curso actual y futuros, y cualquiera que las haya encontrado en internet.

Asimismo, sugiero fuertemente consultar [**Hungerford**] (un clásico) para teoría de cuerpos, como así también [**Alaca&Williams**] (contiene muchísimos ejemplos y cálculos explícitos en casos particulares) y [**Narasimhan et al**] (notas rápidas para entender muchos conceptos en poco tiempo) para teoría algebraica de números.

En idioma español, me han recomendado [**Ivorra Castillo**], aunque no he tenido el gusto de leerlo. Al googlearlo para citarlo encontré que en la página web del autor (Carlos Ivorra Castillo) hay varios libros disponibles sobre diferentes temas, todos en castellano. Las notas cortas [**Lauret**] introducen la teoría algebraica de números en el caso particular de los cuerpos cuadráticos. Me gustaría también mencionar las notas [**Barseghian**] y [**Campagnolo & Guzmán**] las cuales fueron escritas por estudiantes del primer curso dictado en 2016 y presentadas en el concurso de Monografías de la Reunión Anual de la Unión Matemática Argentina en Bahía Blanca en 2016. El tema del concurso era el Teorema de Stark-Heegner, el cual clasifica los cuerpos cuadráticos imaginarios tales que su correspondientes anillos de enteros son dominios de factorización única. Desafortunadamente, ninguna de las notas están (aún) disponibles en internet.

La organización de estas notas es como sigue. En Capítulo 1 introduciremos las nociones básicas de extensiones de cuerpos arbitrarios, tales como extensiones finitas, algebraicas, normales, y separables. En Capítulo 2 veremos de una manera resumida la Teoría de Galois para extensiones finitas. Esto nos permitirá deducir diversas propiedades de las extensiones ciclotómicas.

A partir del tercer capítulo consideraremos exclusivamente extensiones finitas de los números racionales, llamados comúnmente cuerpos de números. Capítulo 3 introducirá los enteros algebraicos y las herramientas traza, norma y discriminante, las cuales serán muy útiles durante el resto de las notas, y en particular para mostrar que el anillo de enteros de un cuerpo de números (así como cualquiera de sus ideales) es un grupo abeliano libre.

En el escueto Capítulo 4 se considerarán dominios de Dedekind, los cuales contienen a los anillos de enteros de cuerpos de números. En estos dominios mostraremos que todo ideal no nulo se escribe de manera única (salvo orden) como producto de ideales primos.

El quinto capítulo estudia la importante noción de grupo de clases de un cuerpo de números. Su objetivo es poder calcular de manera explícita el grupo de clases de diversos ejemplos. La cota de Minkowski, que cuenta con una demostración algo trabajosa, será muy importante para simplificar el procedimiento de determinación del grupo de clases de un cuerpo de números. También veremos el Teorema de las Unidades de Dirichlet. El capítulo finaliza con la demostración de una gran cantidad de casos del conocido Último Teorema de Fermat usando los conocimientos previos.

Quiero aprovechar esta prefacio para renovar mi profundo agradecimiento a mi mentor Roberto Miatello, en esta oportunidad, por el dictado de tantos cursos de posgrado en FaMAF. También agradezco a los estudiantes que padecieron mis clases de este curso, principalmente a Lucas Villagra quien hizo un increíble trabajo corrigiendo una versión preliminar de este texto.

Será extremadamente bienvenida cualquier corrección, vía correo electrónico preferentemente.

Emilio Lauret
Córdoba, Argentina,
Febrero de 2019.

Índice general

Capítulo 1

Extensiones de cuerpos

1. Extensiones algebraicas

DEFINICIÓN 1.1. Sean E y F cuerpos. Decimos que E es una *extensión de* F si F está contenido en E, lo que denotamos por $E|F$. En ese caso, $[E:F] := \dim_F E$ ($\in \mathbb{N} \cup \{0\}$), la dimensión de E como F-espacio vectorial. Además, $\alpha \in E$ se dice *algebraico sobre* F si existe $f(x) \in F[x]$ no nulo tal que $f(\alpha) = 0$.

EJEMPLO 1.2. $\sqrt{2} \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$, mientras que $\pi \in \mathbb{C}$ no lo es.

PROPOSICIÓN 1.3. *Si $k \subset F \subset E$ son cuerpos, entonces*

$$[E:k] = [E:F][F:k].$$

En particular, $E|k$ es finita (i.e. $[E:k] < \infty$) si y sólo si $E|F$ y $F|k$ son finitas.

DEMOSTRACIÓN. Sea $\{a_i\}_{i\in I}$ una k-base de F y sea $\{b_j\}_{j\in J}$ una F-base de E. Veamos que $\{a_i b_j\}_{(i,j)\in I\times J}$ es una k-base de E.

Para mostrar que el conjunto genera, tomemos $\gamma \in E$ y los escribamos como combinación lineal de ella. Como $\{b_j\}_{j\in J}$ es una F-base de E, existen elementos $\beta_j \in F$ para cada $j \in J$, con $\beta_j = 0$ para todo $j \in J$ salvo una cantidad finita, tales que

$$\gamma = \sum_{j\in J} \beta_j b_j.$$

Como $\{a_i\}_{i\in I}$ es una k-base de F, para cada $j \in J$ con $\beta_j \neq 0$, existen $\alpha_{j,i} \in k$ para cada $i \in I$, con $\alpha_{j,i} = 0$ para todo $i \in I$ salvo una cantidad finita, tales que $\beta_j = \sum_{i\in I} \alpha_{j,i} a_i$. Concluimos que

$$\gamma = \sum_{j\in J} \left(\sum_{i\in I} \alpha_{j,i} a_i \right) b_j = \sum_{(i,j)\in I\times J} \alpha_{j,i}\, a_i b_j.$$

Supongamos que elementos $\gamma_{j,i} \in k$ para $(i,j) \in I \times J$, con $\gamma_{j,i} = 0$ para todo $(i,j) \in I \times J$ salvo una cantidad finita, cumple que $\sum_{(i,j)\in I\times J} \gamma_{j,i} a_i b_j = 0$. Entonces, $0 = \sum_{j\in J} \left(\sum_{i\in I} \gamma_{j,i} a_i \right) b_j$, lo que implica que $\sum_{i\in I} \gamma_{j,i} a_i = 0$ para todo $j \in J$, por lo tanto $\gamma_{j,i} = 0$ para todo $(i,j) \in I \times J$. Esto nos dice que $\{a_i b_j\}_{(i,j)\in I\times J}$ es linealmente independiente, y por lo tanto es base, lo cual finaliza la prueba. □

DEFINICIÓN 1.4. Sean F un cuerpo y X un subconjunto de F. Llamamos a

- $\bigcap_{E\subset F:\, X\subset E} E$ el *subcuerpo de F generado por X*;
- $\bigcap_{R\subset F:\, X\subset R} R$ el *subanillo de F generado por X*.

Sea k un subcuerpo de F. Denotamos

- $k(X)$ al subcuerpo de F generado por $k \cup X$;

- $k[X]$ al subanillo de F generado por $k \cup X$.

Cuando $X = \{u_1, \dots, u_n\}$, escribimos $k(u_1, \dots, u_n) = k(X)$ y $k[u_1, \dots, u_n] = k[X]$.

PROPOSICIÓN 1.5. *Sean $F|k$, $u, u_1, \dots, u_n \in F$, $X \subset F$. Se tienen las siguientes identidades:*

(1) $k[u] = \{f(u) : f \in k[x]\}$.
(2) $k[u_1, \dots, u_n] = \{f(u_1, \dots, u_n) : f \in k[x_1, \dots, x_n]\}$.
(3) $k[X] = \bigcup_{n\in\mathbb{N}} \{f(v_1, \dots, v_n) : f \in k[x_1, \dots, x_n], v_1, \dots, v_n \in X\}$.
(4) $k(u) = \{\frac{f(u)}{g(u)} : f, g \in k[x],\ g(u) \neq 0\}$.
(5) $k(u_1, \dots, u_n) = \{\frac{f(u_1,\dots,u_n)}{g(u_1,\dots,u_n)} : f, g \in k[x_1, \dots, x_n],\ g(u_1, \dots, u_n) \neq 0\}$.
(6) $k(X) = \bigcup_{n\in\mathbb{N}} \left\{ \dfrac{f(v_1, \dots, v_n)}{g(v_1, \dots, v_n)} : \begin{array}{l} f, g \in k[x_1, \dots, x_n],\ v_1, \dots, v_n \in X, \\ g(v_1, \dots, v_n) \neq 0 \end{array} \right\}$.

La demostración es un ejercicio simple.

EJEMPLO 1.6. La proposición anterior implica inmediatamente que

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

¿Quién cree que será $\mathbb{Q}(\sqrt{2})$? El siguiente resultado nos dará una linda respuesta a esta pregunta. Primero necesitamos algo de notación.

Sea $F|k$ una extensión y supongamos que $\alpha \in F$ es algebraico sobre k. Sea $\Phi : k[x] \to F$ un morfismo de anillos k-lineal determinado por $x \mapsto \alpha$. El núcleo de Φ, $\mathrm{Nu}(\Phi) = \{f \in k[x] : f(\alpha) = 0\}$, es un ideal en $k[x]$. Como $k[x]$ es un dominio de ideales principales, $\mathrm{Nu}(\Phi)$ está generado por un elemento, esto es, $\mathrm{Nu}(\Phi) = \langle m_\alpha(x)\rangle$ con $m_\alpha(x) \in k[x]$ que asumiremos mónico (notar que es único con esta propiedad) y lo llamaremos *polinomio minimal de α sobre k*.

PROPOSICIÓN 1.7. *Sean $F|k$ una extensión y $\alpha \in F$ algebraico sobre k. Entonces $k(\alpha) = k[\alpha]$, y $[k(\alpha) : k] = \mathrm{gr}(m_\alpha(x))$.*

DEMOSTRACIÓN. Es claro que $k[\alpha] \subset k(\alpha)$. Para establecer la igualdad, es suficiente mostrar que $k[\alpha]$ es un cuerpo ya que esto implica que $k(\alpha) \subset k[\alpha]$ por ser $k(\alpha)$ el menor cuerpo que contiene a $k \cup \{\alpha\}$.

Veamos que $m_\alpha(x)$ es irreducible. Supongamos que $m_\alpha(x) = f(x)g(x)$ con $f, g \in k[x]$. Como $0 = m_\alpha(\alpha) = f(\alpha)g(\alpha)$, $f(\alpha) = 0$ o $g(\alpha) = 0$. Supongamos que $f(\alpha) = 0$. Tenemos que $f \in \mathrm{Nu}(\Phi)$, lo que implica que existe $h \in k[x]$ tal que $f(x) = m_\alpha(x)h(x)$. Luego $m_\alpha(x) = m_\alpha(x)h(x)g(x)$, de lo que sigue que $1 = h(x)g(x)$ por ser $k[x]$ anillo íntegro (i.e. no tiene divisores de cero). Concluimos que g es una unidad en $k[x]$, es decir, un polinomio constante no nulo, lo que muestra que $m_\alpha(x)$ es irreducible.

El ideal $\langle m_\alpha(x)\rangle$ es maximal por ser $m_\alpha(x)$ irreducible, por lo que obtenemos que

$$k[x]/\langle m_\alpha(x)\rangle = k[x]/\mathrm{Nu}(\Phi) \simeq \mathrm{Im}(\Phi) = k[\alpha]$$

es un cuerpo. Esto prueba que $k[\alpha] = k(\alpha)$.

Sea $d = \mathrm{gr}(m_\alpha(x))$. Veamos que $[k(\alpha) : k] = d$, mostrando que $\{1, \alpha, \dots, \alpha^{d-1}\}$ es una k-base de $k(\alpha)$. Para ver la independencia lineal, supongamos $0 = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ con $a_i \in k$ para todo i. Tenemos que el polinomio $g(x) := \sum_{i=1}^{d-1} a_i x^i$ se anula en α, por lo

que es necesariamente divisible por $m_\alpha(x)$, el cual tiene grado $d > \mathrm{gr}(g(x))$. Esto implica que $g(x) \equiv 0$, es decir, $a_i = 0$ para todo i.

Ahora veamos que el conjunto $\{1, \alpha, \ldots, \alpha^{d-1}\}$ genera $k(\alpha)$. Sea $f(\alpha) \in k[\alpha] = k(\alpha)$ con $f \in k[x]$. Por el algoritmo de la división en $k[x]$, existen $g, h \in k[x]$, con $h \equiv 0$ ó $\mathrm{gr}(h(x)) < d$, tales que $f(x) = m_\alpha(x)g(x) + h(x)$. Entonces $f(\alpha) = 0$ ó $f(\alpha) = h(\alpha)$ respectivamente. Este último es claramente una combinación lineal de $1, \alpha \ldots, \alpha^{d-1}$. □

EJEMPLOS 1.8. $\mathbb{R}[i] = \mathbb{C}$, $\mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q}$, $\mathbb{Q}(\sqrt{18}) = \mathbb{Q}(3\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

EJEMPLO 1.9. Sea $\alpha \in \mathbb{C}$ una raíz del polinomio irreducible $f(x) := x^3 + x + 1$ sobre $\mathbb{Q}$. Como $\alpha^4, (1+\alpha)^{-1} \in k(\alpha) = k[\alpha]$, estos elementos se pueden escribir (de manera única) como combinación lineal sobre $\mathbb{Q}$ de $1, \alpha, \alpha^2$. Esto se hace usando el algoritmo de la división en $k[x]$ de una manera adecuada:

$$x^4 = (x^3 + x + 1)x + (-x^2 - x) \qquad \Longrightarrow \qquad \alpha^4 = -\alpha^2 - \alpha,$$
$$x^3 + x + 1 = (x+1)(x^2 - x + 2) - 1 \qquad \Longrightarrow \qquad (1+\alpha)^{-1} = 2 - \alpha + \alpha^2.$$

EJEMPLO 1.10. Sea p entero primo (siempre será asumido positivo). El cuerpo $F_p := \mathbb{Z}/p\mathbb{Z}$ tiene p elementos. El polinomio $p(x) = x^2 + x + 1 \in F_2[x]$ es irreducible (notar que basta ver que 0 y 1 no son raíces). Entonces $F_p[x]/\langle p(x)\rangle$ es un cuerpo de cuatro elementos.

De manera similar, $E_1 = F_3[x]/\langle x^2 + 1\rangle$ y $E_2 = F_3[x]/\langle x^2 + x + 2\rangle$ son cuerpos con $3^2 = 9$ elementos. Se puede ver que $E_1 \simeq E_2$. Probaremos más adelante que todo cuerpo finito tiene cardinalidad p^n para algún p primo y $n \in \mathbb{N}$, y es único con esta propiedad (salvo isomorfismo).

DEFINICIÓN 1.11. Una extensión $F|k$ es *algebraica* si todo $\alpha \in F$ es algebraico sobre k. La extensión $F|k$ se dice *trascendente* en caso de no ser algebraica.

OBSERVACIÓN 1.12. Aunque no estudiaremos extensiones trascendentes en este curso, cabe mencionar un ejemplo. Se prueba que π es trascendente sobre $\mathbb{Q}$, por lo tanto

$$\mathbb{Q}(\pi) = \left\{ \frac{f(\pi)}{g(\pi)} : f, g \in \mathbb{Q}[x],\ g \neq 0 \right\} \simeq \text{cuerpo de fracciones de } \mathbb{Q}[x].$$

PROPOSICIÓN 1.13. *Si una extensión $F|k$ es finita (i.e. $[F : k] < \infty$), entonces $F|k$ es algebraica.*

DEMOSTRACIÓN. Sigue del hecho que para cualquier $\alpha \in F$, se tiene que el conjunto $\{1, \alpha, \ldots, \alpha^n\}$ es linealmente dependiente para todo $n > [F : k]$. □

OBSERVACIÓN 1.14. Una extensión algebraica no es necesariamente finita. Por ejemplo, se puede ver que $\mathbb{Q}(\{\sqrt[n]{2} : n \in \mathbb{N}\})|\mathbb{Q}$ es algebraica pero no finita. Otro ejemplo es $\overline{\mathbb{Q}}|\mathbb{Q}$, donde $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ es algebraico sobre } \mathbb{Q}\}$.

PROPOSICIÓN 1.15. *Si $F|k$ es finita, entonces F es finitamente generado sobre k, es decir, $F = k(\alpha_1, \ldots, \alpha_n)$ para ciertos $\alpha_1, \ldots, \alpha_n \in F$, con α_i algebraico sobre k para todo i.*

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una k-base de F. Entonces $F = k(\alpha_1 \ldots, \alpha_n)$. En efecto, la inclusión $\supset$ es obvia, mientras que la otra dirección sigue de $F = \{\sum_{j=1}^n a_j\alpha_j : a_1, \ldots, a_n \in k\} \subset k(\alpha_1 \ldots, \alpha_n)$. □

DEFINICIÓN 1.16. Para E y F subcuerpos de L, el *cuerpo composición de E y F* se define por $EF := E(F) = F(E)$.

OBSERVACIÓN 1.17. Sean $k \subset E, F \subset L$ cuerpos y $\alpha_1, \ldots, \alpha_n \in L$.

- Si $E = k(\alpha_1, \ldots, \alpha_n)$, entonces $EF = F(\alpha_1, \ldots, \alpha_n)$.
- Si α_1 es algebraico sobre k, entonces también lo es sobre F.
- $k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.
- $k[\alpha_1, \ldots, \alpha_n] = k[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$.

EJERCICIO 1.18. Sean E_1 y E_2 extensiones de k contenidas en un cuerpo más grande E, y sea σ una incrustación de E a otro cuerpo L. Probar que $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$.

El siguiente resultado se puede considerar como una pseudo-recíproca de Proposición 1.13.

PROPOSICIÓN 1.19. *Supongamos que $E = k(\alpha_1, \ldots, \alpha_n)$, con α_i algebraico sobre k para todo i. Entonces $E|k$ es una extensión finita y algebraica.*

DEMOSTRACIÓN. Consideremos la siguiente sucesión de extensiones:

$$k \subset k(\alpha_1) \subset k(\alpha_1)(\alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n).$$

Notemos que cada una de las extensiones dadas por '$\subset$' son finitas por ser α_i algebraico sobre k y en particular sobre $k(\alpha_1, \ldots, \alpha_{i-1})$. Luego, $k(\alpha_1, \ldots, \alpha_n)|k$ es finita por Proposición 1.3, y en consecuencia algebraica por Proposición 1.13. □

EJEMPLO 1.20. Tomemos $k = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt{2}]$ y $F = \mathbb{Q}[\sqrt[3]{2}]$, todos ellos subcuerpos de $\mathbb{C}$. Veamos que

$$EF = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}].$$

Como $\mathbb{Q} \subset E$, $\sqrt{2} \in E$ y $\sqrt[3]{2} \in F$, se tiene que $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}] \subset EF$. La otra inclusión sigue de que $EF = E(\sqrt[3]{2})$ es el menor cuerpo que contiene al conjunto $E \cup \{\sqrt[3]{2}\}$, el cual está incluido en $\mathbb{Q}[\sqrt{2}][\sqrt[3]{2}] = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$.

PROPOSICIÓN 1.21. *La clase de extensiones finitas y la clase de extensiones algebraicas son* distinguidas*, es decir, cumplen:*

(1) *Si $k \subset F \subset E$ son cuerpos, entonces $E|k$ es finita (algebraica) si y sólo si $E|F$ y $F|k$ son finitas (algebraicas). (En otras palabras, se mantienen por levantamientos.)*
(2) *Si $E|k$ es finita (algebraica) y $F|k$ es arbitraria, entonces $EF|F$ es finita (algebraica).*
(3) *Si $E|k$ y $F|k$ son finitas (algebraicas), entonces $EF|k$ es finita (algebraica).*

Los cuerpos k, F, E están siempre incluidos en un cuerpo más grande.

DEMOSTRACIÓN. Comencemos con el caso de extensiones finitas. El primero ya fue demostrado en Proposición 1.3.

Para el segundo ítem, supongamos que $E|k$ es finita. Por Proposición 1.15, $E = k(\alpha_1, \ldots, \alpha_n)$ para ciertos $\alpha_1, \ldots, \alpha_n \in E$, todos algebraicos sobre k. Entonces $EF = F(\alpha_1, \ldots, \alpha_n)$ (ver Observación 1.17), con α_i algebraico sobre F para todo i, lo que implica que $EF|F$ es finita por Proposición 1.19. El tercer caso sigue de los dos primeros, para cualquier clase de extensiones.

Ahora consideremos las extensiones algebraicas. Para el primer ítem, supongamos que $k \subset F \subset E$. Si $E|k$ es algebraica, entonces claramente $E|F$ es algebraica (pues $k \subset F$) y $F|k$ es algebraica (pues $F \subset E$).

Ahora supongamos que $E|F$ y $F|k$ son algebraicas, y sea $\alpha \in E$, el cual queremos ver que es algebraico sobre k. Como $E|F$ es algebraica, existen $a_0, \dots, a_n \in F$ (no todos nulos) tales que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Por Proposición 1.19, las inclusiones

$$k \subset F_0 := k(a_0, \dots, a_n) \subset F_0(\alpha).$$

son extensiones finitas de cuerpos, ya que $a_0, \dots, a_n \in F_0 \subset F$ son algebraicos sobre k, y α es algebraico sobre F_0. Luego $F_0(\alpha)|k$ es finita por Proposición 1.3, lo que implica que $k(\alpha)|k$ también lo es, y por lo tanto α es algebraico sobre k.

Finalicemos mostrando el segundo ítem. Sea $\alpha \in EF = F[E]$. Sabemos que existen $f \in F[x_1, \dots, x_n]$ y $a_1, \dots, a_n \in E$ tales que $\alpha = f(a_1, \dots, a_n)$. Notemos que las extensiones dadas por cada una de las inclusiones

$$F \subset F(a_1) \subset F(a_1, a_2) \subset \cdots \subset F(a_1, \dots, a_n)$$

son finitas, pues cada a_i es algebraico sobre k (por estar en E) y por consiguiente también sobre $F(a_1, \dots, a_{i-1})$. Luego, $F(a_1, \dots, a_n)|F$ es finita, y como $F(\alpha) \subset F(a_1, \dots, a_n)$, obtenemos que α es algebraico sobre F. □

Problemas.

1.1. Sea $\alpha = \sqrt[4]{2}$, esto es, la única raíz real positiva de $x^4 - 2 = 0$.

(a) Calcular el polinomio minimal $m_\alpha(x)$ de α sobre $\mathbb{Q}$. (Ayuda: usar el criterio de Eisenstein: si $f(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{Z}[x]$ con $a_m \neq 0$ y existe un primo racional p tal que $p \mid a_j$ para todo $0 \leq j \leq m-1$, $p \nmid a_m$ y $p^2 \nmid a_0$, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$).

(b) Determinar todos los cuerpos F tales que $\mathbb{Q} \subsetneq F \subsetneq \mathbb{Q}(\alpha)$.

(c) ¿Existe $\beta \in \mathbb{C}$ tal que $\mathbb{Q}(\alpha, i) = \mathbb{Q}(\beta)$?

1.2. (a) Hallar el polinomio minimal sobre $\mathbb{Q}$ de $\sqrt{2} + \sqrt{3}$, $\sqrt{2}\sqrt{3}$, $\sqrt{2} + \sqrt[3]{5}$.

(b) Caracterizar en $F := \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ los elementos $\alpha \in F$ tal que $F \neq \mathbb{Q}(\alpha)$.

1.3. Dar dos elementos α, β algebraicamente independientes sobre un cuerpo k, tales que $k(\alpha, \beta) \ncong k(x_1, x_2)$.

1.4. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(a) Si $E = F(\alpha)$ con α algebraico sobre F y tal que el grado de $m_\alpha(x)$ es impar, entonces $F(\alpha^2) = E$.

(b) Si $E|k$ y $F|k$ son finitas tales que $[E : k]$ y $[F : k]$ son coprimos, entonces $E \cap F = k$.

(c) Si $E|F$ algebraica y $\alpha, \beta \in E$ tales que $\mathrm{mcd}(m_\alpha(x), m_\beta(x)) = 1$, entonces $m_\beta(x)$ es irreducible en $F(\alpha)[x]$.

(d) Existe una extensión de $\mathbb{Q}(\pi)$ de grado 3.

2. Clausura algebraica

DEFINICIÓN 1.22. Un cuerpo k se dice *algebraicamente cerrado* si todo polinomio en $k[x]$ de grado ≥ 1 tiene una raíz en k.

OBSERVACIÓN 1.23. Si k es algebraicamente cerrado y $f \in k[x]$ con $\mathrm{gr}(f) = n$, entonces existen $c, \alpha_1, \ldots, \alpha_n \in k$ tales que

$$f(x) = c(x - \alpha_1) \ldots (x - \alpha_n).$$

Esto se prueba recursivamente, usando que si $\alpha_1 \in k$ es raíz de f, entonces $f(x) = (x - \alpha_1)g(x)$ para algún $g(x) \in k[x]$ de grado $n - 1$ por el algoritmo de la división.

El próximo objetivo es probar que para todo cuerpo k, existe un único (salvo isomorfismo) cuerpo $\bar{k}$ algebraicamente cerrado tal que la extensión $\bar{k}|k$ es algebraica.

PROPOSICIÓN 1.24. *Dados k un cuerpo y $f \in k[x]$ con $\mathrm{gr}(f) \geq 1$, existe una extensión $F|k$ tal que f tiene una raíz en F.*

DEMOSTRACIÓN. Sea $p(x)$ un polinomio irreducible en $k[x]$ que divide a $f(x)$. El cuerpo $F := k[x]/\langle p(x)\rangle$ contiene a k[1]. Además, si denotamos la clase de un elemento de $k[x]$ en F con una barra, es claro que $p(\bar{x}) = \overline{p(x)} = 0$. Por lo tanto el polinomio $f(x)$ se anula en $\bar{x}$. □

TEOREMA 1.25. *Todo cuerpo está dentro de un cuerpo algebraicamente cerrado.*

DEMOSTRACIÓN. A cada polinomio $f \in k[x]$ con $\mathrm{gr}(f) \geq 1$, le asociamos una indeterminada x_f. Sea

$$S = \{x_f : f \in k[x], \mathrm{gr}(f) \geq 1\}.$$

Dentro del anillo $k[S]$ de polinomios con coeficientes en k y variables en S, consideramos el ideal

$$I := \langle \{f(x_f) : f \in k[x],\ \mathrm{gr}(f) \geq 1\} \rangle.$$

AFIRMACIÓN. $I \neq k[S]$.

DEMOSTRACIÓN. Supongamos que $I = k[S]$. Como el polinomio idénticamente 1 está en I, existen $f_1, \ldots, f_n \in k[x]$ con $\mathrm{gr}\, f_i \geq 1$ para todo $1 \leq i \leq n$ y $g_1, \ldots, g_n \in k[S]$ tales que

$$1 = g_1\, f_1(x_{f_1}) + \cdots + g_n\, f_n(x_{f_n}).$$

Escribamos $x_i = x_{f_i}$ para todo $1 \leq i \leq n$, y sean $x_{n+1}, \ldots, x_m$ las demás indeterminadas involucradas en los polinomios $g_1, \ldots, g_n$. Luego,

$$1 = \sum_{i=1}^{n} g_i(x_1, \ldots, x_m)\, f_i(x_i).$$

Por repetidas aplicaciones de Proposición 1.24 para $f_1, \ldots, f_n$, existe una extensión $F|k$ tales que f_i tiene una raíz $\alpha_i \in F$ para todo $1 \leq i \leq n$. Tomemos $\{\alpha_f\}_{f \in S}$ con $\alpha_{f_i} = \alpha_i$ para todo $1 \leq i \leq n$ y $\alpha_f = 0$ para todo $f \notin \{f_1, \ldots, f_i\}$. Entonces, evaluando la última fórmula en este elemento, obtenemos

$$1 = \sum_{i=1}^{n} g_i(\alpha_1, \ldots, \alpha_m)\, f_i(\alpha_i) = 0,$$

lo cual es una contradicción proveniente de haber asumido que $I = k[S]$. ■

[1]Aunque la afirmación es clara, existe cierta imprecisión. Se recomienda ver [**Lang**, Prop. 2.3, Ch. V]

Existe un ideal maximal (propio) $\mathfrak{m}$ tal que $I \subset \mathfrak{m} \subset k[S]$ pues $I \neq k[S]$. Luego

$$E_0 := k \subset k[S]/\mathfrak{m} =: E_1,$$

esto es, $E_0 = k$ es un subcuerpo del cuerpo E_1, y se cumple que todo polinomio en $E_0[x] = k[x]$ tiene al menos una raíz en E_1.

Repitiendo este procedimiento con E_1 y luego recursivamente, obtenemos una torre de cuerpos

$$E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n \subset \cdots,$$

con la propiedad de que cualquier polinomio en $E_i[x]$ de grado al menos uno tiene una raíz en E_{i+1}, para todo $i \geq 0$. Definimos

$$E = \bigcup_{i \geq 0} E_i.$$

Es claro que E es un cuerpo. Además, E es algebraicamente cerrado. En efecto, si $f \in E[x]$ con $\mathrm{gr}(f) \geq 1$, entonces existe $i \geq 0$ tal que todos los coeficientes de f pertenecen a E_i, por lo que f tendrá una raíz en $E_{i+1} \subset E$. Esto completa la demostración pues $k \subset E$. □

Corolario 1.26. *Dado k un cuerpo, existe $\bar{k}$ un cuerpo algebraicamente cerrado tal que la extensión $\bar{k}|k$ es algebraica.*

Demostración. Por Teorema 1.25, existe un cuerpo E algebraicamente cerrado que contiene a k. Sea

$$\bar{k} = \bigcup_{\substack{k \subset F \subset E: \\ F|k \text{ es algebraico}}} F = \{\alpha \in E : \alpha \text{ es algebraico sobre } k\}.$$

Resta ver que $\bar{k}$ es el cuerpo requerido.

Sean α, β en $\bar{k}$. La extensión $k(\alpha, \beta)|k$ es finita por Proposición 1.19 pues α y β son algebraicos sobre k. Entonces $\alpha - \beta, \alpha\beta^{-1}$ están en $k(\alpha, \beta) \subset \bar{k}$. Esto muestra que $\bar{k}$ es un cuerpo. La extensión $\bar{k}|k$ es algebraica por definición. Resta ver que $\bar{k}$ es algebraicamente cerrado.

Sea $f \in \bar{k}[x]$ y $\alpha \in E$ raíz de f, veamos que $\alpha \in \bar{k}$. Como α es algebraico sobre $\bar{k}$, se tiene que las extensiones $k \subset \bar{k} \subset \bar{k}(\alpha)$ son algebraicas. Concluimos que α es algebraico sobre k por Proposición 1.21, lo que asegura que $\alpha \in \bar{k}$. □

Resta probar la unicidad de la clausura algebraica. Probaremos de hecho algo más general.

Lema 1.27. *Sean $E|k$ una extensión algebraica y $\phi : E \to E$ un morfismo de cuerpos sobre k (i.e. $\phi|_k = \mathrm{Id}_k$). Entonces ϕ es un isomorfismo.*

Demostración. Como $\mathrm{Nu}(\phi)$ es un ideal en un cuerpo, éste debe ser necesariamente trivial ($\phi(1) = 1$, lo que implica que ϕ no puede ser idénticamente nula), y por lo tanto ϕ es inyectiva. Veamos que ϕ es suryectiva.

Tomemos $\alpha \in E$ y veamos que está en la imagen de ϕ. Sea E' el subcuerpo de E generado por k y todas las raíces de $m_\alpha \in k[x]$ en E. Como E' está generada por una cantidad finita de raíces, y todas ellas son algebraicas sobre k, Proposición 1.19 asegura que la extensión $E'|k$ es finita.

Sea β una raíz de $m_\alpha(x)$. Entonces $\phi(\beta)$ también es raíz de $m_\alpha(x)$. En efecto, si $m_\alpha(x) = \sum_{i=0}^{n} a_i x^i$, entonces

$$m_\alpha(\phi(\beta)) = \sum_{i=0}^{n} a_i\, \phi(\beta)^i = \phi(\sum_{i=0}^{n} a_i \beta^i) = \phi(m_\alpha(\beta)) = \phi(0) = 0.$$

Como ϕ es inyectiva, y lleva el conjunto finito de raíces de $m_\alpha(x)$ en E en sí mismo, entonces α está en la imagen de ϕ. □

Sean $E|k$ una extensión algebraica, L un cuerpo algebraicamente cerrado, y $\sigma : k \to L$ un morfismo de cuerpos. Una *extensión a E de σ* es un morfismo de cuerpos $\tau : E \to L$ tal que $\tau|_k = \sigma$, esto es, $\tau(a) = \sigma(a)$ para todo $a \in k$.

¿Cuántas extensiones a E existen de σ?

Comencemos respondiendo esta pregunta en el caso $E = k(\alpha)$ con α algebraico sobre k. (En Sección 4 estudiaremos más en profundidad esta pregunta.)

NOTACIÓN 1.28. Para $f(x) = \sum_i a_i x^i \in k[x]$, denotaremos $f^\sigma(x) = \sum_i \sigma(a_i) x^i \in L[x]$.

Notemos que si τ extiende σ a E, entonces $\tau(\alpha)$ es necesariamente raíz de $m_\alpha^\sigma(x)$. Ahora, sea β cualquier raíz de $m_\alpha^\sigma(x)$. Podemos definir $\tau : E \to L$ por $\tau(\alpha) = \beta$. En efecto, como todo elemento de E se escribe como $f(\alpha)$ con $f = \sum_i a_i x^i \in k[x]$, $\tau(f(\alpha))$ queda determinado por

$$\tau(f(\alpha)) = \tau(\sum_i a_i \alpha^i) = \sum_i \sigma(a_i)\, \tau(\alpha)^i = \sum_i \sigma(a_i)\, \beta^i = f^\sigma(\beta).$$

Veamos la buena definición de τ, suponiendo que hay un elemento en $k(\alpha)$ que se escribe como $f(\alpha) = g(\alpha)$ con $f, g \in k[x]$. Como $m_\alpha(x)$ divide a $f(x) - g(x)$, entonces $m_\alpha^\sigma(x)$ divide a $f^\sigma(x) - g^\sigma(x)$, lo que implica que

$$\tau(f(\alpha)) = f^\sigma(\beta) = g^\sigma(\beta) = \tau(g(\alpha)).$$

Hemos demostrado el siguiente resultado.

PROPOSICIÓN 1.29. *Sea α algebraico sobre k y sea $E = k(\alpha)$. El número de posibles extensiones a $k(\alpha)$ es igual al número de raíces distintas de $m_\alpha(x)$. Más aún, las extensiones quedan determinadas por el valor en α, el cual debe ser necesariamente una raíz de $m_\alpha^\sigma(x)$.*

El resultado anterior será fundamental en la demostración del siguiente teorema, el cual finaliza la prueba de la unicidad de la clausura algebraica.

TEOREMA 1.30. *Sean $E|k$ una extensión algebraica, $\sigma : k \to L$ un morfismo de cuerpos, y L un cuerpo algebraicamente cerrado. Entonces existe una extensión de σ a E. Además, si E es algebraicamente cerrado y la extensión $L|\sigma(k)$ es algebraica, entonces cualquier extensión de σ a E es un isomorfismo.*

COROLARIO 1.31. *Dado k un cuerpo, existe una única (salvo isomorfismo) extensión $\bar{k}$ algebraicamente cerrada tal que la extensión $\bar{k}|k$ es algebraica.*

DEFINICIÓN 1.32. El cuerpo $\bar{k}$ del corolario anterior es llamado *clausura algebraica* de k.

DEMOSTRACIÓN DE TEOREMA 1.30. Usaremos el Lema de Zorn. En el conjunto

$$\mathcal{S} := \{(F, \tau) : k \subset F \subset E,\ \tau : F \to L,\ \tau|_k = \sigma\}$$

consideremos el orden parcial definido por $(F, \tau) \preceq (F', \tau')$ si $F \subset F'$ y $\tau'|_F = \tau$. Tenemos que $\mathcal{S}$ es no vacío pues contiene a (k, σ).

Sea $\{(F_i, \tau_i)\}_{i\in\mathbb{N}}$ una cadena ordenada (i.e. $(F_i, \tau_i) \preceq (F_{i+1}, \tau_{i+1})$ para todo $i \in \mathbb{N}$). Tomemos $F = \cup_i F_i$ y $\tau : F \to L$ dado por restricción a τ_i apropiado. Entonces $(F_i, \tau_i) \preceq (F, \tau)$ para todo $i \in \mathbb{N}$.

Como hemos chequeado $\mathcal{S} \neq \emptyset$ y que toda cadena en él tiene cota superior, Lema de Zorn nos asegura que existe un elemento maximal $(\widetilde{E}, \lambda)$ en $\mathcal{S}$. Veamos que $\widetilde{E} = E$. Si $\alpha \in E \smallsetminus \widetilde{E}$, entonces existe una extensión de λ a $\widetilde{E}(\alpha)$, contradiciendo la maximalidad de $(\widetilde{E}, \lambda)$.

Ahora veamos la segunda parte. Asumamos que E es algebraicamente cerrado y la extensión $L|\sigma(k)$ es algebraica. Tenemos que $\sigma(E)$ es algebraicamente cerrado y que la extensión $L|\sigma(E)$ es algebraica. Si $\alpha \in L$, entonces existe $f \in \sigma(E)[x]$ que anula a α, lo que implica que $\alpha \in \sigma(E)$ por ser algebraicamente cerrado. Esto prueba que $L = \sigma(E)$. □

Problemas.

1.5. Probar que si $E|k$ es algebraica, entonces $\bar{E}$ es una clausura algebraica de k. Dar un contraejemplo si la extensión $E|k$ no es necesariamente algebraica.

1.6. Mostrar que si k es un cuerpo finito, entonces $\bar{k}$ es numerable. Además, para un cuerpo infinito k, probar que $\bar{k}$ tiene la misma cardinalidad que k.

1.7. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(a) Si $E|k$ es una extensión arbitraria y $\varphi : E \to E$ es un k-morfismo, entonces φ es un isomorfismo.

(b) No existe ningún cuerpo algebraicamente cerrado F que satisfaga $\overline{\mathbb{Q}} \subsetneq F \subsetneq \mathbb{C}$.

3. Extensiones normales

Sean k un cuerpo y $f \in k[x]$ con $\mathrm{gr}(f) \geq 1$. Un *cuerpo de descomposición* (*splitting field*) de f es un cuerpo F que contiene a todas las raíces $\alpha_1, \ldots, \alpha_n$ y que además $F = k(\alpha_1, \ldots, \alpha_n)$. Claramente, $F|k$ es una extensión finita por Proposición 1.19 y además $f(x)$ se descompone en F como

$$f(x) = c(x - \alpha_1) \ldots (x - \alpha_n),$$

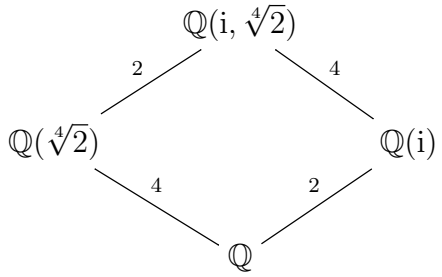
para algún $c \in k$.

EJEMPLO 1.33. Si $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ y $g(x) = x^2 + 2 \in \mathbb{Q}[x]$, entonces $\mathbb{Q}_f := \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ es un cuerpo de descomposición de f y $\mathbb{Q}_g := \mathbb{Q}(\sqrt{-2}, -\sqrt{-2}) = \mathbb{Q}(\sqrt{-2})$ es un cuerpo de descomposición de g.

EJEMPLO 1.34. Sea $h(x) = x^4 - 2 \in \mathbb{Q}[x]$. Se puede ver que el cuerpo de descomposición $\mathbb{Q}_h := \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{-2})$ de h coincide con $\mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$. En efecto, como $\pm\sqrt[4]{2}, \pm\sqrt[4]{-2} \in \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$ se tiene que $\mathbb{Q}_h \subset \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$. La otra contención sigue de que $\mathrm{i} = \frac{1}{2}\sqrt[4]{-2}(\sqrt[4]{2})^3 \in \mathbb{Q}_h$. Más aún, $[\mathbb{Q}_h : \mathbb{Q}] = 8$ pues $x^2 + 1$ es irreducible en $\mathbb{Q}(\sqrt[4]{2})$ (¿por qué?) lo que implica que

$$[\mathbb{Q}_h : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \mathrm{i}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \,.\, 4 = 8.$$

El siguiente gráfico muestra de manera clara los grados de cada una de las extensiones:



El siguiente resultado nos asegura que existe un único cuerpo de descomposición en una clausura algebraica fija.

TEOREMA 1.35. *Sean k un cuerpo y $f \in k[x]$ con $\mathrm{gr}(f) \geq 1$. Si $E_1|k$ y $E_2|k$ son cuerpos de descomposición de f, entonces existe $\phi : E_1 \to E_2$ un isomorfismo de cuerpos sobre k.*

DEMOSTRACIÓN. Primero veamos que $\bar{E}_2$ es una clausura algebraica de k, donde recordemos, $\bar{E}_2$ denota la única (salvo isomorfismo) clausura algebraica de E_2 (ver Definición 1.32). Como $k \subset E_2$, todo polinomio de grado ≥ 1 con coeficientes en k tiene todas sus raíces en $\bar{E}_2$. Además, $\bar{E}_2|k$ es algebraica por Proposición 1.21(1) pues $\bar{E}_2|E_2$ y $E_2|k$ lo son.

Por Teorema 1.30, existe $\phi : E_1 \to \bar{E}_2$ un k-morfismo de cuerpos. Como todo morfismo de cuerpos es inyectivo, sólo resta mostrar que $\phi(E_1) = E_2$. Denotemos $\alpha_1, \ldots, \alpha_n$ las raíces de f en E_1. Como $\phi(\alpha_1), \ldots, \phi(\alpha_n)$ son raíces de f en $\bar{E}_2$, deben estar en E_2. Más aún, como ϕ es inyectivo, $\phi(\alpha_1), \ldots, \phi(\alpha_n)$ son todas las raíces de f en E_2, y por lo tanto

$$\phi(E_1) = \phi\big(k(\alpha_1, \ldots, \alpha_n)\big) = k(\phi(\alpha_1), \ldots, \phi(\alpha_n)) = E_2.$$

Concluimos que $\phi : E_1 \to E_2$ es sobre. □

DEFINICIÓN 1.36. Para $k \subset E \subset \bar{k}$, la extensión $E|k$ se dice *normal* si para todo $\sigma : E \to \bar{k}$ morfismo sobre k se tiene que $\sigma(E) = E$.

Notar que $\sigma : E \to E$ en la definición anterior es necesariamente un isomorfismo pues todo morfismo de cuerpos es inyectivo.

EJEMPLO 1.37. Claramente, $\mathbb{Q}(\sqrt{2})$ es normal pues si $\sigma : \mathbb{Q}(\sqrt{2}) \to \bar{\mathbb{Q}}$ es un $\mathbb{Q}$-morfismo, entonces $\sigma(\sqrt{2})$ debe ser una raíz de $x^2 - 2$, por lo tanto

$$\sigma(\mathbb{Q}(\sqrt{2})) \subset \mathbb{Q}(\sigma(\sqrt{2})) = \mathbb{Q}(\pm\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Más aún, se puede ver que toda extensión de grado 2 es normal.

EJEMPLO 1.38. El cuerpo $\mathbb{Q}(\sqrt[4]{2})$ no es normal sobre $\mathbb{Q}$. En efecto, $\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \bar{\mathbb{Q}}$, determinado por $\sqrt[4]{2} \mapsto \mathrm{i}\sqrt[4]{2}$ es un $\mathbb{Q}$-morfismo, pero $\sigma(\mathbb{Q}(\sqrt[4]{2})) = \mathbb{Q}(\mathrm{i}\sqrt[4]{2}) \neq \mathbb{Q}(\sqrt[4]{2})$.

EJEMPLO 1.39. El cuerpo $\mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$ es normal sobre $\mathbb{Q}$ por el teorema siguiente.

TEOREMA 1.40. *Sean $k \subset E \subset \bar{k}$ cuerpos. Las siguientes afirmaciones son equivalentes:*

(1) *la extensión $E|k$ es normal;*
(2) *E es el cuerpo de descomposición de una familia de polinomios;*

(3) *todo polinomio irreducible $p(x) \in k[x]$ que tiene una raíz en E, tiene necesariamente todas sus raíces en E.*

DEMOSTRACIÓN. Veamos primero que (1) implica (3). Sea $p(x) \in k[x]$ irreducible con $\alpha \in E$ una raíz de p, y sea $\beta \in \bar{k}$ una raíz de $p(x)$. Queremos mostrar que $\beta \in E$.

Definimos $\sigma : k(\alpha) \to k(\beta)$ el k-morfismo de cuerpos determinado por $\sigma(\alpha) = \beta$. Por Teorema 1.30, existe $\psi : E \to \bar{k}$ una extensión de σ. Como $E|k$ es normal por hipótesis, se tiene que $\psi(E) = E$. Concluimos que $\beta \in E$.

Notemos que, bajo la hipótesis en (1), acabamos de probar que para cualquier $\alpha \in E$, el polinomio $m_\alpha(x) \in k[x]$ tiene todas sus raíces en E. Entonces E coincide con el cuerpo de descomposición de la familia $\{m_\alpha(x)\}_{\alpha \in E}$. Esto muestra que (1) implica (2).

Ahora veamos que (2) implica (1). Sea E el cuerpo de descomposición de la familia $\{f_i(x)\}_{i \in I}$. Para $i \in I$, denotemos $\alpha_{i,j}$ con $1 \leq j \leq n_i$ las raíces de $f_i(x)$. Para probar que $E|k$ es normal, sea $\sigma : E \to \bar{k}$ un k-morfismo de cuerpos, y mostremos que $\sigma(E) = E$, o equivalentemente, $\alpha_{i,j} \in E$ para todo i, j. Esto es cierto pues $\sigma(\alpha_{i,j})$ es raíz de $f_i(x)$ (por ser σ un k-morfismo), lo que implica que $\alpha_{i,j} \in k(\alpha_{i,1}, \ldots, \alpha_{i,n_i}) \subset E$.

Ahora asumamos (3) y tomemos nuevamente un k-morfismo $\sigma : E \to \bar{k}$. Sea $\alpha \in E$, y veamos que $\sigma(\alpha) \in E$. Esto sigue de que $\sigma(\alpha)$ es raíz del polinomio irreducible $m_\alpha(x)$ por la hipótesis en (3). □

Se puede ver que la clase de extensiones normales no es distinguidas. Asimismo, varias de las propiedades son válidas.

TEOREMA 1.41. *Las siguientes afirmaciones son verdaderas.*

(1) *La normalidad se mantiene por levantamientos, esto es, si $E|k$ es una extensión normal, entonces la extensión $EF|F$ es también normal.*
(2) *Si $k \subset F \subset E$ son cuerpos tales que la extensión $E|k$ es normal, entonces la extensión $E|F$ también lo es.*
(3) *Si $E|k$ y $F|k$ son extensiones normales (dentro de una misma clausura algebraica de k), entonces $EF|k$ y $E \cap F|k$ son también extensiones normales.*

DEMOSTRACIÓN. Para ver (1), sea $\sigma : EF \to \bar{k}$ un F-morfismo de cuerpos. Como $\sigma|_E : E \to \bar{k}$ es un k-morfismo, se tiene que $\sigma(E) = E$ por ser la extensión $E|k$ normal por hipótesis. Entonces $\sigma(EF) = \sigma(E)\sigma(F) = EF$ (ver Ejercicio 1.18), tal como queríamos.

El ítem (2) sigue inmediatamente del hecho que todo F-morfismo $\sigma : E \to \bar{k}$ es necesariamente un k-morfismo. Luego, $\sigma(E) = E$ por hipótesis.

Sea $\sigma : EF \to \bar{k}$ un k-morfismo. Claramente, $\sigma|_E : E \to \bar{k}$ y $\sigma|_F : F \to \bar{k}$ son k-morfismos, y como $E|k$ y $F|k$ son normales por hipótesis, tenemos que $\sigma(EF) = \sigma(E)\sigma(F) = EF$. Si $\sigma : E \cap F \to \bar{k}$, entonces $\sigma(E \cap F) = \sigma(E) \cap \sigma(F) = E \cap F$. □

Finalizamos la subsección dejando algunas propiedades simples de ejercicio, las cuales serán útiles en el resto de las notas.

EJERCICIO 1.42. Sea $E|k$ una extensión finita y sean $\sigma_1, \ldots, \sigma_n$ todos los k-morfismos de E a $\overline{E}$. Probar las siguientes afirmaciones:

(a) La extensión normal de k que contiene a E más pequeña es

$$E' := \bigcap_{\substack{F \supset E \\ F|k \text{ normal}}} F.$$

(b) $E' = \sigma_1(E) \dots \sigma_n(E)$.
(c) Si $E = k(\alpha)$ con α algebraico sobre k, entonces $E' = k(\sigma_1(\alpha), \dots, \sigma_n(\alpha))$.

Problemas.

1.8. Sea $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Sabemos que la extensión $E|k$ es normal por Ejemplos 1.34 y Teorema 1.40.

(a) Probar que $E|\mathbb{Q}(i)$ es una extensión normal.
(b) ¿Existe $F \subset E$ tal que $E|F$ no sea normal?
(c) ¿Existe $F \subset E$ tal que $F|\mathbb{Q}$ no sea normal?

1.9. Sea $\alpha = \sqrt[3]{2} \in \mathbb{C}$, esto es, el único número real positivo α tal que $\alpha^3 = 2$.

(a) Calcular $m_\alpha(x)$ sobre $\mathbb{Q}$.
(b) Probar que el cuerpo de descomposición de $m_\alpha(x)$ es $\mathbb{Q}(\sqrt[3]{2}, \omega)$, donde $\omega = e^{2\pi i/3}$, y que su dimensión como $\mathbb{Q}$-espacio vectorial es igual a 6.
(c) ¿Existe un cuerpo F tal que $\mathbb{Q} \subsetneq F \subsetneq E$ y $F|\mathbb{Q}$ normal?

1.10. Sea $f(x) = x^6 + x^3 + 1$.

(a) Describir el cuerpo de descomposición de f sobre $\mathbb{Q}$.
(b) Sea α raíz de $f(x)$. Hallar todos los morfismos de $\mathbb{Q}(\alpha)$ a $\mathbb{C}$.

1.11. Probar las siguientes afirmaciones, donde E y F son extensiones de k.

(a) Si $E|k$ es normal, entonces $EF|F$ es normal.
(b) Para $k \subset F \subset E$, si $E|k$ es normal, entonces $E|F$ es normal.
(c) Si $E|k$ y $F|k$ son normales, entonces $EF|k$ y $E \cap F|k$ son normales.
(d) Si $k \subset F \subset E$ y $E|k$ es normal, entonces $F|k$ no necesariamente es normal. En particular, la clase de extensiones normales no es distinguida.
(e) Sean $k \subset F \subset E$ cuerpos tales que las extensiones $E|F$ y $F|k$ son normales. ¿Es $E|k$ necesariamente normal?

4. Extensiones separables

Sean L un cuerpo algebraicamente cerrado y $\sigma : k \to L$ un morfismo de cuerpos. Proposición 1.45 nos asegura que la cantidad de formas de extender σ a una extensión de la forma $E = k(\alpha)$ es igual al número de raíces distintas de $m_\alpha(x)$. En efecto, tales morfismos están determinados por el elemento al que enviamos α, el cual necesariamente debe ser una raíz de $m_\alpha^\sigma(x)$.

DEFINICIÓN 1.43. Sea $E|k$ una extensión algebraica. Llamamos el *grado de separabilidad de la extensión* $E|k$ a

$$[E : k]_s := \#\{\tau : E \to L : \tau|_k = \sigma\}.$$

EJERCICIO 1.44. Probar que el grado de separabilidad de una extensión algebraica está bien definida, es decir, no depende de la elección del cuerpo algebraicamente cerrado L ni del morfismo σ. En particular, se puede tomar $L = \bar{k}$ y $\sigma = \mathrm{id}$.

Teorema 1.30 nos asegura que $[E : k]_s \geq 1$.

TEOREMA 1.45. *Sean $k \subset F \subset E$ cuerpos tales que la extensión $E|k$ es algebraica. Entonces*

$$[E : k]_s = [E : F]_s \, [F : k]_s.$$

Además, si la extensión $E|k$ es finita, entonces $[E : k]_s$ es finita y $[E : k]_s \leq [E : k]$.

DEMOSTRACIÓN. Fijemos un morfismo $\sigma : k \to L$, con L algebraicamente cerrado. Denotemos por $\{\sigma_i\}_{i\in I}$ a la familia de extensiones de σ a F. Para cada $i \in I$, sea $\{\tau_{i,j}\}_{j\in J_i}$ la familia de extensiones de σ_i a E. Luego,

$$\#\{\tau_{i,j}\}_{i\in I,\, j\in J_i} = \sum_{i\in I} \#J_i = \sum_{i\in I} [E : F]_s = [E : F]_s \#I = [E : F]_s [F : k]_s.$$

Resta ver que cualquier extensión τ de σ a E es algún $\tau_{i,j}$ para ciertos i, j. Sea τ una extensión de σ a E. Como $\tau|_F$ extiende a σ a F, entonces $\tau|_F = \sigma_i$ para algún $i \in I$. Como τ extiende a $\tau|_F = \sigma_i$ a E, $\tau = \tau_{i,j}$ para algún $j \in J$.

Ahora asumamos que $[E : k] < \infty$. Por Proposición 1.15, E es finitamente generado, es decir, existen $\alpha_1, \ldots, \alpha_n \in E$ tales que $E = k(\alpha_1, \ldots, \alpha_n)$. Denotemos $F_0 = k$ y $F_{l+1} = F_l(\alpha_{l+1})$ para $0 \le l \le n-1$. Gráficamente,

$$F_0 = k \subset F_1 = k(\alpha_1) \subset F_2 = k(\alpha_1, \alpha_2) \subset \cdots \subset F_n = k(\alpha_1, \ldots, \alpha_n) = E.$$

Por lo mencionado al comienzo de la sección, $[F_{l+1} : F_l]_s$ es igual a la cantidad de raíces distintas del polinomio irreducible de α_{l+1} sobre F_l. Por lo tanto

$$[F_{l+1} : F_l]_s \le [F_{l+1} : F_l],$$

pues este último es igual al grado del mencionado polinomio. Por lo mostrado en la primera parte, concluimos que

$$[E : k]_s = [F_1 : F_0]_s \ldots [F_n : F_{n-1}]_s \le [F_1 : F_0] \ldots [F_n : F_{n-1}] = [E : k],$$

lo cual completa la demostración. □

OBSERVACIÓN 1.46. Será útil para el resto de las notas notar que la igualdad $[E : k]_s = [E : k]$ se da únicamente si (en la demostración se tiene que)

$$[F_{l+1} : F_l]_s = [F_{l+1} : F_l] \quad \text{para todo } 0 \le l \le n-1.$$

DEFINICIÓN 1.47. Para una extensión finita $E|k$, decimos que E es *separable sobre* k si $[E : k]_s = [E : k]$. Decimos que un elemento algebraico α sobre k es *separable* si $k(\alpha)$ es separable sobre k. Decimos que un polinomio $f(x) \in k[x]$ es *separable* si no tiene raíces repetidas en $\bar{k}$.

OBSERVACIÓN 1.48. Por lo visto anteriormente, un elemento α (algebraico sobre k) es separable si y sólo si $m_\alpha(x)$ es separable. Esto explica las idénticas denominaciones para elementos de un cuerpo y para polinomios presentes en la definición anterior.

Veremos que si la característica del cuerpo es cero (i.e. $n\alpha \neq 0$ para todo α no nulo y n entero positivo), entonces toda extensión de k es separable. El siguiente ejemplo muestra un elemento no separable. Se verá que no es un ejemplo simple, y se usan diversas herramientas que se complementarán en el resto del curso.

EJEMPLO 1.49. Sea p un primo racional. Consideremos el cuerpo $F_p := \mathbb{Z}/p\mathbb{Z}$, el cual tiene p elementos. Sea $k = F_p(t)$, donde t es una variable independiente (i.e. t es algebraicamente independiente sobre F_p). A k se lo conoce como el *cuerpo de funciones racionales* de F_p. Claramente, $p\alpha = 0$ para todo $\alpha \in k$ (i.e. k tiene característica p).

Sean $n \in \mathbb{N}$ y $f(x) = x^n - t \in k[x]$. El polinomio $f(x)$ es irreducible por el criterio de Eisenstein (¡creerlo! Aunque aún no estamos en condiciones de enunciar la versión de este criterio necesaria para aplicarla en este caso). Sea $\alpha \in \bar{k}$ raíz de f. Queremos determinar cuándo α es una raíz repetida de $f(x)$. Para esto usaremos que β es una raíz repetida de

un polinomio $g(x)$ si y sólo si $g(\beta) = g'(\beta) = 0$, donde $g'(x)$ es la derivada formal del polinomio g. Si $p \nmid n$, entonces $f'(x) = nx^{n-1} \neq 0$.

Supongamos ahora que $n = p^\mu$ para algún μ entero positivo. Entonces $f'(x) = 0$. Además, $\alpha^{p^\mu} = t$ pues $f(\alpha) = 0$. Luego,

$$f(x) = x^{p^\mu} - \alpha^{p^\mu} = (x - \alpha)^{p^\mu}.$$

(Notar que $f(x) = (x-\alpha)^{p^\mu} = (x+\alpha)^{p^\mu}$cuando $p = 2$.) Concluimos que α no es separable, ya que es la única raíz de su polinomio minimal sobre k.

El siguiente es un ejercicio simple: si $k \subset F \subset E$ son cuerpos y $\alpha \in E$ es separable sobre k, entonces α es separable sobre F.

TEOREMA 1.50. *Sea $E|k$ una extensión finita. Entonces, E es separable sobre k si y sólo si todo α es separable sobre k para todo $\alpha \in E$.*

DEMOSTRACIÓN. Demostraremos sólo la ida. Supongamos que E es separable sobre k y veamos que todo $\alpha \in E$ es separable sobre k. Extendamos la torre de cuerpos $k \subset k(\alpha) \subset E$ a

$$F_0 := k \subset F_1 := k(\alpha) \subset F_2 \subset \cdots \subset F_n := E$$

con la propiedad que $F_{l+1} = F_l(\alpha_{l+1})$ para algún $\alpha_{l+1} \in E$, para todo $0 \leq l \leq n-1$ ($\alpha_1 = \alpha$). Esto es posible pues la extensión $E|k$ es finita.

Como E es separable sobre k, tenemos $[E : k]_s = [E : k]$, lo cual era posible si y sólo si $[F_{l+1} : F_l]_s = [F_{l+1} : F_l]$ para todo $0 \leq l \leq n-1$ (ver Nota 1.48). En particular, $[k(\alpha) : k]_s = [k(\alpha) : k]$, esto es, α es separable sobre k. □

EJERCICIO 1.51. Completar la demostración de Teorema 1.50 probando la recíproca. (Ayuda: usar Proposición 1.15 y una torre apropiada para aplicar Observación 1.48.)

DEFINICIÓN 1.52. Para una extensión algebraica $E|k$ (no necesariamente finita), decimos que E es separable sobre k si toda subextensión finitamente generada (i.e. finita) de E es separable sobre k.

TEOREMA 1.53. *La clase de extensiones separables es distinguida, es decir:*

1. *Para $k \subset F \subset E$, E es separable sobre k si y sólo si E es separable sobre F y F es separable sobre k.*
2. *Si E es separable sobre k y $F|k$ es arbitraria, entonces EF es separable sobre F.*
3. *Si E y F son separables sobre k, entonces EF es separable sobre k.*

Los cuerpos k, F, E están siempre incluidos en un cuerpo más grande.

DEMOSTRACIÓN. Asumiremos que todas las extensiones de k son finitas. Para el caso general, ver [**Lang**, Thm. 4.5, Ch. V].

(1) sigue de Observación 1.48. Resta ver (2), ya que (3) era consecuencia de (1) y (2).

Supongamos que $E|k$ es finita y separable. Se tiene que $E = k(\alpha_1, \ldots, \alpha_n)$ para algunos $\alpha_1, \ldots, \alpha_n \in E$ por Proposición 1.15. Notar que $\alpha_1, \ldots, \alpha_n$ son separables sobre k por Teorema 1.50. Luego, $EF = F(\alpha_1, \ldots, \alpha_n)$ por Observación 1.17, con α_i separable sobre F para todo $1 \leq i \leq n$. Se obtiene que EF es separable sobre F usando el argumento de la torre de cuerpos generados por un elemento en cada paso y Observación 1.48. □

TEOREMA 1.54 (del elemento primitivo). *Sea $E|k$ una extensión finita y separable. Entonces existe $\alpha \in E$ tal que $E = k(\alpha)$.*

DEMOSTRACIÓN. Comenzamos considerando el caso $E = k(\alpha, \beta)$ para $\alpha, \beta \in E$. Además, podemos asumir que k es infinito. En efecto, si k es un cuerpo finito, entonces E también lo es, y todo cuerpo finito cumple que el grupo de elementos no nulos (con respecto a la multiplicación) es cíclico, esto es $E^\times = \langle \gamma \rangle$ para algún $\gamma \in E$ y por lo tanto $E = k(\gamma)$.

Sean $\sigma_1, \dots, \sigma_n$ todos los k-morfismos (distintos) de E a $\bar{k}$. Notar que

$$n = [k(\alpha, \beta) : k]_s = [k(\alpha, \beta) : k],$$

pues E es separable sobre k por hipótesis. Consideremos el polinomio

$$P(x) := \prod_{i \neq j} (\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta)).$$

Cada $\sigma_i : k(\alpha, \beta) \to \bar{k}$ queda determinado por $\sigma_i(\alpha)$ y $\sigma_i(\beta)$. Como $\sigma_i \neq \sigma_j$ para $i \neq j$, $P(x)$ no es idénticamente nulo. Por lo tanto existe $c \in k$ tal que $P(c) \neq 0$ (notar que k debe ser infinito para poder concluir esto, ya que no existe un polinomio no nulo con infinitas raíces).

Obviamente $k(\alpha + c\beta) \subset k(\alpha, \beta)$. Veamos que vale la igualdad mostrando que tienen la misma dimensión. Como

$$0 \neq P(c) = \prod_{i \neq j} (\sigma_i(\alpha + c\beta) - \sigma_j(\alpha + c\beta)),$$

los elementos $\sigma_1(\alpha + c\beta), \dots, \sigma_n(\alpha + c\beta)$ son todos distintos. Entonces $m_{\alpha + c\beta}(x) \in k[x]$ tiene al menos n raíces, por lo tanto

$$n \leq [k(\alpha + c\beta) : k] \leq [k(\alpha, \beta) : k] = n.$$

Esto concluye la prueba de que $k(\alpha + c\beta) = k(\alpha, \beta)$.

Resta mostrar el caso general. Como $E|k$ es finita, entonces $E = k(\alpha_1, \dots, \alpha_n)$ para algunos $\alpha_1, \dots, \alpha_n \in$ por Proposición 1.15. Hemos visto que $k(\alpha_{n-1}, \alpha_n) = k(\beta_{n-1})$ para algún $\beta_{n-1} \in E$. Luego,

$$E = k(\alpha_{n-1}, \alpha_n)(\alpha_1, \dots, \alpha_{n-2}) = k(\alpha_1, \dots, \alpha_{n-2}, \beta_{n-1}).$$

Repitiendo este procedimiento $n - 2$ veces, obtenemos que $E = k(\beta_1)$ para algún $\beta_1 \in E$. □

PROPOSICIÓN 1.55. *Sea k un cuerpo y sea $\alpha \in \bar{k}$ cuyo polinomio minimal es $m_\alpha(x) \in k[x]$.*

- *Si $\mathrm{char}(k) = 0$, entonces todas las raíces de $m_\alpha(x)$ tienen multiplicidad uno (i.e. $m_\alpha(x)$ es separable), por lo tanto α es separable sobre k y $[k(\alpha) : k]_s = \mathrm{gr}(m_\alpha)$.*
- *Si $p := \mathrm{char}(k) > 0$, entonces existe $\mu \geq 0$ entero tal que toda raíz de $m_\alpha(x)$ tiene multiplicidad p^μ,*

  $$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s,$$

  y α^{p^μ} es separable sobre k.

DEMOSTRACIÓN. Sean $\alpha_1, \dots, \alpha_r$ las raíces distintas de $m_\alpha(x)$ en $\bar{k}$, tal que $\alpha_1 = \alpha$. Sea m_j la multiplicidad de α_j en $m_\alpha(x)$, esto es,

$$m_\alpha(x) = \prod_{j=1}^{r} (x - \alpha_j)^{m_j}.$$

Para cada $1 \leq i \leq r$, tomemos la aplicación σ_i determinada por

$$\begin{aligned} \sigma_i : k(\alpha) &\longrightarrow k(\alpha_i), \\ \alpha &\longmapsto \alpha_i, \end{aligned}$$

y lo extendemos a $\sigma_i : \bar{k} \to \bar{k}$.

Como $m_\alpha(x)$ tiene coeficientes en k, tenemos que $m_\alpha^{\sigma_i}(x) = m_\alpha(x)$ para todo i. Luego,

$$\prod_{j=1}^{r}(x - \sigma_i(\alpha_j))^{m_j} = \prod_{j=1}^{r}(x - \alpha_j)^{m_j}.$$

Por la factorización única de polinomios sobre $\bar{k}$, obtenemos que la multiplicidad de la raíz α_i debe ser igual en ambos lados, esto es, $m_1 = m_i$. Como esto es válido para cualquier i, tenemos $m := m_1 = \cdots = m_r$.

Hemos probado que toda raíz de $m_\alpha(x)$ tiene multiplicidad m. Resta mostrar que

$$m = \begin{cases} 1 & \text{si } \operatorname{char}(k) = 0, \\ p^\mu & \text{si } \operatorname{char}(k) = p, \end{cases}$$

para algún entero no negativo μ.

Supongamos que $m \geq 2$ y sea β una raíz de $m_\alpha(x)$. Tenemos que $m_\alpha(\beta) = 0 = m'_\alpha(\beta)$. Luego,

$$\operatorname{mcd}(m_\alpha(x), m'_\alpha(x)) \mid m_\alpha(x).$$

Más aún, como el término del lado izquierdo no es una unidad, y el del derecho es irreducible, entonces ambos son iguales. Entonces $m_\alpha(x) \mid m'_\alpha(x)$, lo cual ocurre solo si $m'_\alpha(x) \equiv 0$.

Cuando $\operatorname{char}(k) = 0$, la conclusión de arriba no puede ocurrir, por lo que hemos mostrado que $m = 1$, esto es, α es separable sobre k.

Ahora asumamos $\operatorname{char}(k) = p$ para algún p primo y $m \geq 2$. La condición $m'_\alpha(x) \equiv 0$ ocurre sólo cuando existe un polinomio $g(x) \in k[x]$ tal que

$$m_\alpha(x) = g(x^p).$$

Luego, $\alpha_1^p, \ldots, \alpha_r^p$ son raíces de $g(x)$, por lo tanto

$$g(x) = \prod_{j=1}^{r}(x - \alpha_j^p)^{m/p},$$

con $\operatorname{gr}(g(x)) = r\frac{m}{p}$. Además

$$[k(\alpha) : k(\alpha^p)] = \frac{[k(\alpha) : k]}{[k(\alpha^p) : k]} = \frac{\operatorname{gr}(m_\alpha(x))}{\operatorname{gr}(g(x))} = \frac{rm}{r\frac{m}{p}} = p$$

Procediendo inductivamente, tomamos el menor entero positivo μ tal que α^{p^μ} es una raíz de un polinomio separable, digamos

$$m_\alpha(x) = h(x^{p^\mu}),$$

con $h(x) \in k[x]$. De la misma manera que arriba, obtenemos que

$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu.$$

Además, como $h(x)$ tiene raíces de multiplicidad uno por ser separable, se tiene que

$$[k(\alpha^{p^\mu}) : k]_s = [k(\alpha^{p^\mu}) : k].$$

Más aún, comparando los grados de $m_\alpha(x)$ y $h(x)$ se ve que el número de raíces distintas de $h(x)$ es r. Luego,

$$r = [k(\alpha) : k]_s = [k(\alpha^{p^\mu}) : k]_s,$$

lo que implica que

$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^\mu})]\,[k(\alpha^{p^\mu}) : k] = p^\mu\,[k(\alpha^{p^\mu}) : k]_s = p^\mu\,[k(\alpha) : k]_s,$$

lo cual completa la demostración. □

COROLARIO 1.56. *Para cualquier extensión finita $E|k$, el grado de separabilidad $[E : k]_s$ divide al grado $[E : k]$. El cociente es 1 si $\mathrm{char}(k) = 0$, y una potencia de p si $\mathrm{char}(k) = p > 0$.*

DEMOSTRACIÓN. Sigue de tomar una torre en donde en cada paso la extensión es generada por un elemento, y luego se aplica la proposición anterior en cada uno de los pasos. □

El *grado de inseparabilidad* de la extensión $E|k$ es definido como el cociente

$$[E : k]_i := \frac{[E : k]}{[E : k]_s}.$$

Se tiene que $[E : k] = [E : k]_s[E : k]_i$. Más información sobre el grado de inseparabilidad, y extensiones *puramente inseparables* (i.e. cuando $[E : k]_s = 1$) se puede consultar en [**Lang**, §V.6].

Problemas.

1.12. Sea $E|k$ una extensión separable. Probar que si existe un entero positivo n tal que $[k(\alpha) : k] \leq n$ para todo $\alpha \in E$, entonces $[E : k] \leq n$. (Ayuda: usar el Teorema del Elemento Primitivo.)

1.13. Una extensión $E|k$ se dice *puramente inseparable* si $[E : k]_s = 1$. Probar que la clase de extensiones puramente inseparables es distinguida.

1.14. Sea k un cuerpo de característica p. Probar que las siguientes afirmaciones son equivalentes.

(a) Toda extensión algebraica de k es separable.
(b) Todo elemento de k tiene una raíz p-ésima en k.

¿Puede dar un cuerpo k donde ocurren estas afirmaciones?

5. Cuerpos finitos

Sea F un cuerpo con una cantidad finita de elementos, digamos q. Consideremos el morfismo de anillos

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow F, \\ 1 &\longmapsto 1, \end{aligned}$$

esto es, $\varphi(m) = m \cdot 1$ para todo $m \in \mathbb{Z}$. Como F es finito, φ tiene núcleo no trivial, el cual es necesariamente un ideal principal de $\mathbb{Z}$, digamos $\mathrm{Nu}(\varphi) = p\mathbb{Z}$ para algún $p \in \mathbb{Z}$. Notar que p debe ser irreducible (i.e. primo) en $\mathbb{Z}$, pues de lo contrario habría divisores de cero en

$$\mathbb{Z}/\,\mathrm{Nu}(\varphi) \simeq \mathrm{Im}(\varphi) \subset F.$$

Concluimos que una copia de $\mathbb{Z}/p\mathbb{Z}$ está en F. En particular, F tiene característica p, pues

$$\underbrace{1+\cdots+1}_{p\text{-veces}}=0.$$

Denotaremos por F_p la copia de $\mathbb{Z}/p\mathbb{Z}$ en F. Como $F_p \subset F$, entonces F tiene una estructura de F_p espacio vectorial. Sea $n = \dim_{F_p} F$, entonces

$$q = \#F = p^n.$$

En efecto, si $\{\omega_1, \ldots, \omega_n\}$ es una F_p-base de F, entonces todo elemento en F puede escribirse de manera única como

$$a_1\omega_1 + \cdots + a_n\omega_n \quad \text{con } a_i \in F_p \text{ para todo } i.$$

El grupo $F^\times$ de unidades de F es obviamente $F \smallsetminus \{0\}$, por lo tanto tiene $q-1$ elementos. Luego,

$$\alpha^{q-1} = 1 \quad \text{para todo } \alpha \in F^\times.$$

Esto nos asegura que el polinomio $f(x) := x^q - x$ se anula en todos los elementos de F. Además, como $\operatorname{gr}(f) = q$, entonces f tiene todas sus raíces distintas, esto es,

$$f(x) = x^q - x = \prod_{\alpha\in F}(x-\alpha).$$

Concluimos que F es el cuerpo de descomposición de $f(x)$. Por lo tanto, F es único salvo isomorfismo por Teorema 1.35. Ahora veremos que la unicidad del cuerpo F con $q = p^n$ elementos es aún más fuerte.

Fijemos p cualquier primo y n un entero positivo, y sea $q = p^n$. Fijemos $\bar{F}_p$ (cualquier) clausura algebraica de F_p. Sea F el cuerpo de descomposición del polinomio $f(x) := x^q - x \in F_p[x]$, esto es,

$$F = F_p(\{\alpha \in \bar{F}_p : f(\alpha) = 0\}).$$

Veamos que

$$F = \{\alpha \in \bar{F}_p : f(\alpha) = 0\}.$$

La inclusión con dirección $\supset$ es clara por la fórmula anterior. Para mostrar $\subset$, es suficiente ver que $E := \{\alpha \in \bar{F}_p : f(\alpha) = 0\}$ es un cuerpo.

Sean $\alpha, \beta \in E$, por lo tanto $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Queremos probar que $\alpha - \beta$ y $\alpha\beta^{-1}$ están en E, o equivalentemente, que son raíces de $f(x) = x^{p^n} - x$. Se tiene que

$$\begin{aligned}
\alpha - \beta \in E \quad &\text{pues} \quad (\alpha-\beta)^{p^n} = \alpha^{p^n} + (-1)^{p^n}\beta^{p^n} = \alpha + (-1)\beta = \alpha - \beta,\\
\alpha\beta^{-1} \in E \quad &\text{pues} \quad (\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}.
\end{aligned}$$

Esto completa la prueba que de E es un cuerpo.

Como además

$$f'(x) = (x^q - x)' = qx^{q-1} - 1 = -1 \neq 0,$$

entonces f no tiene raíces múltiples, por lo tanto $\#F = \operatorname{gr}(f) = q$.

Hemos probado que dentro de $\bar{F}_p$ hay un único cuerpo con p^n elementos, sin necesidad de agregar 'salvo isomorfismo'.

TEOREMA 1.57. *Para cada primo p y $n \geq 1$, existe un cuerpo finito con p^n elementos, únicamente determinado dentro de cualquier clausura algebraica de F_p. Éste es el cuerpo de descomposición del polinomio $x^{p^n} - x \in F_p[x]$, y sus elementos son precisamente sus raíces. Todo cuerpo finito es isomorfo a uno como este para algún p y n como arriba, el cual denotaremos F_{p^n}.*

El resultado de existencia anterior es algo teórico. Veamos una construcción explícita en el caso (no trivial) más simple, es decir, el cuerpo con cuatro elementos.

EJEMPLO 1.58. El único polinomio cuadrático irreducible sobre F_2 es $f(x) := x^2+x+1$. En efecto, tal polinomio debe ser necesariamente de la forma $x^2 + bx + 1$ con $b = 0, 1$, pero $x^2 + 1 = (x + 1)^2$ no es irreducible.

Tenemos que el ideal en $F_2[x]$ generado por $f(x)$ es maximal. Luego, el cociente $F_2[x]/\langle f(x)\rangle$ es un cuerpo de dimensión $\mathrm{gr}(f) = 2$ sobre F_2, esto es, con cuatro elementos.

Se puede ver que hay dos polinomios irreducibles cúbicos sobre F_2. De todas maneras, Teorema 1.57 nos asegura que los dos cuerpos construidos como arriba de $2^3 = 8$ elementos son isomorfos.

COROLARIO 1.59. *Sea F_q un cuerpo finito con q elementos, y sea $m \geq 1$. Dentro de (cualquier) $\bar{F}_q$, existe una única extensión $F|F_q$ de grado m, la cual es F_{q^m}.*

DEMOSTRACIÓN. Denotemos $q = p^n$. Notemos que $\bar{F}_q$ es una clausura algebraica de F_p, pues la extensión $F_q|F_p$ es algebraica por ser finita. Luego, $F_{q^m} = F_{p^{mn}}$ es el cuerpo de descomposición de $x^{p^{mn}} - x$ en $\bar{F}_q$. Si $\alpha \in F_q$, entonces $\alpha^q = \alpha$, por lo tanto

$$\alpha^{q^m} = (\alpha^q)^{q^{m-1}} = \alpha^{q^{m-1}} = (\alpha^q)^{q^{m-2}} = \cdots = \alpha^q = \alpha,$$

lo que equivale a $\alpha \in F_{q^m}$. Esto nos asegura que $F_q \subset F_{q^m}$. Además, por Proposición 1.3 tenemos que

$$[F_{q^m} : F_q] = \frac{[F_{q^m} : F_p]}{[F_q : F_p]} = \frac{mn}{n} = m.$$

Esto muestra la existencia de la extensión de F_q de grado m, usando precisamente F_{q^m}.

Veamos ahora la unicidad de tal extensión. Sea $F|F_q$ extensión de grado m. Entonces $\#F = (\#F_q)^m = (p^n)^m = p^{mn}$, esto es, $F = F_{p^{mn}}$ por Teorema 1.57. □

PROPOSICIÓN 1.60. *Dentro de (cualquier) $\bar{F}_p$, $F_{p^m} \subset F_{p^n}$ si y sólo si m divide a n.*

DEMOSTRACIÓN. Supongamos que $F_{p^m} \subset F_{p^n}$. Sea $r = [F_{p^n} : F_{p^m}]$. Entonces

$$p^n = \#F_{p^n} = (\#F_{p^m})^r = (p^m)^r = p^{mr},$$

y $n = mr$, esto es, m divide a n.

Para la recíproca, supongamos $n = mr$ para algún $r \in \mathbb{Z}$ positivo. Claramente,

$$p^{mr} - 1 = (p^m)^r - 1 = (p^m - 1)(1 + p^m + \cdots + (p^m)^{r-1}).$$

Abreviemos $t = (1 + p^m + \cdots + (p^m)^{r-1})$, esto es $p^{mr} - 1 = (p^m - 1)t$. Luego,

$$x^{p^{mr}-1} - 1 = (x^{p^m-1})^t - 1 = (x^{p^m-1} - 1)(1 + x + \cdots + x^{(p^m-1)(t-1)}),$$

lo que implica que $x^{p^m-1} - 1$ divide a $x^{p^{mr}-1} - 1$, y $x^{p^m} - x$ divide a $x^{p^{mr}} - x$. Concluimos que $F_{p^m} \subset F_{p^{mr}}$, pues los elementos de F_{p^m} y $F_{p^{mr}}$ son raíces de $x^{p^m} - x$ y $x^{p^{mr}} - x$. □

PROPOSICIÓN 1.61. *Si $g(x) \in F_p[x]$ es irreducible y $\mathrm{gr}(g(x))$ divide a n, entonces $g(x)$ divide a $x^{p^n} - x$.*

DEMOSTRACIÓN. Sea $\alpha \in \bar{F}_p$ raíz de $g(x)$. Se tiene que $[F_p(\alpha) : F_p] = \mathrm{gr}(g) =: m$, por lo tanto $\#F_p(\alpha) = p^m$, y $F_p(\alpha) = F_{p^m}$ por Teorema 1.57.

Como m divide a n por hipótesis, Proposición 1.60 implica que $F_p(\alpha) \subset F_{p^n}$, es decir, α es raíz de $x^{p^n} - x$. Sigue que $x^{p^n} - x$ vive en el ideal $\{h \in F_p[x] : h(\alpha) = 0\}$, el cual es generado por $m_\alpha(x) = g(x)$, por lo tanto $g(x)$ divide a $x^{p^n} - x$. □

EJEMPLOS 1.62. Tomemos $p = 2$. ¿Cómo se factorea el polinomio $f(x) := x^8 - x \in F_2[x]$? La proposición anterior resultará extremadamente útil para este tipo de problemas.

Tenemos que $f(x) = x^{2^3} - x$. Luego, Proposición 1.61 asegura que cualquier polinomio irreducible $g(x)$ que divida a $f(x)$ debe tener grado un divisor de 3. No es difícil mostrar a mano que todos los polinomios irreducibles con coeficientes en F_2 de grado menor o igual a 3 son

$$x, \qquad x+1, \qquad x^2+x+1, \qquad x^3+x^2+1, \qquad x^3+x+1.$$

(Esto se puede ver mostrando que el resto de los polinomios tiene a 0 o 1 como raíz. En efecto, el término constante de un polinomio irreducible debe ser 1, y los polinomios restantes x^2+1, x^3+1, x^3+x^2+x+1 se anulan en 1.) Luego, el polinomio $x(x+1)(x^3+x^2+1)(x^3+x+1)$ divide a $f(x)$, y como ambos tienen grado ocho, obtenemos que

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

Tomemos ahora $f(x) = x^{16} - x \in F_2[x]$. Para factorear $f(x)$ usando Proposición 1.61, necesitamos saber todos los polinomios irreducibles de grado 4 con coeficientes en F_2. Luego de listarlos a todos (son 32), y descartar aquellos que se anulen en 0 o 1, nos quedan

$$x^4+x^2+1 \qquad x^4+x+1, \qquad x^4+x^3+1, \qquad x^4+x^3+x^2+x+1.$$

Supongamos que uno de ellos, digamos $g(x)$, no es irreducible. Entonces existe un polinomio $h(x)$ de grado m, con $1 < m < 4$, que divide a $g(x)$. Si $m = 1$, entonces $h(x)$ es x o $x+1$, por lo tanto 0 o 1 es raíz $g(x)$, lo cual no es cierto. De manera similar, si $m = 3$ entonces $g(x)/h(x)$ es un polinomio de grado uno, por lo que nuevamente obtenemos que 0 o 1 es raíz de $g(x)$, lo cual es una contradicción.

Nos queda considerar el caso en que $m = 2$, es decir, existe un polinomio $h(x)$ cuadrático que divide a $g(x)$. Si el cociente $g(x)/h(x)$ que tiene grado dos no fuera irreducible, entonces nuevamente obtenemos que 0 o 1 es raíz de él, y por lo tanto de $g(x)$. Resta solamente considerar el caso en que $g(x)$ es divisible por un polinomio irreducible cuadrático $h(x)$ tal que el polinomio cuadrático $g(x)/h(x)$ es también irreducible. Como el único polinomio cuadrático irreducible en $F_2[x]$ es x^2+x+1, tenemos que $g(x)$ debe ser divisible por x^2+x+1 y $g(x)/(x^2+x+1) = x^2+x+1$, esto es,

$$g(x) = (x^2+x+1)^2 = x^4+x^2+1.$$

Concluimos que todos los polinomios de grado 4 irreducibles en $F_2[x]$ son

$$x^4+x+1, \qquad x^4+x^3+1, \qquad x^4+x^3+x^2+x+1.$$

Luego,

$$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1),$$

pues Proposición 1.61 nos asegura que el polinomio de la derecha divide al de la izquierda, y ambos tienen grado 16.

En los ejemplos anteriores hemos visto que $x^{2^3} - x$ y $x^{2^4} - x$ se descomponen en $F_2[x]$ como el producto de todos los polinomios irreducibles en $F_2[x]$ cuyo grado divide a 3 o 4 respectivamente. El siguiente teorema muestra que esto no ha sido una casualidad.

TEOREMA 1.63. *Para cualquier p primo y n entero positivo, tenemos que*

$$x^{p^n} - x = \prod_{\substack{f \in F_p[x] \text{ irred y mónico:} \\ \mathrm{gr}(f) | n}} f(x).$$

DEMOSTRACIÓN. Llamemos $g(x)$ al polinomio del lado derecho de la fórmula que queremos probar. Proposición 1.61 nos asegura que todos los factores de $g(x)$ dividen a $x^{p^n} - x$, y como éstos son coprimos (por ser irreducibles), entonces $g(x)$ divide a $x^{p^n} - x$. Escribamos $x^{p^n} - x = g(x)h(x)$ para algún $h(x) \in F_p[x]$, el cual es necesariamente mónico. Debemos probar $h(x) = 1$.

Supongamos que $\mathrm{gr}(h(x)) \geq 1$. Existe un polinomio irreducible $m(x) \in F_p[x]$ divisor de $h(x)$ con $d := \mathrm{gr}(m(x)) \geq 1$. Notemos que d no divide a n. En efecto, si d dividiera a n, $m(x)$ dividiría a $g(x)$ y nuevamente a $x^{p^n} - x$, lo que nos dice que $m(x)^2$ divide a $x^{p^n} - x$, lo cual es una contradicción pues $x^{p^n} - x$ no tiene raíces dobles.

Sea $\alpha \in \bar{F}_p$ raíz de $m(x)$. Como $[F_p(\alpha) : F_p] = \mathrm{gr}(m(x)) = d$, entonces $\#F_p(\alpha) = p^d$, lo que implica que $F_p(\alpha) = F_{p^d}$ por Teorema 1.57. Además, α es también necesariamente raíz de $x^{p^n} - x$, por lo tanto $F_{p^d} = F_p(\alpha) \subset F_{p^n}$, y Proposición 1.60 implica que d divide a n, lo cual es una contradicción proveniente de asumir $\mathrm{gr}(h(x)) \geq 1$. Concluimos que $h(x) = 1$ y $g(x) = x^{p^n} - x$. □

El próximo objetivo es describir el grupo de automorfismos $\mathrm{Aut}(F_q)$ de F_q. Claramente $\mathrm{Aut}(F_p) = \{\mathrm{id}_{F_p}\}$, pues un automorfismo arbitrario σ de F_p debe cumplir $\sigma(1) = 1$ y por lo tanto $\sigma(m) = m$ para todo $m \in F_p$.

Ahora supongamos que $q = p^n$ para p un primo racional y n un entero positivo. Sea

$$\begin{aligned} \varphi : F_q &\longrightarrow F_q, \\ x &\longmapsto x^p, \end{aligned}$$

el cual es conocido como el *morfismo de Frobenius*. Veamos que efectivamente es un morfismo. Esto sigue de que, para todo $\alpha, \beta \in F$,

$$\begin{aligned} \varphi(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \varphi(\alpha) + \varphi(\beta), \\ \varphi(\alpha\beta) = (\alpha\beta)^p = \alpha^p \beta^p = \varphi(\alpha)\varphi(\beta). \end{aligned}$$

Además, φ es inyectiva pues el núcleo es no nulo e ideal dentro de un cuerpo, lo que asegura que es trivial. Esto además implica que es suryectivo pues $\varphi(F_p) \subset F_p$ y $\#F_q = q$. Concluimos que $\varphi \in \mathrm{Aut}(F_q)$. Más aún, $\varphi | F_p = \mathrm{id}_{F_p}$, i.e. φ es un F_p-morfismo, por el Pequeño Teorema de Fermat: $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$.

TEOREMA 1.64. *Sean n un entero positivo, p un número primo, y $q = p^n$. Entonces*

$$\mathrm{Aut}(F_q) = \langle \varphi \rangle,$$

de orden n.

DEMOSTRACIÓN. Sea $G = \langle \varphi \rangle$. Claramente $\varphi^n = \mathrm{id}$, pues $\varphi^n(x) = x^{p^n} = x$ para todo $x \in F_q$. Más aún, n es el orden de φ. En efecto, si $d \mid n$ es el orden de φ, entonces

$x = \varphi^d(x) = x^{p^d}$ para todo $x \in F_q$, esto es, $x^{p^d} - x$ tiene $\#F_q = p^n$ raíces, por lo tanto $p^d = \mathrm{gr}(x^{p^d} - x) \geq p^n$, y $d = n$.

Resta ver que $G = \mathrm{Aut}(F_q)$. Cualquier automorfismo de F_q deja invariante a F_p, es decir, es un F_p-morfismo. Por Teorema 1.45, obtenemos que

$$n \leq \#\,\mathrm{Aut}(F_q) = [F_q : F_p]_s \leq [F_q : F_p] = n,$$

lo que implica que $G = \mathrm{Aut}(F_q)$. □

Problemas.

1.15. Probar que un dominio de integridad finito con unidad es un cuerpo.

1.16. Probar que si F es un cuerpo finito, entonces $(F^\times, \cdot)$ es un grupo cíclico. (Ayuda: usar el teorema de descomposición de grupos abelianos.)

1.17. Hallar la factorización en elementos irreducibles del polinomio $f(x) = x^{27} - x$ en $\mathbb{F}_3[x]$.

1.18. Sean p primo racional, $n \geq 1$, $q = p^n$.

(a) Probar que

$$q = \sum_{d|n} d\,\phi(d),$$

donde $\phi(d)$ denota la cantidad de polinomios irreducibles sobre F_q de grado d.

(b) Concluir que

$$n\,\phi(n) = \sum_{d|n} \mu(d) q^{n/d},$$

donde μ es la función de Möbius. (Ayuda: glooglear *Möbius function.*)

1.19. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(1) Toda extensión de cuerpos finitos es normal.
(2) Toda extensión de cuerpos de característica p es normal.
(3) Toda extensión de cuerpos finitos es separable.
(4) En F_q, $q = p^n$, todo elemento tiene una única raíz p-ésima en F_q.
(5) El grupo $\mathrm{Aut}_{F_q}(\overline{F}_q)$ es abeliano con todos sus elementos no triviales de orden finito.

Capítulo 2

Teoría de Galois

1. Correspondencia de Galois

DEFINICIÓN 2.1. Una extensión $E|k$ se dice *Galoisiana* (o *de Galois*) si es normal y separable. Se llama a $\mathrm{Aut}_k(E) = \{\phi : E \to E : k\text{-isomorfismo}\}$ el *grupo de Galois* de la extensión $E|k$, y se denota $\mathcal{G}(E|k)$.

OBSERVACIÓN 2.2. Para una extensión Galoisiana $E|k$, las siguientes propiedades son claras.

- Es claro que $\mathcal{G}(E|k)$ es un grupo.
- Si G es un subgrupo de $\mathrm{Aut}_k(E)$, entonces
$$E^G := \{\alpha \in E : \phi(\alpha) = \alpha \text{ para todo } \phi \in G\}$$
es un subcuerpo de E.
- Sean H y G subgrupos de $\mathrm{Aut}_k(E)$. Entonces, $H \subset G$ si y sólo si $E^H \supset E^G$.
- Como $E|k$ es normal (y asumimos $E \subset \bar{k}$), el grupo $\mathcal{G}(E|k)$ coincide con
$$\{\phi : E \to \bar{k} : k\text{-morfismo}\}.$$

TEOREMA 2.3. *Sea $E|k$ una extensión de Galois, y denotemos $G = \mathcal{G}(E|k)$. Entonces, $E^G = k$. Además, si $k \subset F \subset E$, entonces $E|F$ es también una extensión de Galois y el mapeo*
$$\Phi : \{F : k \subset F \subset E\} \longrightarrow \{\textit{subgrupos de } G\},$$
$$F \longmapsto \mathcal{G}(E|F)$$
es inyectivo.

DEMOSTRACIÓN. La contención $k \subset E^G$ es clara por ser k-morfismos todos los elementos de $\mathcal{G}(E|k)$. Sea $\alpha \in E^G$ y veamos que necesariamente $\alpha \in k$. Sea $\sigma : k(\alpha) \to \bar{k}$ cualquier extensión del morfismo $\mathrm{id} : k \to k$, cuya existencia está garantizada por Teorema 1.30. Extendemos σ a E de cualquier manera, esto es, a un k-morfismo $\sigma : E \to \bar{k}$. Se tiene que $\sigma \in \mathcal{G}(E|k) = G$ por la observación de arriba. Luego, $\sigma(\alpha) = \alpha$ por hipótesis. Como α es separable sobre k, obtenemos que
$$1 = [k(\alpha) : k]_s = [k(\alpha) : k],$$
y por lo tanto $\alpha \in k$.

Ahora tomemos un cuerpo intermedio F de $E|k$, i.e. $k \subset F \subset E$. Tenemos que $E|F$ es una extensión Galoisiana por Proposición 1.21 y Teorema 1.53. En particular, acabamos de probar que $F = E^{\mathcal{G}(E|F)}$.

Supongamos que F y F' son cuerpos intermedios tales que $\mathcal{G}(E|F) = \mathcal{G}(E|F')$. Entonces $F = E^{\mathcal{G}(E|F)} = E^{\mathcal{G}(E|F')} = F'$. Luego, el mapeo Φ es inyectivo. □

COROLARIO 2.4. *Sea $E|k$ una extensión de Galois, y sean F y F' cuerpos intermedios de $E|k$. Entonces*

(1) $E^{\mathcal{G}(E|F)} = F$.
(2) $E^{\mathcal{G}(E|F)\cap\mathcal{G}(E|F')} = FF'$.
(3) $E^{\langle\mathcal{G}(E|F),\mathcal{G}(E|F')\rangle} = F \cap F'$.
(4) $F \subset F'$ *si y sólo si* $\mathcal{G}(E|F) \supset \mathcal{G}(E|F')$.

DEMOSTRACIÓN. (1) fue parte del teorema anterior.

Veamos (2). Tenemos que $\mathcal{G}(E|FF') \subset \mathcal{G}(E|F) \cap \mathcal{G}(E|F')$, lo que implica que

$$FF' = E^{\mathcal{G}(E|FF')} \supset E^{\mathcal{G}(E|F)\cap\mathcal{G}(E|F')}.$$

Para la otra contención, notamos que $F = E^{\mathcal{G}(E|F)} \subset E^{\mathcal{G}(E|F)\cap\mathcal{G}(E|F')}$, y de manera similar $F' \subset E^{\mathcal{G}(E|F)\cap\mathcal{G}(E|F')}$. Luego, el cuerpo composición FF' también está incluido en $E^{\mathcal{G}(E|F)\cap\mathcal{G}(E|F)}$.

(3) queda como ejercicio para el lector.

Para mostrar (4), asumamos que $F \subset F'$. Si $\sigma \in \mathcal{G}(E|F')$, entonces $\sigma : E \to \bar{k}$ es un F'-morfismo, y en particular un F-morfismo. Luego $\mathcal{G}(E|F') \subset \mathcal{G}(E|F)$. Para la recíproca, $\mathcal{G}(E|F) \supset \mathcal{G}(E|F')$ implica que $F = E^{\mathcal{G}(E|F)} \subset E^{\mathcal{G}(E|F')} = F'$. □

EJERCICIO 2.5. Finalizar la demostración de Corolario 2.4 probando el ítem (3).

COROLARIO 2.6. *Sea $E|k$ una extensión finita y separable, y sea E' la extensión normal más pequeña de k que contiene a E. Entonces, $E'|k$ es una extensión de Galois y existen una cantidad finita de cuerpos intermedios de $E|k$.*

OBSERVACIÓN 2.7. En Ejercicio 1.42 mostramos que la extensión normal de k más pequeña que contiene a E es igual a

$$E' = \sigma_1(E) \dots \sigma_n(E),$$

donde $\sigma_1, \dots, \sigma_n$ son todos los k-morfismos de E a $\bar{k}$, y además $E'|k$ es separable.

DEMOSTRACIÓN. Lo que resta de probar a partir de la observación anterior es la finitud de la cantidad de cuerpos intermedios de $E|k$. Esto sigue de que el mapeo Φ es inyectivo y $\mathcal{G}(E'|k)$ es finito. □

TEOREMA 2.8 (de Artin). *Sean E un cuerpo, G un subgrupo finito de* $\mathrm{Aut}(E)$ *de orden n, y $k = E^G$. Entonces $E|k$ es una extensión de Galois finita con $\mathcal{G}(E|k) = G$, y $[E : k] = n$.*

DEMOSTRACIÓN. Veamos primero que la extensión $E|k$ es separable, viendo que todo elemento $\alpha \in E$ es separable. Sea $\{\sigma_1, \dots, \sigma_r\}$ un conjunto maximal de elementos de G tal que los elementos

$$\sigma_1(\alpha), \dots, \sigma_r(\alpha)$$

son distintos entre sí. Si $\tau \in G$, entonces el vector $(\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha))$ es una permutación del vector $(\sigma_1(\alpha), \dots, \sigma_r(\alpha))$. En efecto, τ es inyectivo y además $\tau\sigma_j(\alpha)$ debe estar en $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$ pues si no $\{\sigma_1, \dots, \sigma_r\}$ no sería maximal.

Claramente, $\sigma_j(\alpha) = \alpha$ para algún j, por lo tanto α es una raíz de

$$f(x) := \prod_{j=1}^{r} (x - \sigma_j(\alpha)).$$

Además, f es separable por tener todas sus raíces distintas y $f^\tau(x) = f(x)$ para todo $\tau \in G$, por lo que los coeficientes de $f(x)$ viven en $E^G = k$.

En conclusión, todo $\alpha \in E$ es raíz de un polinomio separable de grado $\leq n$, y este polinomio tiene todas sus raíces en E. Por lo tanto, $E|k$ es separable. Además, Problema 1.12 nos asegura que $[E : k] \leq n$.

La extensión $E|k$ es normal pues para cualquier $\tau : E \to \bar{E} = \bar{k}$ y $\alpha \in E$, $\tau(\alpha) = \sigma_i(\alpha)$ para algún i con $\sigma_1, \ldots, \sigma_r$ como arriba, por lo tanto $\tau(E) \subset E$. La igualdad $\tau(E) = E$ sigue pues ambos cuerpos tienen la misma dimensión.

Además,

$$n = \#G \leq \#\mathcal{G}(E|k) = [E : k]_s = [E : k] \leq n,$$

por lo tanto $\mathcal{G}(E|k) = G$. □

COROLARIO 2.9. *Sea $E|k$ una extensión de Galois finita. Entonces para todo H subgrupo de $\mathcal{G}(E|k)$, existe un único cuerpo intermedio F de $E|k$ tal que $H = \mathcal{G}(E|F)$. En particular, el mapeo Φ es suryectivo con mapeo inverso dado por*

$$\Psi : \{\textit{subgrupos de } G\} \longrightarrow \{F : k \subset F \subset E\},$$

$$H \longmapsto E^H.$$

EJERCICIO 2.10. Sean $E|k$ una extensión de Galois y $\lambda : E \to \lambda E$ un isomorfismo de cuerpos. Probar las siguientes afirmaciones.

(a) $\lambda E|\lambda k$ es Galois.
(b) $\mathcal{G}(\lambda E|\lambda k) = \lambda \mathcal{G}(E|k)\lambda^{-1}$.
(c) Si $\lambda(E) = E$ y $k \subset F \subset E$, entonces $\mathcal{G}(E|\lambda F) = \lambda \mathcal{G}(E|F)\lambda^{-1}$.

TEOREMA 2.11. *Sean $E|k$ una extensión Galoisiana con grupo de Galois $\mathcal{G}(E|k)$, y F un cuerpo intermedio ($k \subset F \subset E$). Entonces, $F|k$ es una extensión normal si y sólo si $\mathcal{G}(E|F)$ es un subgrupo normal de $\mathcal{G}(E|k)$. En este caso,*

$$\mathcal{G}(E|k) \longrightarrow \mathcal{G}(F|k),$$

$$\sigma \longmapsto \sigma|_F$$

es un morfismo suryectivo con núcleo $\mathcal{G}(E|F)$. En particular,

$$\mathcal{G}(F|k) \simeq \mathcal{G}(E|k)/\mathcal{G}(E|F).$$

DEMOSTRACIÓN. Para un cuerpo intermedio fijo $k \subset F \subset E$, abreviemos $G = \mathcal{G}(E|k)$ y $H = \mathcal{G}(E|F)$. Supongamos primero que $F|k$ es una extensión normal, y en consecuencia de Galois. Denotemos $G' = \mathcal{G}(F|k)$. Sea $\sigma \in G$, esto es, un k-morfismo $\sigma : E \to E$. Como $F|k$ es normal, $\sigma(F) = F$. Por lo tanto, $\sigma|_F \in G'$. Luego, tenemos el morfismo de grupos

$$\Theta : G \longrightarrow G',$$

$$\sigma \longmapsto \sigma|_F.$$

Se tiene que

$$\sigma \in \mathrm{Nu}(\Theta) \iff \sigma|_F = \mathrm{id}_F \iff \sigma \in H,$$

por lo tanto, $\mathrm{Nu}(\Theta) = H$ y en consecuencia H es un subgrupo normal de G.

Veamos la recíproca. Supongamos que H es normal en G y tomemos $\lambda : F \to \bar{k}$ un k-morfismo. Queremos mostrar que $\lambda(F) = F$. Extendemos λ a E por Teorema 1.30. Luego $\lambda \in G$ por Observación 2.2. Ejercicio 2.10 nos asegura que

$$\mathcal{G}(E|F) = \lambda\, \mathcal{G}(E|F)\, \lambda^{-1} = \mathcal{G}(E|\lambda F).$$

Entonces $F = E^{\mathcal{G}(E|F)} = E^{\mathcal{G}(E|\lambda F)} = \lambda F$, esto es, $\lambda(F) = F$ y $F|k$ es normal. □

Problemas.

2.1. Una extensión de Galois $E|k$ se dice *abeliana* (*cíclica*) si $\mathcal{G}(E|k)$ es un grupo abeliano (cíclico). Probar las siguientes afirmaciones.

(a) Si $E|k$ es una extensión de Galois abeliana y $k \subset F \subset E$, entonces $F|k$ es una extensión de Galois abeliana.
(b) Si $E|k$ es una extensión de Galois cíclica y $k \subset F \subset E$, entonces $F|k$ es una extensión de Galois cíclica.
(c) Si $E|k$ y $F|k$ son extensiones de Galois abelianas, entonces $EF|k$ también lo es.

2.2. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(a) La clase de extensiones de Galois es distinguida.
(b) La clase de extensiones de Galois abelianas es distinguida.

2. Ejemplos de grupos de Galois

El siguiente enunciado resume lo que probamos en la sección anterior para extensiones finitas.

TEOREMA 2.12. *Sea $E|k$ una extensión de Galois finita. Entonces la aplicación*

$$\Phi : \{F : k \subset F \subset E\} \longrightarrow \{\textit{subgrupos de } \mathcal{G}(E|k)\},$$
$$F \longmapsto \mathcal{G}(E|F)$$

es una biyección con inversa $\Psi(H) = E^H$.

Se cumple que $[E : E^H] = \#H$ para todo subgrupo H de $\mathcal{G}(E|k)$, y además $[E : F] = \#\mathcal{G}(E|F)$ para todo cuerpo intermedio F de $E|k$.

Además, $F|k$ es una extensión de Galois si y sólo si $\mathcal{G}(E|F)$ es un subgrupo normal de $\mathcal{G}(E|k)$, y en ese caso $\sigma \mapsto \sigma|_E$ induce

$$\mathcal{G}(E|k)/\mathcal{G}(E|F) \simeq \mathcal{G}(F|k).$$

EJEMPLO 2.13 (Extensiones cuadráticas). Tomemos la extensión de $k = \mathbb{Q}$ dada por $E = \mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z}$ libre de cuadrados. Denotemos $\alpha = \sqrt{m}$. Claramente $m_\alpha(x) = x^2 - m$ y E es el cuerpo de descomposición de $m_\alpha(x)$, por lo tanto la extensión $E|k$ es normal por Teorema 1.40. Además E es separable sobre k pues la característica de k es cero.

Concluimos que $E|k$ es una extensión de Galois. El correspondiente grupo de Galois está dado por

$$\mathcal{G}(E|k) = \{\mathrm{id}, \sigma\},$$

donde $\sigma : E \to E$ está determinado por $\sigma(\sqrt{m}) = -\sqrt{m}$, esto es,

$$\sigma(a + b\sqrt{m}) = a - b\sqrt{m} \quad \text{para todo } a, b \in \mathbb{Q}.$$

Cuando $m < 0$, σ coincide con la conjugación compleja restringida a E.

Obviamente no hay cuerpos intermedios propios en una extensión cuadrática por un simple argumento de dimensión. Este hecho también sigue de manera simple notando que no hay subgrupos propios en un grupo de dos elementos.

OBSERVACIÓN 2.14. Sea $f \in k[x]$ un polinomio separable. En $\bar{k}$, tenemos la descomposición

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n),$$

con $\alpha_i \neq \alpha_j$ para todo $i \neq j$. El cuerpo de descomposición E de f es una extensión de Galois de k por Teorema 1.40. Sigue que el grupo de Galois $\mathcal{G}(E|k)$ permuta las raíces $\{\alpha_1, \dots, \alpha_n\}$ de $f(x)$, por lo tanto se incrusta en el grupo simétrico de n letras,

$$\mathcal{G}(E|k) \hookrightarrow \mathbb{S}_n.$$

Esta aplicación no es necesariamente sobre.

EJEMPLO 2.15. Sea $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Las raíces de $f(x)$ son

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\,\omega, \quad \sqrt[3]{2}\,\omega^2,$$

donde $\omega = e^{2\pi \mathrm{i}/3}$. Luego, se ve que el cuerpo de descomposición de f cumple

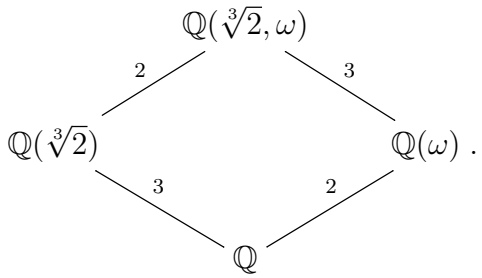
$$E := \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Tal como lo aseguró la observación anterior, $E|\mathbb{Q}$ es una extensión de Galois.

El polinomio $x^2 + x + 1$ es claramente irreducible en $\mathbb{Q}[x]$, pues sus raíces en $\bar{\mathbb{Q}}$ son ω y ω^2. Más aún, como $\omega, \omega^2 \notin \mathbb{R}$, $\omega, \omega^2 \notin \mathbb{Q}(\sqrt[3]{2})$, el polinomio $x^2 + x + 1$ es también irreducible en $\mathbb{Q}(\sqrt[3]{2})[x]$. Por esto, obtenemos que

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})]\ [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \times 3 = 6.$$

Abreviamos todo lo anterior en el diagrama



Ahora describiremos el grupo de Galois $G := \mathcal{G}(E|\mathbb{Q})$. Definimos los elementos σ y τ en G por

$$\sigma : \begin{cases} \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2}, \\ \omega & \mapsto & \omega, \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} & \mapsto & \sqrt[3]{2}, \\ \omega & \mapsto & \omega^2, \end{cases}$$

Se ve fácilmente que $\sigma^3 = \mathrm{id}$, $\tau^2 = \mathrm{id}$. Además,

$$\tau\sigma\tau^{-1} : \begin{cases} \sqrt[3]{2} & \mapsto & \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2}, \\ \omega & \mapsto & \omega^2 & \mapsto & \omega^2 & \mapsto & \omega, \end{cases}$$

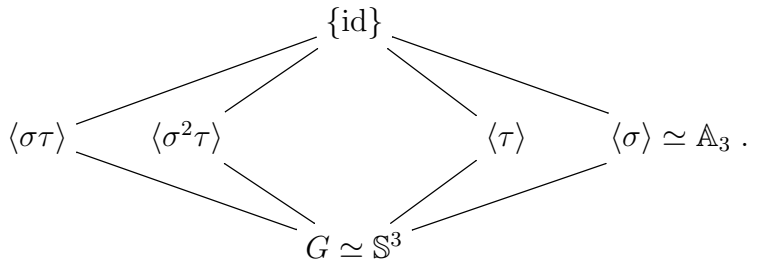
por lo tanto $\tau\sigma\tau^{-1} = \sigma^2$ y $\tau\sigma = \sigma^2\tau$. Luego,

$$\mathbb{S}^3 \supset G \supset \langle \sigma, \tau \rangle = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Como $\mathbb{S}^3$ tiene seis elementos, obtenemos que

$$\mathbb{S}^3 = G = \langle \sigma, \tau \rangle.$$

Graficamos el esquema de subgrupos de $\mathbb{S}^3$ como



Ahora buscamos el correspondiente esquema de cuerpos intermedios de $E|\mathbb{Q}$. El cuerpo intermedio correspondiente a $H := \langle\sigma\tau\rangle$ es E^H. Para determinarlo, notemos que

$$\sigma\tau : \begin{cases} \sqrt[3]{2} & \mapsto & \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2}, \\ \omega & \mapsto & \omega^2 & \mapsto & \omega^2. \end{cases}$$

Luego, $\langle\sigma\tau\rangle = \{\mathrm{id}, \sigma\tau\}$. Como,

$$\sigma\tau(\omega^2\sqrt[3]{2}) = \sigma\tau(\omega)^2\,\sigma\tau(\sqrt[3]{2}) = \omega^4\omega\sqrt[3]{2} = \omega^2\sqrt[3]{2}.$$

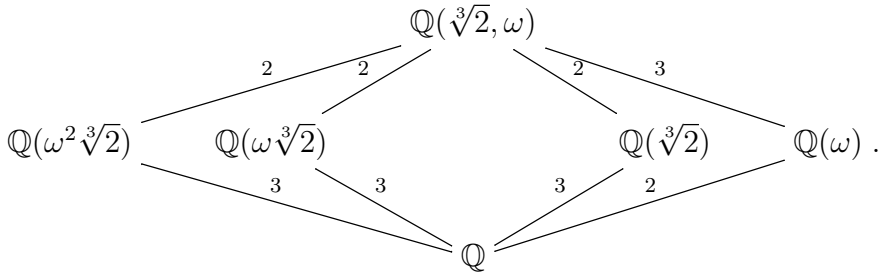
se tiene que $E^{\langle\sigma\tau\rangle} \supset \mathbb{Q}(\omega^2\sqrt[3]{2})$. Además, como $[\mathbb{Q}(\omega^2\sqrt[3]{2}) : \mathbb{Q}] = 3$, se tiene que

$$2 = [E : \mathbb{Q}(\omega^2\sqrt[3]{2})] \geq [E : E^{\langle\sigma\tau\rangle}] = \#\langle\sigma\tau\rangle = 2$$

por lo que concluimos que

$$E^{\langle\sigma\tau\rangle} = \mathbb{Q}(\omega^2\sqrt[3]{2}).$$

Los demás cuerpos intermedios se obtienen de manera similar, obteniendo el diagrama



Los siguientes teoremas facilitarán el cálculo del grupo de Galois para extensiones que involucran un cuerpo de composición.

TEOREMA 2.16. *Sean $E|k$ una extensión de Galois finita, y sea F una extensión arbitraria de k, tal que E y F están contenidos ambos en un cuerpo más grande. Entonces $EF|F$ y $E|E \cap F$ son extensiones de Galois y*

$$\mathrm{rest} : \mathcal{G}(EF|F) \longrightarrow \mathcal{G}(E|E \cap F),$$
$$\sigma \longmapsto \sigma|_E$$

es un isomorfismos de grupos.

DEMOSTRACIÓN. Por hipótesis, $E|k$ es una extensión de Galois. Esto implica las siguientes consecuencias:

- $E|E \cap F$ es de Galois pues $k \subset E \cap F \subset E$ y Teorema 2.3.
- $EF|F$ es normal por Teorema 1.41.
- $EF|F$ es separable por Teorema 1.53.

Concluimos que $EF|F$ es una extensión de Galois.

Denotemos $H = \mathcal{G}(EF|F)$ y $G = \mathcal{G}(E|k)$. Si $\sigma \in H$, entonces $\sigma|_E$ es un k-morfismo, por lo tanto $\sigma|_E \in G$. Esto nos define la aplicación rest. Ésta es inyectiva pues si $\text{rest}(\sigma) = \sigma|_E = \text{id}_E$, junto a que $\sigma|_F = \text{id}_F$, tenemos que $\sigma = \text{id}_{EF}$ pues

$$EF = \left\{ \frac{\sum_i a_i b_i}{\sum_i c_i d_i} : a_i, c_i \in E,\, b_i, d_i \in F,\, \sum_i c_i d_i \neq 0 \right\}.$$

Veamos que rest es suryectiva. Sea H' su imagen, la cual es un subgrupo de G. Para $\sigma \in H'$, claramente tenemos que $\sigma|_{E\cap F} = \text{id}_{E\cap F}$ (pues $E \cap F \subset F$), por lo tanto $E \cap F \subset E^{H'}$. Sea $\alpha \in E^{H'}$. Se tiene que $\alpha \in (EF)^H = F$, por lo tanto $\alpha \in E \cap F$. Concluimos que $E \cap F = E^{H'}$. Como $E|k$ es finita, entonces $H' = \mathcal{G}(E|E \cap F)$ y por lo tanto rest es sobre. □

Corolario 2.17. *Bajo las hipótesis del teorema anterior,*

$$[EF : F] \quad \textit{divide a} \quad [E : k].$$

Demostración. Sigue de que $[EF : F] = \#\mathcal{G}(EF|F) = \#\mathcal{G}(E|E\cap F)$, el cual divide a $\#\mathcal{G}(E|k) = [E : k]$. □

Teorema 2.18. *Sean $E_1|k$ y $E_2|k$ extensiones de Galois, con E_1 y E_2 contenidos en un cuerpo más grande. Entonces $E_1E_2|k$ es una extensión de Galois. El mapeo*

$$\mathcal{G}(E_1E_2|k) \longrightarrow \mathcal{G}(E_1|k) \times \mathcal{G}(E_2|k),$$
$$\sigma \longmapsto (\sigma|_{E_1}, \sigma|_{E_2})$$

es inyectivo. Si $E_1 \cap E_2 = k$, entonces el mapeo es una biyección.

Demostración. Es claro que la extensión $E_1E_2|k$ es de Galois por Teoremas 1.41 y 1.53.

El mapeo es un morfismos de grupos por definición. Veamos primero que es inyectivo. Si $\sigma \in \mathcal{G}(E_1E_2|k)$ cumple $(\sigma|_{E_1}, \sigma|_{E_2}) = (\text{id}_{E_1}, \text{id}_{E_2})$, entonces claramente $\sigma = \text{id}_{E_1E_2}$ por la misma razón que en la demostración de Teorema 2.16.

Queda de ejercicio para el lector mostrar que el mapeo es sobre cuando $E_1 \cap E_2 = k$. □

Ejemplo 2.19. Sea $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. En Ejemplo 1.34 vimos que el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$ es

$$E := \mathbb{Q}(\sqrt[4]{2}, \text{i})$$

y además que $[E : \mathbb{Q}] = 8$. Luego, $\#\mathcal{G}(E|\mathbb{Q}) = 8$.

Definimos τ y σ en $\mathcal{G}(E|\mathbb{Q})$ determinados por

$$\tau : \begin{cases} \sqrt[4]{2} & \mapsto & \sqrt[4]{2}, \\ \text{i} & \mapsto & -\text{i}, \end{cases} \qquad \sigma : \begin{cases} \sqrt[4]{2} & \mapsto & \text{i}\sqrt[4]{2}, \\ \text{i} & \mapsto & \text{i}. \end{cases}$$

Claramente $\tau^2 = \text{id}$ y σ tiene orden 4. Además, τ fija $\mathbb{Q}(\sqrt[4]{2})$ mientras que σ fija $\mathbb{Q}(\text{i})$. Más aún, $\tau \notin \langle\sigma\rangle = \{\text{id}, \sigma, \sigma^2, \sigma^3\}$, por lo tanto $\mathcal{G}(E|\mathbb{Q}) = \langle\sigma, \tau\rangle$. En efecto, como

$$\tau\sigma\tau^{-1} : \begin{cases} \sqrt[4]{2} & \mapsto & \sqrt[4]{2} & \mapsto & \text{i}\sqrt[4]{2} & \mapsto & -\text{i}\sqrt[4]{2}, \\ \text{i} & \mapsto & -\text{i} & \mapsto & -\text{i} & \mapsto & \text{i}, \end{cases}$$

FIGURA 1. Esquema de subgrupos del grupo de Galois de $\mathcal{G}(E|\mathbb{Q})$ de la extensión $E = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})|\mathbb{Q}$. Los subgrupos seguidos del símbolo * son los subgrupos normales de $\mathcal{G}(E|\mathbb{Q})$.

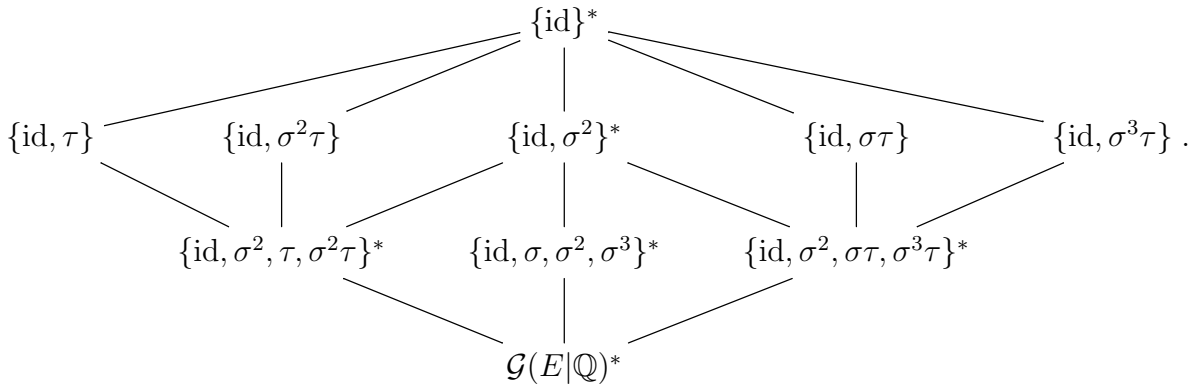
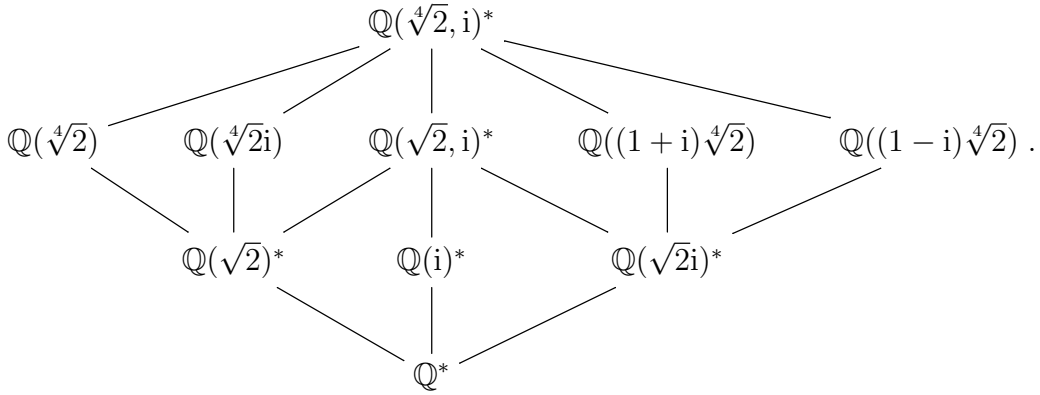


FIGURA 2. Esquema de cuerpos intermedios de la extensión $E = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})|\mathbb{Q}$. Un cuerpo F seguido del símbolo * significa que la extensión $F|\mathbb{Q}$ es normal.



se tiene que $\tau\sigma\tau^{-1} = \sigma^3$, esto es, $\tau\sigma = \sigma^3\tau$, lo que implica que $\langle\sigma, \tau\rangle$ tiene ocho elementos. Más precisamente,

$$\mathcal{G}(E|\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

El esquema de subgrupos de $\mathcal{G}(E|\mathbb{Q})$ se puede ver en Figura 1, mientras que el correspondiente esquema de cuerpos intermedios de la extensión $E|\mathbb{Q}$ está en Figura 2. Veamos un ejemplo de cómo se determinaron estos esquemas.

Tomemos $H = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, el cual es normal en $\mathcal{G}(E|\mathbb{Q})$ por ser de índice dos. Luego, $E|E^H$ es una extensión normal. Claramente, $E^H \supset \mathbb{Q}(\mathrm{i})$. Además, vale la igualdad pues ambas son extensiones cuadráticas de $\mathbb{Q}$.

EJEMPLO 2.20. Estudiemos el grupo de Galois de una extensión dada por el cuerpo de descomposición de un polinomio cúbico con coeficientes racionales. Sea

$$f(x) = x^3 + bx^2 + cx + d \in \mathbb{Q}[x].$$

Notemos que

$$\begin{aligned} f(x-\tfrac{b}{3}) &= (x-\tfrac{b}{3})^3 + b(x-\tfrac{b}{3})^2 + c(x-\tfrac{b}{3}) + d \\ &= x^3 + (\tfrac{b^2}{3} - \tfrac{2b^2}{3} + c)x + (-\tfrac{b^3}{27} + \tfrac{b^3}{9} - \tfrac{bc}{3} + d) \\ &= x^3 + px + q. \end{aligned}$$

Como el mapeo $x \mapsto x - \frac{b}{3}$ se extiende a un automorfismo de $\mathbb{Q}[x]$, se tiene que los cuerpos de descomposición sobre $\mathbb{Q}$ de $f(x)$ y $f(x-\frac{b}{3})$ coinciden.

El párrafo anterior nos permite asumir que

$$f(x) = x^3 + px + q$$

sin perder generalidad. Supongamos que $f(x)$ no tiene raíces en $\mathbb{Q}$, lo que implica que es irreducible sobre $\mathbb{Q}$ por tener grado tres. Sean $\alpha_1, \alpha_2, \alpha_3$ las raíces de $f(x)$ y sea $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$. Definimos

$$\begin{aligned} \Delta &= (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3), \\ D &= \Delta^2. \end{aligned}$$

Por Observación 2.14,

$$G := \mathcal{G}(E|\mathbb{Q}) \hookrightarrow \mathbb{S}^3.$$

Como $\#G = [E : \mathbb{Q}] = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \geq 3$, tenemos que $G = \mathbb{S}^3$ o $G = \mathbb{A}_3$, el subgrupo de $\mathbb{S}^3$ de permutaciones pares. Como todo elemento en G permuta las raíces $\alpha_1, \alpha_2, \alpha_3$, obtenemos que $\sigma(D) = D$ para todo $\sigma \in G$, lo que implica que $D \in E^G = \mathbb{Q}$ por Teorema 2.3. Se tiene que

$$G \simeq \mathbb{S}^3 \iff D \text{ no es un cuadrado en } \mathbb{Q} \iff \Delta \notin \mathbb{Q}.$$

Esto se debe a que son las permutaciones pares los que dejan invariante a Δ, es decir,

$$\{\sigma \in G : \sigma(\Delta) = \Delta\} \simeq \mathbb{A}_3.$$

En efecto, $G = \{\sigma \in G : \sigma(\Delta) = \Delta\}$ implica que $\Delta \in E^G = \mathbb{Q}$, mientras que $G \neq \{\sigma \in G : \sigma(\Delta) = \Delta\}$ implica que $\Delta \notin E^G = \mathbb{Q}$.

Más aún, la equivalencia de arriba es muy útil gracias a la expresión explícita

$$D = -4p^3 - 27q^2.$$

Ésta sigue de la siguiente manera. La igualdad $x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ implica que

$$\begin{cases} 0 = \alpha_1 + \alpha_2 + \alpha_3, \\ p = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\ q = -\alpha_1\alpha_2\alpha_3, \end{cases}$$

por lo tanto resta verificar la tediosa igualdad

$$(\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_1 - \alpha_3)^2 = -4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^3 - 27(-\alpha_1\alpha_2\alpha_3)^2.$$

Una forma más apropiada es usar polinomios simétricos (ver [**Lang**, §IV.6]).

En conclusión,

un polinomio separable $f(x) = x^3 + px + q$ con raíces no racionales tiene grupo de Galois isomorfo a $\mathbb{S}^3$ (o más precisamente el grupo de Galois del cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$ es isomorfo $\mathbb{S}^3$) si y sólo si $-4p^3 - 27q^2$ no es un cuadrado en $\mathbb{Q}$. En caso contrario, el mencionado grupo de Galois es isomorfo a $\mathbb{A}_3$, el cual tiene tres elementos.

Como ejemplo, tomemos $f(x) = x^3 - 3x + 1$. Se puede ver que no tiene raíces reales racionales, por lo tanto es irreducible sobre $\mathbb{Q}$. Además, $D = -4(-3)^3 - 27(1)^2 = 81$. Concluimos que $\mathcal{G}(\mathbb{Q}_f|\mathbb{Q}) \simeq \mathbb{A}_3$.

Ahora tomemos $g(x) = x^3 - 4x + 2$, el cual es irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein. Como $D = -4(-4)^3 - 27(2)^2 = 4 \times 37$ no es un cuadrado, entonces $\mathcal{G}(\mathbb{Q}_g|\mathbb{Q}) \simeq \mathbb{S}^3$.

COMENTARIO 2.21. Se sabe que para cada entero positivo n existe una extensión E de $\mathbb{Q}$ tal que $\mathcal{G}(E|\mathbb{Q}) \simeq \mathbb{S}^n$. Luego, cualquier grupo finito G se incrusta en $\mathbb{S}^n$ para algún n, y por lo tanto existe un cuerpo intermedio F de $E|\mathbb{Q}$ tal que $\mathcal{G}(E|F) \simeq G$. En palabras, todo grupo finito se realiza como el grupo de Galois de alguna extensión $E|F$ con $\mathbb{Q} \subset F$. Contrariamente, el siguiente problema está abierto:

¿Para cualquier grupo finito G existe una extensión $E|\mathbb{Q}$ tal que $\mathcal{G}(E|\mathbb{Q}) \simeq G$?

OBSERVACIÓN 2.22. Teorema 2.12 nos resume la correspondencia de Galois de extensiones **finitas**. La intención de esta observación es mencionar, sin demasiado detalles, la correspondencia de Galois para extensiones no necesariamente finitas. Se recomienda ver [**Lang**, §VI.14] para más detalles.

Notemos que no asumimos la finitud de las extensiones en algunos resultados de Sección 1. En efecto, mostramos que para una extensión de Galois $E|k$ arbitraria, tenemos que

$$\{F : k \subset F \subset E\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{subgrupos de } \mathcal{G}(E|k)\},$$

donde $\Phi(F) = \mathcal{G}(E|F)$ y $\Psi(H) = E^H$, y estos mapeos satisfacen

$$(\Psi \circ \Phi)(F) = F$$

para todo cuerpo intermedio F. Asimismo, es clara la contención

$$(\Phi \circ \Psi)(H) \supset H$$

pues

$$H \subset \{\sigma \in \mathrm{Aut}_k(E) : \sigma|_{E^H} = \mathrm{id}_{E^h}\} = \mathcal{G}(E|E^H) = (\Phi \circ \Psi)(H).$$

La igualdad $(\Phi \circ \Psi)(H) = H$ en general no es cierta, sino que

$$(\Phi \circ \Psi)(H) = \bar{H},$$

donde $\bar{H}$ denota la clausura de H en $\mathcal{G}(E|k)$ con respecto a la *topología de Krull* en $\mathcal{G}(E|k)$. Ésta es definida por la base de entornos de id_E en $\mathcal{G}(E|k)$ dada por

$$\{V \subset \mathcal{G}(E|k) : V \supset \mathcal{G}(E|F) \text{ para alguna extensión } F|k \text{ finita}\}.$$

Se prueba que G es un grupo topológico compacto con esta topología.

Por ejemplo, se puede ver que la extensión infinita de $\mathbb{Q}$ dada por

$$E := \mathbb{Q}(\{\sqrt{p} : p \text{ primo}\})$$

tiene grupo de Galois

$$\mathcal{G}(E|\mathbb{Q}) \simeq \prod_{p \text{ primo}} \mathbb{Z}/2\mathbb{Z},$$

y como consecuencia su cardinal es no numerable.

Otro ejemplo es la extensión infinita de F_q (q primo) dada por

$$E := \bigcup_{n\geq 0} F_{q^{p^n}},$$

donde p es cualquier número primo. En este caso, se tiene el isomorfismo de grupos topológicos

$$\mathcal{G}(E|F_q) \simeq \mathbb{Z}_p := \left\{ \sum_{k\geq 0} a_k p^k : 0 \leq a_k < p \right\},$$

donde $\mathbb{Z}_p$ denotan los *enteros p-ádicos*.

Problemas.

2.3. Mostrar una extensión E de $\mathbb{Q}$ cuyo grupo de Galois sea isomorfo a cada uno de los siguientes grupos:

(a) C_3 (el grupo cíclico de 3 elementos).
(b) $C_2 \times C_2 \times C_2$.
(c) C_5.
(d) $\mathbb{S}^5$ (el grupo simétrico).
(e) $\mathbb{A}_5$ (el grupo alternante).
(f) $\mathbb{D}_5$ (el grupo diedral).

3. Extensiones ciclotómicas

Esta sección está basada en [**Hungerford**, §V.8].

DEFINICIÓN 2.23. Se llama la *extensión ciclotómica de orden n de un cuerpo k* al cuerpo de descomposición del polinomio $x^n - 1$ sobre k.

OBSERVACIÓN 2.24. Supongamos que la característica del cuerpo k divide a n, digamos $n = p^h m$ con $p = \text{char}(k)$, $h \in \mathbb{N}$ y $\text{mcd}(m, p) = 1$. Se tiene que

$$x^n - 1 = (x^m - 1)^{p^h},$$

por lo tanto, las extensiones ciclotómicas de orden n y m son iguales.

A partir de ahora, asumiremos que $\text{char}(k)$ no divide a n, esto es, $\text{char}(k) = 0$ o $\text{char}(k) = p$ con p primo que no divide a n.

DEFINICIÓN 2.25. La función de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ está dada por

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{j \in \mathbb{Z} : 0 \leq j < n,\ \text{mcd}(j, n) = 1\}.$$

EJERCICIO 2.26. Mostrar que el grupo $(\mathbb{Z}/p\mathbb{Z})^\times$ es cíclico para todo p primo.

Para $n \in \mathbb{N}$ en general, el grupo $(\mathbb{Z}/n\mathbb{Z})^\times$ es abeliano pero no necesariamente cícliclo. Por ejemplo

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

TEOREMA 2.27. *Sean n un entero positivo, k un cuerpo cuya característica no divide a n, y F la extensión ciclotómica de k de orden n. Entonces:*

(1) *$F = k(\xi)$, donde $\xi \in F$ es cualquier raíz n-ésima de 1 primitiva;*
(2) *$[F : k]$ divide a $\varphi(n)$;*
(3) *la extensión $F|k$ es de Galois y $\mathcal{G}(F|k)$ es isomorfo a un subgrupo de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

DEMOSTRACIÓN. Es claro que $\mathcal{U}_n := \{\alpha \in \bar{k} : \alpha^n = 1\}$ es un subgrupo abeliano de $\bar{k}^\times$. Además, $\#\mathcal{U}_n = n$ pues la derivada del polinomio $x^n - 1$, nx^{n-1}, no se anula en ningún elemento de $\mathcal{U}_n$ pues $\mathrm{char}(k)$ no divide a n. Veamos que $\mathcal{U}_n$ es cíclico. Por el teorema de descomposición de grupos abelianos, se tiene que existen enteros positivos r y $m_1 \mid m_2 \mid \cdots \mid m_r$ tales que

$$\mathcal{U}_n \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}.$$

Entonces, $\xi^{m_r} = 1$ para todo $\xi \in \mathcal{U}_n$. Como $\#\mathcal{U}_n = n$ y el polinomio $x^{m_r} - 1$ tiene a lo sumo m_r raíces distintas, necesariamente se tiene que $m_r = n$ y $r = 1$, esto es, $\mathcal{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Sea $\xi \in \mathcal{U}_n$ tal que $\mathcal{U}_n = \langle\xi\rangle = \{\xi^l : 0 \le l < n\}$. Entonces, el cuerpo de descomposición F de $x^n - 1$ es generado por ξ, esto es,

$$F = k(\{\xi^l : 0 \le l < n\}) = k(\xi).$$

Luego, la extensión $F|k$ es separable, y por lo tanto de Galois por ser normal por Teorema 1.40. Más aún, si $\sigma \in \mathcal{G}(F|k)$, entonces $\sigma(\xi) = \xi^h$ para algún h tal que $0 \le h < n$ y $\mathrm{mcd}(h, n) = 1$, ya que $\sigma(\xi)$ debe ser nuevamente una raíz primitiva de $x^n - 1$. Entonces, la asignación

$$\begin{aligned} \mathcal{G}(F|k) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \\ \sigma &\longmapsto h \end{aligned}$$

es un monomorfismo de grupos. En efecto, si $\sigma_i(\xi) = \xi^{h_i}$ para $i = 1, 2$, entonces

$$\sigma_1(\sigma_2(\xi)) = \sigma_1(\xi^{h_2}) = \sigma_1(\xi)^{h_2} = (\xi^{h_1})^{h_2} = \xi^{h_1 h_2}.$$

Luego, $[F : k] = \#\mathcal{G}(F|k)$ divide a $\varphi(n)$ y $\mathcal{G}(F|k)$ es isomorfo a la imagen de la aplicación de arriba. □

EJEMPLO 2.28. Sea $\xi = e^{2\pi \mathrm{i}/3}$. Su polinomio minimal está dado por $m_\xi(x) = x^2 + x + 1$, por lo tanto $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$. Notar que $\varphi(3) = \#(\mathbb{Z}/3\mathbb{Z})^\times = 2$, por lo tanto

$$\mathcal{G}(\mathbb{Q}(\xi)|\mathbb{Q}) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}.$$

En efecto, $\mathcal{G}(\mathbb{Q}(\xi)|\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, donde $\sigma(\alpha) = \bar{\alpha}$ (conjugación compleja) pues $\sigma(\xi) = \xi^2 = \bar{\xi}$.

En el siguiente ejemplo vemos que la aplicación de arriba puede estar lejos de ser suryectiva.

EJEMPLO 2.29. Sea n cualquier entero positivo mayor a 2. Si $\xi^n - 1 = 0$ y $\xi \neq \pm 1$, entonces $\mathbb{R}(\xi) = \mathbb{C}$, por lo que $\#\mathcal{G}(\mathbb{C}|\mathbb{R}) = 2 < \varphi(n)$ para todo n suficientemente grande (¿Cuánto?).

DEFINICIÓN 2.30. Sean n un entero positivo y k un cuerpo cuya característica no divide a n. El *n-ésimo polinomio ciclotómico sobre k* es

$$\Phi_n(x) := (x - \xi_1) \dots (x - \xi_r),$$

donde $\xi_1, \dots, \xi_r$ son las raíces n-ésimas de la unidad primitivas.

EJEMPLO 2.31. Consideremos $k = \mathbb{Q}$. Claramente $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$. Además, $\Phi_3(x) = x^2 + x + 1$ por Ejemplo 2.28, y $\Phi_4(x) = x^2 + 1$ pues las raíces primitivas cuartas de la unidad son i y $-$i.

PROPOSICIÓN 2.32. *Sean n un entero positivo y k un cuerpo cuya característica no divide a n. Se tiene*

(1) $x^n - 1 = \prod_{d|n} \Phi_d(x)$;
(2) $\Phi_n(x) \in k[x]$, *y si* $k = \mathbb{Q}$ *entonces* $\Phi_n(x) \in \mathbb{Z}[x]$ *y es mónico;*
(3) $\mathrm{gr}(\Phi_n(x)) = \varphi(n)$.

DEMOSTRACIÓN. Sea ξ una raíz n-ésima de 1 primitiva. Como $\{\alpha \in \bar{k} : \alpha^n = 1\} = \langle\xi\rangle = \{\xi^h : 0 \leq h < n\}$, obtenemos que

$$x^n - 1 = \prod_{h=0}^{n-1}(x - \xi^h) = \prod_{d|n} \prod_{\substack{0\leq h<n:\\ \mathrm{mcd}(h,n)=\frac{n}{d}}} (x - \xi^h) = \prod_{d|n} \Phi_d(x).$$

La última igualdad sigue de que el elemento ξ^h con $\mathrm{mcd}(h, n) = \frac{n}{d}$ tiene orden d.

Ahora veamos la segunda afirmación. Para $\sigma \in \mathcal{G}(k(\xi)|k)$,

$$\Phi_n^\sigma(x) = \prod_{\substack{0\leq h<n:\\ \mathrm{mcd}(h,n)=1}} (x - \sigma(\xi^h)) = \prod_{\substack{0\leq h<n:\\ \mathrm{mcd}(h,n)=1}} (x - \xi^h),$$

pues σ permuta las raíces n-ésimas de la unidad primitivas. Concluimos que $\Phi_n(x)$ tiene coeficientes en $k(\xi)^{\mathcal{G}(k(\xi)|k)} = k$.

Supongamos $k = \mathbb{Q}$. Obviamente $\Phi_1(x) = x - 1$. Sigue que $\Phi_n(x)$ tiene coeficientes enteros por inducción fuerte. En efecto, como

$$\Phi_n(x) = (x^n - 1)/\prod_{d|n,\, d\neq n} \Phi_d(x),$$

$x^n - 1 \in \mathbb{Z}[x]$, y $\Phi_d(x) \in \mathbb{Z}[x]$ para todo divisor d de n con $d < n$ por hipótesis inductiva fuerte, entonces $x^n - 1 = \Phi_n(x)q(x)$ con $q(x) \in \mathbb{Z}[x]$, por lo que la unicidad del algoritmo de la división en $\mathbb{Z}[x]$ nos dice que $\Phi_n(x) \in \mathbb{Z}[x]$.

La tercera afirmación sigue de que $\mathrm{gr}(\Phi_n(x))$ es igual al número de raíces n-ésimas de la unidad primitivas, el cual es igual a $\varphi(n)$. □

EJEMPLOS 2.33. Proposición 2.32 nos asegura que

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{(x^3 - 1)(x^3 + 1)}{(x + 1)(x^3 - 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

para todo cuerpo de característica distinta de 2 y 3. Además, para cualquier número primo p, se tiene que

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

para cualquier cuerpo k de característica distinta a p. También tenemos que

$$\begin{aligned}\Phi_{2p}(x) &= \frac{x^{2p} - 1}{\Phi_1(x)\Phi_2(x)\Phi_p(x)} = \frac{(x^p - 1)(x^p + 1)}{(x^p - 1)(x + 1)} \\ &= x^{p-1} - x^{p-2} + \cdots + x^2 - x + 1 = \Phi_p(-x)\end{aligned}$$

si k tiene característica distinta a 2 y p.

Sea k un cuerpo de característica distinta de p. Veamos que

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

para cualquier $r \in \mathbb{N}$. Fijemos $r \in \mathbb{N}$ y llamemos $f(x)$ al polinomio de la derecha. Notar que $f(x)$ se anula en toda raíz primitiva de la unidad de orden p^r, ya que todas ellas son anuladas por el polinomio $x^{p^r}-1$ pero no por $x^{p^{r-1}}-1$. Luego, $\Phi_{p^r}(x)$ divide a $f(x)$. La igualdad sigue de que ambos tienen grado igual a $\varphi(p^r) = (p-1)p^{r-1}$.

A partir de ahora nos concentraremos en el caso $k = \mathbb{Q}$.

TEOREMA 2.34. *Sea n un entero positivo y sea F la extensión ciclotómica de orden n en $\mathbb{Q}$. Entonces*

(1) *$\Phi_n(x)$ es irreducible en $\mathbb{Q}[x]$;*
(2) *$[F:\mathbb{Q}] = \varphi(n)$;*
(3) *$\mathcal{G}(F|\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

DEMOSTRACIÓN. Es claro que (1) implica (2) y (3). Para probar (1) usaremos el siguiente lema (ver por ejemplo [**Hungerford**, Lem. 6.13]):

> Sean D un dominio de factorización única, k el cuerpo cociente de D, y $f(x) \in D[x]$ primitivo (i.e. el ideal en D generado por sus coeficientes es D) de grado positivo. Entonces, f es irreducible en $D[x]$ si y sólo si es irreducible en $k[x]$.

Luego, es suficiente ver que $\Phi_n(x)$ es irreducible sobre $\mathbb{Z}[x]$. Sea $h(x) \in \mathbb{Z}[x]$ un factor irreducible de $\Phi_n(x)$ de grado positivo, por lo que $\Phi_n(x) = h(x)f(x)$ para algún $f(x) \in \mathbb{Z}[x]$. Notar que los coeficientes principales de h y f son ambos iguales a 1 o -1 pues $\Phi_n(x)$ es mónico. Podemos asumir que son iguales a 1 multiplicando por -1 a ambos en caso de ser necesario.

AFIRMACIÓN. *Si ξ es una raíz de $h(x)$, entonces ξ^p es también una raíz de $h(x)$ para todo p primo tal que $p \nmid n$.*

DEMOSTRACIÓN. Sea p primo tal que $p \nmid n$ y sea ξ una raíz de $h(x)$. Como ξ es también raíz de $\Phi_n(x)$, ξ^p es una raíz n-ésima de la unidad primitiva. Luego, ξ^p es raíz de $h(x)$ o de $f(x)$.

Supongamos que ξ^p es raíz de $f(x)$. Escribimos $f(x) = \sum_{i=0}^r a_i x^i$. Entonces ξ es raíz de $h(x)$ y del polinomio $f(x^p) = \sum_{i=0}^r a_i x^{ip}$. Como $h(x)$ es irreducible, tenemos que $h(x)$ divide a $f(x^p)$ en $\mathbb{Q}[x]$, esto es,

$$f(x^p) = h(x)k(x)$$

para algún $k(x) \in \mathbb{Q}[x]$. Aplicando el algoritmo de la división en $\mathbb{Z}[x]$, tenemos que existen $k_1(x), r_1(x) \in \mathbb{Z}[x]$ tales que

$$f(x^p) = h(x)k_1(x) + r_1(x).$$

Estas situaciones fuerzan a que $k(x) = k_1(x) \in \mathbb{Z}[x]$ y $r_1 \equiv 0$.

Consideremos el morfismo

$$\begin{aligned} \mathbb{Z}[x] &\longrightarrow \mathbb{Z}/p\mathbb{Z}[x], \\ g(x) = \sum b_i x^i &\longmapsto \bar{g}(x) = \sum \bar{b}_i x^i, \end{aligned}$$

donde $\bar{b}$ denota la clase de $b \in \mathbb{Z}$ en $\mathbb{Z}/p\mathbb{Z}$. En el anillo $\mathbb{Z}/p\mathbb{Z}[x]$, tenemos que

$$\bar{h}(x)\bar{k}(x) = \bar{f}(x^p) = (\bar{f}(x))^p.$$

Luego, todo factor irreducible de $\bar{h}(x)$ en $\mathbb{Z}/p\mathbb{Z}$ divide a $\bar{f}(x)$.

Además, Φ_n divide a $x^n - 1$, por lo tanto $x^n - 1 = \Phi_n(x)q(x)$ para algún $q(x) \in \mathbb{Z}[x]$. Nuevamente en el anillo $\mathbb{Z}/p\mathbb{Z}[x]$, tenemos que

$$\overline{x^n - 1} = \bar{h}(x)\bar{f}(x)\bar{q}(x).$$

Por lo tanto hay un polinomio irreducible en $\mathbb{Z}/p\mathbb{Z}[x]$ que divide a $\bar{h}(x)$ y $\bar{f}(x)$, lo cual es una contradicción pues $x^n - 1$ es separable en $\mathbb{Z}/p\mathbb{Z}[x] = F_p[x]$ ya que $p \nmid n$. El absurdo proviene de suponer que ξ^p es raíz de $f(x)$, por lo tanto la afirmación está demostrada. ■

Sea ξ una raíz de $h(x)$. Repetidas aplicaciones de la afirmación aseguran que ξ^r es una raíz de $h(x)$ para todo $r \in \mathbb{Z}$ satisfaciendo $0 \leq r < n$ y $\operatorname{mcd}(r, n) = 1$. En efecto, usando la factorizando en primos $r = p_1^{k_1} \dots p_s^{k_s}$ con $p_i \nmid n$ para todo i, tenemos que ξ^{p_1} es raíz de $h(x)$, por lo tanto $\xi^{p_1^2} = (\xi^{p_1})^{p_1}$ es raíz de $h(x)$, y así sucesivamente.

Como $\operatorname{gr}(\Phi_n(x)) = \varphi(n)$, número que coincide con el número de raíces en

$$\{\xi^r : r \in \mathbb{Z},\ 0 \leq r < n,\ \operatorname{mcd}(r, n) = 1\}$$

de $h(x)$, concluimos que $\Phi_n(x) = h(x)$, y por lo tanto $\Phi_n(x)$ es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$, lo cual finaliza la prueba. □

Ejemplo 2.35. Sea E la extensión ciclotómica de orden 7 en $\mathbb{Q}$, esto es, E es el cuerpo de descomposición sobre $\mathbb{Q}$ de $x^7 - 1$. Teorema 2.27 nos asegura que $E = \mathbb{Q}(\xi)$ donde $\xi = e^{2\pi \mathrm{i}/7}$. Estudiemos cuáles son los cuerpos intermedios F de la extensión $E|\mathbb{Q}$.

Por Teorema 2.34, $[E : \mathbb{Q}] = \varphi(7) = 6$ y

$$G := \mathcal{G}(E|\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

En consecuencia, existen elementos σ y τ en G de orden 3 y 2 respectivamente tales que

$$G = \langle \sigma, \tau \rangle = \{\sigma^i \tau^j : 0 \leq i \leq 2,\ 0 \leq j \leq 1\}.$$

En $(\mathbb{Z}/7\mathbb{Z})^\times$, $\bar{2}$ tiene orden 3 pues $2^3 = 8 \equiv 1 \pmod 7$ y $\bar{6}$ tiene orden 2 pues $6^2 = 36 \equiv 1 \pmod 7$. El isomorfismo entre G y $(\mathbb{Z}/7\mathbb{Z})^\times$ dado en la demostración de Teorema 2.27 nos dice que podemos tomar $\sigma, \tau : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi)$ determinados por

$$\sigma(\xi) = \xi^2, \qquad \tau(\xi) = \xi^6.$$

Claramente, los únicos subgrupos propios de G son $\langle \sigma \rangle$ y $\langle \tau \rangle$. Luego, $E^{\langle \sigma \rangle} = E^\sigma$ y $E^{\langle \tau \rangle} = E^\tau$ son los únicos cuerpos intermedios de $E|\mathbb{Q}$. Veamos una descripción más explícita de ellas.

Sabemos que $\{1, \xi, \dots, \xi^5\}$ es una $\mathbb{Q}$-base de E pues $\Phi_7(x) = x^6 + \dots + x + 1$ es el polinomio irreducible de ξ. Luego, $\alpha := \sum_{i=0}^5 a_i \xi^i \in E^\tau$ si y sólo si

$$\begin{aligned}
\alpha = \tau(\alpha) &= \sum_{i=0}^{5} a_i \xi^{6i} = a_0 + a_1\xi^6 + a_2\xi^{12} + a_3\xi^{18} + a_4\xi^{24} + a_5\xi^{30} \\
&= a_0 - a_1(1 + \xi + \dots + \xi^5) + a_2\xi^5 + a_3\xi^4 + a_4\xi^3 + a_5\xi^2 \\
&= (a_0 - a_1) - a_1\xi + (a_5 - a_1)\xi^2 + (a_4 - a_1)\xi^3 + (a_3 - a_1)\xi^4 + (a_2 - a_1)\xi^5.
\end{aligned}$$

Igualando coeficientes, obtenemos que $\alpha \in E^\tau$ si y sólo si

$$\begin{aligned} a_0 &= a_0 - a_1, & a_2 &= a_5 - a_1, & a_4 &= a_3 - a_1, \\ a_1 &= -a_1, & a_3 &= a_4 - a_1, & a_5 &= a_2 - a_1. \end{aligned}$$

Esto nos dice que

$$E^\tau = \{a_0 + a_2(\xi^2 + \xi^5) + a_3(\xi^3 + \xi^4) : a_0, a_2, a_3 \in \mathbb{Q}\}.$$

Ahora veamos que $E^\tau = \mathbb{Q}(\xi^2 + \xi^5)$. La igualdad $(\xi^2 + \xi^5)^2 = 2 + \xi^3 + \xi^4$ nos asegura que $E^\tau \subset \mathbb{Q}(\xi^2 + \xi^5)$. Además,

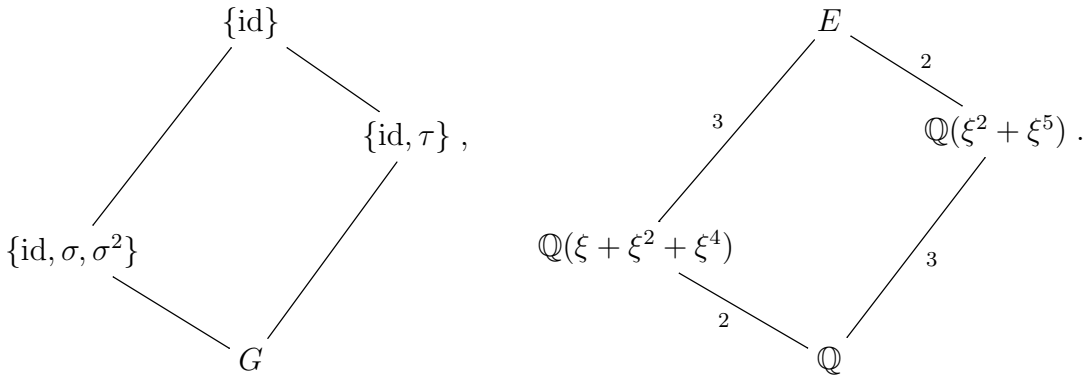
$$\begin{aligned} (\xi^2 + \xi^5)^3 &= (\xi^2 + \xi^5)(2 + \xi^3 + \xi^4) = 2(\xi^2 + \xi^5) + \xi^5 + \xi^6 + \xi + \xi^2 \\ &= 2(\xi^2 + \xi^5) - (1 + \xi^3 + \xi^4) = 2(\xi^2 + \xi^5) + 1 - (\xi^2 + \xi^5)^2, \end{aligned}$$

lo que implica que $\xi^2 + \xi^5$ es raíz de $x^3 + x^2 - 2x - 1$, por lo tanto $[\mathbb{Q}(\xi^2 + \xi^5) : \mathbb{Q}] \leq 3$. Concluimos que

$$E^\tau = [\mathbb{Q}(\xi^2 + \xi^5) : \mathbb{Q}].$$

Más aún, se puede mostrar que el polinomio minimal de $\xi^2 + \xi^5$ es igual a $x^3 + x^2 - 2x - 1$ (ver Ejercicio 2.36).

De manera similar (y levemente más simple) se ve que $E^\sigma = \mathbb{Q}(\xi + \xi^2 + \xi^4)$ (ver Ejercicio 2.36). Concluimos que los esquemas de subgrupos de G y de cuerpos intermedios de la extensión $E|\mathbb{Q}$ son



Por último, se puede ver que $E^\sigma = \mathbb{Q}(\sqrt{-7})$ (ver Ejercicio 2.36). Observación 2.37 muestra que este hecho proviene de una situación más general.

Ejercicio 2.36. Completar los detalles en Ejemplo 2.35 probando las siguientes afirmaciones:

(a) Mostrar que el polinomio minimal de $\xi^2 + \xi^5$ sobre $\mathbb{Q}$ es igual a $x^3 + x^2 - 2x - 1$.
(b) Mostrar que $E^\sigma = \{a_0 + a_1(\xi + \xi^2 + \xi^4) : a_0, a_1 \in \mathbb{Q}\}$, donde $\sigma : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi)$ está determinado por $\sigma(\xi) = \xi^2$.
(c) Determinar el polinomio minimal sobre $\mathbb{Q}$ de $\xi + \xi^2 + \xi^4$ y concluir que $E^\sigma = \mathbb{Q}(\xi + \xi^2 + \xi^4)$.
(d) Mostrar que $\mathbb{Q}(\xi + \xi^2 + \xi^4) = \mathbb{Q}(\sqrt{-7})$.

Observación 2.37. Sea p un primo arbitrario y consideremos $E = \mathbb{Q}(\xi)$ con $\xi = e^{2\pi i/p}$. Luego, $[E : \mathbb{Q}] = p - 1$ es un número par. Factoreando $p - 1 = 2^{r_0} p_1^{r_1} \dots p_h^{r_h}$, obtenemos que

$$\mathcal{G}(E|\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/2^{r_0}\mathbb{Z} \times \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_h^{r_h}\mathbb{Z}.$$

Notemos que existe un único subgrupo H de $\mathcal{G}(E|\mathbb{Q})$ de orden $\frac{p-1}{2}$, el cual es isomorfo a

$$2(\mathbb{Z}/2^{r_0}\mathbb{Z}) \times \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_h^{r_h}\mathbb{Z} \simeq \mathbb{Z}/2^{r_0-1}\mathbb{Z} \times \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_h^{r_h}\mathbb{Z}.$$

Teorema 2.12 nos asegura que E^H es el único cuerpo intermedio con $[E : E^H] = \frac{p-1}{2}$. Como

$$[E^H : \mathbb{Q}] = \frac{[E : \mathbb{Q}]}{[E : E^H]} = \frac{p-1}{\frac{p-1}{2}} = 2,$$

concluimos que existe un único cuerpo intermedio de $E|\mathbb{Q}$ de grado 2 sobre $\mathbb{Q}$.

EJERCICIO 2.38. Mostrar que el único cuerpo intermedio F de la extensión $\mathbb{Q}(e^{2\pi i/p})|\mathbb{Q}$ (como en Observación 2.37) de grado dos sobre $\mathbb{Q}$ es igual a

$$F = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{si } p \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-p}) & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Problemas.

2.4. Para cualquier entero positivo n, determinar la extensión ciclotómica de orden n sobre F_2.

2.5. Dado p un primo impar, mostrar que el único subgrupo de índice dos de $(\mathbb{Z}/p\mathbb{Z})^\times$ es el grupo de residuos cuadráticos

$$\{\overline{h^2} \in (\mathbb{Z}/p\mathbb{Z})^\times : h \in \mathbb{Z},\ 0 \leq h < p\}.$$

Capítulo 3

Anillos de enteros

1. Enteros algebraicos

A partir de ahora, nuestro cuerpo base k será el cuerpo de los números racionales $\mathbb{Q}$. Recordemos que en Definición 1.1 llamamos a $\alpha \in \mathbb{C}$ un número algebraico si existe un polinomio $f \in \mathbb{Q}[x]$ no nulo tal que $f(\alpha) = 0$. Además, denotamos

$$\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ es algebraico}\},$$

el cual coincide con la clausura algebraica de $\mathbb{Q}$.

Definición 3.1. Decimos que $\alpha \in \mathbb{C}$ es un *entero algebraico* si existe un polinomio mónico $f(x) \in \mathbb{Z}[x]$ tal que $f(x) = 0$.

Ejemplos 3.2. Aquí van diversos ejemplos de enteros algebraicos:

- $m \in \mathbb{Z}$ pues $x - m \in \mathbb{Z}[x]$ lo anula;
- $\sqrt[n]{m}$ con $m \in \mathbb{Z}$ y $n \in \mathbb{N}$ pues $x^n - m \in \mathbb{Z}[x]$ lo anula;
- $e^{2\pi i h/m}$ para $m \in \mathbb{N}$ y $h \in \mathbb{Z}$, pues $x^m - 1 \in \mathbb{Z}[x]$ lo anula;

Observación 3.3. Veamos que si $\alpha \in \bar{\mathbb{Q}}$, entonces existe $n \in \mathbb{N}$ tal que $n\alpha$ es un entero algebraico. Escribimos el polinomio minimal $m_\alpha(x) \in \mathbb{Q}[x]$ de α como

$$m_\alpha(x) = x^d + \sum_{k=0}^{d-1} \frac{a_k}{b_k} x^k.$$

Luego, basta tomar $n = b_0 \dots b_{d-1}$. En efecto,

$$0 = n^d \, m_\alpha(\alpha) = (n\alpha)^d + \sum_{k=0}^{d-1} a_k \frac{n^{d-k}}{b_k} (n\alpha)^k = f(n\alpha),$$

donde el polinomio

$$f(x) := x^m + \sum_{k=0}^{d-1} a_k \frac{n^{d-k}}{b_k} x^k$$

tiene coeficientes enteros y es mónico.

El siguiente objetivo es mostrar que el conjunto

$$\mathcal{O} := \{\alpha \in \mathbb{C} : \alpha \text{ es entero algebraico}\}$$

es un anillo, esto es, la suma y la multiplicación de enteros algebraicos vuelven a ser enteros algebraicos. El siguiente resultado será muy útil para su demostración.

Teorema 3.4. *Las siguientes afirmaciones son equivalentes para cualquier $\alpha \in \mathbb{C}$:*

(1) *α es entero algebraico;*
(2) *$m_\alpha(x) \in \mathbb{Z}[x]$;*

(3) $\mathbb{Z}[\alpha]$ *es un* $\mathbb{Z}$*-módulo finitamente generado;*
(4) *existe un* $\mathbb{Z}$*-submódulo finitamente generado* M *de* $\mathbb{C}$ *tal que* $\alpha M \subset M$.

DEMOSTRACIÓN. Comencemos mostrando que (1) implica (2). Supongamos que α es un entero algebraico. Sea $f(x) \in \mathbb{Z}[x]$ mónico tal que $f(\alpha) = 0$. Existe $g(x) \in \mathbb{Q}[x]$ tal que

$$f(x) = m_\alpha(x)g(x).$$

Notar que $g(x)$ es mónico pues $f(x)$ y $m_\alpha(x)$ lo son. Escribimos

$$m_\alpha(x) = \tfrac{a}{b}\, h_1(x), \qquad\qquad g(x) = \tfrac{c}{d}\, g_1(x),$$

con $a, b, c, d \in \mathbb{Z}$, $bd \neq 0$, $\operatorname{mcd}(a, b) = 1 = \operatorname{mcd}(c, d)$, y $h_1(x), g_1(x) \in \mathbb{Z}[x]$ primitivos. Lema de Gauss (ver por ejemplo [**Lang**, Thm. 2.1, Ch. IV]) nos asegura que $h_1(x)g_1(x)$ es primitivo.

Luego,

$$bd\, f(x) = ac\, h_1(x)g_1(x).$$

Tomando el máximo común divisor entre los coeficientes de estos dos polinomios, obtenemos que $f(x) = \pm h_1(x)g_1(x)$. Esto nos asegura que los términos principales de $h_1(x)$ y $g_1(x)$ son ± 1. Como $m_\alpha(x)$ es mónico, obtenemos que $\frac{a}{b} = \pm 1$, y concluimos que $m_\alpha(x) = \pm h_1(x) \in \mathbb{Z}[x]$.

Notar que (2) implica (3) sigue de manera muy simple. En efecto, $m_\alpha(x) \in \mathbb{Z}$ nos dice que $\mathbb{Z}[\alpha]$ es generado como $\mathbb{Z}$-módulo por $\{\alpha^k : 0 \leq k \leq d-1\}$, donde $d = \operatorname{gr}(m_\alpha(x))$. Además, (3) implica (4) es inmediata.

Resta ver (4) implica (1). Supongamos que M es un $\mathbb{Z}$-submódulo de $\mathbb{C}$ finitamente generado tal que $\alpha M \subset M$. Sean $a_1, \ldots, a_n$ generadores de M, esto es,

$$M = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n.$$

Para $1 \leq i \leq n$ fijo, como $\alpha a_i \in M$ se tiene que existen $c_{i,1}, \ldots, c_{i,n} \in \mathbb{Z}$ tales que

$$\alpha a_i = c_{i,1}a_1 + \cdots + c_{i,n}a_n.$$

Formando la matriz $C = (c_{i,j})_{i,j}$, notamos que

$$C \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \alpha \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

es decir, α es un autovalor de C. Luego,

$$0 = \det(\alpha I - C) = \alpha^n - \operatorname{Tr}(C)\, \alpha^{n-1} + \ldots.$$

Como C tiene todos sus coeficientes en $\mathbb{Z}$, se tiene que el polinomio mónico $\det(xI - C)$ también tiene sus coeficientes en $\mathbb{Z}$. Concluimos que α es entero algebraico. □

COROLARIO 3.5. *El conjunto* $\mathcal{O}$ *es subanillo de* $\mathbb{C}$.

DEMOSTRACIÓN. Sean $\alpha, \beta \in \mathcal{O}$, y veamos que los elementos $\alpha\beta$ y $\alpha + \beta$ están nuevamente en $\mathcal{O}$. Por Teorema 3.4, $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ son finitamente generados como $\mathbb{Z}$-módulos. Esto implica que el $\mathbb{Z}$-módulo $\mathbb{Z}[\alpha, \beta]$ es finitamente generado. En efecto, si $\{1, \alpha, \ldots, \alpha^{c-1}\}$ y $\{1, \beta, \ldots, \beta^{d-1}\}$ generan $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ respectivamente, entonces $\{\alpha^i\beta^j : 0 \leq i \leq c-1,\ 0 \leq j \leq d-1\}$ genera $\mathbb{Z}[\alpha, \beta]$.

Luego, como $\alpha\beta$ y $\alpha+\beta$ pertenecen a $\mathbb{Z}[\alpha, \beta]$, concluimos por Teorema 3.4 (implicación (4)⇒(1)) que α es entero algebraico. □

DEFINICIÓN 3.6. Todo cuerpo K en $\mathbb{C}$ tal que $K|\mathbb{Q}$ es una extensión finita de $\mathbb{Q}$ es llamado *cuerpo de números*. Dado K un cuerpo de números, el anillo

$$\mathcal{O}_K := K \cap \mathcal{O}$$

se llama el *anillo de enteros de* K.

OBSERVACIÓN 3.7. Por Teorema 3.4, se sigue de manera inmediata que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. En efecto, si $\alpha \in \mathbb{Q} \cap \mathcal{O}$, entonces el polinomio minimal de α tiene coeficientes en $\mathbb{Z}$. Como $m_\alpha(x) = x - \alpha$, obtenemos que $\alpha \in \mathbb{Z}$.

Se puede ver que cualquier extensión cuadrática de $\mathbb{Q}$ es de la forma $\mathbb{Q}(\sqrt{m})$ para algún $m \in \mathbb{Z}$ libre de cuadrados, y estos últimos son no isomorfos de a pares. Cada uno de ellos es llamado un *cuerpo cuadrático*. Además, $\mathbb{Q}(\sqrt{m})$ con $m > 0$ (resp. $m < 0$) es llamado *cuerpos cuadrático real* (resp. *cuerpo cuadrático imaginario*), pues $\mathbb{Q}(\sqrt{m}) \subset \mathbb{R}$ ($\mathbb{Q}(\sqrt{m}) \not\subset \mathbb{R}$ y $\mathbb{Q}(\sqrt{m}) \subset \mathbb{C}$).

PROPOSICIÓN 3.8. *Si $m \in \mathbb{Z}$ es libre de cuadrados, entonces*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{si } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

DEMOSTRACIÓN. Sean $m \in \mathbb{Z}$ libre de cuadrados, $K = \mathbb{Q}(\sqrt{m})$ y σ la incrustación de K en $\mathbb{C}$ no trivial (i.e. el elemento no trivial en $\mathcal{G}(K|\mathbb{Q})$). Sea $\alpha := a + b\sqrt{m} \in K$, con $a, b \in \mathbb{Q}$. Se tiene que

$$\begin{aligned} m_\alpha(x) &= (x - \alpha)(m - \sigma(\alpha)) = (x - (a + b\sqrt{m}))(x - (a - b\sqrt{m})) \\ &= (x - a)^2 - mb^2 = x^2 - 2ax + (a^2 - mb^2). \end{aligned}$$

Luego,

$$\alpha \in \mathcal{O}_K \iff \alpha \in \mathcal{O} \iff m_\alpha(x) \in \mathbb{Z}[x] \iff \begin{cases} 2a \in \mathbb{Z}, \\ a^2 - mb^2 \in \mathbb{Z}. \end{cases}$$

Resta mostrar que la última condición es equivalente a que

$$a + b\sqrt{m} \in A := \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{si } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Supongamos primero que $2a$ y $a^2 - mb^2$ son números enteros. Obviamente $a \in \frac{1}{2}\mathbb{Z}$, y veamos que b también. Como $4a^2 \in \mathbb{Z}$ y $4(a^2 - mb^2) \in \mathbb{Z}$, $4mb^2 \in \mathbb{Z}$, lo cual implica que $b \in \frac{1}{2}\mathbb{Z}$ (¿Por qué?). Escribimos $a = r/2$ y $b = s/2$ con $r, s \in \mathbb{Z}$. Como $\mathbb{Z} \ni a^2 - mb^2 = \frac{r^2 - ms^2}{4}$, tenemos que

$$r^2 \equiv ms^2 \pmod 4.$$

Si $m \equiv 1 \pmod 4$, entonces $r^2 \equiv s^2 \pmod 4$, lo que equivale a que $r \equiv s \pmod 2$, lo que a su vez implica que $a + b\sqrt{m} \in A$. En efecto,

$$\mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] = \{k + l\tfrac{1+\sqrt{m}}{2} = \tfrac{2k+l+l\sqrt{m}}{2} : k, l \in \mathbb{Z}\} = \{\tfrac{r+s\sqrt{m}}{2} : r, s \in \mathbb{Z},\ r \equiv s \pmod 2\}.$$

Cuando $m \equiv 2, 3 \pmod 4$, $r^2 \equiv ms^2 \pmod 4$ implica que $r \equiv s \equiv 0 \pmod 2$, esto es, $a + b\sqrt{m} = \frac{r}{2} + \frac{s}{2}\sqrt{m} \in \mathbb{Z}[\sqrt{m}] = A$.

Ahora supongamos que $a + b\sqrt{m} \in A$. Si $m \not\equiv 1 \pmod 4$, entonces $a, b \in \mathbb{Z}$, por lo tanto es obvio que $2a, a^2 - mb^2 \in \mathbb{Z}$. Ahora supongamos $m \equiv 1 \pmod 4$. Por la identidad

de arriba para $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, tenemos que $a+b\sqrt{m} = \frac{r+s\sqrt{m}}{2}$ para algún $r, s \in \mathbb{Z}$ con $r \equiv s$ (mód 2). Esto implica que $a = r/2$ y $b = s/2$, por lo que concluimos que $2a = r$ y $a^2 - mb^2 = \frac{r^2-ms^2}{4}$ son números enteros pues $m \equiv 1$ (mód 4). □

Problemas.

3.1. Determinar el anillo de enteros $\mathcal{O}_K$ para los siguientes cuerpos de números:
(a) $K = \mathbb{Q}(\sqrt[3]{2})$.
(b) $K = \mathbb{Q}[\sqrt{5}, \sqrt{7}]$.
(c) $K =$ un cuerpo ciclotómico de orden 5.

2. Traza y norma

Consideremos una torre de cuerpos $\mathbb{Q} \subset K \subset E$, con $n = [E : K] < \infty$, y $\sigma_1, \dots \sigma_n : E \to \mathbb{C}$ todos los K-morfismos (distintos) de E a $\mathbb{C}$.

DEFINICIÓN 3.9. Sean K y E como arriba. Se definen para $\alpha \in E$

- la *traza relativa* como $T_K^E(\alpha) := \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$, y
- la *norma relativa* como $N_K^E(\alpha) := \sigma_1(\alpha) \dots \sigma_n(\alpha)$.

En el caso que $K = \mathbb{Q}$, abreviaremos

- $T_E(\alpha) := T_{\mathbb{Q}}^E(\alpha)$, la *traza* de E, y
- $N_E(\alpha) := N_{\mathbb{Q}}^E(\alpha)$, la *norma* de E.

OBSERVACIÓN 3.10. Para $\alpha, \beta \in E$ y $q \in \mathbb{Q}$, se ve fácilmente que

- $T_K^E(\alpha + \beta) = T_K^E(\alpha) + T_K^E(\beta)$;
- $N_K^E(\alpha\beta) = N_K^E(\alpha) N_K^E(\beta)$;
- $T_K^E(q) = nq$, $N_K^E(q) = q^n$;
- $T_K^E(q\alpha) = qT_K^E(\alpha)$, $N_K^E(q\alpha) = q^n N_K^E(\alpha)$.

OBSERVACIÓN 3.11. Para $\alpha \in \bar{\mathbb{Q}}$, recordemos que por Proposición 1.29 cada incrustación de $K(\alpha)$ en $\mathbb{C}$ está determinada por dónde mapea α, que debe ser necesariamente una raíz del polinomio minimal $m_\alpha^K(x)$ de α sobre K. En otras palabras, si $\{\sigma_1, \dots, \sigma_n\} = \{\sigma : E \to \mathbb{C} : \sigma|_K = \mathrm{id}_K\}$, entonces $\alpha_1 := \sigma_1(\alpha), \dots, \alpha_d := \sigma_d(\alpha)$ son todas las raíces (distintas) de $m_\alpha^K(x)$.

EJERCICIO 3.12. Dado K un cuerpo de números y $\alpha \in K$, sea $U_\alpha : K \to K$ la transformación lineal (sobre $\mathbb{Q}$) dada por $U_\alpha(\beta) = \alpha\beta$. Probar que $T_K(\alpha) = \mathrm{Tr}(U_\alpha)$ y $N_K(\alpha) = \det(U_\alpha)$.

PROPOSICIÓN 3.13. *Sean $\mathbb{Q} \subset K \subset E$ tales que $[E : \mathbb{Q}] < \infty$. Para $\alpha \in E$ tenemos que*

$$T_K^E(\alpha) = [E : K(\alpha)]\big(\alpha_1 + \cdots + \alpha_d\big),$$
$$N_K^E(\alpha) = (\alpha_1 \dots \alpha_d)^{[E:K(\alpha)]},$$

donde $\alpha_1, \alpha_2, \dots, \alpha_d$ son las raíces del polinomio minimal $m_\alpha^K(x)$ de α sobre K.

DEMOSTRACIÓN. Tomemos $\{\sigma_1, \dots, \sigma_n\} = \{\sigma : E \to \mathbb{C} : \sigma|_K = \mathrm{id}_K\}$. Por Observación 3.11, es claro que

$$T_K^{K(\alpha)}(\alpha) = \alpha_1 + \cdots + \alpha_d, \qquad N_K^{K(\alpha)}(\alpha) = \alpha_1 \dots \alpha_d,$$

donde $\alpha_j = \sigma_j(\alpha)$ para todo $1 \leq j \leq d$.

Por otro lado, tenemos la torre de cuerpos $K \subset K(\alpha) \subset E$. Para cada $1 \leq j \leq d$, existen $[E : K(\alpha)]$ distintas extensiones de σ_j desde $K(\alpha)$ a K, y todas ellas envían α a algún α_j. Más aún, la unión con $1 \leq j \leq d$ de todas estas incrustaciones forman el conjunto de todas las K-incrustaciones de E en $\mathbb{C}$. Las identidades para $T_K^E(\alpha)$ y $N_K^E(\alpha)$ siguen de manera inmediata de lo anterior. □

COROLARIO 3.14. *Sean $\mathbb{Q} \subset K \subset E$ tales que $[E : \mathbb{Q}] < \infty$. Entonces*

- *$T_K^E(\alpha), N_K^E(\alpha) \in K$ para todo $\alpha \in E$;*
- *$T_K^E(\alpha), N_K^E(\alpha) \in \mathcal{O}_K$ para todo $\alpha \in \mathcal{O}_E$.*

En particular,

- *$T_E(\alpha), N_E(\alpha) \in \mathbb{Q}$ para todo $\alpha \in E$;*
- *$T_E(\alpha), N_E(\alpha) \in \mathbb{Z}$ para todo $\alpha \in \mathcal{O}_E$.*

DEMOSTRACIÓN. Sea $\alpha \in E$. Denotemos $\alpha_1, \ldots, \alpha_d$ a las raíces de $m_\alpha^K(x)$. Entonces

$$\begin{aligned} m_\alpha^K(x) &= (x - \alpha_1) \ldots (x - \alpha_d) \\ &= x^d - (\alpha_1 + \cdots + \alpha_d)x^{d-1} + \cdots + (-1)^d \alpha_1 \ldots \alpha_d. \end{aligned}$$

Como $m_\alpha^K(x) \in K[x]$, tenemos que $\alpha_1 + \cdots + \alpha_d$ y $\alpha_1 \ldots \alpha_d$ están en K, por lo tanto $T_K^E(\alpha)$ y $N_K^E(\alpha)$ también están en K por Proposición 3.13.

Probaremos la segunda afirmación sólo en el caso $K = \mathbb{Q}$. Si $\alpha \in \mathcal{O}_E$, entonces $m_\alpha^K(x) \in \mathbb{Z}[x]$ por Teorema 3.4, con lo que concluimos que $T_E(\alpha)$ y $N_E(\alpha)$ son números enteros de la misma manera que arriba. □

EJERCICIO 3.15. Completar la demostración anterior, esto es, mostrar que $T_K^E(\alpha)$ y $N_K^E(\alpha)$ viven en $\mathcal{O}_K$ para todo $\alpha \in \mathcal{O}_E$ (no está en [**Marcus**], pero se puede buscar en otros libros).

EJEMPLO 3.16. Supongamos $K = \mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ libre de cuadrados. Se tiene de manera inmediata que

$$\begin{aligned} T_K(a + b\sqrt{m}) &= (a + b\sqrt{m}) + (a - b\sqrt{m}) = 2a, \\ N_K(a + b\sqrt{m}) &= (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2. \end{aligned}$$

Por la demostración de Proposición 3.8, tenemos que

$$\alpha \in \mathcal{O}_K \quad \Longleftrightarrow \quad T_K(\alpha), N_K(\alpha) \in \mathbb{Z},$$

para todo $\alpha \in K$.

TEOREMA 3.17. *Sean $\mathbb{Q} \subset K \subset F \subset E$ tales que $[E : \mathbb{Q}] < \infty$. Para $\alpha \in E$ tenemos que*

- *$T_K^F(T_F^E(\alpha)) = T_K^E(\alpha)$,*
- *$N_K^F(N_F^E(\alpha)) = N_K^E(\alpha)$.*

DEMOSTRACIÓN. Denotemos $\sigma_1, \ldots, \sigma_n : F \to \mathbb{C}$ todos los K-morfismos de F a $\mathbb{C}$, y $\tau_1, \ldots, \tau_m : E \to \mathbb{C}$ todos los F-morfismos de E a $\mathbb{C}$. Antes de componer σ_i con τ_j (lo cual no es válido todavía) extendemos a cada uno de ellos (de cualquier manera) a $\widetilde{E}$, la menor extensión de E tal que la extensión $\widetilde{E}|K$ es normal. La existencia de cada extensión está garantizada por Teorema 1.30, y la denotamos con su mismo símbolo, por lo tanto tenemos $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m : \widetilde{E} \to \widetilde{E}$, con $\sigma_i|_K = \mathrm{id}_K$ y $\tau_j|_F = \mathrm{id}_F$ para todo i y j.

Tenemos que

$$T_K^F(T_F^E(\alpha)) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(\alpha) \right) = \sum_{i,j} (\sigma_i \circ \tau_j)(\alpha) = T_K^E(\alpha),$$

$$N_K^F(N_F^E(\alpha)) = \prod_{i=1}^{n} \sigma_i \left(\prod_{j=1}^{m} \tau_j(\alpha) \right) = \prod_{i,j} (\sigma_i \circ \tau_j)(\alpha) = N_K^E(\alpha).$$

La última igualdad en cada una de las dos filas de arriba sigue del hecho de que el conjunto

$$\{\sigma_i \circ \tau_j : 1 \leq i \leq n,\ 1 \leq j \leq m\}$$

son todos los K-morfismos (distintos) de E a $\mathbb{C}$. □

Problemas.

3.2. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(a) Para $\alpha \in K$, $T_K(\alpha), N_K(\alpha) \in \mathbb{Z}$ implica que $\alpha \in \mathcal{O}_K$.
(b) $(\sqrt{3} + \sqrt{7})/2 \in \mathcal{O}$.

3. Enteros algebraicos irreducibles, primos y unidades

En esta sección usaremos las herramientas traza y norma para caracterizar las unidades en $\mathcal{O}_K$, y dar condiciones suficientes sobre elementos de $\mathcal{O}_K$ para ser irreducibles y primos, todo esto para K un cuerpo de números. Primero recordemos estas nociones.

RECORDATORIO 3.18. Sea R un dominio de integridad (anillo conmutativo con unidad y sin divisores de cero). Un elemento $\alpha \in R$ es unidad si existe $\beta \in R$ tal que $\alpha\beta = 1$. El conjunto de unidades en R se denota $R^\times$, el cual es un grupo con la multiplicación. Para $\alpha \in R$ no nulo y no unidad,

- α es irreducible si $\alpha = \beta\gamma$ implica que β o γ es unidad;
- α es primo si $\alpha \mid \beta\gamma$ implica que $\alpha \mid \beta$ o $\alpha \mid \gamma$;
- todo elemento primo es irreducible: sea α primo tal que $\alpha = \beta\gamma$. Como $\alpha \mid \beta\gamma$, entonces $\alpha \mid \beta$ o $\alpha \mid \gamma$, por lo tanto $\beta = \alpha\delta_1$ para algún $\delta_1 \in R$ o $\gamma = \alpha\delta_2$ para algún $\delta_2 \in R$. Como $\alpha = \beta\delta_1\alpha$ en el primer caso, o $\beta = \beta\delta_2\alpha$ en el segundo, obtenemos que $\beta\delta_1 = 1$ o $\gamma\delta_2 = 1$, es decir, β o γ es una unidad en R.
- La recíproca no es cierta (ver Ejemplo 3.26).

PROPOSICIÓN 3.19. *Sea K un cuerpo de números. El conjunto $\mathcal{O}_K^\times$ de unidades de $\mathcal{O}_K$ es igual a*

$$\{\alpha \in \mathcal{O}_K : N_K(\alpha) = \pm 1\}.$$

DEMOSTRACIÓN. Si $\alpha \in \mathcal{O}_K^\times$, entonces existe $\beta \in \mathcal{O}_K$ tal que $1 = \alpha\beta$, lo que implica que

$$1 = N_K(1) = N_K(\alpha\beta) = N_K(\alpha)N_K(\beta),$$

por lo tanto $N_K(\alpha) = \pm 1$ pues $N_K(\alpha), N_K(\beta) \in \mathbb{Z}$.

Ahora supongamos que $\alpha \in \mathcal{O}_K$ satisface $N_K(\alpha) = \pm 1$. Denotemos $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ las raíces de $m_\alpha(x)$ y $l = [K : \mathbb{Q}(\alpha)]$. Proposición 3.13 implica que

$$\pm 1 = N_K(\alpha) = (\alpha_1 \ldots \alpha_d)^l,$$

por lo tanto

$$\alpha^{-1} = \pm \alpha_1^{l-1}(\alpha_2 \ldots \alpha_d)^l \in \mathcal{O}_K$$

pues $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. □

EJEMPLOS 3.20. Las soluciones de la ecuación

$$\pm 1 = N_{\mathbb{Q}(\sqrt{-2})}(a + b\sqrt{-2}) = a^2 + 2b^2 \qquad (a, b \in \mathbb{Z}),$$

son claramente $(a, b) = (\pm 1, 0)$. Luego, $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{-2})} = \{\pm 1\}$. Más generalmente, para $K = \mathbb{Q}(\sqrt{m})$ con $m < 0$ entero libre de cuadrados (i.e. K es un cuerpo cuadrático imaginario), se puede ver que

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \{\pm 1\} & \text{para } m < -3, \\ \{\pm 1, \pm e^{2\pi \mathrm{i}/3}, \pm e^{-2\pi \mathrm{i}/3}\} & \text{para } m = -3, \\ \{\pm 1, \pm \mathrm{i}\} & \text{para } m = -1. \end{cases}$$

EJERCICIO 3.21. Demostrar la fórmula de arriba que determina las unidades de todo cuerpo cuadrático imaginario.

La situación con las unidades en el caso de los cuerpos cuadráticos reales es muy distinta. El siguiente ejemplo muestra la punta del iceberg.

EJEMPLO 3.22. Consideremos $K = \mathbb{Q}(\sqrt{2})$. En este caso la ecuación es

$$\pm 1 = N_K(a + b\sqrt{2}) = a^2 - 2b^2, \qquad (a, b \in \mathbb{Z}).$$

Por ejemplo, $1 + \sqrt{2}$ está en $\mathcal{O}_K^\times$, al igual que todas sus potencias, lo cual asegura que hay infinitas unidades.

EJERCICIO 3.23. Probar que $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{2})} = \{\pm(1 + \sqrt{2})^k : k \in \mathbb{Z}\}$.

Para m un entero positivo libre de cuadrados con $m \not\equiv 1 \pmod 4$, la ecuación

$$1 = a^2 - mb^2 \qquad (a, b \in \mathbb{Z})$$

es llamada la *ecuación de Pell*. Cada solución de esta ecuación determina una unidad en el anillo de enteros de $\mathbb{Q}(\sqrt{m})$.

PROPOSICIÓN 3.24. *Sea K un cuerpo de números y sea $\alpha \in \mathcal{O}_K$. Si $N_K(\alpha)$ es primo (en $\mathbb{Z}$), entonces α es irreducible en $\mathcal{O}_K$.*

DEMOSTRACIÓN. Supongamos que $\alpha = \beta\gamma$ con $\beta, \gamma \in \mathcal{O}_K$. Tenemos que

$$p = N_K(\alpha) = N_K(\beta)N_K(\gamma)$$

es un número primo en $\mathbb{Z}$, lo que implica que $N_K(\beta) = \pm 1$ o $N(\alpha) = \pm 1$, esto es, β o γ es una unidad en $\mathcal{O}_K$ por Proposición 3.19. Esto muestra que α es irreducible en $\mathcal{O}_K$. □

Veamos que la recíproca no es cierta, esto es, hay elementos irreducibles α en $\mathcal{O}_K$ tal que $N_K(\alpha)$ no es primo.

EJEMPLO 3.25. Veamos que 3 es irreducible en $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\mathrm{i}]$, aunque $N(3) = 9$ no es primo. Supongamos que $3 = \alpha\beta$ con $\alpha, \beta \in \mathcal{O}_K$. Se tiene que

$$9 = N_K(3) = N_K(\alpha)N_K(\beta),$$

por lo tanto $N_K(\alpha), N_K(\beta) \in \{\pm 1, \pm 3, \pm 9\}$. Asimismo, la ecuación

$$\pm 3 = N_K(a + \mathrm{i}b) = a^2 + b^2 \qquad (a, b \in \mathbb{Z})$$

no tiene soluciones (si $a^2 + b^2 = 3$ entonces $a^2 + b^2 \equiv 3 \pmod 4$, la cual obviamente no tiene soluciones). Luego, $N_K(\alpha) = 1$ o $N(\beta) = 1$, esto es, α o β es una unidad en $\mathcal{O}_K$.

Ahora veamos que la recíproca de "primo ⇒ irreducible" no es cierta.

EJEMPLO 3.26. Tomemos $K = \mathbb{Q}(\sqrt{-14})$. El elemento 3 es irreducible en $\mathcal{O}_K$ pues $N_K(3) = 9$ y $N_K(\alpha) \neq \pm 3$ para todo $\alpha \in \mathcal{O}_K$ (muy similar al ejemplo anterior).

Por otro lado, 3 no es primo en $\mathcal{O}_K$ pues 3 divide a

$$15 = (1 + \sqrt{-14})(1 - \sqrt{-14}),$$

pero claramente no divide $1 + \sqrt{-14}$ ni a $1 - \sqrt{-14}$.

El siguiente resultado muestra en un anillo de enteros de un cuerpo de números, siempre existe una factorización en elementos irreducibles. Veremos en Observación 3.28 que esta factorización no es necesariamente única en general.

PROPOSICIÓN 3.27. *Sea K un cuerpo de números. Todo $\alpha \in \mathcal{O}_K$ no nulo y no unidad se factoriza como producto de elementos irreducibles en $\mathcal{O}_K$.*

DEMOSTRACIÓN. (Idea.) Si α no es irreducible, entonces $\alpha = \beta\gamma$ para algunos $\beta, \gamma \in \mathcal{O}_K$, ninguno de ellos unidad. Tenemos que

$$|N_K(\alpha)| > |N_K(\beta)| > 1.$$

Si β no es irreducible, hacemos con β lo mismo que hicimos con α al comienzo de la demostración, y siguiendo así, este proceso debe necesariamente finalizar pues $|N_K(\delta)| \in \mathbb{Z}_{\geq 0}$ para todo $\delta \in \mathcal{O}_K$. Por lo tanto, encontramos un elemento irreducible β_1 que divide a α. Aplicando el mismo procedimiento a $\alpha\beta_1^{-1} \in \mathcal{O}_K$ obtenemos una factorización de α en elementos irreducibles. □

OBSERVACIÓN 3.28. Tomemos $K = \mathbb{Q}(\sqrt{-14})$. Ya vimos que 3 es irreducible en $\mathcal{O}_K = \mathbb{Z}(\sqrt{-14})$ en Ejemplo 3.26. Tenemos que

$$3^4 = 81 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}) = \alpha\bar{\alpha},$$

donde $\alpha = 5 + 2\sqrt{-14}$. Veamos que α y $\bar{\alpha}$ son irreducibles, y así obtenemos dos factorizaciones en irreducibles de 81 distintas. De hecho, el número de factores irreducibles es distinto.

Supongamos que $\alpha = \beta\gamma$ con $\beta, \gamma \in \mathcal{O}_K$. Tenemos que

$$81 = N_K(\alpha) = N_K(\beta)N_K(\gamma).$$

Entonces

$$N_K(\beta) \in \{1, 3, 9, 27, 81\}.$$

Como $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$, y

$$N_K(a + b\sqrt{-14}) = a^2 + 14b^2 \neq 3, 27$$

para todo $a, b \in \mathbb{Z}$, las opciones restantes son $N_K(\beta) \in \{1, 9, 81\}$. Además, $N_K(\beta) = 9$ implica que $\beta = \pm 3$, que no divide a α. Concluimos que $N_K(\beta) = 1$ o $N_K(\beta) = 81$, por lo tanto α es irreducible en $\mathcal{O}_K$.

OBSERVACIÓN 3.29. Sabemos que todo dominio de ideales principales es un dominio de factorización única. (Veremos en Teorema 4.23 que la recíproca es cierta para dominios de Dedekind, en particular para cualquier anillo de enteros de un cuerpos de número.) Luego, Ejemplo 3.28 nos asegura que $\mathbb{Z}[\sqrt{-14}]$ no es un dominio de ideales principales. Ejemplifiquemos este hecho.

Queremos mostrar que el ideal

$$\mathfrak{a} := \langle 2, \sqrt{-14}\rangle = 2\,\mathcal{O}_{\mathbb{Q}(\sqrt{-14})} + \sqrt{-14}\,\mathcal{O}_{\mathbb{Q}(\sqrt{-14})}$$

no es principal. Supongamos que $\mathfrak{a} = \langle \alpha \rangle$ para algún $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{-14})}$.

- Como α divide a 2, $N_K(\alpha)$ divide a $N_K(2) = 4$, esto es, $N_K(\alpha) \in \{1, 2, 4\}$.
- Como α divide a $\sqrt{-14}$, $N_K(\alpha)$ divide a $N_K(\sqrt{-14}) = 14$, esto es, $N_K(\alpha) \in \{1, 2, 7, 14\}$.

Concluimos que $N_K(\alpha) \in \{1, 2\}$. Como $N_K(a+b\sqrt{-14}) = a^2+14b^2 \neq 2$ para todo $a, b \in \mathbb{Z}$, obtenemos que $N_K(\alpha) = 1$, lo que implica que $\alpha \in \mathcal{O}_K^\times$ y por lo tanto $\mathfrak{a} = \mathbb{Z}[\sqrt{-14}]$. Esto es una contradicción pues $1 \notin \mathfrak{a}$, ya que en caso contrario, existirían $a, b, c, d \in \mathbb{Z}$ tales que

$$1 = 2(a + b\sqrt{-14}) + \sqrt{-14}(c + d\sqrt{-14}) = (2a - 14d) + (2b + c)\sqrt{-14},$$

lo que implica que $1 = 2(a - 7d)$.

Existen otras aplicaciones muy simples de la traza y la norma (e.g. Problema 3.3). Por ejemplo, se pueden utilizar para estudiar *dominios Euclídeos* (ver Problema 3.5). Un estudio profundo sobre ellos se puede encontrar en [**Alaca&Williams**, §2].

Problemas.

3.3. (Ejercicio 16 de [**Marcus**, Ch. 2].) Sea $\alpha = \sqrt[4]{2}$. Usar la traza $T_{\mathbb{Q}(\alpha)}$ para mostrar que $\sqrt{3} \notin \mathbb{Q}(\alpha)$. (Ayuda: Escribir $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$ y mostrar que $a = 0$, luego que $b = 0$, y por último $c = 0$ obteniendo una contradicción, calculando $T_{\mathbb{Q}(\alpha)}(\sqrt{3})$.)

3.4. Para cada una de las siguientes propiedades, encontrar un cuerpo de números K que la satisfaga (¡No vale usar los ejemplos del teórico!).

(a) $\mathcal{O}_K$ no es un dominio de factorización única.
(b) $\mathcal{O}_K$ no es un dominio de ideales principales (se puede usar el anterior, pero hay que explicitar un ideal que no sea principal).
(c) Existe un elemento α irreducible en $\mathcal{O}_K$ que no es un elemento primo en $\mathcal{O}_K$.
(d) Existe un elemento α irreducible en $\mathcal{O}_K$ tal que $N_K(\alpha)$ no es primo en $\mathbb{Z}$.
(e) $\mathcal{O}_K^\times$ es infinito. (¿Existe K tal que $\mathcal{O}_K^\times$ es infinito y no tiene elementos de torsión?)

3.5. (Ejercicio opcional, sólo para interesados en dominios Euclídeos.) Sea $K = \mathbb{Q}(\sqrt{m})$ un cuerpo cuadrático imaginario, por lo que podemos asumir que m es un entero negativo libre de cuadrados.

(a) Probar que $\mathcal{O}_K$ es un dominio Euclídeo con $|N(\cdot)|$ si y sólo si para todo $x \in K$ existe $\alpha \in \mathcal{O}_K$ tal que $N(x - \alpha) < 1$.
(b) Probar que el anillo de enteros $\mathcal{O}_K$ es un dominio Euclídeo con $|N(\cdot)|$ si y sólo si $m \in \{-1, -2, -3, -7, -11\}$.
(c) Probar que $\mathcal{O}_K$ es un dominio Euclídeo con respecto a alguna función si y sólo si lo es con respecto a $|N(\cdot)|$.
(d) Probar que $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ es un dominio Euclídeo.

4. Discriminante

Sea K un cuerpo de números de orden $n = [K : \mathbb{Q}]$, y sean $\sigma_1, \ldots, \sigma_n$ todos los morfismos de K a $\mathbb{C}$.

DEFINICIÓN 3.30. El *discriminante* de una n-upla $(\alpha_1, \ldots, \alpha_n)$ en K^n está dado por

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) := \det\left([\sigma_i(\alpha_j)]_{i,j}\right)^2.$$

EJERCICIO 3.31. Mostrar que $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ no depende del orden de $\alpha_1, \ldots, \alpha_n$, ni tampoco del orden de $\sigma_1, \ldots, \sigma_n$.

TEOREMA 3.32. *Dados $\alpha_1, \ldots, \alpha_n \in K$, se tiene que*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det\left([T_K(\alpha_i\alpha_j)]_{i,j}\right).$$

DEMOSTRACIÓN. Sigue de la identidad

$$[\sigma_j(\alpha_i)]_{i,j}[\sigma_i(\alpha_j)]_{i,j} = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)]_{i,j} = [T_K(\alpha_i\alpha_j)]_{i,j},$$

tomando el determinante a ambos lados. □

OBSERVACIÓN 3.33. En el caso que $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, se tiene que

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}.$$

En efecto, $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det([T_K(\alpha_i\alpha_j)]_{i,j})$ por Teorema 3.32, y como $T_K(\alpha) \in \mathbb{Z}$ para todo $\alpha \in \mathcal{O}_K$ por Corolario 3.14, resulta que $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ es el determinante de una matriz entera.

TEOREMA 3.34. *Dados $\alpha_1, \ldots, \alpha_n \in K$,*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0 \iff \alpha_1, \ldots, \alpha_n \text{ son linealmente dependientes sobre } \mathbb{Q}.$$

DEMOSTRACIÓN. Denotemos $B : K \times K \to \mathbb{C}$ la forma bilineal dada por $B(\alpha, \beta) = T_K(\alpha\beta)$. Notemos que es no degenerada pues si $\alpha \neq 0$, entonces $B(\alpha, \alpha^{-1}) = T_K(1) = [K : \mathbb{Q}] = n \neq 0$.

Por otro lado, tenemos que $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Q}$-base de K si y sólo si la matriz $[B(\alpha_i, \alpha_j)]_{i,j}$ es no degenerada, lo cual equivale a que $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$ por Teorema 3.32. □

TEOREMA 3.35. *Sea $\alpha \in \bar{\mathbb{Q}}$ y sean $\alpha_1, \ldots, \alpha_n$ los conjugados de α (i.e. las raíces del polinomio minimal $m_\alpha(x)$ de α sobre $\mathbb{Q}$). En el cuerpo $\mathbb{Q}(\alpha)$, se tiene que*

$$\operatorname{disc}(1, \alpha, \ldots \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \epsilon\, N_{\mathbb{Q}(\alpha)}(m'_\alpha(\alpha)),$$

donde $\epsilon = 1$ si $n \equiv 0, 1 \pmod 4$, y $\epsilon = -1$ en caso contrario.

DEMOSTRACIÓN. Primero notemos que, tal como vimos en Proposición 1.29, cualquier morfismo $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$ está determinado por su valor en α, el cual debe ser necesariamente una raíz de $m_\alpha(x)$. Tenemos que

$$\operatorname{disc}(1, \alpha, \ldots \alpha^{n-1}) = \det([\sigma_i(\alpha^{j-1})]_{i,j})^2 = \det([\alpha_i^{j-1}]_{i,j})^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \epsilon \prod_{i \neq j}(\alpha_i - \alpha_j).$$

El penúltimo paso sigue de la clásica fórmula del determinante de la matriz de Vandermonde, mientras que el último paso se deja como ejercicio al lector (ϵ fue definido en el enunciado).

Por otro lado,

$$N_{\mathbb{Q}(\alpha)}(m'_\alpha(\alpha)) = \prod_{i=1}^{n} \sigma_i(m'_\alpha(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\sigma_i(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\alpha_i).$$

Como $m_\alpha(x) = \prod_{k=1}^n (x - \alpha_k)$, tenemos que $m'_\alpha(x) = \sum_{k=1}^n \prod_{j\neq k}(x-\alpha_j)$ y por lo tanto $m'_\alpha(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$. Concluimos que

$$N_{\mathbb{Q}(\alpha)}(m'_\alpha(\alpha)) = \prod_{i=1}^n \prod_{j\neq i}(\alpha_i - \alpha_j),$$

lo cual completa la demostración. □

EJEMPLO 3.36. Tomemos $K = \mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ libre de cuadrados. Supongamos primero que $m \equiv 2, 3 \pmod 4$. Entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ por Proposición 3.8. El polinomio minimal de $\alpha := \sqrt{m}$ es $m_\alpha(x) = x^2 - m$. Luego, Teorema 3.35 nos dice que

$$\operatorname{disc}(1, \sqrt{m}) = -N_K(m'_\alpha(\alpha)) = -N_K(2\sqrt{m}) = 4m.$$

Ahora supongamos $m \equiv 1 \pmod 4$. Proposición 3.8 nos asegura que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. El polinomio minimal de $\alpha = \frac{1+\sqrt{m}}{2}$ es

$$m_\alpha(x) = (x - \tfrac{1+\sqrt{m}}{2})(x - \tfrac{1-\sqrt{m}}{2}) = x^2 - x + \tfrac{1-m}{4}.$$

Concluimos que

$$\operatorname{disc}(1, \tfrac{1+\sqrt{m}}{2}) = -N_K(2\alpha - 1) = -N_K(\sqrt{m}) = m.$$

EJEMPLO 3.37. Para p un número entero primo, sean $\xi = e^{2\pi \mathrm{i}/p}$ y $K = \mathbb{Q}(\xi)$. Luego, $[K : \mathbb{Q}] = p - 1$ y $m_\xi(x) = 1 + x + x^2 + \cdots + x^{p-1}$ por Teorema 2.34.

Para obtener una buena expresión para $m'_\xi(\xi)$, usaremos la identidad $x^p - 1 = (x - 1)m_\xi(x)$. Derivándola, obtenemos que

$$p\, x^{p-1} = m_\xi(x) + (x-1)\, m'_\xi(x),$$

para concluir que

$$m'_\xi(\xi) = \frac{p\,\xi^{p-1}}{\xi - 1} = \frac{p}{\xi(\xi - 1)}.$$

Para calcular la norma de $m'_\xi(\xi)$, notamos que los conjugados de ξ son $\xi, \xi^2, \ldots, \xi^{p-1}$, por lo tanto $N_K(\xi) = \prod_{k=1}^{p-1} \xi^k = \xi^{\frac{p(p-1)}{2}} = 1$ y

$$N_K(\xi - 1) = \prod_{k=1}^{p-1}(\xi^k - 1) = (-1)^{p-1}\, m_\xi(1) = p.$$

Luego,

$$N_K(m'_\xi(\xi)) = \frac{N_K(p)}{N_K(\xi)N_K(\xi - 1)} = \frac{p^{p-1}}{p} = p^{p-2}.$$

Finalmente, Teorema 3.35 nos dice que

$$\operatorname{disc}(1, \xi, \ldots, \xi^{p-2}) = \pm p^{p-2}.$$

EJEMPLO 3.38. Ahora consideremos un cuerpo ciclotómico de orden m no necesariamente primo, esto es, $K = \mathbb{Q}(\xi)$ con $\xi = e^{2\pi \mathrm{i}/m}$. Mostraremos que

$$\operatorname{disc}(1, \xi, \xi^2, \ldots, \xi^{\varphi(m)-1}) \text{ divide (en } \mathbb{Z}) \text{ a } m^{\varphi(m)}.$$

Procedemos de manera similar al ejemplo anterior. Desde Proposición 2.32 sabemos que $x^m - 1 = \prod_{d|m} \Phi_d(x)$ y $\Phi_d(x) \in \mathbb{Z}[x]$ para todo d. Luego, $x^m - 1 = \Phi_m(x)\, g(x)$ para algún $g(x) \in \mathbb{Z}[x]$. Derivando esta identidad obtenemos que

$$m\, x^{m-1} = \Phi_m(x)'\, g(x) + \Phi_m(x)\, g'(x).$$

Evaluando en ξ se tiene que $m = \xi\, \Phi'_m(\xi) g(\xi)$. Esto implica que

$$m^{\varphi(m)} = N_K(m) = N_K(\Phi'_m(\xi))\, N_K(\xi\, g(\xi)) = \pm \operatorname{disc}(1, \xi, \dots, \xi^{\varphi(m)-1})\, N_K(\xi\, g(\xi)).$$

Como $\xi\, g(\xi) \in \mathcal{O}_K$, $N_K(\xi\, g(\xi)) \in \mathbb{Z}$, lo que demuestra lo afirmado.

5. Estructura aditiva de $\mathcal{O}_K$

El objetivo de esta sección es mostrar que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $[K : \mathbb{Q}]$.

Fijemos K un cuerpo de números de orden $n = [K : \mathbb{Q}]$. Sea $\{\alpha_1, \dots, \alpha_n\}$ una $\mathbb{Q}$-base de K. Por Observación 3.3, podemos suponer que $\alpha_i \in \mathcal{O}_K$ para todo i multiplicando cada α_i por un entero apropiado en caso de ser necesario. Consideremos el $\mathbb{Z}$-módulo

$$A := \bigoplus_{j=1}^{n} \alpha_j \mathbb{Z} = \{a_1\alpha_1 + \cdots + a_n\alpha_n : a_1, \dots, a_n \in \mathbb{Z}\}.$$

Claramente tenemos que $A \subset \mathcal{O}_K$.

Teorema 3.39. *Sea K un cuerpo de números de orden n, y sea $\{\alpha_1, \dots, \alpha_n\}$ una $\mathbb{Q}$-base de K con $\alpha_j \in \mathcal{O}_K$ para todo j. Sea $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Entonces, todo elemento en $\mathcal{O}_K$ puede escribirse como*

$$\frac{a_1\alpha_1 + \cdots + a_n\alpha_n}{d}$$

para ciertos $a_1, \dots, a_n \in \mathbb{Z}$ tales que $d \mid a_j^2$ para todo j.

Demostración. Sea $\alpha \in \mathcal{O}_K$. Escribimos $\alpha = r_1\alpha_1 + \cdots + r_n\alpha_n$ con $r_j \in \mathbb{Q}$ para todo j. Denotemos $\sigma_1, \dots, \sigma_n$ los morfismos de K a $\mathbb{C}$. Entonces

$$\sigma_i(\alpha) = \sigma_i(\alpha_1)r_1 + \cdots + \sigma_i(\alpha_n)r_n$$

para todo i. Luego,

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

Por la Regla de Cramer, obtenemos que

$$r_i = \frac{\det(M_i)}{\det(M)},$$

donde $M = [\sigma_i(\alpha_j)]_{i,j}$ y

$$M_i = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_{i-1}) & \sigma_1(\alpha) & \sigma_1(\alpha_{i+1}) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_{i-1}) & \sigma_n(\alpha) & \sigma_n(\alpha_{i+1}) & \dots & \sigma_n(\alpha_n) \end{pmatrix}.$$

Notar que $d = \det(M)^2$ por Definición 3.30. Por lo tanto $dr_i = \det(M)\det(M_i) \in \mathcal{O}_K$. Como además $d \in \mathbb{Z}$ por Observación 3.33, $dr_i \in \mathbb{Q}$ para todo i. Concluimos que $dr_i \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ para todo i.

Tomemos $a_i = dr_i$ para todo i. Sigue que

$$\alpha = r_1\alpha_1 + \cdots + r_n\alpha_n = \frac{a_1\alpha_1 + \cdots + a_n\alpha_n}{d}.$$

Resta ver que $d \mid a_i^2$ para todo i. Tenemos que $a_i^2/d = (a_i/d)a_i = r_i a_i \in \mathbb{Q}$ para todo i. Además,

$$\frac{a_i^2}{d} = \frac{(dr_i)^2}{d} = \frac{\det(M)^2 \det(M_i)^2}{d} = \det(M_i)^2 \in \mathcal{O}_K,$$

por lo que concluimos que $a_i^2/d \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. □

COROLARIO 3.40. *Para K un cuerpo de números, $\mathcal{O}_K$ es un grupo abeliano libre de rango $[K : \mathbb{Q}]$.*

DEMOSTRACIÓN. Usando la notación del teorema anterior, tenemos que

$$\bigoplus_{i=1}^{n} \alpha_i\mathbb{Z} \subset \mathcal{O}_K \subset \bigoplus_{i=1}^{n} \frac{\alpha_i}{d}\mathbb{Z},$$

lo que asegura que $\mathcal{O}_K$ es un módulo libre de rango $n = [K : \mathbb{Q}]$. □

Como $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $n = [K : \mathbb{Q}]$, existe una $\mathbb{Z}$-base $\{\beta_1, \ldots, \beta_n\}$ de $\mathcal{O}_K$, esto es,

$$\mathcal{O}_K = \bigoplus_{i=1}^{n} \beta_i\mathbb{Z} = \{a_1\beta_1 + \cdots + a_n\beta_n : a_1, \ldots, a_n \in \mathbb{Z}\}.$$

Notar que a su vez, $\{\beta_1, \ldots, \beta_n\}$ es también una $\mathbb{Q}$-base de K. Tal base es llamada *base entera de K*.

Por Observación 3.33, el discriminante de una base entera es un número entero.

TEOREMA 3.41. *Sea K un cuerpo de números. Si $\{\beta_1, \ldots, \beta_n\}$ y $\{\gamma_1, \ldots, \gamma_n\}$ son bases enteras de $\mathcal{O}_K$, entonces*

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n).$$

DEMOSTRACIÓN. Para cada $1 \leq i \leq n$, como $\beta_i \in \mathcal{O}_K$ (resp. $\gamma_i \in \mathcal{O}_K$) y $\{\gamma_1, \ldots, \gamma_n\}$ (resp. $\{\beta_1, \ldots, \beta_n\}$) es una $\mathbb{Z}$-base de $\mathcal{O}_K$, existen $b_{i,1}, \ldots, b_{i,n} \in \mathbb{Z}$ (resp. $c_{i,1}, \ldots, c_{i,n} \in \mathbb{Z}$) tales que $\beta_i = \sum_{j=1}^{n} b_{i,j}\gamma_j$ (resp. $\gamma_i = \sum_{j=1}^{n} c_{i,j}\beta_j$). Tomando $B = [b_{i,j}]_{i,j=1}^{n}$ y $C = [c_{i,j}]_{i,j=1}^{n}$, tenemos que

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = B \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}, \qquad \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Claramente BC es la matriz identidad, por lo tanto $\det(B) = \det(C) = \pm 1$ por tener coeficientes enteros.

Además, como

$$[\sigma_j(\beta_i)]_{i,j} = B\,[\sigma_j(\gamma_i)]_{i,j},$$

concluimos que

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \det([\sigma_j(\beta_i)]_{i,j})^2 = \det(B)^2 \det([\sigma_j(\gamma_i)]_{i,j})^2 = \operatorname{disc}(\gamma_1, \ldots, \gamma_n),$$

tal como queríamos. □

DEFINICIÓN 3.42. El *discriminante* de un cuerpo de números K, el cual se denota por $\operatorname{disc}(K)$, está dado por el discriminante de cualquier base entera de K.

EJEMPLO 3.43. Desde Ejemplo 3.36, tenemos que para $m \in \mathbb{Z}$ libre de cuadrados,

$$\operatorname{disc}(\mathbb{Q}(\sqrt{m})) = \begin{cases} 4m & \text{si } m \equiv 2,3 \pmod 4, \\ m & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

TEOREMA 3.44. *Tomemos $K = \mathbb{Q}(\xi)$ donde $\xi = e^{2\pi \mathrm{i}/m}$ con $m = p^r$ y p primo. Entonces $\mathcal{O}_K = \mathbb{Z}[\xi]$.*

DEMOSTRACIÓN. Obviamente tenemos que $\mathbb{Z}[\xi] = \mathbb{Z}[1-\xi] \subset \mathcal{O}_K$. Veremos que $\mathbb{Z}[1-\xi] = \mathcal{O}_K$.

Notemos que

$$\begin{aligned} d &:= \operatorname{disc}(1, 1-\xi, (1-\xi)^2, \dots, (1-\xi)^{\phi(m)-1}) \\ &= \prod_{\substack{1 \le i < j \le m: \\ \operatorname{mcd}(m,i)=1=\operatorname{mcd}(m,j)}} \big((1-\xi^i) - (1-\xi^j)\big)^2 \\ &= \prod_{\substack{1 \le i < j \le m: \\ \operatorname{mcd}(m,i)=1=\operatorname{mcd}(m,j)}} (\xi^j - \xi^i)^2 = \operatorname{disc}(1, \xi, \dots, \xi^{\varphi(m)-1}), \end{aligned}$$

pues los conjugados de ξ son $\{\xi^j : 0 \le j < m,\ \operatorname{mcd}(j,p) = 1\}$, y por lo tanto los conjugados de $1-\xi$ son $\{1-\xi^j : 0 \le j < m,\ \operatorname{mcd}(j,p) = 1\}$. Por lo visto en Ejemplo 3.38, obtenemos que d divide a $m^{\varphi(m)} = (p^r)^{\varphi(m)}$, por lo tanto d es necesariamente una potencia de p. Escribamos $d = p^s$.

Sea $\alpha \in \mathcal{O}_K$. Por Teorema 3.39, existen $a_0, \dots, a_{\varphi(m)-1} \in \mathbb{Z}$ tales que $d \mid a_j^2$ para todo j y

$$\alpha = \frac{a_0 + a_1(1-\xi) + a_2(1-\xi)^2 + \cdots + a_{\varphi(m)-1}(1-\xi)^{\varphi(m)-1}}{d}.$$

Supongamos que $\mathbb{Z}[1-\xi] \neq \mathcal{O}_K$. Luego, debe haber al menos un $\alpha \in \mathcal{O}_K$ tal que los correspondientes coeficientes enteros $a_0, \dots, a_{\varphi(m)-1}$ como arriba no son todos divisibles por d. Se puede ver que existe un elemento en $\mathcal{O}_K$ de la forma

$$\beta := \frac{a_{i-1}(1-\xi)^{i-1} + a_i(1-\xi)^i + \cdots + a_{\varphi(m)-1}(1-\xi)^{\varphi(m)-1}}{p},$$

con $1 \le i \le \varphi(n)$, $a_{i-1}, \dots, a_{\varphi(m)-1}$ enteros no divisibles por p (Ejercicio 3.45).

AFIRMACIÓN. *Se tiene que*

$$\prod_{\substack{1 \le k \le m: \\ \operatorname{mcd}(m,k)=1}} (1-\xi^k) = p.$$

Como consecuencia, $p/(1-\xi)^i \in \mathbb{Z}[\xi]$ y $N_K(1-\xi) = p$.

DEMOSTRACIÓN. En Ejemplos 2.33, vimos que

$$\Phi_{p^r}(x) = \prod_{\substack{1 \le k \le m: \\ \operatorname{mcd}(m,k)=1}} (x-\xi^k) = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}.$$

Evaluando en $x = 1$ obtenemos la fórmula requerida. Además, $N_K(1-\xi)$ es por definición igual al lado izquierdo de tal fórmula, ya que los conjugados de $1-\xi$ son $1-\xi^k$ para $1 \leq k \leq m$ con $\mathrm{mcd}(m,k) = 1$.

Resta ver que $(1-\xi)^i$ divide en $\mathbb{Z}[\xi]$ a p. Esto sigue del hecho que $1-\xi$ divide en $\mathbb{Z}[\xi]$ a $1-\xi^k$ para todo k. Luego, la fórmula implica que $(1-\xi)^{\varphi(m)}$ divide a p en $\mathbb{Z}[\xi]$, en particular también lo hace $(1-\xi)^i$. ■

Tenemos que $\beta p/(1-\xi)^i \in \mathcal{O}_K$. Restando el elemento $\sum_{j=i}^{\varphi(m)-1} a_j(1-\xi)^{j-i}$ que claramente está en $\mathcal{O}_K$, obtenemos que

$$\frac{a_{i-1}}{1-\xi} \in \mathcal{O}_K.$$

Esto implica que $N_K(1-\xi)$ divide (en $\mathbb{Z}$) a $N_K(a_{i-1}) = a_{i-1}^{\varphi(m)-1}$. Esto es una contradicción pues $N_K(1-\xi) = p$ por la afirmación. □

EJERCICIO 3.45. Demostrar la existencia del elemento β en la demostración del Teorema 3.44. (Ayuda para confundir: parece fácil por cómo está escrito en la demostración de [**Marcus**, Thm. 10, Ch. 2].)

Es importante aclarar que Teorema 3.44 vale en realidad para m arbitrario (ver la parte final del capítulo 2 de [**Marcus**]).

Al siguiente resultado no lo demostraremos pero podrá ser usado para hacer los ejercicios. Es muy útil por ejemplo para determinar los anillos de enteros de cuerpos de números de la forma $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ para $a, b \in \mathbb{Z}$.

TEOREMA 3.46. *Sean K y F cuerpos de números de órdenes m y n respectivamente. Denotemos $d = \mathrm{mcd}(m,n)$ y $E = KF$. Si $[E:\mathbb{Q}] = mn$, entonces*

$$\mathcal{O}_K\mathcal{O}_F \subset \mathcal{O}_E \subset \tfrac{1}{d}\,\mathcal{O}_K\mathcal{O}_F.$$

En particular, si $d = 1$, entonces $\mathcal{O}_E = \mathcal{O}_K\mathcal{O}_F$.

EJERCICIO 3.47. Demostrar Teorema 3.46. Consultar [**Marcus**, Thm. 12, Ch. 2].

Problemas.

3.6. Determinar $\mathcal{O}_K$ para cada uno de los siguientes cuerpos de números K. Incluir una base entera para cada uno de ellos.

(a) $K = \mathbb{Q}(\sqrt[3]{2})$.
(b) $K = \mathbb{Q}(\sqrt[3]{12})$.
(c) $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$.
(d) $K = \mathbb{Q}(\alpha)$ donde α es una raíz de $x^3 - x - 1$.

3.7. Decidir si las siguientes afirmaciones son verdaderas o falsas, donde K y F son cuerpos de números.

(a) $K = F$ si y sólo si $\mathrm{disc}(K) = \mathrm{disc}(F)$.
(b) $K \simeq F$ si y sólo si $\mathrm{disc}(K) = \mathrm{disc}(F)$.
(c) Si $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ cumple que $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(K)$, entonces $\alpha_1, \ldots, \alpha_n$ es una base entera de $\mathcal{O}_K$.
(d) Dados $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ es libre de cuadrados (en $\mathbb{Z}$) si y sólo si $\{\alpha_1, \ldots, \alpha_n\}$ es base entera de $\mathcal{O}_K$.

Capítulo 4

Dominios de Dedekind

1. Definición

En $\mathbb{Z}$, el Teorema Fundamental de la Aritmética implica que

todo ideal no nulo de $\mathbb{Z}$ se escribe como producto de ideales primos.

En efecto, si I es un ideal no nulo de $\mathbb{Z}$, entonces $I = \langle m \rangle$ para algún $m \in \mathbb{Z}$. La factorización en primos $m = p_1^{r_1} \dots p_l^{r_l}$ implica que

$$I = \langle p_1^{r_1} \dots p_l^{r_l} \rangle = \langle p_1 \rangle^{r_1} \dots \langle p_l \rangle^{r_l},$$

donde cada $\langle p_i \rangle$ es un ideal irreducible.

El siguiente objetivo es generalizar este resultado a todo anillo de enteros de un cuerpo de números. De hecho, trabajaremos en una clase más general de anillos, los llamado dominios de Dedekind.

Repasaremos primero algunos conceptos básicos de la teoría de anillos.

RECORDATORIO 4.1. Sea R un dominio de integridad (i.e. anillo conmutativo con unidad y sin divisores de cero).

- $\mathfrak{a} \subset R$ es un ideal si para cada $\alpha \in \mathfrak{a}$ y $\beta \in R$ se tiene que $\alpha\beta \in \mathfrak{a}$.
- $R/\mathfrak{a}$ es un anillo cuando $\mathfrak{a}$ es un ideal.
- Un ideal $\mathfrak{p} \subset R$ es primo si $\mathfrak{p} \neq R$ y si cada vez que tenemos $\alpha\beta \in \mathfrak{p}$ implica que $\alpha \in \mathfrak{p}$ o $\beta \in \mathfrak{p}$, lo cual equivale a que cada vez que tengamos $\mathfrak{ab} \subset \mathfrak{p}$ implica que $\mathfrak{a} \subset \mathfrak{p}$ o $\mathfrak{b} \subset \mathfrak{p}$.
- El anillo $R/\mathfrak{p}$ es un dominio de integridad si y sólo si $\mathfrak{p}$ es primo, para $\mathfrak{p}$ cualquier un ideal de R.
- Un ideal $\mathfrak{m} \subset R$ es maximal si $\mathfrak{m} \neq R$ y si cada vez que $\mathfrak{m} \subset \mathfrak{a} \subset R$ con $\mathfrak{a}$ ideal implica que $\mathfrak{a} = R$ o $\mathfrak{a} = \mathfrak{m}$.
- $R/\mathfrak{m}$ es un cuerpo si y sólo si $\mathfrak{m}$ es maximal, para cualquier $\mathfrak{m}$ ideal de R.
- Todo ideal maximal es primo (la recíproca no es cierta pues $\{0\}$ es un ideal primo en $\mathbb{Z}$ pero no es maximal).
- Para $p \in R$, p es primo si sólo si el ideal $\langle p \rangle = pR$ es primo.
- Para $c \in R$, c es irreducible si y sólo si el ideal $\langle c \rangle = cR$ es maximal entre los ideales principales.

PROPOSICIÓN 4.2. *Sea K un cuerpo de números de orden n, y sean $\mathfrak{a}$ y $\mathfrak{p}$ ideales no nulos de $\mathcal{O}_K$, con $\mathfrak{p}$ primo. Las siguientes propiedades son válidas:*

(1) *Existe $a \in \mathbb{Z} \setminus \{0\}$ tal que $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$.*
(2) *Existe $p \in \mathbb{Z}$ primo tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Notar que p es el único primo en $\mathbb{Z}$ que vive en $\mathfrak{p}$.*
(3) *Existen $\beta_1, \dots, \beta_n \in \mathcal{O}_K$ tales que $\mathfrak{a} = \beta_1\mathbb{Z} + \dots + \beta_n\mathbb{Z}$.*
(4) $\#(\mathcal{O}_K/\mathfrak{a}) < \infty$.

DEMOSTRACIÓN. (1) Claramente $\mathfrak{a} \cap \mathbb{Z}$ es un ideal en $\mathbb{Z}$. Resta ver que es no nulo. Sea $\alpha \in \mathfrak{a}$ con $\alpha \neq 0$. Como $\alpha \in \mathcal{O}_K$, los coeficientes de su polinomio minimal $m_\alpha(x) = x^r + \sum_{k=0}^{r-1} a_k x^k$ viven en $\mathbb{Z}$ por Teorema 3.4. Como $m_\alpha(\alpha) = 0$, obtenemos que

$$a_0 = -(\alpha^r + \sum_{k=1}^{r-1} a_k \alpha^k) \in \mathfrak{a}.$$

Además, $a_0 \neq 0$ pues $m_\alpha(x)$ es irreducible en $\mathbb{Q}[x]$.

(2) Por el ítem anterior, tenemos que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para algún $p \in \mathbb{Z}$ no nulo. Resta ver que p es primo en $\mathbb{Z}$. Supongamos que $p \mid ab$ para $a, b \in \mathbb{Z}$. Tenemos que $ab \in \mathfrak{p}$, por lo tanto $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, esto es, $a \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ o $b \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, lo que implica que $p \mid a$ o $p \mid b$.

(3) Por Corolario 3.40, sabemos que $\mathcal{O}_K$ es un grupo abeliano libre de rango n, esto es, existen $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ tales que $\mathcal{O}_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$. Luego, como $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$, tenemos que

$$a\alpha_1\mathbb{Z} + \cdots + a\alpha_n\mathbb{Z} = a\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}.$$

Esto implica que $\mathfrak{a}$ es también un grupo abeliano libre de rango n, lo cual completa la demostración de este ítem.

(4) Ya vimos que $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ y $a\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$, por lo tanto

$$\#(\mathcal{O}_K/\mathfrak{a}) \leq \#(\mathcal{O}_K/a\mathcal{O}_K) = |a|^n < \infty,$$

tal como lo aseguramos. □

DEFINICIÓN 4.3. Un *dominio de Dedekind* R es un dominio de integridad que satisface las siguientes propiedades:

(1) R es Noetheriano.
(2) Todo ideal primo no nulo es maximal.
(3) R es íntegramente cerrado en su cuerpo cociente $K := \{\frac{\alpha}{\beta} : \alpha, \beta \in R,\ \beta \neq 0\}$.

Explicaremos algunas de los términos que aparecieron en la definición anterior, junto a algunos comentarios.

OBSERVACIÓN 4.4. El ítem (3) significa que si $\frac{\alpha}{\beta} \in K$ es raíz de un polinomio mónico en $R[x]$, entonces $\frac{\alpha}{\beta} \in R$, esto es, β divide a α.

El ítem (1) es equivalente a cualquiera de los siguientes:

(1') Todo ideal es finitamente generado.
(1") Toda cadena ascendente de ideales es estacionaria. En otras palabras, si $I_1 \subset I_2 \subset I_3 \subset \ldots$ son ideales, entonces existe $N \in \mathbb{N}$ tal que $I_n = I_N$ para todo $n \geq N$.
(1"') Todo subconjunto no vacío de ideales propios de R, parcialmente ordenados con la inclusión, tiene un elemento maximal. En otras palabras, si $\mathcal{S}$ es un conjunto de ideales propios no vacío, entonces existe $M \in \mathcal{S}$ tal que cada vez que tengamos $M \subset I$ para algún $I \in \mathcal{S}$ implica que $I = M$.

El siguiente ejercicio está destinado a los que disfrutan del álgebra. Se puede encontrar más información sobre anillos Noetherianos en [**Lang**, Ch. X] y [**Hungerford**, §VIII.4].

EJERCICIO 4.5. Demostrar las equivalencia entre (1'), (1") y (1"').

TEOREMA 4.6. *Para K un cuerpo de números, $\mathcal{O}_K$ es un dominio de Dedekind.*

DEMOSTRACIÓN. Mostraremos (1'). Sea $\mathfrak{a}$ un ideal en $\mathcal{O}_K$. Por Proposición 4.2, existen $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ tales que $\mathfrak{a} = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$. Como $\{\beta_1, \ldots, \beta_n\}$ genera a $\mathfrak{a}$ como $\mathbb{Z}$-módulo, es obvio que también lo genera como anillo, por lo tanto $\mathfrak{a}$ es finitamente generado.

(2) Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. El dominio de integridad $\mathcal{O}_K/\mathfrak{p}$ es finito por Proposición 4.2, lo que implica que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, lo que a su vez nos asegura que $\mathfrak{p}$ es maximal.

(3) Sea y un elemento del cuerpo cociente de $\mathcal{O}_K$, es decir, K. Supongamos que y es raíz de un polinomio mónico $f(x) = x^r + \sum_{k=1}^{r-1} \alpha_k x^k \in \mathcal{O}_K[x]$. Para mostrar que y pertenece a $\mathcal{O}_K$, chequearemos la condición (4) en Teorema 3.4, esto es, mostraremos que existe M un $\mathbb{Z}$-submódulo de $\mathbb{C}$ finitamente generado que cumple que $yM \subset M$.

Sea $M = \mathbb{Z}[\alpha_0, \ldots, \alpha_{r-1}, y]$. Denotemos $\mathrm{gr}(m_{\alpha_k}(x)) = h_k$ para todo k. Notemos que M es un $\mathbb{Z}$-módulo finitamente generado ya que el conjunto finito

$$\{\alpha_0^{l_0} \ldots \alpha_{r-1}^{l_{r-1}} y^l : 0 \leq l_k < h_k \text{ para cada } 0 \leq k \leq r-1,\ 0 \leq l < r\}$$

genera a M como $\mathbb{Z}$-módulo. Además, es claro que $yM \subset M$, lo que completa la demostración. □

Problemas.

4.1. Dar un ejemplo de:

(a) un dominio íntegro que no sea Noetheriano.
(b) un dominio íntegro que contenga algún ideal primo no nulo que no sea maximal.
(c) un dominio íntegro que no sea íntegramente cerrado en su cuerpo de fracciones.

2. Factorización de ideales

En esta sección trabajaremos en un dominio de Dedekind R. Denotaremos K a su cuerpo de fracciones. Por Teorema 4.6, todo lo que probaremos será válido para un anillo de enteros de un cuerpo de números.

LEMA 4.7. *Todo ideal no nulo en R contiene un producto de ideales primos.*

DEMOSTRACIÓN. Supongamos que no es cierto. Sea $\mathcal{S}$ el conjunto de todos los ideales no nulos en R que no contienen un producto de ideales primos. Tenemos que $\mathcal{S}$ es no vacío por hipótesis.

Por la equivalencia (1'''), existe un elemento maximal $\mathfrak{m}$ en $\mathcal{S}$. Tenemos que $\mathfrak{m}$ no es primo, sino $\mathfrak{m}$ contendría al ideal $\mathfrak{m}^2$, el cual es producto de dos ideales primos. Luego, existen elementos $r, s \in R \setminus \mathfrak{m}$ tales que $rs \in \mathfrak{m}$. Como los ideales $\mathfrak{m} + \langle r \rangle$ y $\mathfrak{m} + \langle s \rangle$ contienen estrictamente a $\mathfrak{m}$, ellos no pertenecen a $\mathcal{S}$. Esto nos dice que $\mathfrak{m} + \langle r \rangle$ y $\mathfrak{m} + \langle s \rangle$ contienen un producto de ideales primos, y como consecuencia, también lo hace su producto

$$(\mathfrak{m} + \langle r \rangle)(\mathfrak{m} + \langle s \rangle) \subset \mathfrak{m},$$

lo cual es una contradicción pues $\mathfrak{m}$ no contiene un producto de ideales primos. □

LEMA 4.8. *Si $\mathfrak{a}$ es un ideal propio de R, entonces existe $\gamma \in K \setminus R$ tal que $\gamma\mathfrak{a} \subset R$.*

DEMOSTRACIÓN. Sea $a \in \mathfrak{a}$ no nulo. Por Lema 4.7, el ideal $\langle a \rangle$ contiene un producto de ideales primos. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideales primos en R tales que $\langle a \rangle \supset \mathfrak{p}_1 \ldots \mathfrak{p}_r$ con r mínimo, esto es, $\prod_{i \neq i_0} \mathfrak{p}_i$ no está contenido en $\mathfrak{a}$ para todo i_0.

Por otro lado, existe $\mathfrak{m}$ un ideal maximal tal que $\mathfrak{a} \subset \mathfrak{m}$. Luego, como $\mathfrak{m}$ es primo y

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \langle a \rangle \subset \mathfrak{a} \subset \mathfrak{m},$$

tenemos que $\mathfrak{p}_i \subset \mathfrak{m}$ para algún i. Reordenando si es necesario, podemos asumir que $\mathfrak{p}_1 \subset \mathfrak{m}$.

Por (2) en Definición 4.3, $\mathfrak{p}_1 = \mathfrak{m}$. Luego,

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \langle a \rangle \subset \mathfrak{a} \subset \mathfrak{p}_1.$$

Sea $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r \setminus \langle a \rangle$. Se tiene que $\gamma := \frac{b}{a} \in K \setminus R$. Veamos que si $c \in \mathfrak{a}$, entonces $\gamma c \in R$. Como $c \in \mathfrak{p}_1$ y $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$, tenemos que $bc \in \mathfrak{p}_1 \dots \mathfrak{p}_r \subset \langle a \rangle$, esto es, $bc = ad$ para algún $d \in R$, por lo que $\gamma c = \frac{bc}{a} = d \in R$. □

Ejemplo 4.9. En $\mathbb{Z}$, para $\mathfrak{a} = a\mathbb{Z}$, se tiene que $\frac{1}{d}\mathfrak{a} \subset \mathbb{Z}$ para todo $d \mid a$.

Teorema 4.10. *Dado $\mathfrak{a}$ un ideal no nulo de R, existe un ideal $\mathfrak{b}$ de R tal que $\mathfrak{ab}$ es un ideal principal de R.*

Demostración. Sea $\alpha \in \mathfrak{a}$ no nulo, y sea

$$\mathfrak{b} = \{\beta \in R : \beta\mathfrak{a} \in \langle \alpha \rangle\}.$$

Tenemos las siguientes consecuencias:

- $\mathfrak{b}$ es un ideal: si $\beta, \beta' \in \mathfrak{b}$ y $\gamma \in R$, entonces $\beta\gamma\mathfrak{a} = \gamma(\beta\mathfrak{a}) \subset \gamma\langle\alpha\rangle \subset \langle\alpha\rangle$ (i.e. $\beta\gamma \in \mathfrak{b}$), y $(\beta + \beta')\mathfrak{a} \subset \beta\mathfrak{a} + \beta'\mathfrak{a} \subset \langle\alpha\rangle + \langle\alpha\rangle = \langle\alpha\rangle$ (i.e. $\beta + \beta' \in \mathfrak{b}$).
- $\mathfrak{b} \neq 0$ pues $\alpha \in \mathfrak{b}$.
- $\mathfrak{ab} \subset \langle\alpha\rangle$: si $\gamma \in \mathfrak{a}$ y $\beta \in \mathfrak{b}$, entonces $\gamma\beta \in \langle\alpha\rangle$.

Veamos que $\mathfrak{ab} = \langle\alpha\rangle$. Consideremos $I = \frac{1}{\alpha}\mathfrak{ab}$. Tenemos:

- $I \subset R$ pues $\mathfrak{ab} \subset \langle\alpha\rangle$.
- I es un ideal: si $\frac{\gamma}{\alpha} \in I$ y $\delta \in R$, entonces $\gamma\delta \in \mathfrak{ab}$ (producto de ideales es ideal), lo que implica que $\frac{\gamma\delta}{\alpha} \in I$.

Si $I = R$, entonces $\mathfrak{ab} = \alpha R = \langle\alpha\rangle$, que es lo que queríamos probar.

Ahora supongamos que $I \neq R$ y busquemos una contradicción. Lema 4.8 nos asegura que existe $\gamma \in K \setminus R$ tal que $\gamma I \subset R$. Tenemos que $I \supset \mathfrak{b}$ pues si $\beta \in \mathfrak{b}$, entonces $\beta = \frac{\alpha\beta}{\alpha} \in I$. Esto nos dice que $\gamma\beta \in \gamma I \subset R$ para todo $\beta \in \mathfrak{b}$. Más aún,

$$\gamma\mathfrak{b} \subset \mathfrak{b}$$

pues si $\beta \in \mathfrak{b}$, entonces $\gamma\beta\frac{\mathfrak{a}}{\alpha} = \gamma\frac{\beta\mathfrak{a}}{\alpha} \subset I$, lo que implica que $\gamma\beta\mathfrak{a} \subset \langle\alpha\rangle$, de lo que se concluye que $\gamma\beta \in \mathfrak{b}$.

Como $\mathfrak{b}$ es finitamente generado, existen $\beta_1, \dots, \beta_n \in \mathfrak{b}$ tal que $\mathfrak{b} = \beta_1 R + \dots + \beta_n R$. Como $\gamma\mathfrak{b} \subset \mathfrak{b}$, entonces existe $A \in R^{n\times n}$ tal que

$$\gamma \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Esto nos dice que el polinomio mónico $P(x) := \det(xI - A) \in R[x]$ anula a γ, por lo tanto $\gamma \in R$ por Definición 4.3(3), lo cual es una contradicción. □

Corolario 4.11 (Ley de cancelación). *Si $\mathfrak{a}$, $\mathfrak{b}$ y $\mathfrak{c}$ son ideales en R tales que $\mathfrak{ac} = \mathfrak{bc}$, entonces $\mathfrak{a} = \mathfrak{b}$.*

DEMOSTRACIÓN. Por Teorema 4.10, existe un ideal $\widetilde{\mathfrak{c}}$ en R tal que $\mathfrak{c}\widetilde{\mathfrak{c}} = \langle\gamma\rangle$ para algún $\gamma \in R$. Multiplicando por $\widetilde{\mathfrak{c}}$ a ambos lados de $\mathfrak{ac} = \mathfrak{bc}$, obtenemos que $\gamma\mathfrak{a} = \gamma\mathfrak{b}$. Esto implica que $\mathfrak{a} = \mathfrak{b}$. En efecto, si $\alpha \in \mathfrak{a}$, entonces existe $\beta \in \mathfrak{b}$ tal que $\gamma\alpha = \gamma\beta$, por lo tanto $\alpha = \beta \in \mathfrak{b}$. □

El resultado anterior nos permite definir la división entre ideales de R.

DEFINICIÓN 4.12. Dados $\mathfrak{a}$ y $\mathfrak{b}$ ideales en R, decimos que $\mathfrak{a}$ *divide a* $\mathfrak{b}$, y lo denotamos por $\mathfrak{a} \mid \mathfrak{b}$, si existe un ideal $\mathfrak{c}$ de R tal que $\mathfrak{b} = \mathfrak{ac}$. En ese caso, escribimos $\mathfrak{ba}^{-1} = \mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{c}$.

COROLARIO 4.13. *Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales en R. Entonces, $\mathfrak{a} \mid \mathfrak{b}$ si y sólo si $\mathfrak{a} \supset \mathfrak{b}$.*

DEMOSTRACIÓN. La ida sigue de que $\mathfrak{a} \mid \mathfrak{b}$ significa que existe $\mathfrak{c}$ tal que $\mathfrak{b} = \mathfrak{ac} \subset \mathfrak{a}$.

Veamos la vuelta. Asumimos $\mathfrak{a} \supset \mathfrak{b}$. Sea $\widetilde{\mathfrak{a}}$ ideal en R tal que $\mathfrak{a}\widetilde{\mathfrak{a}} = \langle\alpha\rangle$, el cual existe por Teorema 4.10. Definimos $\mathfrak{c} = \frac{1}{\alpha}\widetilde{\mathfrak{a}}\mathfrak{b}$. Tenemos:

- $\mathfrak{c} \subset R$ pues $\frac{1}{\alpha}\widetilde{\mathfrak{a}}\mathfrak{b} \subset \frac{1}{\alpha}\widetilde{\mathfrak{a}}\mathfrak{a} = \frac{1}{\alpha}\langle\alpha\rangle = R$.
- $\mathfrak{c}$ es un ideal en R: si $\frac{\beta}{\alpha} \in \mathfrak{c}$ y $\gamma \in R$, entonces $\beta\gamma \in \widetilde{\mathfrak{a}}\mathfrak{b}$, lo que asegura que $\frac{\beta}{\alpha}\gamma \in \mathfrak{c}$.
- $\mathfrak{b} = \mathfrak{ac}$ pues $\mathfrak{ac} = \mathfrak{a}\frac{1}{\alpha}\widetilde{\mathfrak{a}}\mathfrak{b} = \frac{1}{\alpha}(\mathfrak{a}\widetilde{\mathfrak{a}})\mathfrak{b} = \mathfrak{b}$.

La prueba está completa. □

Estamos en condiciones de probar el resultado principal de esta sección.

TEOREMA 4.14. *Todo ideal propio de R se representa de manera única (salvo el orden) como producto de ideales primos.*

DEMOSTRACIÓN. Primero veamos la existencia de la factorización, esto es, que todo ideal propio se escribe como producto de ideales primos. Asumamos lo contrario, y tomemos

$$\mathcal{F} = \{\text{ideales propios en } R \text{ que no se escriben como producto de ideales primos}\}.$$

Como asumimos que $\mathcal{F}$ es no vacío, la equivalencia (1''') de Definición 4.3(1) nos dice que existe un ideal maximal $\mathfrak{a}$ en $\mathcal{F}$.

Existe $\mathfrak{p}$ un ideal maximal (y por lo tanto primo) en R tal que $\mathfrak{a} \subset \mathfrak{p}$. Como $\mathfrak{p} \mid \mathfrak{a}$ por Corolario 4.13, existe $\mathfrak{b}$ ideal en R tal que $\mathfrak{a} = \mathfrak{pb}$. Esto implica que $\mathfrak{a} \subset \mathfrak{b}$ y $\mathfrak{a} \neq \mathfrak{b}$ (si $\mathfrak{a} = \mathfrak{b}$, entonces $\mathfrak{p} = R$, lo cual no es cierto). Como $\mathfrak{a}$ es maximal en $\mathcal{F}$, tenemos que $\mathfrak{b} \notin \mathcal{F}$, por lo que existen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideales primos en R tal que $\mathfrak{b} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$. Concluimos que

$$\mathfrak{a} = \mathfrak{pb} = \mathfrak{p}\,\mathfrak{p}_1 \ldots \mathfrak{p}_r,$$

lo cual contradice a que $\mathfrak{a} \in \mathcal{F}$. El absurdo proviene de suponer que $\mathcal{F} \neq \emptyset$.

Ahora establezcamos la unicidad de la factorización. Supongamos que existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ tales que

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{q}_1 \ldots \mathfrak{q}_s.$$

Se sigue que $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subset \mathfrak{p}_1$, por lo tanto $\mathfrak{q}_i \subset \mathfrak{p}_1$ para algún $1 \leq i \leq s$. Reordenando en caso de ser necesario, tenemos $\mathfrak{q}_1 \subset \mathfrak{p}_1$. Más aún, como $\mathfrak{q}_1$ y $\mathfrak{p}_1$ son ideales maximales por Definición 4.3(2), tenemos que $\mathfrak{p}_1 = \mathfrak{q}_1$, y por lo tanto

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r = \mathfrak{q}_2 \ldots \mathfrak{q}_s.$$

Procediendo de esta manera, obtendremos que $r = s$ y $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ es solo una permutación de $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. □

3. Ejemplos y consecuencias

Luego de tantos teoremas, volvamos al mundo real con algunos ejemplos. Ejemplo 4.16 será importante para el resto del curso ya que veremos el método de multiplicar ideales dados por generadores.

EJEMPLO 4.15. Sea R un dominio de ideales principales. Para $\mathfrak{a}$ un ideal no nulo de R, se tiene que $\mathfrak{a} = \langle \alpha \rangle$ para algún α en R. Por la factorización única en elementos irreducibles, $\alpha = p_1^{k_1} \dots p_r^{k_r}$ con $p_j \in R$ irreducible (= primo) para todo j. Concluimos que

$$\mathfrak{a} = \langle p_1 \rangle^{k_1} \dots \langle p_r \rangle^{k_r}$$

es la factorización de $\mathfrak{a}$ asegurada por Teorema 4.14 ya que $\langle p_j \rangle$ es primo en R para todo j.

EJEMPLO 4.16. Sea $K = \mathbb{Q}(\sqrt{-5})$. El anillo de enteros $\mathcal{O}_K$ de K no es un dominio de factorización única. En efecto,

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

mientras que $2, 3, 1 \pm \sqrt{-5}$ son todos irreducibles en $\mathcal{O}_K$ (usar la norma $N_K(\cdot)$ para chequear esto). Luego,

$$\langle 2 \rangle \langle 3 \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle.$$

Veamos que esta identidad no contradice la factorización única de Teorema 4.14 mostrando que ninguno de estos ideales es primo, a pesar de ser ideales principales generados por elementos irreducibles.

Definimos

$$\mathfrak{p}_0 = \langle 2, 1 + \sqrt{-5} \rangle,$$
$$\mathfrak{p}_1 = \langle 3, 1 + \sqrt{-5} \rangle,$$
$$\mathfrak{p}_2 = \langle 3, 1 - \sqrt{-5} \rangle.$$

Tenemos que $\mathfrak{p}_0 = \langle 2, 1 - \sqrt{-5} \rangle$. Para mostrar esto, basta ver que los generadores de cada lado están en el otro ideal. Esto sigue fácilmente de que $-(1 - \sqrt{-5}) = 1 + \sqrt{-5} - 2$. Además tenemos que

$$\mathfrak{p}_0^2 = \langle 4, 2(1 \pm \sqrt{-5}), 6 \rangle = \langle 2 \rangle.$$

En efecto, $\subset$ es clara pues todos los generadores de $\langle 4, 2(1 \pm \sqrt{-5}), 6 \rangle$ son múltiplos de 2, mientras que $\supset$ sigue de que $2 = 6 - 4 \in \langle 4, 2(1 \pm \sqrt{-5}), 6 \rangle$. De manera similar se pueden mostrar las identidades del siguiente ejercicio.

EJERCICIO 4.17. Mostrar las siguientes identidades:

$$\mathfrak{p}_1 \mathfrak{p}_2 = \langle 3 \rangle,$$
$$\mathfrak{p}_0 \mathfrak{p}_1 = 6 \rangle = \langle 1 + \sqrt{-5} \rangle,$$
$$\mathfrak{p}_0 \mathfrak{p}_2 = \langle 1 - \sqrt{-5} \rangle.$$

A partir de ahora realizaremos estos cálculos sin dar los detalles ni hacer mención de ellos, ya que será muy común y el método siempre es similar.

Mostraremos que $\mathfrak{p}_0$, $\mathfrak{p}_1$ y $\mathfrak{p}_2$ son ideales primos por ser maximales. Para esto último, el siguiente ejercicio será de mucha utilidad. Más adelante, esta tarea será más simple usando la herramienta norma que introduciremos al comienzo de Capítulo 5.

EJERCICIO 4.18. Probar las siguientes identidades:

$$\mathfrak{p}_0 = 2\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z},$$
$$\mathfrak{p}_1 = 3\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z},$$
$$\mathfrak{p}_2 = 3\mathbb{Z} + (1-\sqrt{-5})\mathbb{Z}.$$

Como $\mathcal{O}_K = \mathbb{Z} + (1+\sqrt{-5})\mathbb{Z} = \mathbb{Z} + (1-\sqrt{-5})\mathbb{Z}$, tenemos que $\mathcal{O}_K/\mathfrak{p}_0 \simeq \mathbb{Z}/2\mathbb{Z}$ y $\mathcal{O}_K/\mathfrak{p}_1 \simeq \mathcal{O}_K/\mathfrak{p}_2 \simeq \mathbb{Z}/3\mathbb{Z}$. Luego, si $\mathfrak{m}$ es un ideal maximal de $\mathcal{O}_K$ tal que $\mathfrak{p}_i \subset \mathfrak{m} \subset \mathcal{O}_K$, entonces $\mathcal{O}_K/\mathfrak{m}$ es un subanillo de $\mathcal{O}_K/\mathfrak{p}_i$, lo que implica que $\mathcal{O}_K/\mathfrak{m}$ debe ser $\mathcal{O}_K/\mathfrak{p}_i$ o $\{0\}$, esto es, $\mathfrak{m} = \mathfrak{p}_i$ o $\mathfrak{m} = \mathcal{O}_K$.

Concluimos que la factorización en ideales primos de $\langle 6\rangle$ es

$$\langle 6\rangle = \mathfrak{p}_0^2\,\mathfrak{p}_1\,\mathfrak{p}_2,$$

lo cual es consistente con lo que vimos al comienzo del ejemplo.

DEFINICIÓN 4.19. Sean $\mathfrak{a} = \mathfrak{p}_1^{h_1}\dots\mathfrak{p}_r^{h_r}$ y $\mathfrak{b} = \mathfrak{p}_1^{k_1}\dots\mathfrak{p}_r^{k_r}$ ideales en R con $\mathfrak{p}_j$ ideal primo en R y $h_j, k_j \in \mathbb{N}_0$ para todo j, y $\mathfrak{p}_i \neq \mathfrak{p}_j$ para todo $i \neq j$. (Notar que siempre podemos escribir así a dos ideales dados permitiendo que h_i o k_i sea 0 para cada i). Definimos

- el *máximo común divisor de* $\mathfrak{a}$ *y* $\mathfrak{b}$ como el ideal $\operatorname{mcd}(\mathfrak{a},\mathfrak{b}) := \prod_{i=1}^r \mathfrak{p}_i^{\min(h_i,k_i)}$,
- el *mínimo común múltiplo de* $\mathfrak{a}$ *y* $\mathfrak{b}$ como el ideal $\operatorname{mcm}(\mathfrak{a},\mathfrak{b}) := \prod_{i=1}^r \mathfrak{p}_i^{\max(h_i,k_i)}$.

EJERCICIO 4.20. Demostrar las siguientes afirmaciones:

- $\operatorname{mcd}(\mathfrak{a},\mathfrak{b})$ coincide con el único ideal $\mathfrak{c}$ de R tal que $\mathfrak{c} \mid \mathfrak{a}$, $\mathfrak{c} \mid \mathfrak{b}$, y si $\mathfrak{d} \mid \mathfrak{a}$ y $\mathfrak{d} \mid \mathfrak{b}$, entonces $\mathfrak{d} \mid \mathfrak{c}$.
- $\operatorname{mcm}(\mathfrak{a},\mathfrak{b})$ coincide con el único ideal $\mathfrak{c}$ de R tal que $\mathfrak{a} \mid \mathfrak{c}$, $\mathfrak{b} \mid \mathfrak{c}$, y si $\mathfrak{a} \mid \mathfrak{d}$ y $\mathfrak{b} \mid \mathfrak{d}$, entonces $\mathfrak{c} \mid \mathfrak{d}$.

PROPOSICIÓN 4.21. *Para* $\mathfrak{a}$ *y* $\mathfrak{b}$ *dos ideales en* R*, se tiene que*

$$\operatorname{mcd}(\mathfrak{a},\mathfrak{b}) = \mathfrak{a} + \mathfrak{b},$$
$$\operatorname{mcm}(\mathfrak{a},\mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}.$$

DEMOSTRACIÓN. Por Corolario 4.13, $\mathfrak{a}+\mathfrak{b}$ divide a $\mathfrak{a}$ y $\mathfrak{b}$ pues $\mathfrak{a}$ y $\mathfrak{b}$ están claramente contenidos en $\mathfrak{a}+\mathfrak{b}$. Además, supongamos que $\mathfrak{d}$ es un ideal de R que divide a $\mathfrak{a}$ y $\mathfrak{b}$. Entonces $\mathfrak{a} \subset \mathfrak{d}$ y $\mathfrak{b} \subset \mathfrak{d}$, lo que implica que $\mathfrak{a}+\mathfrak{b} \subset \mathfrak{d}$, esto es, $\mathfrak{d}$ divide a $\mathfrak{a}+\mathfrak{b}$. Concluimos que $\mathfrak{a}+\mathfrak{b} = \operatorname{mcd}(\mathfrak{a},\mathfrak{b})$.

El otro caso es muy similar. □

TEOREMA 4.22. *Sean* $\mathfrak{a}$ *un ideal en* R *y* $\alpha \in \mathfrak{a}$ *no nulo. Existe* $\beta \in \mathfrak{a}$ *tal que*

$$\mathfrak{a} = \langle \alpha, \beta\rangle = \alpha R + \beta R.$$

DEMOSTRACIÓN. Buscamos $\beta \in R$ tal que

$$\mathfrak{a} = \operatorname{mcd}(\langle\alpha\rangle, \langle\beta\rangle) = \langle\alpha\rangle + \langle\beta\rangle = \langle\alpha,\beta\rangle.$$

Sea

$$\mathfrak{a} = \mathfrak{p}_1^{k_1}\dots\mathfrak{p}_r^{k_r}$$

la factorización en ideales primos de $\mathfrak{a}$, esto es, $k_i \in \mathbb{N}$ y $\mathfrak{p}_i$ ideal primo de R para todo i, y $\mathfrak{p}_i \neq \mathfrak{p}_j$ para todo $i \neq j$. Como $\langle\alpha\rangle \subset \mathfrak{a}$, tenemos que la factorización en ideales primos de $\langle\alpha\rangle$ es de la forma

$$\langle\alpha\rangle = \mathfrak{p}_1^{h_1}\dots\mathfrak{p}_r^{h_r}\mathfrak{q}_1^{l_1}\dots\mathfrak{q}_s^{l_s},$$

con $h_i \geq k_i$ para todo $1 \leq i \leq r$, $l_i \geq 0$ para todo $1 \leq i \leq s$, $\mathfrak{q}_i \neq \mathfrak{q}_j$ para todo $i \neq j$, y $\mathfrak{p}_i \neq \mathfrak{q}_j$ para todo i, j.

Notemos que el elemento β que buscamos debe tener factorización en ideales primos de la forma

$$\langle \beta \rangle = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \mathfrak{b},$$

con $\operatorname{mcd}(\mathfrak{b}, \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s) = R$.

Para cada $1 \leq i \leq r$, tomemos $\beta_i \in \mathfrak{p}_i^{k_i} \smallsetminus \mathfrak{p}_i^{k_i+1}$. (Notar que la factorización única nos impide que $\mathfrak{p}^k = \mathfrak{p}^{k+1}$ para cualquier ideal primo $\mathfrak{p}$ y $k \in \mathbb{N}_0$.) Usaremos el siguiente resultado sin demostración.

Teorema Chino del Resto: *Si $I_1, \dots, I_r$ son ideales en R coprimos entre sí (i.e. $I_i + I_j = R$ para todo $i \neq j$), entonces el mapeo obvio*

$$R/\bigcap_{i=1}^{r} I_i \longrightarrow R/I_1 \times \dots \times R/I_r$$

es un isomorfismo.

En nuestro caso,

$$\begin{aligned}
&R = \operatorname{mcd}(\mathfrak{p}_i^{k_i+1}, \mathfrak{p}_j^{k_j+1}) = \mathfrak{p}_i^{k_i+1} + \mathfrak{p}_j^{k_j+1} && \text{para } 1 \leq i < j \leq r,\\
&R = \operatorname{mcd}(\mathfrak{p}_i^{k_i+1}, \mathfrak{q}_j) = \mathfrak{p}_i^{k_i+1} + \mathfrak{q}_j && \text{para } 1 \leq i \leq r \text{ y } 1 \leq j \leq s,\\
&R = \operatorname{mcd}(\mathfrak{q}_i, \mathfrak{q}_j) = \mathfrak{q}_i + \mathfrak{q}_j && \text{para } 1 \leq i < j \leq s.
\end{aligned}$$

Concluimos que existe $\beta \in R$ tal que el isomorfismo lo mapea a

$$(\beta_1, \dots, \beta_r, 1, \dots, 1) \in R/\mathfrak{p}_1^{k_1+1} \times \dots \times \mathfrak{p}_r^{k_r+1} \times \mathfrak{q}_1 \times \dots \times \mathfrak{q}_s,$$

esto es

$$\begin{aligned}
&\beta - \beta_i \in \mathfrak{p}_i^{k_i+1} \quad \text{para todo } 1 \leq i \leq r,\\
&\beta - 1 \in \mathfrak{q}_j \quad \text{para todo } 1 \leq j \leq s.
\end{aligned}$$

Para cada $1 \leq i \leq r$, tenemos que $\beta = (\beta - \beta_i) + \beta_i \in \mathfrak{p}_i^{k_i}$, por lo que $\langle \beta \rangle \subset \mathfrak{p}_i^{k_i}$ y $\mathfrak{p}_i^{k_i} \mid \langle \beta \rangle$. Entonces

$$\langle \beta \rangle \subset \bigcap_{i=1}^{r} \mathfrak{p}_i^{k_i} = \operatorname{mcm}(\mathfrak{p}_1^{k_1}, \dots, \mathfrak{p}_r^{k_r}).$$

Por la factorización única en ideales primos (Teorema 4.14), existe un ideal $\mathfrak{b}$ tal que

$$\langle \beta \rangle = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}\, \mathfrak{b}.$$

Resta ver que $\mathfrak{b}$ es coprimo a $\mathfrak{p}_i$ y $\mathfrak{q}_j$ para todo i, j.

Como $\beta \in \mathfrak{b}$ y $\beta - 1 \in \mathfrak{q}_j$, se tiene que $\operatorname{mcd}(\mathfrak{b}, \mathfrak{q}_i) = \mathfrak{b} + \mathfrak{q}_i = R$. Además $\operatorname{mcd}(\mathfrak{b}, \mathfrak{p}_i) = R$, pues de lo contrario $\operatorname{mcd}(\mathfrak{b}, \mathfrak{p}_i) = \mathfrak{p}_i$, lo que implica que $\beta \in \mathfrak{p}_i^{k_i} \mathfrak{p}_i = \mathfrak{p}_i^{k_i+1}$, lo cual es imposible pues $\beta_i \notin \mathfrak{p}_i^{k_i+1}$ y $\beta - \beta_i \in \mathfrak{p}_i^{k_i+1}$.

Concluimos que $R = \operatorname{mcd}(\mathfrak{b}, \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s)$, lo que a su vez asegura que

$$\langle \alpha \rangle + \langle \beta \rangle = \operatorname{mcd}(\langle \alpha \rangle, \langle \beta \rangle) = \operatorname{mcd}(\mathfrak{p}_1^{h_1} \dots \mathfrak{p}_r^{h_r} \mathfrak{q}_1^{l_1} \dots \mathfrak{q}_s^{l_s}, \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \mathfrak{b}) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} = \mathfrak{a},$$

que prueba la afirmación. □

Teorema 4.23. *Si un dominio de Dedekind R es un dominio de factorización única, entonces R es un dominio de ideales principales.*

DEMOSTRACIÓN. Tomamos un ideal $\mathfrak{a}$ en R y veamos que es principal. Por Teorema 4.10, existe un ideal $\mathfrak{b}$ en R tal que $\mathfrak{ab} = \langle\alpha\rangle$ para algún $\alpha \in R$. La factorización en elementos irreducibles $\alpha = p_1^{k_1} \dots p_r^{k_r}$ en R implica que

$$\mathfrak{ab} = \langle\alpha\rangle = \langle p_1\rangle^{k_1} \dots \langle p_r\rangle^{k_r}.$$

Notemos que $\mathfrak{p}_i := \langle p_i\rangle$ es un ideal primo de R por ser p_i primo en R. Luego, la factorización única de ideales nos asegura que existe $h_1, \dots, h_r \in \mathbb{Z}$ tales que $0 \leq h_i \leq k_i$ para todo i y

$$\mathfrak{a} = \mathfrak{p}_1^{h_1} \dots \mathfrak{p}_r^{h_r} = \langle p_1^{h_1} \dots p_r^{h_r}\rangle.$$

En particular, $\mathfrak{a}$ es principal. □

OBSERVACIÓN 4.24. El anillo $\mathbb{Z}[x]$ es un ejemplo de un dominio de factorización única que no es un dominio de ideales principales. En particular, $\mathbb{Z}[x]$ no es un dominio de Dedekind.

Finalizamos este capítulo con el siguiente resultado que será utilizado (únicamente) en Proposición 5.6.

LEMA 4.25. *Dados $\mathfrak{a}$ y $\mathfrak{b}$ ideales de un dominio de Dedekind R, existe $\alpha \in \mathfrak{a}$ tal que* $\operatorname{mcd}(\mathfrak{ab}, \langle\alpha\rangle) = \mathfrak{a}$.

DEMOSTRACIÓN. Supongamos que $\mathfrak{a} = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}$ y $\mathfrak{b} = \mathfrak{p}_1^{h_1} \dots \mathfrak{p}_r^{h_r}$ con $k_i \in \mathbb{N}_0$ y $\mathfrak{p}_i$ ideal primo en R para todo i, y $\mathfrak{p}_i \neq \mathfrak{p}_j$ para todo $i \neq j$. Para cada $1 \leq i \leq r$, sea

$$\alpha_i \in \mathfrak{p}_1^{k_1+1} \dots \mathfrak{p}_{i-1}^{k_{i-1}+1} \mathfrak{p}_i^{k_i} \mathfrak{p}_{i+1}^{k_{i+1}+1} \dots \mathfrak{p}_r^{k_r+1} \smallsetminus \mathfrak{p}_1^{k_1+1} \dots \mathfrak{p}_r^{k_r+1}.$$

Tomemos $\alpha = \alpha_1 + \dots + \alpha_n$, y veamos que cumple con la afirmación.

Escribimos

$$\langle\alpha\rangle = \mathfrak{p}_1^{l_1} \dots \mathfrak{p}_r^{l_r} \mathfrak{c},$$

con $\mathfrak{c}$ ideal de R coprimo a $\mathfrak{p}_i$ para todo i. Como $\alpha \in \mathfrak{p}_i^{k_i}$ para todo i, y $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ son coprimos de a pares, entonces $\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \mid \langle\alpha\rangle$, por lo tanto $l_i \geq k_i$ para todo i.

Afirmamos que $l_i = k_i$ para todo i. Supongamos que $l_i > k_i$ para algún i, es decir, $\mathfrak{p}_i^{k_i+1} \mid \langle\alpha\rangle$, o equivalentemente $\alpha \in \mathfrak{p}_i^{k_i+1}$. Como además $\alpha_j \in \mathfrak{p}_i^{k_i+1}$ para todo $j \neq i$, resulta que $\alpha_i \in \mathfrak{p}_i^{k_i+1}$. Por definición, $\alpha_i \in \mathfrak{p}_j^{k_j+1}$ para todo $j \neq i$, por lo tanto

$$\alpha_i \in \mathfrak{p}_i^{k_i+1} \bigcap \prod_{j \neq i} \mathfrak{p}_j^{k_j+1} = \operatorname{mcm}\left(\mathfrak{p}_i^{k_i+1}, \prod_{j \neq i} \mathfrak{p}_j^{k_j+1}\right) = \prod_j \mathfrak{p}_j^{k_j+1}.$$

Esto es una contradicción ya que $\alpha_i \notin \prod_j \mathfrak{p}_j^{k_j+1}$ por definición. El absurdo provino de suponer $l_i > k_i$, por lo tanto $l_i = k_i$ para todo i. Concluimos que

$$\operatorname{mcd}(\mathfrak{ab}, \langle\alpha\rangle) = \operatorname{mcd}(\mathfrak{p}_1^{k_1+h_1} \dots \mathfrak{p}_r^{k_r+h_r}, \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \mathfrak{c}) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} = \mathfrak{a},$$

que es lo que buscábamos. □

Problemas.

4.2. Sea $K = \mathbb{Q}(\sqrt{-14})$, por lo tanto $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$. Descomponer como producto de ideales primos a los ideales $\langle 15\rangle$ y $\langle 81\rangle$. Recordar que en §3 vimos que 15 y 81 se descomponen como producto de elementos irreducibles en $\mathcal{O}_K$ de dos formas distintas:

$$15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}),$$
$$81 = 3^4 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

4.3. Sea $K = \mathbb{Q}(\sqrt{-1})$, por lo tanto $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$.

(a) Para p un primo racional, descomponer el ideal $\langle p \rangle = p\mathcal{O}_K$ en producto de ideales primos de $\mathcal{O}_K$.

(b) Determinar todos los ideales primos en $\mathcal{O}_K$.

Hacer lo mismo con $K = \mathbb{Q}(\sqrt{2})$ y con $K = \mathbb{Q}(\sqrt{-3})$.

Capítulo 5

Grupo de clases de ideales

1. Norma de ideales

En esta sección consideramos el anillo de enteros $\mathcal{O}_K$ de un cuerpo de números K de orden n.

DEFINICIÓN 5.1. Dado $\mathfrak{a}$ un ideal en $\mathcal{O}_K$, definimos la *norma de* $\mathfrak{a}$ como $N(\mathfrak{a}) := \#(\mathcal{O}_k/\mathfrak{a})$.

OBSERVACIÓN 5.2. Si $\mathfrak{a}$ es un ideal en $\mathcal{O}_K$ tal que $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ con $a > 0$, entonces $\langle a \rangle \subset \mathfrak{a}$, por lo tanto

$$N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a}) \leq \#(\mathcal{O}_K/\langle a \rangle) = a^n.$$

OBSERVACIÓN 5.3. Supongamos que $\mathfrak{a}$ es un ideal de $\mathcal{O}_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$. Como $\mathfrak{a}$ es un $\mathbb{Z}$-módulo libre de rango n, existen $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ y una matriz $A = (a_{i,j})_{i,j} \in \mathbb{Z}^{n\times n}$ triangular inferior (i.e. $a_{i,j} = 0$ para $i < j$) con entradas diagonales positivas (i.e. $a_{i,i} > 0$ para todo i) tales que

$$\mathfrak{a} = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z} \quad \text{y} \quad \beta_i = \sum_{j=1}^{n} a_{i,j}\alpha_j \quad \text{para todo } 1 \leq i \leq n.$$

Las n identidades de la derecha se resumen así:

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \\ a_{n,1} & \ldots & a_{n,n} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

LEMA 5.4. *Bajo la notación de Observación 5.3, tenemos que*

$$N(\mathfrak{a}) = a_{1,1} \ldots a_{n,n}.$$

DEMOSTRACIÓN. Es suficiente ver que

$$\{b_1\alpha_1 + \cdots + b_n\alpha_n : 0 \leq b_i < a_{i,i}\}$$

es un conjunto de representantes de $\mathcal{O}_K/\mathfrak{a}$.

Sea $\gamma = \sum_{i=1}^{n} c_i\alpha_i \in \mathcal{O}_K$ con $c_i \in \mathbb{Z}$ para todo i. Por el algoritmo de la división en $\mathbb{Z}$, existen $m_1, b_1 \in \mathbb{Z}$ tales que $c_1 = m_1a_{1,1} + b_1$ con $0 \leq b_1 < a_{1,1}$. Luego,

$$\gamma_1 := \gamma - b_1\alpha_1 - m_1\beta_1 \in \mathcal{O}_K \cap (\alpha_2\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}).$$

De la misma manera, existen $m_2, b_2 \in \mathbb{Z}$ con $0 \leq b_2 < a_{2,2}$ tales que

$$\gamma_2 := \gamma_1 - b_2\alpha_2 - m_2\beta_2 \in \mathcal{O}_K \cap (\alpha_3\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}).$$

Procediendo de esta manera, tenemos que

$$\gamma = \sum_{i=1}^{n}(m_i\beta_i + b_i\alpha_i) = \underbrace{\sum_{i=1}^{n} m_i\beta_i}_{\in\mathfrak{a}} + \sum_{i=1}^{n} b_i\alpha_i.$$

donde $m_i, b_i \in \mathbb{Z}$ y $0 \leq b_i < a_{i,i}$ para todo $1 \leq i \leq n$. Esto muestra que $\sum_{i=1}^{n} b_i\alpha_i$ representa a γ en $\mathcal{O}_K/\mathfrak{a}$.

Ahora veamos que no hay dos representantes asociados entre sí. Esto sigue mostrando que si $\sum_{i=1}^{n} b_i\alpha_i \in \mathfrak{a}$ con $b_i \in \mathbb{Z}$ y $0 \leq b_i < a_{i,i}$ para todo i, entonces $b_i = 0$ para todo i. □

PROPOSICIÓN 5.5. *Para $\alpha \in \mathcal{O}_K$, se tiene que $N(\langle\alpha\rangle) = |N_K(\alpha)|$.*

DEMOSTRACIÓN. Escribimos

$$\mathcal{O}_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$$

para ciertos $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, lo cual está asegurado por Corolario 3.40. Sean $\beta_1, \ldots, \beta_n \in \langle\alpha\rangle$ y $A \in \mathbb{Z}^{n\times n}$ como en Observación 5.3, en particular,

$$\langle\alpha\rangle = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z} \quad \text{y} \quad \begin{pmatrix}\beta_1\\ \vdots \\ \beta_n\end{pmatrix} = A\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix}.$$

Por Lema 5.4, tenemos que

$$N(\langle\alpha\rangle) = a_{1,1}\ldots a_{n,n} = \det(A).$$

Veamos que $|N_K(\alpha)| = \det(A)$. Notemos que

$$\langle\alpha\rangle = \alpha\alpha_1\mathbb{Z} + \cdots + \alpha\alpha_n\mathbb{Z}.$$

Como $\{\beta_1, \ldots, \beta_n\}$ es también otra $\mathbb{Z}$-base de $\langle\alpha\rangle$, existe $R \in \mathbb{Z}^{n\times n}$ con $\det(R) \neq 0$ tal que

$$\alpha\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix} = R\begin{pmatrix}\beta_1\\ \vdots \\ \beta_n\end{pmatrix} = RA\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix}$$

Por otro lado, en Ejercicio 3.12 vimos que el determinante de la transformación lineal

$$\begin{aligned} U_\alpha : K^n &\longrightarrow K^n,\\ \gamma &\longmapsto \alpha\gamma, \end{aligned}$$

es precisamente $N_K(\alpha)$. Concluimos que

$$N_K(\alpha) = \det(U_\alpha) = \det(RA) = \det(R)\det(A) = \pm a_{1,1}\ldots a_{n,n} = \pm N(\langle\alpha\rangle),$$

pues R es una matriz invertible en $\mathbb{Z}^{n\times n}$ y por lo tanto su determinante es invertible en $\mathbb{Z}$, y además A es triangular superior por lo que su determinante es igual al producto de las entradas diagonales. □

PROPOSICIÓN 5.6. *La norma de ideales es multiplicativa, esto es,*

$$N(\mathfrak{ab}) = N(\mathfrak{a})\,N(\mathfrak{b})$$

para $\mathfrak{a}$ y $\mathfrak{b}$ ideales en $\mathcal{O}_K$.

DEMOSTRACIÓN. Denotemos $r = N(\mathfrak{a})$ y $s = N(\mathfrak{b})$. Además, sean $\{\mu_1, \dots, \mu_r\}$ y $\{\eta_1, \dots, \eta_s\}$ conjuntos de representantes de $\mathcal{O}_K/\mathfrak{a}$ y $\mathcal{O}_K/\mathfrak{b}$ respectivamente.

Lema 4.25 nos asegura que existe $\alpha \in \mathfrak{a}$ tal que

$$\mathfrak{a} = \mathrm{mcd}(\mathfrak{ab}, \langle\alpha\rangle) = \mathfrak{ab} + \langle\alpha\rangle.$$

Es suficiente mostrar que

$$\mathcal{R} := \{\mu_i + \alpha\,\eta_j : 1 \le i \le r,\ 1 \le j \le s\}$$

es un conjunto de representantes de $\mathcal{O}_K/\mathfrak{ab}$ pues $\#\mathcal{R} = rs = N(\mathfrak{a})N(\mathfrak{b})$.

Veamos que dos elementos en $\mathcal{R}$ no son equivalentes módulo $\mathfrak{ab}$. Supongamos que

$$(\mu_i + \alpha\,\eta_j) - (\mu_k + \alpha\,\eta_l) \in \mathfrak{ab}.$$

Entonces

$$\mu_i - \mu_k = (\mu_i + \alpha\,\eta_j) - (\mu_k + \alpha\,\eta_l) - \alpha(\eta_j - \eta_l) \in \mathfrak{ab} + \langle\alpha\rangle = \mathfrak{a},$$

por lo tanto $i = k$. Esto implica que

$$\alpha(\eta_j - \eta_l) \in \mathfrak{ab}.$$

(Notar que el hecho que α pertenezca a $\mathfrak{a}$ no es suficiente para asegurar que $\eta_j - \eta_l \in \mathfrak{b}$.) Como $\mathrm{mcd}(\mathfrak{ab}, \langle\alpha\rangle) = \mathfrak{a}$, tenemos que $\langle\alpha\rangle = \mathfrak{ac}$ para algún $\mathfrak{c}$ ideal en $\mathcal{O}_K$ coprimo a $\mathfrak{b}$. Luego,

$$\mathfrak{ab} \mid \langle\alpha\rangle\langle\eta_j - \eta_l\rangle = \mathfrak{ac}\langle\eta_j - \eta_l\rangle,$$

de lo que obtenemos que $\mathfrak{b} \mid \langle\eta_j - \eta_l\rangle$ tal como queríamos, pues esto fuerza a que $j = l$.

Ahora veamos que un elemento arbitrario en $\mathcal{O}_K$ es equivalente módulo $\mathfrak{ab}$ a algún elemento en $\mathcal{R}$. Sea $\gamma \in \mathcal{O}_K$. Sabemos que $\gamma - \mu_i \in \mathfrak{a}$ para algún $1 \le i \le r$. Como $\mathfrak{a} = \mathfrak{ab} + \langle\alpha\rangle$, existe $\eta \in \mathcal{O}_K$ tal que

$$\gamma - \mu_i - \alpha\eta \in \mathfrak{ab}.$$

También sabemos que $\delta := \eta - \eta_j \in \mathfrak{b}$ para algún $1 \le j \le s$. Como $\alpha\delta \in \mathfrak{ab}$, obtenemos que

$$\gamma - \mu_i - \alpha\eta_j = \gamma - \mu_i - \alpha\eta + \alpha\delta \in \mathfrak{ab},$$

tal como queríamos. □

PROPOSICIÓN 5.7. *Sea $\mathfrak{a}$ un ideal en $\mathcal{O}_K$, para K un cuerpo de números de grado n.*

1. *Si $N(\mathfrak{a})$ es primo en $\mathbb{Z}$, entonces $\mathfrak{a}$ es un ideal primo de $\mathcal{O}_K$.*
2. *Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ y $\mathfrak{p} \cap \mathbb{Z} = \langle p\rangle$, entonces $N(\mathfrak{p}) = p^f$ para algún $0 < f \le n$.*
3. *Dado p primo en $\mathbb{Z}$, existen a lo sumo n ideales primos que contienen a p.*

DEMOSTRACIÓN. (1) Sea $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ la factorización de $\mathfrak{a}$ en ideales primos. Tomando la norma en ambos lados obtenemos que $N(\mathfrak{p}_1) \dots N(\mathfrak{p}_r)$ es un entero primo, lo cual implica que $r = 1$ pues $N(\mathfrak{p}_i) > 1$ para todo i.

(2) Como $p \in \mathfrak{p}$, tenemos que $\mathfrak{p} \mid \langle p\rangle$, y por lo tanto $N(\mathfrak{p})$ divide a $N(\langle p\rangle) = |N_K(p)| = p^n$.

(3) La factorización de $\langle p\rangle$ en ideales primos

$$\langle p\rangle = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \qquad (\mathfrak{p}_i \neq \mathfrak{p}_j \quad \forall\, i \neq j,\ \ k_1, \dots, k_r \in \mathbb{N})$$

nos asegura que $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ son los únicos ideales primos en $\mathcal{O}_K$ que contienen a p. En efecto, si $p \in \mathfrak{q}$ para algún ideal primo $\mathfrak{q}$, entonces $\langle p\rangle \subset \mathfrak{q}$ y por lo tanto $\mathfrak{q} \mid \langle p\rangle$ por

Corolario 4.13, por lo que concluimos que $\mathfrak{q} = \mathfrak{p}_i$ para algún i por la unicidad de la factorización (Teorema 4.14). Escribimos $N(\mathfrak{p}_i) = p^{f_i}$ con $0 < f_i \leq n$. Como

$$p^n = |N_K(p)| = N(\langle p \rangle) = N(\mathfrak{p}_1)^{k_1} \dots N(\mathfrak{p}_r)^{k_r} = p^{f_1 k_1 + \dots + f_r k_r},$$

se tiene que $n = f_1 k_1 + \dots + f_r k_r$, lo que implica de manera inmediata que $r \leq n$ pues $f_i k_i \geq 1$ para todo i. □

TEOREMA 5.8. *Sea K un cuerpo de números. Dado $\lambda > 0$, existe una cantidad finita de ideales de norma $\leq \lambda$.*

DEMOSTRACIÓN. Como obviamente existe una cantidad finita de números primos positivos menores o iguales a λ, Proposición 5.7 nos asegura que existe una cantidad finita de ideales primos de norma $\leq \lambda$. Por la factorización única de ideales como producto de ideales primos (Teorema 4.14), concluimos que existe una cantidad finita de ideales enteros en $\mathcal{O}_K$ de norma menor a λ. □

Problemas.

5.1. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(a) Sea $\mathfrak{a}$ un ideal en un dominio de Dedekind R. Probar que $N(\mathfrak{a}) = \#(R/\mathfrak{a})$ es un primo racional si y sólo si $\mathfrak{a}$ es un ideal primo en R.
(b) $N(\langle \alpha, \beta \rangle) = \text{mcd}(|N_K(\alpha)|, |N_K(\beta)|)$ para todo $\alpha, \beta \in \mathcal{O}_K$.

2. Número de clases de ideales

En esta sección seguimos denotando por K a un cuerpo de números de orden n.

DEFINICIÓN 5.9. Decimos que dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ de $\mathcal{O}_K$ están en la misma clase si existen $\alpha, \beta \in \mathcal{O}_K$ no nulos tales que $\alpha\mathfrak{a} = \beta\mathfrak{b}$. En este caso, denotamos $\mathfrak{a} \sim \mathfrak{b}$.

EJERCICIO 5.10. Demostrar que $\sim$ es una relación de equivalencia. Además, probar que todos los ideales principales están en la misma clase.

LEMA 5.11. *Todo ideal en la misma clase que un ideal principal es necesariamente principal.*

DEMOSTRACIÓN. Supongamos que existen un ideal $\mathfrak{a}$ y elementos $\alpha, \beta \in \mathcal{O}_K$ tales que $\alpha\mathfrak{a} = \langle \beta \rangle$. Como $\beta \in \alpha\mathfrak{a} \subset \langle \alpha \rangle$, existe $\gamma \in \mathcal{O}_K$ tal que $\beta = \alpha\gamma$. Veamos que $\mathfrak{a} = \langle \gamma \rangle$.

Sea $\delta \in \mathfrak{a}$. Como $\alpha\delta \in \alpha\mathfrak{a} = \langle \beta \rangle$, $\delta\alpha = \beta\mu$ para algún $\mu \in \mathcal{O}_K$. Entonces $\delta\beta = \delta(\gamma\alpha) = \beta\mu\gamma$, por lo tanto $\delta = \mu\gamma \in \langle \gamma \rangle$. Luego, $\mathfrak{a} \subset \langle \gamma \rangle$. Ahora sea $\gamma\delta \in \langle \gamma \rangle$ para algún $\delta \in \mathcal{O}_K$. Entonces $\gamma\delta\alpha = \delta\beta \in \langle \beta \rangle = \alpha\mathfrak{a}$, por lo tanto $\gamma\delta \in \mathfrak{a}$. Concluimos que $\mathfrak{a} = \langle \gamma \rangle$. □

OBSERVACIÓN 5.12. El conjunto de clases forma un grupo abeliano con la multiplicación obvia (i.e. $\bar{\mathfrak{a}} \cdot \bar{\mathfrak{b}} = \overline{\mathfrak{ab}}$, donde $\bar{\mathfrak{a}}$ y $\bar{\mathfrak{b}}$ denotan las clases de $\mathfrak{a}$ y $\mathfrak{b}$). En efecto,

- $\overline{\langle 1 \rangle} = \overline{\mathcal{O}_K}$ es el elemento neutro.
- Asociatividad: $(\bar{\mathfrak{a}} \cdot \bar{\mathfrak{b}}) \cdot \bar{\mathfrak{c}} = \bar{\mathfrak{a}} \cdot (\bar{\mathfrak{b}} \cdot \bar{\mathfrak{c}})$ pues $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$.
- Inverso: dado $\mathfrak{a}$ un ideal de $\mathcal{O}_K$, Teorema 4.10 asegura que existe un ideal $\mathfrak{b}$ de $\mathcal{O}_K$ tal que $\mathfrak{ab}$ es principal, esto es $\bar{\mathfrak{a}}^{-1} = \bar{\mathfrak{b}}$.

DEFINICIÓN 5.13. El grupo de la observación anterior es llamado el *grupo de clases de ideales de $\mathcal{O}_K$*. Su orden, que se denota $\mathfrak{h}_K$, es llamado el *número de clase de $\mathcal{O}_K$*.

OBSERVACIÓN 5.14. Claramente, $\mathcal{O}_K$ es un dominio de ideales principales si y sólo si $\mathfrak{h}_K = 1$. Recordemos que por Teorema 4.23, si $\mathcal{O}_K$ es un dominio de factorización única, entonces necesariamente es un dominio de ideales principales. En particular, cualquier cuerpo de números K tal que $\mathcal{O}_K$ no es un dominio de factorización única (e.g. $K = \mathbb{Q}(\sqrt{-5})$ por Ejemplo 4.16) cumple $\mathfrak{h}_K > 1$.

Ahora veamos una forma equivalente de definir el grupo de clases, la cual es más clásica.

DEFINICIÓN 5.15. Un *ideal fraccionario* de K es un $\mathcal{O}_K$-submódulo $\mathfrak{a}$ de K tal que existe $b \in \mathbb{Z} \setminus \{0\}$ tal que $b\mathfrak{a} \subset \mathcal{O}_K$.

Los ideales (clásicos) de $\mathcal{O}_K$, que son obviamente fraccionarios, son usualmente llamados *ideales enteros*.

EJEMPLO 5.16. El $\mathbb{Z}$-submódulo $\frac{1}{3}\mathbb{Z}$ es un ideal fraccionario de $\mathbb{Q}$.

EJERCICIO 5.17. Demostrar las siguientes afirmaciones:

(a) Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales fraccionarios, entonces $\mathfrak{a} + \mathfrak{b}$ y $\mathfrak{ab}$ también lo son.
(b) Dado $\mathfrak{a}$ ideal de $\mathcal{O}_K$, el conjunto
$$\mathfrak{a}^{-1} := \{y \in K : y\mathfrak{a} \subset \mathcal{O}_K\}$$
es un ideal fraccionario que cumple $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.
(c) El conjunto
$$G_K := \{\text{ideales fraccionarios no nulos de } K\}$$
es un grupo abeliano con el producto, mientras que
$$G_K^0 := \{\text{ideales fraccionarios no nulos principales de } K\} = \{y\mathcal{O}_K : y \in K^\times\}$$
es un subgrupo de G_K.

OBSERVACIÓN 5.18. Cualquier ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}_K$ se descompone como
$$\mathfrak{a} = \frac{\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}}{\mathfrak{q}_1^{l_1} \dots \mathfrak{q}_s^{l_s}},$$
con $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ ideales primos de $\mathcal{O}_K$ mutuamente coprimos y $k_i, l_j \in \mathbb{N}$ para todo i, j. Esto se demuestra de la siguiente manera. Existe $b \in \mathbb{Z}$ no nulo tal que $b\mathfrak{a}$ es un ideal de $\mathcal{O}_K$. Luego, el ideal entero $b\mathfrak{a}$ tendrá cierta factorización en ideales primos por Teorema 4.14, al igual que $\langle b \rangle$. Por lo tanto, simplificando ambas factorizaciones en la expresión $\mathfrak{a} = \frac{b\mathfrak{a}}{\langle b \rangle}$ obtenemos la factorización de $\mathfrak{a}$ deseada.

DEFINICIÓN 5.19. El *grupo de clases de* $\mathcal{O}_K$ se define como
$$\mathcal{H}_K := G_K / G_K^0.$$

EJERCICIO 5.20. Demostrar la equivalencia entre las dos definiciones del *grupo de clase de ideales* (Definiciones 5.13 y 5.19).

El próximo objetivo es probar que el número de clase $\mathfrak{h}_K = \#\mathcal{H}_K$ es finito.

PROPOSICIÓN 5.21. *Sea K un cuerpo de números. Existe $\lambda_K > 0$ (que depende de K) tal que todo ideal entero no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ contiene algún $\alpha \in \mathcal{O}_K$ no nulo que satisface*
$$|N_K(\alpha)| \leq \lambda_K \, N(\mathfrak{a}).$$

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de $\mathcal{O}_K$ y sean $\sigma_1, \ldots, \sigma_n$ las incrustaciones de K en $\mathbb{C}$. Veamos que

$$\lambda_K := \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$$

cumple con lo requerido en el enunciado.

Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$. Existe un único $h \in \mathbb{N}$ tal que

$$h^n \leq N(\mathfrak{a}) < (h+1)^n.$$

Como $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$, entonces necesariamente entre los $(h+1)^n$-miembros del conjunto

$$\{a_1\alpha_1 + \cdots + a_n\alpha_n : 0 \leq a_j \leq h \text{ para todo } j\}$$

existen dos (distintos) tal que su diferencia vive en $\mathfrak{a}$. Denotemos $\alpha = \sum_{j=1}^{n} c_j\alpha_j \in \mathfrak{a}$ a tal diferencia. Notar que $|c_j| \leq h$ para todo j. Concluimos que

$$|N_K(\alpha)| \leq \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |c_j||\sigma_i(\alpha_j)| \leq h^n\, \lambda_K \leq \lambda_K\, N(\mathfrak{a}),$$

tal como lo aseguramos. □

TEOREMA 5.22. *Toda clase de ideales de un cuerpo de números K contiene un ideal entero $\mathfrak{b}$ que satisface $N(\mathfrak{b}) \leq \lambda_K$, con λ_K como en Proposición 5.21. En particular, el número de clases de un cuerpo de números es finito.*

DEMOSTRACIÓN. Sea C una clase de ideales y sea $\mathfrak{a}$ un ideal entero en la case de C^{-1}. Por Proposición 5.21, existe $\alpha \in \mathfrak{a}$ tal que $|N_K(\alpha)| \leq \lambda_K N(\mathfrak{a})$.

Por otro lado, como $\langle\alpha\rangle \subset \mathfrak{a}$, esto es, $\mathfrak{a} \mid \langle\alpha\rangle$, existe un ideal entero $\mathfrak{b}$ tal que

$$\langle\alpha\rangle = \mathfrak{a}\mathfrak{b}.$$

Luego, la clase del ideal $\mathfrak{b}$, $\bar{\mathfrak{b}}$, coincide con $\bar{\mathfrak{a}}^{-1} = (C^{-1})^{-1} = C$. Además,

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\langle\alpha\rangle) = |N_K(\alpha)| \leq \lambda_K\, N(\mathfrak{a}),$$

por lo tanto $N(\mathfrak{b}) \leq \lambda_K$ con $\bar{\mathfrak{b}} \in C$.

La finitud de $\mathfrak{h}_K$ sigue de lo recién mostrado y Teorema 5.8 el cual asegura que existe una cantidad finita de ideales enteros de norma $\leq \lambda_K$. □

EJEMPLO 5.23. Tomemos $K = \mathbb{Q}(\sqrt{-5})$ como en Ejemplo 4.16. Tenemos que $\mathcal{O}_K = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$ y $\{\alpha_1 := 1, \alpha_2 := \sqrt{-5}\}$ es una base entera de $\mathcal{O}_K$. Las incrustaciones de K en $\mathbb{C}$ son $\sigma_1(\alpha) = \alpha$ y $\sigma_2(\alpha) = \bar{\alpha}$ para $\alpha \in K$, donde $\bar{\alpha}$ denota la conjugación compleja. Luego, el número λ_K definido en Proposición 5.21 es

$$\lambda_K = \prod_{i=1}^{2} \sum_{j=1}^{2} |\sigma_i(\alpha_j)| = \left(|1| + |\sqrt{-5}|\right)\left(|1| + |-\sqrt{-5}|\right) = (1+\sqrt{5})^2 \approx 10{,}47.$$

Primero buscamos los ideales primos con norma menor a λ_K para luego aplicar Teorema 5.22. Éstos necesariamente deberán participar en la factorización de $\langle 2\rangle$, $\langle 3\rangle$, $\langle 5\rangle$, o $\langle 7\rangle$.

Definimos

$$\mathfrak{p}_0 = \langle 2, 1+\sqrt{-5}\rangle, \qquad \mathfrak{p}_2 = \langle 3, 1-\sqrt{-5}\rangle, \qquad \mathfrak{p}_4 = \langle 7, 3+\sqrt{-5}\rangle,$$
$$\mathfrak{p}_1 = \langle 3, 1+\sqrt{-5}\rangle, \qquad \mathfrak{p}_3 = \langle \sqrt{-5}\rangle, \qquad \mathfrak{p}_5 = \langle 7, 3-\sqrt{-5}\rangle.$$

En Ejemplo 4.16 vimos que

$$\langle 2\rangle = \mathfrak{p}_0^2, \qquad \langle 3\rangle = \mathfrak{p}_1\mathfrak{p}_2.$$

De manera muy similar se descomponen $\langle 5\rangle$ y $\langle 7\rangle$.

EJERCICIO 5.24. Probar que

$$\langle 5\rangle = \mathfrak{p}_3^2, \qquad \langle 7\rangle = \mathfrak{p}_4\mathfrak{p}_5.$$

Por las descomposiciones de arriba, claramente $N(\mathfrak{p}_i) = p_i$ donde p_i es el único primo racional positivo que vive en $\mathfrak{p}_i$. Más precisamente,

$$N(\mathfrak{p}_0) = 2, \qquad N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 3,$$
$$N(\mathfrak{p}_3) = 5, \qquad N(\mathfrak{p}_4) = N(\mathfrak{p}_5) = 7.$$

En particular, el ideal $\mathfrak{p}_i$ es primo para todo i por Proposición 5.7. Luego, es fácil chequear que todos los ideales enteros de norma ≤ 10 son:

$N(\mathfrak{a})$	2	3	4	5	6	7	8	9	10
$\mathfrak{a}$	$\mathfrak{p}_0$	$\mathfrak{p}_1, \mathfrak{p}_2$	$\mathfrak{p}_0^2$	$\mathfrak{p}_3$	$\mathfrak{p}_0\mathfrak{p}_1, \mathfrak{p}_0\mathfrak{p}_2$	$\mathfrak{p}_4, \mathfrak{p}_5$	$\mathfrak{p}_0^3$	$\mathfrak{p}_1^2, \mathfrak{p}_2^2, \mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_0\mathfrak{p}_3$

Con toda esta información, determinemos el grupo de clases $\mathcal{H}_K$. El ideal $\mathfrak{p}_0$ no es principal, por lo tanto su clase $\bar{\mathfrak{p}}_0$ es distinta al elemento neutro $e := \overline{\langle 1\rangle} = \overline{\mathcal{O}_K}$. Veamos que

$$\mathcal{H}_K = \{e, \bar{\mathfrak{p}}_0\},$$

es decir, $\mathfrak{h}_K = 2$ y todo ideal fraccionario no principal debe ser equivalente a $\mathfrak{p}_0$. Esto sigue de mostrar que los ideales enteros no principales listados en la tabla de arriba son equivalentes a $\mathfrak{p}_0$. Los cálculos de los productos de los ideales de abajo son dejados al lector.

- $\mathfrak{p}_0\mathfrak{p}_1 = \langle 1 + \sqrt{-5}\rangle$ implica que $\bar{\mathfrak{p}}_1 = (\bar{\mathfrak{p}}_0)^{-1}$ y $\overline{\mathfrak{p}_0\mathfrak{p}_1} = e$.
- $\mathfrak{p}_0\mathfrak{p}_2 = \langle 1 - \sqrt{-5}\rangle$ implica que $\bar{\mathfrak{p}}_2 = (\bar{\mathfrak{p}}_0)^{-1}$ y $\overline{\mathfrak{p}_0\mathfrak{p}_2} = e$.
- $\mathfrak{p}_0^2 = \langle 2\rangle$ implica que $\bar{\mathfrak{p}}_0 = (\bar{\mathfrak{p}}_0)^{-1}$.
- $\mathfrak{p}_3 = \langle\sqrt{-5}\rangle$ implica que $\bar{\mathfrak{p}}_3 = e$.
- $\mathfrak{p}_0^3 = \langle 2\rangle\mathfrak{p}_0$ implica que $\overline{\mathfrak{p}_0^3} = \bar{\mathfrak{p}}_0$.
- $\overline{\mathfrak{p}_0^3} = \bar{\mathfrak{p}}_0\overline{\mathfrak{p}_0^2} = \bar{\mathfrak{p}}_0 e = \bar{\mathfrak{p}}_0$.
- $\overline{\mathfrak{p}_1^2} = (\bar{\mathfrak{p}}_1)^2 = (\bar{\mathfrak{p}}_0)^2 = e$.
- $\overline{\mathfrak{p}_2^2} = (\bar{\mathfrak{p}}_2)^2 = (\bar{\mathfrak{p}}_0)^2 = e$.
- $\mathfrak{p}_1\mathfrak{p}_2 = \langle 3\rangle$ implica que $\overline{\mathfrak{p}_1\mathfrak{p}_2} = e$.
- $\overline{\mathfrak{p}_0\mathfrak{p}_3} = \bar{\mathfrak{p}}_0 e = \bar{\mathfrak{p}}_0$.

EJERCICIO 5.25. Probar las descomposiciones listadas arriba.

Restan considerar $\mathfrak{p}_0\mathfrak{p}_4$ y $\mathfrak{p}_0\mathfrak{p}_5$.

AFIRMACIÓN. $\mathfrak{p}_0\mathfrak{p}_4 = \langle 3 + \sqrt{-5}\rangle$ *y* $\mathfrak{p}_0\mathfrak{p}_5 = \langle 3 - \sqrt{-5}\rangle$.

DEMOSTRACIÓN. Vale la pena comenzar con el siguiente intento fallido:

$$\mathfrak{p}_0\mathfrak{p}_4 = \langle 2, 1 + \sqrt{-5}\rangle\langle 7, 3 + \sqrt{-5}\rangle = \langle 14, 2(3 + \sqrt{-5}), 7(1 + \sqrt{-5}), -2 + 4\sqrt{-5}\rangle.$$

Notar que no es claro cómo seguir.

Ahora sí veamos la demostración correcta. Como $\langle 3+\sqrt{-5}\rangle \subset \mathfrak{p}_4$, existe un ideal entero $\mathfrak{b}$ tal que $\langle 3+\sqrt{-5}\rangle = \mathfrak{p}_4\mathfrak{b}$. Como

$$N(\mathfrak{b}) = \frac{N(\langle 3+\sqrt{-5}\rangle)}{N(\mathfrak{p}_4)} = \frac{|N_K(3+\sqrt{-5})|}{7} = \frac{14}{7} = 2,$$

tenemos que $\mathfrak{b} = \mathfrak{p}_0$.

El otro caso es totalmente análogo. ■

La afirmación anterior nos asegura que $\bar{\mathfrak{p}}_4 = (\bar{\mathfrak{p}}_0)^{-1} = \bar{\mathfrak{p}}_0$ y $\bar{\mathfrak{p}}_5 = (\bar{\mathfrak{p}}_0)^{-1} = \bar{\mathfrak{p}}_0$, por lo que concluimos el análisis requerido para asegurar que $\mathcal{H}_K = \{e, \bar{\mathfrak{p}}_0\}$. Luego, $\mathfrak{h}_K = 2$ y $\mathcal{H}_K \simeq \mathbb{Z}/2\mathbb{Z}$.

COMENTARIO 5.26. Gauss conjeturó que

$$\lim_{m\to-\infty} \mathfrak{h}_{\mathbb{Q}(\sqrt{m})} = +\infty,$$

lo cual fue demostrado por Hebronn en 1934. En particular, esto nos dice que dado $h \in N$ existe sólo una cantidad finita de cuerpos cuadráticos imaginarios con número de clase igual a h.

El listado de los cuerpos cuadráticos imaginarios que son dominios de factorización única (i.e. el número de clase es 1) es

$$\mathbb{Q}(\sqrt{m}) \quad \text{con } m \in \{-1,-3,-7,-2,-11,-19,-43,-67,-163\}.$$

Los cuerpos cuadráticos imaginarios con número de clase igual a 2 fueron obtenidos en la década del 70.

El problema del número de clase de Gauss dice:

> *Encontrar un algoritmo efectivo para determinar todos los cuerpos cuadráticos imaginarios con número de clase dado.*

Éste fue resuelto por Dorian Goldfeld usando curvas elípticas. Junto a Gross y Zagier probaron que para todo $\epsilon > 0$ existe $c > 0$ tal que

$$\mathfrak{h}_K > c\,(\log|\operatorname{disc}(K)|)^{1-\epsilon},$$

donde K es cualquier cuerpo cuadrático imaginario. Este resultado resuelve (salvo una cantidad finita de cálculos) el problema de Gauss.

De manera anterior al año 2004, sólo se habían clasificados los cuerpos cuadráticos imaginarios con número de clase $h \leq 7$. En 2004, con siete meses de cálculos computacionales, la clasificación se extendió hasta $h \leq 100$. Por ejemplo, la cantidad de cuerpos cuadráticos imaginarios con número de clase igual a 100 es 1736, mientras que el máximo discriminante alcanzado por ellos es igual a 1.856.563.

La siguiente pregunta está abierta:

> *¿Existen infinitos cuerpos cuadráticos reales con número de clase igual a uno?*

Problemas.

5.2. Sean R un dominio de Dedekind, F el cuerpo de fracciones de R, y $\mathfrak{a}$ un ideal entero de R.

(a) Definir ideales fraccionarios en F de manera análoga a Definición 5.15.
(b) Probar que $\mathfrak{a}^{-1} := \{y \in F : y\mathfrak{a} \subseteq R\}$ es un ideal fraccionario de F y $\mathfrak{a}\mathfrak{a}^{-1} = R$.
(c) Probar que todo ideal principal fraccionario de F es de la forma yR con $y \in F^\times$.

5.3. Sea $K=\mathbb{Q}(\sqrt{-5})$. Encontrar $\alpha,\beta\in\mathcal{O}_K$ tales que

$$\langle\alpha\rangle\langle 2,1-\sqrt{-5}\rangle=\langle\beta\rangle\langle 3,1+\sqrt{-5}\rangle.$$

3. Descomposición de $\langle p\rangle$ en un anillo de enteros cuadrático

Se puede apreciar en Ejemplo 5.23 la importancia de poseer la descomposición de los ideales de la forma $\langle p\rangle$ para calcular el número de clase. Esta sección resuelve completamente este problema en el caso de extensiones cuadráticas. En este caso seguiremos [**Narasimhan et al**, §III.1].

Sea K un cuerpo de números arbitrario de orden $[K:\mathbb{Q}]=n$. Sea $p\in\mathbb{Z}$ primo positivo. Por la descomposición única de ideales como producto de ideales primos (Teorema 4.14), se tiene que existen $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ ideales primos coprimos entre sí (i.e. $\mathcal{O}_K=\operatorname{mcd}(\mathfrak{p}_i,\mathfrak{p}_j)=\mathfrak{p}_i+\mathfrak{p}_j$ para todo $i\neq j$), y $k_1,\dots,k_r\in\mathbb{N}$ tales que

$$\langle p\rangle=p\mathcal{O}_K=\mathfrak{p}_1^{k_1}\dots\mathfrak{p}_r^{k_r}.$$

Como

$$p^n=|N_K(p)|=N(\langle p\rangle)=N(\mathfrak{p}_1)^{k_1}\dots N(\mathfrak{p}_r)^{k_r},$$

se tiene que $N(\mathfrak{p}_i)=p^{c_i}$ para algún $c_i\in\mathbb{N}$ con $c_1k_1+\dots+c_nk_n=n$.

Definición 5.27. Bajo la notación anterior, se dice que

- p *ramifica en* K si $c_i>1$ para algún i.
- p *se parte en* K si $c_i=1$ para todo i.

A partir de ahora asumimos que K es un cuerpo cuadrático (i.e. $n=2$). Como ya mencionamos en el párrafo anterior a Proposición 3.8, todo cuerpo cuadrático es de la forma $\mathbb{Q}(\sqrt{m})$ con $m\in\mathbb{Z}$ libre de cuadrados. En este caso, la ecuación de arriba $c_1k_1+\dots+c_rk_r=n=2$ fuerza a que $r\leq 2$ y $c_1,c_2\in\{0,1,2\}$. Esto es, dado p primo racional positivo, tenemos las siguientes posibilidades:

$$\langle p\rangle=\begin{cases}\mathfrak{p}_1\mathfrak{p}_2 \quad \text{con } \mathfrak{p}_1\neq\mathfrak{p}_2 & (p \textit{ se parte en } K),\\ \mathfrak{p}_1 & (p \textit{ permanece primo en } K),\\ \mathfrak{p}_1^2 & (p \textit{ ramifica en } K).\end{cases}$$

Ejemplo 5.28. Consideremos nuestro cuerpo cuadrático favorito, $K=\mathbb{Q}(\sqrt{-5})$. En Ejemplo 5.23 vimos que

- 2 y 5 ramifican en K pues $\langle 2\rangle=\langle 2,1+\sqrt{-5}\rangle^2$ y $\langle 5\rangle=\langle\sqrt{-5}\rangle^2$;
- 3 y 7 se parten en K pues $\langle 3\rangle=\langle 3,1+\sqrt{-5}\rangle\langle 3,1-\sqrt{-5}\rangle$ y $\langle 7\rangle=\langle 7,3+\sqrt{-5}\rangle\langle 7,3-\sqrt{-5}\rangle$.

Veamos además que 13 permanece primo en K. Sea $\mathfrak{p}$ ideal maximal de $\mathcal{O}_K$ tal que $\langle 13\rangle\subset\mathfrak{p}$. Queremos mostrar que $\mathfrak{p}=\langle 13\rangle$. Supongamos que esto no es cierto. Como $N(\mathfrak{p})$ divide a $N(\langle 13\rangle)=|N_K(13)|=13^2$, tenemos que $N(\mathfrak{p})=13$ pues $\mathfrak{p}\neq\langle 13\rangle$. Sea $\alpha\in\mathfrak{p}\smallsetminus\langle 13\rangle$. Escribimos $\alpha=a+b\sqrt{-5}$ con $a,b\in\mathbb{Z}$, y podemos asumir que $13\nmid\operatorname{mcd}(a,b)$. Como $\mathfrak{p}\mid\langle\alpha\rangle$, $13=N(\mathfrak{p})$ divide a $N(\langle\alpha\rangle)=|N_K(\alpha)|=a^2+5b^2$. Veamos que esto es imposible.

Tenemos que 13 divide a a^2+5b^2, esto es $a^2\equiv -5b^2 \pmod{13}$, lo que implica que

$$(2a)^2\equiv -20b^2\equiv 6b^2 \pmod{13}.$$

Como 13 no divide a b (si lo hiciera, entonces 13 también dividiría a a, por lo tanto tendríamos que $13 \mid \mathrm{mcd}(a,b) = 1$), multiplicamos a ambos lados por el cuadrado del inverso de b módulo 13, i.e. por c^2 con $c \in \mathbb{Z}$ tal que $bc \equiv 1 \pmod{13}$, obteniendo que

$$(2ac)^2 \equiv 6 \pmod{13}.$$

En otras palabras, 6 es un cuadrado en $\mathbb{Z}/13\mathbb{Z}$. Se puede verificar fácilmente que esto no es cierto.

Recordemos que en Ejemplo 3.36 mostramos que el discriminante de $K = \mathbb{Q}(\sqrt{m})$ está dado por

$$d_K := \mathrm{disc}(K) = \begin{cases} 4m & \text{si } m \equiv 2,3 \pmod 4, \\ m & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Observación 5.29. Veamos que

$$\left\{1, \frac{d_K + \sqrt{d_K}}{2}\right\}$$

es base entera de $\mathcal{O}_K$. Tenemos que

$$\frac{d_K + \sqrt{d_K}}{2} = \begin{cases} \frac{4m+\sqrt{4m}}{2} = 2m + \sqrt{m} & \text{si } m \equiv 2,3 \pmod 4, \\ \frac{m+\sqrt{m}}{2} = \frac{m-1}{2} + \frac{1+\sqrt{m}}{2} & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Se sigue que todo elemento en

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \sqrt{m}\mathbb{Z} & \text{si } m \equiv 2,3 \pmod 4, \\ \mathbb{Z} + \frac{1+\sqrt{m}}{2}\mathbb{Z} & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

puede escribirse como combinación lineal de entera de 1 y $\frac{d_K+\sqrt{d_K}}{2}$.

Definición 5.30. El *símbolo de Legendre* para $p \in \mathbb{Z}$ primo impar y $a \in \mathbb{Z}$ se define por

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod p \text{ tiene solución en } \mathbb{Z}, \\ -1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod p \text{ no tiene solución en } \mathbb{Z}, \\ 0 & \text{si } p \mid a. \end{cases}$$

Ejercicio 5.31. Mostrar las siguientes identidades para $a, b \in \mathbb{Z}$ y p primo impar:

(a) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ si $a \equiv b \pmod p$;

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

(c) $\left(\frac{a^2}{p}\right) = \begin{cases} 1 & \text{si } p \nmid a, \\ 0 & \text{si } p \mid a; \end{cases}$

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

Además de las identidades simples del ejercicio anterior, usaremos la famosa *ley de reciprocidad cuadrática*:

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

para p y q primos impares.

TEOREMA 5.32. *Sean p un primo racional impar y $K=\mathbb{Q}(\sqrt{m})$ un cuerpo cuadrático con discriminante d_K. Entonces se tienen las siguientes equivalencias.*

(i) $\langle p\rangle=\mathfrak{p}^2$ *si y sólo si* $\left(\dfrac{d_K}{p}\right)=0$.

(ii) $\langle p\rangle=\mathfrak{p}\mathfrak{p}'$ *con* $\mathfrak{p}\neq\mathfrak{p}'$ *si y sólo si* $\left(\dfrac{d_K}{p}\right)=+1$.

(iii) $\langle p\rangle=\mathfrak{p}$ *si y sólo si* $\left(\dfrac{d_K}{p}\right)=-1$.

DEMOSTRACIÓN. Comencemos suponiendo que $\langle p\rangle=\mathfrak{p}^2$. Como $\mathfrak{p}\neq\langle p\rangle$, existe $\pi=a+b\frac{d_K+\sqrt{d_K}}{2}\in\mathfrak{p}\smallsetminus\langle p\rangle$ con $a,b\in\mathbb{Z}$. Sin embargo,

$$\begin{aligned}\pi^2 &= \left(\frac{2a+bd_K}{2}+\frac{b}{2}\sqrt{d_K}\right)^2\\ &= \tfrac{1}{4}\Big((2a+bd_K)^2+d_Kb^2\Big)+\tfrac{1}{2}(2a+bd_K)b\sqrt{d_K}\in\langle p\rangle\end{aligned}$$

por lo tanto p divide (en $\mathbb{Z}$) a $(2a+bd_K)^2+d_Kb^2$ y a $(2a+bd_K)b$. Si $p\mid b$ entonces $p\mid a$ y en consecuencia p divide a π en $\mathcal{O}_K$, lo cual contradice la hipótesis. Esto implica que $p\mid 2a+bd_K$ y $p\nmid b$, sumado a que $p\mid(2a+bd_K)^2+d_Kb^2$, resulta $p\mid d_K$, es decir, $\left(\frac{d_K}{p}\right)=0$.

Ahora supongamos que $p\mid d_K$. Consideremos $\mathfrak{p}=\langle p,\sqrt{d_K}\rangle$. Se tiene que

$$\mathfrak{p}^2=\langle p^2,p\sqrt{d_K},d_K\rangle=\langle p\rangle.$$

En efecto, $p^2\nmid d_K$, por lo tanto $\operatorname{mcd}(d_K,p^2)=p$, lo que asegura que p puede escribirse como combinación lineal entera de d_K y p^2. Luego, $N(\mathfrak{p})=p$, y por lo tanto $\mathfrak{p}$ es primo por Proposición 5.7.

Supongamos que $\left(\frac{d_K}{p}\right)=1$, es decir, existe $a\in\mathbb{Z}$ tal que $a^2\equiv d_K\pmod p$. Tomemos $\mathfrak{p}=\langle p,a+\sqrt{d_K}\rangle$ y $\mathfrak{p}'=\langle p,a-\sqrt{d_K}\rangle$. Se verifica que

$$\mathfrak{p}\mathfrak{p}'=\langle p^2,p(a+\sqrt{d_K}),p(a-\sqrt{d_K}),a^2-d_K\rangle=\langle p\rangle, \tag{1}$$

lo que a su vez implica que $\mathfrak{p}$ y $\mathfrak{p}'$ son ideales primos como en el caso anterior. Además $\mathfrak{p}\neq\mathfrak{p}'$ pues $\mathfrak{p}+\mathfrak{p}'=\mathcal{O}_K$.

Recíprocamente, si $\langle p\rangle=\mathfrak{p}\mathfrak{p}'$ con $\mathfrak{p}\neq\mathfrak{p}'$, entonces $N(\mathfrak{p})=N(\mathfrak{p}')=p$. Tomemos $\alpha=a+b\frac{d_K+\sqrt{d_K}}{2}\in\mathfrak{p}\smallsetminus\langle p\rangle$ donde $a,b\in\mathbb{Z}$ satisfacen que $p\nmid\operatorname{mcd}(a,b)$. Como $\langle\alpha\rangle\subset\mathfrak{p}$ se tiene $\mathfrak{p}\mid\langle\alpha\rangle$, por lo tanto $p=N(\mathfrak{p})$ divide a

$$N(\langle\alpha\rangle)=|N_K(\alpha)|=\left|N\Big(\Big(\tfrac{2a+bd_K}{2}+\tfrac{b}{2}\sqrt{d_K}\Big)\Big)\right|=\tfrac{1}{4}\left|(2a+bd_K)^2-b^2d_K\right|,$$

en particular $(2a+bd_K)^2\equiv b^2d_K\pmod p$. Si $p\mid b$ entonces $p\mid a$ lo cual contradice la hipótesis. Luego $p\nmid b$, entonces existe $c\in\mathbb{Z}$ tal que $bc\equiv 1\pmod p$ (i. e. c es el inverso de b módulo p), por lo tanto $x^2\equiv d_K\pmod p$ tiene solución $x=(2a+bd_K)c$.

El último caso es inmediato a partir de los dos ítems anteriores. □

DEFINICIÓN 5.33. El *símbolo de Kronecker* para $d\in\mathbb{Z}$ con $d\equiv 0,1\pmod 4$ se define por

$$\left(\frac{d}{2}\right)=\begin{cases}+1 & \text{si } d\equiv 1 \pmod 8,\\ -1 & \text{si } d\equiv 5 \pmod 8,\\ 0 & \text{si } d\equiv 0 \pmod 4.\end{cases}$$

TEOREMA 5.34. *Sea $K = \mathbb{Q}(\sqrt{m})$ un cuerpo cuadrático con discriminante d_K. Entonces se tienen las siguientes equivalencias.*

(i) $\langle 2\rangle = \mathfrak{p}^2$ *si y sólo si* $\left(\dfrac{d_K}{2}\right) = 0$.

(ii) $\langle 2\rangle = \mathfrak{p}\mathfrak{p}'$ *con* $\mathfrak{p} \neq \mathfrak{p}'$ *si y sólo si* $\left(\dfrac{d_K}{2}\right) = +1$.

(iii) $\langle 2\rangle = \mathfrak{p}$ *si y sólo si* $\left(\dfrac{d_K}{2}\right) = -1$.

EJERCICIO 5.35. Demostrar Teorema 5.34.

Problemas.

5.4. Calcular el número de clases $\mathfrak{h}_K$ para los siguientes cuerpos de números.
(a) $K = \mathbb{Q}(\sqrt{-1})$ (no usar el hecho que $\mathcal{O}_K$ es un dominio Euclídeo).
(b) $K = \mathbb{Q}(\sqrt{2})$.
(c) $K = \mathbb{Q}(\sqrt{-3})$.

5.5. Elegir un cuerpo cúbico K y descomponer el ideal $\langle p\rangle$ para tres primos racionales distintos.

4. Cota de Minkowski

En esta sección mejoraremos la cota λ_K dada en Proposición 5.21, lo cual facilitará el cálculo de $\mathfrak{h}_K$.

Sea K un cuerpo de números. Una incrustación $\sigma : K \to \mathbb{C}$ se dice *real* si $\sigma(K) \subset \mathbb{R}$, y *compleja* en caso contrario. Recordar que $\bar{\sigma}$ también es una incrustación, donde $\bar{\cdot}$ denota la conjugación compleja. Luego, σ es real si y sólo si $\sigma = \bar{\sigma}$.

EJEMPLO 5.36. Tomemos el cuerpo de números $\mathbb{Q}(\sqrt[3]{2})$, y sea $\omega = e^{2\pi \mathrm{i}/3}$. Una incrustación $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ está determinada por $\sigma(\sqrt[3]{2})$, el cual debe estar en $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ por ser raíz de $x^3 - 2$. Concluimos que la incrustación σ determinada por $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ es real, mientras que las otras dos son complejas conjugadas.

Denotemos $\sigma_1, \ldots, \sigma_r$ todas las incrustaciones reales de K y $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s$ las incrustaciones complejas de K. Notar que $n = [K : \mathbb{Q}] = r + 2s$. Sea $\Phi : K \to \mathbb{R}^n$ dada por

$$\Phi(\alpha) = \big(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \ldots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha))\big).$$

Claramente $\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta)$ y $\mathrm{Nu}(\Phi) = \{0\}$.

TEOREMA 5.37. *Sea K un cuerpo de números. El conjunto $\Lambda_{\mathcal{O}_K} := \Phi(\mathcal{O}_K)$ es un retículo en $\mathbb{R}^n$ de covolumen*

$$\mathrm{vol}(\mathbb{R}^n/\Lambda_{\mathcal{O}_K}) = \frac{\sqrt{|\operatorname{disc}(K)|}}{2^s}.$$

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de $\mathcal{O}_K$. Como $\mathcal{O}_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$, se tiene que

$$\Lambda_{\mathcal{O}_K} = \Phi(\mathcal{O}_K) = \bigoplus_{i=1}^{n} \Phi(\alpha_i)\mathbb{Z}.$$

Demostremos que $\Lambda_{\mathcal{O}_K}$ es un retículo en $\mathbb{R}^n$, mostrando que $\{\Phi(\alpha_1),\dots,\Phi(\alpha_n)\}$ es una $\mathbb{R}$-base de $\mathbb{R}^n$.

Sea M la matriz $n\times n$ con i-ésima fila $\Phi(\alpha_i)^t$, esto es,

$$M=\begin{pmatrix}\Phi(\alpha_1)^t\\ \vdots\\ \Phi(\alpha_n)^t\end{pmatrix}\in\mathbb{R}^{n\times n}.$$

Teniendo en cuenta que

$$\begin{pmatrix}a_1+\mathrm{i}b_1 & a_1-\mathrm{i}b_1\\ \vdots & \vdots\\ a_n+\mathrm{i}b_n & a_n-\mathrm{i}b_n\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}2a_1 & -2\mathrm{i}b_1\\ \vdots & \vdots\\ 2a_n & -2\mathrm{i}b_n\end{pmatrix}$$

para $a_1,b_1,\dots,a_n,b_n\in\mathbb{R}$, obtenemos que

$$\begin{aligned}\det(M)&=\frac{1}{(-2\mathrm{i})^s}\ \det\begin{pmatrix}\sigma_1(\alpha_1) & \dots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1(\alpha_1)} & \dots & \tau_s(\alpha_1) & \overline{\tau_s(\alpha_1)}\\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ \sigma_1(\alpha_n) & \dots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1(\alpha_n)} & \dots & \tau_s(\alpha_n) & \overline{\tau_s(\alpha_n)}\end{pmatrix}\\ &=\frac{1}{(-2\mathrm{i})^s}\ \sqrt{\operatorname{disc}(K)}\neq 0.\end{aligned}$$

Esto nos asegura que $\{\Phi(\alpha_1),\dots,\Phi(\alpha_n)\}$ es una base de $\mathbb{R}^n$. Más aún, se tiene que $\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathcal{O}_K})=|\det(M)|$. □

Corolario 5.38. *El conjunto $\Phi(K)$ es denso en $\mathbb{R}^n$.*

Demostración. Sea $\{\alpha_1,\dots,\alpha_n\}$ una base entera de $\mathcal{O}_K$. Se tiene que $K=\bigoplus_{j=1}^{n}\alpha_i\mathbb{Q}$, por lo tanto

$$\overline{\Phi(K)}=\overline{\bigoplus_{j=1}^{n}\Phi(\alpha_i)\mathbb{Q}}=\mathbb{R}^n,$$

pues $\{\Phi(\alpha_1),\dots,\Phi(\alpha_n)\}$ es linealmente independiente. □

Es sabido que si $\Lambda_2\subset\Lambda_1$ son retículos completos en $\mathbb{R}^n$ (i.e. tienen rango n), entonces

$$\operatorname{vol}(\mathbb{R}^n/\Lambda_2)=\operatorname{vol}(\mathbb{R}^n/\Lambda_1)\ \#(\Lambda_1/\Lambda_2),$$

con Λ_1/Λ_2 un grupo abeliano finito. Luego, para $\mathfrak{a}$ un ideal entero en K, $\Lambda_{\mathfrak{a}}:=\Phi(\mathfrak{a})\subset\Lambda_{\mathcal{O}_K}$, y por lo tanto

$$\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathfrak{a}})=\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathcal{O}_K})\ \#(\mathcal{O}_K/\mathfrak{a})=\frac{\sqrt{|\operatorname{disc}(K)|}}{2^s}\ N(\mathfrak{a}).$$

Ahora definamos una *norma* especial en $\mathbb{R}^n$. Sea $\mathcal{N}:\mathbb{R}^n\longrightarrow\mathbb{R}$ dada por

$$\mathcal{N}(x_1,\dots,x_n)=x_1\dots x_r(x_{r+1}^2+x_{r+2}^2)\dots(x_{n-1}^2+x_n^2).$$

Luego,

$$\mathcal{N}(\Phi(\alpha))=N_K(\alpha)$$

para todo $\alpha\in\mathcal{O}_K$.

TEOREMA 5.39. *Todo retículo Λ de $\mathbb{R}^n$ contiene $x \neq 0$ tal que*

$$|\mathcal{N}(x)| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Antes de demostrar este teorema veamos algunas consecuencias.

COROLARIO 5.40. *Sea K un cuerpo de números con r incrustaciones reales y s complejas de orden $n = r + 2s$. Dado $\mathfrak{a}$ ideal entero no nulo de K, existe $\alpha \in \mathfrak{a}$ con $\alpha \neq 0$ tal que*

$$|N_K(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}\, N(\mathfrak{a}).$$

COROLARIO 5.41. *Bajo las mismas hipótesis del corolario anterior, toda clase de ideales en el grupo de clases $\mathcal{H}_K$ de K contiene un ideal entero $\mathfrak{a}$ tal que*

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}.$$

La demostración de este último corolario es idéntica a la de Teorema 5.22. El siguiente ejemplo muestra que la cantidad de cálculos requeridos usando Corolario 5.41 en lugar de Teorema 5.22 es significativamente menor.

EJEMPLO 5.42. En Ejemplo 5.23 habíamos considerado $K = \mathbb{Q}(\sqrt{-5})$ y chequeado todos los ideales enteros de norma menor o igual a $\lambda_K \approx 10{,}47$. Corolario 5.41 nos asegura que es suficiente chequear los ideales de norma menor o igual a

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{20} \approx 2{,}84.$$

Luego, era suficiente considerar únicamente $\mathfrak{p}_1 = \langle 2, 1\sqrt{-5}\rangle$.

OBSERVACIÓN 5.43. Notar que para cualquier ideal entero $\mathfrak{a}$ de un cuerpo de números $K \neq \mathbb{Q}$, se tiene que

$$1 \leq N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|} < \sqrt{|\operatorname{disc}(K)|}$$

pues $\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s > 1$ si $n \geq 2$. Concluimos que $|\operatorname{disc}(K)| > 1$ para todo cuerpo de números K distinto a $\mathbb{Q}$.

El resto de la sección está destinada a demostrar Teorema 5.39, en el cual no está involucrado ningún cuerpo de números. Se asumirá algunos pocos conocimientos de retículos Euclídeos. El lector puede consultar las notas [**Rossetti**].

LEMA 5.44 (de Minkowski). *Sea Λ un retículo en $\mathbb{R}^n$ y sea E un subconjunto de $\mathbb{R}^n$ convexo, medible y simétrico (i.e. $x \in \Lambda \iff -x \in \Lambda$) tal que*

$$\operatorname{vol}(E) > 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Entonces E contiene un punto no nulo de Λ. Además, si E es compacto, el símbolo $>$ en la hipótesis de arriba se puede reemplazar por $\geq$.

DEMOSTRACIÓN. Sea $\{v_1, \ldots, v_n\}$ una $\mathbb{Z}$-base de Λ, y

$$F := \left\{ \sum_{i=1}^{n} t_i v_i : 0 \leq t_i < 1 \text{ para todo } i \right\}.$$

Claramente F es un *dominio fundamental de* $\mathbb{R}^n/\Lambda$, es decir,

$$\mathbb{R}^n = \bigcup_{y\in\Lambda}(y+F)$$

y la unión es disjunta. Denotemos $tE = \{ty : y \in E\}$ para cualquier $t > 0$. Por hipótesis, tenemos que

$$\begin{aligned}\operatorname{vol}(F) = \operatorname{vol}(\mathbb{R}^n/\Lambda) < \frac{\operatorname{vol}(E)}{2^n} = \operatorname{vol}(\tfrac{1}{2}E) &= \sum_{x\in\Lambda}\operatorname{vol}\big((\tfrac{1}{2}E)\cap(x+F)\big)\\ &= \sum_{x\in\Lambda}\operatorname{vol}\big((\tfrac{1}{2}E-x)\cap F\big).\end{aligned}$$

Concluimos que los subconjuntos $(\frac{1}{2}E-x)\cap F$ de F no pueden ser mutuamente disjuntos.

Sean $x, y \in \Lambda$ distintos tales que

$$(\tfrac{1}{2}E-x)\cap(\tfrac{1}{2}E-y)\neq\emptyset.$$

Esto nos dice que existen $v, w \in E$ tales que $\frac{v}{2}-x = \frac{w}{2}-y$, lo cual implica que

$$x-y = \frac{v-w}{2} \in E\cap\Lambda$$

pues $-w \in E$ por ser E simétrico, y $\frac{v+(-w)}{2} \in E$ por ser E convexo. Esto completa la demostración de la primera afirmación.

Ahora supongamos que E es compacto y $\operatorname{vol}(E) = 2^n \operatorname{vol}(F)$. Por la primera afirmación ya probada, se tiene que

$$\operatorname{vol}\big((1+\tfrac{1}{m})E\big) > 2^n \operatorname{vol}(F)$$

para cada $m \in \mathbb{N}$. Luego, para cada $m \in \mathbb{N}$ existe $x_m \in \Lambda\cap(1+\frac{1}{m})E$ no nulo. Notemos que $\Lambda\cap 2E$ es un conjunto finito pues Λ es discreto y $2E$ es compacto. Como $x_m \in \Lambda\cap 2E$, existe $x \in \Lambda\cap 2E$ tal que $x = x_m$ para una cantidad infinita de $m \in \mathbb{N}$, digamos para la subsucesión x_{m_j} con $j \in \mathbb{N}$. Todo esto nos dice que el elemento no nulo x cumple

$$x = \lim_{j\to\infty} x_{m_j} \in \bar{E}\cap\Lambda = E\cap\Lambda,$$

que es exactamente lo que queríamos probar. □

Corolario 5.45. *Sea A un subconjunto de $\mathbb{R}^n$ compacto, convexo, simétrico tal que $\operatorname{vol}(A) > 0$ y con la propiedad $|\mathcal{N}(a)| \leq 1$ para todo $a \in A$. Entonces, dado Λ un retículo de $\mathbb{R}^n$, existe $x \in \Lambda\smallsetminus\{0\}$ tal que*

$$|\mathcal{N}(x)| \leq \frac{2^n}{\operatorname{vol}(A)}\operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Demostración. Sea $t > 0$ determinado por

$$t^n = \frac{2^n}{\operatorname{vol}(A)}\operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Tomando $E = tA$, el cual es compacto, convexo, medible y cumple que

$$\operatorname{vol}(E) = t^n \operatorname{vol}(A) = 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda),$$

Lema 5.44 implica que existe $x \in \Lambda \cap E$ no nulo. Concluimos que x es el elemento requerido pues

$$\mathcal{N}(x) = \mathcal{N}(t(t^{-1}x)) = t^n \mathcal{N}(t^{-1}x) \leq t^n = \frac{2^n}{\mathrm{vol}(A)} \mathrm{vol}(\mathbb{R}^n/\Lambda),$$

lo cual completa la prueba. □

Demostración de Teorema 5.39. Definimos

$$A = \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{r} |x_i| + 2 \sum_{j=1}^{s} \sqrt{x_{r+2j-1}^2 + x_{r+2j}^2} \leq n \right\}.$$

Claramente, A es compacto, simétrico, convexo (¡convencerse! o ver [**Marcus**, Exercise 4, Ch. 5]), y de volumen positivo.

Veamos que A cumple la propiedad restante en las hipótesis de Corolario 5.45. Sea $a = (a_1, \ldots, a_n) \in A$. Se tiene que

$$\begin{aligned} |\mathcal{N}(a)| &= |a_1| \ldots |a_r| \, (a_{r+1}^2 + a_{r+2}^2) \ldots (a_{n-1}^2 + a_n^2) \\ &= |a_1| \ldots |a_r| \sqrt{a_{r+1}^2 + a_{r+2}^2} \sqrt{a_{r+1}^2 + a_{r+2}^2} \cdots \sqrt{a_{n-1}^2 + a_n^2} \sqrt{a_{n-1}^2 + a_n^2}. \end{aligned}$$

La clásica desigualdad entre la media geométrica y la media aritmética

$$(\text{i.e.} \quad (y_1 \ldots y_m)^{1/m} \leq \frac{y_1 + \cdots + y_m}{m} \quad \text{para todo } y_1, \ldots, y_m > 0)$$

nos asegura que

$$|\mathcal{N}(a)|^{1/n} \leq \frac{|a_1| + \cdots + |a_r| + 2(\sqrt{a_{r+1}^2 + a_{r+2}^2} + \cdots + \sqrt{a_{n-1}^2 + a_n^2})}{n}.$$

Esto implica que efectivamente $|\mathcal{N}(a)| \leq 1$ para todo $a \in A$.

Por Corolario 5.45, existe $x \in \Lambda$ no nulo tal que

$$|\mathcal{N}(x)| \leq \frac{2^n}{\mathrm{vol}(A)} \mathrm{vol}(\mathbb{R}^n/\Lambda) = \frac{n!}{n^n} \frac{2^n}{2^r} \left(\frac{2}{\pi}\right)^s \mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Solo resta probar que

$$\mathrm{vol}(A) = \frac{n^n}{n!} \, 2^r \left(\frac{\pi}{2}\right)^s,$$

placer que es dejado al lector como ejercicio. □

Ejercicio 5.46. Probar la fórmula para $\mathrm{vol}(A)$ de arriba.

5. Ejemplos de grupos de clases

Luego de haber determinado completamente la descomposición como producto de ideales primos de ideales de la forma $\langle p \rangle$, con p primo en $\mathbb{Z}$, en un cuerpo cuadrático K, y de haber mejorado la cota λ_K en Corolario 5.41, estamos en condiciones de calcular el grupo de clases $\mathcal{H}_K$ para diversos casos de cuerpos cuadráticos K. Para cuerpos que no sean cuadráticos daremos únicamente un ejemplo, pero se recomienda fuertemente ver [**Marcus**, Ch. 5].

EJEMPLO 5.47. Determinemos el grupo de clases $\mathcal{H}_K$ de $K := \mathbb{Q}(\sqrt{-163})$. En este caso tenemos que $n = [K : \mathbb{Q}] = 2$, $r = 0$ (ninguna incrustación real), $s = 1$ (dos incrustaciones complejas), y $\operatorname{disc}(K) = -163$. Por Corolario 5.41, para cada clase en $\mathcal{H}_K$ existe un ideal $\mathfrak{a}$ en ella tal que

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{163} \approx 8{,}13.$$

Luego, es necesario descomponer $\langle p\rangle$ para $p = 2, 3, 5, 7$.

Por Teoremas 5.32 y 5.34, se tiene que

$$\begin{aligned}
\left(\frac{-163}{3}\right) = \left(\frac{-165+2}{3}\right) = \left(\frac{2}{3}\right) = -1 \qquad &\Longrightarrow \quad \langle 3\rangle \text{ es primo en } \mathcal{O}_K,\\
\left(\frac{-163}{5}\right) = \left(\frac{-165+2}{5}\right) = \left(\frac{2}{5}\right) = -1 \qquad &\Longrightarrow \quad \langle 5\rangle \text{ es primo en } \mathcal{O}_K,\\
\left(\frac{-163}{7}\right) = \left(\frac{-161-2}{7}\right) = \left(\frac{5}{3}\right) = -1 \qquad &\Longrightarrow \quad \langle 7\rangle \text{ es primo en } \mathcal{O}_K,\\
\left(\frac{-163}{2}\right) = \left(\frac{-160-3}{2}\right) = \left(\frac{5}{2}\right) = -1 \qquad &\Longrightarrow \quad \langle 2\rangle \text{ es primo en } \mathcal{O}_K.
\end{aligned}$$

Rápidamente concluimos que $\mathfrak{h}_K = 1$.

EJEMPLO 5.48. Sea $K = \mathbb{Q}(\sqrt{-14})$, por lo que $n = 2$, $r = 0$, $s = 1$, y $\operatorname{disc}(K) = -14 \times 4 = -56$. Por Corolario 5.41, basta considerar los ideales $\mathfrak{a}$ con

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{56} \approx 4{,}76.$$

Como $\left(\frac{-56}{2}\right) = 0$, Teorema 5.34 nos dice que $\langle 2\rangle = \mathfrak{p}_1^2$ para algún ideal primo $\mathfrak{p}_1$. Se puede ver que $\mathfrak{p}_1 = \langle 2, \sqrt{-14}\rangle$. De manera similar, como

$$\left(\frac{-56}{3}\right) = \left(\frac{-57+1}{3}\right) = \left(\frac{1}{3}\right) = +1,$$

Teorema 5.32 asegura que existen ideales primos $\mathfrak{p}_2$ y $\mathfrak{p}_3$ tales que $\langle 3\rangle = \mathfrak{p}_2\mathfrak{p}_3$. Se puede ver que se puede escoger $\mathfrak{p}_2 = \langle 3, 1+\sqrt{-14}\rangle$ y $\mathfrak{p}_3 = \langle 3, 1-\sqrt{-14}\rangle$.

Dentro del grupo de clases $\mathcal{H}_K$, se tiene que

$$\bar{\mathfrak{p}}_1 = (\bar{\mathfrak{p}}_1)^{-1}, \qquad\qquad \bar{\mathfrak{p}}_2 = (\bar{\mathfrak{p}}_3)^{-1}.$$

Queremos escribir $\bar{\mathfrak{p}}_1$ o $\bar{\mathfrak{p}}_2$ en términos del otro. Como

$$2 - \sqrt{-14} = 3 - (1 + \sqrt{-14}) \in \mathfrak{p}_1 \cap \mathfrak{p}_2$$

y además $\mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1\mathfrak{p}_2$ por Proposición 4.21, existe un ideal entero $\mathfrak{a}$ tal que

$$\langle 2 - \sqrt{-14}\rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{a}.$$

Esto implica que

$$18 = N(\langle 2 - \sqrt{-14}\rangle) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{a}) = 6\,N(\mathfrak{a}), \quad \text{por lo tanto} \quad N(\mathfrak{a}) = 3.$$

Esto nos dice que $\mathfrak{a}$ debe coincidir con $\mathfrak{p}_2$ o $\mathfrak{p}_3$. Si $\mathfrak{a} = \mathfrak{p}_3$, entonces

$$\langle 2 - \sqrt{-14}\rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = \mathfrak{p}_1\langle 3\rangle \subset \langle 3\rangle,$$

lo cual es una contradicción pues 3 no divide a $2-\sqrt{-14}$ en $\mathcal{O}_K$. Concluimos que $\mathfrak{a}=\mathfrak{p}_2$, por lo tanto $\bar{\mathfrak{p}}_1=(\bar{\mathfrak{p}}_2)^{-2}$ y $(\bar{\mathfrak{p}}_2)^4=(\bar{\mathfrak{p}}_1^2)^{-1}=e$.

Hasta ahora hemos visto que

$$\mathcal{H}_K=\{e,\,\bar{\mathfrak{p}}_2,\,(\bar{\mathfrak{p}}_2)^2,\,(\bar{\mathfrak{p}}_2)^3\},$$

aunque no es claro aún que estos elementos sean distintos entre ellos. Es claro que $\mathfrak{p}_2$ y $\mathfrak{p}_2^3$ no son ideales principales ya que sus normas son 3 y 27, los cuales no pueden escribirse como $N_K(a+b\sqrt{-14})=a^2+14b^2$ con $a,b\in\mathbb{Z}$. Si $\mathfrak{p}_2^2$ fuese principal, entonces también lo sería $\mathfrak{p}_1$, por lo tanto existirían $a,b\in\mathbb{Z}$ tal que $\langle 2,\sqrt{-14}\rangle=\langle a+b\sqrt{-14}\rangle$. Tomando normas a ambos lados, obtenemos que

$$a^2+14b^2=N_K(a+b\sqrt{-14})=N(\langle 2,\sqrt{-14}\rangle)=2,$$

lo cual es imposible.

Luego, como $\bar{\mathfrak{p}}_2,(\bar{\mathfrak{p}}_2)^2,(\bar{\mathfrak{p}}_2)^3$ son elementos no triviales, el cociente de dos de ellos nunca será trivial. Concluimos que e, $\bar{\mathfrak{p}}_2$, $(\bar{\mathfrak{p}}_2)^2$, $(\bar{\mathfrak{p}}_2)^3$ son todos los elementos distintos, $\mathcal{H}_K\simeq C_4$ y $\mathfrak{h}_K=4$.

EJEMPLO 5.49. Sea $K=\mathbb{Q}(\sqrt[3]{2})$. En esta caso tenemos que $n=[K:\mathbb{Q}]=3$, $r=1$ (la incrustación determinada por $\sqrt[3]{2}\mapsto\sqrt[3]{2}$ es real) y $s=1$ (la incrustación determinada por $\sqrt[3]{2}\mapsto e^{2\pi\mathrm{i}/3}\sqrt[3]{2}$ es compleja).

EJERCICIO 5.50. Mostrar que $\operatorname{disc}(\mathbb{Q}(\sqrt[3]{2}))=-108$. (Ayuda: ver [**Alaca&Williams**, Example 7.1.6]).

La cota proveniente de Corolario 5.41 es

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{108}\approx 2{,}94.$$

Luego, se necesita únicamente determinar los ideales de norma ≤ 2, lo cual es trivial pues

$$\langle 2\rangle=\langle\sqrt[3]{2}\rangle^3,$$

ya que esto implica que el ideal principal $\langle\sqrt[3]{2}\rangle$ es el único. Concluimos que $\mathfrak{h}_K=1$.

Problemas.

5.6. Mostrar que el anillo de enteros de $\mathbb{Q}(\sqrt{m})$ es un dominio de factorización única para

$$m=-1,-2,-3,-7,-11,-19,-43,-67,-163.$$

Se puede probar que éstos son todos los cuerpos cuadráticos imaginarios con número de clase uno, pero su demostración es bastante más engorrosa. Para ella, se pueden consultar las notas [**Campagnolo & Guzmán**] o [**Barseghian**].

5.7. Probar que el grupo de clases de ideales de $\mathbb{Q}(\sqrt{-17})$ es cíclico de orden 4.

5.8. Encontrar algún cuerpo cuadrático real K con $\mathfrak{h}_K>1$.

5.9. Probar que el anillo de enteros de $\mathbb{Q}(\sqrt{2},\sqrt{-3})$ es un dominio de factorización única.

5.10. Encontrar algún cuerpo cúbico K con $\mathfrak{h}_K>1$.

6. Unidades

Como motivación para esta sección, recordemos que en Ejemplo 3.20 mencionamos que para los cuerpos cuadráticos imaginarios se tiene que el grupo de unidades (de su correspondiente anillo de enteros) está dado por

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \{\pm 1\} & \text{para } m < -3, \\ \{\pm 1, \pm e^{2\pi \mathrm{i}/3}, \pm e^{-2\pi \mathrm{i}/3}\} & \text{para } m = -3, \\ \{\pm 1, \pm \mathrm{i}\} & \text{para } m = -1. \end{cases}$$

Notar que en estos casos las unidades son todas raíces de la unidad, lo cual equivale a

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{m})} = \mathcal{O}_{\mathbb{Q}(\sqrt{m})} \cap \{\text{raíces de la unidad}\}.$$

También vimos que el caso cuadrático real mostraba una dificultad mayor ya que las unidades están en correspondencia con soluciones de la ecuación de Pell. Por ejemplo,

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{2})} = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\} \simeq \{\pm 1\} \times \{(1+\sqrt{2})^k : k \in \mathbb{Z}\} \simeq C_2 \times \mathbb{Z}.$$

(Recordemos que C_k denota el grupo cíclico de orden k.) En este caso, $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{2})}$ es isomorfo al producto directo de un grupo libre con el grupo de torsión

$$\{\pm 1\} = \mathcal{O}_{\mathbb{Q}(\sqrt{2})} \cap \{\text{raíces de la unidad}\}.$$

El siguiente teorema generaliza estos hechos para un cuerpo de números arbitrario.

Teorema 5.51. *Sea K un cuerpo de números con r incrustaciones reales y $2s$ incrustaciones complejas (por lo tanto $n := [K : \mathbb{Q}] = r + 2s$). Entonces,*

$$\mathcal{O}^\times_K \simeq W \times V,$$

donde $W = \mathcal{O}_K \cap \{\text{raíces de la unidad}\}$ es cíclico y V es un grupo abeliano libre de rango $r + s - 1$ (i.e. $V \simeq \mathbb{Z}^{r+s-1}$).

Demostración. Sean $\sigma_1, \ldots, \sigma_r$ las incrustaciones reales de K y $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s$ las incrustaciones complejas de K. Recordemos que en Sección 4 definimos $\Phi : K \to \mathbb{R}^n$ como

$$\Phi(\alpha) = \big(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \ldots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha))\big).$$

Además, definimos $\log : \mathbb{R}^n \smallsetminus \{(x_1, \ldots, x_n) : x_i \neq 0 \text{ y } x_{r+2j-1}^2 + x_{r+2j}^2 \neq 0 \text{ para todo } 1 \leq i \leq r,\ 1 \leq j \leq s\} \to \mathbb{R}^{r+s}$ como

$$\log(x_1, \ldots, x_n) = \left(\ln|x_1|, \ldots, \ln|x_r|, \ln(x_{r+1}^2 + x_{r+2}^2), \ldots, \ln(x_{n-1}^2 + x_n^2)\right),$$

donde $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ denota el logaritmo natural. Consideremos el esquema

$$\mathcal{O}^\times_K \hookrightarrow \mathcal{O}_K \smallsetminus \{0\} \xrightarrow{\Phi} \Lambda_{\mathcal{O}_K} \smallsetminus \{0\} \xrightarrow{\log} \mathbb{R}^{r+s}.$$

Notemos que la composición $\log \circ \Phi$ está bien definida pues si $\alpha \in \mathcal{O}_K$, entonces $\Phi(\alpha)$ tiene una coordenada nula si y sólo si todas sus coordenadas son nulas. En efecto, si $\sigma_i(\alpha) = 0$ para algún $1 \leq i \leq r$ o $\tau_j(\alpha) = 0$ para algún $1 \leq j \leq s$, entonces $\alpha = 0$ y por lo tanto $\Phi(\alpha) = (0, \ldots, 0)$.

Denotemos $\mathrm{Log} = \log \circ \Phi$. Las siguientes propiedades son verdaderas:

(1) $\mathrm{Log}(\alpha + \beta) = \mathrm{Log}\,\alpha + \mathrm{Log}\,\beta$ para todo $\alpha, \beta \in \mathcal{O}_K \smallsetminus \{0\}$.
(2) $\mathrm{Log}(\mathcal{O}^\times_K) \subset H := \{(y_1, \ldots, y_{r+s}) : y_1 + \cdots + y_{r+s} = 0\}$.
(3) Si $C \subset \mathbb{R}^{r+s}$ es acotado, entonces $\#(\log^{-1}(C) \cap \Lambda_{\mathcal{O}_K}) < \infty$.

(1) sigue del hecho $\ln(ab) = \ln(a) + \ln(b)$ para todos $a, b \in \mathbb{R}_{>0}$. (3) sigue de que $\log^{-1}(C)$ es acotado en $\mathbb{R}^n$, por lo tanto $\log^{-1}(C) \cap \Lambda_{\mathcal{O}_K} \subset \overline{\log^{-1}(C)} \cap \Lambda_{\mathcal{O}_K}$ es finito pues $\Lambda_{\mathcal{O}_K}$ es discreto y $\overline{\log^{-1}(C)}$ es compacto. (2) sigue de que si $\alpha \in \mathcal{O}_K^\times$, entonces por Proposición 3.19 se tiene que

$$1 = |N_K(\alpha)| = |\sigma_1(\alpha)| \dots |\sigma_r(\alpha)||\tau_1(\alpha)|^2 \dots |\tau_s(\alpha)|^2,$$

lo cual implica que

$$0 = \sum_{i=1}^{r} (\mathrm{Log}(\alpha))_i + \sum_{j=1}^{s} (\mathrm{Log}(\alpha))_{r+j}.$$

Aquí, para cualquier $1 \leq i \leq r+s$, denotamos $(\mathrm{Log}(\alpha))_i$ a la i-ésima coordenada de $\mathrm{Log}(\alpha)$.

Tenemos por (1) y (2) que

$$\mathrm{Log}\,|_{\mathcal{O}_K^\times} : (\mathcal{O}_K^\times, \cdot) \longrightarrow (H, +)$$

es un morfismo de grupos (abelianos) con núcleo W finito. Además, (3) nos asegura que su núcleo está dado por

$$W = \mathcal{O}_K \cap \{z \in \mathbb{C} : |z| = 1\} = \{\text{raíces de la unidad en } \mathcal{O}_K\}.$$

En efecto, la inclusión $\subset$ es trivial mientras que $\supset$ sigue así: si $\alpha \in W$, entonces (3) nos asegura que el conjunto $\Phi(\{\alpha^k : k \in \mathbb{Z}\})$ es finito por estar incluido dentro de $\log^{-1}(\{0\})$, lo que implica que $\{\alpha^k : k \in \mathbb{Z}\}$ es finito, y por lo tanto α es una raíz de la unidad. Concluimos que W es un subgrupo finito de $\{z \in \mathbb{C} : |z| = 1\}$, por lo tanto W es cíclico por el siguiente hecho bien conocido.

Ejercicio 5.52. Demostrar que todo subgrupo finito de $\{z \in \mathbb{C} : |z| = 1\}$ es cíclico.

Tomemos V como la imagen de Log, i.e. $V = \mathrm{Log}(\mathcal{O}_K^\times)$. Tenemos que

$$\mathcal{O}_K^\times \simeq \mathrm{Nu}(\mathrm{Log}) \times \mathrm{Im}(\mathrm{Log}) = W \times V.$$

Ejercicio 5.53. Demostrar que si G es un subgrupo de $(\mathbb{R}^n, +)$ tal que $\#(G \cap C) < \infty$ para todo $C \subset \mathbb{R}^n$ acotado, entonces G es un retículo en $\mathbb{R}^n$ (i.e. un subgrupo discreto de rango $\leq n$).

Este ejercicio nos asegura que V es un retículo en $\mathbb{R}^{r+s}$. Además, V tiene rango $d \leq r+s-1$ pues $V \subset H$. Resta ver que $d = r+s-1$. Para esto, construiremos $r+s-1$ vectores en V linealmente independiente sobre $\mathbb{R}$.

Lema 5.54. *Fijamos $1 \leq k \leq r+s$. Para cada $\alpha \in \mathcal{O}_K$ existe $\beta \in \mathcal{O}_K$ con*

$$|N_K(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{\mathrm{disc}(K)},$$

tal que si denotamos $\mathrm{Log}(\alpha) = (a_1, \dots, a_{r+s})$ y $\mathrm{Log}(\beta) = (b_1, \dots, b_{r+s})$, entonces $b_i < a_i$ para todo $i \neq k$.

Demostración. Sea $\alpha \in \mathcal{O}_K$ y escribimos $\mathrm{Log}(\alpha) = (a_1, \dots, a_{r+s})$. Tomemos números reales positivos $c_1, \dots, c_{r+s}$ tales que $c_i < e^{a_i}$ para todo $i \neq k$, y

$$c_1 \dots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{\mathrm{disc}(K)}.$$

Sea

$$E = \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n : \begin{array}{l} |x_i| \le c_i \text{ para todo } 1 \le i \le r, \\ x_{r+2j-1}^2 + x_{r+2j}^2 \le c_{r+j} \text{ para todo } 1 \le j \le s \end{array} \right\}.$$

EJERCICIO 5.55. Mostrar que $\mathrm{vol}(E) = 2^r \pi^s c_1 \dots c_{r+s}$.

Luego, $\mathrm{vol}(E) = 2^{r+s} \sqrt{\mathrm{disc}(K)}$, y Teorema 5.37 implica que

$$\mathrm{vol}(E) = 2^n \, \mathrm{vol}(\mathbb{R}^n / \Lambda_{\mathcal{O}_K}) \, .$$

Además, E es claramente convexo, simétrico y compacto. Aplicando Lema de Minkowski (Lema 5.44) obtenemos que existe un elemento $y \in (\Lambda_{\mathcal{O}_K} \smallsetminus \{0\}) \cap E$. Sea $\beta \in \mathcal{O}_K$ tal que $y = \Phi(\beta)$, y escribimos $\mathrm{Log}(\beta) = (b_1, \dots, b_{r+s})$. Como $\Phi(\beta) \in E$, tenemos que

$$N_K(\beta) = \mathcal{N}(\Phi(\beta)) \le c_1 \dots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{\mathrm{disc}(K)}$$

y $e^{b_i} \le c_i$ para todo i, por lo tanto $b_i \le \log c_i \le a_i$ para todo $i \neq k$. ■

LEMA 5.56. *Fijamos $1 \le k \le r+s$. Entonces existe $u \in \mathcal{O}_K^\times$ tal que si denotamos $\mathrm{Log}(u) = (y_1, \dots, y_{r+s})$, entonces $y_i < 0$ para todo $i \neq k$.*

DEMOSTRACIÓN. Sea $\alpha_1 \in \mathcal{O}_K$ no nulo. Aplicando repetidas veces Lema 5.54, obtenemos una sucesión $\{\alpha_j\}_j \subset \mathcal{O}_K \smallsetminus \{0\}$ tal que

$$|N_K(\alpha_j)| \le \left(\frac{2}{\pi}\right)^s \sqrt{\mathrm{disc}(K)}$$

para todo j.

Los ideales en la familia infinita $\{\langle \alpha_j \rangle\}_j$ tienen norma acotada. Como la cantidad de ideales enteros de norma $\le \lambda$ es finita para cualquier $\lambda > 0$ fijo por Proposición 5.8, existen índices $i < j$ tales que $\langle \alpha_i \rangle = \langle \alpha_j \rangle$. Entonces, existe $u \in \mathcal{O}_K^\times$ tal que $\alpha_j = u\alpha_i$.

Veamos que u cumple lo requerido. Escribimos $\mathrm{Log}(u) = (y_1, \dots, y_{r+s})$. Si $h \neq k$, entonces

$$(\mathrm{Log}(\alpha_j))_h = (\mathrm{Log}(\alpha_i) + \mathrm{Log}(u))_j > (\mathrm{Log}(\alpha_i))_h + (\mathrm{Log}(u))_h,$$

lo cual implica que $(\mathrm{Log}(u))_h < (\mathrm{Log}(\alpha_j))_h - (\mathrm{Log}(\alpha_i))_h < 0$. ■

Por Lema 5.56, existen $u_1, \dots, u_{r+s}$ tales que $(\mathrm{Log}(u_j))_i < 0$ para todo $i \neq j$ y

$$(\mathrm{Log}(u_j))_j = -\sum_{i \neq j} (\mathrm{Log}(u_j))_i > 0.$$

LEMA 5.57. *Sea $A = (a_{i,j})_{i,j} \in \mathbb{R}^{m \times m}$ tal que*

- *$a_{i,i} > 0$ para todo i,*
- *$a_{i,j} < 0$ para todo $i \neq j$, y*
- *$\sum_{j=1}^m a_{i,j} = 0$ para todo i.*

Entonces el rango de A es igual a $m-1$.

DEMOSTRACIÓN. Veamos que las primeras columnas $v_1, \dots, v_{m-1}$ son linealmente independientes. Supongamos que $\sum_{j=1}^m t_j v_j = 0$ para algunos $t_1, \dots, t_{m-1} \in \mathbb{R}$ no todos nulos. Podemos suponer que $t_j \le 1$ para todo j y $t_k = 1$ para algún k, dividiendo a todos (de ser necesario, i.e. $t_j > 1$ para algún j) por $\max_j t_j$.

En la k-ésima fila, tenemos

$$0 = \sum_{j=1}^{m-1} t_j a_{k,j} = a_{k,k} + \sum_{\substack{1\le j\le m-1,\\ j\neq k}} \underbrace{t_j a_{k,j}}_{\ge a_{k,j}} \ge \sum_{j=1}^{m-1} a_{k,j} > \sum_{j=1}^{m} a_{k,j} = 0,$$

lo cual es una contradicción. ■

Como la matriz $((\mathrm{Log}(u_j))_i)_{i,j}$ cumple las hipótesis de Lema 5.57 tal como lo acabamos de ver, esta matriz tiene rango $r+s-1$ que es lo que restaba. □

Problemas.

5.11. Determinar las unidades del anillo de enteros de algún cuerpo cuadrático real diferente a $\mathbb{Q}(\sqrt{2})$.

5.12. Determinar las unidades del anillo de enteros de algún cuerpo de números cúbico que posea exactamente una incrustación real, y otro con tres incrustaciones reales.

7. Último teorema de Fermat

Se puede decir que la teoría algebraica de números nació como una herramienta para demostrar el último teoría de Fermat, el cual asegura que para cualquier $n > 2$, la llamada *ecuación de Fermat*

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

no tiene soluciones enteras $(x, y, z) \neq (0, 0, 0)$. Este problema muy famoso cuenta con una interesante historia, antigua y reciente, digna de una película. Un resumen se puede encontrar en Wikipedia.

Notamos fácilmente que si el último teorema de Fermat es cierto para n, entonces también lo es para cualquier múltiplo de n. En efecto, una solución (no trivial) (x, y, z) de

$$x^{mn} + y^{mn} = z^{mn}$$

aportaría inmediatamente (x^m, y^m, z^m) como solución de la ecuación de grado n pues

$$(x^m)^n + (y^m)^n = (z^m)^n.$$

Luego, es suficiente considerar los casos $n = 4$ y $n = p$ con p primo impar arbitrario.

Ejercicio 5.58. Probar que si $x^4 + y^4 = z^4$ con $x, y, z \in \mathbb{Z}$, entonces $x = y = z = 0$. (Primera ayuda: usar ternas pitagóricas.) (Segunda ayuda: ver [**Marcus**, Exercise 15, Ch. 1].)

Fijemos p un número primo impar. Consideremos el cuerpo ciclotómico de orden p, esto es, $K = \mathbb{Q}(\xi)$ con $\xi = e^{2\pi \mathrm{i}/p}$, el cual tiene orden $[K : \mathbb{Q}] = p - 1$ (ver Teorema 2.27). Sabemos por Teorema 3.44 que el anillo de enteros de K es $\mathcal{O}_K = \mathbb{Z}[\xi]$, es decir, todo entero algebraico en K se escribe como combinación lineal entera de $\{1, \xi, \xi^2, \ldots, \xi^{p-1}\}$. Denotemos

$$\lambda = 1 - \xi \in \mathcal{O}_K \quad \text{y} \quad \mathfrak{q} = \langle \lambda \rangle.$$

El objetivo de esta sección es demostrar el siguiente teorema, el cual es una hermosa aplicación altamente no trivial de lo que hemos visto en estas notas a este famoso problema.

TEOREMA 5.59. *Si p es un primo impar tal que p no divide al número de clases $\mathfrak{h}_K$ de K, entonces no existen enteros x, y, z tales que*

$$x^p + y^p = z^p \qquad y \qquad p \nmid xyz.$$

OBSERVACIÓN 5.60. El caso en que p divide a exactamente uno de $\{x, y, z\}$ se demuestra con herramientas más sofisticadas y no lo consideraremos en estas notas.

El resto de la sección será dedicada a la demostración de Teorema 5.59. Comenzamos suponiendo que p es cualquier primo impar.

LEMA 5.61. *Tenemos que $\mathfrak{q}^{p-1} = \langle p \rangle$, $N(\mathfrak{q}) = p$, y en consecuencias $\mathfrak{q}$ es un ideal primo en $\mathcal{O}_K$.*

DEMOSTRACIÓN. La identidad

$$1 + t + t^2 + \cdots + t^{p-1} = (t - \xi)(t - \xi^2) \dots (t - \xi^{p-1})$$

evaluada en $t = 1$ nos asegura que $p = \prod_{j=1}^{p-1}(1 - \xi^j)$, lo que a su vez nos dice que

$$\langle p \rangle = \prod_{j=1}^{p-1} \langle 1 - \xi^j \rangle.$$

Veamos que $\langle \lambda \rangle = \langle 1 - \xi^j \rangle$ para todo $1 \leq j \leq p - 1$.

Como $1 - \xi^j = (1 - \xi)(1 + \xi + \cdots + \xi^{j-1})$, sigue que $\lambda = 1 - \xi$ divide a $1 - \xi^j$ para todo $1 \leq j \leq p - 1$. Por otro lado, tomando $k \in \mathbb{Z}$ tal que $jk \equiv 1 \pmod{p}$, vemos que

$$\lambda = 1 - \xi = 1 - \xi^{kj} = (1 - \xi^j)(1 + \xi^j + \xi^{2j} + \cdots + \xi^{j(k-1)}),$$

lo que asegura que $1 - \xi^j$ divide a λ para todo $1 \leq j \leq p - 1$. Esto asegura para cualquier $1 \leq j \leq p - 1$ que λ y $1 - \xi^j$ difieren por una unidad, y en consecuencia $\langle \lambda \rangle = \langle 1 - \xi^j \rangle$.

Concluimos (desde la penúltima fórmula centrada) que $\langle p \rangle = \langle \lambda \rangle^{p-1} = \mathfrak{q}^{p-1}$. Esto a su vez implica que

$$p^{p-1} = |N_K(p)| = N(\langle p \rangle) = N(\mathfrak{q})^{p-1},$$

por lo tanto $N(\mathfrak{q}) = p$. □

A partir de ahora, supongamos que la ecuación de Fermat para $n = p$ sí tiene solución $\{x, y, z\}$ con $p \nmid xyz$. Claramente podemos asumir que $\text{mcd}(x, y, z) = 1$. Luego,

$$z^p = x^p + y^p = (x + y)(x + \xi y)(x + \xi^2 y) \dots (x + \xi^{p-1} y).$$

Por lo tanto

$$\langle z \rangle^p = \langle z^p \rangle = \prod_{j=0}^{p-1} \langle x + \xi^j y \rangle.$$

AFIRMACIÓN. *$\langle x + \xi y \rangle = \mathfrak{a}^p$ para algún ideal $\mathfrak{a}$ en $\mathcal{O}_K$.*

DEMOSTRACIÓN. Sea $\mathfrak{p}$ un ideal primo en $\mathcal{O}_K$ tal que $\mathfrak{p}$ divide a $\langle x + \xi y \rangle$, y en consecuencia también a $\langle z \rangle^p$ y a $\langle z \rangle$. Entonces $\mathfrak{p}^p$ divide a $\langle z \rangle^p$.

Si $\mathfrak{p}$ fuera coprimo a $\langle x + y \rangle \prod_{j=2}^{p-1} \langle x + \xi^j y \rangle$ para cualquier ideal primo $\mathfrak{p}$ que divide a $\langle x + \xi y \rangle$, entonces $\mathfrak{p}^p$ dividiría a $\langle x + \xi y \rangle$ y la afirmación estaría probada.

Supongamos que existe un ideal primo $\mathfrak{p}$ divisor de $\langle x+\xi y\rangle$ tal que $\mathfrak{p}$ divide también a $\langle x+\xi^j y\rangle$ para algún $j\in\{0,2,3\ldots,p-1\}$. Como tanto $x+\xi y$ y $x+\xi^j y$ pertenecen a $\mathfrak{p}$, también lo hace su diferencia, esto es,

$$\mathfrak{p}\ni y(\xi-\xi^j)=y\xi(1-\xi^{j-1})=y\xi u(1-\xi)=y\xi u\lambda$$

para algún $u\in\mathcal{O}_K^\times$ (por lo visto en la demostración de Lema 5.61).

Como ξu es una unidad, tenemos que $y\lambda\in\mathfrak{p}$, y en consecuencia $y\in\mathfrak{p}$ o $\lambda\in\mathfrak{p}$ por ser $\mathfrak{p}$ primo. Veamos que ambos casos implican contradicciones.

Supongamos que $y\in\mathfrak{p}$. Luego $x=(x+\xi y)-\xi y\in\mathfrak{p}$. Como además $z\in\mathfrak{p}$, $\mathfrak{p}$ contiene al ideal $\langle x,y,z\rangle$ el cual igual a $\mathcal{O}_K$ pues x,y,z son coprimos en $\mathbb{Z}$.

Ahora supongamos que $\lambda\in\mathfrak{p}$. Entonces $\mathfrak{p}$ divide a $\langle\lambda\rangle=\mathfrak{q}$ y por lo tanto $\mathfrak{p}=\mathfrak{q}$. Como $z\in\mathfrak{q}$, tenemos que $p=N(\mathfrak{q})$ divide a $N(\langle z\rangle)=z^{p-1}$, lo que implica que p divide a z lo cual es una contradicción por hipótesis. □

El ideal $\mathfrak{a}$ (proveniente de la afirmación anterior) cumple que $(\bar{\mathfrak{a}})^p=e$, el elemento trivial en el grupo de clases $\mathcal{H}_K$ de K. Asumamos como en Teorema 5.59 que p no divide a $\mathfrak{h}_K=\#\mathcal{H}_K$. Entonces $\bar{\mathfrak{a}}=e$, por lo que existe $\delta\in\mathcal{O}_K$ tal que $\mathfrak{a}=\langle\delta\rangle$. Más aún, como $\mathfrak{a}^p=\langle x+\xi y\rangle$, tenemos que existe $u\in\mathcal{O}_K^\times$ tal que $x+\xi y=u\delta^p$.

Lema 5.62 (de Kummer). *Toda unidad de $\mathcal{O}_K$ es de la forma $r\xi^g$ con $r\in\mathbb{R}$ y $g\in\mathbb{Z}$.*

Usando este resultado que no demostraremos, obtenemos que

$$x+\xi y=\delta^p r\xi^g.$$

Será muy útil usar la notación $\alpha\equiv\beta\pmod{\mathfrak{b}}$ cuando $\alpha-\beta\in\mathfrak{b}$, para $\mathfrak{b}$ un ideal en $\mathcal{O}_K$ y $\alpha,\beta\in\mathcal{O}_K$.

Afirmación. *Existe $a\in\mathbb{Z}$ tal que $\delta^p\equiv a\pmod{\mathfrak{q}^p}$.*

Demostración. Claramente $\{0,1,\ldots,p-1\}$ es un conjunto de representantes de las coclases $\mathcal{O}_K/\mathfrak{q}=\mathcal{O}_K/\langle 1-\xi\rangle$. Luego, existe un entero $0<b<p$ tal que $\delta\equiv b\pmod{\mathfrak{q}}$. Sea $a=b^p$. Entonces

$$\delta^p-a^p=\delta^p-b^p=\prod_{j=0}^{p-1}(\delta-\xi b)\equiv\prod_{j=0}^{p-1}(\delta-b)\equiv 0\pmod{\mathfrak{q}^p},$$

tal como lo afirmado. La primer congruencia sigue de que $\xi\equiv 1\pmod{\mathfrak{q}}$. □

Tenemos entonces que

$$x+\xi y\equiv ar\xi^g\pmod{\mathfrak{q}^p}\quad\text{y}\quad x+\xi y\equiv ar\xi^g\pmod{\langle p\rangle}.$$

Este último sigue de que $\mathfrak{q}^p\subset\mathfrak{q}^{p-1}=\langle p\rangle$. Entonces

$$\begin{aligned}\xi^{-g}(x+\xi y)&\equiv ar\pmod{\langle p\rangle}&&(\text{pues }\xi^{-g}\in\mathcal{O}_K^\times),\\ \xi^{g}(x+\xi^{-1}y)&\equiv ar\pmod{\langle p\rangle}&&(\text{tomando conjugación compleja}).\end{aligned}$$

Tomando la diferencia entre estas dos últimas identidades de congruencias obtenemos que

$$x\xi^{-g}+y\xi^{1-g}-x\xi^g-y\xi^{g-1}\equiv 0\pmod{\langle p\rangle},$$

esto es, existe $\alpha\in\mathcal{O}_K$ tal que

$$\alpha p=x\xi^{-g}+y\xi^{1-g}-x\xi^g-y\xi^{g-1}.$$

Escribimos

$$\alpha = \frac{x}{p}\,\xi^{-g} + \frac{y}{p}\,\xi^{1-g} - \frac{x}{p}\,\xi^{g} - \frac{y}{p}\,\xi^{g-1}.$$

Como $\alpha \in \mathcal{O}_K$, $\{\xi^j : 0 \le j \le p-1\}$ es una base entera de $\mathcal{O}_K$ y $p \nmid xy$, resulta que los índices $\{-g, 1-g, g, g-1\}$ no puede ser todos distintos en $\mathbb{Z}/p\mathbb{Z}$ pues de lo contrario, los coeficientes de $\xi^{-g}, \xi^{1-g}, \xi^{g}, \xi^{g-1}$ serían números racionales que no están en $\mathbb{Z}$.

AFIRMACIÓN. *p no divide (en $\mathbb{Z}$) a g ni a $g-1$.*

DEMOSTRACIÓN. Recordemos que

$$x\xi^{-g} + y\xi^{1-g} - x\xi^{g} - y\xi^{g-1} \equiv 0 \pmod{\langle p\rangle},$$

Si p divide a g, entonces $\xi^g = 1$ y por lo tanto $y(\xi - \xi^{-1}) \in \langle p\rangle$, lo que implica que p divide (en $\mathcal{O}_K$) a $y\xi^{-1}(\xi^2 - \xi) = -y\xi(1+\xi)(1-\xi)$. Como ξ y $1+\xi$ son unidades en $\mathcal{O}_K$, obtenemos que p divide a $y(1-\xi) = y\lambda$, lo que nos dice que

$$\langle\lambda\rangle^{p-1} = \langle p\rangle \supset \langle y\rangle\langle\lambda\rangle.$$

Cancelando $\langle\lambda\rangle$ en ambos lados (por Corolario 4.11), obtenemos que $y \in \langle\lambda\rangle^{p-2} \subset \langle\lambda\rangle$. Esto a su vez implica que $y^{p-1} \in \langle\lambda\rangle^{p-1} = \langle p\rangle$, por lo tanto p divide a y^{p-1} en $\mathcal{O}_K$ y también en $\mathbb{Z}$, en consecuencia p divide a y en $\mathbb{Z}$ lo cual es una contradicción.

El caso $p \mid g-1$ es similar. □

La única posibilidad restante para que $\{-g, 1-g, g, g-1\}$ no sean distintos en $\mathbb{Z}/p\mathbb{Z}$ es que p divida (en $\mathbb{Z}$) a $2g-1$. En este caso tenemos que

$$\alpha p\xi^g = x + y\xi - x\xi^{2g} - y\xi^{2g-1} = x(1-\xi) + y(\xi - 1) = (x-y)(1-\xi) = (x-y)\lambda.$$

Tomando norma a ambos extremos,

$$\underbrace{N_K(p)}_{=p^{p-1}}\, N_K(\alpha)\, \underbrace{N_K(\xi^g)}_{=1} = \underbrace{N_K(\lambda)}_{=p}\, \underbrace{N_K(x-y)}_{(x-y)^{p-1}},$$

lo cual implica que p divide en $\mathbb{Z}$ a $x-y$, i.e. $x - y \in p\mathbb{Z}$.

Hemos mostrado que si x, y, z son enteros tales que $p \nmid xyz$, $\mathrm{mcd}(x,y,z) = 1$ y $x^p + y^p = z^p$, entonces $p \mid x - y$. Más aún, para tales x, y, z, también se tiene que $x, -z, -y$ cumple las propiedades recién mencionadas pues $p \nmid x(-z)(-y)$, $\mathrm{mcd}(x, -z, -y) = 1$ y $x^p + (-z)^p = (-y)^p$, por lo tanto $p \mid x - (-z) = x + z$. Esto implica que (en $\mathbb{Z}$) tenemos que

$$0 \equiv x^p + y^p - z^p \equiv x^p + x^p + x^p = 3x^p \pmod{p},$$

por lo tanto p divide a 3, i.e. $p = 3$. Esto es una contradicción pues es muy simple chequear que la ecuación de Fermat para $n = 3$ no tienen soluciones. En efecto, $c^3 \equiv \pm 1 \pmod 9$ para todo $c \in \mathbb{Z}$ no divisible por 3, por lo tanto

$$0 \equiv x^3 + y^3 + (-z)^3 \equiv \pm 1 \pm 1 \pm 1 \pmod 9.$$

Esto finaliza la demostración de Teorema 5.59.

COMENTARIO 5.63. Los números primos p que no dividen al número de clases $\mathfrak{h}_{\mathbb{Q}(e^{2\pi \mathrm{i}/p})}$ de la extensión ciclotómica $\mathbb{Q}(e^{2\pi \mathrm{i}/p})$ de orden p son llamados *regulares* Los primos irregulares menores a 200 son

$$37, \quad 59, \quad 67, \quad 101, \quad 131, \quad 149, \quad 157.$$

Bibliografía

[Alaca&Williams] S. Alaca, K.S. Williams. Introductory Algebraic Number Theory. Cambridge University Press, 2003. DOI: 10.1017/CBO9780511791260.

[Barseghian] E. Barseghian. Teorema de Stark-Heegner. Tercer lugar en el *Concurso de Monografías* de la Reunión Anual de la Unión Matemática Argentina (UMA) 2016.

[Campagnolo & Guzmán] E. Campagnolo, J. Guzmán. El Teorema de Stark-Heegner. Segundo lugar en el *Concurso de Monografías* de la Reunión Anual de la Unión Matemática Argentina (UMA) 2016.

[Hungerford] T.W. Hungerford. Algebra. *Grad. Texts in Math.* **73**. Reprint of the 1974 original. Springer-Verlag, New York-Berlin, 1980. DOI: 10.1007/978-1-4612-6101-8.

[Ivorra Castillo] C. Ivorra Castillo. Teoría algebraica de números. No está publicado de manera formal; disponible en su página web.

[Lang] S. Lang. Algebra. *Grad. Texts in Math.* **211**. Revised third edition. Springer, New York, 2002. DOI: 10.1007/978-1-4613-0041-0.

[Lauret] E. Lauret. Anillos de enteros de cuerpos cuadráticos. Notas de curso del Encuentro Nacional de Álgebra VI (elENA), Julio 2012. Disponible en la página web del autor.

[Narasimhan et al] R. Narasimhan, S. Raghavan, S.S. Rangachari, Sunder Lal. Algebraic number theory. Lectures from Tata Institute of Fundamental Research, Bombay, 1966.

[Marcus] D. Marcus. Number fields. *Universitext*. Springer-Verlag, New York-Heidelberg, 1977. DOI: 10.1007/978-1-4684-9356-6.

[Rossetti] J.P. Rossetti. Retículos en espacios euclídeos. Notas de curso del Encuentro Nacional de Álgebra III (elENA), Julio 2006. Disponible en la página web de Publicaciones de FaMAF.