EL GRUPO DE CLASE DE UN ANILLO DE ENTEROS ALGEBRAICOS

JUAN DAVID RUEDA CENTENO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2023

EL GRUPO DE CLASE DE UN ANILLO DE ENTEROS ALGEBRAICOS

JUAN DAVID RUEDA CENTENO

Trabajo de grado para optar al título de
Matemático

Director
Héctor Edonis Pinedo Tapia
Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2023

DEDICATORIA

A mis padres, mi hermana y mi nona.

AGRADECIMIENTOS

Agradezco profundamente a mi familia por el apoyo incondicional que me han dado toda mi vida. También agradezco a todos los profesores que han pasado por mi recorrido académico, en especial al profesor Ángel Niño, quien fue el profesor que me hizo enamorarme de las matemáticas, y al profesor Héctor Pinedo por su apoyo en la realización de este trabajo de grado. Quiero agradecer a mis amigos que siempre estuvieron ahí para ayudarme, especialmente a Natalia, ya que sin ella esto no hubiera sido posible.

RESUMEN

TÍTULO: EL GRUPO DE CLASE DE UN ANILLO DE ENTEROS ALGEBRAICOS [*]

AUTOR: JUAN DAVID RUEDA CENTENO [**]

PALABRAS CLAVE: ANILLOS, ENTEROS ALGEBRAICOS, IDEALES PRIMOS, GRUPO DE CLASE.

DESCRIPCIÓN: La teoría algebraica de números es una rama de la teoría de números que a través del algebra abstracta estudia los números enteros, racionales y generalizaciones de estos, como por ejemplo el anillo de los enteros algebraicos de una extensión de cuerpos finita de $\mathbb{Q}$. Históricamente, estos anillos han sido una herramienta para resolver ecuaciones diofánticas y otros problemas relacionados con los números enteros. A partir de estos anillos se definen algunos conceptos que ayudan a entender sus propiedades, entre estos el grupo de clase.

En el primer capítulo, repasaremos algunos resultados y conceptos del algebra abstracta, a su vez definiremos algunas aplicaciones para $\mathbb{Q}$ las cuales son importantes para el desarrollo del escrito. En el siguiente capítulo primeramente se introduce el concepto de entero algebraico para luego definir el anillo de enteros algebraicos y mencionar algunas de sus propiedades. Luego definiremos el concepto de ideal fraccionario, para así poder demostrar que la colección de ideales de un anillo de enteros algebraicos posee factorización única en ideales primos. Por último, definiremos el grupo de clase. Mostraremos que es finito y algunas de sus aplicaciones como ayudar a solucionar ecuaciones diofánticas y encontrar un ejemplo de un dominio de ideales principales que no sea euclídeo.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

ABSTRACT

TITLE: THE CLASS GROUP OF A RING OF ALGEBRAIC INTEGERS [*]

AUTHOR: JUAN DAVID RUEDA CENTENO [**]

KEYWORDS: RINGS, ALGEBRAIC INTEGERS, PRIME IDEALS, CLASS GROUP.

DESCRIPTION: Algebraic number theory is a branch of number theory that through abstract algebra studies integers, rational numbers and generalizations of these, such as the ring of algebraic integers of a finite field extension of $\mathbb{Q}$. Historically, these rings have been a tool for solving diophantine equations and other problems involving integers. From these rings, some concepts are defined that help to understand their properties, including the class group.

In the first chapter, we will review some results and concepts of abstract algebra. At the same time, we will define some applications for $\mathbb{Q}$ which are important for this writing. In the next chapter, the concept of algebraic integers will be introduced, then we will define the ring of algebraic integers and mention some of its properties. After that, we will show the concept of fractional ideal, in order to demonstrate that the collection of ideals of a ring of algebraic integers has a unique factorization in prime ideals. Finally, we will define the class group. We will show that it is finite and some of its applications such as helping to solve diophantine equations and finding an example of a domain of principal ideals that is not euclidean.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

Introducción

La teoría algebraica de números es una rama de la teoría de números que a través del algebra abstracta estudia los números enteros, racionales y generalizaciones de estos, como por ejemplo el anillo de los enteros algebraicos de una extensión de cuerpos finita de $\mathbb{Q}$. El cual consiste en todos los elementos de la extensión que son raíz de un polinomio mónico con coeficientes enteros. Aunque el anillo de los enteros algebraicos sea una extensión de anillo de $\mathbb{Z}$, lamentablemente no siempre se extiende una de las propiedades más importantes de $\mathbb{Z}$, la factorización única en elementos irreducibles. Sin embargo, en dicho anillo si vale la factorización de ideales en ideales primos. Los dominios con esta propiedad son llamados dominios de Dedekind.
En este tipo de dominios se satisface que un dominio es de ideales principales si, y solo si, es un dominio de factorización única. Es en este punto donde aparece el grupo de clase (ver la sección 3.3) como una medida de la desviación del anillo de enteros algebraicos de ser un dominio de ideales principales y por tanto de factorización única, ya que el anillo es de ideales principales si, y solo si, el grupo de clase es trivial.

En este trabajo de grado nos interesa estudiar propiedades estructurales del anillo de enteros algebraicos de una extensión finita de $\mathbb{Q}$ donde veremos como a través de su grupo de clase es posible resolver ecuaciones diofánticas y encontrar un ejemplo de un dominio de ideales principales que no es euclídeo.

1. Preliminares

En este capítulo empezaremos recordando algunas nociones y resultados principales sobre anillos y cuerpos. Usaremos como referencia general los libros [1] y [2]. Posteriormente mencionaremos algunos resultados sobre extensiones de cuerpos, haciendo énfasis en las extensiones finitas de $\mathbb{Q}$. Por último definiremos algunas aplicaciones de extensiones finitas de $\mathbb{Q}$ en $\mathbb{C}$ que usaremos en capítulos posteriores.

1.1. Anillos y Cuerpos

Definición 1.1.1. Un **anillo** $\langle R, +, \cdot \rangle$ es una tripla que consiste de un conjunto R dotado con dos operaciones binarias $+$ y $\cdot$ llamadas suma y producto que satisfacen los siguientes axiomas:

I) $\langle R, + \rangle$ es un grupo abeliano.

II) La operación binaria $\cdot$ es asociativa sobre R.

III) Para todo $a, b, c \in R$ la ley distributiva a la izquierda, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ y la ley distributiva a la derecha, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ se cumplen.

Si en un anillo R la operación $\cdot$ es conmutativa decimos que R es un anillo **conmutativo**. Por otro lado, si existe un elemento $e \in R$ tal que para todo $a \in R$, $e \cdot a = a \cdot e = a$ decimos que R es un anillo **con unidad,** es fácil ver que esta unidad es única y es denotada por $1_R \neq 0$, donde 0 es el elemento neutro del anillo. De ahora en adelante por anillo entenderemos anillo conmutativo con unidad.

Ejemplo 1.1.2. Sea A un anillo, denotemos por $A[x]$ a los polinomios con coeficientes en A, es fácil ver que:

I) $A[x]$ es un anillo bajo la suma y el producto usual de polinomios.

II) $A[x]$ es un anillo conmutativo si, y solo si, A es un anillo conmutativo.

---

[1] Jhon FRALEIGH. *A First Course in Abstract Algebra*. Addison-Wesley, 2003.

[2] Karlheinz SPINDLER. *Abstract Algebra with Applications. Volume 2: Rings and Fiels*. Chapman, Hall/CRC Pure y Applied Mathematics, 1993.

III) $A[x]$ es un anillo con unidad si, y solo si, A es un anillo con unidad.

Definición 1.1.3. Sea R un anillo con unidad $1_R \neq 0$. Un elemento $u \in R$ es llamado **invertible** si existe $v \in R$ tal que $u \cdot v = v \cdot u = 1_R$, el conjunto de todos los elementos invertibles de R es denotado por $U(R)$. Si cada elemento diferente del cero es invertible, entonces R es un anillo **con división**. Un **cuerpo** es un anillo conmutativo con división.

Ejemplo 1.1.4. $\mathbb{Z}$ no es un cuerpo ya que por ejemplo 2 no es invertible, a diferencia de $\mathbb{Q}$ que si es un cuerpo.

Definición 1.1.5. Sea $\langle R, +, \cdot \rangle$ un anillo. Un conjunto $S \subseteq R$ es llamado **subanillo** si $\langle S, +, \cdot \rangle$ es un anillo. Además si I un subanillo de R tal que $aI \subseteq I$ y $Ib \subseteq I$ para todo $a, b \in R$, se dice que I es un **ideal** de R.

Ejemplo 1.1.6. Sea R un anillo. Si $\alpha \in R$ entonces el conjunto αR es un ideal de R. En efecto, sean $x, y \in \alpha R$ y $r \in$ R. Primero $\alpha R \neq \emptyset$ ya que $0 \in R$, entonces $\alpha \cdot 0 = 0 \in \alpha R$. Basta mostrar que $x - y \in \alpha R$ y que $rx \in \alpha R$. Como $x, y \in \alpha R$ existen $r_x, r_y \in R$ tal que $x = \alpha r_x$ y $y = \alpha r_y$, entonces $x - y = \alpha r_x - \alpha r_y = \alpha(r_x - r_y) \in \alpha R$. También $rx = r(\alpha r_x) = (r\alpha) r_x = \alpha(r r_x) \in \alpha R$.

Los ideales que se escriben de esta manera son llamados ideales **principales** y los denotaremos por $\langle \alpha \rangle$. Además de estos ideales presentamos otro tipo de ideales que usaremos a lo largo del desarrollo del escrito.

Definición 1.1.7. Sea $\mathfrak{p}$ un ideal propio del anillo R. Se dice que $\mathfrak{p}$ es un ideal **primo** si $ab \in \mathfrak{p}$ implica que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. A su vez, $\mathfrak{m}$ es llamado ideal **maximal** si para todo ideal propio N de R tal que $\mathfrak{m} \subseteq N$ entonces $\mathfrak{m} = N$.

Ejemplo 1.1.8. Sea $p \in \mathbb{Z}$ un número primo, entonces $\langle p \rangle$ es un ideal primo y maximal de $\mathbb{Z}$. Es claro que $\langle p \rangle$ es un ideal primo ya que si $ab \in \langle p \rangle$ implica que $p|ab$, entonces $p|a$ o $p|b$ que es lo mismo que $a \in \langle p \rangle$ o $b \in \langle p \rangle$. Ahora, sea I un ideal diferente de $\langle p \rangle$ tal que $\langle p \rangle \subset I$, como I es diferente de $\langle p \rangle$ existe $q \in I$ tal que $p \nmid q$ y como p es primo entonces es coprimo con q, así por el lema de Bezout existen $x, y \in \mathbb{Z}$ tal que $px + qy = 1$ y como $p, q \in I$ tenemos que $1 \in I$ por lo que $I = \mathbb{Z}$.

Definición 1.1.9. Sea $\langle R, +, \cdot \rangle$ un anillo y R_I el conjunto de todos los ideales de R. Si $A, B \in R_I$ se definen:

$$A + B = \{a + b \mid a \in A, b \in B\} \qquad A \cdot B = \left\{ \sum_{i=1}^{n} a_i \cdot b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}$$

Con estas operaciones R_I es un anillo con unidad $1_{R_I} = R$, elemento neutro 0_R y el inverso aditivo de un ideal A es el ideal $-A$.

Definición 1.1.10. Sea $\langle R, +, \cdot \rangle$ un anillo. Un elemento $a \in R$ diferente del cero es llamado **divisor de cero** si existe $b \in R$ diferente de cero tal que $a \cdot b = 0$. Un **dominio entero** es un anillo conmutativo con unidad que no tiene divisores de cero.

Recordaremos ahora una caracterización de los ideales primos y maximales.

Proposición 1.1.11. *Sea R un anillo, entonces:*

I) $\mathfrak{p}$ *es un ideal primo de* R *si, y solo si,* $R/\mathfrak{p}$ *es un dominio entero.*

II) $\mathfrak{m}$ *es un ideal maximal de* R *si, y solo si,* $R/\mathfrak{m}$ *es un cuerpo.*

Demostración. I) Sea $\mathfrak{p}$ un ideal primo y $\overline{a}, \overline{b} \in R/\mathfrak{p}$ con $\overline{ab} = \overline{0}$, entonces $ab \in \mathfrak{p}$ por lo que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, así $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$. Recíprocamente, sea $\mathfrak{p}$ un ideal tal que $R/\mathfrak{p}$ es un dominio entero, y sean $a, b \in R$ tal que $ab \in \mathfrak{p}$, entonces $\overline{ab} = \overline{0}$ por lo que $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$, así $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$ lo que implica que $\mathfrak{p}$ es un ideal primo.

II) Sea $\mathfrak{m}$ un ideal maximal y $\overline{a} \in R/\mathfrak{m}$ con $\overline{a} \neq \overline{0}$, entonces $a \notin \mathfrak{a}$. Es claro que $\langle a \rangle + \mathfrak{m}$ es un ideal de R que contiene a $\mathfrak{m}$ propiamente, como $\mathfrak{m}$ es maximal tenemos que $\langle a \rangle + \mathfrak{m} = R$ así existen $x \in R$ y $m \in \mathfrak{m}$ tal que $ax + m = 1$ por lo que $ax - 1 \in \mathfrak{m}$ lo que implica que $\overline{ax} = \overline{1}$, así $\overline{x}$ es el inverso de $\overline{a}$. Recíprocamente, sea $\mathfrak{m}$ un ideal de R e I un ideal de R que contiene propiamente a $\mathfrak{m}$, entonces existe $a \in I$ tal que $a \notin \mathfrak{m}$ por lo que $\overline{a} \in R/\mathfrak{m}$ es diferente de la clase del cero, y como $R/\mathfrak{m}$ es cuerpo existe $x \in R$ tal que $\overline{ax} = \overline{1}$ así $ax - 1 \in \mathfrak{m} \subset I$ y como $a \in I$ tenemos que $1 \in I$. Luego, $I = R$.

□

Proposición 1.1.12. *Sea* R *un anillo y* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *ideales arbitrarios, si* $\mathfrak{p}$ *es un ideal primo y* $\mathfrak{p} \supset \mathfrak{a}_1 \ldots \mathfrak{a}_n$ *entonces* $\mathfrak{p} \supset \mathfrak{a}_i$ *para algún* $i = 1, \ldots, n$.

Demostración. Sea $\mathfrak{p}$ un ideal primo de R y sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de R. Asumamos por contradicción que $\mathfrak{p} \not\supseteq \mathfrak{a}_i$ para todo $i = 1, \ldots, n$. Por lo tanto para cada $\mathfrak{a}_i$ existe un a_i tal que $a_i \notin \mathfrak{p}$ pero $a_1 a_2 \cdots a_n$ si pertenece a $\mathfrak{p}$, lo que implica que algun a_i pertenece a $\mathfrak{p}$ ya que este es un ideal primo, lo cual es una contradicción. □

A continuación mencionaremos dos tipos de dominios que serán de nuestro interés.

Definición 1.1.13. Sea R un dominio entero. Si todo ideal de R es un ideal principal decimos que R es **dominio de ideales principales**. Un dominio R es **dominio euclídeo** si existe una función $N: R \to \mathbb{N}$ con $N(0_R) = 0$ tal que dados $a, b \in R$ con $b \neq 0_R$ existen $q, r \in R$ tal que $a = qb + r$ con $r = 0_R$ o $N(r) < N(b)$.

Ejemplo 1.1.14. $\mathbb{Z}$ es un dominio euclídeo y es un dominio de ideales principales. Sabemos que $\mathbb{Z}$ es dominio entero, ahora veamos que es dominio euclídeo. Sea $N: \mathbb{Z} \to \mathbb{N}$ donde $N(x) = |x|$ para todo $x \in \mathbb{Z}$, tenemos que $N(0) = 0$. Sean $a, b \in \mathbb{Z}$ con $b \neq 0_R$ y $S = \{a - bq \mid q \in \mathbb{Z} \text{ y } a - bq \geq 0\}$. Como $S \subseteq \mathbb{N}$, $a \in S \neq \emptyset$ y $\mathbb{N}$ esta bien ordenado tenemos que S tiene mínimo. Sea r el mínimo de S, veamos que $N(r) < N(b)$. Por contradicción, supongamos que $N(r) \geq N(b) = |b|$, ya que $r \in S$ existe $q \in \mathbb{Z}$ tal que $a - bq = r$ además que $r \geq 0$ así $N(r) = r$. Ahora notemos que $b||b|$ entonces existe $m \in \mathbb{Z}$ tal que $bm = |b|$ por lo que $r - |b| = a - bq - |b| = a - b(q - m)$, como $r \geq |b|$ entonces $r - |b| = a - b(q - m) \geq 0$ por lo tanto $r - |b| \in S$ lo que contradice que r es el mínimo. Con esto concluimos que $N(r) < N(b)$, así $a = bq + r$ con $N(r) < N(b)$.

Ahora para demostrar que $\mathbb{Z}$ es dominio de ideales principales usaremos el siguiente teorema.

Teorema 1.1.15. *Todo dominio euclídeo es un dominio de ideales principales.*

Demostración. Sea R un dominio euclídeo e I un ideal de R. Si $I = \{0_R\}$ entonces es principal, si $I \neq \{0_R\}$ entonces $I - \{0_R\} \neq \emptyset$, así $N(I - \{0_R\}) \subseteq \mathbb{N}$ y es diferente de vacío por lo tanto tiene mínimo. Sea $N(x)$ el mínimo, ahora veamos que $\langle x \rangle = I$. Como I es ideal y $x \in I$ es claro que $\langle x \rangle \subseteq I$, por otro lado tomemos $a \in I$, dado que R es euclídeo existen $q, r \in R$ tal que $a = xq + r$ con $r = 0_R$ o $N(r) < N(x)$ pero esto segundo no es posible ya que $r = a - xq \in I$ y así $r = 0_R$, lo que nos deja con $a = xq \in \langle x \rangle$ completando así la prueba. □

La recíproca del Teorema 1.1.15 no es cierta, veremos un ejemplo de esto en la Sección 3 (ver Corolario 2.3.15). Ahora, generalizaremos el concepto de división en $\mathbb{Z}$ para anillos en general.

Definición 1.1.16. Sea R un anillo. Un elemento $u \in R$ **divide** a $v \in R$ si existe un elemento $w \in R$ tal que $uw = v$ y esto es denotado por $u|v$. Cuando $u|v$ y $v|u$ se dice que estos elementos son **asociados**.

En los dominios enteros tenemos la siguiente caracterización de los elementos asociados.

Proposición 1.1.17. *Sea R un dominio entero y $u, v \in R$ no nulos, u y v son asociados, si y solo si, existe $w \in U(R)$ tal que $uw = v$*

Demostración. Sean $u, v \in R$ asociados no nulos, por definición $u|v$ y $v|u$ entonces existen $a, b \in R$ tal que $ua = v$ y $vb = u$, donde reemplazando obtenemos $uab = u$, entonces $u(ab - 1) = 0$ y como R es dominio entero tenemos que $ab = 1$ y con esto $a, b \in U(R)$. Recíprocamente, sea $w \in U(R)$ tal que $uw = v$, entonces $w^{-1} \in R$ y $u = vw^{-1}$ por lo tanto $v|u$ y $u|v$ lo que implica que son asociados. □

Definición 1.1.18. Sea R un anillo, un elemento de R es llamado **irreducible** si sus únicos divisores son invertibles o asociados a él.

Ejemplo 1.1.19. Sea R un anillo y $\mathfrak{m}$ un ideal maximal de R, entonces $\mathfrak{m}$ es irreducible en R_I. En efecto sean $\mathfrak{a}, \mathfrak{b}$ ideales de R tal que $\mathfrak{ab} = \mathfrak{m}$, como $\mathfrak{a}$ es un ideal tenemos que $\mathfrak{a} \supseteq \mathfrak{ab} = \mathfrak{m}$ por lo tanto $\mathfrak{a} \supseteq \mathfrak{m}$ y como $\mathfrak{m}$ es máximal entonces $\mathfrak{a} = R$ o $\mathfrak{a} = \mathfrak{m}$, si $\mathfrak{a} = R$ entonces es invertible y si $\mathfrak{a} = \mathfrak{m}$ entonces son asociados.

1.2. Extensiones de Cuerpos

En esta sección nos enfocaremos en las extensiones de cuerpos. Empezaremos estudiando los elementos algebraicos y sus polinomios minimales para así probar que toda extensión finita de $\mathbb{Q}$ es simple, un resultado de suma importancia en este trabajo de grado.

Definición 1.2.1. Sean F y K cuerpos.

I) Decimos que K es una **extensión de cuerpos** de F si $F \subseteq K$. Esto es denotado por K/F.

II) Dada una extensión de cuerpos K/F. Denotamos por $F(\alpha)$ al menor subcuerpo de K que contiene a F y a α. Igualmente para $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ denotamos por $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ al menor subcuerpo de K que contiene a F y a $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Si K/F una extensión de cuerpos, entonces K es un F-espacio vectorial donde la suma de vectores es la suma usual en K y la multiplicación por un escalar es la multiplicación usual en K. Denotamos por $[K : F]$ a la dimensión de K como F-espacio vectorial. Si esta es finita, decimos que K/F es una **extensión finita**.

Ejemplo 1.2.2. $\mathbb{Q}(i\sqrt{5})$ es una extensión finita de $\mathbb{Q}$. En cambio $\mathbb{R}$ no lo es. Por definición $\mathbb{Q}(i\sqrt{5})$ es una extensión de cuerpos de $\mathbb{Q}$, ahora veamos que $\mathbb{Q}(i\sqrt{5})$ tiene una base finita como $\mathbb{Q}$-espacio vectorial. Sea $\mathfrak{B} = \{1, i\sqrt{5}\}$, veamos que esta es base de $\mathbb{Q}(i\sqrt{5})$. Es claro que es L.I. debido a que $i\sqrt{5}$ no es un número racional, ahora solamente nos falta ver que $\mathfrak{B}$ genera $\mathbb{Q}(i\sqrt{5})$.

Para esto primero veamos que $gen(\mathfrak{B}) = \{q_1 + q_2 i\sqrt{5} \ : \mid q_1, q_2 \in \mathbb{Q}\}$ es un cuerpo. Es claro que $0, 1 \in gen(\mathfrak{B})$ y sean $a = x + y(i\sqrt{5})$ y $b = w + z(i\sqrt{5}) \in gen(\mathfrak{B})$, con lo cual tenemos que $a - b = x - w + (y - z)(i\sqrt{5}) \in gen(\mathfrak{B})$ y también $ab^{-1} = \frac{x+y(i\sqrt{5})}{w+z(i\sqrt{5})} = \frac{(x+y(i\sqrt{5}))(w-z(i\sqrt{5}))}{w^2+5z^2} = \frac{yw-zx}{w^2+5z^2} + \frac{xw+yz}{w^2+5z^2}(i\sqrt{5}) \in gen(\mathfrak{B})$. Así $gen(\mathfrak{B})$ es un cuerpo que contiene a $\mathbb{Q}$ y a $i\sqrt{5}$ entonces por definición $\mathbb{Q}(i\sqrt{5}) \subseteq gen(\mathfrak{B})$ por lo tanto $\mathbb{Q}(i\sqrt{5}) = gen(\mathfrak{B})$ lo que implica que $\mathfrak{B}$ es su base y por ende es una extensión finita.

Por otro lado, es claro que $\mathbb{R}$ al ser cuerpo es una extensión de $\mathbb{Q}$ y por contradicción asumamos que es finita, entonces existe $\mathfrak{B} = \{r_1, r_2 \ldots, r_n\} \subseteq \mathbb{R}$ base de $\mathbb{R}$ como $\mathbb{Q}$-espacio vectorial, es decir, para todo $r \in \mathbb{R}$ existen $q_1, q_2, \ldots, q_n \in \mathbb{Q}$ tal que $r = r_1 q_1 + r_2 q_2 + \cdots + r_n q_n$ y esta representación es única, tienendo esto en cuenta podemos definir una función $f : \mathbb{Q}^n \to \mathbb{R}$ tal que $f((q_1, \ldots, q_n)) = r_1 q_1 + \cdots + r_n q_n$ la cual es biyectiva. Por lo tanto $\mathbb{R}$ sería numerable, lo que es una contradicción. Además de esto, se puede probar que la dimensión de $\mathbb{R}$ como $\mathbb{Q}$-espacio vectorial es no numerable.

Definición 1.2.3. Sea K/F una extensión de cuerpos.

I) Un elemento $\alpha \in K$ es llamado **algebraico** sobre F si existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Un número $\alpha \in \mathbb{C}$ es llamado algebraico si es algebraico sobre $\mathbb{Q}$.

II) Sea $\alpha \in K$ algebraico sobre F, entonces existe un polinomio mónico $f(x) \in F[x]$ de grado mínimo que admite a α como raíz y es llamado el **polinomio minimal** de α sobre F.

Ejemplo 1.2.4. Cualquier elemento de $\mathbb{Q}(i\sqrt{5})$ es algebraico. En efecto, sea $z \in \mathbb{Q}(i\sqrt{5})$. Como vimos en el ejemplo anterior $z = a + bi\sqrt{5}$ con $a, b \in \mathbb{Q}$ ahora considere el polinomio $p(x) = (x-a)^2 + 5b^2 \in \mathbb{Q}[x]$, note que $p(a + bi\sqrt{5}) = (a + bi\sqrt{5} - a) + 5b^2 = (bi\sqrt{5})^2 + 5b^2 = -5b^2 + 5b^2 = 0$, y al $p(x)$ ser mónico este es el polinomio minimal de $a + bi\sqrt{5}$.

Teorema 1.2.5. *Sea K/F una extensión de cuerpos y $\alpha \in K$ un número algebraico sobre*

F con polinomio minimal $p(x) \in F[x]$. Entonces dado $f(x) \in F[x]$, $f(\alpha) = 0$, si, y solo si, $p(x)|f(x)$. En particular, esto muestra que α posee un único polinomio minimal.

Demostración. Supongamos que $f(\alpha) = 0$. Por el algoritmo de la división para polinomios $f(x) = p(x)q(x) + r(x)$ con $\partial r(x) < \partial p(x)$ por lo que $f(\alpha) = p(\alpha)q(\alpha) + r(\alpha)$ así, $r(\alpha) = 0$ lo que contradeciría la minimalidad de p, a menos que $r(x)$ es el polinomio nulo lo que implica que $p(x)|f(x)$, por otro lado es claro que si $p(x)|f(x)$ entonces $f(\alpha) = 0$. Por último, sean $p(x)$ y $q(x)$ polinomios minimales de α, entonces por el anterior teorema $p(x)|q(x)$ y $q(x)|p(x)$ y como $p(x)$ y $q(x)$ son mónicos tenemos que $p(x) = q(x)$. □

Definición 1.2.6. Sea K/F una extensión de cuerpos y sea $\alpha \in K$ un número algebraico sobre F con polinomio minimal $p(x) \in F[x]$. Las raíces de $p(x)$ que pertenecen a K son llamadas los **conjugados** de α sobre K.

El siguiente ejemplo muestra que no todas las raíces del polinomio minimal de un elemento $\alpha \in \mathbb{C}$ son conjugados en cualquier extensión de $\mathbb{Q}$.

Ejemplo 1.2.7. El único conjugado de $\sqrt[3]{2}$ en $\mathbb{R}$ es si mismo. Note que el polinomio minimal de $\sqrt[3]{2}$ es $x^3 - 2$ y veamos que las otras raíces de este polinomio son $\omega\sqrt[3]{2}$ y $\overline{\omega}\sqrt[3]{2}$ donde $\omega = \frac{-1+i\sqrt{3}}{2}$. Tenemos que $\omega^3 = \frac{(-1+i\sqrt{3})^3}{8} = \frac{2(-1-1i\sqrt{3})(-1+i\sqrt{3})}{8} = \frac{2(4)}{8} = 1$, y analogamente $\overline{\omega}^3 = 1$, así $(\omega\sqrt[3]{2})^3 - 2 = \omega^3(2) - 2 = 0$ y lo mismo para $\overline{\omega}$ por lo que las otras raíces de $x^3 - 2$ son números complejos y no pertenecen a $\mathbb{R}$.

Ahora mostraremos un representación explícita de los elementos de $F(\alpha)$, cuando α es algebraico sobre F.

Teorema 1.2.8. *Sea K/F una extensión de cuerpos y sea $\alpha \in K$ un número algebraico sobre F con polinomio minimal $p(x) \in F[x]$ de grado n. Entoces*

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in F\}.$$

En particular, $[F(\alpha) : F] = n$.

Demostración. Ver [3], página 267. □

Proposición 1.2.9. *Sea L/F una extensión de cuerpos. Un número $\alpha \in L$ es algebraico si, y solo si, α pertenece a una extensión finita K de F contenida en L.*

---

[3] MOREIRA Carlos SALDANHA Nicolau TENGAN Eduardo BROCHERO Fabio. *Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro*. Terceira edição. IMPA.

Demostración. Sea $\alpha \in L$ un elemento algebraico, entonces por el teorema anterior tenemos que $F(\alpha)$ es una extensión de F contenida en L. Recíprocamente, supongamos que existe $K \subseteq L$ extensión finita de F tal que $\alpha \in K$. Como K es extensión finita de F tenemos que $[K : F] = n$ lo que implica que K es un F-espacio vectorial de dimensión n, así $1, \alpha, \alpha^2, \ldots, \alpha^n$ son linealmente dependientes, luego existen escalares no todos nulos $c_{n-1}, \ldots, c_1, c_0 \in F$ tales que $\alpha^n = c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$ por lo tanto α es raiz del polinomio no nulo $x^n - c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ el cual pertenece a $F[x]$. □

El siguiente teorema muestra que todas las extensiones finitas de $\mathbb{Q}$ son simples.

Teorema 1.2.10. *(Teorema del elemento primitivo). Sea $K/\mathbb{Q}$ una extensión finita de cuerpos. Entonces existe un elemento $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.*

Demostración. Como K es una extensión finita de $\mathbb{Q}$, entonces existen $\alpha_1, \ldots, \alpha_n \in K$ tales que estos elementos son un base de K como $\mathbb{Q}$-espacio vectorial, por lo tanto $K \supseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ debido a que $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es un cuerpo que contiene tanto a $\mathbb{Q}$ como a $\alpha_1, \ldots, \alpha_n$ además, K es una extensión de $\mathbb{Q}$ que contiene $\alpha_1, \ldots, \alpha_n$ entonces por definición $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) \supset K$, así tenemos que $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Haremos esta prueba por inducción en n, para el caso base tomemos $n = 1$, en este caso $K = \mathbb{Q}(\alpha_1)$. Antes de realizar el paso inductivo haremos el caso para $n = 2$, entonces existen $\alpha, \beta \in \mathbb{C}$ tal que $K = \mathbb{Q}(\alpha, \beta)$, tomemos $\theta = \alpha + c\beta$ con un $c \in \mathbb{Q}$ conveniente y veamos que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$, por como definimos θ es claro que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$, ahora mostremos que $\beta \in \mathbb{Q}(\theta)$.

Como α y β pertenecen a una extensión finita de $\mathbb{Q}$ entonces son algebraicos, sean $\alpha_1, \ldots, \alpha_s$ y $\beta_1, \ldots, \beta_t$ las raíces del polinomio minimal sobre $\mathbb{Q}$ de α y β respectivamente, escojamos c de modo que los números de la forma $\alpha_i + c\beta_j$ con $1 \leq i \leq s$ y $1 \leq j \leq t$ sean disjuntos dos a dos. Esto es posible ya que para que los números $\alpha_i + c\beta_j$ y $\alpha_k + c\beta_l$ sean iguales $c = \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$ (note que en el caso donde $\beta_l = \beta_j$ es claro que $\alpha_i = \alpha_j$) y como hay finitas raíces de los polinomios minimales de α y β podemos escoger un c diferente de esto.

Sean $p(x)$ y $q(x)$ los polinomios minimales de α y β respectivamente, note que β es raiz de los polinomios $p(\theta - cx), q(x) \in \mathbb{Q}(\theta)[x]$ por lo que su polinomio minimal $f(x) \in \mathbb{Q}(\theta)[x]$ los divide. Además, sea r una raiz en común de estos dos polinomios, como r es raiz de $q(x)$ entonces $r = \beta_j$ y como también r es raiz de $p(\theta - cx)$ tenemos que $\theta - cr = \theta - c\beta_j$

es una raíz del polinomio $p(x)$ luego $\theta - c\beta_j = \alpha_i$, lo que implica que $\alpha + c\beta = \alpha_i + c\beta_j$ y por la elección del c esto solo pasa si $\beta_j = \beta$ por lo tanto la única raiz en común de estos dos polinomios es β, lo que implica que la única raiz de $f(x)$ es β y $f(x)$ al ser el polinomio minimal de β sobre $\mathbb{Q}(\theta)$ debe ser $f(x) = x - \beta$ así $\beta \in \mathbb{Q}(\theta)$. Sabiendo esto es claro que $\alpha = \theta - c\beta \in \mathbb{Q}(\theta)$ por lo tanto $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. Continuando con la inducción veamos que si $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\theta)$ entonces existe θ_2 tal que $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}) = \mathbb{Q}(\theta_2)$. Sabemos que $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)(a_{n+1}) = \mathbb{Q}(\theta)(\alpha_{n+1}) = \mathbb{Q}(\theta, \alpha_{n+1})$ y por lo hecho anteriormente para $n = 2$ tenemos que $\mathbb{Q}(\theta, \alpha_{n+1}) = \mathbb{Q}(\theta_2)$. □

Note que la demostración anterior nos proporciona un método para encontrar el elemento primitivo de una extensión finita de $\mathbb{Q}$.

Ejemplo 1.2.11. El elemento primitivo de la extensión finita $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es $\sqrt{2} + \sqrt{3}$. Es claro que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, ahora veamos que $\sqrt{2}$ y $\sqrt{3}$ pertenecen a $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Sabemos que $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ es un cuerpo entonces $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$ pertenece, por lo tanto $\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ y además $\frac{1}{\sqrt{2}+\sqrt{3}} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ debido a que es cuerpo, entonces $\frac{2+\sqrt{6}}{\sqrt{2}+\sqrt{3}} = \frac{\sqrt{2}(\sqrt{2}+\sqrt{3})}{\sqrt{2}+\sqrt{3}} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ y con esto también concluimos que $\sqrt{3}$ también pertenece, así $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \supset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ lo que implica que son iguales.

1.3. Inmersiones, Traza y Norma

Definición 1.3.1. Sea $K/\mathbb{Q}$ una extensión finita de cuerpos. Una **inmersion** $\sigma : K \to \mathbb{C}$ es una función inyectiva que preserva la suma y el producto de elementos en K, esto es:

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{y} \quad \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$$

para todo $a, b \in K$.

Ejemplo 1.3.2. Solo existe una inmersión de $\mathbb{Q}$ en $\mathbb{C}$, y esta es la inclusión ($f(x) = x$). Es claro que esta función es una inmersión de $\mathbb{Q}$, veamos que es la única. Sea $\sigma : \mathbb{Q} \to \mathbb{C}$ una inmersion, primero $\sigma(0) = \sigma(0+0) = 2\sigma(0)$ por lo tanto $\sigma(0) = 0$, ahora $\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)^2$ por lo que $\sigma(1) = 0$ o $\sigma(1) = 1$ pero como σ es inyectiva tenemos que $\sigma(1) = 1$. Cuando $x \in \mathbb{Z}^+$ $\sigma(x) = \sigma(1 + \cdots + 1) = x\sigma(1) = x$, cuando $x \in \mathbb{Z}^-$ tenemos que $0 = \sigma(x - x) = \sigma(x) + \sigma(-x) = \sigma(x) - x$ por lo tanto $\sigma(x) = x$. Note que para cualquier entero no nulo x vale que $1 = \sigma\left(\frac{x}{x}\right) = \sigma(x)\sigma\left(\frac{1}{x}\right)$, así $\sigma\left(\frac{1}{x}\right) = \frac{1}{x}$ por lo que para cualquier $\frac{a}{b} \in \mathbb{Q}$ tenemos que $\sigma\left(\frac{a}{b}\right) = \sigma(a)\sigma\left(\frac{1}{b}\right) = \frac{a}{b}$.

El siguiente teorema nos dice que la cantidad de inmersiones de una extensión finita $K/\mathbb{Q}$ coincide con su dimensión.

Teorema 1.3.3. *Sea* $[K:\mathbb{Q}]=n$, *existen exactamente* n *inmersiones de* K *en* $\mathbb{C}$.

Demostración. Sea $\sigma: K \to \mathbb{C}$ una inmersión y sea $k \in K$, como K es una extensión finita de $\mathbb{Q}$, por el Teorema 1.2.10 existe $\theta \in K$ tal que $K=\mathbb{Q}(\theta)$, así $k=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$ con $a_0, a_1 \ldots, a_{n-1} \in \mathbb{Q}$ por lo que

$$\sigma(k)=\sigma(a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1})=\sigma(a_0)+\sigma(a_1)\sigma(\theta)+\cdots+\sigma(a_{n-1})\sigma(\theta)^{n-1}$$

y como vimos en el ejemplo anterior σ fija los numeros racionales, así $\sigma(k)=a_0+a_1\sigma(\theta)+\cdots+a_{n-1}\sigma(\theta)^{n-1}$ por lo que el valor de $\sigma(k)$ solo depende del valor de $\sigma(\theta)$. Ahora sea $p(x) \in \mathbb{Q}[x]$ el polinomio minimal de θ, es claro que $\sigma(p(x))=p(\sigma(x))$ por lo que reemplazando x por θ tenemos que $0=\sigma(0)=p(\sigma(\theta))$, entonces $\sigma(\theta)$ es una raiz de $p(x)$ por lo tanto la cantidad de posibles inmersiones de K a $\mathbb{C}$ es máximo n que es el grado de $p(x)$.
Ahora sea θ_i una raiz de $p(x)$, veamos que podemos definir una inmersión σ_i tal que $\sigma_i(\theta)=\theta_i$. Sea $k \in K$, sabemos que $k=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$ entonces definamos $\sigma_i(k)=a_0+a_1\theta_i+\cdots+a_{n-1}\theta_i^{n-1}$, veamos que σ_i es una inmersión. Es claro que σ_i preserva la suma, por lo tanto es un homomorfismo de grupos, así que veamos que el $\mathrm{Ker}(\sigma_i)=0$. Sea $\alpha \in K$ tal que $\sigma_i(\alpha)=0$, sabemos que $\alpha=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$ así $0=a_0+a_1\theta_i+\cdots+a_{n-1}\theta_i^{n-1}$ pero como la forma de escribir a 0 de esta manera en $\mathbb{Q}(\theta_i)$ es única, entonces $a_0=a_1=\cdots=a_{n-1}=0$ por lo tanto $\alpha=0$. Ahora solo nos falta probar que σ_i conserva el producto, sea $\beta \in K$ entonces $\beta=b_0+b_1\theta+\cdots+b_{n-1}\theta^{n-1}$, tambien $\alpha\beta=c_0+c_1\theta+\cdots+c_{n-1}\theta^{n-1}$ entonces θ es raiz del polinomio

$$f(x)=(a_0+a_1x+\cdots+a_{n-1}x^{n-1})(b_0+b_1x+\cdots+b_{n-1}x^{n-1})-(c_0+c_1x+\cdots+c_{n-1}x^{n-1})$$

por lo tanto por el Teorema 1.2.5 $p(x)|f(x)$ lo que implica que θ_i tambien es raiz de $f(x)$ así

$$(a_0+a_1\theta_i+\cdots+a_{n-1}\theta_i^{n-1})(b_0+b_1\theta_i+\cdots+b_{n-1}\theta_i^{n-1})=c_0+c_1\theta_i+\cdots+c_{n-1}\theta_i^{n-1}$$

que es lo mismo que $\sigma_i(\alpha)\sigma_i(\beta)=\sigma_i(\alpha\beta)$. Teniendo en cuenta que para cada raiz de $p(x)$ podemos definir una inmersión solo nos falta ver que todas la raíces de $p(x)$ son diferentes. Supongamos por contradicción que existe θ tal que θ no es una raiz simple,

entonces θ es raiz de $p'(x)$ lo que implica que $p(x)|p'(x)$ por el Teorema 1.2.5, lo cual es un absurdo. □

A partir de las inmersiones surgen las siguientes dos funciones que serán fundamentales en el estudio del anillo de enteros algebraicos.

Definición 1.3.4. Sea $K/\mathbb{Q}$ una extensión finita de cuerpos y $\alpha \in K$. Sean $\sigma_i : K \to \mathbb{C}$, $i = 1, \ldots, n$ todas las $n = [K : \mathbb{Q}]$ inmersiones de K en $\mathbb{C}$. La traza $Tr_{K/\mathbb{Q}}(\alpha)$ y la norma $N_{K/\mathbb{Q}}(\alpha)$ de α son definidos respectivamente por

$$Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{y} \quad N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Ejemplo 1.3.5. Sean $a, b \in \mathbb{Q}$, tenemos que $Tr_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = 2a$ y $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = a^2+b^2$. Esto es claro debido que al conjugado de $a+bi$ en $\mathbb{Q}(i)$ es $a-bi$, entonces $Tr_{\mathbb{Q}[i]/\mathbb{Q}}(a+bi) = a + bi + a - bi = 2a$ y $N_{\mathbb{Q}[i]/\mathbb{Q}}(a + bi) = (a + bi)(a - bi) = a^2 - b^2$.

A continuación enunciaremos algunas propiedades de la traza y la norma.

Proposición 1.3.6. *Sea $K/\mathbb{Q}$ una extensión finita y sean $\alpha, \beta \in K$. Tenemos que:*

I) *La traza es aditiva y la norma es multiplicativa, esto es:*

$$Tr_{K/\mathbb{Q}}(\alpha + \beta) = Tr_{K/\mathbb{Q}}(\alpha) + Tr_{K/\mathbb{Q}}(\beta)$$

$$N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$$

II) $Tr_{K/\mathbb{Q}}(\alpha)$ *y* $N_{K/\mathbb{Q}}(\alpha)$ *son números racionales.*

III) *Sea $T_\alpha : K \to K$ la transformación $\mathbb{Q}$-lineal dada por la multiplicación por α, entonces $Tr_{K/\mathbb{Q}}(\alpha)$ y $N_{K/\mathbb{Q}}(\alpha)$ son respectivamente la traza y el determinante de T_α.*

Demostración. Ver [3], página 272. □

2. El grupo de clase de un anillo de enteros algebraicos

En este capítulo se presentan los principales resultados de este trabajo de grado, empezaremos definiendo un entero algebraico y con este el anillo de enteros algebraicos. Luego, mencionaremos algunas propiedades de los ideales de este anillo y de como la colección de estos tiene factorización única en ideales primos ayudándonos de los ideales fraccionarios. Por último, definiremos el grupo de clase de un anillo de enteros algebraicos y estudiaremos su cardinalidad, para así ver algunas de sus aplicaciones más importantes en la teoría algebraica de números.

2.1. Enteros Algebraicos

Dada $K/\mathbb{Q}$ una extensión finita, definiremos una colección de elementos de K que cumplan propiedades similares a las que cumple $\mathbb{Z}$ respecto a $\mathbb{Q}$. Probaremos que está colección es una extensión de anillo de $\mathbb{Z}$ y que puede generarse con una base de K tomando sus $\mathbb{Z}$-combinaciones. Dicha base es conocida como una base entera.

Definición 2.1.1. Sean R y S anillos. Decimos que S es una **extensión de anillo** de R si $R \subseteq S$. Sea $\alpha \in S$, denotamos $R[\alpha]$ al menor subanillo de S que contiene a R y a α; es decir, $R[\alpha]$ consiste de todos los polinomios sobre R evaluados en α. Analogamente para $\alpha_1, \alpha_2, \ldots, \alpha_n \in S$ denotamos por $R[\alpha_1, \alpha_2, \ldots, \alpha_n]$ el menor subanillo de S que contiene a R y al conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Ejemplo 2.1.2. El conjunto $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{C}$ y es una extensión de anillo de $\mathbb{Z}$. Es claro que $\mathbb{Z} \subseteq R$ ya que para todo $z \in \mathbb{Z}$ este se puede escribir como $z + 0i$ el cual pertenece a R. Ahora veamos que R es un subanillo de $\mathbb{C}$, y más aún, $R = \mathbb{Z}[i]$. Sabemos que $0 = 0 + 0i \in R$, y sean $a + bi, c + di \in R$, tenemos que $a + bi + c + di = a + c + (b + d)i \in R$ y también $(a + bi)(c + di) = ac - bd + (ad + bc)i \in R$. Como R es un anillo que contiene a $\mathbb{Z}$ y también $i \in R$, entonces por definición $\mathbb{Z}[i] \subseteq R$ y sea $a + bi \in R$, tenemos que $a, b, i \in \mathbb{Z}[i]$ por lo tanto $a + bi \in \mathbb{Z}[i]$ ya que $\mathbb{Z}[i]$ es anillo. Este anillo R es más conocido como el anillo de los enteros gaussianos.

Definición 2.1.3. Sea B una extensión de anillo de A. Un elemento $\theta \in B$ es llamado **entero** sobre A si es la raíz de un polinomio mónico sobre $A[x]$. Un número complejo θ que es entero sobre $\mathbb{Z}$ es llamado **entero algebraico.**

Ejemplo 2.1.4. Todo elemento de $\mathbb{Z}[i]$ es entero algebraico.

Demostración. Sea $a+bi \in \mathbb{Z}[i]$ es claro que $p(x) = (x-a)^2+b^2 = x^2-2ax+a^2+b^2 \in \mathbb{Z}[x]$ y es mónico, además $p(a+bi) = (a+bi-a)^2+b^2 = (bi)^2+b^2 = 0$. Por lo tanto cualquier entero gaussiano es un entero algebraico. □

Definición 2.1.5. Sea B una extensión de anillo de A. Se dice que B es una extensión **finita** de A si existen elementos $\omega_1, \omega_2, \ldots, \omega_n \in B$ tales que cualquier elemento de B se escribe como combinación A-$lineal$ de los ω_i, esto es:

$$B = A\omega_1 + \cdots + A\omega_n \overset{\text{def}}{=} \{a_1\omega_1 + \cdots + a_n\omega_n \mid a_i \in A\}$$

Ejemplo 2.1.6. Si θ es un entero algebraico, entonces $\mathbb{Z}[\theta]$ es una extensión finita de $\mathbb{Z}$. Sea $R = \{\partial p(x) \mid p(\theta) = 0$ y $p \in \mathbb{Z}[x]$ mónico$\}$, es claro que $R \subseteq \mathbb{N}$ y es no vacío ya que θ es un entero algebraico, por lo tanto tiene minimo, llamemos n a ese mínimo. Con este n probemos que:

$$\mathbb{Z}[\theta] = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$$

Para esto veamos que $\mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$ es un subanillo de $\mathbb{C}$. Es claro que los elementos de este anillo pueden verse como $f(\theta)$ con $f(x) \in \mathbb{Z}[x]$ y $\partial f(x) < n$. Sean $f(x), g(x) \in \mathbb{Z}[x]$ con $\partial f(x) < n$ y $\partial g(x) < n$, note que $f(x) - g(x) \in \mathbb{Z}[x]$ y $\partial(f-g)(x) = \text{máx}\{\partial f(x), \partial g(x)\} < n$ por lo tanto $f(\theta) - g(\theta) \in \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$.

Ahora veamos que $\theta^i \in \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$ para todo $i \geq n$ por inducción. Para el caso $i = n$, recordemos que existe $p(x) \in \mathbb{Z}[x]$ mónico con $\partial p(x) = n$ tal que $p(\theta) = 0$, como $p(x)$ es mónico tenemos que $p(x) = x^n + \widetilde{p}(x)$ con $\partial\widetilde{p}(x) = n-1$, así evaluando θ en $p(x)$ obtenemos $0 = p(\theta) = \theta^n + \widetilde{p}(\theta)$ por lo tanto $\theta^n = -\widetilde{p}(\theta) \in \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$. Supongamos que $\theta^k = f(\theta)$ con $\partial f(x) < n$, veamos que $\theta^{k+1} = g(\theta)$ con $\partial g(x) < n$, sabemos que $\theta^{k+1} = \theta f(\theta)$ y si $\partial f(x) < n-1$ entonces $xf(x)$ es un polinomio con grado menor que n por lo que solo nos falta ver el caso cuando $\partial f(x) = n-1$. En este caso $\theta f(\theta) = a_n\theta^n + \widetilde{f}(\theta)$ con $\widetilde{f}(x)$ un polinomio de grado menor que n, así $\theta^{k+1} = \theta f(\theta) = a_n(-\widetilde{p}(\theta)) + \widetilde{f}(\theta) \in \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$. Con esto podemos ver que $f(\theta)g(\theta) = \sum_{i=0}^{m} a_i\theta^i \in \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$ debido a que cada $a_i\theta^i$ pertenece y como la suma de estos también pertenece entonces $f(\theta)g(\theta) \in \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$. Teniendo en cuenta que $\mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$ es un anillo que contiene a $\mathbb{Z}$ y a θ entonces $\mathbb{Z}[\theta] \subseteq \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$, la otra contenencia se sigue de que $\mathbb{Z}[\theta]$ es un anillo y con

esto concluimos lo deseado.

A continuación mostraremos una caracterización de los enteros de una extensión de anillos.

Teorema 2.1.7. *Sea A un anillo con unidad y C una extensión de anillo de A.*

I) *Un elemento $\theta \in C$ es entero sobre A si, y solamente si, θ pertenece a una subextensión finita B de C; es decir, $\theta \in B$ donde B es un subanillo de C que además, B es una extensión finita de A.*

II) *El subconjunto de C formado por todos los elementos enteros sobre A es un subanillo de C.*

Demostración. I) Sea $\theta \in C$, considere $A[\theta]$ y note que análogamente como en el Ejemplo 2.1.6 podemos mostrar que $A[\theta]$ es una extensión finita de A contenida en C. Para la recíproca, sea $B \subseteq C$ una extensión finita de anillo de A con $\theta \in B$. Ya que B es una extensión finita de A existen $\omega_1, \omega_2 \ldots, \omega_n$ tal que $B = A\omega_1 + A\omega_2 \cdots + A\omega_n$ como $\theta \in B$ entonces $\theta\omega_i \in B$ para todo $i = 1, \ldots, n$ así existen $a_{ij} \in A$ tal que

$$\theta\omega_1 = a_{11}\omega_1 + a_{12}\omega_2 \cdots + a_{1n}\omega_n$$

$$\theta\omega_2 = a_{21}\omega_1 + a_{22}\omega_2 \cdots + a_{2n}\omega_n$$

$$\vdots$$

$$\theta\omega_n = a_{n1}\omega_1 + a_{n2}\omega_2 \cdots + a_{nn}\omega_n$$

que reescribiendolo tenemos

$$(\theta - a_{11})\omega_1 - a_{12}\omega_2 \cdots - a_{1n}\omega_n = 0$$

$$-a_{21}\omega_1 + (\theta - a_{22})\omega_2 \cdots - a_{2n}\omega_n = 0$$

$$\vdots$$

$$-a_{n1}\omega_1 - a_{n2}\omega_2 \cdots + (\theta - a_{nn})\omega_n = 0$$

y tomando la matriz $M = (a_{ij})$ podemos decir que el vector $\omega = (\omega_1, \omega_2, \ldots, \omega_n)^T$ es solución al sistema de ecuaciones homogéneo con matriz de coeficientes $I_n\theta - M$, y debido a que ω es un vector no nulo tenemos que el sistema homogéneo

tiene solución no trivial, así que $\det(I_n\theta - M) = 0$. El polinomio $p(x) = \det(I_n x - M)$ se conoce como polinomio caracteristico de M y claramente es mónico y sus coeficientes pertenecen a A, además por lo anterior tenemos que $p(\theta) = 0$, por lo tanto θ es entero.

II) Sean α, β enteros sobre A, entonces existen polinomios mónicos de grado mínimo n y m respectivamente para los cuales ellos son raiz, así analogamente como en el Ejemplo 2.1.6 podemos demostrar que $A[\alpha, \beta]$ es una extensión finita de A, más especificamente

$$A[\alpha, \beta] = \left\{ \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij}\alpha^i\beta^j \mid a_{ij} \in A \right\}$$

y por el ítem anterior podemos concluir que todo elemento de una extensión finita es entero, en particular $\alpha - \beta$ y $\alpha\beta$. Luego, el conjunto de todos los enteros es subanillo.

□

Definición 2.1.8. Sea $K/\mathbb{Q}$ una extension de cuerpos. Denotamos por $\mathcal{O}_K$ el conjunto de todos los enteros algebraicos que pertenecen a K, esto es:

$$\mathcal{O}_K = \{z \in K \mid (\exists f \in \mathbb{Z}[x])(f(z) = 0) \text{ con } f \text{ mónico y no nulo } \}$$

Por el teorema anterior se sigue que $\mathcal{O}_K$ es subanillo de K.

Ejemplo 2.1.9. El anillo de todos los enteros algebraicos que pertenecen a $\mathbb{Q}$ es $\mathbb{Z}$. Esto es $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Es claro que todo entero α también es entero algebraico ya que α es raíz del polinomio $x - \alpha$, por lo que solo hace falta probar que todo entero algebraico racional es entero. Sea $\frac{a}{b} \in \mathbb{Q}$ con $b \neq 0$ entero algebraico, sin perdida de generalidad supongamos que a y b son primos relativos. Como $\frac{a}{b} \in \mathbb{Q}$ es entero algrebracio existe $p(x) \in \mathbb{Z}[x]$ mónico tal que $\frac{a}{b} \in \mathbb{Q}$ es raíz, así:

$$\left(\frac{a}{b}\right)^n + p_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + p_1\left(\frac{a}{b}\right) + p_0 = 0$$

luego de multiplicar por b^n tenemos que:

$$a^n = -ba^{n-1}p_{n-1} - \cdots - b^{n-1}ap_1 + b^n p_0$$

$$a^n = b(-a^{n-1}p_{n-1} - \cdots - b^{n-2}ap_1 + b^{n-1}p_0)$$

por lo que $b|a^n$. Ahora si $|b| > 1$ entonces existe un primo $p|b$ y por transitividad $p|a^n$ lo que implica que $p|a$ así a y b no son coprimos lo cual es una contradicción, asi $b = 1$ o $b = -1$ y con esto $\frac{a}{b} \in \mathbb{Z}$.

Teorema 2.1.10. *Sea $K/\mathbb{Q}$ una extensión finita de cuerpos y $\theta \in \mathcal{O}_K$. Entonces $Tr_{K/\mathbb{Q}}(\theta) \in \mathbb{Z}$ y $N_{K/\mathbb{Q}}(\theta) \in \mathbb{Z}$.*

Demostración. Sean $\theta \in \mathcal{O}_K$, $p(x)$ un polinomio mónico con coeficientes enteros para el cual θ es raíz y $\sigma_i : K \to \mathbb{C}$ con $i = 1, \ldots, n$ las inmersiones de K en $\mathbb{C}$. Es claro que $0 = \sigma_i(p(\theta)) = p(\sigma_i(\theta))$ por lo tanto todos los $\sigma_i(\theta)$ son enteros algebraicos, por lo que $Tr_{K/\mathbb{Q}}(\theta)$ y $N_{K/\mathbb{Q}}(\theta)$ también lo son al ser suma y producto de enteros algebraicos respectivamente, además por la Proposición 1.3.6 tanto la traza como la norma son racionales así que pertenecen a $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. □

Es natural preguntarse si $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$, para todo α algebraico sobre $\mathbb{Q}$. El siguinte teorema nos muestra que esto no es cierto.

Teorema 2.1.11. *Sea d un entero libre de cuadrados. Entonces el anillo de enteros algebraicos de $\mathbb{Q}(\sqrt{d})$ es*

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

Demostración. Primero debemos recordar lo siguiente, si z es un entero par entonces $z^2 \equiv 0 (\text{mód} 4)$ y si z es un entero impar $z^2 \equiv 1 (\text{mód} 4)$. Teniendo esto en cuenta veamos primero el caso cuando $d \equiv 2, 3 (\text{mód} 4)$. Es fácil ver que todo elemento de $\mathbb{Q}(\sqrt{d})$ puede escribirse como $a+b\sqrt{d}$ con $a, b \in \mathbb{Q}$ entonces solo falta mostrar que si $a+b\sqrt{d}$ es un entero algebraico entonces $a, b \in \mathbb{Z}$. Es claro que $Tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a+b\sqrt{d}) = (a+b\sqrt{d})+(a-b\sqrt{d}) = 2a$ y $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$, además por el teorema anterior sabemos que $z_1 = 2a \in \mathbb{Z}$ y $z_2 = a^2 - b^2 d \in \mathbb{Z}$ entonces $z_1^2 - 4z_2 = (2b)^2 d \in \mathbb{Z}$. Adicionalmente, tenemos que $2b \in \mathbb{Q}$ por lo que existen $x, y \in \mathbb{Z}$ coprimos tales que $\frac{x}{y} = 2b$ y como $\left(\frac{x}{y}\right)^2 d \in \mathbb{Z}$ tenemos que $y^2|dx^2$ pero x, y son coprimos entonces $y^2|d$ pero d es libre de cuadrados así que $y = 1$ o $y = -1$ lo que implica que $z_3 = 2b \in \mathbb{Z}$. Volviendo a la ecuación $z_1^2 - 4z_2 = z_3^2 d$ podemos aplicar módulo 4 lo que nos deja con las ecuaciones $z_1^2 \equiv 2z_3^2 (\text{mód} 4)$ y $z_1^2 \equiv 3z_3^2 (\text{mód} 4)$ para $d \equiv 2, 3 (\text{mód} 4)$ respectivamente, así que por lo visto al inicio ambas ecuaciones solo tienen solución cuando $z_1^2 \equiv z_3^2 \equiv 0 (\text{mód} 4)$ por lo tanto z_1 y z_3 son números pares entonces $a = \frac{z_1}{2} \in \mathbb{Z}$ y $b = \frac{z_3}{2} \in \mathbb{Z}$.

Para cuando $d \equiv 1(\text{mód}4)$, primero veamos que cualquier elemento de $\mathbb{Q}(\sqrt{d})$ puede escribirse como $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ con a, b en $\mathbb{Q}$. Sea $x + y\sqrt{d}$ con $x, y \in \mathbb{Q}$ tome $b = 2y$ y $a = x - y$, es claro que $x + y\sqrt{d} = a + b\left(\frac{1+\sqrt{d}}{2}\right)$. Como cualquier elemento de $\mathbb{Q}(\sqrt{d})$ puede escribirse como $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ con $a, b \in \mathbb{Q}$ entonces solo falta probar que si $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ es un entero algebraico entonces $a, b \in \mathbb{Z}$. Note que $Tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\left(\frac{1+\sqrt{d}}{2}\right)) = Tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}) = 2a + b$ y $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\left(\frac{1+\sqrt{d}}{2}\right)) = N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}) = a^2 + ab + \frac{b^2}{4} - \frac{b^2 d}{4}$ y nuevamente por el teorema anterior sabemos que $z_1 = 2a + b \in \mathbb{Z}$ y $z_2 = a^2 + ab - \frac{b^2(d-1)}{4} \in \mathbb{Z}$, entonces $z_1^2 - 4z_2 = b^2 d \in \mathbb{Z}$, sabemos que $b \in \mathbb{Q}$ por lo que existen $x, y \in \mathbb{Z}$ coprimos tales que $\frac{x}{y} = b$ y como $\left(\frac{x}{y}\right)^2 d \in \mathbb{Z}$ tenemos que $y^2 | dx^2$ pero x, y son coprimos entonces $y^2 | d$ pero d es libre de cuadrados así que $y = 1$ o $y = -1$ lo que implica que $b \in \mathbb{Z}$ y volviendo a la ecuación $z_1^2 - 4z_2 = b^2 d$ podemos aplicar módulo 4 lo que nos deja con $z_1^2 \equiv b^2 (\text{mód}4)$ ya que $d \equiv 1(\text{mód}4)$ lo que implica que z_1 y b tienen la misma paridad por lo que $z_1 - b = 2a$ es un número par, así $a = \frac{2a}{a} \in \mathbb{Z}$. □

Ejemplo 2.1.12. El anillo de todos los elementos algebraicos que pertenecen a $\mathbb{Q}(i\sqrt{5})$ es $\mathbb{Z}[i\sqrt{5}]$. En efecto, como -5 es libre de cuadrados y $-5 \equiv 3(\text{mód}4)$, entonces por el teorema anterior se sigue que $\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \mathbb{Z}[i\sqrt{5}]$.

Es bien conocido que para cualquier número racional a existe un número entero b tal que ab sea entero, mostraremos ahora la generalización de este hecho.

Lema 2.1.13. *Sea θ un número algebraico, existe un entero $a \in \mathbb{Z} \setminus \{0\}$ tal que $a\theta$ es un entero algebraico.*

Demostración. Sea θ un número algebraico entonces existen $\frac{a_0}{b_0}, \frac{a_1}{b_1}, \ldots, \frac{a_{n-1}}{b_{n-1}} \in \mathbb{Q}$ tales que $\theta^n + \frac{a_{n-1}}{b_{n-1}}\theta^{n-1} + \cdots + \frac{a_1}{b_1}\theta + \frac{a_0}{b_0} = 0$ por lo que multiplicando por $b_0 b_1 \ldots b_{n-1}$ tenemos que $c_n\theta^n + \cdots + c_1\theta + c_0 = 0$ con $c_0, c_1, \ldots, c_n \in \mathbb{Z}$ y multiplicando todo por c_n^{n-1} obtenemos $(c_n\theta)^n + c_{n-1}(c_n\theta)^{n-1} + \cdots + c_0 c_n^{n-1} = 0$. Luego, $c_n\theta$ es un entero algebraico. □

Mostraremos que $\mathcal{O}_K$ es generado por un base K como $\mathbb{Q}$ al tomarse sus $\mathbb{Z}$-combinaciones. Para esto usaremos los siguientes dos lemas.

Lema 2.1.14. *Sean $\omega_1, \ldots, \omega_n$ y $\tau_1, \ldots \tau_n$ bases de K sobre $\mathbb{Q}$ y sea $C = (c_{ij})$ la matriz de cambio de base:*

$$\omega_i = c_{i1}\tau_1 + \cdots + c_{in}\tau_n \quad i = 1, \ldots, n.$$

Sean $\Delta(\omega_1, \ldots, \omega_n) = \det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j))$ *y* $\Delta(\tau_1, \ldots, \tau_n) = \det(Tr_{K/\mathbb{Q}}(\tau_i\tau_j))$ *los discriminantes de las dos bases. Entonces*

$$\Delta(\omega_1, \ldots, \omega_n) = \Delta(\tau_1, \ldots, \tau_n)(\det C)^2$$

y ambos discriminantes son no nulos.

Demostración. Sean $\sigma_i : K \to \mathbb{C}$ las inmersiones de K en $\mathbb{C}$. Considere la matriz $\delta(\omega_1, \ldots, \omega_n) = (\sigma_j(\omega_i))$. Multiplicando por la transpuesta obtenemos que el término i, j-ésimo de la matriz $\delta(\omega_1, \ldots, \omega_n)\delta(\omega_1, \ldots, \omega_n)^T$ es:

$$\sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i\omega_j) = Tr_{K/\mathbb{Q}}(\omega_i\omega_j),$$

lo que implica que $\delta(\omega_1, \ldots, \omega_n)\delta(\omega_1, \ldots, \omega_n)^T = (Tr_{K/\mathbb{Q}}(\omega_i\omega_j))$ Igualmente tenemos que

$$\delta(\omega_1, \ldots, \omega_n) = \left(\sum_{k=1}^{n} c_{ik}\sigma_j(\tau_k)\right) = C \cdot \delta(\tau_1, \ldots, \tau_n)$$

Asimismo,

$$\Delta(\omega_1, \ldots, \omega_n) = \det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j)) = \det(\delta(\omega_1, \ldots, \omega_n))^2 = (\det C)^2 \det(\delta(\tau_1, \ldots, \tau_n))^2$$

$$= \Delta(\tau_1, \ldots, \tau_n)(\det C)^2$$

Solo hace falta ver que los discriminantes son no nulos, para esto es claro que solo necesitamos demostrarlo para una base en específico. Sabemos que $K = \mathbb{Q}(\theta)$ para algún $\theta \in K$ y por lo tanto $1, \theta, \ldots, \theta^{n-1}$ es una base de K sobre $\mathbb{Q}$. Siendo $\theta_i = \sigma_i(\theta)$ los conjugados de θ en $\mathbb{C}$, tenemos que

$$\delta(1, \theta, \ldots, \theta^{n-1}) = ((\theta_j)^{i-1})$$

y esta matriz es una matriz de Vandermonde, que por inducción se puede demostrar que su determinante sigue la siguiente formula

$$\det(\delta(1, \theta, \ldots, \theta^{n-1})) = \prod_{1=i<j=n} (\theta_j - \theta_i).$$

Es claro que es no nulo debido a que los conjugados son distintos dos a dos y por lo tanto

$\Delta(1, \theta, \ldots, \theta^{n-1}) = \det(\delta(1, \theta, \ldots, \theta^{n-1}))^2$ es no nulo. □

Lema 2.1.15. *Sean $n = [K : \mathbb{Q}]$. Entonces existe una base de $\omega_1, \ldots, \omega_n$ de K sobre $\mathbb{Q}$ y un entero $D \in \mathbb{Z}$ no nulo tal que:*

$$\mathbb{Z} \cdot \omega_1 + \cdots + \mathbb{Z} \cdot \omega_n \subset \mathcal{O}_K \subset \mathbb{Z} \cdot \frac{\omega_1}{D} + \cdots + \mathbb{Z} \cdot \frac{\omega_n}{D}.$$

Demostración. Sea $\omega_1, \ldots, \omega_n$ una base de K sobre $\mathbb{Q}$, es claro que los ω_i son algebraicos ya que pertenecen a una extensión finita de $\mathbb{Q}$ y por lo tanto para cada ω_i existe un $a_i \neq 0$ tal que $a_i\omega_i \in \mathcal{O}_K$, y estos $a_i\omega_i$ siguen formando una base de K ya que sigue teniendo la misma dimensión y como los $a_i \neq 0$ son linealmente independientes.

De esta forma podemos considerar una base $\omega_1, \ldots, \omega_n$ de K sobre $\mathbb{Q}$ contenida en $\mathcal{O}_K$. Como $\mathcal{O}_K$ es un anillo tenemos que $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n \subset \mathcal{O}_K$. Por otro lado, sea $\alpha \in \mathcal{O}_K$ como los ω_i forman una base de K sobre $\mathbb{Q}$ tenemos que $\alpha = a_1\omega_1 + \cdots a_n\omega_n$, multiplicando por ω_i y sacando trazas obtenemos

$$Tr_{K/\mathbb{Q}}(\alpha\omega_1) = a_1 Tr_{K/\mathbb{Q}}(\omega_1\omega_1) + \cdots + a_n Tr_{K/\mathbb{Q}}(\omega_1\omega_n)$$

$$Tr_{K/\mathbb{Q}}(\alpha\omega_2) = a_1 Tr_{K/\mathbb{Q}}(\omega_2\omega_1) + \cdots + a_n Tr_{K/\mathbb{Q}}(\omega_2\omega_n)$$

$$\vdots$$

$$Tr_{K/\mathbb{Q}}(\alpha\omega_n) = a_1 Tr_{K/\mathbb{Q}}(\omega_n\omega_1) + \cdots + a_n Tr_{K/\mathbb{Q}}(\omega_n\omega_n)$$

Note que los $\alpha\omega_i$ y los $\omega_i\omega_j$ son enteros algebraicos por lo tanto todas las trazas son números enteros. Asimismo, el determinante $D = \det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j)) = \Delta(\omega_1, \ldots, \omega_n) \in \mathbb{Z}$ y como vimos en el Lema 2.1.14 este discriminante es diferente de cero, así la matriz de coeficientes del sistema de ecuaciones es invertible por lo tanto podemos usar la regla de Cramer para obtener que $a_i \in \mathbb{Z}\frac{1}{D}$; luego $\mathcal{O}_K \subset \mathbb{Z} \cdot \frac{\omega_1}{D} + \cdots + \mathbb{Z} \cdot \frac{\omega_n}{D}$. □

Teorema 2.1.16. *(Base Entera). Sea $n = [K : \mathbb{Q}]$. Entonces existe una base de K sobre $\mathbb{Q}$ $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ tal que:*

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n,$$

es decir, cualquier entero algebraico en $\mathcal{O}_K$ se escribe de manera única como combinación lineal de los ω_i con coeficientes en $\mathbb{Z}$.

Demostración. Por el lema anterior sabemos que existe una base $\tau_1, \ldots, \tau_n \in \mathcal{O}_K$ de K

sobre $\mathbb{Q}$ y un entero positivo D tal que

$$\mathbb{Z}\cdot\tau_1+\cdots+\mathbb{Z}\cdot\tau_n\subset\mathcal{O}_K\subset\mathbb{Z}\cdot\frac{\tau_1}{D}+\cdots+\mathbb{Z}\cdot\frac{\tau_n}{D}.$$

Definamos para $i=1,\ldots,n$

$$N_i=\left\{a_i\frac{\tau_i}{D}+\cdots+a_n\frac{\tau_n}{D}\in\mathcal{O}_K\mid a_i,a_{i+1},\ldots,a_n\in\mathbb{Z}\right\}$$

Note que $\tau_i=D\frac{\tau_i}{D}\in N_i$ y por lo tanto el conjunto $\{a_i\in\mathbb{N}\mid a_i\frac{\tau_i}{D}+\cdots+a_n\frac{\tau_n}{D}\in N_i\}\neq\emptyset$, así podemos escoger un $\omega_i\in N_i$ tal que a_i sea mínimo. Vamos a mostrar que los elementos ω_i obtenidos de estan manera generan $\mathcal{O}_K$ sobre $\mathbb{Z}$

Sea $\beta\in\mathcal{O}_K$, entonces $\beta=b_1\frac{\tau_1}{D}+\cdots+b_n\frac{\tau_n}{D}\in N_1$ con $b_i\in\mathbb{Z}$. Sea a_1 el coeficiente de $\frac{\tau_1}{D}$ en ω_1, dividiendo b_1 por a_1 obtenemos cociente q_1 y residuo r_1, así $b_1=a_1q_1+r_1$ con $0\leq r_1<a_1$. Como $\mathcal{O}_K$ es un anillo tenemos que $\beta-q_1\omega_1\in N_1$ y el coeficiente de $\frac{\tau_1}{D}$ de este elemento es r_1 entonces por la minimalidad de a_1 tenemos que $r_1=0$ de modo que $\beta-q_1\omega_1\in N_2$. Análogamente para este elemento obtenemos $q_2\in\mathbb{Z}$ tal que $\beta-q_1\omega_1-q_2\omega_2\in N_3$ y asi sucesivamente hasta que finalmente obtenemos $\beta-q_1\omega_1-\cdots-q_n\omega_n=0$ lo que implica que β es una combinación $\mathbb{Z}$-lineaL de los ω_i. Por tanto,

$$\mathcal{O}_K=\mathbb{Z}\omega_1+\cdots+\mathbb{Z}\omega_n.$$

Ahora veamos que estos ω_i son una base de K sobre $\mathbb{Q}$. Sea $\theta\in K$, como θ es un número algebraico existe un $a\in\mathbb{Z}$ tal que $a\theta\in\mathcal{O}_K$ y por lo tanto $a\theta=a_1\omega_1+\cdots+a_n\omega_n$. Dividiendo por a obtenemos $\theta=\frac{a_1}{a}\omega_1+\cdots+\frac{a_n}{a}\omega_n$ lo que implica que los ω_i generan K y como son n elementos forman una base de K sobre $\mathbb{Q}$. Con esto podemos darnos cuenta que cualquier elemento de $\mathcal{O}_K$ se escribe de manera única como combinaciones $\mathbb{Z}$-lineales de los ω_i. □

Corolario 2.1.17. *Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$ entonces $\mathfrak{a}$ tiene una base entera.*

Demostración. Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$, entonces existe α no nulo tal que $\alpha\in\mathfrak{a}$, veamos que existe un $b\in\mathbb{Z}$ tal que $b\in\mathfrak{a}$. Como α es no nulo entonces existe $\alpha^{-1}\in K$ el cuál como pertenece a una extensión finita de $\mathbb{Q}$ es un número algebraico por lo que existe un entero b no nulo tal que $b\alpha^{-1}\in\mathcal{O}_K$ y así $b=\alpha b\alpha^{-1}\in\mathfrak{a}$. Considere $\omega_1,\ldots,\omega_n$ una base entera de $\mathcal{O}_K$, es claro que $b\omega_1,\ldots,b\omega_n$ es una base de K como $\mathbb{Q}$ espacio vectorial ya que son n y al b ser no nulo siguen siendo linealmente independientes. Teniendo esto

en cuenta obtenemos que

$$\mathbb{Z}b\omega_1 + \cdots + \mathbb{Z}b\omega_n \subset \mathfrak{a} \subset \mathbb{Z}\frac{b\omega_1}{b} + \cdots + \mathbb{Z}\frac{b\omega_n}{b} = \mathcal{O}_K$$

Note que $\mathfrak{a}$ cumple las condiciones que cumplía $\mathcal{O}_K$ para demostrar el Teorema 2.1.16 entonces siguiendo la misma demostración definimos

$$M_i = \{a_i\omega_i + \cdots + a_n\omega_n \in \mathfrak{a} \mid a_i, a_{i+1}, \ldots, a_n \in \mathbb{Z}\}$$

entonces podemos escoger $\tau_i \in M_i$ tal que

$$\mathfrak{a} = \mathbb{Z}\tau_1 + \cdots + \mathbb{Z}\tau_n$$

donde $\tau_1, \ldots, \tau_n$ es una base de K sobre $\mathbb{Q}$. □

Observación 2.1.18. El corolario anterior implica que todo ideal de $\mathcal{O}_K$ es finitamente generado.

2.2. Factorización única en ideales primos

El objetivo principal de esta sección es probar la factorización única de los ideales de $\mathcal{O}_K$ en ideales primos. Para esto probaremos un par de propiedades de $\mathcal{O}_K$ y definiremos los ideales fracciones quienes serán la herramienta principal para lograr este objetivo.

Proposición 2.2.1. *El anillo $\mathcal{O}_K$ es integralmente cerrado en K; es decir, si θ es entero sobre $\mathcal{O}_K$, entonces $\theta \in \mathcal{O}_K$.*

Demostración. Sea $\theta \in K$ un entero sobre $\mathcal{O}_K$, entonces $\mathcal{O}_K[\theta]$ es una extensión finita de $\mathcal{O}_K$ y como $\mathcal{O}_K$ es una extensión finita de $\mathbb{Z}$, tenemos que $\mathcal{O}_K[\theta]$ es una extensión finita de $\mathbb{Z}$ y como θ pertenece a ella entonces θ es un entero algebraico. □

Proposición 2.2.2. *Sea R un anillo. Entonces son equivalentes las siguientes condiciones:*

I) *Todo ideal $\mathfrak{a}$ de R es finitamente generado.*

II) *Toda cadena ascendente de ideales estabiliza, esto es, dada una cadena de ideales*

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$$

entonces $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ *para un* i *suficientemente grande.*

III) *Todo conjunto no vacío* $\mathcal{I}$ *de ideales de* R *posee un ideal* $\mathfrak{a}$ *que es maximal en* $\mathcal{I}$ *con relación a la inclusión; es decir, si* $\mathfrak{b} \in \mathcal{I}$ *y* $\mathfrak{b} \supseteq \mathfrak{a}$ *entonces* $\mathfrak{b} = \mathfrak{a}$.

Demostración. Primero veamos que 1 y 2 son equivalentes. Sea R un anillo tal que todo ideal $\mathfrak{a}$ es finitamente generado y sea $\mathfrak{a}_i$ una cadena ascendente de ideales. Tome $\mathfrak{a} = \bigcup_{i\geq 0} \mathfrak{a}_i$, afirmamos que $\mathfrak{a}$ es un ideal. En efecto, sean $a, b \in \mathfrak{a}$ y $r \in R$ entonces existe un i suficientemente grande tal que $a, b \in \mathfrak{a}_i$ y como $\mathfrak{a}_i$ es un ideal tenemos que $a + b \in \mathfrak{a}_i \subset \mathfrak{a}$ y $ra \in \mathfrak{a}_i \subset \mathfrak{a}$. Como $\mathfrak{a}$ es un ideal de R entonces es finitamente generado y por lo tanto sean $a_1, \ldots, a_n$ los generadores de $\mathfrak{a}$. Como R tiene unidad $a_1, \ldots, a_n \in \mathfrak{a}$ por lo que existe un i_0 tal que $a_1, \ldots, a_n \in \mathfrak{a}_{i_0}$ y así $\mathfrak{a}_{i_0} = \mathfrak{a}$, lo que implica que $\mathfrak{a}_{i_0} = \mathfrak{a}_{i_0+1}$. Recíprocamente, sea $\mathfrak{a}$ un ideal de R y tome $a_1 \in \mathfrak{a}$. Si $\langle a_1 \rangle \neq \mathfrak{a}$, tome $a_2 \in \mathfrak{a} \setminus \langle a_1 \rangle$, si $\mathfrak{a} \neq \langle a_1, a_2 \rangle$ tome $a_3 \in \mathfrak{a} \setminus \langle a_1, a_2 \rangle$. Siguiendo este mismo procedimiento obtenemos la cadena

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \cdots,$$

y como la cadena estabiliza tenemos que $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$ para algún n.

Por último veamos que 2 y 3 son equivalentes. Sea I un conjunto no vacío de ideales, supongamos que no tiene elemento maximal con la inclusión. Como I es no vacío existe $\mathfrak{a}_1 \in I$, como $\mathfrak{a}_1$ no es maximal existe $\mathfrak{a}_2 \in I$ tal que $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$ y como $\mathfrak{a}_2$ no es maximal existe $\mathfrak{a}_3$ tal que $\mathfrak{a}_2 \subsetneq \mathfrak{a}_3$ y así construimos la cadena ascendente $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$ que no se estabiliza, lo cual es una contradicción. Recíprocamente, dada una cadena ascendente $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$ definimos el conjunto $I = \{\mathfrak{a}_i \mid i \geq 0\}$ el cual es claramente no vacío por lo que tiene un elemento maximal. Sea a_{i_0} un elemento maximal de I, como $a_{i_0+1} \in I$ y $a_{i_0+1} \supseteq a_{i_0}$ tenemos que $a_{i_0} = a_{i_0+1}$, por lo tanto la cadena estabiliza. □

Definición 2.2.3. Un anillo R es **noetheriano** si satisface cualquiera de las anteriores condiciones equivalentes.

Es claro que $\mathcal{O}_K$ es noetheriano ya que por la Observación 2.1.18 todos sus ideales son finitamente generados. Antes introducir el concepto de ideal fraccionario, veamos algunos lemas que usaremos en la prueba del Teorema 2.2.12.

Lema 2.2.4. *Sea* R *un dominio noetheriano. Entonces todo ideal* $\mathfrak{a} \neq \langle 0 \rangle$ *contiene un producto de ideales primos no nulos.*

Demostración. Supongamos por contradicción que existe un ideal $\mathfrak{a}$ que no contiene un producto de ideales primos no nulos, y sea I el conjunto de los ideales que no cumplen esta propiedad, es claro que $I \neq \emptyset$ ya que $\mathfrak{a} \in I$ y como R es noetheriano I tiene elemento maximal. Sea $\mathfrak{b}$ ese elemento maximal. Note que $\mathfrak{b}$ no es primo ya que en caso contrario dado que $\mathfrak{b} \subseteq \mathfrak{b}$ si contendría un producto de ideales primos no nulos, lo que contradeciría que $\mathfrak{b} \in I$. Luego, existen $a, b \notin \mathfrak{b}$ tal que $ab \in \mathfrak{b}$, entonces $\mathfrak{b} \subsetneq \langle a \rangle + \mathfrak{b}$ y $\mathfrak{b} \subsetneq \langle b \rangle + \mathfrak{b}$, además por la maximalidad de $\mathfrak{b}$ tanto $\langle a \rangle + \mathfrak{b}$ como $\langle b \rangle + \mathfrak{b}$ contienen un producto de ideales primos no nulos. Es claro que $(\langle a \rangle + \mathfrak{b})(\langle b \rangle + \mathfrak{b}) \subseteq (\langle ab \rangle + \mathfrak{b}) \subseteq \mathfrak{b}$, por lo tanto $\mathfrak{b}$ contiene un producto de ideales primos no nulos lo cual es una contradicción. □

Lema 2.2.5. *Sea R un dominio noetheriano. Entonces todo ideal propio $\mathfrak{a}$ esta contenido en un ideal maximal de R.*

Demostración. Sea I el conjunto de todos los ideales propios de R que contienen a $\mathfrak{a}$, es claro que es no vacío ya que $\mathfrak{a} \in I$ entonces R al ser noetheriano I tiene un elemento maximal. Sea $\mathfrak{m}$ uno de estos elementos, veamos que $\mathfrak{m}$ es maximal. Sea $\mathfrak{b}$ un ideal propio de R tal que $\mathfrak{b} \supseteq \mathfrak{m}$ entonces por transitividad $\mathfrak{a} \subseteq \mathfrak{b}$ por lo que $\mathfrak{b} \in I$, pero como $\mathfrak{m}$ es un maximal en I y además $\mathfrak{m} \subseteq \mathfrak{b}$ tenemos que $\mathfrak{m} = \mathfrak{b}$. □

Lema 2.2.6. *Sea K una extensión finita de $\mathbb{Q}$ y sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$. Entonces el anillo cociente $\mathcal{O}_K/\mathfrak{a}$ es finito. Además, sean $\omega_1, \ldots, \omega_n$ y $\tau_1, \ldots, \tau_n$ bases enteras de $\mathcal{O}_K$ y $\mathfrak{a}$ respectivamente, y $a_{ij} \in \mathbb{Z}$ los enteros tales que:*

$$\tau_i = \sum_{j=0}^{n} a_{ij}\omega_j$$

entonces $|\mathcal{O}_K/\mathfrak{a}| = |\det(a_{ij})|$.

Demostración. Sean $\omega_1, \ldots, \omega_n$ una base entera de $\mathcal{O}_K$ y $\tau_1, \ldots, \tau_n$ la base entera de $\mathfrak{a}$ generada en el Colorario 2.1.17, entonces existen $a_{ij} \in \mathbb{Z}$ tales que

$$\tau_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

y así la matriz $A = (a_{ij})$ es triangular superior. Afirmamos que los elementos de la forma $\sum_{i=1}^{n} r_i\omega_i$ con $0 \leq r_i < |a_{ii}|$ son un sistema completo de residuos módulo $\mathfrak{a}$. En efecto, sea $y \in \mathcal{O}_K$ sabemos que existen enteros b_i tales que $y = b_1\omega_1 + b_2\omega_2 + \cdots + b_n\omega_n$. Por el algoritmo de la división existen $q_1, r_1 \in \mathbb{Z}$ con $0 \leq r_1 < |a_{11}|$ tales que $b_1 = q_1a_{11} + r_1$. Así,

$y - r_1\omega_1 - q_1\tau_1 = (b_2 - q_1a_{12})\omega_2 + \cdots + (b_n - q_1a_{1n})\omega_n$ y realizando el algoritmo de la división entre $b_2 - q_1a_{12}$ y a_{22} encontramos q_2 y r_2 con $0 \leq r_2 < |a_{22}|$ tales que $b_2 - q_1a_{12} = q_2a_{22} + r_2$ y asi sucesivamente encontramos los q_i y r_i tales que

$$y - \sum_{i=1}^{n} r_i\omega_i - \sum_{i=1}^{n} q_i\tau_i = 0,$$

lo que nos permite concluir que $y - \sum_{i=1}^{n} r_i\omega_i \in \mathfrak{a}$. Por otro lado, supongamos que $\sum_{i=1}^{n} r_i\omega_i - \sum_{i=1}^{n} r'_i\omega_i \in \mathfrak{a}$ con $0 \leq r_i, r'_i < |a_{ii}|$, entonces existen $b_1, \ldots, b_n \in \mathbb{Z}$ tales que $\sum_{i=1}^{n}(r_i - r'_i)\omega_i = \sum_{i=1}^{n} b_i\tau_i$ y teniendo en cuenta que A es triangular superior concluimos que $b_1a_{11} = r_1 - r'_1$, lo que implica que a_{11} divide a $r_1 - r'_1$ pero teniendo en cuenta las condiciones de estos r sabemos que $-|a_{11}| < r_1 - r'_1 < |a_{11}|$. Luego, $r_1 - r'_1 = 0$ y por lo tanto $r_1 = r'_1$ y $b_1 = 0$. Siguiendo este procedimiento concluimos que $r_i = r'_i$.

Es claro que la cantidad de elementos de la forma $\sum_{i=1}^{n} r_i\omega_i$ con $0 \leq r_i < |a_{ii}|$ es $\prod_{i=1}^{n}|a_{ii}|$. Dado que estos elementos forman un sistema completo de residuos y la matriz A es triangular superior obtenemos que $|\mathcal{O}_K/\mathfrak{a}| = \prod_{i=1}^{n}|a_{ii}| = |\det A|$. En general si $\tau'_1, \ldots, \tau'_n$ es una base entera de $\mathfrak{a}$ cualquiera podemos considerar B como la matriz de cambio de base de τ' a τ y B^{-1} como la matriz de cambio de base de τ a τ', es claro que los coeficientes de ambas matrices son números enteros, así sus determinantes son enteros y como $\det B \det B^{-1} = 1$ tenemos que $\det B = \pm 1$. Considere A' la matriz de cambio de base de τ' a ω entonces $A' = BA$ lo que implica que $|\det(A')| = |\det(A)||\det(B)| = |\det(A)| = |\mathcal{O}_K/\mathfrak{a}|$. □

Proposición 2.2.7. *Sea K una extensión finita de $\mathbb{Q}$. Entonces:*

I) *$\mathcal{O}_K$ es integralmente cerrado en K.*

II) *$\mathcal{O}_K$ es noetheriano.*

III) *Todo ideal primo no nulo de $\mathcal{O}_K$ es maximal.*

Demostración. Por la Proposición 2.2.1 y por la Observación 2.1.17 ya hemos probado tanto el primer como el segundo ítem, así que solo nos falta probar el tercer ítem. Sea $\mathfrak{p}$ un ideal primo no nulo y sea $d \in \mathcal{O}_K/\mathfrak{p}$ no nulo. El conjunto de las potencias positivas de d es un subconjunto de $\mathcal{O}_K/\mathfrak{p}$ y por el Lema 2.2.6 $\mathcal{O}_K/\mathfrak{p}$ es finito, luego este subconjunto es finito. Así, existen $i > j$ tales que $d^i = d^j$ entonces $d^j(d^{i-j} - 1) = 0$ y debido a que $\mathfrak{p}$

es primo $\mathcal{O}_K/\mathfrak{p}$ es dominio entero así $d^{i-j} = 1$ y como $i > j$ entonces $i - j$ es diferente de cero por lo que d es invertible, implicando así que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, luego $\mathfrak{p}$ es maximal. □

Un dominio que satisface las tres propiedades de la proposición anterior es llamado un **Dominio de Dedekind**. A continuación extenderemos ligeramente el concepto de ideal.

Definición 2.2.8. Sea $K/\mathbb{Q}$ una extensión finita. Un subconjunto $\mathfrak{f} \subset K$ es llamado **ideal fraccionario** de $\mathcal{O}_K$ si existe un ideal $\mathfrak{a} \subset \mathcal{O}_K$ y un elemento no nulo $d \in \mathcal{O}_K$ tal que

$$\mathfrak{f} = \frac{1}{d} \cdot \mathfrak{a} \overset{\text{def}}{=} \left\{ \frac{a}{d} \mid a \in \mathfrak{a} \right\}.$$

Ejemplo 2.2.9. Sean elementos arbitrarios $a_1, \ldots, a_n \in K$ tenemos que:

$$(a_1, \ldots, a_n) \overset{\text{def}}{=} \{a_1 x_1 + \cdots + a_n x_n \mid x_i \in \mathcal{O}_K\}$$

es un ideal fraccionario de $\mathcal{O}_K$. Esto es claro debido a que cada uno de los a_i es un número algebraico entonces para cada i existe $z_i \in \mathbb{Z}$ tal que $a_i z_i \in \mathcal{O}_K$ y tomando $z = \prod_{i=1}^{n} z_i$ tenemos que $\langle za_1, \ldots, za_n \rangle$ es un ideal de $\mathcal{O}_K$ y por lo tanto

$$(a_1, \ldots, a_n) = \frac{1}{z} \langle za_1, \ldots, za_n \rangle$$

es un ideal fraccionario.

Lo último que necesitamos probar antes de la demostración del Teorema 2.2.12 es que los ideales primos son invertibles.

Lema 2.2.10. *Sean $\mathfrak{f}$ un ideal fraccionario de $\mathcal{O}_K$ y $a \in K$ un elemento tal que $a\mathfrak{f} \subset \mathfrak{f}$, entonces $a \in \mathcal{O}_K$.*

Demostración. Sea $\mathfrak{f}$ un ideal fracionario de $\mathcal{O}_K$, entonces existe $d \in \mathcal{O}_K$ y $\mathfrak{a}$ ideal de $\mathcal{O}_K$ tal que $\mathfrak{f} = \frac{1}{d}\mathfrak{a}$. Como $\mathfrak{a}$ es finitamente generado por $\tau_1, \ldots, \tau_n$ es claro que $\mathfrak{f}$ es finitamente generado por $\frac{\tau_1}{d}, \ldots, \frac{\tau_n}{d}$ y así existen $\omega_1, \ldots, \omega_n$ tales que

$$\mathfrak{f} = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Como $a\mathfrak{f} \subset \mathfrak{f}$ tenemos que $a\omega_i \in \mathfrak{f}$ por lo que podemos definir el siguiente sistema de ecuaciones

$$a\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

$$0 = a\omega_i - \sum_{j=1}^{n} a_{ij}\omega_j$$

Definamos $A = (a_{ij})$, este sistema de ecuaciones tiene una solución no nula, luego $\det(a \cdot I - A) = 0$ por lo que a es raiz del polinomio mónico característico $p(x) = \det(x \cdot I - A)$ que tiene coeficientes en los enteros y así $a \in \mathcal{O}_K$. □

Proposición 2.2.11. *Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. Sea $\mathfrak{p}^{-1}$ el ideal fraccionario*

$$\mathfrak{p}^{-1} = \{a \in K \mid a\mathfrak{p} \subset \mathcal{O}_K\}$$

Entonces $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Demostración. Sea $\mathfrak{p}$ un ideal no nulo de $\mathcal{O}_K$, entonces existe $d \in \mathfrak{p}$ no nulo. Veamos que $d\mathfrak{p}^{-1}$ es un ideal de $\mathcal{O}_K$. Por la definición de $\mathfrak{p}^{-1}$ es claro que $d\mathfrak{p}^{-1} \subset \mathcal{O}_K$, ahora sean $a, b \in \mathfrak{p}^{-1}$ y $\theta \in \mathcal{O}_K$. Tenemos que $a\mathfrak{p}$ y $b\mathfrak{p}$ estan contenidos en $\mathcal{O}_K$ por lo que $(a-b)\mathfrak{p} \subset a\mathfrak{p} - b\mathfrak{p} \subset \mathcal{O}_K$ y tambien es claro que $\theta a\mathfrak{p} \subset \mathcal{O}_K$. De lo anterior también podemos concluir que $\mathfrak{p}\mathfrak{p}^{-1}$ es un ideal de $\mathcal{O}_K$ y claramente $\mathcal{O}_K \subset \mathfrak{p}^{-1}$, así $\mathfrak{p}\mathfrak{p}^{-1} \supset \mathfrak{p}$ y como $\mathfrak{p}$ es primo entonces por el ítem 3 de la Proposición 2.2.7 es maximal por lo tanto para probar que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$ solo debemos probar que $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$.

Asumamos por contradicción que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ y sea $\alpha \in \mathfrak{p}^{-1}$, como $\alpha\mathfrak{p} \subset \mathfrak{p}$ por el lema anterior $\alpha \in \mathcal{O}_K$, así $\mathfrak{p}^{-1} = \mathcal{O}_K$. Sea $\alpha \in \mathfrak{p}$ no nulo entonces por el Lema 2.2.4 tenemos que $\langle\alpha\rangle \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$ y asumamos que n es la menor cantidad de primos no nulos tal que su producto este contenido en $\langle\alpha\rangle$. Como $\mathfrak{p} \supset \langle\alpha\rangle$ tenemos sin perdida de generalidad que $\mathfrak{p} \supset \mathfrak{p}_1$ y como $\mathfrak{p}_1$ es maximal y $\mathfrak{p}$ es un ideal propio sabemos que $\mathfrak{p}_1 = \mathfrak{p}$. Además tenemos que $\mathfrak{p}_2 \cdots \mathfrak{p}_n \nsubseteq \langle\alpha\rangle$ ya que n es mínimo por lo que existe $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ tal que $b \notin \langle\alpha\rangle$, entonces $\dfrac{b}{\alpha} \notin \mathcal{O}_K$ pero como $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ tenemos que $b\mathfrak{p} \subset \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset \langle\alpha\rangle$, así $\dfrac{b}{\alpha}\mathfrak{p} \subset \mathcal{O}_K$ entonces por definición $\dfrac{b}{\alpha} \in \mathfrak{p}^{-1}$ pero $\dfrac{b}{\alpha} \notin \mathcal{O}_K$, una contradicción. □

Teorema 2.2.12. *Cualquier ideal propio no nulo de $\mathcal{O}_K$ puede escribirse como producto de ideales primos. Esta factorización es única a menos del orden de los factores.*

Demostración. Supongamos por contradicción que existe $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ que no se escribe como producto de ideales primos y sea I el conjunto de los ideales propios de $\mathcal{O}_K$ que no se escriben como producto de ideales primos, es claro que $I \neq \emptyset$ ya que $\mathfrak{a} \in I$

por lo que existe $\mathfrak{b}$ un elemento maximal de I. Como $\mathfrak{b}$ es un ideal propio de $\mathcal{O}_K$ por el Lema 2.2 existe $\mathfrak{p}$ maximal tal que $\mathfrak{p} \supset \mathfrak{b}$ multiplicando por $\mathfrak{p}^{-1}$ obtenemos que $\mathcal{O}_K \supset \mathfrak{p}^{-1}\mathfrak{b}$ por lo que $\mathfrak{p}^{-1}\mathfrak{b}$ es un ideal de $\mathcal{O}_K$ y además es propio ya que si no lo fuera $\mathfrak{b} = \mathfrak{p} \notin I$. Por otro lado, como $\mathfrak{p}^{-1} \supset \mathcal{O}_K$ tenemos que $\mathfrak{p}^{-1}\mathfrak{b} \supset \mathfrak{b}$ y esta inclusión es propia debido a que si no es el caso tendriamos que $\mathfrak{p}^{-1} = \mathcal{O}_K$ y en la demostración de la proposición anterior vimos que esto no era posible, con esto concluimos que $\mathfrak{p}^{-1}\mathfrak{b}$ es un ideal propio de $\mathcal{O}_K$ que contiene propiamente a $\mathfrak{b}$ por lo que $\mathfrak{p}^{-1}\mathfrak{b} \notin I,$ así existen ideales primos tales que

$$\mathfrak{p}^{-1}\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \Rightarrow \mathfrak{b} = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

entonces $\mathfrak{b} \notin I,$ una contradicción.

Por último probemos la unicidad, sea $\mathfrak{a}$ un ideal propio no nulo de $\mathcal{O}_K$ con dos factorizaciones

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

primeramente probemos que $r = s$. Supongamos por contradicción y sin perdida de generalidad que $r < s$. Sabemos que $\mathfrak{p}_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ así existe algún q_i tal que $p_1 \supseteq \mathfrak{q}_i$ y sabiendo que $\mathfrak{q}_i$ es maximal tenemos que $p_1 = \mathfrak{q}_i$ además podemos reordenar los $\mathfrak{q}$ tal que $\mathfrak{q}_i = \mathfrak{q}_1,$ realizando este procedimiento y multiplicando por el inverso de $\mathfrak{p}_1$ obtenemos

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$$

repitiendo este procedimiento otras $r - 1$ veces obtenemos que $\mathcal{O}_K = \mathfrak{q}_{r+1} \cdots \mathfrak{q}_s$ por lo que $\mathfrak{q}_s^{-1} = \mathfrak{q}_{r+1} \cdots \mathfrak{q}_{s-1} \subset \mathcal{O}_K$ así $\mathfrak{q}_s^{-1} = \mathcal{O}_K$ lo que es una contradicción, por lo tanto $r = s$ e igualmente podemos concluir que $p_i = q_i$ para $i = 1, \ldots, r$ realizando el mismo procedimiento que hicimos en el paso anterior. □

Es importante resaltar que si consideramos las potencias negativas de los ideales primos podemos extender el resultado anterior a los ideales fraccionarios.

Corolario 2.2.13. *Cualquier ideal fraccionario $\mathfrak{f} \neq 0, \mathcal{O}_K$ de $\mathcal{O}_K$ se escriben, de manera única, como*

$$\mathfrak{f} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} \qquad e_i \in \mathbb{Z} \setminus \{0\}$$

donde $\mathfrak{p}_i \subset \mathcal{O}_K$ son ideales primos distintos.

Demostración. Sea $\mathfrak{f}$ un ideal fraccionario de $\mathcal{O}_K,$ entonces existe $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ y

$d \in \mathcal{O}_K$ tal que $\mathfrak{f} = \frac{1}{d} \cdot \mathfrak{a}$, por el teorema anterior tenemos que $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ así $\mathfrak{f} = \frac{1}{d} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n = \left(\frac{1}{d}\right) \mathfrak{p}_1 \cdots \mathfrak{p}_n$ por lo que solo nos falta probar que

$$\left(\frac{1}{d}\right) = \prod_{j=1}^{n} \mathfrak{q}_j^{e_j}$$

Es claro que $\frac{1}{d}\mathfrak{p}_i = \left(\frac{1}{d}\right) \cdot \mathfrak{p}_i$ además que $\left(\frac{1}{d}\right) = \langle d \rangle^{-1}$ y teniendo en cuenta que $\langle d \rangle$ es un ideal de $\mathcal{O}_K$ tenemos que $\langle d \rangle = \mathfrak{q}_i \cdots \mathfrak{q}_n$, así $\left(\frac{1}{d}\right) = \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_n^{-1}$ por lo que

$$\mathfrak{f} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_m \qquad e_j \in \mathbb{Z} \setminus \{0\}$$

Luego juntando primos iguales concluimos lo deseado. □

Corolario 2.2.14. *El conjunto de los ideales fraccionarios no nulos de $\mathcal{O}_K$ es un grupo bajo la multiplicación de ideales.*

Demostración. Es claro que el producto de ideales fraccionarios de $\mathcal{O}_K$ es clausurativo y asociativo debido a que el producto entre ideales de $\mathcal{O}_K$ también lo es, además el elemento identidad es $\mathcal{O}_K$ por lo que solo faltaria comprobar que todos los ideales fraccionarios son invertibles. Sea $\mathfrak{f}$ un ideal fraccionario de $\mathcal{O}_K$, entonces por el corolario anterior tenemos que $\mathfrak{f} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, así $\mathfrak{f}^{-1} = (\mathfrak{p}^{-1})^{e_1} \cdots (\mathfrak{p}_n^{-1})^{e_n}$ el cual es el producto de ideales fraccionarios por lo tanto también es un ideal fraccionario. □

Con los resultados obtenidos anteriormente podemos adaptar las propiedades de divisibilidad de los enteros a los ideales de $\mathcal{O}_K$.

Definición 2.2.15. Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}_K$ diremos que $\mathfrak{a}|\mathfrak{b}$ si, y solo si, $\mathfrak{a} \supset \mathfrak{b}$.

Proposición 2.2.16. *Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}_K$, tenemos que:*

$$\mathfrak{a} \supset \mathfrak{b} \Leftrightarrow \text{ existe un ideal } \mathfrak{c} \text{ de } \mathcal{O}_K \text{ tal que } \mathfrak{b} = \mathfrak{a}\mathfrak{c}.$$

Demostración. Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}_K$ tales que $\mathfrak{a} \supset \mathfrak{b}$ es claro que $\mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{b}$ entonces solo nos faltaría probar que $\mathfrak{a}^{-1}\mathfrak{b}$ es un ideal de $\mathcal{O}_K$. Como $\mathfrak{a}^{-1}$ es un ideal fraccionario tenemos que $\mathfrak{a}^{-1}\mathfrak{b}$ es un ideal fraccionario, además como $\mathfrak{a} \supset \mathfrak{b}$ podemos concluir que $\mathcal{O}_K \supset \mathfrak{a}^{-1}\mathfrak{b}$ por lo tanto es un ideal de $\mathcal{O}_K$. Recíprocamente, es claro que $\mathfrak{a} \supset \mathfrak{a}\mathfrak{c} = \mathfrak{b}$. □

Lema 2.2.17. *Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$. Entoces la cantidad de divisores de $\mathfrak{a}$ es*

finita. Además sea

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} \qquad e_i \in \mathbb{Z}^+$$

la factorización única de $\mathfrak{a}$ *en ideales primos, entonces la cantidad de divisores de* $\mathfrak{a}$ *es*

$$\prod_{i=1}^{n} (e_i + 1)$$

Demostración. Veamos que los ideales de la forma

$$\prod_{i=1}^{n} \mathfrak{p}_i^{f_i} \qquad 0 \leq f_i \leq e_i$$

son todos los divisores de $\mathfrak{a}$. Sea $\mathfrak{b}$ un ideal no nulo de $\mathcal{O}_K$ tal que $\mathfrak{b}|\mathfrak{a}$, entonces por definición $\mathfrak{b} \supset \mathfrak{a}$, además como es no nulo tenemos que

$$\mathfrak{b} = \prod_{i=1}^{m} \mathfrak{q}_i^{f_i} \supset \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} = \mathfrak{a}$$

Por lo tanto $\mathfrak{q}_i \supset \mathfrak{p}_j$ para algún $j = 1 \ldots, m$ por lo que luego de un reordenamiento tenemos

$$\mathfrak{b} = \prod_{j=1}^{m} \mathfrak{p}_j^{f_j}.$$

Es claro que $f_j > 0$, veamos que $f_j \leq e_j$, asumamos por contradicción y sin perdida de generalidad que $e_1 < f_1$ entonces $\mathfrak{p}_1 \subset \mathfrak{p}_1^{e_1 - f_1} \subset \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$ lo que implica que $\mathfrak{p}_1 = \mathfrak{p}_i$ para un $i \neq 1$ lo que es una contradicción. Por último sabemos que $\mathfrak{b}$ tiene m ideales primos diferentes en su factorización este m debe ser menor o igual que n ya que la cantidad de primos diferentes de $\mathfrak{b}$ es menor o igual que la de $\mathfrak{a}$ por lo tanto podemos añadirle a $\mathfrak{b}$ los primos que le falten para que tengan la misma cantidad de primos pero usando en el exponente cero, así

$$\mathfrak{b} = \prod_{i=1}^{n} \mathfrak{p}_i^{f_i} \qquad 0 \leq f_i \leq e_i$$

Finalmente, para saber la cantidad de elementos que se escriben de esta forma usamos el principio multiplicativo sabiendo que cada f_i tiene $e_i + 1$ opciones. □

Para finalizar esta sección definiremos el concepto norma para ideales de $\mathcal{O}_K$ el cual

será fundamental en el estudio de la cardinalidad del grupo clase de un anillo de enteros algebraicos.

Definición 2.2.18. Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$. La norma $N(\mathfrak{a})$ de $\mathfrak{a}$ es definida como el número de elementos del cociente $\mathcal{O}_K/\mathfrak{a}$.

De ahora en adelante, si $\alpha \in \mathcal{O}_K$ escribemos $N(\alpha)$ en vez de $N_{K/\mathbb{Q}}(\alpha)$ para no sobrecargar la escritura de las pruebas.

Proposición 2.2.19. *Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}_K$. Entonces:*

I) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

II) $N(\langle\alpha\rangle) = |N(\alpha)|$, *para todo* $\alpha \in \mathcal{O}_K$.

III) $N(\mathfrak{a}) \in \mathfrak{a}$.

Demostración. Para mostrar 1 debido a la factorización única solo es necesario probar que $N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p})$ para todo $\mathfrak{a}$ ideal no nulo y $\mathfrak{p}$ un ideal primo cualquiera. Sabemos, por el tercer teorema de isomorfismo que $|\mathcal{O}_K/\mathfrak{ap}| = |\mathcal{O}_K/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|$ por lo que solo nos faltaria mostrar que $\mathcal{O}_K/\mathfrak{p}$ es equipotente a $\mathfrak{a}/\mathfrak{ap}$. Note que $\mathfrak{a} \neq \mathfrak{ap}$ debido a la unicidad de la factorización prima, por lo tanto existe $\omega \in \mathfrak{a} \setminus \mathfrak{ap}$ y sea n el exponente de $\mathfrak{p}$ en la factorización prima de $\mathfrak{a}$ (en el caso que no aparezca entonces $n = 0$) por lo que a su vez n también va a ser el exponente de $\langle\omega\rangle$ en su factorización prima debido a que $\mathfrak{a} \supset \langle\omega\rangle$ entonces el mínimo exponente de $\mathfrak{p}$ en $\langle\omega\rangle$ es n pero no puede ser mayor debido a que $\langle\omega\rangle \nsubseteq \mathfrak{ap}$ teniendo esto en cuenta definamos la función $f : \mathcal{O}_K/\mathfrak{p} \to \mathfrak{a}/\mathfrak{ap}$ tal que $f(x + \mathfrak{p}) = x\omega + \mathfrak{ap}$. Primeramente veamos que esta bien definida, sean $x, y \in \mathcal{O}_K$ tal que $x + \mathfrak{p} = y + \mathfrak{p}$, entonces $x - y \in \mathfrak{p}$, además como $\omega \in \mathfrak{a}$ tenemos que $(x - y)\omega \in \mathfrak{ap}$ por lo que $x\omega + \mathfrak{ap} = y\omega + \mathfrak{ap}$ lo que implica que $f(x + \mathfrak{p}) = f(y + \mathfrak{p})$. Ahora veamos que $\mathfrak{f}$ es inyectiva, para esto primero veamos que f es un homomorfismo, note que $f(x + \mathfrak{p} + y + \mathfrak{p}) = f(x + y + \mathfrak{p}) = \omega(x + y) + \mathfrak{ap} = x\omega + \mathfrak{ap} + y\omega + \mathfrak{ap} = f(x + \mathfrak{p}) + f(y + \mathfrak{p})$ entonces para que f sea inyectiva solo hace falta ver que $\mathrm{Ker}(f) = 0$. Sea $x \in \mathcal{O}_K$ tal que $f(x + \mathfrak{p}) = x\omega + \mathfrak{ap} = 0 + \mathfrak{ap}$ entonces $x\omega \in \mathfrak{ap}$, así $\langle x\rangle\langle\omega\rangle = \langle x\omega\rangle \subset \mathfrak{ap}$ por lo que el exponente de la factorización prima de $\mathfrak{p}$ en $\langle x\rangle\langle\omega\rangle$ es mayor o igual que $n + 1$ y el exponente de $\mathfrak{p}$ en $\langle\omega\rangle$ es n, así $\mathfrak{p} \supset \langle x\rangle$, entonces $x \in \mathfrak{p}$ concluyendo así que f es inyectiva.

Para mostrar que f es sobreyectiva primero veamos que $\mathfrak{a} = \langle\omega\rangle + \mathfrak{ap}$. Es claro

que $\mathfrak{a} \supset \langle\omega\rangle + \mathfrak{a}\mathfrak{p}$ y supongamos por contradicción que $\langle\omega\rangle + \mathfrak{a}\mathfrak{p} \not\supseteq \mathfrak{a}$, es evidente que $\langle\omega\rangle + \mathfrak{a}\mathfrak{p} \supset \mathfrak{a}\mathfrak{p}$ entonces $(\langle\omega\rangle + \mathfrak{a}\mathfrak{p})^{-1}\mathfrak{a}\mathfrak{p}$ es un ideal de $\mathcal{O}_K$ y note que $\mathfrak{p} \not\supseteq (\langle\omega\rangle + \mathfrak{a}\mathfrak{p})^{-1}\mathfrak{a}\mathfrak{p}$ ya que de otro modo $(\langle\omega\rangle + \mathfrak{a}\mathfrak{p})\mathfrak{p} \supset \mathfrak{a}\mathfrak{p}$ lo que implica que $\langle\omega\rangle + \mathfrak{a}\mathfrak{p} \supset \mathfrak{a}$ por lo tanto el exponente de $\mathfrak{p}$ en $\langle\omega\rangle + \mathfrak{a}\mathfrak{p}$ es $n+1$ lo que significa que $\mathfrak{p}^{n+1} | \langle\omega\rangle + \mathfrak{a}\mathfrak{p}$. Como también $p^{n+1} | \mathfrak{a}\mathfrak{p}$ tenemos que $\mathfrak{p}^{n+1} | \langle\omega\rangle$ lo cual es una contradicción debido a que el exponente de $\mathfrak{p}$ en $\langle\omega\rangle$ es n, concluyendo así que $\langle\omega\rangle + \mathfrak{a}\mathfrak{p} \supseteq \mathfrak{a}$ y con esto también la igualdad. Teniendo esto en cuenta sea $y \in \mathfrak{a}$, entonces existe $x \in \mathcal{O}_K$ tal que $y - \omega x \in \mathfrak{a}\mathfrak{p}$ por lo tanto $f(x+\mathfrak{p}) = \omega x + \mathfrak{a}\mathfrak{p} = y + \mathfrak{a}\mathfrak{p}$, concluyendo así que f es sobreyectiva y por lo tanto biyectiva.

Continuando con la demostración de 2 sea $\omega_1, \ldots, \omega_n$ una base entera de $\mathcal{O}_K$ y $\alpha \in \mathcal{O}_K$, es claro que $\alpha\omega_1, \ldots, \alpha\omega_n$ es una base entera para $\langle\alpha\rangle$ además de ser una base de K sobre $\mathbb{Q}$, así definimos la matriz de cambio de base $A = (a_{ij})$ donde

$$\alpha\omega_i = \sum_{j=0}^{n} a_{ij}\omega_j$$

por lo que teniendo en cuenta el Lema 2.2.6 tenemos que $N(\langle\alpha\rangle) = |\det(A)|$. Note que la matriz A es la matriz asociada a la transformación T_α definida en la Proposición 1.3.6 y de esta misma proposición podemos decir que $N(\alpha) = \det(A)$ y con esto conclumios que $N(\langle\alpha\rangle) = |N(\alpha)|$.

Por último para demostrar 3, sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$, teniendo en cuenta que $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ por el Teorema de Lagrange tenemos que $N(\mathfrak{a}) \cdot x \in \mathfrak{a}$ para todo $x \in \mathcal{O}_K$, más especificamente para $x = 1$ por lo tanto $N(\mathfrak{a}) \in \mathfrak{a}$. □

Proposición 2.2.20. *Sea $\alpha \in \mathcal{O}_K$, entonces $|N(\alpha)| = 1$ si, y solo si, $\alpha \in U(\mathcal{O}_K)$.*

Demostración. Sea $\alpha \in \mathcal{O}_K$ tal que $|N(\alpha)| = 1$, entonces $N(\langle\alpha\rangle) = |N(\alpha)| = 1$ por lo que $\langle\alpha\rangle = \mathcal{O}_K$, así que existe $x \in \mathcal{O}_K$ tal que $\alpha x = 1$ por lo tanto α es invertible. Recíprocamente, si $\alpha \in U(\mathcal{O}_K)$ entonces $\alpha | 1$, así que $\langle\alpha\rangle = \mathcal{O}_K$ por lo tanto $1 = N(\langle\alpha\rangle) = |N(\alpha)|$. □

2.3. Grupo de Clase

En esta última sección definiremos una relación de equivalencia en el grupo de ideales fraccionarios de $\mathcal{O}_K$ y a su vez una operación binaria en la colección de las clases de equivalencia que le dará a esta colección una estructura de grupo. Luego, estudiaremos

la cardinalidad de este grupo y con esto resolveremos una ecuación diófantica y mostraremos un ejemplo de un dominio de ideales principales que no es euclídeo.

Definición 2.3.1. Sea K una extensión finita de $\mathbb{Q}$ de grado $n = [K : \mathbb{Q}]$. Una inmersión $\sigma : K \to \mathbb{C}$ es llamada **real** si la imagen de σ esta contenida en $\mathbb{R}$, caso contrario σ es llamada **compleja**.

Las inmersiones complejas simpre van en pares pues si σ es una inmersión compleja entonces $\overline{\sigma}$ es una inmersión compleja diferente a σ. Llamaremos r a la cantidad de inmersiones reales y $2s$ a la cantidad de inmersiones complejas de K.

Ejemplo 2.3.2. $\mathbb{Q}(\sqrt[3]{2})$ tiene una inmersión real y dos inmersiones complejas. Recordemos que en el Ejemplo 1.2.7 vimos que el polinomio $x^3 - 2$ tiene una raiz real y dos raíces complejas, así que la inmersion real es la identidad, y las otras dos inmersiones complejas son las que mandan a $\sqrt[3]{2}$ a las otras raíces de $x^3 - 2$ complejas.

Lema 2.3.3. *Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Entonces existe un elemento $a \in \mathfrak{a}$, $a \neq 0$, tal que*

$$|N(a)| \leq \left(\frac{2}{\pi}\right)^s N(\mathfrak{a})\sqrt{|\Delta(\omega_1, \ldots, \omega_n)|}.$$

Demostración. Ver [3], página 297. □

Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales fraccionarios de $\mathcal{O}_K$. Decimos que $\mathfrak{a}$ y $\mathfrak{b}$ son equivalentes si difieren entre si por un ideal principal; es decir:

$$[\mathfrak{a}] = [\mathfrak{b}] \Leftrightarrow \mathfrak{a} = \mathfrak{b} \cdot (c) \qquad \text{para algún } c \in U(K).$$

Afirmamos que la relación anterior es una relación de equivalencia sobre el grupo multiplicativo de los ideales fraccionarios. En efecto, es reflexiva pues $\mathfrak{a} = \mathfrak{a} \cdot (1)$, es simétrica ya que si $\mathfrak{a} = \mathfrak{b} \cdot (c)$ entonces $\mathfrak{b} = \mathfrak{a} \cdot (c^{-1})$ y es transitiva ya que si $\mathfrak{a} = \mathfrak{b} \cdot (c)$ y $\mathfrak{b} = \mathfrak{f} \cdot (d)$ entonces $\mathfrak{a} = \mathfrak{f} \cdot (cd)$.

Definición 2.3.4. El **grupo de clase** de $\mathcal{O}_K$ es un grupo cuyos elementos son las clases de equivalencia $[\mathfrak{a}]$ de relación de equivalencia definida anteriormente. De esta forma, podemos definir la siguiente operación entre clases:

$$[\mathfrak{a}] \cdot [\mathfrak{b}] \stackrel{\text{def}}{=} [\mathfrak{a} \cdot \mathfrak{b}].$$

Esta operación vuelve al conjunto de las clases un grupo multiplicativo. Donde la identidad es $[\mathcal{O}_K]$ y $[\mathfrak{a}]^{-1} = [\mathfrak{a}^{-1}]$.

Para aclarar que la definición es correcta, probaremos que la operación entre clases esta bien definida. Supongamos que $[\mathfrak{a}] = [\mathfrak{b}]$ y $[\mathfrak{c}] = [\mathfrak{f}]$ entonces $\mathfrak{a} = \mathfrak{b} \cdot (x)$ y $\mathfrak{c} = \mathfrak{f} \cdot (y)$ para algunos $x, y \in U(K)$ así, $\mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b} \cdot (x) \cdot \mathfrak{f} \cdot (y) = \mathfrak{b} \cdot \mathfrak{f} \cdot (xy)$ por lo tanto $[\mathfrak{a} \cdot \mathfrak{c}] = [\mathfrak{b} \cdot \mathfrak{f}]$.
A continuación probaremos uno de los resultados mas importantes sobre el grupo de clases.

Teorema 2.3.5. *El grupo de clase del anillo de enteros $\mathcal{O}_K$ es finito.*

Demostración. Primero veamos que hay una cantidad finita de ideales con norma menor o igual a $C = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\omega_1, \ldots, \omega_n)|}$, sabemos que hay finitos enteros entre 1 y C entonces solo falta comprobar que para cada entero z solo existen finitos ideales de $\mathcal{O}_K$ tales que su norma sea z. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ tal que $N(\mathfrak{a}) = z$, por la Proposición 2.2.19 tenemos que $z \in \mathfrak{a}$, así $\mathfrak{a} \supset \langle z \rangle$ por lo tanto lo divide y por el Lema 2.2.17 sabemos que $\langle z \rangle$ tiene finitos divisores por lo que solo hay una cantidad finita de ideales de $\mathcal{O}_K$ que tengan norma z. Sea S el conjunto de los ideales de $\mathcal{O}_K$ que tienen norma menor o igual a C veamos que cualquier ideal fraccionario de $\mathcal{O}_K$ es equivalente al inverso de algún elemento de S. Sea $\mathfrak{f}$ un ideal fraccionario y $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ tal que $\mathfrak{f} = \frac{1}{d} \cdot \mathfrak{a}$ para algún $d \in \mathcal{O}_K$, es claro que $\mathfrak{f}$ es equivalente a $\mathfrak{a}$ ya que $\mathfrak{a} = \mathfrak{f} \cdot \langle d \rangle$, además por el Lema 2.3.3 tenemos que existe $a \in \mathfrak{a}$ con $a \neq 0$ tal que $N(\langle a \rangle) = |N(a)| \leq C \cdot N(\mathfrak{a})$ y como $a \in \mathfrak{a}$ tenemos que $\mathfrak{a} \supset \langle a \rangle$ así que existe $\mathfrak{b}$ ideal de $\mathcal{O}_K$ tal que $\mathfrak{a}\mathfrak{b} = \langle a \rangle$ por lo tanto $[\mathfrak{a}] = [\mathfrak{b}^{-1}]$. De igual forma, tenemos que $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) = N(\langle a \rangle) \leq C \cdot N(\mathfrak{a})$ por lo que cancelando $N(\mathfrak{a})$ obtenemos que $N(\mathfrak{b}) \leq C$ y así $\mathfrak{b} \in S$ con lo que concluimos que $[\mathfrak{f}] = [\mathfrak{a}] = [\mathfrak{b}^{-1}]$. Luego, la cardinalidad del grupo de clase de $\mathcal{O}_K$ es a lo sumo el tamaño de S y por lo tanto dicho grupo es finito. □

Teorema 2.3.6. *El grupo de clase de $\mathcal{O}_K$ es trivial si, y solo si, $\mathcal{O}_K$ es DIP.*

Demostración. Sea $K/\mathbb{Q}$ una extensión de cuerpos tal que el grupo de clase de $\mathcal{O}_K$ es trivial y sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$, entonces $[\mathfrak{a}] = [\mathcal{O}_K]$ así que existe $c \in U(K)$ tal que $\mathfrak{a} = (c)\mathcal{O}_K = (c)$ pero como $c \in \mathfrak{a} \subset \mathcal{O}_K$ entonces $(c) = \langle c \rangle$, así concluimos que $\mathfrak{a} = \langle c \rangle$. Recíprocamente, supongamos que $\mathcal{O}_K$ es DIP y veamos que cualquier ideal $\mathfrak{a}$ no nulo es equivalente a $\mathcal{O}_K$, como $\mathcal{O}_K$ es DIP y $\mathfrak{a}$ es no nulo existe $c \in \mathfrak{a}$ y $c \neq 0$ tal que $\mathfrak{a} = \langle c \rangle$ y multiplicando por (c^{-1}) obtenemos $\mathfrak{a}(c^{-1}) = \mathcal{O}_K$ por lo tanto $[\mathcal{O}_K] = [\mathfrak{a}]$. □

Ejemplo 2.3.7. El grupo de clase del anillo $\mathbb{Z}[i\sqrt{5}]$ tiene dos elementos y por tanto es isomorfo al grupo cíclico C_2. Recordemos del Ejemplo 2.1.12 que $\mathbb{Z}[i\sqrt{5}] = \mathcal{O}_{\mathbb{Q}(i\sqrt{5})}$ por lo que tiene sentido que hablemos del grupo de clase de $\mathbb{Z}[i\sqrt{5}]$. Para mostrar que solo hay dos clases primero tienemos que hallar el valor de $C = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\omega_1, \ldots, \omega_n)|}$. Es claro que $1, i\sqrt{5}$ es una base de $\mathbb{Z}[i\sqrt{5}]$ y podemos calcular el discriminante para esta base recordando la formula $\Delta(\omega_1, \ldots, \omega_n) = \det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j))$, así

$$\Delta(1, i\sqrt{5}) = \begin{vmatrix} Tr(1) & Tr(i\sqrt{5}) \\ Tr(i\sqrt{5}) & Tr(-5) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & -10 \end{vmatrix} = -20$$

Y para hallar el valor de s notemos que $\mathbb{Q}(i\sqrt{5})$ es una extensión de grado 2 y las dos inmersiones a $\mathbb{C}$ son complejas entonces $s = 1$, por lo tanto el valor de $C = \frac{2}{\pi}\sqrt{20}$ es $2{,}85$ lo que quiere decir es que solo debemos buscar los ideales de $\mathbb{Z}[i\sqrt{5}]$ que tengan norma 1 o 2, ya que por el Teorema 2.3.5 todos los ideales fraccionarios seran equivalentes al inverso de alguno de ellos. Sea $\mathfrak{a}$ un ideal de $\mathbb{Z}[i\sqrt{5}]$ con $N(\mathfrak{a}) = 1$, es claro que si $N(\mathfrak{a}) = |\mathbb{Z}[i\sqrt{5}]/\mathfrak{a}| = 1$ entonces $\mathfrak{a} = \mathbb{Z}[i\sqrt{5}]$. Ahora si $N(\mathfrak{a}) = 2$ por la Proposición 2.2.19 tenemos que $2 \in \mathfrak{a}$ lo que implica que $\langle 2\rangle \subset \mathfrak{a}$, entonces $\mathfrak{a}$ divide a $\langle 2\rangle$ así que tenemos que encontrar todos los divisores de $\langle 2\rangle$ y por el Lema 2.2.17 es lo mismo de encontrar su factorización en ideales primos.

Primero veamos que $\langle 2\rangle$ no es primo. Por la proposición 2.2.7 es suficiente probar que este ideal no es maximal. que no es maximal. Afirmamos que el elemento $1 + i\sqrt{5} \notin \langle 2\rangle$. Supongamos por contradicción que $1 + i\sqrt{5} \in \langle 2\rangle$ entonces $1 + i\sqrt{5} = 2a + 2bi\sqrt{5}$ para algún $a, b \in \mathbb{Z}$,lo que quiere decir que $1 = 2a$ lo cual es una contradicción, por lo tanto el ideal $\langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle$ contiene propiamente a $\langle 2\rangle$ entonces solo nos falta verificar que es un ideal propio. Para esto veamos que $\langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle = \{a + bi\sqrt{5} | a, b \in \mathbb{Z}$ y $a \equiv b(\text{mód}2)\}$ Sea $a + bi\sqrt{5}$ con $a, b \in \mathbb{Z}$ y $a \equiv b(\text{mód}2)$ como a y b tienen la misma paridad entonces $2|a - b$ por lo tanto existe $x \in \mathbb{Z}$ tal que $2x = a - b$ por lo que $a + bi\sqrt{5} = a - b + b(1 + i\sqrt{5}) \in \langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle$, recíprocamente sea $z \in \langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle$ entonces existen $a, b, c, d \in \mathbb{Z}$ tales que $z = 2(a + bi\sqrt{5}) + (1 + i\sqrt{5})(c + di\sqrt{5}) = 2a + c - 5d + (2b + d + c)i\sqrt{5}$ y si nos damos cuenta $2a + c - 5d - (2b + d + c) = 2a - 2b - 6c$ el cual es un número par con es claro que $\langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle$ es un ideal propio ya que $1 = 1 + 0i\sqrt{5}$ y 1 y 0 no tienen la misma paridad. Note también que $\langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle$ es un ideal maximal ya que si $\mathfrak{b}$ es un ideal tal que $\langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle \subsetneq \mathfrak{b}$ entonces existe $x + iy\sqrt{5} \notin \langle 2\rangle + \left\langle 1 + i\sqrt{5}\right\rangle$ por lo tanto $2 \nmid x - y$

así $x-y=2k+1$ con esto tenemos que $1=-2k+x+yi\sqrt{5}-y(1+i\sqrt{5})\in\mathfrak{b}$ entonces $\mathfrak{b}=\mathbb{Z}[i\sqrt{5}]$ y $\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle$ es maximal. Por último tenemos que

$$\begin{aligned}\left(\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle\right)^2&=\langle 4\rangle+\left\langle 2+2i\sqrt{5}\right\rangle+\left\langle 2+2i\sqrt{5}\right\rangle+\left\langle (1+i\sqrt{5})^2\right\rangle\\&=\langle 4\rangle+\left\langle 2+2i\sqrt{5}\right\rangle+\left\langle -4+2i\sqrt{5}\right\rangle\\&=\langle 2\rangle\left(\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle+\left\langle -2+i\sqrt{5}\right\rangle\right)\end{aligned}$$

y debido a que $\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle+\left\langle -2+i\sqrt{5}\right\rangle$ contiene a $\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle$ y son diferentes puesto que $-2+i\sqrt{5}\notin\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle$ tenemos que $\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle+\left\langle -2+i\sqrt{5}\right\rangle=\mathbb{Z}[i\sqrt{5}]$ y con esto concluimos que la factorización en ideales primos de $\langle 2\rangle$ es $\left(\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle\right)^2$.

Así los ideales que dividen a $\langle 2\rangle$ son $\mathbb{Z}[i\sqrt{5}],\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle,\langle 2\rangle$ de los cuales $\mathbb{Z}[i\sqrt{5}]$ y $\langle 2\rangle$ ya son equivalentes por lo tanto solo hace falta mostrar que $\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle$ no es equivalente a $\mathbb{Z}[i\sqrt{5}]$ o lo que es lo mismo que probar que no es principal. Supongamos por contradicción que $\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle=\langle d\rangle$ para algún $d\in\mathbb{Z}[i\sqrt{5}]$ no nulo, por lo tanto tenemos que $d|2$ y $d|1+i\sqrt{5}$ entonces $N(d)|N(2)=4$ y $N(d)|N(1+i\sqrt{5})=6$ y también $d=a+bi\sqrt{5}$ con $a,b\in\mathbb{Z}$ entonces $N(d)=a^2+5b^2>0$ así $N(d)=1$ o $N(d)=2$ pero si $N(d)=1$ entonces $\langle d\rangle=\mathbb{Z}[i\sqrt{5}]$ lo cual no puede ser, así $N(d)=a^2+5b^2=2$, pero esta ecuación no tiene solución en $\mathbb{Z}$, ya que si la tuviera $b=0$ y $a^2=2$, lo cual no es posible. En conclusión el grupo de clase de $\mathbb{Z}[i\sqrt{5}]$ solo tiene dos clases diferentes $[\mathbb{Z}[i\sqrt{5}]]$ y $[\langle 2\rangle+\left\langle 1+i\sqrt{5}\right\rangle]$.

Ahora veamos como el grupo de clase es una herramienta para dar respuesta a algunas ecuaciones diofánticas.

Ejemplo 2.3.8. La ecuación diófantica $y^3=x^2+5$ no tiene soluciones enteras. Primero note que x es par ya que si este fuera impar sabemos que $x^2\equiv 1(\text{mód}8)$ por lo tanto $y^3\equiv 6(\text{mód}8)$ lo cual es una contradicción debido a que $y^3\equiv 0(\text{mód}8)$ o $y^3\equiv 1(\text{mód}8)$ dependiendo si y es par o impar respectivamente. Como x es par es claro que y es impar, asímismo $5\nmid y$ supongamos que $5|y$ entonces $5|x$ así existen $n,m\in\mathbb{Z}$ tal que $y=5n$ y $x=5m$, por lo tanto $125n^3=25m^2+5$ y reescribiendo obtenemos $25(5n^3-m^2)=5$ lo que quiere decir que $25|5$ una contradicción. Para mostrar que la ecuación diofántica no tiene soluciones enteras, veamos que tampoco tiene soluciones en $\mathbb{Z}[i\sqrt{5}]$. Sabemos que el polinomio x^2+5 se puede factorizar en $\mathbb{Z}[i\sqrt{5}]$ por lo que la ecuación diofántica la

podemos reescribir como $y^3 = (x + i\sqrt{5})(x - i\sqrt{5})$ por lo tanto tenemos que

$$\langle y \rangle^3 = \left\langle x + i\sqrt{5} \right\rangle \left\langle x - i\sqrt{5} \right\rangle$$

Veamos que $\left\langle x + i\sqrt{5} \right\rangle$ y $\left\langle x - i\sqrt{5} \right\rangle$ son coprimos, sea $\mathfrak{p}$ un ideal primo que los divide a ambos, entonces $2i\sqrt{5} = x + i\sqrt{5} - (x - i\sqrt{5}) \in \mathfrak{p}$ así $\mathfrak{p} \supset \left\langle 2i\sqrt{5} \right\rangle$ y también tenemos que $\left\langle 2i\sqrt{5} \right\rangle = \langle 2 \rangle \left\langle i\sqrt{5} \right\rangle = \left(\langle 2 \rangle + \left\langle 1 + i\sqrt{5} \right\rangle \right)^2 \left\langle i\sqrt{5} \right\rangle$ y por el ejemplo anterior sabemos que esta es su factorización prima, por lo tanto $\mathfrak{p} = \langle 2 \rangle + \left\langle 1 + i\sqrt{5} \right\rangle$ o $\mathfrak{p} = \left\langle i\sqrt{5} \right\rangle$. Note que si ocurre el primer caso $N(\mathfrak{p}) = 2$ ya que por el ejemplo anterior $\left(\langle 2 \rangle + \left\langle 1 + i\sqrt{5} \right\rangle \right)^2 = \langle 2 \rangle$ entonces $N(\langle 2 \rangle + \left\langle 1 + i\sqrt{5} \right\rangle)^2 = N(\langle 2 \rangle) = 4$, pero también sabemos que $\mathfrak{p} | \langle y \rangle$ entonces $2 | N(\langle y \rangle) = y^2$ lo cual es imposible debido a que y es impar. Por otro lado, si $\mathfrak{p} = \left\langle i\sqrt{5} \right\rangle$ tenemos que $5 = N(\mathfrak{p}) | y^2$ lo cual tampoco es posible ya que y no es múltiplo de 5. Recordando la ecuación $\langle y \rangle^3 = \left\langle x + i\sqrt{5} \right\rangle \left\langle x - i\sqrt{5} \right\rangle$ y como estos dos ideales son coprimos deben existir $\mathfrak{a}, \mathfrak{b}$ ideales de $\mathbb{Z}[i\sqrt{5}]$ tales que $\left\langle x + i\sqrt{5} \right\rangle = \mathfrak{a}^3$ y $\left\langle x - i\sqrt{5} \right\rangle = \mathfrak{b}^3$.

Del ejemplo anterior sabemos que el grupo de clase de $\mathbb{Z}[i\sqrt{5}]$ tiene solamente dos elementos entonces por el Teorema de Lagrange tenemos que $[\mathfrak{a}]^2 = [\mathfrak{a}^2] = [\mathbb{Z}[i\sqrt{5}]]$ y como $\mathfrak{a}^3$ es un ideal principal también tenemos que $[\mathbb{Z}[i\sqrt{5}]] = [\mathfrak{a}^3] = [\mathfrak{a}^2][\mathfrak{a}] = [\mathfrak{a}]$ por lo tanto $\mathfrak{a}$ es un ideal principal, entonces existe $d = a + bi\sqrt{5}$ con $a, b \in \mathbb{Z}$ tal que $\mathfrak{a} = \langle d \rangle$ y por lo tanto $\left\langle x + i\sqrt{5} \right\rangle = \langle d^3 \rangle$. Esto implica que d^3 y $x + i\sqrt{5}$ son asociados y además $U(\mathbb{Z}[i\sqrt{5}]) = \pm 1$ debido a que $N(m + ni\sqrt{5}) = m^2 + 5n^2 = 1$ solo pasa si $m = 1$ o $m = -1$, por lo tanto $x + i\sqrt{5} = \pm d^3 = \pm(a^3 - 15b^2a + (-5b^3 + 3a^2b)i\sqrt{5})$, e igualando partes imaginarias obtenemos $\pm 1 = -5b^3 + 3a^2b$ de aqui podemos decir que $b | \pm 1$ entonces $b = \pm 1$ y con esto tenemos que $b^2 = 1$. Así $\pm 1 = b(-5 + 3a^2)$ y como $b^{-1} = \pm 1$ tenemos que $\pm 1 = -5 + 3a^2$ y de aqui tenemos dos casos, primero $-1 = -5 + 3a^2$ lo que nos deja con $4 = 3a^2$ pero 3 no divide a 4 entonecs solo nos queda el otro caso $1 = -5 + 3a^2$ por lo que $a^2 = 2$ lo cual tampoco tiene sentido con lo que podemos concluir que la ecuación diofantica no tiene solución en $\mathbb{Z}[i\sqrt{5}]$ y más especificamente no tiene soluciones enteras.

Además el grupo de clase nos facilita encontrar algunos ejemplos de anillos que son dominios de ideales principales, pero no dominios euclídeos.

Lema 2.3.9. *Sean $K = \mathbb{Q}(-\sqrt{n})$ con $n \equiv -5 \pmod{24}$, $z \in \mathcal{O}_K$ y $p \in \mathbb{Z}$ un primo tal que $p = 2$ o $p = 3$ o si $p > 3$, entonces $\left(\frac{n}{p}\right) = -1$. Entonces que $p | N(z)$ implica que $p | z$.*

Demostración. Veamos que esto se cumple para $p = 2$. Sea $z \in \mathcal{O}_K$ tal que $2 | N(z)$. Como n es libre de cuadrados y $-n \equiv 5 (\text{mód} 24)$ entonces $-n \equiv 1 (\text{mód} 4)$, así

por el Teorema 2.1 tenemos que $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})} = \mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$. Así $z = a + b\left(\frac{1+\sqrt{-n}}{2}\right)$ y tambien $N(z) = (a + b\left(\frac{1+\sqrt{-n}}{2}\right))(a + b\left(\frac{1-\sqrt{-n}}{2}\right)) = a^2 + ab + b^2\frac{(n+1)}{4}$, entonces $N(z) = a^2 + ab + b^2\frac{(n+1)}{4} \equiv 0(\mathrm{mód}\, 2)$ y como $n + 5 \equiv 0(\mathrm{mód}\, 24)$ entonces $n + 5 \equiv 0(\mathrm{mód}\, 8)$, así $n + 5 = 8k$ con $k \in \mathbb{Z}$ y dividiendo por 4 tenemos que $\frac{n+1}{4} + 1 = 2k$ por lo tanto $\frac{n+1}{4} \equiv 1(\mathrm{mód}\, 2)$. Reemplazando esto en la primera ecuación obtenemos $a^2 + ab + b^2 \equiv 0(\mathrm{mód}\, 2)$ si $a \equiv 1(\mathrm{mód}\, 2)$ entonces $1 + b + b^2 \equiv 0$ pero $b + b^2$ siempre es par así $1 \equiv 0(\mathrm{mód}\, 2)$ lo que implica que $a \equiv 0(\mathrm{mód}\, 2)$ por lo tanto $b^2 \equiv 0(\mathrm{mód}\, 2)$ y con esto $b \equiv 0(\mathrm{mód}\, 2)$ concluyendo así que $2|z$.

Ahora probemos lo mismo para $p = 3$. Sea $z \in \mathcal{O}_K$ tal que $3|N(z)$, entonces $N(z) = a^2+ab+b^2\frac{(n+1)}{4} \equiv 0(\ \mathrm{mód}\ 3)$ y como $n+5 \equiv 0(\ \mathrm{mód}\ 24)$ entonces $n+5 \equiv 0(\ \mathrm{mód}\ 12)$, así $n + 5 = 12k$ con $k \in \mathbb{Z}$ y dividiendo por 4 tenemos que $\frac{n+1}{4} + 1 = 3k$ por lo tanto $\frac{n+1}{4} \equiv -1(\mathrm{mód}\, 3)$. Reemplazando esto en la primera ecuación obtenemos $a^2 + ab - b^2 \equiv 0(\mathrm{mód}\, 3)$ si $3 \nmid a, b$ entonces por el pequeño Teorema de Fermat $a^2 - b^2 \equiv 0(\mathrm{mód}\, 3)$ por lo que $ab \equiv 0(\mathrm{mód}\, 3)$ entonces $3|a$ o $3|b$ lo cual no es posible, entonces si $3|a$ tenemos que $-b^2 \equiv 0$ por lo tanto $3|b$ el otro caso es análogo por lo que concluimos que $3|z$.

Para el caso cuando $p > 3$ mostraremos la contrarecíproca. Sea $z \in \mathcal{O}_K$ tal que $p \nmid z$, sabemos que $N(z) = a^2 + ab + b^2\left(\frac{n+1}{4}\right)$ y multiplicando por 4 y factorizando obtenemos que $4N(z) = (2a + b)^2 + b^2n$, veamos que $p \nmid 4N(z)$. Supongamos por contradicción que $(2a + b)^2 + b^2n \equiv 0(\mathrm{mód}p)$, si $b \equiv 0(\mathrm{mód}p)$ entonces $4a^2 \equiv 0(\mathrm{mód}p)$ pero 4 y p son coprimos ya que $p > 3$ entonces 4 es invertible módulo p, asi $a \equiv 0(\mathrm{mód}p)$ lo que implica que $p|z$ lo cual es una contradicción, si $p \nmid b$ entonces son coprimos por lo tanto $-b$ es invertible módulo p, así $n \equiv ((2a + b)(-b)^{-1})^2(\mathrm{mód}p)$ lo que implica que $\left(\frac{n}{p}\right) = 1$ una contradicción por lo que $p \nmid 4N(z)$ específicamente $p \nmid N(z)$.

□

Teorema 2.3.10. *Los anillos de enteros $\mathcal{O}_K$ de $K = \mathbb{Q}(\sqrt{-n})$ para $n = 19, 43, 67, 173$ son dominios de ideales principales.*

Demostración. Primeramente veamos algunas propiedades que cumplen estos n.

I) Son números primos

II) $n \equiv -5(\mathrm{mód}\, 24)$

III) Sea $p > 3$ un primo tal que $p < \frac{2}{\pi}\sqrt{n}$, entonces $\left(\frac{n}{p}\right) = -1$

Para las primeras dos propiedades es fácil comprobar que son verdad, ahora mostremos que la tercera también es verdad. Para $n = 19$ y $n = 43$ no existen primos mayores que 3 tales que sean menores que $\frac{2}{\pi}\sqrt{n}$, cuando $n = 67$ para el único primo que hay que probar es para $p = 5$, entonces $\left(\frac{67}{5}\right) \equiv \left(\frac{2}{5}\right) (\text{mód} 5)$ y es claro que 2 no es residuo cuadrático ya que $2^{\frac{5-1}{2}} \equiv -1(\text{mód} 5)$ por lo que solo nos falta probar para $n = 173$ hay que probar para $p = 5$ y para $p = 7$, con el primero tenemos que $\left(\frac{173}{5}\right) \equiv \left(\frac{3}{5}\right) (\text{mód} 5)$ y es claro que 3 no es residuo cuadratico ya que $3^{\frac{5-1}{2}} \equiv -1(\text{mód} 5)$ y para $p = 7$ tenemos $\left(\frac{173}{7}\right) \equiv \left(\frac{-2}{7}\right)$ y es claro que -2 no es residuo cuadratico ya que $(-2)^{\frac{7-1}{2}} \equiv -1(\text{mód} 7)$.

Luego para probar que es DIP por el Teorema 2.3.6 sabemos que solo es necesario probar que el grupo de clase tiene un elemento, además como n es libre de cuadrados y $-n \equiv 5(\text{mód} 24)$ entonces $-n \equiv 1(\text{mód} 4)$, así por el Teorema 2.1 tenemos que $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})} = \mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$. Entonces debemos calcular el discriminante de la base $1, \frac{1+\sqrt{-n}}{2}$

$$\Delta\left(1, \frac{1+i\sqrt{n}}{2}\right) = \begin{vmatrix} Tr(1) & Tr(\frac{1+i\sqrt{n}}{2}) \\ Tr(\frac{1+i\sqrt{n}}{2}) & Tr(\frac{1-n+2i\sqrt{n}}{4}) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1-n}{2} \end{vmatrix} = -n$$

Además que $\frac{1+i\sqrt{n}}{2}$ es raíz de un polinomio cuadratico entonces $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ tiene solo 2 inmersiones y como $\frac{1+i\sqrt{n}}{2}$ es un número complejo entonces las dos inmersiones son complejas así $s = 1$ por lo tanto $C = \left(\frac{2}{\pi}\right)^1 \sqrt{|\Delta(1, \frac{1+\sqrt{-n}}{2})|} = \frac{2}{\pi}\sqrt{n}$. Como en la demostración del Teorema 2.3.5 solo debemos probar que los ideales de $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ que tengan norma menor que C son principales, pero primero veamos que esto ocurre con los ideales primos con norma menor que C.

Sea $\mathfrak{p}$ un ideal primo tal que $N(\mathfrak{p}) < C$, como $\mathfrak{p}$ es un ideal propio entonces $N(\mathfrak{p}) > 1$ así $N(\mathfrak{p}) = q_1 \cdots q_n$ con $q_i \in \mathbb{Z}$ numeros primos además que $N(\mathfrak{p}) \in \mathfrak{p}$ por lo tanto $\mathfrak{p} \supset \langle N(\mathfrak{p}) \rangle = \langle q_1 \rangle \cdots \langle q_n \rangle$ y como $\mathfrak{p}$ es primo existe i tal que $\mathfrak{p} \supset \langle q_i \rangle$ por lo que solo nos falta ver que $\langle q_i \rangle$ es un elemento maximal. Sabemos que $q_i | N(\mathfrak{p})$ entonces $q_i \leq N(\mathfrak{p}) < C = \frac{2}{\pi}\sqrt{n}$ entonces dividamos en casos los primos menores que C. Primer caso $q_i = 2, 3$. Sea I un ideal de $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ que contiene propiamente a $\langle 2 \rangle$ entonces existe $z \in I$ tal que $2 \nmid z$, entonces por la contrarecíproca del Lema 2.3.9 tenemos que $2 \nmid N(z)$ y como $z \in I$, entonces $N(\langle z \rangle) = |N(z)| \in \langle z \rangle \subset I$ por lo que tanto 2 como $N(z)$ pertenecen a I además que son coprimos así que por el Lema de Bezout $1 \in I$

por lo que $I = \mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$. Para el caso $q_i = 3$ es análogo al caso anterior. El último caso cuando $q_i > 3$, como esto sucede además que $q_i < \frac{2}{\pi}\sqrt{n}$ por la propiedad 3 tenemos que $\left(\frac{n}{q_i}\right) = -1$, sea J un ideal de $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ que contiene propiamente a $\langle q_i \rangle$ entonces existe $z \in J$ tal que $q_i \nmid z$ y por la contrecíproca del Lema 2.3.9 tenemos que $q_i \nmid N(z)$ por lo tanto son coprimos y por el Lema de Bezout $1 \in J$.

Terminados los casos podemos concluir que $\mathfrak{p} = \langle q_i \rangle$, solo nos falta ver que cualquier ideal con norma menor que C es principal. Sea $\mathfrak{a}$ un ideal con $N(\mathfrak{a}) < C$ como $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ tenemos que $C > N(\mathfrak{a}) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_n)$ y como todas las normas son números enteros positivos entonces $C > N(\mathfrak{p}_i)$, para todo $1 \leq i \leq n$, entonces por lo demostrado anteriormente $\mathfrak{p}_i = \langle q_i \rangle$. Así, $\mathfrak{a} = \langle q_1 \cdots q_n \rangle$ y por lo tanto principal, de esta forma cualquier ideal de $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ con norma menor que C es equivalente a $[\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]]$ por lo tanto el grupo de clase solo tiene un elemento. □

Como parte final de esta monografía, presentaremos ahora una condición para saber cuando un anillo de enteros algebraicos no es un dominio euclídeo. Para esto es necesario introducir primero el siguiente concepto.

Definición 2.3.11. Sea D un dominio entero y denotemos $\widetilde{D}$ el conjunto de los invertibles de D junto con el cero. Un elemento $u \in D \setminus \widetilde{D}$ es llamado un **divisor universal** si para todo $x \in D$ existe $z \in \widetilde{D}$ tal que $u \mid x - z$.

Ejemplo 2.3.12. 2 y 3 son divisores universales de $\mathbb{Z}$. Note que $\widetilde{\mathbb{Z}} = \{-1, 0, 1\}$ y sea $z \in \mathbb{Z}$ si z es par entonces $2|z+0$ y si es impar entonces $2|z+1$ por lo tanto 2 es divisor universal, ahora si z es divisible por 3 entonces $3|z+1$ si z deja residuo 1 al dividirse por 3 entonces $3|z-1$ y si z deja residuo 2 al dividirse por 3 entonces $3|z+1$, por lo tanto 3 también es divisor universal.

Lema 2.3.13. *Sea D un dominio entero que no es un cuerpo tal que D no tiene divisores universales. Entonces D no es un dominio euclídeo.*

Demostración. Supongamos por contradicción que D es un dominio euclídeo, entonces existe $N : D \to \mathbb{N}$ con $N(0_D) = 0$ tal que dados $a, b \in D$ con $b \neq 0_D$ existen $q, r \in D$ tal que $a = qb + r$ con $r = 0_D$ o $N(r) < N(b)$. Note que el conjunto $N(D \setminus \widetilde{D})$ es no vacío debido a que D no es cuerpo y como $N(D \setminus \widetilde{D})$ esta contenido en los números naturales entonces tiene mínimo. Sea m ese mínimo y $d \in D$ tal que $N(d) = m$, veamos que d es un divisor universal. Sea $a \in D$, como D es euclídeo existen $q, r \in D$ tal que $a = dq + r$

con $r = 0_D$ o $N(r) < N(d)$ pero como $N(d)$ es el mínimo de $N(D \setminus \widetilde{D})$, entonces $r \notin D \setminus \widetilde{D}$, así $r \in \widetilde{D}$ y como $d|a - r$ se tiene que d es un divisor universal. □

Teorema 2.3.14. *Los anillos de enteros de* $\mathbb{Q}(\sqrt{-n})$ *donde* n *es libre de cuadrados,* $n > 4$ *y* $n \equiv -5(\text{mód}24)$ *no son euclídeos.*

Demostración. Debido a que $-n \equiv 5(\text{mód}24)$ entonces $-n \equiv 1(\text{mód}4)$, así por el Ejemplo 2.1 tenemos que $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})} = \mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$. Veamos primero que $U(\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]) = \{-1, 1\}$. Sea $a+b\left(\frac{1+\sqrt{-n}}{2}\right)$ invertible, entonces $N(a+b\left(\frac{1+\sqrt{-n}}{2}\right)) = \pm 1$, así $\pm 1 = N(a+b\left(\frac{1+\sqrt{-n}}{2}\right)) = (a+b\left(\frac{1+\sqrt{-n}}{2}\right))(a+b\left(\frac{1-\sqrt{-n}}{2}\right)) = a^2+ab+b^2\frac{(n+1)}{4}$ y multiplicando todo por 4 y factorizando obtenemos $\pm 4 = (2a+b)^2 + b^2 n$. Como $n > 0$ entonces la norma debe ser positiva, luego si $b \neq 0$ entonces $b^2 n > 4$ debido a que $n > 4$ además como $4 < b^2 n < (2a+b)^2 + b^2 n = 4$ lo que sería una contradicción por lo tanto $b = 0$ lo que nos deja con $4 = (2a)^2$ y entonces $a = \pm 1$. Con esto podemos decir que $\widetilde{\mathbb{Z}}[\frac{1+\sqrt{-n}}{2}] = \{-1, 0, 1\}$.

Supongamos por contradicción que existe d divisor universal de $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$, entonces por definición d divide a $2-1$ o $2+0$ o $2+1$ así que como d no puede ser invertible entonces $d|2$ o $d|3$ pero veamos que $2, 3$ son irreducibles en $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$. Sea $z = a + b\left(\frac{1+\sqrt{-n}}{2}\right)$ un divisor de 2 que no sea invertible, comprobemos que es asociado a 2, como $z|2$ entonces $N(z)|N(2) = 4$ y los divisores de 4 en los enteros son $\pm 1, \pm 2, \pm 4$ pero como z no es invertible entonces $N(z) = \pm 2$ o $N(z) = \pm 4$ por lo que podemos concluir que $2|N(z)$ y por el Lema 2.3.9 tenemos que $2|z$ lo que implica que z y 2 son asociados. La prueba para el número 3 es análogo al caso anterior.. Entonces al 2 y 3 ser irreducible y $d|2$ o $d|3$ y d no es invertible entonces $d = \pm 2$ o $d = \pm 3$, además como d es un divisor universal entonces d divide a alguno de los siguientes numeros

$$\frac{1+\sqrt{-n}}{2} - 1 = \frac{-1+\sqrt{-n}}{2}, \quad \frac{1+\sqrt{-n}}{2} + 0 = \frac{1+\sqrt{-n}}{2}, \quad \frac{1+\sqrt{-n}}{2} + 1 = \frac{3+\sqrt{-n}}{2}$$

entonces $N(d)$ divide a la norma de alguno de estos 3 y como $N(d) = 4$ o $N(d) = 9$ entonces una de estas normas debe ser múltiplo de 2 o múltiplo de 3 por lo que solo nos falta ver que esto no es verdad.

En el primer caso, $N\left(\frac{-1+\sqrt{-n}}{2}\right) = \frac{1+n}{4}$ como $n + 5 \equiv 0(\text{mód}24)$ entonces $n + 5 = 24k$ y reescribiendo y dividiendo por 4 obtenemos que $\frac{n+1}{4} + 1 = 6k$ lo que implica que $\frac{n+1}{4} \equiv -1(\text{mód}6)$, así $\frac{n+1}{4} \equiv 1(\text{mód}2)$ y $\frac{n+1}{4} \equiv -1(\text{mód}3)$ por lo tanto ni 2 ni 3 dividen a esta norma. Ahora, $N\left(\frac{1+\sqrt{-n}}{2}\right) = \frac{1+n}{4}$ la cual es la misma norma del número anterior así

que ya está. Finalmente, $N\left(\frac{3+\sqrt{-n}}{2}\right) = \frac{9+n}{4}$ como $n+5 \equiv 0(\mathrm{mód}\, 24)$ entonces $n+5 = 24k$ y reescribiendo y dividiendo por 4 obtenemos que $\frac{n+9}{4} - 1 = 6k$ lo que implica que $\frac{n+9}{4} \equiv 1(\mathrm{mód} 6)$, así $\frac{n+9}{4} \equiv 1(\mathrm{mód} 2)$ y $\frac{n+9}{4} \equiv 1(\mathrm{mód} 3)$ por lo tanto ni 2 ni 3 dividen a esta norma. Por lo que con esto podemos concluir que $\mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ no tiene divisores universales y por el Lema anterior no es euclídeo. □

Corolario 2.3.15. *Los anillos de enteros $\mathcal{O}_K$ de $K = \mathbb{Q}(\sqrt{-n})$ para $n = 19, 43, 67, 173$ son dominios de ideales principales y no son euclídeos.*

Bibliografía

BROCHERO Fabio, MOREIRA Carlos SALDANHA Nicolau TENGAN Eduardo. *Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro*. Terceira edição. IMPA (vid. págs. 14, 18, 39).

FRALEIGH, Jhon. *A First Course in Abstract Algebra*. Addison-Wesley, 2003 (vid. pág. 8).

SPINDLER, Karlheinz. *Abstract Algebra with Applications. Volume 2: Rings and Fiels*. Chapman, Hall/CRC Pure y Applied Mathematics, 1993 (vid. pág. 8).