SOBRE PRIMOS REGULARES Y EL ÚLTIMO TEOREMA DE FERMAT

MARÍA ANGÉLICA OLIVEROS CAICEDO

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE CIENCIAS

ESCUELA DE MATEMÁTICAS

BUCARAMANGA

2020

SOBRE PRIMOS REGULARES Y EL ÚLTIMO TEOREMA DE FERMAT

MARÍA ANGÉLICA OLIVEROS CAICEDO

Trabajo de Grado para optar al título de
Matemática

Director
Héctor Edonis Pinedo Tapia
Doctor en ciencias

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2020

AGRADECIMIENTOS

Varias personas han contribuido de una u otra forma construyéndome profesional y personalmente. Especialmente quiero agradecer a:

Agradezco a mis padres: Rosmira Caicedo Florez y Orlando Oliveros Jaimes, por su apoyo incondicional. También agradezco al profesor **Dr. Héctor Edonis Pinedo** por su colaboración y empeño en el desarrollo de este trabajo, y a mis maestros por su ayuda para realizar este libro como lo son: Michael Rincón Villamizar y Jorge Eliécer Gómez Ríos, a mis hermanas especialmente a mi gemela y amiga Alejandra Oliveros.

Agradezco a Crhistian por su cariño y apoyo en la realización de este documento. Y finalmente agradezco a mis amigas por su cariño y apoyo, tanto en mi camino por lograr mi título en matemáticas como en lo personal.

CONTENIDO

RESUMEN

TÍTULO: SOBRE PRIMOS REGULARES Y EL ÚLTIMO TEOREMA DE FERMAT [1]

AUTOR: MARÍA ANGÉLICA OLIVEROS CAICEDO [2]

PALABRAS CLAVE: EXTENSIONES DE CUERPOS, CUERPOS CICLOTÓMICOS, GRUPO DE CLASE, NORMA, TRAZA.

DESCRIPCIÓN:

El Último Teorema de Fermat, conjeturado por Pierre de Fermat en 1637, establece que la ecuación diofántica

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

no tiene soluciones enteras no nulas si $n \geq 3$.

Esta conjetura fue escrita por Fermat en el margen del libro de la *Arithmetica* de Diofanto y así mismo incluyó: “Poseo una demostración en verdad maravillosa para este hecho, pero este margen es demasiado estrecho para contenerla", con lo cual el Último Teorema de Fermat pasó a ser una conjetura de interés para grandes matemáticos como lo son: Euler, Dirichlet, Legendre, Gauss, Sophie Germain y Lebesgue, quienes en sus intentos por demostrarla hicieron fuertes aportes a la matemática, algunos de ellos llegando a probar el Último Teorema de Fermat para un n en específico. Al querer dar una prueba general nunca antes lograda, fue evolucionando la teoría algebraica de números. En 1839 Lamé había conseguido dar una demostración general, pero esta prueba afirmaba una factorización única en $\mathbb{Z}[\zeta_n]$, donde $\zeta_n = e^{\frac{2\pi i}{n}}$. Más adelante Kummer probó que $\mathbb{Z}[\zeta_n]$ no siempre tiene factorización única; en efecto $\mathbb{Z}[\zeta_{23}]$ no tiene factorización única.

Kummer consiguió demostrar el Último Teorema de Fermat para una clase de n específico, los llamados *primos regulares*. En esta monografía, estudiaremos algunos detalles de la demostración para tales n, que nos garantiza factorización única en $\mathbb{Z}[\zeta_n]$.

---

[1] Trabajo de grado.

[2] Facultad ciencias, escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en ciencias P.H.D.

ABSTRACT

TÍTULO: ABOUT REGULAR PRIMES AND THE LAST FERMAT THEOREM [3]

AUTHOR: MARÍA ANGÉLICA OLIVEROS CAICEDO [4]

KEYWORDS: FIELD EXTENSIONS, CYCLOTOMIC FIELDS, CLASS GROUP, NORM, TRACE.

DESCRIPTION:

Fermat's Last Theorem, surmised by Pierre de Fermat in 1637, states that the diophantic equation

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

doesn't have whole solutions not zero if ≥ 3.

This conjecture was written by Fermat in the margin of the book of *the Arithmetic* of Diophanto and also included: "I possess a truly wonderful proof for this fact, but this margin is too narrow to contain it", thus making Fermat's Last Theorem an interesting conjecture for great mathematicians such as they are: Euler, Dirichlet, Legendre, Gauss, Sophie Germain and Lebesgue, who in their attempts to prove it made strong contributions to mathematics, some of them even proving Fermat's Last Theorem for a specific n. By wanting to give a general proof never before achieved, the algebraic theory of numbers was evolving. In 1839 Lamé had managed to give a general proof, but this proof claimed a unique factorization in $\mathbb{Z}[\zeta_n]$, where $\zeta_n = e^{\frac{2\pi i}{n}}$. Kummer later proved that $\mathbb{Z}[\zeta_n]$ does not always have unique factoring; indeed $\mathbb{Z}[\zeta_{23}]$ does not have unique factoring.

Kummer managed to prove Fermat's Last Theorem for a specific class of n, the so-called *regular prime*. We will limit ourselves to the proof for such a n.In this monograph, we will study some details of the proof for such n, which guarantees us unique factorization into $\mathbb{Z}[\zeta_n]$.

---

[3] Grade work.

[4] Faculty of Science, Math school. Director: Héctor Edonis Pinedo Tapia, Doctor of science P.H.D.

INTRODUCCIÓN

El llamado “Último Teorema de Fermat" (UTF) planteado en 1637 por Pierre de Fermat, demostrado por Andres Wiles [5] tres siglos más tarde, es un resultado fundamental en la teoría de números y presenta un problema sobre las soluciones de una ecuación diofántica. La búsqueda de su demostración estimuló el desarrollo de varias ramas de la matemática, especialmente la teoría algebraica de números.

El teorema establece que:

Si $n \in \mathbb{Z}$ con $n \geq 3$, entonces no existen $x, y, z \in \mathbb{Z}$ no nulos tales que se cumpla la igualdad

$$x^n + y^n = z^n. \tag{1}$$

Ernst Kummer (1810-1893) [6] en 1844 encontró una manera de demostrar el Último Teorema de Fermat para un gran número de posibles valores para n, los llamados *primos regulares*[7]. El argumento de Kummer consiste en factorizar la ecuación de Fermat (1) en el anillo de enteros $\mathbb{Z}[\zeta_p]$ del cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$, donde ζ_p es la raíz $p-$ésima de la unidad [8] dada por $\zeta_p = e^{\frac{2\pi i}{p}}$. Observe que

$$x^p + y^p = \prod_{i=0}^{p-1} (x + {\zeta_p}^i y) = z^p.$$

Se creía que este anillo de enteros compartían para todo ζ_p la mismas propiedades, en particular que se tenía factorización única. Sin embargo Ernst Kummer mostró que no siempre se da un Dominio de Factorización Única (DFU). De hecho, $\mathbb{Z}[\zeta_{23}]$ no satisface la propiedad de factorización única. En el

---

[5] A. WILES. “Modular elliptic curves and Fermat’s last theorem”. En: *Ann. of Math. (2)* 141.3 (1995), págs. 443-551. DOI: 10.2307/2118559.

[6] S. SINGH. *Fermat’s enigma*. The epic quest to solve the world’s greatest mathematical problem, With a foreword by John Lynch. Walker y Company, New York, 1997, págs. xx+315.

[7] *Primo Regular:* p es un primo regular si no divide al número de clase del cuerpo ciclótomico p. Ver Definición (3.3.6).

[8] Recordemos que las raíces $p-$ésimas de la unidad son las raíces de $x^p - 1 = 0$ y todas vienen dada por ${\zeta_p}^i$ con $i \in \{0, 1, \cdots, p-1\}$.

siguiente texto se darán herramientas necesarias para garantizar factorización única, condición que se podrá determinar cuando n es un primo regular.

Esta monografía consta de (5) capítulos. En el primer capítulo se presentan las definiciones de extensión de cuerpos, elemento algebraico y grado de una extensión, e introduciremos la definición de cuerpo numérico, anillo de enteros y daremos algunos ejemplos.

Para el segundo capítulo, dado un cuerpo numérico se darán algunas proposiciones para determinar su anillo de enteros, el cual es dominio entero. Se recordarán algunos resultados sobre los conceptos de ideales, elementos: asociados, irreducibles, primos; sobre estos dominios enteros.

Sabemos que toda extensión de cuerpos de $\mathbb{L}$ sobre $\mathbb{K}$ permite que $\mathbb{L}$ actúe como un $\mathbb{K}$ espacio vectorial. Si esta extensión es finita, entonces $\mathbb{L}$ tiene dimensión finita como $\mathbb{K}-$espacio vectorial, y esto nos proporciona explícitamente una base. Así, en el tercer capítulo enunciaremos la definición de base en un cuerpo, y extenderemos tal concepto para módulos, en particular, definiremos $\mathbb{Z}-$base para un $\mathbb{Z}-$módulo libre. Introduciremos la definición de discriminante, la cual nos permitirá decir si los elementos de una $\mathbb{Q}-$base forman una $\mathbb{Z}-$base y finalmente introducir la definición de grupo de clase sobre un anillo de enteros.

En el cuarto capítulo veremos que el cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$ es un cuerpo numérico y $\mathbb{Z}[\zeta_p]$ coincide con el anillo de enteros de $\mathbb{Q}(\zeta_p)$, veremos cómo las definiciones y resultados anteriores se comportan sobre estas estructuras algebraicas. Finalmente, presentaremos la prueba del Último Teorema de Fermat para n primo regular.

1. PRELIMINARES

En esta sección se darán algunas definiciones preliminares y ejemplos sobre extensiones de cuerpos y números algebraicos, e introduciremos las definiciones de: cuerpo numérico, anillo de enteros, norma y traza en cuerpos numéricos. Se mencionarán teoremas y proposiciones cuyas demostraciones pueden encontrarse en: [9], [10], [11] y [12]. Estas definiciones, teoremas y proposiciones serán necesarias para comprender el fundamento teórico de la prueba del Último Teorema de Fermat para n un primo regular.

1.1. EXTENSIONES DE CUERPOS

Definición 1.1.1. Sean $\mathbb{L}$ y $\mathbb{K}$ cuerpos. Decimos que $\mathbb{L}$ es una extensión de $\mathbb{K}$ si $\mathbb{K} \subseteq \mathbb{L}$. Cuando esto ocurra usaremos la notación $\mathbb{L}/\mathbb{K}$.

Dada la extensión de cuerpos $\mathbb{L}/\mathbb{K}$, entonces $\mathbb{L}$ tiene estructura de espacio vectorial sobre $\mathbb{K}$, en donde los elementos en el cuerpo $\mathbb{L}$ son vectores y los elementos en el cuerpo $\mathbb{K}$ son escalares. Aquí la operación de adición es la suma en $\mathbb{L}$ y producto de un elemento de $\mathbb{K}$ por un elemento de $\mathbb{L}$ define la operación de producto por escalar.

Ejemplo 1.1.2. Algunos ejemplos de extensiones son $\mathbb{C}/\mathbb{R}$ y $\mathbb{R}/\mathbb{Q}$, pues $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Definición 1.1.3. Sea $\mathbb{L}/\mathbb{K}$ una extensión, se llama grado de la extensión a la dimensión de $\mathbb{L}$ como $\mathbb{K}$ espacio vectorial y se denota por $[\mathbb{L} : \mathbb{K}] = dim_{\mathbb{K}}(\mathbb{L})$. Diremos que la extensión es finita, sí la dimensión de $\mathbb{L}$ como $\mathbb{K}-$espacio vectorial es finita y la denotaremos como

---

[9] D. S. DUMMIT y R. M. FOOTE. *Abstract algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991, págs. xiv+658.

[10] GOMEZ R. *El anillo de los enteros algebraicos y dominios de Dedekind*. Bucaramanga - Colombia, 2015.

[11] K. SPINDLER. *Abstract algebra with applications. Vol. II*. Rings and fields. Marcel Dekker, Inc., New York, 1994, págs. xvi+531.

[12] D. STEWART I. Y TALL. *Algebraic number theory and Fermat's last theorem*. Third. A K Peters, Ltd., Natick, MA, 2002, págs. xx+313.

$$dim_{\mathbb{K}}(\mathbb{L}) < +\infty.$$

Recordemos el siguiente resultado, el cual nos garantiza la existencia de raíces de polinomios.

Teorema 1.1.4 (Teorema de Kronecker)**.** Sean $\mathbb{K}$ un cuerpo y $p(t)$ un polinomio no constante en $\mathbb{K}[t]$. Entonces existe una extensión de cuerpos $\mathbb{L}/\mathbb{K}$ y un elemento $\alpha \in \mathbb{L}$ tal que $p(\alpha) = 0$.
Demostración: Véase Proposición 13.1. [11].

Definición 1.1.5. Sean $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos y $p(t) = a_0 + \cdots + a_n t^n \in \mathbb{K}[t]$. Diremos que el grado de $p(t)$ es el mayor n tal que a_n es no nulo y este se denota por $\partial p(t)$.

Definición 1.1.6. Sean $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos y $p(t) \in \mathbb{K}[t]$. Diremos que $p(t)$ es irreducible sobre $\mathbb{K}$, si no existen polinomios $q, r \in \mathbb{K}[t]$ tal que:

$$p(t) = q(t)r(t), \text{ con } \max\{\partial q, \partial r\} < \partial p.$$

Ejemplo 1.1.7. Sea $p(t) = t^5 + t^4 + 1 \in \mathbb{Z}_2[t]$. Podemos escribir a $p(t)$ como producto de irreducibles, así $p(t) = (t^2 + t + 1)(t^3 + t + 1)$. Sigue de la demostración del Teorema de Kronecker que para encontrar una extensión de cuerpos $\mathbb{L}$ de $\mathbb{Z}_2$ en la que $p(t)$ tiene una raíz en $\mathbb{L}$, podemos tomar a $\mathbb{L}$ como $\mathbb{Z}_2[t]/\langle t^2 + t + 1\rangle$ o $\mathbb{Z}_2[t]/\langle t^3 + t + 1\rangle$.

Teorema 1.1.8 (Criterio de irreducibilidad de Eisenstein)**.** Sean $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$ y p un número primo tal que:
(a) $p \mid a_i$ con $i \neq n$
(b) $p \nmid a_n$
(c) $p^2 \nmid a_0$
Entonces $f(t)$ es irreducible sobre $\mathbb{Q}[t]$.
Demostración: Véase Teorema 1.8. [12].

Definición 1.1.9. Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos, $\alpha \in \mathbb{L}$. Entonces $\mathbb{K}(\alpha)$ denota al cuerpo más pequeño tal que $K \subseteq \mathbb{K}(\alpha)$ y $\alpha \in \mathbb{K}(\alpha)$.

Observación: Note que $\mathbb{K}(\alpha)$ coincide con el cuerpo de fracciones de $\mathbb{K}[\alpha]$. Se puede ver que

$$\mathbb{K}(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : \ f, g \in \mathbb{K}[t], g(\alpha) \neq 0 \right\}.$$

Definición 1.1.10. Un elemento primitivo de una extensión de cuerpos $\mathbb{L}/\mathbb{K}$ es un elemento $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$.

Definición 1.1.11. Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos. Diremos que $\alpha \in \mathbb{L}$ es algebraico sobre $\mathbb{K}$ si existe $f \in \mathbb{K}[t]$ no nulo tal que $f(\alpha) = 0$. En caso contrario, diremos que α es trascendente sobre $\mathbb{K}$.

Ejemplo 1.1.12. En la extensión $\mathbb{C}/\mathbb{Q}$ tenemos que

- $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$, pues es raíz del polinomio $t^2 - 2$.
- $\sqrt[n]{m}$ es algebraico sobre $\mathbb{Q}$, siendo raíz del polinomio $x^n - m$, con $m \in \mathbb{Q}$.
- π, e son trascendentes sobre $\mathbb{Q}$ (véase en Página 51 [13]).

La suma y producto de elementos algebraicos es algebraico. Veamos el siguiente ejemplo: Sean $\sqrt{2}, i \in \mathbb{C}$ dos elementos algebraicos sobre $\mathbb{Q}$, cuyos polinomios son $t^2 - 2$ y $t^2 + 1$ respectivamente, veamos que para afirmar que $\sqrt{2} + i$ es algebraico sobre $\mathbb{Q}$ debemos hallar un polinomio $p(t) \in \mathbb{Q}[t]$ tal que $p(\sqrt{2} + i) = 0$, así:

$$\begin{aligned} t &= \sqrt{2} + i, \\ t^2 &= (\sqrt{2} + i)^2, \\ t^2 &= (2 + 2\sqrt{2}i + i^2), \\ t^2 &= 1 + 2\sqrt{2}i, \\ (t^2 - 1)^2 &= (2\sqrt{2i})^2, \\ t^4 - 2t^2 + 1 &= 8i^2, \\ t^4 - 2t^2 + 1 &= -8, \\ t^4 - 2t^2 + 9 &= 0, \end{aligned}$$

donde $p(t) = t^4 - 2t^2 + 9 \in \mathbb{Q}[t]$. Así, existe un polinomio $p(t) \in \mathbb{Q}[t]$ tal que $p(\sqrt{2} + i) = 0$. Esto no sucede en el caso de los trascendentes ya que, por ejemplo, $\pi - \pi = 0$ y 0 no es trascendente.

Definición 1.1.13. Una extensión $\mathbb{L}/\mathbb{K}$ se dice algebraica si cada elemento de $\mathbb{L}$ es algebraico sobre $\mathbb{K}$. En caso contrario, diremos que $\mathbb{L}/\mathbb{K}$ es trascendente.

Ejemplo 1.1.14. Algunos ejemplos de la Definición (1.1.13)

- Sea α algebraico sobre $\mathbb{Q}$, entonces la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ es algebraica ya que todo elemento de $\mathbb{Q}$ es algebraico y α es algebraico.

---

[13] C. GÓMEZ. *Biografías de cinco números maravillosos* $\varphi,\ \pi,\ c,\ e,\ i$.. Editorial Universidad de Caldas., 2005.

- La extensión $\mathbb{Q}(\pi)/\mathbb{Q}$ no es algebraica ya que π no es algebraico.

Definición 1.1.15. Sea $p(t) = a_0 + \cdots + a_n t^n \in \mathbb{K}[t]$. Diremos que

- a_n es el coeficiente principal de $p(t)$.
- $p(t)$ es llamado mónico si su coeficiente principal es 1.

Proposición 1.1.16. Sea $\alpha \in \mathbb{L}$ algebraico sobre $\mathbb{K}$. Entonces existe un único polinomio mónico e irreducible $p(t) \in \mathbb{K}[t]$ tal que $p(\alpha) = 0$.
Demostración: Véase Capítulo 13, Proposición 9 [9].

Definición 1.1.17. Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos. El polinomio de la Proposición (1.1.16) es llamado polinomio minimal de α sobre $\mathbb{K}$ y lo denotamos por $m_\alpha(t)$. El grado de $m_\alpha(t)$ es llamado el grado de α.

Ejemplo 1.1.18. Note que $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$. Ya que si $p(t) = t^2 + 1$ entonces:

1. i es una raíz de $p(t)$, pues, $p(i) = i^2 + 1 = -1 + 1 = 0$.
2. $p(t)$ es mónico, ya que su coeficiente principal es 1.
3. $p(t)$ es irreducible.

Así, $p(t)$ es el polinomio minimal de i sobre $\mathbb{R}$.

Teorema 1.1.19. Si $\mathbb{L}/\mathbb{K}$ es una extensión y $\alpha \in \mathbb{L}$, entonces α es algebraico sobre $\mathbb{K}$ si, y solo si, $\mathbb{K}(\alpha)$ es una extensión finita de $\mathbb{K}$. En este caso, $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$.

Demostración: Véase Teorema 1.11. [12].

Teorema 1.1.20. Sean $\mathbb{L}/\mathbb{K}$ una extensión y $\alpha \in \mathbb{L}$ algebraico sobre $\mathbb{K}$, entonces:

(a) El polinomio minimal de α divide a todo polinomio $p(t) \in \mathbb{K}[t]$ tal que $p(\alpha) = 0$.

(b) El conjunto $I_\alpha := \{f(t) \in \mathbb{K}[t] - \{0\} \ : \ f(\alpha) = 0\}$ es un ideal no nulo de $\mathbb{K}[t]$.

(c) $[\mathbb{K}(\alpha) : \mathbb{K}] = n$, donde $n = \partial m_\alpha(t)$ y una base para $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$ es $\mathcal{B} := \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$.

Demostración: Véase (a), (b) en Proposición 12.7. y (c) en Teorema 12.10. [11].

Proposición 1.1.21. Toda extensión finita es algebraica.
Demostración:

Demostraremos por reducción al absurdo que $\mathbb{L}/\mathbb{K}$ es algebraica. Supongamos que $\mathbb{L}/\mathbb{K}$ es trascendente. Luego existe $\alpha \in \mathbb{L}$ trascendente sobre $\mathbb{K}$ es decir, para todo $n \in \mathbb{N}$ $\{1, \alpha, \cdots, \alpha^n\}$ es linealmente independiente[14]. Así $[\mathbb{L} : \mathbb{K}] = +\infty$, lo cual es absurdo pues $\mathbb{L}/\mathbb{K}$ es finita. Por tanto $\mathbb{L}/\mathbb{K}$ es algebraica.

El recíproco no es cierto, veamos el siguiente ejemplo:

Ejemplo 1.1.22. Sean $\mathbb{R}/\mathbb{Q}$ una extensión de cuerpos y $\overline{\mathbb{Q}}$ la clausura algebraica[15] de $\mathbb{Q}$ en $\mathbb{R}$. Veamos que $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. En efecto, para cada $n \leq 1$ $\sqrt[n]{2}$ es algebraico, pues es raíz del polinomio mónico $f(t) = t^n - 2$, que también es irreducible en $\mathbb{Q}[t]$ por el criterio de Eisenstein con $p = 2$. Así $f(t)$ es el polinomio minimal de $\sqrt[n]{2}$ sobre $\mathbb{Q}$, con lo cual $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, con n arbitrario, por tanto $\overline{\mathbb{Q}}/\mathbb{Q}$ no puede ser finita, pues $\mathbb{Q}(\sqrt[n]{2}) \subseteq \overline{\mathbb{Q}}$, para cada $n \in \mathbb{N}$.

1.2. SOBRE ELEMENTOS ALGEBRAICOS EN EL SUBCUERPO DE LOS NÚMEROS COMPLEJOS.

En esta sección introduciremos la definición de: número algebraico, entero algebraico, cuerpo numérico y anillo de enteros de un cuerpo numérico, las cuales se determinan al realizar una extensión de cuerpos sobre $\mathbb{Q}$.

Definición 1.2.1. Diremos que $\alpha \in \mathbb{C}$ es un número algebraico si es algebraico sobre $\mathbb{Q}$.

Definición 1.2.2. Sean $\mathbb{K}$, $\mathbb{W}$, $\mathbb{L}$ cuerpos tales que $\mathbb{K} \subseteq \mathbb{W} \subseteq \mathbb{L}$. Entonces $\mathbb{W}$ es llamado un cuerpo intermedio de la extensión $\mathbb{L}/\mathbb{K}$.

Teorema 1.2.3. Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos con cuerpo intermedio $\mathbb{W}$. Entonces se satisface la siguiente expresión:

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{W}][\mathbb{W} : \mathbb{K}].$$

---

[14] En caso contrario, al ser linealmente dependiente, existen $\lambda_0, \cdots, \lambda_n \in \mathbb{K}$ tales que $\lambda_0 + \lambda_1\alpha + \cdots + \lambda_n\alpha^n = 0$, y en tal caso α es raíz de $\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n \in \mathbb{K}[x]$, lo que contradice que α es trascendente.

[15] La clausura algebraica de $\mathbb{Q}$, denotada por $\overline{\mathbb{Q}}$ se define como:

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \exists p(t) \in \mathbb{Q}[t] \; tal \; que \; p(\alpha) = 0\}.$$

En particular, $[\mathbb{L} : \mathbb{K}]$ es finita si, y solo si, $[\mathbb{L} : \mathbb{W}][\mathbb{W} : \mathbb{K}]$ son ambas finitas.

Demostración: Véase Teorema 12.11, página 221 [11].

Cuando tenemos los números algebraicos $\alpha_1, \cdots, \alpha_n$ tenemos la extensión $\mathbb{Q}(\alpha_1) \cdots, (\alpha_n)$, a esta la denotaremos como $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$.

Teorema 1.2.4. El conjunto A de números algebraicos es un subcuerpo del cuerpo de los complejos $\mathbb{C}$.

Demostración:

Por (c) del Teorema (1.1.20) tenemos que si α es un número algebraico, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es finito. Supongamos que α, β son números algebraicos entonces

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Dado que β es algebraico sobre $\mathbb{Q}$, también es algebraico sobre $\mathbb{Q}(\alpha)$, y por la Proposición (1.1.21) $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ es finito, por tanto $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ es finito. Y para cada α, β algebraicos entonces $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, y $\alpha\beta^{-1}$ con $\beta \neq 0$ pertenecen a $\mathbb{Q}(\alpha, \beta)$. Así todos estos están en A por tanto es cuerpo.

Definición 1.2.5. Sea $\mathbb{K} \subseteq \mathbb{C}$ subcuerpo. Decimos que $\mathbb{K}$ es un cuerpo numérico si $[\mathbb{K} : \mathbb{Q}]$ es finita.

Teorema 1.2.6. Si $\mathbb{K}$ es un cuerpo numérico, entonces $\mathbb{K} = \mathbb{Q}(\alpha)$, para algún número algebraico α.

Demostración: Véase Teorema 2.2. [12]

Ejemplo 1.2.7. Sea d libre de cuadrados, con $\sqrt{d} \in \mathbb{C}$. Tenemos al cuerpo numérico $\mathbb{Q}(\sqrt{d})$, llamado cuerpo cuadrático.

Definición 1.2.8. Un número complejo α es un entero algebraico si existe $p(t) \in \mathbb{Z}[t]$ mónico tal que $p(\alpha) = 0$. El conjunto $B = \{\alpha \in \mathbb{C} : p(\alpha) = 0 \; con \; p(t) \in \mathbb{Z}[t], \text{ mónico}\}$, es llamado el conjunto de los enteros algebraicos.

Teorema 1.2.9. El conjunto de los enteros algebraicos es un subanillo del cuerpo de los números algebraicos.

Demostración: Véase Teorema 2.9. [12] y Corolario 2.3. [10]

Definición 1.2.10. Si $\mathbb{K}$ es un cuerpo numérico, se define el anillo de enteros de $\mathbb{K}$, el cual representamos por $\mathcal{K}$, como

$$\mathcal{K} = \mathbb{K} \cap B,$$

donde B es el anillo de los enteros algebraicos.

En adelante usaremos $\mathcal{K}$ para referirnos al anillo de enteros de un cuerpo numérico $\mathbb{K}$.

Proposición 1.2.11. Si d es un entero libre de cuadrados, entonces el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es:

$$\mathcal{K} = \begin{cases} \mathbb{Z}[\sqrt{d}] & si \quad d \not\equiv 1 \ (\text{mód } 4) \\ \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & si \quad d \equiv 1 \ (\text{mód } 4) \end{cases}$$

Demostración: Véase Proposición 1.24. [16].

Definición 1.2.12. La característica de un cuerpo $\mathbb{K}$ se define como el mínimo $n \in \mathbb{Z}$ tal que $nx = 0$, para todo $x \in \mathbb{K}$.

Proposición 1.2.13. Un cuerpo $\mathbb{K}$ tiene característica cero o p, con p un número primo.
Demostración: Véase Proposición 1, página 510. [9].

Ejemplo 1.2.14. Los cuerpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ tienen característica cero, pues, el n tal que satisface la definición es $n = 0$.

Ejemplo 1.2.15. Si p primo $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo, cuya característica es p, ya que para todo $[x] \in \mathbb{Z}_p$ tenemos que $xp \equiv 0 \ (\text{mód } p)$.

Definición 1.2.16. Sean $\mathbb{K}$ un cuerpo y $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{K}[t]$, la derivada de f se define como $f' = Df = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}$.

Se verifica directamente que

$$\begin{aligned} D(f+g) &= Df + Dg, \\ D(fg) &= (Df)g + f(Dg), \\ D(f \circ g) &= (Df \circ g)(Dg). \end{aligned}$$

Proposición 1.2.17. Sean $\mathbb{K}$ un cuerpo de característica cero y $p(t) \in \mathbb{K}[t]$. Si $D(p(t)) = 0$, para todo t, entonces $p(t)$ es constante.

---

[16] A. RIOS. *Teoría de números algebraicos*. 2019.

Demostración: Sea $p(t) = a_0 + \cdots + a_n t^n$ luego $Dp(t) = a_1 + 2a_2 t + \cdots + na_n t^{n-1}$, por hipótesis tenemos que $Dp(t) = 0$, para todo t entonces:

$$\begin{aligned} Dp(t) &= a_1 + 2a_2 t + \cdots + na_n t^{n-1} \\ &= 0 + 0t + \cdots + 0t^{n-1}. \end{aligned}$$

Así, $a_1 = 0$, $2a_2 = 0$, $3a_3 = 0$, $\cdots$, $na_n = 0$, y puesto que $\mathbb{K}$ tiene característica cero, tenemos $a_1 = a_2 = \cdots = a_n = 0$. Por tanto, $p(t) = a_0$, así concluimos que $p(t)$ es constante.

Es importante hacer énfasis en la necesidad de la hipótesis de que un cuerpo $\mathbb{K}$ tenga característica cero en la Proposición (1.2.17), lo cual se hace visible en el siguiente ejemplo:

Ejemplo 1.2.18. Sean $\mathbb{K}$ un cuerpo con característica p con p primo y $f(x) = x^p$ notemos que $Df(x) = px^{p-1} = 0$, para todo $x \in \mathbb{K}$ y $f(x)$ no es constante.

Definición 1.2.19. Sean $f, g \in \mathbb{K}[t]$. Diremos que el máximo común divisor de los polinomios f y g es el polinomio $d \in \mathbb{K}[t]$, denotado por $(f, p) = d$, que satisface las siguientes condiciones:

- $\partial d > 0$.
- $d \mid f$ y $d \mid g$.
- Si $h \in \mathbb{K}[t]$ es tal que $h \mid f$ y $h \mid g$, entonces $f \mid d$.

Teorema 1.2.20. Si $\mathbb{K}$ es un cuerpo de característica cero. Un polinomio f no nulo en $\mathbb{K}$ es divisible por el cuadrado de un polinomio no constante g tal que $\partial g > 0$ si, y solo si, f y Df tiene un factor común g tal que $\partial g > 0$.

Demostración:

$\Rightarrow$) Supongamos $f = g^2 h$. Entonces $Df = g^2 Dh + 2g(Dg)h = g(g(Dh) + 2(Dg)h)$ así f y Df tienen a g como un factor común.

$\Leftarrow$) Supongamos f no es divisible por un polinomio cuadrado es decir $f = gh$, con $(g, h) = 1$. Entonces $Df = (Dg)h + g(Dh)$, por hipótesis f y Df tienen un factor común g, entonces g es un factor de $h(Dg)$. Sí $Dg = 0$ luego por la Proposición (1.2.17) g es constante, lo cual es absurdo pues $\partial g > 0$.

Si $Dg \neq 0$ entonces como g divide a $h(Dg)$ y, g y h son primos relativos entonces $g \mid Dg$ por tanto

existe $w \in \mathbb{K}$, así al sustituir en Df tenemos que

$$\begin{aligned} Df &= h(Dg) + g(Dh) \\ &= h(gw) + g(Dh) \\ &= g((hw) + Dh). \end{aligned}$$

Con $\partial g > 1$, esto implica un absurdo pues f tendría un factor cuadrado en g.

Proposición 1.2.21. Un polinomio irreducible sobre un cuerpo numérico $\mathbb{K}$ no tiene ceros repetidos.
Demostración:
Sea $f \in \mathbb{K}[t]$ un polinomio irreducible sobre $\mathbb{K}$. Entonces $(f, Df) = 1$, es decir, no tienen factores en común. En efecto, si tuvieran un factor en común entonces $(f, Df) = g$ y por definición $g \mid f$ y $g \mid Df$. Por el Teorema (1.2.20) f sería divisible por el cuadrado de un polinomio de grado mayor a cero esto negaría que f es irreducible. Así, $(f, Df) = 1$ y por tanto existen $a, b \in K[t]$ tales que $af + bDf = 1$. La misma ecuación interpretada sobre $\mathbb{C}$ muestra que f y Df son coprimos sobre $\mathbb{C}$ y por el Teorema (1.2.20), f no podrá tener ceros repetidos en $\mathbb{C}$.

Teorema 1.2.22. Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos, $\alpha \in \mathbb{L}$ y consideremos el homomorfismo evaluación $e_\alpha : \mathbb{K}[x] \to \mathbb{L}$. Entonces α es trancendente sobre $\mathbb{L}$ si, y solo si, e_α es un monomorfismo.
Demostración: α es trascendente sobre $\mathbb{K}$ si, y solo si, $f(\alpha) \neq 0$ para todo polinomio no constante $f(x) \in \mathbb{K}[x]$ y por definición de homomorfismo $e_\alpha(f(x)) \neq 0$ entonces $ker(e_\alpha) = \{0\}$, por tanto e_α es monomorfismo.

Teorema 1.2.23. Sea $\mathbb{K} = \mathbb{Q}(\alpha)$ un cuerpo numérico de grado n sobre $\mathbb{Q}$. Entonces, existen exactamente n distintos monomorfismos $\sigma_i : \mathbb{K} \to \mathbb{C}$ $(i = 1, 2, \cdots, n)$. Más aún, los elementos $\sigma_i(\alpha) = \theta_i$ son los distintos ceros en $\mathbb{C}$ del polinomio minimal de α sobre $\mathbb{Q}$.
Demostración:
Dado que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, entonces $\partial(m_\alpha(t)) = n$ y como el polinomio minimal $m_\alpha(t)$ es irreducible, por el Teorema (1.2.21) tiene n distintos ceros entonces, definamos $\sigma_i : \mathbb{K} \to \mathbb{C}$, con $\sigma_i(\alpha) = \theta_i$, para $i = 1, 2, \cdots, n$ donde los θ_i son los distintos ceros del polinomio minimal. Veamos que solo hay n monomorfismos, supongamos que existe otro monomorfismo $\sigma_{n+1} : \mathbb{K} \to \mathbb{C}$ entonces por definición

$$\sigma_{n+1}(0) = 0 \tag{2}$$

ya que $m_\alpha(\alpha) = 0$ entonces sustituimos en (2) y obtenemos

$$\begin{aligned}\sigma_{n+1}(m_\alpha(\alpha)) &= \sigma_{n+1}(\alpha^n + a_{n+1}\alpha^{n-1} + \cdots + a_1\alpha + a_0),\\ &= (\sigma_{n+1}(\alpha))^n + a_{n-1}(\sigma_{n+1}(\alpha))^{n-1} + \cdots a_1\sigma_{n+1}(\alpha) + a_0),\\ &= 0.\end{aligned}$$

Así $\sigma_{n+1}(\alpha)$ es un cero del polinomio minimal $m_\alpha(x)$ y éste tiene n ceros, por tanto $\sigma_{n+1}(\alpha) = \theta_i$, para algún $i = 1, 2, \cdots, n$ y como σ_{n+1} es monomorfismo, luego coincide con uno de los σ_i, con $i = 1, 2, \cdots, n$, entonces existen exactamente n monomorfismos.

Los monomorfismos $\sigma_i(\alpha)$ para $i = 1, \cdots, n$ del Teorema (1.2.23) son llamados los $\mathbb{K}-$conjugados de α.

Definición 1.2.24. Para cada $\alpha \in \mathbb{K} = \mathbb{Q}(\theta)$, se define el polinomio base de α sobre $\mathbb{K}$ como sigue:

$$f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha)).$$

Observación: Note que $f_\alpha(t) \in \mathbb{K}[t]$.

Ejemplo 1.2.25. $\alpha = a + bi \in \mathbb{Q}(i)$. Entonces los $\mathbb{K}-$conjugados de α están dados por $\sigma_1(a + bi) = a + bi$ y $\sigma_2(a + bi) = a - bi$, por tanto el polinomio base de α sobre $\mathbb{Q}(i)$ viene dado por:

$$\begin{aligned}f_\alpha(t) &= (t - \sigma_1(a + bi))(t - \sigma_2(a + bi))\\ &= (t - (a + bi))(t - (a - bi))\\ &= t^2 - (a - bi)t - (a + bi)t + ((a + bi)(a - bi))\\ &= t^2 - at + bit - at - bit + a^2 + b^2\\ &= t^2 - 2at + a^2 + b^2.\end{aligned}$$

1.3. NORMA Y TRAZA.

Sea $\mathbb{K}$ un cuerpo numérico sobre $\mathbb{Q}$ de grado n, para $1 \leq i \leq n$ sean $\sigma_i : \mathbb{K} \to \mathbb{C}$ los n distintos monomorfismos, garantizados por el Teorema(1.2.23) dado $\alpha \in \mathbb{K}$ definimos su norma como

$$N(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha),$$

y su traza por

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Proposición 1.3.1. Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos, si α, $\beta \in \mathbb{L}$ y $a \in \mathbb{K}$ entonces:

(a) $N(\alpha\beta) = N(\alpha)N(\beta)$

(b) $N(\alpha + \beta) = N(\alpha) + N(\beta)$.

(c) $N(a) = a^{[\mathbb{L}:\mathbb{K}]}$.

(d) $T(\alpha)(\alpha\beta) = T(\alpha)(\alpha)T(\alpha)(\beta)$

(e) $T(\alpha)(\alpha + \beta) = T(\alpha)(\alpha) + T(\alpha)(\beta)$.

(f) $T(a) = [\mathbb{L} : \mathbb{K}]a$.

Demostración: Véase Página 88. [17].

Ejemplo 1.3.2. Sea $\mathbb{K} = \mathbb{Q}(i)$, el polinomio minimal de i es $t^2+1 = t^2-(i)^2 = (t-i)(t+i)$, de donde los σ_j están dados por:

$$\sigma_1(p + qi) = p + qi,$$
$$\sigma_2(p + qi) = p - qi.$$

Ahora, dado $\alpha \in \mathbb{Q}(i)$ tenemos $\alpha = p + qi$ con $p, q \in \mathbb{Q}$ entonces

$$N(\alpha) = N(\alpha)(p + qi) = (p + qi)(p - qi) = p^2 + q^2,$$
$$T(\alpha) = T(p + qi) = (p + qi) + (p - qi) = 2p.$$

En particular, si $\alpha \in \mathbb{Q}$ nos queda

$$N(\alpha) = N(p) = p^2,$$
$$T(\alpha) = T(p) = 2p.$$

---

[17] S. ZARISKI O. y PIERRE. *Commutative algebra, Volume I*. The University Series in Higher Mathematics. With the cooperation of I. S. Cohen. D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, págs. xi+329.

Proposición 1.3.3. Sean $p, z \in \mathcal{K}$, con $\mathcal{K}$ el anillo de enteros de $\mathbb{K}$ introducido en la Definición(1.2.10). Si $p|z$, entonces $N(p)|N(z)$.
Demostración:
Por hipótesis $p|z$, entonces $z = pk$, para algún $k \in \mathcal{K}$. Entonces por (a) de la Proposición (1.3.1) $N(z) = N(pk) = N(p)N(k)$ para algún $k \in \mathcal{K}$ entonces $N(p)|N(z)$.

A partir de este capítulo de la monografía es posible concluir que dado un número algebraico α se puede definir un cuerpo numérico $\mathbb{Q}(\alpha)$ y el polinomio minimal de α sobre $\mathbb{Q}[t]$. Al tener el polinomio minimal y su grado, se determina la dimensión de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}-$espacio vectorial y sus respectivos monomorfismos, que serán indispensables para calcular la norma y traza de α o de algún otro elemento de $\mathbb{Q}(\alpha)$.

2. DOMINIOS

Un anillo R conmutativo y con unidad es llamado un dominio entero si dados $a, b \in R$, la igualdad $ab = 0$ implica $a = 0$ o $b = 0$. En este capítulo se darán algunas propiedades particulares en el anillo de enteros $\mathcal{K}$ de un cuerpo numérico $\mathbb{K}$.

Proposición 2.0.1. Si $\mathbb{K}$ es un dominio entero, entonces $\mathbb{K}[x]$ es un dominio entero.
Demostración: Véase Teorema 8.3. [11].

Ejemplo 2.0.2. Como $\mathbb{Q}$ es un cuerpo, $\mathbb{Q}[x]$ es un dominio entero. El cuerpo de fracciones de $\mathbb{Q}[x]$ es el conjunto de todas las funciones racionales $p(x)/q(x)$, donde $q(x) \neq 0$ y se denota por $\mathbb{Q}(x)$.

Ejemplo 2.0.3. Ya que $\mathbb{Z}[x]$ es un dominio entero entonces

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_n{\zeta_p}^n \ : \ a_i \in \mathbb{Z},\ \zeta_p = e^{\frac{2\pi i}{p}}\}$$

es un dominio entero.

2.1. IDEALES DESTACADOS EN UN ANILLO

En esta sección recordaremos algunas definiciones de ideales como ideal maximal e ideal primo, luego introduciremos las definiciones de ideal comaximal, ideal fraccionario, ideal fraccionario principal y norma de un ideal para después desarrollar algunas características de estas definiciones en ideales de los llamados anillos de enteros.

Definición 2.1.1. Un ideal $\mathcal{M}$ de R es llamado maximal si $\mathcal{M} \neq R$ y dado I ideal de R tal que $\mathcal{M} \subseteq I$ entonces $\mathcal{M} = I$ o $I = R$.

Definición 2.1.2. Sea R un anillo conmutativo P un ideal de R con $R \neq P$ es llamado ideal primo si dados $a, b \in R$ tales que $ab \in P$ entonces $a \in P$ o $b \in P$.

Teorema 2.1.3 (Existencia de ideales máximales)**.** Todo anillo R conmutativo con unidad tiene ideal maximal.
Demostración: Véase Proposición 6.16 [11].

Definición 2.1.4. Diremos que los ideales I y J de R son comaximales $I + J = R$.

Teorema 2.1.5. Sea R un anillo conmutativo con unidad

1. $\mathcal{M}$ es un ideal maximal si, y solo si, $R/\mathcal{M}$ es un cuerpo.
2. P es un ideal primo si, y solo si, R/P es un dominio entero.

Demostración: Véase para (a) la Proposición 12 y para (b) Proposición 13, página 254. [9]

Teorema 2.1.6. Sea R un anillo con unidad, si $\mathcal{M}$ es un ideal máximal, entonces $\mathcal{M}$ es un ideal primo.
Demostración: Véase Corolario 14 página 256. [9]

El recíproco del Teorema (2.1.6) no siempre se satisface, veamos el siguiente ejemplo.

Ejemplo 2.1.7. $\mathbb{Z} \approxeq \mathbb{Z}[x]/\langle x\rangle$ es un dominio entero, con $\langle x\rangle$ un ideal primo; notemos que

$$\langle x\rangle \subsetneq \langle x\rangle + \langle 2\rangle \subsetneq \mathbb{Z}[x]$$

por tanto $\langle x\rangle$ no es ideal maximal.

Proposición 2.1.8. En un anillo con unidad todo ideal propio está contenido en un ideal maximal.
Demostración: Véase Proposición 11. [9]

Definición 2.1.9. Un $\mathcal{K}-$módulo $\mathfrak{a}$ de $\mathbb{K}$ es llamado ideal fraccionario de $\mathcal{K}$, si existe algún $c \in \mathcal{K}$ no nulo tal que $c\mathfrak{a} \subseteq \mathcal{K}$. Denotamos por $\mathcal{F}_{\mathcal{K}}$ a el conjunto de ideales fraccionarios de $\mathcal{K}$.

Ejemplo 2.1.10. Los ideales fraccionarios de $\mathbb{Z}$ son de la forma $r\mathbb{Z}$, donde $r \in \mathbb{Q}$.

Definición 2.1.11. Un ideal fraccionario $I \in \mathcal{F}_{\mathcal{K}}$ es principal si existe $x \in \mathbb{K}$ tal que $I = \mathcal{K}x$. Denotamos $\mathcal{P}_{\mathcal{K}}$ al conjunto de ideales fraccionarios principales de $\mathcal{K}$.

En la monografía (véase [10]) titulado “Anillo de enteros algebraicos y dominios de Dedekind" se concluye que los dominios de Dedekind son aquellos que cumplen ciertas condiciones de finitud y se establece una caracterización importante en términos de factorización única de ideales. También se prueba que en dichos dominios todo ideal propio se puede factorizar como producto de ideales primos y este producto es único salvo el orden de los factores. En este contexto, el anillo de los enteros de un cuerpo es un dominio de Dedekind, aunque no necesariamente es dominio de ideales principales ni de factorización única. A continuación daremos algunas de las caracterizaciones con respecto a que sean dominios de ideales principales y de factorización única.

Teorema 2.1.12. Todo ideal no nulo de $\mathcal{K}$ puede ser escrito como un producto de ideales primos de manera única, salvo el orden de los factores.
Demostración: Véase Teorema 5.6. [12]

Teorema 2.1.13. El anillo de enteros $\mathcal{K}$ de un cuerpo numérico $\mathbb{K}$ tiene las siguientes propiedades:
(a) $\mathcal{K}$ es un dominio y $\mathbb{K}$ su cuerpo de fracciones.
(b) Todo ideal primo no nulo de $\mathcal{K}$ es maximal.
(c) Si $\alpha \in \mathbb{K}$ es raíz de un polinomio mónico con coeficientes en $\mathcal{K}$, entonces $\alpha \in \mathcal{K}$.
Demostración: Véase Teorema 5.5. [12] y Teorema 1.5. [10]

Observación: Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{K}$, tenemos que el cociente $\mathcal{K}/\mathfrak{a}$ es finito. En este trabajo omitiremos la prueba de este resultado pues usa teoría de grupos abelianos libres finitamente generados. Véase Lema (2.16). [16].

Definición 2.1.14. Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{K}$ entonces el cociente $\mathcal{K}/\mathfrak{a}$ es finito. Definimos la norma de un ideal $\mathfrak{a}$ como

$$\mathcal{N}(\mathfrak{a}) = |\mathcal{K}/\mathfrak{a}|.$$

Proposición 2.1.15. Si $\mathfrak{a}$, $\mathfrak{b}$ ideales no nulos de $\mathcal{K}$, entonces

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

Demostración: Sea $\mathfrak{b}$ un ideal no nulo, por que Teorema (2.1.12) podemos suponer que $\mathfrak{b} = \mathfrak{p}$, con $\mathfrak{p}$ un ideal primo. es suficiente probar que $\mathcal{N}(\mathfrak{ap}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{p})$ donde $\mathfrak{p}$ es primo [18].

$$\mathcal{N}(\mathfrak{ap}) = |\mathcal{K}/\mathfrak{ap}| = |\mathcal{K}/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|,$$

---

[18] por el tercer Teorema de Isomorfía. Tenemos, si IP, I son subgrupos normales de un grupo R, con $IP \subseteq I$, entonces$R/I \simeq \frac{R/IP}{I/IP}$ (Véase Teorema 5.13, (c) (K. SPINDLER. *Abstract algebra with applications. Vol. II*. Rings and fields. Marcel Dekker, Inc., New York, 1994, págs. xvi+531)).

y además [19], se tiene que, $|\mathfrak{a}/\mathfrak{a}\mathfrak{p}| = |\mathcal{K}/\mathfrak{p}|$, así:

$$\begin{aligned}\mathcal{N}(\mathfrak{a}\mathfrak{p}) &= |\mathcal{K}/\mathfrak{a}\mathfrak{p}| = |\mathcal{K}/\mathfrak{a}||\mathfrak{a}/\mathfrak{a}\mathfrak{p}| \\ &= |\mathcal{K}/\mathfrak{a}||\mathcal{K}/\mathfrak{p}| \\ &= \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{p}),\end{aligned}$$

como quería probarse.

Definición 2.1.16. Sean $\mathfrak{a},\ \mathfrak{b}$ ideales no nulos de $\mathcal{K}$. Definimos la relación "divide.[en] ideales como:

$$\mathfrak{a} \mid \mathfrak{b} \text{ si, y solo si, } \mathfrak{b} \subseteq \mathfrak{a}$$

Teorema 2.1.17. Sea $\mathfrak{a} \neq 0$ un ideal de un anillo de enteros, entonces
(a) Si $\mathcal{N}(\mathfrak{a})$ es primo, entonces $\mathfrak{a}$ es primo.
(b) $\mathcal{N}(\mathfrak{a})$ es un elemento de $\mathfrak{a}$, o equivalentemente $\mathfrak{a}|\langle\mathcal{N}(\mathfrak{a})\rangle$.
Demostración:
(a). Supongamos que $\mathfrak{a}$ no es primo entonces $\mathfrak{a}$ se puede escribir como producto de factores primos, siendo $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$

$$\begin{aligned}\mathcal{N}(\mathfrak{a}) &= \mathcal{N}(\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k) \\ &= \mathcal{N}(\mathfrak{p}_1)\mathcal{N}(\mathfrak{p}_2) \cdots \mathcal{N}(\mathfrak{p}_k)\end{aligned}$$

absurdo, ya que por hipótesis $N(\mathfrak{a})$ es primo, por tanto $\mathfrak{a}$ es primo.

(b). Por definición $\mathcal{N}(\mathfrak{a}) = |\mathcal{K}/\mathfrak{a}|$, luego para algún $x \in \mathcal{K}$ tenemos que $\mathcal{N}(\mathfrak{a})x \in \mathfrak{a}$, esto es $\langle\mathcal{N}(\mathfrak{a})\rangle \subseteq \mathfrak{a}$, entonces $\mathfrak{a}|\langle\mathcal{N}(\mathfrak{a})\rangle$.

En la teoría algebraica se tiene que todo ideal máximal es un ideal primo y el recíproco no se satisface, en la sección anterior se vió que en los anillos de enteros $\mathcal{K}$ de un cuerpo numérico $\mathbb{K}$ se da que todo ideal primo no nulo de $\mathcal{K}$ es maximal, además se definió la norma sobre un ideal no nulo del anillo de enteros $\mathcal{K}$.

---

[19] Por el primer Teorema de Isomorfía deducimos que si P, I son subgrupos de R con $IP \subseteq I$, entonces $R/P \simeq I/IP$ y por lo tanto $[R : P] = [I : IP]$ (Véase Teorema 5.13, (b) [18]).

2.2. ASOCIADOS EN DOMINIOS ENTEROS

En esta sección dado un dominio entero recordaremos las definiciones de: asociados, irreducible y primo, y enunciaremos como es la norma en los elementos mencionados. Cabe recordar que la factorización única salvo el orden en el anillo $\mathbb{Z}$ son los números primos, en esta sección queremos mostrar la factorización de forma general en dominios enteros, y mencionar condiciones suficientes para tener factorización única, a los dominios enteros cuya factorización es única se les llama Dominio de Factorización Única. En adelante R denotará un dominio entero.

Definición 2.2.1. Sean $a, b, p \in R$. Diremos que:

- Si $ab = 1$, entonces, sin pérdida de generalidad, a es una unidad de R. Al conjunto de las unidades de R, se denotará por $U(R)$.
- a divide a b, y escribimos $a \mid b$, si existe $c \in R$ tal que $b = ac$.
- p es primo si siempre que $p \mid ab$, entonces $p \mid a$ o $p \mid b$.
- a y b son asociados y lo denotaremos por $a \sim b$, si $a \mid b$ y $b \mid a$.
- Sea $x \in R - (U(R) \cup \{0\})$ diremos que x es irreducible si dado $r \in R$ tal que $r \mid x$ entonces $r \in U(R)$ o $r \sim x$.

Proposición 2.2.2. Sean $a, b \in R$. Entonces $a \sim b$ si, y solo si, existe $u \in U(R)$ tal que $a = ub$.
Demostración:
$\Rightarrow$) Si $a \sim b$, entonces $a|b$ y $b|a$. Por tanto existen $c, d \in R$ tales que $b = ac$ y $a = bd$; así $b = (bd)c = b(dc)$, por tanto $bc = 1$ luego $c \in U(R)$.
$\Leftarrow$) Sea $u \in U(R)$ tal que $a = ub$, entonces $b|a$ y además existe $u^{-1} \in R$ tal que $uu^{-1} = 1$; así $au^{-1} = b$, por tanto $a|b$ así $a \sim b$.

Los conceptos de divisibilidad, asociados e irreducibles se pueden expresar en términos de los ideales generados, de la siguiente forma:

Proposición 2.2.3. Sea R un dominio entero y $a, b \in R$ entonces

(a) $\langle a \rangle \subseteq \langle b \rangle$ si, y solo si, $b|a$.

(b) $\langle a \rangle = \langle b \rangle$ si, y solo si, $a \sim b$.

(c) a es primo si, y solo si, $\langle a \rangle$ es primo.

(d) a es irreducible si, y solo si, $\langle a \rangle$ es máximal.

(e) Si $x \in U(R)$ si, y solo si, $\langle x \rangle = R$.

Demostración:

(a) $\Rightarrow$) Si $\langle a \rangle \subseteq \langle b \rangle$, entonces $a \in \langle b \rangle$, luego existe $r \in R$ tal que $a = rb$ así $b \mid a$.

$\Leftarrow$) Si $b \mid a$ por definición $a = rb$, para algún $r \in R$, así $a \in \langle b \rangle$ y por tanto $\langle a \rangle \subseteq \langle b \rangle$.

(b) $\Rightarrow$) Si $\langle a \rangle = \langle b \rangle$ tenemos que $\langle a \rangle \subseteq \langle b \rangle$ y $\langle b \rangle \subseteq \langle a \rangle$. Así, por lo probado en el ítem (a) se tiene que $a \mid b$ y $b \mid a$, esto es, $a \sim b$.

$\Leftarrow$) Si $a \sim b$ entonces por definición $a|b$ y $b|a$ por el item (a) tenemos que $\langle a \rangle \subseteq \langle b \rangle$ y $\langle b \rangle \subseteq \langle a \rangle$ así $\langle b \rangle = \langle a \rangle$.

(c) $\Rightarrow$) Sea $x \cdot y \in \langle a \rangle$, entonces $x \cdot y = ar$ para algún r, por tanto $a|xy$ y por hipótesis a es primo entonces $a|x$ ó $a|y$ así $x \in \langle a \rangle$ ó $y \in \langle a \rangle$ por tanto $\langle a \rangle$ es primo.

$\Leftarrow$) Supongamos que $a \mid xy$, entonces $xy \in \langle a \rangle$, por hipótesis $\langle a \rangle$ es primo, luego $x \in \langle a \rangle$ o $y \in \langle a \rangle$ así $a \mid x$ o $a \mid y$ por tanto a es primo.

(d) $\Rightarrow$) Si a es irreducible, para ver que $\langle a \rangle$ es maximal deberá probarse que $\langle a \rangle = \langle r \rangle$ o $\langle r \rangle = R$. Dado $r \in R$ tal que $r \mid a$ entonces $r \in U(R)$ o $r \sim x$. Si $r \mid a$, entonces por la Definición (2.1.16) $\langle a \rangle \subseteq \langle r \rangle$, si $r \in U(R)$ entonces $\langle r \rangle = R$, ahora, si $r \sim a$ por el ítem (b) $\langle r \rangle = \langle a \rangle$. Por tanto hemos probado que $\langle r \rangle = R$ o $\langle a \rangle = \langle r \rangle$, así $\langle a \rangle$ es maximal.

$\Leftarrow$) Sea $r \in R$ un ideal de R, por hipótesis $\langle a \rangle$ es maximal entonces por definición $\langle a \rangle = \langle r \rangle$ o $\langle r \rangle = R$ así por el ítem (b) $a \sim r$ o $r \in U(R)$ por tanto a es irreducible.

(e) $\Rightarrow$) Si $x \in U(R)$ y $r \in R$ arbitrario, entonces $r = (rx^{-1})x \in Rx = \langle x \rangle$ así $R \subseteq \langle x \rangle$, por tanto $R = \langle x \rangle$.

$\Leftarrow$) Supongamos $\langle x \rangle = R$, es decir, $Rx = R$. Así, $1 \in xR$, por tanto hay un elemento $y \in R$ con $xy = yx = 1$ entonces x es invertible luego, $x \in U(R)$.

Proposición 2.2.4. Sean $\mathcal{K}$ el anillo de enteros de un cuerpo numérico $\mathbb{K}$, $x, b \in \mathcal{K}$. Se verifican las siguientes proposiciones:

(1) $x \in U(\mathcal{K})$ si, y solo si, $N(x) = \pm 1$.

(2) Si $x \sim y$, entonces $N(x) = \pm N(y)$.

(3) Si $N(x)$ es un primo, entonces x es irreducible.

Demostración:

(**1**) $\Rightarrow$) Sea $x \in U(\mathcal{K})$, entonces existe $u \in \mathcal{K}$ tal que $xu = 1$, al evaluar la norma en ux tenemos $N(ux) = N(x)N(u) = 1$. Así $N(x) = \pm 1$.

$\Leftarrow$) $N(x) = \pm 1$, luego

$$N(x) = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x) = \pm 1,$$

donde σ_i son los monomorfismos $\mathbb{K} \to \mathbb{C}$. Supongamos $\sigma_1(x) = x$ y todos los demás σ_i con $i \neq 1$ son enteros algebraicos. Si

$$u = \pm\sigma_2(x)\cdots\sigma_n(x),$$

entonces $xu = 1$, así $x \in U(\mathcal{K})$.

(2) Si $x \sim y$, por tanto $x = uy$, para $u \in U(\mathcal{K})$, así $N(x) = N(uy) = N(u)N(y)$ y por la prueba anterior $N(x) = \pm N(y)$.

(3) Sea $x = yz$. Entonces $N(y)N(z) = N(yz) = N(x) = p$, con p un primo, por tanto, sin pérdida de generalidad, $N(y) = \pm p$ y $N(z) = \pm 1$, por el ítem (1), z es una unidad, así x es irreducible.

El Teorema Fundamental de la Aritmética (TFA) nos dice que todo $n \in \mathbb{Z}$, con $n > 1$, se escribe de manera única como producto de números primos, salvo el orden en que aparecen estos. La pregunta es si esta factorización se puede realizar en anillos. Cuya respuesta dependerá del anillo, será afirmativa en los anillos que satisfacen la definición de Dominios de Factorización Única.

Definición 2.2.5. Decimos que R es un dominio de factorización si todo elemento de R que no sea ni cero ni unidad se puede escribir como producto de irreducibles de R.
Un Dominio de Factorización Única (DFU) es un dominio de R con factorización tal que si

$$p_1p_2\cdots p_r = q_1q_2\cdots q_s,$$

con todos los p_i y q_i irreducibles de R se verifica que:
(1) $r = s$.
(2) Existe una permutación π de $\{1, 2, \cdots, r\}$ tal que $p_i \sim q_{\pi(i)}$, para todo i.

Ejemplo 2.2.6. No todo dominio integral es un DFU. Por ejemplo el anillo $\mathbb{Z}[\sqrt{3}i]$ es un dominio integral, pero el elemento 4 tiene dos factorizaciones distintas en elementos irreducibles;

$$4 = 2 \cdot 2 = (1 - \sqrt{3}i)(1 + \sqrt{3}i), \tag{3}$$

y 2 no es asociado a $1-\sqrt{3}i$. Para ver esto, supongamos que son asociados, esto es $2 \sim (1-\sqrt{3}i)$, entonces por la Proposición (2.2.2), se tiene que $2 = (1-\sqrt{3}i)\cdot u$, para algún $u \in U(\mathbb{Z}[\sqrt{3}i]) = \{\pm 1, \pm\omega\}$, donde $\omega = \frac{-1+\sqrt{3}i}{2}$. En efecto, para el caso en que $u = \pm 1$ tenemos que $2 = \pm(1-\sqrt{3}i)$ y esto es falso. Ahora, veamos cuando $u = \pm\omega$

$$
\begin{aligned}
2 &= (1-\sqrt{3}i)\left[\pm\left(\frac{-1+\sqrt{3}i}{2}\right)\right],\\
2 &= \pm\frac{1}{2}(1-\sqrt{3}i)(-1+\sqrt{3}i),\\
2 &= \mp\frac{1}{2}(1-\sqrt{3}i)^2,\\
2 &= \mp\frac{1}{2}(-2-2\sqrt{3}i),\\
2 &= \pm(1+\sqrt{3}i);
\end{aligned}
$$

y esto es falso, por tanto no son asociados. Así 4 no tiene factorización única en $\mathbb{Z}[\sqrt{3}i]$.

Teorema 2.2.7. En un dominio en el cual la factorización entre irreducibles es posible, la factorización es única si, y solo si, todo irreducible es primo.

Demostración:
$\Rightarrow$) Supongamos la factorización es única y p es un irreducible. Mostraremos que p es primo, en efecto si

$$p|ab, \text{ entonces } pc = ab \text{ con } c \in D.$$

Consideremos el caso no trivial $a \neq 0,\ b \neq 0$ que implica $c \neq 0$. Al factorizar a, b, c entre irreducibles[20] tenemos:

$$
\begin{aligned}
a &= u_1 p_1 \cdots p_n,\\
b &= u_2 q_1 \cdots q_m,\\
c &= u_3 r_1 \cdots r_s,
\end{aligned}
$$

---

[20] Sea D un dominio. Por el Teorema (2.1.12), para todo $x \in D$ no nulo se tiene que

$$x = up_1 \cdots p_r, \tag{4}$$

donde u es una unidad y $p_1, \cdots, p_r$ son irreducibles. Cuando $r = 0$ entonces $x = u$ es unidad y cuando $r \geq 1$, entonces up_1 es un irreducible, así x es un producto de irreducibles $up_1, \cdots, p_r$.

donde para cada i, u_i es una unidad, y p_i, q_i y r_i son irreducibles. Al remplazar tenemos:

$$p(u_3 r_1 \cdots r_s) = (u_1 p_1 \cdots p_n)(u_2 q_1 \dots q_m),$$

y la factorización única implica que p es un asociado (por lo tanto, divide) de uno de los p_i o q_j, así divide a a o b respectivamente. Por lo tanto p es primo.

$\Leftarrow$) Supongamos que todo irreducible es primo, probaremos que si

$$u_1 p_1 \cdots p_m = u_2 q_1 \cdots q_n, \tag{5}$$

donde u_1, u_2 son unidades y p_i, q_j son irreducibles, entonces $m = n$ y hay una permutación π de $\{1, \cdots, m\}$ tal que p_i y $q_{\pi(i)}$ son asociados ($1 \leq i \leq m$).

Esto es verdadero para $m = 0$.

Para $m \geq 1$, en la ecuación (5) $p_m | u_2 q_1 \cdots q_n$. Pero p_m es primo, así $p_m | u_2$ o $p_m | q_j$ para algún $j = 1, \cdots, n$. En el primer caso implicará que p_m es una unidad entonces $p_m | 1$ lo cual es absurdo, así veamos cuando $p_m | q_j$. Supongamos $p_m | q_n$ y $q_n = p_m u$ donde u es una unidad. Así

$$u_1 p_1 \cdots p_m = u_2 q_1 \cdots q_{n-1} u p_m,$$

cancelando p_m tenemos que:

$$u_1 p_1 \cdots p_{m-1} = (u_2 u) q_1 \cdots q_{n-1}.$$

Por inducción suponemos que $m - 1 = n - 1$ y así hay una permutación de $1, \cdots, m-1$ tal que $p_i, q_{\pi(i)}$ son asociados para $i = 1, \cdots, m-1$. Entonces podemos extender π a $\{1, \cdots, m\}$ definiendo $\pi(m) = m$ por tanto hemos probado la factorización única.

Teorema 2.2.8. La factorización de elementos de R entre irreducibles es única si, y solo si, todo ideal de R es principal.

Demostración:

$\Rightarrow$) Por hipótesis la factorización en R es única, será suficiente demostrar que todo ideal primo es principal, ya que cualquier otro ideal, siendo un producto de ideal primos, sería principal. Sea $\mathfrak{p} \neq 0$ un ideal primo de $\mathcal{K}$ entonces por el ítem (b) del Teorema (2.1.17), $N(\mathfrak{p}) = q$ un entero tal que $\mathfrak{p} | \langle q \rangle$,

al factorizar a q como producto de elementos irreducibles en R, tenemos:

$$q = \pi_1 \cdots \pi_s,$$

dado que, $\mathfrak{p}|\langle q\rangle$ y $\mathfrak{p}$ es ideal primo, así también $\mathfrak{p}|\langle \pi_j\rangle$, para algún $j = 1, \cdots, s$. Por el Teorema (2.2.7) tenemos que π_j es primo, luego $\langle \pi_j\rangle$ es primo, como $\mathfrak{p}|\langle \pi_j\rangle$ y ambos son primos en R con factorización única, entonces

$$\mathfrak{p} = \langle \pi_j\rangle.$$

Así $\mathfrak{p}$ es principal.
$\Leftarrow$) Si R es un Dominio de Ideales Principales, entonces R es un dominio de Factorización Única (Véase Teorema 4.15 [12]).

2.3. CONGRUENCIAS

En esta sección se recordarán algunos teoremas importantes en la teoría de números como lo son: El Teorema de Fermat, el Pequeño Teorema de Fermat y otros teoremas que se dan a partir de estos.

Teorema 2.3.1 (Teorema de Fermat)**.** Si p es un número primo entonces

$$a^p \equiv a \text{ (mód } p).$$

Demostración: Véase Colorario 4.39.[21].

Proposición 2.3.2 (Pequeño teorema de Fermat)**.** Si p es un número primo y $a \in \mathbb{N}$ tal que $(a, p) = 1$, entonces

$$a^{p-1} \equiv 1 \text{ (mód } p).$$

Demostración: Véase Teorema 4.44. [21].

Proposición 2.3.3. Si p es un primo impar, y $p \nmid a$ entonces

---

[21] GORDILLO J. y RUBIANO-G. JIMÉNEZ L. *Teoría de números*. Para principiantes. [For beginners]. Universidad Nacional de Colombia, Facultad de Ciencias, Departamento de Estadística, Bogotá, 1999, págs. ii+216.

$$a^{\frac{p-1}{2}} \equiv \pm 1 \text{ (mód } p).$$

Demostración: Por el pequeño teorema de Fermat tenemos que

$$a^{p-1} \equiv 1 \text{ (mód } p).$$

Como p es un primo impar, $p-1$ es par, por tanto es divisible por 2, así

$$\begin{aligned}\left(a^{\frac{p-1}{2}\cdot 2}\right) &\equiv 1 \text{ (mód } p),\\ \left(a^{\frac{p-1}{2}}\right)^2 &\equiv 1 \text{ (mód } p),\\ a^{\frac{p-1}{2}} &\equiv \pm 1 \text{ (mód } p);\end{aligned}$$

como quería probarse.

Proposición 2.3.4. Sean $a, b \in \mathbb{Z}$. Si p es un número primo tal que $(a,p) = 1$, $(b,p) = 1$, y $a^p \equiv b^p$ (mód p), entonces

$$a^p \equiv b^p \text{ (mód } p^2).$$

Demostración: Por el Teorema de Fermat tenemos que:

$$\begin{aligned}a^p &\equiv a \text{ (mód } p)\\ b^p &\equiv b \text{ (mód } p).\end{aligned}$$

Además, por hipótesis $a^p \equiv b^p$ (mód p), luego, $a \equiv b$ (mód p), es decir, $p \mid (a-b)$ entonces existe $k \in \mathbb{Z}$, tal que $(a-b) = kp$. Ahora, al descomponer $(a^p - b^p)$ tenemos que:

$$\begin{aligned}a^p - b^p &= \underbrace{(a-b)}_{\text{divisible por } p} \overbrace{(a^{p-1} + a^{p-2}b + a^{p-3}b^3 + \cdots + b^{p-1})}^{p \text{ sumando congruentes con } a^{p-1}}\\ &= kp \cdot (a^{p-1}p)\\ &= a^{p-1}kp^2\end{aligned}$$

por tanto $p^2 \mid (a^p - b^p)$, es decir, $a^p \equiv b^p$ (mód p^2), como quería probarse.

3. BASES

Dada una extensión de cuerpos finita $\mathbb{L}/\mathbb{K}$, tenemos que $\mathbb{L}$ tiene una dimensión finita como $\mathbb{K}-$espacio vectorial, esto es, $\mathbb{L}$ como $\mathbb{K}-$espacio vectorial tiene una base finita, esto se podrá definir siempre que $\mathbb{K}$ sea un cuerpo, en este capítulo se desarrollará la base de $\mathbb{L}$ como $\mathbb{Q}-$espacio vectorial, a ésta la llamaremos $\mathbb{Q}-$base. También se definirán: una base entera o $\mathbb{Z}-$base a partir de la definición de base como $\mathbb{Z}-$módulo, y el discriminante de una base. Se mostrará la relación entre norma y discriminante, donde omitiremos algunas demostraciones ya que para éstas se requiere desarrollar la teoría de grupos abelianos libres.

3.1. $\mathbb{Q}$-BASE

Definición 3.1.1. Sea $\mathbb{K} = \mathbb{Q}(\alpha)$ un cuerpo numérico de grado n sobre $\mathbb{Q}$. Una base o $\mathbb{Q}-$Base de $\mathbb{K}$ es una base para $\mathbb{K}$ como un espacio vectorial sobre $\mathbb{Q}$.

Ejemplo 3.1.2. Sean $\mathbb{Q}(\alpha)/\mathbb{Q}$ una extensión de grado n con α algebraico. Por el ítem (c) del Teorema (1.1.20) tenemos que una base para $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ es $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$.

Ejemplo 3.1.3. Sea $i \in \mathbb{C}$, cuyo polinomio minimal es $m_i(t) = t^2 + 1$. Entonces $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, y tenemos que una $\mathbb{Q}-$base para $\mathbb{Q}(i)$ es $\{1, i\}$.

3.2. $\mathbb{Z}$-BASE

Definición 3.2.1. Para un $R-$módulo M el conjunto $\{e_1, \cdots, e_n\} \subseteq M$ es una base para M, si, y solo si:

1. $\{e_1, \cdots, e_n\}$ es un conjunto generador para M, es decir para todo $m \in M$

$$m = r_1 e_1 + \cdots + r_n e_n,$$

   con $r_1, \cdots, r_n \in R$.

2. $\{e_1, \cdots, e_n\}$ es linealmente independiente es decir si

$$r_1 e_1 + \cdots + r_n e_n = 0$$

entonces $r_1 = \cdots = r_n = 0$.

Si M tiene una base con n elementos, entonces se dice que M es de rango n.

Definición 3.2.2. Una base entera o $\mathbb{Z}-$base de $\mathbb{K}$ es una base de $\mathcal{K}$ como $\mathbb{Z}-$módulo.

Ejemplo 3.2.3. Sea $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, donde d es un entero libre de cuadrados y

$$\delta = \begin{cases} \sqrt{d}, & si \quad d \equiv 2,3 \text{ (mód } 4) \\ \\ \frac{1+\sqrt{d}}{2}, & si \quad d \equiv 1 \text{ (mód } 4) \end{cases}$$

Entonces, por la Proposición (1.2.11) $\{1, \delta\}$ es una base de $\mathcal{K}$ como $\mathbb{Z}-$módulo. También puede verse esta prueba en Teorema 2.9[10].

Definición 3.2.4. Sean $\mathbb{K} = \mathbb{Q}(\theta)$ de grado n, y $\{\alpha_1, \cdots, \alpha_n\}$ una base de $\mathbb{K}$ sobre $\mathbb{Q}$. Definimos el discriminante de la base como

$$\Delta[\{\alpha_1, \cdots, \alpha_n\}] = (\det(\sigma_i(\alpha_j)))^2,$$

donde los σ_i son los $\mathbb{K}-$conjugados de θ.

Ejemplo 3.2.5. Sea d un entero libre de cuadrados, entonces, por el Ejemplo (3.2.3) tenemos que una $\mathbb{Z}-$base, $\mathcal{B}$, es $\{1, \sqrt{d}\}$ si $d \not\equiv 1 \text{ (mód } 4)$ o $\{1, \frac{1+\sqrt{d}}{2}\}$ si $d \equiv 1 \text{ (mód } 4)$. Por tanto

$$\Delta(\mathcal{B}) = \begin{cases} \left| \begin{smallmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{smallmatrix} \right|^2 = 4d \quad si \quad d \equiv 2,3 \text{ (mód } 4) \\ \\ \left| \begin{smallmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{smallmatrix} \right|^2 = d \quad si \quad d \equiv 1 \text{ (mód } 4) \end{cases}$$

Proposición 3.2.6. Sean $\mathbb{K} = \mathbb{Q}(\theta)$ y $\{\alpha_1, \cdots, \alpha_n\} \subseteq \mathcal{K}$ una $\mathbb{Q}-$base para $\mathbb{K}$. Si $\Delta[\{\alpha_1, \cdots, \alpha_n\}]$ es libre de cuadrados entonces $\{\alpha_1, \cdots, \alpha_n\}$ forma una $\mathbb{Z}-$base de $\mathbb{K}$.

Demostración: Véase Teorema 2.17.[12].
Toda $\mathbb{Z}-$base es una $\mathbb{Q}-$base, pero no toda $\mathbb{Q}-$base es $\mathbb{Z}-$base, veamos el siguiente ejemplo.

Ejemplo 3.2.7. Considere el cuerpo numérico $\mathbb{K} = \mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \ : \ a, b \in \mathbb{Q}\}$. Note que $\frac{1+\sqrt{5}}{2}$ y $\sqrt{5}$ son raíces de $t^2 - t - 1$ y $t^2 - 5$ respectivamente, así $\frac{1+\sqrt{5}}{2}, \sqrt{5} \in \mathcal{K}$.

Además, puesto que $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, los dos monomorfismos son:

$$\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5},$$
$$\sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}.$$

De modo que al calcular el discriminante para $\{1, \sqrt{5}\}$ tenemos:

$$\Delta[\{1, \sqrt{5}\}] = \begin{vmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{vmatrix}^2 = 2^2 \cdot 5.$$

Pero, para la base $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$, el discriminante viene dado por:

$$\Delta\left[\left\{1, \frac{1+\sqrt{5}}{2}\right\}\right] = \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix}^2 = 5,$$

y 5 es un entero libre de cuadrados. Así por la Proposición (3.2.6) $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ determina una $\mathbb{Z}-$base para $\mathcal{K}$, además, por el Ejemplo (3.1.2) tenemos que $\{1, 5\}$ es una $\mathbb{Q}-$base para $\mathbb{Q}(\sqrt{5})$ y por el Ejemplo (3.2.3) $\{1, 5\}$ no una $\mathbb{Z}-$base, por tanto $\mathcal{K} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Teorema 3.2.8. Sea X un subconjunto de un grupo abeliano G distinto de vacío. Las siguientes condiciones acerca de X son equivalentes:

1. Cada elemento a distinto de cero en G se puede expresar de manera única en la forma $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$, para $n_i \neq 0$ en $\mathbb{Z}$ y x_i distintas en X.
2. X genera a G y $n_1x_1 + \cdots + n_rx_r = 0$, para $n_i \in \mathbb{Z}$ y $x_i \in X$ distintas, si, y solo si, $n_1 = n_2 = \cdots = n_r = 0$.

Demostración: Véase Teorema 20.1[22]

Definición 3.2.9. Un grupo abeliano con un conjunto generador no vacío X que satisface las condiciones descritas en el Teorema (3.2.8) es un grupo abeliano libre y X es una base del grupo.

Definición 3.2.10. Si G es un grupo abeliano libre, el rango de G es el número de elementos en una base de G. (Se puede mostrar que todas las bases tienen el mismo número de elementos.)

---

[22] J. B. FRALEIGH. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967, págs. xvi+447.

Así, un grupo abeliano libre es un grupo abeliano que tiene una base en el sentido de que cada elemento del grupo se puede escribir de manera unívoca como combinación lineal de los elementos de la base. Veamos el siguiente ejemplo:

Ejemplo 3.2.11. Sea G el grupo que es la suma directa $\mathbb{Z} \oplus \mathbb{Z}$ de dos copias del grupo cíclico infinito $\mathbb{Z}$. Simbólicamente, $G = \{(a, b) \mid a, b \in \mathbb{Z}\}$. Una base de este grupo es $\{(1, 0), (0, 1)\}$. Si escribimos $e_1 = (1, 0)$ y $e_2 = (0, 1)$, entonces podemos escribir el elemento $(4, 3)$, como $(4, 3) = 4e_1 + 3e_2$ donde la multiplicación se define de la manera siguiente: $4e_1 := e_1 + e_1 + e_1 + e_1$. Con esta base no hay otra manera de escribir $(4, 3)$, pero si elegimos como base $\{(1, 0), (1, 1)\}$, donde $f_1 = (1, 0)$ y $f_2 = (1, 1)$ podemos escribir $(4, 3)$, como $(4, 3) = f_1 + 3f_2$.

Teorema 3.2.12. Todo cuerpo numérico $\mathbb{K}$ tiene una $\mathbb{Z}-$base y su anillo de enteros es un grupo abeliano libre cuyo rango coincide con la dimensión de $\mathbb{K}$ como $\mathbb{Q}-$espacio vectorial.

Demostración: Véase Teorema 1.31[16]

Lema 3.2.13. Sea G un subgrupo aditivo de $\mathcal{K}$ con base $\{\alpha_1, \cdots, \alpha_n\}$. Si $G \neq \mathcal{K}$, entonces existe un primo p tal que p^2 divide a $\Delta[\{\alpha_1, \cdots, \alpha_n\}]$ y un entero algebraico no nulo de la forma

$$\frac{1}{p}(c_1\alpha_1 + \cdots + c_n\alpha_n),$$

con $c_1, \cdots, c_n$ enteros entre 0 y $p - 1$. Demostración: Véase Lema 1.34[16].

Ejemplo 3.2.14. Sea $\mathbb{Q}(\sqrt{7})$ notemos que $7 \equiv 3 \pmod 4$ por el Ejemplo (3.2.3) tenemos que una $\mathbb{Z}-$base para $\mathbb{Q}(\sqrt{7})$ es $\mathcal{B} = \{1, \sqrt{7}\}$. Por tanto, por el Ejemplo (3.2.5) $\Delta(\mathcal{B}) = 4 \cdot 7 = 28$, así, existe $p = 2$, primo, tal que $p^2 \mid \Delta(\mathcal{B})$ y un entero algebraico no nulo de la forma $\frac{1}{2}(1 + \sqrt{7})$, pues es raíz del polinomio $p(t) = t^2 - t - 2 \in \mathbb{Z}[t]$.

Teorema 3.2.15. Sea G un grupo abeliano libre de rango r, y H un subgrupo normal de G. Entonces G/H es finito si, y solo si, el rango de G y H son iguales. En este caso, si G y H tienen una $\mathbb{Z}-$base $x_1, \cdots, x_r$ y $y_1, \cdots, y_r$ respectivamente, con $y_i = \sum_j a_{ij}x_j$, entonces

$$|G/H| = |det(a_{ij})|.$$

Demostración: Véase Teorema 1.17[12].

Ejemplo 3.2.16. Sea G un grupo de rango 3 y $\mathbb{Z}-$base $\{x, y, z\}$; y H subgrupo de G con $\mathbb{Z}-$base

$$\begin{aligned} 3x + y - 2z, \\ 4x - 5y + z, \\ x \qquad + 7z, \end{aligned}$$

Entonces $|G/H|$ es el valor absoluto de

$$\begin{vmatrix} 3 & 1 & -2 \\ 4 & -5 & 1 \\ 1 & 0 & 7 \end{vmatrix} = |(-105 + 1 + 0) - (10 + 0 + 28)| = |-104 - 38| = |-142|.$$

Teorema 3.2.17. Sean $\mathbb{K}$ un cuerpo numérico con anillo de enteros $\mathcal{K}$ y $\mathfrak{a}$ un ideal no nulo de $\mathcal{K}$, entonces

1. $\mathfrak{a}$ tiene una $\mathbb{Z}-$base $\{\alpha_1, \cdots, \alpha_n\}$, donde n es el grado de $\mathbb{K}$.
2. $N(\mathfrak{a}) = \left|\frac{\Delta[\{\alpha_1, \cdots, \alpha_n\}]}{\Delta}\right|^{1/2}$, donde Δ es el discriminante de $\mathbb{K}$ sobre la $\mathbb{Q}-$base, definida en el Ejemplo (3.1.2).

Demostración: Véase Teorema 5.9[12].

Proposición 3.2.18. Sean $\mathbb{K}$ un cuerpo numérico con anillo de enteros $\mathcal{K}$ y $\mathfrak{a} = \langle\alpha\rangle$ un ideal principal entonces $\mathcal{N}(\mathfrak{a}) = |N(\alpha)|$.

Demostración: Una $\mathbb{Z}-$base para $\mathfrak{a}$ es dada por $\{\alpha\omega_1, \cdots, \alpha\omega_n\}$ donde n es el grado de $\mathbb{K}$ así

$$\begin{aligned} \mathcal{N}(\mathfrak{a}) = |\mathcal{K}/\mathfrak{a}| &= \left|\frac{\Delta[\{\alpha\omega_1, \cdots, \alpha\omega_n\}]}{\Delta}\right|^{1/2}, \\ &= \left|\frac{(det(\sigma_i(\alpha\omega_j))^2}{(det(\sigma_i(\omega_j))^2}\right|^{1/2}, \\ &= \left|\frac{(det(\sigma_i(\alpha)\sigma_i(\omega_j))^2}{(det(\sigma_i(\omega_j))^2}\right|^{1/2}, \\ &= \left|\frac{(det(\sigma_i(\alpha))^2(det(\sigma_i(\omega_j))^2}{(det(\sigma_i(\omega_j))^2}\right|^{1/2}. \\ &= |(det(\sigma_i(\alpha))^2|^{1/2} \\ &= |(det(\sigma_i(\alpha))|^{2\cdot 1/2} \\ &= |(det(\sigma_i(\alpha))| \\ &= |\sigma_1(\alpha) \cdot \sigma_2(\alpha) \cdots \sigma_n(\alpha)| \\ &= |N(\alpha)|. \end{aligned}$$

Como quería probarse.

Proposición 3.2.19. Sea $\mathbb{K} = \mathbb{Q}(\theta)$ un cuerpo numérico, donde θ tiene polinomio minimal p de grado n. Entonces la $\mathbb{Q}-$base $\{1, \theta, \cdots, \theta^{n-1}\}$ tiene discriminante

$$\Delta[\{1, \cdots, \theta^{n-1}\}] = (-1)^{n(n-1)/2} N(Dp(\theta)), \tag{6}$$

donde Dp es la derivada de p.
Demostración: Véase Proposición 2.18[12].

Veamos la Proposición anterior en el siguiente ejemplo

Ejemplo 3.2.20. Sea $\mathbb{Q}(\sqrt{7})$ un cuerpo numérico, donde $\sqrt{7}$ tiene polinomio minimal $m_{\sqrt{7}}(t) = t^2 - 7$ de grado 2. Al calcular la derivada del polinomio minimal obtenemos, $D(m_{\sqrt{7}}(t)) = 2t$, entonces $N(D(m_{\sqrt{7}}(t)) = N(2t)$, que evaluada en $\sqrt{7}$ nos da $N(2\sqrt{7}) = (2\sqrt{7})(-2\sqrt{7}) = -28$ así al reemplazar en la ecuación (6) tenemos que

$$\begin{aligned} \Delta[\{1, \sqrt{7}\}] &= (-1)^{2(2-1)/2} N(Dm_{\sqrt{7}}(\sqrt{7})), \\ &= (-1)(-28), \\ &= 28. \end{aligned}$$

Al compararlo con el Ejemplo (3.2.14), coinciden. Así, el discriminante de la $\mathbb{Q}-$base de $\mathbb{Q}(\sqrt{7})$ es $\Delta[\{1, \sqrt{7}\}] = 28$.

En esta sección se desarrolló la definición de discriminante, sobre los elementos de una base ya sea de $\mathbb{Z}$ o de $\mathbb{Q}$. Además se enlazó la definición de discriminante con respecto a la norma sobre los elementos de la base, mostrando algunos ejemplos sobre los cuerpos cuadráticos denotados por $\mathbb{Q}(\sqrt{d})$, donde d es un entero libre de cuadrado.

3.3. GRUPO DE CLASE

Sean $I, J \in \mathcal{F}_{\mathcal{K}}$, entonces $IJ \in \mathcal{F}_{\mathcal{K}}$. Dotado de esta operación, $\mathcal{F}_{\mathcal{K}}$ es un grupo abeliano cuyo elemento neutro es $\mathcal{K}$, ya que dado un ideal $I \in \mathcal{F}_{\mathcal{K}}$ existe un ideal $I^{-1} \in \mathcal{F}_{\mathcal{K}}$ tal que $II^{-1} = \mathcal{K}$. Además $\mathcal{P}_{\mathcal{K}}$ es un subgrupo normal de $\mathcal{F}_{\mathcal{K}}$. En esta sección definiremos grupo de clase, número de clase y primo regular, Adicional daremos una forma de calcular a los primos regulares, los cuales son de gran importancia en la demostración del Último Teorema de Fermat.

Definición 3.3.1. Llamaremos el grupo de clases de ideales de $\mathcal{K}$ al cociente $\mathcal{H}_{\mathcal{K}} = \mathcal{F}_{\mathcal{K}}/\mathcal{P}_{\mathcal{K}}$.

Teorema 3.3.2. El grupo de clases $\mathcal{H}_{\mathcal{K}}$ es finito. Demostración: Véase Teorema 6.3 pág. 36 [23].

Definición 3.3.3 (Número de clase)**.**

$$h_{\mathcal{K}} = |\mathcal{H}_{\mathcal{K}}|,$$

es llamado el número de clase de $\mathcal{K}$.

Teorema 3.3.4. La factorización en un anillo de enteros $\mathcal{K}$ es única si, y solo si $h_{\mathcal{K}} = 1$.

Demostración:
$\Rightarrow$) Sea $\mathcal{K}$ un anillo de enteros con factorización única, por el Teorema (2.2.8) todo ideal de $\mathcal{K}$ es principal, es decir todo ideal fraccionario es principal, por tanto $\mathcal{F}_{\mathcal{K}} = \mathcal{P}_{\mathcal{K}}$, así, $h_{\mathcal{K}} = |\mathcal{H}_{\mathcal{K}}| = |\mathcal{F}_{\mathcal{K}}/\mathcal{P}_{\mathcal{K}}| = 1$ como quería probarse.
$\Leftarrow$) Sea $h_{\mathcal{K}} = 1$, es decir, $|\mathcal{H}_{\mathcal{K}}| = |\mathcal{F}_{\mathcal{K}}/\mathcal{P}_{\mathcal{K}}| = 1$. Entonces $\mathcal{F}_{\mathcal{K}} = \mathcal{P}_{\mathcal{K}}$. Por tanto todo ideal fraccionario es principal así todo ideal de $\mathcal{K}$ es principal, luego $\mathcal{K}$ es un anillo de enteros con Factorización Única.

Diremos que dos ideales I y $J \in \mathcal{F}_{\mathcal{K}}$ son asociados (y escribiremos $I \sim J$) si están en la misma clase módulo $\mathcal{P}_{\mathcal{K}}$, es decir $I = \mathfrak{a}J$, para algún $\mathfrak{a} \in \mathcal{P}_{\mathcal{K}}$. La clase de equivalencia de I por esta relación de equivalencia será denotada por $[I]$. Es decir,

$$I \sim J \text{ si, y solo si, } aI = bJ \text{ con } a, b \in \mathcal{P}_{\mathcal{K}}.$$

Dados $M,\ N$ ideales del anillo de enteros $\mathcal{K}$ definimos su producto como:

$$MN := \left\{ \sum_{i=1}^{k} m_i n_i \ : \ m_i \in M, n_i \in N,\ i = 1, \cdots, k,\ k \in \mathbb{N} \right\}$$

El conjunto $\mathfrak{a}^h = \mathfrak{a} \cdots \mathfrak{a}$ ($\mathfrak{a}$- h veces) se define como

$$\mathfrak{a}^h := \left\{ \sum_{i=1}^{k} \prod_{j=1}^{h} a_{ij} \ : \ a_{ij} \in \mathfrak{a}; i = 1, \cdots, k;\ j = 1, \cdots, h;\ k,\ h \in \mathbb{N} \right\}.$$

---

[23] J. NEUKIRCH. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992, págs. xiii+595. DOI: 10.1007/978-3-540-37663-7.

Proposición 3.3.5. Sea $\mathbb{K}$ un cuerpo numérico con número de clase h, y $\mathfrak{a}$ un ideal del anillo de enteros $\mathcal{K}$. Entonces

(a) $\mathfrak{a}^h$ es principal.

(b) Si q es primo relativo a h y $\mathfrak{a}^q$ es principal, entonces $\mathfrak{a}$ es principal.

Demostración:

(a). Sea $h = |\mathcal{H}_\mathcal{K}|$, tenemos[24], $[\mathfrak{a}]^h = [\mathcal{K}]$ para todo $[\mathfrak{a}] \in \mathcal{H}_\mathcal{K}$, porque $[\mathcal{K}]$ es el elemento identidad de $\mathcal{H}_\mathcal{K}$. Ya que $[\mathfrak{a}^h] = [\mathfrak{a}]^h = [\mathcal{K}]$, así $\mathfrak{a}^h \sim \mathcal{K}$, así $\mathfrak{a}^h$ es principal.

(b). Dado que $(q, h) = 1$, tomamos $u, v \in \mathbb{Z}$ tales que $uh + vq = 1$. Además, como $[\mathfrak{a}]^q$ es principal, entonces $[\mathfrak{a}]^q = [\mathcal{K}]$. De modo que

$$\begin{aligned}
[\mathfrak{a}] &= [\mathfrak{a}]^{uh+vq}, \\
&= ([\mathfrak{a}]^h)^u([\mathfrak{a}]^q)^v, \\
&= [\mathcal{K}]^u[\mathcal{K}]^v, \\
&= [\mathcal{K}].
\end{aligned}$$

Así, $\mathfrak{a}$ es principal.

Definición 3.3.6. Sea p un número primo, diremos que p es primo regular si no divide al número de clase del $p-$ésimo cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$.

Ejemplo 3.3.7. Los primeros primos regulares son:

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41$$

Esto puede evidenciarse en Criterio 11.9, página 198 [12], utilizando programación para calcular el número de clase con p un número primo.

Es de gran importancia saber cuando un número primo p es regular, en esta parte del libro mostraremos una forma adicional de calcular el número de clase, para así determinar algunos primos regulares. Supongamos que el grado de $\mathbb{K}$ es $n = r + 2s$, donde r y s se definen como: r es el número de inclusiones reales de $\mathbb{K}$ y $2s$ es el conjunto de inclusiones complejas de $\mathbb{K}$. Estos se eligen según el cuerpo numérico, ejemplo: para el cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$, con d entero positivo libre de

---

[24] Si $\mathcal{H}_\mathcal{K}$ es un grupo finito y $[\mathfrak{a}]$ es elemento de $\mathcal{H}$ $[\mathfrak{a}]^{|\mathcal{H}|} = 1_\mathcal{H}$.

cuadrados, cuyo grado $n = r+2s = 2$, se tienen 2 inclusiones reales y 0 inclusiones complejas ya que $\sqrt{d} \in \mathbb{R}$, mientras que para $\mathbb{Q}(\sqrt{-d})$ con $n = 2$ se tienen 0 inclusiones reales y 1 par de inclusiones complejas. Recordemos que Δ denota el discriminante de $\mathbb{K}$ sobre su $\mathbb{Q}-$ base. Introduciremos la definición de la constante de Minkowski para poder determinar si el número de clase de un anillo de enteros $\mathcal{K}$ es 1.

Definición 3.3.8. Sea $\mathcal{K}$ el anillo de enteros de un cuerpo numérico $\mathbb{K}$ con r inclusiones reales, s parejas de inclusiones complejas y discriminante Δ sobre una $\mathbb{Q}-$base de $\mathbb{K}$. Definimos la constante de Minkowski que denotaremos por M_{rs} como:

$$M_{rs} = \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n}.$$

Corolario 3.3.9. Sea $\mathcal{K}$ el anillo de enteros de un cuerpo numérico $\mathbb{K}$. Supongamos que todo ideal primo de $\mathcal{K}$ que contiene un número primo $p \leq M_{rs}\sqrt{|\Delta|}$ es principal. Entonces el número de clase de $\mathcal{K}$ es 1 y por tanto $\mathcal{K}$ es un DIP.

Demostración: Véase Corolario 4.8 [16].

Ejemplo 3.3.10. Veamos que para $p = 5$, tenemos a ζ_5 cuyo cuerpo ciclotómico $\mathbb{Q}(\zeta_5)$ es de grado $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = p - 1 = 4$. Además, sus inclusiones reales son $r = 0$ y las inclusiones complejas son 2 (ya que $2s = 4$), El discriminante sobre la $\mathbb{Q}-$base dada en la Proposición (3.2.19) está dado por:

$$\begin{aligned}\Delta\left[\left\{1, \zeta_5, \zeta_5^2, \zeta_5^3\right\}\right] &= (-1)^{(p-1)/2} \cdot p^{(p-2)} \\ &= (-1)^2 \cdot 5^3 \\ &= 5^3 \\ &= 125.\end{aligned}$$

Luego sustituyendo en M_{rs} tenemos que $M_{rs} \leq 0.152\sqrt{125} < 2$. Entonces por el Corolario (3.3.9) $p = 5$ es un primo regular.

Ejemplo 3.3.11. Veamos que para $p = 7$, tenemos a ζ_7 cuyo cuerpo ciclotómico $\mathbb{Q}(\zeta_7)$ es de grado $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = p - 1 = 6$. Además, sus inclusiones reales son $r = 0$ y el par de inclusiones complejas son 3 (ya que $2 \cdot 3 = 6$), El discriminante sobre la $\mathbb{Q}-$base dada en la Proposición (3.2.19) es

determinado por:

$$\begin{aligned}\Delta\left[\left\{1,\zeta_7,\zeta_7^2,\zeta_7^3,\zeta_7^4,\zeta_7^5\right\}\right] &= (-1)^{(p-1)/2}\cdot p^{(p-2)}\\ &= (-1)^3\cdot 7^5\\ &= -7^5\\ &= -16807.\end{aligned}$$

Luego sustituyendo en $M_{rs} \leq 0.032\sqrt{16807} < 5$. Entonces debemos considerar los primos $p = 2, 3$ el polinomio minimal de ζ_7 es $p(t) = t^6 + t^5 + \cdots + t + 1$. Pasamos a descomponer a $p(t)$ en $\mathbb{Z}_2[t]$ y en $Z_3[t]$ y nos queda:

$$\begin{aligned}&\mathbb{Z}_2[t]:\ f(t) = (t^3 + t^2 + 1)(t^3 + t + 1),\\ &\mathbb{Z}_3[t]:\ f(t) \text{ es irreducible en } \mathbb{Z}_3,\ \langle 3\rangle \text{ es primo.}\end{aligned}$$

Luego, $\langle 2\rangle = P_1P_2$ donde P_1, P_2 son ideales primos distintos. Por otro lado

$$\langle 2\rangle = \langle\zeta_7^3 + \zeta_7^2 + 1\rangle\langle\zeta_7^3 + \zeta_7 + 1\rangle.$$

Sin pérdida de generalidad $P_1 = \langle\zeta_7^3 + \zeta_7^2 + 1\rangle$ y $P_2 = \langle\zeta_7^3 + \zeta_7 + 1\rangle$ que son principales, por tanto 7 es primo regular.

Para $\mathbb{Z}_3[t],\ f(t)$ es irreducible, así $\langle 3\rangle$ es primo. Así, tenemos que todo ideal primo de $\mathcal{K}$ es principal, por el Corolario (3.3.9) $\mathcal{K}$ es un DIP, luego 7 es primo regular.

4. CUERPOS CICLOTÓMICOS

Sea $\zeta_p = e^{\frac{2\pi i}{p}}$ una raíz primitiva de la unidad (solución de la ecuación $x^p - 1 = 0$). El llamado cuerpo ciclotómico. En este capítulo desarrollaremos las definiciones, proposiciones y teoremas dados en los capítulos 1,2,3 en el contexto de los cuerpos ciclotómicos $\mathbb{Q}(\zeta_p)$.

Proposición 4.0.1. El polinomio mínimal de $\zeta_p = e^{\frac{2\pi i}{p}}$, con p un primo impar, sobre $\mathbb{Q}$ es

$$f(t) = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Luego el grado de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ es $p - 1$.

Demostración:
Veamos que $f(t)$ es el polinomio minimal de ζ_p. En efecto,

1. $f(t)$ es mónico, su coeficiente principal es 1.
2. $f(t)$ es irreducible, bastará con verificar que $f(t+1)$ es irreducible. Se tiene que:

$$f(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{r=1}^{p} \binom{p}{r} t^{r-1}.$$

   Ahora, por el criterio de Eisenstein tenemos que $f(t+1)$ es irreducible, ya que el coeficiente binomial $\binom{p}{r}$ es divisible por p si $1 \leq r \leq p-1$, y $\binom{p}{1} = p$ no es divisible por p^2. Por tanto, $f(t)$ es irreducible.

3. ζ_p es raíz de $f(t)$, de hecho

$$f(t) = \sum_{i=0}^{p-1} t^i, \ luego$$
$$tf(t) = t \cdot \sum_{i=0}^{p-1} t^i = \sum_{i=1}^{p} t^i.$$

sigue que

$$(1-t)f(t) = \sum_{i=0}^{p-1} t^i - t^{i+1} = 1 - t^p,$$

Así,

$$f(t) = \frac{t^p - 1}{t - 1}. \tag{7}$$

Vemos que ${\zeta_p}^p = 1$, pues ${\zeta_p}^p = (e^{\frac{2\pi i}{p}})^p = e^{2\pi i} = cos(2\pi) + isen(2\pi) = 1$ y $\zeta_p - 1 \neq 0$. Entonces ζ_p es raíz de $f(t)$. Por tanto, hemos probado que $f(t)$ es el polinomio minimal de ζ_p sobre $\mathbb{Q}$. Luego

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \partial f(t) = p - 1.$$

como quería probarse.

Proposición 4.0.2. La norma de $\mathbb{Q}(\zeta_p)$, donde $\zeta_p = e^{\frac{2\pi i}{p}}$ y p es un primo impar, es

$$N(\zeta_p) = N({\zeta_p}^i) = (-1)^{p-1} = 1.$$

Demostración: Dado que ${\zeta_p}^p = 1$, sea f definida en la Proposición(4.0.1) se tiene que $f(\zeta_p) = 0$. También para todo $i \in \{1, 2, \cdots, p-1\}$, tenemos

$$f({\zeta_p}^i) = \frac{{\zeta_p}^{ip} - 1}{{\zeta_p}^i - 1} = \frac{({\zeta_p}^p)^i - 1}{{\zeta_p}^i - 1} = \frac{1^i - 1}{{\zeta_p}^i - 1} = 0$$

y ${\zeta_p}^i - 1 \neq 0$ ya que $(p, i) = 1$.
El polinomio $f(t)$ es irreducible luego tiene $p - 1$ raíces diferentes en $\mathbb{C}$. Así las $p - 1$ raíces de $f(t)$ son las potencias de ${\zeta_p}^i$, con $1 \leq i \leq p - 1$. Entonces por el teorema del factor se sigue que

$$f(t) = (t - \zeta_p) \cdot (t - {\zeta_p}^2) \cdots (t - {\zeta_p}^{p-1}) = \prod_{i=1}^{p-1} (t - {\zeta_p}^i)$$

Así los conjugados de ζ_p son $\zeta_p, {\zeta_p}^2, \cdots, {\zeta_p}^{p-1}$, y los monomorfismos $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$, para $i = 1, 2, \cdots, p-1$ satisfacen:

$$\sigma_i(\zeta_p) = {\zeta_p}^i, \ (1 \leq i \leq p - 1).$$

En particular,

$$N(\zeta_p) = \prod_{i=1}^{p-1} \sigma_i(\zeta_p) = \zeta_p \cdot {\zeta_p}^2 \cdots {\zeta_p}^{p-1}$$

Como ζ_p es raíz de la unidad, por la Proposición (2.2.4) concluimos que

$$N(\zeta_p) = (-1)^{p-1} = 1.$$

Definición 4.0.3 (La función φ de Euler)**.** Para cada entero positivo n, definimos $\varphi(n)$ como el número de enteros positivos menores o iguales que n y primos relativos con n.

Observación:

1. Para un número compuesto $n = p_1^{e_1} \cdots p_k^{e_k}$, con p_i primo y $(p_i, p_j) = 1$, para cada $i \neq j$ tenemos que $\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k})$, donde $\varphi(p^a) = p^a - p^{a-1}$.
2. Para un número primo p como $\varphi(p) = p - 1$.

Lema 4.0.4. Los conjugados de ζ_m son los elementos de la forma ζ_m^k, con $(k, m) = 1$. Luego,

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) \;\; y \;\; m_{\zeta_m}(t) = \prod_{\substack{1 \leq k < m \\ (k,m)=1}} (t - \zeta_m^k)$$

Demostración: Véase Proposición 1.38. [16].

Corolario 4.0.5. Si m es una potencia de un primo p, entonces

$$N(1 - \zeta_m) = p.$$

Demostración: Sea $m = p^k$, para algún $k \in \mathbb{N}$ y por el Lema (4.0.4) tenemos que

$$m_{\zeta_m}(t) = \prod_{\substack{1 \leq k < m \\ (k,m)=1}} (t - \zeta_m^k) = \frac{t^{p^r}-1}{t^{p^{r-1}}-1} = 1 + t^{p^{r-1}} + \cdots + t^{p^{r-1}(p-1)}.$$

Además, las raíces de $t^{p^r} - 1$ son las raíces p^r-ésimas de la unidad. Por tanto

$$\begin{aligned} N(1 - \zeta_m) &= \prod_{1 \leq k < m} \sigma_i(1 - \zeta_m) \\ &= \prod_{1 \leq k < m} \sigma_i(1) - \sigma_i(\zeta_m) \\ &= \prod_{1 \leq k < m} (1 - \sigma_i(\zeta_m)) \\ &= m_{\zeta_m}(1) \\ &= p. \end{aligned}$$

como quería probarse.

Teorema 4.0.6. El anillo de enteros de $\mathbb{Q}(\zeta_n)$ es $\mathbb{Z}[\zeta_n]$.

Demostración: Véase Teorema 3.5. [12] y Teorema 1.42. [16].

Teorema 4.0.7. El discriminante de $\mathbb{Q}(\zeta_p)$, donde $\zeta_p = e^{\frac{2\pi i}{p}}$ y p primo impar, es:

$$(-1)^{p-1/2} \cdot p^{p-2}.$$

Demostración: Una $\mathbb{Z}-$base de $\mathcal{K}$ es $\{1, \zeta_p, \cdots, {\zeta_p}^{p-2}\}$, pues $\mathcal{K} = \mathbb{Z}[\zeta_p]$. Ya que por la Proposición (3.2.19) el discriminante es igual a

$$(-1)^{(p-1)(p-2)/2} \cdot N(Df(\zeta_p)), \tag{8}$$

siendo $f(t)$ como en la Proposición (4.0.1). Puesto que p es impar, la Ecuación (8) queda de la forma

$$(-1)^{(p-1)/2} N(Df(\zeta_p)).$$

Note que la derivada de $f(t) = \frac{t^{p-1}-1}{t-1}$, es

$$Df(t) = \frac{pt^{p-1}(t-1) - (t^p - 1)}{(t-1)^2},$$

así, al evaluar $Df(\zeta_p)$ tenemos

$$\begin{aligned} Df(\zeta_p) &= \frac{p{\zeta_p}^{p-1}(\zeta_p - 1) - ({\zeta_p}^p - 1)}{(\zeta_p - 1)^2} \\ &= \frac{p{\zeta_p}^{p-1}(\zeta_p - 1)}{(\zeta_p - 1)^2} \\ &= \frac{p{\zeta_p}^{p-1}}{(\zeta_p - 1)} \\ &= \frac{-p{\zeta_p}^{p-1}}{(1 - \zeta_p)}. \end{aligned}$$

Si evaluamos la norma sobre $Df(\zeta_p)$ obtenemos

$$\begin{aligned} N(Df(\zeta_p)) &= \frac{-N(p)N(\zeta_p)^{p-1}}{N(1-\zeta_p)} \\ &= \frac{(-p)^{p-1}}{p} \\ &= p^{p-2}. \end{aligned}$$

Finalmente al sustituir en la Ecuación (8) se tiene

$$(-1)^{p-1/2} \cdot p^{p-2}$$

Ejemplo 4.0.8. Para ζ_p con $p = 3$, entero algebraico de grado 2, tal que

$$\zeta_p = e^{2\pi i/3} = \tfrac{-1+\sqrt{-3}}{2}.$$

Según el resultado del Ejemplo (3.2.5) el discriminante de la $\mathbb{Q}-$base de $\mathbb{Q}(\sqrt{-3})$ es -3 (ya que $-3 \equiv 1 \pmod 4$ y por el Teorema (4.0.7) tenemos que $(-1)^{2/2}3^1 = -3$, así, evidenciamos que coinciden.

Teorema 4.0.9. Todo ideal no nulo del anillo de enteros $\mathbb{Z}[\zeta_p]$ puede escribirse como un producto de ideales primos, de forma única, salvo el orden de los factores.

Demostración Véase Teorema 5.6 [12].

Teorema 4.0.10. Toda unidad de $\mathbb{Z}[\zeta_p]$ es de la forma $r{\zeta_p}^g$, donde $r \in \mathbb{R}$ y $g \in \mathbb{Z}$.

Demostración: Véase Lema 11.7. [12].

Teorema 4.0.11. Sea $\zeta_p = e^{\frac{2\pi i}{p}}$. Entonces

1. $\langle 1-\zeta_p\rangle^{p-1} = \langle p\rangle$.
2. $\mathcal{N}(\langle 1-\zeta_p\rangle) = p$.

Demostración:

1. Notemos que para todo $j = 1, \cdots, p-1$ los números $(1-\zeta_p)$ y $(1-{\zeta_p}^j)$ son asociados en $\mathbb{Z}[\zeta_p]$. Ya que $(1-\zeta_p) \mid (1-{\zeta_p}^j)$ para todo $j \not\equiv 0 (\text{mód } p)$ y para un determinado t tenemos que $jt \equiv 1 (\text{mód } p)$ así $(1-\zeta_p) = (1-{\zeta_p}^{jt})$, luego $(1-{\zeta_p}^j) \mid (1-\zeta_p)$. Por tanto hemos probado que

$(1-\zeta_p) \sim (1-{\zeta_p}^j)$.

Por otra parte, la norma de $1-\zeta_p$ está dada por:

$$\begin{aligned} N(1-\zeta_p) &= \prod_{i=1}^{p-1} \sigma_i(1-\zeta_p) \\ &= \prod_{i=1}^{p-1} (\sigma_i(1) - \sigma - i(\zeta_p)) \\ &= \prod_{i=1}^{p-1} (1-{\zeta_p}^i). \end{aligned}$$

Pero, por la Proposición (4.0.1) tenemos que

$$\prod_{i=1}^{p-1} (t-{\zeta_p}^i) = 1 + t + \cdots + t^{p-1}.$$

Así, para $t=1$ tenemos

$$\prod_{i=1}^{p-1} (1-{\zeta_p}^i) = 1 + 1 + \cdots + 1^{p-1} = p.$$

De lo anterior, concluimos que

$$\prod_{i=1}^{p-1} (1-{\zeta_p}^i) \sim p.$$

Así, por (b) de la Proposición (2.2.3) tenemos que

$$\prod_{i=1}^{p-1} \langle 1-{\zeta_p}^i \rangle = \langle p \rangle,$$

y $\langle 1-{\zeta_p}^i \rangle = \langle 1-\zeta_p \rangle$, para $i = 1, \cdots, p-1$, entonces

$$\langle p \rangle = \prod_{i=1}^{p-1} \langle 1-{\zeta_p}^i \rangle = \prod_{i=1}^{p-1} \langle 1-\zeta_p \rangle = \langle 1-\zeta_p \rangle^{p-1},$$

como quería probarse.

2. Dado que $\langle 1-\zeta_p \rangle$ es un ideal principal, por la Proposición (3.2.18) tenemos que $N(\langle 1-\zeta_p \rangle) = |N(1-\zeta_p)| = |p| = p$.

La prueba del Teorema (4.0.11)(b) concluimos que $|\mathbb{Z}[\zeta_p]/\langle 1-\zeta_p\rangle| = p$, así observamos, sea $\mathbb{Z}[\zeta_p] \to \mathbb{Z}[\zeta_p]/\langle 1-\zeta_p\rangle$ el homomorfismo natural, sigue que todo elemento de $\mathbb{Z}[\zeta_p]$ es congruente módulo $\langle 1-\zeta_p\rangle$ a algún $r = 0, 1, \cdots, p-1$. Y por tanto continuamos con el siguiente teorema.

Teorema 4.0.12. Para cada $\alpha \in \mathbb{Z}[\zeta_p]$, existe $a \in \mathbb{N}$ tal que $\alpha^p \equiv a \pmod{\mathfrak{l}^p}$, donde $\mathfrak{l} = \langle 1-\zeta_p\rangle$.
Demostración: Sea $\alpha \in \mathbb{Z}[\zeta_p]$, afirmamos que existe $b \in \mathbb{Z}$ tal que $\alpha \equiv b \pmod{\langle 1-\zeta_p\rangle}$. Ahora

$$\alpha^p - b^p = \prod_{j=0}^{p-1} (\alpha - {\zeta_p}^j b).$$

Puesto que $\zeta_p \equiv 1 \pmod{\mathfrak{l}}$ cada factor de la igualdad es congruente con $\alpha - b \equiv 0 \pmod{\mathfrak{l}}$. Por tanto, por la Proposición (2.3.4) $\alpha^p - b^p \equiv 0 \pmod{\mathfrak{l}^p}$.

5. EL TEOREMA DE ERNS KUMMER

En este capítulo presentaremos los detalles de la demostración del Último Teorema de Fermat para n un primo regular, fundamentada por Erns Kummer.

Teorema 5.0.1. Si p es un primo regular impar, entonces la ecuación

$$x^p + y^p = z^p, \tag{9}$$

no tiene soluciones en enteros no nulos $x,\ y,\ z$ satisfaciendo

$$p \nmid x,\ p \nmid y,\ p \nmid z.$$

Demostración:
Realizamos la demostración por reducción al absurdo. Supongamos que existen $x, y, z \in \mathbb{Z}$ no nulos que satisfacen la ecuación (9) con p primo regular. Podemos, como de costumbre, asumir además que x, y, z son pares coprimos (ya que si hay un máximo común divisor, éste podría factorizarse), es decir, sin pérdida de generalidad $(x, y) = (y, z) = (x, z) = 1$. Al factorizar el lado izquierdo de la ecuación (9) en $\mathbb{Q}(\zeta_p)$ obtenemos

$$\begin{aligned} x^p + y^p &= -y^p \left(\frac{-x^p}{y^p} - 1 \right) \\ &= -y^p \left(\left(\frac{-x}{y} \right)^p - 1 \right) \\ &= -y^p (t^p - 1), \text{ donde } t = \frac{-x}{y}, \end{aligned}$$

Por la Proposición (4.0.1) tenemos

$$\begin{aligned} x^p + y^p &= -y^p (t-1)(t^{p-1} + t^{p-2} + \cdots + t + 1) \\ &= -y^p (t-1)(t-\zeta_p) \cdots (t-{\zeta_p}^{p-1}) \\ &= -y^p \prod_{i=0}^{p-1} (t-{\zeta_p}^i). \end{aligned}$$

y sustituyendo $t = \frac{-x}{y}$ tenemos

$$\begin{aligned} x^p + y^p &= -y^p \prod_{i=0}^{p-1} \left(\frac{-x}{y} - {\zeta_p}^i \right) \\ &= \prod_{i=0}^{p-1} y \left(\frac{x}{y} + {\zeta_p}^i \right) \\ &= \prod_{j=0}^{p-1} (x + {\zeta_p}^j y). \end{aligned}$$

De modo que,

$$x^p + y^p = \prod_{j=0}^{p-1} (x + {\zeta_p}^j y) = z^p.$$

Así, $\prod_{j=0}^{p-1} (x + {\zeta_p}^j y) \sim z^p$ y $\mathbb{Z}[\zeta_p]$ es un dominio entero, entonces, por la Proposición (2.2.3) (b) se tiene que $\left\langle \prod_{j=0}^{p-1} x + {\zeta_p}^j y \right\rangle = \langle z^p \rangle$. Ahora como $\mathbb{Z}[\zeta_p]$ es un anillo conmutativo con unidad tenemos [25]

$$\prod_{j=0}^{p-1} \langle x + {\zeta_p}^j y \rangle = \langle z \rangle^p. \tag{10}$$

Probaremos que todos los factores de la ecuación (10) son comaximales dos a dos. Supongamos que no son comaximales dos a dos. Por la Definición (2.1.4) dados $\langle x + {\zeta_p}^l y \rangle$, $\langle x + {\zeta_p}^k y \rangle$, con $l \neq k$ entonces $\langle x + {\zeta_p}^l y \rangle + \langle x + {\zeta_p}^k y \rangle \neq \mathbb{Z}[\zeta_p]$. Por el Teorema (2.1.3) existe en $\mathbb{Z}[\zeta_p]$ un ideal maximal $\mathcal{M}$ y por definición $\langle x + {\zeta_p}^l y \rangle$, $\langle x + {\zeta_p}^k y \rangle$ son ideales, entonces $\langle x + {\zeta_p}^l y \rangle + \langle x + {\zeta_p}^k y \rangle$ es ideal de $\mathbb{Z}[\zeta_p]$ y por la Proposición (2.1.8) se tiene que

$$\langle x + {\zeta_p}^l y \rangle + \langle x + {\zeta_p}^k y \rangle \ \subseteq \mathcal{M} \ : \ 0 \leqslant k < l \leqslant p - 1.$$

Por otro lado,

$$(x + {\zeta_p}^k y) - (x + {\zeta_p}^l y) = {\zeta_p}^k y (1 - {\zeta_p}^{l-k}). \tag{11}$$

Sea $j = l - k$, probaremos que $(1 - {\zeta_p}^j) \ \sim \ (1 - \zeta_p)$, es decir por la Definición(2.2.1) veremos que $(1 - \zeta_p) \mid (1 - {\zeta_p}^j)$ y $(1 - {\zeta_p}^j) \mid (1 - \zeta_p)$.

---

[25] por inducción se puede probar que en un anillo conmutativo con unidad $\left\langle \prod_{i=0}^{n} \alpha_i \right\rangle = \prod_{i=0}^{n} \langle \alpha_i \rangle$

Notemos que $(1-\zeta_p) \mid (1-{\zeta_p}^j)$, para todo $j = \{0, 1, 2, \cdots, p-1\}$, veamos que $(1-{\zeta_p}^j) \mid (1-\zeta_p)$. Si elegimos $t \in \mathbb{Z}$ tal que $jt \equiv 1$ (mód), ya que $(1-{\zeta_p}^j) \mid (1-{\zeta_p}^{jt})$ y $(1-{\zeta_p}^{jt}) \mid (1-\zeta_p)$, por transitividad de la relación "divide" $(1-{\zeta_p}^j) \mid (1-\zeta_p)$, así $(1-{\zeta_p}^j) \sim (1-\zeta_p)$.

Por la Proposición (2.2.2), existe $u \in \mathcal{U}(\mathbb{Z}[\zeta_p])$ tal que $1-{\zeta_p}^k = (1-\zeta_p)u$ y ${\zeta_p}^k \in \mathcal{U}(\mathbb{Z}[\zeta_p])$. Por definición de unidad existe ${\zeta_p}^{p-k} \in \mathbb{Z}[\zeta_p]$, tal que ${\zeta_p}^k \cdot {\zeta_p}^{p-k} = {\zeta_p}^p = 1$, entonces sustituyendo en (11)

$$y(1-\zeta_p)u{\zeta_p}^k \in \mathcal{M} \quad u, {\zeta_p}^k \in \mathcal{U}(\mathbb{Z}[\zeta_p]). \tag{12}$$

Así $u{\zeta_p}^k \in \mathcal{U}(\mathbb{Z}[\zeta_p])$, y $y(1-\zeta_p) \in \mathcal{M}$. Por el Teorema (2.1.6) $\mathcal{M}$ es un ideal primo. Luego de la Definición (2.1.2) tenemos que $y \in \mathcal{M}$ o $(1-\zeta_p) \in \mathcal{M}$. Veamos que $z \in \mathcal{M}$ por la ecuación (10) tenemos que $\langle x+{\zeta_p}^i y\rangle \mid \langle z\rangle^p$, para todo $i = 0, 1, \cdots, p-1$, luego $\langle z\rangle^p \subseteq \langle x+{\zeta_p}^i y\rangle \subseteq \mathcal{M}$, y $\langle z\rangle^p \subseteq \mathcal{M}$. Entonces $z^p \in \mathcal{M}$ y como $\mathcal{M}$ es primo, $z \in \mathcal{M}$.

Caso 1. ($y \in \mathcal{M}$). Por hipótesis sean y, z coprimos, entonces existen $a, b \in \mathbb{Z}$ tales que $ay + bz = 1$ de lo que sigue que $1 \in \mathcal{M}$ lo cual es absurdo, pues $\mathcal{M}$ es maximal.

Caso 2 ($(1-\zeta_p) \in \mathcal{M}$). Por la Definición (1.3.1) $N(1-\zeta_p) = \prod_{i=1}^{p-1} \sigma_i(1-\zeta_p)$, donde $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$, para todo $i = \{1, 2, \cdots, p-1\}$ es un monomorfismo, entonces por el Teorema (1.2.23) tenemos que $N(1-\zeta_p) = \prod_{i=1}^{p-1} 1-\sigma_i(\zeta_p)$, con $\sigma_i(\zeta_p)$ los distintos ceros en $\mathbb{C}$ del polinomio minimal de ζ_p sobre $\mathbb{Q}$, con $p_{\zeta_p}(t) = \sum_{i=0}^{p-1} t^i = \prod_{i=1}^{p-1} (t-{\zeta_p}^i)$, así $\sigma_i(\zeta_p) = {\zeta_p}^i$, con $i = 1, 2, \cdots, p-1$. Entonces

$$N(1-\zeta_p) = \prod_{i=1}^{p-1}(1-{\zeta_p}^i) = \sum_{i=0}^{p-1} 1 = p. \tag{13}$$

Por la Proposición (2.1.17) $(1-\zeta_p)$ es primo, luego, por la Proposición (2.2.3) (c), $\langle 1-\zeta_p\rangle$ es primo y $\mathcal{M} \mid \langle 1-\zeta_p\rangle$, así, $\mathcal{M} = \langle 1-\zeta_p\rangle$ y $z \in \mathcal{M}$. De esta $\langle 1-\zeta_p\rangle \mid z$ y por la Proposición (1.3.3) tenemos que $N(\langle 1-\zeta_p\rangle) \mid N(z) = p \mid z^{p-1}$. Luego $p \mid z$ contradiciendo nuestra hipótesis.

Ya que en ambos casos se da un absurdo, entonces, $\langle x+{\zeta_p}^l y\rangle$ y $\langle x+{\zeta_p}^k y\rangle$, con $l \neq k$, son comaximales.

Es decir podemos escribir a $\mathbb{Z}[\zeta_p] = \langle x+{\zeta_p}^l y\rangle$ y $\langle x+{\zeta_p}^k y\rangle$, con $l \neq k$, por ser $\mathbb{Z}[\zeta_p]$ un dominio, $\langle 1-\zeta_p\rangle$ es primo y es irreducible. Por el Teorema (2.2.8) se sigue que, la factorización de (10) es única salvo el orden de los factores. Luego

$$\prod_{i=1}^{p-1} \langle x+{\zeta_p}^i y\rangle \tag{14}$$

y cada factor es primo e irreducible. Esto prueba que $\langle x + {\zeta_p}^i y\rangle$ es un ideal principal, y deducimos que todo factor es una p potencia de un ideal

$$\langle x + {\zeta_p}^i y\rangle = \mathfrak{a}_i^p,$$

con $\mathfrak{a}_i^p$ ideal principal, para todo $i = \{0, 1, \cdots, p-1\}$.
Como p es un primo regular, si h es el número de clase de $\mathbb{Q}(\zeta_p)$, entonces $p \nmid h$. Por la Proposición (3.3.5) (b), $\mathfrak{a}$ es principal, sea $\langle\delta\rangle = \mathfrak{a}$, así $\langle\delta\rangle \sim \mathfrak{a}$, entonces existe $\epsilon \in \mathcal{U}(\mathbb{Z}[\zeta_p])$ tal que $x + \zeta_p y = \epsilon\delta^p$ por el Teorema (4.0.10) $\epsilon = r{\zeta_p}^g$, donde $r \in \mathbb{R}$ y $g \in \mathbb{Z}$ entonces

$$x + \zeta_p y = r{\zeta_p}^g \delta^p. \tag{15}$$

Por el Teorema (4.0.12) existe $a \in \mathbb{Z}$ tal que $\delta^p \equiv a \pmod{\mathfrak{l}^p}$. Reemplazando en (15) tenemos

$$x + \zeta_p y \equiv ra{\zeta_p}^g \pmod{\mathfrak{l}^p}.$$

Ahora, por el Teorema (4.0.11), $\langle p\rangle \mid \mathfrak{l}^p$ y la definición de congruencia $\mathfrak{l}^p \mid (x + \zeta_p y - ra{\zeta_p}^g)$ y $\langle p\rangle \mid \mathfrak{l}^p$. Sigue por transitividad que $\langle p\rangle \mid (x + \zeta_p y - ra{\zeta_p}^g)$, entonces $x + \zeta_p y \equiv ra{\zeta_p}^g \pmod{\langle p\rangle}$. Sabemos que ${\zeta_p}^{-g} \in \mathcal{U}(\mathbb{Z}[\zeta_p])$ y de esto

$${\zeta_p}^{-g}(x + \zeta_p y) \equiv ra \pmod{\langle p\rangle}, \tag{16}$$

$${\zeta_p}^g(x + {\zeta_p}^{-1} y) \equiv ra \pmod{\langle p\rangle}. \tag{17}$$

restando (16) con (17) obtenemos

$$x{\zeta_p}^{-g} + y{\zeta_p}^{1-g} - x{\zeta_p}^g - y{\zeta_p}^{g-1} \equiv 0 \pmod{\langle p\rangle}. \tag{18}$$

Supongamos para (18) que $g \equiv 0 \pmod{p}$, entonces ${\zeta_p}^g = 1$. Así, los términos en x se anulan y obtenemos:

$$y\zeta_p - y{\zeta_p}^{-1} = y(\zeta_p - {\zeta_p}^{-1}) = y\frac{{\zeta_p}^2 - 1}{\zeta_p} \equiv 0 \pmod{\langle p\rangle}.$$

Notemos que $\zeta_p \in \mathcal{U}(\mathbb{Z}[\zeta_p])$, entonces

$$y({\zeta_p}^2 - 1) = y(1 - \zeta_p)(1 + \zeta_p) \equiv 0 \pmod{\langle p\rangle} \tag{19}$$

y además $(\zeta_p + 1) \in \mathcal{U}(\mathbb{Z}[\zeta_p])$, pues $\zeta_p \in \mathcal{U}(\mathbb{Z}[\zeta_p])$ y $1 \in \mathcal{U}(\mathbb{Z}[\zeta_p])$. Por tanto,

$$y(1 - \zeta_p) \equiv 0 \text{ (mód } \langle p \rangle).$$

De nuevo, por Teorema(4.0.11) tenemos que $l^{p-1} = \langle 1 - \zeta_p \rangle^{p-1} = \langle p \rangle$ y $p - 1 > 2$. Así, $y(1 - \zeta_p) \in \langle 1 - \zeta_p \rangle^{p-1}$ y $1 - \zeta_p \in \langle 1 - \zeta_p \rangle$. De este modo, $y \in \langle 1 - \zeta_p \rangle^{p-1}$ y $(1 - \zeta_p) \mid y$. Aplicando norma $N(1 - \zeta_p) = p \mid y^{p-1} = N(y)$ y $p \mid y^{p-1}$. Luego $p \mid y$ contradiciendo nuestra hipótesis pues $p \mid z$. Por tanto, $g \not\equiv 0$ (mód p).

Si $g \equiv 1$ (mód p), luego $g - 1 \equiv 0$ (mód p). De modo que en (18) los términos con las potencias $1 - g$ y $g - 1$ se anulan por tanto tenemos que

$$x({\zeta_p}^{-1} - \zeta_p) = x\frac{1 - {\zeta_p}^2}{\zeta_p} = x(1 - {\zeta_p}^2) = x(1 - \zeta_p)(1 + \zeta_p) \equiv 0 \text{ (mód } \langle p \rangle),$$

con $(1 + \zeta_p) \in \mathcal{U}(\mathbb{Z}[\zeta_p])$. Así $x(1 - \zeta_p) \equiv 0$ (mód $\langle p \rangle$) y $(1 - \zeta_p) \mid x$. Aplicando norma encontramos que $p|x$ lo cual contradice nuestra hipótesis. Luego $g \not\equiv 1$ (mód p) y por definición de congruencia escribimos la ecuación (18) como:

$$\alpha p = x{\zeta_p}^{-g} + y{\zeta_p}^{1-g} - x{\zeta_p}^{g} - y{\zeta_p}^{g-1}, \tag{20}$$

para algún $\alpha \in \mathbb{Z}[\zeta_p]$ donde los exponentes $-g,\ 1-g,\ g,\ g-1$ no son divisibles por p de esto,

$$\alpha = \frac{x}{p}{\zeta_p}^{-g} + \frac{y}{p}{\zeta_p}^{1-g} - \frac{x}{p}{\zeta_p}^{g} - \frac{y}{p}{\zeta_p}^{g-1}.$$

Pero, $\{1, \zeta_p, {\zeta_p}^2, \cdots, {\zeta_p}^{p-2}\}$ es una $\mathbb{Z}$- base para $\mathbb{Z}[\zeta_p]$ y $\alpha \in \mathbb{Z}[\zeta_p]$ entonces $\frac{x}{p}, \frac{y}{p}, \frac{z}{p} \in \mathbb{Z}$, lo cual contradice nuestra hipótesis. El hecho de que $g \not\equiv 0, 1$ (mód p) obliga que $\frac{x}{p}, \frac{y}{p}, \frac{z}{p} \in \mathbb{Z}$ entonces realizando las posibles combinaciones dos a dos de $g, 1-g, -g, g-1$ obtenemos que $2g \equiv 1$ (mód p). Al multiplicar ${\zeta_p}^g$ en ambos lados de la igualdad de (20) tenemos

$$\begin{aligned}
\alpha p{\zeta_p}^g &= x + y\zeta_p - x{\zeta_p}^{2g-1+1} - y{\zeta_p}^{2g-1} \\
&= x + y\zeta_p - x\zeta_p - y \\
&= x(1 - \zeta_p) + y(-(1 - \zeta_p)) \\
&= (x - y)(1 - \zeta_p).
\end{aligned}$$

Sigue que $(1-\zeta_p) \mid (x-y)$ al evaluar la norma obtenemos, $p \mid (x-y)^{p-1}$. De modo que $p \mid (x-y)$ esto es $x \equiv y \pmod{p}$ y por la simetría de (9) tenemos que $y \equiv z \pmod{p}$. De lo anterior

$$0 \equiv x^p + y^p + z^p \equiv 3x^p \pmod{p}.$$

Por hipótesis $p \nmid x$ entonces $p = 3$. Luego, la ecuación (9) queda $x^3 + y^3 = z^3$. Por Teorema (2.3.1) $x^3 \equiv x \pmod{3}$, $y^3 \equiv y \pmod{3}$ y $z^3 \equiv z \pmod{3}$. Así mismo del Teorema (2.3.3) tenemos que $x \equiv \pm 1 \pmod{3}$, $y \equiv \pm 1 \pmod{3}$ y $z \equiv \pm 1 \pmod{3}$; luego $x^p \equiv \pm 1 \pmod{3}$, $y^p \equiv \pm(1 \text{ mód } 3)$ y $z^p \equiv \pm 1 \pmod{3}$. Por la Proposición (2.3.4) tenemos que $x^p \equiv \pm 1 \pmod{9}$, $y^p \equiv \pm 1 \pmod{9}$ y $z^p \equiv \pm 1 \pmod{9}$. Esto implica que

$$\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{9},$$

lo cual es imposible. Así $p \neq 3$ y tenemos una contradicción. Por tanto, no existen enteros $x, y, z \in \mathbb{Z}$ no nulos que satisfacen la ecuación (9) tales que $(x,z) = (y,z) = (x,y) = 1$ y con p primo regular.

6. COMENTARIOS FINALES

El trabajo de Kummer sobre las congruencias para los números de clases en los cuerpos ciclotómicos fueron generalizadas en el siglo XX por Iwasawa y, por Kubota y Leopoldt en su teoría de las funciones zeta p-ádicas.

Vamos a presentar una relación entre los primos regulares y los números de Bernoulli, los cuales constituyen una sucesión de números racionales con profundas conexiones en teoría de números. También aparecen en la expansión de las funciones tangente y tangente hiperbólica mediante series de Taylor, en la fórmula de Euler-Maclaurin [26] y en las expresiones de ciertos valores de la función zeta de Riemann [27].

Definición 6.0.1. Los números de Bernoulli denotados por B_k, se definen por la ecuación

$$\frac{u}{e^u - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} u^k$$

Evaluando en la fórmula obtenemos

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_{2k+1} = 0\ para\ k = 1, 2, \cdots ;\ y$$

los números B_{2k} son no nulos y de signo alternado. Véase página 99. [28].

Teorema 6.0.2. Un primo p es regular si, y solo si, p divide al numerador del número de Bernoulli B_k para algún índice par $2k$ en el intervalo $2 \leq 2k \leq p - 3$.
Esto puede verificarse en Criterio 11.9. página 198. [12].

---

[26] la fórmula de Euler-Maclaurin: relaciona a integrales con series. Esta fórmula puede ser usada para aproximar integrales por sumas finitas o, de forma inversa, para evaluar series (finitas o infinitas) resolviendo integrales.

[27] La función zeta de Riemann: es una función que tiene una importancia significativa en la teoría de números, por su relación con la distribución de los números primos. También tiene aplicaciones en otras áreas tales como la física, la teoría de probabilidades y estadística aplicada.

[28] C. IVORRA. *Funciones de variable compleja con aplicaciones a la teoría de números*.

BIBLIOGRAFÍA

DUMMIT, D. S. y R. M. FOOTE. *Abstract algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991, págs. xiv+658 (vid. págs. 11, 14, 17, 24).

FRALEIGH, J. B. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967, págs. xvi+447 (vid. pág. 36).

GÓMEZ, C. *Biografías de cinco números maravillosos* $\varphi,\ \pi,\ c,\ e,\ i$.. Editorial Universidad de Caldas., 2005 (vid. pág. 13).

IVORRA, C. *Funciones de variable compleja con aplicaciones a la teoría de números* (vid. pág. 57).

JIMÉNEZ L., GORDILLO J. y RUBIANO-G. *Teoría de números*. Para principiantes. [For beginners]. Universidad Nacional de Colombia, Facultad de Ciencias, Departamento de Estadística, Bogotá, 1999, págs. ii+216 (vid. pág. 32).

NEUKIRCH, J. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992, págs. xiii+595. DOI: 10.1007/978-3-540-37663-7 (vid. pág. 40).

R., GOMEZ. *El anillo de los enteros algebraicos y dominios de Dedekind*. Bucaramanga - Colombia, 2015 (vid. págs. 11, 16, 24, 25, 35).

RIOS, A. *Teoría de números algebraicos*. 2019 (vid. págs. 17, 25, 37, 42, 46, 47).

SINGH, S. *Fermat's enigma*. The epic quest to solve the world's greatest mathematical problem, With a foreword by John Lynch. Walker y Company, New York, 1997, págs. xx+315 (vid. pág. 9).

SPINDLER, K. *Abstract algebra with applications. Vol. II*. Rings and fields. Marcel Dekker, Inc., New York, 1994, págs. xvi+531 (vid. págs. 11, 12, 14, 16, 23, 25, 26).

STEWART I. Y TALL, D. *Algebraic number theory and Fermat's last theorem*. Third. A K Peters, Ltd., Natick, MA, 2002, págs. xx+313 (vid. págs. 11, 12, 14, 16, 25, 32, 35, 37-39, 41, 47, 48, 57).

WILES, A. "Modular elliptic curves and Fermat's last theorem". En: *Ann. of Math. (2)* 141.3 (1995), págs. 443-551. DOI: 10.2307/2118559 (vid. pág. 9).

ZARISKI O. y PIERRE, S. *Commutative algebra, Volume I*. The University Series in Higher Mathematics. With the cooperation of I. S. Cohen. D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, págs. xi+329 (vid. pág. 21).