Sobre Dominios Euclídeos y Cuerpos Ciclotómicos

Johan Sebastián Cortés Villamizar

Trabajo de Grado para optar al título de Matemático

Director

Arnoldo Rafael Teherán Herrera

Doctorado en Matemáticas

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Matemáticas

Bucaramanga

2021

Dedicatoria

Este trabajo viene dedicado para todas aquellas personas que apoyaron el desarrollo y ejecución de este trabajo de grado.

Agradecimientos

Quiero agradecer a las personas que me estuvieron apoyando desde que me matriculé, madre, padre, tíos, familiares y amigos de infancia Bayron y Jhojan, también quiero agradecer a la gente que fui conociendo en estos 4 años Camilo Rueda, Edson Suarez, Elian Rueda, a mi pareja Jennyfer, compañeros de olimpiadas, Jorge Eliécer Gómez que me mostraron la cara más organizada y responsable que hay en el rol de profesor y como último, agradezco al profesor Arnoldo Teherán Herrera por la dirección del trabajo y al profesor Gilberto Arenas Díaz por el apoyo.

Tabla de Contenido

Introducción **9**

1. Preliminares **11**

1.1. Preliminares en teoría de números 11

1.2. Algunos resultados sobre grupos, anillos, cuerpos y módulos 13

1.3. El cuerpo de los números complejos 23

2. Polinomios ciclotómicos **27**

2.1. Raíz primitiva de la unidad 27

2.2. Algunos resultados sobre $\Phi_n(x)$ 29

3. Dominios euclídeos **45**

3.1. Estructura de los dominios euclídeos 46

3.2. Condiciones necesarias para que un cuerpo sea euclídeo 57

3.3. Condiciones suficientes para que un cuerpo sea euclídeo 65

4. Cuerpos de funciones algebraicas **70**

4.1. Lugares 71

4.2. Cuerpos de funciones racionales 84

4.3. Cuerpos de funciones ciclotómicos 90

Referencias Bibliográficas **99**

Lista de Tablas

Tabla 1. Tomado de Akhtar (1995) 65

Resumen

TÍTULO: Sobre Dominios Euclídeos y Cuerpos Ciclotómicos [*]

AUTOR: Johan Sebastián Cortés Villamizar [**]

PALABRAS CLAVE: Polinomios Ciclotómicos, Dominios Euclídeos, Cadenas Euclídeas, Lugares, Cuerpos de Funciones Ciclotómicas.

DESCRIPCIÓN:

En este trabajo consiste en estudiar algunos conceptos y resultados de la teoría de anillos y cuerpos. En el primer capítulo se retoman conceptos y resultados clásicos sobre grupos, anillos, cuerpos y módulos, necesarios para entender la parte central del trabajo.

En el segundo capítulo se definen las raíces primitivas de la unidad, los polinomios ciclotómicos y se prueban resultados que nos permiten calcular un polinomio ciclotómico $\Phi_n(x)$ independiente del valor de $n \in \mathbb{Z}^+$, además se muestran algunos ejemplos donde se usan esos resultados.

En el tercer capítulo se retoma la definición de dominio euclídeo y se introducen nuevos conceptos como conjunto derivado, cadena euclídea y unos ejemplos donde se hace uso de estos para probar cuando un anillo es un dominio euclídeo. Se presentan las condiciones necesarias y suficientes para que un anillo sea un dominio euclídeo, llegando a un resultado importante, basado en desigualdades para mostrar cuando dominio es euclídeo.

En el último capítulo se presentan el cuerpo de funciones algebraicas, lugares y valuaciones, con el objetivo de mostrar la construcción del cuerpo de funciones ciclotómicos, se exponen algunos resultados mostrados en el capítulo anterior, vía esta nueva construcción.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas, Matemáticas. Director: Arnoldo Rafael Teherán Herrera, Doctorado en Matemáticas

Abstract

TITLE: On Euclidean Domains and Cyclotomic Fields [*]

AUTHOR: Johan Sebastián Cortés Villamizar [**]

KEYWORDS: Cyclotomic Polynomials, Eucliean Domain, Euclidean Chains, Places, Cyclotomic Function Fields.

DESCRIPTION:

This work consists of studying some concepts and results of the theory of rings and fields. In the first chapter, classical concepts and results on groups, rings, fields and modules, necessary for the proper understanding on the discussion following in the next three chapters are taken up.

In the second chapter we introduce the concepts of the primitive roots of unity, cyclotomic polynomials and we prove results that allow us to compute a cyclotomic polynomial $\Phi_n(x)$ independent of the value of $n \in \mathbb{Z}^+$, and we show some examples where these results are used.

In the third chapter the definition of euclidean domain is taken up again and new concepts are introduced such as derived set, product subset, euclidean chain and some examples where these concepts are used to prove when a ring is a euclidean domain. The necessary and sufficient conditions for a ring to be a euclidean domain are presented, reaching an important result, based on inequalities to show when a domain is euclidean.

In the last chapter we present the algebraic functions field, places and valuations, with the objective of showing the construction of the cyclotomic functions field, we present some results shown in the previous chapter, via this new construction.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas, Matemáticas. Director: Arnoldo Rafael Teherán Herrera, Doctorado en Matemáticas.

Introducción

Las raíces griegas de la palabra *ciclotomía* significan “círculo” y “cortar”, es decir, cortar el círculo unitario en arcos iguales. En este sentido si $n \in \mathbb{Z}^+$ y ζ_k es una **raíz $n-$ésima de la unidad** en el cuerpo de los números complejos $\mathbb{C}$; es decir,

$$\zeta_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right),$$

con, $k \in \mathbb{Z}^+ \cup \{0\}$ y $k < n$, podemos interpretar geométricamente los ζ_k como los vértices del $n-$ágono regular inscrito en la circunferencia de radio uno y centro en el origen.

Si $mcd(k,n) = 1$, ζ_k es llamada una **raíz n-ésima primitiva** de la unidad, por lo tanto si denotamos por $T_n \subseteq \mathbb{C}$, el conjunto de todas estas raíces, entonces el polinomio

$$\Phi_n(x) = \prod_{\zeta_k \in T_n} (x - \zeta_k),$$

es conocido en la literatura como $n-$**ésimo polinomio ciclotómico** y además $\Phi_n(x) \in \mathbb{Z}[x]$ es un polinomio de grado $\varphi(n)$, donde como es usual $\mathbb{Z}$ denota el anillo de los enteros y φ la **función de Euler**.

Por ejemplo:

$$\begin{aligned}
\Phi_1(x) &= x-1,\\
\Phi_2(x) &= x+1,\\
\Phi_3(x) &= (x-j)\left(x-\overline{j}\right) = x^2+x+1, \text{ donde } j=\frac{-1+\sqrt{3}i}{2}\in\mathbb{C}\\
\Phi_4(x) &= (x-i)\left(x-\overline{i}\right) = x^2+1.
\end{aligned}$$

Se tiene que para $n>1$, $\Phi_n(x)$ es irreducible sobre $\mathbb{Z}$ y además,

$$\Phi_n(x) = \frac{x^n-1}{\prod\limits_{d\in D_n-\{n\}}\Phi_d}$$

donde D_n es el conjunto de todos los divisores no negativos de n.

Dado que cada raíz primitiva de la unidad ζ_k es entero sobre $\mathbb{Z}$, tenemos que $\mathbb{Z}[\zeta_k]\subseteq\mathbb{C}$ es un anillo que llamaremos $k-$**anillo ciclotómico**; en este caso es natural preguntarse:

- ¿Bajo que condiciones $\mathbb{Z}[\zeta_k]$ es un dominio euclídeo?.
- ¿Bajo que condiciones $\mathbb{Z}[\zeta_k]$ es euclídeo normado?.

De otro lado, si K es un cuerpo y $K(x)$ es el cuerpo de funciones racionales en la variable x, podemos hacer una construcción de un cuerpo de funciones ciclotómicas donde apropiadamente se pueden obtener resultados análogos a los polinomios ciclotómicos dados en el Capítulo 2, vía

esta construcción, también sobre propiedades del cuerpo de funciones racionales, entre otros.

1. Preliminares

En este capítulo se establecen algunos conceptos y resultados conocidos del álgebra, que son fundamentales en el desarrollo y comprensión de los capítulos posteriores. Varios de estos conceptos y resultados preliminares, así como algunos ejemplos aparecen en Apostol (1998),Gallian (2012),Grillet (2007),Lezama (2020) y Hungerford (2012).

1.1. Preliminares en teoría de números

Definición 1.1. Diremos que entero no nulo t es un **divisor** de s si hay un entero u tal que $s = tu$, en este caso escribiremos $t|s$ para denotar que t divide a s.

En caso contrario, diremos que t no divide a s y lo denotaremos por $t \nmid s$.

Teorema 1.2. ***El algoritmo de la división.*** *Sean $a, b \in \mathbb{Z}$, con $|b| > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que*

$$a = bq + r \text{ y } 0 \leq r < |b|. \tag{1}$$

Demostración. Ver en Capítulo *I* de Hungerford (2012). □

Teorema 1.3. ***El teorema fundamental de la aritmética.*** *Todo entero no nulo $n \neq \pm 1$, se puede factorizar como producto de primos y esta factorización es única salvo por el orden de los factores.*

Demostración. Ver en Capítulo *I* de Apostol (1998). □

Las funciones que tienen como dominio el conjunto de los enteros positivos con valores en $\mathbb{C}$ se denominan funciones aritméticas o funciones numéricas. A continuación dos de ellas.

Definición 1.4. Para cada entero positivo n la **función ϕ de Euler**, se define como el número de enteros positivos menores o iguales que n y primos relativos con n.

Definición 1.5. La **función de Möbius** μ donde $n \in \mathbb{Z}^+$, se define

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n = p_1 \dots p_r \text{ donde los } p_i \text{ son primos distintos,} \\ 0 & \text{Si } p^2 | n \text{ para algún primo } p. \end{cases}$$

La noción que nos dan estas funciones son el número de primos relativos que tiene un número n que sean menores que él y distinguir si en su factorización en primos hay un primo que se repite, respectivamente para cada función.

Las funciones ϕ de Euler y μ cumplen una propiedad muy importante que se usará frecuentemente, esta es la de ser funciones multiplicativas.

Definición 1.6. Una función aritmética se llama **multiplicativa** si satisface la condición:

- Si $f(mn) = f(m)f(n)$ para cada par de enteros positivos tales que $\text{mcd}(m,n) = 1$.
- Si $f(mn) = f(m)f(n)$ para todo m, n enteros positivos, entonces f se llama **completamente multiplicativa**.

Teorema 1.7. *Las funciones ϕ de Euler y μ de Möbius son multiplicativas.*

Además,

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & si\ n = 1, \\ 0 & En\ otro\ caso. \end{cases}$$

donde d son los divisores positivos de n.

Demostración. Ver en Capítulo *II* de Apostol (1998). □

Teorema 1.8. ***Formula de Inversión de Möbius.*** *Sea f y F funciones de $\mathbb{Z}^+$ en un anillo de D, tales que*

$$F(n) = \sum_{d|n} f(d), \tag{2}$$

si y solo si

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right). \tag{3}$$

Demostración. Ver en el Apéndice *B* de Chadid and Caicedo (1987). □

1.2. Algunos resultados sobre grupos, anillos, cuerpos y módulos

Definición 1.9. Sea G un conjunto no vacío y $\cdot$ una operación binaria definida en G. Se dice que $(G,\cdot)$ es un **grupo** si cumple las siguientes propiedades:

1. Propiedad clausurativa, si $a, b \in G$, entonces $a \cdot b \in G$, donde se denotará por ab para simplificar la notación.

2. Propiedad asociativa, esto es $(ab)c = a(bc)$ para todo $a, b, c \in G$.

3. Existencia de elemento neutro, hay un elemento $e \in G$ tal que $ae = ea = a$ para todo $a \in G$.

4. Existencia de elemento inverso, para cada elemento a en G, existe un elemento b en G tal que $ab = ba = e$, este elemento lo denotaremos por a^{-1}.

Se dice que un grupo es **abeliano** si ademas satisface la propiedad conmutativa, es decir:

5 Si $ab = ba$ para todo a, b en G.

Observación 1.10. Diremos que un grupo es finito o de orden finito si tiene un número finito de elementos. En este caso, el número de elementos de G es llamado el orden de G y es denotado por $|G|$. Un grupo con infinitos elementos se dice que tiene orden infinito.
Sea elemento a en un grupo G, decimos que a tiene orden finito si $a^k = e$ para algún entero positivo k. En este caso el orden de a será el menor entero positivo n tal que $a^n = e$. Un elemento se dice que tiene orden infinito si $a^k \neq e$ para todo entero positivo k.

Definición 1.11. Un grupo $(G, \cdot)$ es llamado **cíclico** si existe un elemento a en G tal que $G = \{a^n : n \in \mathbb{Z}\}$. Este elemento a es llamado el generador de G y denotaremos por $G = \langle a \rangle$.

Proposición 1.12. *Un **grupo cíclico** $(G, \cdot)$ cumple las siguientes propiedades:*

1. *$(G, \cdot)$ es abeliano.*

2. *Sea G un grupo cíclico, entonces si $x \in G$ y $x \neq e$, se tiene que $x = a^r$, con $r \in \mathbb{Z}^+$ y $G = (x)$ si y solo si* $\text{mcd}(n, r) = 1$.

3. *$\mathbb{Z}$ y $\mathbb{Z}_n$ son cíclicos y todo grupo cíclico es isomorfo a $\mathbb{Z}$ o $\mathbb{Z}_n$.*

Demostración. Ver en Capítulo I de Grillet (2007). □

Definición 1.13. Un **anillo** $(R,+,\cdot)$ es una tripla donde R conjunto no vacío con dos operaciones binarias, adición denotada por "$+$" y multiplicación denotada por " $\cdot$ ", tal que:

1. $(R,+)$ es un grupo abeliano.

2. $a(bc) = (ab)c$ para todo $a,b,c \in R$.

3. $a(b+c) = ab+ac$ y $(b+c)a = ba+ca$ para todo $a,b,c \in R$.

Veamos rápidamente unas definiciones.

Adicionalmente, sea $(R,+,\cdot)$ un anillo.

1. Diremos que $(R,+,\cdot)$ es un **anillo conmutativo**, si para todo $a,b \in R$, $ab = ba$.

2. Si existe un elemento no nulo en el anillo, denotado por 1, tal que $1a = a1 = a$ para todo $a \in R$, diremos que $(R,+,\cdot)$ es un anillo con 1

3. Un subconjunto $S \subseteq R$, diremos que $(S,+,\cdot)$ es **subanillo** de $(R,+,\cdot)$, si S es un anillo.

4. Un **cuerpo** es un anillo conmutativo con 1, tal que el conjunto de las unidades de R definido por:

$$U(R) = \{a \in R - \{0\} : \exists b \in R - \{0\}, ab = 1\}$$

es exactamente $R - \{0\}$.

Para simplificar la notación, denotaremos por R al anillo $(R,+,\cdot)$.

Definición 1.14. Sea R un anillo conmutativo, que a su vez es un domino entero. Definimos el cuerpo de fracciones de R como:

1. Producto cartesiano $R \times R - \{0\}$, compuesto por todos los pares ordenados (a,b), donde $a,b \in R$ y $b \neq 0$.

2. Definimos la relación $\mathscr{R}$ dada por

$$(a,b)\mathscr{R}(c,d) \Leftrightarrow ad = bc.$$

   Esta relación $\mathscr{R}$ es una relación de equivalencia.

Para simplificar la notación la pareja (a,b) será denotada por $\frac{a}{b}$.

Definición 1.15. Un **ideal** de un anillo R es un subgrupo I de $(R,+)$ tal que si $x \in I$, implica que $xy \in I$ y $yx \in I$ para todo y en R.

Claramente R y $\{0\}$ son ideales de R y se llaman **ideales triviales**.

Definición 1.16. Sea I un ideal de un anillo R. Decimos que dos elementos $a,b \in R$ son congruentes módulo I, y escribimos $a \equiv b \,(\text{mód } I)$ si $a - b \in I$.

Tenemos que la relación de congruencia módulo I es una relación de equivalencia en R lo que nos permite asociar a cada elemento $a \in R$ una clase de equivalencia que llamaremos **clase de**

congruencia módulo I dada por:

$$\begin{aligned}[a] &= \{b \in R : b \equiv a \,(\text{mód } I)\} \\ &= \{b \in R : b - a = i, \text{ con } i \in I\} \\ &= \{b \in R : b = a + i, \text{ con } i \in I\} \\ &= \{a + i : i \in I\} := a + I.\end{aligned}$$

Teorema 1.17. *Sea I un ideal en un anillo R, entonces el conjunto de todas las clases de congruencia módulo I, denotado por:*

$$R/I = \{a + I : a \in R\},$$

es un anillo con las operaciones adición y multiplicación que se definen de la siguiente manera: Dados $a \in I$ y $b \in I$ en R/I, entonces:

$$(a+I)+(b+I) := (a+b)+I \text{ y } (a+I)(b+I) := ab+I,$$

respectivamente.

Demostración. Ver Capítulo I de Grillet (2007). □

Definición 1.18. Sea R un anillo conmutativo con 1.

1. Un ideal P de R es llamado **ideal primo** si $P \neq R$ y para todo $a, b \in R$ tal que $ab \in P$, entonces $a \in P$ o $b \in P$.

2. Un ideal M de R es llamado **maximal** si $M \neq R$ y si I es un ideal tal que $M \subseteq I \subseteq R$, entonces $I = M$ o $I = R$.

Definición 1.19. Sea R un anillo, diremos que es un **anillo local** si tiene un único ideal maximal.

Existen anillos que tienen un único ideal maximal, por ejemplo los cuerpos, donde sus únicos ideales son $\{0\}$ y el mismo.

Proposición 1.20. *Un anillo R es local si y solo si $R - U(R)$ es un ideal de R, donde*

$$U(R) = \{r \in R : \text{ existe } s \in R \text{ tal que } rs = 1\},$$

en tal caso $R - U(R)$ es ideal maximal de R.

Demostración. Ver en Capitulo VII de Grillet (2007). □

Definición 1.21. Un anillo R es un **dominio entero**, si R es conmutativo y no tiene divisores de cero, es decir si $a, b \in R$ son tales que $ab = 0$, entonces $a = 0$ o $b = 0$, es decir, R no tiene divisores de cero no nulos.

Definición 1.22. Un dominio entero R es llamado un **dominio de ideales principales** (DIP) si cada ideal de R es principal, es decir, sea $a \in R$, el ideal generado por a denotado por $(a) = \{ab : b \in R\}$ es llamado **ideal principal**.

Sea X subconjunto de R, el ideal generado por el subconjunto X se denota por (X) y está definido por

$$(X) = \{c_1a_1 + \cdots + c_na_n : c_i \in R \text{ y } a_i \in X, \text{ para todo } i = 1, \ldots, n\}.$$

Para anillos conmutativos con identidad se tiene la siguiente caracterización de los ideales primos y maximales.

Teorema 1.23. *Sea R un anillo conmutativo con* 1 *y sea I subconjunto de R, entonces:*

1. *I es un ideal primo de R si, y solo si el anillo cociente R/I es un dominio entero.*

2. *I es un ideal maximal de R si, y solo si el anillo cociente R/I es un cuerpo.*

Demostración. Ver en Capítulo 0 de Roman (2005). □

En particular todo ideal maximal de *R* es ideal primo de *R*.

Definición 1.24. La **característica** de un anillo, es el menor entero positivo *n* tal que $nx = 0$ para todo *x* en el anillo. Si *n* no existe, diremos que el anillo tiene característica 0.

Teorema 1.25. *Todo cuerpo tiene característica p o* 0*, donde p es primo.*

Demostración. Ver en Capítulo *IX* de Roman (2005). □

Proposición 1.26. *Cada subgrupo finito multiplicativo de un cuerpo es cíclico.*

Demostración. Ver en Capitulo 0 de Roman (2005). □

Se dice que un cuerpo es finito si sólo posee un número finito de elementos. Si F es un cuerpo con q elementos, entonces existe $p, n \in \mathbb{Z}^+$ tal que $q = p^n$, todos los cuerpos finitos del mismo orden son isomorfos entre sí (ver Capitulo *IX* de Roman (2005)). En tal caso denotamos al único cuerpo finito con q elementos por $\mathbb{F}_q$ o $GF(q)$.

Definición 1.27. Una extensión de un cuerpo K, es un cuerpo E del cual K es subcuerpo $K \subseteq E$.

Definición 1.28. El grado $[E : K]$ de una extensión de cuerpo $K \subseteq E$ es su dimensión como espacio vectorial sobre K. Una extensión de cuerpo $K \subseteq E$ es finita, cuando esta tiene grado finito y es infinita en caso contrario.

Proposición 1.29. *Si* $K \subseteq E \subseteq F$, *entonces* $[F : K] = [F : E]\,[E : K]$.

Demostración. Ver en Capítulo V de Grillet (2007). □

Definición 1.30. Dado un cuerpo K y una extensión $L \supseteq K$, diremos que $\alpha \in L$ es **algebraico** sobre K si existe un polinomio $p(x) \in K[x]$ no nulo, tal que $p(\alpha) = 0$.
En caso contrario se dice que α es **trascendente**.

Definición 1.31. Sea K un cuerpo y $f \in K[x]$ un polinomio no constante, f es **separable** cuando no tiene raíces múltiples en $\overline{K}$.

Definición 1.32. Un elemento α es **separable** sobre K cuando α es algebraico sobre K y el polinomio irreducible de α en K es separable. Una extensión algebraica E de K es separable y E es separable sobre K, cuando cada elemento de E es separable sobre K.
Un **cuerpo numérico algebraico** es una extensión K de $\mathbb{Q}$ tal que la extensión $K/\mathbb{Q}$ tiene grado finito.

Definición 1.33. Un polinomio $f \in K[x]$ se descompone en una extensión de cuerpo E de K, cuando tiene una una factorización $f(x) = a(x-a_1)(a_2)\cdots(x-a_n)$ en $E[x]$.

En la definición anterior, $a \in K$ es el coeficiente principal de f, n el grado de f y $a_1, a_2, \cdots, a_n \in E$ son las raíces (no necesariamente distintas) de f en E.

Definición 1.34. Sea K un cuerpo. Un **cuerpo de descomposición** sobre K de un polinomio $f \in K[x]$ es una extensión E de K tal que f se descompone en E y E es generado sobre K por las raíces de f. Un cuerpo de descomposición sobre K de un conjunto $S \subseteq K[x]$ de polinomios, es una extensión de cuerpo E de K tal que cada $f \in S$ se descompone en E y E es generado sobre K por las raíces de todos los $f \in S$.

Proposición 1.35. *Para una extensión algebraica $K \subseteq E \subseteq \overline{K}$, las siguientes condiciones son equivalentes:*

1. *E es el cuerpo de descomposición sobre K de un conjunto de polinomios.*
2. *$\phi(E) = E$ para cada K - homomorfismo $\phi : E \to \overline{K}$.*
3. *$\phi(E) \subseteq E$ para cada K - homomorfismo $\phi : E \to \overline{K}$.*
4. *$\sigma(E) = E$ para cada K- automorfismo σ de $\overline{K}$.*
5. *$\sigma(E) \subseteq E$ para cada K- automorfismo σ de $\overline{K}$.*
6. *Cada polinomio irreducible $q \in K[x]$ con una raíz en E, se descompone en E.*

Demostración. Ver Capitulo V de Grillet (2007). □

Definición 1.36. Una extensión **normal** de cuerpo K es una extensión algebraica de K tal que satisface las condiciones dadas en la Proposición (1.35) para alguna clausura algebraica de K.

Definición 1.37. Una extensión de **Galois** de un cuerpo K es una extensión normal y separable E de K, diremos que E es Galois sobre K.

Definición 1.38. Sea $(M,+)$ un grupo abeliano y $(A,+,\cdot)$ un anillo. Se dice que M tiene una estructura de $A-$**módulo** a la derecha sobre el anillo A, si se ha definido un producto entre elementos de M y A, es decir, una función

$$\begin{aligned} M \times A &\rightarrow M \\ (m,a) &\mapsto m \cdot a \end{aligned}$$

para el cual se cumplen las siguientes condiciones:

1. $(m_1+m_2)a = m_1a + m_2a$.
2. $m(a_1+a_2) = ma_1 + ma_2$.
3. $m(a_1a_2) = (ma_1)a_2$.
4. $m \cdot 1 = m$.

Con $m, m_1, m_2 \in M$ y $a, a_1, a_2 \in A$.

Definición 1.39. Sea M un $A-$módulo y N un subconjunto no vacío de M. Se dice que N es un $A-$**submódulo** de M, si N es un subgrupo de $(M,+)$ y además

$$na \in N \text{ para cada } n \in N \text{ y cada } a \in A.$$

1.3. El cuerpo de los números complejos

Sea $\mathbb{R}[x]$ el anillo de los polinomios en la variable x y coeficientes reales. Dado que $\mathbb{R}$ es un cuerpo, entonces $\mathbb{R}[x]$ es un dominio de ideales principales (DIP), consideremos $p(x) = x^2+1 \in \mathbb{R}[x]$, claramente $p(x)$ no tiene raíces en $\mathbb{R}$ y por lo tanto es irreducible sobre $\mathbb{R}$, entonces $M = (p(x))$ el ideal de $\mathbb{R}[x]$ generado por $p(x)$ es un ideal maximal de $\mathbb{R}[x]$ y así $F = \mathbb{R}[x]/M$ es un cuerpo.

Note que si $f(x)+M = \overline{f(x)}$, entonces $\overline{x^2+1} = \overline{0}$, $M = \overline{0}$ es el cero de F y en consecuencia $\overline{x^2} = \overline{-1} = -\overline{1}$, note también que cada elemento de F es de la forma $a+bx+M := \overline{a}+\overline{b}\overline{x}$, donde $a,b \in \mathbb{R}$, dado que $\mathbb{R} \subseteq F$, naturalmente

$$\begin{aligned} \varphi &: \mathbb{R} \to F \\ & t \mapsto \overline{t} \end{aligned}$$

es un homomorfismo inyectivo, entonces $\mathbb{R} \cong \mathrm{Im}\varphi$ es un subcuerpo de F.

Si denotamos por $\overline{t} := t$, $t \in \mathbb{R}$ y $\overline{x} = i$, entonces cada elemento de F se puede escribir en la forma $a+bi$, $a,b \in \mathbb{R}$ es decir,

$$\begin{aligned} F &= \{a+bi : a,b \in \mathbb{R}\}, \\ &:= \mathbb{C}, \end{aligned}$$

el cuerpo de los números complejos.

De esta forma es como usualmente tenemos en $\mathbb{C}$ definidas las operaciones suma, multiplicación, norma o módulo de un número complejo.

$$(a+ib)+(c+id)=(a+c)+i\,(b+d)\,,$$

$$(a+ib)\,(c+id)=(ac-bd)+i\,(ad+bc)\,,$$

$$|a+bi|=\sqrt{a^2+b^2}.$$

Cada $z\in\mathbb{C}-\{0\}$ se puede escribir de forma trigonométrica y también tenemos otra representación llamada polar, estas son:

Existe $\theta\in\mathbb{R}$ con $-\pi<\theta\leq\pi$ tal que:

$$z=|z|\,(\cos\theta+i\,\mathrm{sen}\,\theta)\,, \tag{4}$$

en tal caso si denotamos $r=|z|$ y $e^{i\theta}=(\cos\theta+i\,\mathrm{sen}\,\theta)$, entonces

$$z=re^{i\theta}, \tag{5}$$

donde a las ecuaciones (4) y (5) las llamaremos la forma trigonométrica y polar de z respectivamente, θ es llamado el argumento principal de z y se denotará por $\theta=\mathrm{Arg}(z)$.

Teorema 1.40 (Teorema de Moivre). *Si $\theta \in \mathbb{R}$, entonces para cada $n \in \mathbb{Z}^+$ se cumple que:*

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta).$$

Lo cuál se puede probar usando el principio de inducción matemática sobre n.

Con este resultado vamos a describir las raíces $n-$ésimas de un número complejo w.

Definición 1.41. Sea $w \in \mathbb{C} - \{0\}$ y $n \in \mathbb{Z}^+$, decimos que un número complejo z es una raíz $n-$ésima de w si

$$z^n = w.$$

Proposición 1.42. *Si $z = |z|(\cos\theta + i\,\mathrm{sen}\,\theta)$ es una raíz $n-$ésima de w, entonces $|z| = |w|^{\frac{1}{n}}$ y $\theta = \frac{1}{n}(\phi + 2k\pi)$ con $k \in \mathbb{Z}$.*

Además solo se tienen n valores diferentes, es decir, w tiene n raíces $n-$ésimas diferentes dadas por:

$$z_k = |w|^{\frac{1}{n}}\left(\cos\left(\frac{\phi + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\phi + 2k\pi}{n}\right)\right),$$

con $k = 1, \ldots, n$.

Demostración. Supongamos que $w = |w|(\cos\phi + i\,\mathrm{sen}\,\phi)$, supongamos que $z = |z|(\cos\theta + i\,\mathrm{sen}\,\theta)$ es una solución de $z^n = w$, reescribiendo su forma polar

$$(|z|(\cos\theta + i\,\mathrm{sen}\,\theta))^n = |w|(\cos\phi + i\,\mathrm{sen}\,\phi),$$

es decir

$$|z|^n(\cos n\theta + i\,\mathrm{sen}\, n\theta) = |w|(\cos\phi + i\,\mathrm{sen}\,\phi),$$

entonces $|z|^n = |w|$, $\cos n\theta = \cos\phi$ y $\mathrm{sen}\, n\theta = \mathrm{sen}\,\phi$, de donde se obtiene que $|w|^{\frac{1}{n}} = |z|$ y que $\theta = \frac{\phi+2\pi k}{n}$ con $k = 1,\ldots,n$. □

Observación 1.43. En caso que $w = 1$, los números complejos z tales que $z^n = 1$ son llamados raíces $n-$ésimas de la unidad, como por ejemplo $1 = \cos 0 + i\,\mathrm{sen}\, 0$. Estas raíces $n-$ésimas que en adelante las denotaremos por ζ_k, son de la forma:

$$\zeta_k = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right) = e^{\frac{2\pi ik}{n}}.$$

Proposición 1.44. *Sea $V_n = \{\zeta_k : k = 1,\ldots,n\}$, entonces V_n es un subgrupo de $\mathbb{C} - \{0\}$ cíclico de orden n.*

Demostración. Primero veamos que V_n es un subgrupo multiplicativo de $\mathbb{C}\backslash\{0\}$, sean $\zeta_j, \zeta_i \in V_n$, veamos que $\zeta_j\zeta_k \in V_n$.

$$\begin{aligned}\zeta_j\zeta_k &= e^{\frac{2i\pi j}{n}} e^{\frac{2i\pi k}{n}},\\ &= e^{\frac{2i\pi(j+n)}{n}},\end{aligned}$$

si $k + j < n$ entonces ya hemos acabado, en caso contrario tendremos que existe $l \in \mathbb{N}$ tal que $e^{\frac{2i\pi(j+k)}{n}} = e^{\frac{2i\pi(n+l)}{n}}$ con $l < n$ y $e^{\frac{2i\pi(n+l)}{n}} = e^{\frac{2i\pi n}{n}} e^{\frac{2i\pi l}{n}} = e^{\frac{2i\pi l}{n}}$.

Note que si $j+k=mn$ con $m \in \mathbb{Z}$, entonces

$$\zeta_j \zeta_k = e^{\frac{2i\pi(j+k)}{n}} = e^{\frac{2i\pi mn}{n}} = e^{2i\pi m} = 1.$$

es decir, todo elemento $\zeta_j \in V_n$ tiene un elemento inverso ζ_k, este debe cumplir que $k+j$ sea un múltiplo de n.

Además de ver que es un subgrupo, vemos que es cíclico (ver 1.26), donde tendremos que $V_n = (\zeta_1) = (e^{\frac{2i\pi}{n}})$. □

2. Polinomios ciclotómicos

En este capitulo introducimos la definición de polinomio ciclotómico y presentamos definiciones, propiedades y ejemplos. Usaremos como referencia las notas de Brett Potter en Porter (2015), pero también son resultados que se pueden encontrar en Apostol (1970),Jameson (2010), y Chadid and Caicedo (1987). Uno de los objetivos en este capitulo, es calcular el polinomio ciclotómico $\Phi_n(x)$ para cualquier $n \in \mathbb{Z}^+$ y el dar una descripción de como son las raíces primitivas de la unidad.

2.1. Raíz primitiva de la unidad

Definición 2.1. Decimos que $\zeta_k \in V_n$ es una **raíz primitiva n-ésima de la unidad** si ζ_k tiene orden n, es decir, ζ_k es un generador del grupo V_n.

En adelante denotaremos este conjunto por:

$$T_n = \{\zeta_k \in V_n : (\zeta_k) = V_n\}.$$

Teorema 2.2. *$\zeta_k \in T_n$ si y solamente si* $\operatorname{mcd}(n,k) = 1$.

Demostración. Por (1.12) tenemos que V_n y $\mathbb{Z}_n$ son isomorfos y

$$v: \quad V_n \to \mathbb{Z}_n,$$

$$\zeta_k \mapsto k,$$

es un isomorfismo de grupos definido por $v(\zeta_k) = k$.

Veamos que está bien definido, sean $\zeta_k \in V_n$, entonces $v(\zeta_k) = k \in \mathbb{Z}_n$, y sean $\zeta_k, \zeta_m \in V_n$ tal que $\zeta_k = \zeta_m$, entonces $v(\zeta_k) = k$ y $v(\zeta_m) = m$, entonces $k = m$. Dado que k es un generador de $\mathbb{Z}_n$ si y solo si k tiene orden primo relativo con n, entonces los ζ_k generan a V_n si y solo si $\operatorname{mcd}(k,n) = 1$. □

Observación 2.3. Sea $\zeta \in V_n$, es una raíz $n-$ésima primitiva de la unidad si $\zeta^n = 1$ y $\zeta^k \neq 1$, para todo $k \in \mathbb{Z}^+$ y $k < n$.

De la sección anterior, tenemos que las raíces de $x^n - 1$, son las raíces de 1 en $\mathbb{C}$, es decir, $\zeta_k = e^{\frac{2i\pi k}{n}} \in V_n$ con $1 \leq k \leq n$, entonces

$$x^n - 1 = \prod_{k=1}^{n} (x - \zeta_k). \tag{6}$$

Definición 2.4. Definimos los **polinomios ciclotómicos** Φ_n con $n \geq 1$ como:

$$\Phi_n(x) = \prod_{\zeta_k \in T_n} (x - \zeta_k), \tag{7}$$

claramente Φ_n es un polinomio mónico y tiene grado $\phi(n)$.

Ejemplo 2.5. A continuación se muestran T_n, V_n y $\Phi_n(x)$ para $n = 1,2,3,4$ y 5.

n	V_n	T_n	$\Phi_n(x)$
1	$\{1\}$	$\{1\}$	$x-1$
2	$\{-1\}$	$\{-1\}$	$x+1$
3	$\left\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\right\}$	$\left\{e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\right\}$	x^2+x+1
4	$\{1, i, -1, -i\}$	$\{i, -i\}$	x^2+1
5	$\left\{1, e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\right\}$	$\left\{e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\right\}$	$x^4+x^3+x^2+x+1$

2.2. Algunos resultados sobre $\Phi_n(x)$

El objetivo principal es calcular explícitamente $\Phi_n(x)$ para cualquier $n \in \mathbb{Z}^+$.

Teorema 2.6. *Sea $p \in \mathbb{Z}^+$ primo, entonces*

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

Demostración. Considere la factorización de $x^p - 1$ dada en la ecuación (6) con $n = p$.

$$x^p - 1 = \prod_{\zeta_k \in T_p} (x - \zeta_k).$$

Pero como p es primo, entonces $T_p = \{\zeta_1, \ldots, \zeta_{p-1}\}$, así para obtener $\Phi_p(x)$ basta remover el factor correspondiente a $k = p$, es decir, $x - \zeta_p = x - 1$. □

Ejemplo 2.7. Calculemos $\Phi_n(x)$ para $n = 3, 5$ y 7.

Como todos los valores son primos, entonces usando el resultado anterior tendríamos que:

1. $\Phi_3(x) = x^2 + x + 1$,
2. $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$,
3. $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Veamos el siguiente lema, el cual será útil para demostrar un resultado importante de los polinomios ciclotómicos.

Lema 2.8. *Sea $n, n_1, d \in \mathbb{Z}^+$, donde $n = n_1 d$, entonces*

$$\Phi_d(x) = \prod_{\text{mcd}(n,k)=n_1} (x - \zeta_k), \tag{8}$$

donde $1 \leq k \leq n$.

Demostración. Por definición el $d-$ésimo polinomio ciclotómico está dado por

$$\Phi_d(x) = \prod_{\zeta_r \in T_d} (x - \zeta_r).$$

Ahora $\frac{r}{d} = \frac{n_1 r}{n}$ y $\text{mcd}(r, d) = 1$ si y solo si $\text{mcd}(n_1 r, n) = n_1$. Así $r \leq d$ si y solo si $n_1 r \leq n_1 d = n$.

Escribiendo $k = n_1 r$ se tiene que

$$\Phi_d(x) = \prod_{\text{mcd}(n,k)=n_1} (x - \zeta_k),$$

donde $1 \leq k \leq n$. □

También se tiene el siguiente resultado, que usaremos posteriormente.

Teorema 2.9. *Si $n \in \mathbb{Z}^+$, entonces*

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{9}$$

Demostración. Sea $\zeta_i \in V_n$ una raíz $n-$ésima de la unidad. Si

$$S_{\zeta_i} = \{k \in \mathbb{Z}^+ : 1 \leq k \leq n \text{ y } \zeta_i^k = 1\}.$$

Entonces $S_{\zeta_i} \neq \emptyset$ porque $n \in S_{\zeta_i}$, por el principio del buen orden, existe $d \in S_{\zeta_i}$, tal que $d = \text{mín}\{k \in S_{\zeta_i}\}$, en consecuencia $\zeta_i^k \neq 1$ si $k \in \mathbb{Z}^+$ y $k < d$; recordando la Observación (2.3), nos permite concluir que ζ_i es una raíz $d-$ésima primitiva de la unidad.

Veamos que $d|n$. Por el algoritmo de la división, existen q, r tales que

$$n = qd + r \text{ con } 0 \leq r < d,$$

luego

$$1 = \zeta^n = \zeta^{qd+r} = \left(\zeta^d\right)^s \zeta^r = \zeta^r,$$

Como $0 \leq r < d$ la condición $0 < r$ es imposible por la minimalidad de d, luego $n = qd$ y por lo tanto

$$V_n \subseteq \bigcup_{d|n} T_d.$$

Recíprocamente, si $\alpha \in \bigcup_{d|n} T_d$, entonces $d|n$ tal que $\alpha \in T_d$ y por lo tanto $\alpha^d = 1$.

Como $d|n$, existe $b \in \mathbb{N}$ tal que $bd = n$, en consecuencia $\alpha^n = \left(\alpha^d\right)^b = 1$.

Así α es una raíz $n-$ésima de la unidad y por lo tanto $\alpha \in V_n$. De lo anterior se infiere que

$$\bigcup_{d|n} T_d \subseteq V_n.$$

Así

$$\bigcup_{d|n} T_d = V_n.$$

Ahora,

$$x^n - 1 = \prod_{\zeta \in V_n} (x - \zeta),$$

entonces

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \left(\prod_{\zeta \in T_s} (x - \zeta) \right) \\ &= \prod_{d|n} \Phi_d(x), \end{aligned}$$

que es lo que queríamos ver. □

Teorema 2.10. *Para todo $n \in \mathbb{Z}^+$, $\Phi_n(x)$ tiene coeficientes enteros.*

Demostración. Usando inducción matemática sobre n, claramente $\Phi_1(x) = x - 1$ (ver tabla 2.5).

Sea $r \in \mathbb{Z}^+$ tal que $\Phi_r(x)$ tenga coeficientes enteros para todo $r < n$.

Por la ecuación (9) se tiene que $x^n - 1 = \Phi_n(x) g_n(x)$, donde

$$g_n(x) = \prod_{d|n,\, 1<d<n} \Phi_d(x).$$

Escriba $\Phi_n(x) = \sum_{r=0}^{m} c_r x^r$, donde $m = \phi(n)$ y $g_n(x) = \sum_{s=0}^{n-m} a_s x^s$. Por la hipótesis de inducción, cada a_s es un entero. Además, $a_0 = g_n(0) = -1$. Si existe un c_r que no es un entero, sea c_k el primero que no lo es.

Entonces el coeficiente de x^k en el producto $\Phi_n(x) g_n(x)$ es

$$c_0 a_k + c_1 a_{k-1} + \cdots + c_{k-1} a_1 - c_k,$$

y no es un entero, pero este producto es $x^n - 1$, lo que es una contradicción, por lo tanto $\Phi_n(x)$

tiene coeficientes enteros para $n \in \mathbb{Z}^+$. □

Teorema 2.11. *Si $n > 1$ es impar, entonces*

$$\Phi_{2n}(x) = \Phi_n(-x).$$

Demostración. Argumentando por inducción matemática sobre $m \in \mathbb{N}$, donde $n = 2m+1$.

Si $m = 1$, $n = 3$, entonces por lema (2.8), se tiene que $x^6 - 1 = \prod_{d|6} \Phi_d(x)$, entonces

$$\begin{aligned} \Phi_6(x) &= \frac{x^6-1}{\Phi_1(x)\Phi_1(2)\Phi_3(x)}, \\ &= \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)}, \\ &= x^2 - x + 1 = \Phi_3(-x). \end{aligned}$$

Sea $m > 1$ es decir $n > 3$, supongamos que para todo k impar con $3 \leq k < n$ se cumple que $\Phi_{2k}(x) = \Phi_k(-x)$, como los divisores de $2n$ son $d, 2d \in \mathbb{Z}^+$ donde $d|n$, entonces podemos factorizar de las siguiente manera

$$x^{2n} - 1 = \prod_{d|2n} \Phi_d(x) = \prod_{k|n} \Phi_k(x) \prod_{k|n} \Phi_{2k}(x),$$

entonces

$$\begin{aligned} x^{2n}-1 &= (x^n-1)\left(\prod_{k|n,\,1<k<n}\Phi_{2k}(x)\right)\Phi_2(x)\Phi_{2n}(x), \\ &= (x^n-1)\left(\prod_{k|n,\,1<k<n}\Phi_k(-x)\right)\Phi_2(x)\Phi_{2n}(x), \\ &= (x^n-1)\left(\prod_{k|n}\Phi_k(-x)\right)\frac{\Phi_2(x)\Phi_{2n}(x)}{\Phi_1(-x)\Phi_n(-x)}, \\ &= (x^n-1)\left((-x)^n-1\right)\frac{(x+1)\Phi_{2n}(x)}{(-x-1)\Phi_n(-x)}. \end{aligned}$$

Cancelando términos tenemos que

$$\Phi_n(-x)=\Phi_{2n}(x).$$

□

Ejemplo 2.12. Calculemos $\Phi_n(x)$ para $n=6,10$ y 14.

Los encontraremos usando el resultado anterior de la siguiente manera.

1. Para $n=6$. Es $\Phi_6(x)=\Phi_3(-x)=x^2-x+1$.

2. Para $n=10$. Es $\Phi_{10}(x)=\Phi_5(-x)=x^4-x^3+x^2-x+1$.

3. Para $n=14$. Es $\Phi_{14}(x)=\Phi_7(-x)=x^6-x^5+x^4-x^3+x^2-x^1+1$.

Teorema 2.13. *Para $n\in\mathbb{Z}^+$ se tiene que:*

$$\Phi_n(x)=\prod_{d|n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}=\prod_{d|n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)},$$

donde μ es la función de Möbius definida en (1.5).

Demostración.

1. Sea $n = 1$. Entonces $\Phi_1(x) = x - 1 = \left(x^1 - 1\right)^{\mu\left(\frac{1}{1}\right)} \left(x^{\frac{1}{1}} - 1\right)^{\mu(1)}$, cumple las condiciones del dadas en el teorema para $n = 1$.

2. Supongamos $n > 1$ y $x > 0$

   a) Si $x > 1$, entonces $\Phi_d(x) > 0$ y $x^d - 1 > 0$, para todo $d \in \mathbb{Z}^+$, como

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

   entonces

   $$\ln\left(x^n - 1\right) = \sum_{d|n} \ln \Phi_d(x).$$

   Aplicando la formula de **inversión de Möbius** definida en (1.8), tenemos que

   $$\ln \Phi_n(x) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \ln\left(x^d - 1\right),$$

   por lo tanto

   $$\ln \Phi_n(x) = \ln \prod_{d|n} \left(x^d - 1\right)^{\mu\left(\frac{n}{d}\right)},$$

como $\ln(x)$ es una función inyectiva se obtiene

$$\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu\left(\frac{n}{d}\right)}.$$

b) Si $0 < x < 1$, entonces $1 - x^d > 0$, como $-\Phi_1(x) > 0$ y $\Phi_d(x) > 0$, para todo $d > 1$.

Definamos,

$$P_d(x) = \begin{cases} -\Phi_1(x) & \text{si } d = 1, \\ \\ \Phi_d(x) & \text{si } d > 1. \end{cases}$$

Entonces

$$1 - x^d = \prod_{d|n} P_d(x),$$

luego

$$\ln\left(1 - x^n\right) = \sum_{d|n} \ln P_d(x),$$

aplicando nuevamente la formula de **inversión de Möbius** se tiene que

$$\ln P_n(x) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \ln\left(1 - x^d\right),$$

entonces

$$\ln P_n(x) = \ln \prod_{d|n} \left(1 - x^d\right)^{\mu\left(\frac{n}{d}\right)},$$

así se tiene que

$$\Phi_n(x) = \prod_{d|n}(1-x^d)^{\mu\left(\frac{n}{d}\right)}.$$

Pero como $n > 1$, entonces

$$\begin{aligned}
\Phi_n(x) &= \prod_{d|n}(1-x^d)^{\mu\left(\frac{n}{d}\right)}, \\
&= \prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}(-1)^{\mu\left(\frac{n}{d}\right)}, \\
&= \prod_{d|n}(-1)^{\mu\left(\frac{n}{d}\right)}\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}, \\
&= (-1)^{\sum_{d|n}\mu\left(\frac{n}{d}\right)}\prod_{d|n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)}, \\
&= \prod_{d|n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)}.
\end{aligned}$$

Si $d|n$, entonces existe un $b \in \mathbb{Z}^+$ tal que $db = n$, si d recorre todos los divisores de n, entonces b también lo hará, así

$$\prod_{d|n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{b|n}\left(x^{\frac{n}{b}}-1\right)^{\mu(b)},$$

y como $b|n$, entonces

$$\prod_{d|n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}.$$

con lo cual se tiene la conclusión. □

Ejemplo 2.14. Calculemos $\Phi_6(x)$ usando el resultado anterior.

Tenemos que

$$\begin{aligned}
\Phi_6(x) &= \prod_{d|6}\left(x^{\frac{6}{d}}-1\right)^{\mu(d)}, \\
&= (x-1)(x^2-1)^{-1}(x^3-1)^{-1}(x^6-1), \\
&= \frac{(x^6-1)}{(x^3-1)(x+1)}, \\
&= \frac{x^3+1}{x+1}, \\
&= x^2-x+1.
\end{aligned}$$

Teorema 2.15. *Si p es primo, entonces*

$$\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right),$$

y por lo tanto

$$\Phi_{p^k}(x) = \sum_{i=1}^{p} x^{ip^{k-1}-p^{k-1}}.$$

Demostración. Por el teorema (2.9) tenemos que

$$x^{p^k}-1 = \prod_{d|p^k}\Phi_d(x) = \left(\prod_{d|p^{k-1}}\Phi_d(x)\right)\Phi_{p^k}(x) = \left(x^{p^{k-1}}-1\right)\Phi_{p^k}(x).$$

Luego

$$\Phi_{p^k}(x) = \frac{\left(x^{p^{k-1}}\right)^p-1}{x^{p^{k-1}}-1} = \Phi_p\left(x^{p^{k-1}}\right).$$

Ahora sea $y = x^{p^{k-1}}$, entonces $\Phi_p(y) = \sum_{i=1}^{p} y^{i-1}$, reemplazando a y, tenemos que

$$\begin{aligned}\Phi_p\left(x^{p^{k-1}}\right) &= \sum_{i=1}^{p}\left(x^{p^{k-1}}\right)^{i-1},\\ &= \sum_{i=1}^{p}\left(x^{p^{k-1}(i-1)}\right),\\ &= \sum_{i=1}^{p}\left(x^{ip^{k-1}-1p^{k-1}}\right).\end{aligned}$$

□

Ejemplo 2.16. Usando el resultado anterior, podemos calcular $\Phi_{81}(x)$.

Como $81 = 3^4$, entonces

$$\begin{aligned}\Phi_{81}(x) &= \Phi_{3^4}(x),\\ &= \Phi_3\left(x^{3^3}\right),\end{aligned}$$

$$\begin{aligned}&= \Phi_3(x^{27}),\\ &= (x^{27})^2 + (x^{27}) + 1,\\ &= x^{54} + x^{27} + 1.\end{aligned}$$

Teorema 2.17. *Si $p, n \in \mathbb{Z}^+$ y p es un primo que no divide a n, entonces*

$$\Phi_{pn}(x)\Phi_n(x) = \Phi_n(x^p).$$

Demostración. Por inducción sobre n.

1. Si $n = 1$, tenemos que

$$\begin{aligned} \Phi_p(x)\Phi_1(x) &= x^p - 1 \\ &= \Phi_1(x^p). \end{aligned}$$

2. Sea $n > 1$ un entero primo relativo con p y supongamos que para todo d tal que $1 \leq d < n$ y $\text{mcd}(d, p) = 1$, se tenga que

$$\Phi_{pd}(x)\Phi_d(x) = \Phi_n(x^d).$$

Si $d|pn$, entonces $\text{mcd}(d, p) = 1$ o $\text{mcd}(d, p) = p$. Luego, $d|n$ o $d = pl$ para algún $l \in \mathbb{Z}^+$.

En el caso de que $d = pl$, entonces $l|n$.

Por otra parte $ps|pn$, para todo entero positivo s que divida a n.

De lo anterior se desprende que

$$\prod_{d|pn} \Phi_d(x) = \prod_{d|n} \Phi_d(x) \prod_{l|n} \Phi_{pl}(x). \tag{10}$$

Como

$$\prod_{d|pn} \Phi_d(x) = x^{pn} - 1 \text{ y } \prod_{d|n} \Phi_d(x) = x^n - 1. \tag{11}$$

Reemplazando las ecuaciones (11) en la ecuación (10), obtenemos

$$x^{pn}-1=(x^n-1)\prod_{l|n}\Phi_{pl}(x), \tag{12}$$

pero

$$\prod_{l|n}\Phi_{pl}(x)\left(\prod_{l|n \text{ y } l<n}\Phi_{pl}(x)\right)\Phi_{pn}(x). \tag{13}$$

Como $\text{mcd}(p,n)=1$, entonces si $l|n$, $\text{mcd}(l,p)=1$.

Por hipótesis de inducción tenemos que

$$\begin{aligned}\prod_{l|n \text{ y } l<n}\Phi_{pl}(x) &= \prod_{l|n \text{ y } l<n}\frac{\Phi_l(x^p)}{\Phi_l(x)}\\ &= \frac{\prod_{l|n}\Phi_l(x^p)}{\prod_{l|n}\Phi_l(x)}\frac{\Phi_n(x)}{\Phi_n(x^p)}\\ &= \frac{(x^p)^n-1}{x^n-1}\frac{\Phi_n(x)}{\Phi_n(x^p)},\end{aligned}$$

Reemplazando esto último en la ecuación (13) y (13) en (12), obtenemos

$$x^{pn}-1=(x^n-1)\frac{x^{pn}-1}{x^n-1}\frac{\Phi_n(x)}{\Phi_n(x^p)}\Phi_{pn}(x),$$

de donde

$$\Phi_{pn}(x)=\frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

□

Ejemplo 2.18. Calculemos $\Phi_n(x)$ para los siguientes valores de $n = 12, 14, 15$. Usando en resultado anterior.

1. Para $n = 12$. Así $\Phi_{12}(x) = \frac{\Phi_4(x^3)}{\Phi_4(x)} = \frac{x^6+1}{x^2+1} = x^4 - x^2 + 1$.

2. Para $n = 14$. Así $\Phi_{14}(x) = \frac{\Phi_2(x^7)}{\Phi_2(x)} = \frac{x^7+1}{x+1} = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$.

3. Para $n = 15$. Así $\Phi_{15}(x) = \frac{\Phi_3(x^5)}{\Phi_3(x)} = \frac{x^{10}+x^5+1}{x^2+x+1} = x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$.

El siguiente resultado nos permite calcular $\Phi_n(x), n \in \mathbb{Z}^+$ y $n > 1$.

Teorema 2.19. *Sea $n \in \mathbb{Z}^+$ con la siguiente descomposición canónica $n = p_1^{k_1} \dots p_r^{k_r}$. Si $n_0 = p_1 \dots p_r$ y $n_1 = \frac{n}{n_0}$, entonces $\Phi_n(x) = \Phi_{n_0}(x^{n_1})$, es decir, podemos calcular $\Phi_n(x)$ para todo $n \in \mathbb{Z}^+$ simplemente usando la descomposición canónica y las propiedades anteriores.*

Demostración. Los divisores positivos de n_0 son los números $d = \prod_{i=1}^{r} p_i^{\varepsilon_i}$, donde $\varepsilon_i \in \{0, 1\}$. Denotemos el conjunto de todos estos divisores por D, entonces

$$\Phi_{n_0}(x) = \prod_{d \in D} \left(x^d - 1\right)^{\mu\left(\frac{n_0}{d}\right)}.$$

Los divisores e de n, tales que cumplen que $\mu\left(\frac{n}{e}\right) \neq 0$ son los números $\prod_{i=1}^{r} p_i^{a_i}$ con $a_i + 1 \leq k_i$ para cada i. Estos números son exactamente $n_1 d$, $(d \in D)$, y $\frac{n}{n_1 d} = \frac{n_0}{d}$, por lo tanto

$$\Phi_n(x) = \prod_{d \in D} \left(x^{n_1 d} - 1\right)^{\mu\left(\frac{n_0}{d}\right)} = \Phi_{n_0}\left(x^{n_1}\right).$$

□

Ejemplo 2.20. Calcular $\Phi_{360}(x)$.

Notemos que $360 = 2^3 \times 3^2 \times 5$, entonces

$$\Phi_{360}(x) = \Phi_{30}\left(x^{12}\right),$$

haciendo $y = x^{12}$, sabemos que $\Phi_{30}(y) = \Phi_{15}(-y)$ y que

$$\Phi_{15}(z) = \frac{\left(z^{15}-1\right)(z-1)}{(z^5-1)(z^3-1)},$$

$$\Phi_{15}(z) = z^8 - z^7 + z^6 - z^5 + z^4 - z^3 + z^2 - z + 1,$$

Ahora reemplazando z por $-y$ tendremos que

$$\Phi_{30}(y) = (-y)^8 - (-y)^7 + (-y)^6 - (-y)^5 + (-y)^4 - (-y)^3 + (-y)^2 - (-y) + 1,$$

$$\Phi_{30}(y) = y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1,$$

y como $y = x^{12}$, entonces

$$\Phi_{30}\left(x^{12}\right) = x^{96} + x^{84} + x^{72} + x^{60} + x^{48} + x^{36} + x^{24} + x^{12} + 1,$$

entonces tenemos que $\Phi_{360}(x) = x^{96} + x^{84} + x^{72} + x^{60} + x^{48} + x^{36} + x^{24} + x^{12} + 1$. Note que aquí calculamos $\Phi_{15}(x)$ de manera diferente a la usada en el ejemplo (2.18).

3. Dominios euclídeos

Esta sección presentamos algunas condiciones y ejemplos de interés, también condiciones suficientes y necesarias para que un anillo sea un dominio euclídeo.

Lo primero es saber que es un dominio euclídeo.

Definición 3.1. Un dominio entero R es llamado dominio euclídeo si existe una función

$$\sigma : R - \{0\} \to \mathbb{N}$$

llamada **función euclídea**, tal que:

1. Para todo $a, b \in R - \{0\}$, se cumple que $\sigma(ab) \geq \sigma(a)$.

2. Para todo $a \in R$, $b \in R - \{0\}$, existen $q, r \in R$ únicos, tal que $a = bq + r$ y además

   a) $r = 0$ o

   b) $\sigma(r) < \sigma(b)$.

Observación 3.2. Note que los dominios euclídeos son los anillos R donde vale la generalización del algoritmo de la división de Euclides en $\mathbb{Z}$. Estos dominios son los que nos interesa estudiar y veremos que además poseen una estructura adicional que nos permitirán dar una caracterización de estos más adelante.

3.1. Estructura de los dominios euclídeos

El grupo de unidades de R, denotado por $U(R)$ está definido por

$$U(R) = \{r \in R : \exists s \in R,\, rs = sr = 1\}.$$

Definición 3.3. Sea R un dominio entero. Dado un subconjunto $P \subseteq R - \{0\}$, el **conjunto derivado** de P, denotado por P', está definido por

$$P' = \{b \in P : \exists a \in R,\, a + bR \subseteq P\}.$$

La $i-$ésima derivada del conjunto P es denotada por $P^{(i)}$, por convención $P^{(0)} = P$.

Teorema 3.4. *Sea $P_0 = R - \{0\}$. Entonces R es un dominio euclídeo si y solo si*

$$\bigcap_{i=0}^{\infty} P_0^{(i)} = \emptyset.$$

Antes de presentar la prueba daremos las herramientas necesarias para ello.

Definición 3.5. Un subconjunto $P \subseteq R - \{0\}$ es llamado un **subconjunto producto** de $R - \{0\}$ si es cerrado bajo la multiplicación en $R - \{0\}$, es decir $P(R - \{0\}) \subseteq P$.

Proposición 3.6. *Sea R un anillo y $P \subset R$, si P es un subconjunto producto, entonces P' también es un subconjunto producto.*

Demostración. Sea $b \in P'$, veamos que $ba \in P'$ para todo $a \in R - \{0\}$.

Sabemos que $b \in P'$, por lo tanto existe un $c \in R$ tal que $c + bR \subseteq P$, es decir para cada $k \in R$ tal que $c + bk \in P$, si esto se cumple, en específico también lo debe hacer para $k \in (R - \{0\})R$, dado que $(R - \{0\})R \subseteq R$. Por lo tanto $P'(R - \{0\}) \subseteq P'$. □

Definición 3.7. Sea R un dominio entero. Una **cadena euclídea** en R es una sucesión $P_0, P_1, \ldots$ o $\{P_i\}_{i\in\mathbb{N}}$ de subconjuntos producto tal que:

1. $P_0 = R - \{0\}$,
2. $P_i \supseteq P_{i+1}$ para todo $i \in \mathbb{N}$,
3. $P_i' \subseteq P_{i+1}$ para todo $i \in \mathbb{N}$,
4. $\bigcap_{i=0}^{\infty} P_i = \emptyset$.

Observación 3.8. Sea $\{Q_i\}_{i\in\mathbb{N}}$ y $\{P_i\}_{i\in\mathbb{N}}$ dos cadenas euclídeas en R, diremos que $\{P_i\}_{i\in\mathbb{N}}$ es **más rápida** que $\{Q_i\}_{i\in\mathbb{N}}$ si $P_i \subseteq Q_i$ para todo $i \in \mathbb{N}$. Si $\{P_i\}_{i\in\mathbb{N}}$ es más rápida que todas las cadenas $\{R_i\}_{i\in\mathbb{N}}$, decimos que $\{P_i\}_{i\in\mathbb{N}}$ es las cadena **más rápida** en R.

Teorema 3.9. *Sea R un dominio entero, existe una correspondencia biyectiva entre las cadenas euclídeas en R y las funciones euclídeas en $R - \{0\}$.*

Demostración. Dada una cadena euclídea $\{P_i\}_{i\in\mathbb{N}}$ y $x \in R - \{0\}$, defina

$$\sigma(x) = \text{máx}\{i : x \in P_i \text{ y } x \notin P_{i+1}\}.$$

Veamos que σ es una función euclídea. Tomemos $a, b \in R - \{0\}$ y supongamos que $\sigma(b) = i$, es decir $b \in P_i$ y $b \notin P_{i+1}$, como P_i es subconjunto producto, entonces $ab \in P_i$, entonces $\sigma(ab) \geq i$ es

decir $\sigma(ab) \geq \sigma(b)$.

Ahora tomemos $a \in R, b \in R - \{0\}$. Si $a = 0$ o $\sigma(a) < \sigma(b)$ escribimos $a = 0 \cdot b + a$.

Supongamos que $\sigma(a) \geq \sigma(b)$ y que σ no es una función euclídea, entonces para cada $q \in R$ se tiene que $\sigma(a - bq) > \sigma(b) = i$ y de la definición de σ, esto quiere decir que $a + b(-q) \in P_n$, con $n > i$, por la condición 2 de ser cadena euclídea, $P_n \subseteq P_i$, por lo tanto $a + b(-q) \in P_i$ y como $q \in R$, entonces $b \in P_i' \subseteq P_{i+1}$ por ser cadena euclídea, lo que nos lleva a que $\sigma(b) \geq \sigma(b) + 1$, que es una contradicción. Por lo tanto σ debe ser una función euclídea.

Recíprocamente, si σ es una función euclídea en R, definamos

$$P_i = \{x \in R - \{0\} : \sigma(x) \geq i\}.$$

Veamos que $\{P_i\}_{i \in \mathbb{N}}$ es una cadena euclídea.

Lo primero es mostrar que P_i es subconjunto producto independiente de i.

Sea $b \in P_i$ es decir $\sigma(b) \geq i$ y como $\sigma(ab) \geq \sigma(b) \geq i$ con $a \in R - \{0\}$, entonces $ab \in P_i$ o escrito de otra manera $P(R - \{0\}) \subseteq P_i$.

Teniendo eso nos queda solo mostrar las últimas propiedades.

1. Como $P_0 = \{x \in R - \{0\} : \sigma(x) \geq 0\}$, y ello se cumple para todo $x \in R - \{0\}$, entonces $P_0 = R - \{0\}$.

2. Sea $x \in P_{i+1}$ es decir, $\sigma(x) \geq i + 1$, i.e. $x \in P_i$ y así $P_{i+1} \subseteq P_i$.

3. Sea $b \in P_i'$. Luego, existe un $a \in R$ tal que $a + b(-q) \in P_i$, para todo $-q \in R$. Como σ

es una función euclídea, al escribir $a = bq + r$ con $\sigma(r) < \sigma(b)$, sigue de la hipótesis que $\sigma(r) = \sigma(a - qb) \geq i$. Dado que $\sigma(b) > \sigma(r) \geq i$, entonces $\sigma(b) \geq i+1$, por lo tanto $b \in P_{i+1}$, así $P_i' \subseteq P_{i+1}$.

4. Supongamos que existe $x \in \bigcap_{i=0}^{\infty} P_i$, para algún $x \in R - \{0\}$ se tiene que $\sigma(x) \geq i$ para todo $i \in \mathbb{N}$, lo cual es una contradicción, ya que $\mathbb{N}$ no es acotado superiormente, por lo tanto $\bigcap_{i=0}^{\infty} P_i = \emptyset$.

□

Proposición 3.10. *Sea R un dominio entero. Para toda cadena euclídea $\{P_i\}_{i\in\mathbb{N}}$ en R existe la cadena más rápida $\{R_i\}_{i\in\mathbb{N}}$ dada por*

$$R_i = P_0^{(i)}. \tag{14}$$

Demostración. Veamos que $\{R_i\}_{i\in\mathbb{N}}$ es una cadena euclídea. Como el derivado de un subconjunto producto también lo es, entonces falta ver que se cumplen las otras 4 condiciones

1. La primera condición es clara, $R_0 = P_0^{(0)} = P_0 = R - \{0\}$.

2. Dado que $R_{i+1} = P_0^{(i+1)}$ y $R_i = P_0^{(i)}$, se sigue de la definición de conjunto derivado

$$P_0^{(i+1)} = \left\{ b \in P_0^{(i)} : \exists a \in R,\, a + bR \subseteq P_0^{(i)} \right\} \subseteq P_0^{(i)},$$

es decir, $R_{i+1} \subseteq R_i$.

3. Por la definición de conjunto derivado, tenemos que $R_{i+1} = P_0^{(i+1)} = \left(P_0^{(i+1)}\right)' = (R_i)'$, y en particular, $(R_i)' \subseteq R_{i+1}$.

4. Ver Sección 1 de Motzkin (1949).

□

Veamos unos ejemplos de algunos dominios euclídeos, vía las cadenas euclídeas.

Ejemplo 3.11. Considere el anillo de los números enteros $\mathbb{Z}$ con la siguiente función euclídea $\sigma(x) = |x|$. Calculemos la cadena euclídea correspondiente.

Usando la correspondencia dada en la demostración del Teorema (3.9), cada P_i está dado por:

$$P_i = \{x \in \mathbb{Z} - \{0\} : \sigma(x) \geq i\} = \mathbb{Z} - \{0, \pm 1, \ldots, \pm(i-1)\}.$$

Veamos que $\{P_i\}_{i\in\mathbb{N}}$ es una cadena euclídea de $\mathbb{Z}$.

Sea P_i con i arbitrario pero fijo y tome $x \in P_i, a \in \mathbb{Z} - \{0\}$. Entonces $\sigma(ax) = |ax| = |a||x|$, pero como $|a| \geq 1$ y $|x| \geq i$, entonces $|ax| \geq i$, es decir, $ax \in P_i$. Por lo tanto P_i es subconjunto producto para cada i.

Es claro que las condiciones i, ii, iv de la Definición (3.7) se cumplen por construcción de $\{P_i\}_{i\in\mathbb{N}}$.

Resta demostrar que $P_i' \subseteq P_{i+1}$. Note que si los $x \in P_{i+1}$, entonces $|x| \geq i+1$, veamos que $i \notin P_i'$.

Si $i \in P_i'$, entonces existe $a \in \mathbb{Z}$ tal que $a + i\mathbb{Z} \subseteq P_i = \mathbb{Z} - \{0, \ldots, \pm(i-1)\}$ o equivalentemente $a + ik \in P_i$ para todo $k \in \mathbb{Z}$. Por el algoritmo de la división, $a = mi + n$ con $n \in \{0, 1, \ldots, i-1\}$ y $a + ik = (mi + n) + ik \in P_i$ para todo $k \in \mathbb{Z}$. Tomando $k = -m$, luego $mi + n - mi = n \in P_i$, lo que

es una contradicción. Luego $i \notin P_i'$ y así $P_i' \subseteq P_{i+1}$.

Como se mencionó en la Proposición (3.10), existe una cadena más rápida. Calculemos tal cadena en este caso.

Esta cadena está dada por $P_i = R_0^{(i)}$, donde $R_0 = \mathbb{Z} - \{0\}$.

Supongamos que $x = 1 \in R_0'$, entonce existe $a \in \mathbb{Z}$ tal que $a + (1)k \in R_0$ para todo $k \in \mathbb{Z}$, entonces tome $k = -a$, obtenemos que $0 \in R_0$ lo que es falso, por lo tanto 1 no está en R_0'. De forma análoga -1 tampoco está en R_0'.

Sea $x \geq 2$ y supongamos $x \notin R_0'$, es decir, que para toda $a \in \mathbb{Z}$, existe un $k \in \mathbb{Z}$ tal que $a + xk = 0$, así $x|a$, pero esto no es posible ya que $x \geq 2$, lo que es una contradicción. Por lo tanto $2 \leq x \in R_0'$ y así $R_0' = \mathbb{Z} - \{0, \pm 1\}$.

Suponga que 2 y 3 están en R_0''. Entonces existen $a, b \in \mathbb{Z}$ tal que para todo $k \in \mathbb{Z}$ se cumple que $a + 2k \in R_0'$ y $b + 3k \in R_0'$.

En el primer caso tenemos que $a = 2m + n$ con $n \in \{0, 1\}$, entonces tomando $k = -m$ y así $a + k(-m) = n$ lo cual es una contradicción.

En el segundo caso de manera análoga tomando $b = 3m + n$ con $n \in \{0, 1, 2\}$, entonces tome $k = -m$ y tenemos que $b + k(-m) = n$ de nuevo una contradicción.

Ahora supongamos que para todo $x \geq 4$ se cumple que para todo $a \in \mathbb{Z}$ existe $k \in \mathbb{Z}$ tal que $a + xk = 0, \pm 1$.

Tome $a = x + 2$, así $k = \frac{-x-2}{x}$ o $k = \frac{\pm 1 - x - 2}{x}$, pero $x \nmid -x - 2$, $x \nmid -x - 1$ y $x \nmid -x - 3$, entonces $k \notin \mathbb{Z}$. Por lo tanto $x \in R_0''$.

Entonces $R_0'' = \mathbb{Z} - \{0, \pm 1, \pm 2, \pm 3\}$.

Ahora veamos por inducción que $R_0^{(i)} = \mathbb{Z} - \{0, \pm 1, \ldots, \pm(2^i - 1)\}$, se tiene que para $i = 1$, $R_0^{(1)} = \mathbb{Z} - \{0, \pm 1, \ldots, \pm(2^1 - 1)\} = \mathbb{Z} - \{0, \pm 1\}$.

Supongamos que se cumple para $i = n$ es decir $R_0^{(n)} = \mathbb{Z} - \{0, \pm 1, \ldots, \pm(2^n - 1)\}$.

Calculemos $R_0^{(n+1)}$.

Queremos ver que si $x \in R_0^{(n+1)}$, entonces $x \notin \{0, \pm 1, \ldots, \pm(2^{n+1} - 1)\}$. Sabemos que $R_0^{(n+1)} \subseteq R_0^{(n)}$, entonces basta ver que $x \notin \{\pm(2^n), \ldots, \pm(2^{n+1} - 1)\}$

Supongamos que para cada $x \in \{\pm(2^n), \ldots, \pm(2^{n+1} - 1)\}$ existe $a \in \mathbb{Z}$ tal que $a + xk \in R_0^{(n)}$ para todo $k \in \mathbb{Z}$.

- Si $x = 2^n$, entonces $a + 2^n k \notin \{0, \ldots, \pm(2^n - 1)\}$, pero $a = 2^n m + j$ con $j \in \{0, \ldots, (2^n - 1)\}$ y tomemos $k = -m$, entonces $a + 2^n(-m) = j$ lo cual es una contradicción.

- Ahora $x = 2^n + 1$, así $a + (2^n + 1)k \notin \{0, \ldots, \pm(2^n - 1)\}$, de nuevo tomemos $a = (2^n + 1)m + j$ con $j < 2^n + 1$. Para $j < 2^n$ tomamos $k = -m$ y sería análogo al inciso anterior. Veamos que pasa para $j = 2^n$ entonces reescribamos

  $a + (2^n + 1)k = (2^n + 1)m + 2^n + (2^n + 1)k = 2^n(m + 1) + m + 2^n k + k$,

  y tome $k = -m - 1$, entonces $2^n(m + 1) + m + 2^n k + k = m - m - 1 = -1$ y por lo tanto para $x = 2^n + 1 \notin R_0^{(i+1)}$.

- Si $x = 2^n + 2$, tomemos $a = (2^n + 2)m + j$ con $j < 2^n + 2$, cuando $j < 2^n$, $k = -n$ así $a + (2^n + 2)k = (2^n + 2)m + j + (2^n + 2)(-m) = j$.

Si $j = 2^n$,

$$a + (2^n + 2)k = (2^n + 2)m + 2^n + (2^n + 2)k = 2^n(m+1) + 2m + 2^n k + 2k,$$

tomando $k = -m - 1$, queda $2^n(m+1) + 2m + 2^n k + 2k = 2m - 2m - 2 = -2$.

Pero $j = 2^n + 1$, tendríamos

$$a + (2^n + 2)k = (2^n + 2)m + 2^n + 1 + (2^n + 2)k = (2^n + 1)(m+1) + m + (2^n + 1)k + k,$$

tomando $k = -m - 1$, queda $(2^n + 1)(m+1) + m + (2^n + 1)k + k = m - m - 1 = -1$.

Así para $x = \pm(2^n + 2) \notin R_0^{(n+1)}$.

- Vemos que para $x = 2^{n+1} - 1$, y al tomar $a = (2^{n+1} - 1)m + j$ con $j < 2^{n+1} - 1$, basta con ver para el caso $j = 2^n$, ya que cuando j va aumentando, entonces se al buscar el k apropiado, la suma $(2^{n+1} - 1)m + j + (2^{n+1} - 1)k$ va disminuyendo. Entonces

$$(2^{n+1} - 1)m + 2^n + (2^{n+1} - 1)k = 2^n(2m + 2k + 1) - m - k$$

tome $k = -m - 1$, entonces $2^n(2m + 2k + 1) - m - k = -2^n + 1$ y como $\pm(2^n - 1)$ no está en $R_0^{(i)}$ concluimos que $x = 2^{n+1} - 1 \notin R_0^{(i+1)}$.

- Veamos que para $x \geq 2^{n+1}$, si existe ese $a \in \mathbb{Z}$

Tome $a = 2^{n-1}$, entonces $a + xk = 2^{n-1} + xk$ y supongamos que para algún k, $a + xk =$

$2^{n-1}+xk = m \in \{0, \pm 1, \ldots, \pm(2^n-1)\}$, así

$$k = \frac{m-2^{n-1}}{2^{n+1}-1} \notin \mathbb{Z}$$

ya que el denominador no dividirá nunca a numerador. Por lo tanto para $x \geq 2^n \in R_0^{(i+1)}$.

Con esto podemos concluir que $R_0^{(i)} = \mathbb{Z} - \{0, \pm 1, \ldots, \pm(2^i-1)\}$.

Ahora veamos como es la función euclídea correspondiente a la cadena euclídea $\{R_0^{(i)}\}_{i\in\mathbb{N}}$, definida por $R_0^{(i)} = \mathbb{Z} - \{0, \pm 1, \ldots, \pm(2^i-1)\}$. De nuevo usando la caracterización dada en el Teorema (3.10) tenemos que

$$\sigma_R(x) = \text{máx}\{i : x \in R_0^{(i)} \text{ y } x \notin R_0^{(i+1)}\}$$

Supongamos que $\sigma_R(x) = i$, veamos cuales x cumplen esto. Por definición serían $2^i \leq |x| < 2^{i+1}$. es decir, $x \in \{\pm 2^i, \pm(2^i+1), \ldots, \pm(2^{i+1}-1)\}$, entonces

$$\begin{aligned} \log_2(2^i) \leq &\ \log_2|x| &< \log_2(2^{i+1}), \\ i \leq &\ \log_2|x| &< i+1, \end{aligned}$$

pero la función debe ir a $\mathbb{N}$, entonces $i \leq \lfloor \log_2|n| \rfloor < i+1$, así $\lfloor \log_2|x| \rfloor = i$, si $2^i \leq x < 2^{i+1}$, por lo tanto esta es nuestra función euclídea.

Ejemplo 3.12. Consideremos el anillo $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$ y la función $\sigma : \mathbb{Z}[i] \to \mathbb{Z}$ dada

por $\sigma(a+ib) = a^2+b^2$.

Podemos probar que usando un procedimiento similar al del ejemplo anterior que $\mathbb{Z}[i]$ es un dominio euclídeo mostrando que la cadena

$$R_0 = \mathbb{Z}[i] - \{0\}$$

$$R_n = \mathbb{Z}[i] - \{x \in \mathbb{Z}[i] : |x|^2 \leq n-1\}$$

Si calculamos la cadena más rápida sobre $\mathbb{Z}[i]$, obtenemos

$$P_0 = \mathbb{Z}[i] - \{0\}$$

$$P_0^{(n)} = \mathbb{Z}[i] - \{x \in \mathbb{Z}[i] : |x| \leq n\}$$

que corresponde a la función euclídea $\phi(x) = |x|^2 - 1$. Los cálculos para mostrar esto, son similares a los realizados en el ejemplo anterior.

Definición 3.13. Sea R un anillo conmutativo. Una no unidad b es llamada **divisor lateral** de $a \in R$ si b divide $a+e$, para algún $e \in U(R) \cup \{0\}$. Si b es un divisor lateral de todo $a \in R$, diremos que b es un **divisor lateral universal**.

Lema 3.14. *Sea R un dominio entero. Si $P_0 = R - \{0\}$, entonces los conjuntos P_0' y P_0'' pueden ser expresados como*

$$P_0' = R - (U(R) \cup \{0\}) \text{ y } P_0'' = P_0' - U,$$

donde U es el conjunto de todos los divisores laterales universales.

Demostración. Veamos que $P_0' = R - (U(R) \cup \{0\})$.

Sea $b \in P_0'$. Supongamos que $b \in U(R)$. Como $b \in P_0'$, por definición existe un $a \in R$ tal que $a + bc \in P_0$ para todo $c \in R$, dado que $b \in U(R)$, existe $s \in R$ tal que $sb = 1$, entonces tomando $c = -sa$, se tiene que $a + b(-sa) = a - (sb)a = a - a = 0$, lo que es una contradicción, por lo tanto $b \notin U(R)$ y así $P_0' \subseteq R - (U(R) \cup \{0\})$.

Recíprocamente, sea $b \in R - (U(R) - \{0\})$ y supongamos que $b \notin P_0'$. Luego para cada $a \in R$ existe c tal que $a + bc = 0$. Al tomar $c = -sa$, se tiene $a + bc = a - (bs)a = a(1 - bs) =$ y como $a \in R$, $bs = 1$ dado que R es un dominio, lo que es un contradicción. Concluyendo que $P_0' = R - (U(R) \cup \{0\})$.

Ahora veamos que $P_0'' = P_0' - U$.

Sea $b \in P_0''$ y supongamos que $b \notin P_0' - U$. Como $b \in P_0''$, existe $a \in R$ tal que para todo $c \in R$ se tiene que $a + bc \in P_0'$. Como $b \in U$, entonces para a se cumple que $b \mid a + e$ con $e \in U(R) \cup \{0\}$, es decir, existe $k \in R$ tal que $bk = a + e$. Reemplazando a se tiene $(bk - e) + bc = b(k + c) - e \in P_0'$ para todo $c \in R$. Tomando $c = -k$, entonces $b(k - k) + e = e \in P_0'$, lo que es una contradicción dado que $P_0' = R - (U(R) \cup \{0\})$. Por lo tanto $b \in P_0' - U$.

Recíprocamente, sea $b \in P_0' - U$ y supongamos que $b \notin P_0''$. Entonces para todo $a \in R$, existe un $c \in R$ tal que $a + bc \notin P_0'$ o equivalentemente $a + bc \in U(R) \cup \{0\}$, es decir, $a + bc = u$, $u \in U(R)$ o $a + bc = 0$. Reescribiendo $bc = u - a$ o $bc = -a$ que por definición implica que $b| - a$ y $b|u - a$ para todo $a \in R$ y así $b \in U$, que contradice el supuesto $b \in P_0' - U$. Por lo tanto $b \in P_0''$ y en consecuencias $P_0'' = P_0' - U$. □

Ejemplo 3.15. Usando este ultimo resultado, veamos que el anillo $R = \mathbb{Z}\left[\sqrt{-5}\right]$ no es un dominio euclídeo.

Veamos cuales son las unidades de R. Tomemos $a + \sqrt{-5}b \in R$, podemos simplificarlo como $a + i\sqrt{5}b$, el inverso multiplicativo en el cuerpo de los números complejos es

$$\frac{a}{a^2 + 5b^2} + i\frac{\sqrt{5}b}{a^2 + 5b^2},$$

pero este número solo pertenece a R cuando $b = 0$ y $a = \pm 1$, así, las únicas unidades de R son ± 1. Luego, como vimos en el Ejemplo (3.11), ± 2 y ± 3 son divisores laterales universales de todo $n \in \mathbb{Z}$. Sin embargo, no existe elemento $k \in R$ tal que $\pm 2k = \sqrt{-5}$ o $\pm 3k = \sqrt{-5}$, entonces ninguno de estos es un divisor lateral de $\sqrt{-5}$, lo que implica que no hay divisores laterales universales en $\mathbb{Z}\left[\sqrt{-5}\right]$, es decir, $U = \emptyset$. Por lo tanto $P_0'' = P_0'$ y así

$$\bigcap_{n=0}^{\infty} P_0^{(n)} \neq \emptyset.$$

Siguiendo del Teorema (3.9) y la Definición (3.7) que $\mathbb{Z}\left[\sqrt{-5}\right]$ no es un dominio euclídeo.

3.2. Condiciones necesarias para que un cuerpo sea euclídeo

Primero veremos unas definiciones y lo que significa que un cuerpo sea euclídeo, con el fin de mostrar algunas condiciones necesarias para que un dominio sea euclídeo.

Definición 3.16. Sea R un dominio entero. Un elemento $x \in R$ es llamado **irreducible** si dados

$y,z \in R$ y $x = yz$, implica que x es unidad o y es unidad.

Definición 3.17. Sea R un anillo conmutativo. Un elemento no nulo $p \in R - U(R)$ es llamado **primo** si $a,b \in R$ y $p|ab$ implica que $p|a$ o $p|b$.

Definición 3.18. Sea R un dominio entero. Diremos que en R se cumple la **existencia de factorización** (EDF), si para cada $x \in R$, la factorización de x en elementos irreducibles termina después de un número finito de pasos.

Definición 3.19. Sea R un dominio entero, R es llamado **dominio de factorización única** (DFU) si:

- En R se cumple la existencia de factorización (EDF).
- Si $b_1 b_2 \dots b_n$ y $c_1 c_2 \dots c_m$ representan dos factorizaciones de $a \in R$ en elementos irreducibles, entonces $m = n$ y existe una permutación ψ de $\{1,\dots,n\}$ tal que $b_i = u_i c_{\psi(i)}$ y cada $u_i \in R$ es una unidad.

Definición 3.20. Sea K el cuerpo de fracciones de un dominio entero R. Diremos que $t \in K$ es **entero** si satisface un polinomio mónico en $R[x]$, esto es, existen $n \in \mathbb{N}$ y $a_0, a_1, \dots, a_n \in R$ tal que

$$t^n + a_{n-1}t^{n-1} + \cdots + a_0 = 0.$$

Diremos que R es **integralmente cerrado** si no hay elementos en $K - R$ (K es el cuerpo de fracciones de R) que sean enteros sobre R.

Definición 3.21. Un dominio entero R, es llamado **Noetheriano** si cumple la condición de cadena ascendente de ideales, es decir si

$$I_1 \subseteq I_2 \subseteq \dots$$

es una cadena ascendente de ideales de R, entonces existe $n \in \mathbb{Z}^+$ tal que $I_n = I_i$ para todo $i \geq n$.

Lema 3.22. *Un anillo R es Noetheriano si y solo si se cumple la existencia de factorización (EDF) en R.*

Demostración. Supongamos que no se cumple la existencia de factorización (EDF) en R, es decir, existe un elemento $x \in R$ y una sucesión de factorizaciones

$$x = y_1 x_1 = y_1 y_2 x_2 = \dots$$

de x, lo que nos da una sucesión infinita ascendente

$$(x) \subseteq (x_1) \subseteq (x_2) \subseteq \dots$$

de distintos ideales principales y por lo tanto R no es Noetheriano.

Recíprocamente si

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

es una sucesión ascendente infinita, entonces para todo i el generador de (a_{i+1}) divide al generador de (a_i), por lo que existe $b_i \in R$ para cada i, tal que $a_i = b_i a_{i+1}$, es decir, obtenemos una factorización

no terminal,

$$a_1 = b_1 a_2 = b_1 b_2 a_3 = \dots$$

Es decir no se tiene la existencia de factorización en R. □

Proposición 3.23. *Sea R un dominio entero en el cual se tiene la existencia de factorización (EDF), entonces cada elemento $p \in R$ primo es irreducible.*

Demostración. Suponga que $p \in R$ es primo y que $p|a$ para algún $a \in R$. Como en R se cumple la EDF, escribimos

$$a = c_1 \dots c_k$$

como un producto de elementos irreducibles. Entonces existe i donde $1 \leq i \leq k$, tal que $p|c_i$. Así $c_i = yp$ para algún $y \in R$, y como c_i es irreducible, y o p debe ser una unidad, como p es primo, y es unidad, y así p es irreducible. □

Proposición 3.24. *Sea R un dominio de ideales principales (DIP) y sea I un ideal de R, entonces I es maximal si y solo si $I = (p)$, donde p irreducible.*

Demostración. Ver Capítulo 0 de Roman (2005). □

Lema 3.25. *Sea R un dominio entero en el cual se tiene la existencia de factorización (EDF), entonces R es in DFU si y solo si cada elemento irreducible es primo.*

Demostración. Supongamos que R es un DFU y que $p \in R$ es un elemento irreducible que no es primo. Entonces existen $a, b \in R$ tal que $p|ab$, pero $p \nmid a$ y $p \nmid b$. Entonces p está en la factorización

de ab, pero no en la factorización de a o de b, lo que es una contradicción.

En el otro sentido, supongamos que cada elemento irreducible es primo, pero que R no es un DFU. Entonces existe $x \in R$ tal que $p_1 p_2 \dots p_k$ y $q_1 q_2 \dots q_n$ son factorizaciones distintas de x en elementos irreducibles. Supongamos que $k \leq n$ y que $p_1 \neq u q_j$ para todo $1 \leq j \leq n$ y $u \in U(R)$. Entonces por definición de primo, $p_1 | q_i$ para algún $1 \leq i \leq n$, pero dado que q_i es irreducible, debe cumplirse que $u p_1 = q_i$ para algún $u \in U(R)$, lo que es una contradicción. □

Note que para verificar que un DIP es un DFU, necesitamos mostrar que la factorización en elementos irreducibles es única, salvo por unidades, que por Lema (3.27) es equivalente a mostrar que cada elemento irreducible es primo y se tiene la EDF en R.

Proposición 3.26. *Sea R un DIP, entonces cada elemento irreducible de R es primo.*

Demostración. Suponga que $p \in R$ es irreducible y $p|ab$ para $a, b \in R$. Luego (p) es un ideal maximal. Consideremos $(p,a) \supseteq (p)$ y $(p,b) \supseteq (p)$.

Si $(p,a) = (p)$, entonces $(a) \subseteq (p)$, así $p|a$ y se tiene la conclusió. Análogo si $(p,b) = (p)$. Dado que (p) es maximal, la única posibilidad es que $(p,a) = (p,b) = (1) = R$. Entonces existen $x, y, v, w \in R$ tal que

$$1 = xp + ya$$

y

$$1 = vp + wb,$$

multiplicando las dos expresiones tenemos

$$1 = xvp^2 + (xwb + vya)p + wyab.$$

Además, dado que $p|ab$, entonces la parte derecha de la igualdad es divisible por p, pero la izquierda no, lo que es una contradicción. □

Lema 3.27. *Sea R un DFU, entonces R es integralmente cerrado.*

Demostración. Sea R un DFU y sea K su cuerpo de fracciones. Si R no es integralmente cerrado, entonces existe un $t \in K - R$ tal que t es solución de un polinomio mónico irreducible

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0,$$

escribiendo $t = \frac{m}{n}$, con $m, n \in R - \{0\}$ y $\text{mcd}(m,n) = 1$,

$$\left(\frac{m}{n}\right)^d + a_{d-1}\left(\frac{m}{n}\right)^{d-1} + \cdots + a_1\left(\frac{m}{n}\right) + a_0 = 0,$$

multiplicando por n^d y reorganizando términos

$$-m^d = a_{d-1}m^{d-1}n + \cdots + a_1 mn^{d-1} + a_0 n^d = n\left(a_{d-1}m^{d-1} + \cdots + a_1 mn^{d-2} + a_0 n^{d-1}\right),$$

por lo tanto $n|m^d$, lo que contradice que $\text{mcd}(n,m) = 1$ y $t \in K - R$. □

Teorema 3.28. *Diremos que K es un **cuerpo númerico** si es una extensión finita de $\mathbb{Q}$. Sea R un dominio entero, entonces:*

1. *Si R es un domino euclídeo, entonces R es un DIP.*

2. *Si R es un DIP, entonces R es un DFU.*

3. *Sea R un subanillo de un cuerpo numérico algebraico K que además es un dominio de factorización única. Entonces R es integralmente cerrado.*

Demostración. 1. Sea R un domino euclídeo, con función euclídea σ y sea $I \subseteq R$ un ideal. Si $I = \{0\}$, es claro que es principal, entonces supongamos que $I \neq \{0\}$. Considere $S = \{\sigma(i) : i \in I\}$. Como S es un subconjunto de $\mathbb{N}$, tiene un elemento mínimo m y escoja $j \in I$ tal que $\sigma(j) = m$. Sea $a \in I$ y usemos que R es un dominio euclídeo para escribir $a = qj + r$. Dado que $a, j \in I$, entonces $a - qj = r \in I$ y como $\sigma(j)$ es el mínimo, $\sigma(r) < \sigma(j)$ is imposible, entonces $r = 0$ y por lo tanto $a = qj$. Así $I = (j)$ y R es un DIP.

2. Por Lema (3.23) es suficiente mostrar que R es Noetheriano. Sea

$$(a_1) \subseteq (a_2) \subseteq \dots$$

una sucesión ascendente infinita de ideales principales. Queremos ver que $I = \bigcup_{i \in \mathbb{N}} (a_i)$ es un ideal. Para esto, tomemos $u, v \in I$ y $r \in R$, entonces existe $n \in \mathbb{N}$ tal que $u, v \in (a_n)$. Dado que (a_n) es un ideal, $u + v, ru$ están en (a_n) y por lo tanto en I.

Dado que R es un DIP, existe un $b \in R$ tal que $I = (b)$, entonces existe $m \in \mathbb{N}$ tal que $b \in (a_m)$.

Por lo tanto para cada $k \in \mathbb{N}$ se tiene que

$$(b) \subseteq (a_m) \subseteq (a_{m+1}) \subseteq \cdots \subseteq (a_{m+k}) \subseteq \cdots \subseteq I = (b),$$

esto muestra que $(b) = (a_m) = (a_{m+k})$ para todo k, así vemos que se cumple la EDF en R y concluimos que R es un DFU.

3. Para esta prueba se usa solamente el Lema (3.27) y resultado (2) del Teorema (3.28). Note que el anillo de los entero R_0 es el menor subanillo que es integralmente cerrado de K, este es el menor de los posibles dominios euclídeos, es decir, cada subanillo R de K que es un dominio euclídeo debe contener a R_0.

□

De esta manera, por el resultado (3.28), las condiciones necesarias, para que un anillo R sea un dominio euclídeo se pueden resumir de la siguiente manera:

$$R \text{ es dominio euclídeo} \Rightarrow R \text{ es DIP} \Rightarrow R \text{ es DFU} \Rightarrow R \text{ es integrralemnte cerrado.}$$

También existe un resultado, que nos dice específicamente para que valores de n, $\mathbb{Z}[\zeta_n]$ es un DIP. Este resultado fue mostrado por los matemáticos estadounidenses *J. Myron Masley* y *Hugh L. Montgomery* en 1974, ver Montgomery and Masley (1976).

Teorema 3.29. *(Masley y Montgomery) Hay precisamente 30 valores de n,* $n \not\equiv 2 \mod 4$ *para los*

cuales $\mathbb{Z}[\zeta_n]$ es un DIP. Estos son:

$$n = 1,3,4,5,7,8,9,11,12,13,15,16,17,19,20,21,24,25,27,28,32,33,35,$$
$$36,40,44,45,48,60,84.$$

3.3. Condiciones suficientes para que un cuerpo sea euclídeo

Finalizamos este capítulo mostrando cuando un dominio es euclídeo de forma sencilla, sin tener la dificultad vista con las cadenas euclídeas.

En la tabla podemos ver para que valores de n, $\mathbb{Z}[\zeta_n]$ es un domino euclídeo.

n	$\phi(n)$	Fecha de la primer prueba	Nombre del matemático
1	1	300	Euclides
4	2	1801	Gauss
5	4	1844	Kummer
7	6	1844	Kummer
3	2	1847	Wantzel
9	6	1847	Cauchy
15	8	1847	Cauchy
8	4	1850	Eisenstein
12	4	1850	Eisenstein
20	8	1975	H. W. Lenstra
11	10	1975	H. W. Lenstra
16	8	1977	T. Ojala
24	8	1978	H. W. Lenstra
13	12	1988	McKenzie

Tabla 1
Tomado de Akhtar (1995)

Definición 3.30. Diremos que K es un **cuerpo númerico** si es una extensión finita de $\mathbb{Q}$.

Si K es un cuerpo númerico definimos

$$Hom(K,\mathbb{C}) := \{\tau : K \to \mathbb{C} : \phi \text{ es un homomorfismo de cuerpos}\}.$$

Sea $x \in K$ y defina su **traza**

$$Tr_{K/\mathbb{Q}}(x) = \sum_{\tau \in Hom(K,\mathbb{C})} \tau(x)$$

y su **norma**

$$N_{K/\mathbb{Q}}(x) = \prod_{\tau \in Hom(K,\mathbb{C})} \tau(x).$$

Observe que para las extensiones de Galois $K/\mathbb{Q}$,

$$Hom(K,\mathbb{C}) = Gal(K,\mathbb{Q}),$$

esto último se puede ver en el Capítulo V de Grillet (2007).

Sea R el anillo de los enteros algebraicos en K. Siendo un subanillo de un cuerpo, R es un dominio entero (también se puede referir a R como anillo numérico).

Definición 3.31. Sea R el anillo numérico de un cuerpo numérico K. Diremos que R es euclídeo para la norma o **euclídeo normado** si para todo $a \in R$ y $b \in R - \{0\}$ existen $q, r \in R$ únicos, tal que $a = bq + r$ y $N(r) < N(b)$, donde N denota el valor absoluto de la norma del cuerpo $N_{K/\mathbb{Q}}$. En este caso, diremos que el cuerpo K es euclídeo.

De lo anterior se sigue que:

Proposición 3.32. *Si R es euclídeo normado, entonces R es un dominio euclídeo.*

Demostración. Basta con tomar N como función euclídea. □

Teorema 3.33. *Sea R el anillo numérico de un cuerpo numérico K. Entonces R es euclídeo normado si y solo si para cada $y \in K$ existe $x \in R$ tal que $N(y-x) < 1$.*

Demostración. Supongamos que R es un euclídeo normado, entonces dado $y \in K$, escriba $y = a/b$, donde $a, b \in R$ y $b \neq 0$. Como R es euclídeo normado, entonces existen $q, r \in R$ tal que $a = bq + r$ y $N(r) < N(b)$.

Dividiendo la ecuación por b nos queda $y = a/b = q + r/b$ y escojamos a $x = q \in R$, así:

$$N(y-x) = N\left(\frac{a}{b} - q\right) = N\left(\frac{r}{b}\right) < 1.$$

En otro sentido, supongamos que para cada $y \in K$ existe $x \in R$ tal que $N(y-x) < 1$, entonces tomando $a \in R$ y $b \in R - \{0\}$, escoja $q \in R$ tal que $N\left(\frac{a}{b} - q\right) < 1$, llamando $r = a - bq$, tenemos:

$$N(r) = N(a-bq) = N\left(b\left(\frac{a}{b} - q\right)\right) = N(b)N\left(\frac{a}{b} - q\right) < N(b).$$

□

Ejemplo 3.34. Los anillos $\mathbb{Z}[\zeta_n]$ son dominios euclídeos para $n = 1, 4, 3, 8$.

Para este resultado nos basaremos en el Teorema (3.33), haciendo uso de desigualdades, lo cual resulta más sencillo que encontrar una cadena euclídea.

1. $n = 1$, $\phi(n) = 1$.

   La prueba de Gauss para este caso se hizo usando el mismo método del caso anterior.

   Para este caso $K = \mathbb{Q}$ y $R = \mathbb{Z}$ y la norma $N_{\mathbb{Q}/\mathbb{Q}}(x) = |x|$ que en este caso, coincide con el valor absoluto.

   Entonces tomemos $a \in \mathbb{Z}$ y $b \in \mathbb{Z} - \{0\}$ y sea $q = \lfloor a/b \rfloor$ y $r = a - bq$, basta ver que $|r| < |b|$. Por definición $|a/b - \lfloor a/b \rfloor| < 1$, multiplicando por $|b|$ nos queda $|a - b\lfloor a/b \rfloor| < |b|$, pero $|a - b\lfloor a/b \rfloor| = |a - bq| = |r|$, así hemos mostrado que $|r| < |b|$.

2. $n = 4$, $\phi(n) = 2$.

   Entonces para este caso $K = \mathbb{Q}(i)$, $R = \mathbb{Z}[i]$ y la norma es $N(a + bi) = a^2 + b^2$. Esta prueba consiste en tomar un $z = a + ib$ y encontrar un $z' = a' + ib'$ tal que $N(a + bi - a' - ib') < 1$. Entonces tomemos $a' = \lfloor a + 1/2 \rfloor$ y de igual manera $b' = \lfloor b + 1/2 \rfloor$. Así $|a - a'|$ y $|b - b'|$ no serán mayores que $1/2$. Además,

$$N\left(a + ib - \left(a' + ib'\right)\right) = N\left((a - a') + i(b - b')\right) = (a - a')^2 + (b - b')^2$$

$$\leq (1/2)^2 + (1/2)^2 = 1/2 < 1.$$

3. $n = 3$, $\phi(n) = 2$.

   Tenemos $K = \mathbb{Q}(\zeta_3)$ y $R = \mathbb{Z}[\zeta_3]$, también llamado *entero de Eisenstein* donde su norma es $N(a + \zeta_3 b) = a^2 - ab + b^2$, este caso es análogo al anterior.

   Dado $z = a + b\zeta_3 \in \mathbb{Q}(\zeta_3)$, donde $a, b \in \mathbb{Q}$ y escogemos $a' = \lfloor a + 1/2 \rfloor$ y $b' = \lfloor b + 1/2 \rfloor$,

entonces

$$N(a+b\zeta_3-(a'+\zeta_3 b')) = (a-a')^2-(a-a')(b-b')+(b-b')^2$$

$$\leq |a-a'|^2+|a-a'||b-b'|+|b-b'|^2 \leq (1/2)^2+(1/2)(1/2)+(1/2)^2 = 3/4 < 1.$$

4. $n = 8$, $\phi(n) = 4$.

Primero recordemos las siguientes inclusiones

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_8),$$

y definamos, para $x \in \mathbb{Q}(\zeta_8)$ la *norma relativa*

$$N_{8/4} = \prod_{\tau \in Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))} \tau(x).$$

Así $N_8 = N_4 \cdot N_{8/4}$. Dado $T = t_0+t_1\zeta_8+t_2\zeta_8^2+t_3\zeta_8^3+t_4\zeta_8^4 \in \mathbb{Q}(\zeta_8)$, tome $S = s_0+s_1\zeta_8+s_2\zeta_8^2+s_3\zeta_8^3+s_4\zeta_8^4 \in \mathbb{Z}(\zeta_8)$ tal que para todo $0 \leq i \leq 3$, $|s_i - t_i| \leq 1/2$ y denotemos $a_i = |s_i - t_i|$ con $0 \leq i \leq 3$, para facilitar la notación.

Observe que

$$N_{8/4}(S-T) = (a_0+a_1\zeta_8+a_2\zeta_8^2+a_3\zeta_8^3)(a_0+a_1\zeta_8^5+a_2\zeta_8^{10}+a_3\zeta_8^{15}).$$

Usando la relación $\zeta_8^4 + 1 = 0$, podemos reescribir

$$N_{8/4}(S-T) = (a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)(a_0 - a_1\zeta_8 + a_2\zeta_8^2 - a_3\zeta_8^3),$$

y simplificando tenemos

$$(a_0^2 + 2a_1a_3 - a_2^2) + (a_3^2 + 2a_0a_2 - a_1^2)i,$$

así,

$$N_8(S-T) = N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}((a_0^2 + 2a_1a_3 - a_2^2) + (a_3^2 + 2a_0a_2 - a_1^2)i),$$

lo que se reduce a

$$(a_0^2 + a_2^2)^2 + (a_1^2 + a_3^2)^2 + 4a_1a_3(a_0^2 - a_2^2) + 4a_0a_2(a_3^2 - a_1^2).$$

Dado que $a_i \leq 1/2$ para $0 \leq i \leq 3$, entonces $a_i^2, a_1a_3, a_0a_2 \leq 1/4$ para $0 \leq i \leq 3$, como $a_0^2 - a_2^2 = (a_0 - a_2)(a_0 + a_2)$ y $(a_0 - a_2), (a_0 + a_2) \leq 1/2$, entonces $a_0^2 - a_2^2 \leq 1/4$ y al multiplicar por $4a_1a_3 \leq 1$ se tiene que $4a_1a_3(a_0^2 - a_2^2) \leq 1/4$, análogo para $4a_0a_2(a_1^2 - a_3^2)$.

Así todos los 4 términos de $N_8(S-T)$ están entre 0 y $1/4$ y por lo tanto $N_8(S-T) \leq 1$, lo que concluye que $\mathbb{Z}(\zeta_8)$ es un dominio euclídeo.

4. Cuerpos de funciones algebraicas

En esta sección final veremos unos fundamentos en la teoría de cuerpos de funciones

algebraicas y aplicaciones, donde introduciremos definiciones básicas y resultados con el fin de tener las herramientas necesarias para poder construir el cuerpo ciclotómico de funciones. Tomamos las definiciones y resultados de Stichtenoth (2009) y para estudiar el cuerpo de funciones ciclotómico se estudió Salvador (2006).

En este capítulo usaremos K para denotar un cuerpo arbitrario, a menos de que se diga lo contrario.

4.1. Lugares

Definición 4.1. Un **cuerpo de funciones algebraicas** F/K de una variable sobre K es una extensión de cuerpos $F \supseteq K$, tal que F es una extensión algebraica finita de $K(x)$ para algún elemento $x \in F$ que es trascendente sobre K.

Definamos el conjunto

$$\tilde{K} = \{z \in F : z \text{ algebraico sobre } K\},$$

que es un subcuerpo de F, dado que sumas, productos e inversión de elementos algebraicos son también son algebraicos. $\tilde{K}$ es llamado el cuerpo de constantes de F/K.

Así $K \subseteq \tilde{K} \subseteq F$. En efecto podemos verificar que $F/\tilde{K}$ también es un cuerpo de funciones algebraicas. Ver Capitulo 2 de Roman (2005).

Ejemplo 4.2. Un ejemplo simple de cuerpos de funciones algebraicas, es el cuerpo de funciones racionales. F/K es llamado racional si $F = K(x)$, para algún x trascendente sobre K.

En este caso, cada $z \in F - \{0\}$ tiene representación única en la forma

$$z = a \prod_i p_i(x)^{n_i},$$

donde $a \in K - \{0\}$, cada $p_i(x)$ es un polinomio mónico irreducible y $n_i \in \mathbb{Z}$.

Ver Capítulo 1 de Stichtenoth (2009).

Definición 4.3. Un **anillo de valuación** de un cuerpo de funciones racionales F/K es un anillo $\mathcal{O} \subseteq F$ con las siguientes propiedades.

1. $K \subsetneq \mathcal{O} \subsetneq F$.

2. Si $z \in F$, entonces $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Esta definición es motivada por la siguiente observación en el caso del cuerpo de funciones racionales $K(x)$

Ejemplo 4.4. Dado un polinomio mónico irreducible $p(x) \in K[x]$, considere el conjunto

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid f(x) \right\}. \tag{15}$$

Es fácil ver que $\mathcal{O}_P$ es un anillo de valuación de $K(x)(K)$. En efecto, para $\mathcal{O}_{p(x)}$ es claro que $K \subsetneq \mathcal{O}_{p(x)} \subsetneq K(x)$. Si tomamos $\frac{f(x)}{g(x)} \in K(x)$, tendremos que $\frac{f(x)}{g(x)}$ si $p(x)|g(x)$, entonces $p(x) \nmid f(x)$, si $\frac{f(x)}{g(x)} \notin \mathcal{O}_{p(x)}$, entonces $g(x)/f(x) \in \mathcal{O}_{p(x)}$.

Note que si $q(x)$ es otro polinomio mónico irreducible, entonces $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Teorema 4.5. *Sea $\mathcal{O}$ un anillo de valuación del cuerpo de funciones algebraicas F/K y sea $P = \mathcal{O} - U(\mathcal{O})$, entonces:*

1. *$\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal P.*

2. *Para cada $x \in F - \{0\}$, se tiene que $x \in P$ si y solo si $x^{-1} \notin \mathcal{O}$.*

3. *$\tilde{K} \subseteq \mathcal{O}$ y $\tilde{K} \cap P = \{0\}$.*

Demostración.

1. Afirmamos que P es un ideal de $\mathcal{O}$.

   Sean $x,y \in P$, si $x = 0$ o $y = 0$, es claro que $x+y \in P$. Supongamos que $x \neq 0 \neq y$, como $\frac{x}{y} \in F$, por la definición de anillo de valuación tenemos que $\frac{x}{y} \in \mathcal{O}$ o $\frac{y}{x} \in \mathcal{O}$, supongamos que $\frac{x}{y} \in \mathcal{O}$ y como $1 \in K \subseteq \mathcal{O}$, así $\frac{x}{y} + 1 \in \mathcal{O}$ como afirmamos que P es ideal, así

   $$x + y = \left(\frac{x}{y} + 1\right) y \in P.$$

   Si $x \in P$ y $y \in \mathcal{O}$, entonces $x,y \in \mathcal{O}$ y como $\mathcal{O}$ es un anillo entonces $xy \in \mathcal{O}$, además $xy \notin U(\mathcal{O})$, ya que si por el contrario $xy \in \mathcal{O}$, entonces $(xy)w = 1$ para algún $w \in \mathcal{O}$, con lo cual $x \in U(\mathcal{O})$, lo que es una contradicción, en consecuencia $xy \in P$ y así P es un ideal de $\mathcal{O}$.

   P es maximal en $\mathcal{O}$, ya que si I es un ideal de $\mathcal{O}$ tal que si $P \subseteq I \subseteq \mathcal{O}$ y tomemos $x \in I$ fijo, si x es unidad, entonces $1 = xx^{-1} \in I$ y así $I = \mathcal{O}$, si por el contrario x no es unidad, entonces

$x \in P$ y por lo tanto $I \subseteq P$ y como $P \subseteq I$, se tiene que $I = P$.

Para ver que tiene un único ideal maximal Ver Capítulo I de Atiyah (2020).

2. Sea $x \in F - \{0\}$, entonces $x \in P$ si y solo si $x \notin U(\mathcal{O})$ y esto se tiene si y solo so $x^{-1} \in \mathcal{O}$, que es cierto por la definición de anillo de valuación.

3. Sea $z \in \tilde{K}$, si $z = 0$ es claro que $z \in \mathcal{O}$. Supongamos que $z \neq 0$ y $z \notin \mathcal{O}$. Como $\mathcal{O}$ es un anillo de valuación, entonces $z^{-1} \in \mathcal{O}$ y puesto que z^{-1} es algebraico sobre K, existe $p(x) \in K[x]$ tal que $p\left(z^{-1}\right) = 0$. Sin perdida de generalidad podemos suponer que $p(x) = \sum_{i=0}^{r} a_i x^i$, donde $a_0 \neq 0$, caso contrario tendríamos $p(x) = xq(x)$, con $q\left(z^{-1}\right) = 0$ y $a_1 \neq 0$.

   Entonces dividiendo $p(x)$ entre a_0, nos queda $b(x) = 1 + \sum_{i=1}^{r} b_i x^i$ con $b_i = \frac{a_i}{a_0}$ y $\sum_{i=1}^{r} b_i z^{-i} = -1$. Por lo tanto $z^{-1}\left(\sum_{1}^{r} b_i z^{-i+1}\right) = -1$, es decir $z = -\left(\sum_{1}^{r} b_i z^{-i+1}\right) \in K\left[z^{-1}\right] \subseteq \mathcal{O}$, lo cual contradice la suposición que $z \notin \mathcal{O}$. En consecuencia $z \in \mathcal{O}$. Ahora veamos que $\tilde{K} \cap P = \{0\}$. Supongamos lo contrario, es decir, sea $z \in \tilde{K} \cup P$ con $z \neq 0$. Como $z \in \tilde{K}$, entonces $p(z) = \sum_{i=0}^{r} a_i z^i = 0$, para algún $p(x) \in K[x]$ y donde $a_0 = 1$. Luego $z(a_n z^n + \cdots + a_1) = -1$, en consecuencia z es una unidad, es decir $z \notin P$, lo que es contradictorio.

□

Veamos un lema que usaremos en la prueba de un resultado posterior.

Lema 4.6. *Sea $\mathcal{O}$ un anillo de valuación del cuerpo de funciones F/K, P su único ideal maximal y $x \in P - \{0\}$. Si $x_1, \ldots, x_n \in P$, son tales que $x_1 = x$ y $x_i \in x_{i+1}P$ para $i = 1, \ldots, n-1$. entonces*

$$n \leq [F : K(x)] < \infty.$$

Demostración. Como $x \in P - \{0\}$ y $P \cap \tilde{K} = \{0\}$, entonces $x \notin \tilde{K}$, en consecuencia x es trascendente sobre K y tenemos que $[F : K(x)] < \infty$. Para completar la prueba es suficiente mostrar que $x_1, \ldots, x_n$ son linealmente independientes sobre $K(x)$. Supongamos que existe una combinación lineal no trivial $\sum_{i=1}^{n} \varphi_i(x)x_i = 0$ con $\varphi_i(x) \in K(x)$. Supongamos que todos los $\varphi_i(x)$ son polinomios en x y que x no los divide a todos los $\varphi_i(x)$ (si los divide para todo i, se factoriza la mayor potencia de x que divida a $\varphi_i(x)$ y quedan como queremos). Tome $a_i := \varphi_i(0)$, el termino constante de $\varphi_i(x)$, y defina $j \in \{1, \ldots, n\}$ con la condición de $a_j \neq 0$ pero $a_j = 0$ para todo $i > j$, obtenemos

$$-\varphi_j(x)x_j = \sum_{i \neq j} \varphi_i(x)x_i, \tag{16}$$

con $\varphi_i(x) \in \mathcal{O}$ para $i = 1, \ldots, n$ (dado $x = x_1 \in P$), $x_i \in x_j P$ para $i < j$ y $\varphi_i(x) = xg_i(x)$ para $i > j$, donde $g_i(x)$ es un polinomio en x. Dividiendo la ecuación (16) por x_j obtenemos

$$-\varphi_j(x) = \sum_{i<j} \varphi_i(x)\frac{x_i}{x_j} + \sum_{i>j} g_i(x)\frac{x_i}{x_j}.$$

Es claro que todos los sumandos de la derecha pertenecen a P, por lo tanto $\varphi_j \in P$. Por otro lado, $\varphi_j(x) = a_j + xg_j(x)$ con $g_i(x) \in K[x] \subseteq \mathcal{O}$ y $x \in P$, así que $a_j = \varphi_j(x) - xg_j(x) \in P \cap K$, pero $a_j \neq 0$, lo que contradice el inciso 3 del Teorema (4.5) □

Teorema 4.7. *Sea $\mathcal{O}$ un anillo de valuación del cuerpo de funciones F/K y P su único ideal maximal, entonces:*

1. *P es principal.*

2. *Si $P = t\mathcal{O}$, entonces cada $z \in F - \{0\}$ tiene representación única en la forma $z = t^n u$, para algún $n \in \mathbb{Z}$ y $u \in U(\mathcal{O})$.*

3. *$\mathcal{O}$ es un dominio de ideales principales. ;ás precisamente, si $P = t\mathcal{O}$ e $I \subseteq \mathcal{O}$ es un ideal no nulo de $\mathcal{O}$, entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.*

Demostración.

1. Supongamos que P no es principal y sea $x \in P - \{0\}$. Dado que P no es principal, entonces $P \neq x_1\mathcal{O}$, donde $x = x_1$. En consecuencia, existe $x_2 \in P - x_1\mathcal{O}$. Es claro que $x_1^{-1}x_2 \notin \mathcal{O}$, caso contrario, $x_1^{-1}x_2 = w \in \mathcal{O}$, luego $x_2 = x_1 w \in \mathcal{O}$, lo que contradice la elección de x_2. Como $x_1^{-1}x_2 \notin \mathcal{O}$, por el Teorema (4.5), tenemos que $x_2^{-1}x_1 = (x_1^{-1}x_2)^{-1} \in P$ y así $x_1 \in x_2 P$.

   Ahora como P no es principal tenemos que $P \neq x_2\mathcal{O}$. Argumentando en la misma forma existe x_2 con $x_2 \in x_3 P$. Más aún, razonando de forma inductiva obtenemos una sucesión infinita $x_1, x_2, \ldots$ tal que para todo $i \in \mathbb{N}$, $x_i \in x_{i+1}P$, lo cual contradice el lema anterior.

2. Supongamos que $z \in \mathcal{O}$, si $z \in U(\mathcal{O})$, entonces $z = t^0 u$ con $u \in U(\mathcal{O})$, con lo cual se tiene la representación. Ahora si $z \notin U(\mathcal{O})$, entonces existe un $m \geq 1$ máximo tal que $z \in t^m\mathcal{O}$, dado que la longitud de la secuencia:

$$x_1 = z, x_2 = t^{m-1}, x_3 = t^{m-1}, \ldots, x_m = t,$$

   es acotada por el lema anterior. Escribiendo $z = t^m u$ con $u \in \mathcal{O}$, entonces u debe ser una unidad de $\mathcal{O}$.

3. Sea $\{0\} \neq I \subseteq \mathscr{O}$ es un ideal. El conjunto $A = \{r \in \mathbb{N} : t^r \in I\}$ es no vacío (si $0 \neq x \in I$, entonces $x = t^r u$ con $u \in \mathscr{O}$ y por lo tanto $t^r = xu^{-1} \in I$). Sea $n = min(A)$. Afirmaremos que $I = t^n\mathscr{O}$. La inclusión $I \supseteq t^n\mathscr{O}$ es trivial, dado que $t^n \in I$. Por otro lado, sea $0 \neq y \in I$. Luego $y = t^s w$ con $w \in U(\mathscr{O})$ y $s \geq 0$. Así $t^s \in I$ y $s \geq n$, y de esto concluimos que $y = t^n t^{s-n} w \in t^n\mathscr{O}$.

□

Definición 4.8. Un anillo con las propiedades del Teorema (4.7) es llamado anillo de **valuación discreta**.

Definición 4.9.

1. Un **lugar** P de un cuerpo de funciones algebraicas F/K es el ideal maximal de algún anillo de valuación $\mathscr{O}$ de F/K. Además cada elemento $t \in P$ tal que $P = t\mathscr{O}$ es llamado un **uniformizante** de P.

2. El conjunto de todos los lugares de F/K es denotado por $\mathbb{P}_F = \{P : P \text{ es un lugar de } F/K\}$.

Ejemplo 4.10. Considere el anillo de valuación $\mathscr{O}_{p(x)}$ definido en el Ejemplo (4.4), el lugar $P_{p(x)}$ dado por

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) | f(x), p(x) \nmid g(x) \right\}.$$

En efecto, primero veamos que $P_{p(x)}$ no tiene unidades. si $p(x) \nmid f(x)$ y $p(x) \nmid g(x)$, entonces $\frac{f(x)}{g(x)}$ y $g(x)/f(x)$ son unidad y están en $\mathscr{O}_{p(x)}$, por lo tanto si $p(x)|f(x)$, $\frac{f(x)}{g(x)}$ no es unidad, así $P_{p(x)}$ es ideal maximal.

Si $\mathcal{O}$ es un anillo de valuación de F/K y P es el ideal maximal, entonces $\mathcal{O}$ está determinado de forma única por P, dada por $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$.

Denotaremos por $\mathcal{O}_P$ el anillo de valuación del lugar P.

Definición 4.11. Una **valuación discreta** de F/K es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ que cumple las siguientes propiedades:

1. $v(x) = \infty$ si y solo si $x = 0$.
2. $v(xy) = v(x) + v(y)$, para todo $x, y \in F$.
3. $v(x+y) \geq \text{mín}\{v(x), v(y)\}$ para todo $x, y \in F$.
4. Existe $z \in F$ tal que $v(z) = 1$.
5. $v(a) = 0$ para todo $a \in K - \{0\}$.

En este contexto, el símbolo ∞ satisface:

$$\infty + n = \infty \text{ y } \infty > n, \text{ para todo } n \in \mathbb{Z}.$$

Definición 4.12. A cada lugar $P \in \mathbb{P}_F$ le asociamos una función

$$v_P : F \to \mathbb{Z} \cup \{\infty\}$$

que es una valuación discreta en la siguiente forma:

Si t es un uniformizante local de P, entonces cada $z \in F - \{0\}$ tiene representación única en la

forma $z = t^n u$, donde $n \in \mathbb{Z}$ y $u \in U(\mathcal{O}_P)$, definimos

$$v_P(z) = n \text{ y } v_P(0) = \infty.$$

Teorema 4.13. *Sea F/K un cuerpo de funciones.*

1. *Para un lugar $P \in \mathbb{P}_F$, la función v_P definida en (4.12) es una valuación discreta de F/K, además:*

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\},$$
$$U(\mathcal{O}_P) = \{z \in F : v_P(z) = 0\},$$
$$P = \{z \in F : v_P(z) > 0\}.$$

2. *Cada $x \in F$ es un uniformizante local de P si y solo si $v_P(x) = 1$.*

3. *Recíprocamente, supongamos que v es una valuación discreta de F/K, entonces el conjunto $P = \{z \in F : v(z) > 0\}$ es un lugar de F/K y $\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\}$ es su correspondiente anillo de valuación.*

4. *Cada anillo de valuación $\mathcal{O}$ es un subanillo maximal propio de F.*

Demostración.

1. De la definición de v_P es claro que $v_P(x) = \infty$ si y solo si $x = 0$.

   Si $x = 0$ o $y = 0$, es claro que $v_P(xy) = \infty = v_P(x) + v_P(y)$. Si $x \neq 0 \neq y$, entonces $x = t^n u$,

$y = t^m w$, donde $n, m \in \mathbb{Z}$ y $u, w \in U(\mathcal{O}_P)$. Ahora $xy = t^{m+n}uw$, entonces $v_P(xy) = m+n = v_P(x) + v_P(y)$.

Si $x = 0$ o $y = 0$, es claro que $v_P(x+y) \geq \text{mín}\{v_P(x), v_P(y)\}$.

Si $x \neq 0 \neq y$, tomamos $x = t^n u$, $y = t^m w$, como se tomó anteriormente. Supongamos que $n \leq m < \infty$. Tenemos

$$x + y = t^n \left(u + t^{m-n} w\right) = t^n z,$$

si $z = 0$, entonces $v_P(x+y) = v_P(0) = \infty > \text{mín}\{v_P(x), v_P(y)\}$. Si $z \neq 0$, tenemos que $z = t^s q$, con $s \in \mathbb{Z}$ y $q \in U(\mathcal{O}_P)$, además $s \geq 0$ y que $z \in \mathcal{O}_P$.

$$v_P(x+y) = v_P(t^n z) = v_P(t^{s+n} q) = n + s \geq n = \text{mín}\{m, n\}.$$

Como $t = t^1 1$, donde $1 \in U(\mathcal{O}_P)$, entonces $v_P(t) = 1$. Si $a \in K - \{0\}$, entonces $a \in U(\mathcal{O})$ y como $a = t^0 a$, por lo tanto $v_P(a) = 0$. Así v_P es una valuación discreta.

Veamos que $U(\mathcal{O}_P) = \{z \in F : v_P(z) = 0\}$. Sea $z \in F$, entonces $z \in U(\mathcal{O}_P)$ si y solo si $z = t^0 z$ si y solo si $v_p(z) = 0$.

Probemos que $P = \{z \in F : v_P(z) > 0\}$. Si $z \in P = r\mathcal{O}_P$, entonces $z = t x_1$, donde $x_1 \in \mathcal{O}_P$. Si $x_1 \in U(\mathcal{O}_P)$, entonces $v_P(z) = 1 > 0$. Si $x_1 \notin U(\mathcal{O}_P)$, entonces $x_1 \in \mathcal{O}_P - U(\mathcal{O}_P) = P$, así $x_1 = t x_2$, $x_2 \in \mathcal{O}_P$, entonces $z = t^2 x_2$ repitiendo el mismo proceso para x_2. Después de un número finito de pasos llegaremos a $z = t^n x_n$, donde $x_n \in U(\mathcal{O}_P)$, $n \in \mathbb{N}$, entonces $v_P(z) = n > 0$.

Ver $\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\}$ es claro, dado que $\mathcal{O}_P = U(\mathcal{O}_P) \cup P$.

2. Si $x \in F$ es un uniformizante local de P, entonces $P = x\mathcal{O}_P$ y como $x = x \cdot 1 = 1 \cdot x$, donde $1 \in U(\mathcal{O}_P)$, entonces $v_P(x) = 1$.

   Recíprocamente Supongamos que $v_P(x) = 1$ y veamos que $P = x\mathcal{O}_P$. Sea t tal que $P = t\mathcal{O}_P$, como $v_P(x) = 1$, entonces $x = tu$, donde $u \in U(\mathcal{O}_P)$.

   Si $z \in P$, entonces

$$\begin{aligned} z &= t^n w, w \in U(\mathcal{O}_P), \\ &= x^n \left(u^{-n} w\right), \\ &= x\left(x^{n-1} u^{-n} w\right) \in x\mathcal{O}_P. \end{aligned}$$

   Entonces $P \subseteq x\mathcal{O}_P$.

   Si $y \in x\mathcal{O}_P$, entonces $y = xa$, con $a \in \mathcal{O}_P$. Luego $y = (tu)a = t(ua) \in t\mathcal{O}_P = P$, así $x\mathcal{O}_P \subseteq P$, que es lo que queríamos probar.

3. Sea v una valuación discreta de F/K y consideremos los conjuntos

$$P = \{z \in F : v(z) \geq 0\} \text{ y } O_P = \{z \in F : v(z) \geq 0\}.$$

   Entonces $\mathcal{O}_P$ un anillo de valuación de F/K. En efecto, como $\mathcal{O}_P \subseteq F$, es suficiente mostrar $\mathcal{O}_P$ es un subanillo de F. Si $x, y \in \mathcal{O}_P$, entonces $v(x) \geq 0$ y $v(y) \geq 0$ y $v(xy) = v(x) + v(y) \geq 0$. Luego $xy \in \mathcal{O}_P$. Como $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$, entonces $x+y \in \mathcal{O}_P$. Ahora, para todo $a \in K - \{0\}$, $v(a) = 0 \geq 0$ y $v(0) = \infty$ y así $K \subseteq \mathcal{O}_P$, existe $t \in F$ tal que $v(t) = 1 \geq 0$ así

$t \in \mathcal{O}_P - K$, así $\mathcal{O}_P \subsetneq K$. Sea $z \in F$ tal que $z \notin \mathcal{O}_P$, entonces $v(z) < 0$ y $v(z^{-1}) > 0$ y así $z^{-1} \in \mathcal{O}_P$, es decir $\mathcal{O}_P$ es un anillo de valuación.

$P = \{z \in F : v(z) \geq 0\}$ es un ideal de $\mathcal{O}_P$. En efecto, sean $x, y \in P$, entonces $v(x) > 0$ y $v(y) > 0$, por lo tanto $v(xy) > 0$ y $v(x+y) > 0$, además tenemos que $v(-x) = v(x) > 0$, es decir $-x \in P$. Si $x \in P$ y $r \in \mathcal{O}_P$, entonces $v(rx) = v(r) + v(x) > 0$.

Falta ver que P es ideal maximal de $\mathcal{O}_P$, para esto es suficiente mostrar que $P = \mathcal{O}_P - U(\mathcal{O}_P)$, lo que es equivalente a probar que $U(\mathcal{O}_P) = \{z \in \mathcal{O}_P : v(z) = 0\}$.

Si $z \in U(\mathcal{O}_P)$, entonces existe $w \in \mathcal{O}_P$ tal que $zw = 1$ y tenemos que $0 = v(1) = v(zw) = v(z) + v(w)$, despejando $v(z) = -v(w) \leq 0$ y como $v(w) \leq 0$ y $w \in \mathcal{O}_P$, entonces $v(z) = 0$.

Recíprocamente, si $z \in \mathcal{O}_P$ y $v(z) = 0$, entonces $z \neq 0$. Luego existe $y \in F$ tal que $xy = 1$, así $v(xy) = 0 = v(x) + v(y)$, por lo tanto $v(y) = 0$ y $y \in \mathcal{O}_P$ es decir $x, y \in U(\mathcal{O}_P)$.

4. Sean $\mathcal{O}$ un anillo de valuación de F/K, P su ideal maximal y v_P la valuación discreta asociada a P. Considere $z \in F - \{0\}$, Como $z \in F$ y $\mathcal{O} \subseteq F$, entonces $\mathcal{O}[z] \subseteq F$. Teniendo que $z \notin \mathcal{O}$, se tiene que $v_P(z) < 0$, así que para cada $k \in \mathbb{Z}^+$ y así $v_P(z^{-k}) = kv_P(z^{-1}) > 0$. Ahora $v_P(yz^{-k}) = v_P(y) + v_P(z^{-k}) > 0$ para $y \in F$ fijo y k lo suficientemente grande tenemos que $kv_P(yz^{-1}) > 0$, es decir, $yz^{-k} \in P \subseteq \mathcal{O}$, por lo tanto $y = wz^k \in \mathcal{O}[z]$ y así $F = \mathcal{O}[z]$ para todo $z \in F - \mathcal{O}$.

   Sea A un subanillo de F tal que $\mathcal{O} \subsetneq A \subseteq F$. Entonces existe $x \in A - \mathcal{O}$ y como $z \in F - \mathcal{O}$ y $A[x] = A$. Luego $F = \mathcal{O}[x] \subseteq A[x] \subseteq F[x] = F$, es decir $A = F$.

□

El resultado anterior nos muestra que lugares, anillos de valuación y valuaciones discretas de un cuerpo de funciones algebraicas son esencialmente las misma cosa.

Definición 4.14. Sea $P \in \mathbb{P}_F$.

1. Definimos el **cuerpo de clases residuales** $F_P := \mathcal{O}_P/P$ de P. Simplificaremos la notación de la siguiente forma $x(P) := x + P$ para $x \in \mathcal{O}_P$.

   La aplicación

$$\begin{aligned} F \to & \quad F_P \cup \{\infty\}, \\ x \mapsto & \begin{cases} x(P) \text{ si } x \in \mathcal{O}_P, \\ \infty \text{ si } x \notin \mathcal{O}_P, \end{cases} \end{aligned}$$

   de F en $F_P \cup \{\infty\}$ se llama **aplicación de clases residuales** de P.

2. $\text{grad}(P) = [F_P : K]$ se llama el grado del lugar P, el cual siempre es finito.

Definición 4.15. Sea $z \in F$ y $P \in \mathbb{P}_F$.

1. Decimos que P es un **cero** de z si $v_P(z) > 0$.

2. Decimos que P es un **polo** de z si $v_P(z) < 0$.

Si $v_P(z) = m > 0$ $(v_P(z) = -m < 0)$, diremos que P es un cero (o un polo) de z de orden m, respectivamente.

4.2. Cuerpos de funciones racionales

Como dice el título, nos enfocaremos en los cuerpos de funciones racionales, es decir, el caso $F = K(x)$, donde x es trascendente sobre K, esto se hará con el fin de entender las definiciones dadas anteriormente. Presentamos a continuación un ejemplo concreto y simple. En el se presentan de manera precisa los conceptos de valuaciones, lugares, entre otros.

Ejemplo 4.16. Dado un polinomio mónico e irreducible $p(x) \in K[x]$, consideremos el anillo de valuación

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}, \tag{17}$$

de $K(x)/K$ con ideal maximal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) | f(x), p(x) \nmid g(x) \right\}. \tag{18}$$

En el caso particular cuando $p(x)$ sea lineal, es decir, $p(x) = x - \alpha$ con $\alpha \in K$, se escribirá

$$P_\alpha = P_{x-\alpha} \in \mathbb{P}_{K(x)}.$$

Este anillo y su lugar ya fueron mostrados anteriormente en lo Ejemplos (4.4) y (4.10). Hay otro anillo de valuación de $K(x)/K$, definido

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \text{grad}(f(x)) \leq \text{grad}(g(x)) \right\}, \tag{19}$$

y su ideal maximal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \text{grad}(f(x)) < \text{grad}(g(x)) \right\}. \tag{20}$$

Para $\mathcal{O}_\infty$ es claro que $K \subsetneq \mathcal{O}_\infty \subsetneq K(x)$, si se tiene que para $\frac{f(x)}{g(x)} \in K(x)$ que $\text{grad}(f(x)) > \text{grad}(g(x))$, entonces $\frac{g(x)}{f(x)}$ si pertenece a $\mathcal{O}_\infty$, por lo tanto $\mathcal{O}_\infty$ es un anillo de valuación.

Veamos que P_∞ no tiene unidades, si $\frac{f(x)}{g(x)}$ con $\text{grad}(f(x)) < \text{grad}(g(x))$, entonces el inverso $\frac{g(x)}{f(x)}$ no está en P_∞, por lo tanto y P_∞ es ideal maximal.

Teorema 4.17. *Sea $F = K(x)$ el cuerpo de funciones racionales.*

1. *Sea $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ el lugar definido en la ecuación (18), donde $p(x) \in K[x]$ es un polinomio irreducible y mónico. Entonces $p(x)$ es un elemento primo para P, y su correspondiente valuación v_P puede ser descrita de la siguiente manera:*
   Si $z \in K(x) - \{0\}$ escrito de la forma $z = p(x)^n \left(\frac{f(x)}{g(x)} \right)$ con $n \in \mathbb{Z}$, con $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ y $p(x) \nmid g(x)$, entonces $v_P(z) = n$. El cuerpo de clases residuales $K(x)_P = \mathcal{O}_P / P$ es isomorfo a $K[x]/(p(x))$ y el isomorfismo está dado por

$$K[x]/(p(x)) \to K(x)_P,$$

$$f(x) \mapsto f(x)(P).$$

   En consecuencia $\text{grad}(P) = \text{grad}(p(x))$.

2. *En el caso específico donde $p(x) = x - \alpha$ con $\alpha \in K$, el grado de $P = P_\alpha$ es uno y la*

aplicación de clases residuales está dado por

$$z(P) = z(\alpha) \text{ para } z \in K(x),$$

donde $z(\alpha)$ *es definido de la siguiente manera:*

Escriba $z = \frac{f(x)}{g(x)} \in K[x]$, *entonces*

$$z(\alpha) = \begin{cases} \frac{f(\alpha)}{g(\alpha)} & \text{si } g(\alpha) \neq 0, \\ \infty & \text{si } g(\alpha) = 0. \end{cases}$$

3. *Sea* $P = P_\infty$ *el lugar infinito de* $K(x)/K$ *definido en la ecuación (20), entonces* $\text{grad}(P_\infty) = 1$.

   Un elemento primo de P_∞ *es* $t = 1/x$ *y la valuación discreta correspondiente* v_∞ *está dada por*

   $$v_\infty\left(\frac{f(x)}{g(x)}\right) = \text{grad}(g(x)) - \text{grad}(f(x)),$$

   donde $f(x), g(x) \in K[x]$. *La aplicación de clases residuales correspondiente a* P_∞ *está definido por* $z(P_\infty) = z(\infty)$ *para* $z \in K(x)$, *donde* $z(\infty)$ *se define como:*

   Si

   $$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}, \text{ con } a_n, b_m \neq 0,$$

entonces

$$z(\infty) = \begin{cases} \frac{a_n}{b_m} & si\ n = m, \\ 0 & si\ n < m, \\ \infty & si\ n > m. \end{cases}$$

4. *K es el cuerpo de constantes de $K(x)/K$.*

Demostración.

1. Sea $P = P_{p(x)}$, $p(x) \in K[x]$ irreducible. El ideal $P_{p(x)} \subseteq \mathcal{O}_{p(x)}$ claramente es generado por $p(x)$, por lo tanto $p(x)$ es un elemento primo para P. Para demostrar la afirmación sobre el cuerpo de la clase de residuos consideramos el homomorfismo de anillos

$$\varphi : K[x] \to K(x)_P,$$
$$f(x) \mapsto \varphi(f(x)) = f(x)(P).$$

Así el kernel de φ es el ideal generado por $p(x)$. Además φ es sobreyectiva: Si $z \in \mathcal{O}_{p(x)}$, podemos escribir $z = u(x)/v(x)$ con $u(x), v(x) \in K[x]$ tal que $p(x) \nmid v(x)$. Luego existe $a(x), b(x) \in K[x]$ con $a(x)p(x) + b(x)v(x) = 1$, por lo tanto

$$z = 1 \cdot z = \frac{a(x)u(x)}{v(x)} p(x) + b(x)u(x),$$

y $z(P) = (b(x)u(x))(P)$ está en la imagen de φ. Así φ induce un isomorfismo ϕ de $K[x]/(p(x))$

sobre $K(x)_P$.

2. Sea $P = P_\alpha$ con $\alpha \in K$. Si $f(x) \in K[x]$, entonces $(x-\alpha)|(f(x)-f(\alpha))$, por lo tanto $f(x)(P) = (f(x)-f(\alpha))(P) + f(\alpha)(P) = f(\alpha)$. Tomemos $z \in \mathcal{O}_P$ de forma arbitraria, que podemos reescribirlo como $z = \frac{f(x)}{g(x)}$ donde $f(x), g(x) \in K[x]$ y $(x-\alpha) \nmid g(x)$, por lo tanto $g(x)(P) = g(\alpha) \neq 0$ y
$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

3. Veamos que $1/x$ es un elemento primo para P_∞. Claramente tenemos que $1/x \in P$. Considere un elemento $z = \frac{f(x)}{g(x)} \in P_\infty$, es decir $\text{grad}(f(x)) < \text{grad}(g(x))$, entonces
$$z = \frac{1}{x}\frac{xf(x)}{g(x)}, \text{ así } \text{grad}(xf(x)) \leq \text{grad}(g(x)).$$
Esto prueba que $z \in (1/x)\mathcal{O}_\infty$, por lo tanto $1/x$ genera el ideal P_∞, es decir, es un elemento primo de P_∞.

4. Escojamos un lugar P de $K(x)/K$ de grado uno, por ejemplo $P = P_\alpha$ con $\alpha \in K$. El cuerpo de constantes $\tilde{K}$ de $K(x)$ está contenido en el cuerpo de clases residuales $K(x)_P$, por lo tanto $K \subseteq \tilde{K} \subseteq K(x)_P = K$.

□

Teorema 4.18. *No existen otros lugares del cuerpo de funciones racionales $K(x)/K$ distintos de $P_{p(x)}$ y P_∞.*

Demostración. Sea P un lugar de $K(x)/K$. Se tiene dos casos.

Caso 1. Supongamos que $x \in \mathcal{O}_P$, entonces $K[x] \subseteq \mathcal{O}_P$ y el conjunto $I = K[x] \cap P$ es un ideal de $K[x]$, de hecho es un ideal primo y además $I \neq \{0\}$. Luego existe un polinomio mónico irreducible $p(x) \in K[x]$ tal que $I = K[x] \cap P = p(x)K[x]$. Cada $g(x) \in K[x]$ con $p(x) \nmid g(x)$ no está en I, entonces no está en P y $1/g(x) \in \mathcal{O}_P$, de lo que se concluye que

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P.$$

Como los anillos de valuación son subanillos propios maximales de $K(x)$, tenemos que $\mathcal{O}_P = \mathcal{O}_{p(x)}$.

Caso 2. Si $x \notin \mathcal{O}_P$, entonces $x^{-1} \in \mathcal{O}_P$ y como $K \subseteq \mathcal{O}_P$, por lo tanto $K\left[x^{-1}\right] \subseteq \mathcal{O}_P$, $x^{-1} \in P \cap K\left[x^{-1}\right]$ y $P \cap K\left[x^{-1}\right] = x^{-1}K\left[x^{-1}\right]$. Como en el Caso 1,

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} : f(x^{-1}), g(x^{-1}) \in K\left[x^{-1}\right], x^{-1} \nmid g(x^{-1}) \right\}, \\
&= \left\{ \frac{a_0 + \cdots + a_n x^{-n}}{b_0 + \cdots + b_m x^{-m}} : b_0 \neq 0 \right\}, \\
&= \left\{ \frac{a_0 x^{m+n} + \cdots + a_n x^m}{b_0 x^{m+n} + \cdots + b_m x^n} : b_0 \neq 0 \right\}, \\
&= \left\{ \frac{u(x)}{v(x)} : u(x), v(x) \in K[x], \operatorname{grad}(u(x)) < \operatorname{grad}(v(x)) \right\}, \\
&= \mathcal{O}_\infty.
\end{aligned}$$

Así $\mathcal{O}_P = \mathcal{O}_\infty$ y $P = P_\infty$. □

Corolario 4.19. *Los lugares de $K(x)/K$ de grado uno están en correspondencia con $K \cup \{\infty\}$.*

Este resultado es inmediato del teorema anterior y que los únicos lugares de grado uno de

$K(x)/K$ son P_∞ y P_α con $\alpha \in K$.

4.3. Cuerpos de funciones ciclotómicos

Primero recordemos unas propiedades de la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Proposición 4.20. *El cuerpo $\mathbb{Q}(\zeta_n)$ es una extensión de Galois de $\mathbb{Q}$, donde ζ_n es la raíz n-ésima de la unidad; $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$ y $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ es isomorfo al grupo de las unidades $U_n = U(\mathbb{Z}_n)$ de $\mathbb{Z}_n$.*

Demostración. Ver Capítulo V de Grillet (2007). □

Este resultado se usará más adelante.

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos, donde $q = p^n$ y $p, n \in \mathbb{Z}^+$ con p primo. Denotemos por $R_T = \mathbb{F}_q[T]$ el anillo de polinomios con variable T sobre $\mathbb{F}_q$ y $K = \mathbb{F}_q(T)$, el cuerpo de fracciones de F, es decir, el cuerpo de funciones algebraicas en la variable T. Denotemos por $\overline{K} = \overline{\mathbb{F}_q(T)}$ la clausura algebraica de K. Un $\mathbb{F}_q$ - endomorfismo sobre $\overline{K}$ es una función $\varphi : \overline{K} \to \overline{K}$ tal que para cada $a, b \in \overline{K}$ y $\alpha \in \mathbb{F}_q$:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

y

$$\varphi(\alpha a) = \alpha\varphi(a).$$

Sea

$$A = \mathrm{End}_{\mathbb{F}_q}(\overline{K}) = \left\{\varphi : \overline{K} \to \overline{K} : \varphi \text{ un } \mathbb{F}_q \text{ - endomorfismo sobre } K\right\},$$

donde A es $\mathbb{F}_q$ - espacio vectorial.

Ejemplo 4.21. En particular $\varphi \in A$ definido por:

$$\begin{aligned} \varphi \quad &: \quad \overline{K} \to \overline{K} \\ &\qquad u \mapsto u^q \end{aligned}$$

es un homomorfismo conocido como **automorfismo de Fröbenius**.

φ es un homomorfismo. En efecto, si $r, s \in K$, entonces

$$\varphi(rs) = (rs)^q = r^q s^q = \varphi(r)\varphi(s)$$

y $\varphi(r+s) = (s+r)^q$ como los elementos de K tienen orden p primo, entonces $(s+r)^q = s^q + r^q$, así $\varphi(r+s) = \varphi(r) + \varphi(s)$, por lo tanto $\varphi \in A$.

Ejemplo 4.22. Definimos:

$$\begin{aligned} \mu_T \quad &: \quad \overline{K} \to \overline{K} \\ &\qquad u \mapsto \mu_T(u) = Tu, \end{aligned}$$

entonces $\mu_T \in A$.

Sea $f(T) \in R_T$. Definiendo la sustitución $T \to \varphi + \mu_T$ en f, da un elemento de A. Es decir,

si $f(T) = a_n T^n + \cdots + a_1 T + a_0$, entonces

$$f(\varphi + \mu_T)(u) = a_n(\varphi + \mu_T)^n + \cdots + a_1(\varphi + \mu_T)(u) + a_0(u),$$

para todo $u \in \overline{K}$. Es fácil ver que $\chi : R_T \to A$ definido por $\chi(f(T)) = f(\varphi + \mu_T)$ es un homomorfismo de anillos y así $\overline{K}$ es dotado de una estructura de R_T-módulo.

Tenemos que

$$(\varphi \circ \mu_T)(u) = \varphi(Tu) = T^q u^q,$$

$$(\mu_T^q \circ \varphi)(u) = \mu_T^q(u^q) = T^q u^q,$$

por lo tanto

$$\varphi \circ \mu_T = \mu_T^q \circ \varphi,$$

pero en general $\varphi \circ \mu_T \neq \mu_T \circ \varphi$.

Si $u \in \overline{K}$ y $M \in R_T$ se denota:

$$u^M := M(\varphi + \mu_T)(u) = M \circ u.$$

Note que si $\alpha \in \mathbb{F}_q$ y $u \in \overline{K}$, entonces $u^\alpha = \alpha u$.

Además, para cada $u \in \overline{K}$ y $M, N \in R_T$, se tiene:

$$u^{M+N} = u^M + u^N$$

y

$$u^{MN} = \left(u^M\right)^N.$$

Lo anterior se relaciona con los cuerpos ciclotómicos como se indica a continuación:

$\mathbb{Z}$ actúa como grupo sobre $U\left(\overline{\mathbb{Q}}\right) = \overline{\mathbb{Q}} - \{0\} = \mathbb{C} - \{0\}$ de la siguiente manera, para $n \in \mathbb{Z}^+$ y $u \in U\left(\overline{\mathbb{Q}}\right)$, tenemos que $nu = u^n$: Los cuerpos numéricos ciclotómicos corresponden a $\{u \in U\left(\overline{\mathbb{Q}}\right)\} = \{\zeta_n^a\}_{a=0}^{n-1}$, donde $\zeta_n = e^{\frac{2\pi i}{n}}$.

Con el siguiente diagrama vemos la semejanza entre estos conjuntos y su comportamiento.

$$\begin{array}{ccc} \overline{\mathbb{Q}} & & \\ | & & \\ \mathbb{Q} & \text{——} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} \overline{K} & & \\ | & & \\ K = \mathbb{F}_q(T) & \text{——} & R_T = \mathbb{F}_q[T] \end{array}$$

En este caso $R_T = \mathbb{F}_q[T]$ actúa sobre $\overline{K}$ por exponenciación: Para $M \in R_T$ y $u \in \overline{K}$, tenemos que $M \circ u = u^M$. Los cuerpos de funciones ciclotómicas corresponderán a $\{u \in \overline{K}_u^M = 0\}$.

Definición 4.23. Sea $M \in R_T$, definimos

$$\Lambda_M = \left\{u \in \overline{K} : u^M = 0\right\}$$

como el conjunto de ceros de u^M (polinomio en u), Λ_M es llamado **módulo de Carlitz-Hayes** de M.

Proposición 4.24. *Para $M \in R_T$, Λ_M es un R_T-submódulo de $\overline{K}$.*

Demostración. Ver Capítulo 12 de Salvador (2006). □

Observación 4.25. Como R_T es un anillo conmutativo, si $u \in \overline{K}$ y $N \in R_T$, tenemos

$$u^M = M \circ u,$$

y dado que

$$M \circ u^N = (u^N)^M = u^{NM} = (u^M)^N = 0^N = 0.$$

Más aún:

Sobre $\mathbb{Q}$ tenemos que $\Lambda_n = \left\{\xi \in U\left(\overline{\mathbb{Q}}\right) : \xi^n = 1\right\} = W_n \cong \prod_{i=1}^{n} W_{p_i}^{\alpha_i}$, donde $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $p_1, \dots, p_r$ son primos y W_s denota el grupo de las n-ésimas raíces de la unidad, así Λ_n es $\mathbb{Z}$-cíclico.

Se podría pensar que lo mismo ocurre sobre $\overline{K}$, es decir

$$\Lambda_M = \left\{u \in \overline{K} : u^M = 0\right\} \cong \prod_{i=1}^{r} \Lambda_{P_i}^{\alpha_i},$$

donde $M = \prod_{i=1}^{r} P_i^{\alpha_i}$, $P_1, \dots, P_r$ son polinomios irreducibles en R_T y Λ_M es R_T-cíclico.

Definición 4.26. Para $M \in R_T - \{0\}$ el grupo $R_T/(M)$ se llama el grupo de las unidades y definimos

$$\Phi(M) = |U(R_T/(M))|.$$

Note que

$$\Phi(M) = \{N \in R_T : \text{mcd}(N,M) = 1 \text{ y } \text{grad}(N) < \text{grad}(M)\}.$$

Proposición 4.27. *Para $N, M \in R_T$:*

1. $\Phi(MN) = \Phi(M)\Phi(N)$ *si y solo si* $\text{mcd}(M,N) = 1$.

2. *Si $P \in R_T$ es irreducible sobre $\mathbb{F}_q$, entonces $\Phi(P) = q^d - 1$, donde $d = \text{grad}(P)$, más aún, para $n \in \mathbb{Z}^+$*

$$\Phi(P^n) = |R_T/(P^{n-1})|\Phi(P) = q^{nd} - q^{(n-1)d}.$$

Demostración. Ver Capítulo 12 de Salvador (2006). □

Definición 4.28. Sea $M \in R_T - \{0\}$, el cuerpo de $K(\Lambda_M)$ definido como la menor extensión de K que contiene a K y Λ_M, o equivalentemente, el cuerpo generado al adjuntarle Λ_M a K, es llamado **cuerpo de funciones ciclotómico** determinado por M sobre K.

Como vimos en la Proposición (4.20), tenemos el siguiente resultado, que es análogo para los cuerpos de funciones.

Proposición 4.29. ***Propiedades de*** $K(\Lambda_M)$

1. *$K(\Lambda_M)/K$ es una extensión de Galois.*

2. *El grupo G_M es un subgrupo de $U(R_T/(M))$. En particular $K(\Lambda_M)/K$ es una extensión*

abeliana y

$$[K(\Lambda_M) : K] \leq \Phi(M) = |U(R_T/(M))|$$

Demostración. Para simplificar la notación, denotaremos por A mód M al residuo que se obtiene al dividir A por M.

1. Dado que $\Lambda_M \cong R_T/(M)$, que es R_T- módulo cíclico generado por λ, tenemos que

$$\lambda^{R_T} = \Lambda_M = \left\{\lambda^A : A \in R_T\right\},$$

entonces $K(\Lambda_M) = K(\lambda)$. En efecto, cualquier elemento $\xi \in \Lambda_M$ es de la forma λ^A para algún $A \in R_T$ y

$$\xi = A(\mu_T + \varphi)(\lambda) \in K(\lambda^q, \{T^S\lambda\}) = K(\lambda).$$

Finalmente, dado que $K(\Lambda_M)$ es el cuerpo de descomposición del polinomio separable $F(u) = u^M \in K[u]$, se sigue que $K(\Lambda_M)/K$ es una extensión de Galois.

2. Dado que $K(\Lambda_M) = K(\lambda)$, un elemento $\sigma \in G_M$ es determinado por su acción sobre λ. Ahora $\sigma\lambda$ es un conjugado de λ, entonces $\sigma(\lambda) \in \Lambda_M$ y $\sigma(\lambda) = \lambda^A$ para algún $A \in R_T$. Veamos que $\sigma\lambda$ es un generador de Λ_M.

   Si $\xi \in \Lambda_M$, entonces $\sigma^{-1}(\xi) \in \Lambda_M$, entonces $\sigma^{-1}(\xi) = \lambda^B$ para algún $B \in R_T$, por lo tanto $\xi = (\sigma\lambda)^B$ y tenemos que $\sigma\lambda$ es generador de Λ_M y se sigue que $\text{mcd}(A, M) = 1$. Así A mód $M \in U(R_T/(M))$. Para ver que A no depende de λ, sea λ_1 otro generador de Λ_M,

suponga que $\lambda_1 = \lambda^B$ para algún $B \in R_T$, entonces

$$\sigma\lambda_1 = \sigma(\lambda^B) = \sigma(\lambda)^B = \lambda^{AB} = (\lambda^B)^A = \lambda_1^A.$$

Ahora, si $\sigma(\lambda) = \lambda^A = \lambda^{A_1}$, tenemos que $\lambda^{A-A_1} = 0$, así $A - A_1 \in (M)$ y $A \equiv A_1 \,(\text{mód } I)$.

Defina $\theta : G_M \to U(R_T/(M))$ dado por $\sigma \mapsto A \,\text{mód}\, M$, donde $\sigma\lambda = \lambda^A$. Si $Psi \in G_M$, tenemos que $\Psi(\lambda) = \lambda^B$ y $(\Psi \circ \sigma)(\lambda) = \Psi(\lambda^A) = \lambda AB$. Por lo tanto $\theta(\Psi\sigma) = AB \,\text{mód}\, M = \theta(\Psi)\theta(\sigma)$, así θ es un homomorfismo de grupos.

Finalmente, si $\theta(\sigma) = 1 \,\text{mód}\, M$, tenemos que $\sigma \in \text{Ker}\theta$ y $\sigma\lambda = \lambda^1 = \lambda$, entonces σ es el homomorfismo identidad. Lo que sigue que

$$G_M \subseteq U(R_T/(M)) \text{ y } |G_M| = [K(\Lambda_M) : K] \leq |U(R_T/(M))| = \Phi(M).$$

Dado que $U(R_T/(M))$ es abeliano, G_M también lo es.

□

Definición 4.30. Sea $S \in R_T$ mónico, se define el S**-polinomio ciclotómico** o **polinomio ciclotómico respecto a** S como

$$\Psi_S(u) = \prod_{\substack{\text{mcd}(B,S)=1 \\ \text{grad}(B)<\text{grad}(S)}} \left(u - \lambda_S^B\right),$$

donde λ_S es un generador de Λ_M.

Se tiene:

Proposición 4.31. *Para $S \in R_T$ mónico.*

1. $\Psi_S(u) \in K(\Lambda_M)[u]$, *más aún* $\Psi_S(u) \in K[u]$.

2. *Si $M, N \in R_T$ son polinomios mónicos distintos, entonces*

$$\operatorname{mcd}(\Psi_M(u), \Psi_N(u)) = 1.$$

3. *Sea M mónico,*

$$u^M = \prod_{\substack{N|M \\ N \text{ mónico}}} \Psi_N(M).$$

4. $\Psi_M(u) = \prod_{N|M} \left(u^N\right)^{\mu(M/N)}$ *con N mónico, donde*

$$\mu(D) = \begin{cases} 1 & \text{si } D = 1, \\ (-1)^s & \text{si } D = P_1 \cdots P_s, \text{ donde } P_1, P_2, \ldots, P_s \text{ son} \\ & \text{polinomios monicos irreducibles distintos en } R_T, \\ 0 & \text{otro caso,} \end{cases}$$

   y M es un polinomio mónico.

5. *Si $P \in R_T$ es mónico e irreducible y $M = P^n$ con $n \in \mathbb{Z}^+$, entonces*

$$\Psi_{P^n}(u) = \frac{u^{P^n}}{u^{P^{n-1}}},$$

por lo tanto $\Psi_{P^n}(u) \in R_T$ *es irreducible.*

Demostración. Ver Capítulo 12 de Salvador (2006). □

Recordando los Teoremas (2.9),(2.13) y (2.15), vemos que tienen una forma similar a los incisos $3, 4$ y 5, esto nos permite ver que se comportan de forma similar al relacionarlos con la función μ y con algunos resultados ya conocidos en los polinomios ciclotómicos.

Referencias Bibliográficas

Akhtar, R. (1995). Cyclotomic euclidean number fields. *Senior Thesis, Harvard Univ*, 20.

Apostol, T. M. (1970). *Resultants of cyclotomic polynomials*, volume 24.

Apostol, T. M. (1998). *Introduction to analytic number theory*. Springer Science & Business Media.

Atiyah, M. F. (2020). *Introducción al álgebra conmutativa*. Reverté.

Chadid, I. C. and Caicedo, J. F. (1987). *Temas de teoría de cuerpos, teoría de anillos y numeros algebraicos*, volume 2. Univ. Nacional de Colombia.

Gallian, J. (2012). *Contemporary abstract algebra*. Nelson Education.

Grillet, P. A. (2007). *Abstract algebra*, volume 242. Springer Science & Business Media.

Hungerford, T. W. (2012). *Abstract algebra: an introduction*. Nelson Education.

Jameson, G. (2010). The cyclotomic polynomials.

Lezama, O. (2020). *Cuadernos de algebra*.

Montgomery, H. L. and Masley, J. M. (1976). Cyclotomic fields with unique factorization. *Journal für die reine und angewandte Mathematik*, 1976(286-287):248–256.

Motzkin, T. (1949). The euclidean algorithm. *Bulletin of the American Mathematical Society*, 55(12):1142–1146.