Trabajo fin de grado

POLINOMIOS CICLOTÓMICOS

Pedro Félez Moliner

Índice

1 Survey

Our main goal in this essay is studying the cyclotomic polynomials. First of all, we are going to define these polynomials and the roots of the unit. After that, we are going to study the field extensions of these polynomials, we will show some examples, and we are going to finish giving an idea of the famous Kronecker-Weber theorem.

Let $n \in \mathbb{N}$, it is said that ξ is a nth *root of the unit* on the field K, if it is a root of the polynomial $x^n - 1_K$, that is to said, $\xi^n = 1_K$. And ξ is *primitive*, if n is the lower number that meet $\xi^n = 1_K$.

It is easy to prove, that the set of all nth roots of the unit is a group, and if ξ is nth primitive root of the unit, then ξ is a generator of the group, and we can write it like:

$$G = \{\xi,\ \xi^2, \ldots,\ \xi^{n-1},\ 1\}$$

If the characteristic of the field K divides n, then all elements of K are nth roots of the unit. So in our study, we are going to suppose that the characteristic of the field K do not divide n.

It is said, that $\phi_n(x)$ is the nth *cyclotomic polynomial*, if ϕ_n is a monic polynomial, and its roots are the nth primitive roots of the unit.

Before continuing studying cyclotomic polynomials, we are going to remember some facts on Galois theory.

F is a *field extension* of the field K, if F is a field and $K \subseteq F$. F is a K vector field, whose dimension is called *degree of the extension*, and written as $|F : K|$.

F is a *splitting field* of the polynomial f on K, if $f = a(x-a_1)\ldots(x-a_k)$, and $F = K(a_1, \ldots,\ a_k)$. It is also said that F is a *normal extension* of K.

If F is a field extension of K, then the *Gaolis group* of the extension is the group:

$$Gal(F/K) = \{\sigma : F \longrightarrow F \ \ isomorphism \mid \sigma(k) = k \ \ \forall\ k \in K\}$$

F is a *cyclotomic split field* over K of n order, if F is the split field of $x^n - 1$ over K. The definition of *Euler function* is to be remembered:

$$\varphi(n) = |\{m \in \mathbb{N} \mid m \leqslant n, \ \ (n, m) = 1\}|$$

After showing these concepts, we are ready to start studying the cyclotomic split field over K.

Theorem 1.1. *Let n be a positibe integer, F a cyclotomic extension of K of order n, then:*

- *$F = K(\xi)$, where ξ is a primitive nth root of unity.*

- *F is an abelian extension of dimension d, where $d \mid \varphi(n)$.*
- *$Aut_K F$ is isomorphic to a subgroup of order d of the multiplicative group of units of $\mathbb{Z}_n$.*

Now, as we know how the cyclotomic extensions are. We are going to see some characteristics of cyclotomic polynomials.

Theorem 1.2. *Let n be a positive integer, F a cyclotomic extension of K of order n, then:*

- *Degree of nth cyclotomic polynomial $\phi_n(x)$ is $\varphi(n)$.*
- *All coefficients of $\phi_n(x)$ lie in the prime subfield P of K.*
- $x^n - 1_K = \Pi_{d|n}\phi_d(x)$

Last point of this theorem gives a constructive way to calculate cyclotomic cyclotomic polynomials; $\phi_n(x) = \frac{x^n-1}{\Pi_{d|n}\phi_d(x)}$.

We have explained cyclotomic polynomials in a field without any restriction, the next example will show it over the field $\mathbb{Q}$.

Theorem 1.3. *Let F a cyclotomic extension of order n of the field $\mathbb{Q}$ of rational numbers and $\phi_n(x)$ the nth cyclotomic polynomial over $\mathbb{Q}$. Then:*

- *$\phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.*
- *$|F : \mathbb{Q}| = \varphi(n)$.*
- *$Gal(F/\mathbb{Q})$ is isomorphic to the multiplicative groupo of units in the ring $\mathbb{Z}_n$.*

As we have seen, the group of units in the ring $\mathbb{Z}_n$ is related with the Galois group of the cyclotomic extensions. For this reason, it is necessary to show some results about the set of units of $\mathbb{Z}_n$.

Hereagter, U_n denotes the units of $\mathbb{Z}_n$. The next result will allow us to find primitive roots in an easier way

Theorem 1.4. *An element $a \in U_n$ is a primitive root if and only if $a^{\frac{\phi(n)}{q}} \neq 1$ in U_n for each prime q dividing $\phi(n)$.*

The following theorem is useful, due to, it explains, when the group U_n is cyclic.

Theorem 1.5. *The group U_n is cyclic if and only if $n = 1,\ 2,\ 4,\ p^e$ or $2p^e$, where p is an odd prime.*

Before studying cyclotomic polynomial in $\mathbb{Z}_n$, we need to know, how the group of U_{2^e} is:

Theorem 1.6. *If $e \geq 3$, then $U_{2^e} = \{\pm 5^i \mid 0 \leq i < 2^{e-2}\}$.*

Now we can start our study of cyclotomic polynomials in $\mathbb{Z}_n$. First of all, we are going to find the roots of this polynomials, ($x^k \equiv 1 \mod n$) when the group of units of $\mathbb{Z}_n$ is cyclic, ($n = 1,\ 2,\ 4,\ p^e$ and $2p^e$, p an odd prime).

In this case, we have to find a primitive root g, after that, we can put x as a power of g, and we obtain equation; $g^{ik} \equiv 1 \equiv g^{\varphi(n)} \mod n$.

If we focus our attention in the exponent of the equation, we can transform it in a linear equation; $in \equiv \varphi(n) \equiv 0 \mod \varphi(n)$. Whose solutions are; $i_1, \ldots,\ i_s$, so the roots of the cyclotomic polynomial are; $g^{i_1}, \ldots,\ g^{i_s}$.

The next step is finding the roots of cyclotomic polynomials when $n = 2^e$ with $e \geqslant 3$.

In this case, as we have seen, all numbers of U_{2^e} can be written like $(\pm 5)^i,\ 0 \leqslant i \leqslant 2^{e-2}$. So we only have to write x and 1 like a power of ± 5, and after that, transform the equation in a linear equation, as we have done in the previous case.

We are ready to study the general case, when $n \in \mathbb{N}$. The first step is factor $n = p_1^{k_1} \ldots p_l^{k_l}$, and then, solve the equations: $x_1^k \equiv 1\ (p_1^{k_1}),\ \ldots\ , x_l^k \equiv 1 \mod p_l^{k_l}$. Making use of the Chinese remind theorem, we take $c_i,\ d_i$, which fulfill:

$$c_1 = \frac{n}{p_1^{k_1}},\ c_2 = \frac{n}{p_2^{k_2}},\ \ldots,\ c_l = \frac{n}{p_l^{k_l}}$$

$$c_1 d_1 \equiv 1 \mod p_1^{k_1}, \quad c_2 d_2 \equiv 1 \mod p_2^{k_2}, \quad \ldots\ , \quad c_l d_l \equiv 1 \mod p_l^{k_l}$$

Therefore, combining all the solutions x_i, we obtain the roots of the cyclotomic polynomial as follows:

$$x \equiv x_1 c_1 d_1 + \ \ldots\ + x_1 c_1 d_1 = \sum_{i=1}^{l} x_1 c_1 d_1 \mod n$$

The last part of this essay, is the study of Kronecker-Weber theorem:

Theorem 1.7. *Every abelian extension of $\mathbb{Q}$ is cyclotomic.*

The proof of the theorem is reduced to the case of extension, whose order is prime power p^k, and where p is the only ramified prime. Then is necessary separate two cases, when $p = 2$, and when p is an odd prime.

The importance of this result resides in the fact that it gathers many branches of Mathematics, like analysis, algebra, geometry and number theory, and it shows that all finite abelian groups exist as Galois groups over $\mathbb{Q}$. Furthermore, it explains how are the extensions over $\mathbb{Q}$.

2. Introducción

Los matemáticos árabes, fueron los primeros que se introdujeron en la búsqueda de soluciones de ecuaciones polinómicas. Desde entonces, los polinomios siempre han teniendo una gran importancia en las matemáticas, ya que nos permiten, crear funciones usando simplemente operaciones aritméticas.

A lo largo de la historia, muchos matemáticos han intentado dar con una fórmula que diera las raíces de los polinomios. Durante un gran periodo, la única conocida fue la de grado dos. Esto fue así, hasta la aparición de Cardano, y su estudiante Ferarri, quienes consiguieron encontrar las fórmulas para los polinomios de grado tres y cuatro.

Durante los siguientes 200 años, pese al gran empeño de los matemáticos, no se consiguió encontrar la fórmula para polinomios de grado igual o mayor que cinco. No se realizó ningún avance en este tema, hasta que Ruffini y Abel, demostraron que no existía dicha fórmula para los polinomios de grado cinco.

Por su parte, Galois con su desarrollo de álgebra abstracta, en lo que ahora se conoce como teoría de Galois, consiguió explicar cuándo un polinomio es resoluble y cuándo no. Al mismo tiempo con su teoría, consiguió responder problemas clásicos en geometría: como la cuadratura del círculo, la duplicación del cubo, la trisección del ángulo, o determinar exactamente, cuando un poligono regular de n lados, era posible construirlo con regla y compás.

El objetivo de este trabajo fin de grado es; en primer lugar estudiar los polinomios ciclotómicos y sus raíces; introduciendo así el tema que vamos a tratar. Luego, estudiaremos como son las extensiones de un cuerpo que contengan las raíces de estos polinomios; para lo que anteriormente, debemos introducir algunos resultados de teoría de Galois.

Una vez hayamos estudiado, estas extensiones sobre cuerpos cualesquiera, el siguientes paso, será el estudio de los polinomios ciclotómicos sobre los números racionales $\mathbb{Q}$, que al ser un caso particular de lo estudiado anteriormente, nos permitirá aplicar lo estudiado.

Terminaremos esta primera sección, dando un método, para resolver los polinomios ciclotómicos sobre los anillos $\mathbb{Z}_n$ con $n \in \mathbb{N}$.

En la segunda sección, daremos alguna aplicación de los polinomios ciclotómicos, en concreto explicaremos el teorema de Kroneker-Weber, y daremos la idea general de su demostración. Este resultado nos hará ver la importancia de los polinomios ciclotómicos. Ya que demuestra, que cualquier extensión abeliana de los números racionales $\mathbb{Q}$, es un subcuerpo de una extensión ciclotómica sobre $\mathbb{Q}$, es decir, simplemente realizando un estudio detallado de las extensiones ciclotómicas de $\mathbb{Q}$, podemos conocer cómo son

las extensiones abelianas de $\mathbb{Q}$.

El motivo por el cual, no demostramos este teorema completamente, es que debido a la limitación de extensión de este trabajo, no tenemos espacio suficiente para explicar todo lo necesario para su demostración, y por lo tanto, nos saltaremos las demostraciones más complicadas, pero mostraremos los pasos intermedios.

3. Polinomios ciclotómicos

Consideramos el polinomio $x^n - 1$, con $n \in \mathbb{N}$, es decir, los números que al elevarlos a n obtenemos uno. Gracias a las propiedades de los números complejos, sabemos que las raíces de estos polinomios son los que forman el conjuto:

$$G = \left\{ e^{\frac{2\pi ik}{n}} \;\middle|\; k = 1,\ \ldots,\ n \right\}$$

Veamos que el conjunto G es un grupo. Sea $x,\ y \in G$, entonces podemos escribir $x = e^{\frac{2\pi ik_1}{n}},\ y = e^{\frac{2\pi ik_2}{n}}$, con $k_1,\ k_2 = 1, \ldots, n$ y por lo tanto $x \cdot y = e^{\frac{2\pi i(k_1+k_2)}{n}}$ de dónde, teniendo en cuenta que $e^{2\pi i} = 1$, se obtiene que $x \cdot y \in G$, por lo qué se deduce, que el grupo tiene elemento neutro.

La asociatividad se desprende, de que el conjunto G está formado por números complejos. Por lo que sólo nos queda probar la existencia de elemento inverso para todo elemento de G. Tomamos cualquier $x = e^{\frac{2\pi ik}{n}} \in G$, con $k = 1, \ldots, n$ entonces, su elemento inverso es $e^{\frac{-2\pi ik}{n}}$, pero teniendo en cuenta que podemos escribir el elemento neutro como; $e^{2\pi i}$ tenemos $e^{\frac{-2\pi ik}{n}} = e^{\frac{2\pi i(n-k)}{n}}$, donde $n - k = 1, \ldots, n$, y por lo tanto, cualquier elemento tiene inverso en el conjunto G. De modo, que G es un grupo, al que se le conoce como el grupo de las unidades.

A los números del grupo G, se les llaman *raíces n-ésimas de la unidad*. En general, si estamos en un cuerpo K, y ξ es una raíz del polinomio $f(x) = x^n - 1_K$, entonces ξ es una raíz n-ésima de la unidad. Se dice que una raíz n-ésima de la unidad ξ es *primitiva*, si el orden de ξ es n, es decir, n es el menor número natural que cumple $\xi^n = 1$.

Podemos suponer, que s la característica de K no divide a n, ya que si la dividiera, tendríamos $n = sq$ con $q \in \mathbb{N}$, y por tanto, por ser s la característica $x^s = 1$ para todo $x \in K$, entonces; $x^n = (x^s)^q = 1$ para todo $x \in K$, de modo que todos los elementos del cuerpo K serían raíces n-ésimas de la unidad.

Es claro, que si ξ es una raíz n-ésima de la unidad primitiva, implica que $(\xi^i)^n = (\xi^n)^i = 1^i = 1 \ \ \forall\ i \in \mathbb{N}$, y por tanto, ξ^i también es raíz n-ésima de la unidad, y raíz del polinomio $x^n - 1$. Como ya sabemos, n es el menor número

que cumple $\xi^n = 1$, así si ξ es raíz primitiva de la unidad todas las potencias de ξ se reducen a: $\xi,\ \xi^2, \ldots,\ \xi^{n-1},\ \xi^n = 1$.

Veamos por reducción al absurdo, que estos números tienen que ser distintos. Supongamos que existen dos números $1 \leq i < j \leq n$ que cumplen, $\xi^i = \xi^j$, esto implica que $\xi^{j-i} = 1$ con $i - j < n$, contradiciendo que ξ es una raíz primitiva. Así que tenemos $\xi,\ \xi^2, \ldots,\ \xi^{n-1},\ \xi^n = 1$, son todas las raíces del polinomio $x^n - 1$. Por tanto las raíces n-ésimas de la unidad son:

$$\{\xi,\ \xi^2, \ldots,\ \xi^{n-1},\ 1\}$$

Es claro, que ξ si no es una raíz primitiva, no puede ser generador del grupo, debido a que; $\xi^i = 1$ con $i < n$, y por tanto, no genera todos los elementos. De modo, que el conjunto de las raíces n-ésimas de la unidad forman un grupo cíclico, donde las raíces primitivas de la unidad son los generadores.

Se define el *n-ésimo polinomio ciclotómico* $\phi_n(x)$ sobre un cuerpo K, cuya característica no divide a n, como el polinomio mónico que tiene por raíces todas las n-ésimas raíces primitivas de la unidad. $\phi_n(x) = \Pi(x - \xi)$ donde, ξ recorre las n-ésimas raíces primitivas de la unidad. Por tanto, el grado de dicho polinomio es el número de n-ésimas raíces primitivas de la unidad.

3.1. Teoría de Galois

Antes de entrar con el estudio de los polinomios ciclotómicos, tenemos que recordar algunos de los principales teoremas de la teoría de Galois. Para ello, tomaremos como referencia el libro [1]. Antes de empezar con los resultados, debemos introducir algunos conceptos.

Se dice que F es una *extensión* del cuerpo K, si F es un cuerpo y $K \subseteq F$. En este caso, F será un K-espacio vectorial, a la dimensión de este espacio vectorial se le llama *grado de la extensión*, y se denota como $|F : K|$.

Sea K un cuerpo, entonces F es un *cuerpo de escisión* de f sobre K, si $f = a(x - a_1)\ldots(x - a_k)$, y $F = K(a_1, \ldots, a_k)$. En este caso, se dice que F es una *extensión normal* de K.

Sea F una extensión del cuerpo K, entonces el *grupo de Galois*, es el grupo:

$$Gal(F/K) = \{\sigma : F \longrightarrow F \ \ isomorfismo \mid \sigma(k) = k \ \ \forall\ k \in K\}$$

Sea f un polinomio no constante, llamaremos el grupo de Galois de f a: $Gal(f) = Gal(F/K)$, donde F es el cuerpo de escisión de f sobre K.

Ahora que ya tenemos los conceptos necesarios, veamos los resultados que necesitaremos en nuestro estudio, de la teoría de Galois.

Teorema 3.1. *Supongamos que F_1 y F_2 son extensiones de los cuerpos K_1 y K_2 respectivamente, y sea $\sigma : K_1 \longrightarrow K_2$ un isomorfismo. Sea $p_1 \in K_1[x]$ irreducible y $p_2 = \sigma(p_1) \in K_2[x]$. Supongamos que, $a_i \in F_i$ es una raíz de p_i para $i = 1, 2$. Entonces σ se extiende a un isomorfismo $\theta : K_1(a_1) \longrightarrow K_2(a_2)$ tal que $\theta(a_1) = a_2$.*

Demostración. Podemos suponer que p_1 (y por tanto p_2) es mónico. Entonces tenemos que p_1 es el polinomio irreducible de a_1 sobre K_1, y que p_2 es el polinomio ireducible de a_2 sobre K_2.
Es facil ver que; $K_1(a_1) = \{f(a_1) \mid f \in K_1[x]\}$ y $K_2(a_2) = \{g(a_2) \mid g \in K_2[x]\}$. Definimos:

$$\begin{array}{rccc} \theta : & K(a_1) & \longrightarrow & K(a_2) \\ & f(a_1) & \longmapsto & \sigma(f)(a_2) \end{array}$$

Veamos que esta aplicación esta bien definida. Notar que si $f, g \in K_1[x]$, entonces $f(a_1) = g(a_1)$, si y sólo si $(f-g)(a_1) = 0$, si y sólo si p_1 divide a $f-g$, si y sólo si $\sigma(p_1) = p_2$ divide a $\sigma(f) - \sigma(g)$, si y sólo si $\sigma(f)(a_2) = \sigma(g)(a_2)$. Lo que prueba que nuestra aplicación está bien definida y es inyectiva.
Que es suprayectiva está claro. Es una comprobación inmediata que θ respeta la suma y multiplicación. Y por tanto θ extiende a σ y $\theta(a_1) = a_2$. □

Corolario 3.2. *Supongamos que F es una extensión del cuerpo K, y sea $p \in K[x]$ irreducible. Si $a, b \in E$ son raíces de p, entonces existe un isomorfismo de cuerpos $\theta : K(a) \longrightarrow K(b)$ tal que $\theta(a) = b$, y $\theta(k) = k$ para todo $k \in K$.*

Demostración. Para demostrar este corolario, basta aplicar el teorema 3.1 anterior tomando $K_1 = K_2 = K$, $F_1 = F_2 = F$ y $\sigma = 1_K$. □

Teorema 3.3. *Supongamos que $\sigma : K_1 \longrightarrow K_2$ es un isomorfismo de cuerpos. Sea $f_1 \in K_1[x]$ no constante y sea $\sigma(f_1) = f_2 \in K_2[x]$. Supongamos que F_i es cuerpo de escisión de f_i sobre K_i para $i = 1, 2$. Entonces existe un isomorfismo $\tau : F_1 \longrightarrow F_2$ que extiende σ.*

Demostración. Probamos el teorema por inducción sobre $|F_1 : K_1|$. Si f_1 se escinde en $K_1[x]$, entonces las raíces de f_1 en cualquier extensión de K_1 están en K_1. Así, $F_1 = K_1$. Como $\sigma(f_1)$ se escinde en $K_2[x]$, ya que σ es un isomorfismo de anillos, tenemos también que $K_2 = F_2$. De modo, que en este caso tenemos demostrado el teorema.
Como $F_1 = K_1$, si y sólo si f_1 se escinde en $K_1[x]$, podemos suponer que $|F_1 : K_1| > 1$. Así, existe un factor irreducible p de f_1 de grado mayor o igual que 2. Como f_1 se escinde en $F_1[x]$, tenemos que p se escinde en $F_1[x]$. Por el mismo argumento, $\sigma(p)$ se escinde en $F_2[x]$.

Sea a una raíz de p en F_1. Sea b una raíz de $\sigma(p) \in K_2[x]$ en F_2. Sabemos por el teorema 3.1 que existe un isomorfismo de cuerpos $\rho : K_1(a) \longrightarrow K_2(b)$ que extiende σ. Notemos que F_1 es cuerpo de escisión de f_1 sobre $K_1(a)$, y que F_2 es cuerpo de escisión de $\sigma(f_1)$ sobre $K_2(b)$. Observar que:

$$|F_1 : K_1| = |F_1 : K_1(a)||K_1(a) : K_1| = |F_1 : K_1(a)|gr(p) > |F_1 : K_1(a)|.$$

Donde llamamos $gr(\cdot)$, a la función que a cada polinomio le asocia su grado. Ahora tenemos un isomorfismo de cuerpos $\rho : \ K_1(a) \longrightarrow K_2(b)$, y un polinomio $f_1 \in K_1(a)[x]$ con $\rho(f_1) = f_2 \in K_2(b)[x]$. De modo que por inducción llegamos a que existe un isomorfismo $\tau : \ F_1 \longrightarrow F_2$ que extiende ρ. □

Corolario 3.4. *Supongamos que F es una extensión normal sobre K, y sean $K \subseteq M_1, \ M_2 \subseteq F$ subcuerpos. Si $\sigma : \ M_1 \longrightarrow M_2$ es un isomorfismo que fija los elementos de K, entonces existe un isomorfismo $\theta : \ F \longrightarrow F$ que extiende σ.*

Demostración. F es un cuerpo de escisión para un $f \in K[x]$ no constante sobre K. De modo que, F también es cuerpo de escisión sobre M_i para $i = 1, \ 2$. Como $f = \sigma(f)$ se tiene el resultado por el teorema 3.3. □

Corolario 3.5. *Supongamos que F es una extensión normal sobre K, y sea $p \in K[x]$ irreducible. Si $a, \ b \in F$ son raíces de p, entonces existe un isomorfismo $\tau : \ F \longrightarrow F$, tal que $\tau(a) = b$ y $\tau(k) = k \ \ \forall \ k \in K$*

Demostración. Es un resultado inmediato de los corolarios 3.2 y 3.4. □

Para seguir con este estudio de la teoría de Galois, necesitamos recordar alguna definición. Supongamos que Ω es un conjunto no vacío, y sea G un grupo. Decimos que G *actúa* sobre Ω, si para todo $\alpha \in \Omega$ y $g \in G$, tenemos definido un único elemento $\alpha \cdot g \in \Omega$ de tal manera que se cumple:

- $(\alpha \cdot g) \cdot h = \alpha \cdot (gh) \ \ \forall \ \alpha \in \Omega \ \ \text{y} \ \ g, \ h \in G.$
- $\alpha \cdot 1_G = \alpha \ \ \forall \ \alpha \in \Omega.$

En este caso decimos que, $\cdot$ define una *acción* de G sobre Ω. Diremos que una acción es *fiel*, si tomando $g \in G$ tal que $\alpha \cdot g = \alpha$ para todo $\alpha \in \Omega$, implica que $g = 1_G$. Por otra parte, diremos que una acción de G en Ω es *transitiva*, si dados $\alpha, \ \beta \in \Omega$ existe $g \in G$ tal que $\alpha \cdot g = \beta$.

Lema 3.6. *Supongamos que F es una extensión sobre K, y sea $f \in K[x]$. Si $a \in F$ es una raíz de f, entonces $\sigma(a)$ es una raíz de f. Además, $Gal(F/K)$ actúa sobre las raíces de f en F.*

Demostración. Consideremos a Ω al conjunto de raíces de f en E. Si $f = a_0 + a_1x + \cdots + a_nx^n$ y $f(a) = 0$, entonces para todo $\sigma \in Gal(F/K)$ y $a \in \Omega$.

$$f(\sigma(a)) = a_0 = a_1\sigma(a) + \cdots + a_n\sigma(a)^n = \sigma(a_0 + a_1a + \cdots + a_na^n) = 0$$

Definimos una acción de $Gal(F/K)$ sobre Ω, del siguiente modo:

$$a \cdot \sigma = \sigma(a)$$

□

Teorema 3.7. *Sea F el cuerpo de escisión de f sobre K. Si $\Omega = \{a_1, \ldots, a_k\}$ es el grupo de las distintas raíces de $f \in K[x]$, que es un polinomio no constante, entonces $G = Gal(F/K)$ actúa fielmente sobre Ω. En particular, G es isomorfo a un subgrupo de S_Ω. Si además f es irreducible en $K[x]$, esta acción es transitiva.*

Demostración. Tenemos que $F = K(a_1, \ldots, a_n)$. Sea $G = Gal(F/K)$. Por el lema 3.6, tenemos que G actúa sobre Ω. Además es claro que si $\sigma \in Gal(F/K)$ tal que $\sigma(a_i) = a_i$ para todo $i = 1, \ldots, n$, entonces $\sigma = 1_F$, y por tanto la acción es fiel. Además si f es irreducible, entonces la acción es transitiva por el corolario 3.5, de lo que obtenemos el resultado. □

3.2. Extensiones ciclotómicas

En esta sección tomamos como referencia el apartado 8 del capítulo V libro [2], aunque también sacaremos alguna idea de la sección 13.6 del libro [3], que nos ayudará a su comprensión.

Decimos que un cuerpo F, es un cuerpo de *escisión ciclotómico de orden n* sobre K, si F es un cuerpo de escisión de $x^n - 1$ sobre K.

Nuestro objetivo en esta sección, será el estudiar el cuerpo de escisión ciclotómico de orden n, sobre un cuerpo K, cuya característica no divide a n. Ya que como hemos notado anteriormente, si eso ocurriera, entonces cualquier elemento de K sería solución de la ecuación ciclotómica de orden n.

Teorema 3.8. *Sea n número natural, F cuerpo de escisión ciclotómico de orden n sobre K, tal que car(K) $\nmid$ n. Entonces $F = K(\xi)$, donde ξ es una n-ésima raíz primitiva de la unidad.*

Demostración. Por ser F cuerpo de escisión ciclotómico, implica que contiene a todas las raíces del polinomio ciclotómico de grado n, es decir, contiene a todas las n-ésimas raíces primitivas de la unidad. Sea ξ una n-ésima raíz de la unidad, entonces $\xi \in F$, y por tanto, $K(\xi) \subseteq F$.

Pero en el conjunto $\{\xi,\ \xi^2, \ldots,\ \xi^{n-1}\}$ están todas las raíces n-ésimas de la unidad, y por tanto, todas las raíces n-ésimas de la unidad primitivas, de modo que todas ellas están en $K(\xi)$, con lo que concluimos que $K(\xi) = F$. □

Gracias a este teorema, tenemos la forma de caracterizar el cuerpo escisión ciclotómico de orden n. Ahora, haciendo uso de la teoría de Galois, veremos la relación que existe entre los automorfismos de F, que dejan fijo el cuerpo K, y el subgrupo de las unidades de $\mathbb{Z}_n$.

Antes de demostrar esto recordemos la función de Euler. Si n es un entero positivo, se llama *función de Euler* φ a;

$$\varphi(n) = |\{m \in \mathbb{N} \mid m \leq n,\ (n, m) = 1\}|.$$

Teorema 3.9. *Sea n número natural, F cuerpo de escisión ciclotómico de orden n sobre K, tal que car(K)* $\nmid$ *n, entonces:*

- *F es una extensión abeliana de grado d, con* $d \mid \varphi(n)$.
- $Gal(F/K)$ *es isomorfo, a un subgrupo de orden d de las unidades de* $\mathbb{Z}_n$.

Demostración. Como F es el cuerpo de escisión sobre K del polinomio ciclotómico, que es resoluble por radicales, entonces se tiene que F/K es una extensión de Galois. Por tanto, si $\sigma \in Gal(F/K)$ queda completamente determinado por $\sigma(\xi)$. De modo que existen $i,\ j$ tal que $1 \leq i,\ j \leq n$, y cumplen $\sigma(\xi) = \xi^i,\ \ \sigma^{-1}(\xi) = \xi^j$. De este modo $\xi = \sigma^{-1}\sigma(\xi) = \xi^{ij}$, lo que implica que $ij \equiv 1 \mod n$, por tanto, $i \in \mathbb{Z}_n$ es una unidad. Así, podemos construir un monomorfismo, que a cada $\sigma \in Gal(F/K)$ le asigne la unidad $i \in \mathbb{Z}_n$ como hemos explicado.
Aunque es verdad, que no todas las unidades de $\mathbb{Z}_n$ les esté asociada un elemento de $Gal(F/K)$. Como el grupo multiplicativo de las unidades tiene orden $\varphi(n)$, así $Gal(F/K) \cong Imf$, lo que implica que el orden de la extensión es d con $d \mid \varphi(n)$. □

Veamos ahora con un ejemplo, que d no siempre es $\varphi(n)$, es decir, un caso en el que d sea un divisor propio de $\varphi(n)$.

Consideramos $K = \mathbb{Q}(i)$, y sea F el cuerpo de escisión ciclotómico de orden 8 sobre K.

Es fácil ver, que K es el cuerpo de escisión ciclotómico de orden 4 sobre $\mathbb{Q}$, ya que $x^4 - 1 = (x-1)(x+1)(x-i)(x+i)$. De modo, que como $\mathbb{Q}(\xi_4) \subseteq \mathbb{Q}(\xi_8)$, tenemos que F es el cuerpo de escisión ciclotómico de orden 8 sobre $\mathbb{Q}$.

El teorema nos dice que $|K : \mathbb{Q}| \leqslant \varphi(4) = 2$, pero es claro que $\mathbb{Q} \subsetneq K$, y por tanto $|K : \mathbb{Q}| = \varphi(4) = 2$. Por otro lado también tenemos que; $|F : \mathbb{Q}| \leqslant \varphi(8) = 4$.

Sabiendo que $\mathbb{Q} \subsetneq K \subseteq F$, se tiene que; $|F : K| < 4$, por lo que en este caso, d es un divisor propio de $\varphi(8)$.

Teorema 3.10. *Sea n número natural, F cuerpo de escisión ciclotómica de orden n sobre K, tal que car(K) $\nmid$ n, y $\phi_n(x)$ el n-ésimo polinomio ciclotómico, entonces el grado de $\phi_n(x)$ es $\varphi(n)$.*

Demostración. Es claro, que el grado de $\phi_n(x)$ es el número de n-ésimas raíces primitivas de la unidad. Sea ξ una n-ésima raíz de la unidad, entonces ξ^i con $1 \leq i \leq n$ es otra raíz primitiva, si y sólo si, $(i, n) = 1$, por tanto el número de raíces primitivas es $\varphi(n)$. □

El siguiente teorema, nos va a dar una idea de cómo son los coeficientes de los polinomios ciclotómicos.

Teorema 3.11. *Sea n número natural, F cuerpo de escisión ciclotómica de orden n sobre K, tal que car(K) $\nmid$ n, los coeficientes del polinomio $\phi_n(x)$ están en el subcuerpo primo P de K.*

Demostración. Lo probaremos por inducción sobre n. Como la unidad es un número primo, se tiene $\phi_1(x) = x - 1 \in P[X]$.
Supongamos que es cierto para $k < n$, y sea $f(x) = \Pi_{d|n \ d<n}\phi_d(x)$. Sabemos que $x^n - 1 \in P[X]$, de modo que aplicando el algoritmo de la división tenemos; $x^n - 1_K = fh + r$ para algunos $h,\ r \in P[X] \subset F[X]$, por la unicidad de la división, tiene que ser $r = 0$ y $\phi_n(x) = h \in P[X]$ □

Teorema 3.12. *Sea $n \in \mathbb{N}$, K un cuerpo tal que car(K) $\nmid$ n, y $\phi_n(x)$ el n-ésimo polinomio ciclotómico sobre K. Entonces $x^n - 1_K = \Pi_{d|n}\phi_d(x)$*

Demostración. Si F es el cuerpo de escisión ciclotómico de orden n sobre K, $\xi \in F$ una raíz primitiva de la unidad. $G = \langle \xi \rangle$ es el grupo de todas las n-ésimas raíces de la unidad, como este es un grupo cíclico, contiene todas las d-ésimas raíces de la unidad para cada d divisor de n. η es una d-ésima raíz de la unidad, si y sólo si, $|\eta| = d$. Por tanto, para cada d divisor de n tenemos que; $\phi_d(x) = \Pi_{\eta \in G\, |\eta|=d}(x - \eta)$ y así, multiplicando todos polinomios ciclotómicos d-ésimos con d divisor de n tenemos:

$$x^n - 1 = \Pi_{\eta \in G}(x - \eta) = \Pi_{d|n}(\Pi_{\eta \in G\, |\eta|=d}(x - \eta)) = \Pi_{d|n}\phi_d(x)$$

□

Denotaremos a la función que a cada polinomio $P \in K(x)$ le asocia su grado como $gr(P)$. De modo que con lo expuesto hasta ahora, es muy fácil

obtener la famosa ecuación de la función de Euler, fijándonos en el grado de la ecuación anterior.

$$n = gr(x^n - 1) = gr(\Pi_{d|n}\phi_d(x)) = \Sigma_{d|n} gr(\phi_d(x)) = \Sigma_{d|n}\varphi(d)$$

Es decir:

$$n = \Sigma_{d|n}\varphi(n)$$

Otra consecuencia de este teorema, es que nos da un procedimiento constructivo para calcular los polinomios ciclotómicos de grado n, a partir de los de menor grado. Si de la igualdad del teorema $x^n - 1_K = \Pi_{d|n}\phi_d(x)$ despejamos el polinomio ciclotómico de grado n, tenemos:

$$\phi_n(x) = \frac{x^n - 1}{\Pi_{d|n}\phi_d(x)}$$

Calculemos mediante este procedimiento, los primeros polinomiso ciclotómicos en el cuerpo de los racionales. En los primeros casos es claro que tenemos $\phi_1(x) = x - 1$ y $\phi_2(x) = x + 1$, calculándolos sucesivamente como hemos indicado obtenemos:

$$\begin{aligned}
\phi_3(x) &= x^2 + x + 1 \\
\phi_4(x) &= x^2 + 1 \\
\phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\phi_6(x) &= x^2 - x + 1 \\
\phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\phi_8(x) &= x^4 + 1 \\
\phi_9(x) &= x^6 + x^3 + 1
\end{aligned}$$

También cabe destacar, que si p es primo, como sus únicos divisores son 1 y p, tenemos; $\phi_p(x) = \frac{x^p-1}{x-1}$, y por tanto:

$$\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \sum_{i=1}^{p-1} x^i$$

3.3. El grupo de las unidades de $\mathbb{Z}_n$

Como hemos visto en el teorema 3.9, si F es un cuerpo de escisión ciclotómico sobre K, entonces el grupo $Gal(F/K)$ es isomorfo a un subrupo de las unidades de $\mathbb{Z}_n$.

Así que ahora, vamos a interrumpir nuestro estudio de los cuerpos de escisión ciclotómicos, para estudiar cómo es el grupo de las unidades de $\mathbb{Z}_n$.

En este estudio tomaremos como referencia principal el capítulo 6 del libro [4].

A partir de este momento, consideraremos a U_n el conjunto de las unidades de $\mathbb{Z}_n$. Recordemos que las unidades de $\mathbb{Z}_n$, son los números que cumplen; $1 \leqslant k \leqslant n$ y $(n,k) = 1$, por lo tanto, el orden de este grupo es $\varphi(n)$.

En este primer teorema, vamos a encontrar una caracterización de las raíces primitivas, que nos ayudará a localizarlas con mayor facilidad.

Teorema 3.13. *Un elemento $a \in U_n$ es una raíz primitiva de la unidad, si y sólo si, $a^{\varphi(n)/q} \neq 1$, para cada q primo que divida a $\varphi(n)$*

Demostración. $\Rightarrow$) Si a es una raíz primitiva de la unidad, entonces su orden es $\varphi(n)$, y por tanto $a^i \neq 1$ para $1 \leqslant i < n$ y en particular, es cierto para $i = \frac{\varphi(n)}{q}$ con q primo dividiendo a $\varphi(n)$.
$\Leftarrow$) Si a no es una raíz primitiva, sea k el orden de a, y por ser un elemento de U_n, entonces, tiene que dividir al orden del grupo, es decir, $k \mid \varphi(n)$. Por tanto, $\frac{\varphi(n)}{k} > 1$; tomamos q, un primo que divida a; $\frac{\varphi(n)}{k}$, entonces, k divide a $\frac{\varphi(n)}{q}$, y por tanto tenemos que; $a^{\frac{\varphi(n)}{q}} = 1$ en U_n. □

Demostremos ahora el llamado teorema chino de los restos, que nos ayudará a simplificar el estudio de las unidades de $\mathbb{Z}_n$.

Teorema 3.14. *Sean $n_1,\ n_2,\ \ldots,\ n_k$ enteros positivos que cumplen $(n_i, n_j) = 1$ $i \neq j$, y sean $a_1,\ a_2, \ldots,\ a_k$ enteros cualesquiera. Entonces, las soluciones del sistema de congruencias lineales:*

$$x \equiv a_1 \mod n_1, \quad x \equiv a_2 \mod n_2,\ \ldots\ , \quad x \equiv a_k \mod n_k$$

constituyen una única clase de congruencia módulo $n = n_1 n_2 \ldots n_k$.

Demostración. Tomamos $c_i = \frac{n}{n_i} = n_1 \ldots n_{i-1} n_{i+1} \ldots n_k$, con $i = 1, \ldots, k$. Como $(n_i, n_j) = 1$, $i \neq j$; implica que, $(n_i, c_i) = 1$, $i = 1,\ 2, \ldots,\ k$. Sabemos que cada congruencia $c_i x \equiv 1 \mod n_i$, tiene una única clase de soluciones d_i módulo n_i. Exigimos que el entero:

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + \cdots + a_k c_k d_k$$

Satisfaga las congruencias $x_0 \equiv a_i \mod n_i$ con $i = 1,\ 2, \ldots,\ k$. Es claro que $n_i \mid c_j$ si $i \neq j$, lo que implica que $a_j c_j d_j \equiv 0 \mod n_i$ y por tanto, $x_0 \equiv a_i c_i d_i \mod n_i \ \forall\ i = 1,\ 2, \ldots,\ k$; que como además se cumple que $c_i d_i \equiv 1 \mod n_i \ \forall\ i = 1,\ 2, \ldots,\ k$, con lo cual finalmente queda:

$$x_0 \equiv a_i \mod n_i \ \forall\ i = 1,\ 2, \ldots,\ k$$

Es decir, x_0 es una solución particular del sistema, ahora veamos que la clase de congruencia $\overline{x_0}$ módulo n es la única solución. Para ver esto, supongamos que x es solución de $x \equiv a_i \mod n_i, \quad i = 1, 2, \ldots, k$.

$$\left.\begin{array}{l} x \equiv a_i \mod n_i \\ x_0 \equiv a_i \mod n_i \end{array}\right\} \implies x \equiv x_0 \mod n_i \implies n_i \mid (x - x_0) \ \forall\, i = 1, 2, \ldots, k$$

Como $n_1, \ldots, n_k$ son primos entre sí, su producto es n, que por tanto divide a $x - x_0$, de modo que; $x \equiv x_0 \mod n$. □

Si factorizamos n en factores primos $n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$, y tomamos $n_i = p_i^{s_i}$ para cada $1 \leq i \leq k$, podemos aplicar el teorema anterior, ya que $(p_i^{s_i}, p_j^{s_j}) = 1$ si $i \neq j$. De este modo, tenemos el isomorfismo entre los siguientes anillos:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_k^{s_k}}$$

Así una unidad de $\mathbb{Z}_n$, está asociada a otra unidad de $\mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_k^{s_k}}$, y las unidades de este producto, vienen dadas cuando en cada uno de los productos tenemos una unidad, y por tanto:

$$U_n \cong U_{p_1^{s_1}} \times \cdots \times U_{p_k^{s_k}}$$

De esta forma hemos simplificado el estudio de U_n con n número natural cualquiera, al estudio de U_{p^e} con p primo y e un número natural.

Teorema 3.15. *Si p es primo, entonces el grupo U_p es cíclico.*

Demostración. Sabemos que hay $\varphi(p-1)$ elementos de orden $p-1$ en U_p. Como $\varphi(p-1) \geq 1$, el grupo tiene al menos un elemento de este orden. Sabemos que U_p tiene orden $\varphi(p) = p - 1$, así que hay al menos un elemento que genera U_p, y por tanto es cíclico. □

Con este teorema, tenemos caracterizados los grupos U_p con p primo, ahora ayudándonos de esto, vamos a estudiarlo para $n = p^e$ con p un primo impar.

Teorema 3.16. *Si p es un primo impar, entonces U_{p^e} es cíclico con orden $p^{e-1}(p-1)$ para todo $e \geq 1$.*

Demostración. Como es una demostración larga, para hacer la más facil de seguir indicamos los tres pasos en los que la realizaremos:

- Elegir una raíz primitiva g módulo p.
- Ver que g o $g + p$ es una raíz primitiva módulo p^2.

- Probar que si h es raíz primitiva módulo p^2, entonces h es raíz primitiva módulo p^e para todo $e \geq 2$.

Como ya hemos visto en el teorema anterior, U_p es un grupo cíclico, por tanto, podemos tomar g raíz primitiva módulo p, con lo que finalizamos el primer paso.

Por ser raíz primitiva, tenemos que $(g, p) = 1$, por lo tanto, también tenemos $(g, p^2) = 1$. Consideramos g como elemento de U_{p^2}. Sea d el orden de g módulo p^2. Lo que implica, que d divide a $\varphi(p^2)$, pero al ser p primo tenemos que; $\varphi(p^2) = p(p-1)$.
Por definición, $g^d \equiv 1 \ \ (p^2)$, por tanto también $g^d \equiv 1 \mod p$, pero como g tiene orden $p-1$ módulo p, entonces $p-1$ divide a d. Como p es primo, tenemos dos opciones $d = p-1$ o $d = p(p-1)$.
Si $d = p(p-1)$ ya habríamos llegado al resultado, así que asumimos que $d = p-1$. Consideramos $h = g + p$, así tenemos que $h \equiv g \mod p$, y h es una raíz primitiva de la unidad módulo p. Repitiendo el mismo argumento que antes, llegamos a que h tiene orden $p(p-1)$ o $p-1$ en U_{p^2}. Como $g^{p-1} \equiv 1$ mód p^2, tenemos que:

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + p^2(\dots) \equiv 1 - pg^{p-2} \mod p^2$$

Como g es coprimo con p, tenemos que $pg^{p-2} \neq 0 \mod p^2$, así $h^{p-1} \neq 1$ mód p^2, y por tanto h no tiene orden $p-1$. De modo, que h tiene orden $p(p-1)$, con lo que completamos el segundo paso.

Sea h una raíz primitiva de la unidad módulo p^2. Probemos por inducción sobre e, que h es raíz primitiva de la unidad módulo p^e, para todo $e \geqslant 2$.
Supongamos, que h es una raíz primitiva módulo p^e para algún $e \geqslant 2$, y sea d el orden de h módulo p^{e+1}. Usando el mismo argumento que antes, tenemos que d divide a $\varphi(p^{e+1}) = p^e(p-1)$, y es divisible por $\varphi(p^e) = p^{e-1}(p-1)$, así $d = p^e(p-1)$ o $d = p^{e-1}(p-1)$. En el primer caso, h es raíz primitiva de la unidad, ahora sólo tenemos que descartar el segundo.
Supongamos que $d = p^{e-1}(p-1)$, e intentemos llegar a contradicción.
Como h es una raíz primitiva de la unidad módulo p^e, tiene orden $\varphi(p^e) = p^{e-1}(p-1)$ en U_{p^e}, así $h^{p^{(e-2)}(p-1)} \not\equiv 1 \ \ (p^e)$. Sin embargo, $p^{e-2}(p-1) = \varphi(p^{e-1})$, así $h^{p^{e-2}(p-1)} \equiv 1 \mod p^{e-1}$. De este modo tenemos, $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$ donde, k es coprimo con p. Así tenemos:

$$\begin{aligned} h^{p^{e-1}(p-1)} &= (1+kp^{e-1})^{p^{e-1}(p-1)} \\ &= 1 + \binom{p}{1} kp^{e-1} + \binom{p}{2} (kp^{e-1})^2 + (p^{e-1})^3(\dots) \\ &= 1 + kp^e + \frac{1}{2}k^2p^{2e-1}(p-1) + (p^{e-1})^3(\dots) \end{aligned}$$

Como $3(e-1) \geqslant e+1$ para $e \geqslant 2$, y p es impar, $\frac{1}{2}k^2p^{2e-1}(p-1)$ es divisible por p^{e+1} ya que $2e-1 \geqslant e+1$ para $e \geqslant 2$, se tiene:

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \mod p^{e+1}$$

Como p no divide a k, tenemos que $h^{p^{e-1}(p-1)} \not\equiv 1 \mod p^{e+1}$, llegando así a contradición, con lo que concluimos el teorema. □

Una vez hemos visto que los grupos U_{p^e}, con p primo impar, y $e \in \mathbb{N}$ son cíclicos, el siguiente paso que debemos realizar, es estudio de U_{2^e} con $e \in \mathbb{N}$.

Teorema 3.17. *El grupo U_{2^e} es cíclico, si y sólo si, $e = 1$ o $e = 2$*

Demostración. El grupo $U_2 = \{1\}$ es cíclico generado por 1.
El grupo $U_4 = \{1, 3\}$ es cíclico generado por 3 ($3^2 = 1 \mod 4$).
Es suficiente probar que U_{2^e}, no tiene elementos de orden $\varphi(2^e) = 2^{e-1}$, probando que:

$$a^{2^{e-2}} \equiv 1 \mod 2^e \text{ para todo } a \text{ impar}$$

Probaremos esto por inducción sobre e. Para el menor valor $e = 3$, es decir, $n = 8$, tomamos a impar mayor que 1 ($a = 2b + 1$ con $b = 1,\ 2,\ 3$). Así; $a^2 = (2b+1)^2 = 4b^2 + 4b + 1 \equiv 4b(b+1) + 1 \equiv 1 \mod 8$, y por tanto es cierto.
Supongamos, que para un $e \geq 3$ se cumple $a^{2^{e-2}} \equiv 1 \mod 2^e$ para todo a impar. Así para cada a tenemos $a^{2^{e-2}} = 1+2^ek$ para un entero k. Desarollando tenemos:

$$a^{2^{(e+1)-2}} = (1 + 2^ek)^2 = 1 + 2^{e+1}k + 2^{2e}k^2 \equiv 1 \mod 2^{e+1}$$

Por tanto, si es cierto para e, también los es para $e+1$, de modo que U_{2^e} no es cíclico si $e \geq 3$. □

Si $e < 3$, sabemos que U_{2^e} es cíclico, pero si $e \geq 3$, lo único que sabemos, es que no es cíclico. El siguiente teorema nos va a dar información de cómo son los grupos U_{2^e}, cuando $e \geq 3$. Para ello, demostraremos un lema previo, que nos aligerará su demostración.

Lema 3.18. $2^{n+2} \mid 5^{2^n} - 1$ *pero* $2^{n+3} \nmid 5^{2^n} - 1$ *para todo* $n \geq 0$.

Demostración. Lo demostraremos por inducción sobre n. Para $n = 0$ es cierto, ya que, tenemos $4 \mid 4$, pero $8 \nmid 4$. Supongamoslo cierto para n. Podemos escribir:

$$5^{2^{n+1}} - 1 = (5^{2^n})^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1)$$

Como $2^{n+2} \mid 5^{2^n} - 1$, pero $2^{n+3} \nmid 5^{2^n} - 1$ y además como $5^{2^n} \equiv 1 \mod 4$ implica que $2 \mid 5^{2^n} + 1$, pero $4 \nmid 5^{2^n} + 1$. De modo, que uniendo estos resultados

tenemos que; $2^{n+3} \mid 5^{2^{n+1}} - 1$, pero $2^{n+4} \nmid 5^{2^{n+1}} - 1$; lo que implica que es cierto para $n+1$. □

Teorema 3.19. *Si $e \geq 3$, entonces $U_{2^e} = \{\pm 5^i \mid 0 \leq i \leq 2^{e-2}\}$*

Demostración. Sea m el orden del elemento 5 en U_{2^e}. Como $\varphi(2^e) = 2^{e-1}$ es el orden de U_{2^e}, entonces, m divide a 2^{e-1}, es decir, $m = 2^k$, para algún natural $k \leq e-2$, ya que como U_{2^e}, no puede tener elementos de orden 2^{e-1}, implica que $k < e-1$.
Poniendo $n = e-3$ en el lema anterior tenemos que $2^{e-1} \mid 5^{2^{e-3}} - 1$ pero $2^{e-1} \nmid 5^{2^{e-3}} - 1$, así $5^{2^{e-3}} \not\equiv 1 \mod 2^e$, por tanto tiene que ser $k > e-3$. Con lo que concluimos que $k = e-2$, así el orden es $m = 2^{e-2}$.
Esto significa que 5 tiene 2^{e-2} distintas potencias 5^i $(0 \leq i < 2^{e-2})$ en U_{2^e}. Ya que $5 \equiv 1 \mod 4$, éstos son todos los representantes congruentes con 1 módulo 4. Éstos representan la midad de los elementos de U_{2^e}. La otra mitad vienen dados por los enteros congruentes con -1 módulo 4, es decir, $(-5)^i$ con $0 \leq i < 2^{e-2}$. Con lo que se concluye que; $U_{2^e} = \{\pm 5^i \mid 0 \leq i \leq 2^{e-2}\}$ □

Ahora, veamos un teorema que nos va a indicar en que casos el grupo de las unidades de $\mathbb{Z}_n$ es cíclico.

Teorema 3.20. *El grupo U_n es cíclico, si y sólo si, $n = 1,\ 2,\ 4,\ p^e$ o $2p^e$ con p primo impar.*

Demostración. $\Leftarrow$) Los casos $n = 1,\ 2$ y 4 son claros, también hemos visto que para $n = p^e$ con p primo impar es cierto. De modo que sólo nos queda probarlo para $n = 2p^e$, con p primo impar. Pero, como ya hemos indicado anteriormente, con el teorema chino de los restos 3.14, lo podemos escribir como el siguiente producto; $U_{2p^e} \cong U_2 \times U_{p^e}$. Como tanto U_2, y U_{p^e} son cíclicos con órdenes primos entre sí, su producto también es cíclico, y por tanto, U_{2p^e} es cíclico.

$\Rightarrow$) Si $n \neq 1,\ 2,\ 4,\ p^e$ o $2p^e$ entonces sólo caben los siguientes casos:

1. $n = 2^e$ con $e \geq 3$.
2. $n = 2^e p^f$ con $e \geq 2,\ f \geq 1$ y p un primo impar.
3. n es divisible por dos primos impares.

Para el primer caso hemos visto que el grupo de las unidades no es cíclico.
Para el segundo caso, tenemos como consecuencia del teorema chino del resto $U_n \cong U_{2^e} \times U_{p^f}$.
Si $e \geq 3$, entonces U_{2^e} no es cíclico, y por tanto U_n no puede ser cíclico.
Si por el contrario $e = 2$, entonces U_4 y U_{p^f} son cíclicos de ordenes 2, y

$p^f - 1$ respectivamente. Como ambos grupos tienen orden par, su producto no puede ser cíclico.
Para el tercer y último caso, tenemos que existen dos primos $p,\ q$ impares, de modo, que podemos escribir $n = p^e q^s k$, donde $(p, k) = 1$ y $(q, k) = 1$. Así como consecuencia del teorema chino del resto, podemos escribir, $U_n \cong U_{p^e} \times U_{q^s} \times U_k$. Donde U_{p^e} y U_{q^s}, son grupos cíclicos de orden par, y por tanto, su producto no puede ser cíclico, de dónde se deduce, que U_n no es cíclico. □

De este modo, tenemos completamente caracterizado cómo es el grupo de las unidades U_n, con n número natural cualquiera. Y en particular, sabemos cuando el grupo de las unidades de $\mathbb{Z}_n$ es cíclico, que es algo, que nos será muy útil, cuando estudiemos los polinomios ciclotómicos sobre $\mathbb{Z}_n$.

3.4. Polinomios ciclotómicos en $\mathbb{Q}$

Una vez estudiados los polinomios ciclotómicos en un cuerpo cualquiera, ahora vamos a ver un ejemplo particular. En esta sección, estudiaremos los polinomios ciclotómicos sobre el cuerpo de los racionales $\mathbb{Q}$. Para este estudio, tomaremos como referencia el apartado 8 del capítulo V libro [2] y la sección 13.6 del libro [3].

Teorema 3.21. *Sea F el cuerpo de escisión ciclotómico de orden n sobre $\mathbb{Q}$, entonces $\phi_n(x)$ es mónico, y tiene sus coeficientes en $\mathbb{Z}$.*

Demostración. Probaremos esto por inducción. El resultado es cierto para el caso $n = 1$. Asumamos que $\phi_d(x) \in \mathbb{Z}[x]$ para $1 \leqslant d < n$.
Entonces tenemos $x^n - 1 = f(x)\phi_n(x)$ con $f(x) = \Pi_{d|n, d<n}\phi_d(x)$ es mónico y con coeficientes en $\mathbb{Z}$. $f(x)$ divide a $x^n - 1$ y ambos tienen sus coeficientes en $\mathbb{Q}$, de modo que $f(x)$ divide a $x^n - 1$ en $\mathbb{Q}[x]$.
Como $f(x),\ \phi_n(x) \in \mathbb{Z}[x]$, dividimos y tenemos $x^n - 1 = f_1(x)\phi_n(x) + r(x)$, por la unicidad del algoritmo de la división en $\mathbb{Q}[x]$, tenemos que $f_1(x) = f(x) \in \mathbb{Z}[x]$ y por tanto, $f(x)$ divide a $x^n - 1$ en $\mathbb{Z}[x]$, y de aquí obtenemos el resultado. □

Teorema 3.22. *Sea F el cuerpo de escisión ciclotómico de orden n sobre $\mathbb{Q}$, entonces, $\phi_n(x)$ es irreducible en $\mathbb{Q}(x)$*

Demostración. Como sabemos que $\phi_n(x) \in \mathbb{Z}[x]$, es suficiente probar que $\phi_n(x)$ es irreducible en $\mathbb{Z}[x]$. Sea h un factor irreducible de $\phi_n(x)$ en $\mathbb{Z}[x]$ con grado $\geqslant 1$, así $\phi_n(x) = f(x)h(x)$ con $f, h \in \mathbb{Z}[x]$.
Sea ξ una raíz de h, y p un número primo tal que $(n, p) = 1$. Así ξ es una raíz n-ésima de la unidad y como $(n, p) = 1$, también lo será ξ^p, y por tanto

será o bien raíz de f o de h.
Supongamos que no es raíz de h, para llegar a contradicción, y así demostrar, que todas las raíces primitivas tienen que ser raíces de h. Así ξ^p es raíz de $f(x) = \Sigma_{i=0}^{r} a_i x^i$. Como h es irreducible en $\mathbb{Q}$, y tiene a ξ como raíz, entonces h tiene que dividir a $f(x^p)$, así $f(x^p) = h(x)k(x)$ con $k \in \mathbb{Q}[x]$.
Dividiendo en $\mathbb{Z}[x]$, tenemos $f(x^p) = h(x)k_1(x) + r_1(x)$ con $k_1,\ r_1 \in \mathbb{Z}[x]$, por la unicidad del algoritmo de la división en $\mathbb{Q}[x]$, tenemos que $k(x) = k_1(x) \in \mathbb{Z}[x]$. Recordar que la proyección canónica $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ que manda $a \longmapsto \overline{a}$, induce el epimorfismo $\mathbb{Z}(x) \longrightarrow \mathbb{Z}_p(x)$, dado por $g = \Sigma_{i=0}^{t} b_i x^i \longmapsto \overline{g} = \Sigma_{i=0}^{t} \overline{b_i} x^i$. Por tanto, pasando a $\mathbb{Z}_p[x]$ tenemos $\overline{f}(x^p) = \overline{h}(x)\overline{k}(x)$. Pero, como en $\mathbb{Z}_p[x]$ se tiene que $\overline{f}(x^p) = \overline{f}(x)^p$ tenemos:

$$\overline{f}(x)^p = \overline{h}(x)\overline{k}(x) \in \mathbb{Z}_p[x]$$

De modo, que algún factor irreducible de $\overline{h}(x)$, tiene que dividir a $\overline{f}(x)^p$, y por lo tanto también dividirá a $\overline{f}(x)$. Por otro lado, tenemos $x^n - 1 = g_n(x)r(x) = f(x)h(x)r(x)$ con $r(x) \in \mathbb{Z}[x]$. Así, en $\mathbb{Z}_p[x]$ tenemos: $x^n - \overline{1} = \overline{x^n - 1} = \overline{f}(x)\overline{g}(x)\overline{r}(x)$.
Como $\overline{f}$ y $\overline{h}$ tienen un factor común, implica que $x^n - \overline{1} \in \mathbb{Z}_p[x]$ tiene una raíz multiple, lo que contradice que las raíces de $x^n - \overline{1}$ son todas distintas, ya que $(p, n) = 1$, de modo, que ξ^p es una raíz de $h(x)$.
De este modo, si tomamos $r \in \mathbb{Z}$ tal que $1 \leqslant r \leqslant n$ y $(r, n) = 1$, factorizando tenemos $r = p_1^{k_1} \dots p_s^{k_s}$ con $k_i > 0$. Entonces tenemos que; $(p_i, n) = 1$ con $1 \leqslant i \leqslant n$ así ξ^{p_i} es otra raíz primitiva, y por tanto, repitiendo este proceso sucesivamente, tenemos que; ξ^r es raíz primitiva, y por tanto raíz de $h(x)$.
Como ya sabemos, hay $\varphi(n)$ números que cumplan $1 \leqslant r \leqslant n$ y $(r, n) = 1$, que es el grado del polinomio ciclotómico, lo que implica que $h(x) = \phi_n(x)$, y como hemos impuesto desde el principio que $h(x)$ es irreducible, tenemos el resultado. □

Ahora que ya sabemos que el polinomio ciclotómico es irreducible en $\mathbb{Q}$, veamos cuál es el grado de extensión del cuerpo de escisión ciclotómico sobre los racionales.

Teorema 3.23. *Sea F el cuerpo de escisión ciclotómico de orden n sobre $\mathbb{Q}$, entonces $[F : \mathbb{Q}] = \varphi(n)$.*

Demostración. Como ya hemos visto anteriormente, tenemos que $F = \mathbb{Q}(\xi)$. Como $\phi_n(x)$ es el polinomio irreducible para cualquier raíz n-ésima de la unidad y su grado es $\varphi(n)$, se tiene el resultado. □

Como el grado de la extensión del cuerpo de escisión ciclotómico, y el grado del polinomio ciclotómico son $\varphi(n)$. Entonces, como el grupo de los

autormorfismos tiene que ser isomorfo a un grupo de las unidades de $\mathbb{Z}_n$, que tiene orden $\varphi(n)$; se deduce, que el grupo de los automorfismos es isomorfo al de las unidades de $\mathbb{Z}_n$.

3.5. Polinomios ciclotómicos en $\mathbb{Z}_n$

Una vez estudiados los polinomios ciclotómicos sobre $\mathbb{Q}$. Nuestro proposito, va a ser estudiarlos sobre sobre $\mathbb{Z}_n$, con $n \in \mathbb{N}$. Es decir, dejamos el estudio de los polinomios ciclotómicos sobre cuerpos, para estuciar como resolver las ecuaciones:

$$x^k \equiv 1 \mod n \quad k,\ n \in \mathbb{N}$$

Para realizar el estudio de la resolución de los polinomios ciclotómicos en $\mathbb{Z}_n$, tomaremos como referencia el capítulo 6 del libro [4].

Estudiemos primero los casos $n = 1,\ 2,\ 4,\ p^e$ y $2p^e$, donde p es un primo impar, que son los casos en los que el grupo de las unidades de $\mathbb{Z}_n$ es cíclico.

En este caso, al ser U_n cíclico, sabemos que existe una raíz primitiva, de modo que lo que hacemos, es poner x como potencia de una raíz primitiva cualquiera, es decir, escribimos; $x = g^i \mod n$, donde g es una raíz primitiva de U_n, e i es desconocido. De modo, que la ecuación queda: $(g^i)^k = g^{ik} \equiv 1 \equiv g^{\varphi(n)} \mod n$, ya que la raíz primitiva tiene orden $\varphi(n)$. Por este mismo motivo, se puede trasformar esta ecuación en una lineal:

$$in \equiv \varphi(n) \equiv 0 \mod \varphi(n)$$

Resolviendo esta congruencia, obtenemos las soluciones: $i_1,\ i_2 \ldots,\ i_s$, así que las soluciones del polinomio ciltotómico son: $x \equiv g^{i_1},\ g^{i_2}, \ldots,\ g^{i_s}$ módulo n.

Ahora, que ya hemos visto el procedimiento para resolver la ecuación en el caso de que el grupo de las unidades sea cíclico, veamos un ejemplo.

Ejemplo 3.24. *Calculemos las soluciones del polinomio ciclotómico de grado* 4 *sobre* $\mathbb{Z}_{25}$.

$$x^4 \equiv 1 \mod 25$$

Como podemos escribir $25 = 5^2$*, sabemos que* U_{25} *es cíclico, así que lo primero que tenemos que hacer es encontrar una raíz primitiva de la unidad. Como ya vimos en el teorema 3.13, como* $\varphi(25) = 20 = 2^2 \cdot 5$*, lo único que tenemos que ver para saber que* c *es raíz primitiva, es que;* $c^{\frac{20}{2}} \neq 1$*, y* $c^{\frac{20}{5}} \neq 1$ *en el anillo* $\mathbb{Z}_{25}$.

Por tanto, como; $2^{10} \equiv 24 \mod 25$ *y* $2^4 \equiv 16 \mod 25$*, el número* 2 *es una raíz primitiva de la unidad. Ahora, poniendo la ecuación como potencia*

de esta raíz primitiva tenemos; $x \equiv 2^i \mod 25$, $1 \equiv 2^{20} \mod 25$, *y por tanto, la ecuación queda:*

$$2^{4i} \equiv 2^{20} \mod 25$$

Como a ambos lados de la equivalencia tenemos la misma potencia, podemos fijarnos únicamente en el exponente, de modo, que reducimos la congruencia no lineal, en una lineal:

$$4i \equiv 0 \mod 20$$

Donde es inmediato, que las soluciones de esta ecuación son $i = 0,\ 5,\ 10,\ 15$, *y por tanto, las soluciones del polinomio ciclotómico son:*

$$\begin{aligned} x = 2^0 = 1 &\quad \text{mód} \quad 25 \\ x \equiv 2^5 = 32 \equiv 7 &\quad \text{mód} \quad 25 \\ x \equiv 2^{10} = 1024 \equiv -1 &\quad \text{mód} \quad 25 \\ x \equiv 2^{15} = 32768 \equiv 18 &\quad \text{mód} \quad 25 \end{aligned}$$

Antes de ver como resolveríamos el polinomio ciclotómico en $\mathbb{Z}_n$, con cualquier $n \in \mathbb{N}$, necesitamos ver como se resuelve el polinomio ciclotómico en $\mathbb{Z}_{2^e}$, con $e \geq 3$, ($x^k \equiv 1 \mod 2^e$).

Como ya vimos, todos los elementos x de U_{2^e}, los podemos escribir como $x = (\pm 5)^i$, con $0 \leq i \leq 2^{e-2}$. Como $1 \in U_{2^e}$ podemos escribir la unidad de esta forma, de modo, que para encontrar las soluciones del polinomio, tenemos que poner x como una potencia de 5, y -5. Teniendo en cuenta que; $(\pm 5)^{2^{e-2}} \equiv 1 \mod 2^e$ las ecuaciones quedan:

$$(\pm 5)^{ki} \equiv (\pm 5)^{2^{e-2}} \mod 2^e$$

Si ahora, nos fijamos sólo en el expoenente, obtenemos una ecuación lineal, y acabamos el procedimiento del mismo modo que antes. El siguiente ejemplo nos ayudará a entenderlo mejor.

Ejemplo 3.25. *Resolvamos el polinomio ciclotómico de grado* 7, *en* $\mathbb{Z}^{16}$.

$$x^7 \equiv 1 \mod 16$$

Como ya sabemos, $U_{16} = \{(\pm 5)^i \mid 0 \leqslant i \leqslant 4\}$, *y además* $(\pm 5)^4 \equiv 1 \mod 16$. *Por tanto, sólo tenemos que resolver las siguientes ecuaciones:*

$$\begin{aligned} (-5)^{7i} &\equiv (-5)^4 \mod 16 \\ 5^{7j} &\equiv 5^4 \mod 16 \end{aligned}$$

De modo, que podemos reducir estas ecuaciones a ecuaciones lineales, y así, tenemos: $7i \equiv 4 \equiv 0 \mod 4$, $7j \equiv 4 \equiv 0 \mod 4$.

De dónde obtenemos, que las soluciones son; $i,\ j = 0$.

Y por tanto, las soluciones son:

$$x \equiv (-5)^0 = 1 \mod 16$$
$$x \equiv 5^0 = 1 \mod 16$$

Es decir, existe una única solución, que es $x = 1$.

Para estudiar el caso general, con n cualquier número natural, lo primero que hacemos es factorizar $n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$, y a continuación, resolvemos las congruencias; $x_1^k \equiv 1\ (p_1^{k_1}), \ \dots\ , x_l^k \equiv 1 \mod p_l^{k_l}$, como ya hemos indicado anteriormente.

Sean $x_i \quad 1 \leq i \leq l$ las distintas soluciones de las ecuaciones $x_i^k \equiv 1 \mod p_i^{k_i}$.

Una vez calculadas las soluciones de estas congruencias, sólo tenemos que aplicar el teorema 3.14 chino de los restos para encontrar las soluciones del polinomio ciclotómico. Tomamos $c_i,\ d_i$ de la siguiente forma:

$$c_1 = \frac{n}{p_1^{k_1}},\ c_2 = \frac{n}{p_2^{k_2}},\ \dots,\ c_l = \frac{n}{p_l^{k_l}}$$

$$c_1 d_1 \equiv 1 \mod p_1^{k_1}, \quad c_2 d_2 \equiv 1 \mod p_2^{k_2}, \ \dots\ , \ c_l d_l \equiv 1 \mod p_l^{k_l}$$

Ahora, tenemos que las soluciones del polinomio ciclotómico, se obtienen combinando todas las soluciones x_i que hemos obtenido:

$$x \equiv x_1 c_1 d_1 + \ \dots\ + x_1 c_1 d_1 = \sum_{i=1}^{l} x_1 c_1 d_1 \mod n$$

Veamos un ejemplo que nos ayudará a comprenderlo mejor.

Ejemplo 3.26. *Resolvamos el polinomio ciclotómico de grado* 7 *en* $\mathbb{Z}_{72}$.

$$x^7 \equiv 1 \mod 72$$

Para empezar, descomponemos 72 *en factores primos, obteniendo;* $72 = 2^3 \cdot 3^2$. *Siguiendo el procedimiento anterior, ahora tenemos que resolver las ecuaciones:* $x_1^7 \equiv 1 \mod 2^3$, *y* $x_2^7 \equiv 1 \mod 3^2$.

Empecemos resolviendo la ecuación $x_1^7 \equiv 1 \mod 2^3$.

Como ya sabemos, $U_{2^3} = \{(\pm 5)^i \mid 0 \leqslant i \leqslant 2\}$ *y* $(\pm 5)^2 \equiv 1 \mod 2^3$. *Poniendo la incognita* x_1 *como potencia de* ± 5 *las ecuaciones nos quedan:*

$$5^{7i} \equiv 5^2 \mod 2^3$$
$$(-5)^{7j} \equiv (-5)^2 \mod 2^3$$

Fijándonos sólo en los exponentes obtenemos las congruencias lineales:

$$7i \equiv 0 \mod 2 \qquad 7j \equiv 0 \mod 2$$

La única solución que obtenemos en ambos casos es $i,\ j = 0$*, así, que la única solución para* x_1 *es* 1*.*

Calculemos ahora las soluciones para la segunda ecuación; $x_2^7 \equiv 1 \mod 3^2$*.* 2 *es una raíz primitiva de la unidad en* $\mathbb{Z}_9$*, ya que;* $2^{\frac{\varphi(9)}{2}} = 2^3 \equiv 8 \mod 9$*, y* $2^{\frac{\varphi(9)}{3}} = 2^2 \equiv 4 \mod 9$*.*

Así, que ahora reescribimos la ecuación poniendola como potencia de esta raíz primitiva y obtenemos:

$$2^{7i} \equiv 2^{\varphi(9)} = 2^6 \mod 9$$

Fijándonos únicamente en los exponentes, obtenemos la congruencia lineal; $7i \equiv 0 \mod 6$*. Donde, es inmediato que la única solución es:* $i \equiv 0 \mod 6$*, y por tanto, la solución de la segunda ecuación es:* $x_2 \equiv 2^0 = 1 \mod 9$*.*

Calculamos ahora los c_i*. Tenemos;* $c_1 = \frac{72}{2^3} = 9,\ c_2 = \frac{72}{3^2} = 8$*. El siguiente paso, es calcular los* d_i *resolviendo las ecuaciones:*

$$9d_1 \equiv 1 \mod 8 \qquad 8d_2 \equiv 1 \mod 9$$

De donde obtenemos; $d_1 \equiv 1 \mod 8$*, y* $d_2 \equiv 8 \mod 9$
Y por tanto, la única solución de la ecuación es:

$$x \equiv x_1c_1d_1 + x_1c_2d_2 = 9 + 8 \cdot 8 = 73 \equiv 1 \mod 72$$

Realizando los mismos pasos que en este ejemplo, podemos resolver cualquier polinomio ciclotómico en los anillos $\mathbb{Z}_n$ cuando n pertenece a los naturales.

4. El Teorema de Kronecker-Weber

Antes de empezar directamente con el teorema, veamos el siguiente resultado, con el que entenderemos la gran repercusión e importancia, que tiene del teorema de Kronecker-Weber.

Teorema 4.1. *Si* $F/\mathbb{Q}$ *es una estensión ciclotómica, y* E *una extensión intermedia, entonces* $E/\mathbb{Q}$ *es una extensión abeliana.*

Demostración. Sea E una extensión intermedia, es decir, $\mathbb{Q} < E < F$. El grupo $Gal(F/E)$ es normal, por ser subgrupo de $Gal(F/\mathbb{Q})$. Por el teorema de Galois la extensión $E/\mathbb{Q}$ es normal, y por tanto, de Galois. Además $Gal(E/\mathbb{Q}) \cong Gal(F/\mathbb{Q})/Gal(E/\mathbb{Q})$, que es abeliano. De modo, que se concluye que $E/\mathbb{Q}$ es una extensión abeliana. □

De este modo, hemos probado, que toda subextensión de una extensión ciclotómica sobre $\mathbb{Q}$, es abeliana. El teorema de Kronecker-Weber prueba el recíproco. Es decir, afirma que cada extensión abeliana finita del cuerpo de los números racionales $\mathbb{Q}$, es un subcuerpo de una extensión ciclotómica sobre los números racionales $\mathbb{Q}$, y por tanto, tenemos, que es cierto el si y sólo si en este teorema.

El teorema de Kronecker-Weber es un resultado importante, ya que después de haber estudiado la teoría de Galois, es natural que nos surja la siguiente pregunta; ¿Qué grupos de Galois se dan sobre $\mathbb{Q}$? Es una pregunta que aún está abierta en muchos casos, pero este teorema nos da una respuesta parcial, ya que nos dice, que cualquier extensión abeliana sobre $\mathbb{Q}$, es subcuerpo de una extensión ciclotómica.

Es un resultado mucho más importante, que simplemente decir, que todo grupo abeliano existe como grupo de Galois sobre $\mathbb{Q}$. Además de esto, también nos dice, que está contenida en el conjunto de los números ciclotómicos (el cuerpo que contiene a los racionales con todas las raíces n-ésimas de la unidad, para todo n natural).

La gran repercusión de este teorema, es fruto de la cantidad de áreas de las matemáticas que se unen en un mismo resultado, como es el álgebra, la geometría, el análisis, y la teoría de números.

La primera demostración de este teorema fue dada por Leopold Kronecker en 1853, pero era una demostración incompleta, ya que no lo probaba, para extensiones abelianas de orden potencia de 2. En 1886, Heinrich Weber probó completamente el teorema, pero en su demostración había fallos, que no se solucionaron hasta la demostración que dió Hilbert en 1896.

No podemos dar una demostración detallada de este teorema, ya que esto excede completamente el objetivo del trabajo fin de grado. Por lo tanto, presentaremos un esquema detallado que describe los pasos que tenemos que dar para llegar a su demostración. Para este proposito, seguiremos principalmente el esquema de los artículos [7], y [6].

Debemos destacar, otros artículos, en los que se realiza la misma demostración que vamos detallar; [8], y [11]. Pero también tenemos señalar, que existe otra demostración del teorema, que en vez de usar la teoría de números, usa la teoría de cuerpos, la que podemos encontrar en los artículos; [9], [11], o [10].

La razón, por la que nos hemos decantado a explicar la demostración que usa la teoría de números, es debido a que usa conceptos mucho más simples, lo que hace su comprensión y exposición más sencilla.

Lema 4.2. *Si el teorema de Kronecker-Weber se cumple para extensiones de grado potencia de primo, entonces se cumple para todas las extensiones abelianas finitas.*

Demostración. Sea K una extensión normal de $\mathbb{Q}$. Aplicando el teorema fundamental de los grupos abelianos finitos, podemos escribir:

$$Gal(K|\mathbb{Q}) = G_1 \times G_2 \times \cdots \times G_n$$

Donde los $G_i \;\; 1 \leq i \leq n$, son grupos cíclicos de orden potencia de primo. Denotamos $K_i = \{k \in K \mid \sigma(k) = k \;\; \forall\, \sigma \in G_i\}$.
Aplicando teoría de Galois se obtiene; $G_i \trianglelefteq Gal(K|\mathbb{Q})$, y $Gal(K_i|\mathbb{Q}) \cong G_i$, de modo, que es una extensión de orden potencia de primo. K es el cuerpo composición de los K_i. Como cada K_i es una extensión ciclotómica, se sigue de aquí que K también lo es. □

Con este primer lema, hemos conseguido reducir la demostración del teorema, a las extensiones de orden potencia de primo. De modo, que ahora nuestro proposito va a ser demostrar que se cumple el teorema en este caso.

Pero antes de seguir con el hilo de la demostración, necesitamos introducir brevemente algunos conceptos básicos de la teoría de números.

Se dice, que un número es *algebraico*, si es una raíz de un polinomio mónico de $\mathbb{Z}[x]$.

Diremos, que un dominio de integridad es un *dominio Dedekind* si cumple las siguientes propiedades:

- Es *noetheriano*, es decir, que cualquier cadena de ideales $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$ tiene longitud finita.
- Es *íntegramente cerrado*, o sea, contiene todo elemento de su cuerpo de fracciones que sea entero.
- Todos los ideales primos distintos de cero son maximales.

Sea K una extensión de $\mathbb{Q}$, denotamos $\mathcal{O}_K$ como los números algebraicos de K. Se puede demostrar, que $\mathcal{O}_K$ es un dominio Dedekind. Debemos notar, que si tomamos $\mathfrak{p} \subseteq \mathcal{O}_K$ un ideal primo distinto de cero, entonces $\mathfrak{p} \cap \mathbb{Z} = <p>$, donde $<p>$ es un ideal primo en $\mathbb{Z}$.

Al grupo $Z_\mathfrak{p} = \{\sigma \in Gal(K|\mathbb{Q}) \mid \sigma\mathfrak{p} = \mathfrak{p}\}$ se le llama *grupo de descomposición* de $\mathfrak{p}$ sobre $\mathbb{Q}$, es decir, es el conjunto de los elementos del grupo de Galois que fijan al primo $\mathfrak{p}$.

Por otro lado, se define *cuerpo de descomposición* de $\mathfrak{p}$ sobre $\mathbb{Q}$, como el conjunto de los elementos de K que son fijados por todos los $\sigma \in Z_{\mathfrak{p}}$.

El índice de descomposición del grupo $Z_{\mathfrak{p}}$, que se extiende en el grupo de Galois, $Gal(K|\mathbb{Q})$ nos indica el número de ideales en los que se extiende el ideal $<p>$ en $\mathcal{O}_K$.

De modo, que si $|G : Z_{\mathfrak{p}}| > 1$, entonces decimos que p *se ramifica* en K, donde p es el número que cumple $\mathfrak{p} \cap \mathbb{Z} = <p>$. Si por el contrario $|G : Z_{\mathfrak{p}}| = 1$, entonces tenemos, que $Z_{\mathfrak{p}} = Gal(K|\mathbb{Q})$, y por tanto, el primo p sigue siendo un ideal en $\mathcal{O}_K$, en este caso se dice que p es *inerte*, o que p se *escinde completamente* en K.

Una vez introducidos estos conceptos, podemos seguir el hilo de la demostración del teorema de Kronecker-Weber, con el siguiente teorema, que utiliza la teoría de números para simplificar aún más la demostración.

Lema 4.3. *Sea K una extensión abeliana sobre $\mathbb{Q}$ de orden q^m con q primo. Entonces es suficiente probar el teorema cuando q es el único primo que se ramifica en K.*

De este lema, se desprenden los siguientes corolarios, que debemos destacar por su utilidad.

Corolario 4.4. *Sea K una extensión abeliana sobre $\mathbb{Q}$ de orden q^m con q primo, supongamos que $p \neq q$ es el único primo que se ramifica en K. Entonces p se escinde completamente en K, $p \equiv 1 \mod q$, y K es el único subcuerpo de $\mathbb{Q}(\xi)$ de grado q^m, donde ξ es raíz primitiva de la unidad de grado p. Y por lo tanto la extensión K sobre $\mathbb{Q}$ es cíclica.*

Corolario 4.5. *Si K es una extensión abeliana sobre $\mathbb{Q}$ con orden impar, entonces 2 no se ramifica en K.*

Con lo expuesto hasta ahora, hemos conseguido reducir la demostración del teorema al caso de extensiones abelianas de orden q con q primo. Para seguir con la demostración, tal y como nos sugieren los dos corolarios anteriores, es necesario dividir los casos en los que $q = 2$, y q sea un primo impar. Y por tanto, el último paso de la demostración sería demostrar:

- Sea K una extensión abeliana sobre $\mathbb{Q}$ de orden q^m, con q un primo impar, (que como ya hemos visto es el único primo que se ramifica). Entonces la extensión K es ciclotómica.
- Sea K una extensión abeliana sobre $\mathbb{Q}$ de orden 2^m. Entonces K es una extensión ciclotómica.

Concluyendo así la demostración del teorema de Kronecker-Weber.

Observamos, la cantidad de ramas de las matemáticas que se conectan en este teorema, tales como la teoría de grupos, la teoría de números, cálculos elementales, y una gran intuición geométrica. Lo que refleja la importancia de este teorema, que consigue juntar todo ello en un único resultado.

Notemos alguna de las importantes consecuencias que se desprenden de este teorema.

Demuestra, que para estudiar las extensiones abelianas, basta con hacer un estudio exhaustivo de las extensiones ciclotómicas, algo que ya hemos conseguido realizar sin mayores dificultades, lo que destaca la tremenda simplificación que hace este teorema.

Veamos ahora que cualquier grupo abeliano, es grupo de Galois sobre $\mathbb{Q}$.

Recordemos, que si tomamos ξ raíz primitiva de la unidad de orden n, entonces $Gal(\mathbb{Q}(\xi)|\mathbb{Q}) = U_n$. De modo, que si tomamos A cualquier grupo abeliano, entonces, por el teorema de Kronecker-Weber, existe $n \in \mathbb{N}$, tal que $A \leq U_n$. Como $A \leq Gal(\mathbb{Q}(\xi)|\mathbb{Q})$, con A y $Gal(\mathbb{Q}(\xi)|\mathbb{Q})$ abelianos, entonces existe $K \leq Gal(\mathbb{Q}(\xi)|\mathbb{Q})$ tal que $Gal(\mathbb{Q}(\xi)|\mathbb{Q})/K = A$.

Haciendo la correspondencia de Galois, tenemos que existe un subcuerpo normal F de $\mathbb{Q}(\xi)$, donde $Gal(F|\mathbb{Q}) = A$, con lo que hemos probado, que dado un grupo abeliano cualquiera, es grupo de Galois sobre $\mathbb{Q}$.

Referencias

[1] Gabriel Navarro, *Un curso de álgebra*, Educació materials, Valencia, 2008.

[2] T. Hungerford, *Algebra*, 2nd edition, Springer-Verlag, New York, 1974.

[3] D. Dummit, R. Forte, *Abstract Algebra*, 3th edition, Jonh Wiley & Sons, Vermont, 2004.

[4] J. Jones, G. Jones, *Elementary Number Theory*, Springer, London, 1998.

[5] P. Ribenboin, *Algebraic Numbers*, Jonh Wiley & Sons, Kingston, 1972.

[6] M. J. Greenberg, *An Elementary Proof of the Kronecker-Weber Theorem*, The American Mathematical Monthly, 81(6):601-607, Jun-Jul 1974.

[7] Amber Verser, *The Kronecker-Weber Theorem: An Exposition*, Lux, Winsconsin, 2013.

[8] Héctor Edonis Pinedo Tapia, *Uma prova elementar do teorema de Kronecker-Weber*, Universidade de São Paulo, São Paulo, 2009.

[9] Lauren Berk, *Lecture 15: Cyclotomic Fields and the Kronecker-Weber Theorem*, University of Berkeley, California, 2012.

[10] Eknath Ghate, *The Kronecker-Weber Theorem*, Adhikari S.D., Pune, 1999.

[11] Lucas Culler, *The Kronecker-Weber Theorem*, University of Chicago, Chicago, 2007