Universitat de les Illes Balears

escola politècnica superior

Trabajo Fin de Grado

GRAU DE MATEMÀTIQUES

Demostración del teorema de Kronecker-Weber

ARTURO GONZÁLEZ MOYA

Tutor
Gabriel Cardona Juanals

Escola Politècnica Superior
Universitat de les Illes Balears
Palma, septiembre de 2020

ÍNDICE GENERAL

CAPÍTULO 1

INTRODUCCIÓN

El teorema de Kronecker-Weber toma el nombre de los matemáticos Leopold Kronecker y Heinrich Martin Weber por su aportación a la demostración de dicho teorema. Kronecker fue un matemático del siglo XIX reconocido por defender que la aritmética y el análisis deben estar fundados en los números enteros, dejando a un lado los irracionales y los imaginarios. Otras aportaciones de Kronecker dentro de las matemáticas son la delta de Kronecker y el producto de Kronecker. Con respecto al teorema que vamos a demostrar en este documento, Kronecker fue el que proporcionó la mayoría de la demostración en el año 1853.

Heinrich Martin Weber fue un matemático del siglo XIX-XX que dedicó gran parte de su vida al estudio del álgebra y la teoría de números. La aportación de Weber a la demostración del teorema que vamos a demostrar fue la de, en 1886, rellenar los huecos que Kronecker dejó en su demostración.

En este trabajo, no estudiaremos la demostración proporcionada por Kronecker y Weber, si no que trataremos con detalle una demostración de M. J. Greenberg en [1], en la cual se utilizan teoría de Galois, teoría de ramificación y el anillo de enteros.

El teorema de Kronecker-Weber es el siguiente:

Teorema 1. *Toda extensión abeliana de $\mathbb{Q}$ está contenida en una extensión ciclotómica, es decir, toda extensión abeliana es una subextensión del cuerpo $\mathbb{Q}$ adjuntándole raíces de la unidad.*

Este teorema tiene una gran importancia ya que determina qué cuerpos contienen las extensiones abelianas de los racionales. Si generalizamos este problema a cuerpos arbitrarios, es decir, establecer qué cuerpos contienen las extensiones abelianas de un cuerpo de números K, da lugar a una de las ramas mas importantes de la teoría de Galois: la teoría de cuerpos de clases. Kronecker fue uno de los que más se centró en este estudio de las extensiones abelianas, intentando encontrar funciones que pudiesen generar la extensión abeliana maximal para cada cuerpo de números.

CAPÍTULO 2

INTRODUCCIÓN AL ANILLO DE ENTEROS DE CUERPOS DE NÚMEROS

Comenzaremos por definir que es el anillo de enteros de un cuerpo que es extensión de los racionales.

Sea $K/\mathbb{Q}$ una extensión de cuerpos finita. El anillo de enteros de K, $\mathcal{O}_K$ se define como la clausura entera de $\mathbb{Z}$ en K, o lo que es lo mismo, $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$, donde $\overline{\mathbb{Z}} = \{$ raíces de polinomios mónicos de $\mathbb{Z}[X]\} \subset \overline{\mathbb{Q}}$ siendo $\overline{\mathbb{Q}}$ la clausura de $\mathbb{Q}$. El anillo de enteros $\mathcal{O}_K$ es un dominio de Dedekind, es decir, es un dominio integro (el anillo carece de elementos divisores de 0) y todo ideal I es producto de ideales primos. Una propiedad de los dominios de Dedekind es que son también anillos noetherianos, lo que nos dice que cualquier ideal $\mathfrak{p} \subset \mathcal{O}_K$ esta finitamente generado. Además, otra propiedad del los dominios de Dedekind es que todo ideal primo es un ideal maximal, por lo tanto, los ideales primos de $\mathcal{O}_K$ son ideales maximales.

El siguiente teorema que se asemeja al teorema fundamental de la aritmética pero con ideales del anillo de enteros, lo podemos encontrar en el libro [2, teorema 12.2.8].

Teorema 2. *Todo ideal $\mathfrak{a} \subset \mathcal{O}_K$ no nulo descompone de manera única (sin contar el orden)*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

siendo los $\mathfrak{p}_i$ ideales primos.

Tomemos $\mathfrak{p} \subset \mathcal{O}_K$ un ideal primo. Entonces se tiene que $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ ya que $\mathfrak{p}$ lo es. Además, por ser $\mathfrak{p}$ un ideal primo, se tiene que $1 \notin$ y entonces $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para algún p primo. Diremos que $\mathfrak{p}$ está sobre p. Si ahora comenzamos con este $p \in \mathbb{Z}$ y generamos el ideal $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ donde los $\mathfrak{p}_i$ son ideales primos, como $\mathfrak{p}$ está sobre p, entonces $\mathfrak{p}$ se encuentra en la factorización de $p\mathcal{O}_K$, es decir, los primos de $\mathcal{O}_K$ que están sobre p son aquellos que aparecen en la factorización. Definimos el índice de ramificación de p en $\mathfrak{p}_i$ como e_i que es el exponente de $\mathfrak{p}_i$ en la descomposición de $p\mathcal{O}_K$. Decimos que p ramifica en $\mathfrak{p}_i$ si $e_i > 1$ y p ramifica si algún $e_i > 1$.

El ideal primo $\mathfrak{p}$ también es un maximal por ser un dominio de Dedekind y entonces $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo finito, por lo que $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{q^f}$ para ciertos q y f. Veamos que q coincide con el primo p de $\mathbb{Z}$ considerado anteriormente. En efecto, consideramos la composición $\mathbb{Z} \hookrightarrow \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}$. El núcleo de esta composición son los elementos de $\mathbb{Z}$ tales que van a parar al neutro de $\mathcal{O}_K/\mathfrak{p}$, es decir, son los elemento de $\mathbb{Z}$ que a su vez están en $\mathfrak{p}$, $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z} = (p)$ como hemos visto anteriormente. Por el primer teorema de isomorfía, se tiene que $\mathbb{Z}/(p)$ es isomorfo a la imagen de la composición y como la segunda parte de la composición es exhaustiva, la imagen es un subcuerpo de $\mathbb{F}_{q^f}$. Por lo tanto, ha de ocurrir que $q = p$ y entonces $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$. Al cuerpo $\mathcal{O}_K/\mathfrak{p}$ se le llama **cuerpo residual en** $\mathfrak{p}$. El entero f tal que $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_q]$ se denomina **grado residual de** $\mathfrak{p}$.

Consideremos ahora $K/\mathbb{Q}$ una extensión de Galois con $G = \mathrm{Gal}(K/\mathbb{Q})$ y p un primo racional. Consideramos también el ideal $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. Tenemos el siguiente teorema que podemos encontrar en [2, teorema 12.3.3]:

Teorema 3. *G actúa transitivamente sobre $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\}$*

Veamos ahora algunos subgrupos de $G = \mathrm{Gal}(K/\mathbb{Q})$ asociados a cada primo $\mathfrak{p}$ de $\mathcal{O}_K$. Definimos el grupo de descomposición Z como

$$Z = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

y gracias al teorema anterior, por ser acción transitiva, tenemos que G/Z está en biyección con $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\}$. Esto nos dice que el índice de Z en G es igual a g que es el número de primos distintos en los que descompone el ideal $p\mathcal{O}_K$ mencionado anteriormente.

Sea $p \in \mathbb{Z}$ y sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ que contiene a p. Por lo que hemos visto anteriormente, $\mathcal{O}_K/\mathfrak{p}$ es isomorfo a $\mathbb{F}_{p^f}$. Sea Z el grupo de descomposición de $\mathfrak{p}$. Todo elemento $\sigma \in Z$ da lugar a un automorfismo $\bar{\sigma} : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$ o lo que es lo mismo, $\bar{\sigma}$ pertenece al grupo de Galois $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$. De esta forma, la aplicación $\sigma \mapsto \bar{\sigma} : Z \to \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ es un epimorfismo que viene dado por el Frobenius ya que $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$ como podemos ver en [3, página 17]. El núcleo de esta aplicación se le denomina grupo de inercia T y viene definido como

$$T = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}}\ \forall \alpha \in \mathcal{O}_K\}.$$

Veamos que $T \subset Z$. En efecto, si tomamos $\alpha \in \mathfrak{p}$ y $\sigma \in T$, por definición de T tenemos que $\sigma(\alpha) \in \alpha + \mathfrak{p}$. Como $\alpha \in \mathfrak{p}$, se tiene que $\sigma(\alpha) \in \alpha + \mathfrak{p} = \mathfrak{p}$. Con esto vemos que $\sigma(\mathfrak{p}) \in \mathfrak{p}$. Para ver la igualdad, tendríamos que repetir el procedimiento anterior pero con $\sigma^{-1} \in T$. De esta forma vemos que $\sigma(\mathfrak{p}) = \mathfrak{p}$ y entonces T es un subgrupo de Z.

Podemos ver también que T es un subgrupo normal de Z. Tomamos $t \in T$ y $z \in Z$. Consideremos también el automorfismo z^{-1} de Z. Por definición de que t pertenezca a T, vemos que $t(z^{-1}(x)) \equiv z^{-1}(x) \pmod{\mathfrak{p}}$, o lo que es lo mismo, $t(z^{-1}(x)) - z^{-1}(x) \in \mathfrak{p}$. Por tanto, $z(t(z^{-1}(x))) - x = z(t(z^{-1}(x)) - z^{-1}(x)) \in z(\mathfrak{p}) = \mathfrak{p}$ ya que $z \in Z$. Acabamos de ver que $z(t(z^{-1}(x))) \equiv x \pmod{\mathfrak{p}}$ sea cual sea x, por lo tanto $z(t(z^{-1})) \in T$ y entonces tenemos que $T \lhd Z$.

Para cualquier $n \geq 1$ podemos definir el subgrupo de G que llamaremos n-ésimo grupo de ramificación de $\mathfrak{p}$, denotado por V_n y que viene dado de la siguiente forma:

$$V_n = \{\alpha \in G : \alpha(x) \equiv x \pmod{\mathfrak{p}^{n+1}}\ \forall x \in \mathcal{O}_K\}$$

Por ser $\mathfrak{p}$ un ideal, tenemos que $\mathfrak{p}^n$ está contenido en $\mathfrak{p}$ y por lo tanto se tiene que V_n es un subgrupo de T. También podríamos observar, de manera análoga a la que hemos empleado para ver que T es un subgrupo normal de Z, que V_n es un subgrupo normal de Z para cualquier $n \geq 1$. Se tiene por tanto la torre de subgrupos normales

$$T = V_0 \rhd V_1 \rhd \cdots \rhd V_n \cdots$$

Consideramos ahora $L/\mathbb{Q}$ una extensión de cuerpos finita y sea K/L un extensión de Galois de grado n, cuyo grupo de Galois es $G = \mathrm{Gal}(K/L)$. Sea $\mathcal{O}_K$ el anillo de enteros de K y sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$. Tenemos que $\mathfrak{p} = \mathfrak{P} \cap L$ es un ideal primo de $\mathcal{O}_L$ (el anillo de enteros de L). En efecto, sean $a, b \in \mathcal{O}_L$, por definición de $\mathcal{O}_L$, $a, b \in L$. Si $ab \in \mathfrak{p} = \mathfrak{P} \cap L$, entonces $ab \in \mathfrak{P}$. Como $\mathfrak{P}$ es un ideal primo, $a \in \mathfrak{P}$ o $b \in \mathfrak{P}$ y por lo tanto $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

Como $\mathfrak{P}$ y $\mathfrak{p}$ son ideales primos, también son ideales maximales y $\hat{K} = \mathcal{O}_K/\mathfrak{P}$, $\hat{L} = \mathcal{O}_L/\mathfrak{p}$ son cuerpos residuales. Tenemos que $\hat{K}$ es isomorfo a $\mathbb{F}_{q^f}$ donde $f = [\mathcal{O}_K/\mathfrak{P} : \mathbb{F}_q]$. Veamos que $\hat{L}$ es un subcuerpo de $\hat{K}$. En efecto, como $\mathcal{O}_L$ está contenido en $\mathcal{O}_K$, tenemos que la composición $\mathcal{O}_L \hookrightarrow \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}$ tiene núcleo $\mathfrak{P} \cap \mathfrak{p} = \mathfrak{p}$ y por lo tanto, $\mathcal{O}_L/\mathfrak{p}$ es un subcuerpo de $\mathbb{F}_{q^f}$. Tenemos que $\hat{L}$ es isomorfo a $\mathbb{F}_q$. De esta forma, los cuerpos residuales $\hat{K}$ y $\hat{L}$ son de orden q^f y q respectivamente.

A continuación se da un teorema que nos será de gran utilidad próximamente pero para ello, necesitaremos un lema que podemos encontrar en el libro [5, páginas 292-296].

Lema 4. *Sea K_T y K_Z los cuerpos fijos por los grupos de inercia y descomposición, respectivamente, de un ideal primo $\mathfrak{P}$ y sean L_Z y L_T las clausuras algebraicas de L en K_Z y K_T. Sean $\mathfrak{P}_Z = \mathfrak{P} \cap K_Z$, $\mathfrak{P}_T = \mathfrak{P} \cap K_T$ los ideales en los cuerpos fijos por los grupos de descomposición y de inercia. Se tiene que si $\hat{K}$ es una extensión separable sobre $\hat{L}$, entonces $\hat{K} = L_T/\mathfrak{P}_T$.*

Teorema 5. *Sea T el grupo de inercia de $\mathfrak{P}$ y sea V_n el n-ésimo grupo de ramificación de $\mathfrak{P}$. Se tiene que T/V_1 es isomorfo a un subgrupo del grupo multiplicativo $\hat{K}^*$ de $\hat{K}$. También se tiene que V_j/V_{j+1} es isomorfo a un subgrupo del grupo aditivo de $\hat{K}$ siendo $j \geq 1$. Para j suficientemente grande tenemos que V_j es trivial.*

Demostración. Antes de comenzar con la demostración de este teorema, explicaremos una técnica que utilizaremos en esta y otras posteriores demostraciones. Sea K un cuerpo de números y sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Se define la **localización** de $\mathcal{O}_K$ en $\mathfrak{p}$ como

$$\mathcal{O}_{K_\mathfrak{p}} = \left\{ \frac{a}{b} | a, b \in \mathcal{O}_K, b \notin \mathfrak{p} \right\}$$

Podemos observar que $\mathcal{O}_K$ está contenido en el anillo $\mathcal{O}_{K_\mathfrak{p}}$ (los elementos de $\mathcal{O}_K$ corresponden a los elementos de $\mathcal{O}_{K_\mathfrak{p}}$ que tienen $b = 1$) y que los únicos elementos no invertibles son los elementos de $\mathfrak{p}$. En particular, $\mathfrak{p}$ es el único ideal maximal de $\mathcal{O}_{K_\mathfrak{p}}$. De hecho, $\mathfrak{p}$ es el único ideal primo y todos los ideales de $\mathcal{O}_{K_\mathfrak{p}}$ son de la forma $\mathfrak{p}^k$ para $k \geq 1$.

Es trivial ver que $\mathcal{O}_{K_\mathfrak{p}}$ es un dominio de Dedekind. Además es un DIP. En efecto, sea $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$; entonces (π) descompone en $\mathcal{O}_{K_\mathfrak{p}}$ como una cierta potencia de π; si tuviésemos $(\pi) = \mathfrak{p}^k$ con $k \geq 2$, se tendría que $\pi \in \mathfrak{p}^2$, contradicción con la hipótesis. Por lo tanto, tenemos que $(\pi) = \mathfrak{p}$.

El anillo $\mathcal{O}_{K_\mathfrak{p}}$ es lo que se denomina como un **anillo de valoración discreta**, y tiene asociada una **valoración** $v : \mathcal{O}_{K_\mathfrak{p}} \setminus \{0\} \to \mathbb{Z}$. La valoración viene definida de la siguiente forma: dado $x \in \mathcal{O}_{K_\mathfrak{p}}$, $x \neq 0$, se tiene que $(x) = \mathfrak{p}^k = (\pi^k)$ de manera que $x = u\pi^k$ (siendo u una unidad, es decir, $u \notin \mathfrak{p}$); entonces se tiene que $v(x) = k$.

Comenzamos la demostración, si es necesario, localizando y por lo tanto tenemos que $\mathfrak{P}$ es un ideal principal generado por un elemento π. Sea s un elemento del grupo de inercia T, entonces por definición tenemos que $s(\pi)$ pertenece a $\mathfrak{P} + \pi$, o lo que es lo mismo $s(\pi)$ pertenece a $\mathfrak{P}$. Además, se tiene que $s(\pi)$ no pertenece a $\mathfrak{P}^2$ ya que si eso ocurriese, tendríamos que $\pi = s^{-1}(s(\pi))$ pertenecería a $\mathfrak{P}^2$ por lo que $\mathfrak{P}^2 = \mathfrak{P}$ y eso no ocurre ya que $\mathfrak{P}^2 \subsetneq \mathfrak{P}$. De esta forma, vemos que $s(\pi)$ es de la forma $x_s\pi$ siendo x_s un elemento de K que no pertenece a $\mathfrak{P}$.

Sea $t \in T$, entonces tenemos que $s(t(\pi)) = s(x_t\pi) = s(x_t)x_s\pi$ donde x_t es un entero de K que no pertenece a $\mathfrak{P}$, tal que $t(\pi) = x_t\pi$. De esta manera, si x_{st} es el entero de K que no pertenece a $\mathfrak{P}$ de tal forma que $s(t(\pi)) = x_{st}\pi$, tenemos que $x_{st} = s(x_t)x_s$. Como s pertenece al grupo de inercia T, por definición sabemos que $s(x_t) \equiv x_t \pmod{\mathfrak{P}}$ y entonces si sustituimos nos queda que $x_{st} \equiv x_t x_s \pmod{\mathfrak{P}}$. Si ahora miramos las clases módulo $\mathfrak{P}$, tenemos que los residuos $\bar{x}_{st}$ y $\bar{x}_t\bar{x}_s$ son iguales. De esta forma observamos que existe un homomorfismo $s \mapsto x_s$ entre el grupo de inercia T y el cuerpo residual $\hat{K}$. Sea H_0 el núcleo del homomorfismo mencionado anteriormente que, por definición de núcleo, son todos aquellos elementos $s \in T$ tales que se satisface $x_s \equiv 1 \pmod{\mathfrak{P}}$. Esto nos dice que los elementos del núcleo son aquellos en los que $x_s - 1$ pertenece a $\mathfrak{P}$. Como π pertenece a $\mathfrak{P}$ ya que es su generador, tenemos que los elementos del núcleo son aquellos automorfirmos s de T tales que $(x_s - 1)\pi = s(\pi) - \pi \in \mathfrak{P}^2$.

De manera similar, para $s \in V_n$ y $n \geq 1$ tenemos que $s(\pi) - \pi \in \mathfrak{P}^n$ y por lo tanto podemos escribir $s(\pi) - \pi = y_s\pi^n$ con $y_s \in K$. Tomamos ahora $t \in V_n$, si y_{st}, y_t son elementos de K que cumplen que $s(t(\pi)) - \pi = y_{st}\pi^n$ y $t(\pi) - \pi = y_t\pi^n$ respectivamente, tenemos que $y_{st}\pi^n = s(t(\pi)) - \pi$. Como $y_t\pi^n = t(\pi) - \pi$, podemos sustituir y tenemos que $y_{st}\pi^n = s(y_t\pi^n + \pi) - \pi$. Aplicando que s es un morfismo y que $s(\pi) - \pi = y_s\pi^n$, tenemos que $y_{st}\pi^n = s(y_t\pi^n + \pi) - \pi = s(y_t\pi^n) + s(\pi) - \pi = s(y_t)(\pi^n y_s + \pi)^n + y_s\pi^n$. Si ahora dividimos entre π^n nos queda que $y_{st} = s(y_t)(\pi^{n-1}y_s + 1)^n + y_s$. Observemos que ya que $s \in V_n$ tenemos que $s(y_t) \equiv y_t \pmod{\mathfrak{P}^n}$. También podemos ver que todos los términos de la expansión $(\pi^{n-1}y_s + 1)^n$ se encuentran en $\mathfrak{P}$ excepto 1^n, que es el único que no esta multiplicado por π. Por lo tanto se tiene que $y_s t \equiv y_t + y_s \pmod{\mathfrak{P}}$. Si pasamos a las clases residuales módulo $\mathfrak{P}$, obtenemos que $\bar{y}_{st} = \bar{y}_t + \bar{y}_s$. De forma similar a lo que hemos visto para un elemento del grupo de inercia, tenemos que $s \mapsto \bar{y}_s$ es un homomorfismo entre V_n y un subgrupo del grupo aditivo de $K/\mathfrak{P}$. Sea H_n su núcleo que viene dado por lo automorfismos $s \in V_n$ tales que $y_s \equiv 0 \pmod{\mathfrak{P}}$, entonces tenemos que $s(\pi) - \pi \in \mathfrak{P}^{n+1}$ ya que $y_s \in \mathfrak{P}$ y $\pi^n \in \mathfrak{P}^n$ por lo tanto $s(\pi) - \pi = y_s\pi^n \in \mathfrak{P}^{n+1}$.

Lo que acabamos de ver con esto es que V_1 y V_{n+1} están contenidos en los núcleos H_0 y H_n respectivamente. Ahora compararemos estos grupos. Supongamos que tenemos un elemento $s \in V_n$ ($n \geq 1$) tal que $s(\pi) - \pi \in \mathfrak{P}^{n+1}$ veamos que entonces se tiene que $s(z) - z \in \mathfrak{P}^{n+1}$ para todo $z \in \mathfrak{P}$. En efecto, sea $z \in \mathfrak{P}$, por ser π un generador de $\mathfrak{P}$, tenemos que $z = a\pi$ siendo a un elemento de K, entonces $s(z) - z = s(a\pi) - a\pi$. Por ser s un morfismo, se tiene que $s(a\pi) - a\pi = s(a)s(\pi) - a\pi$ y si ahora sumamos y restamos el elemento $s(a)\pi$ nos queda que $s(z) - z = s(a)(s(\pi) - \pi) + \pi(s(a) - a)$ donde

$\pi \in \mathfrak{P}$, $s(a) \in K$, $s(\pi) - \pi \in \mathfrak{P}^{n+1}$ ya que es nuestra suposición y $s(a) - a \in \mathfrak{P}^n$ ya que s pertenece a V_n. Por lo tanto tenemos que

$$s(z) - z \in \mathfrak{P}^{n+1}. \tag{2.1}$$

Ya hemos visto que ocurre con un elemento de $\mathfrak{P}$, ahora veamos lo que pasa con uno de K (no tiene por qué ser de $\mathfrak{P}$). Sea $x \in K$, escribimos $s^p(x) - x = s^{p-1}(s(x) - x) + s^{p-2}(s(x) - x) + \cdots s(s(x) - x) + (s(x) - x)$ donde p es el primo de $\mathbb{Z}$ tal que $\mathfrak{P} \cap \mathbb{Z} = p$. Ya que $s \in V_n$, entonces $s(x) - x \in \mathfrak{P}^n$ y por lo tanto $s(x) - x$ también es un elemento de $\mathfrak{P}$. Aplicando lo que hemos probado en 2.1, como $s(x) - x \in \mathfrak{P}$, tenemos que $s(x) - x \equiv s(s(x) - x) \pmod{\mathfrak{P}^{n+1}}$. Como la relación de congruencia es transitiva, tenemos que todos los elementos de la suma en la que hemos expresado $s^p(x) - x$ son congruentes con $s(x) - x$ módulo $\mathfrak{P}^{n+1}$, por lo tanto $s^p(x) - x \equiv p(s(x) - x) \pmod{\mathfrak{P}^{n+1}}$. Ya que $p \in \mathfrak{P}$ y $s(x) - x \in \mathfrak{P}^n$, se tiene que $s^p(x) - x \in \mathfrak{P}^{n+1}$ y por lo tanto $s^p \in V_{n+1}$. Lo que acabamos de ver con esto es que si consideramos el grupo cociente V_n / V_{n+1}, entonces todos los elementos del subgrupo $G'_n = H_n / V_{n+1}$ son de orden p. Entonces el orden de G'_n es una potencia de p. Aplicando el primer teorema de isomorfía a lo que hemos visto anteriormente, tenemos que el grupo cociente T / H_0 es isomorfo a un subgrupo del grupo multiplicativo $\hat{K}$ y el grupo cociente V_n / H_n ($n \geq 1$) es isomorfo con un subgrupo del grupo aditivo de $\hat{K}$.

Para finalizar con la demostración, tendríamos que ver que $H_n = V_{n+1}$. Lo demostraremos usando que nuestra extensión es de Galois, en particular, es separable. Anteriormente hemos visto que $V_{n+1} \subseteq H_n$ por lo que para ver la igualdad solo nos faltaría demostrar que $H_n \subset V_{n+1}$, o lo que es lo mismo, para $s \in H_n$ se tiene que $s(x) - x \in \mathfrak{P}^{n+1}$ para todo $x \in K$. Por ahora sabemos que es cierto para los elementos de $\mathfrak{P}$. Pero en el caso de ser la extensión separable, por el Lema 4 se tiene que los cuerpos cocientes $K/\mathfrak{P}$ y $L_T/\mathfrak{P}_T$ son iguales (siendo L_T la clausura de L en el cuerpo fijo por el grupo de inercia, K_T, y $\mathfrak{P}_T = L_T \cap \mathfrak{P}$). Por lo tanto, tenemos que un elemento $x \in K$ se puede escribir de la forma $x = y + z$, siendo y un elemento de L_T y z un elemento de $\mathfrak{P}$, entonces $s(x) - x = s(y) - y + s(z) - z \in \mathfrak{P}^{n+1}$ ya que $s(z) - z \in \mathfrak{P}^{n+1}$ por lo que hemos visto anteriormente y $s(y) = y$ ya que como $s \in V_n$ y hemos visto que los grupos de ramificación forman una cadena descendente de subgrupos, tenemos que $s \in T$ y como L_T es la clausura del cuerpo fijo por el grupo de inercia, por definición de cuerpo fijo, $s(y) = y$. Con esto queda finalizada la demostración. □

En la demostración de este teorema, también hemos visto que todos los elementos de V_n / V_{n+1} son de orden p, por lo tanto tenemos que V_n / V_{n+1} es trivial o producto directo de grupos cíclicos de orden p.

CAPÍTULO 3

DEMOSTRACIÓN DEL TEOREMA DE KRONECKER-WEBER

Dividiremos la demostración en dos partes principales. Primero veremos que basta demostrar el teorema de Kronecker-Weber (K-W a partir de ahora) para extensiones cíclicas de orden potencia de un primo y, tras esto, demostraremos estos casos, separando según si es un primo impar o si es dos.

Comenzamos construyendo donde vamos a trabajar y con unos hechos que utilizaremos durante toda la demostración. Aquí solo estarán referenciados para poder hacer alusión a ellos más fácilmente.

Sea $L/\mathbb{Q}$ una extensión de cuerpos finita y sea K/L un extensión de Galois de grado n, cuyo grupo de Galois es $G = \mathrm{Gal}(K/L)$. Sea $\mathcal{O}_K$ el anillo de enteros de K y sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$. Como hemos visto anteriormente, tenemos que $\mathfrak{p} = \mathfrak{P} \cap L$ es un ideal primo de $\mathcal{O}_L$ (el anillo de enteros de L).

Como $\mathfrak{P}$ y $\mathfrak{p}$ son ideales primos, también son ideales maximales y $\hat{K} = \mathcal{O}_K/\mathfrak{P}$, $\hat{L} = \mathcal{O}_L/\mathfrak{p}$ son cuerpos residuales. Tenemos que $\hat{K}$ es isomorfo a $\mathbb{F}_{q^f}$ donde $f = [\mathcal{O}_K/\mathfrak{P} : \mathbb{F}_q]$ y $\hat{L}$ es isomorfo a $\mathbb{F}_q$.

$$
\begin{array}{l}
K \\
\Big| \, n;\ \mathrm{Gal} \\
L \\
\Big| \, <\infty \\
\mathbb{Q}
\end{array}
$$

3.1 Hechos

En esta sección, recopilaremos diferentes resultados que han salido durante el capítulo anterior y pondremos aquí para que queden más claras y sean más fáciles de referenciar.

Comenzamos con el primer hecho, en el que resaltaremos la propiedad de que $\mathcal{O}_K$ sea un anillo de Dedekind y veremos que ocurre con el anillo de enteros de una extensión de Galois.

HECHO 1. *El ideal* $\mathfrak{p}\mathcal{O}_K$ *es igual a un producto de la forma*

$$\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

donde los $\mathfrak{P}_i$ *son ideales primos distintos. Como la extensión es de Galois, tenemos que* $e_1 = e_2 = \cdots = e_g = e$*. Por lo tanto*

$$\left(\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g\right)^e$$

donde $\mathfrak{P}_1 = \mathfrak{P}$ *y los demás* $\mathfrak{P}_i$ *son imágenes de* $\mathfrak{P}$ *por automorfismos de G (G actúa transitivamente sobre* $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g$*).*

Por ser una extensión de Galois, se tiene que

$$n = efg$$

donde:

- *e: es el exponente de ramificación de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$
- *f: es el grado residual de* $\mathfrak{p}$
- *g: es el número de primos diferentes en la descomposición de* $\mathfrak{p}\mathcal{O}_K$
- *n: es el grado de la extensión*

Al igualdad $n = efg$ hecho anterior la podemos encontrar en [5, página 289].

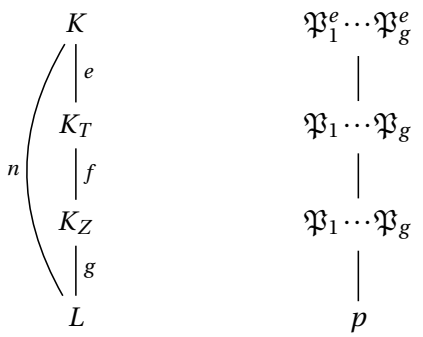
En el próximo hecho, veremos la relación que existe entre el grupo cociente del grupo de descomposición y el grupo de inercia (Z/T) y el grupo de Galois de la extensión de $\hat{K}/\hat{L}$ definida anteriormente. Podemos encontrarlo en el apartado 2.

HECHO 2. *El morfismo* $\sigma \mapsto \bar{\sigma}$ *definido en el apartado 2 página 4, induce un isomorfismo de* Z/T *con el grupo de Galois* $\overline{G} = \mathrm{Gal}(\hat{K}/\hat{L})$*. En particular,* Z/T *es cíclico generado por un automorfismo tal que*

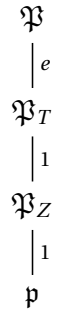
$$\sigma x \equiv x^q \pmod{\mathfrak{P}}$$

En este hecho podremos ver como se relacionan el orden del grupo de inercia con el exponente de ramificación. Podemos encontrarlo mas detalladamente en [5, páginas 291-292].

HECHO 3. *El exponente de ramificación de* $\mathfrak{P}$*, e, es también el orden del grupo de inercia* T*. Si la extensión es de Galois, existe una biyección entre* G/Z *y* $\{\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g\}$ *y por lo tanto g es el índice de Z en G. Si* K_T *es el cuerpo fijo por T y* $\mathfrak{P}_T = \mathfrak{P} \cap K_T$*, entonces* $\mathfrak{P}_T$ *no ramifica sobre* $\mathfrak{p}$ *y* $\mathfrak{P}$ *ramifica totalmente sobre* $\mathfrak{P}_T$*. Sea* K_Z *el cuerpo fijo por Z, entonces tenemos el siguiente esquema de subcuerpos.*



Ahora si definimos $\mathfrak{P}_Z = \mathfrak{P} \cap K_Z$*, el esquema de los ideales sería el siguiente.*



Como hemos visto en la parte de teoría previa, existen propiedades con respecto a los grupos de ramificación que nos resultaran muy útiles y nos vendría bien tenerlas referenciadas de forma directa. Esto se ve reflejado en el hecho próximo.

HECHO 4. *T/V_1 es isomorfo a un subgrupo del grupo multiplicativo $\hat{K}^*$ de $\hat{K}$, por lo tanto es cíclico y su orden divide a $q^f - 1$. También tenemos que V_j/V_{j+1} $(j \geq 1)$ es isomorfo a un subgrupo del grupo aditivo de $\hat{K}$ y, si $\hat{L}$ tiene característica p, entonces V_j/V_{j+1} es el trivial o producto directo de grupos cíclicos de orden p. Para j suficientemente grande, V_j es trivial.*

En el siguiente hecho, mencionaremos un teorema que nos será de gran utilidad. Este teorema lo podemos encontrar en [5, página 303] y en [3, página 120]

HECHO 5 (TEOREMA DE MINKOWSKI)**.** *Para toda extensión finita no trivial de $\mathbb{Q}$ el conjunto de primos que ramifican en esta extensión es finito y no vacío.*

En este hecho, veremos propiedades de las extensiones ciclotómicas y de sus respectivos grados sobre $\mathbb{Q}$.

HECHO 6. *Sea ζ_m la raíz primitiva m-ésima de la unidad. Si p es un primo impar, entonces para todo r, $\mathbb{Q}_{\zeta_{p^r}}$ es cíclico de orden $p^{r-1}(p-1)$, mientras que para $r \geq 3$, $\mathbb{Q}_{\zeta_{2^r}}$ es el producto directo de dos grupos cíclicos, uno de orden 2^{r-2} y otro de orden 2 generado por el automorfismo $\zeta \mapsto \zeta^{-1}$. Para cualquier p y cualquier r, p es el único primo que ramifica en $\mathbb{Q}_{\zeta_{p^r}}$ y ramifica totalmente (excepto para $p = 2$ y $r = 1$). Para todo $m > 2$, los primos que ramifican en $\mathbb{Q}_{\zeta_m}$ son los primos que dividen a m.*

Esto último lo podemos ver en el libro [4, páginas 256-262]

Para finalizar con los hechos, veremos un teorema que nos determina el grupo de Galois de la composición de dos extensiones de Galois.

HECHO 7. *Si K/E y L/E son extensiones de Galois cuyos grupos son G y H respectivamente, y KL/E es la composición de K y L, entonces KL/E es de Galois y su grupo de Galois es isomorfo a un subgrupo del subgrupo de $G \times H$ formado por las parejas (σ, τ) tales que σ y τ tienen las mismas restricciones en $K \cap L$.*

Con esto terminamos con los hechos y pasamos directamente con la prueba del teorema.

3.2 Demostración

Realizaremos la demostración de este teorema mediante la prueba de pequeños lemas que, al final, acabaremos relacionando para acabar con la demostración.

Comenzamos con la demostración de un lema que nos servirá de apoyo.

Lema 6. *Si Z/V_1 es abeliano, entonces T/V_1 es cíclico de orden un divisor de $q-1$*

Demostración. Localizando si es necesario, asumimos que $\mathfrak{P}$ es un ideal principal generado por un elemento π. Entonces para todo $\sigma \in Z$, como hemos visto en la demostración del teorema 5, se tiene que $\sigma(\pi) = a\pi$ donde a es un entero de K no divisible por $\mathfrak{P}$. Si $\bar{a}$ es el residuo módulo $\mathfrak{P}$, entonces por el Hecho 4, tenemos que la asignación $\sigma \mapsto \bar{a}$ induce un isomorfismo de T/V_1 en el grupo multiplicativo $\hat{K}^*$. Por lo tanto, T/V_1 es cíclico.

Ahora veremos que el orden de T/V_1 es un divisor de $q-1$. En efecto, sea $\tau \in T$ tal que la clase de τ genera T/V_1. Escogemos $\sigma \in Z$ que induce el automorfismo de Frobenius $\xi \mapsto \xi^q$ de $\hat{K}/\hat{L}$ que viene dado en el Hecho 2. Tenemos entonces que:

$$\sigma\pi = a\pi, \ \ \tau\pi = b\pi, \ \ \sigma\tau\sigma^{-1}\pi = c\pi$$

donde b y c son enteros de K no divisibles por $\mathfrak{P}$. Veamos que $\sigma^{-1}\pi = \sigma^{-1}(a)^{-1}\pi$. En efecto, partiendo de que $\sigma\pi = a\pi$, aplicando σ^{-1} en ambos lados, obtenemos que $\sigma^{-1}(\sigma\pi) = \sigma^{-1}(a\pi)$. En la parte izquierda de la igualdad, observamos que $\sigma^{-1}(\sigma\pi) = \pi$ ya que σ es un automorfismo, mientras que en la parte derecha, obtenemos que $\sigma^{-1}(a\pi) = \sigma^{-1}(a)\sigma^{-1}(\pi)$ por ser σ^{-1} morfismo. Si ahora multiplicamos en ambas partes de la igualdad $\pi = \sigma^{-1}(a)\sigma^{-1}(\pi)$ por $\sigma^{-1}(a)^{-1}$, conseguimos la expresión que buscábamos.

Si ahora utilizamos la hipótesis de que Z/V_1 es abeliano, entonces como el grupo de ramificación V_1 es un subgrupo del grupo de inercia T que a su vez es un subgrupo del grupo de descomposición Z, tenemos que el residuo de $\sigma\tau\sigma^{-1}(\pi)$ es igual al residuo de $\tau\sigma\sigma^{-1}(\pi)$ y por ser σ automorfismo, se obtiene que el residuo de $\sigma\tau\sigma^{-1}(\pi)$ (que es igual a $\bar{c}$) es exactamente el mismo que el residuo de $\tau(\pi)$ (siendo este último igual a $\bar{b}$). De esta forma, obtenemos que $\bar{c} = \bar{b}$.

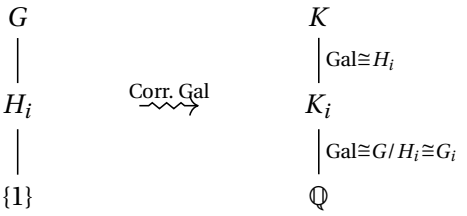
Calculamos ahora el valor de c. Anteriormente hemos definido que $\sigma\tau\sigma^{-1}\pi = c\pi$. También hemos visto que $\sigma^{-1}\pi = \sigma^{-1}(a)^{-1}\pi$. Si sustituimos podemos ver que $c\pi = \sigma(\tau(\sigma^{-1}(a)^{-1}\pi))$. Por ser τ morfismo y como $\tau\pi = b\pi$, tenemos que $c\pi = \sigma(\tau(\sigma^{-1}(a)^{-1})b\pi)$.

Por ser σ morfismo se obtiene que $c\pi = \sigma(\tau(\sigma^{-1}(a)^{-1}))\sigma(b)a\pi$ y si eliminamos π a cada lado de la igualdad nos queda que $c = \sigma(\tau(\sigma^{-1}(a)^{-1}))\sigma(b)a$. Reducimos esta ecuación módulo $\mathfrak{P}$, utilizando que $\bar{\tau} = \tau_0 = \mathrm{id}$ ya que por definición, si $t \in T$ entonces $\tau(x) \equiv x$ (mód $\mathfrak{P}$) $\forall x \in K$. También tenemos que $\overline{\sigma(b)} = \sigma_0(\bar{b}) = \bar{b}^q$ que nos da el Fobrenius del Hecho 2. De esta forma $\bar{c} = \overline{\sigma(\tau(\sigma^{-1}(a)^{-1}))\sigma(b)a}$. Si $\sigma_0 = \bar{\sigma}$, $\tau_0 = \bar{\tau}$ y $\sigma_0^{-1} = \bar{\sigma}^{-1}$ tenemos que $\bar{c} = \sigma_0\tau_0\sigma_0^{-1}(\bar{a})^{-1}\sigma_0(\bar{b})\bar{a}$. Como hemos visto anteriormente, τ_0 es la identidad, por lo que $\bar{c} = \sigma_0\sigma_0^{-1}(\bar{a})^{-1}\sigma_0(\bar{b})\bar{a}$. También hemos visto que $\overline{\sigma(b)} = \sigma_0(\bar{b})$ y como por ser σ automorfismo tenemos que $\sigma_0\sigma_0^{-1} = \mathrm{id}$, nos deja que $\bar{c} = (\bar{a})^{-1}(\bar{b})^q\bar{a} = \bar{b}^q$. Igualando con lo obtenido anteriormente, finalmente nos queda que $\bar{b} = \bar{c} = \bar{b}^q$. Por lo tanto $1 = \bar{b}^{q-1}$. Como la clase de tau es el generador de T/V_1 y hemos visto que $\bar{b}^{q-1} = 1$, es decir, que el residuo es de orden un divisor de $q-1$, tenemos que T/V_1 es de orden un divisor de $q-1$. □

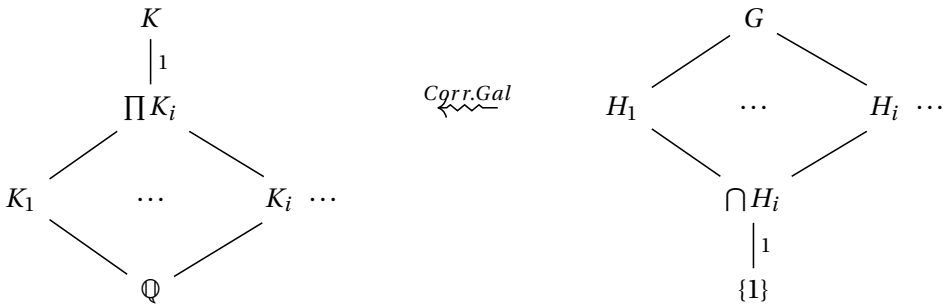
Ahora vamos a demostrar un lema que nos permitirá simplificar la demostración del teorema de K-W. Pasaremos de tener que demostrarlo para cualquier extensión abeliana a demostrarlo solo para extensiones cíclicas de orden potencia de un primo.

Lema 7. *Si el teorema de K-W es válido para extensiones cíclicas de orden potencia de un primo, entonces es válido para extensiones abelianas arbitrarias, es decir, suponiendo que todas las extensiones cíclicas de orden potencia de un primo están incluidas en una extensión ciclotómica, entonces toda extensión abeliana está incluida en una extensión ciclotómica.*

Demostración. Sea $K/\mathbb{Q}$ una extensión abeliana cuyo grupo de Galois es $G = \mathrm{Gal}(K/\mathbb{Q})$. Aplicando el teorema de clasificación de los grupos abelianos finitos, se tiene que $G \cong G_1 \times \cdots \times G_l$ donde cada G_i es cíclico de orden potencia de un primo. Si K_i es el cuerpo fijo de $H_i = \prod_{j\neq i} G_j$, entonces $K_i/\mathbb{Q}$ tiene grupo de Galois isomorfo a G_i. Veamoslo. Ya que G es abeliano, tenemos que cada H_i es un subgrupo normal de G. Por la correspondencia de Galois entre cuerpos y grupos tenemos que el grupo de Galois de la extensión K/K_i es H_i y que el grupo de Galois de la extensión $K_i/\mathbb{Q}$ es $G/H_i \cong G_i$.



Además K es la composición de todos los K_i, ya que los H_i son aquellos que tienen el neutro en la componente i-ésima de $\prod G_i$, por lo que $\bigcap H_i = \{1\}$ y entonces $K = \prod K_i$.



Por la hipótesis del lema que estamos demostrando, tenemos que los cuerpos K_i están contenidos en una extensión ciclotómica. Por lo tanto, la composición de estos K_i, que hemos visto que es igual a K, también esta contenida es una extensión ciclotómica que es lo que queríamos demostrar. □

Una vez visto que solo necesitamos considerar extensiones de grado potencia de un número primo, pasamos con un lema que establecerá, bajo algunas suposiciones adicionales, una relación entre las extensiones abelianas de grado potencia de un primo en las cuales solo dicho primo ramifica y cualquier extensión abeliana de grado potencia de un primo.

Lema 8. *Supongamos cierta la siguiente afirmación: "Sea $K/\mathbb{Q}$ una extensión abeliana de grado λ^m (con λ un número primo) donde ningún primo $p \neq \lambda$ ramifica, entonces K está incluido en una extensión ciclotómica". Entonces toda extensión abeliana de grado λ^m (con λ un número primo) está incluida en una extensión ciclotómica.*

Demostración. La estrategia de la demostración de este lema consistirá en la construcción de un cuerpo en el cual ningún primo distinto de λ ramifique. Veremos también que existe una relación entre el cuerpo construido y el cuerpo inicial, de tal forma que si el cuerpo que hemos construido está contenido en una extensión ciclotómica, entonces el cuerpo inicial también está contenido en una extensión ciclotómica.

Sea $K/\mathbb{Q}$ una extensión abeliana de grado λ^m con λ primo y sea G el grupo de Galois de la extensión $K/\mathbb{Q}$. Por el Hecho 5 sabemos que existen primos que ramifican en K. Supongamos que existe $p \neq \lambda$ que ramifica en K ya que si dicho p no existe, entonces por hipótesis la extensión $K/\mathbb{Q}$ estaría contenida en una extensión ciclotómica y habríamos terminado. Sea $\mathfrak{P}$ un ideal primo de K sobre p. Veamos que p no divide al orden de ningún cociente de subgrupos de G.

Sean H_1, H_2 subgrupos de G tales que $H_1 \subseteq H_2$. Como G es abeliano, tenemos que $H_1 \lhd G$ y por lo tanto $H_1 \lhd H_2$ (ya que si H_1 es un subgrupo normal de G y H_2 es un subgrupo de G, entonces H_1 es un subgrupo normal de H_2). Aplicando el teorema de Lagrange, sabemos que el orden de H_1 es un divisor del orden de G, el orden de H_2 es un divisor del orden de G y que $|H_2| = |H_1|[H_2 : H_1]$, lo que implica que el índice de H_1 en H_2 es un divisor del orden de G. Como p no es un divisor de $\lambda^r = |G|$ para todo $r = 1, \ldots, m$ concluimos que p no divide al índice de H_1 en H_2.

Demostremos ahora que todos los grupos de ramificación V_j , $j \geq 1$, de $\mathfrak{P}$ son triviales.

Sea $\hat{E} = \mathbb{Z}/p$ el cuerpo finito de p elementos. Aplicando la parte del Hecho 4 que nos dice que si $\hat{E}$ tiene característica p, se tiene que V_j/V_{j+1} es trivial o producto directo de grupos cíclicos de orden p. La segunda no es posible ya que, por lo visto anteriormente, $p \nmid [V_j : V_{j+1}]$. Lo que nos deja que V_j/V_{j+1} es el trivial. También por el Hecho 4 sabemos que para j suficientemente grande, V_j es trivial, lo que implica que V_{j-1} es trivial. Iterando, obtenemos que todos los V_j son triviales.

Ahora, como $T \hookrightarrow G$, tenemos que por el teorema de Lagrange $|T| \,||G|$, lo que nos dice que $|T| = \lambda^u$ para un cierto $u \leq m$.

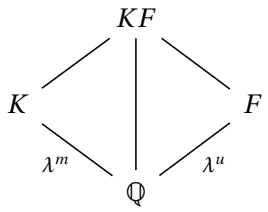
Aplicamos el Lema 6 considerando el caso en el que $L = \mathbb{Q}$, $q = p$ y como V_1 es trivial, $Z/V_1 \cong Z$ y es abeliano por ser subgrupo de G que es abeliano por hipótesis, entonces $T/V_1 \cong T$ es cíclico de orden divisor de $p-1$, o lo que es lo mismo, como $|T| = \lambda^u$, $p \equiv 1 \pmod{\lambda^u}$

Como p es primo, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es una extensión cíclica de orden $p-1$. Por lo visto justo anteriormente, λ^u divide a $p-1$ entonces al ser $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ cíclica, existe un único subgrupo H de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ con índice λ^u. Por la correspondencia de Galois entre grupos y cuerpos vemos que el grado de la extensión $F/\mathbb{Q}$ es λ^u como podemos ver en el siguiente esquema.

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & & \mathbb{Q}(\zeta_p) \\ \Big| \lambda^u & \overset{Corr.Gal}{\rightsquigarrow} & \Big| \\ H & & F \\ \Big| & & \Big| \lambda^u \\ \{1\} & & \mathbb{Q} \end{array}$$

Tenemos que F es el único subcuerpo de $\mathbb{Q}(\zeta_p)$ de grado λ^u sobre $\mathbb{Q}$ y además es cíclico. Por el Hecho 6, p es el único primo que ramifica en $\mathbb{Q}(\zeta_p)$ y ramifica totalmente. Como $F \subset \mathbb{Q}(\zeta_p)$, p también ramifica totalmente en F ya que si p no ramificase en F, como ningún otro primo ramifica en F, por el Hecho 5 tendríamos que $F = \mathbb{Q}$ y tendríamos una contradicción.

Construimos la composición de K y F y veamos que grado tiene sobre $\mathbb{Q}$.



El levantamiento de una extensión de Galois es de Galois y su grupo es isomorfo a un subgrupo del inicial, por lo tanto el grado de la extensión $[KF:K]$ es un divisor de λ^u, es decir, $[KF:K] = \lambda^v$ con $v \leq u$ y $[KF:\mathbb{Q}] = [K:\mathbb{Q}][KF:K] = \lambda^{m+v}$

Sea $\mathfrak{P}'$ un ideal primo de KF sobre $\mathfrak{P}$, T' el grupo de inercia de $\mathfrak{P}'$ sobre p, H el grupo de Galois de $F/\mathbb{Q}$. Por el Hecho 7, tenemos que el monomorfismo habitual es $\mathrm{Gal}(KF/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q})$, donde se asigna σ al par $(\sigma|_K, \sigma|_F)$. Si tomamos un elemento de T', la primera componente de la imagen está en T (ya que como $\mathfrak{P}'$ contiene a $\mathfrak{P}$, se tiene que T es un subgrupo de T'), por lo que tenemos que $T' \lhd T \times H$.

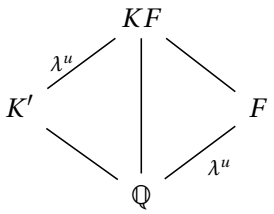
Por el Hecho 3, el orden de T' es el índice de ramificación de $\mathfrak{P}'$ sobre p y ya que T es un subgrupo de T', tenemos que $|T'| \geq \lambda^u$. Podemos verlo en el siguiente esquema.

$$\begin{array}{ccc} \mathfrak{P}' & & \\ \Big| \geq 1 & & \\ \mathfrak{P} & \longrightarrow & |T'| \geq \lambda^u \\ \Big| \lambda^u & & \\ p & & \end{array}$$

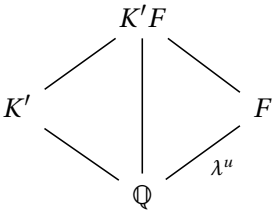
Al igual que ocurría con T, todos los V_j' para $j \geq 1$ de $\mathfrak{P}'$ son triviales y por el Lema 6 se tiene que T' es cíclico. Además, $T \times H$ no tiene elementos de orden mayor que

λ^u ya que $|T| = \lambda^u = |H|$, lo que implica que si tomamos $(\alpha, \beta) \in T \times H$, $|\langle(\alpha, \beta)\rangle| = \text{mcm}(|\alpha|, |\beta|) \leq \lambda^u$. Con esto llegamos a que $|T'| = \lambda^u$

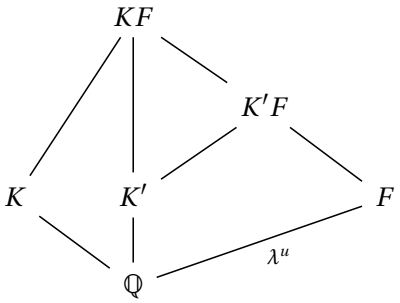
Definimos K' como el cuerpo fijo por T'. El Hecho 3 nos dice que si K' es el cuerpo fijo por T' y $\mathfrak{P}'' = \mathfrak{P}' \cap K'$, entonces $\mathfrak{P}''$ no ramifica sobre p. Aparte, $K' \cap F = \mathbb{Q}$ por la expresión $n = efg$, ya que si p ramifica totalmente en F, entonces $g = f = 1$ y si p no ramifica en K', entonces $e = 1$. Esto implica que $n = 1$ y el grado de la extensión $[K' \cap F : \mathbb{Q}] = 1$ y $K' \cap F = \mathbb{Q}$.



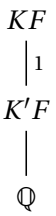
Como K' es el cuerpo fijo por T' que es un subgrupo de $\text{Gal}(KF/\mathbb{Q})$, por el teorema de Artin tenemos que grado de la extensión KF/K' es el orden de T', λ^u, que coincide con $[F : \mathbb{Q}]$.



Como $K' \cap F = \mathbb{Q}$ y hemos visto que $[KF : K'] = \lambda^u = [F : \mathbb{Q}]$, se tiene que $[K'F : \mathbb{Q}] = [K' : \mathbb{Q}][F : \mathbb{Q}] = [K' : \mathbb{Q}][KF : K'] = [KF : \mathbb{Q}]$. Podemos verlo en el siguiente esquema.



Por lo tanto tenemos que $K'L \subseteq KL$ por construcción y que $[K'F : \mathbb{Q}] = [KF : \mathbb{Q}]$, lo que implica que $K'L = KL$.



Si demostrásemos que K' está contenido en una extensión ciclotómica, entonces $K'F = KF$ estaría contenido en una extensión ciclotómica, con lo que K también lo estaría. Lo que ocurre es que ahora p no ramifica en K' y además no existen nuevos primos que ramifiquen en K'. Veamos esto último con algo más de detalle.

Supongamos que p^* ramifica en K' y p^* no ramifica en K. Como ramifica en K', p^* ramifica en $K'F = KF$. Sea T'_{p^*} el grupo de inercia de un ideal primo de KF, $\mathfrak{Q}'$, que contiene a p^* y sea T_{p^*} el grupo de inercia de un ideal primo de K, $\mathfrak{Q}$, que contiene a p^*. Hemos visto anteriormente que $T'_{p^*} \subset T_{p^*} \times H$ pero como p^* no ramifica en K, $T_{p^*} = \{e\}$ y $H = \{e\}$ lo que implica que $T'_{p^*} = \{e\}$. Contradicción con la suposición de que p^* ramifica en K'.

Repitiendo este proceso, construiríamos un cuerpo en el cual ningún primo distinto de λ ramificaría, llamémoslo K_λ. Para demostrar que K está contenido en una extensión ciclotómica, como hemos visto anteriormente, tendríamos que demostrar que K_λ está contenido en una extensión ciclotómica y por hipótesis, K_λ lo está. □

Ahora vamos con un par de corolarios cuyas demostraciones se deducen de forma trivial del lema anterior.

Corolario 8.1. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado λ^m (λ primo) y suponemos que $p \neq \lambda$ es el único primo que ramifica en K. Entonces p ramifica totalmente en K,*

$$p \equiv 1 \pmod{\lambda^m}$$

y K es el único subcuerpo de $\mathbb{Q}(\zeta_p)$ de grado λ^m, en particular, $K/\mathbb{Q}$ es una extensión cíclica.

Demostración. En la demostración del lema anterior hemos construido K' que era el cuerpo fijo por T'. Hemos visto que en este cuerpo p no ramifica y ningún otro primo nuevo ramifica, por lo que por el Hecho 5, $K' = \mathbb{Q}$ y $K'F = F = KF$, lo que implica que $K = F$. Las propiedades de F eran que p ramificaba totalmente en él, $p \equiv 1 \pmod{\lambda^m}$, era el único subcuerpo de $\mathbb{Q}(\zeta_p)$ de orden λ^m y era cíclico. Con esto concluye la demostración de este corolario. □

Corolario 8.2. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado impar, entonces 2 no ramifica en K*

Demostración. En el Lema 8 hemos visto que V_j son triviales para todo $j \geq 1$, en particular lo es V_1. Como $Z/V_1 \cong Z$ es abeliano ya que $G = \mathrm{Gal}(K/\mathbb{Q})$ es abeliano, podemos aplicar el Lema 6 que nos dice que $T/V_1 \cong T$ es cíclico de orden $2-1=1$. Por el Hecho 3 el orden del grupo de inercia coincide con índice de ramificación, lo que nos dice que 2 no ramifica en K. □

Hasta aquí, lo que hemos hecho ha sido reducir el teorema de tal forma que solo necesitaremos considerar el caso de las extensiones de grado λ^m, con λ el único primo que ramifica. A partir de ahora, separaremos en dos diferentes casos: el primero es que λ sea un primo impar y el segundo es que $\lambda = 2$.

Comencemos con el primer caso, extensiones abelianas de grado λ^m con λ primo impar. Demostraremos que estas extensiones son cíclicas, pero para ello, necesitaremos el siguiente lema.

Lema 9. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado un primo impar, λ, en la cual el único primo que ramifica es λ, entonces V_2 es trivial.*

Demostración. Utilizaremos la misma técnica que en la demostración del Lema 6. Localizando, si es necesario, suponemos que el ideal primo $\mathfrak{p}$ es principal y esta generado por un elemento π. Sea $f(x)$ el polinomio mínimo de π sobre $\mathbb{Q}$; sea v la valoración de K asociada a $\mathfrak{p}$ (la definición de la valoración se encuentra en el teorema 5). Por el Hecho 4 sabemos que para j suficientemente grande, V_j es trivial. Supongamos que V_{j+1} es el primer grupo de ramificación trivial.

Por el Hecho 4 otra vez, tenemos que V_j/V_{j+1} es trivial o cíclico de orden λ, pero en el caso que nos ocupa, se tiene que $V_j/V_{j+1} \cong V_j$ es de orden λ. Puesto que el orden de G es λ, tenemos que $G = V_j$.

Veamos ahora que $v(f'(\pi)) = (j+1)(\lambda-1)$.

La derivada del polinomio irreducible $f'(\pi)$ se puede ver como $\prod_{x_j \neq \pi}(\pi - x_j)$ donde $x_j = \sigma\pi$ son las imágenes de π por los elementos de G tales que $\sigma \neq \mathrm{id}$. Por lo tanto $f'(\pi) = \prod_{\sigma \neq \mathrm{id}}(\pi - \sigma\pi)$. Como $V_j = G$ y $V_{j+1} = \{e\}$, entonces las sigmas que aparecen en el producto anterior también se pueden escribir como las sigmas de $V_j - V_{j+1}$.

Ya que $\sigma \in V_j$, implica que $\pi - \sigma\pi \in \mathfrak{p}^j$. Por lo que hemos visto en la demostración del teorema 5, tenemos que $\pi - \sigma\pi \in \mathfrak{p}^{j+1}$ y entonces $v(\pi - \sigma\pi) \geq (j+1)$. Como hemos considerado que $\sigma \neq \mathrm{id}$ y que V_{j+1} es trivial, podemos decir que $\pi - \sigma\pi$ no pertenece a $\mathfrak{p}^k$ para todo $k \geq j+2$, por lo tanto $v(\pi - \sigma\pi) = (j+1)$. Juntando esto con el hecho de que $|V_j - V_{j+1}| = \lambda - 1$, obtenemos lo que buscábamos, que $v(f'(\pi)) = v(\prod_{\sigma \in V_j - V_{j+1}}(\pi - \sigma\pi)) = (j+1)(\lambda-1)$.

Por otra parte podemos escribir $f'(\pi)$ de la siguiente forma:

$$f'(\pi) = \lambda\pi^{\lambda-1} + a_{\lambda-1}(\lambda-1)\pi^{\lambda-2} + \cdots + a_1$$

donde los a_i son enteros por ser los coeficientes de un polinomio irreducible de un entero algebraico.

Sea T el grupo de inercia de $\mathfrak{p}$, entonces por el Hecho 3, λ no ramifica en $K' = \{\alpha \in K : \sigma\alpha = \alpha \ \forall \sigma \in T\}$. Sea $G' = \mathrm{Gal}(K'/\mathbb{Q}) \cong G/T$ donde $G = \mathrm{Gal}(K/\mathbb{Q})$. Por el Hecho 5, como ningún primo ramifica en K', $K' = \mathbb{Q}$, lo que implica que $G' = \{e\} \cong G/T$ siendo $G \neq \{e\}$. De esta forma vemos que ha de ocurrir que $T = G$ y gracias al Hecho 3 sabemos que el índice de ramificación es igual a $|T| = \lambda^m$ y λ ramifica totalmente en K. De esta forma, tenemos que $v(\lambda) = \lambda$.

Como λ es primo, la potencia más pequeña de π que da un entero (de $\mathbb{Z}$) es λ ya que si no ocurriera esto, λ factorizaría. Además, la valoración de todo entero (de $\mathbb{Z}$) es múltiplo de λ. En efecto, si una cierta potencia π^k de π es entera, entonces, tomando $b = k \pmod{\lambda}$, tendríamos que π^b es un entero con $b < \lambda$, lo que contradice lo visto anteriormente. Con esto hemos visto que $v(a_i) \equiv 0 \pmod{\lambda}$.

Ahora consideramos $a_{\lambda-i+1}(\lambda-i+1)\pi^{\lambda-i}$ que es el término de $f'(\pi)$ que involucra $\pi^{\lambda-i}$ para cada i. Entonces consideremos $v_i = v(a_{\lambda-i+1}(\lambda-i+1)\pi^{\lambda-i})$. La valoración del producto es igual a la suma de las valoraciones por lo que $v_i = v(a_{\lambda-i+1}) + v(\lambda-i+1) + v(\pi^{\lambda-i})$. Veamos que ocurre con la valoración de cada término por separado. Como $a_{\lambda-i+1}$ y $\lambda-i+1$ son enteros, tenemos que $v(a_{\lambda-i+1}) \equiv 0 \pmod{\lambda}$ y $v(\lambda-i+1) \equiv 0 \pmod{\lambda}$. Por definición de valoración tenemos que $v(\pi^{\lambda-i}) = \lambda - i$. De esta forma obtenemos que $v_i \equiv \lambda - i \pmod{\lambda}$.

Comprobaremos ahora que $v(f'(\pi))$ es igual al mínimo de todos los v_i mencionados antes. Hemos visto que $v_i \equiv \lambda - i \pmod{\lambda}$ por lo que todas las valoraciones son diferentes. Supongamos que b y c son dos enteros tales que $v_i = v(b)$ y $v_j = v(c)$ para ciertos $i, j \in \{1, \dots, \lambda - 1\}$. Veamos que si $v_i < v_j$ entonces $v(c+b) = v(b)$. En efecto, lo que nos dice la valoración es que $b = \pi^{v(b)u}$ y $pi^{v(c)u'}$ siendo u y u' dos unidades. Entonces $b + c = \pi^{v(b)(u+(v(c)-v(b))u')}$ donde π no divide a $u + (v(c) - v(b))u'$, por lo tanto tenemos que $v(c+b) = v(b)$. Si aplicamos esto iterativamente para todos los v_i, tendremos que $v(f'(\pi)) = v(\sum v_i) = \min_{1 \le i \le \lambda - 1}\{v_i\}$. Consideramos la valoración de v_1 que es la siguiente:

$$v_1 = v(\lambda \pi^{\lambda - 1}) = v(\lambda) + v(\pi^{\lambda - 1}) = \lambda + \lambda - 1 = 2\lambda - 1$$

Entonces, para acabar con la demostración de este lema, observemos que $2\lambda - 1 \ge v(f'(\pi)) = \min_{1 \le i \le \lambda - 1}\{v_i\} = (j+1)(\lambda - 1)$ que es lo que hemos visto durante la prueba del lema. Como $\lambda > 2$, el único $j \ge 1$ que satisface la inecuación es $j = 1$, por lo tanto $V_{j+1} = \{e\} = V_2$ es trivial. □

Lema 10. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado λ^m, siendo λ primo impar, en la cual el único primo que ramifica es λ, entonces $K/\mathbb{Q}$ es cíclica.*

Demostración. Sea T el grupo de inercia de un primo $\mathfrak{p}$ que contiene a λ, entonces por lo visto anteriormente en el Lema 9, podemos decir que λ ramifica totalmente en K. Por ser λ totalmente ramificado, $|\hat{K}| = |\mathcal{O}_K/\mathfrak{p}| = q^f$ siendo $f = 1$, $q = \lambda$ y $\hat{K}$ el cuerpo finito con λ elementos. Como ninguna potencia de λ divide a $\lambda - 1$, por el Hecho 4 tenemos que $T = V_1$ y también sabemos que para $j \ge 1$, V_j/V_{j+1} es trivial o es cíclico de orden λ.

Para el caso $m = 1$, en el Lema 9 hemos visto que V_2 es trivial. Considerando que $G = T = V_1$ y como $V_1/V_2 \cong V_1$ es cíclico, para el caso $m = 1$ la extensión $K/\mathbb{Q}$ es cíclica.

Para el caso $m > 1$, si vemos que V_2 es el único subgrupo de $G = V_1$ de índice λ, entonces G sería cíclico. Esto ocurre por el siguiente motivo:

Nuestra hipótesis es que V_2 es el único subgrupo de índice λ. Si G es abeliano de orden λ^m, por el teorema de clasificación de los grupos abelianos finitos, $G \cong G_1 \times \cdots \times G_n$ siendo los G_i cíclicos. Supongamos que G no es cíclico, entonces existen al menos dos grupos G_1, G_2 grupos cíclicos tales que $G \cong G_1 \times G_2 \cdots$. Como G_i son cíclicos y son de orden una potencia de λ, tienen un único subgrupo de índice λ, llamémoslos H_i. Entonces $H_1 \times G_2 \cdots$ y $G_1 \times H_2 \cdots$ son subgrupos de índice λ. Contradicción con nuestra hipótesis y G es cíclico.

Veamos que V_2 es el único subgrupo de índice λ de G. Sea H un subgrupo de G de índice λ, $\tilde{K}$ es el cuerpo fijo por H, $\tilde{G} \cong G/H$ es el grupo de Galois de $\tilde{K}$ sobre $\mathbb{Q}$, $\tilde{V}_j$ el j-ésimo grupo de ramificación de $\tilde{K}$.

$$\begin{array}{ccc} G & & K \\ \Big| \lambda & & \Big| \\ H & \overset{Corr.Gal}{\rightsquigarrow} & \tilde{K} \\ \Big| & & \Big| \lambda \\ \{1\} & & \mathbb{Q} \end{array}$$

Tenemos que V_j restringido a $\tilde{K}$ es $\tilde{V}_j$ y por el Lema 9, sabemos que $\tilde{V}_2$ es trivial, por lo tanto $V_2 \lhd H$. Tenemos que V_2 es distinto de G ya que V_2 es un subgrupo de H

que a su vez está estrictamente contenido en G. De esta forma, por lo que hemos visto anteriormente en la demostración de este lema, V_j/V_{j+1} es trivial o cíclico de orden λ y entonces se tiene que V_1/V_2 es cíclico de orden λ ya que $G = V_1 \neq V_2$. Podemos tomar como H al primer $V_j \neq G$ ya que este sería un subgrupo de G de índice λ como hemos visto durante la demostración de este lema, entonces tomamos $H = V_2$ al tener que $(G = V_1)/V_2$ es de orden λ.

Podemos tomar como H al primer $V_j \neq G$ ya que este sería un subgrupo de G de índice λ por lo que hemos visto durante la demostración

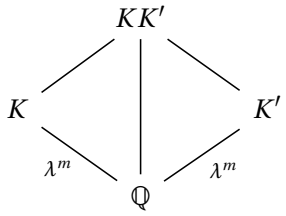
Veamos que V_2 es el único subgrupo de índice λ. Hemos visto que $V_2 \lhd H$ para todo H de índice λ. Si V_2 y H son dos subgrupos con el mismo índice en G y uno está contenido en el otro, han de ser el mismo. Por esto V_2 es el único subgrupo de índice λ de G y $K/\mathbb{Q}$ es cíclica. □

En el siguiente lema veremos que el teorema de K-W es valido para las extensiones que estamos estudiando ahora.

Lema 11. *El teorema de K-W se cumple para extensiones abelianas $K/\mathbb{Q}$ de grado λ^m, λ primo impar.*

Demostración. Gracias al Lema 8 y al Hecho 5, podemos suponer que λ es el único primo que ramifica en K. Sea ζ la raíz λ^{m+1}-ésima de la unidad. Sea K' el único subcuerpo de $\mathbb{Q}(\zeta)$ de grado λ^m sobre $\mathbb{Q}$ (por el Hecho 6, $\mathbb{Q}(\zeta)$ es cíclico de orden $\lambda^m(\lambda-1)$, por lo que existe un único subgrupo de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ con índice λ^m). También por el Hecho 6, λ es el único primo que ramifica en K'.

Lo que queremos ver es que $K = K'$ para completar la demostración de este lema. Lo veremos por contradicción. Supongamos que $K' \neq K$, entonces λ sería el único primo que ramifica en la composición KK' que es abeliana.



Como $K' \neq K$. tenemos que el grado de la extensión KK' sobre $\mathbb{Q}$ es $[KK' : \mathbb{Q}] = \lambda^n$ con n tal que $n > m$.

Por Lema 10, sabemos que KK' es cíclico sobre $\mathbb{Q}$ pero por el Hecho 7, ningún elemento de $\mathrm{Gal}(KK'/\mathbb{Q})$ tiene orden $> \lambda^m$. Veamoslo.

Tenemos que $\mathrm{Gal}(KK'/\mathbb{Q})$ es cíclico, sea σ su generador. Sean $G = \mathrm{Gal}(K/\mathbb{Q})$ y $G' = \mathrm{Gal}(K'/\mathbb{Q})$ los grupos cíclicos generados por τ_1 y τ_2 respectivamente. Por el isomorfismo del Hecho 7 entre $\mathrm{Gal}(KK'/\mathbb{Q})$ y un subgrupo de $G \times G'$ se tiene que $\sigma = (\tau_1^s, \tau_2^s)$. Entonces el orden de σ es igual al $\mathrm{mcm}(|\tau_1^s|, |\tau_2^s|) \leq \lambda^m$. Contradicción ya que el orden de $\mathrm{Gal}(KK'/\mathbb{Q})$ es mayor que λ^m. Esta contradicción viene de suponer que $K \neq K'$. Con esto acabamos la demostración de este lema ya que hemos visto que K es está contenido en una extensión ciclotómica. □

El siguiente corolario viene directamente de la demostración del Lema 11.

Corolario 11.1. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado λ^m, λ un primo impar, donde λ es el único primo que ramifica, entonces K es el único subcuerpo de $\mathbb{Q}(\zeta_{\lambda^{m+1}})$ de grado λ^m.*

Con esto finalizamos el caso de las extensiones de grado λ^m con λ primo impar. Ahora comenzaremos con el caso de extensiones de grado 2^m. En el siguiente lema veremos el caso con $m = 1$.

Lema 12. *Toda extensión cuadrática de $\mathbb{Q}$ está contenida en una extensión ciclotómica.*

Demostración. La demostración de este lema se reduce a considerar solo las extensiones cuadráticas de la forma $\mathbb{Q}(\sqrt{\pm p})$ siendo p primo ya que si tenemos a que no es primo, entonces se tiene que $a = \pm p_1^{r_1} \cdots p_k^{r_k}$ donde $p_1 \cdots p_k$ son primos y $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{\pm \prod_i p_i})$ y por lo tanto $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_k})$.

Separaremos en dos casos:

El primer caso es en el que $p = 2$. Tenemos que $\mathbb{Q}(\sqrt{\pm 2}) \subseteq \mathbb{Q}(\zeta_8)$ ya que

$$\zeta_8 + \zeta_8^{-1} = e^{\frac{2\pi i}{8}} + \frac{1}{e^{\frac{2\pi i}{8}}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} + \frac{\sqrt{2}(1-i)}{2} = \sqrt{2}$$

y

$$\zeta_8 + \zeta_8^3 = e^{\frac{2\pi i}{8}} + e^{\frac{3\pi i}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \sqrt{-2}$$

A partir de ahora, consideraremos p como un primo impar. Puesto que p es un número primo, el polinomio irreducible de ζ_p es $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Consideramos el discriminante del polinomio que viene definido de la siguiente forma:

$$\Delta = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2$$

que es un cuadrado de $\mathbb{Q}(\zeta_p)$ ya que $\zeta_p^i \in \mathbb{Q}(\zeta_p)\ \forall i$ y la resta y producto de elementos de $\mathbb{Q}(\zeta_p)$ pertenece a $\mathbb{Q}(\zeta_p)$ por definición de cuerpo. Utilizaremos el discriminante para ver que $\sqrt{\pm p}$ están contenidos en una extensión ciclotómica.

Veamos que $\Delta = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Sea $g(x) = x^p - 1$. Para calcular el discriminante de g, lo calcularemos mediante la resultante de g y g' ya que $\operatorname{res}(g, g') = (-1)^{\frac{p(p-1)}{2}} \operatorname{disc}(g)$. Veamos que vale $\operatorname{res}(g, g')$.

$$\operatorname{res}(g, g') = \prod_{i=1}^{p} g'(\alpha_i) = \prod_{i=1}^{p} p\alpha_i^{p-1} = p^p \left(\prod_{i=1}^{p} \alpha_i \right)^{p-1} = (-1)^{p(p-1)} p^p = p^p$$

ya que $p(p-1)$ es par, entonces $(-1)^{p(p-1)} = 1$. Aquí vemos que $\operatorname{disc}(g) = (-1)^{\frac{p(p-1)}{2}} p^p$ y como p es impar tenemos que $\operatorname{disc}(g) = (-1)^{\frac{(p-1)}{2}} p^p$.

Para calcular el discriminante de f, Δ, que es lo que buscamos, consideramos el polinomio $r(x) = x - 1$. De esta forma tenemos que $rf = g$, lo que implica que $(-1)^{\frac{(p-1)}{2}} p^p = \operatorname{disc}(g) = \operatorname{disc}(rf)$. La derivada de r es $r' = 1$ lo que implica que $\operatorname{disc}(r') = 1 = \operatorname{res}(p.p')$. De este modo, $\operatorname{res}(f, r) = (-1)^{p-1} \prod f(\beta_i) = f(1) = p$ donde β_i son las raíces de $r(x)$. Aplicando el resultado que nos dice que

$$\operatorname{disc}(rf) = \operatorname{disc}(f) \operatorname{disc}(r) \operatorname{res}(r, f)^2$$

obtenemos que el discriminante de f es el siguiente

$$\text{disc}(f) = \Delta = (-1)^{\frac{(p-1)}{2}} p^{p-2}$$

Para terminar de ver que $\mathbb{Q}(\sqrt{\pm p})$ está contenido en una extensión ciclotómica, probaremos que $\sqrt{\pm p} \in \mathbb{Q}(\zeta_p, i)$

Podemos escribir $\sqrt{p}$ como

$$\sqrt{p} = \frac{\sqrt{(-1)^{(p-1)/2}\Delta}}{p^{\frac{p-3}{2}}}$$

que es una combinación de elementos de $\mathbb{Q}(\zeta_p, i)$ ya que hemos visto que Δ es un elemento de $\mathbb{Q}(\zeta_p)$, $(-1)^{(p-1)/2}$ es un elemento de $\mathbb{Q}$ si $(p-1)/2$ es par y es un elemento de $\mathbb{Q}(i)$ si $(p-1)/2$ es impar, por lo tanto la raíz cuadrada del producto entre $(-1)^{(p-1)/2}$ y Δ pertenece a $\mathbb{Q}(\zeta_p, i)$ y como $p^{\frac{p-3}{2}}$ es un elemento de $\mathbb{Q}$, tenemos que $\frac{\sqrt{(-1)^{(p-1)/2}\Delta}}{p^{\frac{p-3}{2}}}$ es un elemento de $\mathbb{Q}(\zeta_p, i)$. Para el caso de $\sqrt{-p}$, lo podemos escribir como

$$\sqrt{-p} = \frac{\sqrt{(-1)^{(p-3)/2}\Delta}}{p^{\frac{p-3}{2}}}$$

que por la misma razón que $\sqrt{p}$, pertenece a $\mathbb{Q}(\zeta_p, i)$.

Para terminar con la demostración de este lema, veamos que $\mathbb{Q}(\zeta_p, i) = \mathbb{Q}(\zeta_{4p})$. Observemos que $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$, entonces tenemos que $\mathbb{Q}(\zeta_p, i) = \mathbb{Q}(\zeta_p, \zeta_4) = \mathbb{Q}(\zeta_{\text{mcm}(4,p)}) = \mathbb{Q}(\zeta_{4p})$. Con esto conseguimos la igualdad y acabamos la demostración de este lema. □

Para finalizar con la demostración del teorema de K-W, solo nos faltaría probar que las extensiones cíclicas de grado 2^m para $m > 1$ están contenidas en una extensión ciclotómica. Vamos a verlo en el siguiente lema.

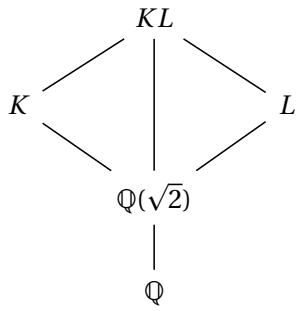
Lema 13. *Toda extensión cíclica $K/\mathbb{Q}$ de grado 2^m está contenida en una extensión ciclotómica.*

Demostración. La demostración de este lema la realizaremos por inducción completa sobre m. Para el caso $m = 1$ ya lo hemos visto, es el Lema 12.

Supongamos cierto ahora desde 1 hasta $m-1$ y veamos si es cierto para m. Gracias al Lema 8 y al Hecho 5, podemos suponer que 2 es el único primo que ramifica en K. Asumimos que K está contenido en el cuerpo de los complejos. La conjugación compleja restringida a K es la identidad o un automorfismo de orden 2 (depende de si K es real o no). Entonces el cuerpo fijo por la conjugación compleja es real (ya que si $x \in K$ es fijo por la conjugación compleja, $\text{conj}(x) = x$, lo que implica que x es real) y tiene grado al menos 2^{m-1} sobre $\mathbb{Q}$. Como $K/\mathbb{Q}$ es cíclica, existe un único subcuerpo cuadrático K' que tiene que ser real (ya que hemos visto que existe un cuerpo K' que es real, contenido en K que es cíclica, de orden al menos 2^{m-1} sobre $\mathbb{Q}$ y estamos suponiendo que $m > 1$). Como el único primo que ramifica en K es 2, tenemos que el único primo que puede ramificar en K' es 2. Por el Hecho 5, como la extensión $K'/\mathbb{Q}$ no es trivial, se tiene que existe algún primo que ramifica en K'. Con estas dos condiciones, tenemos que 2 ramifica en K' y es el único primo que ramifica. Ya que $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es la

única extensión cuadrática en la que 2 es el único primo que ramifica, observamos que $K' = \mathbb{Q}(\sqrt{2})$.

Sea $\zeta = \zeta_{4n}$ siendo $n = 2^m = [K : \mathbb{Q}]$. Por el Hecho 6 sabemos que $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong T \times S$ donde T es cíclico de orden n y S es de orden 2 generado por el automorfismo $\zeta \mapsto \zeta^{-1}$, por lo que $L = \mathbb{Q}(\zeta + \zeta^{-1})$ es el cuerpo fijo por S. Además, 2 es el único primo que ramifica en $\mathbb{Q}(\zeta)$, entonces también es el único primo que ramifica en L. Al igual que antes, $\mathbb{Q}(\sqrt{2})$ es el único subcuerpo cuadrático de L.



El grado de la extensión $[KL : \mathbb{Q}]$ es menor que n^2 ya que tienen un subcuerpo de grado 2 sobre $\mathbb{Q}$ en común.

Sea Γ el grupo de Galois de la extensión $KL/\mathbb{Q}$ que es un subgrupo propio de $G \times H$ donde $G = \mathrm{Gal}(K/\mathbb{Q})$ y $H = \mathrm{Gal}(L/\mathbb{Q})$. Como G y H son cíclicos, tomamos σ, τ que son los generadores de cada uno respectivamente. Se tiene que $(\sigma, \tau) \in \Gamma$ y generan un subgrupo Δ de orden n (σ y τ tienen orden n). El cuerpo fijo F de Δ tiene grado 2^r sobre $\mathbb{Q}$ con $r < m$ ya que $|\Delta| = n \leq |\Gamma| < n^2$ lo que implica que $[\Gamma : \Delta] < \frac{n^2}{n} = n = 2^m$ y $[\Gamma : \Delta] \mid 2^m$. Además, 2 sigue siendo el único primo que ramifica en F, entonces por inducción, F está incluido en una extensión ciclotómica. Ahora si vemos que $FL = KL$, como F y L están incluidos en una extensión ciclotómica, la composición está incluida en una extensión ciclotómica y entonces K ha de estar incluido en una extensión ciclotómica que es lo que buscamos.

La inclusión $FL \subseteq KL$ es trivial ya que por construcción $F \subseteq KL$. Para ver la igualdad, nos faltaría ver que el grupo de Galois $\mathrm{Gal}(KL/FL)$ es trivial.

Sea $\phi \in \mathrm{Gal}(KL/FL)$, en particular, ϕ fija FL por definición de los elementos del grupo de Galois y por lo tanto fija $F \subseteq FL$. Entonces $\phi \in \Delta$ por ser F el cuerpo fijo por $\Delta = \langle(\sigma, \tau)\rangle$ y $\phi = (\sigma^k, \tau^k)$. Por el mismo motivo que ϕ fija F, también fija L y esto nos dice que $\tau^k = \mathrm{id}$ ya que por construcción de L, tenemos que el único automorfismo de Δ que restringido a L sea la identidad es el propio automorfismo identidad. Como τ y σ tienen el mismo orden, $\sigma^k = \mathrm{id}$. Hemos visto que para cualquier elemento $\phi \in \mathrm{Gal}(KL/FL)$ es la identidad y $\mathrm{Gal}(KL/FL)$ es trivial. Por lo dicho anteriormente, K está incluido en una extensión ciclotómica. □

Con serie de lemas, podemos pasar a demostrar el teorema de Kronecker-Weber.

Teorema 14 (Teorema de Kronecker-Weber)**.** *Toda extensión abeliana finita $K/\mathbb{Q}$ está contenida en una extensión ciclotómica.*

Demostración. Sea $K/\mathbb{Q}$ una extensión abeliana. Por el Lema 7 podemos suponer que esta extensión es de grado λ^m con λ primo. Gracias al Lema 8 podemos suponer que λ es el único primo que ramifica en K. En el Lema 10 vemos que la extensión $K/\mathbb{Q}$ es

cíclica. Acabamos la demostración de este teorema con el Lema 11 si λ es un primo impar y con el Lema 13 si $\lambda = 2$. □

CAPÍTULO 4

CONCLUSIONES

En este documento hemos visto una de varias demostraciones del teorema de Kronecker-Weber realizada por M, J. Greenberg. Comenzamos con una pequeña introducción al anillo de enteros y a la teoría de ramificación, viendo conceptos como el de dominio de Dedekind, definiendo el grupo de descomposición, los grupos de ramificación y comentando algunas de las propiedades que cumplen. En este apartado hemos probado lo que en el documento de Greenberg (y más tarde nosotros) llama "Hechos".

Si pasamos al Capítulo 3, donde podemos encontrar la parte principal de este documento, hemos explicado con más detalle los "Hechos", añadiendo esquemas que ayudan a visualizar la teoría que contienen.

Ahora se detallaran qué resultados han sido más desarrollados.

En el Lema 6 hemos expandido detalles que quedaban algo escuetos, como el significado de localizar y el por qué el orden de $\bar{b}$ nos indica el orden de T/V_1. También hemos realizado más detalladamente todos los cálculos que aparecen en este lema.

Continuamos con el Lema 7. En este lema, especialmente, hemos demostrado que $K_i/\mathbb{Q}$ tiene grupo de Galois isomorfo a G_i y que $K = \prod K_i$. También hemos añadido dos esquemas que representan lo que ocurre en esta demostración.

Proseguimos con el Lema 8, el que más se ha desarrollado en este documento. Se ha añadido la demostración de por qué p no divide al orden de ningún subgrupo del grupo de Galois. También hemos visto que todos los grupos de ramificación (menos el grupo de inercia) son triviales. Hemos realizado el cálculo de grado de extensiones y las hemos apoyado con esquemas que los explican. Para acabar con la demostración de este lema, hemos visto que no existen nuevos primos que ramifiquen en el cuerpo K' y que si K' estuviese contenido en una extensión ciclotómica, entonces K también estaría contenido en una extensión ciclotómica.

En los próximos corolarios, prácticamente no se ha añadido nada ya que ambos se deducen de forma trivial del Lema 8.

El Lema 9 coincide con el sublema del documento de Greenberg. En este lema hemos demostrado las propiedades de la valoración de un entero y hemos expandido todos los cálculos de valoraciones.

Si seguimos con el Lema 10, lo que hemos añadido es un esquema explicativo y la demostración de por qué si vemos que V_2 es el único subgrupo de orden λ del grupo de Galois, entonces el grupo de Galois es cíclico.

En el Lema 11 se ha extendido la demostración de que $K = K'$ y además se ha añadido un esquema representativo.

Para el Lema 12, la demostración del caso $p = 2$ se ha realizado de forma más extensa, expresando todos los cálculos. Para el caso de p primo, se ha añadido todo el cálculo del discriminante de del polinomio irreducible de ζ_p. Además, se ha comprobado que $\sqrt{\pm p}$ está contenido en una extensión ciclotómica que es $\mathbb{Q}(\zeta_{4p})$.

En el último lema, el lema Lema 13, se ha explicado el funcionamiento de la conjugación compleja como automorfismo del grupo de Galois. También se ha añadido un esquema y se ha demostrado con más detalle que $FL = KL$.

Para acabar con el documento, se ha añadido un teorema en el que se enlazan los lemas demostrados para concluir con la demostración del teorema de Kronecker-Weber.

BIBLIOGRAFÍA

[1] M. J. Greenberg. An elementary proof of the kronecker-weber theorem. *The American Mathematical Monthly*, 81(6):601–607, 1974. ISSN 00029890, 19300972. URL `http://www.jstor.org/stable/2319208`.

[2] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, second edition, 1990.

[3] Serge Lang. *Algebraic Number Theory*. Addison-Wesley, 1970.

[4] E. Weiss. *Algebraic Number Theory*. McGraw-Hill, 1963.

[5] Oscar Zariski and Pierre Samuel. *Commutative algebra volume I*. Springer, 1975.