FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMÁTICAS

TRABAJO DE FIN DE MÁSTER:

El Teorema de Kronecker-Weber

AUTOR: Patricia Pascual Ortigosa

Dirigido por:
Enrique González Jiménez

Índice general

Introducción. **7**
Introducción histórica. 7
Objetivo del trabajo. 8

1. Base algebraica. **11**
1.1. Anillos y cuerpos. 11
1.2. Factorización de polinomios. 14
1.3. Extensiones de cuerpos. 17
1.4. Polinomios simétricos. 18
1.5. Módulos. 20
1.6. Grupos abelianos libres. 22
1.7. Anillos de Dedekind. 25
1.8. Anillos locales y localización. 26
1.8.1. Anillos locales. 26
1.8.2. Localización. 27

2. Cuerpos de números. **29**
2.1. Cuerpos de números. 29
2.2. Conjugados y discriminantes. 31
2.3. Enteros algebraicos. 33
2.4. Bases enteras. 36
2.5. Normas y trazas. 39
2.6. Anillos de enteros. 41
2.7. Cuerpos cuadráticos. 43
2.8. Cuerpos ciclotómicos. 45
2.9. El anillo de enteros en de Dedekind. 49

3. Grupos de ramificación. **51**
3.1. Extensiones de Galois. 51

3.2. Descomposición de primos. 53
3.3. Teorema de Hermite-Minkowski 57
3.4. Grupos de descomposición e inercia. 61
3.4.1. Grupos de Galois sobre cuerpos finitos. 63
3.4.2. La secuencia exacta. 64
3.5. Elementos de Frobenius. 65
3.6. Grupos de ramificación superior. 66

4. El Teorema de Kronecker-Weber. 73
4.1. El caso moderadamente ramificado. 74
4.2. El caso potencia de un primo. 77
4.2.1. El caso potencia de un primo impar. 77
4.2.2. El caso cuadrático. 80
4.2.3. El caso potencia de un primo par. 82

Problema Inverso de Galois. 85
Referencias. 89

Introducción.

Figura 1: David Hilbert (1862–1943) fue un matemático alemán que se ganó su reputación como matemático y científico gracias al desarrollo de un gran abanico de ideas: teoría de invariantes, axiomatización de la geometría, noción de espacio de Hilbert... En 1900 presentó un conjunto de problemas que establecieron el curso de gran parte de la investigación matemática del siglo XX.

Introducción histórica.

El Teorema de Kronecker-Weber es uno de los resultados más tempranos de la Teoría de Clases de Cuerpos. Este teorema fue enunciado en 1853 por Leopold Kronecker y nos dice lo siguiente:

Teorema 0.0.1 (Kronecker-Weber)**.** *Dada una extensión $K/\mathbb{Q}$ abeliana, existe un entero positivo n y una raíz primitiva n-ésima de la unidad ξ_n de manera que $K \subseteq \mathbb{Q}(\xi_n)$.*

Sin embargo, aunque Kronecker fue quien enunció el teorema, únicamente fue capaz de demostrarlo para extensiones cíclicas de grado potencia de dos.

En 1886, Wilhelm Eduard Weber publicó una prueba completa de dicho teorema[4]. Esta demostración poseía algunos errores que fueron corregidos en 1981 por Olaf Neumann [9].

La primera prueba completa del Teorema de Kronecker-Weber fue dada por David Hilbert en 1896. Por ello, el teorema también se conoce como Teorema de Kronecker-Weber-Hilbert, aunque casi siempre suele llamarse únicamente por el nombre de los dos primeros.

Debido a la relevancia de este teorema, pronto empezaron a surgir ideas sobre una posible generalización. Este hecho es conocido como *Kronecker's Jugendtraum (sueño de juventud de Kronecker)* o *duodécimo problema de Hilbert* perteneciente a la lista de 23 problemas abiertos que presentó en el Congreso Internacional de Matemáticos de París celebrado en 1900. Lo que plantea esta generalización es la posibilidad de extender el Teorema de Kronecker-Weber de extensiones abelianas sobre $\mathbb{Q}$ a cualquier cuerpo base. Es decir, se buscan análogos a ξ tales que generen toda una familia de cuerpos de números que sean análogos a los cuerpos ciclotómicos y sus subcuerpos.

Con Teoría Clásica de la Multiplicación Compleja se consiguió resolver el *Kronecker's Jugentraum* para el caso en que el cuerpo base sea un cuerpo cuadrático imaginario. Para ello se emplean funciones modulares y funciones elípticas elegidas en un retículo particular del cuerpo.

En 1961, Goro Shimura y Yutaka Taniyama extendieron el Teorema de Kronecker-Weber a *cuerpos CM*. Un cuerpo de números K se dice que es un *cuerpo CM* si es una extensión cuadrática K/F donde F es un cuerpo totalmente real y K es totalmente imaginario.

Lubin y Tate (1965, 1966) probaron el Teorema Local de Kronecker-Weber[1]

Generalizar todavía más el Teorema de Kronecker-Weber es un tema abierto a día de hoy.

Objetivo del trabajo.

El objetivo del trabajo es dar una prueba completa del Teorema de Kronecker-Weber. Para ello, hemos dividido el trabajo en cinco capítulos.

En el primer capítulo damos la base algebraica necesaria para presentar herramientas más potentes que serán necesarias para cumplir nuestro objetivo. Todos los conceptos explicados en este capítulo son comunes en todos los Grados de Matemáticas. En particular, los resultados relacionados con los anillos de Dedekind serán de suma importancia a lo largo del trabajo, pues todos los resultados que se dan en el capítulo cuatro pueden generalizarse a dichos anillos. Esta generalización se puede encontrar en [13].

El segundo capítulo está completamente dedicado a los cuerpos de números. Los cuerpos de números son una parte importante dentro de la Teoría Algebraica de Números que, a diferencia de los conceptos explicados en el primer capítulo, no es una asignatura común a todos los programas del Grado en Matemáticas. Los cuerpos de números van a ser una herramienta básica y necesaria en lo que restará de trabajo. Sobre todo, nos centraremos en los anillos de enteros asociados a un cuerpo de números y los estudiaremos con detenimiento. Uno de los resultados más importantes de este capítulo va a ser demostrar que el anillo de enteros de un cuerpo de números es un anillo de Dedekind. Gracias a este resultado, el capítulo cuatro puede ser generalizado a anillos de Dedekind. Para profundizar más en este tema se recomienda mirar el libro de Ian Stewart y David Tall [12].

[1] El Teorema Local de Kronecker-Weber asegura que cualquier extensión abeliana de un *cuerpo local* puede ser construida usando extensiones ciclotómicas y *extensiones de Lubin-Tate*.

En el tercer capítulo tratamos los grupos de descomposición, inercia y ramificación superior. Estos grupos van a ser la clave para poder realizar la demostración del Teorema de Kronecker-Weber en el capítulo cuatro. Para ahondar más en estos temas, se puede acudir a las notas del seminario impartido por Artur Travesa [13] y a las notas de William Stein [11].

Por último, en este trabajo se ha decidido probar el Teorema de Kronecker-Weber desarrollando Teoría de Grupos de ramificación. Otra opción para realizar la demostración de este teorema es utilizar números p-ádicos. A lo largo de la historia se han dado numerosas demostraciones de éste teorema, (mirar por ejemplo [1] o [10]).

Capítulo 1

Base algebraica.

En este primer capítulo del trabajo recordaremos conceptos indispensables para la comprensión del mismo. Refrescaremos los conceptos de anillo y cuerpo, así como muchas de sus propiedades: factorización de polinomios sobre anillos y cuerpos, extensiones de cuerpos y polinomios simétricos. Después, explicaremos módulos, grupos abelianos libres y terminaremos el capítulo tratando anillos de Dedekind, un concepto muy relevante en lo que restará de trabajo.

1.1. Anillos y cuerpos.

Definición 1.1.1. *Un* anillo R *es un conjunto con dos operaciones binarias*

$$+ : R \times R \to R \qquad \cdot : R \times R \to R$$

$$(a, b) \mapsto a + b \qquad (a, b) \mapsto a \cdot b$$

tales que $\forall a, b, c \in R$ *se verifica*

I) $(R, +)$ *es un grupo abeliano. Denotamos el elemento neutro por* 0 *y al opuesto del elemento* a *por* $-a$.

II) *La operación* $\cdot$ *es asociativa:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

III) *Se cumplen las leyes distributivas:* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Dado un anillo R, diremos que es *conmutativo* si $a \cdot b = b \cdot a, \forall a, b \in R$. A lo largo de este trabajo, siempre que consideremos un anillo, éste será conmutativo.

Diremos que un subconjunto S de un anillo R es un *subanillo* de R si el elemento identidad de R está en S y siempre que $s, t \in S$, entonces $s - t, st \in S$.

Sea R un anillo. Un elemento $a \in R$ es un *divisor de cero* si existe $b \in R$ tal que $a \cdot b = 0$. Si un anillo R no tiene divisores de cero, diremos que es un *dominio de integridad*.

Dado R un anillo, diremos que $a \in R$ es *invertible o unidad* si $\exists b \in R$ tal que $ab = 1$. Diremos que b es el *inverso* de a y lo denotaremos por a^{-1}.

Sea R un anillo tal que el elemento identidad es distinto del neutro y tal que todos sus elementos no nulos invertibles. Diremos entonces que R es un *cuerpo*. Lo denotaremos por K. Un subconjunto F de un cuerpo K es un *subcuerpo* de K si el elemento identidad de K está en F y siempre que $s, t \in F$, entonces $s - t, st^{-1} \in F$.

Definición 1.1.2. *Sea R un anillo e $I \subset R$, con $I \neq \phi$. Decimos que I es un ideal de R, y lo denotamos por $I < R$, si se verifica que, $\forall a, b, i \in I$:*

I) $a - b \in I$.

II) *Si $a \in R$, entonces $ra \in I$.*

Sea R un anillo e $I \lhd R$. Definimos el *anillo cociente de R por I* como el conjunto:

$$R/I = \{r + I \mid r \in R\},$$

junto con las operaciones

$$(r + I) + (s + I) = (r + s) + I$$

y

$$(r + I)(s + I) = (rs) + I, r, s \in R.$$

Definición 1.1.3. *Sean R_1 y R_2 dos anillos. Decimos que $f : R_1 \to R_2$ es un homomorfismo de anillos si verifica las siguientes propiedades:*

I) $f(1_{R_1}) = 1_{R_2}$.

II) $f(r + s) = f(r) + f(s), \forall r, s \in R_1$.

III) $f(rs) = f(r)f(s), \forall r, s \in R_1$.

Un homomorfismo de anillos es un monomorfismo *si es inyectivo y un* isomorfismo *si es biyectivo.*

Sea R un anillo y X, Y subconjuntos de R. Definimos

$$X + Y = \{x + y \mid x \in X, y \in Y\},$$

$$XY = \left\{ \sum x_i y_i \mid x_i \in X, y_i \in Y \right\}.$$

Además, si X, Y son ideales de R, entonces $X+Y$ y XY también son ideales de R.

El *ideal generado* por $S \subseteq R$ es el menor ideal de R que contiene a S. Es decir, si $S = \{s_1, \ldots, s_n\}$, entonces

$$\langle S \rangle = \langle s_1, \ldots, s_n \rangle = \{r_1 s_1 + r_2 s_r + \cdots + r_n s_n \mid s_i \in S, r_i \in R\}.$$

Si existe $S = \{s_1, \ldots, s_n\} \subset R$ finito tal que $I = \langle S \rangle$, entonces I está *finitamente generado* como ideal de R. Sea $x \in R$. Si $I = \langle x \rangle$, es decir, está generado por un solo elemento, entonces I se dice *ideal principal generado por* x.

Si K es un cuerpo y R es un subanillo de K, entonces R es un dominio. De igual manera, si D es un dominio, definimos su *cuerpo de fracciones* L como

$$L = \left\{ \frac{d}{e} \mid d, e \in D, e \neq 0 \right\}.$$

Obviamente, $D \subset L$.

Teorema 1.1.4. *Todo dominio de integridad finito es un cuerpo.*

Demostración. Sea D un dominio de integridad finito. Tenemos que $1_D \neq 0_D$, por lo tanto D tiene al menos dos elementos.

Tomamos $x \in D$ con $x \neq 0_D$. Entonces xy_i, con $y_i \in D$, son distintos. Vamos a comprobarlo: si fueran iguales tendríamos $xy_1 = xy_2 \Rightarrow x(y_1 - y_2) = 0$ y como estamos en un dominio y no hay divisores de cero, tendríamos que $y_1 = y_2$.

De esta manera, tenemos que $D = \{xy_i\}$ y como $1_D \in D$ entonces existe y_j tal que $xy_j = 1_D$, con $y_j \in D$. Por lo tanto, D es un cuerpo. □

Vamos a recordar los conceptos de ideal maximal e ideal primo. Sea R es un anillo. Decimos que el ideal $\mathfrak{a}$ de R es un *ideal maximal* si es un ideal propio de R y no existe otro ideal $\mathfrak{b}$ de R tal que $\mathfrak{a} \subset \mathfrak{b} \subset R$. Un ideal $\mathfrak{a}$ de R decimos que es *primo* si $\mathfrak{a} \neq R$ y, siempre que $\mathfrak{b}, \mathfrak{c}$ son ideales de R tales que $\mathfrak{bc} \subset \mathfrak{a}$, se tiene que $\mathfrak{b} \subset \mathfrak{a}$ o $\mathfrak{c} \subset \mathfrak{b}$.

Lema 1.1.5. *Sea R un anillo y $\mathfrak{a}$ un ideal de R. Entonces*

a) $\mathfrak{a}$ *es maximal si y solo si* $R/\mathfrak{a}$ *es un cuerpo.*

b) $\mathfrak{a}$ *es primo si y solo si* $R/\mathfrak{a}$ *es dominio de integridad.*

Demostración.

a) Tomamos la aplicación $\phi : R/\mathfrak{a} \to R$ definida por $\phi(I) = \mathfrak{a} \subseteq I \subseteq R$. Notemos que la aplicación ϕ es biyectiva. Por lo tanto, $\mathfrak{a}$ es maximal si y solo si $R/\mathfrak{a}$ no tiene ideales propios no nulos y esto ocurre si y solo si $R/\mathfrak{a}$ es un cuerpo.

b) Supongamos primero que el ideal $\mathfrak{a}$ es primo. Sean $x, y \in R$ tales que $(x + \mathfrak{a})(y + \mathfrak{a}) = 0$ en $R/\mathfrak{a}$. Esto implica que $xy \in \mathfrak{a}$ y esto nos dice que $\langle x\rangle\langle y\rangle \subseteq \mathfrak{a}$. Como $\mathfrak{a}$ es primo, tenemos que $\langle x\rangle \subseteq \mathfrak{a}$ o $\langle y\rangle \subseteq \mathfrak{a}$. Esto implica que $x \in \mathfrak{a}$ o $y \in \mathfrak{a}$. Por lo tanto, necesariamente $(x + \mathfrak{a})$ o $(y + \mathfrak{a})$ es cero en $R/\mathfrak{a}$. Luego $R/\mathfrak{a}$ no tiene divisores de cero, es decir, $R/\mathfrak{a}$ es un dominio.

Por hipótesis tenemos que $R/\mathfrak{a}$ es un dominio. Entonces $|R/\mathfrak{a}| \neq 1$ y esto implica que $\mathfrak{a} \neq R$. Supongamos ahora que $\mathfrak{bc} \subseteq \mathfrak{a}$ pero $\mathfrak{b} \nsubseteq \mathfrak{a}$ y $\mathfrak{c} \nsubseteq \mathfrak{a}$, es decir, $\mathfrak{a}$ no es primo. Así, podemos encontrar $b \in \mathfrak{b}$ y $c \in \mathfrak{c}$ tales que $b, c \notin \mathfrak{a}$, pero $bc \in \mathfrak{a}$. Esto implica que $(b + \mathfrak{a})$ y $(c + \mathfrak{a})$ son divisores de cero en $R/\mathfrak{a}$, pero esto es absurdo, puesto que $R/\mathfrak{a}$ era un dominio. Por lo tanto, $\mathfrak{a}$ es un ideal primo. □

Tenemos el siguiente corolario a este lema:

Corolario 1.1.6. *Todo ideal maximal es primo.*

1.2. Factorización de polinomios.

Sea R un anillo y $a, b, c \in R$ tales que $a = bc$. Decimos entonces que b y c son *factores* de a y lo denotamos de la siguiente manera: $b \mid a$ y $c \mid a$.

Si $e \in R$ es un elemento invertible, tenemos que $a = e(e^{-1}a)$. Por lo tanto, un elemento invertible es factor de cualquier elemento de un anillo R.

Definición 1.2.1. *Sea* R *un anillo y* $a, b, c \in R$ *de manera que* $a = bc$. *Si* b *y* c *no son invertibles, entonces* a *es* reducible *y* b *y* c *se llaman* factores propios *de* a.

Notemos que si a es un elemento invertible de R con $a = bc$, entonces $1 = aa^{-1} = bca^{-1}$, luego b y c son invertibles. Es decir, un elemento invertible no puede tener factorización propia.

Definición 1.2.2. *Sea* R *un anillo y* $a \in R$ *no invertible. Entonces* a *es* irreducible *si no tiene factores propios.*

Vamos a definir a continuación los anillos de polinomios.

Definición 1.2.3. *Sea R un anillo. Denotamos el* anillo de polinomios con coeficientes en R y en variable t *como $S = R[t]$ y los elementos de S son de la forma $f(t) = r_0 + r_1 t + \cdots + r_n t^n$, con $r_i \in R$ y definimos el* grado *de dicho polinomio como el mayor n para el que $r_n \neq 0$.*

Sea $f(t)$ un polinomio. Decimos que α es un *cero de* $f(t)$ si $f(\alpha) = 0$ o, de manera equivalente, $(t - \alpha) \mid f(t)$. Así mismo, decimos que α es un *cero de multiplicidad* m de $f(t)$ si $(t - \alpha)^m \mid f(t)$, para $m \geq 2$.

Vamos a enunciar a continuación un teorema que nos va a ayudar a identificar si un polinomio tiene factores repetidos en un cuerpo. Para ello, necesitamos conocer el concepto de derivada formal. Si $f = \sum_{i=0}^{n} r_i t^i$ es un polinomio de $R[t]$, denotamos por Df a la *derivada formal de* f:

$$Df = \sum_{i=0}^{n} i r_i t^{i-1}.$$

Teorema 1.2.4. *Sea K un cuerpo de característica cero. Un polinomio $f \neq 0$ definido sobre K es dividido por el cuadrado de un polinomio de grado mayor que cero si y solo si f y Df tienen un factor común de grado mayor que cero.*

Demostración.

$\Rightarrow$) Por hipótesis sabemos que el cuadrado de un factor g de grado mayor que cero divide a f, es decir $f = g^2 h$. Así, $Df = g^2 Dh + 2gDgh$, luego f y Df tienen un factor en común.

$\Leftarrow$) Por hipótesis, f y Df tienen un factor de grado mayor que cero común.

Supongamos que f no tiene ningún factor cuadrado irreducible, entonces para cualquier factor irreducible g de f existe h tal que $f = gh$ con g y h coprimos. Así, $Df = gDh + Dgh$. Usando la hipótesis tenemos que Dgh tiene que tener a g por factor, y como h y g son coprimos, entonces Dg tiene a g como factor. Sin embargo, tenemos que el grado de Dg es menor que el grado de g, luego $g \mid Dg$ si y solo si $Dg = 0$. Pero como la característica de K es cero, entonces g es constante, lo que implica que f y g no pueden tener factores comunes triviales. □

Observemos que si el cuerpo K tiene característica p, entonces la primera implicación se verifica, pero la segunda es falsa.

Corolario 1.2.5. *Un polinomio irreducible sobre un subcuerpo K de $\mathbb{C}$ no tiene ceros repetidos en $\mathbb{C}$.*

Demostración. Sea f un polinomio irreducible sobre K. Entonces f y Df son coprimos, si no, por el Teorema 1.2.4 f tendría ceros repetidos y no sería irreducible. Así, existen g, h polinomios definidos sobre K tales que $1 = gf + hDf$. Interpretándolo sobre $\mathbb{C}$ tenemos que f y Df son coprimos en $\mathbb{C}$, luego f y Df no tienen factores comunes. Por lo tanto no hay ceros repetidos en $\mathbb{C}$. □

Lema 1.2.6. *Sea $p \in \mathbb{Z}[t]$ y supongamos que $p = gh$ con $g, h \in \mathbb{Q}[t]$. Entonces existe $\lambda \in \mathbb{Q}$, con $\lambda \neq 0$, tal que $\lambda g, \lambda^{-1} h \in \mathbb{Z}[t]$.*

Demostración. Sea $f = gh$, con $g, h \in \mathbb{Q}[t]$. Sea n el producto de los denominadores de g y h. Entonces obtenemos

$$nf = g'h',$$

con $h', g' \in \mathbb{Z}[t]$. Esto implica que n divide a los coeficientes de g' y h'.

Sean k_i los factores primos de n que, en particular, dividen a nf y a $g'h'$. Dividimos ambos por los factores primos de n y obtenemos $f = \overline{g}\overline{h}$, con $\overline{g}\overline{h} \in \mathbb{Z}[t]$. Además, $\overline{g}$ y $\overline{h}$ son múltiplos racionales de g y h. De esta manera, escribiendo $\overline{g} = \lambda g, \lambda \in \mathbb{Q}$, obtenemos que $\overline{h} = \lambda^{-1} h$.

Nos queda comprobar que si

$$g' = g_0 + g_1 t + \cdots + g_r t^r$$

$$h' = h_0 + h_1 t + \cdots + h_r t^r$$

y k divide a todos los coeficientes de $g'h'$, entonces $k \mid g_i$ y $k \mid h_j$, para todo i, j.

Supongamos que k no divide a todos los g_i, h_j. Tomamos entonces g_m, h_q los primeros coeficientes no divisibles por k. Sabemos que el coeficiente de t^{m+q} de $g'h'$ es

$$g_0 h_{m+q} + g_1 h_{m+q-1} + \cdots + g_m h_q + \cdots + g_{m+q-1} h_1 + g_{m+q} h_0.$$

Así, este coeficiente no sería divisible por k pues $g_m h_q$ no lo es, pero esto es una contradicción pues habíamos tomado $g'h'$ de forma que todos sus coeficientes fuesen divisibles por k.

Tenemos entonces que si

$$g' = g_0 + g_1 t + \cdots + g_r t^r$$

$$h' = h_0 + h_1 t + \cdots + h_r t^r$$

y k divide a todos los coeficientes de $g'h'$, entonces $k \mid g_i$ y $k \mid h_j$, para todo i, j, y el lema quedaría probado. □

Teorema 1.2.7 (Reducción módulo n)**.** *Si $p \in \mathbb{Z}[t]$ y su imagen $\overline{p} \in \mathbb{Z}_n[t]$ es irreducible y el grado de $\overline{p}$ es igual al grado de p, entonces p es irreducible en $\mathbb{Z}[t]$.*

Demostración. Supongamos $p \neq 0 \in \mathbb{Z}[t]$ reducible, es decir, $p = qr$. El homomorfismo que va de $\mathbb{Z}$ a $\mathbb{Z}_n$ induce el homomorfismo de $\mathbb{Z}[t]$ a $\mathbb{Z}_n[t]$, entonces $\overline{p} = \overline{qr}$. Si el grado de p es igual al grado de $\overline{p}$, entonces el grado de $\overline{r}$ es igual al grado r y lo mismo ocurre con q. Por tanto, p es reducible. □

1.3. Extensiones de cuerpos.

Para encontrar las raíces de un polinomio $f(t)$ definido sobre un cuerpo K, usualmente necesitamos recurrir a un cuerpo L más grande que K que contenga dicha raíz. Decimos entonces que el cuerpo L es una *extensión* del cuerpo K y lo denotaremos por K/L. La definición de extensión de cuerpos no es única. Sean K y L dos cuerpo y $j : K \to L$ un monomorfismo. Identifiquemos K con $j(K) \subset L$. Se dice entonces que el par (K, L) con $K \subset L$ es una extensión de cuerpos.

Si L/K es una extensión de cuerpos, podemos ver que L tiene estructura de espacio vectorial sobre K. A la dimensión de este espacio vectorial L sobre K lo llamaremos *grado de L sobre K o grado de la extensión L/K* y lo denotaremos por $[L : K]$.

Teorema 1.3.1. *Si $H \subseteq K \subseteq L$ cuerpos, entonces $[L : H] = [L : K][K : H]$.*

Demostración. Como L es un espacio vectorial sobre K, consideramos $\{a_i\}_{i \in I}$ una base de dicho espacio sobre K. Del mismo modo, consideramos $\{b_j\}_{j \in J}$ una base de K sobre H. De esta manera, $\{a_i b_j\}_{(i,j) \in I \times J}$ es una base de L sobre H, de donde se sigue el resultado. □

Decimos que una extensión L/K es *finita* si su grado es finito, es decir, si $[L : K] < \infty$.

Definición 1.3.2. *Sea L/K una extensión de cuerpos, $\alpha \in L$ y $f(t) \in K[t]$ un polinomio no nulo e irreducible. Decimos que α es* algebraico sobre K *si $f(\alpha) = 0$. Si α no es raíz del polinomio, entonces decimos que es* trascendente sobre K.

Si todos los elementos de L son algebraicos sobre K, diremos que L/K es una *extensión algebraica*. En otro caso, diremos que la extensión es *trascendente*.

Si un elemento $\alpha \in L$ es algebraico sobre K, entonces existe un único polinomio $q(t) \in K[t]$ irreducible y mónico tal que $q(\alpha) = 0$. Este polinomio se denomina *polinomio mínimo de α sobre K*.

Sean $\alpha_1, \ldots, \alpha_n$ elementos del cuerpo L. El subcuerpo $K(\alpha_1, \ldots, \alpha_n) \subset L$ es el subcuerpo más pequeño de L que contiene a K y a $\alpha_1, \ldots, \alpha_n$.

Teorema 1.3.3. *Sea L/K una extensión de cuerpos y $\alpha \in L$. Entonces, α es algebraico sobre K si y solo si $[K(\alpha) : K]$ es finito. En este caso, $[K(\alpha) : K]$ es el grado de polinomio mínimo de α sobre K.*

Demostración.

$\Leftarrow$) Si $[K(\alpha) : K] = n < \infty$, entonces las potencias $1, \alpha, \ldots, \alpha^n$ son linealmente dependientes. Por lo tanto, α es algebraico sobre K.

$\Rightarrow$) Por hipótesis tenemos que α es algebraico sobre K y debemos comprobar que $[K(\alpha) : K]$ es finito.

Sea $f(t) \in K[t]$ el polinomio mínimo de α sobre K, de grado m.

Vamos a comprobar que $K(\alpha)$ es el espacio vectorial sobre K expandido por $1, \alpha, \ldots, \alpha^{m-1}$: tenemos que $K(\alpha)$ es cerrado bajo suma y resta y también bajo multiplicación por α: $\alpha^m = -f(\alpha) + \alpha^m = q(\alpha)$, con grado de q menor que m. Por lo tanto, $K(\alpha)$ es un anillo. Nos queda comprobar que si $0 \neq l \in K(\alpha)$, entonces $\frac{1}{l} \in K(\alpha)$. Tenemos que $l = h(\alpha)$, para cierto $h(t) \in K[t]$ cuyo grado es menor que m. Como f es irreducible, entonces f y h son coprimos. Por lo tanto, existen $g, p \in K[t]$ tales que $1 = fg + hp$. Sustituyendo t por α tenemos que $1 = h(\alpha)p(\alpha)$, luego $\frac{1}{l} = p(\alpha) \in K(\alpha)$.

Ya comprobado que $K(\alpha)$ es el espacio vectorial sobre K expandido por $1, \alpha, \ldots, \alpha^{m-1}$, tenemos que $[K(\alpha) : K] = dim_K K(\alpha) = m$ y el teorema queda demostrado.

□

1.4. Polinomios simétricos.

Sea $R[t_1, \ldots, t_n]$ el anillo de polinomios en las indeterminadas $t_1, \ldots, t_n$ con coeficientes en el anillo R. Sea S_n el grupo simétrico de permutaciones en $\{1, \ldots, n\}$. Entonces, para cualquier permutación $\pi \in S_n$ y cualquier polinomio $f \in R[t_1, \ldots, t_n]$, definimos $f^\pi(t_1, \ldots, t_n) = f(t_{\pi(1)}, \ldots, t_{\pi(n)})$.

Definición 1.4.1. *Un polinomio f es* simétrico *si $f^\pi = f$, $\forall \pi \in S_n$.*

Visto ya lo que es un polinomio simétrico, vamos a definir los polinomios simétricos elementales que denotaremos por $s_r(t_1,\dots,t_n), 1 \leq r \leq n$. Definimos los *polinomios simétricos elementales* $s_r(t_1,\dots,t_n)$ como la suma de todos los posibles productos distintos de r distintos t_i. Es decir,

$$s_1(t_1,\dots,t_n) = t_1 + t_2 + \cdots + t_n,$$

$$s_2(t_1,\dots,t_n) = t_1t_2 + t_1t_3 + \cdots + t_1t_n + t_2t_3 + \cdots + t_{n-1}t_n,$$

$$\dots$$

$$s_n(t_1,\dots,t_n) = t_1t_2t_3\dots t_{n-1}t_n.$$

Consideremos un polinomio de grado n sobre un cuerpo $K \subseteq \mathbb{C}$:

$$f = a_0 + a_1t + \cdots + a_nt^n.$$

Entonces, sobre $\mathbb{C}$ tenemos que el polinomio descompone de la siguiente manera:

$$f = a_n(t-\alpha_1)...(t-\alpha_n),$$

por lo tanto, $f = a_n(t^n - s_1t^{n-1} + \cdots + (-1)^n s_n)$, con $s_i = s_i(\alpha_1,\dots,\alpha_n)$.

Si nos fijamos, un polinomio en $s_1,\dots,s_n$ se puede reescribir como un polinomio simétrico en $t_1,\dots,t_n$. Pero, ¿el inverso es posible? El siguiente teorema nos asegura que sí.

Teorema 1.4.2. *Sea R un anillo. Entonces todo polinomio simétrico en $R[t_1,\dots,t_n]$ se puede expresar como un polinomio con coeficientes en R en los polinomios simétricos elementales $s_1,\dots,s_n$.*

La demostración de este teorema da una técnica para reducir de un polinomio simétrico a uno con coeficientes en polinomios simétricos elementales. Al terminar la demostración se dará un ejemplo para ver cómo funciona.

Demostración.

1. Lo primero que hay que hacer es ordenar los monomios $t_1^{\alpha_1}\dots t_n^{\alpha_n}$ de modo que $t_1^{\alpha_1}\dots t_n^{\alpha_n}$ precede a $t_1^{\beta_1}\dots t_n^{\beta_n}$ si el primer $\alpha_i - \beta_i$ no nulo es positivo.

2. Dado $p \in R[t_1,\dots,t_n]$ ordenamos sus términos de la manera vista en 1.

3. Si p es simétrico, entonces para cada monomio $t_1^{\alpha_1} \dots t_n^{\alpha_n}$ ocurre un monomio similar con los exponentes permutados. Sea α_1 el mayor exponente de los monomios de p. Entonces hay algún término que contiene a $t_1^{\alpha_1}$. El primer término del polinomio ordenado que hemos conseguido en 2. contiene a $t_1^{\alpha_1}$. Entre todos los monomios que contienen a $t_1^{\alpha_1}$, seleccionamos al que tiene mayor potencia de t_2 y así continuamos hasta tenerlo ordenado. En particular, el término líder en un polinomio simétrico es de la forma $at_1^{\alpha_1} \dots t_n^{\alpha_n}$, con $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$.

   Por ejemplo, el término líder de $p = s_1^{k_1} s_2^{k_2} \dots s_n^{k_n} = (t_1 + \dots + t_n)^{k_1} \dots (t_1 \dots t_n)^{k_n}$ es $t_1^{k_1+\dots+k_n} t_2^{k_2+\dots+k_n} \dots t_n^{k_n}$.

   Como $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$, podemos elegir $k_1 = \alpha_1 - \alpha_2, \dots, k_{n-1} = \alpha_{n-1} - \alpha_n, k_n = \alpha_n$, y después podemos aplicarle el procedimiento anterior al término líder de p. Entonces

$$p' = p - as_1^{\alpha_1-\alpha_2} \dots s_{n-1}^{\alpha_{n-1}-\alpha_n} s_n^{\alpha_n}.$$

   Este polinomio tiene como término líder lexicográfico a $bt_1^{\beta_1} \dots t_n^{\beta_n}$, con $\beta_1 \geq \beta_2 \geq \dots \geq \beta_n$, que va tras $at_1^{\alpha_1} \dots t_n^{\alpha_n}$. Sin embargo, solo un número finito de monomios $t_1^{\gamma_1} \dots t_n^{\gamma_n}$ verificando $\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_n$ siguen a $at_1^{\alpha_1} \dots t_n^{\alpha_n}$. Por lo tanto, con un número finito de iteraciones, conseguiremos reducir a p a un polinomio en $s_1, \dots, s_n$.

□

Ejemplo 1.4.3. *Tenemos el polinomio simétrico*

$$f = t_1^2 t_2 + t_1^2 t_3 + t_1 t_2^2 + t_1 t_3^2 + t_2 t_3^2.$$

Si nos fijamos en el método que nos da la demostración del teorema anterior, ya lo tenemos ordenado como necesitamos. Así, $n = 3$, $\alpha_1 = 2$, $\alpha_2 = 1$ *y* $\alpha_3 = 0$. *De esta manera obtenemos* $f - s_1 s_2 = 3t_1 t_2 t_3 = 3s_3$. *Así,* $f = 3s_3 + s_1 s_2$.

Corolario 1.4.4. *Sea L una extensión del cuerpo K, $f \in K[t]$ con el grado de f igual a n y $\theta_1, \theta_2, \dots, \theta_n \in L$ ceros de dicho polinomio. Si $h(t_1, \dots, t_n) \in K[t_1, \dots, t_n]$ es simétrico, entonces $h(\theta_1, \dots, \theta_n) \in K$.*

1.5. Módulos.

En esta sección nos centraremos en módulos. Comenzaremos dando la definición de módulo, expondremos algún ejemplo y finalizaremos explicando cómo generar módulos.

Definición 1.5.1. *Sea R un anillo. Un R-*módulo *M es un grupo abeliano aditivo junto con una función $\alpha : R \times M \to M$, con $\alpha(r, m) = rm, r \in R, m \in M$ que satisface las siguientes propiedades:*

I) $(r + s)m = rm + rs$, $\forall r, s \in R, \forall m \in M$.

II) $r(m + n) = rm + rn$, $\forall r \in R, \forall m, n \in M$.

III) $r(sm) = (rs)m$, $\forall r, s \in R, \forall m \in M$.

IV) $1m = m$, $\forall m \in M$.

*La aplicación α se denomina R-*acción en *M.*

Si R es un cuerpo, entonces ser un R-módulo es equivalente a ser un espacio vectorial sobre R. A continuación, vamos a definir R-submódulos. Si M es un R-módulo, decimos que N es un *R-submódulo de M* si N es subgrupo de M y siempre que $n \in N$ y $r \in R$, entonces $rn \in N$.

Sea M un R-módulo y N un R-submódulo de M. Definimos el *módulo cociente de M por N*, M/N con R-acción que actúa de la siguiente manera: $r(N + m) = N + rm, r \in R, m \in M$.

Sea $X \subseteq M$, con M un R-módulo. El *submódulo de M generado por X* es el menor submódulo conteniendo a X y lo denotamos por $\langle X \rangle_R$. Además, si $M = \langle x_1, \ldots, x_n \rangle_R$, entonces decimos que M es *finitamente generado.*

Ejemplo 1.5.2.

1. *Un $\mathbb{Z}$-módulo es un grupo abeliano M.*

2. *Un grupo aditivo abeliano M se puede convertir en $\mathbb{Z}$-módulo definiendo $0m = 0$ y $1m = 1, m \in M$. De aquí se obtiene que $(n + 1)m = nm + m$, $(-n)m = -nm, n \in \mathbb{Z}$.*

Para finalizar esta sección, vamos a ver de qué acción debemos dotar a un determinado subanillo o ideal para que sea un módulo.

1. Sea S un subanillo del anillo R, entonces R es un S-módulo bajo la acción $\alpha(s, r) = sr, r \in R, s \in S$.

2. Sea I un ideal de un anillo R. Entonces I es un R-módulo bajo la acción $\alpha(r, i) = ri, r \in R, i \in I$.

3. Sea $J \subseteq I$ otro ideal del anillo R. Entonces J es R-módulo y el módulo cociente I/J actúa bajo la acción $r(J + i) = J + ri, i \in I, r \in R$.

1.6. Grupos abelianos libres.

Sea G un grupo aditivo. Si G es finitamente generado como $\mathbb{Z}$-módulo, entonces existen $g_1, \ldots, g_n \in G$ tales que cada $g \in G$ se escribe como

$$g = g_1 m_1 + \cdots + g_n m_n,$$

con $m_i \in \mathbb{Z}$. Si esto ocurre, se dice que G es un *grupo abeliano finitamente generado*. Los elementos $g_1, \ldots, g_n \in G$, con G grupo abeliano, son *linealmente independientes sobre* $\mathbb{Z}$ si, siempre que se verifica la ecuación $g_1 m_1 + \cdots + g_n m_n = 0$, implica que $m_i = 0, \forall i = 1, \ldots, n$. Si $\{g_1, \ldots, g_n\}$ son linealmente independientes y generan G, entonces forman una base de G y cada elemento $g \in G$ tiene una única representación.

Definición 1.6.1. *Un grupo abeliano cuya base tiene n elementos se llama* grupo abeliano libre de rango n.

Como ya sabemos, dos bases distintas de un grupo G tienen el mismo número de elementos. Sean $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_n\}$ dos bases distintas de G. Entonces podemos obtener los elementos de una base a partir de la otra de la siguiente manera:

$$x_i = \sum_j b_{ij} y_j,$$

$$y_i = \sum_j a_{ij} x_j.$$

Vamos a llamar A a la matriz (a_{ij}) y B a la matriz (b_{ij}). Tenemos así que $AB = I_n$. Si tomamos determinantes, tenemos que $\det(A)\det(B) = \det(I_n) = 1$. Por lo tanto, $\det(A) = \det(B) = \pm 1$.

Definición 1.6.2. *Una matriz cuadrada sobre* $\mathbb{Z}$ *con determinante* ± 1 *se llama* matriz unimodular.

Lema 1.6.3. *Sea G un grupo abeliano libre de rango n con base $\{x_1, \ldots, x_n\}$. Entonces los elementos $y_i = \sum_j a_{ij} x_j$ forman una base para G si y solo si (a_{ij}) es unimodular.*

Demostración. Solo tenemos que hacer la implicación en la que por hipótesis tenemos que (a_{ij}) es unimodular pues la otra implicación ya la hemos visto.

Por hipótesis tenemos que $A = (a_{ij})$ es unimodular. Entonces $\det(A) = \pm 1 \neq 0$, por lo tanto los y_j son linealmente independientes. Además, sabemos que $A^{-1} = \frac{A^*}{\det(A)}$, y como $\det(A) = \pm 1$, entonces $A^{-1} = \pm A^*$, con entradas enteras. Así, $B = A^{-1} = (b_{ij})$ y tenemos que $x_i = \sum_j b_{ij} y_j$. Por lo tanto $\{y_1, \ldots, y_n\}$ genera G, luego tenemos que $\{y_1, \ldots, y_n\}$ es base para G. $\square$

Teorema 1.6.4. *Sea G un grupo abeliano libre de rango n. Todo subgrupo H de G es libre de rango $s \leq n$. Además, existe $\{u_1, \ldots, u_n\}$ base de G y $\alpha_1, \ldots, \alpha_s$ enteros positivos tales que $\{\alpha_1 u_1, \ldots, \alpha_s u_s\}$ forman una base de H.*

Demostración. Para demostrar este teorema vamos a aplicar inducción sobre el rango del grupo G.

Si $n = 1$, tenemos entonces que G es un grupo cíclico. Por lo tanto, el resultado se sigue por la estructura del grupo.

Tomamos ahora n el rango del grupo G y $\{\omega_1, \ldots, \omega_n\}$ una base de dicho grupo. Así, cualquier $h \in H \neq \{0\}$ se puede escribir como

$$h = h_1\omega_1 + \cdots + h_n\omega_n.$$

De todos los coeficientes, tomamos $\lambda(\omega_1, \ldots, \omega_n)$ el último coeficiente positivo y elegimos la base de forma que este λ sea mínimo. Llamamos α_1 a este valor.

Definimos entonces

$$v_1 = \alpha_1\omega_1 + \beta_1\omega_2 + \cdots + \beta_n\omega_n \in H,$$

siendo $\beta_i = \alpha_1 q_i + r_i, 2 \leq i \leq n, 0 \leq r_i < \alpha_1$.

Definimos ahora

$$u_1 = \omega_1 + q_2\omega_2 + \cdots + q_n\omega_n,$$

de donde obtenemos que $\{u_1, \omega_2, \ldots, \omega_n\}$ es base de G. Respecto a esta nueva base tenemos que

$$v_1 = \alpha_1 u_1 + r_2\omega_2 + \cdots + r_n\omega_n,$$

pero como α_1 era mínimo, tenemos que $r_i = 0$. Por lo tanto, $v_1 = \alpha_1 u_1$.

Respecto a la nueva base $\{u_1, \omega_2, \ldots, \omega_n\}$, tomamos

$$H_1 = \{m_1u_1 + m_2\omega_2 + \cdots + m_n\omega_n \mid m_1 = 0\},$$

$$V_1 = \langle v_1 \rangle.$$

Tenemos que $H_1 \cap V_1 = \{0\}$.

Vamos a comprobar que $H = H_1 + V_1$.

Sea $h \in H$, con $h = \gamma_1 u_1 + \gamma_2\omega_2 + \cdots + \gamma_n\omega_n$. Tomamos ahora $\gamma_1 = \alpha_1 q + r_1$, tenemos entonces que

$$h = (\alpha_1 q + r_1)u_1 + \gamma_2\omega_2 + \cdots + \gamma_n\omega_n \Rightarrow h - qv_1 = r_1u_1 + \gamma_2\omega_2 + \cdots + \gamma_n\omega_n.$$

Por la minimalidad de α_1, tenemos que $r_1 = 0$. Por lo tanto, $h - qv_1 \in H_1$. Así, $H \cong H_1 \times V_1$, con $H_1 < G'$ grupo abeliano de rango $n-1$ cuya base es $\{\omega_2, \ldots, \omega_n\}$.

Por inducción, H_1 es un grupo abeliano libre de rango menor o igual que $n-1$ y existe una base $\{u_2, \ldots, u_n\}$ de G' y $v_2, \ldots, v_s \in H_1$ tales que $v_i = \alpha_i u_i$, con $\alpha_i \in \mathbb{Z}^+$ y ya tenemos demostrado lo que queríamos probar. □

Teorema 1.6.5. *Sea G un grupo abeliano libre de rango n y H un subgrupo de G. Entonces G/H es finito si y solo si los rangos de G y H son iguales. Si eso ocurre y G y H tienen $\mathbb{Z}$-bases $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_n\}$ con $y_i = \sum_j a_{ij}x_j$, entonces $|G/H| = |\det(a_{ij})|$.*

Demostración. Sea H subgrupo de G de rango s. Usando el Teorema 1.6.4 podemos elegir $\mathbb{Z}$-bases $\{u_1, \ldots, u_n\}$ de G y $\{v_1, \ldots, v_s\}$ de H con $v_i = \alpha_i u_i$.

G/H es el producto directo de grupos cíclicos finitos de orden $\alpha_1, \ldots, \alpha_s$ y $r-s$ grupos cíclicos infinitos. Entonces $|G/H|$ es finito si y solo si $r = s$ y, en ese caso $|G/H| = \alpha_1 \cdot \cdots \cdot \alpha_s$.

Tenemos además que $u_i = \sum_j b_{ij}x_j$, $v_i = \sum_j c_{ij}u_j$ y $y_i = \sum_j d_{ij}v_i$, con $B = (b_{ij})$ y $D = (d_{ij})$ unimodulares. Entonces

$$C = (c_{ij}) = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_s \end{pmatrix}.$$

Si $A = (a_{ij})$ entonces $A = BCD$. Entonces $|\det(A)| = |\det(B)| \cdot |\det(C)| \cdot |\det(D)| = |\pm 1| \cdot |\alpha_1 \cdot \cdots \cdot \alpha_s| \cdot |\pm 1| = |\alpha_1 \cdot \cdots \cdot \alpha_s| = |G/H|$. □

Ejemplo 1.6.6. *Sea G de rango 3 y $\mathbb{Z}$-base $\{x, y, z\}$ y sea H un subgrupo de G con $\mathbb{Z}$-base $\{3x + y - 2z, 4x - 5y + z, x + 7z\}$, entonces*

$$|G/H| = \left| \begin{vmatrix} 3 & 1 & -2 \\ 4 & -5 & 1 \\ 1 & 0 & 7 \end{vmatrix} \right| = 142.$$

Supongamos que G es un grupo abeliano finitamente generado con generadores $\omega_1, \ldots, \omega_n$ linealmente independientes. Podemos definir una aplicación $f : \mathbb{Z}^n \to G$ tal que $f(m_1, \ldots, m_n) = m_1\omega_1 + \cdots + m_n\omega_n$. Observamos que f es una aplicación sobreyectiva, por lo tanto $G \cong \mathbb{Z}/Ker(f)$, siendo $Ker(f) = H$, subgrupo de G.

Podemos elegir una nueva base $\{u_1, \ldots, u_n\}$ de $\mathbb{Z}^n$ de tal forma que $\alpha_1 u_1, \ldots, \alpha_s u_s$ sea base de H. Sea A un subgrupo de $\mathbb{Z}^n$ generado por

$u_1, \ldots, u_s$ y B otro generado por $u_{s+1}, \ldots, u_n$, entonces $G \cong (A/H) \times B$, con $n - s$ generadores. Queda así demostrada la siguiente proposición:

Proposición 1.6.7. *Cada grupo abeliano finitamente generado con n generadores es el producto directo de un grupo finito abeliano y un grupo libre de k generadores, con $k \leq n$.*

Si K es un subgrupo de G, con G un grupo abeliano finitamente generado, entonces $G = F \times B$, con F finito y B finitamente generado y libre, por la Proposición 1.6.7. Entonces $K \cong (F \cap K) \times H$ con H un subgrupo de B. Entonces $F \cap K$ es finito y H finitamente generado y libre. Por lo tanto, K es finitamente generado. Hemos probado así la siguiente proposición:

Proposición 1.6.8. *Un subgrupo de un grupo abeliano finitamente generado es finitamente generado.*

1.7. Anillos de Dedekind.

Figura 1.1: Julius Wilhelm Richard Dedekind (1831–1916) fue un matemático alemán doctorado en 1852 por la Universidad de Gotinga, bajo la supervisión de Gauss. En su tesis trató las integrales eulerianas; después estudió teoría de números, funciones abelianas y elípticas... Hasta que finalmente encontró su campo de trabajo: el álgebra y la teoría de números algebraicos.

En esta sección nuestro objetivo es definir anillo de Dedekind y enunciar una proposición que nos asegura que un anillo de Dedekind con un número finito de ideales primos es un dominio de ideales principales, es decir, un dominio cuyos ideales son todos principales. Este resultado cobrará gran importancia en el capítulo cuatro.

Definición 1.7.1. *Sea R dominio de integridad y K su cuerpo de fracciones. Decimos que R es* enteramente cerrado en *K si para cualquier $\alpha \in K$ y α satisfaciendo un polinomio mónico en $R[t]$, entonces $\alpha \in R$.*

Definición 1.7.2. *Un anillo es* noetheriano *si satisface la condición de la cadena ascendente, es decir, ninguna cadena ascendente puede prolongarse indefinidamente.*

Con estas definiciones ya estamos en disposición de definir la noción de anillo de Dedekind:

Definición 1.7.3. *Un dominio de integridad noetheriano, enteramente cerrado y de dimensión uno es un* anillo de Dedekind*. Es decir, un anillo de Dedekind es un anillo noetheriano íntegro, enteramente cerrado, que no es cuerpo, y tal que todo ideal primo no nulo es maximal.*

El siguiente resultado va a sernos de utilidad más adelante:

Proposición 1.7.4. *Sea A un anillo de Dedekind. Supongamos que A tiene solo un número finito de ideales primos. Entonces A es un dominio de ideales principales.*

Demostración. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ todos los ideales primos no nulos de A. Fijado uno de ellos, por ejemplo $\mathfrak{p} = \mathfrak{p}_1$, podemos elegir $a \in \mathfrak{p}$ de forma que $a \notin \mathfrak{p}^2$. Por el Teorema Chino del Resto, tenemos que el sistema de congruencias

$$\left\{ \begin{array}{c} x \equiv a (\text{mód } \mathfrak{p}) \\ x \equiv 1 (\text{mód } \mathfrak{p}_i), i > 1 \end{array} \right\}$$

tiene solución en A. Una solución x de este sistema es un generador del ideal $\mathfrak{p}$, ya que en la descomposición en producto de ideales primos del ideal principal xA no puede aparecer ningún primo distinto de $\mathfrak{p}$ y tampoco $\mathfrak{p}^2$. Además, el ideal xA no es todo el anillo A puesto que $x \in \mathfrak{p}$ por satisfacer la primera ecuación. En consecuencia, todo ideal primo de A es un ideal principal. □

1.8. Anillos locales y localización.

Esta sección va a ser un repaso del concepto de anillo local y alguna propiedad que verifica. Para terminar, trataremos el tema de localización.

1.8.1. Anillos locales.

Definición 1.8.1. *Un anillo A se dice* local *si tiene un único ideal maximal $\mathfrak{m}$ o, equivalentemente, si todos los elementos no invertibles forman un ideal.*

Vamos a ver a continuación unos resultados asociados a anillos locales. Estos resultados los hemos visto durante el curso del máster, pero es útil recordarlos.

Lema 1.8.2. *Sea A un anillo y $\mathfrak{m}$ un ideal propio de A. Son equivalentes:*

I) *Cada elemento $x \in A \setminus \mathfrak{m}$ es invertible.*

II) *A es un anillo local con ideal maximal $\mathfrak{m}$.*

Demostración. Dado un ideal propio $\mathfrak{a}$ de A, sus elementos no son invertibles y, como $\mathfrak{m}$ es maximal, obtenemos directamente que $\mathfrak{a} \subseteq \mathfrak{m}$. □

Proposición 1.8.3. *Sea A un anillo y $\mathfrak{m}$ un ideal maximal de A tal que cada elemento $x \in 1 + \mathfrak{m}$ es invertible. Entonces A es un anillo local.*

Demostración. Dado $x \in A\backslash\mathfrak{m}$ tenemos que $\mathfrak{m} + Ax = A$. Luego existen $m \in \mathfrak{m}$ y $a \in A$ tales que $m + ax = 1$. Despejando, tenemos que $ax = 1 - m \in 1 + \mathfrak{m}$, de donde obtenemos que ax es invertible y, por tanto, x también lo es. Así, aplicando el Lema 1.8.2 ya hemos terminado. □

1.8.2. Localización.

Vamos a pasar a tratar el tema de localización. El proceso de localización está asociado a la formación de anillos de fracciones y es una técnica muy importante.

Sea A un anillo y $S \subseteq A$ un subconjunto multiplicativamente cerrado. Suponemos además que $0 \notin S$. Consideramos el producto cartesiano $A \times S$ y definimos la siguiente relación de equivalencia

$$(a_1, s_1) \sim (a_2, s_2) \text{ si, y solo si, existe } t \in S \text{ tal que } (a_1 s_2 - a_2 s_1)t = 0.$$

Lema 1.8.4. *Sea A un anillo y S un conjunto multiplicativo. Entonces $(A \times S)/\sim$, con operaciones definidas por*

$$\overline{(a_1, s_1)} + \overline{(a_2, s_2)} = \overline{(a_1 s_2 + a_2 s_1, s_1 s_2)},$$

$$\overline{(a_1, s_1)} \cdot \overline{(a_2, s_2)} = \overline{(a_1 a_2, s_1 s_2)}$$

y elemento neutro igual a $\overline{(1,1)}$, es un anillo conmutativo.

Para simplificar notación, vamos a denotar a $(A \times S)/\sim$ por $S^{-1}A$ y lo llamaremos anillo de fracciones de A. Lo que hemos hecho ha sido *localizar* en A por el subconjunto S. El elemento $\overline{(a, s)}$ lo denotamos por $\frac{a}{s}$.

Demostración. La operación suma está bien definida.

Sea $\frac{a}{b} = \frac{a'}{b'}$, por lo tanto se tiene $s \in S$ tal que $(ab' - a'b)s = 0$. Para cada $\frac{c}{d} \in S^{-1}A$ se tiene

$$\left(\frac{a}{b} + \frac{c}{d}\right) - \left(\frac{a'}{b'} + \frac{c}{d}\right) = \frac{ad + bc}{bd} - \frac{a'd + b'c}{b'd} = \frac{(ad + bc)b'd - (a'd + b'c)bd}{bb'd^2}.$$

Para comprobar que es cero basta con manipular algebraicamente lo que hemos obtenido:

$$s[(ad + bc)b'd - (a'd + b'c)bd = s[ab'd^2 + bb'cd - a'bd^2 - bb'cd] =$$

$$= s(ab'd^2 - a'bd^2) = s(ab' - a'b)d^2 = 0.$$

□

Sea ahora A un anillo conmutativo y $\mathfrak{p}$ un ideal primo de A. Tenemos entonces que $S = A \setminus \mathfrak{p}$ es un subconjunto multiplicativo de A. Al anillo de fracciones $S^{-1}A$ con la notación que acabamos de dar, lo denotaremos por $A_{\mathfrak{p}}$ y cumple la siguiente propiedad:

Lema 1.8.5. *$A_{\mathfrak{p}}$ es un anillo local con ideal maximal*

$$S^{-1}\mathfrak{p} = \{\frac{a}{s} \in A_{\mathfrak{p}} \mid a \in \mathfrak{p}, s \in A \setminus \mathfrak{p}\}.$$

Demostración. Es claro que los elementos a/s, con $a \in \mathfrak{p}$ forman un ideal $S^{-1}\mathfrak{p}$ en $A_{\mathfrak{p}}$.

Ahora bien, si $x/s \notin A_{\mathfrak{p}}$, entonces $x \notin \mathfrak{p}$. Por lo tanto, $x \in S$ y, por lo tanto, x/s es un elemento invertible en $A_{\mathfrak{p}}$. De aquí se sigue que, si $\mathfrak{a} \not\subseteq S^{-1}\mathfrak{p}$ es un ideal en $A_{\mathfrak{p}}$, entonces $\mathfrak{a}$ contiene algún elemento invertible y, por lo tanto, $\mathfrak{a}$ es todo el anillo. Por lo tanto, $A_{\mathfrak{p}}$ solo tiene un único ideal maximal: $S^{-1}\mathfrak{p}$; y, por lo tanto, $A_{\mathfrak{p}}$ es un anillo local. □

Capítulo 2

Cuerpos de números.

2.1. Cuerpos de números.

Ya vimos en el capítulo anterior que $\alpha \in \mathbb{C}$ es *algebraico* si es raíz de un polinomio no nulo con coeficientes en $\mathbb{Q}$.

Teorema 2.1.1. *El conjunto $\mathcal{A}$ de números algebraicos es un subcuerpo de $\mathbb{C}$.*

Demostración. Por el Teorema 1.3.3 ya sabemos que α es algebraico si y solo si $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es finito.

Supongamos que α y β son algebraicos. Entonces, por el Teorema 1.3.1 tenemos que

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

Así, como β es algebraico sobre $\mathbb{Q}$, en particular lo es sobre $\mathbb{Q}(\alpha)$, por lo tanto $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ es finito y como $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ también lo es, entonces $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ es finito. Por lo tanto, $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, $\frac{\alpha}{\beta} \in \mathbb{Q}(\alpha, \beta)$, luego en particular están en $\mathcal{A}$. □

Definición 2.1.2. *Sea K un subcuerpo de $\mathbb{C}$. Decimos que K es un* cuerpo de números *si cumple que $[K : \mathbb{Q}]$ es finito, es decir, todo elemento de K es algebraico sobre $\mathbb{C}$.*

Observemos que $K \subseteq \mathcal{A}$, siendo $\mathcal{A}$ el conjunto de números algebraicos. Si nos fijamos bien, tenemos que $[\mathcal{A} : \mathbb{Q}]$ no es finito. Sin embargo, si K es un cuerpo de números, entonces $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, para un número finito n.

Teorema 2.1.3. *Si K es un cuerpo de números, entonces $K = \mathbb{Q}(\theta)$, para algún θ algebraico.*

Demostración. Utilizando inducción, es suficiente probar que si $K = K_1(\alpha, \beta)$, entonces $K = K_1(\theta)$, para algún θ algebraico y $K_1 \subset K$.

Sean f y g los polinomios mínimos de α y β sobre K_1 y supongamos que descomponen en $\mathbb{C}$ de la siguiente manera:

$$f(t) = (t - \alpha_1) \cdot \cdots \cdot (t - \alpha_n),$$

$$g(t) = (t - \beta_1) \cdot \cdots \cdot (t - \beta_m).$$

Tomamos $\alpha_1 = \alpha$ y $\beta_1 = \beta$. Sabemos también que los α_i son todos diferentes y lo mismo ocurre con los β_j. Por lo tanto, $\forall i$ y $\forall k \neq 1$, existe como mucho un elemento $x \in K_1$ tal que $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$.

Como sólo hay un número finito de estas ecuaciones, elegimos $c \neq 0, c \in K_1$ diferente a estos x y entonces $\alpha_i + cx\beta_k \neq \alpha_1 + c\beta_1$, para $1 \leq i \leq n$ y $2 \leq k \leq m$.

Definimos ahora $\theta = \alpha + c\beta$ y vamos a probar por doble contenido que $K(\alpha, \beta) = K(\theta)$.

$K(\alpha, \beta) \supseteq K(\theta)$: Trivial.

$K(\alpha, \beta) \subseteq K(\theta)$: Como $\theta = \alpha + c\beta$, entonces $\alpha = \theta - c\beta$. Por lo tanto, debemos ver que $\beta \in K(\theta)$. Tenemos que $f(\theta - c\beta) = f(\alpha) = 0$. Definimos el polinomio $h(t) = f(\theta - ct) \in K_1(\theta)[t]$. Entonces β es un cero de $g(t)$ y de $h(t)$. Estos polinomios tienen un único cero en común puesto que si $h(\xi) = g(\xi)$, entonces ξ es $\beta_1, \ldots, \beta_m$ y $\theta - c\xi$ es $\alpha_1, \ldots, \alpha_n$ y por nuestra elección de c tendríamos que $\xi = \beta$. Sea $r(t)$ el polinomio mínimo de β sobre $K_1(\theta)$, entonces $r(t) \mid g(t)$ y $r(t) \mid h(t)$. Como $g(t)$ y $h(t)$ tienen un único cero en común en $\mathbb{C}$, entonces el grado de $r(t)$ es uno y $r(t) = t + \mu$, con $\mu \in K_1(\theta)$, y además $r(\beta) = 0 = \beta + \mu$, es decir, $-\mu = \beta$, luego $\beta \in K_1(\theta)$. □

Ejemplo 2.1.4. *Sea $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ un cuerpo de números. Sea*

$$f(t) = t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$$

el polinomio mínimo de $\alpha = \sqrt{2}$, es decir, $\alpha_1 = \sqrt{2}$ y $\alpha_2 = -\sqrt{2}$. De manera equivalente, $g(t) = t^3 - 5 = (t - \sqrt[3]{5})(t - \sqrt[3]{5}\omega)(t - \sqrt[3]{5}\omega^2)$, con $\omega = \frac{1}{2}(-1 + i\sqrt{3})$, el polinomio mínimo de $\beta = \sqrt[3]{5}$. Es decir, $\beta_1 = \sqrt[3]{5}$, $\beta_2 = \sqrt[3]{5}\omega$ y $\beta_2 = \sqrt[3]{5}\omega^2$.

Si $c = 1$ se satisface

$$\alpha_i + c\beta_k \neq \alpha + c\beta,$$

para $i = 1, 2$ y $k = 2, 3$. Por lo tanto, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$.

2.2. Conjugados y discriminantes.

En esta sección vamos a tratar los conjugados y los discriminantes de un cuerpo de números. Comenzaremos definiendo los conjugados de un número algebraico, dando algunas propiedades y caracterizaciones. Terminaremos la sección definiendo el concepto de discriminante de un cuerpo de números.

Teorema 2.2.1. *Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números de grado n sobre $\mathbb{Q}$. Entonces hay exactamente n monomorfismos diferentes $\sigma_i : K \to \mathbb{C}$, $i = 1, \ldots, n$. Los elementos $\sigma_i(\theta) = \theta_i$ son los distintos ceros en $\mathbb{C}$ del polinomio mínimo de θ sobre K.*

Demostración. Sean $\theta_1, \ldots, \theta_n$ los distintos ceros en $\mathbb{C}$ del polinomio mínimo f de θ sobre $\mathbb{Q}$. Cada θ_i tiene un polinomio mínimo f_i (que divide a f). Por lo tanto, existe un único isomorfismo de cuerpos $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tal que $\sigma_i(\theta) = \theta_i$.

De hecho, si $\alpha \in \mathbb{Q}(\theta)$, entonces $\alpha = g(\theta)$, para un único $g(t) \in \mathbb{Q}[t]$, con el grado de g menor que n. Entonces, $\sigma_i(\alpha) = g(\theta_i)$.

Por otra parte, si $\sigma : K \to \mathbb{C}$ es un monomorfismo, entonces $\sigma = Id_{\mathbb{Q}}$, luego $0 = \sigma(f(\theta)) = f(\sigma(\theta))$. O lo que es lo mismo, $\sigma(\theta) = \theta_i$. Esto implica que $\sigma = \sigma_i$. □

Para cada $\alpha \in K = \mathbb{Q}(\theta)$ denotamos por $f_\alpha(t)$ a

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

Teorema 2.2.2. *Sea $\alpha \in K$, entonces $f_\alpha(t) \in \mathbb{Q}[t]$.*

Demostración. Sea $\alpha = f(\theta)$, con $f \in \mathbb{Q}[t]$ y con el grado de f menor que $n = [K : \mathbb{Q}]$. Entonces $f_\alpha(t) = \prod_i (t - f(\theta_i))$, con θ_i los ceros del polinomio mínimo de θ. Los coeficientes de f_α son de la forma $h(\theta_1, \ldots, \theta_n)$, con $h(t_1, \ldots, t_n)$ polinomios simétricos en $\mathbb{Q}[t_1, \ldots, t_n]$. Así, por el Corolario 1.4.4 tenemos que $h(\theta_1, \ldots, \theta_n) \in \mathbb{Q}$. □

Definición 2.2.3. *Los elementos $\sigma_i(\alpha), i = 1, \ldots, n$, se denominan K-conjugados de α.*

Observemos que aunque los θ_i son siempre distintos, no siempre es cierto que los K-conjugados de α lo sean. Por ejemplo, $\sigma_i(1) = 1, \forall i$.

Teorema 2.2.4. *Sea p_α el polinomio mínimo de $\alpha \in K$ sobre $\mathbb{Q}$ y sea n el grado de K sobre $\mathbb{Q}$. Entonces:*

I) *El polinomio f_α es una potencia de p_α.*

II) *Los K-conjugados de α son los ceros de p_α en $\mathbb{C}$, cada uno repetido $\frac{n}{m}$ veces, donde m es el grado de p_α.*

III) *$\alpha \in \mathbb{Q}$ si y solo si todos los K-conjugados son iguales.*

IV) *$\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ si y solo si todos los K-conjugados de α son distintos.*

Demostración.

I) Sea $q = p_\alpha$ irreducible y α un cero de $f = f_\alpha$. Esto implica que $f = q^s h$, con q y h coprimos. h es constante, pues si no lo fuera, algún $\alpha_i = \sigma_i(\alpha) = r(\theta_i)$ sería cero de h, con $\alpha = r(\theta)$. Entonces si $g(t) = h(r(t))$, tendríamos que $g(\theta_i) = 0$.

Sea p el polinomio mínimo de θ sobre $\mathbb{Q}$, por lo tanto también de θ_i. Entonces $p \mid g$ y esto implica que $g(\theta_i) = 0, \forall i$. En particular, $g(\theta) = 0$. Por lo tanto, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$ y esto implica que $q \mid h$ y esto es absurdo pues hemos elegido q y h coprimos. Entonces, h es constante y mónico. Por lo tanto, $f = q^s$.

II) Directo por I).

III) Si $\alpha \in \mathbb{Q}$, entonces $\sigma_i(\alpha) \in \mathbb{Q}$.

Para probar la otra implicación, si todos los $\sigma_i(\alpha)$ son iguales, como los ceros de p_α son distintos y $f_\alpha = q^s$, entonces el grado de q es uno y esto implica que $\alpha \in \mathbb{Q}$.

IV) Si todos los $\sigma_i(\alpha)$ son distintos, entonces el grado de p_α es n. Esto implica que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n = [\mathbb{Q}(\theta) : \mathbb{Q}]$, por lo tanto $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$.

Probemos ahora la otra implicación. Si $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$, entonces los σ_i son distintos pues el grado de p_α es n.

□

Definición 2.2.5. *Sea $K = \mathbb{Q}(\theta)$ de grado n sobre $\mathbb{Q}$. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de K como espacio vectorial sobre $\mathbb{Q}$. Definimos el* discriminante *de esta base como $\triangle[\alpha_1, \ldots, \alpha_n] = (\det(\sigma_i(\alpha_j)))^2$.*

Observemos que si tomamos otra base $\{\beta_1, \ldots, \beta_n\}$, entonces podemos escribir los β_k de la siguiente manera.

$$\beta_k = \sum_{i_1}^{n} c_{ik}\alpha_i,$$

con $c_{ik} \in \mathbb{Q}$ y $\det(c_{ik}) \neq 0$. Entonces

$$\triangle[\beta_1, \ldots, \beta_n] = (\det(c_{ik}))^2 \triangle [\alpha_1, \ldots, \alpha_n].$$

Teorema 2.2.6. *El discriminante de cualquier base de $K = \mathbb{Q}(\theta)$ es racional y no nulo. Si todos los K-conjugados de θ son reales, entonces el discriminante de cualquier base es positivo.*

Demostración. Tomamos la base $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. Si los conjugados de θ son $\theta_1, \ldots, \theta_n$, entonces $\triangle[1, \theta, \theta^2, \ldots, \theta^{n-1}] = det(\theta_i^j)^2$. Esto implica que

$$\triangle = \triangle[1, \theta, \theta^2, \ldots, \theta^{n-1}] = [\prod(\theta_i - \theta_j)]^2.$$

Este producto es simétrico. Estonces, por el Corolario 1.4.4 tenemos que $\triangle$ es racional.

Ahora bien, como $\triangle$ es racional y los θ_i son distintos, entonces $\triangle \neq 0$. Sea $\{\beta_1, \ldots, \beta_n\}$ una base cualquiera de K. Entonces

$$\triangle[\beta_1, \ldots, \beta_n] = (\det(c_{ik}))^2 \triangle,$$

con $c_{ik} \in \mathbb{Q}$ y $\det(c_{ik}) \neq 0$. Así, $\triangle[\beta_1, \ldots, \beta_n] \neq 0$ y $\triangle[\beta_1, \ldots, \beta_n] \in \mathbb{Q}$.

Si $\theta_i \in \mathbb{R}$, entonces $\triangle \in \mathbb{R}^+$. Por lo tanto $\triangle[\beta_1, \ldots, \beta_n] \in \mathbb{R}^+$. □

2.3. Enteros algebraicos.

Decimos que $\theta \in \mathbb{C}$ es un *entero algebraico* si existe un polinomio mónico $p(t)$ con coeficientes enteros tal que $p(\theta) = 0$. Vamos a llamar $\mathcal{B}$ al conjunto de enteros algebraicos.

Ejemplo 2.3.1.

1. *$\theta = \sqrt{3}$ es entero algebraico pues $p(t) = t^2 - 3$ verifica que $p(\theta) = 0$.*
2. *$\theta = \frac{2}{3}$ no es entero algebraico pues $p(t) = 3t-2$ no es mónico o $p(t) = t-\frac{2}{3}$ no tiene coeficientes en $\mathbb{Z}$.*

Teorema 2.3.2. *Un número complejo θ es entero algebraico si y solo si el grupo aditivo generado por las potencias $1, \theta, \theta^2, \ldots$ es finitamente generado.*

Demostración.

$\Rightarrow$) Por hipótesis tenemos que θ es entero algebraico, es decir, $\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = 0$, con $a_i \in \mathbb{Z}$.

Vamos a ver que todas las potencias de θ están en el grupo aditivo Γ generado por $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Tenemos que $\theta^n \in \Gamma$ y usando inducción, si $m \geq n$, entonces

$$\theta^{m+1} = \theta^{m+1-n}\theta^n = \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - \cdots - a_0) \in \Gamma.$$

Por lo tanto, toda potencia de θ esta en Γ, que es finitamente generado.

$\Leftarrow$) Supongamos ahora que toda potencia de θ está en un grupo aditivo G finitamente generado. El subgrupo Γ de G generado por $1, \theta, \theta^2, \ldots, \theta^n$ también es finitamente generado. Por lo tanto, Γ tiene generadores $v_1, \ldots, v_n$. Cada v_i es un polinomio en θ con coeficientes enteros. Por lo tanto, θv_i también es polinomio, luego existen enteros b_{ij} tales que

$$\theta v_i = \sum_{j=1}^{n} b_{ij} v_j.$$

Obtenemos así el sistema homogéneo

$$\begin{cases} (b_{11} - \theta)v_1 + b_{12}v_2 + \cdots + b_{1n}v_n = 0, \\ b_{21}v_1 + (b_{22} - \theta)v_2 + \cdots + b_{2n}v_n = 0, \\ \qquad\qquad \cdots \\ b_{n1}v_1 + b_{n2}v_2 + \cdots + (b_{nn} - \theta)v_n = 0. \end{cases}$$

Y como existen $v_1, \ldots, v_n$ no todos nulos que son solución del sistema, entonces

$$\begin{vmatrix} (b_{11} - \theta) & b_{12} & \ldots & b_{1n} \\ b_{21} & (b_{22} - \theta) & \ldots & b_{2n} \\ & & \cdots & \\ b_{n1} & b_{n2} & \ldots & (b_{nn} - \theta) \end{vmatrix} = 0.$$

Esto implica que θ es raíz de algún polinomio con coeficientes en $\mathbb{Z}$ y, por lo tanto, θ es algebraico. □

Teorema 2.3.3. *El anillo $\mathcal{B}$ de enteros algebraicos es subanillo del cuerpo de números algebraicos $\mathcal{A}$.*

Demostración. Sean $\theta, \alpha \in \mathcal{B}$. Tenemos que comprobar que $\theta + \alpha$ y $\theta\alpha$ pertenecen a $\mathcal{B}$.

Usando el Teorema 1.3.2 tenemos:

- Todas las potencias de θ están en un subgrupo aditivo finitamente generado Γ_θ de $\mathbb{C}$.

- Todas las potencias de α están en un subgrupo aditivo finitamente generado Γ_α de $\mathbb{C}$.

Además, todas las potencias de $\alpha+\theta$ y $\alpha\theta$ son combinaciones lineales de elementos $\alpha^j\theta^i \in \Gamma_\theta\Gamma_\alpha \subseteq \mathbb{C}$.

Si $v_1,\ldots,v_n$ generan Γ_θ y $w_1,\ldots,w_m$ generan Γ_α, entonces v_iw_j generan $\Gamma_\alpha\Gamma_\theta$, con $1\leq i\leq n, 1\leq j\leq m$. Con esto, tenemos que $\theta+\alpha$ y $\theta\alpha$ y sus potencias están en un grupo aditivo finitamente generado de $\mathbb{C}$ y, por el Teorema 2.3.2, $\theta+\alpha$ y $\theta\alpha$ están en $\mathcal{B}$. □

Teorema 2.3.4. *Sea θ un número complejo satisfaciendo un polinomio mónico cuyos coeficientes son enteros algebraicos. Entonces θ es entero algebraico.*

Demostración. Supongamos que $\theta^n+\alpha_{n-1}\theta^{n-1}+\cdots+\alpha_0=0$, con $\alpha_i\in\mathcal{B}$, genera un subanillo $\psi\subset\mathcal{B}$. Por el Teorema 2.3.2, todas las potencias de θ están en un ψ-submódulo M de $\mathbb{C}$ finitamente generado, expandido por $1,\theta,\theta^2,\ldots,\theta^{n-1}$. Usando el Teorema 2.3.2, cada α_i y todas sus potencias están en un grupo aditivo finitamente generado Γ_i con generadores γ_{ij}, $1\leq j\leq n_i$. Entonces M está dentro del grupo aditivo generado por $\gamma_{1j_1},\gamma_{2j_2},\ldots,\gamma_{n-1\ j_{n-1}}\theta^k$, con $1\leq j_i,n_i,\ 0\leq i\leq n-1$ y $0\leq k\leq n-1$. Esto es un conjunto finito y, por tanto, M es finitamente generado. □

Definimos el *anillo de enteros de un cuerpo de número K* como $\mathcal{O}_K=\mathcal{B}\cap K$. Como $K,\mathcal{B}$ son subanillos de $\mathbb{C}$, entonces $\mathcal{O}_K$ es subanillo de K. En concreto, $\mathbb{Z}\subset\mathbb{Q}\subseteq K$ y $\mathbb{Z}\subseteq\mathcal{B}$. Luego $\mathbb{Z}\subseteq\mathcal{O}_K$.

Lema 2.3.5. *Si $\alpha\in K$, entonces, para algún $c\in\mathbb{Z}$, $c\alpha\in\mathcal{O}_K$.*

Demostración. Como $\alpha\in K$, en particular es algebraico puesto que por el Teorema 2.1.3 sabemos que $K=\mathbb{Q}(\beta)$, para cierto β algebraico. Así, α es raíz de cierto polinomio $p(t)\in\mathbb{Q}[t]$. Utilizando ahora el Lema 2.2.6 tenemos que existe $\lambda\in\mathbb{Z}$ de forma que $\lambda p(t)\in\mathbb{Z}[t]$. Por lo tanto, va a existir $\beta\in\mathbb{Z}$ tal que $\beta\alpha$ es raíz del polinomio λp obteniendo así que $\beta\alpha$ es un número entero. □

Corolario 2.3.6. *Si K es un cuerpo de números, entonces $K=\mathbb{Q}(\theta)$, para algún θ entero algebraico.*

Demostración. Tenemos que $K=\mathbb{Q}$, para α algebraico. Por el Lema 2.3.5, $\theta=c\alpha$ es entero algebraico, con $c\in\mathbb{Z}\setminus 0$. Entonces $\mathbb{Q}(\theta)=\mathbb{Q}(\alpha)$. □

Lema 2.3.7. *Un número algebraico α es entero algebraico si y solo si su polinomio mínimo sobre $\mathbb{Q}$ tiene coeficientes en $\mathbb{Z}$.*

Demostración.

$\Leftarrow$) Sea p el polinomio mínimo de α sobre $\mathbb{Q}$. Si $p \in \mathbb{Z}[t]$, entonces α es entero algebraico por definición.

$\Rightarrow$) Si α es entero algebraico, entonces $q(\alpha) = 0$ para algún $q \in \mathbb{Z}[t]$ mónico y $p \mid q$, siendo p el polinomio mínimo de α sobre $\mathbb{Q}$. Usando el Lema 2.2.6 tenemos que $p \in \mathbb{Z}[t]$, puesto que existe algún racional λ tal que $\lambda p \in \mathbb{Z}[t]$ y $\lambda \mid q$, y como p y q son mónicos, entonces $\lambda = 1$. □

Lema 2.3.8. *Un entero algebraico es un número racional si y solo es entero. Equivalentemente, $\mathcal{B} \cap \mathbb{Q} = \mathbb{Z}$.*

Demostración. El contenido $\mathbb{Z} \subseteq \mathcal{B} \cap \mathbb{Q}$ ya lo hemos visto antes. Vamos a ver el contenido que nos falta. Sea $\alpha \in \mathcal{B} \cap \mathbb{Q}$. Como $\alpha \in \mathbb{Q}$, su polinomio mínimo sobre $\mathbb{Q}$ es $t - \alpha$. Por el Lema 2.3.7, los coeficientes están en $\mathbb{Z}$, luego $-\alpha \in \mathbb{Z}$. Es decir, $\alpha \in \mathbb{Z}$. □

2.4. Bases enteras.

Dado K un cuerpo de números de grado n sobre $\mathbb{Q}$, una $\mathbb{Q}$-base de K es una base para K como espacio vectorial sobre $\mathbb{Q}$. Además, ya hemos visto anteriormente que $K = \mathbb{Q}(\theta)$, siendo θ un entero algebraico. Entonces, el polinomio mínimo de θ sobre $\mathbb{Q}$ es de grado n y $\{1, \theta, \theta^2, \dots \theta^{n-1}\}$ es una base para K.

Definición 2.4.1. *Una $\mathbb{Z}$-base para $(\mathcal{O}_K, +)$ se denomina* base entera para K o $\mathcal{O}_K$.

Podemos caracterizar del siguiente modo a las bases enteras: una base

$$\{\alpha_1, \dots, \alpha_s\}$$

es una base entera si y solo si $\alpha_i \in \mathcal{O}_K$ y cada elemento de $\mathcal{O}_K$ se puede expresar de forma única como $v_1\alpha_1 + \cdots + \alpha_s v_s$, con $v_i \in \mathbb{Z}$.

Observemos que una base entera es, en particular, una $\mathbb{Q}$-base. Además, se verifica que $s = n$. Podemos asegurar que si $K = \mathbb{Q}(\theta)$ con θ entero algebraico, entonces $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ es $\mathbb{Q}$-base de K de enteros algebraicos pero no implica que sea una base entera.

Vamos a ver a continuación que la base entera de un cuerpo de números existe. La existencia de esta base será equivalente a ver que $(\mathcal{O}_K, +)$ es un grupo abeliano libre de rango n.

Lema 2.4.2. *Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de K de enteros algebraicos, entonces $\triangle[\alpha_1, \ldots, \alpha_n]$ es un número entero distinto de cero.*

Demostración. Por el Teorema 2.2.6 tenemos que $\triangle = \triangle[\alpha_1, \ldots, \alpha_n]$ es racional y no nulo. En particular es entero algebraico porque los α_i lo son. Por el Lema 2.3.8 sabemos que $\triangle[\alpha_1, \ldots, \alpha_n]$ es entero. □

Teorema 2.4.3. *Todo cuerpo de números K tiene una base entera y el grupo aditivo de $\mathcal{O}_K$ es abeliano libre de rango n, siendo n el grado de K.*

Demostración. Por ser K un cuerpo de números, tenemos que $K = \mathbb{Q}(\theta)$ con θ un entero algebraico. Esto implica que existe una base de enteros algebraicos para K

$$\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}.$$

Sabemos además que el discriminante de una $\mathbb{Q}$-base de enteros algebraicos es siempre un entero, entonces tomamos una base de enteros algebraicos

$$\{\omega_1, \ldots, \omega_n\}$$

de manera que $|\triangle[\omega_1, \ldots, \omega_n]|$ sea mínimo. Esta es la base entera, pues si no lo es, existiría $\omega \in K$ tal que $\omega = a_1\omega_1 + \cdots + a_n\omega_n$, con no todos los a_i en $\mathbb{Z}$. Veámoslo: si tomamos $a_1 \notin \mathbb{Z}$, entonces tendríamos que $a_1 = a + r$, con $a \in \mathbb{Z}$ y $r \in (0, 1)$. Definimos $\psi_1 = \omega - a\omega_1$ y $\psi_i = \omega_i, i = 2, \ldots, n$. Entonces $\{\psi_1, \ldots, \psi_n\}$ es una base de enteros algebraicos. El determinante relacionado con el cambio de base de $\omega's$ a $\psi's$ tenemos

$$\begin{vmatrix} (a_1 - a) & a_2 & \ldots & a_n \\ 0 & 1 & \ldots & 0 \\ & & \ddots & \\ 0 & & \ldots & 1 \end{vmatrix} = r.$$

Esto implica que

$$\triangle[\psi_1, \ldots, \psi_n] = r^2 \triangle [\omega_1, \ldots, \omega_n],$$

pero como $r \in (0, 1)$ tenemos una contradicción pues $\triangle[\omega_1, \ldots, \omega_n]$ era mínimo. Por lo tanto $\{\omega_1, \ldots, \omega_n\}$ es una base entera y que $(\mathcal{O}_K, +)$ es un grupo abeliano libre de rango n. □

Definición 2.4.4. *Un número entero es* libre de cuadrados *si no es divisible por el cuadrado de un número primo.*

Vamos a enunciar un teorema que nos va a ayudar a identificar si una base es entera.

Teorema 2.4.5. *Supongamos que $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ forman una $\mathbb{Q}$-base de K. Si $\triangle\,[\alpha_1, \ldots, \alpha_n]$ es libre de cuadrados entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera.*

Demostración. Sea $\{\beta_1, \ldots, \beta_n\}$ una base entera. Entonces existen $c_{ij} \in \mathbb{Z}$ tales que $\alpha_i = \sum_j c_{ij}\beta_j$ y $\triangle[\alpha_1, \ldots, \alpha_n] = (\det(c_{ij}))^2 \triangle\,[\beta_1, \ldots, \beta_n]$.

Por hipótesis teníamos que $\triangle[\alpha_1, \ldots, \alpha_n]$ era libre de cuadrados, luego $(\det(c_{ij})) = \pm 1$, es decir (c_{ij}) es unimodular. Por el Lema 2.6.2 tenemos que $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Z}$-base para $\mathcal{O}_K$, luego es base entera para K. □

Ejemplo 2.4.6. *Sea $K = \mathbb{Q}(\sqrt{5})$. Vamos a comprobar que $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{5}\}$ es una base entera.*

Tenemos que $1, \frac{1}{2} + \frac{1}{2}\sqrt{5} \in \mathcal{O}_K$. Calculamos el discriminante de esta base:

$$\begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{5} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{5} \end{vmatrix}^2 = 5.$$

Así, como el discriminante de esta base es 5 y 5 es un número libre de cuadrados, tenemos que, efectivamente, $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{5}\}$ es una base entera.

Observemos que dadas dos bases enteras $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ de un cuerpo de números algebraicos K, tenemos que

$$\triangle[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2 \triangle\,[\beta_1, \ldots, \beta_n].$$

Esto implica que

$$\triangle[\alpha_1, \ldots, \alpha_n] = \triangle[\beta_1, \ldots, \beta_n].$$

A este número lo denominamos *discriminante de K*. Notar que el discriminante de un cuerpo de números algebraicos K es siempre entero y no nulo.

2.5. Normas y trazas.

En esta sección vamos a definir los conceptos de norma y traza. Vamos a relacionar dichos conceptos con el discriminante de un cuerpo de números.

Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números de grado n y $\sigma_1, \ldots, \sigma_n$ morfismos definidos de K en $\mathbb{C}$.

Definición 2.5.1. *Dado $\alpha \in K$, definimos la* norma de α en K *como*

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Definimos la traza de α en K *como*

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

Recordemos que habíamos asociado a $\alpha \in K$ el polinomio

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

También habíamos visto que $\alpha \in K$ es un entero algebraico si y solo si $f_\alpha(t) \in \mathbb{Z}[t]$. De aquí deducimos que si α es entero algebraico, entonces $\mathrm{N}_K(\alpha)$ y $\mathrm{Tr}_K(\alpha)$ son números enteros.

Como σ_i son monomorfismos, para $\alpha, \beta \in K$, se verifican las siguientes propiedades:

$$\mathrm{N}_K(\alpha\beta) = N_K(\alpha)N_K(\beta),$$
$$\mathrm{Tr}_K(\alpha + \beta) = T_K(\alpha) + T_K(\beta).$$

Ejemplo 2.5.2. *Sea $K = \mathbb{Q}(\sqrt{7})$. Una $\mathbb{Q}$-base de K es $\{1, \sqrt{7}\}$, por lo que*

$$\mathbb{Q}(\sqrt{7}) = \{p + q\sqrt{7} \mid p, q \in \mathbb{Q}\}.$$

Así, los σ_i son de la forma

$$\sigma_1(p + q\sqrt{7}) = p + q\sqrt{7}, \qquad \sigma_2(p + q\sqrt{7}) = p - q\sqrt{7}.$$

Por lo tanto, la norma y la traza de un elemento $\alpha = p + q\sqrt{7}$ son como siguen:

$$N_K(p + q\sqrt{7}) = p^2 - 7q^2.$$
$$Tr_K(p + q\sqrt{7}) = 2p.$$

Proposición 2.5.3. *Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números, donde θ tiene como polinomio mínimo p de grado n. La $\mathbb{Q}$-base $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ tiene discriminante*

$$\triangle[1, \theta, \theta^2, \ldots, \theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}} N_K(D_p(\theta)),$$

donde D_p es la derivada de p.

Demostración. Tenemos que

$$\triangle = \triangle[1, \theta, \theta^2, \ldots, \theta^{n-1}] = \prod_{1 \leq i,j \leq n} (\sigma_i - \sigma_j)^2,$$

donde los σ_i son los conjugados de θ. Por lo tanto,

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

Derivando, obtenemos que la derivada del polinomio p es

$$D_p(t) = \sum_{j=1}^{n} \prod_{i=1, i \neq j}^{n} (t - \theta_i).$$

Si evaluamos este último cálculo en θ_j obtenemos

$$D_p(\theta_j) = \prod_{i=1, i \neq j}^{n} (\theta_j - \theta_i).$$

Multiplicando tenemos que

$$\prod_{j=1}^{n} D_p(\theta_j) = \prod_{i,j=1, i \neq j}^{n} (\theta_j - \theta_i).$$

Si nos fijamos, la parte izquierda de la igualdad es la norma de la derivada formal de p, es decir, $N_K(D_p(\theta)) = \prod_{j=1}^{n} D_p(\theta_j)$.

En la parte derecha de la igualdad tenemos que cada factor $(\theta_i - \theta_j), i < j$ aparece dos veces: $(\theta_i - \theta_j)$ y $(\theta_j - \theta_i)$. Si los multiplicamos obtenemos $-(\sigma_i - \sigma_j)^2$.

Multiplicándolos todos tenemos que $\triangle$ está multiplicados por $(-1)^s$, con s el número de pares (i, j), $1 \leq i, j \leq n$, es decir, $s = \frac{n(n-1)}{2}$. Por lo tanto, tenemos que

$$\triangle[1, \theta, \theta^2, \ldots, \theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}} N_K(D_p(\theta)).$$

□

Proposición 2.5.4. *Si $\{\alpha_1, \ldots, \alpha_n\}$ es cualquier $\mathbb{Q}$-base de un cuerpo de números K, entonces*

$$\triangle[\alpha_1, \ldots, \alpha_n] = \det(Tr_K(\alpha_i\alpha_j)).$$

Demostración. Vamos a comenzar calculando cuánto vale $\mathrm{Tr}_K(\alpha_i\alpha_j)$:

$$\mathrm{Tr}_K(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j).$$

Ahora tenemos que

$$\triangle[\alpha_1, \ldots, \alpha_n] = [\det(\sigma_i(\alpha_j))]^2 = [\det(\sigma_j(\alpha_i))][\det(\sigma_i(\alpha_j))] =$$

$$= \det(\sum_{r=1}^{n} \sigma_i(\alpha_j)\sigma_j(\alpha_i)) = \det(\mathrm{Tr}_K(\alpha_i\alpha_j)).$$

□

2.6. Anillos de enteros.

En esta sección vamos a ver cómo calcular el anillo de enteros algebraicos de un cuerpo de números. Probaremos primero una serie de teoremas y proposiciones y, finalmente, daremos un procedimiento explícito para calcular el anillo de enteros de un cuerpo dado.

Teorema 2.6.1. *Sea G un subgrupo aditivo de $\mathcal{O}_K$ de rango igual al grado de K, con $\mathbb{Z}$-base $\{\alpha_1, \ldots, \alpha_n\}$. Entonces,*

$$|\mathcal{O}_K/G|^2 \mid \triangle[\alpha_1, \ldots, \alpha_n] = \triangle_G.$$

Demostración. Por el Teorema 1.6.4 tenemos que existe una $\mathbb{Z}$-base de $\mathcal{O}_K$ de la forma $\{\beta_1 \ldots, \beta_n\}$ tal que G tiene $\mathbb{Z}$-base $\{\mu_1\beta_1 \ldots, \mu_n\beta_n\}$, para ciertos $\mu_i \in \mathbb{Z}$.

Ya sabemos que al cambiar de base tenemos que utilizar una matriz unimodular, por lo tanto, $\triangle[\beta_1 \ldots, \beta_n] = \triangle[\mu_1\beta_1 \ldots, \mu_n\beta_n]$.

Además, $\triangle[\mu_1\beta_1 \ldots, \mu_n\beta_n] = (\mu_1 \cdot \ldots \cdot \mu_n)^2 \triangle[\beta_1 \ldots, \beta_n] = (\mu_1 \cdot \ldots \cdot \mu_n)^2\triangle$, siendo $\triangle \in \mathbb{Z}$ el discriminante de K.

Pero gracias al Teorema 1.6.5 sabemos que $|(\mu_1 \cdot \ldots \cdot \mu_n)| = |\mathcal{O}/G|$, luego $|(\mu_1 \cdot \ldots \cdot \mu_n)|^2 = |\mathcal{O}/G|^2$. Esto implica que

$$|\mathcal{O}_K/G|^2 \mid \triangle[\alpha_1, \ldots, \alpha_n] = \triangle_G.$$

□

Proposición 2.6.2. *Sea G un subgrupo aditivo de $\mathcal{O}_K$ de rango igual al grado de K, con $\mathbb{Z}$-base $\{\alpha_1, \ldots, \alpha_n\}$ y supongamos que $G \neq \mathcal{O}_K$. Entonces existe un entero algebraico de la forma $\frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n)$, con $0 \leq \lambda_i \leq p-1, \lambda_i \in \mathbb{Z}$ y p primo, tal que $p^2 \mid \triangle_G$.*

Demostración. Tenemos que si $G \neq \mathcal{O}_K$, entonces $|\mathcal{O}_K/G| > 1$.

Por teoría de grupos abelianos finitos, sabemos que existe p primo tal que $p \mid |\mathcal{O}_K/G|$ y $u \in \mathcal{O}_K/G$ tal que $g = pu \in G$.

Usando el teorema anterior, tenemos que $p^2 \mid |\mathcal{O}_K/G|$. En particular, $g = pu$ implica que $u = \frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n)$, pues $\{\alpha_1, \ldots, \alpha_n\}$ es $\mathbb{Z}$-base de G. □

Vamos a dar ya el método para calcular $\mathcal{O}_K$. Tomamos un subgrupo G que sepamos seguro que va a estar contenido dentro de $\mathcal{O}_K$.

1. Calculamos $\triangle_G$.

2. Si $\triangle_G$ es libre de cuadrados, entonces $G = \mathcal{O}_K$. Si no, $\forall p$ primo tal que $p^2 \mid \triangle_G$, comprobar todos los números de la forma vista en la Proposición 2.6.2 y ver cuáles son enteros algebraicos y cuales no.

3. Si hay enteros algebraicos nuevos, tomamos G' igual a la unión de G con los enteros algebraicos nuevos y calculamos $\triangle_{G'} = \frac{\triangle_G}{p^2}$.

4. Repetir 3 y 4 hasta que no se consigan más enteros algebraicos nuevos.

Ejemplo 2.6.3. *Vamos a calcular el anillo de enteros algebraicos del cuerpo de números $K = \mathbb{Q}(\sqrt[3]{5})$.*

Tomamos $\theta \in \mathbb{R}$ tal que $\theta^3 = 5$ y de manera que $\mathcal{O}_K$ tenga $\mathbb{Z}$-base entera $\{1, \theta, \theta^2\}$. Sea G el subgrupo generado por este conjunto y $\omega = e^{\frac{2\pi i}{3}}$. Calculamos $\triangle_G$:

$$\triangle_G = \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \omega\theta & \omega^2\theta \\ 1 & \omega^2\theta & \omega\theta^2 \end{vmatrix} = \theta^6 \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix} = -3^3 \cdot 5^2.$$

Así, tenemos que considerar los casos

a) $\alpha = \frac{1}{3}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2),\ 0 \leq \lambda_i \leq 2.$

b) $\alpha = \frac{1}{5}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2),\ 0 \leq \lambda_i \leq 4.$

Vamos a ver el caso b). Para hacer el caso a) habría que repetir el procedimiento que vamos a hacer ahora.

Tenemos que la traza de α *es* $T(\alpha) = \frac{3\lambda_1}{5} \in \mathbb{Z}$*, puesto que la traza de un entero algebraico es un número entero. Entonces* $\lambda_1 \in 5\mathbb{Z}$*. Así,* $\alpha_1 = \frac{1}{5}(\lambda_2\theta + \lambda_3\theta^2)$ *tiene que ser también un número entero algebraico.*

Vamos a calcular ahora la norma de α_1*:*

$$N(a\theta + b\theta^2) = 5a^3 + 25b^3 \Rightarrow N(\alpha') = \frac{\lambda_2^3 + 5\lambda_3^3}{25}.$$

Ahora, para que α_1 *pueda ser un entero algebraico, tiene que ocurrir que* $\lambda_2^3 + 5\lambda_3^3$ *sea divisible por 25, es decir* $\lambda_2^3 + 5\lambda_3^3 \equiv 0 \pmod{25}$*.*

Supongamos que esta congruencia es cierta. Si $\lambda_3 \equiv 0 \pmod 5$*, entonces* λ_2 *también debe serlo, lo que implicaría que* $\lambda_2 = \lambda_3 = 0$*. En este caso* $\alpha' = 0$ *y sería irrelevante. Si* $\lambda_3 \not\equiv 0 \pmod 5$*, entonces* $5 \equiv (\frac{-\lambda_2}{\lambda_3})^3 \pmod{25}$*. Esto implicaría que* 5 *es residuo cúbico módulo 25, pero esto no puede ocurrir puesto que* $5 \equiv 0 \pmod{25}$*. Por lo tanto, no hay números algebraicos de esta forma.*

2.7. Cuerpos cuadráticos.

En esta sección vamos a ver cómo son los anillos de enteros de un cuerpo cuadrático, así como también veremos la forma de sus bases y sus normas y trazas.

Un *cuerpo cuadrático* es un cuerpo de números de grado 2 sobre $\mathbb{Q}$. Es decir, $K = \mathbb{Q}(\theta)$, con θ entero algebraico raíz de $t^2 + at + b \in \mathbb{Z}[t]$. Es decir,

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Sea $a^2 - 4b = r^2 d$, con $r, d \in \mathbb{Z}$ y d libre de cuadrados. Tenemos entonces que

$$\theta = \frac{-a \pm r\sqrt{d}}{2},$$

por lo tanto, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$. Como resultado de esto, tenemos la siguiente proposición:

Proposición 2.7.1. *Los cuerpos cuadráticos son de la forma* $\mathbb{Q}(\sqrt{d})$*, para un* d *entero libre de cuadrados. Si* $d \geq 0$*, diremos que el cuerpo cuadrático es real. En caso contrario lo llamaremos cuerpo cuadrático imaginario.*

El siguiente teorema nos va a decir quién es el anillo de enteros, cual es su base y qué discriminante tiene, dependiendo del número d.

Teorema 2.7.2. *Sea d un número entero libre de cuadrados. Sea $K = \mathbb{Q}(\sqrt{d})$. Tenemos entonces que se cumplen:*

a) Si $d \not\equiv 1 (\text{mód } 4)$, entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, tiene base entera de la forma $\{1, \sqrt{d}\}$ y discriminante $4d$.

b) Si $d \equiv 1 (\text{mód } 4)$, entonces $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$, tiene base entera de la forma $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ y discriminante d.

Demostración. Ya sabemos que los elementos $\alpha \in \mathbb{Q}(\sqrt{d})$ son de la forma $\alpha = r + s\sqrt{d}$, con $s, q \in \mathbb{Q}$. Equivalentemente, podemos escribir $\alpha = \frac{a+b\sqrt{d}}{c}$, con $a, b, c \in \mathbb{Z}$, $c > 0$ y no hay ningún primo que los divida a todos.

Notemos que α es entero algebraico si y solo si los coeficientes del polinomio mínimo de α son enteros. Ya sabemos que el polinomio mínimo de α es

$$p(t) = \left(t - \frac{a + b\sqrt{d}}{c}\right)\left(t - \frac{a - b\sqrt{d}}{c}\right) = t^2 + \frac{a^2 - b^2 d}{c^2}t + \frac{2a}{c}.$$

Es decir, $\frac{a^2-b^2d}{c^2}, \frac{2a}{c} \in \mathbb{Z}$.

Si a y c tienen un factor primo p en común, entonces $p \mid b^2$. Pero esto no puede pasar, pues hemos elegido a, b, c de forma que no haya un factor primo que divida a los tres a la vez. Por lo tanto, c tiene que valer 1 o 2. Analicemos estos dos casos:

- Si $c = 1$, entonces α es entero algebraico en $\mathbb{Q}$.
- Si $c = 2$, a y b son ambos impares y $\frac{a^2-b^2d}{4} \in \mathbb{Z}$. O lo que es lo mismo, $a^2 - b^2 d \equiv 0 (\text{mód } 4)$. Observemos que un número impar tiene cuadrado $(2k+1)^2 = 4k^2 + 2k + 1 \equiv 1 (\text{mód } 4)$, de donde deducimos

  $$a^2 \equiv 1 \equiv b^2 (\text{mód } 4) \Rightarrow d \equiv 1 (\text{mód } 4).$$

  Así, si $d \equiv 1 (\text{mód } 4)$ y a, b impares, entonces α es entero algebraico pues $\frac{a^2-b^2d}{c^2}, \frac{2a}{c} \in \mathbb{Z}$.

Hemos visto ya lo siguiente:

- Si $d \not\equiv 1 (\text{mód } 4)$, entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

- Si $d \equiv 1 \pmod 4$, entonces $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$.

De aquí se deduce que la base entera es:

- Si $d \not\equiv 1 \pmod 4$, entonces $\{1, \sqrt{d}\}$.
- Si $d \equiv 1 \pmod 4$, entonces $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$.

Por lo tanto, solo nos queda comprobar el valor de los discriminantes:

- Si $d \not\equiv 1 \pmod 4$, entonces $\{1, \sqrt{d}\}$. Por lo tanto, el discriminante es

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = (-2\sqrt{d})^2 = 4d.$$

- Si $d \equiv 1 \pmod 4$, entonces $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$. Luego el discriminante es

$$\begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix} = (-\sqrt{d})^2 = d.$$

Con esto ya hemos demostrado todo lo que nos decía el teorema. □

Sean $\mathbb{Q}(\sqrt{d_1})$ y $\mathbb{Q}(\sqrt{d_2})$ dos cuerpos de números cuadráticos. Observemos que si $d_1 \neq d_2$, entonces $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$. Por último, notemos que

$$\mathrm{N}_K(r + s\sqrt{d}) = r^2 - ds^2 \quad \text{y} \quad \mathrm{Tr}_K(r + s\sqrt{d}) = 2r.$$

2.8. Cuerpos ciclotómicos.

En esta sección, como en la anterior, vamos a analizar los cuerpos de números K generados por una raíz n-ésima de la raíz. Estudiaremos su anillo de enteros, su base entera y el discriminante asociado.

Definición 2.8.1. *Un* cuerpo ciclotómico *es aquel que se obtiene al extender por la raíz n-ésima de la unidad, es decir, $K = \mathbb{Q}(\xi_n)$, con $\xi_n = e^{\frac{2\pi i}{n}}$.*

Vamos a considerar $n = p$ primo impar.

Lema 2.8.2. *El polinomio mínimo de $\xi_p = e^{\frac{2\pi i}{p}}$ sobre $\mathbb{Q}$, con p primo impar, es*

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

Además, $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.

Demostración. Observamos que

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

Además, como $\xi_p \neq 1$ y $\xi_p^p = 1$, tenemos que $f(\xi_p) = 0$, es decir, $f(t)$ es el polinomio mínimo de ξ_p. Así, solo nos queda comprobar la irreducibilidad del polinomio. Para ello, vamos a utilizar el criterio de Eisenstein:

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

De aquí observamos que $\binom{p}{r}$ es divisible por p si $1 \leq r \leq p-1$ y $p^2 \nmid \binom{p}{1}$. Por el criterio de Eisenstein, $f(t+1)$ es irreducible. Por lo tanto, $f(t)$ también lo es.

Para comprobar que $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$ solo tenemos que observar que el grado del polinomio mínimo es $p - 1$. □

Notemos que las potencias $\{\xi_p^i\}_{i=0}^{i=p-1}$ también son raíces de la unidad. Por lo tanto, también tienen al polinomio $f(t)$ del lema anterior como polinomio mínimo. Así, también podemos reescribir $f(t)$ como

$$f(t) = (t - \xi_p)(t - \xi_p^2) \dots (t - \xi_p^{p-1}).$$

Además, hay $p - 1$ monomorfismos $\sigma_i : \mathbb{Q}(\xi_p) \to \mathbb{C}$ distintos, que vienen dados por $\sigma_i(\xi_p) = \xi_p^i$, con $i \in \{1, \dots, p-1\}$.

Observemos también que una base de $\mathbb{Q}(\xi_p)$ sobre $\mathbb{Q}$ es

$$\{1, \xi_p, \xi_p^2, \dots, \xi_p^{p-2}\}.$$

Es fácil darse cuenta de que

$$\mathrm{N}_K(\xi_p) = \mathrm{N}_K(\xi_p^i) = (-1)^{p-1} = 1 \quad \text{y} \quad \mathrm{Tr}_K(\xi_p) = -1.$$

Además,

$$\mathrm{Tr}_K(\xi_p^i) = \begin{cases} -1 \text{ si } i \not\equiv 0 (\text{mód } p). \\ p - 1 \text{ si } i \equiv 0 (\text{mód } p). \end{cases}$$

Dado $\alpha = a_0 + a_1\xi_p + a_2\xi_p^2 + \cdots + a_{p-2}\xi_p^{p-2}$, con pocos calculos podemos obtener

$$\mathrm{Tr}_K(\alpha) = pa_0 - \sum_{i=1}^{p-2} a_i.$$

Calcular la norma para un elemento general es más complicado. Sin embargo, un caso realmente sencillo y útil es $\mathrm{N}_K(1-\xi_p)=p$.

Vamos a enunciar y a demostrar los dos teoremas principales de este sección:

Teorema 2.8.3. *Sea p un número primo. El anillo de enteros algebraicos de $K=\mathbb{Q}(\xi_p)$ es $\mathcal{O}_K=\mathbb{Z}[\xi_p]$.*

Demostración. Supongamos que $\alpha=a_0+a_1\xi_p+a_2\xi_p^2+\cdots+a_{p-2}\xi_p^{p-2}$ es entero algebraico sobre $\mathbb{Q}$. Vamos a ver que todos los $\{a_i\}_{i=0}^{i=p-2}$ son enteros.

Para $0\leq k\leq p-2$, tenemos que $\alpha\xi_p^{-k}-\alpha\xi_p$ es entero algebraico. Esto implica que su traza es un número entero. Vamos a calcularla:

$$\mathrm{Tr}_K(\alpha\xi_p^{-k}-\alpha\xi_p)=$$

$$=\mathrm{Tr}_K(a_0\xi_p^{-k}+a_1\xi_p^{-k+1}+\cdots+a_k+\cdots+a_{p-2}\xi_p^{p-k-2}-a_0\xi_p-\cdots-a_{p-2}\xi_p^{p-2})$$

$$=pa_k-(a_0+\cdots+a_{p-2})-(-a_0-\cdots-a_{p-2})=pa_k.$$

Tenemos entonces que $b_k=pa_k\in\mathbb{Z}$. Tomamos $\lambda=1-\xi_p$. Entonces

$$p\alpha=b_0+b_1\xi_p+\cdots+b_{p-2}\xi_p^{p-2}$$

$$=c_0+c_1\lambda+\cdots+c_{p-2}\lambda^{p-2}.$$

Ahora, sustituyendo $\xi_p=1-\lambda$, obtenemos que

$$c_i=\sum_{j=1}^{p-2}(-1)^i\binom{j}{i}b_j.$$

De manera equivalente, como $\lambda=1-\xi_p$, tenemos

$$b_i=\sum_{j=1}^{p-2}(-1)^i\binom{j}{i}c_j.$$

Vamos a comprobar a continuación que p divide a todos los c_i, con $i\leq k-1$. Para ello, vamos a emplear inducción. Notemos que una vez que demostremos esto, habremos visto que los b_i son enteros, luego α tendrá coeficientes enteros y, por tanto, el anillo de enteros será el enunciado en el teorema.

Observemos que

$$c_0=b_0+\cdots+b_{p-2}=p(T(\alpha)-b_0),$$

de donde obtenemos que $p \mid c_0$.

Como $\prod_{i=1}^{p-1}(1-\xi_p^i) = p$, tenemos que

$$p = \prod_{i=1}^{p-1}(1-\xi_p^i) = (1-\xi_p)^{p-1}\prod_{i=1}^{p-1}(1+\xi_p+\cdots+\xi_p^{i-1}) = \lambda^{p-1}\kappa,$$

con $\kappa \in \mathbb{Z}[\xi_p] \subseteq \mathcal{O}_K$.

Recordemos que $c_i = \sum_{j=1}^{p-2}(-1)^i\binom{j}{i}b_j$. Vamos a considerarlo módulo el ideal $\langle\lambda^{k+1}\rangle \subseteq \mathcal{O}_K$.

Acabamos de ver que

$$p \equiv 0(\text{mód } \langle\lambda^{k+1}\rangle).$$

Así, tenemos que la parte izquierda de $c_i = \sum_{j=1}^{p-2}(-1)^i\binom{j}{i}b_j$ también es congruente con $0(\text{mód } \langle\lambda^{k+1}\rangle)$ y los términos hasta $c_{k-1}\lambda^{k-1}$, desaparecen; de igual manera, los términos mayores de $c_{k+1}\lambda^{k+1}$ también. Por lo tanto, nos queda

$$c_k\lambda^k \equiv 0(\text{mód } \langle\lambda^{k+1}\rangle) \Leftrightarrow c_k\lambda^k = \mu\lambda^{k+1},$$

para algún $\mu \in \mathcal{O}_K$. Lo que implica que $c_k = \mu\lambda$.

Tomando normas tenemos $N(c_k) = c_k^{p-1}$ y $N(c_k) = N(\mu)N(\lambda) = pN(\mu)$. Es decir,

$$c_k^{p-1} = pN(\mu).$$

Por lo tanto, $p \mid c_k^{p-1}$ y esto implica que $p \mid c_k$.

Utilizando ahora inducción, tenemos que $p \mid c_k$, para todo k. Luego $p \mid b_k$ y esto implica que $a_k \in \mathbb{Z}$, que era lo que queríamos comprobar.

Es decir, hemos visto que $\mathcal{O}_K = \mathbb{Z}[\xi_p]$. □

Teorema 2.8.4. *El discriminante de* $K = \mathbb{Q}(\xi_p)$ *es* $\triangle = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$.

Demostración. Por el teorema anterior sabemos que una base de $\mathbb{Q}[\xi_p]$ sobre $\mathbb{Q}$ es

$$\{1, \xi_p, \xi_p^2, \ldots, \xi_p^{p-2}\}.$$

La Proposición 2.5.3 nos dice cómo calcular el discriminante de una base de esta forma:

$$\triangle[1, \xi_p, \ldots, \xi_p^{p-2}] = (-1)^{\frac{(p-1)(p-2)}{2}} N_K(Df(\xi_p)).$$

Como p es un primo impar, el primer factor se reduce a $(-1)^{\frac{p-1}{2}}$.

Nos queda comprobar entonces que el segundo factor toma la forma p^{p-2}. Veámoslo:

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

Evaluando en ξ_p obtenemos

$$Df(\xi_p) = \frac{-p\xi_p^{p-1}}{1 - \xi_p}.$$

Calculemos ahora la norma de este resultado y comprobemos que es p^{p-2}:

$$N_K(Df(t)) = \frac{N_K(p)N_K(\xi_p)^{p-1}}{N(1-\xi_p)} = \frac{(-p)^{p-1}1^{p-1}}{p} = p^{p-2}.$$

Reuniendo toda la información que teníamos hemos obtenido

$$\triangle[1, \xi_p, \ldots, \xi_p^{p-2}] = (-1)^{\frac{(p-1)(p-2)}{2}} N_K(Df(\xi_p)) = (-1)^{\frac{p-1}{2}} p^{p-2},$$

que es lo que queríamos probar. □

2.9. El anillo de enteros de un cuerpo de números es un anillo de Dedekind.

Vamos a enunciar a continuación el teorema que nos va a asegurar que el anillo de enteros algebraicos de un cuerpo de números es un anillo de Dedekind.

Teorema 2.9.1. *Sea K un cuerpo de números de grado n y $\mathcal{O}_K$ su anillo de enteros algebraicos. $\mathcal{O}_K$ tiene las siguientes propiedades:*

a) es un dominio, con cuerpo de fracciones K.

b) es Noetheriano.

c) Si $\alpha \in K$ satisface un polinomio mónico con coeficientes en $\mathcal{O}_K$, entonces $\alpha \in \mathcal{O}_K$.

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

Demostración.

a) Esta propiedad es trivial por la definición de anillo de enteros.

b) Por el Teorema 2.4.3 sabemos que $(\mathcal{O}_K, +)$ es un grupo abeliano libre de rango n. Si tomamos $\mathfrak{a}$ un ideal de $\mathcal{O}_K$, por el Teorema 1.6.4 tenemos que $(\mathfrak{a}, +)$ es un grupo abeliano de rango menor o igual que n. Por lo tanto, toda $\mathbb{Z}$-base de $\mathfrak{a}$ genera a $\mathfrak{a}$ como ideal. Es decir, todo ideal de $\mathcal{O}_K$ es finitamente generado. Por lo tanto, $\mathcal{O}_K$ es noetheriano.

c) Esta afirmación es consecuencia inmediata del Teorema 2.3.4.

d) Solo nos queda comprobar que todo ideal primo no nulo de $\mathcal{O}_K$ es maximal.

Tomamos $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. Sea $\alpha \in \mathfrak{p}$, con $\alpha \neq 0$. Entonces

$$N = \mathrm{N}_K(\alpha) = \alpha_1 \dots \alpha_n \in \mathfrak{p},$$

siendo α_i los conjugados de α y $\alpha_1 = \alpha$. Así, $\langle N \rangle \subseteq \mathfrak{p}$ y, por lo tanto, $\mathcal{O}_K/\mathfrak{p}$ es un anillo cociente de $\mathcal{O}_K/N\mathcal{O}_K$. Éste último cociente es finito pues es un grupo abeliano finitamente generado con todos sus elementos de orden finito. Tenemos entonces que $\mathcal{O}_K/\mathfrak{p}$ es un dominio (por el Lema 1.1.5) y además es finito. Utilizando ahora el Teorema 1.1.4 tenemos que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo y, nuevamente utilizando el Lema 1.1.5, tenemos que $\mathfrak{p}$ es maximal.

□

Capítulo 3

Grupos de descomposición, inercia y ramificación superior.

Figura 3.1: Évariste Galois (1811–1832) fue un matemático francés cuyo trabajo dio lugar a las bases fundamentales para la teoría que lleva su nombre, una rama principal del álgebra abstracta.

En este capítulo vamos a tratar los grupos de inercia, descomposición y de ramificación superior. Todos los resultados van a estar demostrados para anillos de enteros puesto que es lo que vamos a necesitar para demostrar el Teorema de Kronecker-Weber. Sin embargo, se pueden generalizar a dominios de Dedekind, como ya dijimos en la introducción.

3.1. Extensiones de Galois.

En esta sección vamos a recordar brevemente conceptos y resultados sobre extensiones de Galois.

Definición 3.1.1. *Una extensión K/L de cuerpos de números es de* Galois *si*

$$|Aut(K/L)| = [K : L],$$

donde $Aut(K/L)$ es el grupo de automorfismos de K que fijan L. Escribimos

$$Gal(K/L) = Aut(K/L).$$

Condiciones necesarias y suficientes para que una extensión K/L sea de Galois es que sea normal, finita y separable.

Ejemplo 3.1.2.

- *Si $K \subset \mathbb{C}$ es un cuerpo de números dentro de $\mathbb{C}$, entonces $K/\mathbb{Q}$ es de Galois si todo homomorfismo de cuerpos $\sigma : K \to \mathbb{C}$ tiene imagen K.*

- *Cualquier extensión cuadrática K/L es Galois sobre L, puesto que es de la forma $K = L(\sqrt{a})$, para cierto a, y el homomorfismo de cuerpos no trivial es $\sqrt{a} \to -\sqrt{a}$.*

- *Si $f \in L[x]$ es un polinomio irreducible de grado tres del que θ es raíz, entonces $L(\theta)$ es de Galois sobre L si y solo si el discriminante de f es un cuadrado perfecto en L.*

Sin embargo, a pesar de los dos últimos ejemplos, para un número arbitrario mayor que dos, la extensión no suele ser de Galois.

Definición 3.1.3. *Si $K = \mathbb{Q}(\theta)$ es un cuerpo de números, entonces la* clausura de Galois K^{Gal} *de K es el cuerpo generado por todos los conjugados de θ.*

Notemos que la clausura de Galois de un cuerpo de números K es siempre de Galois sobre $\mathbb{Q}$. Esto ocurre puesto que la imagen por una incrustación de cualquier polinomio en conjugados de θ vuelve a ser un polinomio en conjugados de θ.

La pregunta natural que surge cuando se ve este resultado es: *¿cuánto más grande es el grado de K^{Gal} comparado con el grado de $K = \mathbb{Q}(\theta)$?* Vamos a analizar un poco la respuesta a esta pregunta. Observemos que hay un embebimiento de $\mathrm{Gal}(K^{\mathrm{Gal}}/\mathbb{Q})$ al grupo de permutaciones de θ. Si θ tiene n conjugados, entonces tendremos $\mathrm{Gal}(K^{\mathrm{Gal}}/\mathbb{Q}) \hookrightarrow S_n$. Por lo tanto, $[K^{\mathrm{Gal}} : \mathbb{Q}] \mid n!$. Además, $\mathrm{Gal}(K^{\mathrm{Gal}}/\mathbb{Q})$ es un subgrupo transitivo de S_n, por lo que las posibilidades sobre qué subgrupo son más limitadas. Vamos a analizar casos:

- Si $n = 2$: ya hemos dicho anteriormente que la extensión es de Galois.

- Si $n = 3$: sabemos que la extensión es de Galois si y solo si el discriminante del polinomio mínimo de θ es un cuadrado perfecto, luego la clausura de Galois de un cuerpo cúbico se obtiene adjuntando la raíz cuadrada del determinante de dicho polinomio.

- Si $n = 5$: es frecuente que la clausura de Galois tenga grado 120. Sin embargo, puede tener también grado 5, 10, 20 y 60, que es el orden de los únicos subgrupos transitivos y propios de S_5.

- Si n es un entero positivo arbitrario: consideramos $K = \mathbb{Q}(\xi_n)$, donde $\xi_n = e^{\frac{2\pi i}{n}}$ es una raíz primitiva n-ésima de la unidad. Si $\sigma : K \hookrightarrow \mathbb{C}$ es una incrustación, entonces $\sigma(\xi_n) = \xi_n^m$ para cierto m invertible módulo n. Entonces $K/\mathbb{Q}$ es de Galois y $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ y esto es un isomorfismo puesto que $[K : \mathbb{Q}] = \varphi(n)$.

Una vez analizado el grado de la clausura de Galois de un cuerpo de números, vamos a pasar a ver un pequeño ejemplo que muestra que la composición de extensiones de Galois da como resultado una extensión de Galois.

Ejemplo 3.1.4. *El cuerpo de números $K = \mathbb{Q}(\sqrt{2}, i)$ es una extensión de Galois de grado 4 y es composición de las extensiones de Galois $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{2})$.*

Para terminar esta sección vamos a ver que el grupo de Galois de un cuerpo de números actúa en varios objetos asociados a este cuerpo K. Dado un cuerpo de números K que es de Galois sobre un cuerpo L, tenemos que $G = Gal(K/L)$ actúa sobre $\mathcal{O}_K$ y el conjunto $S_{\mathfrak{p}} = \{\text{divisores primos de } \mathfrak{p}\mathcal{O}_K\}$.

3.2. Descomposición de primos.

En esta sección vamos a ver cómo podemos descomponer ideales primos y propiedades asociadas a estas descomposiciones.

Sea $K/\mathbb{Q}$ una extensión de Galois, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ e $I \subset \mathcal{O}_K$ un ideal del anillo de enteros. Tenemos entonces que $\sigma(I) = \{\sigma(x) \mid x \in I\}$ también es un ideal de $\mathcal{O}_K$.

Definición 3.2.1. *Sea $K/\mathbb{Q}$ una extensión de Galois y p primo de forma que*

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_g^{e_g},$$

donde $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_g$ son ideales primos distintos de $\mathcal{O}_K$. Llamamos índice de ramificación de $\mathfrak{P}_i$ sobre p *al entero e_i. El índice de ramificación suele denotarse por $e_{\mathfrak{P}/p}$. Si $e_i > 1$, entonces decimos que $\mathfrak{P}_i$ ramifica sobre p.*

Definición 3.2.2. *Sea $K/\mathbb{Q}$ una extensión de Galois y $\mathfrak{P}$ un ideal de $\mathcal{O}_K$ que ramifica sobre $p \in \mathbb{Z}$ primo. Definimos el* grado residual de $\mathfrak{P}$ en la extensión $K/\mathbb{Q}$ *como*

$$f_{\mathfrak{P}/p} = [\mathcal{O}_K/\mathfrak{P} : \mathbb{Z}/p].$$

Además, al cuerpo $\mathcal{O}_K/\mathfrak{P}$ lo llamamos cuerpo residual de $\mathcal{O}_K$ en $\mathfrak{P}$.

De ambas definiciones se deduce inmediatamente que si $M/K/\mathbb{Q}$ es una torre de extensiones de cuerpos y $\mathfrak{q}$ es un primo de M que ramifica sobre el ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$ que, a su vez, ramifica sobre el primo $p \in \mathbb{Z}$, tenemos que

$$f_{\mathfrak{q}/p} = [\mathcal{O}_M/\mathfrak{q} : \mathbb{Z}/p] = [\mathcal{O}_M/\mathfrak{q} : \mathcal{O}_K/\mathfrak{P}] \cdot [\mathcal{O}_K/\mathfrak{P} : \mathbb{Z}/p] = f_{\mathfrak{q}/\mathfrak{P}} \cdot f_{\mathfrak{P}/p}.$$

De manera equivalente obtenemos

$$e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}/\mathfrak{P}} \cdot e_{\mathfrak{P}/\mathfrak{p}}.$$

Definimos S_p como el conjunto de ideales primos de $\mathcal{O}_K$ que dividen a $p\mathcal{O}_K$, es decir, el conjunto de ideales primos que contienen a $p\mathcal{O}_K$. Explícitamente, dado $p \in \mathbb{Z}$ primo y $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ que divide a p, tenemos que

$$S_{\mathfrak{p}} = \{\mathfrak{P} \subset \mathcal{O}_K \text{ primo} \quad : \ \mathfrak{P}|\mathfrak{p}\mathcal{O}_K\}.$$

Notemos que si $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ y $\mathfrak{P} \in S_p$, entonces σ induce un isomorfismo de cuerpos finitos $\mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\sigma(\mathfrak{P})$ que fija al subcuerpo $\mathbb{Q}/\mathfrak{p}$, que está contenido tanto en $\mathcal{O}_K/\mathfrak{P}$ como en $\mathcal{O}_K/\sigma(\mathfrak{P})$. Por lo tanto, el grado residual de $\mathfrak{P}$ y $\sigma(\mathfrak{P})$ es el mismo. De hecho, se verifica el siguiente teorema:

Teorema 3.2.3. *Sea $K/\mathbb{Q}$ una extensión de Galois y sea $p \in \mathbb{Z}$ primo. Escribimos $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, con $\mathfrak{P}_i$ ideales primos de $\mathcal{O}_K$, y denotamos por $f_i = f_{\mathfrak{P}_i/p}$. Entonces $G = Gal(K/\mathbb{Q})$ actúa de manera transitiva sobre S_p y*

$$e_1 = \cdots = e_g, \ f_1 = \cdots = f_g.$$

Además, si denotamos por e al valor común de los e_i, por f al valor común de los f_i y $[K : \mathbb{Q}] = n$, tenemos

$$efg = n.$$

Demostración. Sea $p \in \mathbb{Z}$, $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ y $S_p = \{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$.

Comprobaremos primero que G actúa en S_p y después comprobaremos que actúa de manera transitiva.

Si $\sigma \in G$ es un $\mathbb{Q}$-automorfismo de K, entonces la imagen por σ de $b \in \mathcal{O}_K$ vuelve a ser un elemento de $\mathcal{O}_K$ puesto que $\sigma(b)$ es un conjugado de b sobre $\mathbb{Q}$ y, por tanto, es raíz del mismo polinomio mónico irreducible con coeficientes en $\mathbb{Z}$. Por lo tanto, σ es un $\mathbb{Z}$-automorfismo de $\mathcal{O}_K$. Ahora bien, la imagen por un isomorfismo de un ideal primo es, de nuevo, un ideal primo. Por lo tanto, G opera en el conjunto de los ideales primos de $\mathcal{O}_K$. Sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$. Si $\mathfrak{P} \cap \mathbb{Z} = \langle p \rangle$, entonces $\sigma(\mathfrak{P}) \cap \mathbb{Z} = \langle p \rangle$,

puesto que $\mathbb{Z}$ es fijo por σ. Por lo tanto, G opera en el conjunto de los ideales primos de $\mathcal{O}_K$ que dividen a $p\mathcal{O}_K$, es decir, G actúa en S_p.

Nos queda demostrar que la acción es transitiva. Sean $\mathfrak{P}_1 \dots \mathfrak{P}_s$, $s \leq g$, los ideales primos de $\mathcal{O}_K$ conjugados de $\mathfrak{P}_1 = \mathfrak{P}$. Supongamos que $s < g$ para, finalmente, llegar a una contradicción y obtener $s = g$.

Claramente, G permuta los ideales $\mathfrak{P}_1, \dots, \mathfrak{P}_s$, así como también permuta los ideales $\mathfrak{P}_{s+1}, \dots, \mathfrak{P}_g$. El producto $\mathfrak{P}_1 \dots \mathfrak{P}_s$ no está incluido en ningún $\mathfrak{P}_i$ si $i > s$. Por lo tanto, existe $b \in \mathfrak{P}_1 \dots \mathfrak{P}_s$ tal que $b \notin \mathfrak{P}_i$ para todo $s < i \leq g$. Entonces

$$\mathrm{N}_K(b) = \prod_{\sigma \in G} \sigma(b) \in \mathfrak{P}_1 \dots \mathfrak{P}_s$$

y

$$\mathrm{N}_K(b) = \prod_{\sigma \in G} \sigma(b) \in \mathbb{Z}.$$

Por lo tanto,

$$\mathrm{N}_K(b) = \prod_{\sigma \in G} \sigma(b) \in \mathfrak{P}_1 \dots \mathfrak{P}_s \cap \mathbb{Z} \subseteq \langle p \rangle.$$

Como consecuencia, $\mathrm{N}_K(b) \in \mathfrak{P}_i$, de forma que para algún $\sigma \in G$ se verifica que $\sigma(b) \in \mathfrak{P}_i$ puesto que $\mathfrak{P}_i$ es un ideal primo de $\mathcal{O}_K$ y $\sigma(b) \in \mathcal{O}_K$ para todo $\sigma \in G$. Pero entonces $b \in \sigma^{-1}(\mathfrak{P}_i)$, de forma que $\sigma^{-1}(\mathfrak{P}_i)$ es uno de los ideales $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ que son los únicos que pueden contener a b y esto es una contradicción con que $s < g$. Por lo tanto $s = g$ y G actúa transitivamente en S_p.

Vamos a comprobar ahora que

$$e_1 = \cdots = e_g, \ f_1 = \cdots = f_g.$$

Tomamos $\mathfrak{P}_j \in S_p$. Como G actúa de manera transitiva en S_p, existe $\sigma \in G$ tal que $\sigma(\mathfrak{P}_j) = \mathfrak{P}_k$, para cierto $k \neq j$. Aplicando σ a la factorización $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ tenemos que

$$\prod_{i=1}^{g} \mathfrak{P}_i^{e_i} = \prod_{i=1}^{g} \sigma(\mathfrak{P}_i)^{e_i}.$$

Tomando el orden de $\mathfrak{P}_j$ en ambos lados y usando el hecho de que la factorización es única, tenemos que $e_j = e_k$. Por lo tanto $e_1 = \cdots = e_g$.

Ya hemos mencionado anteriormente que para cualquier $\sigma \in G$,

$$\mathcal{O}_K/\mathfrak{P}_i \simeq \mathcal{O}_K/\sigma(\mathfrak{P}_i).$$

Usando transitividad tenemos que $f_1 = \cdots = f_g$.

Vamos a comprobar finalmente que $n = efg$. aplicando el Teorema Chino del Resto tenemos que $|\mathcal{O}_K/(\mathfrak{P}^m)| = |(\mathcal{O}_K/\mathfrak{P}^m)|$, así:

$$n = [K : \mathbb{Q}] = \dim_{\mathbb{Z}} \mathcal{O}_K = \dim_{\mathbb{F}_p} \mathcal{O}_K/p\mathcal{O}_K =$$
$$= \dim_{\mathbb{F}_p}(\bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}) = \sum_{i=1}^{g} e_i f_i = efg.$$

□

Definición 3.2.4. *Sea $K/\mathbb{Q}$ una extensión finita (no es necesario que sea de Galois). Sea $\mathcal{O}_K/\mathbb{Z}$ la extensión de sus anillos de enteros, $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ y $\langle p\rangle = \mathfrak{P} \cap \mathbb{Z}$.*

Decimos que la extensión $\mathcal{O}_K/\mathbb{Z}$ es ramificada en $\mathfrak{P}$ *cuando* $e(\mathfrak{P}/p) > 1$ *o* $(\mathcal{O}_K/\mathfrak{P})/\mathbb{F}_p$ *es no separable; se dice que* la extensión $\mathcal{O}_K/\mathbb{Z}$ es ramificada en p *cuando hay algún ideal primo* $\mathfrak{P}$ *en* $\mathcal{O}_K$ *tal que* $\mathfrak{P}^2$ *divide a* $p\mathcal{O}_K$.

Decimos que la extensión $\mathcal{O}_K/\mathbb{Z}$ es no ramificada en $\mathfrak{P}$ *cuando* $e(\mathfrak{P}/p) = 1$ *o* $(\mathcal{O}_K/\mathfrak{P})/(\mathbb{Z}/p)$ *es separable; se dice que* la extensión $\mathcal{O}_K/\mathbb{Z}$ es no ramificada en p *cuando es no ramificada en todo ideal primo* $\mathfrak{P}$ *de* $\mathcal{O}_K$ *que divide a* $p\mathcal{O}_K$.

Para finalizar esta sección, vamos a ver qué ocurre en las extensiones cuadráticas. Supongamos que $K/\mathbb{Q}$ es una extensión de grado 2. Hemos visto que, entonces, $K/\mathbb{Q}$ es de Galois. Luego para cada primo $p \in \mathbb{Z}$ tenemos $2 = efg$. Tenemos entonces las siguientes posibilidades:

- Ramifica: $e = 2, f = g = 1$. Tenemos así que el primo p ramifica en $\mathcal{O}_K$, luego $p\mathcal{O}_K = \mathfrak{P}^2$. Notemos que solo hay un número finito de estos primos puesto que si $f(x)$ es el polinomio mínimo de un generador de $\mathcal{O}_K$, entonces p ramifica si y solo si $f(x)$ tiene una raíz múltiple módulo p. Sin embargo, $f(x)$ tiene una raíz múltiple módulo p si y solo si p divide al discriminante de dicho polinomio, que sabemos que no es cero puesto que el polinomio es irreducible sobre $\mathbb{Z}$. Este argumento nos muestra que solo hay un número finito de primos que ramifican en un cuerpo de números. De hecho, los primos que ramifican van a ser los que dividen al discriminante.

- Inerte: $e = g = 1, f = 2$. El primo p es inerte en $\mathcal{O}_K$, luego $p\mathcal{O}_K = \mathfrak{P}$ es primo.

- Escinde: $e = f = 1, g = 2$. El primo p escinde en $\mathcal{O}_K$, es decir, $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$, con $\mathfrak{P}_1 \neq \mathfrak{P}_2$.

3.3. Discriminante y ramificación: Teorema de Hermite -Minkowski.

En esta sección vamos a ver que podemos estudiar los ideales primos que ramifican gracias al discriminante de la extensión.

Lo que resta de sección vamos a asumir que $K/\mathbb{Q}$ es un cuerpo de números de grado n.

Figura 3.2: Hermann Minkowski (1864–1909) fue un matemático ruso que desarrolló la Teoría Geométrica de los Números. Sus trabajos más destacados fueron realizados en las áreas de la Teoría de Números, física matemática y Teoría de la Relatividad.

Definición 3.3.1. *Llamamos* discriminante de la extensión $\mathcal{O}_K/\mathbb{Z}$*, y lo denotamos por* $\triangle(\mathcal{O}_K/\mathbb{Z})$*, al ideal de* $\mathcal{O}_K$ *generado por todas las posibles* $\mathbb{Z}$*-bases de* K*.*

De manera equivalente, llamamos discriminante de la extensión $S^{-1}\mathcal{O}_K/S^-$ *y lo denotamos por* $\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z})$*, al ideal de* $S^{-1}\mathcal{O}_K$ *generado por todas las posibles* $S^{-1}\mathbb{Z}$*-bases de* K*.*

Lema 3.3.2. *Sea* $\{\alpha_1, \ldots, \alpha_n\}$ *una* $\mathbb{Q}$*-base de* K*, con los* $\alpha_i \in \mathcal{O}_K$*. El ideal*

$$\triangle[\alpha_1, \ldots, \alpha_n]\mathcal{O}_K \subseteq \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z},$$

es decir, $\triangle[\alpha_1, \ldots, \alpha_n]\mathcal{O}_K$ *es un* $\mathbb{Z}$*-módulo libre.*

Demostración. Tomamos $\alpha \in \mathcal{O}_K$. Podemos escribir

$$\alpha = \sum_{i=1}^{n} a_i\alpha_i,$$

con $a_i \in K$. Multiplicando por α_j tenemos

$$\alpha_j\alpha = \sum_{i=1}^{n} a_i\alpha_i\alpha_j \Rightarrow \mathrm{Tr}(\alpha\alpha_j) = \sum_{i=1}^{n} a_i\mathrm{Tr}(\alpha_i\alpha_j).$$

Como $\alpha\alpha_j, \alpha_i\alpha_j \in \mathcal{O}_K$, sus trazas pertenecen a $\mathbb{Z}$ y, por la regla de Cramer podemos asegurar que los coeficientes a_i se obtienen como cociente de un determinante formado por elementos de A por el determinante de la matriz $(\mathrm{Tr}(\alpha_i\alpha_j)$. Por lo tanto, $a_i \in \frac{1}{\triangle[\alpha_1,\ldots,\alpha_n]}\mathbb{Z} \subseteq \mathbb{Q}$ y ya lo tenemos. □

Proposición 3.3.3. *Si* $\{\alpha_1, \ldots, \alpha_n\}$ *es una* $\mathbb{Z}$*-base de* $\mathcal{O}_K$*, entonces*

$$\triangle(\mathcal{O}_K/\mathbb{Z}) = \langle\triangle[\alpha_1, \ldots, \alpha_n]\rangle.$$

Demostración. Sea $\{\beta_1, \ldots, \beta_n\}$ otra $\mathbb{Q}$-base de K formada por elementos de $\mathcal{O}_K$. Como $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Z}$-base de $\mathcal{O}_K$, existe una matriz $(a_{ij}) \in M_n(\mathbb{Z})$, no necesariamente invertible en $\mathbb{Z}$, de forma que

$$\triangle[\beta_1, \ldots, \beta_n] = \det(a_{ij})^2 \triangle [\alpha_1, \ldots, \alpha_n].$$

Por lo tanto,

$$\triangle(\mathcal{O}_K/\mathbb{Z}) = \langle \triangle[\alpha_1, \ldots, \alpha_n] \rangle.$$

□

Proposición 3.3.4. *Sea S un conjunto multiplicativo de $\mathbb{Z}$. Entonces*

$$\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}) = S^{-1} \triangle (\mathcal{O}_K/\mathbb{Z}).$$

Demostración. Vamos a demostrar esta proposición usando doble contenido.

- $\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}) \subseteq S^{-1} \triangle (\mathcal{O}_K/\mathbb{Z})$: Toda $\mathbb{Q}$-base de K formada por elementos de $\mathcal{O}_K$ es $\mathbb{Q}$-base de K formada por elementos de $S^{-1}\mathcal{O}_K$. Por lo tanto,

  $$\triangle(\mathcal{O}_K/\mathbb{Z}) \subseteq \triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}) \Rightarrow S^{-1}\triangle(\mathcal{O}_K/\mathbb{Z}) \subseteq \triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}).$$

- $\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}) \supseteq S^{-1} \triangle (\mathcal{O}_K/\mathbb{Z})$: Sea $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base de K formada por elementos de $S^{-1}\mathcal{O}_K$. Entonces existe $\beta \in S$ de forma que $\beta\alpha_i \in \mathcal{O}_K$, para todo i. Esto implica que

  $$\triangle[\beta\alpha_1, \ldots, \beta\alpha_n] \in \triangle(\mathcal{O}_K/\mathbb{Z}).$$

  Además, se verifica la igualdad $\triangle[\beta\alpha_1, \ldots, \beta\alpha_n] = s^{2n} \triangle [\alpha_1, \ldots, \alpha_n]$. Por lo tanto $\triangle[\alpha_1, \ldots, \alpha_n] \in S^{-1} \triangle (\mathcal{O}_K \mid \mathbb{Z})$ y esto implica

  $$\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}) \supseteq S^{-1} \triangle (\mathcal{O}_K/\mathbb{Z}).$$

□

Vamos a pasar ya a demostrar el Teorema de Hermite-Minkowski:

Teorema 3.3.5 (Hermite-Minkowski)**.** *Sea $K/\mathbb{Q}$ un cuerpo de números y $\mathfrak{P} \subset \mathbb{Z}$ un ideal primo. Condición necesaria y suficiente para que $\mathfrak{P}$ ramifique en la extensión $\mathcal{O}_K/\mathbb{Z}$ es que $\mathfrak{P}$ divida al discriminante $\triangle(\mathcal{O}_K/\mathbb{Z})$.*

Demostración. Lo que queremos comprobar es que el conjunto de ideales primos de $\mathbb{Z}$ que ramifican en $\mathcal{O}_K$ está formado por los ideales que dividen al discriminante.

Para demostrar esto vamos a comenzar estudiando el comportamiento local del discriminante y la ramificación.

Sea $\mathfrak{p}$ un ideal primo de $\mathbb{Z}$ y definimos el conjunto multiplicativo $S := \mathbb{Z} - \mathfrak{p}$. Tenemos que $S^{-1}\mathfrak{p}$ es un ideal primo de $S^{-1}\mathbb{Z}$. Lo que queremos ver es que $\triangle(\mathcal{O}_K/\mathbb{Z}) \subseteq \mathfrak{p}$ (o, equivalentemente, $\mathfrak{p}$ divide a $\triangle(\mathcal{O}_K/\mathbb{Z})$). Localizando en S tenemos $S^{-1}\triangle(\mathcal{O}_K/\mathbb{Z}) \subseteq S^{-1}\mathfrak{p}$ y, utilizando la Proposición 3.3.4, esto es equivalente a $\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z}) \subseteq S^{-1}\mathfrak{p}$.

Por otra parte, $S^{-1}\mathbb{Z}$ es un anillo local (por el Lema 1.8.5) y $S^{-1}\mathcal{O}_K$ es su clausura entera en K. Además, si $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1}\dots\mathfrak{P}_g^{e_g}$ es la descomposición de $\mathfrak{p}\mathcal{O}_K$ en $\mathcal{O}_K$, la descomposición de $\mathfrak{p}S^{-1}\mathcal{O}_K$ en $S^{-1}\mathcal{O}_K$ será $(S^{-1}\mathfrak{P}_1)^{e_1}\dots(S^{-1}\mathfrak{P}_g)^{e_g}$. Así,

$$\mathfrak{p} \text{ ramifica en } \mathcal{O}_K \Leftrightarrow S^{-1}\mathfrak{p} \text{ ramifica en } S^{-1}\mathcal{O}_K.$$

Pero, como $S^{-1}\mathbb{Z}$ y $S^{-1}\mathcal{O}_K$ son anillos de Dedekind, por la Proposición 1.7.4 son dominios de ideales principales. Por lo tanto, el ideal $\triangle(S^{-1}\mathcal{O}_K/S^{-1}\mathbb{Z})$ es principal y está generado por el discriminante de una $S^{-1}\mathbb{Z}$-base de $S^{-1}\mathcal{O}_K$.

Como localizar no modifica las propiedades de los anillos, tenemos que $\mathbb{Z}$ es un dominio de ideales principales y un anillo local, y podemos suponer que $\mathfrak{p}$ es el único ideal primo no nulo.

Además, si $\{\alpha_1,\dots,\alpha_n\}$ es una $\mathbb{Z}$-base de $\mathcal{O}_K$, también es una $\mathbb{Q}$-base de K y $\{\alpha_1+\mathfrak{p}\mathcal{O}_K,\dots,\alpha_n+\mathfrak{p}\mathcal{O}_K\}$ es una $\mathbb{Z}/\mathfrak{p}$-base de $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

Tomamos ahora un elemento $\beta \in \mathcal{O}_K$. Multiplicar por dicho elemento induce una aplicación $\mathbb{Z}$-lineal $m_\beta : \mathcal{O}_K \to \mathcal{O}_K$ que, en la $\mathbb{Z}$-base $\{\alpha_1,\dots,\alpha_n\}$ admite una matriz $(a_{ij}) \in M_n(\mathbb{Z})$. Ahora bien, podemos reducir esta aplicación módulo $\mathfrak{p}$, obteniendo así una aplicación $\mathbb{Z}/\mathfrak{p}$-lineal $\overline{m_\beta} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, multiplicando por $\beta+\mathfrak{p}$. Esta aplicación admite una matriz $(a_{ij}+\mathfrak{p}) \in M_n(\mathbb{Z}/\mathfrak{p})$. En particular se satisface la siguiente igualdad

$$\mathrm{Tr}_K(m_\beta) + \mathfrak{p} = \mathrm{Tr}_K(\overline{m_\beta}).$$

Así, la reducción módulo $\mathfrak{p}$ del discriminante $\triangle[\alpha_1,\dots,\alpha_n]$ es el discriminante

$$\overline{\triangle[\alpha_1,\dots,\alpha_n]} := \det(\mathrm{Tr}_K((\alpha_i+\mathfrak{p}\mathcal{O}_K)(\alpha_j+\mathfrak{p}\mathcal{O}_K))).$$

Ahora bien, como $\triangle(\mathcal{O}_K/\mathbb{Z})$ es el ideal generado por $\triangle[\alpha_1,\dots,\alpha_n]$, decir que $\triangle(\mathcal{O}_K/\mathbb{Z}) \subseteq \mathfrak{p}$ es equivalente a decir que $\triangle[\alpha_1,\dots,\alpha_n] \in \mathfrak{p}$ y esto

equivale a decir que $\overline{\triangle[\alpha_1,\ldots,\alpha_n]}=0$ en $\mathbb{Z}/\mathfrak{p}$. Vamos a comprobar que esto se verifica y así habremos terminado.

Habíamos dicho anteriormente que la descomposición de $\mathfrak{p}\mathcal{O}_K$ en $\mathcal{O}_K$ es $\mathfrak{p}\mathcal{O}_K=\mathfrak{P}_1^{e_1}\ldots\mathfrak{P}_g^{e_g}$. Por el Teorema Chino del Resto

$$\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K=\bigoplus_{i=1}^{g}\mathcal{O}_K/\mathfrak{P}_i^{g_i},$$

siendo $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$ subespacios vectoriales sobre $\mathbb{Z}/\mathfrak{p}$. Podemos considerar así una $\mathbb{Z}/\mathfrak{p}$-base de $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ construida reuniendo bases de los sumandos $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$. Si $\gamma\in\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ es un elemento cualquiera y $\alpha=\gamma_1+\cdots+\gamma_g$ es su descomposición en sumandos $\gamma_i\in\mathcal{O}_K/\mathfrak{P}_i^{g_i}$, la matriz de la multiplicación por α en $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ en esta nueva base se expresa como una matriz con cajas en la diagonal, cada una correspondiente a la multiplicación por γ_i en la base que hemos tomado en $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$. Esto nos permite asegurar que la traza de la aplicación multiplicación por α en $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ es la suma de las trazas de las aplicaciones multiplicación por γ_i en $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$. Como consecuencia, la matriz de las trazas de los productos toma la forma de una matriz de cajas en la diagonal en donde cada una es la matriz de las trazas de la base de $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$, ya que los productos de elementos de diferentes factores de $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$ se anulan. Sabemos además que los determinantes de las matrices de una forma bilineal simétrica en dos bases diferentes son iguales, salvo la multiplicación por el cuadrado del determinante de la matriz de cambio de base P y, además, este determinante siempre es invertible. Obtenemos así

$$\overline{\triangle[\alpha_1,\ldots,\alpha_n]}=\det P^2\prod_{i=1}^{g}\overline{D_i},$$

donde $\overline{D_i}$ es el determinante de la matriz de las trazas de los productos de los elementos de la base que hemos elegido en $\mathcal{O}_K/\mathfrak{P}_i^{g_i}$.

Vamos a comprobar, para terminar, que:

1. $\mathfrak{p}$ ramifica en $\mathcal{O}_K$ implica $\overline{\triangle[\alpha_1,\ldots,\alpha_n]}=0$ en $\mathbb{Z}/\mathfrak{p}$.

2. $\mathfrak{p}$ no ramifica en $\mathcal{O}_K$ implica $\overline{\triangle[\alpha_1,\ldots,\alpha_n]}\neq 0$ en $\mathbb{Z}/\mathfrak{p}$.

Vamos a ver primero 2. Que $\mathfrak{p}$ no ramifique en $\mathcal{O}_K$ quiere decir que las extensiones $\mathcal{O}_K/\mathfrak{P}_i^{e_i}$, para $1\leq i\leq g$, tienen que ser separables y $e_i=1$. Como las extensiones son separables, los determinantes $\overline{D_i}\neq 0$, luego $\overline{\triangle[\alpha_1,\ldots,\alpha_n]}\neq 0$ en $\mathbb{Z}/\mathfrak{p}$.

Para finalizar, vamos a comprobar que se verifica 1. Supongamos que $e_1>1$. Podemos elegir la $\mathbb{Z}/\mathfrak{p}$-base de $\mathcal{O}_K/\mathfrak{P}_1^{e_1}$ completando bases en

$\mathfrak{P}_1^a/\mathfrak{P}_1^{e_1}$, con $0 \leq a \leq e_1 - 1$. Observemos que el primer vector de esta base, v_1, es nilpotente ($v_1^{e_1} = 0$). Esto implica que la aplicación multiplicación por v_1 es un endomorfismo nilpotente de $\mathcal{O}_K/\mathfrak{P}_1^{e_1}$. Además, la multiplicación de este elemento por otro también es nilpotente, al igual que la multiplicación de estos productos por los endomorfismos de $\mathcal{O}_K/\mathfrak{P}_1^{e_1}$. Por lo tanto, las trazas de los productos son nulos y la matriz necesaria para calcular $\overline{D_1}$ tiene una columna de ceros, luego $\overline{D_1} = 0$ y $\overline{\triangle[\alpha_1, \ldots, \alpha_n]} = 0$ en $\mathbb{Z}/\mathfrak{p}$.

□

3.4. Grupos de descomposición e inercia.

Sea K un cuerpo de números de manera que $K/\mathbb{Q}$ es de Galois. Denotamos por $G = \mathrm{Gal}(K/\mathbb{Q})$. Fijamos $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ divisor de $p \in \mathbb{Z}$ primo.

Definición 3.4.1. *El* grupo de descomposición de $\mathfrak{P}$ *es el subgrupo*

$$D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Definimos el grupo de inercia $I_{\mathfrak{P}}$ *como el núcleo del morfismo*

$$\varphi_{\mathfrak{P}} : D_{\mathfrak{P}} \to Gal((\mathcal{O}_K/\mathfrak{P})/(\mathbb{Z}/\langle p\rangle)).$$

Notemos que $\mathbb{Z}/\langle p\rangle = \mathbb{F}_p$ y vamos a denotar por $k_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$. A lo largo de esta sección nos vamos a encargar de probar que existe una secuencia exacta

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p) \to 1.$$

Observemos que $D_{\mathfrak{P}}$ es el estabilizador de $\mathfrak{P}$ bajo la acción de G en el conjunto de divisores primos p. Recordemos que el Teorema 3.2.3 nos decía que G actúa de manera transitiva en el conjunto de primos $\mathfrak{P}$ que dividen a p. El Teorema órbita-estabilizador[1] nos dice que

$$[G : D_{\mathfrak{P}}] = |\mathrm{Órb}(\mathfrak{P})|.$$

Por el Teorema 3.2.3 sabemos que este cardinal es el número de ideales primos que dividen a p, luego $[G : D_{\mathfrak{P}}] = g$. También sabemos que $|I_{\mathfrak{P}}| = e$, donde e es el exponente de $\mathfrak{P}$ en la factorización de $p\mathcal{O}_K$.

[1] El Teorema órbita-estabilizador nos dice que dado un grupo G que actúa en un conjunto finito X, dado $x \in X$, $\mathrm{Órb}(x)$ la órbita del elemento x, $\mathrm{Stab}(x)$ el estabilizador de x por G y $[G : \mathrm{Stab}(x)]$ el índice del estabilizador de x en G, entonces

$$|\mathrm{Órb}(x)| = [G : \mathrm{Stab}(x)].$$

Lema 3.4.2. *Los grupos de descomposición $D_{\mathfrak{P}}$ correspondiente a los primos $\mathfrak{P}$ divisores de p son conjugados como subgrupos de G.*

Demostración. Sean σ, τ cualesquiera elementos de G. Tenemos que

$$\tau^{-1}\sigma\tau\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma\tau\mathfrak{P} = \tau\mathfrak{P},$$

luego

$$\sigma \in D_{\tau\mathfrak{P}} \Leftrightarrow \tau^{-1}\sigma\tau \in D_{\mathfrak{P}}.$$

Así,

$$\sigma \in D_{\mathfrak{P}} \Leftrightarrow \tau\sigma\tau^{-1} \in D_{\tau\mathfrak{P}}.$$

Esto implica

$$\tau D_{\mathfrak{P}}\tau^{-1} = D_{\tau\mathfrak{P}},$$

que es lo que queríamos probar. □

Vamos a estudiar a continuación el cuerpo fijado por $D = D_{\mathfrak{P}}$.

Proposición 3.4.3. *El cuerpo fijado por D*

$$K^D = \{a \in K \mid \sigma(a) = a, \forall \sigma \in D\}$$

es el menor subcuerpo $L \subseteq K$ tal que el ideal primo $\mathfrak{P} \cap \mathcal{O}_L$ tiene $g = 1$; es decir, hay un único primo de $\mathcal{O}_K$ sobre $\mathfrak{P} \cap \mathcal{O}_L$.

Demostración. Supongamos que $L = K^D$. Por Teoría de Galois sabemos que $\mathrm{Gal}(K/L) \simeq D$. Por el Teorema 3.2.3, D actúa de manera transitiva en los primos de K que dividen a $\mathfrak{P} \cap \mathcal{O}_L$. Uno de estos primos es $\mathfrak{P}$, y D fija a $\mathfrak{P}$ por definición de D. Por lo tanto hay un solo primo de K que divide a $\mathfrak{P} \cap \mathcal{O}_L$, es decir, $g = 1$.

Supongamos ahora $L \subseteq K$ tal que $\mathfrak{P} \cap \mathcal{O}_L$ tiene $g = 1$. Entonces $\mathrm{Gal}(K/L)$ fija a $\mathfrak{P}$ (puesto que es el único primo que divide a $\mathfrak{P} \cap \mathcal{O}_L$). Esto implica $\mathrm{Gal}(K/L) \subset D$, luego $K^D \subseteq L$. □

Hemos visto en la proposición anterior que p no escinde de K^D a K, puesto que $g = 1$. Lo que ocurrirá es que, o bien p ramifica, o bien es inerte.

La siguiente proposición que vamos a presentar nos va a asegurar que p escinde completamente y que no ramifica en $K^D/\mathbb{Q}$.

Proposición 3.4.4. *Sea $K/\mathbb{Q}$ una extensión de Galois, $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ que divide a $p \in \mathbb{Z}$ primo, D el grupo descomposición de $\mathfrak{P}$ y sea $L = K^D$. Sea $e = e(L/\mathbb{Q})$, $f = f(L/\mathbb{Q})$, $g = g(L/\mathbb{Q})$ para $L/\mathbb{Q}$ y p. Entonces, $e = f = g = 1$, $g = [L : \mathbb{Q}]$, $e(K/\mathbb{Q}) = e(K/L)$ y $f(K/\mathbb{Q}) = f(K/L)$.*

Demostración. Ya hemos mencionado que, gracias al Teorema órbita-estabilizador, $g(K/\mathbb{Q}) = [G : D]$. Además, por Teoría de Galois sabemos que $[G : D] = [L : \mathbb{Q}]$. Tenemos así que $g(K/\mathbb{Q}) = [L : \mathbb{Q}]$.

La Proposición 3.4.3 nos dice que $g(K/L) = 1$, aplicando el Teorema 3.2.3 tenemos

$$e(K/L) \cdot f(K/L) = [K : L] = [K : \mathbb{Q}]/[L : \mathbb{Q}] =$$
$$= \frac{e(K/\mathbb{Q}) \cdot f(K/\mathbb{Q}) \cdot g(K/\mathbb{Q})}{[L : \mathbb{Q}]} = e(K/\mathbb{Q}) \cdot f(K/\mathbb{Q}).$$

Ahora bien, como $e(K/L) \leq e(K/\mathbb{Q})$ y $f(K/L) \leq f(K/\mathbb{Q})$, entonces $e(K/L) = e(K/\mathbb{Q})$ y $f(K/L) = f(K/\mathbb{Q})$.

Por otra parte, como $e(K/\mathbb{Q}) = e(K/L) \cdot e(L/\mathbb{Q})$ y$f(K/\mathbb{Q}) = f(K/L) \cdot f(L|/\mathbb{Q})$, se sigue que $e(L/\mathbb{Q}) = f(L/\mathbb{Q}) = 1$ y concluimos la prueba. □

3.4.1. Grupos de Galois sobre cuerpos finitos.

Sea $K/\mathbb{Q}$ un cuerpo de números, $p \in \mathbb{Z}$ un número primo y $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ que divide a $p\mathcal{O}_K$. Sabemos que $\sigma \in D$ está bien definido sobre el cuerpo finito $k_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ puesto que σ está bien definida sobre $\mathcal{O}_K$ y, además, como $\sigma \in D$, σ fija $\mathfrak{P}$. Por lo tanto, obtenemos un homomorfismo

$$\varphi : D \to \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p).$$

Vamos a denotar por $f = [k_{\mathfrak{P}} : \mathbb{F}_p]$. El grupo $\mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ contiene al elemento Frob_p definido por $\mathrm{Frob}_p(x) = x^p$, puesto que

$$(xy)^p = x^p y^p$$

y

$$(x + y)^p = x^p + px^{p-1}y + \cdots + y^p \equiv x^p + y^p (\text{mód } p).$$

Tenemos que $k^*_{\mathfrak{P}}$ es cíclico pues ya sabemos que cualquier subgrupo finito de un grupo multiplicativo K^*, siendo K un cuerpo, es cíclico. Por lo tanto, existe $a \in k^*_{\mathfrak{P}}$ de orden $p^f - 1$ y $k^*_{\mathfrak{P}} = \mathbb{F}_p(a)$. Entonces $\mathrm{Frob}^n_p(a) = a^{p^n} = a$ si y solo si $p^f - 1 \mid p^n - 1$. Esto ocurre cuando $f \mid n$; luego el orden de $\mathrm{Frob}_p = f$. Como el orden del grupo de automorfismos de un cuerpo es, como mucho, el orden de la extensión, podemos concluir que $\mathrm{Aut}(k_{\mathfrak{P}}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$. Además, $\mathrm{Aut}(k_{\mathfrak{P}}/\mathbb{F}_p)$ tiene orden igual al grado de la extensión. Concluimos así que $k_{\mathfrak{P}}/\mathbb{F}_p$ es de Galois, con $\mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ cíclico de orden f generado por Frob_p.

Con esto hemos demostrado el siguiente teorema:

Teorema 3.4.5.

$$Gal(\kappa_{\mathfrak{P}}/\mathbb{F}_p) = \langle Frob_p \rangle.$$

3.4.2. La secuencia exacta.

En la sección anterior hemos visto que, como $D_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}$, hay un homomorfismo

$$\varphi_{\mathfrak{P}} : D_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p).$$

Vamos a ver que este homomorfismo es sobreyectivo. Así, tendremos que la secuencia

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p) \to 1$$

es exacta.

Teorema 3.4.6. *El homomorfismo φ es sobreyectivo.*

Demostración. Sea $\overline{a} \in k_{\mathfrak{P}}$ un elemento tal que $k_{\mathfrak{P}} = \mathbb{F}_p(\overline{a})$. Levantamos $\overline{a}$ a un entero algebraico $a \in \mathcal{O}_K$ y tenemos que

$$f(x) = \prod_{\sigma \in D_{\mathfrak{P}}} (x - \sigma(a)) \in K^D[x]$$

es el polinomio característico de a sobre K^D. Usando la Proposición 3.4.4 vemos que $f(x)$ se reduce a un múltiplo del polinomio mínimo de $\overline{a}$

$$\overline{f}(x) = \prod (x - \overline{\sigma(a)}) \in \mathbb{F}_p[x].$$

Las raíces de $\overline{f}(x)$ son de la forma $\overline{\sigma(a)}$ y el elemento $\mathrm{Frob}_p(a)$ es también una raíz de $\overline{f}(x)$. Por lo tanto $\mathrm{Frob}_p(a)$ es de la forma $\overline{\sigma(a)}$. Así, tenemos que $\mathrm{Frob}_p(a)$, que es el generador de $\mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ está en la imagen de $\varphi_{\mathfrak{P}}$. Por lo tanto, $\varphi_{\mathfrak{P}}$ es sobreyectivo. □

Ya habíamos definido el grupo de inercia como el núcleo de φ, por lo tanto, tenemos que, efectivamente, la secuencia

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p) \to 1$$

es exacta.

Corolario 3.4.7. *Sea $\mathfrak{P}$ ideal primo de K que divide a p, entonces*

$$|I_{\mathfrak{P}}| = e(\mathfrak{P}/p).$$

Demostración. Por la secuencia que hemos demostrado que es exacta tenemos que

$$|I_{\mathfrak{P}}| = \frac{|D_{\mathfrak{P}}|}{f(K/\mathbb{Q})}.$$

Aplicando las Proposiciones 3.4.3 y 3.4.4 tenemos

$$|D_{\mathfrak{P}}| = [K : L] = \frac{[K : \mathbb{Q}]}{g} = \frac{efg}{g} = ef \Rightarrow |D_{\mathfrak{P}}| = ef.$$

Dividiendo en ambos lados por f obtenemos la igualdad que nos da el corolario. □

Figura 3.3: Ferdinand Georg Frobenius (1849–1917) fue un matemático alemán doctorado por la Universidad Humboldt de Berlín bajo la supervisión de Weierstrass. Realizó importantes aportes a la Teoría de Ecuaciones Diferenciales y Teoría de Grupos. Frobenius demostró los Teoremas de Sylow mediante grupos abstractos.

Vamos a ver, para finalizar esta sección, una caracterización del grupo de inercia.

Proposición 3.4.8. *Sea $K/\mathbb{Q}$ una extensión de Galois con grupo de Galois G y sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ que divide a $p \in \mathbb{Z}$ primos. Entonces*

$$I_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(a) \equiv a (\text{mód } \mathfrak{P}), \forall a \in \mathcal{O}_K\}.$$

Demostración. Por definición sabemos

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \mid \sigma(a) \equiv a (\text{mód } \mathfrak{P}), \forall a \in \mathcal{O}_K\}.$$

Así, es suficiente ver que si $\sigma \notin D_{\mathfrak{P}}$ entonces existe $a \in \mathcal{O}_K$ tal que $\sigma(a) \not\equiv a$ (mód $\mathfrak{P}$).

Si $\sigma \notin D_{\mathfrak{P}}$, entonces $\sigma^{-1} \notin D_{\mathfrak{P}}$. Por lo tanto $\sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$. Como ambos ideales son maximales, existe $a \in \mathfrak{P}$ tal que $a \notin \sigma^{-1}\mathfrak{P}$ o, equivalentemente, $\sigma(a) \notin \mathfrak{P}$. Por lo tanto, $\sigma(a) \not\equiv a$(mód $\mathfrak{P}$). □

3.5. Elementos de Frobenius.

Supongamos que $K/\mathbb{Q}$ es una extensión de Galois con grupo de Galois G y $p \in \mathbb{Q}$ es un primo que no ramifica en K. Entonces $I = I_{\mathfrak{P}} = 1$ para cualquier $\mathfrak{P}$ que divida a p. Así, el homomorfismo φ_p definido al comenzar la sección 3.4.2 es un isomorfismo, es decir, $D_{\mathfrak{P}} \simeq \text{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$.

Gracias al Teorema 3.4.5 sabemos que $\text{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ es cíclico con generador Frob_p. El *elemento de Frobenius* correspondiente a $\mathfrak{P}$ es $\text{Frob}_p \in D_{\mathfrak{P}}$. Este elemento es el único elemento de G tal que para todo $a \in \mathcal{O}_K$ ocurre

$$\text{Frob}_p(a) \equiv a^p \text{ (mód } \mathfrak{P}).$$

Vamos a ver ahora que, al igual que los ideales primos y los grupos de descomposición son conjugados, los elementos de Frobenius correspondientes a los primos $\mathfrak{P}$ que dividen a p también lo son.

Proposición 3.5.1. *Para cada $\sigma \in G$ se tiene que*

$$Frob_{\sigma\mathfrak{P}} = \sigma Frob_{\mathfrak{P}}\sigma^{-1}.$$

En particular, los elementos de Frobenius correspondientes a los ideales primos que dividen a p son todos conjugados.

Demostración. Tomamos $\sigma \in G$ fijo. Para cualquier $a \in \mathcal{O}_K$ tenemos

$$\mathrm{Frob}_{\mathfrak{P}}(\sigma^{-1}(a)) - \sigma^{-1}(a)^p \in \mathfrak{P}.$$

Aplicando σ a ambos lados tenemos

$$\sigma\mathrm{Frob}_{\mathfrak{P}}(\sigma^{-1}(a)) - a^p \in \sigma\mathfrak{P},$$

luego $\sigma\mathrm{Frob}_{\mathfrak{P}}\sigma^{-1} = \mathrm{Frob}_{\sigma\mathfrak{P}}$. □

Hemos visto entonces que la conjugación de la clase de $\mathrm{Frob}_{\mathfrak{P}}$ en G es una función bien definida en p. Además, si G es un grupo abeliano, $\mathrm{Frob}_{\mathfrak{P}}$ no depende de la elección del primo $\mathfrak{P}$ que divide a p y obtenemos el *símbolo de Artin*, denotado por

$$\left(\frac{K/\mathbb{Q}}{p}\right) = \mathrm{Frob}_{\mathfrak{P}} \in G.$$

3.6. Grupos de ramificación superior.

Los grupos de ramificación superior van a ser la herramienta básica para la demostración que vamos a dar del Teorema de Kronecker Weber. Por ello, vamos a estudiar con detenimiento el concepto y las propiedades que tienen dichos grupos.

Los grupos de ramificación superior son subgrupos del grupo de inercia y, por tanto, heredan algunas de sus propiedades.

Como en la sección anterior, vamos a trabajar con las hipótesis de que $K/\mathbb{Q}$ es una extensión finita de Galois con grupo de Galois G, $\mathfrak{P}$ un ideal primo de $\mathcal{O}_K$ que divide a $p \in \mathbb{Z}$ primo.

Definición 3.6.1. *Sea $k \geq 1$ un número entero. El conjunto*

$$G_k(\mathfrak{P}/p) = \{\sigma \in I_{\mathfrak{P}} \mid \sigma(b) \equiv b(\text{mód } \mathfrak{P}^{k+1}), \forall b \in \mathcal{O}_K\}$$

formado por los elementos $\sigma \in I_{\mathfrak{P}}$ que actúan trivialmente en el anillo cociente $\mathcal{O}_K/\mathfrak{P}^{k+1}$, es un subgrupo normal de $I_{\mathfrak{P}}$ y se denomina k-ésimo grupo de ramificación de $\mathfrak{P}$ sobre p.

Notemos que el k-ésimo grupo de ramificación no es más que el núcleo del homomorfismo de grupos

$$I_{\mathfrak{P}} \to \mathrm{Aut}\left((\mathcal{O}_K/\mathfrak{P}^{k+1})/\mathbb{F}_p\right).$$

Si nos fijamos en la definición que hemos dado del k-ésimo grupo de ramificación, el subíndice del grupo es una unidad inferior al exponente de $\mathfrak{P}$ que utilizamos en el anillo cociente $\mathcal{O}_K/\mathfrak{P}^{k+1}$ sobre el cual pedimos que la acción sea trivial. Observemos que la definición que hemos dado coincide con la dada previamente para los grupos de descomposición (G_{-1}) e inercia (G_0). Además, $\forall k \geq -1$, el grupo G_{k+1} es un subgrupo de G_k. Obtenemos así una sucesión de subgrupos de $I_{\mathfrak{P}}$:

$$G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k \supseteq G_{k+1} \supseteq \ldots$$

Como $\mathcal{O}_K$ es de Dedekind, en particular es Noetheriano, por lo tanto satisface

$$\bigcap_{k\geq -1} \mathfrak{P}^k = \{0\}.$$

Como $I_{\mathfrak{P}}$ es finito, entonces existe $m \in \mathbb{Z}$ tal que $\forall k \geq m$, tenemos que $G_k = \{1\}$. Así, los subgrupos G_k forman una cadena finita y normal de $D_{\mathfrak{P}} = G_{-1}$.

Lo que realmente nos interesa de los grupos de ramificación superior son los cocientes G_k/G_{k+1}, así que vamos a estudiarlos con un poco de detenimiento.

Lema 3.6.2. *El cociente $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ es isomorfo a $Gal(\kappa_{\mathfrak{P}}/\mathbb{F}_p)$.*

Demostración. Ya vimos anteriormente que la sucesión

$$1 \to I_{\mathfrak{P}} \xrightarrow{\varphi_1} D_{\mathfrak{P}} \xrightarrow{\varphi_2} \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p) \to 1$$

es exacta. Por el primer teorema de isomorfía sabemos que

$$D_{\mathfrak{P}}/\mathrm{Ker}(\varphi_1) \simeq \mathrm{Img}(\varphi_2) \Rightarrow D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(\kappa_{/\mathfrak{P}}/\mathbb{F}_p).$$

□

Proposición 3.6.3. *Para todo entero $k \geq 1$, los grupos cociente G_k/G_{k+1} son abelianos.*

La demostración de la Proposición 3.6.3 es consecuencia de un resultado de los conmutadores

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1},$$

con $\sigma \in G_k$ y $\tau \in G_n$, $k, n \geq 0$:

Lema 3.6.4. *Sean $\sigma \in G_k$ y $\tau \in G_n$, $k, n \geq 0$, entonces $[\sigma, \tau] \in G_{k+n}$.*

Demostración. Vamos a comenzar la demostración de este lema viendo que para todo $b \in \mathfrak{P}^{n+1}$ se verifica que $\sigma(b) - b \in \mathfrak{P}^{k+n+1}$. Para comprobar esto es suficiente tomar $b := b_1 \cdot b_2 \cdot \cdots \cdot b_{n+1}$ de manera que $b_j \in \mathfrak{P}$, ya que estos elementos generan $\mathfrak{P}^{n+1}$ como grupo abeliano aditivo. Con esta notación tenemos

$$\sigma(b) - b = \textstyle\sum_{j=1}^{n+1} \sigma(b_1)\sigma(b_2)\ldots\sigma(b_{j-1})(\sigma(b_j) - b_j)b_{j+1}\ldots b_{n+1} =$$

$$= (\sigma(b_1) - b_1) \cdot b_2 \cdot \cdots \cdot b_{n+1} + \sigma(b_1)\,(\sigma(b_2) - b_2) \cdot b_3 \cdot \cdots \cdot b_{n+1} + \ldots$$
$$\cdots + \sigma(b_1)\sigma(b_2) \cdot \ldots \cdot \cdots \sigma_{n-1}\,(\sigma(b_n) - b_n) \cdot b_{n+1} +$$
$$+\sigma(b_1)\sigma(b_2) \cdot \ldots \cdot \cdots \sigma b_n\,(\sigma(b_{n+1}) - b_{n+1}) =$$

$$= \sigma(b_1)b_2\ldots b_{n+1} - b_1b_2\ldots b_{n+1} + \sigma(b_1)\sigma(b_2)b_3\ldots b_{n+1} - \sigma(b_1)b_2\ldots b_{n+1} +$$
$$+\sigma(b_1)\sigma(b_2)\sigma(b_3)b_4\ldots b_{n+1} - \sigma(b_1)\sigma(b_2)b_3b_4\ldots b_{n+1} +$$
$$+\sigma(b_1)\ldots\sigma(b_{n+1}) - \sigma(b_1)\ldots\sigma(b_n)b_{n+1} =$$

$$= \sigma(b_1)\ldots\sigma(b_{n+1}) - b_1\ldots b_{n+1}$$

que muestra que $\sigma(b) - b \in \mathfrak{P}^{k+n+1}$, ya que todo $\sigma(b_j) - b_j \in \mathfrak{P}^{k+1}$ para $b_j \in \mathcal{O}_K$ y $\sigma \in G_k$.

De manera análoga se comprueba que para todo $c \in \mathfrak{P}^{k+1}$ se verifica que $c - \tau(c) \in \mathfrak{P}^{k+n+1}$.

Tomamos ahora un elemento $x \in \mathcal{O}_K$ cualquiera y pongamos $y := \sigma^{-1}\tau^{-1}(x)$, $b := \tau(y) - y$ y $c := \sigma(y) - y$. Por la elección de σ y τ se verifica

que $b \in \mathfrak{P}^{n+1}$ y $c \in \mathfrak{P}^{k+1}$. Así, obtenemos que $\sigma(b) - b, \tau(c) - c \in \mathfrak{P}^{k+n+1}$. Restamos ambas expresiones:

$$\sigma(b) - b - (\tau(c) - c) = \sigma(b) - b - \tau(c) + c =$$

$$= \sigma(\tau(y) - y) - (\tau(y) - y) - \tau(\sigma(y) - y) + (\sigma(y) - y) =$$

$$= \sigma\tau(y) - \tau\sigma(y) \in \mathfrak{P}^{k+n+1},$$

es decir, tenemos que $[\sigma, \tau](x) - x \in \mathfrak{P}^{k+n+1}$. Esto implica que $[\sigma, \tau] \in G_{k+n}$. □

Demostración. Proposición 3.6.3.
Para terminar la demostración de que los cocientes G_k/G_{k+1} son abelianos basta tomar $n = k$ en el Lema 3.6.4, obteniendo así que $[\sigma, \tau] \in G_{2k}$. Como $k \geq 1$, tenemos que $2k \geq k + 1$ y esto implica que G_k/G_{k+1} es abeliano. □

Proposición 3.6.5. *Sea $\kappa_{\mathfrak{P}}/\mathbb{F}_p$ separable. Entonces se verifican:*

I) *El cociente G_0/G_1 es isomorfo a un subgrupo finito del grupo multiplicativo $(\kappa_{\mathfrak{P}})^*$; en particular, es cíclico de orden primo con la característica residual (si es positiva).*

II) *Para $k \geq 1$, los cocientes G_k/G_{k+1} son isomorfos a subgrupos fnitos del grupo aditivo del cuerpo residual $\kappa_{\mathfrak{P}}$; en particular, si $\kappa_{\mathfrak{P}}$ es un cuerpo de característica $p > 0$, los cocientes son p-grupos abelianos elementales. Si la característica residual es cero, los cocientes son triviales y $G_1 = \{0\}$.*

Demostración.

Vamos a demostrar este teorema para el caso en el que $\mathcal{O}_K$ sea un dominio de ideales principales. La demostración en el caso general se puede encontrar en [13].

I) Tomamos x un generador de $\mathfrak{P}$. Definimos el siguiente homomorfismo de grupos abelianos:

$$\varphi : G_0 \to (\mathcal{O}_K/\mathfrak{P})^*.$$

Dado $\sigma \in G_0$, el elemento $\sigma(x) \in \mathfrak{P}$ puesto que $\sigma(\mathfrak{P}) = \mathfrak{P}$. Sin embargo, $\sigma(x) \notin \mathfrak{P}^2$ porque si no, aplicando σ^{-1} tendríamos que $x \in \mathfrak{P}^2$. Por lo tanto, existe $u_\sigma \in \mathcal{O}_K$, con $u_\sigma \notin \mathfrak{P}$ de manera que $\sigma(x) = u_\sigma x$. Si ahora tomamos $\tau \in G_0$, tenemos que $u_{\tau\sigma}x = \tau\sigma(x) = \tau(u_\sigma)u_\tau x$, de forma

que $u_{\tau\sigma} = \tau(u_\sigma)u_\tau$. Reduciendo módulo $\mathfrak{P}$ tenemos que $\tau(u_\sigma) \equiv u_\sigma$ mód $\mathfrak{P}$, puesto que $\tau \in G_0$. Por lo tanto,

$$u_{\sigma\tau} \equiv u_\sigma u_\tau \quad \text{mód } \mathfrak{P}.$$

Podemos definir entonces una aplicación multiplicativa $G_0 \to (\mathcal{O}_K/\mathfrak{P})$ y como $u_\sigma \in \mathcal{O}_K$ y $u_\sigma \notin \mathfrak{P}$, la imagen de dicha aplicación está incluida en $(\mathcal{O}_K/\mathfrak{P})^*$. De forma que se obtiene el morfismo de grupos $G_0 \to (\mathcal{O}_K/\mathfrak{P})^*$. Vamos a estudiar el núcleo de este morfismo.

El núcleo de este homomorfismo está formado por los $\sigma \in G_0$ tales que $u_\sigma \equiv 1 \mod \mathfrak{P}$; es decir, tales que $\sigma(x) \equiv x \mod \mathfrak{P}^2$. Y decir esto es equivalente a decir que $\sigma(b) \equiv b \mod \mathfrak{P}^2$, para todo $b \in \mathcal{O}_K$. Vamos a comprobar que esto se verifica:

Tomamos K^I el subcuerpo de K fijado por I y vamos a denotar por $\mathcal{O}_{K^I} = \mathcal{O} \cap K^I$ y $\mathfrak{P}_I = \mathfrak{P} \cap K^I$. Como La extensión residual es separable, tenemos que la extensión ramifica en $\mathfrak{P}$. Esto implica que $e(\mathfrak{P}/p) = 1$ y, como consecuencia del Corolario 3.4.6 tenemos que I es trivial. Por lo tanto, I fija todo K y esto implica que

$$\mathcal{O}_K/\mathfrak{P} = \mathcal{O}_{K^I}/\mathfrak{P}_I.$$

Así, podemos escribir cada elemento $b \in \mathcal{O}_K$ como $b = c + d$, con $c \in \mathcal{O}_{K^I}$ y $d \in \mathfrak{P}$. Ahora bien, como $\sigma \in G_0 = I$ y $c \in \mathcal{O}_{K^I}$, tenemos que $\sigma(c) = c$. Por lo tanto, solo tendríamos que comprobar que $\sigma(d) \equiv d$ mód $\mathfrak{P}^2$. Como $d \in \mathfrak{P}$, podemos tomar $d = ax$, con $a \in \mathcal{O}_K$. Tenemos así

$$\sigma(d) - d = \sigma(ax) - ax = \sigma(a)\sigma(x) - ax =$$

$$= \sigma(a)(\sigma(x) - x) + x(\sigma(a) - a) \in \mathfrak{P}^2,$$

pues $\sigma(a) \in \mathcal{O}_K$, $\sigma(a) - a \in \mathfrak{P}$, pues $a \in \mathcal{O}_K$ y $\sigma \in G_0 = I$ y ya teníamos que $\sigma(x) - x \in \mathfrak{P}^2$.

Luego el núcleo de $G_0 \to (\mathcal{O}_K/\mathfrak{P})^*$ es G_1 y por el primer teorema de isomorfía tenemos que $G_0/G_1 \simeq K$, con $K \subseteq (\mathcal{O}_K/\mathfrak{P})^*$. Hemos probado, por lo tanto, la primera afirmación de la proposición.

II) Esta segunda afirmación se demuestra de manera análoga a como hemos demostrado la primera. Vamos a definir el homomorfismo de grupos abelianos

$$\phi : G_k \to \mathcal{O}_K/\mathfrak{P}.$$

Dado $\sigma \in G_k$ tenemos que el elemento $\sigma(x) - x \in \mathfrak{P}^{k+1}$, pero no pertenece a $\mathfrak{P}^{k+2}$. Por lo tanto, existe $u_\sigma \in \mathcal{O}_K$, con $u_\sigma \in \mathfrak{P}^{k+1}$, de forma que $\sigma(x) - x = u_\sigma x^{k+1}$. Tomando $\tau \in G_k$ tenemos que

$$u_{\tau\sigma}x^{k+1} = \tau\sigma(x) - \tau(x) = \tau\sigma(x) - x = \tau(\sigma(x) - x) + (\tau(x) - x)$$

$$= \tau(u_\sigma x^{k+1}) + u_\tau x^{k+1} = \tau(u_\sigma)\tau(x)^{k+1} + u_\tau x^{k+1} =$$

$$= \tau(u_\sigma)(x + u_\tau x^{k+1})^{k+1} + u_\tau x^{k+1} = x^{k+1}(\tau(u_\sigma)(1 + u_\tau x^k)^{k+1} + u_\tau).$$

Dividiendo por x^{k+1} tenemos

$$u_{\tau\sigma} = (\tau(u_\sigma)(1 + u_\tau x^k)^{k+1} + u_\tau).$$

Reduciendo módulo $\mathfrak{P}$ tenemos $u_{\tau\sigma} = \tau(u_\sigma) + u_\tau)$ y, como $\tau(u_\sigma) \equiv u_\sigma$ mód $\mathfrak{P}$ obtenemos

$$u_{\tau\sigma} \equiv u_\sigma + u_\tau \quad \text{mód } \mathfrak{P}.$$

Por lo tanto, reduciendo módulo $\mathfrak{P}$ obtenemos el morfismo aditivo

$$\phi : G_k \to \mathcal{O}_K/\mathfrak{P}.$$

Vamos a estudiar el núcleo de ϕ que está formado por los $\sigma \in G_k$ tales que $u_\sigma \equiv 0 \mod \mathfrak{P}$, es decir, tales que $\sigma(x) - x \in \mathfrak{P}^{k+2}$. Y, como en la prueba de I), decir esto es equivalente a decir que para todo $b \in \mathcal{O}_K$ se verifica $\sigma(b) - b \in \mathfrak{P}^{k+2}$. Vamos a comprobarlo:

Tomamos K^I el subcuerpo de K fijado por I y vamos a denotar por $\mathcal{O}_{K^I} = \mathcal{O} \cap K^I$ y $\mathfrak{P}_I = \mathfrak{P} \cap K^I$. Como La extensión residual es separable, tenemos que la extensión ramifica en $\mathfrak{P}$. Argumentando igual que antes tenemos que

$$\mathcal{O}_K/\mathfrak{P} = \mathcal{O}_{K^I}/\mathfrak{P}_I.$$

Así, podemos escribir cada elemento $b \in \mathcal{O}_K$ como $b = c + d$, con $c \in \mathcal{O}_{K^I}$ y $d \in \mathfrak{P}^{k+1}$. Ahora bien, como $\sigma \in G_k$ y $c \in \mathcal{O}_{K^I}$, tenemos que $\sigma(c) = c$. Por lo tanto, solo tendríamos que comprobar que $\sigma(d) \equiv d$ mód $\mathfrak{P}^{k+2}$. Podemos tomar $d = ax$, con $a \in \mathcal{O}_K$. Tenemos así

$$\sigma(d) - d = \sigma(ax) - ax = \sigma(a)\sigma(x) - ax =$$

$$= \sigma(a)(\sigma(x) - x) + x(\sigma(a) - a) \in \mathfrak{P}^{k+2},$$

pues $\sigma(a) \in \mathcal{O}_K$, $\sigma(a) - a \in \mathfrak{P}^{k+1}$, pues $a \in \mathcal{O}_K$ y $\sigma \in G_k$ y ya teníamos que $\sigma(x) - x \in \mathfrak{P}^{k+2}$.

Así, el núcleo de ϕ es G_{k+1} y ya hemos terminado de demostrar esta segunda afirmación.

□

Corolario 3.6.6. *Supongamos que el cuerpo residual es de característica positiva p. Entonces G_1 es un p-grupo abeliano y el cociente G_0/G_1 es un grupo abeliano de orden no divisible por p.*

Definición 3.6.7. *Sea $K/\mathbb{Q}$ un cuerpo de números. La extensión $\mathcal{O}_K/\mathbb{Z}$ de anillos de Dedekind se dice* moderadamente ramificada *en un ideal primo no nulo $\mathfrak{P} \subset \mathcal{O}_K$ cuando el índice de ramificación $e(\mathfrak{P}/p)$ no es divisible por la característica residual en $\mathfrak{P}$. En caso contrario, se llama* salvajemente ramificada*.*

Para terminar este capítulo, notemos que en el caso de que la extensión $K/\mathbb{Q}$ sea de Galois, decir moderadamente ramificada en $\mathfrak{P}$ es lo mismo que decir que el grupo de ramificación G_1 es trivial.

Notemos que ser moderadamente ramificada es un caso particular de no ser ramificada.

Con todo lo visto hasta ahora, ya tenemos las herramientas suficientes para probar el Teorema de Kronecker-Weber.

Capítulo 4

El Teorema de Kronecker-Weber.

Figura 4.1: Leopold Kronecker (1829-1891) fue un matemático alemán. Se doctoró en 1845 en la Universidad de Berlín, donde tuvo como tutor a Dirichlet, y ese mismo año escribió su disertación sobre Teoría de Números. Kronecker defendía que el análisis y la aritmética deberían estar basados únicamente en los números enteros, dejando a un lado los números imaginarios e irracionales ya que *Dios hizo los números enteros; el resto es obra del hombre.*

En este capítulo del trabajo vamos a realizar una demostración completa del Teorema de Kronecker-Weber. Primero veremos que si el Teorema de Kronecker-Weber se satisface para todas las extensiones cíclicas de grado potencia de primo, entonces se va a satisfacer para todas las extensiones abelianas. Una vez visto dicho resultado, haremos la demostración en el caso de que la extensión sea moderadamente ramificada y en el caso de que extensión sea de grado potencia de primo, ramificando únicamente en el primo que divide al grado de la extensión.

Nuestro objetivo es demostrar el siguiente teorema:

Teorema 4.0.8 (Kronecker-Weber)**.** *Sea $K/\mathbb{Q}$ una extensión abeliana. Entonces, existe un entero positivo n y una raíz primitiva n-ésima de la unidad ξ_n tal que $K \subseteq \mathbb{Q}(\xi_n)$.*

Vamos a comprobar que, si el Teorema de Kronecker-Weber se verifica para todas las extensiones cíclicas de grado potencia de un primo, entonces se satisface para todas las extensiones abelianas.

Lema 4.0.9. *Si el Teorema de Kronecker-Weber se satisface para todas las extensiones cíclicas de grado potencia de primo, entonces se satisface para todas las extensiones abelianas.*

Demostración. Para demostrar este lema solo debemos considerar que toda extensión abeliana descompone en producto linealmente disjunto de extensiones cíclicas de grado potencia de primo. Esto ocurre porque todo grupo abeliano descompone en producto directo de p-subgrupos y estos en producto directo de subgrupos cíclicos.

Por hipótesis sabemos que el Teorema de Kronecker-Weber se satisface para todas las extensiones cíclicas de grado potencia de primo.

Sea $G = \mathrm{Gal}(K/\mathbb{Q})$ abeliano de manera que

$$G = \prod_i G_i,$$

con G_i un p_i-grupo cíclico, siendo p_i un número primo cualquiera. Vamos a denotar por K_i el subcuerpo de K fijado por el subgrupo $\prod_{j\neq i} G_j$ de G. Entonces K_i /$\mathbb{Q}$ es una extensión cíclica de manera que $[K_i : \mathbb{Q}] = p_i^m$. Por hipótesis, existe una raíz de la unidad ξ_i de manera que $K_i \subseteq \mathbb{Q}(\xi_i)$.

Sean $n_i \in \mathbb{Z}$ tales que ξ_i es una raíz primitiva n_i-ésima de la unidad y sea $n := \mathrm{mcm}\{n_i\}$ y ξ una raíz primitia n-ésima de la unidad. Como K es la composición de los cuerpos K_i, obtenemos $K \subseteq \mathbb{Q}(\xi)$, que es lo que queríamos probar. □

Ya demostrada esta parte, pasamos al caso moderadamente ramificado.

4.1. El caso moderadamente ramificado.

Ya hemos visto en capítulos anteriores que toda extensión de $\mathbb{Q}$ ramifica en algún número primo. Lo que vamos a hacer va a ser reducir la prueba del Teorema de Kronecker-Weber al caso en el que el conjunto de números primos que ramifican consista únicamente en el primo que divide al grado. Es decir, vamos a poder suponer que la extensión va a ser cíclica de grado p^m y no va a ramificar en l primo, con $l \neq p$. Es decir, vamos a demostrar la siguiente proposición:

Proposición 4.1.1. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado p^n tal que l es moderadamente ramificado sobre $\mathbb{Q}$. Entonces existe una extensión F de K y un subcuerpo $L \subseteq \mathbb{Q}(\xi_n)$ para cierto n de forma que:*

I. *Todo primo no ramificado en K es no ramificado en F.*

II. *l no ramifica en F.*

III. *$LK = LF$.*

Demostración. Tenemos $K/\mathbb{Q}$ extensión cíclica, con $[K : \mathbb{Q}] = p^n$ y $l \neq p$ un número primo en el que la extensión ramifica.

Tomamos $\mathfrak{L}$ un ideal de $\mathcal{O}_K$ que divide a l. En particular, tenemos que $K/\mathbb{Q}$ es moderadamente ramificada en l, o, equivalentemente, $G_1(\mathfrak{L}/l)$ es trivial.

Como $|G_0(\mathfrak{L}/l)| \mid p^n$, tenemos que $|G_0(\mathfrak{L}/l)| = p^m$, con $m \leq n$. Ademas, $\mathbb{Z}/l\mathbb{Z} = \mathbb{F}_l$ y el cociente G_{-1}/G_1 es abeliano, por lo tanto tenemos que

$$l \equiv 1(\text{mód } p^m).$$

Ahora bien, la extensión $\mathbb{Q}(\xi_l)\ /\mathbb{Q}$ es cíclica, totalmente ramificada en l y no ramificada fuera de l. Como consecuencia, existe un único subcuerpo $L \subseteq \mathbb{Q}(\xi_l)$ tal que la extensión $L/\mathbb{Q}$ es cíclica, totalmente ramificada en l, no ramificada fuera de l y de grado p^m.

Consideramos ahora el cuerpo composición KL. Como las extensiones $K/\mathbb{Q}$ y $L/\mathbb{Q}$ son abelianas de grado potencia de p, la composición $KL/\mathbb{Q}$ también es una extensión abeliana de grado potencia de p: $[K : \mathbb{Q}] = p^{n+t}$, con $t \leq m$.

Sea $\mathfrak{L}'$ un ideal primo del anillo de enteros $\mathcal{O}_{KL}$ que divide a $\mathfrak{L}$, $I' = G_0(\mathfrak{L}'/l)$ el grupo de inercia de $\mathfrak{L}'$ sobre l y $H := \text{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/p^m\mathbb{Z}$.

El morfismo restricción $\text{Gal}(KL/\mathbb{Q}) \to \text{Gal}(K/\mathbb{Q})$ aplica el grupo de inercia I' en el grupo de inercia $G_0(\mathfrak{L}/l)$. Obtenemos así la inclusión $I' \subseteq G_0(\mathfrak{L}/l) \times H$ por vía la identificación de $\text{Gal}(KL/\mathbb{Q})$ con un subgrupo de $\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q})$.

Sabemos también que el orden del grupo de inercia I' es múltiplo del orden del grupo de inercia $G_0(\mathfrak{L}/l)$, puesto que el índice de ramificación de $\mathfrak{L}'$ sobre l es divisible por el índice de ramificación de $\mathfrak{L}$ sobre l. Así, $|I'| = p^i$.

Además, $G_i(\mathfrak{L}'/l)$ son triviales para todo $i \geq 1$ puesto que la extensión es de grado potencia del primo p y p no divide a la característica residual l. Por lo tanto, I' es cíclico.

Otro dato que conocemos es que el orden de los elementos del grupo $G_0(\mathfrak{L}/l) \times H$ es un divisor de p^m, ya que los ambos son subgrupos de orden divisor de p^m.

Tenemos entonces que I' es cíclico, p^m divide a $|I'|$ e $I' \subseteq G_0(\mathfrak{L}/l) \times H$. Por lo tanto, $|I'| = p^m$.

Denotando ahora por K' el subcuerpo de KL fijado por I', tenemos que $K'/\mathbb{Q}$ no ramifica en l. Como $L/\mathbb{Q}$ es totalmete ramificada en l, entonces $K' \cap L = \mathbb{Q}$.

Por otra parte tenemos que $K'L \subseteq KL$ y $K'L$ es de grado

$$[K'L : \mathbb{Q}] = [K' : \mathbb{Q}][L : \mathbb{Q}] = \frac{[KL : \mathbb{Q}]}{e(\mathfrak{L}'/l)}[L : \mathbb{Q}] = \frac{[KL : \mathbb{Q}]}{[L : \mathbb{Q}]}[L : \mathbb{Q}] = [KL : \mathbb{Q}].$$

De aquí deducimos que $KL = K'L$.

Ya hemos visto que L es ciclotómico por ser subcuerpo de un cuerpo ciclotómico. Así, si comprobamos que K' también es ciclotómico, tendremos que $KL = K'L$ también lo será. Tendremos entonces que $K' = K$ es

ciclotómico. Por lo tanto, nuestro objetivo es comprobar que K' es ciclotómico.

Por cómo hemos construido K', éste no ramifica en l y además el conjunto de primos que ramifican en K' es un subgrupo del conjunto de primos que ramifican en K. El conjunto de primos que ramifican en K es finito, luego podemos repetir el proceso hasta conseguir que $K/\mathbb{Q}$ no ramifique fuera de los ideales primos que dividen a p. □

Con esto, podemos demostrar el Teorema de Kronecker-Weber en caso de que la extensión sea moderadamente ramificada:

Proposición 4.1.2. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado potencia de un número primo p, $[K:\mathbb{Q}] = p^m$, que solo ramifica en un primo $l \neq p$. Entonces $l \equiv 1 (\text{nód } p^m)$, la extensión $K/\mathbb{Q}$ es totalmente ramificada en l y K es el único subcuerpo de $\mathbb{Q}(\xi_l)$ de grado p^m. En consecuencia, la extensión $K/\mathbb{Q}$ es cíclica.*

Demostración. Supongamos primero que la extensión $K/\mathbb{Q}$ es cíclica de grado potencia del primo p: $[K:\mathbb{Q}] = p^m$.

Sea l el primo diferente de p en el que la extensión ramifica. Ya hemos probado anteriormente que $l \equiv 1 (\text{nód } p^m)$. Eligiendo K' como en el razonamiento anterior, tenemos que $K'/\mathbb{Q}$ es no ramificada en todo lugar.

Por el Teorema de Minkowski-Hermite, todo cuerpo de números ramifica en algún número primo. Con esto tenemos que $K' = \mathbb{Q}$, pues, si no, ramificaría en algún primo.

Como consecuencia, $K \subseteq KL = K'L = L$. Es decir, $K = L$ y L es el único subcuerpo de grado p^m de $\mathbb{Q}(\xi_l)$.

Para finalizar tenemos que ver que la extensión $K/\mathbb{Q}$ es cíclica:

Sabemos que $\mathbb{Q}(\xi_l)/\mathbb{Q}$ es cíclica y $K \subseteq \mathbb{Q}(\xi_l)$, podemos considerar K como composición de extensiones cíclicas de $\mathbb{Q}(\xi_l)$. Con esto tenemos que $K/\mathbb{Q}$ es cíclica. □

Corolario 4.1.3. *Sea $K/\mathbb{Q}$ una extensión abeliana y moderadamente ramificada en todos los ideales primos. Entonces existe una raíz de la unidad ξ tal que $K \subseteq \mathbb{Q}(\xi)$. En particular, si $K/\mathbb{Q}$ ramifica en $l_1, \ldots, l_k$, entonces el cuerpo K es un subcuerpo del cuerpo ciclotómico $\mathbb{Q}(\xi)$, donde ξ es una raíz n-ésima de la unidad, siendo $n = l_1 \cdot \cdots \cdot l_k$.*

Demostración. Por la Proposición 4.1.1 tenemos que existen $L_1 \subseteq \mathbb{Q}(\xi_{l_1})$ y F_1 tal que $l_2, \ldots, l_k$ son los primos ramificados en $F_1/\mathbb{Q}$ y $L_1K = L_1F_1$.

Aplicando de nuevo la Proposición 4.1.1 a $F_1/\mathbb{Q}$ tenemos que existen $L_2 \subseteq \mathbb{Q}(\xi_{l_2})$ y F_2 tales que $l_3, \ldots, l_k$ son ramificados en $F_2\mathbb{Q}$ y $L_2F_1 = L_2F_2$.

Reiterando el proceso para $i = 2, \ldots, k-1$ tenemos que existen $L_i \subseteq \mathbb{Q}(\xi_{l_1})$ y F_i tales que $l_{i+1}, \ldots, l_k$ son ramificados en F_i y $L_i F_{i-1} = L_i F_i$.

Finalmente, existe $L_k \subseteq \mathbb{Q}(\xi_{l_k})$ y F_k tales que $F_k/\mathbb{Q}$ es no ramificada en ningún primo y $L_k F_{k-1} = L_k F_k$.

Como L_k no ramifica en ningún primo, por el Teorema de Hermite-Minkowski tenemos que $L_k = \mathbb{Q}$ y, por lo tanto, $L_k F_{k-1} = L_k$, lo que implica que $F_{k-1} \subseteq L_k$. Como

$$L_{k-1} F_{k-2} = L_{k-1} F_{k-1} \subseteq F_k L_{k-1},$$

tenemos que $F_{k-2} \subseteq L_k L_{k-2}$. Reiterando el proceso tenemos que

$$K \subseteq L_k L_{k-1} \ldots L_2 L_1 \subseteq \mathbb{Q}(\xi_{l_1 \ldots l_k}).$$

Con esto, hemos probado lo que aseguraba el enunciado.

□

Figura 4.2: Wilhelm Eduard Weber (1804–1891) fue un físico alemán que estudió en la Universidad de Halle-Wittenberg y después fue profesor en la Universidad de Gotinga, recomendado por su amigo Gauss. Junto a éste último, inventó el telégrafo de Gauss-Weber.

4.2. El caso cíclico de grado una potencia de un primo.

En el apartado anterior hemos visto que para demostrar el Teorema de Kronecker-Weber es suficiente con probarlo para extensiones cíclicas de grado potencia de un primo p y que solo ramifican en p.

Distinguiremos el caso en el que p se par o impar.

4.2.1. El caso cíclico de grado una potencia de primo impar.

Vamos a comenzar demostrándolo en el caso de que el primo p sea impar. Para ello, necesitamos el siguiente resultado:

Proposición 4.2.1. *Sean p un primo impar y $K/\mathbb{Q}$ una extensión abeliana de grado p^m que solo ramifica en el primo p. Entonces $K/\mathbb{Q}$ es totalmente ramificada en p y cíclica.*

Demostración. Sea $\mathfrak{P}$ un ideal primo del anillo de enteros $\mathcal{O}_K$ que divide a p e $I := G_0(\mathfrak{P}/p)$.

El cuerpo fijado por I es un cuerpo extensión de $\mathbb{Q}$ que no ramifica en ningún ideal primo. Por lo tanto, gracias al Teorema de Hermite-Minkowski tenemos que $K^I = \mathbb{Q}$ y la extensión $K/\mathbb{Q}$ es totalmente ramificada en p o, equivalentemente, el grupo de inercia es todo el grupo de Galois de la extensión. En particular, la extensión residual es trivial y el cuerpo residual

de K en $\mathfrak{P}$ es $\mathbb{F}_p$. Ya conocemos la estructura de los cocientes sucesivos de los grupos de ramificación superior. Podemos asegurar así que el grupo de inercia coincide con G_1 y que para todo $k \geq 1$ el cociente G_k/G_{k+1} es un grupo abeliano trivial o cíclico de orden p. Por lo tanto, la extensión es totalmente ramificada en p.

Para comprobar que la extensión es cíclica tenemos que aplicar el siguiente reultado:

Lema 4.2.2. *Supongamos que $K/\mathbb{Q}$ es una extensión abeliana de grado p^m que solo ramifica en p. Entonces el grupo de ramificación $G_1(\mathfrak{P}/p)$ es trivial.*

Demostración. Localizando en $S = \mathbb{Z} - p\mathbb{Z}$, obtenemos que $\mathcal{O}_K$ es un dominio de ideales principales. Por lo tanto, podemos elegir un generador x de $\mathfrak{P}$. Sea $f(t)$ el polinomio mínimo de $\mathbb{Q}[t]$ que tiene a x por raíz. De hecho, como x es entero sobre $S^{-1}\mathbb{Z}$, tenemos que $f(t) \in S^{-1}\mathbb{Z}[t]$. Ya hemos visto que, los grupos de ramificación superior forman una cadena finita de $D_{\mathfrak{P}}$. Es decir, existe un entero k tal que $G_k \neq \{1\}$ pero $G_{k+1} = \{1\}$. Además, hemos visto en el principio de la demostración que $G_0 = G_1 \simeq \mathbb{Z}/p\mathbb{Z}$, luego $k \geq 1$. Vamos a comprobar que $k = 1$.

Comenzamos viendo que se verifica que $f'(x) \in \mathfrak{P}^{(k+1)(p-1)}$ pero $f'(x) \notin \mathfrak{P}^{(k+1)(p-1)+1}$. Podemos escribir la derivada de f como

$$f'(t) = \prod_{\sigma \in G_k, \sigma \neq 1} (t - \sigma(x))$$

y, evaluando en x obtenemos

$$f'(x) = \prod_{\sigma \in G_k, \sigma \neq 1} (x - \sigma(x)).$$

Como $x \in \mathfrak{P}$ y $\sigma \in G_k$, tenemos que $x - \sigma(x) \in \mathfrak{P}^{k+1}$ pero $x - \sigma(x) \notin \mathfrak{P}^{k+2}$ puesto que $\sigma \notin G_{k+1}$. Multiplicando por todos los posibles $\sigma \neq 1$ obtenemos que $f'(x) \in \mathfrak{P}^{(k+1)(p-1)}$ y $f'(x) \notin \mathfrak{P}^{(k+1)(p-1)+1}$.

Además, podemos escribir

$$f'(x) = px^{p-1} + (p-1)a_{p-1}x^{p-2} + \cdots + 2a_2x + a_1,$$

donde $a_j \in S^{-1}\mathbb{Z}$. Es decir, los a_j son números racionales cuyo denominador no es divisible por p. Como $K/\mathbb{Q}$ es totalmente ramificada en p y $[K : \mathbb{Q}] = p^m$, tenemos que la extensión de p es el ideal $\mathfrak{P}^p$, de forma que cada uno de los coeficientes a_j que no sea nulo es un elemento de una potencia $\mathfrak{P}^{pm_j}$, con $m_j \geq 0$. En particular, vamos a denotar por n_j al exponente de $\mathfrak{P}$ que

contiene al sumando $ja_j x^{j-1}$ pero tal que no pertenezca a $\mathfrak{P}^{n_j+1}$. Obtenemos de aquí que $n_j \equiv j-1 (\text{mód } p)$. Como consecuencia, todos los coeficientes no nulos están en potencias distintas de $\mathfrak{P}$, luego $f'(x)$ estará en el que tiene la potencia n_j más pequeña. En particular, tenemos

$$(k+1)(p-1) \leq n_{p-1} = 2p-1,$$

y como $k \geq 1$ y $p \geq 2$, tenemos que $k = 1$. Por lo tanto, $G_2 = \{1\}$, concluyendo así la prueba del lema. □

Para concluir la demostración de la proposición sabíamos que $G = G_0 = G_1$. Sea $k \geq 2$ tal que $G = G_k$ pero $G_{k+1} \subset G_k$. Gracias a la Proposición 3.6.5 sabemos que el cociente G_k/G_{k+1} es un grupo abeliano cíclico de orden p.

Como G es un p-grupo abeliano finito, si fuese cíclico solo debería poseer un subgrupo cíclico de orden p. Por lo tanto, es suficiente probar que G_{k+1} es el único subgrupo de G de índice p.

Supongamos que H es un subgrupo de G de índice p y que $H \neq G_{k+1}$. Consideramos los cuerpos fijos K^H y $K^{G_{k+1}}$ y sean $\mathfrak{P}_H = \mathfrak{P} \cap K^H$ y $\mathfrak{P}_{k+1} = \mathfrak{P} \cap K^{G_{k+1}}$. Vamos a calcular los grupos de ramificación superior para las extensiones $K^H/\mathbb{Q}$ y $K^{G_{k+1}}/\mathbb{Q}$. Como $\text{Gal}(K/K^{G_{k+1}}) = G_{k+1}$ tenemos

$$G_i(\mathfrak{P}/\mathfrak{P}_{k+1}) = \begin{cases} G_i \cap G_{k+1} = G_{k+1} & \text{si } 0 \leq i \leq k+1, \\ G_i \cap G_{k+1} = G_i & \text{si } i > k+1, \end{cases}$$

$$G_i(\mathfrak{P}/\mathfrak{P}_H) = \begin{cases} G_i \cap H = H & \text{si } 0 \leq i \leq k, \\ G_i \cap G_{k+1} \subset G_{k+1} & \text{si } i > k. \end{cases}$$

Notemos que la última inclusión es porque $H \neq G_{k+1}$ y los dos son subgrupos de índice p de G. Con estos cálculos podemos comparar los exponentes de $\mathfrak{P}$ en las extensiones $K^H/\mathbb{Q}$ y $K^{G_{k+1}}/\mathbb{Q}$ de forma que, como los k primeros sumandos son iguales, el sumando $k+1$ satisface la desigualdad estricta y los siguientes satisfacen la desigualdad, se verifica

$$\sum_{i \geq 0} (|G_i \cap H| - 1) < \sum_{i \geq 0} (|G_i \cap G_{k+1}| - 1).$$

Gracias al Lema 4.2.2 tenemos los grupos G_0 y G_1 de los dos subgrupos son cíclicos de orden p y G_2 son triviales. Además, como $K/\mathbb{Q}$ es totalmente ramificada y $[K : \mathbb{Q}] = p^m$, tenemos que $p = \mathfrak{P}^{p^m}$. Por otra parte, $K^H/\mathbb{Q}$ y $K^{G_{k+1}}/\mathbb{Q}$ son de igual grado (p^{m-1}) y totalmente ramificadas en p. Luego tenemos que $\mathfrak{P}_H$ y $\mathfrak{P}_{k+1}$ son ambos de la forma: $\mathfrak{P}^{p^{m-1}}$. Tenemos entonces que $H = G_{k+1}$ y, por lo tanto, G es cíclico.

□

Proposición 4.2.3. *Sea p un primo impar y $K/\mathbb{Q}$ una extensión cíclica de grado p^m que solo ramifica en p. Entonces K es el único subcuerpo de $\mathbb{Q}(\xi)$ de grado p^m, donde ξ es una raíz primitiva p^{m+1}-ésima de la unidad.*

Demostración. Sea K' el único subcuerpo de $\mathbb{Q}(\xi)$ de grado p^m. Tenemos así que ambas extensiones, $K'/\mathbb{Q}$ y $K/\mathbb{Q}$ verifican las condiciones del enunciado: son cíclicas, de grado p^m y ramifican únicamente en p.

Vamos a comprobar que $K = K'$ y, así, tendríamos demostrada la proposición:

Consideramos el cuerpo composición KK'. Tenemos que $KK'/\mathbb{Q}$ es una extensión abeliana que solo ramifica en p y de grado potencia de p. Por la Proposición 4.2.1, tenemos que $KK'/\mathbb{Q}$ es cíclica de grado potencia de p. Como $K, K' \subseteq KK'$ y $K/\mathbb{Q}$ y $K'/\mathbb{Q}$ tienen el mismo grado y ramifican en el mismo primo, entonces $K = K'$.

Tenemos así que K es el único subcuerpo de $\mathbb{Q}(\xi)$ de grado p^m, donde ξ es una raíz primitiva p^{m+1}-ésima de la unidad. □

4.2.2. El caso cuadrático.

Ya vimos que si una extensión $K/\mathbb{Q}$ es cuadrática, tenemos que $K = \mathbb{Q}(\sqrt{D})$, donde D es un entero libre de cuadrados. Es decir, $D = -1$ o $\pm D$ es un producto de números primos diferentes.

Claramente, la extensión $K/\mathbb{Q}$ es abeliana. Lo que vamos a demostrar es que existe una ráiz ξ primitiva de la unidad tal que $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\xi)$.

Vamos a comenzar considerando un número primo p impar y una raíz primitiva p-ésima de la unidad ξ. Vamos a comenzar primero encontrando todas las subextensiones cuadráticas de $\mathbb{Q}(\xi)/\mathbb{Q}$.

Definición 4.2.4. *Sea p un número primo impar. Denotamos por*

$$p^* := \left(\frac{-1}{p}\right) p.$$

Recordemos que

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n, \\ 1 & \text{si } p \nmid n \text{ y } \exists z \in \mathbb{Z} \text{ tal que } z^2 \equiv n (\text{mód } p), \\ -1 & \text{en otro caso.} \end{cases}$$

En nuestro caso $n = -1$ y p es un primo natural, por lo tanto $(\frac{-1}{p}) \in \{-1, 1\}$. En particular, $p^* \equiv 1 \pmod 4$. Como corolario a esta observación tenemos el siguiente resultado:

Corolario 4.2.5. *Sea p un número primo impar y sea ξ una raíz primitiva p-ésima de la unidad. Entonces $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\xi)$.*

Por último, necesitamos la siguiente proposición:

Proposición 4.2.6. *Las únicas extensiones cuadráticas de $\mathbb{Q}$ con discriminante una potencia de 2 son $\mathbb{Q} = \mathbb{Q}(\xi_4)$, $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(i\sqrt{2})$.*

Demostración. Sea $K = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados. Como el discriminante de esta extensión es d o $4d$ y, a la vez, tiene que ser una potencia de 2, tenemos que $d = \pm 1, \pm 2$. El caso $d = 1$ queda descartado, por lo tanto, K es uno de los cuerpos expuestos en el enunciado.

Ahora bien,

$$\xi_8 = \sqrt{\sqrt{-1}} = \sqrt[4]{-1} = \frac{\cos \pi/4 + \sin \pi/4}{2} = \frac{\sqrt{2}}{2}(1 + i).$$

Por lo tanto,

$$\xi_8 + \overline{\xi_8} = \sqrt{2}, \xi_8 - \overline{\xi_8} = i\sqrt{2},$$

de donde se sigue que

$$\mathbb{Q}(\xi_4), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(\xi_8).$$

□

Pasemos a demostrar el Teorema de Kronecker-Weber en el caso de que la extensión sea cuadrática:

Teorema 4.2.7. *Sea D un entero libre de cuadrados. Entonces se cumple $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\xi)$, donde ξ es una raíz primitiva $|4D|$-ésima de la unidad.*

Demostración. Ya sabemos que i es raíz cuarta primitiva de la unidad. Además, $\mathbb{Q}(\sqrt{-p^*})$ es subcuerpo de la composición de los cuerpos ciclotómicos $\mathbb{Q}(\sqrt{p^*})$ y $\mathbb{Q}(i)$ y, como la composición de cuerpos ciclotómicos es ciclotómico, tenemos que las extensiones $\mathbb{Q}(\sqrt{\pm p}) \mid \mathbb{Q}$, con p un número primo impar, son subextensiones de un cuerpo ciclotómico.

Tomamos ahora la raíz octava primitiva de la unidad $\xi_8 = \frac{1+i}{\sqrt{2}}$. Como $i \in \mathbb{Q}(\xi_8)$, entonces $\sqrt{2}$ y $\sqrt{-2}$ también están en $\mathbb{Q}(\xi_8)$. De esta manera, los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2})$ son subextensiones de cuerpos ciclotómicos.

Para finalizar, sea $D = \pm p_1 p_2 \dots p_r$ la descomposición de D en números primos. Se satisface la inclusión siguiente:

$$\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \sqrt{p_2^*}, \dots, \sqrt{p_r^*}).$$

Como cada uno de los subcuerpos $\mathbb{Q}(\sqrt{p_i^+})$ es un subcuerpo de un cuerpo ciclotómico, tenemos que $\mathbb{Q}(\sqrt{D})$ también es un subcuerpo de un cuerpo ciclotómico. Queda así demostrado el teorema. □

4.2.3. El caso cíclico de grado una potencia de 2.

Ya hemos probado el Teorema de Kronecker-Weber en caso de que la extensión sea cíclica de grado potencia de primo impar. Solo nos queda demostrar el caso en que la extensión sea cíclica de grado potencia de 2 y solo ramifique en éste último.

Proposición 4.2.8. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado 2^m que solo ramifica en 2. Entonces K es exactamente el subcuerpo maximal $\mathbb{Q}(\xi+\xi^{-1})$ del cuerpo $\mathbb{Q}(\xi)$, donde ξ es una raíz primitiva 2^{m+2}-ésima de la unidad.*

Demostración. Comenzamos viéndolo para $m = 1$. Ya sabemos que toda extensión cuadrática de $\mathbb{Q}$ es ciclotómica y que, si solo ramifica en 2, es uno de los siguientes cuerpos: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ o $\mathbb{Q}(\sqrt{-2})$. Estos son los tres únicos subcuerpos cuadráticos de $\mathbb{Q}(\xi)$, siendo ξ una $2^{m+2} = 8$-ésima raíz primitiva de la unidad. Tenemos que $\mathbb{Q}(\sqrt{2})$ es el único subcuerpo real; por lo tanto el resultado es claro en este caso.

Supongamos ahora $m \geq 2$. Como $K/\mathbb{Q}$ es una extensión abeliana de grado divisible por 2, K contiene un subcuerpo cuadrático. Como K es real y la extensión solo ramifica en 2, tenemos las mismas restricciones que en el caso anterior; esto implica que el grupo de Galois de la extensión $K/\mathbb{Q}$ solo tiene un subgrupo de índice 2 y, en consecuencia, es cíclico.

Vamos a comparar ahora el cuerpo K con el cuerpo $L := \mathbb{Q}(\xi+\xi^{-1})$. El cuerpo composición KL es un cuerpo real y la extensión $KL/\mathbb{Q}$ es abeliana, no ramificada fuera de 2 y de grado potencia de 2. Por lo tanto, $KL/\mathbb{Q}$ es cíclica. Como $K, L \subseteq KL$ y ambas extensiones son del mismo grado sobre $\mathbb{Q}$ y ramifican en 2, tenemos $K = L$ y, así, hemos probado lo que queríamos ver. □

Visto este resultado, ya estamos en disposición de probar el Teorema de Kronecker-Weber en caso de que la extensión sea cíclica de grado potencia de 2:

Proposición 4.2.9. *Sea $K/\mathbb{Q}$ una extensión abeliana de grado 2^m y no ramificada fuera de 2. Entonces K es uno de los tres subcuerpos $\mathbb{Q}(\xi^2)$, $\mathbb{Q}(\xi+\xi^{-1})$ o $\mathbb{Q}(\xi-\xi^{-1})$ del cuerpo ciclotómico $\mathbb{Q}(\xi)$, donde ξ es una raíz primitiva 2^{m+2}-ésima de la unidad. Estos cuerpos son los únicos subcuerpos de $\mathbb{Q}(\xi)$ de grado 2^m sobre $\mathbb{Q}$.*

Demostración. El cuerpo composición de K con $\mathbb{Q}(i)$, K_i, es una extensión abeliana de $\mathbb{Q}$ no ramificada fuera de 2 y de grado potencia de 2: $[K_i : \mathbb{Q}] = 2^n$, con $n \geq m + 1$.

Sea $K_i^+ = K_i \cap \mathbb{R}$ el subcuerpo real maximal de K_i. Tenemos que K_i^+ es no ramificado fuera de 2 y de grado 2^s, con $s \leq n - 1 \leq m$, puesto que $i \notin K_i^+$. Así, K_i^+ es subcuerpo de $\mathbb{Q}(\xi + \xi^{-1})$, pues este es el único cuerpo real que satisface las condiciones.

Para terminar, es suficiente demostrar que K_i es el cuerpo $K_i^+(i)$, que es un subcuerpo de $\mathbb{Q}(\xi + \xi^{-1})(i) = \mathbb{Q}(i)$. Pero $K_i^+(i) \subseteq K_i$ y los dos son de grado 2 sobre K_i^+ y ramifican solo en 2. Por lo tanto coinciden. □

Anexo

Aplicación al Problema Inverso de Galois para grupos abelianos finitos.

El Problema Inverso de Galois para grupos finitos nos plantea la siguiente pregunta:

Dado un grupo finito G, ¿existe una extensión de Galois $\mathbb{Q} \subseteq K$ tal que $Gal(K/\mathbb{Q}) = G$?

La solución a este problema no es, en general, conocida. Sin embargo, hay determinados casos en los que sabemos que la respuesta es afirmativa. Por ejemplo, en el caso de grupos resolubles o simétricos. Además, en Freid y Kollar [2] se puede ver que un grupo abeliano finito arbitrario se puede construir como el grupo de Galois de una extensión finita de $\mathbb{Q}$. Sin embargo, esta extensión no es, normalmente, de Galois.

Utilizando el Teorema de Kronecker-Weber, podemos asegurar que todo grupo abeliano finito es el grupo de Galois de cierta extensión de Galois sobre $\mathbb{Q}$. La demostración de este hecho se puede encontrar en las notas de E. Ghate [3]. Sin embargo, vamos a dar unos ejemplos que dan una idea de como se prueba el resultado.

Ejemplo. *En este ejemplo vamos a construir la extensión de Galois de $\mathbb{Q}$ que tiene como grupo de Galois al grupo*

$$G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

La idea es construir una extensión de Galois que contenga todos los factores cíclicos de G. Si podemos hacer esto de forma que estas extensiones sean

linealmente disjuntas, entonces habremos terminado puesto que podremos tomar la composición de estas extensiones y obtendremos el resultado.

Vamos a comenzar construyendo una extensión de Galois que tenga como grupo de Galois a $\mathbb{Z}/5\mathbb{Z}$*. El truco consiste en tomar un número primo* p *de forma que* $p \equiv 1 (\text{mód } 5)$*. El primer primo que verifica este hecho es* $p = 11$*. Consideramos ahora la extensión* $\mathbb{Q}(\xi_{11})/\mathbb{Q}$*. El siguiente teorema nos asegura que esta extensión de Galois tiene como grupo de Galois* $\mathbb{Z}/10\mathbb{Z}$*:*

Teorema. *Sea* $\varphi(n)$ *el cardinal de* $(\mathbb{Z}/n\mathbb{Z})^*$*. Entonces* $\mathbb{Q}(\xi_n)$ *es una extensión abeliana de* $\mathbb{Q}$ *de grado* $\varphi(n)$*. En concreto, hay un isomorfismo*

$$(\mathbb{Z}/n\mathbb{Z})^* \to Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$$

que envía $a (\text{mód } n)$ *a* σ_a*, donde* $\sigma_a(\xi_n) = \xi_n^a$*.*

Así, como $5 \mid 10$*, tenemos que* $\mathbb{Q}(\xi_{11})$ *tiene un subcuerpo* K_1 *que tiene como grupo de Galois* $\mathbb{Z}/5\mathbb{Z}$*.*

De manera similar podemos construir otra extensión $K_2/\mathbb{Q}$ *cuyo grupo de Galois es* $\mathbb{Z}/7\mathbb{Z}$*. Como antes, tenemos que encontrar un primo* p *tal que* $p \equiv 1 (\text{mód } 7)$*. Si elegimos* $p = 29$ *esto se verifica, luego, usando de nuevo el teorema tenemos que* $Gal(\mathbb{Q}(\xi_{29})/\mathbb{Q}) = \mathbb{Z}/28\mathbb{Z}$*. Como* $7 \mid 28$*, existe* K_2 *de forma que* $Gal(K_2/\mathbb{Q}) = \mathbb{Z}/7\mathbb{Z}$*.*

Para finalizar, como K_1 *y* K_2 *son disjuntos puesto que están en cuerpos ciclotómicos* $\mathbb{Q}(\xi_p)$ *con* p *distintos, tomando* $K = K_1K_2$ *tenemos que* $Gal(K/\mathbb{Q}) \cong G$ *y hemos terminado.*

Ejemplo. *En este ejemplo vamos a construir la extensión de Galois de* $\mathbb{Q}$ *que tiene como grupo de Galois a*

$$G = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}.$$

Vamos a comenzar construyendo una extensión de Galois que tenga como grupo de Galois a $\mathbb{Z}/7\mathbb{Z}$*. Como en el ejemplo anterior, tenemos que tomar un número primo* p *de forma que* $p \equiv 1 (\text{mód } 7)$*. El primer primo que verifica este hecho es* $p = 29$*. Consideramos ahora la extensión* $\mathbb{Q}(\xi_{29})/\mathbb{Q}$*. Por el teorema expuesto en el ejemplo anterior sabemos que esta extensión de Galois tiene como grupo de Galois* $\mathbb{Z}/28\mathbb{Z}$*. Si nos fijamos en el ejemplo anterior, este es el mismo cuerpo* K_2 *del ejemplo anterior.*

Además, como $7 \mid 28$*, tenemos que* $\mathbb{Q}(\xi_{29})$ *tiene un subcuerpo* K_1 *que tiene como grupo de Galois* $\mathbb{Z}/7\mathbb{Z}$*.*

Como antes, podemos construir otra extensión $K_2/\mathbb{Q}$ *cuyo grupo de Galois es* $\mathbb{Z}/13\mathbb{Z}$*. Como ya hemos hecho en el caso anterior, tenemos que encontrar un primo* p *tal que* $p \equiv 1 (\text{mód } 13)$*. Si elegimos* $p = 53$ *esto se verifica,*

luego, usando de nuevo el teorema tenemos que $Gal(\mathbb{Q}(\xi_{53})/\mathbb{Q}) = \mathbb{Z}/52\mathbb{Z}$. *Como* $13 \mid 52$, *existe* K_2 *de forma que* $Gal(K_2/\mathbb{Q}) = \mathbb{Z}/13\mathbb{Z}$.

Ya solo nos queda otro factor $\mathbb{Z}/13$. *No podemos volver a elegir* $p = 53$ *como antes, pues entonces tendríamos que* K_2 *y* K_3 *no serían disjuntos. Sin embargo, tomando* $p = 79$ *tenemos que* $79 \equiv 1 \pmod{13}$. *Así,* $Gal(\mathbb{Q}(\xi_{79})/\mathbb{Q}) = \mathbb{Z}/78\mathbb{Z}$. *Como* $13 \mid 78$, *existe* K_3 *de forma que* $Gal(K_3/\mathbb{Q}) = \mathbb{Z}/13\mathbb{Z}$.

Ahora bien, como K_1, K_2 *y* K_3 *son disjuntos puesto que están en cuerpos ciclotómicos* $\mathbb{Q}(\xi_p)$ *con* p *distintos, tomando* $K = K_1K_2K_3$ *tenemos que* $Gal(K/\mathbb{Q}) \cong G$, *concluyendo así el ejemplo.*

Ejemplo. *En este ejemplo vamos a encontrar la extensión* $K/\mathbb{Q}$ *tal que su grupo de Galois sea*

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

Vamos a comenzar buscando un cuerpo K_1 *que tenga como grupo de Galois a* $\mathbb{Z}/11\mathbb{Z}$.

Repitiendo el procedimiento de los ejercicios anteriores tenemos que encontrar un número primo p *de forma que* $p \equiv 1 \pmod{11}$. *Tomando* $p = 23$ *tenemos que esto se verifica. Por lo tanto, El grupo de Galois de la extensión* $\mathbb{Q}(\xi_{23})/\mathbb{Q}$ *es* $\mathbb{Z}/22\mathbb{Z}$. *Como* $11 \mid 22$ *tenemos que* $\mathbb{Q}(\xi_{23})$ *tiene un subcuerpo* K_1 *de forma que*

$$Gal(K_1/\mathbb{Q}) \cong \mathbb{Z}/11\mathbb{Z}.$$

Vamos a encontrar ahora los cuerpos que tengan como grupos de Galos a $\mathbb{Z}/2\mathbb{Z}$.

En el primero de todos los casos, tomamos $p = 3$, *donde se verifica que* $3 \equiv 1 \pmod{2}$. *Así, por el teorema del primer ejemplo tenemos que el grupo de Galois de la extensión* $\mathbb{Q}(\xi_3)/\mathbb{Q}$ *es* $\mathbb{Z}/2\mathbb{Z}$. *En este caso en particular,* $K_2 = \mathbb{Q}(\xi_3)$.

Ahora, tenemos que encontrar K_3 *de forma que su grupo de Galois también sea* $\mathbb{Z}/2\mathbb{Z}$, *pero no puede ser* $\mathbb{Q}(\xi_3)$ *porque si no,* K_2 *y* K_3 *no serían disjuntos. Tomando* $p = 5$ *tenemos que* $5 \equiv 1 \pmod{2}$, *luego el grupo de Galois de* $\mathbb{Q}(\xi_5)/\mathbb{Q}$ *es* $\mathbb{Z}/4\mathbb{Z}$ *y, como* $2 \mid 4$ *tenemos que* $\mathbb{Q}(\xi_5)$ *tiene un subcuerpo* K_3 *de forma que* $Gal(K_3/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Reiterando este procedimiento podemos encontrar $K_4 \subset \mathbb{Q}(\xi_7)$ *y* $K_5 \subset \mathbb{Q}(\xi_{11})$ *tales que* $Gal(K_4/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ *y* $Gal(K_5/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Como K_1, K_2, K_3, K_4 *y* K_5 *son disjuntos por estar en cuerpos ciclotómicos* $\mathbb{Q}(\xi_p)$ *con números* p *primos distintos, tomando* $K = K_1K_2K_3K_4K_5$ *tenemos que*

$$Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

Ejemplo. *En este último ejemplo vamos a encontrar la extensión K que tiene como grupo de Galois a*

$$G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}.$$

Vamos a comenzar buscando los cuerpos que tienen como grupo de Galois a $\mathbb{Z}/5\mathbb{Z}$.

Tomando $p = 11$ tenemos que $11 \equiv 1 (\text{mód } 5)$. Consideramos ahora la extensión $\mathbb{Q}(\xi_{11})/\mathbb{Q}$. Esta extensión de Galois tiene como grupo de Galois $\mathbb{Z}/10\mathbb{Z}$ y, como $5 \mid 10$, entonces existe un subcuerpo K_1 de $\mathbb{Q}(\xi_{11})$ tal que $Gal(K_1/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

Tomando ahora $p = 31$, tenemos que $31 \equiv 1 (\text{mód } 5)$ y que $\mathbb{Q}(\xi_{31})/\mathbb{Q}$ tiene como grupo de Galois $\mathbb{Z}/30\mathbb{Z}$. Como $5 \mid 30$, $\mathbb{Q}(\xi_{31})$ tiene un subcuerpo K_2 de forma que $Gal(K_2/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

Tenemos que repetir ahora el proceso para encontrar K_2 y K_3 que tengan como grupo de Galois a $\mathbb{Z}/17\mathbb{Z}$.

Para el primero de los factores, tomando $p = 103$, tenemos que $103 \equiv 1 (\text{mód } 17)$. Luego $Gal(\mathbb{Q}(\xi_{103})/\mathbb{Q} = \mathbb{Z}/102\mathbb{Z}$ y, como $17 \mid 102$ tenemos que $\mathbb{Q}(\xi_{103})$ tiene un subcuerpo K_3 de forma que $Gal(K_3/\mathbb{Q} \cong \mathbb{Z}/17\mathbb{Z}$.

Para el segundo factor, tomando $p = 137$, tenemos que $137 \equiv 1 (\text{mód } 17)$. Luego $Gal(\mathbb{Q}(\xi_{137})/\mathbb{Q} = \mathbb{Z}/136\mathbb{Z}$ y, como $17 \mid 136$ tenemos que $\mathbb{Q}(\xi_{136})$ tiene un subcuerpo K_4 de forma que $Gal(K_4/\mathbb{Q} \cong \mathbb{Z}/17\mathbb{Z}$.

Para finalizar, como todos los K_i, para $i = 1, \ldots, 4$, son disjuntos por estar en cuerpos ciclotómicos generados por una raíz p-ésima de la unidad con p primos distintos, tenemos que $K = K_1K_2K_3K_4$ y que

$$Gal(K/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}.$$

Bibliografía

[1] L. Culler, *The Kronecker-Weber Theorem*, http://www.math.uchicago.edu/~ may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Culler.pdf

[2] E. Fried and J. Kollar, *Automorphism groups of algebraic number fields*, Math Z. **165** (1978) Nº 2, 121-123.

[3] E. Ghate, *The Kronecker-Weber Theorem*, Summer School on Cyclotomic fields, Pune, June 7-30, 1999.

[4] D. Hilbert, *Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper* (en alemán), Nachrichten der Gesellschaft der Wissenschaften zu Göttingen : 29–39, 1896.

[5] C. Ivorra Castillo, *Teoría de cuerpos de Clases*, https://www.uv.es/ivorra/Libros/Cuerpos.pdf

[6] C. Ivorra Castillo, *Teoría de cuerpos de Números*, https://www.uv.es/ivorra/Libros/Numeros.pdf

[7] L. Kronecker, *Über die algebraisch auflösbaren Gleichungen* (en alemán), Berlin K. Akad. Wiss.: 365–374, Collected works volume 4, 1853.

[8] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, 1999.

[9] O. Neumann, *Two proofs of the Kronecker-Weber theorem according to Kronecker and Weber*, Journal für die reine und angewandte Mathematik 323: 105–126, 1981.

[10] N. H. Ordulu, *A simple proof of Kronecker-Weber Theorem*, http://wstein.org/129-05/final_papers/Nizameddin_Ordulu.pdf

[11] W. Stein, *Algebraic Number Theory, A Computational Approach*, http://wstein.org/books/ant/ant.pdf, 2012.

[12] I. Stewart y D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3^{rd} Edition, A. K. Peters, 2002.

[13] A. Travesa, *Cuerpos de Números*, 2005. En P. Bayer (coord.), *El Sueño de Juventud de Kronecker*: Notes del seminari de Teoría de Nombres (pp. 77-162). Barcelona: Universitat Politècnica de Catalunya, Universitat Autònoma de Barcelona y Universitat Politècnica de Barcelona.