USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Sobre o problema inverso de Galois para grupos abelianos finitos

Raquel Lago Fidalgo

Xullo, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Sobre o problema inverso de Galois para grupos abelianos finitos

Raquel Lago Fidalgo

Xullo, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Sobre o problema inverso de Galois para grupos abelianos finitos
Breve descrición do contido
O Problema Inverso de Galois é un problema non resolto. Na súa versión clásica o Problema Inverso de Galois consiste en dar resposta á pregunta: É calquera grupo finito o grupo de Galois dunha extensión finita do corpo dos números racionais? Presentaremos o Problema Inverso de Galois centrándonos na exposición da solución positiva ó problema no caso dos grupos abelianos finitos.
Recomendacións
Outras observacións

Índice

Resumo

O Problema Inverso de Galois, no seu enunciado clásico, trata de determinar para que grupos finitos G existe unha extensión de Galois sobre $\mathbb{Q}$ que teña grupo de Galois isomorfo a G. Neste traballo tratarase o caso particular no cal o grupo finito sexa ademais abeliano. A exposición do traballo divídese en dúas partes. Na primeira parte probarase que, no caso de grupos abelianos, sempre existe unha extensión que resolve o Problema Inverso de Galois. Na segunda parte demóstrase o Teorema de Kronecker-Weber, o cal establece que toda extensión de Galois de $\mathbb{Q}$ con grupo de Galois abeliano é unha extensión ciclotómica. Para os corpos ciclotómicos analizaremos a estrutura dos seus grupos de Galois sobre $\mathbb{Q}$. Ademais, introduciremos a teoría de corpos de números necesaria para a proba do Teorema de Kronecker-Weber, en concreto, presentarase o anel de enteiros dun corpo de números alxébricos, a factorización de ideais primos nunha extensión de corpos de números, así coma, os grupos de descomposición e inercia.

Abstract

The Inverse Galois Problem, in its classic formulation, asks whether given a finite group G there exists a Galois extension over $\mathbb{Q}$ whose Galois group is isomorphic to G. This work will address the special case in which the finite group is also abelian. The content of this paper is divided into two parts. In the first part we will prove that, if G is any finite abelian groups, then we can find a Galois extension of $\mathbb{Q}$ that solves the Inverse Galois Problem for G. In the second part we will prove the Kronecker-Weber Theorem, which states that if the Galois group of a Galois extension of $\mathbb{Q}$ is abelian then the extension is cyclotomic. For cyclotomic fields we study the structure of their Galois groups over $\mathbb{Q}$. Moreover, we will present some concepts of the theory of algebraic number fields that are necessary to prove the Kronecker-Weber Theorem. Specifically, we will introduce the ring of integers of an algebraic number field, the prime decomposition in extensions of number rings and the decomposition and inertia groups.

Introdución

Nos primeiros anos do século XIX desenvolveuse grazas ao traballo de Évariste Galois (1811-1832) a Teoría que leva o seu nome a cal emprega a teoría de grupos para estudar as solucións das ecuacións polinómicas con coeficientes nun corpo. Galois morreu novo, con só vinte anos, pero antes de morrer conseguiu probar que unha ecuación é resoluble por radicais se, e soamente se, o seu grupo de Galois é resoluble (os aspectos concernentes á biografía de Galois pódense consultar en [10]). Este feito mostra de forma clara a relación que establece a Teoría de Galois entre a teoría de grupos e as extensións de corpos. Pero ao mesmo tempo que aquela nova teoría permitía resolver antigos problemas tamén deu lugar a novas preguntas sendo unha delas o tema deste traballo o Problema Inverso de Galois.

Na actualidade o enunciado do Problema Inverso de Galois é moi xeral: Dado un corpo K e un grupo finito G, ¿existe unha extensión de Galois sobre K con grupo de Galois isomorfo a G? Ademais a resolución do Problema Inverso de Galois non só pretende saber se existe a devandita extensión senón tamén estudar como son tódalas extensións que teñan a G por grupo de Galois. Por exemplo é un tema de investigación moi activo a construción de polinomios, ou familias de polinomios, sobre o corpo base K que teñan a G como grupo de Galois. Unha das primeiras solucións, para un tipo de grupos concreto, deuna David Hilbert no ano 1892 ao probar que para os grupos simétricos S_n e alternados A_n sempre existe unha extensión sobre $\mathbb{Q}$ que resolve o problema. Pero o problema continua sen estar resolto, por exemplo, descoñécese a solución para o grupo de Mathieu $\mathbf{M}_{23}$ (pódese consultar en [4]).

Na súa versión clásica o Problema Inverso de Galois consiste en determinar a existencia dunha extensión de Galois sobre $\mathbb{Q}$ con grupo de Galois isomorfo a un grupo finito dado. O inicio do desenvolvemento da Teoría de Galois está ligado a resolución da versión clásica do problema. O estudo das extensións con grupo de Galois abeliano sitúanos no ano 1853 no cal Leopold Kronecker enunciou o teorema que agora se coñece coma o Teorema de Kronecker-Weber, este é a clave para a clasificación das extensións abelianas. O teorema estable que dada unha extensión abeliana $K|\mathbb{Q}$, existe un enteiro positivo n, e unha raíz primitiva n-ésima da unidade $\varepsilon_n \in \mathbb{C}$ de forma que K é un subcorpo do corpo ciclotómico $\mathbb{Q}(\varepsilon_n)$. Kronecker só o demostrou para

extensións cíclicas de grao unha potencia de dous.

En 1886, Wilhelm Eduard Weber publicou unha proba completa do teorema, pero a súa demostración presentaba erros os cales foron corrixidos a posterior por Olaf Neumann no ano 1981, e publicado en [7]. A primeira proba completa que non contiña erros do Teorema de Kronecker-Weber foi dada por David Hilbert en 1896.

Debido a gran importancia deste teorema deseguida comezaron a xurdir ideas sobre a súa posible xeneralización. Esta xeneralización é á que está dedicado o duodécimo problema de Hilbert, pertencente a lista dos 23 problemas abertos que presentou no Congreso Internacional de Matemáticas de París do ano 1900. Esta xeneralización amosa a posibilidade de estender o Teorema de Kronecker-Weber, enunciado sobre extensións abelianas con corpo base $\mathbb{Q}$, a extensións abelianas con calquera outro corpo base. É dicir, trátase de buscar análogos a ε_n que xeren toda unha familia de corpos de números os cales sexan análogos aos corpos ciclotómicos e os seus subcorpos. A xeneralización a corpos base arbitrarios do Teorema de Kronecker-Weber segue sendo na actualidade un problema aberto.

Neste traballo imos estudar o Problema Inverso de Galois para os grupos abelianos finitos centrando o noso interese na demostración do Teorema de Kronecker-Weber. A exposición divídese en dúas partes. A primeira parte ten coma finalidade probar a existencia dunha extensión ciclotómica sobre $\mathbb{Q}$ con grupo de Galois isomorfo a G, para todo grupo abeliano G. Comprenderá só o primeiro capítulo onde, despois de introducir as notacións e resultados básicos sobre grupos abelianos e extensións de Galois, estudaremos, para as extensión ciclotómicas, a estrutura dos seus grupos de Galois sobre $\mathbb{Q}$.

O obxectivo da segunda parte é probar o Teorema de Kronecker-Weber e introducir a teoría de corpos de números alxébricos necesaria para a proba. No capítulo segundo definiremos o concepto de anel de enteiros alxébricos dun corpo de números e veremos que este é un dominio de Dedekind. Tamén introduciremos a traza, a norma e o discriminante. O terceiro capítulo tratará sobre a factorización dos ideais primos non nulos nunha extensión de corpos de números. Ademais, definiremos o ideal diferente que nos permitirá estudar, xunto co discriminante, a ramificación dos ideais primos. Para rematar este capítulo, enunciaremos o Teorema de Minkowski o cal será imprescindible para a demostración do Teorema de Kronecker-Weber pero non incluiremos a proba do mesmo debido á súa complexidade, a cal supera os obxectivos deste traballo. Tamén omitiremos as demostracións dos resultados relacionados co ideal diferente. No cuarto capítulo definiremos, para as extensións de Galois, os grupos de descomposición e inercia, así coma, os grupos de ramificación. Finalmente demostraremos no quinto capítulo o Teorema de Kronecker-Weber.

Notacións

Neste traballo empregaremos a notación habitual: $\mathbb{N}$ para o conxunto dos números naturais, $\mathbb{Z}$ para o dos números enteiros, $\mathbb{Q}$ para o dos racionais, $\mathbb{R}$ para o dos reais e $\mathbb{C}$ para o dos complexos.

Todos os aneles consideramos serán aneles conmutativos e unitarios. Se $R = (R, +, \cdot)$ é un anel, representaremos por $R = (R, +)$ ao grupo aditivo de R e por $R^\times = (R^\times, \cdot)$ o grupo multiplicativo das unidades de R.

Se L é un corpo e $R \subseteq L$ un subanel, dado $\alpha \in L$ un elemento $R[\alpha] \subseteq L$ é o menor subanel de L que contén tanto a R coma ao elemento α. En cambio se $K = R$ é un corpo, $K(\alpha) \subseteq L$ é o menor subcorpo de L que contén a K e α.

Se $n \in \mathbb{N}$, denotaremos por $a(\mathrm{mod}\ n)$ ao elemento de $\mathbb{Z}/n\mathbb{Z}$ correspondente á clase de $a \in \mathbb{Z}$, e indicaremos con $b \equiv a\,(\mathrm{mod}\ n)$ que $b(\mathrm{mod}\ n) = a\,(\mathrm{mod}\ n)$, é dicir que $b - a$ é múltiplo de n, $b - a = \dot{n}$.

En xeral, dado un ideal $\mathfrak{a}$ do anel R, denotaremos por $R/\mathfrak{a}$ ao anel cociente, e os seus elementos por $a(\mathrm{mod}\ \mathfrak{a})$ con $a \in R$. Indicaremos con $b \equiv a\,(\mathrm{mod}\ \mathfrak{a})$ que $b(\mathrm{mod}\ \mathfrak{a}) = a\,(\mathrm{mod}\ \mathfrak{a})$, é dicir que $b - a \in \mathfrak{a}$.

Empregaremos as letras $\mathfrak{a}, \mathfrak{b}, \ldots$ para denotar ideais dun anel R, reservaremos as letras $\mathfrak{p}, \mathfrak{q}, \mathfrak{P}, \mathfrak{Q}, \ldots$ para aqueles ideais que sexan primos. O conxunto de tódolos ideais primos dun anel R denótase $\mathrm{Spec}(R)$, e o conxunto dos maximais $\mathrm{Spm}(R)$.

Capítulo 1

O problema inverso de Galois para grupos abelianos

Imos comezar coa primeira parte do noso traballo coa finalidade de probar que, para todo grupo abeliano finito, o Problema Inverso de Galois ten resposta afirmativa. As primeiras seccións están adicadas a introducir a notación e os resultados precisos para establecer e demostrar o resultado principal do capítulo, o Teorema 1.21, o cal establece que se G é un grupo abeliano finito entón é isomorfo ao grupo de Galois dunha extensión ciclotómica sobre $\mathbb{Q}$.

1.1. Grupos abelianos finitos

O estudo dos grupos abelianos é o estudo dos módulos sobre o anel $\mathbb{Z}$, o exemplo de anel mais sinxelo e prototipo dos dominios de ideais principais (DIP). Nesta sección recordaremos varios resultados sobre grupos abelianos finitamente xerados que non deixan de ser a particularización a $\mathbb{Z}$ dos coñecidos teoremas de clasificación de módulos finitamente xerados sobre un DIP.

Dado un natural $r \in \mathbb{N}$, dise que un grupo abeliano finitamente xerado é *un grupo libre de rango* r se é isomorfo a un grupo da forma $\mathbb{Z}^r = \mathbb{Z} \times \overset{r)}{\cdots} \times \mathbb{Z}$. Dicimos que un grupo abeliano G é finito cando ten unha cantidade finita n de elementos, o natural $|G| = n$ denomínase *orde do grupo* G.

Verifícanse as seguintes propiedades:

Proposición 1.1. *Se G é un grupo abeliano libre de rango r e $H < G$ é un subgrupo de G entón H é un grupo abeliano libre de rango menor ou igual ca r.*

Teorema 1.2 (Teorema Fundamental dos Grupos Abelianos Finitamente Xerados)**.** *Dado G un*

grupo abeliano finitamente xerado tense:

(*i*) *Existen naturais* $r, s \in \mathbb{N}$, *e enteiros* $d_i \geq 2$, *con* $i \in \{1, \ldots, s\}$, *tales que* $d_{i+1} \mid d_i$, *se* $1 \leq i \leq s-1$, *e un isomorfismo de grupos:*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}.$$

(*ii*) *A expresión anterior é única, é dicir se existe un isomorfismo de grupos*

$$G \cong \mathbb{Z}^{r'} \times \mathbb{Z}/d_1'\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{s'}'\mathbb{Z},$$

con $r', s' \in \mathbb{N}$, *e* $d_i' \geq 2$, *con* $i \in \{1, \ldots, s'\}$ *enteiros tales que* $d_{i+1}' \mid d_i'$ *para* $1 \leq i \leq s'-1$, *entón* $r' = r$, $s' = s$ *e* $d_i' = d_i$, $\forall i \in \{1, \ldots, s\}$.

Corolario 1.3. *Se* G *é un grupo abeliano finito entón* $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$, *sendo* $s \in \mathbb{N}$ *e, para cada* $i \in \{1, \ldots, s\}$, $d_i \geq 2$ *enteiros tales que* $d_{i+1} \mid d_i$, $\forall i \in \{1, \ldots, s-1\}$.

O seguinte resultado pódese deducir a partir anterior, en particular, son equivalentes.

Teorema 1.4. *Sexa* G *un grupo abeliano finito de orde* $n > 1$ *e sexa* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *a factorización en primos de* n, *entón:*

(*i*) *Existen grupos abelianos* $A_1, \ldots, A_k$ *tales que:*

- $G \cong A_1 \times \cdots \times A_k$,
- *para cada* $i \in \{1, \ldots, k\}$, $|A_i| = p_i^{\alpha_i}$ *e existen enteiros* $\beta_{i1} \geq \cdots \geq \beta_{it_i} \geq 1$ *e un isomorfismo*

$$A_i \cong \mathbb{Z}/p_i^{\beta_{i1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i^{\beta_{it_i}}\mathbb{Z}$$

os expoñentes $\beta_{i1} \geq \cdots \geq \beta_{it_i} \geq 1$, *tales que* $\beta_{i1} + \cdots + \beta_{it_i} = \alpha_i$, *están determinados de modo único por* A_i, *e denomínanse factores invariantes de* A_i.

(*ii*) *A descomposición en (i) é única no sentido de que se* $G \cong B_1 \times \cdots \times B_k$, *con* $|B_i| = p_i^{\alpha_i}$, *para cada* $i \in \{1, \ldots, k\}$, *entón* $B_i \cong A_i$ *e* B_i *e* A_i *teñen os mesmos factores invariantes.*

1.2. Extensións de Galois

Recordemos algunhas definicións e resultados básicos, que se poden consultar en [3].

Se K e L son corpos tales que $K \subset L$ e K é un subcorpo de L, dise que L é unha *extensión* de K, e represéntase mediante a expresión $L|K$. Neste caso, L é un K-espacio vectorial e a súa dimensión denomínase *grao da extensión*, denótase como $[L\colon K]$. Cando $[L\colon K] < \infty$ dise que a extensión é finita. As extensións pódense encadear sendo o grao é unha función multiplicativa.

Un elemento $\alpha \in L$ dise *alxébrico sobre* K se é un cero ou raíz dun polinomio non nulo $f \in K[\mathrm{X}]$; se $\alpha \in L$ é alxébrico sobre K existe un único polinomio mónico irredutible con coeficientes en K do cal α é raíz, denomínase o polinomio *irredutible de* α sobre K, e denótase $\mathrm{Irr}(\alpha, K)$. A extensión máis pequena que contén a K e a un elemento α denótase $K(\alpha)$. Que α sexa alxébrico sobre K equivale a que a extensión $K(\alpha)|K$ sexa finita, en tal caso o grao da extensión é $[K(\alpha)\colon K] = \partial(\mathrm{Irr}(\alpha, K))$, o cal xustifica o uso do termo *grao* para a dimensión do K-espacio vectorial. O *elemento* $\alpha \in L$ dise *separable* sobre K se é alxébrico e as raíces do polinomio $\mathrm{Irr}(\alpha, K)$ son todas distintas. Por exemplo, se K é un corpo de característica cero (e dicir, se contén a $\mathbb{Q}$), todo elemento alxébrico é separable sobre K.

Se dada a extensión $L|K$ todo elemento de L é alxébrico sobre K dise que a *extensión* $L|K$ é *alxébrica*. Se L é a extensión máis pequena de K que contén a un conxunto finito de elementos $\alpha_1, \ldots, \alpha_s \in L$ dise que a extensión $L|K$ é *finitamente xerada* e escríbese $L = K(\alpha_1, \ldots, \alpha_s)$. Unha extensión $L|K$ é finita se, e só se, é alxébrica e finitamente xerada, o cal equivale a que sexa finitamente xerada mediante elementos alxébricos.

Dada unha extensión alxébrica $L|K$ existe unha extensión $\overline{K}|L$ alxébrica tal que calquera polinomio no nulo $f \in \overline{K}[\mathrm{X}]$ ten tódalas súas raíces en $\overline{K}$, é dicir, podemos atopar en $\overline{K}$ tódalas solucións de calquera ecuación alxébrica non trivial con coeficientes en K, dise que o corpo $\overline{K}$ é un corpo alxebricamente pechado, e ademais é unha clausura alxébrica de K. O corpo dos números complexos $\mathbb{C}$ cumpre que $\overline{\mathbb{R}} = \mathbb{C}$, e $\overline{\mathbb{Q}} \subset \mathbb{C}$ é o conxunto de tódolos complexos alxébricos sobre $\mathbb{Q}$.

No caso no cal o polinomio $f \in K[\mathrm{X}]$ sexa irredutible, se α é unha solución da ecuación alxébrica $f(\mathrm{X}) = 0$, coñecer tódolos K-encaixes $\sigma\colon K(\alpha) \to \overline{K}$ é equivalente a coñecer tódalas solucións da ecuación $f(\mathrm{X}) = 0$, porque $\sigma(\alpha)$ son as solucións da ecuación $f(\mathrm{X}) = 0$. Dados $\alpha, \beta \in \overline{K}$, que $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$ é equivalente a que exista un K-isomorfismo $\sigma\colon K(\alpha) \to K(\beta)$ tal que $\sigma(\alpha) = \beta$, o cal é necesariamente único.

Se $L|K$ e $L'|K$ son extensións de corpos, os homomorfismos de corpos $\sigma\colon L \to L'$ tales que $\sigma|_K = \mathrm{id}_K$ denomínanse K-homomorfismos ou K-encaixes, por ser aplicacións inxectivas. Toda extensión $K \subset L$ ten asociado un grupo, o grupo dos K-automorfismos de L, $\mathrm{Aut}_K(L)$.

A estratexia para estudar a resolución dunha ecuación alxébrica $f(\mathrm{X}) = 0$ consiste en asociar ao polinomio f una extensión de corpos $E_{K,f}|K$, e estudar o seu grupo de automorfismos $\mathrm{Aut}_K(E_{K,f})$. A extensión $E_{K,f}|K$ é a minimal obtida engadindo a K tódalas raíces de f en $\overline{K}$; o corpo $E_{K,f}$ denomínase corpo de escisión de f sobre K. Este tipo de extensións finitas son *normais*:

Definición 1.5. Unha *extensión* alxébrica $L|K$ é *normal* se verifica as condicións equivalentes:

(i) Todo polinomio irredutible $g \in K[\mathrm{X}]$ que teña unha raíz en L escinde en L.

(*ii*) Para calquera K-encaixe $\sigma : L \longrightarrow \overline{L}$, $\sigma(L) = L$.

(*iii*) Existe un polinomio non nulo $f \in K[\mathrm{X}]$ tal que $L = E_{K,f}$.

Se unha extensión $E|K$ é normal, con $K \subseteq E \subseteq L$, e $\sigma\colon L \to L'$ é calquera K-encaixe entón $\sigma(E) = E$. Denotaremos $\sigma_E\colon E \to E$ ao K-automorfismo inducido pola restrición de σ.

Unha *extensión* alxébrica $E|K$ dise *separable* se todo elemento $\alpha \in E$ é separable sobre K. Que unha extensión $E|K$ sexa separable e finitamente xerada equivale a que sexa da forma $E = K(\beta)$ con $\beta \in E$ un elemento separable sobre K, o elemento β denomínase elemento primitivo da extensión $E|K$, isto é o *Teorema do elemento primitivo*, e ademais $[E\colon K] = \partial(f)$ sendo $f = \mathrm{Irr}(\beta, K)$. Tódalas extensións que empregaremos neste traballo serán separables. Para estas extensións existen tantos K-encaixes $\sigma\colon E \to \overline{E}$ como raíces ten o polinomio $f = \mathrm{Irr}(\beta, K)$ en $\overline{E}$, e dicir tantas como o grado da extensión $[E\colon K]$.

Se $E|K$ e unha extensión, o corpo fixo asociado a un subgrupo $H < \mathrm{Aut}_K(E)$ é o corpo intermedio $K \subseteq E^H \subseteq E$, definido pola expresión $E^H = \{\, \alpha \in E \,;\, \sigma(\alpha) = \alpha,\ \forall \sigma \in H \,\}$.

Definición 1.6. Unha extensión finita $E|K$ é de Galois se, denotando $G = \mathrm{Aut}_K(E)$, cúmprense as seguintes condicións equivalentes:

(*i*) $|\,\mathrm{Gal}_K(E)| = [E : K]$.

(*ii*) A extensión $E|K$ é normal e separable.

(*iii*) $K = E^G$.

Neste caso o grupo $\mathrm{Aut}_K(E)$ denomínase *grupo de Galois da extensión*, e denótase $\mathrm{Gal}_K(E)$.

O seguinte resultado é o Teorema fundamental de correspondencia da Teoría de Galois:

Teorema 1.7 (Teorema Fundamental de Correspondencia da Teoría de Galois)**.** *Se $E|K$ é unha extensión de Galois con grupo de Galois $G = \mathrm{Gal}_K(E)$. A correspondencia entre os subgrupos de G e as subextensións de $E|K$, que asigna a un subgrupo $H < G$ a subextensión $K \subseteq E^H \subseteq E$, é bixectiva e inverte as inclusións. Cada subextensión $E|F$, $K \subseteq F \subseteq E$, é de Galois e a correspondencia asígnalle o seu grupo de Galois $H = \mathrm{Gal}_F(E) < G$, e tense que $F = E^H$.*

Dado un subgrupo $H < G$, a extensión $K|E^H$ é normal se, e só se, H é un subgrupo normal de G, e neste caso $\mathrm{Gal}_K(E^H)$ é canonicamente isomorfo ao grupo G/H.

Definición 1.8. Unha *extensión abeliana* é unha extensión de Galois que ten grupo de Galois abeliano.

Se a extensión $E|K$ é abeliana, entón son abelianas as dúas subextensións intermedias en calquera cadea de corpos $K \subseteq F \subseteq E$.

Se $K \subseteq K_1, \ldots, K_s \subseteq L$ son extensións de corpos, denotase por $K_1K_2\cdots K_s$ ao corpo composición, é dicir o menor subcorpo de L que contén aos corpos K_i. Os seguintes resultados sobre a composición de corpos, relacionados coas definicións que acabamos de dar, resultaranos de utilidade.

Proposición 1.9. *Sexan $K_1|K$ e $K_2|K$ extensións finitas. Se $K_2|K$ é unha extensión de Galois entón $K_1K_2|K$ é unha extensión de Galois. Ademais, tense que $K_1 \cap K_2 = K$ se, e só se, $[K_1K_2\colon K] = [K_1\colon K][K_2\colon K]$.*

Demostración. Primeiro imos ver que como a extensión $K_2|K$ é de Galois entón $K_1K_2|K_1$ tamén o é, para isto imos probar que é normal. Coma $K_2|K$ é unha extensión normal finita tense que K_2 é o corpo de escisión sobre K dun polinomio non nulo $f \in K[\mathrm{X}]$, entón K_1K_2 é corpo de escisión sobre K_1 do polinomio $f \in K[\mathrm{X}] \subset K_1[\mathrm{X}]$, polo tanto $K_1K_2|K_1$ é unha extensión normal finita.

Ao ser $K_2|K$ normal, $\sigma(K_2) = K_2$ para calquera $\sigma \in \mathrm{Gal}_{K_1}(K_1K_2) \subset \mathrm{Gal}_K(K_1K_2)$; denotemos $\sigma_{K_2}\colon K_2 \to K_2$ ao K-automorfismo definido pola restrición de σ. A restrición define un homomorfismo de grupos

$$\begin{array}{rccc} \psi : G = \mathrm{Gal}_{K_1}(K_1K_2) & \longrightarrow & \mathrm{Gal}_K(K_2) \\ \sigma & \longmapsto & \sigma_{K_2} \end{array}$$

Vexamos que ψ é inxectiva:

$$\left.\begin{array}{lcl} \sigma \in G & \Longrightarrow & \sigma_{K_1} = \mathrm{id}_{K_1} \\ \sigma \in \mathrm{Ker}\,\psi & \Longrightarrow & \psi(\sigma) = \sigma_{K_2} = \mathrm{id}_{K_2} \end{array}\right| \Longrightarrow \sigma = \mathrm{id}_{K_1K_2}$$

Entón $G \cong \mathrm{Im}(\psi) < \mathrm{Gal}_K(K_2)$. A extensión $K_2|K$ é de Galois, calculemos o subcorpo de K_2 dos elementos fixos por $H := \mathrm{Im}(\psi)$:

$$\begin{aligned} K_2^H =& \{\, \alpha \in K_2\,;\, \tau(\alpha) = \alpha,\, \forall \tau \in H \,\} = \{\, \alpha \in K_2\,;\, \sigma_{K_2}(\alpha) = \alpha,\, \forall \sigma \in G \,\} = \\ =& \{\, \alpha \in K_2\,;\, \sigma(\alpha) = \alpha,\, \forall \sigma \in G \,\} = \{\, \alpha \in K_2\,;\, \alpha \in (K_1K_2)^G \,\} = K_2 \cap K_1, \end{aligned}$$

a última identidade tense por ser a extensión $K_1K_2|K_1$ de Galois con grupo de Galois G. Polo tanto $H = \mathrm{Gal}_{K_2\cap K_1}(K_2)$. Entón, tendo en conta que $H < \mathrm{Gal}_K(K_2)$ e que $|G| = |H|$, tense a equivalencia:

$$\begin{array}{rcccl} K_2 \cap K_1 = K & \Longleftrightarrow & \mathrm{Gal}_{K_2\cap K_1}(K_2) = \mathrm{Gal}_K(K_2) & \Longleftrightarrow & |H| = |\,\mathrm{Gal}_K(K_2)| \\ & \Longleftrightarrow & [K_1K_2\colon K_1] = [K_2\colon K] & \Longleftrightarrow & [K_1K_2\colon K] = [K_2\colon K][K_1\colon K]. \quad \square \end{array}$$

Proposición 1.10. *Se $K_1\,|\,K$ e $K_2\,|\,K$ son extensións de Galois entón $K_1K_2\,|\,K$ é unha extensión de Galois. Ademais o grupo $\mathrm{Gal}_K(K_1K_2)$ é isomorfo a un subgrupo de $\mathrm{Gal}_K(K_1) \times \mathrm{Gal}_K(K_2)$.*

Demostración. Para ver que a extensión $K_1K_2|K$ é de Galois é suficiente con ver que é normal. Consideremos $K \subseteq K_1K_2 \subseteq \overline{K}$, onde $\overline{K}$ é unha clausura alxébrica de K, entón dado un K-monomorfismo $\sigma : K_1K_2 \longrightarrow \overline{K}$ temos que $K_1K_2|K$ é normal se, e só se, $\sigma(K_1K_2) = K_1K_2$. Pero notemos o seguinte, $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2)$ e $K_1|K$ e $K_2|K$ son normais polo que $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = K_1K_2$.

Por ser cada unha das extensións $K_i|K$ normal, calquera K-automorfismo $\sigma \in \mathrm{Gal}_K(K_1K_2)$ restrínxese a un K-automorfismo $\sigma_{K_i} \colon K_i \to K_i$, de modo que a aplicación

$$\begin{aligned} \rho \colon \mathrm{Gal}_K(K_1K_2) &\longrightarrow \mathrm{Gal}_K(K_1) \times \mathrm{Gal}_K(K_2) \\ \sigma &\longmapsto (\sigma_{K_1}, \sigma_{K_2}) \end{aligned}$$

é un homomorfismo de grupos. O homomorfismo ρ é inxectivo. Tomemos $\sigma \in \mathrm{Ker}\,\rho$ e $\alpha \in K_1K_2$, temos que $\rho(\sigma) = (\sigma_{K_1}, \sigma_{K_2}) = (\mathrm{id}_{K_1}, \mathrm{id}_{K_2})$ e ademais $\alpha = \sum_{i=1}^{n} a_ib_i$ con $a_i \in K_1$ e $b_i \in K_2$, entón tense que $\sigma(\alpha) = \sum_{i=1}^{n} \sigma(a_i)\sigma(b_i) = \sum_{i=1}^{n} a_ib_i = \alpha$. Deste modo, $\sigma = \mathrm{id}_{K_1K_2}$ e ρ é inxectiva. Polo tanto $\mathrm{Gal}_K(K_1K_2) \cong \rho(\mathrm{Gal}_K(K_1K_2)) < \mathrm{Gal}_K(K_1) \times \mathrm{Gal}_K(K_2)$. □

Corolario 1.11. *Se $K_1|K$ e $K_2|K$ son extensións de abelianas entón $K_1K_2|K$ tamén o é.*

Demostración. O resultado séguese do encaixe de grupos ρ definido na proposición anterior. □

1.3. Corpos ciclotómicos

Nesta sección estudaremos as extensións de $\mathbb{Q}$ obtidas engadindo as solucións complexas da ecuación $\mathrm{X}^n - 1 = 0$, chamadas raíces n-ésimas da unidade, sendo n calquera número natural:

$$U(n) := \{\, \epsilon \in \mathbb{C}\,;\, \epsilon^n = 1 \,\}$$

O conxunto $U(n) \subset \mathbb{C}^\times = \mathbb{C} - \{0\}$ é un subgrupo finito de $(\mathbb{C}^\times, \cdot)$, o grupo multiplicativo do corpo dos complexos, entón é cíclico (o resultado que nos garante isto pódese ver en [3, Chapter 9, Proposition 18, p. 314]).

Cada un dos xeradores do grupo $U(n)$ denomínase raíz primitiva da unidade. Se $\varepsilon_n \in \mathbb{C}$ é unha raíz primitiva da unidade, e dicir se $U(n) = \langle \varepsilon_n \rangle$, entón $\mathbb{Q}(\varepsilon_n)$ é o corpo de escisión do polinomio $\mathrm{X}^n - 1$ sobre $\mathbb{Q}$, denomínase *corpo ciclotómico*, ou corpo ciclotómico n-ésimo. Entón $\mathbb{Q}(\varepsilon_n)|\mathbb{Q}$ é unha extensión de Galois de grao $[\mathbb{Q}(\varepsilon_n) \colon \mathbb{Q}] = \partial(\mathrm{Irr}(\varepsilon_n, \mathbb{Q}))$.

O grupo $(U(n), \cdot)$ é isomorfo ao grupo $(\mathbb{Z}/n\mathbb{Z}, +)$, entón o número de raíces n-ésimas distintas da unidade ven dado por lo valor do indicador de Euler en n,

$$\varphi(n) := |\{r \in \mathbb{N}\,;\, 1 \leq r \leq m, \text{ tal que } \mathrm{mcd}(n, r) = 1\,\}|,$$

é dicir, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ sendo $(\mathbb{Z}/n\mathbb{Z})^\times$ as unidades do anel $\mathbb{Z}/n\mathbb{Z}$.

Se $\varepsilon_n \in \mathbb{C}$ é unha raíz primitiva n-ésima da unidade entón o conxunto

$$\mathtt{P}_n := \{\, \varepsilon_n^r \,;\, r \in \mathbb{N},\, 1 \leq r \leq m,\ \text{e}\ \operatorname{mcd}(n,r) = 1 \,\}$$

é o conxunto de tódalas raíces primitivas n-ésimas da unidade. O polinomio

$$\Phi_n(\mathrm{X}) = \prod_{\varepsilon \in \mathtt{P}_n} (X - \varepsilon),$$

que ten por raíces exactamente tódalas raíces primitivas n-ésimas da unidade, é irredutible. Polo tanto $\Phi_n(\mathrm{X}) = \operatorname{Irr}(\varepsilon, \mathbb{Q})$, $\forall \varepsilon \in \mathtt{P}_n$. En particular a extensión ciclotómica $\mathbb{Q}(\varepsilon_n)|\mathbb{Q}$ ten grao $[\mathbb{Q}(\varepsilon_n)\colon \mathbb{Q}] = \partial(\Phi_n(\mathrm{X})) = \varphi(n)$.

O polinomio $\Phi_n(\mathrm{X})$ denomínase *polinomio ciclotómico n-ésimo*. Tendo en conta que o polinomio $\Phi_n(\mathrm{X})$ divide ó polinomio mónico $\mathrm{X}^n - 1 \in \mathbb{Z}[X]$ en $\mathbb{Q}[\mathrm{X}]$, polo Lema de Gauss [6, p.10], tense que $\operatorname{Irr}(\varepsilon_n, \mathbb{Q}) \in \mathbb{Z}[X]$. Ademais,

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

Neste traballo non só nos interesan os corpos ciclotómicos, senón tamén calquera dos seus subcorpos:

Definición 1.12. Unha extensión de corpos $K|\mathbb{Q}$ dise unha *extensión ciclotómica* se existe un enteiro $n > 0$ e unha raíz primitiva n-ésima da unidade $\varepsilon_n \in \mathbb{C}$, tal que $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\varepsilon_n)$.

O seguinte resultado será de utilidade.

Proposición 1.13. *A composición de corpos ciclotómicos é un corpo ciclotómico. De forma máis precisa, sendo n, $m > 0$ enteiros, $\mathbb{Q}(\varepsilon_n)\mathbb{Q}(\varepsilon_m) = \mathbb{Q}(\varepsilon_{\operatorname{mcm}(n,m)})$.*

Demostración. Resulta inmediato que $\mathbb{Q}(\varepsilon_n)\mathbb{Q}(\varepsilon_m) \subseteq \mathbb{Q}(\varepsilon_{\operatorname{mcm}(n,m)})$. Vexamos o outro contido, sabemos que $\operatorname{mcd}(n,m) = nm/\operatorname{mcm}(n,m)$ entón existen $a, b \in \mathbb{Z}$ tal que $an + bm = mn/\operatorname{mcm}(n,m)$, polo que, $a/m + b/n = 1/\operatorname{mcm}(n,m)$. Deste modo $\varepsilon_n^b \varepsilon_m^a = \varepsilon_{\operatorname{mcm}(n,m)}$, podendo concluír que $\mathbb{Q}(\varepsilon_{\operatorname{mcm}(n,m)}) \subseteq \mathbb{Q}(\varepsilon_n)\mathbb{Q}(\varepsilon_m)$. □

A continuación imos ver que as extensións ciclotómicas son abelianas. Para máis información sobre os definicións que acabamos de ver, e resultados asociadas a estas, pódese consultar en [3, §13.4 e §13.6].

Proposición 1.14. *Sexa $n \in \mathbb{N}$ e $\varepsilon_n \in \mathbb{C}$ unha raíz primitiva n-ésima da unidade. A extensión de Galois $\mathbb{Q}(\varepsilon_n)|\mathbb{Q}$ é unha extensión abeliana, máis precisamente o grupo de Galois $\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$ é isomorfo ao grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Demostración. Por ser ε_n unha raíz primitiva n-ésima da unidade, o conxunto de todas elas é $\mathtt{P}_n = \{\, \varepsilon_n^r \,;\, r \in \mathbb{N},\, 1 \leq r \leq m, e \operatorname{mcd}(n,r) = 1 \,\}$, as raíces do irredutible Φ_n. Deste modo, cada automorfismo $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$ está determinado de forma única pola imaxe de ε_n, $\sigma(\varepsilon_n) = \varepsilon_n^k \in \mathtt{P}_n$ e, neste caso, denotamos $\sigma_k = \sigma$. Tendo en conta que $\varepsilon_n^{k+n} = \varepsilon_n^k$, a expresión $\sigma_{\overline{k}} := \sigma_k$ está ben definida para cada clase $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Notemos que $(\sigma_{\overline{k}}\sigma_{\overline{r}})(\epsilon_n) = \sigma_{\overline{k}}(\varepsilon_n^r) = \varepsilon_n^{kr} = \sigma_{\overline{kr}}(\varepsilon_n)$, polo tanto a aplicación sobrexectiva

$$\begin{array}{rccc} \Psi_n : & (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n)) \\ & \overline{k} & \longmapsto & \sigma_{\overline{k}}. \end{array}$$

é un homomorfismo, de feito, é un isomorfismo de grupos. □

Como consecuencia da proposición anterior basta con estudar a estrutura de $(\mathbb{Z}/n\mathbb{Z})^\times$ para coñecer a de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$. Estudaremos en que casos o grupo das unidades, $(\mathbb{Z}/n\mathbb{Z})^\times$, é cíclico. Seguiremos a referencia [5].

Proposición 1.15. *Se p, $e > 0$ son enteiros e p é un primo impar, o grupo $(\mathbb{Z}/p^e\mathbb{Z})^\times$ é cíclico.*

Demostración. Para todo primo $p \in \mathbb{N}$, $\mathbb{Z}/p\mathbb{Z}$ é un corpo finito entón o seu grupo de unidades $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{0\}$ é cíclico. Polo tanto o caso $e = 1$ é certo. Supoñamos que $e > 1$. Para demostrar que $(\mathbb{Z}/p^e\mathbb{Z})^\times$ é cíclico o que imos facer é construír un elemento primitivo, empezaremos polo caso $e = 2$ e logo analizaremos o caso $e > 2$.

O grupo $(\mathbb{Z}/p\mathbb{Z})^\times$ é cíclico polo que podemos tomar $g \in \mathbb{Z}$ tal que $g \pmod p$ é un xerador de $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Como $\operatorname{mcd}(g,p) = 1$, $g \pmod{p^2} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$, calculemos k a súa orde. En primeiro lugar, como a orde de $(\mathbb{Z}/p^2\mathbb{Z})^\times$ é $\varphi(p^2) = p(p-1)$ sabemos que $k \mid p(p-1)$. Por outro lado, como $g^k \equiv 1 \pmod{p^2}$, temos que $g^k \equiv 1 \pmod p$ polo tanto $p-1 \mid k$, porque $g \pmod p$ ten orde $p-1$ en $(\mathbb{Z}/p\mathbb{Z})^\times$. Temos dúas posibilidades ou ben $k = p(p-1)$ ou ben $k = p-1$. No primeiro caso $g \pmod{p^2}$ é un xerador de $(\mathbb{Z}/p^2\mathbb{Z})^\times$. No segundo caso, cando $k = p-1$ tomemos $h = g+p$. Nótese que $h \pmod{p^2} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$, imos ver que $h \pmod{p^2}$ é un xerador de $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Como $h \equiv g \pmod p$ é un xerador de $(\mathbb{Z}/p\mathbb{Z})^\times$ polo tanto a súa orde en $(\mathbb{Z}/p^2\mathbb{Z})^\times$ é $p(p-1)$ ou $p-1$. Supoñamos que $h \pmod{p^2}$ ten orde $p-1$ en $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Pola fórmula do binomio temos que

$$h^{p-1} = (g+p)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} g^{p-1-i}p^i \equiv (1 - pg^{p-2}) \pmod{p^2},$$

como $p \nmid g$ temos que $pg^{p-2} \not\equiv 0 \pmod{p^2}$ polo tanto $p-1$ non pode ser a orde de $h \pmod{p^2}$. Así $h \pmod{p^2}$ é un xerador de $(\mathbb{Z}/p^2\mathbb{Z})^\times$.

Sea agora $e > 2$. Sabemos que existe $h \in \mathbb{Z}$ tal que $h \pmod{p^2}$ é un xerador de $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Supoñamos por hipótese de indución que $h \pmod{p^e}$ é un xerador de $(\mathbb{Z}/p^e\mathbb{Z})^\times$, e sexa k á orde de $h \pmod{p^{e+1}}$ en $(\mathbb{Z}/p^{e+1}\mathbb{Z})^\times$ sabemos que k divide a $\varphi(p^{e+1}) = p^e(p-1)$ e é divisible por

$\varphi(p^e) = p^{e-1}(p-1)$, entón, as posibilidades son $k = p^e(p-1)$ ou $p^{e-1}(p-1)$. Se $k = p^e(p-1)$ entón $h \pmod{p^{e+1}}$ é xerador de $(\mathbb{Z}/p^{e+1}\mathbb{Z})^\times$ e xa rematamos coa demostración. Supoñamos entón que $k = p^{e-1}(p-1)$. Como $h \pmod{p^e}$ é un xerador de $(\mathbb{Z}/p^e\mathbb{Z})^\times$, temos que $h^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$ pero $h^{\varphi(p^{e-1})} = h^{p^{e-2}(p-1)} \equiv 1 \pmod{p^{e-1}}$ entón sabemos que $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$ con $p \nmid k$. Podemos elevar a p ambos lados da igualdade e, pola fórmula do binomio,

$$h^{p^{e-1}(p-1)} = (1 + kp^{e-1})^p = 1 + \sum_{i=1}^{p} \binom{p}{i} (kp^{e-1})^i,$$

Agora ben, cando $i \geq 3$ tense que $(p^{e-1})^3 \mid (kp^{e-1})^i$ polo tanto, como $e \geq 2$ tense que $3(e-1) \geq e+1$, así que $p^{e+1} \mid (kp^{e-1})^i$ e polo tanto todos estes termos son nulos módulo p^{e+1}. Ademais coma p é un primo impar, o terceiro termo $\frac{1}{2}k^2p^{2e-1}(p-1)$ é un numero enteiro divisible por p^{e+1} porque $2e-1 \geq e+1$ ao ser $e \geq 2$. Entón $h^{p^{e-1}(p-1)} \equiv (1 + kp^e) \pmod{p^{e+1}}$. Como $p \nmid k$ chegamos a unha contradición, en consecuencia a orde de $h \pmod{p^{e+1}}$ é $k = p^e(p-1)$. □

Proposición 1.16. *Dado $e \geq 1$ un enteiro, o grupo $(\mathbb{Z}/2^e\mathbb{Z})^\times$ é cíclico se, e só se, $e = 1$ ou 2.*

Demostración. En primeiro lugar, os grupos $(\mathbb{Z}/2\mathbb{Z})^\times$ e $(\mathbb{Z}/2^2\mathbb{Z})^\times$ son cíclicos trivialmente. Imos ver que se $e > 2$ o grupo $(\mathbb{Z}/2^e\mathbb{Z})^\times$ non é cíclico. Para isto basta con probar que tódolos elementos teñen orde menor que $\varphi(2^e) = 2^{e-1}$, en concreto, imos ver que dado $a \in \mathbb{Z}$ impar $a^{2^{e-2}} \equiv 1 \pmod{2^e}$. Probemos isto por indución. Se $e = 3$ como podemos escribir $a = 2b+1$, con $b \in \mathbb{Z}$, temos que $a^2 = 4b(b+1)+1$, como uns dos valores b ou $b+1$ é par, concluímos que $a^2 \equiv 1 \pmod{2^3}$. Supoñamos que temos probado o resultado para un natural $e > 3$, imos ver que entón é certo para $e+1$. Por hipótese de indución $a^{2^{e-2}} = 1 + 2^e m$ para $m \in \mathbb{Z}$ entón, tomando cadrados

$$a^{2^{(e+1)-2}} = a^{2^{e-1}} = 1 + 2^{e+1}(m + 2^{e-1}m^2) \equiv 1 \pmod{2^{e+1}},$$

quedando así probado o que queríamos. □

Agora imos ver un caso no que o grupo $(\mathbb{Z}/n\mathbb{Z})^\times$ non é cíclico:

Lema 1.17. *Se $n = rs$ con $r, s > 2$ enteiros e $\mathrm{mcd}(r,s) = 1$, o grupo $(\mathbb{Z}/n\mathbb{Z})^\times$ non é cíclico.*

Demostración. Como $\mathrm{mcd}(r,s) = 1$, $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times$ e $\varphi(n) = \varphi(r)\varphi(s)$. Sendo $r, s > 2$, tense que $\varphi(r) \geq 2$ e $\varphi(s) \geq 2$ son pares. Entón existe un elemento de orde dous $a \pmod r \in (\mathbb{Z}/r\mathbb{Z})^\times$ e un elemento de orde dous $b \pmod s \in (\mathbb{Z}/r\mathbb{Z})^\times$. O grupo $(\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times$ non pode ser cíclico porque ten dous elementos distintos de orde dous, os elementos $(a \pmod r, 1 \pmod s)$ e $(1 \pmod r, b \pmod s)$. □

Con tódolos resultados anteriores podemos enunciar e demostrar o seguinte teorema:

Teorema 1.18. *O grupo* $(\mathbb{Z}/n\mathbb{Z})^\times$ *é cíclico se, e só se,* $n = 2$, 4, p^e *ou* $2p^e$, *onde* p, $e > 0$ *son enteiros e* p *un primo impar.*

Demostración. Primeiro probemos a implicación cara a esquerda. Os casos $n = 2, 4$ obtéñense da Proposición 1.16 e o caso $n = p^e$ da Proposición 1.15. Vexamos o caso $n = 2p^e$, sabemos que $(\mathbb{Z}/2p^e\mathbb{Z})^\times$ é un grupo de orde $\varphi(2p^e) = \varphi(p^e)$, para construír un xerador imos traballar con $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Pola Proposición 1.15 sabemos que existe $g \in \mathbb{Z}$ tal que $g \,(\mathrm{mod}\ p^e)$ é xerador de $(\mathbb{Z}/p^e\mathbb{Z})^\times$, ademais $(g+p^e)(\mathrm{mod}\ p^e)$ tamén é un xerador. Temos que, ou ben, g é impar ou $g+p^e$ é impar entón podemos tomar $h \in \mathbb{Z}$ que sexa impar e tal que $h(\mathrm{mod}\ p^e)$ tamén é un xerador de $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Deste modo, h é coprimo con 2 e p^e, é dicir, $h \,(\mathrm{mod}\ 2p^e) \in (\mathbb{Z}/2p^e\mathbb{Z})^\times$. Agora ben, se $h^i \equiv 1 \,(\mathrm{mod}\ 2p^e)$ entón $h^i \equiv 1 \,(\mathrm{mod}\ p^e)$ polo tanto i ten que dividir a $\varphi(p^e) = \varphi(2p^e)$ e polo tanto $h \,(\mathrm{mod}\ 2p^e)$ ten orde $\varphi(2p^e)$ podendo concluír así que $(\mathbb{Z}/2p^e\mathbb{Z})^\times$ é cíclico.

Probemos agora a outra implicación. Se o enteiro $n > 0$ non é da forma do enunciado, distínguense tres casos:

(*i*) $n = 2^e$ con $e > 2$,
(*ii*) $n = 2^e p^f$ con $e \geq 2$, $f \geq 1$ e p un primo impar,
(*iii*) $n = mp^f$ con $m > 1$, $m \neq 2^e$, p un primo impar tal que $p \nmid m$ e $f \geq 1$.

O caso (i) demostrouse na Proposición 1.16 e os casos (ii) e (iii) no Lema 1.17. □

1.4. Problema inverso de Galois para grupos abelianos finitos

Nesta sección, como aplicación dos resultados introducidos neste primeiro capítulo, probaremos que para todo grupo abeliano finito G o problema inverso de Galois ten resposta afirmativa e ademais veremos, na propia demostración, que non só existe unha extensión de Galois de $\mathbb{Q}$ con grupo de Galois isomorfo a G senón que a extensión de Galois pódese elixir ciclotómica.

O teorema de Dirichlet (1837) sobre progresións aritméticas establece que, se a e n son naturais coprimos entón hai infinitos primos na sucesión $\{\, a+n,\, a+2n,\, a+3n, \ldots \}$. Na proba do resultado central desta sección faremos uso do Teorema 1.19, que é o caso particular para $a = 1$ do Teorema de Dirichlet sobre progresións aritméticas, e o Lema 1.20 que é un resultado sinxelo sobre congruencias.

Teorema 1.19. *Dado un enteiro* $n > 0$, *existen infinitos primos* p *de modo que* $p \equiv 1 (\mathrm{mod}\ n)$.

Demostración. Supoñamos que non se cumpre o enunciado do teorema para o enteiro $n > 0$, deste modo, o conxunto $P = \{\, p \in \mathbb{N} \,/\, p$ é primo e $p \equiv 1(\mathrm{mod}\ n) \,\}$ é finito. Sendo $P = \{\, p_1, p_2, \ldots, p_r \,\}$, tomemos $m := \prod_{i=1}^{r} p_i$.

Consideremos agora o polinomio ciclotómico $\Phi_n = X^{\varphi(n)} + \cdots + a_1 X + a_0$; ao ser mónico existe un enteiro $k > 0$, suficientemente grande, de modo que $\Phi_n(knm) > 1$. Entón podemos tomar un primo $p \in \mathbb{N}$ tal que $p \,|\, \Phi_n(knm)$. Se $n > 1$, o termo independente de Φ_n é $a_0 = 1$, e no caso trivial $n = 1$, o termo independente é $a_0 = -1$. Necesariamente $p \nmid knm$ xa que, en caso contrario, como $p \mid \Phi_n(knm)$ e $\Phi_n(knm) = (knm)^{\varphi(n)} + \cdots + a_1(knm) + a_0$ teríamos que p divide a a_0, é dicir $p \mid 1$.

Deste modo, por ser p primo, como $p \nmid knm$ tense que $p \nmid m$, e que $\mathrm{mcd}(p, knm) = 1$. Polo tanto $p \notin P$, ademais $knm (\mathrm{mod}\ p) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Supoñamos demostrado que a orde de $knm (\mathrm{mod}\ p) \in (\mathbb{Z}/p\mathbb{Z})^\times$ é n. Entón, polo teorema de Lagrange, temos que $n \,|\, p-1$, é dicir $p \equiv 1 (mod\ n)$. Isto contradí que $p \notin P$ e necesariamente o conxunto P é infinito.

Completemos a demostración xustificando que n é a orde do elemento $knm (\mathrm{mod}\ p) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Consideremos o polinomio $f(X) = X^n - 1$. Avaliando en knm a expresión polinómica en $\mathbb{Z}[X]$

$$f(X) = \prod_{1 \le d \le n,\ d \mid n} \Phi_d(X),$$

e tendo en conta que $p \mid \Phi_n(knm)$, dedúcese que $p | f(kmn)$; sendo $f(knm) = (kmn)^n - 1$ tense $(kmn)^n \equiv 1 (\mathrm{mod}\ p)$. Sexa r a orde do elemento $knm (\mathrm{mod}\ p) \in (\mathbb{Z}/p\mathbb{Z})^\times$, polo anterior, sabemos que $r \le n$ *e* $r | n$. Denotemos por $\overline{a} = a (\mathrm{mod}\ p)$ aos elementos do anel $\mathbb{Z}/p\mathbb{Z}$ e por $\overline{g}(X) \in \frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ á imaxe dun polinomio $g(X) \in \mathbb{Z}[X]$ polo homomorfismo canónico $\mathbb{Z}[X] \to \frac{\mathbb{Z}}{p\mathbb{Z}}[X]$. Imos ter que $\overline{f}(X) = X^n - \overline{1} \in \frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ é separable. Se $\overline{\alpha}$ é unha raíz de $\overline{f}$ temos que $\overline{\alpha}^n - \overline{1} = 0$ e se fora múltiple $\overline{f}'(\overline{\alpha}) = \overline{n}\,\overline{\alpha}^{n-1} = \overline{0}$. Deste modo, como $p \nmid n$, $\overline{\alpha}^n = \overline{\alpha}^{n-1}\overline{\alpha} = \overline{0}$ o cal contradí que $\overline{\alpha}^n = \overline{1}$.

Sabemos que $\overline{kmn}$ é unha raíz de $\overline{\Phi}_n$ en $\mathbb{Z}/p\mathbb{Z}$ debido a que $p \,|\, \Phi_n(knm)$ o cal equivale a $\overline{\Phi}_n(\overline{kmn}) = \overline{0}$ en $\mathbb{Z}/p\mathbb{Z}$. Se ademais supoñemos que $r < n$, teríamos que $(kmn)^r \equiv 1 (\mathrm{mod}\ p)$, é dicir, $(\overline{kmn})^r - \overline{1} = \overline{0}$, e $\overline{kmn} \in \mathbb{Z}/p\mathbb{Z}$ sería unha raíz de $\overline{X^r - 1} = \prod_{1 \le d \le r,\ d \mid r} \overline{\Phi_d}(X)$. Deste modo, $\overline{knm}$ sería unha raíz de $\overline{\Phi_n}$ e de $\overline{\Phi_d}$ para un natural d tal que $1 \le d \le r$ *e* $d | r$. Entón, como $r | n$, $\overline{knm}$ sería unha raíz múltiple de $\overline{f}(X) = \prod_{1 \le d \le n,\ d \mid n} \overline{\Phi}_d(x)$ e chegamos a unha contradición. Conclusión $r = n$. □

Lema 1.20. *Sexan d, $p \in \mathbb{Z}$, con $p > 1$ un primo de modo que $p \equiv 1 (\mathrm{mod}\ \ d)$. Entón a asignación $\mathtt{g}(a+(p-1)\mathbb{Z}) = a+d\mathbb{Z}$ define un homomorfismo de grupos sobrexectivo $\mathtt{g}\colon \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$.*

Demostración. Obsérvese que a condición $p \equiv 1 (\mathrm{mod}\ d)$ equivale a $p - 1 \equiv 0 (\mathrm{mod}\ d)$. Entón $(p-1)\mathbb{Z} \subset d\mathbb{Z}$ e deste modo temos o seguinte diagrama conmutativo, onde `i`, `j` e `k` son as inclusións naturais e tanto `p` como `q` son os homomorfismos sobrexectivos canónicos de paso ó

cociente,

$$\begin{array}{ccccc} (p-1)\mathbb{Z} & \xhookrightarrow{\mathtt{j}} & \mathbb{Z} & \xrightarrow{\mathtt{p}} & \mathbb{Z}/(p-1)\mathbb{Z} \\ \downarrow{\scriptstyle \mathtt{i}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathtt{g}} \\ d\mathbb{Z} & \xhookrightarrow{\mathtt{k}} & \mathbb{Z} & \xrightarrow{\mathtt{q}} & \mathbb{Z}/d\mathbb{Z} \end{array}$$

entón $\mathtt{g}$ é unha aplicación ben definida e é un homomorfismo sobrexectivo de grupos. □

Cos resultados anteriores podemos proceder a demostrar o resultado central deste capítulo:

Teorema 1.21. *Todo grupo abeliano finito é isomorfo ao grupo de Galois dunha extensión de Galois sobre $\mathbb{Q}$ que é unha extensión ciclotómica.*

Demostración. Sexa G un grupo abeliano finito. Polo teorema de clasificación dos grupos abelianos finitos (Corolario 1.3), G es isomorfo a un grupo da forma $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$, con $d_1, \ldots, d_s > 1$ enteiros de modo que $d_s \,|\, d_{s-1} \,|\, \cdots \,|\, d_1$. Sexa $\mathtt{h}\colon \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z} \longrightarrow G$ un isomorfismo de grupos.

O Teorema 1.19 garante a existencia de primos distintos $p_1, \ldots, p_s \in \mathbb{Z}$ de modo que $p_i \equiv 1 (\mathrm{mod}\ d_i)$, $\forall i \in \{1, \ldots, s\}$. O Lema 1.20 establece a existencia de homomorfismos canónicos sobrexectivos $\mathtt{g}_i : \mathbb{Z}/(p_i - 1)\mathbb{Z} \longrightarrow \mathbb{Z}/d_i\mathbb{Z}$, con $i \in \{1, \ldots, s\}$. Deste modo, tomando o produto $\mathtt{g} := \mathtt{g}_1 \times \cdots \times \mathtt{g}_s$, obtemos un homomorfismo sobrexectivo:

$$\mathbb{Z}/(p_1 - 1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_s - 1)\mathbb{Z} \xrightarrow{\mathtt{g}} \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}.$$

Ademais sabemos que os grupos das unidades $(\mathbb{Z}/p_i\mathbb{Z})^\times$ son grupos cíclicos de orde $\varphi(p_i) = p_i - 1$ e polo tanto temos isomorfismos $\mathtt{r}_i\colon ((\mathbb{Z}/p_i\mathbb{Z})^\times, \cdot) \to (\mathbb{Z}/(p_i - 1)\mathbb{Z}, +)$. Tomando o produto temos un isomorfismo $\mathtt{r} := \mathtt{r}_1 \times \cdots \times \mathtt{r}_s$,

$$(\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^\times \xrightarrow{\mathtt{r}} \mathbb{Z}/(p_1 - 1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_s - 1)\mathbb{Z}.$$

Por outro lado, polo teorema chino dos restos, [3, p. 265], como $p_1, \ldots, p_s$ son primos distintos, se $n = p_1 \cdots p_s$, o homomorfismo canónico de aneis

$$\mathtt{v}\colon \mathbb{Z} \longrightarrow \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s\mathbb{Z}$$

é sobrexectivo e define un isomorfismo de aneis $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s\mathbb{Z}$, que establece un isomorfismo entre os correspondentes grupos de unidades

$$\mathtt{u} = \mathtt{v}^\times\colon (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^\times.$$

Entón temos un diagrama de homomorfismos de grupos:

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\mathtt{u}} \prod_{i=1}^{s}(\mathbb{Z}/p_i\mathbb{Z})^\times \xrightarrow{\mathtt{r}} \prod_{i=1}^{s}\mathbb{Z}/(p_i-1)\mathbb{Z} \xrightarrow{\mathtt{g}} \prod_{i=1}^{s}\mathbb{Z}/d_i\mathbb{Z} \xrightarrow{\mathtt{h}} G.$$

A composición $\mathtt{t}\colon (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow G$ dos homomorfismos do diagrama é un homomorfismo sobrexectivo. Entón se $T := \mathrm{Ker}(\mathtt{t})$ temos que $(\mathbb{Z}/n\mathbb{Z})^\times/T \cong G$, deste modo para demostrar o teorema basta atopar unha extensión de Galois de $\mathbb{Q}$ con grupo de Galois isomorfo a $(\mathbb{Z}/n\mathbb{Z})^\times/T$.

En primeiro lugar pola Proposición 1.14 sabemos que $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$. Consideremos o subgrupo $H < \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$ correspondente ao subgrupo $T < (\mathbb{Z}/n\mathbb{Z})^\times$ polo isomorfismo $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$. A extensión $\mathbb{Q}(\varepsilon_n)\,|\,\mathbb{Q}$ é de Galois, entón sabemos, polo Teorema fundamental de correspondencia da teoría de Galois (Teorema 1.7), que ao subgrupo $H < \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$ correspóndelle a subextensión $\mathbb{Q} \subset \mathbb{Q}(\varepsilon_n)^H \subset \mathbb{Q}(\varepsilon_n)$ de xeito que $\mathrm{Gal}_{\mathbb{Q}(\varepsilon_n)^H}(\mathbb{Q}(\varepsilon_n)) = H$. Ademais, H é un subgrupo normal de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$, por ser $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))$ abeliano, e polo tanto a extensión $\mathbb{Q}(\varepsilon_n)^H|\mathbb{Q}$ é de Galois e o seu grupo de Galois $\mathrm{Gal}_{\mathbb{Q}}\left(\mathbb{Q}(\varepsilon_n)^H\right)$ é isomorfo a $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))/H$ e polo tanto a G:

$$\mathrm{Gal}_{\mathbb{Q}}\left(\mathbb{Q}(\varepsilon_n)^H\right) \cong \frac{\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_n))}{H} \cong \frac{(\mathbb{Z}/n\mathbb{Z})^\times}{T} \cong G. \qquad \square$$

Capítulo 2

O anel de enteiros dun corpo de números

Neste capítulo introduciremos a teoría de corpos de números necesaria para a demostración do Teorema de Kronecker-Weber que realizaremos no quinto capítulo. Comezaremos coas definicións básicas.

Definición 2.1. Un *corpo de números*, ou *corpo de números alxébricos*, é calquera subcorpo $K \subseteq \mathbb{C}$ tal que a extensión $K|\mathbb{Q}$ é finita.

Definición 2.2. Dado un número complexo, $\alpha \in \mathbb{C}$, dicimos que α é un *enteiro alxébrico* se existe un polinomio mónico $f \in \mathbb{Z}[X]$ de modo que $f(\alpha) = 0$.

Na definición anterior non pedimos que f sexa irredutible pero no caso de pedilo a definición sería equivalente:

Proposición 2.3. *Un elemento $\alpha \in \mathbb{C}$ é un enteiro alxébrico se, e só se,* $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$.

Demostración. Se $f \in \mathbb{Z}[X]$ é tal que $f(\alpha) = 0$, entón $\mathrm{Irr}(\alpha, \mathbb{Q})$ divide a f en $\mathbb{Q}[X]$, e sendo $f \in \mathbb{Z}[X]$ mónico, tense que $\mathrm{Irr}(\alpha, \mathbb{Q})$ ten coeficientes enteiros, polo Lema de Gauss [6, p.10]. □

Pódese definir un enteiro alxébrico coma aquel $\alpha \in \mathbb{C}$ que é "alxébrico sobre $\mathbb{Z}$" e o polinomio $\mathrm{Irr}(\alpha, \mathbb{Z})$ é mónico. Existen outros enunciados equivalentes. En [6, p.11] pódese atopar:

Teorema 2.4. *Para $\alpha \in \mathbb{C}$, equivalen:*

(*i*) *O elemento α é un enteiro alxébrico.*

(*ii*) *O anel $\mathbb{Z}[\alpha]$ é un $\mathbb{Z}$-módulo finitamente xerado.*

(*iii*) *O elemento α pertence a algún $\mathbb{Z}$-submódulo de $\mathbb{C}$ finitamente xerado.*

(*iv*) *Existe un $\mathbb{Z}$-módulo finitamente xerado M, que é non nulo, tal que $\alpha M \subseteq M$.*

Corolario 2.5. *O conxunto de enteiros alxébricos forman un anel.*

Demostración. Tomemos $\alpha, \beta \in \mathbb{C}$ enteiros alxébricos entón probemos que $\alpha+\beta$ e $\alpha\beta$ tamén son enteiros alxébricos. Dados α e β temos que $\mathbb{Z}[\alpha]$ e $\mathbb{Z}[\beta]$ son $\mathbb{Z}$-módulos finitamente xerados. Se $\alpha_1, \cdots, \alpha_n$ e $\beta_1, \cdots, \beta_m$ son xeradores de $\mathbb{Z}[\alpha]$ e $\mathbb{Z}[\beta]$ respectivamente, o conxunto de elementos $\alpha_i\beta_j$, con $1 \leq i \leq n$, $1 \leq j \leq m$ xera $\mathbb{Z}[\alpha, \beta]$. Como $\alpha + \beta$ e $\alpha\beta$ pertencen a $\mathbb{Z}[\alpha, \beta]$ temos que están nun $\mathbb{Z}$-submódulo de $\mathbb{C}$ e rango finito e queda probado o que queríamos. □

Definición 2.6. Dado K un corpo de números chamamos *anel de enteiros de K* ao anel formado polos enteiros alxébricos que están en K, o denotamos por $\mathcal{O}_K$.

Os conceptos que acabamos de definir pódense xeneralizar a un anel R contido nun corpo L: Un elemento $\alpha \in L$ dise enteiro sobre R se existe un polinomio $f \in R[X]$ mónico que ten a α coma raíz. ; chámase clausura íntegra de R en L ao conxunto de elementos de L que son enteiros sobre R. Pódese atopar máis información sobre isto en [8, Chapter 2].

Observación 2.7. Trivialmente $\mathcal{O}_K \subseteq \mathcal{O}_L$, para calquera extensión de corpos de números $L|K$. As únicas raíces racionais dun polinomio mónico con coeficientes en $\mathbb{Z}$ son raíces enteiras. É dicir, os únicos elementos de $\mathbb{C}$ que son *enteiros alxébricos de* $\mathbb{Q}$ son os números enteiros: $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$. Por iso xeneralízase a denominación de "enteiro" entre os racionais, á da "enteiro alxébrico" cando traballamos cunha extensión alxébrica $K|\mathbb{Q}$.

Para rematar esta sección imos calcular o anel de enteiros dun corpo cadrático.

Proposición 2.8. *Para unha extensión de corpos $\mathbb{Q}(\sqrt{n})|\mathbb{Q}$, con n libre de cadrados, verifícase:*

(*i*) *Se $n \equiv 2, 3 \pmod 4$, entón $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]$*

(*ii*) *Se $n \equiv 1 \pmod 4$, entón $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$*

Demostración. Se $\alpha \in \mathbb{Q}(\sqrt{n})$ tense que $\alpha = a + b\sqrt{n}$, con $a, b \in \mathbb{Q}$, e $\mathrm{Irr}(\alpha, \mathbb{Q}) = x^2 - 2ax + a^2 - nb^2$ cando $b \neq 0$. Pola Proposición 2.3, sabemos que $\alpha \in \mathcal{O}_{\mathbb{Q}}(\sqrt{n})$ se, e só se, $2a$ e $a^2 - nb^2$ pertencen a $\mathbb{Z}$. Entón se $2a, a^2 - nb^2 \in \mathbb{Z}$ temos que $4nb^2 \in \mathbb{Z}$ e, como n está libre de cadrados, $2b \in \mathbb{Z}$. Agora ben, $4(a^2 - nb^2) = (2a)^2 - n(2b)^2 \equiv 0 (\mathrm{mod}\ 4)$ e necesariamente tense $(2a)^2 (\mathrm{mod}\ 4) = (2b)^2 (\mathrm{mod}\ 4) = 0 (\mathrm{mod}\ 4)$ ou $(2a)^2 (\mathrm{mod}\ 4) = (2b)^2 (\mathrm{mod}\ 4) = n (\mathrm{mod}\ 4) = 1 (\mathrm{mod}\ 4)$, porque dado $m \in \mathbb{Z}$ tense $m^2 \equiv 0, 1 (\mathrm{mod}\ 4)$.

Se estamos no caso (i) a única posibilidade é que $(2a)^2 = (2b)^2 \equiv 0 (\mathrm{mod}\ 4)$ polo tanto $a, b \in \mathbb{Z}$ e $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]$. Se estamos no caso (ii) pode ocorre coma antes que $(2a)^2 = (2b)^2 \equiv 0 (\mathrm{mod}\ 4)$

ou que $(2a)^2(\text{mod } 4) = (2b)^2(\text{mod } 4) = 1(\text{mod } 4)$. No último caso teríamos que $2a$ e $2b$ son impares, é dicir, $2a - 2b$ é par, séguese que

$$a + b\sqrt{n} = a - b + b - b\sqrt{n} = \frac{2a - 2b}{2} + 2b\frac{1 + \sqrt{n}}{2} \in \mathbb{Z}[\frac{1 + \sqrt{n}}{2}]$$

en consecuencia $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$. □

Máis adiante calcularemos o anel de enteiros dun corpo ciclotómico pero antes precisamos introducir varios conceptos, comezaremos pola noción de traza e norma na seguinte sección.

2.1. A traza e a norma

Sexa $L|K$ unha extensión de corpos de números de grao $n = [L\colon K]$. O número de K-encaixes, e dicir de K-homomorfismos, de L en $\mathbb{C}$ é n, e a partir de eles podemos definir a norma e traza dun elemento de L coma segue. (Pódese consultar máis sobre isto en [6].)

Definición 2.9. Sexan $\sigma_1, \cdots, \sigma_n$ os n K-encaixes de L en $\mathbb{C}$, entón dado $\alpha \in L$:

- $\mathrm{T}_K^L(\alpha) := \sum_{i=1}^n \sigma_i(\alpha)$ denomínase traza de α respecto a extensión $L|K$.
- $\mathrm{N}_K^L(\alpha) := \prod_{i=1}^n \sigma_i(\alpha)$ denomínase norma de α respecto a extensión $L|K$.

Se $\alpha \in \mathbb{C}$ é un elemento alxébrico sobre K definimos:

- $\mathrm{t}_K(\alpha) := \mathrm{T}_K^{K(\alpha)}(\alpha)$,
- $\mathrm{n}_K(\alpha) := \mathrm{N}_K^{K(\alpha)}(\alpha)$.

Nótese que estes valores corresponden, respectivamente, a suma e o produto das raíces do polinomio $\mathrm{Irr}(\alpha, K)$.

Se a extensión é $L|\mathbb{Q}$ entón as denotamos por $\mathrm{T}^L(\alpha) := \mathrm{T}_{\mathbb{Q}}^L(\alpha)$ e $\mathrm{N}^L(\alpha) := \mathrm{T}_{\mathbb{Q}}^L(\alpha)$, ou como $\mathrm{T}(\alpha)$ e $\mathrm{N}(\alpha)$ se non existe ambigüidade. Para $\alpha \in \mathbb{C}$ un elemento alxébrico sobre $\mathbb{Q}$ escribimos

- $\mathrm{t}(\alpha) := \mathrm{t}_{\mathbb{Q}}(\alpha) = \mathrm{T}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)$,
- $\mathrm{n}(\alpha) := \mathrm{n}_{\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)$.

Proposición 2.10. *Nas condicións da definición anterior, dados $\alpha, \beta \in L$:*

- $\mathrm{T}_K^L(\alpha + \beta) = \mathrm{T}_K^L(\alpha) + \mathrm{T}_K^L(\beta)$,
- $\mathrm{N}_K^L(\alpha + \beta) = \mathrm{N}_K^L(\alpha)\,\mathrm{N}_K^L(\beta)$.

Demostración. Resulta inmediato a partir da definición de traza e norma. □

Proposición 2.11. *Se $L|K$ é unha extensión finita con $[L\colon K] = m$, e $\alpha \in L$ é tal que $d = [K(\alpha)\colon K]$, entón:*

- $\mathrm{T}_K^L(\alpha) = \frac{m}{d}\,\mathrm{t}_K(\alpha)$,
- $\mathrm{N}_K^L(\alpha) = (\mathrm{n}_K(\alpha))^{\frac{m}{d}}$.

Demostración. Basta con notar que $\frac{m}{d} = [L\colon K(\alpha)]$, polo tanto cada encaixe de $K(\alpha)$ en $\mathbb{C}$ que deixe fixo K pódese estender a $\frac{m}{d}$ encaixes de L en $\mathbb{C}$ que deixen fixo K. □

Corolario 2.12. *Dada unha extensión de corpos de números $L|K$ e un elemento $\alpha \in L$:*

(*i*) $\mathrm{T}_K^L(\alpha)$ *e* $\mathrm{N}_K^L(\alpha)$ *pertencen a* K.

(*ii*) *Se* $\alpha \in \mathcal{O}_L$ *entón* $\mathrm{T}_K^L(\alpha)$ *e* $\mathrm{N}_K^L(\alpha)$ *pertencen a* $\mathcal{O}_K$.

Demostración. Grazas a proposición anterior para demostrar (i) basta con observar que $\mathrm{t}_K(\alpha)$ e $\mathrm{n}_K(\alpha)$ son elementos de K e isto cúmprese porque $-\mathrm{t}_K(\alpha)$ e, salvo o signo, $\mathrm{n}_K(\alpha)$ son, respectivamente, o segundo termo e o termo independente do polinomio $\mathrm{Irr}(\alpha, K) = (X-\alpha_1)\cdots(X-\alpha_d)$, onde α_i son as raíces do irredutible. Para probar (ii) chega con comprobar que se $\alpha \in \mathcal{O}_L$ a $\mathrm{t}_K(\alpha)$ e $\mathrm{n}_K(\alpha)$ son enteiros alxébricos. Como $\alpha \in \mathcal{O}_L$ tense que $g = \mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$, ademais se $f = \mathrm{Irr}(\alpha, K)$ este divide a g en $K[X]$, polo tanto tódalas raíces de f, $\alpha_1, \ldots, \alpha_d$, son enteiros alxébricos e obtemos o resultado. □

No caso de que teñamos unha torre de corpos $K \subseteq L \subseteq M$ podemos relacionar a traza e norma das distintas extensións da seguinte forma:

Teorema 2.13. *Sexan $M|L$ e $L|K$ extensións de corpos de números. Dado $\alpha \in M$ tense:*

(*i*) $\mathrm{T}_K^L(\mathrm{T}_L^M(\alpha)) = \mathrm{T}_K^M(\alpha)$

(*ii*) $\mathrm{N}_K^L(\mathrm{N}_L^M(\alpha)) = \mathrm{N}_K^M(\alpha)$

Demostración. A proba pódese consultar en [6, Theorem 5, Chapter 2]. □

A definición de traza e norma que acabamos de dar pódese xeneralizar a un anel S e un subanel R que cumpran que S é un R-módulo libre de rango finito, para ver as definicións e máis información sobre isto pódese consultar en [8, Chapter 2].

2.2. O Discriminante

O discriminante vai ser indispensable para a demostración do Teorema de Kronecker-Weber nun caso concreto, imos definilo nesta sección pero non será ata o próximo capítulo onde veremos a súa utilidade.

Definición 2.14. Sexa K un corpo de números de grao $[K\colon \mathbb{Q}] = n$, denotemos por $\sigma_1, \ldots, \sigma_n$ os n encaixes, e dicir, $\mathbb{Q}$-encaixes, de K en $\mathbb{C}$. Dados $\alpha_1, \ldots, \alpha_n \in K$ defínese o discriminante de $\alpha_1, \ldots, \alpha_n$ como:

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) := \Big| \Big(\sigma_i(\alpha_j)\Big) \Big|^2$$

sendo

$$\Big(\sigma_i(\alpha_j)\Big) := \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \in M_{n\times n}(K)$$

Teorema 2.15. *Nas condicións da definición,* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \Big| \Big(\mathrm{T}(\alpha_i\alpha_j)\Big) \Big|$, *sendo*

$$\Big(\mathrm{T}(\alpha_i\alpha_j)\Big) := \begin{pmatrix} \mathrm{T}(\alpha_1\alpha_1) & \cdots & \mathrm{T}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{T}(\alpha_n\alpha_1) & \cdots & \mathrm{T}(\alpha_n\alpha_n) \end{pmatrix} \in M_{n\times n}(K)$$

Demostración. Séguese do feito seguinte:

$$\Big(\sigma_i(\alpha_j)\Big)^{\mathsf{t}} \Big(\sigma_i(\alpha_j)\Big) = \Big(\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)\Big) = \Big(\mathrm{T}(\alpha_i\alpha_j)\Big)$$

Aplicando o determinante chegamos ao resultado. □

Corolario 2.16. *Nas mesmas condicións que antes, tense:*

(*i*) $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$.

(*ii*) *Se os* $\alpha_i \in \mathcal{O}_K$, *para* $i \in \{1, \ldots, n\}$, *entón* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Demostración. É inmediato a partir do teorema anterior máis o Corolario 2.12. □

Máis a diante imos definir o discriminante do anel de enteiros dun corpo a partir dunha base enteira do mesmo, no seguinte teorema imos ver que o discriminante dunha base é sempre distinto de cero.

Teorema 2.17. *Dados* $\alpha_1, \ldots, \alpha_n \in K$ *temos que* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ *se, e só se,* $\alpha_1, \ldots, \alpha_n$ *son linealmente dependentes sobre* $\mathbb{Q}$.

Demostración. Temos o seguinte

$$\operatorname{disc}(\alpha_1,\dots,\alpha_n)=0 \iff \left|\Big(\sigma_i(\alpha_j)\Big)\right|=0,$$

é dicir, as columnas de matriz $\Big(\sigma_i(\alpha_j)\Big)$ son $\mathbb{Q}$-linealmente dependentes. Entón, $\forall j\in\{1,\dots,n\}$, existe una combinación lineal $\lambda_1\sigma_j(\alpha_1)+\cdots+\lambda_n\sigma_j(\alpha_n)=0$ con $\lambda_i\in\mathbb{Q}$ e algún $\lambda_i\neq 0$, o cal equivale a $\sigma_j(\lambda_1(\alpha_1)+\cdots+\lambda_n(\alpha_n))=0$, e, por ser σ_j un encaixe, isto equivale a $\lambda_1(\alpha_1)+\cdots+\lambda_n(\alpha_n)=0$, con $\lambda_i\in\mathbb{Q}$ e algún deles non nulo, é dicir, $\alpha_1,\dots,\alpha_n$ son linealmente dependentes sobre $\mathbb{Q}$. □

No caso de que a base a considerar sea da forma $\{1,\alpha,\dots,\alpha^{n-1}\}$ podemos obter unha forma alternativa de calcular o seu discriminante coma aparece no seguinte resultado:

Teorema 2.18. *Sexa $K=\mathbb{Q}(\alpha)$ e $\alpha_1,\dots\alpha_n$ os ceros de $f=\operatorname{Irr}(\alpha,\mathbb{Q})$, entón*

$$\operatorname{disc}(1,\alpha,\dots,\alpha^{n-1})=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2=\pm\operatorname{N}(f'(\alpha))$$

Na última igualdade temos o signo + cando $n\equiv 0,1(\mathrm{mod}\ 4)$ e − noutro caso.

Demostración. A proba pódese consultar en [6, p.19]. □

A partir de agora, para cada $\alpha\in\mathbb{C}$, denotaremos $\operatorname{disc}(\alpha):=\operatorname{disc}(1,\alpha,\dots,\alpha^{n-1})$.

A continuación veremos que dado un corpo de números K o seu anel de enteiros $\mathcal{O}_K$ é un grupo abeliano libre de rango $n=[K\colon\mathbb{Q}]$. Isto permitiranos definir o discriminante de $\mathcal{O}_K$ a partir dunha base.

Lema 2.19. *Dado $\beta\in\mathbb{C}$ alxébrico sobre $\mathbb{Q}$, existe $m\in\mathbb{Z}-\{0\}$ de forma que $m\beta\in\mathbb{C}$ é un enteiro alxébrico.*

Demostración. Sea $f(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0\in\mathbb{Z}[X]$, con $a_n\neq 0$, un polinomio tal que $f(\beta)=0$. Basta tomar $m=a_n$. En efecto, o polinomio $g(X)=X^n+a_{n-1}X^{n-1}+a_{n-2}a_nX^{n-2}+\cdots+a_1a_n^{n-2}X+a_0a_n^{n-1}\in\mathbb{Z}[X]$ é mónico e é tal que $g(m\beta)=(m\beta)^n+a_{n-1}(m\beta)^{n-1}+a_{n-2}a_n(m\beta)^{n-2}+\cdots+a_1a_n^{n-2}m\beta+a_0a_n^{n-1}=a_n^{n-1}f(\beta)=0$. □

Unha $\mathbb{Q}$-base dun corpo de números K formada por elementos enteiros alxébricos dirase unha *base enteira* de K. Como consecuencia do lema anterior, calquera corpo de números K ten bases enteiras: Se $\{\beta_1,\dots,\beta_n\}$ é unha base de K sobre $\mathbb{Q}$ basta tomar a base $\{\alpha_1,\dots,\alpha_n\}=\{m\beta_1,\dots,m\beta_n\}$ formada por enteiros alxébricos, onde $m=m_1\cdots m_n$ e $m_i\in\mathbb{Z}-\{0\}$ obtense aplicando o lema anterior a β_i, con $i\in\{1,\dots,n\}$. Podemos enunciar o seguinte resultado:

Proposición 2.20. *Sexa* $\{\alpha_1, \ldots, \alpha_n\}$ *unha base enteira de* K *sobre* $\mathbb{Q}$ *e* $\alpha \in \mathcal{O}_K$ *entón, se* $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$*, tense que*

$$\alpha = \frac{d_1\alpha_1 + \cdots + d_n\alpha_n}{d}$$

con $d_i \in \mathbb{Z}$, $\forall i \in \{1, \ldots, n\}$.

Demostración. Tomemos $\{\alpha_1, \ldots, \alpha_n\}$ a base enteira de K sobre $\mathbb{Q}$ do enunciado e $\alpha \in \mathcal{O}_K$ entón $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ con $a_i \in \mathbb{Q}$, $\forall i \in \{1, \ldots, n\}$. Apliquemos agora σ_1, $\sigma_2, \ldots, \sigma_n$, os n encaixes de K en $\mathbb{C}$, a α obtendo o seguinte sistema

$$\begin{cases} \sigma_1(\alpha) &= a_1\sigma_1(\alpha_1) + \cdots + a_n\sigma_1(\alpha_n) \\ \vdots & \ddots \\ \sigma_n(\alpha) &= a_1\sigma_n(\alpha_1) + \cdots + a_n\sigma_n(\alpha_n) \end{cases}$$

Podemos resolver este sistema empregando o regra de Cramer e obtemos $a_i = \frac{b_i}{b}$ onde b é o determinante da matriz $\Big(\sigma_i(\alpha_k)\Big)$ e b_i é o determinante da matriz anterior substituíndo a columna i por la columna $\Big(\sigma_j(\alpha)\Big) \in M_{n\times 1}$. Resulta natural que b_i e b son enteiros alxébricos, por selo os α_i e α, ademais $b^2 = d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. Así obtemos que $da_i = bb_i$ é un número racional que ademais é un enteiro alxébrico polo tanto $da_i = bb_i \in \mathbb{Z}$. Así, denotando por $d_i = da_i$, obtemos que

$$\alpha = \frac{d_1\alpha_1 + \cdots + d_n\alpha_n}{d}$$

con $d_i \in \mathbb{Z}$, $\forall i \in \{1, \ldots, n\}$. □

Teorema 2.21. *O anel de enteiros dun corpo de números* K *é un grupo abeliano libre de rango* $n = [K\colon \mathbb{Q}]$.

Demostración. Grazas á proposición anterior, Proposición 2.20, temos que $\mathcal{O}_K$ está contido en $\frac{\alpha_1}{d}\mathbb{Z} \oplus \cdots \oplus \frac{\alpha_n}{d}\mathbb{Z}$ que é nun grupo abeliano libre de rango n polo tanto, pola Proposición 1.1, é un grupo abeliano libre de rango $\leq n$. Ademais contén a $\alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$ que é un grupo abeliano libre de rango n. Tendo en conta ambos contidos obtemos o resultado.

$$\alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \frac{\alpha_1}{d}\mathbb{Z} \oplus \cdots \oplus \frac{\alpha_n}{d}\mathbb{Z}\ .$$ □

Nas condicións do teorema anterior, como $\mathcal{O}_K$ é un grupo abeliano libre de rango n sabemos que existen $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ de modo que dado $\alpha \in \mathcal{O}_K$ este escríbese de forma única como $a_1\beta_1 + \cdots + a_n\beta_n$ con $a_i \in \mathbb{Z}$. O conxunto $\{\alpha_1, \ldots, \alpha_n\}$ chámase *base enteira* de $\mathcal{O}_K$ sobre $\mathbb{Z}$, nótese que ademais $\{\alpha_1, \ldots, \alpha_n\}$ é unha base enteira de K sobre $\mathbb{Q}$.

Teorema 2.22. *Sexan* $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ *e* $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ *dúas bases enteiras de* $\mathcal{O}_K$ *entón* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(\beta_1, \ldots, \beta_n)$.

Demostración. Podemos poñer os elementos de $\mathcal{A}$ coma combinación dos elementos de $\mathcal{B}$, escribindo isto en forma matricial obtemos

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix},$$

con $M = \Big(m_{ij}\Big) \in M_{n\times n}(\mathbb{Z})$ unha matriz invertible. Como os $m_{ij} \in \mathbb{Z}$ se calculamos a imaxe das matrices anteriores mediante σ_j con $j \in \{1, \ldots, n\}$, os n encaixes de K en $\mathbb{C}$, obtemos que $\Big(\sigma_j(\alpha_i)\Big) = M\Big(\sigma_j(\beta_i)\Big)$. Entón, por definición, $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = |M|^2 \operatorname{disc}(\beta_1, \ldots, \beta_n)$. Como $|M| \in \mathbb{Z}$ podemos concluír que o discriminante $\operatorname{disc}(\beta_1, \ldots, \beta_n)$ divide ao discriminante $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$, se agora escribimos os elementos de $\mathcal{B}$ como combinación dos elementos de $\mathcal{A}$ e facemos o mesmo razoamentos chegaríamos a que $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ divide ao discriminante $\operatorname{disc}(\beta_1, \ldots, \beta_n)$ e polo tanto teñen que ser iguais. □

Grazas aos resultados anteriores podemos dar a seguinte definición.

Definición 2.23. Sexa K un corpo numérico e $\{\alpha_1, \ldots, \alpha_n\}$ unha base enteira de $\mathcal{O}_K$ entón chamamos *discriminante de* $\mathcal{O}_K$ a $\operatorname{disc}(\mathcal{O}_K) := \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

Calculemos agora o discriminante do anel de enteiros alxébricos dunha extensión cadrática de $\mathbb{Q}$, empregaremos este resultado na demostración do Teorema de Kronecker-Weber.

Proposición 2.24. *Sexa a extensión $\mathbb{Q}(\sqrt{n})|\mathbb{Q}$, con n libre de cadrados, tense que:*

(*i*) *Se* $n \equiv 2, 3 \pmod 4$ *entón* $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 4n$.

(*ii*) *Se* $n \equiv 1 \pmod 4$ *entón* $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = n$.

Demostración. En primeiro lugar, sabemos pola Proposición 2.8 que se $n \equiv 2, 3 \pmod 4$ temos $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]$ e podemos tomar $\{1, \sqrt{n}\}$ como base enteira de $\mathcal{O}_{\mathcal{O}_{\mathbb{Q}(\sqrt{n})}}$, en cambio se $n \equiv 1 \pmod 4$ temos $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ e a base sería $\{1, \frac{1+\sqrt{n}}{2}\}$.

Por outro lado, os $\mathbb{Q}$-encaixes de $\mathcal{O}_{\mathbb{Q}(\sqrt{n})}$ en $\mathbb{C}$ son ι, a inclusión, e σ o $\mathbb{Q}$-encaixe determinado por $\sigma(\sqrt{n}) = -\sqrt{n}$:

$$\begin{array}{rccc} \iota: & \mathcal{O}_{\mathbb{Q}(\sqrt{n})} & \longrightarrow & \mathbb{C} \\ & \sqrt{n} & \mapsto & \sqrt{n} \end{array} \qquad \begin{array}{rccc} \sigma: & \mathcal{O}_{\mathbb{Q}(\sqrt{n})} & \longrightarrow & \mathbb{C} \\ & \sqrt{n} & \mapsto & -\sqrt{n} \end{array}$$

Con isto xa podemos calcular o discriminante e obtemos:

$$\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = \begin{vmatrix} 1 & \sqrt{n} \\ 1 & -\sqrt{n} \end{vmatrix}^2 = 4n \qquad Se \quad n \equiv 2, 3 \pmod 4.$$

$$\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = \begin{vmatrix} 1 & \frac{1+\sqrt{n}}{2} \\ 1 & -\frac{1+\sqrt{n}}{2} \end{vmatrix}^2 = n \qquad Se \quad n \equiv 1 \,(\mathrm{mod}\ 4).$$

□

2.3. Anel de enteiros dun corpo ciclotómico

Nesta sección queremos probar que o anel de enteiros dun corpo ciclotómico $\mathbb{Q}(\varepsilon_n)$ é $\mathcal{O}_{\mathbb{Q}(\varepsilon_n)} = \mathbb{Z}[\varepsilon_n]$. Primeiro enunciaremos varios resultados que serán necesarios para a demostración.

Proposición 2.25. *Sexan K e L corpos de números tales que $n = [K\colon \mathbb{Q}]$ e $m = [L\colon \mathbb{Q}]$ entón se $[KL\colon \mathbb{Q}] = nm$ e $\mathrm{mcd}(\operatorname{disc}(\mathcal{O}_K), \operatorname{disc}(\mathcal{O}_L)) = 1$ tense que $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.*

Demostración. Pódese ver en [6, p.24-26]. □

Proposición 2.26. *Sexa $\varepsilon_n \in \mathbb{C}$ a raíz primitiva n-ésima da unidade entón $\operatorname{disc}(\varepsilon_n) \mid n^{\varphi(n)}$.*

Demostración. Sabemos que ε_n é raíz do polinomio $\mathrm{X}^n - 1 = fg$, onde $f = \mathrm{Irr}(\varepsilon_n, \mathbb{Q})$, e $f, g \in \mathbb{Z}[X]$ (polo Lema de Gauss). Se derivamos e avaliamos en ε_n o polinomio anterior obtemos a identidade $n\varepsilon_n^{n-1} = f'(\varepsilon_n)g(\varepsilon_n)$ que equivale a $n = \varepsilon_n f'(\varepsilon_n)g(\varepsilon_n)$. Aplicando a norma á identidade anterior e empregando o Teorema 2.18 obtemos $n^{\varphi(n)} = \pm \operatorname{disc}(\varepsilon_n)\,\mathrm{N}(\varepsilon_n g(\varepsilon_n))$. Como ademais $\mathrm{N}(\varepsilon_n g(\varepsilon_n)) \in \mathbb{Z}$, porque $g(\varepsilon_n) \in \mathbb{Z}[\varepsilon_n]$, podemos concluír que $\operatorname{disc}(\varepsilon_n) \mid n^{\varphi(n)}$. □

Lema 2.27. *Sexa $\varepsilon_n \in \mathbb{C}$ a raíz primitiva n-ésima da unidade, con $n = p^r$, entón*

$$\prod_{i \in \{1 \le i \le n,\, p \nmid i\}} (1 - \varepsilon_n^i) = p. \tag{2.1}$$

Demostración. Tomemos

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}.$$

Como os ε_n^i do enunciado son raíces primitivas n-ésimas da unidade temos que son raíces de $X^{p^r} - 1$ pero non o son de $X^{p^{r-1}} - 1$, polo tanto son raíces de h. Ademais o número de raíces primitivas é $\varphi(n) = \varphi(p^r) = (p-1)p^{r-1}$ chegando así a que $h(X) = \prod_{i \in \{1 \le i \le n,\, p \nmid i\}} (X - \varepsilon_n^i)$. Avaliando h en 1 obtemos o resultado. □

Proposición 2.28. *Sexa o corpo ciclotómico $K = \mathbb{Q}(\varepsilon_{p^r})$, con p primo, entón $\mathcal{O}_K = \mathbb{Z}[\varepsilon_{p^r}]$.*

Demostración. Denotemos por $n = p^r$. Para a demostración imos traballar tanto con ε_n coma con $1 - \varepsilon_n$. En primeiro lugar, temos que $\mathbb{Z}[1 - \varepsilon_n] = \mathbb{Z}[\varepsilon_n]$ e ademais polo Teorema 2.22 sabemos

que $\text{disc}(\varepsilon_n) = \text{disc}(1-\varepsilon_n)$, notar que o teorema está enunciado para o anel de enteiros dun corpo de números pero isto non influe na súa demostración.

Pola Proposición 2.20 sabemos que dado $\alpha \in \mathcal{O}_{\mathbb{Q}(\varepsilon_n)}$

$$\alpha = \frac{d_1 + d_2(1-\varepsilon_n) + \cdots + d_n(1-\varepsilon_n)^{\varphi(n)-1}}{d}$$

con $d_i \in \mathbb{Z}$, $\forall i \in \{1, \ldots, n\}$ e $d = \text{disc}(\varepsilon_n) = \text{disc}(1-\varepsilon_n)$. Supoñamos que $\mathbb{Z}[1-\varepsilon_n] \subsetneq \mathcal{O}_{\mathbb{Q}(\varepsilon_n)}$ entón $\exists \alpha \in \mathcal{O}_{\mathbb{Q}(\varepsilon_n)}$ da forma anterior con algún d_i non divisible entre d.

Pola Proposición 2.26 sabemos que d é unha potencia de p entón podemos tomar $\beta \in \mathcal{O}_{\mathbb{Q}(\varepsilon_n)}$ que sexa da seguinte forma

$$\beta = \frac{d_j(1-\varepsilon_n)^{j-1} + d_{j+1}(1-\varepsilon_n)^{j} + \cdots + d_n(1-\varepsilon_n)^{\varphi(n)-1}}{p}$$

con d_j non divisible por p. Por outro lado, como $(1-\varepsilon_n) \mid (1-\varepsilon_n^i)$ temos polo Lema 2.27 que $\frac{p}{(1-\varepsilon_n)^{\varphi(n)}} \in \mathbb{Z}[\varepsilon_n]$. Así $\frac{p}{(1-\varepsilon_n)^j} \in \mathbb{Z}[\varepsilon_n]$ e polo tanto $\beta\frac{p}{(1-\varepsilon_n)^j} \in \mathbb{Z}[\varepsilon_n]$. Como case tódolos termos que aparecen en $\beta\frac{p}{(1-\varepsilon_n)^{\varphi(n)}}$ pertencen de forma evidente a $\mathbb{Z}[\varepsilon_n]$ chegamos a que $\frac{d_j}{(1-\varepsilon_n)} \in \mathbb{Z}[\varepsilon_n]$. Deste modo $\text{N}(1-\varepsilon_n) \mid \text{N}(d_j)$ pero isto é unha contradición porque, polo Lema 2.27, $\text{N}(1-\varepsilon_n) = p$ e $N(d_j) = d_j^{\varphi(n)}$. □

Podemos proceder a calcular o anel de enteiros dun corpo ciclotómico $\mathbb{Q}(\varepsilon_n)$.

Proposición 2.29. *Dado $n > 0$ enteiro, para o corpo ciclotómico $\mathbb{Q}(\varepsilon_n)$ tense que $\mathcal{O}_{\mathbb{Q}(\varepsilon_n)} = \mathbb{Z}[\varepsilon_n]$.*

Demostración. Se n é a potencia dun primo o resultado está probado pola Proposición. 2.28, Supoñamos entón que $n = n_1 n_2$, con n_1 e n_2 coprimos. Imos ver que se $\mathcal{O}_{\mathbb{Q}(\varepsilon_{n_i})} = \mathbb{Z}[\varepsilon_{n_i}]\, para i = 1, 2$ entón $\mathcal{O}_{\mathbb{Q}(\varepsilon_n)} = \mathbb{Z}[\varepsilon_n]$. Reiterando o argumento para cada n_i quedaría probada a proposición.

Sabemos pola Proposición 1.13 que $\mathbb{Q}(\varepsilon_n) = \mathbb{Q}(\varepsilon_{n_1})\mathbb{Q}(\varepsilon_{n_2})$ e $[\mathbb{Q}(\varepsilon_n)\colon \mathbb{Q}] = [\mathbb{Q}(\varepsilon_{n_1})\colon \mathbb{Q}][\mathbb{Q}(\varepsilon_{n_2})\colon \mathbb{Q}]$. Suposto que o $\text{disc}(\mathcal{O}_{\mathbb{Q}(\varepsilon_{n_1})})$ e o $\text{disc}(\mathcal{O}_{\mathbb{Q}(\varepsilon_{n_2})})$ son coprimos, podemos aplicar a Proposición 2.25 e concluír que $\mathcal{O}_{\mathbb{Q}(\varepsilon_n)} = \mathbb{Z}[\varepsilon_{n_1}]\mathbb{Z}[\varepsilon_{n_2}] = \mathbb{Z}[\varepsilon_n]$, a proba da última igualdade é análoga á demostración da Proposición 1.13. Probemos que

$$\text{mcd}(\text{disc}(\mathcal{O}_{\mathbb{Q}(\varepsilon_{n_1})}), \text{disc}(\mathcal{O}_{\mathbb{Q}(\varepsilon_{n_2})})) = 1,$$

aplicando a Proposición 2.26 temos que $\text{disc}(\mathcal{O}_{\mathbb{Q}(\varepsilon_{n_i})}) \mid n_i^{\varphi(n_i)}$, $i = 1, 2$ entón por ser n_1 e n_2 son coprimos chegamos ao resultado. □

2.4. Dominios de Dedekind

O obxectivo desta sección é ver que no anel de enteiros $\mathcal{O}_K$ dun corpo de números K todo ideal non nulo pódese descompoñer de forma única no produto de ideais primos. En concreto, veremos que $\mathcal{O}_K$ é un dominio de Dedekind. Ímonos centrar en definir os dominios de Dedekind e as súas propiedades omitindo as demostracións dos resultados, seguiremos a referencia [8].

Recordemos que, un *dominio de integridade* ou *dominio* e un anel conmutativo R non trivial que non contén divisores de cero. Se R é un dominio pódese construír $K(R)$ o seu corpo de fraccións de xeito que $R \subseteq K(R)$.

Definición 2.30. Sexa R un anel, dicimos que é *noetheriano* se cumpre as seguintes condicións equivalentes:

(*i*) Toda cadea estritamente ascendente de ideais de R é finita, é dicir, é estacionaria.

(*ii*) Toda familia non baleira de ideais de R ten un elemento maximal.

(*iii*) Todo ideal de R é de tipo finito.

Se ademais R non ten divisores de cero diremos que é un *dominio noetheriano.*

Unha demostración de por que as tres condicións anteriores son equivalentes pódese consultar en [8, §1.4, Theorem 1, p. 20].

Definición 2.31. Sexa R un dominio e K o seu corpo de fraccións, dicimos que R é *integramente pechado* se tódolos elementos de K que son enteiros sobre R pertencen a R.

Definición 2.32. Dicimos que un dominio de integridade R é un *dominio de Dedekind* se cúmprense as tres condicións seguintes:

(*i*) R é Noetheriano,

(*ii*) R é integramente pechado,

(*iii*) todo ideal primo non nulo de R é maximal.

Nótese que por definición $\mathbb{Z}$ é un dominio de Dedekind, a importancia deste feito reflíctese no seguinte teorema que nos garante que dada unha extensión $K|\mathbb{Q}$ o anel de enteiros de K é un dominio de Dedekind.

Teorema 2.33. *Sexa R un dominio de Dedekind e K o seu corpo de fraccións. Se $L|K$ é unha extensión alxébrica finita entón a clausura integra de R en L é un dominio de Dedekind.*

Demostración. Pódese ver a demostración en [11, Chapter V, Theorem 19, pp. 281-282]. □

Corolario 2.34. *O anel de enteiros alxébricos $\mathcal{O}_K$ dun corpo de números K é un dominio de Dedekind.*

Demostración. Como $\mathbb{Z}$ é un dominio de Dedekind e $\mathbb{Q}$ é o seu corpo de fraccións podemos aplicar o teorema anterior obtendo que dada a extensión $K|\mathbb{Q}$ alxébrica e finita o anel de enteiros de K é un dominio de Dedekind. □

Unha propiedade fundamental dun dominio de Dedekind R é que os seus ideais non nulos co produto de ideais forman un monoide, se engadimos os "inversos" dos ideais obtemos un grupo, para considerar tanto os ideais de R como os seus "inversos" temos que ampliar o conxunto de ideais considerando certos R-submódulos do corpo de fracciones de R, os ideais fraccionarios:

Definición 2.35. Sexa R un dominio e K o seu corpo de fraccións, dado $\mathfrak{I}$ un R-submódulo non nulo de K dicimos que é un *ideal fraccionario* se existe $d \in R$ non nulo tal que $d\mathfrak{I} \subseteq R$. Todo ideal non nulo de R é un ideal fraccionario (tomando $d = 1$), denominase ideal enteiro de R.

Teorema 2.36. *Sexa R un dominio de Dedekind e denotemos por* $\mathrm{Spm}(R)$ *o conxunto formado polos ideais primos non nulos de R, é dicir o conxuntos dos ideais maximais, entón:*

(*i*) *Todo ideal fraccionario $\mathfrak{a}$ de R pódese expresar de forma única coma produto finito de ideais primos de R, é dicir:*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathrm{Spm}(R)} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

con $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ e $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ para case todo $\mathfrak{p} \in \mathrm{Spm}(R)$.

(*ii*) *O monoide dos ideais fraccionarios de R é un grupo.*

Demostración. Pódese ver en [8, §3.4, Theorem 3, pp. 50-51]. □

Para finalizar esta sección imos recoller algunhas propiedades dos índices $v_{\mathfrak{p}}(\mathfrak{a})$ que denota, como vimos no teorema, o expoñente co cal aparece $\mathfrak{p}$ na descomposición do ideal fraccionario $\mathfrak{a}$.

Dados $\mathfrak{a}$ e $\mathfrak{b}$ ideais fraccionarios de R, tense:

(*i*) $v_{\mathfrak{p}}(\mathfrak{ab}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$.

(*ii*) $\mathfrak{a}$ é un ideal de R se, e só se, $v_{\mathfrak{p}}(\mathfrak{a}) \geq 0,\ \forall \mathfrak{p} \in \mathrm{Spec}(R)$.

(*iii*) $\mathfrak{a} \subseteq \mathfrak{b}$ se, e só se, $v_{\mathfrak{p}}(\mathfrak{a}) \geq v_{\mathfrak{p}}(\mathfrak{b}),\ \forall \mathfrak{p} \in \mathrm{Spec}(R)$.

(*iv*) $v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \text{ínf}\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$.

(*v*) $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \sup\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$.

Máis detalle sobre estas propiedades pódense consultar en [8, §3.4, pp. 51-52].

Capítulo 3

Factorización de ideais nunha extensión de corpos de números

Como o anel de enteiros dun corpo de números K é un dominio de Dedekind, calquera ideal non nulo dun anel de $\mathcal{O}_K$ factorízase no produto de ideais primos non nulos e o fai de forma única. Ademais os ideais primos non nulos destes aneis son precisamente os ideais maximais.

Neste capítulo imos traballar con extensións de corpos de números $L|K$ e a correspondente extensión de aneis entre os seus aneis de enteiros $\mathcal{O}_L|\mathcal{O}_K$. Dado un ideal primo $\mathfrak{p} \subset \mathcal{O}_K$ podemos definir o *ideal extensión do ideal* $\mathfrak{p}$ a $\mathcal{O}_L$ como o ideal mais pequeno de $\mathcal{O}_L$ que contén a $\mathfrak{p}$:

$$\mathfrak{p}\mathcal{O}_L := \left\{ \sum_{i=1}^{r} p_i\alpha_i \,;\;\; p_i \in \mathfrak{p},\, \alpha_i \in \mathcal{O}_L \right\}$$

O ideal extensión $\mathfrak{p}\mathcal{O}_L \subseteq \mathcal{O}_L$ é un ideal non nulo, pero non é necesariamente un primo de $\mathcal{O}_L$. Como $\mathcal{O}_L$ é un dominio de Dedekind, podemos considerar a descomposición do ideal $\mathfrak{p}\mathcal{O}_L$ no produto de ideais primos de $\mathcal{O}_L$ que será da forma:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i},$$

para certos naturais $\mathbf{g}, \mathbf{e}_1, \ldots, \mathbf{e}_{\mathbf{g}}$. Os primos $\mathfrak{P}_i$ que aparecen na descomposición de $\mathfrak{p}$ son os primos de $\mathcal{O}_L$ que están sobre $\mathfrak{p}$. Imos ver agora que significa isto.

Definición 3.1. Sexa $L|K$ unha extensión de corpos de números. Dados $\mathfrak{p} \in \mathcal{O}_K$ e $\mathfrak{P} \in \mathcal{O}_L$ ideais primos dise que o *primo* $\mathfrak{P}$ *está sobre o primo* $\mathfrak{p}$ se $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

Observación 3.2. Sexa R un anel. Dados $\mathfrak{a}, \mathfrak{b} \subseteq R$ ideais de R, dise que $\mathfrak{a}$ divide a $\mathfrak{b}$, e represéntase $\mathfrak{a} \mid \mathfrak{b}$, se existe un ideal $\mathfrak{c} \subset R$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Se R é dominio de Dedekind, entón a relación $\mathfrak{a} \mid \mathfrak{b}$ equivale a relación $\mathfrak{b} \subset \mathfrak{a}$. Como consecuencia de esta propiedade pode probarse o seguinte resultado (ver [6, p. 44]):

Teorema 3.3. *Sexa $L|K$ unha extensión de corpos de números. Para ideais primos $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ e $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ equivalen:*

(*i*) $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$.

(*ii*) $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_K$.

(*iii*) $\mathfrak{P} \supseteq \mathfrak{p}$.

(*iv*) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

(*v*) $\mathfrak{P} \cap K = \mathfrak{p}$.

Se $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ e $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ son ideais primos non nulos da extensión de corpos $L|K$, como $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$ se, e só se, $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, os únicos primos de $\mathcal{O}_L$ que están sobre $\mathfrak{p} \in \mathcal{O}_K$ son exactamente aqueles que aparecen na factorización en produto de primos do ideal $\mathfrak{p}\mathcal{O}_L \subseteq \mathcal{O}_L$. Sempre vaise ter que $\mathfrak{p}\mathcal{O}_K \subsetneq \mathcal{O}_K$ polo que van a existir un número finito de ideais primos de $\mathcal{O}_K$ sobre $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$. Por outro lado, se collemos un primo $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ tense que $\mathfrak{P} \cap \mathcal{O}_K \in \mathrm{Spm}(\mathcal{O}_K)$ e polo tanto todo primo de $\mathcal{O}_L$ vai estar sobre un primo de $\mathcal{O}_K$.

Notación: A partir de agora ímonos referir ao natural $v_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L)$ coma o maior expoñente de $\mathfrak{P}$ que divide a $\mathfrak{p}\mathcal{O}_L$, ou potencia exacta de $\mathfrak{P}$ dividindo a $\mathfrak{p}\mathcal{O}_L$, o cal resulta coherente grazas ao teorema anterior.

O que acabamos de dicir recóllese no seguinte resultado:

Teorema 3.4. *Dada unha extensión de corpos de números $L|K$, tense que todo primo $\mathfrak{P}$ de $\mathcal{O}_L$ está sobre un único primo $\mathfrak{p}$ de $\mathcal{O}_K$, reciprocamente, para todo primo $\mathfrak{p}$ de $\mathcal{O}_K$ existe polo menos un primo $\mathfrak{P}$ de $\mathcal{O}_L$ que está sobre $\mathfrak{p}$.*

Demostración. A demostración atópase en [6, p. 45]. □

3.1. Índice de ramificación e grao residual

Sexa a extensión $L|K$ e tomemos $\mathfrak{p}$ primo de $\mathcal{O}_K$ non nulo, consideremos a súa descomposición en primos de $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}. \tag{3.1}$$

Definición 3.5. O número de ideais primos distintos que aparecen na descomposición de $\mathfrak{p}$ denótase por $\mathbf{g}_{\mathfrak{p}} = \mathbf{g}$. No caso que esteamos traballando con máis dunha extensión de corpos o denotamos por $\mathbf{g}_{\mathfrak{p}}(L|K) = \mathbf{g}$.

Definición 3.6. Dada a descomposición anterior chamamos *índice de ramificación* aos expoñentes $\mathbf{e}_i$ asociados a cada primo $\mathfrak{P}_i \in \mathcal{O}_L$. Os denotamos por $\mathbf{e}_{\mathfrak{P}_i/\mathfrak{p}} = \mathbf{e}_i$. Ademais se, fixado j, $\mathbf{e}_j = \mathbf{e}_{\mathfrak{P}_j/\mathfrak{p}} > 1$ dise que $\mathfrak{P}_i$ *ramifica sobre* $\mathfrak{p}$, en caso contrario dise que *non ramifica sobre* $\mathfrak{p}$. Se algún dos $\mathfrak{P}_i$ ramifica sobre $\mathfrak{p}$ dicimos que $\mathfrak{p}$ ramifica en $\mathcal{O}_L$, pola contra se non ocorre isto dicimos que $\mathfrak{p}$ non ramifica en $\mathcal{O}_L$.

O seguinte que definiremos é o grao residual para isto consideremos os aneis de enteiros $\mathcal{O}_K$ e $\mathcal{O}_L$, tomemos $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ e $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ que estea sobre $\mathfrak{p}$. Como os ideais que estamos considerando son maximais, é dicir son primos non nulos porque os aneis de enteiros son dominios de Dedekind, os aneis $\mathcal{O}_K/\mathfrak{p}$ e $\mathcal{O}_L/\mathfrak{P}$ son corpos que reciben o nome de *corpos residuais*. Estes corpos son finitos como consecuencia da seguinte proposición.

Proposición 3.7. *Sexa K un corpo de números. Se $\mathfrak{I}$ é un ideal non nulo de $\mathcal{O}_K$ entón o anel $\mathcal{O}_K/\mathfrak{I}$ é finito.*

Demostración. Tomemos un elemento $\alpha \in \mathfrak{I}$ non nulo e consideremos $m = \mathrm{N}(\alpha) \in \mathbb{Z}$, nótese que $m \neq 0$. Imos ver que $m \in \mathfrak{I}$, por definición da norma $m = \alpha\beta$ onde β é o produto dos conxugados de α, distintos de α, se agora consideramos K' unha clausura alxébrica de K temos que $\beta \in \mathcal{O}_{K'}$ e ademais $\beta = m/\alpha \in K$ así $\beta \in \mathcal{O}_K$. Entón $m = \alpha\beta \in \mathfrak{I}$ polo tanto se $\mathcal{O}_K/m\mathcal{O}_K$ é finito $\mathcal{O}_K/\mathfrak{I}$ tamén o é. Que $\mathcal{O}_K/m\mathcal{O}_K$ sexa un grupo finito débese a que, ao a ser $\mathcal{O}_K$ un grupo abeliano libre de rango $n = [K\colon \mathbb{Q}]$, temos os seguintes isomorfismos $\mathcal{O}_K/m\mathcal{O}_K \cong \mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$. □

Dada unha extensión de corpos de números $L|K$, se $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ é un primo sobre $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$, os primos $\mathfrak{p}$ e $\mathfrak{P}$ están relacionados pola expresión $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, grazas a isto podemos establecer unha relación entre os seus corpos residuais. Sabemos que existe un homomorfismo $\mathcal{O}_K \longrightarrow \mathcal{O}_L/\mathfrak{P}$ que obtemos ao compoñer a inclusión $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ coa proxección $\mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{P}$, o núcleo deste homomorfismo é $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ podendo asegurar así que o homomorfismo canónico $\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathcal{O}_L/\mathfrak{P}$ é inxectivo. Grazas a este homomorfismo canónico podemos ver a $\mathcal{O}_K/\mathfrak{p}$ coma un subcorpo de $\mathcal{O}_L/\mathfrak{P}$ e, como ambos son corpos finitos, a extensión $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}$ vai ter grao finito.

Definición 3.8. Coa notación anterior, chamamos *grao residual* a $\mathbf{f}_{\mathfrak{P}/\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{P}\colon \mathcal{O}_K/\mathfrak{p}]$, onde $\mathcal{O}_L/\mathfrak{P}$ e $\mathcal{O}_K/\mathfrak{p}$ son os corpos residuais asociado a cada primo.

Con estas definicións podemos enunciar os seguintes resultados:

Proposición 3.9. *Dada unha torre de corpos de números $K \subseteq L \subseteq M$ e ideais $\mathfrak{Q} \in \mathrm{Spm}(\mathcal{O}_M)$, $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ e $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ tales que $\mathfrak{Q} \cap \mathcal{O}_L = \mathfrak{P}$ e $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ tense:*

(*i*) $\boldsymbol{e}_{\mathfrak{Q}/\mathfrak{p}} = \boldsymbol{e}_{\mathfrak{Q}/\mathfrak{P}}\, \boldsymbol{e}_{\mathfrak{P}/\mathfrak{p}}$.

(*ii*) $\boldsymbol{f_{\mathfrak{Q}/\mathfrak{p}} = f_{\mathfrak{Q}/\mathfrak{P}} f_{\mathfrak{P}/\mathfrak{p}}}$.

Demostración. Para demostrar (i) basta con notar que $\mathbf{e}_{\mathfrak{Q}/\mathfrak{P}}$ é a potencia exacta de $\mathfrak{Q}$ dividindo a $\mathfrak{P}\mathcal{O}_M$ e $\mathbf{e}_{\mathfrak{P}/\mathfrak{p}}$ é a potencia exacta de $\mathfrak{P}$ dividindo a $\mathfrak{p}\mathcal{O}_L$. Polo tanto a potencia exacta de $\mathfrak{Q}$ dividindo a $\mathfrak{p}\mathcal{O}_M$ é $\mathbf{e}_{\mathfrak{Q}/\mathfrak{P}}\,\mathbf{e}_{\mathfrak{P}/\mathfrak{p}} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{p}}$, obsérvese que $\mathfrak{Q} \cap \mathcal{O}_L = \mathfrak{P}$. Para demostrar (ii) basta con empregar a multiplicidade das extensión de corpos. □

Teorema 3.10. *Sexa $L|K$ unha extensión de corpos de números de grao n entón:*

(*i*) *Dados $\mathfrak{a}$ e $\mathfrak{b}$ ideais de $\mathcal{O}_K$ tense que $|\mathcal{O}_K/\mathfrak{ab}| = |\mathcal{O}_K/\mathfrak{a}| \cdot |\mathcal{O}_K/\mathfrak{b}|$.*

(*ii*) *Dado $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ tense que $|\mathcal{O}_L/\mathfrak{a}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{a}|^n$.*

(*iii*) *Dado $\alpha \in \mathcal{O}_K$ non nulo tense que $|\mathcal{O}_K/\alpha\mathcal{O}_K| = |\,\mathrm{N}_{\mathbb{Q}}^K(\alpha)|$.*

Demostración. A demostración atópase en [6, pp. 46-49]. □

Teorema 3.11. *Sexa $L|K$ unha extensión de grao n, dado $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ tal que $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}$ tense que $\sum_{i=1}^{\mathbf{g}} \mathbf{e}_i\,\mathbf{f}_i = n$, onde $\mathbf{e}_i = \mathbf{e}_{\mathfrak{P}_i/\mathfrak{p}}$ e $\mathbf{f}_i = \mathbf{f}_{\mathfrak{P}_i/\mathfrak{p}}$.*

Demostración. Como $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}$ empregando o apartado (i) do Teorema 3.10 obtemos:

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = \prod_{i=1}^{\mathbf{g}} |\mathcal{O}_L/\mathfrak{P}_i|^{\mathbf{e}_i} = \prod_{i=1}^{\mathbf{g}} (|\mathfrak{p}|^{\mathbf{f}_i})^{\mathbf{e}_i}.$$

Ademais, aplicando o apartado (ii) do Teorema 3.10, temos que $|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K\mathfrak{p}|^n$ obtendo así o resultado. □

Antes vimos o significado de que un primo $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ ramifique ou non ramifique en $\mathcal{O}_L$ agora imos ver que significa que ramifique completamente.

Definición 3.12. Sexa $L|K$ unha extensión de corpos de números de grao n, dicimos que un primo $\mathfrak{p}$ de $\mathcal{O}_K$ *ramifica completamente* en $\mathcal{O}_L$ se $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$, con $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$. Grazas ao Teorema 3.11, sabemos que isto equivale a dicir que hai un único primo de $\mathcal{O}_L$ sobre $\mathfrak{p}$.

3.2. Escisión de primos en extensións de Galois

As extensións coas que imos traballar na demostración do Teorema de Kronecker-Weber van a ser extensións de Galois polo tanto imos ver coma se comportan a descomposición de ideais primos nestas extensións.

Dada unha extensión normal de corpos de números $L|K$, se tomamos un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$, con factorización en $\mathcal{O}_L$ da forma $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}$, entón fixado un $\mathfrak{P}_i$ a súa imaxe mediante

$\sigma \in \mathrm{Gal}_K(L)$ vai ser $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Isto débese a que a imaxe de $\sigma(\mathfrak{P}_i)$ é un ideal primo que está sobre $\sigma(\mathfrak{p}) = \mathfrak{p}$. O seguinte teorema danos aínda máis información sobre coma actúa o grupo de Galois de $L|K$ sobre estes primos:

Teorema 3.13. *Sexa $L|K$ unha extensión de Galois de corpos de números. Dados $\mathfrak{P}$ e $\mathfrak{P}'$ primos de $\mathcal{O}_L$ sobre $\mathfrak{p}\,\mathrm{Spm}(\mathcal{O}_K)$ tense que existe $\sigma \in \mathrm{Gal}_K(L)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Demostración. Supoñamos que o enunciado é falso, é dicir, $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$, $\forall \sigma \in \mathrm{Gal}_K(L)$ entón podemos formular o sistema de congruencias

$$\begin{cases} x \equiv 0 \,(\mathrm{mod}\ \mathfrak{P}') \\ x \equiv 1 \,(\mathrm{mod}\ \sigma(\mathfrak{P})),\ \forall \sigma \in \mathrm{Gal}_K(L) \end{cases}$$

Como a imaxe de $\sigma(\mathfrak{P})$ é un ideal primo non nulo, e polo tanto maximal, podemos aplicar o Teorema Chino dos Restos e obtemos unha solución $\alpha \in \mathcal{O}_L$. Se consideramos a $\mathrm{N}_K^L(\alpha)$ tense que $\mathrm{N}_K^L(\alpha) \in \mathcal{O}_K \cap \mathfrak{P}' = \mathfrak{p}$, porque $\alpha \in \mathfrak{P}'$ é un dos elementos que aparece no produto que define a norma. Por outro lado, tense que $\alpha \neq \sigma(\mathfrak{P})$ entón $\sigma^{-1}(\alpha) \neq \mathfrak{P}$, $\forall \sigma \in \mathrm{Gal}_K(L)$. Obsérvese que a $\mathrm{N}_K^L(\alpha)$ pódese expresar coma o produto de tódolos $\sigma^{-1}(\alpha)$ e así $\mathrm{N}_K^L(\alpha) \notin \mathfrak{P}$, por ser este un ideal primo. Chegamos a unha contradición ao ter $\mathrm{N}_K^L(\alpha) \in \mathfrak{p} \subseteq \mathfrak{P}$. □

Corolario 3.14. *Se $L|K$ é unha extensión normal, dados $\mathfrak{P}$ e $\mathfrak{P}'$ primos de $\mathcal{O}_L$ sobre $\mathfrak{p}$ primo $\mathcal{O}_K$ tense $\mathbf{e}_{\mathfrak{P}/\mathfrak{p}} = \mathbf{e}_{\mathfrak{P}'/\mathfrak{p}}$ e $\mathbf{f}_{\mathfrak{P}/\mathfrak{p}} = \mathbf{f}_{\mathfrak{P}'/\mathfrak{p}}$, denotaremos estes valores por $\mathbf{e}$ e $\mathbf{f}$. Coma consecuencia, se $n = [L\colon K]$ e $\mathbf{g} = \mathbf{g}_{\mathfrak{p}}$, tense $\mathbf{g}\,\mathbf{e}\,\mathbf{f} = n$.*

Demostración. Se $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}$ é a descomposición de $\mathfrak{p}$ en $\mathcal{O}_L$ podemos supoñer sen perdida de xeneralidade que $\mathfrak{P} = \mathfrak{P}_1$ e $\mathfrak{P}' = \mathfrak{P}_2$. Tomemos $\sigma \in \mathrm{Gal}_K(L)$ tal que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$, sabemos que $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$ entón

$$\prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i} = \mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}) = \prod_{i=1}^{\mathbf{g}} \sigma(\mathfrak{P}_i)^{\mathbf{e}_i} = \mathfrak{P}_2^{\mathbf{e}_1}\mathfrak{P}_1^{\mathbf{e}_2} \prod_{i=3}^{\mathbf{g}} \mathfrak{P}_i^{\mathbf{e}_i}.$$

Pola unicidade da descomposición podemos concluír que $\mathbf{e}_{\mathfrak{P}/\mathfrak{p}} = \mathbf{e}_1 = \mathbf{e}_2 = \mathbf{e}_{\mathfrak{P}'/\mathfrak{p}}$.

Sabemos que $\sigma : L \longrightarrow L$ é un K-isomorfismo entón $\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_L\sigma(\mathfrak{P}) \cong \mathcal{O}_L/\mathfrak{P}'$ e así $\mathbf{f}_{\mathfrak{P}/\mathfrak{p}} = \mathbf{f}_{\mathfrak{P}'/\mathfrak{p}} = \mathbf{f}$.

A última parte do enunciado é inmediata a partir do que acabamos de demostrar e do Teorema 3.11, $\mathbf{g}\,\mathbf{e}\,\mathbf{f} = \sum_{i=1}^{\mathbf{g}} \mathbf{e}_i\,\mathbf{f}_i = n$. □

3.3. O discriminante e o diferente na ramificación de primos

Nesta sección imos estudar que primos de $\mathcal{O}_K$ ramifican en $\mathcal{O}_L$, onde $L|K$ é unha extensión de corpos de números alxébricos. Para isto imos empregar o discriminante e o ideal diferente.

Comecemos polo discriminante, imos traballar coa extensión $K|\mathbb{Q}$ e veremos que primos $p \in \mathbb{Z}$ *ramifican en* $\mathcal{O}_K$, enténdese que p ramifica en $\mathcal{O}_K$ cando o ideal $p\mathbb{Z}$ ramifica en $\mathcal{O}_K$.

O discriminante tamén se pode empregar para estudar a ramificación nunha extensión de corpos de números $L|K$, para isto habería que definir o ideal discriminante o cal non será necesario neste traballo, pódese consultar máis información en [8].

Teorema 3.15. *Sexa $K|\mathbb{Q}$ unha extensión de corpos de números. Dado $p \in \mathbb{Z}$ primo tense que p ramifica en $\mathcal{O}_K$ se, e só se, $p \mid \operatorname{disc}(\mathcal{O}_K)$.*

Demostración. A demostración de que se p ramifica en $\mathcal{O}_K$ entón $p \mid \operatorname{disc}(\mathcal{O}_K)$ pódese atopar en [6, pp. 50-51] A demostración da outra implicación atópase en [6, pp. 79-80]. □

Corolario 3.16. *Dada unha extensión de corpos de números $K|\mathbb{Q}$ hai, como moito, un número finito de primos de $\mathbb{Z}$ que ramifiquen en $\mathcal{O}_K$.*

Demostración. É inmediato a partir do Teorema 3.15. □

Corolario 3.17. *Dada unha extensión de corpos de números $L|K$ hai, como moito, un número finito de primos de $\mathcal{O}_K$ que ramifiquen en $\mathcal{O}_L$.*

Demostración. Dado $\mathfrak{p}$ un primo de $\mathcal{O}_K$ que ramifique en $\mathcal{O}_L$ temos que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ tamén ramifica en $\mathcal{O}_L$, grazas á Proposición 3.9. O número de primos de $\mathbb{Z}$ que ramifican en $\mathcal{O}_L$ é finito e ademais, fixado un destes primos, só hai un número finito de primos de $\mathcal{O}_K$ que estean sobre el. Entón só pode haber un número finito de primos de $\mathcal{O}_K$ que ramifiquen en $\mathcal{O}_L$. □

A continuación veremos coma ramifica un primo $p \in \mathbb{Z}$ nunha extensión ciclotómica do tipo $\mathbb{Q}(\varepsilon_n)|\mathbb{Q}$.

Lema 3.18. *Sexan $p, k > 0$ enteiros, $\varepsilon_{p^k} \in \mathbb{C}$ unha raíz primitiva p^k-ésima da unidade, e consideremos a extensión $\mathbb{Q}(\varepsilon_{p^k})|\mathbb{Q}$. Entón o primo $p \in \mathbb{Z}$ ramifica completamente en $\mathcal{O}_{\mathbb{Q}(\varepsilon_{p^k})}$ e ademais $p\mathbb{Z}[\varepsilon_{p^k}] = (1-\varepsilon_{p^k})^{\varphi(p^k)}$.*

Demostración. Denotemos por $n = p^k$. O primeiro que faremos é probar que $p = u(1-\varepsilon_n)^{\varphi(n)}$ en $\mathbb{Z}[\varepsilon_{p^k}]$. Polo Lema 2.27 verifícase que

$$p = \prod_{i \in \{1 \leq i \leq n,\, p \nmid i\}} (1 - \varepsilon_n^i)$$

Fixado $i \in \mathbb{N}$ tal que $1 \leq i \leq n$ e $p \nmid i$, sabemos que ε_n^i é unha raíz primitiva polo tanto $\exists j \in \mathbb{N}$ tal que $\varepsilon_n = (\varepsilon_n^i)^j$ e temos:

$$\frac{1-\varepsilon_n^i}{1-\varepsilon_n} = 1 + \varepsilon_n + \cdots + \varepsilon_n^{i-1},$$

$$\frac{1-\varepsilon_n}{1-\varepsilon_n^i} = \frac{1-(\varepsilon_n^i)^j}{1-\varepsilon_n^i} = 1+\varepsilon_n^i+\cdots+(\varepsilon_n^i)^{j-1}$$

É dicir, $1+\varepsilon_n+\cdots+\varepsilon_n^i-1$ é unha unidade de $\mathbb{Z}[\varepsilon_n]$. Con todo isto podemos escribir

$$p = \prod_{i\in\{1\leq i\leq n,\, p\nmid i\}} (1-\varepsilon_n^i) = \prod_{i\in\{1\leq i\leq n,\, p\nmid i\}} (1-\varepsilon_n)(1+\varepsilon_n+\cdots+\varepsilon_n^i-1) = u(1-\varepsilon_n)^{\varphi(n)}$$

Entón $p\mathbb{Z}[\varepsilon_n] = (1-\varepsilon_n)^{\varphi(n)}$. Se tomamos $\mathfrak{P} \in \operatorname{Spec}(\mathbb{Z}[\varepsilon_n])$ que divida a $(1-\varepsilon_n)$ temos que $\mathbf{e}_{\mathfrak{P}/p\mathbb{Z}} \geq \varphi(n)$. Ademais $[\mathbb{Q}(\varepsilon_n)\colon \mathbb{Q}] = \varphi(n)$ e aplicando o Corolario 3.14 podemos concluír que $\mathfrak{P} = (1-\varepsilon_n)$ e $p\mathbb{Z}[\varepsilon_n] = \mathfrak{P}^{\varphi(n)}$ é a factorización en primos de $\mathbb{Z}[\varepsilon_n]$. Queda demostrado que p ramifica completamente. □

Lema 3.19. *Sexa $n>0$ un enteiro, $\varepsilon_n \in \mathbb{C}$ unha raíz primitiva n-ésima da unidade, e consideremos a extensión $\mathbb{Q}(\varepsilon_n)|\mathbb{Q}$. Se o primo $p\in\mathbb{Z}$ e tal que $p\nmid n$, entón p non ramifica en $\mathbb{Z}[\varepsilon_n]$ ademais, dado $\mathfrak{P}$ un primo sobre $p\mathbb{Z}$, $\mathbf{f}_{\mathfrak{P}/p\mathbb{Z}}$ é a orde multiplicativa de $p \pmod n$.*

Demostración. Para probar que p non ramifica en $\mathbb{Z}[\varepsilon_n]$ imos empregar o Teorema 3.15. Sabemos pola Proposición 2.26 que $\operatorname{disc}(\mathbb{Z}[\varepsilon_n]) \mid n^{\varphi(n)}$ entón como $p\nmid n$ tense que $p\nmid \operatorname{disc}(\mathbb{Z}[\varepsilon_n])$ e necesariamente p non ramifica en $\mathbb{Z}[\varepsilon_n]$.

Entón $p\mathbb{Z}[\varepsilon_n] = \prod_{i=1}^{\mathbf{g}} \mathfrak{P}_i$ e, como a extensión é normal, polo Corolario 3.14 temos $\mathbf{g}\,\mathbf{f} = \varphi(n)$. Imos ver que $\mathbf{f}$ é a orde de $p \pmod n$. Empregaremos a Proposición 1.14, sexa Ψ o isomorfismo definido na demostración da proposición como $p\nmid n$ podemos tomar $\sigma \in \operatorname{Gal}_{\mathbb{Q}}(\varepsilon_n)$ tal que $\Psi(\overline{p}) = \sigma$, é dicir, $\sigma(\varepsilon_n) = \varepsilon_n^p$. O subgrupo $<\sigma>$ ten a mesma orde que $p \pmod n$ polo tanto basta ver que $<\sigma>$ ten orde $\mathbf{f}$.

Para ver o anterior tomemos $\mathfrak{P} \in \operatorname{Spm}(\mathbb{Z}[\varepsilon_n])$ sobre $p\in\mathbb{Z}$. Como $\mathbf{f} = [\mathbb{Z}[\varepsilon_n]/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]$ temos que o grupo de Galois de $\mathbb{Z}[\varepsilon_n]/\mathfrak{P}$ sobre $\mathbb{Z}/p\mathbb{Z}$ é cíclico de orde $\mathbf{f}$. Ademais está xerado por $\tau \in \operatorname{Gal}_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{Z}[\varepsilon_n]/\mathfrak{P})$ que envía un elemento de $\mathbb{Z}[\varepsilon_n]/\mathfrak{P}$ na súa potencia p-ésima (pódese consultar máis información sobre isto en [6]). Evidentemente a orde de τ é $\mathbf{f}$ entón se vemos que σ ten a mesma orde que τ teremos rematado coa demostración, probemos isto:

En primeiro lugar,

$$\sigma^r = \mathrm{id} \iff \varepsilon_n^{p^r} = \varepsilon_n \iff p^r \equiv 1 \pmod n$$

e

$$\tau^r = \mathrm{id} \iff \varepsilon_n^{p^r} \equiv \varepsilon_n \pmod{\mathfrak{P}}.$$

Probemos que tamén se ten a equivalencia seguinte

$$\varepsilon_n^{p^r} \equiv \varepsilon_n \pmod{\mathfrak{P}} \iff p^r \equiv 1 \pmod n.$$

A implicación cara a esquerda é inmediata. Probemos a outra, sexa $p^r \equiv b \pmod n$ con $1\leq b\leq n$ entón $\varepsilon_n^b = \varepsilon_n^{p^r} \equiv \varepsilon_n \pmod{\mathfrak{P}}$. Supoñamos agora que a igualdade $(1-\varepsilon)(1-\varepsilon^2)\cdots(1-\varepsilon^{n-1}) = n$

é certa, se $b > 1$ teríamos que $(1-\varepsilon)(1-\varepsilon^2)\cdots(1-\varepsilon^{b-1})\cdots(1-\varepsilon^{n-1}) \equiv 0 \pmod{\mathfrak{P}}$ e polo tanto $n \in \mathfrak{P}$ o cal entra en contradición co feito de que $\mathfrak{P} \cap \mathbb{Z} = p$ e $\mcd(n,p) = 1$. Entón $b = 1$ e $\sigma^r = \mathrm{id} \iff p^r \equiv 1 \pmod{n} \iff \tau^r = \mathrm{id}$, é dicir, teñen a mesma orde coma queríamos probar.

Falta por demostrar que $(1-\varepsilon)(1-\varepsilon^2)\cdots(1-\varepsilon^{n-1}) = n$, tomemos

$$f(X) = \frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \cdots + X^+1$$

Sabemos que as $n-1$ raíces de f son as n-ésimas raíces da unidade excluíndo o un entón podemos escribir $f(X) = (X-\varepsilon)(X-\varepsilon^2)\cdots(X-\varepsilon^{n-1})$, así $f(1) = (1-\varepsilon)(1-\varepsilon^2)\cdots(1-\varepsilon^{n-1}) = n$. □

Teorema 3.20. *Sexa a extensión ciclotómica $\mathbb{Q}(\varepsilon_n)|\mathbb{Q}$, fixemos p primo de $\mathbb{Z}$ e escribamos $n = p^k m$ tal que $p \nmid m$. Entón, dado $\mathfrak{P} \in \mathrm{Spec}(\mathbb{Z}[\varepsilon_n])$ sobre $p\mathbb{Z}$, $\mathbf{e}_{\mathfrak{P}/p\mathbb{Z}} = \varphi(p^k)$ e $\boldsymbol{f}_{\mathfrak{P}/p\mathbb{Z}}$ é a orde multiplicativa de $p \pmod{m}$.*

Demostración. Imos empregar os dous lemas anteriores entón consideremos os aneis $\mathbb{Z}[\varepsilon_m]$ e $\mathbb{Z}[\varepsilon_{p^k}]$. Polo Lema 3.19 sabemos que en $\mathbb{Z}[\varepsilon_m]$ o primo p non ramifica obtendo $p\mathbb{Z}[\varepsilon_m] = \prod_{i=1}^{\mathbf{g}} \mathfrak{p}_i$, ademais $\mathbf{f} = \mathbf{f}_{\mathfrak{p}_i/p\mathbb{Z}}$ é a orde multiplicativa de $p \pmod{m}$. Tomemos $\mathfrak{P}_1, \ldots, \mathfrak{P}_{\mathbf{g}}$ primos de $\mathbb{Z}[\varepsilon_n]$ tales que $\mathfrak{P}_i$ está sobre $\mathfrak{p}_i$ en $\mathbb{Z}[\varepsilon_m]$. Entón $\mathfrak{P}_i$ está sobre $p\mathbb{Z}$ en $\mathbb{Z}$ e $g_{p\mathbb{Z}}(\mathbb{Q}(\varepsilon_n)|\mathbb{Q}) \geq g$. Por outro lado, polo Lema 3.18 $\mathfrak{P}_i$ está sobre $(1-\varepsilon_{p^k})$ en $\mathbb{Z}[\varepsilon_{p^k}]$ e ademais $\mathbf{e}_{(1-\varepsilon_{p^k})/p\mathbb{Z}} = \varphi(p^k)$.

Empregando a Proposición 3.9 obtemos o seguinte:

$$\mathbf{e}_{\mathfrak{P}/p\mathbb{Z}} \geq \mathbf{e}_{(1-\varepsilon_{p^k})/p\mathbb{Z}} = \varphi(p^k)$$

$$\mathbf{f}_{\mathfrak{P}/p\mathbb{Z}} \geq \mathbf{f}_{\mathfrak{p}/p\mathbb{Z}} = \mathbf{f}$$

Ademais como $\mathbf{g}\,\mathbf{f} = \varphi(m)$, polo Lema 3.19, se multiplicamos esta identidade por $\varphi(p^k)$ obtemos $\varphi(p^k)\,\mathbf{g}\,\mathbf{f} = \varphi(n)$ e necesariamente a única posibilidade é $\mathbf{e}_{\mathfrak{P}/p\mathbb{Z}} = \varphi(p^k)$ e $\mathbf{f}_{\mathfrak{P}/p\mathbb{Z}} = \mathbf{f}$. □

Imos rematar este capítulo falando sobre o ideal diferente. Dada unha extensión $K|\mathbb{Q}$ o ideal diferente permítenos saber que primos de $\mathcal{O}_K$ ramifican sobre $\mathbb{Z}$ e polo tanto tamén sabemos que primos de $\mathbb{Z}$ ramifican en $\mathcal{O}_K$. Enténdese que nunha extensión de corpos de números $L|K$ un ideal $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ *ramifica sobre* $\mathcal{O}_K$ se $\mathbf{e}_{\mathfrak{P}/\mathfrak{P}\cap\mathcal{O}_K} > 1$. Resulta evidente que o diferente danos máis información ca o discriminante porque este só nos permite saber que primos de $\mathbb{Z}$ ramifican en $\mathcal{O}_K$ pero non cales son os primos de $\mathcal{O}_K$ que ramifican sobre $\mathbb{Q}$.

Se extensión non ten corpo base $\mathbb{Q}$, é dicir temos unha extensión de corpos de números alxébricos $L|K$, o resultado que acabamos de explicar sobre o diferente pódese xeneralizar: dado un ideal $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ o ideal diferente permítenos saber se $\mathfrak{P}$ ramifica sobre $\mathcal{O}_K$. Máis información sobre isto último pódese consultar en [11].

Nesta parte centrarémonos en dar as definicións e resultados que necesitamos para a demostración do Teorema de Kronecker-Weber omitindo a proba dos resultados, seguiremos a referencia [9].

Definición 3.21. Sexa M un $\mathcal{O}_K$-submódulo de L que contén unha base de $L|K$, definimos o *dual* de M como $M^* := \{\alpha \in L\,;\, \mathrm{T}_L^K(\alpha M) \subseteq \mathcal{O}_K\}$

Definición 3.22. Sexa M un $\mathcal{O}_K$-submódulo de L que contén unha base de $L|K$, definimos $M^{-1} := \{\alpha \in L\,;, \alpha M \subseteq \mathcal{O}_L\}$

Para unha extensión $L|K$ pódese considerar $\mathcal{O}_L$ coma un $\mathcal{O}_K$-módulo que contén unha base de $L|K$.

Definición 3.23. Definimos o *ideal diferente* dunha extensión $L|K$ como $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K) := (\mathcal{O}_L^*)^{-1}$.

Unha vez definido podemos ver coma se aplica na ramificación dos primos dunha extensión $K|\mathbb{Q}$:

Teorema 3.24. *Sexa a extensión $K|\mathbb{Q}$ e $\mathfrak{p}$ un primo de $\mathcal{O}_K$ sobre p primo de $\mathbb{Z}$. Entón dado o ideal diferente de K, $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$, os primos que o dividen son precisamente os primos de $\mathcal{O}_K$ que ramifican sobre $\mathbb{Z}$.*

En concreto, dado un ideal $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ sobre $p \in \mathbb{Z}$ con $\boldsymbol{e} = \boldsymbol{e}_{\mathfrak{p}|p\mathbb{Z}}$, tense:

(*i*) *Se $e \not\equiv 0 \pmod p$, a potencia exacta de $\mathfrak{p}$ dividindo a $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$ é $\mathfrak{p}^{e-1}$.*

(*ii*) *Se $e \equiv 0 \pmod p$, $\mathfrak{p}^e$ divide a $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$.*

Demostración. A demostración atópase en [2, Theorem 4.8 (Dedekind), pp. 8-10]. □

Na demostración do Teorema de Kronecker-Weber imos empregar o diferente dunha extensión $L|K$, algún dos resultados que necesitaremos son os seguintes:

Proposición 3.25. *Sexan K,L e M corpos de números alxébricos tal que $K \subseteq L \subseteq M$. Entón* $\mathrm{diff}(\mathcal{O}_M|\mathcal{O}_K) = \mathrm{diff}(\mathcal{O}_M|\mathcal{O}_L)(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)\mathcal{O}_L)$.

Demostración. A demostración pódese consultar en [9, Proposition 3, pp. 5-6]. □

Proposición 3.26. *Sexa $L|K$ unha extensión de corpos de números alxébricos de grao n. Tomemos un primo $\mathfrak{p}$ de $\mathcal{O}_K$ que ramifique completamente en $\mathcal{O}_L$ entón fixado $\pi \in \mathfrak{P} - \mathfrak{P}^2$, onde $\mathfrak{P}$ é o primo de $\mathcal{O}_L$ que está sobre $\mathfrak{p}$, tense o seguinte:*

(*i*) *$\{1, \pi, \ldots, \pi^{n-1}\}$ é unha base de L sobre K.*

(*ii*) *Se* $\alpha_0, \ldots, \alpha_{n-1} \in \mathcal{O}_K$ *cumpren que* $a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \in \mathfrak{P}^n$ *entón* $a_i \in \mathfrak{p}$ *con* $i \in \{0, \ldots, n-1\}$.

(*iii*) *Existe un elemento* $\beta \in \mathcal{O}_K - \mathfrak{p}$ *tal que* $\beta\mathcal{O}_L \subseteq \mathcal{O}_K[\pi]$.

Demostración. A demostración atópase en [9, Lemma 4, pp. 8-9]. □

Para rematar esta sección imos enunciaremos o seguinte resultado que será imprescindible para a demostración do Teorema de Kronecker-Weber:

Teorema 3.27 (Minkowski)**.** *Sexa* K *un corpo de números distinto de* $\mathbb{Q}$ *entón* $\operatorname{disc}(|\mathcal{O}_K)| > 1$.

O incluímos nesta sección porque grazas a el podemos asegurar que se temos un corpo de números K distinto de $\mathbb{Q}$ entón vai a haber polo menos un primo de $\mathbb{Z}$ que ramifique en $\mathcal{O}_K$. Non incluímos a demostración deste teorema porque á súa complexidade supera os obxectivos deste traballo (pódese consultar en [6, Chapter 5, Corollary 3, p. 96]).

Capítulo 4

O grupos de Galois na descomposición de primos

Neste capítulo imos traballar con extensións normais de corpos de números $L|K$ e veremos coma se emprega o seu grupo de Galois para estudar a factorización dos ideais primos da extensión $L|K$.

4.1. Grupo de descomposición e grupo de inercia

Sexa $L|K$ unha extensión normal de corpos de números. Dado un ideal primo $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$, comezaremos definindo o seu grupo de descomposición e grupo de inercia.

Definición 4.1. Sexa unha extensión de Galois $L|K$, dado un primo $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ definimos:
O *grupo de descomposición* de $\mathfrak{P}$

$$\mathrm{D} = \mathrm{D}_{\mathfrak{P}}(L|K) := \{\sigma \in \mathrm{Gal}(L|K) \ ; \ \sigma(\mathfrak{P}) = \mathfrak{P} \ \}.$$

O *grupo de inercia* de $\mathfrak{P}$

$$\mathrm{I} = \mathrm{I}_{\mathfrak{P}}(L|K) := \{\sigma \in \mathrm{Gal}(L|K) \ ; \ \sigma(\alpha) \equiv \alpha (\mathrm{mod}\ \mathfrak{P}), \forall \alpha \in \mathcal{O}_L \ \}$$

Nótese que o grupo de inercia é un subgrupo do grupo de descomposición, se tomamos $\sigma \in \mathrm{I}$ vaise ter $\sigma(\alpha) \equiv \alpha \,(\mathrm{mod}\ \mathfrak{P}) \equiv 0 \,(\mathrm{mod}\ \mathfrak{P})$, $\forall \alpha \in \mathfrak{P}$, e polo tanto $\sigma(\mathfrak{P}) = \mathfrak{P}$, é dicir, $\sigma \in \mathrm{D}$.

Proposición 4.2. *Nas condicións da definición anterior,* I *é un subgrupo normal de* D *e temos un homomorfismo inxectivo de grupos* $\mathrm{D}\,/\,\mathrm{I} \to \mathrm{Gal}_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{P})$*, onde* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$*.*

Demostración. A demostración atópase en [1, pp. 50-51]. □

Como o grupo de descomposición e de inercia son subgrupos do grupo de Galois podemos considerar o corpo fixo por estes os cales denomínamos coma *corpo de descomposición* e *corpo de inercia*, respectivamente. Se consideramos unha extensión de Galois $L|K$ os corpos L^{D} e L^{I} van ser subcorpos de L, polo tanto dado un primo $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ sobre $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ podemos estudar a descomposición de $\mathfrak{p}$ en L^{D} e L^{I}, veremos isto no seguinte teorema. Imos denotar por $\mathfrak{P}^{\mathrm{D}} = \mathfrak{P} \cap \mathcal{O}_{L^{\mathrm{D}}}$ e $\mathfrak{P}^{\mathrm{I}} = \mathfrak{P} \cap \mathcal{O}_{L^{\mathrm{I}}}$ aos primos sobre os que está $\mathfrak{P}$ no anel de enteiros correspondente.

Teorema 4.3. *Coa notación establecida e escribindo* $\mathrm{I} = \mathrm{I}_{\mathfrak{P}}(L|K)$, $D = \mathrm{D}_{\mathfrak{P}}(L|K)$ *e* $G = \mathrm{Gal}(L|K)$, *temos o seguinte diagrama asociado a cadea de subgrupos* $\mathrm{I} < \mathrm{D} < G$*:*

$$\begin{array}{ccccccc}
\mathfrak{p} & \xhookrightarrow[\mathbf{f}_{\mathfrak{P}^D/\mathfrak{p}} = 1]{\mathbf{e}_{\mathfrak{P}^D/\mathfrak{p}} = 1} & \mathfrak{P}^D & \xhookrightarrow[\mathbf{f}_{\mathfrak{P}^{\mathrm{I}}/\mathfrak{P}^D} = \mathbf{f}]{\mathbf{e}_{\mathfrak{P}^{\mathrm{I}}/\mathfrak{P}^D} = 1} & \mathfrak{P}^T & \xhookrightarrow[\mathbf{f}_{\mathfrak{P}/\mathfrak{P}^{\mathrm{I}}} = 1]{\mathbf{e}_{\mathfrak{P}/\mathfrak{P}^{\mathrm{I}}} = \mathbf{e}} & \mathfrak{P} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
K & \xhookrightarrow{[L^D : K] = \mathbf{g}} & L^D & \xhookrightarrow{[L^{\mathrm{I}} : L^D] = \mathbf{f}} & L^{\mathrm{I}} & \xhookrightarrow{[L : L^{\mathrm{I}}] = \mathbf{e}} & L
\end{array}$$

Onde $\mathbf{e} = \mathbf{e}_{\mathfrak{P}/\mathfrak{p}}$, $\mathbf{f} = \mathbf{f}_{\mathfrak{P}/\mathfrak{p}}$ *e* $\mathbf{g} = \mathbf{g}_{\mathfrak{p}}(L|K)$.

Demostración. A demostración atópase en [6, pp. 70-71]. □

Dous corolarios deste teorema son os seguintes.

Corolario 4.4. *O homomorfismo inxectivo de grupos* $\mathrm{D}\,/\,\mathrm{I} \to \mathrm{Gal}_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{P})$ *definindo na Proposición 4.2 é un isomorfismo.*

Demostración. Grazas ao teorema anterior podemos asegurar que $|\,\mathrm{D}\,/\,\mathrm{I}\,| = [L^{\mathrm{I}}\colon L^{\mathrm{D}}] = \mathbf{f} = |\,\mathrm{Gal}_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{P})|$, polo tanto temos un encaixe sobrexectivo, é dicir, un isomorfismo. □

Corolario 4.5. *Nas condicións do teorema anterior, se* D *é un subgrupo normal de* $\mathrm{Gal}_K(L)$ *entón* $\mathfrak{p}$ *escinde en* g *primos distintos,* $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$*, en* L^{D}*. Se ademais* I *tamén é normal cada primo* $\mathfrak{P}_i$ *mantense primo en* $\mathfrak{P}^{\mathrm{I}}$*.*

Demostración. Se D é un grupo normal de $\mathrm{Gal}_K(L)$ entón $L^{\mathrm{D}}|\mathbb{Q}$ é unha extensión normal entón, polo Corolario 3.14, todo primo de $\mathcal{O}_{L^{\mathrm{D}}}$ sobre $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ ten o mesmo índice de ramificación e grao de inercia que $\mathfrak{P}^{\mathrm{D}}$ os cales sabemos que son 1, polo teorema anterior. Tamén sabemos polo Corolario 3.14 que $\mathbf{g}_{\mathfrak{p}}(L^{\mathrm{D}}|K) = [L^{\mathrm{D}}\colon K] = \mathbf{g}$ quedando demostrada a primeira parte do enunciado. Imos denotar por $\mathfrak{P}_1, \ldots, \mathfrak{P}_{\mathbf{g}}$ aos primos de $\mathcal{O}_{L^{\mathrm{D}}}$ que están sobre $\mathfrak{p}$.

Como hai, tanto, $\mathbf{g}$ primos de $\mathcal{O}_L$ sobre $\mathfrak{p}$, coma, $\mathbf{g}$ primos de $\mathcal{O}_{L^{\mathrm{D}}}$ sobre $\mathfrak{p}$ entón hai exactamente $\mathbf{g}$ primos de $\mathcal{O}_{L^{\mathrm{I}}}$ que estean sobre $\mathfrak{p}$. Deste modo, para cada $i \in \{1, \ldots, \mathbf{g}\}$ hai un único primo de $\mathcal{O}_{L^{\mathrm{I}}}$, ao que denotamos por $\mathfrak{P}'_i$, que estea sobre $\mathfrak{P}_i$. Se I é normal entón $L^{\mathrm{I}}|K$ tamén

é normal e teríamos que tódolos $\mathfrak{P}'_i$ terían o mesmo índice de ramificación sobre $\mathfrak{p}$ que $\mathfrak{P}^{\mathrm{I}}$ o cal sabemos polo teorema anterior que é 1. Así $\mathfrak{P}\mathcal{O}_{L^{\mathrm{I}}} = \mathfrak{P}'_i$, é dicir, $\mathfrak{P}_i$ mantense primo en $\mathcal{O}_{L^{\mathrm{I}}}$. □

Unha consecuencia do Teorema 4.3 é o resultado seguinte.

Teorema 4.6. *Sexa $L|K$ unha extensión de Galois e tomemos $\mathfrak{P}$ primo de $\mathcal{O}_L$ sobre $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$. Se denotamos por K' a un corpo intermedio da extensión $L|K$ e por $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{K'}$ temos o seguinte:*

(i) L^{D} *é o maior K' tal que* $\mathbf{e}_{\mathfrak{P}'/\mathfrak{p}} = \mathbf{f}_{\mathfrak{P}'/\mathfrak{p}} = 1$.

(ii) L^{D} *é o menor K' tal que $\mathfrak{P}$ é o único primo de $\mathcal{O}_L$ sobre $\mathfrak{P}'$.*

(iii) L^{I} *é o maior K' tal que* $\mathbf{e}_{\mathfrak{P}'/\mathfrak{p}} = 1$.

(iv) L^{I} *é o menor K' tal que $\mathfrak{P}$ ramifica completamente sobre $\mathfrak{P}'$.*

Demostración. A demostración pódese consultar en [6, pp. 73-74]. □

A seguinte proposición empregarase na demostración do Teorema de Kronecker-Weber porque imos traballar de forma reitera coa composición de distintos corpos.

Proposición 4.7. *Sexan $L|K$ e $M|K$ extensións de corpos de números e LM a composición de L e M. Se dado un primo non nulo $\mathfrak{p}$ de $\mathcal{O}_K$ este non ramifica en $\mathcal{O}_L$ nin $\mathcal{O}_M$ entón tampouco o fai en $\mathcal{O}_{LM}$.*

Demostración. Sexa $\mathfrak{p}$ un primo de $\mathcal{O}_K$ que non ramifica en $\mathcal{O}_L$ nin $\mathcal{O}_M$ e fixemos $\mathfrak{P}$ un dos primos de $\mathcal{O}_{LM}$ que está sobre $\mathfrak{p}$. Se consideramos N unha extensión normal de K que conteña a LM podemos tomar $\mathfrak{P}' \in \mathrm{Spm}(\mathcal{O}_N)$ que estea sobre $\mathfrak{P}$. Polo tanto, $\mathfrak{P}'$ tamén está sobre $\mathfrak{p}$, tomando $\mathrm{I} = \mathrm{I}_{\mathfrak{P}'/\mathfrak{p}}$ sabemos polo teorema anterior, Teorema 4.6, que N^{I} é o maior corpo intermedio K' tal que $\mathbf{e}_{\mathfrak{P}'\cap\mathcal{O}_{K'}/\mathfrak{p}} = 1$. En consecuencia $L \subseteq N^{\mathrm{I}}$ e $M \subseteq N^{\mathrm{I}}$ tendo entón que $LM \subseteq N^{\mathrm{I}}$. Necesariamente $\mathfrak{P} = \mathfrak{P}' \cap \mathcal{O}_{LM}$ non ramifica sobre $\mathcal{O}_K$. Como isto ocorre para tódolos primos de LM que están sobre $\mathfrak{p}$ temos que $\mathfrak{p}$ non ramifica en LM. □

4.2. Grupos de ramificación

Neste sección definiremos os grupos de ramificación que van a ser subgrupos do grupo de descomposición. Defínense a continuación:

Definición 4.8. Sexa unha extensión de Galois de corpos de números $L|K$, dado un primo $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ definimos: O *m-ésimo grupo de ramificación* de $\mathfrak{P}$

$$\mathrm{V}_m = \mathrm{V}_m(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L|K)\,;\ \sigma(\alpha) \equiv \alpha (\mathrm{mod}\ \mathfrak{P}^{m+1}),\ \forall \alpha \in \mathcal{O}_L\ \} \tag{4.1}$$

Onde $\mathfrak{p}$ é o primo de $\mathcal{O}_K$ sobre o que está $\mathfrak{P}$.

Resulta inmediato que temos unha cadea descendente de subgrupos

$$\mathrm{I}_{\mathfrak{P}/\mathfrak{p}} = \mathrm{V}_0 \supseteq \mathrm{V}_1 \supseteq \cdots$$

e ademais van ser subgrupos normais de $\mathrm{D}_{\mathfrak{P}/\mathfrak{p}}$, próbase a continuación:

Proposición 4.9. *Nas condicións da definición anterior,* $\mathrm{V}_m = \mathrm{V}_m(\mathfrak{P}|\mathfrak{p})$ *é un subgrupo normal de* $\mathrm{D} = \mathrm{D}_{\mathfrak{P}/\mathfrak{p}}$.

Demostración. Sexa $\sigma \in \mathrm{D}$ e $\tau \in \mathrm{V}_m$ queremos ver que $\sigma^{-1}\tau\sigma \in \mathrm{V}_m$. Sexa $\alpha \in \mathcal{O}_L$ temos $\sigma^{-1}\tau\sigma(\alpha) - \alpha = \sigma^{-1}(\tau(\sigma(\alpha)) - \sigma(\alpha))$, como $\tau \in \mathrm{V}_m$ e $\sigma(\alpha) \in \mathcal{O}_L$ temos $\tau(\sigma(\alpha)) \equiv \sigma(\alpha) (\mathrm{mod}\ \mathfrak{P}^{m+1})$ e como $\sigma \in \mathrm{D}$ chegamos a que $\sigma^{-1}(\tau(\sigma(\alpha))) \equiv \sigma^{-1}(\sigma(\alpha)) (\mathrm{mod}\ \mathfrak{P}^{m+1})$, é dicir, $\sigma^{-1}\tau\sigma(\alpha) \equiv \alpha\,(\mathrm{mod}\ \mathfrak{P}^{m+1})$. Polo tanto $\sigma^{-1}\tau\sigma \in \mathrm{V}_m$. □

A continuación veremos varios resultados sobre os grupos de ramificación onde reflectirase a relación que hai entre grupos consecutivos. Dada unha extensión $L|K$ de Galois e $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ sobre $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$, imos denotar por $\mathrm{D} = \mathrm{D}_{\mathfrak{P}/\mathfrak{p}}$, $\mathrm{I} = \mathrm{I}_{\mathfrak{P}/\mathfrak{p}}$ e $\mathrm{V}_m = \mathrm{V}_m(\mathfrak{P}|\mathfrak{p})$.

Proposición 4.10. *Sexa $L|K$ unha extensión de Galois de corpos de números e $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$. Fixemos $\pi \in \mathfrak{P} - \mathfrak{P}^2$ entón dado $\sigma \in \mathrm{V}_{m-1}$ tense que $\sigma \in \mathrm{V}_m$ se, e só se, $\sigma(\pi) \equiv \pi\,(\mathrm{mod}\ \mathfrak{P}^{m+1})$.*

Demostración. A demostración atópase en [1, pp. 61-62]. □

Proposición 4.11. *Sexa $L|K$ extensión de Galois de corpos de números e sea $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$. Entón existe un encaixe de grupos, e dicir un homomorfismo inxectivo grupos, $\mathrm{I}\,/\,\mathrm{V}_1 \longrightarrow (\mathcal{O}_L/\mathfrak{P})^{\times}$.*

Demostración. A demostración atópase en [1, pp. 62-63]. □

Proposición 4.12. *Sexa a extensión $L|K$ de Galois de corpos de números e $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$. Entón existe un encaixe de $\mathrm{V}_{m-1}\,/\,\mathrm{V}_m$ no grupo aditivo $\mathcal{O}_L/\mathfrak{P}$, $\forall m \geq 2$, onde $\mathrm{V}_m = \mathrm{V}_m(\mathfrak{P}|\mathfrak{p})$.*

Demostración. A demostración atópase en [1, pp. 63-64]. □

Lema 4.13. *Dada unha extensión $L|K$ de Galois entre corpos de números temos que existe un natural $n \in \mathbb{N}$ suficientemente grande tal que V_n é trivial. Polo tanto $\mathrm{V}_m = \{\mathrm{id}\}$ $\forall m \geq n$.*

Demostración. Sexa $\mathrm{V}_m = \mathrm{V}_m(\mathfrak{P}|\mathfrak{p})$, para probar o enunciado imos ver primeiro que $\cap_{k=1}^{\infty}\mathfrak{P}^k = \{0\}$. Se supoñemos que $\cap_{k=1}^{\infty}\mathfrak{P}^k \neq \{0\}$ entón é un ideal non nulo de $\mathcal{O}_L$ e ten factorización en ideais primos de $\mathcal{O}_L$. Agora ben, $\cap_{k=1}^{\infty}\mathfrak{P}^k \subseteq \mathfrak{P}^m$, $\forall m \geq 1$ é dicir $\mathfrak{P}^m \mid \cap_{k=1}^{\infty}\mathfrak{P}^k$, $\forall m \geq 1$ pero

non pode ocorrer que na factorización dun ideal non nulo un dos ideais primos teña expoñente infinito, polo tanto $\cap_{k=1}^{\infty}\mathfrak{P}^k = \{0\}$.

Probemos que $\cap_{k=0}^{\infty}V_k = \{\mathrm{id}\}$, sexa $\sigma \in \cap_{k=0}^{\infty}V_k$ tense que, dado $\alpha \in \mathcal{O}_L$, $\sigma(\alpha) = \alpha \pmod{\mathfrak{P}^m}$, $\forall m \geq 1$. Entón $\sigma(\alpha) - \alpha \in \cap_{k=1}^{\infty}\mathfrak{P}^k = \{0\}$ e polo tanto $\sigma(\alpha) = \alpha$, $\forall \alpha \in \mathcal{O}_L$. Como sabemos que existe unha base de L formada por enteiros alxébricos temos que $\sigma(\alpha) = \alpha$, $\forall \alpha \in L$ o cal equivale a $\sigma = \mathrm{id}$.

Ademais os grupos V_m son finitos, entón a cadea descendente $V_0 \supseteq V_1 \supseteq \cdots$ é estacionaria e así, para n suficientemente grande, $V_n = \cap_{k=0}^{\infty}V_k = \{\mathrm{id}\}$. □

Proposición 4.14. *Sexa $K|\mathbb{Q}$ unha extensión de Galois, tomemos $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ sobre o primo $p \in \mathbb{Z}$. Entón tense que o primeiro grupo de ramificación $\mathrm{V}_1 = \mathrm{V}_1(\mathfrak{p}|p\mathbb{Z})$ é o p-Sylow do grupo de inercia $\mathrm{I} = \mathrm{I}_{\mathfrak{p}/p\mathbb{Z}}$.*

Demostración. Escribamos $|\,\mathrm{I}\,| = p^k n$ con $p \nmid n$. Podemos aplicar a Proposición 4.11 e temos que $|\,\mathrm{I}\,/\,\mathrm{V}_1\,|$ divide a $|(\mathcal{O}_K/\mathfrak{p})^{\times}| = |(\mathcal{O}_K/\mathfrak{p})| - 1$ pero, nas condicións do enunciado, $|(\mathcal{O}_K/\mathfrak{p})| - 1 = |\mathbb{Z}/p\mathbb{Z}|^{\mathrm{f}_{\mathfrak{p}/p}} - 1 = p - 1$ o cal non divide a p. Así

$$\left|\frac{\mathrm{I}}{\mathrm{V}_1}\right| = \frac{|\,\mathrm{I}\,|}{|\,\mathrm{V}_1\,|} = \frac{p^k n}{m}$$

Non divide a p e necesariamente $m = p^k m'$.

Queremos ver que $m' = 1$, se aplicamos a Proposición 4.12 temos que, para $r \geq 2$, $|\,\mathrm{V}_{r-1}\,/\,\mathrm{V}_r\,| = p^l$, con $l \geq 0$ porque a orde de $\mathrm{V}_{r-1}\,/\,\mathrm{V}_r$ divide a $|\mathcal{O}_K/\mathfrak{p}| = p^{\mathrm{f}_{\mathfrak{p}/p\mathbb{Z}}}$. Se $m' \neq 1$, por indución, teríamos que $m' \mid |V_r|$, $\forall r \geq 1$, o cal contradí o lema anterior, Lema 4.13, polo tanto $m' = 1$ e V_1, é un p-Sylow de I.

No enunciado dicimos que V_1 é o p-Sylow de I, non que sexa un p-Sylow, isto débese a que pola Proposición 4.9 V_1 é un subgrupo normal de D, polo tanto tamén é un subgrupo normal de I, en consecuencia, V_1 é o único p-Sylow. □

Proposición 4.15. *Nas condicións da Proposición 4.12, se $\mathrm{D}\,/\,\mathrm{V}_1$ é un grupo abeliano entón o encaixe manda $\mathrm{I}\,/\,\mathrm{V}_1$ en $(\mathcal{O}_K/\mathfrak{p})^{\times}$. Neste caso, $\mathrm{I}\,/\,\mathrm{V}_1$ é un grupo cíclico con orde dividindo a $|\mathcal{O}_K/\mathfrak{p}| - 1$.*

Demostración. A demostración atópase en [1, pp. 66-67]. □

A proposición anterior vai resultar especialmente útil se V_1 é trivial porque entón $\mathrm{I} \cong \mathrm{I}\,/\,\mathrm{V}_1$ e podemos asegurar que I é un grupo cíclico con orde dividindo a $|\mathcal{O}_K/\mathfrak{p}| - 1$. Se ademais atopámonos nas condicións da Proposición 4.14 e $\mathrm{V}_1 = \{\mathrm{id}\}$, é dicir $p \nmid |\,\mathrm{I}\,|$, entón a orde de I divide a $|\mathbb{Z}/p\mathbb{Z}| - 1 = p - 1$.

Para finalizar esta sección imos enunciar un teorema que relaciona os grupos de ramificación co ideal diferente.

Teorema 4.16. *Sexa $L|K$ unha extensión de Galois entre corpos de números, e $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ un primo que ramifica completamente en $\mathcal{O}_L$, sexa $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ o primo sobre $\mathfrak{p}$. Se d é a potencia exacta de $\mathfrak{P}$ dividindo a $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)$ tense:*

(*i*) *Fixado $\pi \in \mathfrak{P} - \mathfrak{P}^2$, d é igual a potencia exacta de $\mathfrak{P}$ dividindo a $f'(\pi)$ como ideal de $\mathcal{O}_L$, onde $f = \mathrm{Irr}(\pi, K)$.*

(*ii*) *$d = \sum_{m \geq 0}(|\,\mathrm{V}_m\,| - 1)$, onde $\mathrm{V}_m = \mathrm{V}_m(\mathfrak{P}|\mathfrak{p})$. Isto coñécese coma fórmula de Hilbert.*

Demostración. A demostración atópase en [9, Theorem 2, pp. 7-10]. □

Capítulo 5

Demostración do teorema de Kronecker-Weber

Neste capítulo demostraremos finalmente que toda extensión abeliana $K|\mathbb{Q}$ é ciclotómica.

Teorema 5.1 (Teorema de Kronecker-Weber)**.** *Dada unha extensión abeliana $K|\mathbb{Q}$, existe un enteiro positivo n e unha raíz primitiva n-ésima da unidade $\varepsilon_n \in \mathbb{C}$, de forma que K é un subcorpo do corpo ciclotómico $\mathbb{Q}(\varepsilon_n)$.*

Demostración. Comecemos xustificando que, consecuencia do Lema 5.2, é suficiente demostrar o Teorema de Kronecker-Weber para as extensións abelianas de grao a potencia dun primo. Facendo uso da notación do Lema 5.2, sendo $[K\colon \mathbb{Q}] = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ a factorización en primos do grao da extensión, existen extensións $K_i \,|\, \mathbb{Q}$ abelianas de grao $p_i^{\alpha_i}$ tales que $K_1 \cdots K_r = K$. Suposto demostrado que para cada unha das extensións $K_i \,|\, \mathbb{Q}$ existe $\varepsilon_{n_i} \in \mathbb{C}$ unha raíz primitiva n_i-ésima tal que $K_i \subset \mathbb{Q}(\varepsilon_{n_i})$. Entón, pola Proposición 1.13, tense que $K = K_1 \cdots K_r \subseteq \mathbb{Q}(\varepsilon_n)$, sendo $n = \operatorname{mcm}(n_1, \ldots, n_r)$.

A demostración do Teorema de Kronecker-Weber complétase demostrando que cada extensión abeliana $K|\mathbb{Q}$ con grao unha potencia dun primo $[K\colon \mathbb{Q}] = p^m$ é ciclotómica. Para a demostración deste resultado, pola Observación 5.4, facendo uso do Lema 5.3 podemos reducir a proba ao caso no que, ademais, na extensión abeliana $K|\mathbb{Q}$ ningún primo de $\mathbb{Z}$ distinto de p ramifique en K. Para extensións abelianas $K|\mathbb{Q}$ con esta hipótese adicional próbase o resultado na Proposición 5.5 cando $p = 2$ e o caso dos primos impares na Proposición 5.9. □

Dedicamos o resto do traballo á demostración dos resultados anunciados.

5.1. Redución ó caso de extensións abelianas de grao unha potencia dun primo

Comezaremos cun resultado que permítenos reducir a demostración do Teorema de Kronecker-Weber ao caso no que a extensión abeliana teña grao a potencia dun primo.

Lema 5.2. *Toda extensión abeliana $K\,|\,\mathbb{Q}$ é a composición de extensións abelianas con grao a potencia dun primo.*

Demostración. Sabemos que $G = \mathrm{Gal}_{\mathbb{Q}}(K)$ é un grupo abeliano finito, polo tanto, polo Teorema 1.4 existe un isomorfismo $\rho\colon \mathrm{Gal}_{\mathbb{Q}}(K) \to G_1 \times \cdots \times G_r$ con $|G_i| = p_i^{\alpha_i}$. Definimos, para cada $i \in \{1,\ldots,r\}$, $H_i < G$ tal que $\rho(H_i) = \prod_{j\neq i} G_j$. Se $K_i = K^{H_i}$ tense que, por ser $\mathrm{Gal}_{\mathbb{Q}}(K)$ abeliano, $K_i\,|\,\mathbb{Q}$ é normal e $\mathrm{Gal}_{\mathbb{Q}}(K_i) \cong G/H_i \cong G_i$. Deste modo, para cada $i \in \{1,\ldots,r\}$, a extensión $K_i\,|\,\mathbb{Q}$ é abeliana de grao $p_i^{\alpha_i}$. Ademais, $[K\colon \mathbb{Q}] = |G| = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, para comprobar que $K = K_1\cdots K_r$ basta con notar que $K_1\cdots K_r \subseteq K$ e que $[K_1\cdots K_r\colon \mathbb{Q}] = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. □

O lema que enunciamos a continuación vainos permitir reducir a demostración do Teorema de Kronecker-Weber ao caso no que ningún primo distinto de p, onde p^m é o grao de K sobre $\mathbb{Q}$, ramifique en K.

Lema 5.3. *Sexa $K|\mathbb{Q}$ unha extensión abeliana de grao $[K\colon \mathbb{Q}] = p^m$, e supoñamos que existe $q \in \mathbb{Z}$ un primo, $q \neq p$, que ramifica en $\mathcal{O}_K$. Entón existe unha extensión $K'\,|\,\mathbb{Q}$ cumprindo:*

(i) O primo $q \in \mathbb{Z}$ non ramifica en $\mathcal{O}_{K'}$ e calquera primo de $\mathbb{Z}$ que non ramifica en K tampouco o fai en K'.

(ii) A extensión $K'\,|\,\mathbb{Q}$ ten grado p^r, con $r \leq m$.

(iii) Se K' está contido nun corpo ciclotómico entón K tamén o está.

Demostración. Tomemos $q \neq p$ un primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$, entón podemos tomar $\mathfrak{q}$ primo de $\mathcal{O}_K$ sobre q tal que $\mathbf{e} := \mathbf{e}_{\mathfrak{q}/q} > 1$. Imos ver que existe un subcorpo $L \subseteq \mathbb{Q}(\varepsilon_q)$ tal que $[L\colon \mathbb{Q}] = q$.

En primeiro lugar, por ser $K\,|\,\mathbb{Q}$ normal, $\mathbf{e}$ divide a $[K\colon \mathbb{Q}]$ polo tanto $\mathbf{e} = p^k$ con $k \leq m$. Sexa $\mathrm{V}_1 = \mathrm{V}_1(\mathfrak{q}|q)$, sabemos, pola Proposición 4.14, que V_1 é un q-Sylow de $\mathrm{I} = \mathrm{I}_{\mathfrak{q}}(K|\mathbb{Q})$, pero, polo Teorema 4.3, a orde do grupo de inercia é $|\,\mathrm{I}\,| = \mathbf{e} = p^k$. Deste a única posibilidade é que $|\,\mathrm{V}_1\,| = 1$ o que equivale a $\mathrm{V}_1 = \{\mathrm{id}\}$. Grazas ao anterior temos que, tomando $\mathrm{D} = \mathrm{D}_{\mathfrak{q}}(K|\mathbb{Q})$, $\mathrm{D}\,/\,\mathrm{V}_1 \cong \mathrm{D} \subseteq \mathrm{Gal}_{\mathbb{Q}}(K)$ e polo tanto $\mathrm{D}\,/\,\mathrm{V}_1$ é abeliano e podemos aplicar a Proposición 4.15. Así chegamos a que $\mathrm{I} \cong \mathrm{I}\,/\,\mathrm{V}_1$ é cíclico con orde dividindo a $|\mathbb{Z}/q\mathbb{Z}| - 1 = q - 1$ polo tanto $\mathbf{e} \mid q - 1$. Con isto L vai ser o único subcorpo de $\mathbb{Q}(\varepsilon_q)$ que ten orde $\mathbf{e}$ sobre $\mathbb{Q}$. Vexamos coma escinde q en

L. Sabemos que q é o único primo de $\mathbb{Z}$ que ramifica en $\mathbb{Q}(\varepsilon_q)$ e ademais ramifica completamente, denotemos por $\mathfrak{Q}_0$ o primo de $\mathbb{Q}(\varepsilon_q)$ sobre q. Debido a isto, hai un único primo en $\mathcal{O}_L$ sobre q e $\mathbf{f}_{\mathfrak{Q}_0\cap L/q} = 1$ e polo tanto $\mathbf{e}_{\mathfrak{Q}_0\cap L/q} = [L:\mathbb{Q}] = \mathbf{e}$ en consecuencia q ramifica completamente en L.

Agora podemos definir K' como $K' = (KL)^{\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})}$ onde $\mathfrak{Q}$ é un primo de $\mathcal{O}_{KL}$ sobre q. A continuación imos ver que se cumpre (i). Sabemos que $\mathrm{Gal}_{\mathbb{Q}}(KL)$ é abeliano, xa que tanto K como L son extensións abelianas, polo tanto $\mathrm{D}_{\mathfrak{Q}}(KL|\mathbb{Q})$ e $\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})$ son subgrupos normais e podemos aplicar o Corolario 4.5 obtendo que q non ramifica en K'. Sexa q' un primo de $\mathbb{Z}$ que non ramifica en K sabemos que tampouco o fai en $\mathbb{Q}(\varepsilon_q)$, precisamente o único que o fai é q, polo que non pode ramificar en L. Deste modo, pola Proposición 4.7, q' non ramifica en KL o que, unha vez máis, implica que non o fai en K'.

O que imos demostrar agora é que $\mathbf{e}_{\mathfrak{Q}/q} = \mathbf{e}$, para isto tomemos $\mathrm{V}_1(\mathfrak{Q}|q)$ e vexamos que é trivial. Se $\sigma \in \mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q}) \subseteq \mathrm{Gal}_{\mathbb{Q}}(KL)$, dado $\alpha \in \mathcal{O}_K \subseteq \mathcal{O}_{KL}$ imos ter $\sigma(\alpha) \cong \alpha (\mathrm{mod}\,(\mathfrak{Q}\cap\mathcal{O}_K)) = \alpha(\mathrm{mod}\,\mathfrak{q})$ polo tanto $\sigma_K \in \mathrm{I}_{\mathfrak{q}}(K|\mathbb{Q}) \subseteq \mathrm{Gal}_{\mathbb{Q}}(K)$. Entón o homomorfismo inxectivo, definido na Proposición 1.10,

$$\rho\colon\ \mathrm{Gal}_{\mathbb{Q}}(KL) \to \mathrm{Gal}_{\mathbb{Q}}(K) \times \mathrm{Gal}_{\mathbb{Q}}(L)$$

define un homomorfismo inxectivo,

$$\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q}) \to \mathrm{I}_{\mathfrak{q}}(K|\mathbb{Q}) \times \mathrm{Gal}_{\mathbb{Q}}(L)$$

Debido ao anterior, sabemos que $|\,\mathrm{I}_{\mathfrak{Q}}(KL|K)| = \mathbf{e}_{\mathfrak{Q}/q}$ divide a $|\,\mathrm{I}_{\mathfrak{q}}(K|\mathbb{Q})| \cdot |\,\mathrm{Gal}_{\mathbb{Q}}(K)| = \mathbf{e}^2 = p^{2k}$ e como $\mathrm{V}_1(\mathfrak{Q}|q)$ é un q-Sylow de $\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})$ tense que $|\,\mathrm{V}_1(\mathfrak{Q}|q)| = 1$ en consecuencia $\mathrm{V}_1(\mathfrak{Q}|q) = \{\mathrm{id}\}$. Así $\mathrm{D}_{\mathfrak{Q}}(KL|\mathbb{Q})/\,\mathrm{V}_1(\mathfrak{Q}|q) \cong \mathrm{D}_{\mathfrak{Q}}(KL|\mathbb{Q}) \subseteq \mathrm{Gal}_{\mathbb{Q}}(KL)$ é abeliano e entón $\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q}) \cong \mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})/\,\mathrm{V}_1(\mathfrak{Q}|q)$ é cíclico, pola Proposición 4.15. Tomemos $\tau \in \mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})$ tal que $\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q}) =< \tau >$ e consideremos a súa imaxe mediante o encaixe anterior $\tau \longmapsto (\tau_K, \tau_L)$. Temos que, se $a = |\tau_K|$ e $b = |\tau_L|$, $|\tau| = \mathrm{mcm}(a,b)$ así séguese que:

$$\left.\begin{array}{ll} a \mid |\,\mathrm{I}_{\mathfrak{q}}(K|\mathbb{Q})| & \text{con} \quad |\,\mathrm{I}_{\mathfrak{q}}(K|\mathbb{Q})| = \mathbf{e} \\ b \mid |\,\mathrm{Gal}_{\mathbb{Q}}(L)| & \text{con} \quad |\,\mathrm{Gal}_{\mathbb{Q}}(L)| = \mathbf{e} \end{array}\right| \quad \Longrightarrow \quad |\tau| \mid \mathbf{e}$$

Por outro lado, $|\,\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})| = \mathbf{e}_{\mathfrak{Q}/q} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{q}}\,\mathbf{e}_{\mathfrak{q}/q} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{q}}$ e entón $\mathbf{e} \mid |\,\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})|$ en consecuencia $|\,\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})| = \mathbf{e}$ e chegamos a que $\mathbf{e}_{\mathfrak{Q}/q} = \mathbf{e}$.

Empregando o que acabamos de demostrar mais o feito de que q non ramifica en K' pero ramifica completamente en L temos que:

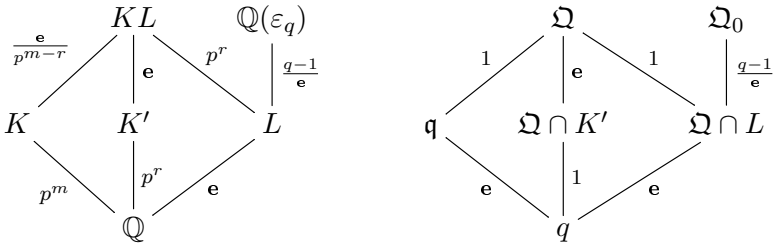
$$\left\{\begin{array}{lll} \mathbf{e}_{\mathfrak{Q}/q} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{Q}\cap L}\,\mathbf{e}_{\mathfrak{Q}\cap L/q} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{Q}\cap L}\,\mathbf{e} & \Longrightarrow & \mathbf{e}_{\mathfrak{Q}/\mathfrak{Q}\cap L} = 1 \\ \mathbf{e}_{\mathfrak{Q}/q} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{Q}\cap K'}\,\mathbf{e}_{\mathfrak{Q}\cap K'/q} = \mathbf{e}_{\mathfrak{Q}/\mathfrak{Q}\cap K'} & \Longrightarrow & \mathbf{e}_{\mathfrak{Q}/\mathfrak{Q}\cap K'} = \mathbf{e} \end{array}\right.$$

Así $\mathfrak{Q}$ non ramifica sobre L pero, en cambio, como $[KL\colon K'] = [KL\colon KL^{\mathrm{I}_{\mathfrak{Q}}(KL|\mathbb{Q})}] = \mathbf{e}_{\mathfrak{Q}/q} = \mathbf{e}$ temos que $\mathfrak{Q}$ ramifica completamente sobre K'.

Debido ao anterior podemos probar (iii), tomemos a composición de corpos $K'L$ e vexamos que $K'L = KL$. En primeiro lugar $K' \subseteq KL$ e $L \subseteq KL$ polo que $K'L \subseteq KL$, así como $\mathfrak{Q}$ é un primo de KL que ramifica completamente sobre K' temos que tamén o fai sobre $K'L$ e como non ramifica en L tampouco o fai en $K'L$. Deste modo, $[KL\colon K'L] = e_{\mathfrak{Q}/\mathfrak{Q}\cap K'L} = 1$ equivalente a $K'L = KL$. Coma consecuencia, se $K' \subseteq \mathbb{Q}(\varepsilon_m)$ entón

$$K \subseteq KL = K'L \subseteq \mathbb{Q}(\varepsilon_m)\mathbb{Q}(\varepsilon_d) = \mathbb{Q}(\varepsilon_{\mathrm{mcm}(m,q)}).$$

Só quédanos ver (ii) para completar a demostración do lema. O grao de K' sobre $\mathbb{Q}$ é unha potencia de p de forma inmediata por ser un subcorpo de KL, debido a que o grado de KL sobre $\mathbb{Q}$ divide a $[K\colon \mathbb{Q}][L\colon \mathbb{Q}] = \mathbf{e}\, p^m = p^k p^m$. Entón $[K'\colon \mathbb{Q}] = p^r$ e como $\mathbf{e}\, p^r = [KL\colon K'][K'\colon \mathbb{Q}] = [KL\colon \mathbb{Q}]$ temos que $r \leq m$.



□

Observación 5.4. Como, polo Teorema 3.15, sabemos que o número de primos de $\mathbb{Z}$ que ramifican sobre K é finito podemos empregar o lema anterior para ir eliminándoos sucesivamente ata chegar a un corpo K', con orde unha potencia de p sobre $\mathbb{Q}$, no que, como moito, só ramifique p. No caso no que p non ramifique sobre K' teremos polo Teorema de Minkowski, Teorema 3.27, que $K' = \mathbb{Q}$ o cal está contido nun corpo ciclotómico de forma trivial.

5.2. Extensións abelianas de grao 2^m

Imos demostrar nesta sección o Teorema de Kronecker-Weber no caso no cal a orde de K sobre $\mathbb{Q}$ sexa unha potencia de 2.

Proposición 5.5. *Sexa $K|\mathbb{Q}$ unha extensión abeliana tal que $[K\colon \mathbb{Q}] = 2^m$, con $m > 0$ un natural. Se 2 é o único primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$ entón $K \subseteq \mathbb{Q}(\varepsilon_{2^{m+2}})$, polo tanto, $K|\mathbb{Q}$ é unha extensión ciclotómica.*

Demostración. Supoñamos primeiro que $m = 1$, temos $K = \mathbb{Q}(\sqrt{n}\,)$, con n libre de cadrados. Imos ver que como 2 é o único primo que ramifica en $\mathbb{Q}(\sqrt{n})$ soamente hai tres posibilidades para

o valor de n que son $-1, 2$ ou -2. Por un lado, o Teorema 3.15 dinos que primos de $\mathbb{Z}$ ramifican en $\mathbb{Q}(\sqrt{n})$ en función do valor do $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})})$ e, por outro lado, a Proposición 2.24 danos o valor do discriminante en función de n. Entón por ser 2 o único primo que ramifica obtemos:

(*i*) Se $n \equiv 2 \pmod 4$ tense que $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 4n$, entón $n = 2$ ou $n = -2$ e $K = \mathbb{Q}(\sqrt{2})$ ou $K = \mathbb{Q}(\sqrt{-2})$.

(*ii*) Se $n \equiv 3 \pmod 4$ tense que $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 4n$, entón $n = -1$ e $K = \mathbb{Q}(i)$.

(*iii*) Se $n \equiv 1 \pmod 4$ tense $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = n$ o cal é incompatible coa hipótese coa que traballamos.

Por último, sendo $m = 1$, o feito de que $K \subseteq \mathbb{Q}(\varepsilon_8)$ é inmediato xa que $i = \varepsilon_8^2$, $\sqrt{2} = \varepsilon_8 + \varepsilon_8^{-1}$ e $\sqrt{-2} = \varepsilon_8 - \varepsilon_8^{-1}$.

Pasamos agora ao caso no que $m > 1$. Primeiro imos ver que $\mathbb{Q}(\sqrt{2}) \subseteq K$, tomemos $K \cap \mathbb{R}$ preséntasenos dous casos ou $K \subseteq \mathbb{R}$ ou $K \subsetneq \mathbb{R}$, e neste segundo caso $K \cap \mathbb{R} = K^{<\sigma>}$ onde $\sigma \in \operatorname{Gal}_{\mathbb{Q}}(K)$ leva un elemento de K no seu conxugado complexo. No primeiro caso $K \cap \mathbb{R}$ ten orde 2^m sobre $\mathbb{Q}$ e no segundo ten orde 2^{m-1}, deste modo sabemos que existe un subcorpo $K' \subseteq K \cap \mathbb{R}$ con orde 2 sobre $\mathbb{Q}$ debido a que $\operatorname{Gal}_{\mathbb{Q}}(K \cap \mathbb{R})$ é un 2-grupo e polo tanto ten un subgrupo de índice 2. Polo Teorema de Minkowski, Teorema 3.27, sabemos que hai algún primo de $\mathbb{Z}$ que ramifica en K' e como 2 é o único primo que ramifica en K temos que é o único que o fai en K'. Ademais temos que $K'|\mathbb{Q}$ é unha extensión abeliana polo tanto atopámonos no caso $m = 1$ obtendo deste modo que $K' = \mathbb{Q}(\sqrt{2}) \subseteq K$ porque $K' \subseteq \mathbb{R}$.

Tomemos agora $L = \mathbb{R} \cap \mathbb{Q}(\varepsilon_{2^{m+2}})$. Sabemos que 2 é o único primo que ramifica en $\mathbb{Q}(\varepsilon_{2^{m+2}})$, e ademais ramifica completamente, en consecuencia 2 é o único primo que ramifica en L e faino por completo. Sabemos que $[L\colon \mathbb{Q}] = 2^m$ estando así nas condicións do enunciado polo que $\mathbb{Q}(\sqrt{2}) \subseteq L$. Ademais $\mathbb{Q}(\sqrt{2})$ é o único subcorpo cadrático de L: se tivéramos outro, que denotamos por M, volveríamos a ter as condicións do enunciado con $m = 1$ e $M \subseteq L \subseteq \mathbb{R}$ polo que $M = \mathbb{Q}(\sqrt{2})$. Grazas ao anterior, podemos asegurar que $\operatorname{Gal}_{\mathbb{Q}}(L)$ ten un único subgrupo de orde 2^{m-1} como ademais $|\operatorname{Gal}_{\mathbb{Q}}(L)| = 2^m$, empregando o Teorema fundamental de grupos abelianos finitamente xerados, temos que $\operatorname{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}/2^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{\alpha_1}\mathbb{Z}$ e así a única posibilidade é que $\operatorname{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}/2^m\mathbb{Z}$, quedando probado que é cíclico.

Co que acabamos de ver, podemos tomar $F = (KL)^{<\tau>}$ onde $\tau \in \operatorname{Gal}_{\mathbb{Q}}(LK)$ é unha extensión de $\nu \in \operatorname{Gal}_{\mathbb{Q}}(L)$ tal que $\operatorname{Gal}_{\mathbb{Q}}(L) =< \nu >$. Imos ver que $F = \mathbb{Q}$, $F = \mathbb{Q}(i)$, ou $F = \mathbb{Q}(\sqrt{2})$. Por un lado, $L \cap F \subseteq \{\alpha \in L\,;\, \tau(\alpha) = \alpha\} = \{\alpha \in L\,;\, \nu(\alpha) = \alpha\} = L^{\operatorname{Gal}_{\mathbb{Q}}(L)} = \mathbb{Q}$. Por outro lado, $[KL\colon \mathbb{Q}]$ é unha potencia de 2, debido a que $[K\colon \mathbb{Q}] = [L\colon \mathbb{Q}] = 2^m$, polo tanto $[F\colon \mathbb{Q}]$ é unha potencia de 2. Se $F = \mathbb{Q}$ xa temos o que queríamos, senón polo Teorema de Minkowski existe algún primo que ramifica en F e como, pola Proposición 4.7, o único primo que ramifica en KL é o 2 temos que o único que o fai en F é 2. No caso de que o grao de F sobre $\mathbb{Q}$ sexa

$2^{m'}$ con $m' > 1$ tense $\mathbb{Q}(\sqrt{2}) \subseteq F$, pero entón $\sqrt{2} \subseteq F \cap L = \mathbb{Q}$ o cal non podo ocorrer. En consecuencia, se $F \neq \mathbb{Q}$, $[F\colon \mathbb{Q}] = 2$ e $F = \mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{-2})$. Grazas a isto podemos asegurar que $F \subseteq \mathbb{Q}(\varepsilon_8) \subseteq \mathbb{Q}(\varepsilon_{2^{m+2}})$.

Para concluír a demostración imos ver que $KL = FL$ e polo tanto $K \subseteq KL = FL \subseteq \mathbb{Q}(\varepsilon_{2^{m+2}})$. Para isto precisamos calcular a orde τ e o imos facer empregando a Proposición 1.10, temos o seguinte:

$$\begin{aligned} \rho\colon \operatorname{Gal}_{\mathbb{Q}}(KL) &\longrightarrow \operatorname{Gal}_{\mathbb{Q}}(K) \times \operatorname{Gal}_{\mathbb{Q}}(L) \\ \tau &\longmapsto (\tau_K, \tau_L) = (\tau_K, \nu) \end{aligned}$$

Así, se $a = |\tau_K|$, temos que a divide a $|\operatorname{Gal}_{\mathbb{Q}}(K)| = 2^m$ polo tanto $|\tau| = |(\tau_K, \tau_L)| = |(\tau_K, \nu)| = \operatorname{mcm}(a, 2^m) = 2^m$.

Agora notemos que $FL \subseteq KL$, porque $F, L \subseteq KL$, e ademais $[KL\colon F] = |\operatorname{Gal}_F(KL)| = |\tau| = 2^m = [L\colon \mathbb{Q}]$. En consecuencia, como $F \cap L = \mathbb{Q}$, pola Proposición 1.9, $[FL\colon \mathbb{Q}] = [L\colon \mathbb{Q}][F\colon \mathbb{Q}] = [KL\colon F][F\colon \mathbb{Q}] = [KL\colon \mathbb{Q}]$ e chegamos a que $FL = KL$. □

5.3. Extensións abelianas de grao p^m, con p un primo impar

Finalmente só queda demostrar o Teorema de Kronecker-Weber no caso dunha extensión abeliana de grao p^m, sendo $m > 0$ un número natural é $p > 0$ un enteiro primo impar. Realizaremos a demostración deste resultado na última proposición desta sección, a Proposición 5.9. Na proba da proposición serán útiles os seguintes lemas.

Lema 5.6. *Sexa $K \,|\, \mathbb{Q}$ unha extensión abeliana de grao $[K\colon \mathbb{Q}] = p$, sendo $p \in \mathbb{Z}$ un primo impar. Se p é o único primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$ entón $\operatorname{diff}(\mathcal{O}_K \,|\, \mathbb{Z}) = \mathfrak{p}^{2(p-1)}$ onde $\mathfrak{p}$ é un primo de $\mathcal{O}_K$ sobre p.*

Demostración. Sexa $\mathfrak{p}$ un primo de $\mathcal{O}_K$ sobre p e consideremos o seu índice de ramificación $\mathbf{e} = \mathbf{e}_{\mathfrak{p}/p} > 1$ e o grado residual $\mathbf{f} = \mathbf{f}_{\mathfrak{p}/p}$ como $K \,|\, \mathbb{Q}$ é unha extensión normal cúmprese que $\mathbf{g}\,\mathbf{e}\,\mathbf{f} = p$ sendo $\mathbf{g}$ o número de primos de $\mathcal{O}_K$ sobre p, en consecuencia $\mathbf{e} = p$ e $\mathbf{g} = \mathbf{f} = 1$. En particular, p ramifica completamente en K e tense que $p\mathcal{O}_K = \mathfrak{p}^p$ e $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Tomemos agora un elemento $\pi \in \mathfrak{p} - \mathfrak{p}^2$, tense que $\pi \notin \mathbb{Q}$ porque $\pi \notin \mathfrak{p}^2$ e polo tanto $\pi \notin \mathfrak{p}^p$. Deste modo $\mathbb{Q} \subsetneq \mathbb{Q}(\pi) \subseteq K$ e por ter K grao p sobre $\mathbb{Q}$, temos que $[\,\mathbb{Q}(\pi)\colon \mathbb{Q}\,] = p$. Debido ao anterior, sabemos que $f = \operatorname{Irr}(\pi, \mathbb{Q}) = \mathrm{X}^p + a_1\mathrm{X}^{p-1} + \cdots + a_p \in \mathbb{Z}[\mathrm{X}]$, por ser π un enteiro alxébrico. Como p ramifica completamente en K, podemos aplicar a Proposición 3.26 para ver que $p \mid a_i$, $\forall i \in \{1, \ldots, p\}$. Temos que $a_1\pi^{p-1} + \cdots + a_p = -\pi^p \in \mathfrak{p}^p \subset \mathfrak{p}$ entón aplicando o apartado (ii) da proposición obtemos o resultado. Consideremos agora o enteiro $k > 0$ tal que $\mathfrak{p}^k$ é a potencia exacta de $\mathfrak{p}$ que divide ao ideal $\operatorname{diff}(\mathcal{O}_K|\mathbb{Z})$. Sabemos pola fórmula de Hilbert (Teorema

4.16) que $k = \sum_{m\geq 0}(|\,\mathrm{V}_m\,| - 1)$, con $\mathrm{V}_m = \mathrm{V}_m(\mathfrak{p}|p)$. Recordemos que $\mathrm{V}_0 \supseteq \mathrm{V}_1 \supseteq \cdots \supseteq \mathrm{V}_m \supseteq \mathrm{V}_{m+1} \supseteq \cdots$, tendo así que $|\,\mathrm{V}_m\,|$ divide a $|\,\mathrm{V}_0\,| = |\,\mathrm{I}_{\mathfrak{p}}(K|\mathbb{Q})| = \mathbf{e}_{\mathfrak{p}/p} = p$. Deste modo, $|\,\mathrm{V}_m\,| = p$ ou $|\,\mathrm{V}_m\,| = 1$ e séguese que k é un múltiplo de $p-1$. Ademais como p ramifica completamente en K podemos aplicar o Teorema 4.16 apartado (i), entón k tamén é o expoñente da potencia exacta de $\mathfrak{p}$ que divide a $f'(\pi)$. A continuación imos traballar coa potencia exacta de $\mathfrak{p}$ que divide a cada un dos termos non nulos da expresión $f'(\pi) = p\pi^{p-1} + (p-1)a_1\pi^{p-2} + \cdots + a_{p-1}$. Sexa $i \in \{1,\ldots,p-1\}$ tal que $(p-i)a_i\pi^{p-i-1}$ é non nulo. Como $\mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$ e $p\mathcal{O}_K = \mathfrak{p}^p$ temos que a potencia exacta de $\mathfrak{p}$ dividindo a $a_i(p-i)$ é un múltiplo de p, ademais sabemos que é maior que 0 porque $p \mid a_i$. Por outro lado, como $\pi \in \mathfrak{p} - \mathfrak{p}^2$, temos que a potencia exacta de $\mathfrak{p}$ dividindo a π^{p-i-1} é $p-i-1$. En consecuencia a potencia exacta de $\mathfrak{p}$ dividindo a $a_i(p-i)\pi^{p-i-1}$ é congruente con $p-i-1 \pmod{p}$. Deste modo os expoñentes de $\mathfrak{p}$ dividindo ós termos non nulos de $f'(\pi)$ son distintos, e k será o mínimo deles. Imos comprobar que $k = 2(p-1)$. En primeiro lugar, $k \geq p$ como consecuencia de que $p \mid a_i$, $\forall i \in \{1,\ldots,p-1\}$, e $k \leq 2p-1$ porque $2p-1$ é a potencia exacta de $\mathfrak{p}$ dividindo ó termo $p\pi^{p-1}$. Por outro lado, vimos antes que k é un múltiplo de $p-1$ e así, como $p \geq 3$, $p-1 < p \leq k \leq 2p-1 < 3(p-1)$ quedando coma única posibilidade que $k = 2(p-1)$.

Acabamos de probar que $\mathfrak{p}^{2(p-1)}$ é a potencia exacta de $\mathfrak{p}$ que divide a $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$. Supoñamos que temos $\mathfrak{q}$ outro ideal primo de $\mathcal{O}_K$ dividindo a $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$ e sexa q o primo de $\mathbb{Z}$ baixo $\mathfrak{q}$, como p ramifica completamente en $\mathcal{O}_K$ e $\mathfrak{q} \neq \mathfrak{p}$, temos que $q \neq p$, e aplicando o Teorema 3.24 obtemos que q ramifica en $\mathcal{O}_K$, pero isto é unha contradición porque por hipótese p é o único primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$. Queda así demostrado que $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathfrak{p}^{2(p-1)}$. □

Lema 5.7. *Sexa $K\,|\,\mathbb{Q}$ unha extensión abeliana de grao p^2, sendo p un primo impar de $\mathbb{Z}$. Se p é o único primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$ entón $G = \mathrm{Gal}_{\mathbb{Q}}(K)$ ten un único subgrupo de orde p.*

Demostración. Primeiro imos ver que p ramifica completamente en $\mathcal{O}_K$. Fixemos $\mathfrak{p}$ un primo de $\mathcal{O}_K$ sobre p e sexa $\mathrm{I} = \mathrm{I}_{\mathfrak{p}}(K|\mathbb{Q})$. Tomando o corpo de inercia, K^{I}, sabemos polo Teorema 4.3 que $\mathbf{e}_{\mathfrak{p}^{\mathrm{I}}/p} = 1$ entón, como $K^{\mathrm{I}}\,|\,\mathbb{Q}$ é unha extensión normal por ser $\mathrm{Gal}_{\mathbb{Q}}(K)$ un grupo abeliano, temos que p non ramifica en K^{I}. Ademais, por hipótese, ningún primo de $\mathbb{Z}$ distinto de p ramifica en K e polo tanto non hai ningún primo de $\mathbb{Z}$ que ramifique en K^{I} e podemos concluír que $K^{\mathrm{I}} = \mathbb{Q}$ como consecuencia do Teorema de Minkowski. Deste modo

$$[K\colon \mathbb{Q}] = [K\colon K^{\mathrm{I}}] = |\,\mathrm{I}\,| = \mathbf{e}_{\mathfrak{p}/p},$$

é dicir, $\mathfrak{p}$ ramifica completamente sobre p.

Debido ao anterior sabemos que $|\,\mathrm{I}\,| = [K : \mathbb{Q}] = p^2$ e ademais, pola Proposición 4.14, $\mathrm{V}_1 = \mathrm{V}_1(\mathfrak{p}|p)$ é un $p-Sylow$ de I e polo tanto $\mathrm{V}_1 = \mathrm{I}$ e $|\,\mathrm{V}_1\,| = p^2$. Se tomamos $\mathrm{V}_r = \mathrm{V}_r(\mathfrak{p}|p)$ como o primeiro grupo de ramificación que ten orde menor que p^2 imos ter que $|\,\mathrm{V}_r\,| = p$ polo seguinte:

Como $r > 1$ pola Proposición 4.12 temos un encaixe $\mathrm{V}_{r-1}\,/\,\mathrm{V}_r \hookrightarrow \mathcal{O}_K/\mathfrak{p}$ e así $|\,\mathrm{V}_{r-1}\,/\,\mathrm{V}_r\,|$ divide a $|\mathcal{O}_K/\mathfrak{p}| = p^{\mathbf{e}_{\mathfrak{p}/p}} = p$. Deste modo, $|\,\mathrm{V}_{r-1}\,/\,\mathrm{V}_r\,| \in \{1, p\}$ pero como $|\,\mathrm{V}_{r-1}\,| = p^2$ e $|\,\mathrm{V}_r\,| < p^2$ a única posibilidade é que $|\,\mathrm{V}_{r-1}\,/\,\mathrm{V}_r\,| = p$ e en consecuencia $|\,\mathrm{V}_r\,| = p$.

Agora imos ver a relación entre o ideal $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$ e os subgrupos de $\mathrm{Gal}_{\mathbb{Q}}(K)$ de orde p, coma é o caso de V_r. Sexa $H \subset \mathrm{Gal}_{\mathbb{Q}}(K)$ un subgrupo de orde $|H| = p$, e tomemos $K^H \subset K$; podemos aplicar a Proposición 3.25 obtendo así que

$$\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K^H})(\mathrm{diff}(\mathcal{O}_{K^H}|\mathbb{Z})\mathcal{O}_K).$$

Por outra parte, temos que $[K^H\,|\,\mathbb{Q}] = p$ e ademais, aplicando o Teorema de Minkowski, sabemos que p ramifica en K^H e é o único, por ser o único que ramifica en K. Así podemos aplicar o lema anterior, Lema 5.6, e obtemos $\mathrm{diff}(\mathcal{O}_{K^H}|\mathbb{Z}) = (\mathfrak{p}^H)^{2(p-1)}$, ademais como $\mathfrak{p}$ ramifica completamente sobre p temos que tamén ramifica completamente sobre $\mathfrak{p}^H$ e polo tanto $\mathfrak{p}^H\mathcal{O}_K = \mathfrak{p}^p$, nótese que $\mathbf{e}_{\mathfrak{p}/\mathfrak{p}^H} = [K\,|\,K^H] = p$. Así obtemos $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K^H})\mathfrak{p}^{2p(p-1)}$.

O que acabamos de probar asegúranos que o $\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K^H})$ é independente do grupo H pero imos ver agora que o expoñente de $\mathfrak{p}$ en $\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K^H})$ maximízase de forma estrita cando H é o grupo V_r, isto contradí a independencia obtendo así que $\mathrm{Gal}_{\mathbb{Q}}(K)$ ten un único subgrupo de orde p que é precisamente V_r quedando así probado o lema.

Demostremos o que falta, pola fórmula de Hilbert sabemos que a potencia exacta de $\mathfrak{p}$ dividindo a $\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K^H})$ é $k = \sum_{m\geq 0}(|\,\mathrm{V}_m(\mathfrak{p}|\mathfrak{p}^H)| - 1)$. Ademais,

$$\begin{aligned}\mathrm{V}_m(\mathfrak{p}|\mathfrak{p}^H) &= \{\,\sigma \in \mathrm{Gal}_{K^H}(K);\, \sigma(\alpha) = \alpha,\, \forall \alpha \in \mathcal{O}_K\,\} = \\ &= \{\,\sigma \in H;\, \sigma \in \mathrm{V}_m(\mathfrak{p}|p)\,\} = H \cap \mathrm{V}_m\end{aligned}$$

entón $|\,\mathrm{V}_m(\mathfrak{p}|\mathfrak{p}^H)|$ é máximo, e de forma estrita, cando $\mathrm{V}_m \subseteq H$ ou $H \subseteq \mathrm{V}_m$.

Agora ben, fixado m temos que se $m \leq r$ entón $|\,\mathrm{V}_m\,| \geq |H|$ e polo tanto, para que $|\,\mathrm{V}_m(\mathfrak{p}|\mathfrak{p}^H)|$ sexa estritamente máximo, necesariamente $H \subseteq \mathrm{V}_m$. Se polo contrario $m \geq r$ entón $|\,\mathrm{V}_m\,| \leq |H|$ e para maximizar $|\,\mathrm{V}_m(\mathfrak{p}|\mathfrak{p}^H)|$ teríase que cumprir $H \supseteq \mathrm{V}_m$. Deste modo obtemos a seguinte cadea de inclusións

$$\mathrm{V}_0 \supseteq \mathrm{V}_1 \supseteq \cdots \supseteq \mathrm{V}_r \supseteq H \supseteq \mathrm{V}_r \supseteq \mathrm{V}_{r+1} \supseteq \cdots$$

é dicir, $|\,\mathrm{V}_m(P|P^H)|$ é máximo de forma estrita cando $H = \mathrm{V}_r$ e polo tanto k tamén. □

Lema 5.8. *Sexa $K\,|\,\mathbb{Q}$ unha extensión abeliana de grao p, sendo p un primo impar de $\mathbb{Z}$. Se p é o único primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$ entón K é o único subcorpo de $\mathbb{Q}(\varepsilon_{p^2})$ que ten grao p sobre $\mathbb{Q}$.*

Demostración. Primeiro imos ver que K nas condicións do enunciado é único. Supoñamos que existe outro corpo L con grao p sobre $\mathbb{Q}$ que ten p coma único primo que ramifica en $\mathcal{O}_L$. Tomemos

a composición de corpos KL, pola Proposición 1.9 , como $K \cap L = \mathbb{Q}$ temos que

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}] = p^2.$$

Ademais pola Proposición 4.7 sabemos que o único primo que ramifica en KL é p e así podemos aplicar o Lema 5.7 anterior, e chegamos a unha contradición, obsérvese que $KL\,|\,\mathbb{Q}$ é abeliana pola Proposición 1.10.

Grazas ao que acabamos de probar só queda ver que $\mathbb{Q}(\varepsilon_{p^2})$ ten un subcorpo nas condicións do enunciado. Como $|\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon_{p^2}))| = [\mathbb{Q}(\varepsilon_{p^2}) : \mathbb{Q}] = p(p-1)$ e ademais é un grupo cíclico imos ter que existe un subcorpo L de grao p sobre $\mathbb{Q}$. Notemos que $L\,|\,\mathbb{Q}$ é abeliana por selo $\mathbb{Q}(\varepsilon_{p^2})\,|\,\mathbb{Q}$ e ademais, como p é o único primo de $\mathbb{Z}$ que ramifica en $\mathbb{Q}(\varepsilon_{p^2})$ tamén é o único que o fai en L, sabemos que ramifica polo Teorema de Minkowski, e así concluímos coa demostración, sendo necesariamente $K = L$. Por último, obsérvese que p ramifica completamente tanto en $\mathbb{Q}(\varepsilon_{p^2})$ coma en K. □

Grazas aos resultados anteriores podemos proceder a probar a proposición seguinte e finalizar así a proba do Teorema de Kronecker-Weber.

Proposición 5.9. *Sexa $K\,|\,\mathbb{Q}$ unha extensión abeliana de grao p^m, sendo $p > 0$ un primo impar de $\mathbb{Z}$ e $m > 0$ un natural. Se p é o único primo de $\mathbb{Z}$ que ramifica en $\mathcal{O}_K$ entón K é o único subcorpo de $\mathbb{Q}(\varepsilon_{p^{m+1}})$ que ten grao p^m sobre $\mathbb{Q}$. Como consecuencia $K\,|\,\mathbb{Q}$ é unha extensión ciclotómica.*

Demostración. Sabemos que $\mathbb{Q}(\varepsilon_{p^{m+1}}) \cong (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$, Proposición 1.14, polo que é cíclico de orde $p^m(p-1)$ e así $\mathbb{Q}(\varepsilon_{p^{m+1}})$ ten un único subcorpo, que denotamos por L, de grao $[L\colon \mathbb{Q}] = p^m$. O grupo $\operatorname{Gal}_{\mathbb{Q}}(L)$ é de orde p^m, entón tamén é cíclico e podemos tomar un xerador do mesmo, ao que denotamos por σ, e estendelo a τ un $\mathbb{Q}$-automorfismo de KL. Consideremos o subcorpo de KL fixo por τ, $F = (KL)^{<\tau>}$. Tense que $F \cap L = \mathbb{Q}$ porque

$$F \cap L \subseteq \{\alpha \in L\,;\, \tau(\alpha) = \alpha\} = \{\alpha \in L\,;\, \sigma(\alpha) = \alpha\} = L^{<\sigma>} = L^{\operatorname{Gal}_{\mathbb{Q}}(L)} = \mathbb{Q}.$$

Como $[FL\colon \mathbb{Q}]$ é unha potencia de p entón $[F\colon \mathbb{Q}] = p^k$. Por outro lado, p é o único primo que ramifica en K e en L así, pola Proposición 4.7, sabemos que tamén é o único que ramifica en KL. Deste modo se $F \neq \mathbb{Q}$, polo Teorema de Minkowski, p ramifica en F e é o único. Neste caso, poderíamos tomar a extensión de corpos $F'\,|\,\mathbb{Q}$, con $F' \subseteq F$, de grao p sobre $\mathbb{Q}$ que ten p como único primo que ramifica e ademais é abeliana, porque $KL\,|\,\mathbb{Q}$ é abeliana, polo tanto podemos aplicar o Lema 5.8 anterior, e temos que F' é o único subcorpo de $\mathbb{Q}(\varepsilon_{p^2})$ que ten grao p sobre $\mathbb{Q}$. Pero isto lévanos a unha contradición porque, neste caso, $F' \subseteq F \cap L = \mathbb{Q}$. Así tense $F = \mathbb{Q}$.

Grazas ao visto, temos que $[KL\colon \mathbb{Q}] = [KL\colon F]$ entón, supoñendo demostrado que $|\tau| = p^m$, chegamos a $[KL\colon \mathbb{Q}] = [KL\colon F] = |\tau| = p^m = [L\colon \mathbb{Q}] = [L\colon \mathbb{Q}]$, podendo concluír así que $K = L$,

como queríamos demostrar. Falta ver que $|\tau| = p^m$. Tomemos a imaxe de τ mediante o encaixe definido na Proposición 1.10,

$$\begin{aligned} \rho\colon \quad \mathrm{Gal}_{\mathbb{Q}}(KL) &\longrightarrow \mathrm{Gal}_{\mathbb{Q}}(K) \times \mathrm{Gal}_{\mathbb{Q}}(L) \\ \tau &\longmapsto (\tau_K, \tau_L) = (\tau_K, \sigma) \end{aligned}$$

Se $a = |\tau_K|$ entón, como $|\mathrm{Gal}_{\mathbb{Q}}(K)| = p^m$, $a \mid p^m$ e así $|\tau| = |((\tau_K, \tau_L))| = |(\tau_K, \sigma)| = \mathrm{mcm}(a, p^m) = p^m$. □

Bibliografía

[1] BAGGETT, J.A.: *An exposition on the Kronecker-Weber Theorem.* `http://hdl.handle.net/11122/11349`

[2] CONRAD, K.: *The Different Ideal.* `https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf`

[3] DUMMIT, D. S. AND FOOTE, R. M.: *Abstract Algebra.* Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[4] JENSEN, C. U.; LEDET, A. AND YUI, N.: *Generic Polynomials: Constructive aspects of the inverse Galois problem.* Mathematical Sciences Research Institute Publications, **45**. Cambridge University Press, Cambridge, 2002.

[5] JONES, G. A. AND JONES J.M.: *Elementary Number Theory*, Springer undergraduate mathematics series (1998), Springer London, 8th printing 2005.

[6] MARCUS, D. A.: *Number fields.* Second edition of [MR0457396]. With a foreword by Barry Mazur. Universitext. Springer, Cham, 2018.

[7] NEUMANN, O.: Two proofs of the Kronecker-Weber theorem ."according to Kronecker, and Weber". *J. Reine Angew. Math.*, **323** (1981).

[8] PIERRE, S.: *Algebraic Theory of Numbers.* Translated from the French by Allan J. Silberger Houghton Mifflin Co., Boston, Mass. 1970.

[9] RAPINCHUK, I.: *A Proof of the Kronecker-Weber Theorem.* Michigan State University, Departament of Mathematics. Expository papers. `https://sites.google.com/view/irapinchuk`.

[10] ROTHMAN, T.: Genius and biographers: The fictionalization of Evariste Galois. *Amer. Math. Monthly* **89** (1982), no. 2, 84-106.

[11] ZARISKI, O. AND SAMUEL, P.: *Commutative Algebra.* 1nd ed., D. Van Nostrand Company, Inc, 1965.