

Global class field theory

Sally Gilles

July 24, 2026

Some references:

- Milne's lecture notes, available at <https://jmilne.org/math/CourseNotes/CFT.pdf>
- Cassels and Fröhlich's *Algebraic Number Theory*
- Neukirch's *Class Field Theory*
- Neukirch-Schmidt-Wingberg's *Cohomology of Number Fields*
- Milne's *Arithmetic Duality Theorems*, available at <https://www.jmilne.org/math/Books/ADTnot.pdf>
- For an historical point of view, see Venkatesh's notes: [https://www.math.ias.edu/ akshay/research/CFT.pdf](https://www.math.ias.edu/akshay/research/CFT.pdf)

Contents

1	Introduction: local class field theory and the case of the field $\mathbb{Q}$	6
1.1	Reminders about number fields	6
1.2	Class field theory: first cases	8
1.3	Finite extensions of $\mathbb{Q}_p$	9
1.3.1	Unramified extensions	9
1.3.2	Totally ramified extensions and Lubin-Tate theory	10
1.3.3	The reciprocity law	11
1.4	Global fields: the case of $L = \mathbb{Q}$	11
1.5	Approximation theorems	13
2	The global Artin map	14
2.1	Artin map	14
2.2	Ray class groups	16
2.3	Finiteness of ray class groups	18
2.4	Main results of global class field theory	20
3	The ring of adèles	21
3.1	Topological considerations: restricted product	21
3.2	Definition of adèles	23
3.3	Base change of the ring of adèles	24
3.4	Strong approximation theorem	26
4	The group of idèles	28
4.1	Definition of idèles	28
4.2	Ray class groups as quotient of idèles	33
4.3	Artin map using idèles	34
5	The cohomology of the idèles	36
5.1	Cohomology of local fields	37
5.1.1	Tate's theorem and main ideas of the proof	37
5.1.2	Herbrand quotients	38
5.2	The first inequality	40
5.2.1	Preliminaries	41
5.2.2	Galois cohomology of the idèles	43
5.2.3	Galois cohomology of the units	45
5.2.4	The first inequality	47
5.3	Consequences of the first inequality	49
6	The second inequality	50
6.1	First reductions	51
6.2	Kummer theory	53

6.3	Second inequality for abelian extensions of exponent p	57
6.3.1	Proof of Proposition 6.15	59
6.3.2	Proof of Proposition 6.16	60
6.3.3	Proof of Proposition 6.17	62
7	Brauer groups	63
7.1	Brauer group of number fields	63
7.2	The fundamental exact sequence	66
7.3	The fundamental class	69
8	Main theorems of Global CFT	72
8.1	Reciprocity Law	72
8.2	The norm limitation theorem	75
8.3	Existence Theorem	76
9	Density of primes	79
9.1	Dirichlet series	79
9.2	Convergence results	81
9.2.1	Dirichlet series and zeta function	81
9.2.2	Euler products	86
9.2.3	The residue formula	87
9.3	Density of splitting primes	91
9.4	Density of primes in an arithmetic progression	95
9.5	The Second Inequality: alternative proof	101
9.6	Chebotarev Density Theorem	101
10	Restricted ramification	104
11	Duality for cohomology of number fields	110
11.1	Global duality	110
11.1.1	General duality result	110
11.1.2	Duality theorem for number fields	111
11.2	Passage from global to local	112
11.2.1	Case of finite modules	112
11.2.2	Case of infinite modules	114
11.3	Digression: Ext-groups	116
11.3.1	Extensions of G -modules	116
11.3.2	Spectral sequence	116
11.3.3	Shapiro's lemma	119
11.4	Poitou-Tate duality	120
11.5	Proof of Lemma 11.23	130
11.6	Some consequences	134

12 Complements	137
12.1 The connected component of $\mathbb{C}_K$	137
12.2 An example: the cohomology of $\mathbf{Z}$	141
12.3 The global Euler-Poincaré characteristic	143
12.3.1 Statement of the main theorem	143
12.3.2 Proof of Theorem 12.8	144
12.3.3 Consequences	149

1 Introduction: local class field theory and the case of the field $\mathbb{Q}$

In this section we recall some classical results about places in number fields and state the main results of local class field theory. We also explain Artin reciprocity in the case where the field is $\mathbb{Q}$.

1.1 Reminders about number fields

Places of a number field. Let K be a finite extension of $\mathbb{Q}$, we denote by $\mathcal{O}_K$ its ring of integers. An equivalence class of absolute values on K is called a prime (or a place) of K . Each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ defines a place on K , which we will normalize by setting $|a|_{\mathfrak{p}} := N(\mathfrak{p})^{-\text{ord}_{\mathfrak{p}}(a)}$. Other places are given by real embeddings and conjugate pairs of complex embeddings. Those three categories describe all places of K . The ones given by prime ideals are called finite (or non-archimedean) places and the real and complex ones are called infinite (or archimedean) places.

If L/K is a finite extension of number fields, $\mathfrak{p}$ an ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ an ideal of $\mathcal{O}_L$ such that the restriction of $|\cdot|_{\mathfrak{q}}$ to K is equivalent to $|\cdot|_{\mathfrak{p}}$, we say that $\mathfrak{q}$ divides (or lies over) $\mathfrak{p}$. This is equivalent to the fact that $\mathfrak{q}$ divides the ideal $\mathfrak{p}\mathcal{O}_L$ (or equivalently, $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$).

Recall that if L/K is a finite extension of number fields then each place v on K extends to a finite number of places w of L and for all x in $L^\times$, we have

$$\prod_{w|v} |x|_w = |\text{Nm}_{L/K}(x)|_v.$$

For K a number field and v a place of K , we write K_v for the completion of K for the norm $|\cdot|_v$.

Decomposition groups. Let K be a number field and consider L a finite Galois extension of K . Write $G := \text{Gal}(L/K)$. The group G acts on the set of primes of L lying over a fixed prime v of K : if w is a place of L and g an element of G , then $g(w)$ is the place of L such that $|g(a)|_{g(w)} = |a|_w$. Note that if $w = \mathfrak{p}$ is finite then $g(w) = g(\mathfrak{p})$.

If $\mathfrak{q}$ is a finite place of L dividing $\mathfrak{p}$ finite place of K , then the decomposition group $D(\mathfrak{q})$ of $\mathfrak{q}$ is the stabilizer of $\mathfrak{q}$ in G , i.e. $D(\mathfrak{q}) := \{g \in \text{Gal}(L/K) \mid g(\mathfrak{q}) = \mathfrak{q}\}$. Equivalently, it is the set of $g \in \text{Gal}(L/K)$ that acts continuously for the $\mathfrak{q}$ -adic topology. For $g \in G$, we have $D_{g(\mathfrak{q})} = gD(\mathfrak{q})g^{-1}$ and each element of $D(\mathfrak{q})$ extends uniquely to a continuous automorphism of L_w . Moreover, the map $D(\mathfrak{q}) \rightarrow \text{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ is an isomorphism.

Let $\mathfrak{p}$ be a prime of K and $\mathfrak{q}$ be an ideal of L dividing it. Recall that the inertia group $I_{\mathfrak{q}}$ of $D_{\mathfrak{q}} \simeq \text{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ is defined as the group $\{g \in D_{\mathfrak{q}} \simeq \text{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \mid g(x) = x \pmod{\mathfrak{q}} \text{ for all } x \in \mathcal{O}_L\}$. We write $e(\mathfrak{q}/\mathfrak{p})$ for the

ramification index, it is the exponent of $\mathfrak{q}$ appearing in the decomposition of $\mathfrak{p}$ in L , and $f(\mathfrak{q}/\mathfrak{p})$ for the inertia degree, it is equal to $[\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$. We have the following diagram:

$$\begin{array}{ccccc}
 \mathfrak{q} & & L & \xrightarrow{\quad} & L_{\mathfrak{q}} & \twoheadrightarrow & k_L \\
 & & \uparrow e & & \uparrow e & & \parallel \\
 \mathfrak{q}_I := \mathfrak{q} \cap L^{I(\mathfrak{q})} & & L^{I(\mathfrak{q})} & \xrightarrow{\quad} & L_{\mathfrak{q}}^{I(\mathfrak{q})} & \twoheadrightarrow & k_L \\
 & & \uparrow f & & \uparrow f & & \uparrow g \\
 \mathfrak{q}_D := \mathfrak{q} \cap L^{D(\mathfrak{q})} & & L^{D(\mathfrak{q})} & \xrightarrow{\quad} & K_{\mathfrak{p}} & \twoheadrightarrow & k_K \\
 & & \uparrow g & & \parallel & & \parallel \\
 \mathfrak{p} = \mathfrak{q} \cap K & & K & \xrightarrow{\quad} & K_{\mathfrak{p}} & \twoheadrightarrow & k_K
 \end{array}$$

Recall that:

- the only prime ideal of L lying over $\mathfrak{q}_D$ is $\mathfrak{q}$,
- the prime ideal $\mathfrak{q}_D$ is unramified in $L^{I(\mathfrak{q})}$ and $f(\mathfrak{q}_I/\mathfrak{q}_D) = f(\mathfrak{q}/\mathfrak{p})$,
- the prime ideal $\mathfrak{q}_I$ is totally ramified in L and $e(\mathfrak{q}/\mathfrak{q}_I) = e(\mathfrak{q}/\mathfrak{p})$,
- if $D_{\mathfrak{q}}$ is normal in G , then we have that $\mathfrak{p}\mathcal{O}_{L^D} = \prod_{\sigma} \sigma(\mathfrak{q}_D)$, where σ runs over a set of representatives for $G/D_{\mathfrak{q}}$.

In summary: that all the ramification of $\mathfrak{q}$ over $\mathfrak{p}$ takes place in the top extension, all the residue field extension takes place in the middle extension, and (when L^D is normal over K) all the splitting takes place in the bottom extension.

The Frobenius element. Assume now $\mathfrak{q}$ is unramified over $\mathfrak{p}$ then there is an isomorphism

$$D_{\mathfrak{q}} \simeq \text{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \xrightarrow{\sim} \text{Gal}(k_L/k_K).$$

Recall that the Galois group $\text{Gal}(k_L/k_K)$ is cyclic, generated by the Frobenius morphism $x \mapsto x^q$ (with $q = |k_K|$). We then obtain that $D(\mathfrak{q})$ itself is cyclic, generated by an element $(\mathfrak{q}, L/K)$ called the Frobenius element. It is the unique element σ of G which satisfies the following two conditions: $\sigma(\mathfrak{q}) = \mathfrak{q}$ and for all x in $\mathcal{O}_L$, $\sigma(x) = x^q \bmod \mathfrak{q}$.

For any g in G , we have

$$(g(\mathfrak{q}), L/K) = g(\mathfrak{q}, L/K)g^{-1}.$$

Thus if G is abelian, then $(\mathfrak{q}, L/K)$ does not depend on the prime $\mathfrak{q}$ dividing $\mathfrak{p}$, but only on $\mathfrak{p}$. We write $(\mathfrak{p}, L/K)$ for this element. If G is not abelian, then the set of elements $(\mathfrak{q}, L/K)$ for $\mathfrak{q}$ prime ideal dividing $\mathfrak{p}$ defines a conjugacy class in G , which we will also denote by $(\mathfrak{p}, L/K)$.

If we are in the following situation:

$$\begin{array}{ccc} M & & \mathfrak{q}_M \\ \uparrow & & \\ L & & \mathfrak{q}_L \\ \uparrow & & \\ K & & \mathfrak{p} \end{array}$$

with $\mathfrak{q}_M$ unramified over $\mathfrak{p}$, then $(\mathfrak{q}_M, M/L) = (\mathfrak{q}_M, M/K)^{f(\mathfrak{q}_L/\mathfrak{p})}$. If moreover L/K is Galois, then $(\mathfrak{q}_M, M/K)|_L = (\mathfrak{q}_L, L/K)$.

1.2 Class field theory: first cases

In class field theory we are interested in the study of abelian extension of local and global fields. Let us first consider the case of local fields.

In the archimedean case, the abelian extensions of $\mathbf{R}$ are $\mathbf{R}$ and $\mathbf{C}$ and we have an isomorphism

$$\mathbf{R}^\times / \mathbf{R}_{>0} \xrightarrow{\sim} \text{Gal}(\mathbf{C}/\mathbf{R})$$

called the *local Artin map* for $\mathbf{R}$.

In the case where $K = \mathbf{Q}_p$, we have the (local) Kronecker-Weber theorem:

Theorem 1.1. *Every finite abelian extension K of $\mathbf{Q}_p$ is contained in $\mathbf{Q}_p(\zeta)$ for some root of unity ζ .*

It follows that the maximal abelian extension $\mathbf{Q}_p^{\text{ab}}$ of $\mathbf{Q}_p$ is equal to $\mathbf{Q}_p(\zeta_n, \zeta_n \text{ primitive root of } 1) \simeq \mathbf{Q}_p(\zeta_n, p \nmid n) \mathbf{Q}_p(\zeta_{p^r}, r \in \mathbf{N})$. Setting $\mathbf{Q}_p^{\text{unr}} := \mathbf{Q}_p(\zeta_n, p \nmid n)$ and $\mathbf{Q}_{p,\infty} := \mathbf{Q}_p(\zeta_{p^r}, r \in \mathbf{N})$, we obtain

$$\begin{aligned} \text{Gal}(\mathbf{Q}_p^{\text{ab}}/\mathbf{Q}_p) &= \text{Gal}(\mathbf{Q}_p^{\text{unr}}/\mathbf{Q}_p) \times \text{Gal}(\mathbf{Q}_{p,\infty}/\mathbf{Q}_p) \\ &= (\varprojlim_n \mathbf{Z}/n\mathbf{Z}) \times \mathbf{Z}_p^\times \\ &= \widehat{\mathbf{Z}} \times \mathbf{Z}_p^\times \\ &= \widehat{\mathbf{Q}_p^\times}, \end{aligned}$$

the profinite completion of the group $\mathbf{Q}_p^\times$.

1.3 Finite extensions of $\mathbf{Q}_p$

In this subsection, we assume that K is a finite extension of $\mathbf{Q}_p$. We fix the following notations:

- v_K is the discrete valuation normalized such that $v_K(K^\times) = \mathbf{Z}$,
- $\mathcal{O}_K = \{x \in K \mid v_K(x) \geq 0\}$ is the ring of integers of K ,
- $U_K := \mathcal{O}_K^\times = \{x \in K \mid v_K(x) = 0\}$ is the ring of units of K ,
- $\mathfrak{m}_K = \{x \in K \mid v_K(x) > 0\}$ is the maximal ideal with uniformiser π_K ,
- $k_K := \mathcal{O}_K/\mathfrak{m}_K$ the residue field and $q := |k_K|$.

1.3.1 Unramified extensions

An extension L/K is unramified if $[L : K] = [k_L : k_K]$. This is equivalent to saying that π_K is inert in L , i.e. that the ramification index $e = v_K(\pi_L)$ is 1. For example, if $K = \mathbf{Q}_p$, the only finite unramified extensions of K are the fields $\mathbf{Q}_p(\zeta_{p^r-1})$. If L/K is unramified and $k_K = \mathbf{F}_q$, then we have an isomorphism

$$\begin{cases} \text{Gal}(L/K) & \xrightarrow{\sim} \text{Gal}(k_L/k_K) \\ \text{Frob}_{L/K} & \mapsto (x \mapsto x^q). \end{cases}$$

We denote by K^{unr} the union of all finite unramified finite extensions of K in $\overline{K}$. Then the residue field of K^{unr} is an algebraic closure of k_K and we have isomorphisms

$$\begin{cases} \text{Gal}(K^{\text{unr}}/K) & \xrightarrow{\sim} \text{Gal}(\overline{k}_K/k_K) \simeq \varprojlim_n \mathbf{Z}/n\mathbf{Z} \\ \text{Frob}_{K^{\text{unr}}} & \mapsto (x \mapsto x^q) \end{cases}$$

Theorem 1.2 (Local reciprocity law). *There exists a unique morphism*

$$\text{Art} : K^\times \rightarrow \text{Gal}(K^{\text{ab}}/K)$$

characterized by the following properties:

- (i) *For any uniformiser π_K of K , we have $\text{Art}(\pi_K)|_{K^{\text{unr}}} = \text{Frob}_{K^{\text{unr}}}$.*
- (ii) *For any finite abelian extension L/K ,*

$$\text{Art}(\text{Nm}_{L/K}(L^\times))|_L = \text{Id}_L,$$

where $\text{Nm}_{L/K} : x \mapsto \prod_{\sigma \in \text{Gal}(L/K)} \sigma(x)$.

Moreover for a finite abelian extension L/K , Art induces an isomorphism

$$K^\times / \text{Nm}_{L/K}(L^\times) \xrightarrow{\sim} \text{Gal}(L/K).$$

In general, Art is an isomorphism onto $W_K^{\text{ab}} := \{\sigma \in \text{Gal}(K^{\text{ab}}/K) \mid \sigma|_{K^{\text{unr}}} = \text{Frob}_{K^{\text{unr}}}^m, m \in \mathbf{Z}\}$.

We also have:

Theorem 1.3 (Local existence theorem). *The norm groups $\text{Nm}_{L/K}(L^\times) \subset K^\times$ are exactly the open subgroups of finite index.*

Note that in particular, the Artin map Art in Theorem 1.2 is continuous.

1.3.2 Totally ramified extensions and Lubin-Tate theory

We say that a finite extension L/K is totally ramified if $e = v_L(\pi_K) = [L : K]$, or equivalently if $k_L = k_K$. Note that L/K is totally ramified if and only if $L = K(a)$ where a is a root of an Eisenstein polynomial in $\mathcal{O}_K[x]$. Examples of totally ramified extensions of $K = \mathbb{Q}_p$ are given by $\mathbb{Q}_p(\zeta_{p^r})$ or $\mathbb{Q}_p((-p)^{\frac{1}{p-1}})$.

We fix a uniformiser $\pi := \pi_K$ of K . Let us denote by $\Phi(X)$ the polynomial $X^q + \pi X$ in $\mathcal{O}_K[[X]]$. Then there exists a unique series $F_\Phi(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that

$$F_\Phi = X + Y \bmod (\deg 2 \text{ terms}) \quad \text{and} \quad \Phi \circ F_\Phi = F_\Phi \circ \Phi.$$

It can be shown that F_Φ defines a one dimensional commutative formal group law over $\mathcal{O}_K$ (i.e., $F_\Phi(X, Y) = F_\Phi(Y, X)$ and $F_\Phi(X, F_\Phi(Y, Z)) = F_\Phi(F_\Phi(X, Y), Z)$). Similarly if a is in $\mathcal{O}_K$, there exists a unique $[a]_\Phi(X) \in \mathcal{O}_K[[X]]$ such that

$$[a]_\Phi(X) = aX \bmod (\deg 2 \text{ terms}) \quad \text{and} \quad [a]_\Phi \circ F_\Phi = F_\Phi \circ [a]_\Phi.$$

Then the map

$$\begin{cases} \mathcal{O}_K & \rightarrow \text{End}_{\mathcal{O}_K}(F_\Phi) \\ a & \mapsto [a]_\Phi \end{cases}$$

is a ring morphism.

Set $\mathfrak{m} := \bigcup_{L/K \text{ finite}} \mathfrak{m}_L$. We endow $\mathfrak{m}$ with the $\mathcal{O}_K$ -module structure given by:

$$\begin{cases} x + y := F_\Phi(x, y) \\ a \cdot x := [a]_\Phi(x) \end{cases} \quad \text{for all } x, y \in \mathfrak{m} \text{ and } a \in \mathcal{O}_K.$$

Define $\Lambda_n := \ker([\pi^n]_\Phi) = \{x \in \mathfrak{m} \mid \Phi^n(x) = 0\}$. It is a $\mathcal{O}_K/\pi^n \mathcal{O}_K$ -module. Defining $K_n := K(\Lambda_n)$, we obtain a tower

$$K \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset \overline{K}.$$

It can be shown that each K_n/K is a finite Galois extension and there is an isomorphism

$$\chi_{K,n} : \text{Gal}(K_n/K) \xrightarrow{\sim} (\mathcal{O}_K/\pi^n)^\times.$$

In particular, the extension K_n/K is totally ramified of degree $(q-1)q^{n-1}$.

Example 1.4. For $K = \mathbf{Q}_p$ and $\pi = p$, we have $\Lambda_n = \mu_{p^n}$. The group law corresponds to the multiplication on μ_{p^n} and the $\mathbf{Z}_p$ -module structure is induced by the map

$$\begin{cases} \mathbf{Z}/p^n\mathbf{Z} \times \mu_{p^n} & \rightarrow \mu_{p^n} \\ (m, \zeta_n) & \mapsto \zeta_n^m \end{cases}$$

Define

$$K_\pi := \bigcup_n K_n \subset \overline{K} \text{ and } \Lambda := \bigcup_n \Lambda_n.$$

We have an isomorphism

$$\chi_K : \text{Gal}(K_\pi/K) \xrightarrow{\sim} \mathcal{O}_K^\times.$$

1.3.3 The reciprocity law

We define $\text{Art}_\pi : K^\times \rightarrow \text{Gal}(K_\pi K^{\text{unr}}/K)$ in the following way: for any $x = u\pi^m$ in $K^\times$, with u in $\mathcal{O}_K^\times$, we set

$$\begin{cases} \text{Art}_\pi(x)|_{K^{\text{unr}}} & = \text{Frob}_{K^{\text{unr}}}^m \\ \text{Art}_\pi(x)|_{K_\pi}(z) & = [u^{-1}]_\Phi(z) \quad \text{for all } z \in \Lambda. \end{cases}$$

We have the following results:

Theorem 1.5. (i) The field $K_\pi K^{\text{unr}}$ and the map Art_π are independent of the choice of π and for any uniformiser π , we have $K_\pi K^{\text{unr}} = K^{\text{ab}}$.

(ii) If L/K is a finite abelian extension, then the following diagram commutes:

$$\begin{array}{ccc} L^\times & \xrightarrow{\text{Art}_L} & \text{Gal}(L^{\text{ab}}/L) \\ \text{Nm}_{L/K} \downarrow & & \downarrow \text{Res} \\ K^\times & \xrightarrow{\text{Art}_K} & \text{Gal}(K^{\text{ab}}/K) \end{array}$$

and it induces a surjective morphism:

$$K^\times / \text{Nm}_{L/K}(L^\times) \rightarrow \text{Gal}(L/K).$$

1.4 Global fields: the case of $L = \mathbf{Q}$

The goal of this course is to obtain similar results when L is any global field. Even though most of the results still hold in the case where L is a finite extension of $\mathbf{F}_q(T)$, we will mostly restrict ourselves to the case where L is a number field.

Let us first explain what happens in the case $L = \mathbf{Q}$. An example of an abelian extension of $\mathbf{Q}$ is (a subfield of) the cyclotomic field $\mathbf{Q}(\zeta_n)$ (where n is a positive integer and ζ_n is a primitive n -th root of unity) and we have $\text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$.

Theorem 1.6 (Global Kronecker-Weber theorem). *Every finite abelian extension K of $\mathbf{Q}$ is contained in $\mathbf{Q}(\zeta_n)$ for some positive integer n .*

The above theorem will follow from its local version Theorem 1.1. Before writing the proof, let us recall Minkowski's theorem:

Theorem 1.7. *There are no nontrivial extensions of $\mathbf{Q}$ which are unramified everywhere.*

Proof of Theorem 1.6. The statement for the global case will follow from the local one.

Let p be a prime number such that K ramifies over p and $\mathfrak{p}$ a prime ideal of K that divides p . By Local Kronecker-Weber theorem (Theorem 1.1), we know that there exists an integer n_p such that the completion $K_{\mathfrak{p}}$ of K is contained in $\mathbf{Q}_p(\zeta_{n_p})$. Define $n := \prod_p p^{v_p(n_p)}$ (note that the product is finite since only finitely many primes ramify in K). Our goal is to show $K \subset \mathbf{Q}(\zeta_n)$. To do that, we prove that we have in fact $K(\zeta_n) = \mathbf{Q}(\zeta_n)$. The right hand side is obviously contained in the left hand side, so it is enough to prove that $[K(\zeta_n) : \mathbf{Q}] \leq [\mathbf{Q}(\zeta_n) : \mathbf{Q}]$.

Set $L := K(\zeta_n)$ and for any prime p , consider I_p the inertia group of p in L . Take $\mathfrak{p}$ a prime ideal of K dividing p and $\mathfrak{q}$ prime ideal of L dividing $\mathfrak{p}$. The elements of the completion $L_{\mathfrak{q}}$ fixed by I_p correspond to the maximal unramified extension F of $\mathbf{Q}_p$ contained in $L_{\mathfrak{q}}$. But since $\mathbf{Q}_p(\zeta_m)/\mathbf{Q}_p$ is unramified for any m prime to p and $L_{\mathfrak{q}} \subset \mathbf{Q}_p(\zeta_{\text{lcm}(n, n_p)})$ (by definition of L), we have

$$L_{\mathfrak{q}} \supset F(\zeta_{p^{v_p(n_p)}}) = F(\zeta_{p^{v_p(n_p)}}, \zeta_n) \supset K_{\mathfrak{p}}(\zeta_n) = L_{\mathfrak{q}},$$

so $L_{\mathfrak{q}} = F(\zeta_{p^{v_p(n_p)}})$ and $I_p = \text{Gal}(F(\zeta_{p^{v_p(n_p)}})/F) \subset (\mathbf{Z}/p^{v_p(n_p)}\mathbf{Z})^\times$. Defining I as the group generated by all the I_p 's, we obtain

$$|I| \leq \prod_{p \text{ prime}} |I_p| \leq \prod \phi(p^{v_p(n_p)}) = \phi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}].$$

Now, the elements of L fixed by I correspond to an extension of $\mathbf{Q}$ which is everywhere unramified. By Minkowski's theorem, only $\mathbf{Q}$ satisfies such a property. This means that $I \simeq \text{Gal}(L/\mathbf{Q})$. We have proved:

$$[L : \mathbf{Q}] = |I| \leq [\mathbf{Q}(\zeta_n) : \mathbf{Q}],$$

as wanted. □

For K a finite abelian extension of $\mathbf{Q}$, the smallest n such that $K \subset \mathbf{Q}(\zeta_n)$ is called the conductor of K .

Using the Kronecker-Weber theorem, we can then construct an Artin map for $\mathbf{Q}$ and deduce a reciprocity law. Indeed, consider $K/\mathbf{Q}$ an abelian extension with conductor n . Let us denote

by S_n the subgroup of $\mathbf{Q}^\times$ generated by all the primes p which do not divide n . For p in S_n , the extension $K/\mathbf{Q}$ is unramified above p so the inertia group I_p is trivial and the decomposition subgroup $D_p \subset \text{Gal}(K/\mathbf{Q})$ is generated by an element Frob_p such that it is equal to $x \mapsto x^p$ module any $\mathfrak{p}$ dividing p . We obtain a morphism

$$(1.4.1) \quad \begin{cases} S_n & \rightarrow \text{Gal}(K/\mathbf{Q}) \\ p & \mapsto \text{Frob}_p. \end{cases}$$

But since K is contained in $\mathbf{Q}(\zeta_n)$, we also have a surjective morphism:

$$(1.4.2) \quad (\mathbf{Z}/n\mathbf{Z})^\times \simeq \text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \rightarrow \text{Gal}(K/\mathbf{Q})$$

Proposition 1.8. *The morphism (1.4.1) factors through the morphism (1.4.2).*

Proof. The image of an element $m \in (\mathbf{Z}/n\mathbf{Z})^\times$ by (1.4.2) sends ζ_n to ζ_n^m . So for p a prime which does not divide n , the image of $m \in (\mathbf{Z}/n\mathbf{Z})^\times$ by (1.4.2) is equal to Frob_p if and only if there exists a prime ideal $\mathfrak{p}$ of K which divides p such that $\zeta_n^m = \zeta_n^p \pmod{\mathfrak{p}}$. But this is possible only if $m \equiv p \pmod{n}$ (exercise). So Frob_p is equal to the image of p by (1.4.2). $\square$

1.5 Approximation theorems

Let us finish this section by recalling/stating the following approximation theorems.

Theorem 1.9 (Weak Approximation Theorem). *Let K be any field and let $|\cdot|_1, \dots, |\cdot|_n$ be pairwise inequivalent non-trivial absolute values on K . Let $a_1, \dots, a_n$ be elements in K and $\varepsilon_1, \dots, \varepsilon_n$ elements in $\mathbf{R}_{>0}$. Then there exists $x \in K$ such that for all $1 \leq i \leq n$, we have $|x - a_i|_i < \varepsilon_i$.*

Proof. Exercise sheet 2. $\square$

Theorem 1.10 (Chinese remainders theorem). *Let A be a Dedekind domain and $K := \text{Frac}(A)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be distinct nonzero prime ideals of A . Let $e_1, \dots, e_n$ be integers.*

(1) *Let $a_1, \dots, a_n$ be in K . Then there exists $x \in K$ such that*

$$\begin{cases} v_{\mathfrak{p}_i}(x - a_i) \geq e_i & \text{for } 1 \leq i \leq n, \\ v_{\mathfrak{q}}(x) \geq 0 & \text{for all } \mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}. \end{cases}$$

(2) *There exists $x \in K$ such that*

$$\begin{cases} v_{\mathfrak{p}_i}(x) = e_i & \text{for } 1 \leq i \leq n, \\ v_{\mathfrak{q}}(x) \geq 0 & \text{for all } \mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}. \end{cases}$$

Proof. Exercise sheet 2. □

Theorem 1.11 (Strong Approximation Theorem). *Let K be a global field and let $|\cdot|_0, |\cdot|_1, \dots, |\cdot|_n$ be pairwise inequivalent non-trivial absolute values on K . Let $a_1, \dots, a_n$ be elements in K and $\varepsilon_1, \dots, \varepsilon_n$ elements in $\mathbf{R}_{>0}$. Then there exists $x \in K$ such that for all $1 \leq i \leq n$, we have $|x - a_i|_i < \varepsilon_i$ and $|x| \leq 1$ for any absolute value $|\cdot|$ not equivalent to $|\cdot|_0, |\cdot|_1, \dots, |\cdot|_n$.*

Proof. Will be proved in Section 3. □

Note that the strong approximation theorem gives a constraint for *all but one* equivalence class of absolute values.

2 The global Artin map

In this section, we define Artin maps for number fields and state the main results of global class field theory (global reciprocity law and global existence theorem).

2.1 Artin map

If K be a number field, we write I_K for its group of fractional ideals. If S is a finite set of primes of K , we denote by I_K^S the subgroup of I_K generated by the prime ideals which are not in S . An element $\mathfrak{a}$ of I_K^S can be uniquely decomposed as a product

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \text{ with } \mathfrak{p}_i \notin S \text{ and } n_i \in \mathbf{Z}.$$

In other words, I_K^S is the free abelian group generated by the prime ideals which are not in S .

Let L/K a finite abelian extension. We know that for a prime ideal $\mathfrak{p}$ of K unramified in L , we have a Frobenius automorphism $(\mathfrak{p}, L/K)$ of L (uniquely characterized by the two conditions given in Section 1.1). Let S be a set of primes of K which contains all prime ideals that ramify in L . Then we define the *global Artin map*

$$\Psi_{L/K} : \begin{cases} I_K^S & \rightarrow \text{Gal}(L/K) \\ \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s} & \mapsto \prod_{i=1}^s (\mathfrak{p}_i, L/K)^{n_i} \end{cases}.$$

Example 2.1. (i) Let $K = \mathbf{Q}(\sqrt{d})$ with d a square-free integer and consider the set S of finite primes which ramify in K . If $d \equiv 1 \pmod{4}$, then S is equal to the set of primes p dividing d . If

$d \not\equiv 1 \pmod{4}$ then S is the set of primes dividing d together with 2. In that case the Artin map corresponds to the Legendre symbol:

$$\begin{cases} I_K^S & \rightarrow \text{Gal}(K/\mathbf{Q}) \simeq \{\pm 1\} \\ p & \mapsto \left(\frac{d}{p}\right) \end{cases}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

(ii) If $K = \mathbf{Q}(\zeta_n)$ with ζ_n a primitive n -th root of 1 with n odd, the set S of finite primes which ramify in K is equal to the set of all primes dividing n . For r and s in $\mathbf{N}$ prime to n , we can define an element $[r/s]$ in $(\mathbf{Z}/n\mathbf{Z})^\times$ by setting $[r/s] = [r][s]^{-1}$. This defines a map

$$\begin{cases} I_K^S & \rightarrow (\mathbf{Z}/n\mathbf{Z})^\times \\ (r/s) & \mapsto [r/s] \end{cases}$$

The Artin map is given by the composition of this map with the isomorphism

$$\begin{cases} (\mathbf{Z}/n\mathbf{Z})^\times & \xrightarrow{\sim} \text{Gal}(K/\mathbf{Q}) \\ [m] & \mapsto (\zeta_n \mapsto \zeta_n^m). \end{cases}$$

Recall that for any finite extension L/K , there exists a norm map $\text{Nm}_{L/K} : I_L \rightarrow I_K$ uniquely characterized by the property that for any prime ideal $\mathfrak{q}$ of L , we have

$$\text{Nm}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})} \text{ with } \mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K.$$

Moreover, this norm map extends the usual norm in the sense that for all x in L , we have $\text{Nm}_{L/K}((x)) = (\text{Nm}_{L/K}(x))$.

Proposition 2.2. *Let L/K be an abelian extension and S be a finite set of primes of K containing all primes that ramify in L .*

(i) *If $K \subset K' \subset L$ is an intermediate field and S' is the set of primes of K' lying over a prime in S , then we have a commutative diagram:*

$$\begin{array}{ccc} I_{K'}^{S'} & \xrightarrow{\Psi_{L/K'}} & \text{Gal}(L/K') \\ \text{Nm}_{K'/K} \downarrow & & \downarrow \\ I_K^S & \xrightarrow{\Psi_{L/K}} & \text{Gal}(L/K) \end{array}$$

(ii) *If now S' is the set of primes of L lying above a prime of S , then the norm group $\text{Nm}_{L/K}(I_L^{S'})$ is contained in the kernel of $\Psi_{L/K} : I_K^S \rightarrow \text{Gal}(L/K)$.*

Proof. Let $\mathfrak{p}'$ be a prime ideal of K' such that $\mathfrak{p} := \mathfrak{p}' \cap K$ is not in S . Then $\Psi_{L/K}(\text{Nm}_{K'/K}(\mathfrak{p}')) = \Psi_{L/K}(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})})$ and to prove that this is equal to $\Psi_{L/K'}(\mathfrak{p}')$, it suffices to show that we have

$$(\mathfrak{p}', L/K') = (\mathfrak{p}', L/K)^{f(\mathfrak{p}'/\mathfrak{p})},$$

which is one of the properties recalled in Section 1.1.

The second point follows from the first one by taking $K' = L$. □

In particular, we see that the Artin map induces a morphism

$$\Psi_{L/K} : I_K^S / \text{Nm}_{L/K}(I_L^S) \rightarrow \text{Gal}(L/K)$$

Note that this map cannot be injective: there are finitely many elements in $\text{Gal}(L/K)$ and the left-hand side is infinite. In order to get something injective, we need to quotient out further.

2.2 Ray class groups

Reminders about ideal class group. We denote by $i : K \rightarrow I_K$ the natural map sending $a \in K$ to the corresponding fractional ideal $a\mathcal{O}_K := \{ax \mid x \in \mathcal{O}_K\}$. The ideal class group is then defined as

$$C_K := I_K / i(K^\times).$$

This defines a finite abelian group. Recall that the fact it is finite follows from the fact that we can find a set of representatives for C_K which consists of (integral) ideals $\mathfrak{a}$ such that

$$(2.2.1) \quad N(\mathfrak{a}) (= |\mathcal{O}_K/\mathfrak{a}|) \leq \frac{d!}{d^s} \left(\frac{4}{\pi}\right)^s |\Delta_K|^{\frac{1}{2}}$$

where $d := [K : \mathbb{Q}]$, Δ_K is the discriminant of $K/\mathbb{Q}$ and $2s$ is the number of complex embeddings of K .

For S a finite set of prime ideals, we write

$$K^S = \{a \in K^\times \mid \text{ord}_{\mathfrak{p}}(a) = 0 \text{ for all finite } \mathfrak{p} \in S\} = \{a \in K^\times \mid (a) \in I_K^S\}.$$

Recall that I_K^S is the free abelian group generated by the prime ideals which are not in S .

We have:

Proposition 2.3. *For any finite set S of prime ideals of $\mathcal{O}_K$, there is an exact sequence:*

$$0 \rightarrow \mathcal{O}_K^\times \rightarrow K^\times \xrightarrow{i} I_K^S \rightarrow C_K \rightarrow 0.$$

Proof. The fact that $0 \rightarrow \mathcal{O}_K^\times \rightarrow K^S \xrightarrow{i} I_K^S \rightarrow C_K$ is exact is clear. Let us prove that the map $I_K^S \rightarrow C_K$ is surjective. Consider a class $[\mathfrak{a}]$ of ideals in C_K , with $\mathfrak{a}$ a (fractional) ideal representing it. We can assume that $\mathfrak{a}$ is integral: if it is not, write $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral and replace $\mathfrak{a}$ by $\mathfrak{a} \cdot (\mathfrak{c})$ for any $c \in \mathfrak{c}$. So from now on, assume that $\mathfrak{a}$ is integral. Our goal is to construct an element $a \in \mathcal{O}_K$ such that $a^{-1}\mathfrak{a}$ is in I_K^S . To do that, we first decompose $\mathfrak{a}$ as a product $(\prod_{\mathfrak{p} \in S} \mathfrak{p}^{m(\mathfrak{p})}) \cdot \mathfrak{a}'$ where $\mathfrak{a}'$ is in I_K^S . Then, by Chinese remainder theorem, we know that there exists an element $a \in \mathcal{O}_K$ such that $\text{ord}_{\mathfrak{p}}(a) = m(\mathfrak{p})$, we thus obtain $a^{-1}\mathfrak{a} \in I_K^S$, as wanted.

□

Remark 2.4. (1) Note that we can in fact represent any class of C_K by an integral ideal $\mathfrak{a} \in I_K^S$: as before, write $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral and replace $\mathfrak{a}$ by $\mathfrak{a} \cdot (\mathfrak{c})$ for any $c \in \mathfrak{c} \cap K^S$ – the latter being non empty by Chinese remainder theorem.

(2) For S a finite set of prime ideals of K , we claim that any element $x \in K^S$ can be written as $\frac{y}{z}$ with $y, z \in \mathcal{O}_K \cap K^S$. Indeed, we can write (x) as $\mathfrak{a} \cdot \mathfrak{b}^{-1}$ with $\mathfrak{a}$ and $\mathfrak{b}$ integral ideals in I_K^S . By definition, this means $[\mathfrak{a}] = [\mathfrak{b}]$ in C_K . Choose $\mathfrak{c}$ an integral ideal of I_K^S representing $[\mathfrak{a}]^{-1}$ in C_K , then there exist $y, z \in \mathcal{O}_K \cap K^S$ such that $\mathfrak{a}\mathfrak{c} = (y)$ and $\mathfrak{b}\mathfrak{c} = (z)$. We obtain $(x) = (y)(z)^{-1}$.

Definition of ray class groups. A modulus $\mathfrak{m}$ for K is a product $\prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ where

- $m(\mathfrak{p})$ is ≥ 0 for all primes $\mathfrak{p}$ and is 0 for all but finitely many $\mathfrak{p}$,
- if $\mathfrak{p}$ is real then $m(\mathfrak{p})$ is in $\{0, 1\}$ and if $\mathfrak{p}$ is complex then $m(\mathfrak{p})$ is zero.

We sometimes write $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$ where $\mathfrak{m}_\infty$ is a product of real primes and $\mathfrak{m}_0$ is a product of powers of prime ideals. In particular, $\mathfrak{m}_0$ can be seen as an ideal of K . We say that a prime $\mathfrak{q}$ divides the modulus $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ if $m(\mathfrak{q}) > 0$. Denote by $S(\mathfrak{m})$ the set of all places (real and finite) which divide $\mathfrak{m}$.

For $\mathfrak{m}$ a modulus, we define the subgroup $K_{\mathfrak{m},1} \subset K^\times$ as

$$K_{\mathfrak{m},1} := \left\{ a \in K^\times \mid \begin{cases} a_v > 0 \text{ for all real place } v \text{ dividing } \mathfrak{m} \\ \text{ord}_{\mathfrak{p}}(a - 1) \geq m(\mathfrak{p}) \text{ for all finite place } \mathfrak{p} \text{ dividing } \mathfrak{m} \end{cases} \right\}.$$

Then for any $x \in K_{\mathfrak{m},1}$ and $\mathfrak{p}$ a prime dividing $\mathfrak{m}$, the $\mathfrak{p}$ -adic valuation of x is zero (to see that, write x as the sum of $(x - 1)$ and 1 and use that $v_{\mathfrak{p}}(x - 1) > v_{\mathfrak{p}}(1)$). This means that the ideal (x) is in $I_K^{S(\mathfrak{m})}$. We write again $i : K_{\mathfrak{m},1} \rightarrow I_K^{S(\mathfrak{m})}$ the map $a \mapsto (a)$. We define the ray class group modulo $\mathfrak{m}$ as the quotient

$$C_{\mathfrak{m}} := I_K^{S(\mathfrak{m})} / i(K_{\mathfrak{m},1}).$$

Example 2.5. (1) If $\mathfrak{m} = 1$ is trivial, we recover the usual ideal class group: $C_{\mathfrak{m}} = C_K$.

(2) If $\mathfrak{m} = \prod_{\mathfrak{p} \text{ real place}} \mathfrak{p}$, we obtain what is called the *narrow class group*: $C_{\mathfrak{m}} = C_K^+$. It is the quotient of I_K by the principal ideal $a\mathcal{O}_K$ with a such that $\sigma(a) > 0$ for any $\sigma : K \hookrightarrow \mathbf{R}$ real

embedding. It is used for solving questions regarding the representation of integers by quadratic forms.

(3) If $K = \mathbf{Q}$ and $\mathfrak{m} = (n)\infty$ then $S(\mathfrak{m})$ is equal to the set of primes dividing n and we obtain $C_{\mathfrak{m}} = (\mathbf{Z}/n\mathbf{Z})^\times$.

Remark 2.6. (1) Let $\mathfrak{m}$ be a modulus for K . Then any element of $C_{\mathfrak{m}}$ can be represented by an integral ideal. Let $\mathfrak{a}$ be an ideal in I_K^S . Write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals in I_K^S . By weak approximation theorem (Theorem 1.9), there exists a nonzero element c in $\mathfrak{c} \cap K_{\mathfrak{m},1}$. Then $c\mathfrak{a}$ is integral and $[c\mathfrak{a}] = [\mathfrak{a}]$ in $C_{\mathfrak{m}}$.

(2) Let $\mathfrak{a}$ and $\mathfrak{b}$ be two integral ideals in $I_K^{S(\mathfrak{m})}$. Using Remark 2.4, we see that $[\mathfrak{a}]$ is equal to $[\mathfrak{b}]$ in $C_{\mathfrak{m}}$ if and only if there exist a, b in $\mathcal{O}_K$ such that

$$\begin{cases} a\mathfrak{a} = b\mathfrak{b}, \\ a = b = 1 \pmod{\mathfrak{m}_0}, \\ \text{sgn}(a_v) = \text{sgn}(b_v) \text{ for any real place } v \text{ dividing } \mathfrak{m}. \end{cases}$$

2.3 Finiteness of ray class groups

The ray class group is actually a finite group. More precisely:

Theorem 2.7. *For any modulus $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$ of K , the group $C_{\mathfrak{m}}$ is finite of order*

$$h_{\mathfrak{m}} = h \cdot |U_K/U_{\mathfrak{m},1}|^{-1} \cdot 2^r \cdot N(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

where r is the number of real places dividing $\mathfrak{m}$ and h is the class number of K and $U_{\mathfrak{m},1} := U_K \cap K_{\mathfrak{m},1}$.

We also set $K_{\mathfrak{m}} := K^{S(\mathfrak{m})} = \{x \in K^\times \mid v_{\mathfrak{p}}(x) = 0 \text{ for all } \mathfrak{p} \text{ dividing } \mathfrak{m}_0\}$. Before proving the theorem, let us first show:

Proposition 2.8. *For any modulus $\mathfrak{m}$, there is an exact sequence:*

$$0 \rightarrow U_K/U_{\mathfrak{m},1} \rightarrow K_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{i} C_{\mathfrak{m}} \rightarrow C_K \rightarrow 0,$$

where the map $C_{\mathfrak{m}} \rightarrow C$ is induced by the inclusion $I_K^{S(\mathfrak{m})} \subset I_K$.

Proof. For this proof only, let us write

$$\begin{aligned} i_1 : K_{\mathfrak{m},1} &\rightarrow I_K^{S(\mathfrak{m})} \\ i_0 : K_{\mathfrak{m}} = K^{S(\mathfrak{m})} &\rightarrow I_K^{S(\mathfrak{m})} \end{aligned}$$

The kernel and cokernel of i_0 were computed in Proposition 2.3. By definition, the cokernel of i_1 is C_m and by construction, its kernel is $U_K \cap K_{m,1}$. In summary, we have:

$$\begin{aligned} \text{Ker}(i_1) &= U_{m,1}, & \text{Coker}(i_1) &\simeq C_m \\ \text{Ker}(i_0) &= U_K, & \text{Coker}(i_0) &\simeq C_K. \end{aligned}$$

The result then follow from the snake lemma applied to the exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K_{m,1} & \longrightarrow & K_m & \longrightarrow & K_m/K_{m,1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & I_K^{S(m)} & \xlongequal{\quad} & I_K^{S(m)} & \longrightarrow & 0 \end{array}$$

□

Proof of Theorem 2.7. In order to prove the theorem, we first show that there is a natural isomorphism

$$(2.3.1) \quad K_m/K_{m,1} \simeq \prod_{v \text{ real s.t. } v|m} \{\pm 1\} \times \prod_{\mathfrak{p} \text{ finite s.t. } \mathfrak{p}|m} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times.$$

If v is a real place dividing m , the map to the corresponding term $\{\pm 1\}$ in the product is obtained by taking the sign of the image $x_v \in \mathbf{R}$ of $x \in K_m$ via the embedding $K \rightarrow \mathbf{R}$ given by v . If $\mathfrak{p}$ is a finite place of K dividing m , then by Lemma 2.4, we can write any element x of K_m as a quotient $\frac{y}{z}$ with $y, z \in \mathcal{O}_K \cap K^{S(m)}$. In particular, this means that $\mathfrak{p}$ does not divide y and z and so their images in $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$ are invertible. We define the map $K_m \rightarrow (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$ by sending x to the class of yz^{-1} in $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$. We obtain a map

$$K_m \rightarrow \prod_{v \text{ real s.t. } v|m} \{\pm 1\} \times \prod_{\mathfrak{p} \text{ finite s.t. } \mathfrak{p}|m} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times.$$

By Theorem 1.9, we know that the above map is surjective. Moreover, its kernel is equal to $K_{m,1}$: this is because we have the following equivalences

$$\begin{aligned} x \in K_{m,1} &\Leftrightarrow \begin{cases} x_v > 0 \text{ for all real place } v \text{ dividing } m \\ \text{ord}_{\mathfrak{p}}(x-1) \geq m(\mathfrak{p}) \text{ for all finite place } \mathfrak{p} \text{ dividing } m \end{cases} \\ &\Leftrightarrow x \mapsto (1, 1, \dots, 1) \text{ in } \prod_{v \text{ real s.t. } v|m} \{\pm 1\} \times \prod_{\mathfrak{p} \text{ finite s.t. } \mathfrak{p}|m} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times. \end{aligned}$$

Note also that by Chinese remainder theorem, we have an isomorphism,

$$(2.3.2) \quad \prod_{\mathfrak{p} \text{ finite s.t. } v|m} \mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})} \simeq \mathcal{O}_K/\mathfrak{m}_0.$$

Let us now compute the order of C_m . From the exact sequence of Proposition 2.8, in order to get the expression from the statement of Theorem 2.7, it suffices to prove that $K_m/K_{m,1}$ has order $2^r \cdot N(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 - \frac{1}{N(\mathfrak{p})})$. But from isomorphisms (2.3.1) and (2.3.2), we are left to check that $(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$ has order $N(\mathfrak{p})^{m(\mathfrak{p})-1}(N(\mathfrak{p}) - 1)$.

The ring $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$ is local with maximal ideal $\mathfrak{p}/\mathfrak{p}^{m(\mathfrak{p})}$ and so we have

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times = (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}) \setminus (\mathfrak{p}/\mathfrak{p}^{m(\mathfrak{p})}).$$

Define the filtration

$$F^i((\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times) := (1 + \mathfrak{p}^i)/\mathfrak{p}^{m(\mathfrak{p})}, \text{ for } 0 \leq i \leq m(\mathfrak{p}) - 1.$$

The quotient gr_F^i is equal to $(\mathcal{O}_K/\mathfrak{p})^\times$ when $i = 0$ and $\mathcal{O}_K/\mathfrak{p}$ otherwise. We get that its order is equal to $N(\mathfrak{p})^{m(\mathfrak{p})-1}(N(\mathfrak{p}) - 1)$. $\square$

2.4 Main results of global class field theory

The two main theorems of global class field theory are the following:

Theorem 2.9 (Reciprocity Law). *Let L be a finite extension abelian of K and consider S the set of all prime ideals of K that ramify in L . Then there exists a modulus $\mathfrak{m}$ with $S = S(\mathfrak{m})$ such that $i(K_{\mathfrak{m},1})$ is in the kernel of the Artin map $\Psi_{L/K} : I_K^S \rightarrow \text{Gal}(L/K)$ and such that the induces map*

$$I_K^{S(\mathfrak{m})} / (i(K_{\mathfrak{m},1}) \cdot \text{Nm}_{L/K}(I_L^{S(\mathfrak{m})'})) \rightarrow \text{Gal}(L/K)$$

is an isomorphism. Here $S(\mathfrak{m})'$ denotes the set of all places of L lying above a place of $S(\mathfrak{m})$.

Theorem 2.10 (Existence Theorem). *Let $\mathfrak{m}$ be a modulus. Then for any group H such that $i(K_{\mathfrak{m},1}) \subset H \subset I_K^{S(\mathfrak{m})}$, there exists a finite abelian extension L/K which is unramified at the primes not in $S(\mathfrak{m})$ and such that $H = i(K_{\mathfrak{m},1}) \cdot \text{Nm}_{L/K}(I_L^{S(\mathfrak{m})'})$.*

The goal of the course will be to prove these two theorems.

Let us now fix a modulus $\mathfrak{m}$. Theorem 2.10 shows that there exists an extension L_m/K such that the Artin map induces an isomorphism $C_m \xrightarrow{\sim} \text{Gal}(L_m/K)$. Then we obtain a bijection

$$\begin{aligned} \{L/K \text{ abelian extensions s.t. } L \subset L_m\} &\xrightarrow{\sim} \{\text{subgroups } H \subset C_m\} \\ L &\mapsto i(K_{\mathfrak{m},1}) \cdot \text{Nm}_{L/K}(I_L^{S(\mathfrak{m})'}) \bmod i(K_{\mathfrak{m},1}). \end{aligned}$$

Conductor. The notion of conductor introduced in the case of $\mathbf{Q}$ can be extended to other extensions of number fields as well. Consider L/K be an abelian extension with Galois group G

and let $\mathfrak{m}$ be the modulus given by Theorem 2.9. Then the Artin map $\Psi_{L/K} : I_K^{S(\mathfrak{m})} \rightarrow G$ factors through $C_{\mathfrak{m}}$. The exact sequence 2.8 induces a map

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \hookrightarrow K_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{i} C_{\mathfrak{m}} \xrightarrow{\Psi_{L/K}} G.$$

Let us write $f(\mathfrak{p})$ the smallest integer such that the above map factors through $(\mathcal{O}_K/\mathfrak{p}^{f(\mathfrak{p})})^\times$. The conductor of L/K is then defined as the modulus

$$\mathfrak{f} := \mathfrak{f}(L/K) := \mathfrak{m}_\infty \prod_{\mathfrak{p}} \mathfrak{p}^{f(\mathfrak{p})}.$$

This is the smallest modulus such that $\Psi_{L/K}$ factors through $C_{\mathfrak{f}}$.

Example 2.11. (1) When $\mathfrak{m}$ is trivial then the ray class field $L_{\mathfrak{m}}$ corresponds to the Hilbert class field, which is the maximal extension of K which is unramified everywhere (we say that a real place in K is unramified in L if it stays real as a place in L). This result is known as the Principal Ideal Theorem:

Theorem 2.12. *Any (fractional) ideal of K becomes principal in the Hilbert class field.*

(2) When $K = \mathbb{Q}$ and $\mathfrak{m} = (n)_\infty$ then $L_{\mathfrak{m}}$ is equal to $\mathbb{Q}(\zeta_n)$.

3 The ring of adèles

We want to construct an isomorphism $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}} \xrightarrow{\sim} \text{Gal}(K^{\text{ab}}/K)$. However, the group $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$ is not very convenient to work with. Instead we will consider the group of the so-called idèles, and $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$ will be a quotient of it. We will study in more details the group of idèles in the next section. It corresponds in fact to the group of units of the ring of adèles. In this section, we focus on the latter ring.

3.1 Topological considerations: restricted product

Recall that we can embed the ring $\mathbb{Z}$ into the product of its non-archimedean completions $\prod_p \mathbb{Z}_p$ via the composition

$$\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$$

Moreover, the space $\prod_p \mathbb{Z}_p$ is compact (as a product of compact spaces, by Tychonoff's theorem). We would like to have a similar result for rational numbers. However, topology does not work well in that case: even though each one of the completion $\mathbb{Q}_p$ is locally compact, this is not true that the product $\prod_p \mathbb{Q}_p$ is so. This is because no compact set C in $\prod_p \mathbb{Q}_p$ contains a nonempty

open set U (otherwise, if $\prod_{n \in S \text{ finite}} U_n \times \prod_{n \in \mathbb{N} \setminus S} \mathbb{Q}_p \subset C$, then the projections $\pi_n(C)$ are $\mathbb{Q}_p$ for infinitely many n and $\mathbb{Q}_p$ is not compact). We are interested in locally compact spaces because in that case, it comes equipped with a Haar measure (any locally compact group has a translation-invariant measure that is unique up to scaling), which is useful. In order to get around that problem, we need to consider *restricted product*.

Definition 3.1. Let $(X_i)_{i \in I}$ be a family of topological spaces and let $(U_i)_{i \in I}$ be a family of open sets $U_i \subset X_i$. The restricted product $\prod_{i \in I} (X_i, U_i)$ is defined as the set

$$\prod_{i \in I} (X_i, U_i) := \{(x_i)_i \in \prod_{i \in I} X_i \mid x_i \in U_i \text{ for all but finitely many } i \in I\}$$

endowed with the topology generated by the basis of open sets

$$\mathcal{B} := \left\{ \prod_{i \in I} V_i \mid V_i \subset X_i \text{ is open for all } i \in I \text{ and } V_i = U_i \text{ for all but finitely many } i \in I \right\}.$$

For this topology, the natural projections $\pi_i : \prod_{i \in I} (X_i, U_i) \rightarrow X_i$ are continuous. As sets, we have inclusions:

$$\prod_{i \in I} U_i \subset \prod_{i \in I} (X_i, U_i) \subset \prod_{i \in I} X_i$$

However, the restricted product topology on $\prod_{i \in I} (X_i, U_i)$ is not the same as the one induced by $\prod_{i \in I} X_i$ via the inclusion $\prod_{i \in I} (X_i, U_i) \subset \prod_{i \in I} X_i$: it has more open sets. Note also that if we have other open sets $U'_i \subset X_i$ such that $U'_i = U_i$ for all but finitely many i then both as sets and topological sets:

$$\prod_{i \in I} (X_i, U_i) = \prod_{i \in I} (X_i, U'_i).$$

For S a finite subset of I , we define

$$(3.1.1) \quad X_S := \prod_{i \in S} X_i \times \prod_{i \notin S} U_i \subset \prod_{i \in I} (X_i, U_i)$$

Then $X_S \in \mathcal{B}$ is open. Note that on X_S the direct product topology coincide with the topology induced by the one coming from $\prod_{i \in I} (X_i, U_i)$.

If $S \subset T$ is an inclusion of finite subsets of I , then $X_S \subset X_T$ and we can define the direct limit $\varinjlim_S X_S$. For $x = (x_i)_i \in \prod_{i \in I} (X_i, U_i)$, let us denote $S(x)$ the finite subset of I such that $i \in S(x)$ iff $x_i \notin U_i$. We have:

Proposition 3.2. Let $(X_i)_{i \in I}$ be a family of topological spaces and let $(U_i)_{i \in I}$ be a family of open sets $U_i \subset X_i$. Write $X := \prod_{i \in I} (X_i, U_i)$ and for any finite $S \subset I$ define X_S as in (3.1.1). Then the natural map

$$X \rightarrow \varinjlim_S X_S$$

sending $x \in X$ to the equivalence class of its image in $X_{S(x)}$ is an isomorphism of topological spaces.

Proof. Exercise. □

We can now apply the above construction in the case in which we are interested.

Proposition 3.3. *Let $(X_i)_{i \in I}$ be a family of locally compact topological spaces and let $(U_i)_{i \in I}$ be a family of open subsets $U_i \subset X_i$ such that all but finitely many U_i are compact. Then the restricted product $X := \prod_{i \in I} (X_i, U_i)$ is locally compact.*

Proof. Let $S \subset I$ be a finite set and consider the space X_S from (3.1.1). Since the U_i 's are open subspaces of X_i , they are locally compact and they are compact except for a finite number of them. We obtain that $\prod_{i \in I \setminus S} U_i$ is a product of an infinite product of compact spaces by a finite product of locally compact spaces: hence, by Tychonoff's theorem it is locally compact. Since the $X_i, i \in S$ are also all locally compact, we see that X_S is locally compact.

Let now x be a point in X . Then x is in $X_{S(x)}$ which is locally compact so x admits a compact neighborhood $x \subset U \subset K \subset X_{S(x)}$. Since K is also compact in X and U open in X (because $X_{S(x)}$ is open) then this defines a compact neighborhood of x in X . □

3.2 Definition of adèles

Definition 3.4. Let K be a global field. The adèle ring of K is the restricted product

$$\mathbb{A}_K := \prod_{v \text{ place of } K} (K_v, \mathcal{O}_v),$$

where we set $\mathcal{O}_v := K_v$ when v is archimedean. As a set, we then have

$$\mathbb{A}_K = \{(a_v) \in \prod_v K_v \mid a_v \in \mathcal{O}_v \text{ for all but finitely many } v\}.$$

We make $\mathbb{A}_K$ a ring by defining addition and multiplication component-wise.

If S is a finite set of places, we define the subring of S -adèles,

$$\mathbb{A}_{K,S} := \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$$

It is a direct product of topological ring. By Proposition 3.2, we can write $\mathbb{A}_K \simeq \varinjlim_S \mathbb{A}_{K,S}$. Since for each element x of K we have $x \in \mathcal{O}_v$ for all but finitely many v , there is a natural map

$$\begin{cases} K & \hookrightarrow \mathbb{A}_K \\ x & \mapsto (x, x, x, \dots). \end{cases}$$

The image of K via the above morphism is called the ring of principal adèles.

For v a place of K , the absolute value $|\cdot|_v$ can be extended to $\mathbb{A}_K$ by setting $|a|_v := |a_v|_v$ and we define the adèlic absolute norm as

$$|a| := \prod_v |a|_v$$

Note that the product is well-defined because $|a|_v \leq 1$ for almost all v . By the product formula, for any non-zero principal adèle a , we have $|a| = 1$.

Proposition 3.5. *Let K be a global field. Then the adèle ring $\mathbb{A}_K$ of K is locally compact and Hausdorff.*

Proof. Note that if v is finite then $\mathcal{O}_v = \{x \in K_v \mid |x|_v \leq 1\}$ is compact. Hence the fact that $\mathbb{A}_K$ is locally compact directly follows from Proposition 3.3. Moreover, since for any place the space K_v is Hausdorff, the product $\prod_v K_v$ is Hausdorff. Take x, y distinct in $\mathbb{A}_K \subset \prod_v K_v$. There exist U, V open subspaces of $\prod_v K_v$ such that $x \in U, y \in V$ and $U \cap V = \emptyset$. Since the subspace topology on $\mathbb{A}_K \subset \prod_v K_v$ is contained in the restricted product topology, we have that $U \cap \mathbb{A}_K$ and $V \cap \mathbb{A}_K$ are also open in $\mathbb{A}_K$. They contain x and y respectively and they are disjoint, hence, $\mathbb{A}_K$ is Hausdorff. $\square$

Example 3.6. For $K = \mathbb{Q}$, the ring of adèles $\mathbb{A}_{\mathbb{Q}}$ is the union of the rings $\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p$ for all S finite set of prime numbers. In other words, it is the subring of $\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Q}_p$ consisting of sequence x such that $|x|_p \leq 1$ for almost all $p \in \{\infty, \text{primes}\}$.

Remark 3.7. We can equip the (additive) group $\mathbb{A}_K$ with a Haar measure μ and since $(\mathbb{A}_K, +)$ defines a locally compact group, we know that it is unique up to scaling. Here is how our μ is defined. For any place v , the group $(K_v, +)$ can be equipped with a (unique) Haar measure μ_v such that $\mu_v(\mathcal{O}_v)$ is 1 if v is finite and μ_v coincides with the Lebesgue measure $\mu_{\mathbb{R}}$ on $\mathbb{R}$ when $K_v \simeq \mathbb{R}$ or with twice the Lebesgue measure $2\mu_{\mathbb{C}}$ on $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$ when $K_v \simeq \mathbb{C}$. On sets of the form $\prod_v B_v$ where each B_v is a measurable set in K_v such that $\mu_v(B_v) < \infty$ and B_v is equal to $\mathcal{O}_v$ for all but finitely many v , we set

$$\mu\left(\prod_v B_v\right) := \prod_v \mu_v(B_v).$$

By construction, this defines a translation invariant measure on $\mathbb{A}_K$ (each of the μ_v are translation invariant and the addition is defined termwise). So μ is a Haar measure and it is unique (up to scaling).

3.3 Base change of the ring of adèles

Proposition 3.8. *Let L/K be a finite extension of number fields. There is a canonical isomorphism of topological rings*

$$\mathbb{A}_K \otimes_K L \xrightarrow{\sim} \mathbb{A}_L$$

such that the following diagram commutes:

$$\begin{array}{ccc} K \otimes_K L & \xrightarrow{\sim} & L \\ \downarrow & & \downarrow \\ \mathbb{A}_K \otimes_K L & \xrightarrow{\sim} & \mathbb{A}_L \end{array}$$

Proof. By Proposition 3.2 and using the fact that tensor products commute with colimit, we see that $\mathbb{A}_K \otimes_K L$ is isomorphic to

$$\begin{aligned} \varinjlim_S (\mathbb{A}_{K,S} \otimes_K L) &\xrightarrow{\sim} \varinjlim_S \left(\prod_{v \in S} K_v \otimes_K L \times \prod_{v \notin S} \mathcal{O}_{K,v} \otimes_{\mathcal{O}_K} \mathcal{O}_L \right) \\ (a_v)_v \otimes x &\mapsto (a_v \otimes x)_v. \end{aligned}$$

The term on the right corresponds to the restricted product $\prod_v (K_v \otimes_K L, \mathcal{O}_{K,v} \otimes_{\mathcal{O}_K} \mathcal{O}_L)$, and this is a topological isomorphism. Moreover, for all place v of K , we also have

$$K_v \otimes_K L \simeq \prod_{w|v} L_w \quad \text{and} \quad \mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L \simeq \prod_{w|v} \mathcal{O}_w.$$

Putting everything together, we obtain isomorphisms of topological rings:

$$\mathbb{A}_K \otimes_K L \simeq \prod_{v \text{ place of } K} (K_v \otimes_K L, \mathcal{O}_{K,v} \otimes_{\mathcal{O}_K} \mathcal{O}_L) \simeq \prod_{w \text{ place of } L} (L_w, \mathcal{O}_w) \simeq \mathbb{A}_L.$$

The commutativity of the diagram is clear. □

In particular, if the extension L/K has degree d , then we have an isomorphism of topological K -vector spaces (and locally compact groups)

$$(3.3.1) \quad \mathbb{A}_L \simeq \mathbb{A}_K \oplus \mathbb{A}_K \oplus \cdots \oplus \mathbb{A}_K$$

where there is $[L : K]$ copies of $\mathbb{A}_K$ in the direct sum. When restricted to the subring of principal adèles, this decomposition recovers the usual decomposition

$$L \simeq K \oplus K \oplus \cdots \oplus K.$$

We can now prove the following result:

Theorem 3.9. *Let L/K be a finite extension of number fields. The principal adèle subring $L \hookrightarrow \mathbb{A}_L$ is a discrete subgroup of the additive group of $\mathbb{A}_L$ and the quotient $\mathbb{A}_L/L$ of topological groups is compact.*

Proof. By (3.3.1), we see that it suffices to prove the result for $L = \mathbf{Q}$. We want to show that $\mathbf{Q}$ is discrete as a subgroup of $\mathbb{A}_{\mathbf{Q}}$ and to do that, it is enough to check that 0 is an isolated point. Define

$$U := \{a \in \mathbb{A}_{\mathbf{Q}} \mid |a|_{\mathbf{R}} < 1 \text{ and } |a|_p \leq 1 \text{ for any prime } p\}.$$

If a is in $\mathbf{Q}^\times$, then $|a|_{\mathbf{R}} \cdot \prod_p |a|_p = 1$ so necessarily, $U \cap \mathbf{Q} = \{0\}$. It follows that 0 is isolated.

Let us now prove that $\mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$ is compact. We claim that it is the image by the continuous map $\mathbb{A}_{\mathbf{Q}} \rightarrow \mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$ of the compact set

$$W := D_{\mathbf{R}}(1) \times \prod_p \mathbf{Z}_p,$$

where $D_{\mathbf{R}}(1)$ is the closed disc of radius 1 in $\mathbf{R}$. To do that, we need to show that W contains a set of representatives of $\mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$. Let a be in $\mathbb{A}_{\mathbf{Q}}$. We construct an element x in $\mathbf{Q}$ such that $a - x$ is in W .

If $v = p$ is finite and $|a_p|_p \leq 1$ then set $x_p := 0$ (so almost all x_p will be zero). If $v = p$ is finite and $|a_p|_p > 1$ then by Theorem 1.10, we can find x_p in $\mathbf{Q}$ such that $|a_p - x_p|_p \leq 1$ and $|x_p|_q \leq 1$ for all prime $q \neq p$. If $v = \infty$ is the real place of $\mathbf{Q}$, then we define $x_\infty \in \mathbf{Z}$ to be the nearest integer to $a_\infty - \sum_p x_p \in \mathbf{Q}$. Then define $x := x_\infty + \sum_p x_p \in \mathbf{Q} \subset \mathbb{A}_{\mathbf{Q}}$. We want to check that $a - x$ is in W , i.e. $|a - x|_v \leq 1$ for all place v . If $v = p$ is finite then

$$|a - x|_p = |a_p - x_p - \sum_{v \neq p} x_v|_p \leq \max(|a_p - x_p|_p, \max_{v \neq p} |x_v|_p) \leq 1$$

and if $v = \infty$, then

$$|a - x|_{\mathbf{R}} = |(a_\infty - \sum_p x_p) - x_\infty|_{\mathbf{R}} \leq 1$$

by definition of x_∞ . This concludes the proof. $\square$

3.4 Strong approximation theorem

We will now use Theorem 3.9 to prove the strong approximation theorem (Theorem 1.11). Let us first prove the following proposition:

Proposition 3.10. *Let $K/\mathbf{Q}$ be a number field. There exists $C > 0$ such that for any x in $\mathbb{A}_K$ with norm $|x| > C$ there exists a nonzero principal adèle element $y \in K \subset \mathbb{A}_K$ for which $|y|_v \leq |x|_v$ for any place v of K .*

Proof. Recall that $\mathbb{A}_K$ is equipped with a Haar measure μ given by the product of (normalized) Haar measures μ_v for the places v . Define $c_0 := \text{covol}(K)$ for this Haar measure. By Theorem 3.9, c_0 is well defined. Set

$$c_1 = \mu(\{a \in \mathbb{A}_K \mid |a|_v \leq 1 \text{ for all } v \text{ and } |a|_v \leq \frac{1}{4} \text{ if } v \text{ is infinite}\}) \text{ and } C := \frac{c_0}{c_1}.$$

Let x be in $\mathbb{A}_K$ such that $|x| > C$. Since $|x|_v \leq 1$ for almost all v and $|x| \neq 0$, this means that $|x|_v = 1$ for almost all v . Define

$$A := \{a \in \mathbb{A}_K \mid |a|_v \leq |x|_v \text{ for all } v \text{ and } |a|_v \leq \frac{1}{4}|x|_v \text{ if } v \text{ is infinite}\}.$$

Then, since μ is defined as the product of the μ_v , we have

$$\mu(A) = c_1 \cdot |x| > c_1 \cdot C = c_0 = \text{covol}(K)$$

and we can find $a_1 \neq a_2$ in A such that $y := a_1 - a_2$ is zero in $\mathbb{A}_K/K$, i.e. $y \in K$. We have:

$$\begin{aligned} |y|_v &= |a_1 - a_2|_v \leq \max(|a_1|_v, |a_2|_v) \leq |x|_v && \text{if } v \text{ is finite,} \\ |y|_v &= |a_1 - a_2|_v \leq |a_1|_v + |a_2|_v \leq \frac{1}{2}|x|_v && \text{if } v \text{ is real,} \\ |y|_v &= |a_1 - a_2|_v \leq (\sqrt{|a_1|_v} + \sqrt{|a_2|_v})^2 \leq |x|_v && \text{if } v \text{ is complex,} \end{aligned}$$

as wanted. $\square$

Theorem 3.11. *Let $K/\mathbf{Q}$ be a number field. Let S be a finite set of places of K and v_0 a place of K such that $v_0 \notin S$. Write T for the set of places of K that are not in $S \cup \{v_0\}$. For each $v \in S$, let a_v be an element of K and ϵ_v a positive real number. Then there exists $x \in K$ such that*

$$\begin{cases} |x - a_v|_v \leq \epsilon_v \text{ for all } v \in S, \\ |x|_v \leq 1 \text{ for all } v \in T. \end{cases}$$

Proof. We have the following lemma:

Lemma 3.12. *Let $W_K := \{a \in \mathbb{A}_K \mid |a|_v \leq 1 \text{ for all place } v \text{ of } K\}$. Then for any u in $K^\times$, we can write $\mathbb{A}_K = K + uW_K$.*

Proof. By the proof of Theorem 3.9 and (3.3.1), we know that W_K contains a set of representatives of $\mathbb{A}_K/K$, so $\mathbb{A}_K = K + W_K$. If u is a non-zero element of K and a an element of $\mathbb{A}_K$ then $u^{-1}a$ is in $\mathbb{A}_K$ and we can write it as a sum $x + y$ with $x \in K$ and $y \in W_K$. It follows that a is equal to $ux + uy \in K + uW_K$ as wanted. $\square$

Let us extend the sequence $(a_v)_{v \in S}$ as an element a of $\mathbb{A}_K$ by setting $a_v = 0$ when $v \notin S$. For any $u \in K^\times$, we can write $a = b_u + c_u$ with $b_u \in K$ and $c_u \in uW_K$. Then

$$|a_v - b_u|_v = |a - b_u|_v = |c_u|_v \leq |u|_v$$

and to prove the theorem, it suffices to show that we can find $u \in K$ such that

$$\begin{cases} |u|_v \leq \epsilon_v \text{ for all } v \in S, \\ |u|_v \leq 1 \text{ for all } v \in T. \end{cases}$$

But this follows from Proposition 3.10 applied to an element $x = (x_v)_v \in \mathbb{A}_K$ such that

$$\begin{cases} 0 < |x_v|_v \leq \varepsilon_v & \text{if } v \in S, \\ 0 < |x_v|_v \leq 1 & \text{if } v \in T, \\ |x_{v_0}| > C \cdot \prod_{v \neq v_0} |x_v|^{-1}. \end{cases}$$

□

In particular, it follows from the above theorem that for K a global field and v_0 any fixed place of K , then K is dense in the restricted product $\prod_{v \neq v_0} (K_v, \mathcal{O}_v)$.

4 The group of idèles

We define now the *group of idèles* $\mathbb{I}_K$ of a number field K , which is the group of units of the ring of adèles defined in the previous section. We will show below that $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$ is a quotient of $\mathbb{I}_K$.

4.1 Definition of idèles

Recall that the group $K_v^\times$ is locally compact: a fundamental system of neighborhoods of 1 which are open and compact is given by

$$1 + \mathfrak{m}_v \supset 1 + \mathfrak{m}_v^2 \supset 1 + \mathfrak{m}_v^3 \supset \cdots \supset 1 + \mathfrak{m}_v^n \supset \cdots.$$

Local field theory and Section 2 suggest that what should appear as the source of the global Artin map should be the group $\prod_v K_v^\times$. As before, the problem is that the product $\prod_v K_v^\times$ is not locally compact. A first guess for what should be the right topological group to consider would be the set

$$\{(a_v)_v \in \mathbb{A}_K \mid a_v \in K_v^\times \text{ for all } v \text{ and } a_v \in \mathcal{O}_v^\times \text{ for almost all } v\}$$

endowed with the subspace topology. However, for this topology, we claim that the inverse map $x \mapsto x^{-1}$ is not necessarily continuous.

This problem can be easily solved by considering instead the restricted product topology:

Definition 4.1. We define the group of idèles of a global field K as the restricted product:

$$\mathbb{I}_K := \prod_v (K_v^\times, \mathcal{O}_v^\times).$$

The multiplication is defined term-wise.

Note that for this topology, we obtain that the natural injective group morphism

$$\begin{cases} \mathbb{I}_K & \rightarrow \mathbb{A}_K \times \mathbb{A}_K \\ x & \mapsto (x, x^{-1}). \end{cases}$$

induces an isomorphism of topological spaces onto its image.

As before, if S is a finite set of primes that contains all infinite primes, we also define:

$$\mathbb{I}_{K,S} := \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times,$$

endowed with the product topology and we have an isomorphism of topological groups $\mathbb{I}_K \simeq \varinjlim_S \mathbb{I}_{K,S}$ by Proposition 3.2. Each $\mathbb{I}_{K,S}$ is open in $\mathbb{I}_K$.

There is a canonical map

$$\begin{cases} \mathbb{I}_K & \rightarrow I_K \\ (a_v) & \mapsto \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})} \end{cases}$$

which is surjective with kernel $\mathbb{I}_{K,S_\infty}$, where S_∞ is the set of infinite places. The canonical embedding $K \hookrightarrow \mathbb{A}_K$ induces a canonical embedding of $K^\times$ into $\mathbb{I}_K$ that we will denote by i .

Proposition 4.2. *Let K be a global field. The idèle group $\mathbb{I}_K$ is a locally compact group.*

Proof. In order to apply Proposition 3.3, we need to check that the spaces $\mathcal{O}_v^\times$ are compact except for a finite numbers of them. But for any nonarchimedean place $\mathfrak{p}$, we see that $\mathcal{O}_{\mathfrak{p}}^\times := \{x \in K_{\mathfrak{p}}^\times \mid |x|_{\mathfrak{p}} = 1\}$ is closed in K_v , which is Hausdorff, hence it is compact. Since the $K_v^\times$'s are all locally compact, this concludes the proof. $\square$

Proposition 4.3. *Let K be a global field. Then $K^\times$ is a discrete subgroup of $\mathbb{I}_K$.*

Proof. Consider the natural embedding $K^\times \hookrightarrow K \times K \subset \mathbb{A}_K \times \mathbb{A}_K$. From Theorem 3.9, we know that K is a discrete subset of $\mathbb{A}_K$, so $K \times K$ is a discrete subset of $\mathbb{A}_K \times \mathbb{A}_K$. But the above embedding factors through $\mathbb{I}_K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, which is a topological embedding. Hence $K^\times$ is a discrete subgroup of $\mathbb{I}_K$. $\square$

We define the idèle class group of K as the quotient $\mathbb{C}_K := \mathbb{I}_K / K^\times$. The map $\mathbb{I}_K \rightarrow I_K$ from above induces a surjective morphism $\mathbb{C}_K \twoheadrightarrow C_K$.

Example 4.4. There is an isomorphism of topological groups (where $\mathbf{Q}^\times$ is given the discrete topology):

$$\begin{cases} \mathbf{Q}^\times \times \mathbf{R}_{>0} \times \prod_p \mathbf{Z}_p^\times & \rightarrow \mathbb{I}_{\mathbf{Q}} \\ (r, \lambda, (u_p)) & \mapsto (r\lambda, (ru_p)), \end{cases}$$

which induces an isomorphism:

$$\mathbb{C}_{\mathbf{Q}} \xrightarrow{\sim} \mathbf{R}_{>0} \times \prod_p \mathbf{Z}_p^{\times} \simeq \mathbf{R}_{>0} \times \widehat{\mathbf{Z}}^{\times}.$$

Group of 1-idèles. We have a continuous surjective morphism of topological groups

$$|\cdot| : \begin{cases} \mathbb{I}_K & \rightarrow \mathbf{R}_{>0} \\ a & \mapsto |a| := \prod_v |a_v|_v. \end{cases}$$

Note that since $|a|_v = 1$ for all but a finite number of v , the product is well-defined. It is non-zero since a_v is in $K_v^{\times}$ for all v . We denote by $\mathbb{I}_K^1$ the kernel of $|\cdot|$, i.e.

$$\mathbb{I}_K^1 := \{a \in \mathbb{I}_K \mid |a| = 1\}.$$

We endow it with the subspace topology. By the product formula, we know that $K^{\times}$ is contained inside $\mathbb{I}_K^1$. We have seen before that the quotient $\mathbb{A}_K/K$ is compact. However, this is not true that $\mathbb{I}_K/K^{\times}$ is compact (since it surjects onto $\mathbf{R}_{>0}$). Our next goal is to prove that in fact the quotient $\mathbb{I}_K^1/K^{\times}$ is compact. We start by collecting a few useful lemmas.

Lemma 4.5. *The subspace topologies on $\mathbb{I}_K^1$ coming from $\mathbb{I}_K$ and $\mathbb{A}_K$ coincide.*

Proof. First note that the restricted product topology on $\mathbb{I}_K$ is finer than the topology on $\mathbb{I}_K$ coming from $\mathbb{I}_K \subset \mathbb{A}_K$. So we only need to show that any open of $\mathbb{I}_K^1 \subset \mathbb{I}_K$ is also an open of $\mathbb{I}_K^1 \subset \mathbb{A}_K$.

Define $K_v^1 := \{x \in K_v^{\times} \mid |x|_v = 1\}$. Let $U = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v^{\times}$ be in the basis of the restricted product topology on $\mathbb{I}_K$. Setting $U_v = K_v^{\times}$ if needed, we can assume that S contains all infinite places. We have

$$U \cap \mathbb{I}_K^1 = \prod_{v \in S} (U_v \cap K_v^1) \times \prod_{v \notin S} \mathcal{O}_v^{\times}.$$

Let us define $U' := \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v$. Since U_v is open in $K_v^{\times}$ which is open in K_v , we see that U' is open in $\mathbb{A}_K$ and we have

$$U \cap \mathbb{I}_K^1 = U' \cap \mathbb{I}_K^1$$

which concludes the proof. □

Lemma 4.6. *The subgroup $\mathbb{I}_K^1$ is a closed subset of $\mathbb{A}_K$.*

Proof. We prove that $\mathbb{A}_K \setminus \mathbb{I}_K^1$ is open. Let x be in $\mathbb{A}_K \setminus \mathbb{I}_K^1$ and write S_0 for the finite set of places v such that $|x|_v > 1$. We also denote by S_{∞} the set of infinite places of K . For S a finite

set of places that contains S_0 and S_∞ and $\varepsilon := (\varepsilon_v)_v$ strictly positive, we define the open set of $\mathbb{A}_K$:

$$U_S(x, \varepsilon) := \{y \in \mathbb{A}_K \mid |x - y|_v < \varepsilon_v \text{ for } v \in S \text{ and } |y|_v \leq 1 \text{ for } v \notin S\}.$$

By construction it contains x . We will show that we can always find S and ε such that $U_S(x, \varepsilon) \subset \mathbb{A}_K \setminus \mathbb{I}_K^1$.

If $|x| < 1$ then we can find a finite set S such that S contains S_0, S_∞ and such that $\prod_{v \in S} |x|_v < 1$. For any v in S , take $\varepsilon < |x|_v$. Then for any element y of $U_S(x, \varepsilon)$, we have $|y|_v = \max(|x - y|_v, |x|_v) = |x|_v$ for $v \in S$. In particular,

$$|y| = \prod_v |y|_v \leq \prod_{v \in S} |y|_v = \prod_{v \in S} |x|_v < 1,$$

and y is not in $\mathbb{I}_K^1$.

Assume now that $|x| > 1$. Let M be such that $\prod_{v \in S_0} |x|_v \leq M$. Consider a finite set of places S such that S contains S_∞, S_0 and all finite places $v = \mathfrak{p}$ such that $N(\mathfrak{p}) \leq 2M$. This means that if v is not in S , then either $|x|_v = 1$ or $|x|_v < \frac{1}{2M}$. Note also that we have

$$1 < |x| \leq \prod_{v \in S} |x|_v \leq M < 2M$$

For any v in S , take $\varepsilon < |x|_v$. Then, as before, $\prod_{v \in S} |y|_v = \prod_{v \in S} |x|_v$. Now if y is in $U_S(x, \varepsilon)$ then either for all v not in S , we have $|y|_v = 1$ and this gives $|y| > 1$. If there exists v not in S such that $|y|_v < 1$, then in particular, for such a $v = \mathfrak{p}$, we have

$$|y|_v = N(\mathfrak{p})^{-\text{ord}_{\mathfrak{p}}(y)} < \frac{1}{2M} \quad \text{since } |y|_v < 1$$

and it follows that $|y| < 1$. In both cases $|y| \neq 1$. □

Theorem 4.7. *Let K be a global field. The group $K^\times$ is a discrete closed subgroup of the abelian group of 1-idèles $\mathbb{I}_K^1$ and the quotient group $\mathbb{I}_K^1/K^\times$ is compact.*

Proof. First note that since $K^\times$ is a discrete subgroup of $\mathbb{I}_K$ (by Lemma 4.3), it is also a discrete subgroup of $\mathbb{I}_K^1$. Since $\mathbb{I}_K^1$ is Hausdorff, we obtain that $K^\times$ is closed in $\mathbb{I}_K^1$. Moreover, by Lemma 4.6, we know that if W is a compact subspace of $\mathbb{A}_K$ then $W \cap \mathbb{I}_K^1$ is compact. So, to prove that $\mathbb{I}_K^1/K^\times$ is compact, it suffices to find a compact $W \subset \mathbb{A}_K$ such that $W \cap \mathbb{I}_K^1$ surjects onto $\mathbb{I}_K^1/K^\times$.

Consider the constant C from Proposition 3.10. Let x be in $\mathbb{A}_K$ such that $|x| > C$. Define

$$W := \{a \in \mathbb{A}_K \mid |a|_v \leq |x|_v \text{ for all } v\}.$$

Let y be in $\mathbb{I}_K^1$. We want to show that y can be written as a product az with a in $K^\times$ and z in $W \cap \mathbb{I}_K^1$. But $|y| = 1$ implies that $|\frac{x}{y}| = |x| > C$ and it follows from Proposition 3.10 that there exists b in $K^\times$ such that $|b|_v < |\frac{x}{y}|_v$ for all v . Setting $a := b^{-1}$ and $z := by$, we obtain the desired decomposition. □

Remark 4.8. Theorem 4.7 can be used to give a new proof of the finiteness of the class number for number fields and Dirichlet's unit theorem (see Exercise sheet 3).

Norm map for idèles. Let L/K be a finite extension of number fields. We define a norm map $\text{Nm}_{L/K} : \mathbb{I}_L \rightarrow \mathbb{I}_K$ in the following way: for $a = (a_w)_w$ in $\mathbb{I}_L$, we set $\text{Nm}_{L/K}(a) = b \in \mathbb{I}_K$ such that $b_v = \prod_{w|v} \text{Nm}_{L_w/K_v}(a_w)$. Recall that for any place v of K , we have an isomorphism $L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$ inducing the equality (as elements of K_v):

$$\text{Nm}_{L/K}(a) = \prod_{w|v} \text{Nm}_{L_w/K_v}(a_w) \text{ for any } a \in L$$

and in particular, the following diagram commutes:

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & I_L \\ \text{Nm}_{L/K} \downarrow & & \text{Nm}_{L/K} \downarrow & & \downarrow \text{Nm}_{L/K} \\ K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & I_K \end{array}$$

and we obtain a commutative diagram:

$$\begin{array}{ccc} \mathbb{C}_L & \longrightarrow & C_L \\ \text{Nm}_{L/K} \downarrow & & \downarrow \text{Nm}_{L/K} \\ \mathbb{C}_K & \longrightarrow & C_K. \end{array}$$

If $\mathfrak{m}$ is a modulus for K , we define:

$$(4.1.1) \quad W_{\mathfrak{m}} := \prod_{v \text{ infinite s.t. } v|\mathfrak{m}} K_v^\times \times \prod_{v \text{ finite s.t. } v \nmid \mathfrak{m}} U_v \times \prod_{v \text{ infinite s.t. } v \nmid \mathfrak{m}} \mathbf{R}_{>0} \times \prod_{v \text{ finite s.t. } v|\mathfrak{m}} 1 + \widehat{\mathfrak{p}}_v^{m(v)},$$

where $\widehat{\mathfrak{p}}_v$ is the maximal ideal of $\mathcal{O}_v$. Then we have:

Proposition 4.9. *Let L/K a finite Galois extension of number fields. Then there exists a modulus $\mathfrak{m}$ of K such that $W_{\mathfrak{m}} \subset \text{Nm}_{L/K}(\mathbb{I}_L)$.*

Proof. This is an immediate consequence of the following facts from local class field theory:

$$(1) \text{Nm}_{\mathbf{C}/\mathbf{R}}(\mathbf{C}^\times) = \mathbf{R}_{>0},$$

(2) If L/K is an extension of non-archimedean local fields then $\text{Nm}_{L/K}(L^\times)$ is an open subgroup of finite index of $K^\times$, in particular there exists m such that $1 + \mathfrak{m}_K^m \subset \text{Nm}_{L/K}(L^\times)$,

(3) If L/K is an extension of non-archimedean local fields such that L/K is unramified, then $\text{Nm}_{L/K} : U_L \rightarrow U_K$ is surjective, in particular $U_K \subset \text{Nm}_{L/K}(L^\times)$. $\square$

In particular, we have:

Corollary 4.10. *Let L/K a finite Galois extension of number fields. Then $\text{Nm}_{L/K}(\mathbb{I}_L)$ is open in $\mathbb{I}_K$.*

4.2 Ray class groups as quotient of idèles

If $\mathfrak{m}$ is a modulus for K , we define:

$$\mathbb{I}_{\mathfrak{m}} = \mathbb{I}_K \bigcap \left(\prod_{v \text{ s.t. } v \nmid \mathfrak{m}} K_v^\times \times \prod_{v \text{ infinite s.t. } v \mid \mathfrak{m}} \mathbf{R}_{>0} \times \prod_{v \text{ finite s.t. } v \mid \mathfrak{m}} 1 + \widehat{\mathfrak{p}}_v^{m(v)} \right).$$

Note that with the previous notations, we have $K_{\mathfrak{m},1} = K^\times \cap \mathbb{I}_{\mathfrak{m}}$.

Proposition 4.11. *If $\mathfrak{m}$ is a modulus for K , then the natural maps $\mathbb{I}_{\mathfrak{m}} \rightarrow I_K^{S(\mathfrak{m})}$ and $\mathbb{I}_{\mathfrak{m}} \rightarrow \mathbb{I}_K$ induce isomorphisms:*

$$\begin{aligned} \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} &\xrightarrow{\sim} C_{\mathfrak{m}} \\ \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} &\xrightarrow{\sim} \mathbb{I}_K/K^\times. \end{aligned}$$

Proof. The first isomorphism follows from the snake lemma applied to:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K_{\mathfrak{m},1} & \longrightarrow & \mathbb{I}_{\mathfrak{m}} & \longrightarrow & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \longrightarrow 0, \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & I_K^{S(\mathfrak{m})} & \xlongequal{\quad} & I_K^{S(\mathfrak{m})} & \longrightarrow & 0 \end{array}$$

using the facts that the first vertical arrow is injective and the second one is surjective with kernel $W_{\mathfrak{m}}$.

For the second isomorphism, first note that the kernel of $\mathbb{I}_{\mathfrak{m}} \rightarrow \mathbb{I}_K/K^\times$ is $K^\times \cap \mathbb{I}_{\mathfrak{m}}$, i.e. $K_{\mathfrak{m},1}$. This gives an injective map $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \hookrightarrow \mathbb{I}_K/K^\times$. Let us prove it is surjective. For a in $\mathbb{I}_K$, by weak approximation theorem, we can find x in $K^\times$ such that $a_v x^{-1}$ is in $\mathbf{R}_{>0}$ if v is real in $S(\mathfrak{m})$ and in $1 + \widehat{\mathfrak{p}}_v^{m(v)}$ if v is finite in $S(\mathfrak{m})$. Then ax^{-1} is in $\mathbb{I}_{\mathfrak{m}}$ and its image in $\mathbb{I}_K/K^\times$ is a . $\square$

In the following proposition, G can be any finite abelian group (even though we will apply it to the case where G is a Galois group). For S a finite set of places, we write $\mathbb{I}_K^S := \{a \in \mathbb{I}_K \mid a_v = 1 \text{ for all } v \in S\}$.

Proposition 4.12. *Let S be a finite set of places of K such that it contains S_∞ . Let $\psi : I_K^S \rightarrow G$ a morphism of groups such that there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \subset S$ and $\psi(K_{\mathfrak{m},1}) = 1$. Then there exists a unique continuous (for the discrete topology on G) morphism $\phi : \mathbb{I}_K \rightarrow G$ such that $\phi(K^\times) = 1$ and on $\mathbb{I}_K^S$, we have $\phi = \psi \circ i$, where i is the natural map $a = (a_v)_v \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(a)}$.*

Conversely, any continuous morphism $\phi : \mathbb{I}_K \rightarrow G$ such that $\phi(K^\times) = 1$ comes from a morphism $\psi : I_K^S \rightarrow G$.

Proof. Since there exists m such that $\psi(K_{m,1}) = 1$, this means that ψ factors through $C_m \rightarrow G$. Define ϕ as the composition:

$$\mathbb{I}_K \rightarrow \mathbb{I}_K/K^\times \xleftarrow{\sim} \mathbb{I}_m/K_{m,1} \rightarrow \mathbb{I}_m/K_{m,1} \cdot W_m \xrightarrow{\sim} C_m \xrightarrow{\psi} G.$$

It is clear that ϕ is continuous and that $\phi(K^\times)$ is trivial. We also have $\phi = \psi \circ i$ on $\mathbb{I}_m$ and so on $\mathbb{I}_K^S$.

To prove the uniqueness of such a map, it suffices to show that $\mathbb{I}_K^S K^\times$ is dense in $\mathbb{I}_K$ (since then, it is determined by its image on $K^\times$ and $\mathbb{I}_K^S$). But for a in $\mathbb{I}_K$, by approximation theorem, we can find x in $K^\times$ such that x is close to a_v for any v of S and we can find b in $\mathbb{I}_K^S$ such that $a_v = xb_v$ for v not in S . Then xb is in $\mathbb{I}_K^S K^\times$ and is closed to a in the group of idèles.

Conversely, let $\phi : \mathbb{I}_K \rightarrow G$ be a continuous morphism such that $\phi(K^\times)$ is trivial. We first prove that there exists some modulus m such that W_m is contained inside $\text{Ker}(\phi)$. Since the kernel $\phi^{-1}(1)$ is open (recall that G is discrete and ϕ is continuous), there exist some S finite set of places and positive number ε such that $U_S(1, \varepsilon) \subset \text{Ker}(\phi)$. Now if v is infinite, then ϕ induces a continuous morphism $\mathbf{R}^\times \rightarrow G$ (respectively $\mathbf{C}^\times \rightarrow G$). Since G is discrete, ϕ is constant equals to 1 on the connected component of $\mathbf{R}^\times$ (respectively $\mathbf{C}^\times$) which contains 1, i.e. $\mathbf{R}_{>0}$ (respectively $\mathbf{C}^\times$). So $\mathbf{R}_{>0}$ (respectively $\mathbf{C}^\times$) is in the kernel. This proves that we can find $W_m \subset \text{Ker}(\phi)$ and so the morphism $\phi : \mathbb{I}_m/K_{m,1} \simeq \mathbb{I}_K/K^\times \rightarrow G$ induces a morphism $\mathbb{I}_m/K_{m,1} \cdot W_m \rightarrow G$. We then use the isomorphism $\mathbb{I}_m/K_{m,1} \cdot W_m \simeq C_m$ to define $\psi : I_K^{S(m)} \rightarrow G$. $\square$

4.3 Artin map using idèles

From local class field theory, we know that for any finite abelian extension L/K , v place of K and w place of L dividing v , there is an Artin map:

$$\phi_v : K_v^\times \rightarrow \text{Gal}(L_w/K_v) \subset \text{Gal}(L/K).$$

Lemma 4.13. *The above map does not depend on the choice of the place w of L that divides v .*

Proof. Let w be a place of L such that $w|v$. Any other prime of L lying above v is of the form $\sigma(w)$ for σ in $\text{Gal}(L/K)$. Such a $\sigma : L \rightarrow L$ can be extended to an isomorphism $L_w \rightarrow L_{\sigma(w)}$ fixing K_v . We have $\text{Gal}(L_{\sigma(w)}/K_v) = \sigma \text{Gal}(L_w/K_v) \sigma^{-1} = \text{Gal}(L_w/K_v)$ since the extension is abelian. $\square$

We can then construct a global version of the Artin map for the idèles, namely:

Proposition 4.14. *Let K be a number field. There exists a unique continuous morphism $\phi_K : \mathbb{I}_K \rightarrow \text{Gal}(K^{\text{ab}}/K)$ such that for any finite abelian extension L/K and any place w of*

L lying over a place v of K , the following diagram commutes:

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \text{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow[\phi_{L/K}]{} & \text{Gal}(L/K), \end{array}$$

where $\phi_{L/K}$ is the map $a \mapsto \phi_K(a)|_L$.

Proof. Let a be in $\mathbb{I}_K$ and consider L/K a finite abelian extension. We define

$$\phi_{L/K}(a) := \prod_v \phi_v(a_v) \in \text{Gal}(L/K).$$

This is well-defined since for a_v in U_v and L_w/K_v unramified we have $\phi_v(a_v) = 1$ and we see that in the above product, almost all terms are equal to 1. Such a morphism is the unique one making the diagram from the statement commute.

We want to show that ϕ_K is continuous. From local reciprocity law, we see that if $L/K'/K$ is an intermediate extension, then there is a commutative diagram:

$$\begin{array}{ccc} \mathbb{I}_{K'} & \longrightarrow & \text{Gal}(L/K') \\ \text{Nm}_{K'/K} \downarrow & & \downarrow \\ \mathbb{I}_K & \longrightarrow & \text{Gal}(L/K). \end{array}$$

Taking $K' = L$, we obtain that $\text{Nm}_{L/K}(\mathbb{I}_L)$ is contained in $\text{Ker}(\phi_{L/K})$. It follows from Proposition 4.9 that $\text{Ker}(\phi_{L/K})$ contains an open subgroup of $\mathbb{I}_K$. This proves that $\phi_{L/K}$ is continuous. $\square$

Note that we have seen in the above proof that $\phi_{L/K}(\text{Nm}_{L/K}(\mathbb{I}_L))$ is trivial. More precisely, we have:

Lemma 4.15. *Let L/K be a finite abelian extension of number fields. Then $\phi_{L/K}$ is surjective and $\text{Nm}_{L/K}(\mathbb{I}_L) \subset \text{Ker}(\phi_{L/K})$.*

Proof. We only have to check the surjectivity, but it follows from the surjectivity of the local Artin maps and the fact that $\text{Gal}(L/K)$ is generated by the Frobenius elements of the subgroups $\text{Gal}(L_w/K_v)$. $\square$

Remark 4.16. If K is a function field, the Artin map is not surjective but injective.

We can now reformulate the reciprocity law and the existence theorem using the group of idèles:

Theorem 4.17 (Reciprocity law). *The Artin map $\phi_K : \mathbb{I}_K \rightarrow \text{Gal}(K^{\text{ab}}/K)$ satisfies the following properties:*

- (1) $\phi_K(K^\times) = 1$,
- (2) for any L/K finite abelian then ϕ_K induces an isomorphism

$$\phi_{L/K} : \mathbb{I}_K / K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L) \xrightarrow{\sim} \text{Gal}(L/K).$$

In other words, we have isomorphisms:

$$\phi_{L/K} : \mathbb{C}_K / \text{Nm}_{L/K}(\mathbb{C}_L) \xrightarrow{\sim} \text{Gal}(L/K).$$

Theorem 4.18 (Existence theorem). *Let $H \subset \mathbb{C}_K$ be an open subgroup of finite index. Then there exists a unique abelian extension L of K such that $\text{Nm}_{L/K}(\mathbb{C}_L) = H$.*

Theorems 4.17 and 4.18 have the following consequences:

Proposition 4.19. *There is a bijection:*

$$\begin{aligned} \{L/K \text{ finite abelian extension}\} &\xrightarrow{\sim} \{H \subset \mathbb{C}_K \text{ open subgroup of finite index}\} \\ L &\mapsto \text{Nm}_{L/K}(\mathbb{C}_L) \end{aligned}$$

and we have

- (1) $L_1 \subset L_2$ if and only if $\text{Nm}_{L_1/K}(\mathbb{C}_{L_1}) \supset \text{Nm}_{L_2/K}(\mathbb{C}_{L_2})$,
- (2) $\text{Nm}_{L_1 \cdot L_2/K}(\mathbb{C}_{L_1 \cdot L_2}) = \text{Nm}_{L_1/K}(\mathbb{C}_{L_1}) \cap \text{Nm}_{L_2/K}(\mathbb{C}_{L_2})$,
- (3) $\text{Nm}_{L_1 \cap L_2/K}(\mathbb{C}_{L_1 \cap L_2}) = \text{Nm}_{L_1/K}(\mathbb{C}_{L_1}) \cdot \text{Nm}_{L_2/K}(\mathbb{C}_{L_2})$.

5 The cohomology of the idèles

In this section we compute the cohomology of the groups $\mathbb{I}_K$ and $\mathbb{C}_K$. This will be used to prove the so-called "first inequality", namely, for any cyclic extension L/K of number fields, we have

$$[L : K] \leq [\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)].$$

Before computing those cohomology groups, we recall some results about Galois cohomology of local fields and explain briefly our main strategy to prove the global reciprocity law and existence theorem.

5.1 Cohomology of local fields

5.1.1 Tate's theorem and main ideas of the proof

Let G be a finite group and M a G -module. Recall that the Tate cohomology groups of M are defined as

$$\hat{H}^i(G, M) = \begin{cases} H^i(G, M), & \text{if } i > 0 \\ M^G / N_G(M) & \text{if } i = 0 \\ \text{Ker}(N_G) / I_G(M) & \text{if } i = -1 \\ H_{-i-1}(G, M) & \text{if } i < -1, \end{cases}$$

where $N_G : M \rightarrow M$ is the norm map $m \mapsto \sum_{g \in G} g \cdot m$ and $I_G(M)$ is the kernel of the augmentation map $\varepsilon : \mathbf{Z}[G] \rightarrow \mathbf{Z}$, $\sum_{g \in G} n_g g \mapsto \sum_{g \in G} n_g$.

If moreover G is cyclic with generator γ , then

$$\begin{aligned} \hat{H}^0(G, M) &= \text{Ker}(\gamma - 1) / \text{Im}(N_G) \\ \hat{H}^{-1}(G, M) &= \text{Ker}(N_G) / \text{Im}(\gamma - 1) \\ \hat{H}^i(G, M) &\simeq \hat{H}^{i+2}(G, M) \text{ for all } i \in \mathbf{Z}. \end{aligned}$$

Let us also recall Tate's theorem:

Theorem 5.1. *Let G be a finite group and M a G -module. Suppose for all subgroup $H \subset G$ (including $H = G$), the group $H^1(H, M)$ is trivial and $H^2(H, M)$ is cyclic of order $|H|$. Let γ be a generator of $H^2(G, M)$. Then there exists an isomorphism for all $i \in \mathbf{Z}$,*

$$\Phi_\gamma : \hat{H}^i(G, \mathbf{Z}) \xrightarrow{\sim} \hat{H}^{i+2}(G, M)$$

uniquely determined by the choice of γ . Moreover, for any $H \subset G$, we have commutative diagrams:

$$\begin{array}{ccc} \hat{H}^i(G, \mathbf{Z}) & \xrightarrow{\Phi_\gamma} & \hat{H}^{i+2}(G, M) \\ \downarrow \text{Res} & & \downarrow \text{Res} \\ \hat{H}^i(H, \mathbf{Z}) & \xrightarrow{\Phi_{\text{Res}(\gamma)}} & \hat{H}^{i+2}(H, M) \end{array} \quad \text{and} \quad \begin{array}{ccc} \hat{H}^i(G, \mathbf{Z}) & \xrightarrow{\Phi_\gamma} & \hat{H}^{i+2}(G, M) \\ \uparrow \text{CoRes} & & \uparrow \text{CoRes} \\ \hat{H}^i(H, \mathbf{Z}) & \xrightarrow{\Phi_{\text{Res}(\gamma)}} & \hat{H}^{i+2}(H, M) \end{array}$$

Let L/K be finite abelian and $G = \text{Gal}(L/K)$. Suppose that we can prove that the G -module $\mathbb{C}_L$ satisfies the hypothesis of Tate's theorem. Then, it gives an isomorphism (for a fixed generator γ of $H^2(G, \mathbb{C}_L)$):

$$\hat{H}^{-2}(G, \mathbf{Z}) \xrightarrow{\sim} \hat{H}^0(G, \mathbb{C}_L).$$

The group on the left is equal to $H_1(G, \mathbf{Z}) \simeq \text{Hom}_{\mathbf{Z}}(\mathbf{Z}, G^{\text{ab}}) \simeq G$ and the one on the right is $\mathbb{C}_K / \text{Nm}_{L/K}(\mathbb{C}_L)$ and our Artin map is in fact the inverse of this isomorphism. Hence, our goal

is to check that the first and second cohomology groups of the G -module $\mathbb{C}_L$ satisfy the right properties to apply Tate's theorem. We will in fact prove slightly weaker results and we will see this is enough for our purposes.

5.1.2 Herbrand quotients

For G a finite cyclic group and M a G -module, if $\widehat{H}^i(G, M)$ is finite, the Herbrand quotient of M is defined as:

$$h(M) := \frac{|\widehat{H}^0(G, M)|}{|\widehat{H}^1(G, M)|}$$

It satisfies the following properties:

Proposition 5.2. *Let G be a finite cyclic group.*

(1) *Let $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ be an exact sequence of G -modules. If two of $h(M')$, $h(M)$, $h(M'')$ are defined then the third one is defined as well and $h(M) = h(M')h(M'')$.*

(2) *If M is a finite G -module then $h(M) = 1$.*

(3) *Let $\alpha : M \rightarrow N$ be a morphism of G -modules such that α has finite kernel and cokernel. Then if $h(M)$ or $h(N)$ is defined, the other one is also defined and $h(M) = h(N)$.*

Proof. Exercise. □

In the following we recall a few lemmas about Galois cohomology of local fields that will be useful to compute the cohomology of the idèles. In the rest of this sub-section, please note that K is now a local field.

Lemma 5.3. *Let K be a local field and L a finite Galois extension of K . Then there exists an open subgroup U of $\mathcal{O}_L$ stable for the action of the Galois group $\text{Gal}(L/K)$ and such that $H^i(G, U)$ is trivial for all $i > 0$.*

Proof. Choose e in L such that $\{\sigma(e) \mid \sigma \in \text{Gal}(L/K)\}$ is a K -basis for L . Up to multiplying by some elements d in $\mathcal{O}_K$, we can assume all the $\sigma(e)$'s are in $\mathcal{O}_L$. Take $U := \sum_{\sigma \in \text{Gal}(L/K)} \mathcal{O}_K \sigma(e)$. Then U is stable by the action of G and for a uniformiser π of $\mathcal{O}_L$ there exists m such that π^m is in U , i.e. $\pi^m \mathcal{O}_L \subset U$. Hence U is open. As G -representations, we have $U \simeq \mathcal{O}_K[G] \simeq \text{Ind}_1^G \mathcal{O}_K$ and it follows that U has trivial cohomology in positive degrees. □

Lemma 5.4. *Let K be a finite extension of $\mathbb{Q}_p$ and L be a finite Galois extension of K . Then there exists an open subgroup V of $\mathcal{O}_L^\times$ stable for the action of the Galois group $G := \text{Gal}(L/K)$ and such that $H^i(G, V)$ is trivial for all $i > 0$.*

The above lemma is also true when K is a local field of positive characteristic (exercise).

Proof. Recall that the p -adic exponential map $\exp : x \mapsto \sum_{i \geq 0} \frac{x^i}{i!}$ defines an isomorphism from an open neighborhood of 0 in L onto an open neighborhood of 1 in $L^\times$ with inverse given by the logarithm $\log : x \mapsto \sum_{i \geq 1} (-1)^{i+1} \frac{(x-1)^i}{i}$. Note that both maps commute with the action of G . Consider U the open neighborhood of 0 given by Lemma 5.3. If π is a uniformiser of $\mathcal{O}_L$, then there exists m such that the exponential is well-defined on $\pi^m U$ and we can take $V := \exp(\pi^m U)$. $\square$

Proposition 5.5. *Let K be a local field and L a cyclic extension of K . Then $h(\mathcal{O}_L^\times) = 1$ and $h(L^\times) = [L : K]$.*

Proof. Consider the open V given by Lemma 5.4. Since $\mathcal{O}_L^\times$ is compact then $\mathcal{O}_L^\times/V$ is finite and by Proposition 5.2(3), we obtain $h(\mathcal{O}_L^\times) = h(V)$. But the choice of V gives $h(V) = 1$ and so $h(\mathcal{O}_L^\times) = 1$.

For $L^\times$, recall that we can write $L^\times = \mathcal{O}_L^\times \cdot \pi^{\mathbf{Z}} \simeq \mathcal{O}_L^\times \times \mathbf{Z}$. In particular, $h(L^\times) = h(\mathcal{O}_L^\times) \cdot h(\mathbf{Z}) = h(\mathbf{Z})$. But if $n = [L : K]$, we have

$$h(\mathbf{Z}) = \frac{|\widehat{H}^0(G, \mathbf{Z})|}{|\widehat{H}^1(G, \mathbf{Z})|} = |\widehat{H}^0(G, \mathbf{Z})| = |\mathbf{Z}/n\mathbf{Z}| = n.$$

$\square$

If V is a finite dimensional $\mathbf{R}$ - (respectively $\mathbf{Q}$ -) vector space and $M \subset V$ a subgroup, we say that M is a full lattice of V if M is finitely generated over $\mathbf{Z}$ and $\mathbf{R} \otimes_{\mathbf{Z}} M \rightarrow V$ (respectively $\mathbf{Q} \otimes_{\mathbf{Z}} M \rightarrow V$) is an isomorphism. In other words, M is the $\mathbf{Z}$ -submodule of V generated by an $\mathbf{R}$ - or $\mathbf{Q}$ -basis of V .

Proposition 5.6. *Let G be a finite cyclic group and M, N two G -modules that are finitely generated as $\mathbf{Z}$ -modules. Assume moreover that $M \otimes_{\mathbf{Z}} \mathbf{Q}$ and $N \otimes_{\mathbf{Z}} \mathbf{Q}$ are isomorphic as G -modules. Then if $h(M)$ or $h(N)$ is defined then the other also is and $h(M) = h(N)$.*

Proof. Let $M_{\text{tors}} \subset M$ be the torsion subgroup. Since M is finitely generated over $\mathbf{Z}$, the group M_{tors} is finite. Applying Proposition 5.2(3) to the map $M \rightarrow M/M_{\text{tors}}$, we see that $h(M) = h(M/M_{\text{tors}})$ (and same for N). In particular, we can assume that M and N are torsion-free.

Let us write α the isomorphism $M \otimes_{\mathbf{Z}} \mathbf{Q} \xrightarrow{\sim} N \otimes_{\mathbf{Z}} \mathbf{Q}$. Then there exists d such that $\alpha(M) \subset d^{-1}N$ (write the elements of the basis of $\alpha(M)$ in the basis of N and take d a common denominator of the coefficients). Up to replacing α by $d\alpha$ we can then assume $\alpha(M) \subset N$. We obtain an exact sequence

$$0 \rightarrow M \xrightarrow{\alpha} N \rightarrow N/\alpha(M) \rightarrow 0$$

with $N/\alpha(M)$ finite. Since $\alpha(M)$ and N have same rank as lattices of $\mathbf{Q}$ (they have full rank) then $N/\alpha(M)$ is finite. By Proposition 5.2(3) we obtain $h(M) = h(N)$. $\square$

Corollary 5.7. *Let G be a finite cyclic group and let V be an $\mathbf{R}$ -vector space with a linear action of G . Let M and N be two G -stable full lattices in V . Then if $h(M)$ or $h(N)$ is defined, the other is also defined and $h(M) = h(N)$.*

Proof. By definition, we have $\mathbf{R}$ -isomorphisms:

$$M \otimes_{\mathbf{Z}} \mathbf{R} \xrightarrow{\sim} V \xleftarrow{\sim} N \otimes_{\mathbf{Z}} \mathbf{R}.$$

But since the lattices are G -stable, the above isomorphism is an isomorphism of $\mathbf{R}[G]$ -modules. To apply Proposition 5.6, we need to check that this is also an isomorphism of $\mathbf{Q}[G]$ -modules $M \otimes_{\mathbf{Z}} \mathbf{Q} \simeq N \otimes_{\mathbf{Z}} \mathbf{Q}$. But this follows from the following general lemma:

Lemma 5.8. *Let G be a finite group and $K_1 \subset K_2$ an extension of (any) infinite fields. Let M and N be $K_1[G]$ -modules of finite K_1 -dimension. Then if $M \otimes_{K_1} K_2$ and $N \otimes_{K_1} K_2$ are isomorphic as $K_2[G]$ -modules, then they are isomorphic as $K_1[G]$ -modules.*

Proof. We claim that we can find $K_1[G]$ -morphisms $f_1, \dots, f_n$ from M to N such that $\{f_1, \dots, f_n\}$ forms a K_2 -basis for the space $\text{Hom}_{K_2[G]}(M \otimes_{K_1} K_2, N \otimes_{K_1} K_2)$. Indeed, if we choose K_1 -basis for M and N , then for all g in G , there exist K_1 -matrices $A_1(g)$ and $A_2(g)$ such that G -equivariant K_1 -morphisms $f : M \rightarrow N$ correspond to K -matrices P such that $PA_1(g) = A_2(g)P$. But $K_2[G]$ -morphisms from $M \otimes_{K_1} K_2$ to $N \otimes_{K_1} K_2$ satisfy the same equations (for the same $A_1(g)$ and $A_2(g)$). Hence, the basis we find for the $K_1[G]$ -morphisms $M \rightarrow N$ also defines a basis for the $K_2[G]$ -morphisms $M \otimes_{K_1} K_2 \rightarrow N \otimes_{K_1} K_2$.

Any $K_2[G]$ -isomorphism between $M \otimes_{K_1} K_2$ and $N \otimes_{K_1} K_2$ can be written as $\sum_{i=1}^n \lambda_i f_i$ with λ_i in K_2 . Consider $\det(\sum_{i=1}^n \lambda_i f_i)$: this is a non-zero polynomial in the λ_i 's with coefficients in K_1 . Let us write $P(\lambda_1, \dots, \lambda_n) \in K_1[\lambda_1, \dots, \lambda_n]$ this polynomial. Since it is non-zero and K_1 is infinite, this means that we can find $(\mu_1, \dots, \mu_n)$ in K_1^n such that $P(\mu_1, \dots, \mu_n)$ is non-zero. In particular, $\sum_{i=1}^n \mu_i f_i$ defines a $K_1[G]$ -isomorphism between M and N , as wanted. $\square$

$\square$

5.2 The first inequality

Recall that in order to apply Tate's theorem, we would need to prove that for L/K a finite abelian extension, $H^1(G, \mathbb{C}_L)$ is trivial and $H^2(G, \mathbb{C}_L)$ has order $[L : K]$. In particular, this would imply $h(\mathbb{C}_L) = [L : K]$. We will not prove this in general but the first step in our proof of Reciprocity law will be to check that if L/K is cyclic we indeed have $h(\mathbb{C}_L) = [L : K]$. It will follow that for L/K a cyclic extension of number fields, then

$$[L : K] \leq [\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)].$$

5.2.1 Preliminaries

Let L/K be a finite Galois extension of number fields, v a prime of K . We write G for the Galois group of L/K . We can extend the action of G on L to $\prod_{w|v} L_w$. Namely, let us first recall the isomorphism:

$$(5.2.1) \quad L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$$

obtained by sending $x \otimes y$ to $(\iota_w(x)y)_w$, where ι_w is the embedding $L \hookrightarrow L_w$. Since G acts on L , it acts on $L \otimes_K K_v$ and we obtain an action of G on $\prod_{w|v} L_w$ via the above isomorphism. Note that this action is continuous for the product topology on $\prod_{w|v} L_w$ and that it fixes the elements of the form $(x, \dots, x)$ with $x \in K_v$. For $(y_w)_w$ in $\prod_{w|v} L_w$, if $y_w = \iota_w(x)$ with x in L , then the w -term of $g((y_w)_w)$ is given by $\iota_w(g \cdot x)$. More generally we have:

Lemma 5.9. *For g in G and $y = (y_w)_w$ in $\prod_{w|v} L_w$, then $(g(y))_w = g \cdot y_{g^{-1}(w)}$.*

Proof. The action on the right is clearly continuous. Using the isomorphism (5.2.1), it suffices to check the two actions coincide on the elements of the form $(x, x, \dots, x)$ with x in K_v and on the ones of the form $(\iota_w(x))_w$ with $x \in L$.

If x is in K_v and $y_w = x$ for all $w|v$, then $g \cdot y_{g^{-1}(w)} = x = (g(y))_w$. If $y_w = \iota_w(x)$ with x in L for all $w|v$, then $g \cdot y_{g^{-1}(w)} = g \cdot (\iota_{g^{-1}(w)}(x))$. But we have a commutative diagram:

$$\begin{array}{ccc} L_w & \xrightarrow{g^{-1}} & L_{g^{-1}(w)} \\ \uparrow \iota_w & & \uparrow \iota_{g^{-1}(w)} \\ L & \xrightarrow{g^{-1}} & L \end{array}$$

and we obtain $g \cdot (\iota_{g^{-1}(w)}(x)) = \iota_w(g \cdot x)$, as wanted. $\square$

The action of G on $\prod_{w|v} L_w$ induces an action of G on $\prod_{w|v} L_w^\times$ and $\prod_{w|v} \mathcal{O}_{L_w}^\times$. Our goal now is to compute the cohomology groups $H^i(G, \prod_{w|v} L_w^\times)$. We have:

Proposition 5.10. *Let L/K be an extension of number fields with Galois group G , let v be a place of K and w_0 a place of L lying above v . Let us denote by $G_{w_0} \subset G$ the decomposition subgroup of w_0 . Then for all i ,*

$$\begin{aligned} H^i(G, \prod_{w|v} L_w^\times) &\simeq H^i(G_{w_0}, L_{w_0}^\times), \quad \text{in particular } H^0(G, \prod_{w|v} L_w^\times) \simeq K_v^\times \\ H^i(G, \prod_{w|v} \mathcal{O}_{L,w}^\times) &\simeq H^i(G_{w_0}, \mathcal{O}_{L,w_0}^\times), \quad \text{in particular } H^0(G, \prod_{w|v} \mathcal{O}_w^\times) \simeq \mathcal{O}_{K,v}^\times. \end{aligned}$$

Proof. Recall Shapiro's lemma:

Lemma 5.11. *For H a subgroup of a group G and N an H -module, for all $i \geq 0$, there is a natural isomorphism*

$$H^i(G, \text{Ind}_H^G(N)) \xrightarrow{\sim} H^i(H, N)$$

where $\text{Ind}_H^G(N) = \{f : G \rightarrow N \mid f(hg) = hf(g) \text{ for all } g \in G \text{ and } h \in H\}$.

The statement of the proposition follows then from Shapiro's lemma and the following result:

Lemma 5.12. *There is an isomorphism of G -modules:*

$$\begin{cases} \prod_{w|v} L_w & \xrightarrow{\sim} \text{Ind}_{G_{w_0}}^G(L_{w_0}) \\ x & \mapsto f_x \end{cases}$$

where for all g in G , we define $f_x(g) := g \cdot x_{g^{-1} \cdot w_0} \in L_{w_0}$. Similarly, there are isomorphisms:

$$\prod_{w|v} L_w^\times \xrightarrow{\sim} \text{Ind}_{G_{w_0}}^G(L_{w_0}^\times) \quad \text{and} \quad \prod_{w|v} \mathcal{O}_{L,w}^\times \xrightarrow{\sim} \text{Ind}_{G_{w_0}}^G(\mathcal{O}_{L,w_0}^\times)$$

Proof. Let us first check that f_x is indeed in $\text{Ind}_{G_{w_0}}^G(L_{w_0})$. Take h in G_{w_0} and g in G . Then, since h is in the stabilizer of w_0 ,

$$f_x(hg) = (hg) \cdot x_{(hg)^{-1} \cdot w_0} = h \cdot g \cdot x_{g^{-1} \cdot w_0} = h \cdot f_x(g),$$

as wanted. We obtain that $x \mapsto f_x$ is a morphism of G -modules $\prod_{w|v} L_w \rightarrow \text{Ind}_{G_{w_0}}^G(L_{w_0})$. Let us construct an inverse. Starting from f in $\text{Ind}_{G_{w_0}}^G(L_{w_0})$, we define $x(f) := (x(f)_w)_{w|v} \in \prod_{w|v} L_w$ as

$$x(f)_w := g \cdot f(g^{-1}) \text{ for } w = g \cdot w_0.$$

We can easily check that $f \mapsto x_f$ and $x \mapsto f_x$ are inverse of one another. □

□

For L , K , v and w_0 as in the proposition, note that if w_1 is another place of L lying above v , then we can write $w_1 = g \cdot w_0$ for some g in G and we have isomorphisms

$$\begin{cases} G_{w_0} & \xrightarrow{\sim} G_{w_1} \\ h & \mapsto ghg^{-1} \end{cases} \quad \text{and} \quad \begin{cases} L_{w_1} & \xrightarrow{\sim} L_{w_0} \\ x & \mapsto g^{-1} \cdot x \end{cases}$$

This yields isomorphisms, for all $i \geq 0$,

$$\alpha_{i,g} : H^i(G_{w_1}, L_{w_1}^\times) \xrightarrow{\sim} H^i(G_{w_0}, L_{w_0}^\times).$$

Now if h is an element of G_{w_0} and we set $g' := gh$, we obtain a commutative diagram:

$$\begin{array}{ccc} H^i(G_{w_1}, L_{w_1}^\times) & \xrightarrow[\sim]{\alpha_{i,g}} & H^i(G_{w_0}, L_{w_0}^\times) \\ & \searrow \alpha_{i,g'} & \downarrow \beta_{i,h} \\ & & H^i(G_{w_0}, L_{w_0}^\times) \end{array}$$

where $\beta_{i,h}$ is the isomorphism induced by the isomorphisms $\sigma \mapsto h\sigma h^{-1}$ from G_{w_0} to itself and $x \mapsto h^{-1}x$ from L_{w_0} to itself. It can be checked (exercise) that $\beta_{i,h}$ is in fact the identity map. Therefore, $H^i(G_{w_0}, L_{w_0}^\times)$ does not depend on the choice of w_0 and we set

$$H^i(G^v, L^v) := H^i(G_{w_0}, L_{w_0}), \quad H^i(G^v, L^{v,\times}) := H^i(G_{w_0}, L_{w_0}^\times) \quad \text{and} \quad H^i(G^v, U^v) := H^i(G_{w_0}, U_{w_0}).$$

5.2.2 Galois cohomology of the idèles

Let us now come back to the computation of the cohomology of idèles. For L/K a Galois extension of number field with Galois group G and v a place of K , we endow the group of idèles with the action of G such that for all places v of K , the injective maps $\prod_{w|v} L_w^\times \hookrightarrow \mathbb{I}_L$ are G -equivariant. Concretely, if $a = (a_w)_w$ is in $\mathbb{I}_L$ then $(g \cdot a)_w = g \cdot a_{g^{-1}(w)}$.

Proposition 5.13. *Let L/K be a Galois extension of number fields with Galois group G . Then, for $i > 0$,*

$$H^i(G, \mathbb{I}_L) = \bigoplus_v H^i(G^v, L^{v,\times}).$$

Proof. If S is a finite set of primes of K , by abuse of notation, we will write $\mathbb{I}_{L,S}$ for the group

$$\mathbb{I}_{L,S} := \prod_{v \in S} \left(\prod_{w|v} L_w^\times \right) \times \prod_{v \notin S} \left(\prod_{w|v} U_w \right).$$

The $\mathbb{I}_{L,S}$ groups are stable under the action of the Galois group G . We also have

$$\mathbb{I}_L \simeq \text{colim}_S \mathbb{I}_{L,S},$$

where the limit is taken over the finite set of places S such that S contains all infinite places and all primes that ramify in S . In particular, we have

$$H^i(G, \mathbb{I}_L) = \text{colim}_S H^i(G, \mathbb{I}_{L,S}).$$

Since the cohomology commutes with infinite product, we obtain (using Proposition 5.10 to get the second equality):

$$\begin{aligned} H^i(G, \mathbb{I}_{L,S}) &= \left(\prod_{v \in S} H^i(G, \prod_{w|v} L_w^\times) \right) \times \left(\prod_{v \notin S} H^i(G, \prod_{w|v} U_w) \right) \\ &= \left(\prod_{v \in S} H^i(G^v, L^{v,\times}) \right) \times \left(\prod_{v \notin S} H^i(G^v, U^v) \right). \end{aligned}$$

Since we have assumed that S contains all primes that ramify in L , we have that for v not in S and w above v , the extension L_w/K_v is unramified and it follows that the cohomology groups $H^i(G^v, U^v) = H^i(G_w, U_w)$ are trivial in degree $i > 0$. Finally, using that S is finite, we get

$$\begin{aligned} H^i(G, \mathbb{I}_L) &= \operatorname{colim}_S \bigoplus_{v \in S} H^i(G^v, L^{v, \times}) \\ &= \bigoplus_{\text{all places } v} H^i(G^v, L^{v, \times}). \end{aligned}$$

□

Corollary 5.14. *Let L/K be a Galois extension of number fields with Galois group G . Then,*

$$\begin{aligned} H^0(G, \mathbb{I}_L) &= \mathbb{I}_K \\ H^1(G, \mathbb{I}_L) &= 0 \\ H^2(G, \mathbb{I}_L) &\simeq \bigoplus_v \left(\frac{1}{n_v} \mathbf{Z} \right) / \mathbf{Z}, \end{aligned}$$

where $n_v := [L_w : K_v]$ for any w place of L dividing v .

Proof. Let us first compute the G -fixed elements of $\mathbb{I}_L$. If $a = (a_w)_w$ is fixed by G then for any place v of K , the subfamily $(a_w)_{w|v}$ is fixed by G . This means that each a_w with w dividing v depends only of v and is in $K_v^\times$. So a comes from an element of $\mathbb{I}_K$ via the natural embedding $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$. We obtain $H^0(G, \mathbb{I}_L) = \mathbb{I}_K$.

The result for $H^1(G, \mathbb{I}_L) = 0$ immediately follows from Proposition 5.13 and Hilbert's theorem 90. For $H^2(G, \mathbb{I}_L)$, it follows from Proposition 5.13 and the computation of the Brauer groups $H^2(G_w, L_w^\times) \simeq (\frac{1}{n_v} \mathbf{Z}) / \mathbf{Z}$, for any w above v . □

Using the computation done in the proof of Proposition 5.13, we can also compute Herbrand quotients of the subrings $\mathbb{I}_{L,S}$ of cyclic extension:

Proposition 5.15. *Let L/K be a finite extension of number fields and set $G := \operatorname{Gal}(L/K)$. Let S be a finite set of primes of K and T be the set of primes of L dividing the primes in S . If L/K is cyclic then*

$$h(\mathbb{I}_{L,T}) = \prod_{v \in S} n_v,$$

where $n_v := [L_w : K_v]$ for any w place of L dividing v .

Proof. We only need to compute H^1 and H^2 . By definition, we have

$$\mathbb{I}_{L,T} = \left(\prod_{v \in S} \prod_{w|v} L_w^\times \right) \times \left(\prod_{v \notin S} \prod_{w|v} U_w \right).$$

Each one of the two factors is stable under the action of G and the Herbrand quotient of $\mathbb{I}_{L,T}$ is the product of the Herbrand quotients of the factors. But we have

$$H^i(G, \prod_{v \in S} \prod_{w|v} L_w^\times) = \prod_{v \in S} H^i(G, \prod_{w|v} L_w^\times) = \prod_{v \in S} H^i(G_{w_v}, L_{w_v}^\times),$$

for any w_v place of L dividing v (we have used Proposition 5.10) and we deduce that

$$h(\prod_{v \in S} \prod_{w|v} L_w^\times) = \prod_{v \in S} h(L_{w_v}^\times).$$

The latter terms were computed in Proposition 5.5, we have $h(L_{w_v}^\times) = n_v$. Similarly, we have

$$H^i(G, \prod_{v \notin S} \prod_{w|v} U_w) = \prod_{v \notin S} H^i(G_{w_v}, U_{w_v}),$$

for any w_v place of L dividing v . We can then decompose the product as

$$\prod_{v \notin S} H^i(G_{w_v}, U_{w_v}) = \left(\prod_{v \notin S \text{ s.t. } v \text{ ramified}} H^i(G_{w_v}, U_{w_v}) \right) \times \left(\prod_{v \notin S \text{ s.t. } v \text{ unramified}} H^i(G_{w_v}, U_{w_v}) \right)$$

where the first product is finite. The cohomology groups in the second factor are all trivial for $i > 0$, hence the Herbrand quotient of $\prod_{v \notin S \text{ s.t. } v \text{ unramified}} U_{w_v}$ is 1. As for the first factor, we have seen in Proposition 5.5, that the Herbrand quotient of each term is also 1 and we take of finite product of them. It follows that $h(\prod_{v \notin S} \prod_{w|v} U_w)$ is 1. $\square$

5.2.3 Galois cohomology of the units

Let us now compute the Herbrand quotient of the units groups. Let L be a finite extension of K with Galois group G . For S a finite set of primes of K , if T is the set of primes of L dividing the primes in S then we define:

$$U(T) := \{x \in L \mid \text{ord}_w(x) = 0 \text{ for all } w \notin T\}.$$

Note that $U(T)$ is stable for the action of G (since T itself is).

Proposition 5.16. *Let L/K be a finite cyclic extension of number fields, with Galois group G . For S a finite set of primes that contains S_∞ and for T as before, the Herbrand quotient of $U(T)$ is well defined and satisfies the following:*

$$[L : K] \cdot h(U(T)) = \prod_{v \in S} n_v,$$

where $n_v := [L_w : K_v]$ for any w place of L dividing v .

Proof. Consider the $\mathbf{R}$ -vector space $V := \text{Maps}(T, \mathbf{R})$ and we endow it with the action of G given by:

$$(5.2.2) \quad (g \cdot f)(w) = f(g^{-1} \cdot w), \quad \text{for all } g \in G \text{ and } w \in T.$$

The idea is to construct two G -stable full lattices of V , one with Herbrand quotient $[L : K] \cdot h(U(T))$ and the other one with Herbrand quotient $\prod_{v \in S} n_v$ and then use Corollary 5.7.

We start by constructing the second lattice. Let $N := \text{Maps}(T, \mathbf{Z})$ endowed with G -action defined via the same formula as in (5.2.2). For any $v \in S$, choose $w(v)$ a prime in T dividing it. Then we can decompose N as the sum $\bigoplus_{v \in S} \text{Maps}(G/G_{w(v)}, \mathbf{Z})$ (a map $f : T \rightarrow \mathbf{Z}$ corresponds to the family of maps $\{f_v : G/G_{w(v)} \rightarrow \mathbf{Z}\}_{v \in S}$ where $f_v(gG_{w(v)}) = f(g \cdot w(v))$ for $g \in G$). Seeing $\mathbf{Z}$ as a trivial $G_{w(v)}$ -module, we have $\text{Maps}(G/G_{w(v)}, \mathbf{Z}) = \text{Ind}_{G_{w(v)}}^G(\mathbf{Z})$. We obtain

$$h(N) = \prod_{v \in S} h(\text{Ind}_{G_{w(v)}}^G(\mathbf{Z})).$$

The Herbrand quotients above are Herbrand quotients for G -modules. But then, by Shapiro's lemma, we have (the first Herbrand quotient is for G -modules and the second one for $G_{w(v)}$ -modules):

$$h_G(\text{Ind}_{G_{w(v)}}^G(\mathbf{Z})) = h_{G_{w(v)}}(\mathbf{Z}) = [L_{w(v)} : K_v] = n_v.$$

We obtain $h(N) = \prod_{v \in S} n_v$.

Let us now define the first lattice M . Consider the map

$$\lambda : \begin{cases} U(T) & \rightarrow V \\ x & \mapsto (w \mapsto \log|x|_w) \end{cases}.$$

This is a G -equivariant map, let us denote by M^0 its image and set $M := M^0 + \mathbf{Z} \cdot e$ where $e := (1, 1, \dots, 1) \in V$ (note that e is fixed by the elements of G). We need to show that M is a lattice in V and compute its Herbrand quotient. This follows from the claim :

Lemma 5.17. M^0 is a lattice of the $\mathbf{R}$ -vector space $V^0 := \{f \in V \mid \sum_{w \in T} f(w) = 0\}$ and $h(M^0) = h(U(T))$.

Proof. The kernel of λ is equal to the set of elements x in $L^\times$ such that $|x|_w = 1$ for all places w of L , and it can be proved that this corresponds exactly to the group μ of root of 1 in L (see Exercise sheet 3). But μ is finite so by Proposition 5.2(2), we obtain $h(U(T)) = h(M^0)$. This proves the second statement of the lemma.

To check that M^0 is a lattice in V^0 , first note that by the product formula, M^0 is contained in V^0 . Then recall that a subgroup of a real vector space is a lattice if and only if it is discrete. Consider $B = \{(x_w)_{w \in T} \in V^0 \mid |x_w| \leq M\}$ for some $M > 0$. Then $B \cap M^0$ is equal to the set of x in $U(T)$ such that $|x|_w \leq \exp(M)$. But there are only finitely many such x (exercise). It follows that M^0 is a lattice. $\square$

Since $M \otimes_{\mathbf{Z}} \mathbf{R} = V^0 + \mathbf{R} \cdot e = V$, we obtain that M is a full lattice in V and we have $h(M) = h(M^0) \cdot h(\mathbf{Z}) = h(M^0) = h(U(T))$ (recall $h(\mathbf{Z}) = 1$, see proof of Proposition 5.5). $\square$

5.2.4 The first inequality

The goal of this section is to prove:

Theorem 5.18 (First inequality). *Let L/K be a finite cyclic extension. Then*

- (1) $h(\mathbb{C}_L) = [L : K]$ and,
- (2) $[\mathbb{I}_K : K^\times \cdot \text{Norm}_{L/K}(\mathbb{I}_L)] \geq [L : K]$.

In order to prove the theorem, we will need the following lemmas.

Lemma 5.19. *Let L/K be a finite extension of number fields with Galois group G . Then the map $\mathbb{C}_K \rightarrow \mathbb{C}_L$ induces an isomorphism $\mathbb{C}_K \xrightarrow{\sim} \mathbb{C}_L^G$.*

Proof. We have a map of short exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathbb{C}_K \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathbb{C}_L \longrightarrow 0 \end{array}$$

After taking cohomology and using Hilbert's theorem 90, we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathbb{C}_K \longrightarrow 0 \\ & & \downarrow \sim & & \downarrow \sim & & \downarrow \\ 0 & \longrightarrow & (L^\times)^G & \longrightarrow & (\mathbb{I}_L)^G & \longrightarrow & \mathbb{C}_L^G \longrightarrow 0 \end{array}$$

where the second vertical map is an isomorphism by Corollary 5.14. It follows that the map $\mathbb{C}_K \rightarrow \mathbb{C}_L^G$ is an isomorphism. $\square$

Consider L/K a cyclic extension with Galois group G . Then it follows from Lemma 5.19 that we have

$$\widehat{H}^0(G, \mathbb{C}_L) = \mathbb{C}_L^G / N_G(\mathbb{C}_L) \simeq \mathbb{C}_K / \text{Nm}_{L/K}(\mathbb{C}_L)$$

and we obtain

$$(5.2.3) \quad h(\mathbb{C}_L) = \frac{[\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)]}{|H^1(G, \mathbb{C}_L)|}.$$

Lemma 5.20. *Let K be a number field and let S be a finite set of places such that S contains the set of infinite places S_∞ of K and a set of generators for the ideal class group C_K of K . Then, the group of idèles can be decomposed in the following way:*

$$\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}.$$

Proof. Since S contains S_∞ , the map $\mathbb{I}_K \rightarrow I_K^S$ sending (a_v) to $\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$ induces an isomorphism $\mathbb{I}_K / \mathbb{I}_{K,S} \xrightarrow{\sim} I_K^S$. We have a commutative diagram:

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & I_K^S \\ \uparrow & & & \nearrow & \\ K^S & & & & \end{array}$$

so in order to prove the lemma, it remains to check that I_K^S / K^S is trivial. But this follows from the fact that S contains a set of generators for the ideal class group C_K : any fractional ideal $\mathfrak{a}$ can be written as $\mathfrak{b} \cdot (c)$ for $\mathfrak{b}$ in the group generated by the prime ideals in S and c in K^S . So if $\mathfrak{a}$ is in I_K^S then $\mathfrak{a} = (c)$. $\square$

We can now prove the main theorem.

Proof of Theorem 5.18. Consider S a finite set of places of K such that S contains the set of infinite places S_∞ of K , all the primes that ramify in L and all the prime ideals of the form $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ for $\mathfrak{q}$ in a set of generators of the ideal class group C_L . Denote by T the set of places of L lying above the places of S . By Lemma 5.20, we can write $\mathbb{I}_L = \mathbb{I}_{L,T} \cdot L^\times$ and so

$$\mathbb{C}_L = \mathbb{I}_{L,T} \cdot L^\times / L^\times \simeq \mathbb{I}_{L,T} / (L^\times \cap \mathbb{I}_{L,T}).$$

But, by definition,

$$L^\times \cap \mathbb{I}_{L,T} = \{x \in L \mid \text{ord}_w(x) = 0 \text{ for all } w \notin T\} = U(T)$$

This yields

$$h(\mathbb{C}_L) = \frac{h(\mathbb{I}_{L,T})}{h(U(T))}$$

and from Proposition 5.15 and Proposition 5.16, we obtain $h(\mathbb{C}_L) = [L : K]$ as wanted.

Now the inequality $[\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)] \geq [L : K]$ follows from (5.2.3), since the order of $H^1(G, \mathbb{C}_L)$ is ≥ 1 . $\square$

5.3 Consequences of the first inequality

Recall that we say that a finite extension of number fields L/K is solvable if it is Galois and the Galois group G is solvable, i.e. it has a composition series whose factors are all cyclic groups of prime order. Theorem 5.18 has the following useful consequence:

Proposition 5.21. *Let L be a finite solvable extension of K . If there exists a subgroup D of $\mathbb{I}_K$ such that $D \subset \text{Nm}_{L/K}(\mathbb{I}_L)$ and $K^\times \cdot D$ is dense in $\mathbb{I}_K$ then L is equal to K .*

Proof. Suppose $L \neq K$. Since L/K is solvable, there exists a field $K' \subset L$ such that K'/K is cyclic and $K' \neq K$. We have

$$\text{Nm}_{K'/K}(\mathbb{I}_{K'}) \supset \text{Nm}_{K'/K}(\text{Nm}_{L/K'}(\mathbb{I}_L)) = \text{Nm}_{L/K}(\mathbb{I}_L) \supset D.$$

Since $K^\times \cdot D$ is dense in $\mathbb{I}_K$ then $K^\times \cdot \text{Nm}_{K'/K}(\mathbb{I}_{K'})$ is dense in $\mathbb{I}_K$ as well and it is open (this is the union of the translates of $\text{Nm}_{K'/K}(\mathbb{I}_{K'})$ which is open by Corollary 4.10). Since open subgroups of a topological group are also closed, we deduce that $K^\times \cdot \text{Nm}_{K'/K}(\mathbb{I}_{K'})$ is dense and closed in $\mathbb{I}_K$, so they are equal. But then the inequality from Theorem 5.18 implies that $K' = K$, contradiction. $\square$

In particular, we obtain:

Theorem 5.22. *Let L be a finite solvable extension of K such that $L \neq K$. Then there are infinitely many primes of K that do not split completely in L .*

Proof. Suppose that there exists only a finite number of primes of K that do not split completely in L and take S a finite set of places that contains S_∞ and all the primes that do not split completely. Consider the subgroup of $\mathbb{I}_K$:

$$D := \{(a_v) \in \mathbb{I}_K \mid a_v = 1 \text{ for all } v \in S\}.$$

We claim that D satisfies the conditions of Proposition 5.21. The fact that D is contained in $\text{Nm}_{L/K}(\mathbb{I}_L)$ follows from the fact that if v is not in S then for any w place of L above v , we have $L_w = K_v$ so any a_v is equal to $\text{Nm}_{L_w/K_v}(a_v)$. We need to check that $K^\times \cdot D$ is dense in $\mathbb{I}_K$. Let $a = (a_v)_v$ be in $\mathbb{I}_K$ and $\varepsilon > 0$. By weak approximation theorem, there exists x in $K^\times$ such that $|a_v - x|_v < \varepsilon$ for v in S . Define $b = (b_v)$ in D such that $b_v = x^{-1}a_v$ for $v \notin S$. Then if we set $a' := xb \in K^\times \cdot D$, we have

$$\begin{aligned} |a_v - a'_v|_v &= |a_v - x|_v < \varepsilon \text{ if } v \in S, \\ |a_v - a'_v|_v &= |a_v - a_v|_v = 0 \text{ if } v \notin S. \end{aligned}$$

This concludes the proof. $\square$

We will see later (using complex analysis) a stronger version of this theorem, which states that the result is true for any finite L/K .

Corollary 5.23. *Let L/K be a finite solvable extension with Galois group G and let S be a finite set of prime ideals of K containing those that ramify in L . Let T be the set of places of L lying above the places of S . Then the set of Frobenius elements $\{(\mathfrak{q}, L/K), \mathfrak{q} \notin T\}$ generates G .*

Proof. Without loss of generality, we can assume that T is stable under the action of the group G (if T is not stable, replace T by a larger set). We denote by H the group generated by $\{(\mathfrak{q}, L/K), \mathfrak{q} \notin T\}$. Then H is a normal subgroup of G . Consider the extension $K' := L^H$. For $\mathfrak{p}$ a prime ideal of K and $\mathfrak{q}$ a prime ideal of L dividing $\mathfrak{p}$, recall that we have

$$(\mathfrak{q} \cap K', K'/K) = (\mathfrak{q}, L/K)|_{K'}.$$

But if $\mathfrak{q}$ is not in T , then $(\mathfrak{q}, L/K)|_{K'}$ is the identity, so $(\mathfrak{p}', K'/K)$ is the identity for any $\mathfrak{p}'$ in K' not lying under a prime of T . This means that if $\mathfrak{p}$ does not lie under a prime of T then it splits completely in K' . Theorem 5.22 implies that $K = K'$ and by Galois theory, $G = H$. $\square$

We can now prove the surjectivity of the Artin map for number fields:

Corollary 5.24. *Let L/K be a finite abelian extension of number fields and S a finite set of places of K that contains S_∞ and all the places that ramify in L . Then the Artin map*

$$\psi_{L/K}^S : \begin{cases} I_K^S & \rightarrow \text{Gal}(L/K) \\ \mathfrak{p} & \mapsto (\mathfrak{p}, L/K) \end{cases}$$

is surjective.

Proof. The group $\psi_{L/K}^S(I_K^S)$ contains all the Frobenius $(\mathfrak{q}, L/K)$ for $\mathfrak{q}$ not lying above a prime of S . But by Corollary 5.23, this generates G . $\square$

6 The second inequality

In this section, we prove the following theorem:

Theorem 6.1 (Second Inequality). *Let L/K be a finite extension of number fields with Galois group G . Then the following statements hold:*

- (1) *The index $[\mathbb{I}_K : K^\times \cdot \text{Norm}_{L/K}(\mathbb{I}_L)]$ is finite and divides $[L : K]$.*
- (2) *The group $H^1(G, \mathbb{C}_L)$ is trivial.*
- (3) *The group $H^2(G, \mathbb{C}_L)$ is finite and its order divides $[L : K]$.*

6.1 First reductions

Note that for any Galois group G , we have

$$\mathbb{I}_K/K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L) \simeq \mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L) = \hat{H}^0(G, \mathbb{C}_L).$$

Lemma 6.2. *It suffices to prove Theorem 6.1 when G is a p -group, for all prime p .*

Proof. Recall the following general result about cohomology of finite groups:

Proposition 6.3. *Let G be a finite group, and let G_p be its Sylow p -subgroup. Then for any G -module M , the restriction map*

$$\text{Res} : \hat{H}^i(G, M) \rightarrow \hat{H}^i(G_p, M)$$

is injective on the p -primary component of $\hat{H}^i(G, M)$ (i.e. the subgroup of elements of order a power of p).

Assume that Theorem 6.1 is true when p -groups for all prime p and let L/K be a finite extension of number fields with Galois group G . For a fixed prime p , let G_p the Sylow p -subgroup of G and write $L_p := L^{G_p}$. By hypothesis the theorem holds for L/L_p . In particular, we have that:

- the order of $\hat{H}^0(G_p, \mathbb{C}_L)$ is a power of p dividing the order of G_p , and in particular, $[L : K]$,
- the group $\hat{H}^1(G_p, \mathbb{C}_L)$ is trivial,
- the order of $\hat{H}^2(G_p, \mathbb{C}_L)$ is a power of p dividing the order of G_p , and in particular, $[L : K]$.

We apply the proposition to the group G and the module $\mathbb{C}_L$. The three bullet points above imply:

- the power of p dividing the order of $\hat{H}^0(G, \mathbb{C}_L)$ is less than the power of p dividing $[L : K]$,
- the prime p does not divide the order of $\hat{H}^1(G, \mathbb{C}_L)$,
- the power of p dividing the order of $\hat{H}^2(G, \mathbb{C}_L)$ is less than the power of p dividing $[L : K]$.

Since the three statements are true for all prime p , we obtain that Theorem 6.1 holds for L/K as well. $\square$

Lemma 6.4. *It suffices to prove Theorem 6.1 when G is a cyclic group of order p (for all prime p).*

Proof. Assume that Theorem 6.1 is true for cyclic groups of order p , for all prime p . Let L/K be a Galois extension of number fields with Galois group G and let p be a fixed prime number. From Lemma 6.2, we can assume that G is a p -group. We prove the theorem by induction on

the order of G . Since G is a p -group, we can find H a normal subgroup of G of index p . Write $K' := L^H$.

Let us first prove statement (1) in Theorem 6.1. We have

$$[\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)] = [\mathbb{C}_K : \text{Nm}_{K'/K}(\mathbb{C}_{K'})] \cdot [\text{Nm}_{K'/K}(\mathbb{C}_{K'}) : \text{Nm}_{L/K}(\mathbb{C}_L)].$$

But G/H is a cyclic group of order p , so by Theorem 6.1(1), $[\mathbb{C}_K : \text{Nm}_{K'/K}(\mathbb{C}_{K'})]$ divides p . Moreover, by induction, $[\mathbb{C}_{K'} : \text{Nm}_{L/K'}(\mathbb{C}_L)]$ divides $[L : K']$ and we have a surjection

$$\text{Nm}_{K'/K} : \mathbb{C}_{K'}/\text{Nm}_{L/K'}(\mathbb{C}_L) \rightarrow \text{Nm}_{K'/K}(\mathbb{C}_{K'})/\text{Nm}_{L/K}(\mathbb{C}_L),$$

so $[\text{Nm}_{K'/K}(\mathbb{C}_{K'}) : \text{Nm}_{L/K}(\mathbb{C}_L)]$ divides $[L : K']$. We obtain that $[\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)]$ divides $[L : K]$, as wanted.

Now, since $(\mathbb{C}_L)^H = \mathbb{C}_{K'}$ (Lemma 5.19) the inflation-restriction exact sequence can be written as

$$0 \rightarrow H^1(G/H, \mathbb{C}_{K'}) \xrightarrow{\text{Inf}} H^1(G, \mathbb{C}_L) \xrightarrow{\text{Res}} H^1(H, \mathbb{C}_L).$$

By Theorem 6.1(2), $H^1(G/H, \mathbb{C}_{K'})$ is trivial and by induction $H^1(H, \mathbb{C}_L)$ is also trivial. It follows $H^1(G, \mathbb{C}_L) = 0$. This proves (2).

Since $H^1(G, \mathbb{C}_L) = 0$, the inflation-restriction exact sequence holds in degree 2 as well:

$$0 \rightarrow H^2(G/H, \mathbb{C}_{K'}) \xrightarrow{\text{Inf}} H^2(G, \mathbb{C}_L) \xrightarrow{\text{Res}} H^2(H, \mathbb{C}_L).$$

By Theorem 6.1(3) for group of order p , we know that the order of $H^2(G/H, \mathbb{C}_{K'})$ divides $[K' : K]$ and in particular, it divides $[L : K]$, and by induction the order of $H^2(H, \mathbb{C}_L)$ divides $[L : K']$ and in particular $[L : K]$. It follows that the order of $H^2(G, \mathbb{C}_L)$ divides $[L : K]$, as wanted. This proves (3). $\square$

In the case where G is a cyclic group we moreover have the following result:

Proposition 6.5. *If L/K is a cyclic extension then statements (1), (2) and (3) in Theorem 6.1 are equivalent and we have*

$$[\mathbb{I}_K : K^\times \cdot \text{Norm}_{L/K}(\mathbb{I}_L)] = |H^2(G, \mathbb{C}_L)| = [L : K].$$

Proof. If G is cyclic then $\widehat{H}^0(G, \mathbb{C}_L) \simeq \widehat{H}^2(G, \mathbb{C}_L)$ and we see that statements (1) and (3) are equivalent. From Theorem 5.18(1), we know that $h(\mathbb{C}_L) = [L : K]$, so (2) is equivalent to (1) (and (3)). $\square$

Combining Proposition 6.5 and Lemma 6.4, we see that in order to prove Theorem 6.1, it suffices to prove that for L/K cyclic extension of order p , then

$$(6.1.1) \quad [\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)] \text{ divides } [L : K] = p.$$

We can make one further reduction:

Lemma 6.6. *To prove (6.1.1) for any L/K cyclic extension of order p , it suffices to prove it in the case where K contains a p -th root of 1.*

Proof. Let L/K be a cyclic extension of degree p . Let ζ be a primitive p -th root of 1, set $K' := K(\zeta)$, $L' := K' \cdot L = L(\zeta)$ and assume that (6.1.1) is true for the extension L'/K' . Since ζ is a primitive p -th root, then the degree $[K' : K]$ divides $p - 1$ and in particular, it is coprime to p . It follows that $[K' \cap L : K] = 1$ and so $K' \cap L = K$ and we have an isomorphism of groups $\text{Gal}(L'/K) \xrightarrow{\sim} \text{Gal}(L/K) \times \text{Gal}(K'/K)$.

Since $\text{Gal}(L/K) \simeq \text{Gal}(L'/K')$ and $\text{Gal}(L'/L) \simeq \text{Gal}(K'/K)$, then the norm maps (defined by $x \mapsto \prod_g g \cdot x$ where the sum is taken over the Galois groups) fit into a commutative diagram:

$$\begin{array}{ccccccc}
\mathbb{C}_L & \xrightarrow{\text{Nm}_{L/K}} & \mathbb{C}_K & \longrightarrow & \mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L) & \longrightarrow & 0 \\
\downarrow i_L & & \downarrow i_K & & \downarrow & & \\
\mathbb{C}_{L'} & \xrightarrow{\text{Nm}_{L'/K'}} & \mathbb{C}_{K'} & \longrightarrow & \mathbb{C}_{K'}/\text{Nm}_{L'/K'}(\mathbb{C}_{L'}) & \longrightarrow & 0 \\
\downarrow \text{Nm}_{L'/L} & & \downarrow \text{Nm}_{K'/K} & & \downarrow & & \\
\mathbb{C}_L & \xrightarrow{\text{Nm}_{L/K}} & \mathbb{C}_K & \longrightarrow & \mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L) & \longrightarrow & 0
\end{array}$$

where i_L and i_K are induced by the maps $\mathbb{I}_L \rightarrow \mathbb{I}_{L'}$ and $\mathbb{I}_K \rightarrow \mathbb{I}_{K'}$. But both the maps $\text{Nm}_{L'/L} \circ i_L$ and $\text{Nm}_{K'/K} \circ i_K$ are given by $(\cdot)^{[K':K]}$ so the right vertical map

$$\mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L) \rightarrow \mathbb{C}_{K'}/\text{Nm}_{L'/K'}(\mathbb{C}_{L'}) \rightarrow \mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L)$$

is also given by $(\cdot)^{[K':K]}$. But if x is in $\mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L)$, we have $x^p = \text{Nm}_{L/K}(x)$ (recall $[L : K] = p$) so $(\cdot)^p$ kills $\mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L)$ and since $[K' : K]$ and p are coprime, we obtain that $(\cdot)^{[K':K]}$ is an automorphism of $\mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L)$. It follows that

$$\mathbb{C}_{K'}/\text{Nm}_{L'/K'}(\mathbb{C}_{L'}) \rightarrow \mathbb{C}_K/\text{Nm}_{L/K}(\mathbb{C}_L)$$

is surjective. In particular, $[\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)]$ divides $[\mathbb{C}_{K'} : \text{Nm}_{L'/K'}(\mathbb{C}_{L'})]$. Since we have assumed that (6.1.1) is true for the extension L'/K' , it follows that $[\mathbb{C}_K : \text{Nm}_{L/K}(\mathbb{C}_L)]$ divides p , as wanted. $\square$

6.2 Kummer theory

Assume that K is a field containing a primitive n -th root of the unity ζ . This means in particular that K is of characteristic 0 or characteristic $p > 0$ for p not dividing n . We denote by μ_n the group of the n -th roots of 1 in K . This is a cyclic group of order n with generator ζ .

Proposition 6.7. *Let $L = K(\alpha)$ where $\alpha \in \overline{K}$ is such that $a := \alpha^n \in K$ and $\alpha^m \notin K$ for all $m < n$. Then L is a Galois extension of K with cyclic Galois group of order n . Conversely, if L is cyclic extension of K of degree n , then $L = K(\alpha)$ for some $\alpha \in \overline{K}$ such that $\alpha^n \in K$.*

Proof. The first assertion comes from the fact that the root of the polynomials $X^n - a$ are of the form $\zeta^i a$ for $i \in \{0, \dots, n-1\}$, so for g in the Galois group $\frac{g(a)}{a}$ is in μ_n . The hypothesis $\alpha^m \notin K$ for all $m < n$ implies that the morphism

$$\begin{cases} G & \rightarrow \mu_n \\ g & \mapsto \frac{g(a)}{a} \end{cases}$$

is an isomorphism. This proves that L/K is cyclic of order n .

Assume now that L/K is cyclic of order n and take g a generator of G and ζ a generator of μ_n . To prove that L can be written as $K(\alpha)$ with α^n in K , it suffices to show that there exists α in $L^\times$ such that $g(\alpha) = \zeta^{-1}\alpha$ (because if this is true, then $\alpha^m \notin K$ for any $0 \leq m < n$). Recall that for L a field and G a group, any finite set of characters $G \rightarrow L^\times$ is linearly independent over K . In particular, the character $\sum_{i=0}^{n-1} \zeta^i g^i$ is non-zero and there exists β in L such that $\sum_{i=0}^{n-1} \zeta^i g^i(\beta) \neq 0$. Take $\alpha = \zeta^i g^i(\beta)$.

□

Note that if we fix an algebraic closure $\overline{K}$ of K , then $K(\alpha) \subset \overline{K}$ depends only on $a := \alpha^n$ and we denote it by $K(a^{\frac{1}{n}})$.

Proposition 6.8. *Two cyclic extensions $K(a^{\frac{1}{n}})$ and $K(b^{\frac{1}{n}})$ are equal if and only if there exist r in $\mathbf{Z}$ prime to n and $\lambda \in K^\times$ such that $a = \lambda^n \cdot b^r$ (in other words, a and b generate the same subgroup of $K^\times / K^{\times n}$).*

Proof. If $a = \lambda^n \cdot b^r$ for some r prime to n and λ in $K^\times$ then we obviously have $K(a^{\frac{1}{n}}) = K(b^{\frac{1}{n}})$.

Conversely, assume $L := K(\alpha) = K(\beta)$ with $\alpha^n = a$ and $\beta^n = b$. Let g be a generator of $\text{Gal}(L/K)$ and let ζ be a primitive n -th root of 1 such that $g(\alpha) = \zeta\alpha$ and $g(\beta) = \zeta^i\beta$ for i prime to n . Since β is in $L = K(\alpha)$, we can write $\beta = \sum_{j=0}^{n-1} \lambda_j \alpha^j$, with $\lambda_j \in K$. Applying $g(\cdot)$ to the latter formula and comparing $g(\beta)$ with $\zeta^i\beta$, we obtain $\zeta^i \lambda_j = \zeta^j \lambda_j$ for all $0 \leq j < n$. It follows that $\lambda_j = 0$ if $j \neq i$, i.e. $\beta = \lambda_i \alpha^i$ as wanted.

□

The above result can be reformulated in the following way:

Corollary 6.9. *Let n be an integer and K be a field containing a primitive n -th root of 1. Fix $\overline{K}$ an algebraic closure of K . There is a one-to-one correspondance*

$$\begin{aligned} \{K \subset L \subset \overline{K} \text{ cyclic of order } n\} &\rightarrow \{H \subset K^\times / K^{\times n} \text{ cyclic subgroup of order } n\} \\ L &\mapsto K^\times \cap L^{\times n} / K^{\times n}. \end{aligned}$$

The extension corresponding to a cyclic subgroup $H \subset K^\times / K^{\times n}$ is $K(a^{\frac{1}{n}})$ where a is a generator of H .

We can in fact extend the results of Corollary 6.9 to all abelian extensions of exponent n . Recall that the exponent of a finite group G is the smallest integer n such that $g^n = 1$ for all $g \in G$. A finite abelian group of exponent n is isomorphic to a subgroup of $(\mathbf{Z}/n\mathbf{Z})^r$.

For any finite Galois extension L/K with Galois group G , the Kummer exact sequence

$$0 \rightarrow \mu_n \rightarrow L^\times \xrightarrow{x \mapsto x^n} L^{\times n} \rightarrow 0$$

induces an exact sequence (using Hilbert's Theorem 90 to get $H^1(G, L^\times) = 0$)

$$0 \rightarrow \mu_n \rightarrow K^\times \xrightarrow{x \mapsto x^n} K^\times \cap L^{\times n} \rightarrow H^1(G, \mu_n) \simeq \text{Hom}(G, \mu_n) \rightarrow 0.$$

This yields the isomorphism:

$$(6.2.1) \quad \begin{cases} K^\times \cap L^{\times n} / K^{\times n} & \xrightarrow{\sim} \text{Hom}(G, \mu_n) \\ \alpha^n & \mapsto (g \mapsto \frac{g(\alpha)}{\alpha}) \end{cases}$$

and if we moreover assume that G has exponent n , then $\text{Hom}(G, \mu_n)$ and G are (non-canonically) isomorphic and it follows that

$$(6.2.2) \quad [L : K] = [K^\times \cap L^{\times n} : K^{\times n}].$$

Theorem 6.10. *Let n be an integer and K be a field containing a primitive n -th root of 1. Fix $\overline{K}$ an algebraic closure of K . There is a one-to-one correspondance*

$$\begin{aligned} \{K \subset L \subset \overline{K} \text{ finite abelian extension of exponent } n\} &\rightarrow \{H \subset K^\times / K^{\times n} \text{ finite subgroup}\} \\ L &\mapsto K^\times \cap L^{\times n} / K^{\times n}. \end{aligned}$$

The extension corresponding to a finite subgroup $H \subset K^\times / K^{\times n}$ is $K[H^{\frac{1}{n}}]$, the smallest subfield of $\overline{K}$ containing K and an n -th root of each element of H .

Moreover, for an extension L corresponding to a subgroup H , we have

$$[L : K] = [H : K^{\times n}].$$

Proof. First note that for any $H \subset K^\times$ such that H contains $K^{\times n}$ as a subgroup of finite index, if $\{a_1, \dots, a_r\}$ is a set of generators for $H/K^{\times n}$, then

$$K(H^{\frac{1}{n}}) \simeq K(a_1^{\frac{1}{n}}) \cdot K(a_2^{\frac{1}{n}}) \cdots K(a_r^{\frac{1}{n}})$$

and we see that L/K is a finite abelian extension of exponent n .

For L/K a finite Galois extension, set $H(L) := K^\times \cap L^{\times n}$. Then for any L , we have $K(H(L)^{\frac{1}{n}}) \subset L$. For any $H \subset K^\times$ such that H contains $K^{\times n}$ as a subgroup of finite

index, we have $H \subset H(K(H^{\frac{1}{n}}))$. Note that with this notation, Equation 6.2.2 becomes $[H(F) : K^{\times n}] = [F : K]$ for all F/K of exponent n . It follows that

$$[L : K] \geq [K(H(L)^{\frac{1}{n}}) : K] = [H(K(H(L)^{\frac{1}{n}})) : K^{\times n}] \geq [H(L) : K^{\times n}],$$

where the equality in the middle holds because $K(H(L)^{\frac{1}{n}})/K$ has exponent n by the remark above. Since we also have $[L : K] = [H(L) : K^{\times n}]$, it follows that the inequalities are in fact equalities and we obtain $K(H(L)^{\frac{1}{n}}) = L$.

Now, if we start from a subgroup $H \subset K^{\times}$ such that H contains $K^{\times n}$ as a subgroup of finite index and define $L := K(H^{\frac{1}{n}})$, we have already seen that L is a finite abelian extension of K with exponent n . Let us write $G := \text{Gal}(L/K)$. The isomorphism

$$H(L)/K^{\times n} \xrightarrow{\sim} \text{Hom}(G, \mu_n)$$

from (6.2.1) induces an isomorphism

$$H/K^{\times n} \xrightarrow{\sim} \text{Hom}(G/H_0, \mu_n), \quad \text{where} \quad H_0 := \{g \in G \mid g(a^{\frac{1}{n}}) = a^{\frac{1}{n}} \text{ for all } a \in H\}.$$

But by definition of L , if g is in H_0 then $g = \text{Id}_L$. Therefore, the two above isomorphisms are in fact equal and $H(K(H^{\frac{1}{n}})) = H(L) = H$, as wanted. $\square$

Example 6.11. (1) The theorem states that quadratic extensions of $\mathbf{R}$ are in one-to-one correspondence with the subgroups of $\mathbf{R}^{\times}/\mathbf{R}^{\times 2} \simeq \{\pm 1\}$.

(2) The finite abelian extensions of $\mathbf{Q}$ of exponent 2 are in one-to-one correspondence with the finite subgroups of

$$\mathbf{Q}^{\times}/\mathbf{Q}^{\times 2} \simeq \{\pm 1\} \times \prod_{p \text{ prime}} \mathbf{Z}/2\mathbf{Z}.$$

We also have:

Proposition 6.12. *Let K be a number field, and let $L = K(a_1^{\frac{1}{n}}, \dots, a_r^{\frac{1}{n}})$. Let v be a finite place of K . If na_i is a unit in K_v for all $1 \leq i \leq r$, then L is unramified at v .*

Proof. By induction, we can reduce the proof to the case $L = K(a^{\frac{1}{n}})$ of degree n . But we have

$$\text{Disc}(X^n - a) = \pm \text{Nm}_{L/K} P'(\alpha) = \pm n^n a^{n-1}.$$

Hence if na is a unit in K_v , this means that the associated prime ideal $\mathfrak{p}_v$ does not divide $\text{Disc}(X^n - a)$ and so, L is unramified at v . $\square$

6.3 Second inequality for abelian extensions of exponent p

The goal of this section is to prove the following theorem:

Theorem 6.13. *Let K be a number field that contains a primitive p -th root of unity and let L/K be a finite abelian extension with exponent p . Then $[\mathbb{I}_K : K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L)]$ divides $[L : K]$.*

Using the reduction results proved in Section 6.1, this would in particular conclude the proof of the second inequality (Theorem 6.1).

Let us fix K a number field that contains a primitive p -th root of unity and let L/K be a finite abelian extension with exponent p . Let r be such that $\text{Gal}(L/K) \simeq \mathbf{Z}/p^r\mathbf{Z}$. Then by Theorem 6.10, we know that we can write $L = K(a_1^{\frac{1}{p}}, \dots, a_r^{\frac{1}{p}})$ with $a_1, \dots, a_r$ in K . Let S be a finite set of places of K such that

- (i) S contains the infinite places of K ,
- (ii) S contains all the places that divide the prime p ,
- (iii) the a_i 's are all in $U(S)$, i.e. $\text{ord}_v(a_i) = 0$ for all $v \notin S$,
- (iv) S contains a set of generators for the ideal class group of K .

Note that by Proposition 6.12, conditions (ii) and (iii) imply that S contains all the places that ramify in L . By Lemma 5.20, condition (iv) implies $\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$. Using the compactness of $\mathbb{I}_K^1/K^\times$ we can prove that $U(S)$ can be decomposed as a product $U(S)_{\text{tors}} \times \mathbf{Z}^{s-1}$ with $s = |S|$ (the proof is the same as the one of Dirichlet's units theorem seen in Sheet 3, Exercise 4 – we just need to replace S_∞ by S), where $U(S)_{\text{tors}}$ is cyclic. But we also have that $U(S)_{\text{tors}}$ is a p -group so

$$(6.3.1) \quad U(S)/U(S)^p \simeq (\mathbf{Z}/p\mathbf{Z})^{s-1} \times (\mathbf{Z}/p\mathbf{Z}) = (\mathbf{Z}/p\mathbf{Z})^s.$$

Consider the Kummer extension $M := K(U(S)^{\frac{1}{p}})$ corresponding (via the correspondance of Theorem 6.10) to the group

$$U(S) \cdot K^{\times p}/K^{\times p} \simeq U(S)/(U(S) \cap K^{\times p}) \simeq U(S)/U(S)^p \simeq (\mathbf{Z}/p\mathbf{Z})^s.$$

Hence $[M : K] = p^s$. Note that since the a_i 's are in $U(S)$, we have that M contains L : in fact, M/L also corresponds (via Theorem 6.10 for extensions of L) to the group

$$U(S) \cdot L^{\times p}/L^{\times p} \simeq U(S)/(U(S) \cap L^{\times p}).$$

We define $t := s - r$ such that $[M : L] = p^t$. We have the following result:

Proposition 6.14. *Let K , L and S as above. Then*

(1) There exists a finite set of places T of K disjoint from S such that the set $\{(\mathfrak{p}, M/K) \mid \mathfrak{p} \in T\}$ forms a basis of the $\mathbb{F}_p$ -vector space $\text{Gal}(M/L)$.

(2) For this T , any element a in $U(S)$ becomes a p -th power in L if and only if a becomes a p -th power in K_v for all $v \in T$.

(3) For this T , the subgroup of $\mathbb{I}_K$

$$W(S, T) := \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^{\times} \times \prod_{v \notin S \cup T} U_v$$

is contained in $\text{Nm}_{L/K}(\mathbb{I}_L)$.

Proof. We start by constructing the set T . Let $\mathfrak{p}$ be a prime of K , $\mathfrak{q}_L$ a prime of L dividing $\mathfrak{p}$ and $\mathfrak{q}_M$ a prime of M dividing $\mathfrak{q}_L$. If $\mathfrak{p}$ is not in S then by Proposition 6.12 and hypothesis on S , the extension $M_{\mathfrak{q}_M}/K_{\mathfrak{p}}$ is unramified so $\text{Gal}(M_{\mathfrak{q}_M}/K_{\mathfrak{p}})$ is cyclic. But since M/K has exponent p and $\text{Gal}(M_{\mathfrak{q}_M}/K_{\mathfrak{p}}) \subset \text{Gal}(M/K)$, we see that $M_{\mathfrak{q}_M}/K_{\mathfrak{p}}$ is cyclic of exponent p . Hence it is either trivial or cyclic with order p . In particular, we obtain that if $M_{\mathfrak{q}_M}$ is not equal to $L_{\mathfrak{q}_L}$ then $L_{\mathfrak{q}_L} = K_{\mathfrak{p}}$.

Write S' the finite set of the places of L which lie above the places of S . From Corollary 5.23, we know that $\{(\mathfrak{q}_M, M/L) \mid \mathfrak{q}_M \text{ does not divide places of } S'\}$ generates the group $\text{Gal}(M/L)$. So we can extract a finite subset T of places of K such that $T \cap S = \emptyset$ and $\{(\mathfrak{q}_M, M/L) \mid \mathfrak{q}_M \text{ above places of } T\}$ generates the $\mathbb{F}_p$ -vector space $\text{Gal}(M/L)$. We can also choose T such that $(\mathfrak{q}_M, M/L) \neq 1$ for places of T , and in particular $M_{\mathfrak{q}_M} \neq L_{\mathfrak{q}_L}$. Then if $\mathfrak{q}_L$ a place of L dividing $\mathfrak{p} \in T$ and $\mathfrak{q}_M$ a place of M above $\mathfrak{q}_L$, the above paragraph tells us that $L_{\mathfrak{q}_L} = K_{\mathfrak{p}}$ and we obtain $(\mathfrak{q}_M, M/L) = (\mathfrak{q}_M, M/K)$. This finishes the proof of (1).

Let us now prove the second point. Assume first that a is in $U(S)$ such that $a = b^p$ for b in L . For all places w of L , $a_w = b_w^p$ in $L_w^{\times}$. If $w = \mathfrak{q}$ is a place dividing some $\mathfrak{p}$ place of T , then by the above, we have $L_{\mathfrak{q}} = K_{\mathfrak{p}}$ so $a_{\mathfrak{p}} = b_{\mathfrak{p}}^p$ in $K_{\mathfrak{p}}^{\times}$ as wanted. Conversely, let a be in $U(S)$ such that for any $\mathfrak{p}$ in T , there exists $c_{\mathfrak{p}}$ in $K_{\mathfrak{p}}^{\times}$ with $a_{\mathfrak{p}} = c_{\mathfrak{p}}^p$. By definition of M , we also know that $a = b^p$ for some $b \in M$. For $\mathfrak{q}$ a place of M dividing a place $\mathfrak{p}$ of T , we can assume $b_{\mathfrak{q}} = c_{\mathfrak{p}}$ (since K contains ζ). In particular b is fixed by $(\mathfrak{p}, M/K)$ for all $\mathfrak{p}$ in T , and so it is fixed by $\text{Gal}(M/L)$. We obtain $b \in L$. This proves (2).

To prove (3), take $a = (a_v)$ an element of $W(S, T)$. We want to show that for each v , the component a_v is on the corresponding norm group. If v is in T and w a place of L dividing v , we have seen that $L_w = K_v$ so a_v is clearly in the image of Nm_{L_w/K_v} . If v is in S and w a place of L dividing v , then we know that the local Artin map induces an isomorphism:

$$K_v^{\times} / \text{Nm}_{L_w/K_v}(L_w^{\times}) \xrightarrow{\sim} \text{Gal}(L_w/K_v).$$

But since L_w/K_v has exponent p , it follows that the exponent of the group $K_v^{\times} / \text{Nm}_{L_w/K_v}(L_w^{\times})$ is p as well, and in particular, $K_v^{\times p}$ is contained in $\text{Nm}_{L_w/K_v}(L_w^{\times})$, as wanted.

If v is not in $S \cup T$ then L_w/K_v is unramified and we know that for unramified extensions of local fields, the norm map $\text{Nm}_{L_w/K_v} : U_w \rightarrow U_v$ is surjective. This concludes the proof of the proposition. $\square$

It follows from the third point of Proposition 6.14 that, in order to prove that $[\mathbb{I}_K : K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L)]$ divides $[L : K] = p^r$, it suffices to prove that $[\mathbb{I}_K : K^\times \cdot W(S, T)]$ divides p^r (since $[\mathbb{I}_K : K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L)]$ divides $[\mathbb{I}_K : K^\times \cdot W(S, T)]$). But by Lemma 5.20, we still have $\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K, S \cup T}$ and so we are reduced to show that

$$(6.3.2) \quad [K^\times \cdot \mathbb{I}_{K, S \cup T} : K^\times \cdot W(S, T)] \text{ divides } p^r.$$

This follows from the following three propositions (recall that $p^r = p^{s+t}$):

Proposition 6.15. *We have:*

$$[K^\times \cdot \mathbb{I}_{K, S \cup T} : K^\times \cdot W(S, T)] = \frac{[\mathbb{I}_{K, S \cup T} : W(S, T)]}{[U(S \cup T) : K^\times \cap W(S, T)]}.$$

Proposition 6.16. *We have $[\mathbb{I}_{K, S \cup T} : W(S, T)] = p^{2s}$.*

Proposition 6.17. *We have $[U(S \cup T) : K^\times \cap W(S, T)] = p^{s+t}$.*

6.3.1 Proof of Proposition 6.15

Since $U(S, T) = \mathbb{I}_{K, S \cup T} \cap K^\times$, Proposition 6.15 immediately follows from the following general lemma:

Lemma 6.18. *Let H be an abelian group and H_1, H_2 and H_3 subgroups of H such that $H_2 \subset H_1$. If two of the indexes $[H_1 : H_2]$, $[H_1 \cdot H_3 : H_2 \cdot H_3]$ and $[H_1 \cap H_3 : H_2 \cap H_3]$ are finite then so is the third one and*

$$[H_1 : H_2] = [H_1 \cap H_3 : H_2 \cap H_3][H_1 \cdot H_3 : H_2 \cdot H_3].$$

Proof. This follows from the commutative diagram with exact rows and columns (the third row is

exact by snake lemma):

$$\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H_2 \cap H_3 & \longrightarrow & H_2 & \longrightarrow & (H_2 \cdot H_3)/H_3 \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H_1 \cap H_3 & \longrightarrow & H_1 & \longrightarrow & (H_1 \cdot H_3)/H_3 \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & (H_1 \cap H_3)/(H_2 \cap H_3) & \longrightarrow & H_1/H_2 & \longrightarrow & (H_1 \cdot H_3)/(H_2 \cdot H_3) \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0
\end{array}$$

□

6.3.2 Proof of Proposition 6.16

We will need the following general result:

Proposition 6.19. (1) Let p be a prime number, if K is a finite extension of $\mathbf{Q}_p$ and $\mu_n(K)$ the groups of n -th roots of 1 in $K^\times$, then we have

$$[U_K : U_K^n] = \frac{1}{|n|_K} \cdot |\mu_n(K)|.$$

(2) If K is a local field of characteristic 0, we have

$$[K^\times : K^{\times n}] = \frac{n}{|n|_K} \cdot |\mu_n(K)|.$$

Proof. For the first point, we regard U_K as an $\mathbf{Z}/n\mathbf{Z}$ -module with trivial action. Then by definition of the Herbrand quotient,

$$[U_K : U_K^n] = h(U_K) \cdot |\mu_n(K)|.$$

It remains to compute $h(U_K)$. We have the following claim:

Claim 6.20. $h(U_K) = h(\mathcal{O}_K)$.

Proof of the claim. We have seen in the proof of Lemma 5.4 (and Proposition 5.5) that there exist subgroups of finite index $V_1 \subset \mathcal{O}_K$ and $V_2 \subset U_K$ such that the exponential map defines an isomorphism between V_1 and V_2 . In particular, $h(V_1) = h(V_2)$.

From Proposition 5.2(3), it also follows that $h(V_1) = h(\mathcal{O}_K)$ and $h(V_2) = h(U_K)$. Hence the desired equality. □

Since $\mathcal{O}_K$ has no n -torsion, we have $h(\mathcal{O}_K) = [\mathcal{O}_K : n\mathcal{O}_K]$ which is by definition the inverse of the norm of n . This proves that

$$h(U_K) = \frac{1}{|n|_K}$$

as wanted.

Let us now prove the second point. In the case where K is a finite extension of $\mathbf{Q}_p$, we can write $K^\times \simeq U_K \times \mathbf{Z}$ and we have

$$[K^\times : K^{\times n}] = [\mathbf{Z} : n\mathbf{Z}][U_K : U_K^n] = n \cdot \frac{1}{|n|_K} \cdot |\mu_n(K)|,$$

by point (1). If $K = \mathbf{C}$, then $\mathbf{C}^n = \mathbf{C}$ and $|\mu_n(\mathbf{C})| = n$. Since $|n|_{\mathbf{C}} = n^2$, (2) is satisfied in that case. Finally, assume $K = \mathbf{R}$. Then

$$[\mathbf{R}^\times : \mathbf{R}^{\times n}] = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even,} \end{cases} \quad \text{and} \quad |\mu_n(\mathbf{R})| = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

Since $|n|_{\mathbf{R}} = n$, both formulas are clearly equal. $\square$

We can now use the above proposition to compute $[\mathbb{I}_{K,S \cup T} : W(S, T)]$.

Proof of Proposition 6.16. Recall that we want to prove $[\mathbb{I}_{K,S \cup T} : W(S, T)] = p^{2s}$ where $s = |S|$ and

$$\begin{aligned} \mathbb{I}_{K,S \cup T} &= \prod_{v \in S} K_v^\times \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v \\ W(S, T) &:= \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v. \end{aligned}$$

We clearly see that

$$[\mathbb{I}_{K,S \cup T} : W(S, T)] = \prod_{v \in S} [K_v^\times : K_v^{\times p}].$$

By Proposition 6.19, we have (there are exactly p p -th roots of 1 in K_v)

$$[K_v^\times : K_v^{\times p}] = \frac{p}{|p|_v} |\mu_p(K_v)| = \frac{p^2}{|p|_v}.$$

Since we have assumed that S contains all the places v such that $|p|_v \neq 1$ then

$$\prod_{v \in S} |p|_v = \prod_{\text{all } v} |p|_v = 1$$

by the product formula. We have proved

$$[\mathbb{I}_{K,S \cup T} : W(S, T)] = p^{2s}.$$

$\square$

6.3.3 Proof of Proposition 6.17

Lemma 6.21. *Let K, L, S and T as in Proposition 6.14. Then the natural map*

$$U(S) \rightarrow \prod_{v \in T} U_v / U_v^p$$

is surjective.

Proof. We write H for the kernel of this map. We want to show that

$$[U(S) : H] = \prod_{v \in T} [U_v : U_v^p].$$

By Proposition 6.19, for any $v \in T$,

$$[U_v : U_v^p] = \frac{|\mu_p(K_v)|}{|p|_v} = |\mu_p(K_v)| = p$$

since by hypothesis on S and T , the norm $|p|_v$ is 1 and K_v is non-archimedean. So $\prod_{v \in T} [U_v : U_v^p] = p^t$.

Let us compute the left hand side. We have seen in Proposition 6.14(2) that H is equal to $U(S) \cap L^{\times p}$. So $U(S)/H \simeq U(S)/(U(S) \cap L^{\times p})$ and this group corresponds via Theorem 6.10 to the extension M/L . Since $[M : L] = p^t$, we obtain $[U(S) : H] = p^t$, as wanted. $\square$

Finally we will use the following consequence of Proposition 5.21:

Proposition 6.22. *Let K be a number field containing a primitive n -th root of 1. Let S be a set of primes containing the infinite primes S_∞ , the primes that divide n and a set of representatives of the ideal class group of K . Let T be a set of primes disjoint from S such that*

$$U(S) \rightarrow \prod_{v \in T} U_v / U_v^n$$

is surjective.

If x is an element of $K^\times$ which is an n -th power in K_v for all v in S and a unit outside $S \cup T$, then x is in fact in $K^{\times n}$.

Proof. Assume that x is an element of $K^\times$ which is an n -th power in K_v for all v in S and in $U(S \cup T)$. Let us set $L := K(x^{\frac{1}{n}})$. We will use Proposition 5.21 to show that $L = K$. Consider the subgroup

$$D := \prod_{v \in S} K_v^\times \times \prod_{v \in T} U_v^n \times \prod_{v \notin S \cup T} U_v.$$

We need to check that D is contained in $\text{Norm}_{L/K}(\mathbb{I}_L)$ and $D \cdot K^\times$ is dense in $\mathbb{I}_K$.

Let $a = (a_v)$ be an element of $D \subset \mathbb{I}_K$. If v is in S , then a_v is in $K_v^\times$ we have $K_v(x^{\frac{1}{n}}) = K_v$ (by definition of x) so $a_v = \text{Norm}_{L_v/K_v}(a_v)$. If v is in T , then a_v can be written b_v^n with b_v in U_v . We know from local CFT that $[K_v^\times : \text{Norm}_{K_v(x^{\frac{1}{n}})/K_v}(K_v(x^{\frac{1}{n}})^\times)] = [K_v(x^{\frac{1}{n}}) : K_v]$. But the degree $[K_v(x^{\frac{1}{n}}) : K_v]$ divides n , so $(-)^n$ kills $K_v^\times / \text{Norm}_{K_v(x^{\frac{1}{n}})/K_v}(K_v(x^{\frac{1}{n}})^\times)$ and we obtain that $a_v = b_v^n$ is in the norm group. If v is not in S nor T , then a_v is in U_v and nx is a unit in K_v . From Proposition 6.12 we see that $K_v(x^{\frac{1}{n}})/K$ is unramified at v and we know that in that case the norm map is surjective on the units. Hence a_v is in the norm group. This proves that D is contained in $\text{Norm}_{L/K}(\mathbb{I}_L)$.

We now show that $D \cdot K^\times = \mathbb{I}_K$. By definition, we have $\mathbb{I}_{K,S}/D = \prod_{v \in T} U_v/U_v^n$ and since we have assumed that the map $U(S) \rightarrow \prod_{v \in T} U_v/U_v^n$ is surjective, we obtain

$$\mathbb{I}_{K,S} \simeq D \cdot U(S).$$

By Lemma 5.20 we have $\mathbb{I}_K \simeq \mathbb{I}_{K,S} \cdot K^\times$, hence

$$\mathbb{I}_K \simeq D \cdot U(S) \cdot K^\times = D \cdot K^\times.$$

□

We can now prove Proposition 6.17.

Proof of Proposition 6.17. We want to show $[U(S \cup T) : K^\times \cap W(S, T)] = p^{s+t}$. Recall that we have $U(S \cup T)/U(S \cup T)^p \simeq (\mathbf{Z}/p\mathbf{Z})^{s+t}$ so $[U(S \cup T) : U(S \cup T)^p] = p^{s+t}$. Moreover we clearly have an inclusion $U(S \cup T)^p \subset K^\times \cap W(S, T)$. So it suffices to prove that $K^\times \cap W(S, T) \subset U(S \cup T)^p$. But this follows from Proposition 6.22. □

7 Brauer groups

In this section, we make use of the computation of the cohomology groups of $\mathbb{C}_L$ to obtain results about Brauer groups of number fields. This will be used later, in the proof of the reciprocity law. We also prove the fundamental exact sequence of global class field theory and construct a fundamental class in the Brauer group.

7.1 Brauer group of number fields

For L/K a Galois extension of (any) fields and $\overline{K}$ an algebraic closure of K , we set:

$$\text{Br}(L/K) := H^2(\text{Gal}(L/K), L^\times) \quad \text{and} \quad \text{Br}(K) := H^2(\text{Gal}(\overline{K}/K), \overline{K}^\times).$$

Recall that if K is a non-archimedean local field, then there exists a canonical isomorphism

$$(7.1.1) \quad \text{inv}_K : \text{Br}(K) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$$

such that for any finite Galois extension of degree d , there is a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Br}(L/K) & \longrightarrow & \text{Br}(K) & \xrightarrow{\text{Res}} & \text{Br}(L) \\ & & & & \downarrow \text{inv}_K & \sim & \downarrow \sim \text{inv}_L \\ 0 & \longrightarrow & \frac{1}{d}\mathbf{Z}/\mathbf{Z} & \longrightarrow & \mathbf{Q}/\mathbf{Z} & \xrightarrow{d} & \mathbf{Q}/\mathbf{Z}. \end{array}$$

In particular, this induces isomorphisms

$$(7.1.2) \quad \text{inv}_{L/K} : \text{Br}(L/K) \xrightarrow{\sim} \frac{1}{d}\mathbf{Z}/\mathbf{Z}.$$

Moreover, if K is the field of real numbers $\mathbf{R}$, then we have

$$\text{inv}_K : \text{Br}(K) \xrightarrow{\sim} \frac{1}{2}\mathbf{Z}/\mathbf{Z}.$$

Let L/K be a finite abelian extension of number fields. Recall that if v is a place of K and w a place of L dividing v , we have seen that $\text{Br}(L_w/K_v)$ depends only on v and we denote by $\text{Br}(L^v/K_v)$ this group.

Theorem 7.1. *Let L/K be a finite Galois extension of number field. There is a natural injective map*

$$\text{Br}(L/K) \rightarrow \bigoplus_{v \text{ place of } K} \text{Br}(L^v/K_v).$$

Similarly, there is a natural injective map

$$\text{Br}(K) \rightarrow \bigoplus_{v \text{ place of } K} \text{Br}(K_v).$$

Note that the above maps land in the direct sum, hence if β is an element of $\text{Br}(K)$, we see that the images β_v of β in $\text{Br}(K_v)$ are zero for almost all v 's.

Proof. Let us first assume that L/K is a finite Galois extension. From Theorem 6.1(2), we know that $H^1(G, \mathbb{C}_L)$ is trivial and in Proposition 5.13, we have computed

$$H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(G^v, L^{\times, v}) = \bigoplus_v \text{Br}(L^v/K_v).$$

Hence, taking the cohomology of the short exact sequence:

$$0 \rightarrow L^\times \rightarrow \mathbb{I}_L \rightarrow \mathbb{C}_L \rightarrow 0$$

we obtain an injective map:

$$H^2(G, L^\times) \hookrightarrow H^2(G, \mathbb{I}_L) = \bigoplus_v \text{Br}(L^v/K_v),$$

as wanted.

We then obtain the result for $\overline{K}$ by passing to the limit (we use the result from Exercise Sheet 5, stating that $H^2(G, \mathbb{I}_{\overline{K}}) = \bigoplus_v \text{Br}(K_v)$ where $\mathbb{I}_{\overline{K}} = \text{colim}_{L/K} \mathbb{I}_L$). $\square$

Let us collect a few facts about cyclic cyclotomic extensions. Let p be a prime number and $r \geq 1$. Recall that for ζ_{p^r} a primitive p^r -th root of 1, there is a natural isomorphism of groups:

$$\begin{cases} (\mathbb{Z}/p^r\mathbb{Z})^\times & \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \\ u & \mapsto \zeta_{p^r}^u. \end{cases}$$

Recall also that we have a decomposition $(\mathbb{Z}/p^r\mathbb{Z})^\times \simeq \Delta_p \times \mathbb{Z}/p^{n_p}\mathbb{Z}$ where $\Delta_p \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ if p is odd and $\mathbb{Z}/2\mathbb{Z}$ when $p = 2$, and $n_p = r-1$ if p is odd and $r-2$ if $p = 2$. We define $K^{(p),r} := \mathbb{Q}(\zeta_{p^r})^{\Delta_p}$ so that $\text{Gal}(K^{(p),r}/\mathbb{Q}) \simeq \mathbb{Z}/p^{n_p}\mathbb{Z}$ is cyclic. A cyclic cyclotomic extension of $\mathbb{Q}$ is the composite of some $K^{(p),r}$ when p and r vary.

Let us pass to infinite cyclic cyclotomic extension. Define $K_0^{(p),\infty} := \bigcup_{r \geq 1} \mathbb{Q}(\zeta_{p^r})$ where the ζ_{p^r} 's are primitive p^r -roots of 1. The above isomorphism of finite groups induces an isomorphism of topological groups

$$\mathbb{Z}_p^\times \xrightarrow{\sim} \text{Gal}(K_0^{(p),\infty}/\mathbb{Q})$$

and we have a decomposition $\mathbb{Z}_p^\times \simeq \Delta_p \times \mathbb{Z}_p$ where Δ_p is as before. Define $K^{(p),\infty} := (K_0^{(p),\infty})^{\Delta_p}$ so that $\text{Gal}(K^{(p),\infty}/\mathbb{Q}_p) \simeq \mathbb{Z}_p$. The infinite cyclic cyclotomic extension of $\mathbb{Q}$ is the composite:

$$\mathbb{Q}^c := K^{(2),\infty} \cdot K^{(3),\infty} \cdot K^{(5),\infty} \cdot \dots \cdot K^{(p),\infty} \cdot \dots$$

with Galois group $\prod_p \mathbb{Z}_p \simeq \widehat{\mathbb{Z}}$.

If we have a finite extension K of $\mathbb{Q}$ then $K \cdot \mathbb{Q}^c$ is a Galois extension of K with Galois group isomorphic to a subgroup of finite index in $\widehat{\mathbb{Z}}$. Such a subgroup is open (note that this is not true if the Galois group is not $\widehat{\mathbb{Z}}$, we are using here that $\widehat{\mathbb{Z}}$ is topologically finitely generated) so it is isomorphic to some $n\widehat{\mathbb{Z}}$ for $n \geq 1$. Hence it is in fact isomorphic to $\widehat{\mathbb{Z}}$ itself and we obtain $\text{Gal}(K \cdot \mathbb{Q}^c/K) \simeq \widehat{\mathbb{Z}}$. We choose such an isomorphism and we consider K_m the extension of K corresponding to $m\widehat{\mathbb{Z}}$. Then we have that K_m/K is cyclic of order m and it is contained in a composite of some $K(\zeta)$'s where the ζ 's are primitive roots of 1. A cyclic cyclotomic extension of K is the composite of such K_m 's.

We have the following result:

Lemma 7.2. *Let K be a number field and let S be a finite set of primes in K . Then for any integer $m > 0$ there exists a cyclic cyclotomic extension L/K such that for all $v \in S$, the integer m divides the degree $[L^v : K_v]$.*

Proof. See Exercise Sheet 6. □

We derive from the lemma the following result:

Proposition 7.3. *Let K be a number field and β an element in $\text{Br}(K)$. Then there exist a cyclic cyclotomic extension L/K such that the image of β by the restriction map $\text{Res} : \text{Br}(K) \rightarrow \text{Br}(L)$ is zero.*

Proof. From Theorem 7.1, we know that there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Br}(L/K) & \longrightarrow & \text{Br}(K) & \longrightarrow & \text{Br}(L) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \bigoplus_{v \text{ place of } K} \text{Br}(L^v/K_v) & \longrightarrow & \bigoplus_{v \text{ place of } K} \text{Br}(K_v) & \longrightarrow & \bigoplus_{w \text{ place of } L} \text{Br}(L_w)
 \end{array}$$

Hence, to show that the image of β is zero in $\text{Br}(L)$ for some extension L , it suffices to show that for any place v of K , the image of β in $\text{Br}(K_v)$ maps to zero in $\text{Br}(L_w)$ for $w|v$. Using the invariant map, it suffices to show that $\text{inv}_w(\text{Res}(\beta))$ is zero in $\mathbf{Q}/\mathbf{Z}$ for all w place of L . But we have

$$\text{inv}_w(\text{Res}(\beta)) = [L_w : K_v] \cdot \text{inv}_v(\beta).$$

So to prove the proposition, it suffices to find a cyclic cyclotomic extension L of K such that for any place v and w dividing v , we have that $[L_w : K_v] \cdot \text{inv}_v(\beta)$ is in $\mathbf{Z}$. But the images of β in the groups $\text{Br}(K_v)$ are zero for almost all v . Let S be the finite set of the places v of K such that $\text{inv}_v(\beta)$ is non-zero. We can find m an integer such that $m \cdot \text{inv}_v(\beta)$ is zero in $\mathbf{Q}/\mathbf{Z}$ for all v (take m to be a common denominator of the $\text{inv}_v(\beta)$ for v in S). Using Lemma 7.2 for such an S and m , we obtain the desired L . □

Remark 7.4. In particular it follows from Proposition 7.3 that $\text{Br}(K \cdot \mathbf{Q}^c/K) \simeq \text{Br}(K)$.

7.2 The fundamental exact sequence

Let L/K be a finite extension of number fields. We define maps (note that the sum is well-defined since almost all β_v are zero):

$$\Sigma : \begin{cases} \bigoplus_v \text{Br}(L^v/K_v) & \rightarrow \mathbf{Q}/\mathbf{Z} \\ (\beta_v)_v & \mapsto \sum_v \text{inv}_v(\beta_v) \end{cases} \quad \text{and} \quad \Sigma : \begin{cases} \bigoplus_v \text{Br}(K_v) & \rightarrow \mathbf{Q}/\mathbf{Z} \\ (\beta_v)_v & \mapsto \sum_v \text{inv}_v(\beta_v) \end{cases}$$

where for any place v , the maps inv_v are the isomorphisms $\text{Br}(L^v/K_v) \xrightarrow{\sim} \frac{1}{n_v} \mathbf{Z}/\mathbf{Z}$ for $n_v := [L^v : K_v]$ and $\text{Br}(K_v) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$ if v is non-archimedean or $\text{Br}(K_v) \xrightarrow{\sim} \frac{1}{2} \mathbf{Z}/\mathbf{Z}$ if v is

real. In particular, note that the image of Σ in the first case is the cyclic subgroup of $\mathbf{Q}/\mathbf{Z}$ of order $n_0 := \text{lcm}(n_v, v \text{ place of } K)$.

Later, we will prove the following result (see Theorem 8.1):

Proposition 7.5. *Let L/K be a finite Galois extension of number fields. Then the sequence*

$$0 \rightarrow \text{Br}(L/K) \rightarrow \bigoplus_v \text{Br}(L^v/K_v) \xrightarrow{\Sigma} \mathbf{Q}/\mathbf{Z}$$

is a complex.

Our goal in this section is to prove the result from Theorem 7.6 below, often called *fundamental exact sequence of global class field theory*.

Theorem 7.6. *Let K be a number field. Then there is an exact sequence:*

$$0 \rightarrow \text{Br}(K) \rightarrow \bigoplus_v \text{Br}(K_v) \xrightarrow{\Sigma} \mathbf{Q}/\mathbf{Z} \rightarrow 0.$$

Proof. Let L/K be a finite Galois extension of order n . Recall that the injective map $\text{Br}(L/K) \rightarrow \bigoplus_v \text{Br}(L^v/K_v)$ comes from the exact sequence $0 \rightarrow L^\times \rightarrow \mathbb{I}_L \rightarrow \mathbb{C}_L \rightarrow 0$ and so we have the following commutative diagram where the first row is exact:

$$(7.2.1) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \text{Br}(L/K) & \longrightarrow & \bigoplus_v \text{Br}(L^v/K_v) & \longrightarrow & H^2(\text{Gal}(L/K), \mathbb{C}_L) \\ & & \parallel & & \parallel & & \downarrow \\ 0 & \longrightarrow & \text{Br}(L/K) & \longrightarrow & \bigoplus_v \text{Br}(L^v/K_v) & \longrightarrow & \mathbf{Q}/\mathbf{Z}. \end{array}$$

The dotted arrow is obtained by factorization, using the fact that the two rows are complexes (Proposition 7.5). Let us denote by $H^2(\mathbb{C}_L)'$ the image of the map $\bigoplus_v \text{Br}(L^v/K_v) \rightarrow H^2(\text{Gal}(L/K), \mathbb{C}_L)$. We write n_0 for the lcm of the $[L^v : K_v]$, v place of K . The above diagram induces a surjective morphism

$$(7.2.2) \quad H^2(\mathbb{C}_L)' \rightarrow \frac{1}{n_0} \mathbf{Z}/\mathbf{Z}.$$

In general $n \neq n_0$ but in the cyclic case we have:

Lemma 7.7. *Let L/K be a finite cyclic extension and let n_0 denote the lcm of the $[L^v : K_v]$, v place of K . Then $n_0 = [L : K]$.*

Proof of the lemma. Consider S a finite set of places of K such that S contains S_∞ and all the primes of K that ramify in L . We know from Proposition 5.24 that the Artin map

$$\psi_{L/K}^S : \begin{cases} I_K^S & \rightarrow \text{Gal}(L/K) \\ \mathfrak{p} & \mapsto (\mathfrak{p}, L/K) \end{cases}$$

is surjective. But if v is not in S , then $(\mathfrak{p}_v, L/K)$ defines an element of the cyclic group $\text{Gal}(L/K)$ and it has of order n_v (which is equal to the inertia degree f_v since v is unramified). So $\psi_{L/K}^S(I_K^S) \subset \text{Gal}(L/K)$ has order n_0 . By surjectivity, we obtain $n_0 = [L : K]$. $\square$

Let us come back to the proof of the theorem. For K a number field, consider the infinite cyclotomic extension $K^c := K \cdot \mathbf{Q}^c$ from before. It is the colimit of the K_m 's where K_m/K is cyclic of order m . From the above lemma, we know that $m = m_0$ where m_0 is the lcm of the degrees $[K_{m,w} : K_v]$ for $w|v$. We also have by Theorem 5.18 and Theorem 6.1 that $H^2(\text{Gal}(K_m/K), \mathbb{C}_{K_m})$ has order m . Hence (7.2.2) gives us a surjective morphism:

$$H^2(\mathbb{C}_{K_m})' \rightarrow \frac{1}{m} \mathbf{Z}/\mathbf{Z}.$$

But the order of $H^2(\mathbb{C}_{K_m})'$ is less than the order of $H^2(\text{Gal}(K_m/K), \mathbb{C}_{K_m})$ which is m . So the above map is an isomorphism and $H^2(\mathbb{C}_{K_m})' = H^2(\text{Gal}(K_m/K), \mathbb{C}_{K_m})$. Hence, the bottom row in diagram (7.2.1) induces a short exact sequence:

$$0 \rightarrow \text{Br}(K_m/K) \rightarrow \bigoplus_v \text{Br}(K_m^v/K_v) \xrightarrow{\Sigma} \frac{1}{m} \mathbf{Z}/\mathbf{Z} \rightarrow 0.$$

Taking the colimit over m , we obtain an exact sequence:

$$0 \rightarrow \text{Br}(K^c/K) \rightarrow \bigoplus_v \text{Br}((K^c)^v/K_v) \xrightarrow{\Sigma} \mathbf{Q}/\mathbf{Z} \rightarrow 0.$$

By Remark 7.4, we know that $\text{Br}(K^c/K) \simeq \text{Br}(K)$. To conclude it remains to check that we have isomorphisms $\text{Br}((K^c)^v/K_v) \simeq \text{Br}(K_v)$ for all v . This follows from Lemma 7.2: for any place v and any integer r , we can find m such that r divides $m_v := [K_m^v : K_v]$. This means that the degrees m_v goes to infinity when m goes to infinity. In particular, taking the colimit of $\text{Br}((K_m^v/K_v) \simeq \frac{1}{m_v} \mathbf{Z}/\mathbf{Z}$ gives $\text{Br}((K^c)^v/K_v) \simeq \mathbf{Q}/\mathbf{Z}$. Hence, $\text{Br}((K^c)^v/K_v) \simeq \text{Br}(K_v)$, as wanted. This concludes the proof of the theorem. $\square$

Remark 7.8. Lemma 7.7 is false in general (see Exercise Sheet 6).

As a consequence of the theorem, we obtain:

Corollary 7.9. *Let L/K be a finite Galois extension of number fields. Then the sequence:*

$$0 \rightarrow \text{Br}(L/K) \rightarrow \bigoplus_v \text{Br}(L^v/K_v) \xrightarrow{\Sigma} \frac{1}{n_0} \mathbf{Z}/\mathbf{Z} \rightarrow 0,$$

where n_0 is the lcm of the $[L^v : K_v]$, is exact.

Proof. This follows from the snake lemma applied to the map of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Br}(K) & \longrightarrow & \bigoplus_v \text{Br}(K_v) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow n_0 \\ 0 & \longrightarrow & \text{Br}(L) & \longrightarrow & \bigoplus_w \text{Br}(L_w) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \longrightarrow 0. \end{array}$$

□

7.3 The fundamental class

Let K be a number field. We have seen that if K'/K is a cyclic extension then there is an invariant map:

$$\text{inv}_{K'/K} : H^2(\text{Gal}(K'/K), \mathbb{C}_{K'}) \xrightarrow{\sim} \frac{1}{[K' : K]} \mathbf{Z}/\mathbf{Z}.$$

In this section, if L/K is a finite Galois extension we will write $\Sigma_{L/K}$ the map $\bigoplus_v \text{Br}(L^v/K_v) \rightarrow \mathbf{Q}/\mathbf{Z}$ from before. It has image contained in $\frac{1}{n_0} \mathbf{Z}/\mathbf{Z}$ where n_0 is the lcm of $[L^v : K_v]$. In order to construct an invariant map for L/K , we will need the following key result:

Theorem 7.10. *Let L/K be a finite Galois extension and L'/K a cyclic extension such that $[L : K] = [L' : K]$. Then*

$$H^2(\text{Gal}(L'/K, \mathbb{C}_{L'}) = H^2(\text{Gal}(L/K, \mathbb{C}_L),$$

as subsets of $H^2(\text{Gal}(\overline{K}/K, \mathbb{C}_{\overline{K}})$ (see Exercise Sheet 5).

Proof. To simplify the notations, we will set

$$H^2(L'/K) := H^2(\text{Gal}(L'/K, \mathbb{C}_{L'}) \text{ and } H^2(L/K) := H^2(\text{Gal}(L/K, \mathbb{C}_L).$$

We first show that $H^2(L'/K) \subset H^2(L/K)$. Define $N := L \cdot L'$. Since L'/K is cyclic, N/L is also cyclic. We have the following inflation-restriction exact sequences:

$$\begin{aligned} 0 \rightarrow H^2(L/K) &\xrightarrow{\text{inf}_{N/L}} H^2(N/K) \xrightarrow{\text{res}_{N/L}} H^2(N/L) \\ 0 \rightarrow H^2(L'/K) &\xrightarrow{\text{inf}_{N/L'}} H^2(N/K) \xrightarrow{\text{res}_{N/L'}} H^2(N/L'). \end{aligned}$$

Take α in $H^2(L'/K)$. We want to show that $\text{inf}_{N/L'}(\alpha)$ comes from an element of $H^2(L/K)$, i.e. that $\text{res}_{N/L}(\text{inf}_{N/L'}(\alpha))$ is zero. But since L'/K is cyclic, we know that the map

$$j : \bigoplus_v \text{Br}(L'^v/K_v) \rightarrow H^2(L'/K)$$

is surjective, hence there exists β in $\bigoplus_v \text{Br}(L'^v/K_v)$ such that $j(\beta) = \alpha$. We also have commutative diagrams:

$$\begin{array}{ccc} \bigoplus_v \text{Br}((L')^v/K_v) & \xrightarrow{j} & H^2(L'/K) \\ \inf_{N/L'} \downarrow & & \downarrow \inf_{N/L'} \\ \bigoplus_v \text{Br}(N^v/K_v) & \xrightarrow{j} & H^2(N/K) \end{array} \quad \text{and} \quad \begin{array}{ccc} \bigoplus_v \text{Br}(N^v/K_v) & \xrightarrow{j} & H^2(N/K) \\ \text{res}_{N/L} \downarrow & & \downarrow \text{res}_{N/L} \\ \bigoplus_w \text{Br}(N^w/L_w) & \xrightarrow{j} & H^2(N/L). \end{array}$$

So, in order to show that $\text{res}_{N/L}(\inf_{N/L'}(j(\beta)))$ is zero it suffices to show that $j(\text{res}_{N/L}(\inf_{N/L'}(\beta)))$ is zero in $H^2(N/L)$. But N/L is cyclic so we have a commutative diagram

$$\begin{array}{ccc} \bigoplus_w \text{Br}(N^w/L_w) & \xrightarrow{\Sigma_{N/L}} & \frac{1}{[N:L]} \mathbf{Z}/\mathbf{Z} \\ j \downarrow & \nearrow \sim & \\ H^2(N/L) & & \end{array}$$

and we see that it suffices to check that $\Sigma_{N/L}(\text{res}_{N/L}(\inf_{N/L'}(\beta)))$ is zero.

But we also have commutative diagrams:

$$\begin{array}{ccc} \bigoplus_v \text{Br}((L')^v/K_v) & \xrightarrow{\Sigma_{L'/K}} & \mathbf{Q}/\mathbf{Z} \\ \inf_{N/L'} \downarrow & & \downarrow \\ \bigoplus_v \text{Br}(N^v/K_v) & \xrightarrow{\Sigma_{N/K}} & \mathbf{Q}/\mathbf{Z} \end{array} \quad \text{and} \quad \begin{array}{ccc} \bigoplus_v \text{Br}(N^v/K_v) & \xrightarrow{\Sigma_{N/K}} & \mathbf{Q}/\mathbf{Z} \\ \text{res}_{N/L} \downarrow & & \downarrow [L:K] \\ \bigoplus_w \text{Br}(N^w/L_w) & \xrightarrow{\Sigma_{N/L}} & \mathbf{Q}/\mathbf{Z}, \end{array}$$

so we obtain

$$\Sigma_{N/L}(\text{res}_{N/L}(\inf_{N/L'}(\beta))) = [L : K] \Sigma_{N/K}(\inf_{N/L'}(\beta)) = [L' : K] \Sigma_{L'/K}(\beta).$$

Since L'/K is cyclic we know that $[L' : K]$ kills the image of $\Sigma_{L'/K}$, and this gives

$$\Sigma_{N/L}(\text{res}_{N/L}(\inf_{N/L'}(\beta))) = 0,$$

as wanted. We have proved

$$H^2(L'/K) \subset H^2(L/K).$$

The group on the left side is a cyclic group of order $[L' : K] = [L : K]$. By the second inequality, the one on the right side has order $\leq [L : K]$ and we obtain that the inclusion is an equality. $\square$

As a direct consequence (see Exercise Sheet 5), we obtain:

Corollary 7.11. *Let K be a number field. Then*

$$H^2(\text{Gal}(\overline{K}/K), \mathbb{C}_{\overline{K}}) = \text{colim}_{L/K \text{ cyclic}} H^2(\text{Gal}(L/K), \mathbb{C}_L).$$

Hence, we obtain an invariant map

$$(7.3.1) \quad \text{inv}_K : H^2(\text{Gal}(\overline{K}/K), \mathbb{C}_{\overline{K}}) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}.$$

In particular, for L/K a finite Galois extension, we have

$$(7.3.2) \quad \text{inv}_{L/K} : H^2(\text{Gal}(L/K), \mathbb{C}_L) \xrightarrow{\sim} \frac{1}{[L:K]} \mathbf{Z}/\mathbf{Z}.$$

Taking the limit, this yields

$$(7.3.3) \quad \text{inv}_K : H^2(\text{Gal}(\overline{K}/K), \mathbb{C}_{\overline{K}}) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}.$$

We obtain:

Theorem 7.12. *Let L/K be a finite Galois extension of number fields. Then $H^2(\text{Gal}(L/K), \mathbb{C}_L)$ is cyclic of order $[L:K]$ and we have a canonical generator $u_{L/K}$ in $H^2(\text{Gal}(L/K), \mathbb{C}_L)$ called the fundamental class.*

Proof. This follows immediately from (7.3.2), we define $u_{L/K}$ as the unique element in $H^2(\text{Gal}(L/K), \mathbb{C}_L)$ such that $\text{inv}_{L/K}(u_{L/K}) = \frac{1}{n}$ in $\mathbf{Q}/\mathbf{Z}$. $\square$

We also have:

Lemma 7.13. *Let $M/L/K$ be a tower of finite Galois extensions. Then,*

$$\begin{aligned} \text{Res}(u_{M/K}) &= u_{M/L} \\ \text{Inf}(u_{L/K}) &= [L:K]u_{M/K}. \end{aligned}$$

Proof. This follows from the definition of the fundamental classes and the commutative diagram with exact row (using again that $H^1(\text{Gal}(L/K), \mathbb{C}_L)$ is trivial by Theorem 6.1):

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(\text{Gal}(L/K), \mathbb{C}_L) & \longrightarrow & H^2(\text{Gal}(M/K), \mathbb{C}_M) & \longrightarrow & H^2(\text{Gal}(M/L), \mathbb{C}_M) \\ & & \downarrow \text{inv}_{L/K} \sim & & \downarrow \text{inv}_{M/K} \sim & & \downarrow \sim \text{inv}_{M/L} \\ 0 & \longrightarrow & \frac{1}{[L:K]} \mathbf{Z}/\mathbf{Z} & \longrightarrow & \frac{1}{[M:K]} \mathbf{Z}/\mathbf{Z} & \xrightarrow{[L:K]} & \frac{1}{[M:L]} \mathbf{Z}/\mathbf{Z} \end{array}$$

$\square$

It follows from Lemma 7.13 that we can apply Tate's theorem (Theorem 5.1) to obtain an isomorphism:

$$\text{Gal}(L/K)^{\text{ab}} \xrightarrow{\sim} \mathbb{C}_K / \text{Norm}_{L/K}(\mathbb{C}_L).$$

Using the fact that the fundamental class $u_{L/K}$ is built from local fundamental classes and that the global Artin map is compatible with the local ones, we can show that the above isomorphism defines an inverse to the global Artin map.

8 Main theorems of Global CFT

In this section we complete the proofs of the global reciprocity law and the existence theorem.

8.1 Reciprocity Law

We start by proving the following theorem:

Theorem 8.1. (1) Let L/K be a finite abelian extension of number fields with Galois group G then the subgroup of principal idèles $K^\times \subset \mathbb{I}_K$ is contained in the kernel of the Artin map

$$\Phi_{L/K} : \begin{cases} \mathbb{I}_K & \rightarrow G \\ (a_v)_v & \mapsto \prod_v \Phi_{L_v/K_v}(a_v). \end{cases}$$

(2) Let L/K be a finite Galois extension of number fields with Galois group G and β a class in $H^2(G, L^\times)$. Then $\sum_v \text{inv}_v(\beta)$ is zero in $\mathbb{Q}/\mathbb{Z}$.

The theorem will follow from the following three lemmas:

Lemma 8.2. Let L/K be a finite abelian extension of number fields.

(1) If statement (2) in Theorem 8.1 is true for L/K then statement (1) is true for L/K .

(2) If we assume moreover that L/K is cyclic, then statement (1) for L/K implies statement (2) for L/K .

Proof. Let L/K be a finite Galois extension of number fields with Galois group G . Assume that for all β in $H^2(G, L^\times)$ then $\Sigma(\beta) = 0$ in $\mathbb{Q}/\mathbb{Z}$. Let x be an element of the principal idèles $K^\times$. We want to show that $\phi_{L/K}(x)$ is zero in $\text{Gal}(L/K)$. To do that, it suffices to show that $\chi(\phi_{L/K}(x)) = 0$ for all character χ in $\text{Hom}(G, \mathbb{Q}/\mathbb{Z})$. So let χ be such a character. Since we have an isomorphism $\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq H^1(G, \mathbb{Q}/\mathbb{Z})$, the image of χ by the edge map coming from the short exact sequence

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

defines an element δ_χ in $H^2(G, \mathbb{Z})$. Since $K^\times \simeq H^0(G, L^\times)$ (respectively $\mathbb{I}_K \simeq H^0(G, \mathbb{I}_L)$), taking the cup product with δ_χ defines a map from $K^\times$ to $H^2(G, L^\times)$ (respectively $\mathbb{I}_K$ to $H^2(G, \mathbb{I}_L)$). We will prove that the following diagram commutes:

$$\begin{array}{ccccc} K^\times & \xrightarrow{\quad} & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G \\ \cup \delta_\chi \downarrow & & \downarrow \cup \delta_\chi & & \downarrow \chi \\ H^2(G, L^\times) & \longrightarrow & H^2(G, \mathbb{I}_L) & \xrightarrow{\Sigma} & \mathbb{Q}/\mathbb{Z} \end{array}$$

The commutativity of the left square is obvious. The fact that the right square commutes can be deduced from the analogous result in the local case, i.e. if v is a place of K and χ_v in $\text{Hom}(G^v, \mathbf{Q}/\mathbf{Z})$ a character of the decomposition subgroup G^v then we have a commutative diagram:

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_{L^v/K_v}} & \text{Gal}(L^v/K_v) \\ \cup \delta_{\chi_v} \downarrow & & \downarrow \chi_v \\ H^2(G^v, K_v^\times) & \xrightarrow{\text{inv}_v} & \mathbf{Q}/\mathbf{Z}. \end{array}$$

This gives us

$$\chi(\phi_{L/K}(x)) = \Sigma(x \cup \delta_\chi) = 0$$

since we have assumed that statement (2) is true for L/K . This shows that $\phi_{L/K}(x) = 0$ for all principal idèle x .

For (2), let us assume that L/K is cyclic and that the Artin map $\phi_{L/K}$ is trivial on the principal idèles. Since G is cyclic, we can write it as $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ for some n and we have an injective character $\chi : G \rightarrow \mathbf{Q}/\mathbf{Z}$ given by the inclusion. Moreover, for a cyclic group we know that the cup product $-\cup \delta_\chi$ induces an isomorphism between the H^0 -group and the H^2 -group. The diagram above becomes:

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G \\ \cup \delta_\chi \downarrow \sim & & \sim \downarrow \cup \delta_\chi & & \downarrow \chi \\ H^2(G, L^\times) & \longrightarrow & H^2(G, \mathbb{I}_L) & \xrightarrow{\Sigma} & \mathbf{Q}/\mathbf{Z} \end{array}$$

A simple diagram chase show that if the map given by the top row is trivial then the map given by the bottom one is also trivial, as wanted. $\square$

Lemma 8.3. *Let L/K be a finite abelian extension of number fields. Then,*

- (1) *If statement (1) in Theorem 8.1 is satisfied for L/K , it is also satisfied for any subextension.*
- (2) *Let K' be a finite abelian extension of K . If statement (1) in Theorem 8.1 is satisfied for L/K , it is also satisfied for the composite $L \cdot K'/K$.*

Proof. Let us first prove (1). Let K' be an intermediate extension $K \subset K' \subset L$. We have a commutative diagram:

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \text{Gal}(L/K) \\ & \searrow \phi_{K'/K} & \downarrow \text{Res} \\ & & \text{Gal}(K'/K) \end{array}$$

so if $K^\times$ is in the kernel of $\phi_{L/K}$, it is in the kernel of $\phi_{K'/K}$. This proves (1).

For the second point, consider K' a finite abelian extension of K and write $L' := L \cdot K'$. We know that locally, for v a place of K and w a place of K' dividing v , we have a commutative

diagram:

$$\begin{array}{ccc} (K'_w)^\times & \xrightarrow{\phi_w} & \text{Gal}((L')^w/K'_w) \\ \text{Norm} \downarrow & & \downarrow \\ (K_v)^\times & \xrightarrow{\phi_v} & \text{Gal}(L^v/K_v). \end{array}$$

Hence, we obtain a commutative diagram

$$\begin{array}{ccccc} K' & \longrightarrow & \mathbb{I}_{K'} & \xrightarrow{\phi_{L'/K'}} & \text{Gal}(L'/K') \\ \text{Norm}_{K'/K} \downarrow & & \text{Norm}_{K'/K} \downarrow & & \downarrow \\ K & \longrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \text{Gal}(L/K). \end{array}$$

In particular, we see that if the image of K in $\text{Gal}(L/K)$ is trivial then the image of K' in $\text{Gal}(L'/K')$ is trivial. $\square$

Lemma 8.4. *If statement (2) of Theorem 8.1 is satisfied for any cyclic cyclotomic extensions then it is satisfied for all finite Galois extensions.*

Proof. Let L/K be a finite Galois extension. Let β be in $\text{Br}(L/K)$. We can see β as an element of $\text{Br}(K)$. We want to show that $\sum_v \text{inv}_v(\beta)$ is zero. From Proposition 7.3, we know that there exists a cyclic cyclotomic extension M/K such that the image of β in $\text{Br}(M)$ is zero. This means that β comes from an element of $\text{Br}(M/K)$. But by hypothesis, statement (2) of Theorem 8.1 is satisfied for M/K . It follows that $\Sigma(\beta) = 0$. $\square$

We can now prove Theorem 8.1.

Proof of Theorem 8.1. Assume that we know that Theorem 8.1(1) is true for extensions of the form $\mathbf{Q}(\zeta)/\mathbf{Q}$ with ζ a primitive root of 1. Then By Lemma 8.3(2), the statement (1) of the theorem is also true for any extension of the form $K(\zeta)/K$ where K is a number field. In particular, it is true for cyclic cyclotomic extensions L/K . By Lemma 8.2(2), this implies that Theorem 8.1(2) is true for cyclic cyclotomic extension. By Lemma 8.4, we obtain that Theorem 8.1(2) is true for any finite Galois extension L/K . From Lemma 8.2(1), this also proves that Theorem 8.1(1) is true for all finite Galois extension L/K . Hence, it suffices to show Theorem 8.1(1) for $\mathbf{Q}(\zeta)/\mathbf{Q}$.

Assume $\zeta = \zeta_m$ is a primitive m -th root of 1. Then $(\mathbf{Z}/m\mathbf{Z})^\times \xrightarrow{\sim} \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ and if n is in $(\mathbf{Z}/m\mathbf{Z})^\times$ we write $[n]$ its image by this isomorphism (i.e. $[n](\zeta) = \zeta^n$). We want to compute the image of $\mathbf{Q}^\times$ via the Artin map $\phi_{\mathbf{Q}(\zeta)/\mathbf{Q}} : \mathbb{I}_{\mathbf{Q}} \rightarrow \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$. Let x be an element in $\mathbf{Q}$. To prove that $\phi(x)$ is trivial on $\mathbf{Q}(\zeta_m)$, it suffices to show that the restrictions $\phi(x)|_{\mathbf{Q}(\zeta_{\ell^r})}$ are trivial for the prime numbers ℓ dividing m . Hence we can assume $m = \ell^r$. We need to describe $\phi_v(x)$ where ϕ_v is the local Artin map for $v \in \{\infty, p \text{ prime number}\}$.

(i) If $v = \infty$, then ϕ_∞ send $x_\infty \in \mathbf{R}^\times / \text{Norm}(\mathbf{C}^\times) \simeq \{-1, 1\}$ to $[\text{sign}(x_\infty)]$ in $\text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$.

(ii) If $v = p$ with $p \neq \ell$, then p is unramified in $\mathbf{Q}(\zeta_m)$, so if we write $x_p = u_p p^s$ with u in $\mathbf{Z}_p^\times$ and $s \geq 0$, then by construction of the local Artin map $\phi_p(x_p) = [p^s]$.

(iii) If $v = \ell$ then ℓ is totally ramified in $\mathbf{Q}(\zeta)$ so if we write $x_\ell = u_\ell \ell^s$ with u in $\mathbf{Z}_\ell^\times$ and $s \geq 0$, then we have $\phi_\ell(x_\ell) = [u_\ell^{-1}]$.

Considering the p -adic (and ℓ -adic) expansions of the units u_p and u_ℓ , we see that it suffices to prove that $\prod_v \phi_v(x_v)$ is trivial for x in $\{-1, q \text{ prime number}\}$. But from the above description we get

$$\begin{aligned}\phi_p(-1) &= \begin{cases} [-1] & \text{if } p = \infty, \\ [-1] & \text{if } p = \ell, \\ [1] & \text{if } p \neq \ell, \infty. \end{cases} \\ \phi_p(\ell) &= \begin{cases} [1] & \text{if } p \neq \ell, \\ [1] & \text{if } p = \ell. \end{cases} \\ \phi_p(q) &= \begin{cases} [q] & \text{if } p = q, \\ [q^{-1}] & \text{if } p = \ell, \\ [1] & \text{if } p \neq \ell, q, \end{cases} \quad \text{where } q \neq \ell,\end{aligned}$$

and we see that in any case,

$$\prod_v \phi_v(x) = 1.$$

This proves that the Artin map is trivial on $\mathbf{Q}(\zeta)^\times$, as wanted. $\square$

We deduce from it the proof of the reciprocity law.

Proof of Global Reciprocity Law (Theorem 4.17). Let L/K be a finite abelian extension of number fields and consider $\phi_{L/K} : \mathbb{I}_K \rightarrow \text{Gal}(L/K)$ the associated Artin map. Recall that we want to prove that $\phi_{L/K}(K^\times)$ is trivial and that it induces an isomorphism

$$\phi_{L/K} : \mathbb{I}_K / K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L) \xrightarrow{\sim} \text{Gal}(L/K).$$

The first statement is exactly the first point of Theorem 8.1. Let us check the second statement. From Lemma 4.15, we know that $\text{Nm}_{L/K}(\mathbb{I}_L)$ is contained in the kernel of $\phi_{L/K}$, hence the map is well-defined on $\mathbb{I}_K / K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L)$. We have seen as a consequence of the first inequality Corollary 5.23 that the Artin map is surjective. Moreover, the second inequality (Theorem 6.1(1)) states that the order of $\mathbb{I}_K / K^\times \cdot \text{Nm}_{L/K}(\mathbb{I}_L)$ is less than the order of $\text{Gal}(L/K)$, hence the map is an isomorphism. $\square$

8.2 The norm limitation theorem

As a consequence of reciprocity law, we obtain the following result:

Theorem 8.5. *Let L be any finite extension of K and let M be the maximal subextension of L such that M/K is an abelian Galois extension. Then we have*

$$\text{Norm}_{L/K}(\mathbb{C}_L) = \text{Norm}_{M/K}(\mathbb{C}_M).$$

Proof. We can find K'/K a Galois extension such that $L \subset K'$. Let us set $G := \text{Gal}(K'/K)$ and $H := \text{Gal}(K'/L)$. From Tate's theorem, we know that there is a commutative diagram:

$$\begin{array}{ccc} \hat{H}^{-2}(H, \mathbf{Z}) & \xrightarrow{\sim} & \hat{H}^0(H, \mathbb{C}_{K'}) \\ \text{Cor} \downarrow & & \downarrow \text{Cor} \\ \hat{H}^{-2}(G, \mathbf{Z}) & \xrightarrow{\sim} & \hat{H}^0(G, \mathbb{C}_{K'}) \end{array}$$

where the top horizontal arrow is the cup product with the fundamental class $\beta \mapsto \beta \cup u_{K'/L}$ and the bottom one $\beta \mapsto \beta \cup u_{K'/K}$. This diagram can be identified with the following one:

$$\begin{array}{ccc} H^{\text{ab}} & \xrightarrow{\sim} & \mathbb{C}_L / \text{Norm}_{K'/L}(\mathbb{C}_{K'}) \\ \downarrow & & \downarrow \text{Norm}_{L/K} \\ G^{\text{ab}} & \xrightarrow{\sim} & \mathbb{C}_K / \text{Norm}_{K'/K}(\mathbb{C}_{K'}). \end{array}$$

We obtain

$$\text{CoKer}(H^{\text{ab}} \rightarrow G^{\text{ab}}) \simeq \mathbb{C}_K / \text{Norm}_{L/K}(\mathbb{C}_L).$$

But by definition of M , we also have

$$\text{CoKer}(H^{\text{ab}} \rightarrow G^{\text{ab}}) \simeq \text{Gal}(M/K).$$

From Global Reciprocity Law, we have an isomorphism $\text{Gal}(M/K) \simeq \mathbb{C}_K / \text{Norm}_{M/K}(\mathbb{C}_M)$. We have proved

$$\mathbb{C}_K / \text{Norm}_{L/K}(\mathbb{C}_L) \simeq \mathbb{C}_K / \text{Norm}_{M/K}(\mathbb{C}_M).$$

Since we also have

$$\text{Norm}_{L/K}(\mathbb{C}_L) = \text{Norm}_{M/K}(\text{Norm}_{L/K}(\mathbb{C}_L)) \subset \text{Norm}_{M/K}(\mathbb{C}_M),$$

we obtain $\text{Norm}_{L/K}(\mathbb{C}_L) = \text{Norm}_{M/K}(\mathbb{C}_M)$.

□

8.3 Existence Theorem

We will need the following lemma:

Lemma 8.6. *Let K be a number field.*

(1) *If $U \subset \mathbb{C}_K$ is a norm group, then any group $V \subset \mathbb{C}_K$ such that $U \subset V$ is a norm group.*

(2) *If U is an open subgroup of finite index of $\mathbb{C}_K$ and there exists a finite extension L/K such that $\text{Norm}_{L/K}^{-1}(U) \subset \mathbb{C}_L$ is a norm group, then U is a norm group.*

Proof. Let us first prove (1). Assume that there exists L/K finite such that $U = \text{Norm}_{L/K}(\mathbb{C}_L)$ and consider $U \subset V$ containing it. We want to show that V is a norm group. From the Global Reciprocity Law (Theorem 4.17), we know that the Artin map induces an isomorphism

$$\phi_{L/K} : \mathbb{C}_K/U = \mathbb{C}_K/\text{Norm}_{L/K}(\mathbb{C}_L) \xrightarrow{\sim} \text{Gal}(L/K).$$

The image $\phi_{L/K}(V)$ of V defines a subgroup of $\text{Gal}(L/K)$, so it corresponds to some extension $K \subset M \subset L$. Since M is fixed by $\phi_{L/K}(V)$, the Artin map induces an isomorphism

$$\mathbb{C}_K/V \xrightarrow{\sim} \text{Gal}(M/K).$$

But by Global Reciprocity Law (Theorem 4.17), the kernel of the Artin map $\phi_K : \mathbb{C}_K \rightarrow \text{Gal}(M/K)$ is $\text{Norm}_{M/K}(\mathbb{C}_M)$, hence $V = \text{Norm}_{M/K}(\mathbb{C}_M)$. This concludes the proof of (1).

Let us now prove the second point. We write $V := \text{Norm}_{L/K}^{-1}(U) \subset \mathbb{C}_L$. By hypothesis, there exists M_0/L a finite abelian extension such that $V = \text{Norm}_{M_0/L}(\mathbb{C}_{M_0})$. Consider M the maximal abelian subextension of M_0/K . By Theorem 8.5, we know that $\text{Norm}_{M/K}(\mathbb{C}_M) = \text{Norm}_{M_0/K}(\mathbb{C}_{M_0})$ and by composition, we have

$$\text{Norm}_{M_0/K}(\mathbb{C}_{M_0}) = \text{Norm}_{L/K}(\text{Norm}_{M_0/L}(\mathbb{C}_{M_0})) = \text{Norm}_{L/K}(V) \subset U$$

and the result follows from point (1). $\square$

We first prove the theorem in a particular case:

Theorem 8.7. *Let K be a number field that contains a primitive p -th root of 1 and let V be an open subgroup of finite index of $\mathbb{C}_K$ such that $\mathbb{C}_K/V$ is a finite group killed by p . Then V is a norm group, i.e. there exists an abelian extension M/K of exponent p such that $V = \text{Norm}_{M/K}(\mathbb{C}_M)$.*

Proof. Let S be a finite set of primes such that S contains S_∞ , the places that divide p and a set of generators of the ideal class group. Let $M := K(U(S)^{\frac{1}{p}})$ the Kummer extension corresponding to the group $U(S) \cdot K^{\times p}/K^{\times p} \simeq U(S)/U(S) \cap K^{\times p}$. Consider the subgroup of $\mathbb{I}_K$:

$$W(S) := \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v.$$

To prove that V is a norm group, we prove:

(a) For such a set S , the group $W(S) \cdot K^\times / K^\times$ is a norm group.

(b) If U is the inverse image of V in $\mathbb{I}_K$ then there exists such a set S so that U contains $W(S) \cdot K^\times$ as a subgroup.

The result then follows from Lemma 8.6 since (b) implies that V contains $W(S) \cdot K^\times / K^\times$ as a subgroup.

Let us first prove (a). We prove that $W(S) \cdot K^\times = \text{Norm}_{M/K}(\mathbb{I}_M) \cdot K^\times$. To do that we check the two following points:

(i) We have an inclusion $W(S) \subset \text{Norm}_{M/K}(\mathbb{I}_M)$.

(ii) The indexes $[\mathbb{I}_K : K^\times \cdot W(S)]$ and $[\mathbb{I}_K : \text{Norm}_{M/K}(\mathbb{I}_M) \cdot K^\times]$ are equal (and they are equal to p^s where $s := |S|$).

We first prove (i). Let a be in $W(S)$. If v is a place in S then $a_v = b_v^p$ with b_v in $K_v^\times$. For w a place of M dividing p , the local Artin map gives an isomorphism $K_v^\times / \text{Norm}_{M_w/K_v}(M_w^\times) \xrightarrow{\sim} \text{Gal}(M_w/K_v)$ and since the Galois group has exponent p , we obtain that b_v^p is zero in $K_v^\times / \text{Norm}_{M_w/K_v}(M_w^\times)$, as wanted. If v is not in S , then it is unramified and the norm map is surjective on the units. We obtain that a is in $\text{Norm}_{M/K}(\mathbb{I}_M)$.

We now prove (ii). The global Reciprocity Law for M/K gives us an equality

$$[\mathbb{I}_K : K^\times \cdot \text{Norm}_{M/K}(\mathbb{I}_M)] = [M : K]$$

and from Kummer theory (Theorem 6.10), we know that

$$[M : K] = [U(S) \cdot K^{\times p} : K^{\times p}] = p^s$$

where $s = |S|$ (we have also used, as before, that $U(S)/U(S)^p \simeq (\mathbf{Z}/p\mathbf{Z})^s$).

For the second term, recall that $\mathbb{I}_K \simeq \mathbb{I}_{K,S} \cdot K^\times$ by Lemma 5.20 and by Lemma 6.18, we have

$$[\mathbb{I}_{K,S} \cdot K^\times : W(S) \cdot K^\times] = \frac{[\mathbb{I}_{K,S} : W(S)]}{[\mathbb{I}_{K,S} \cap K^\times : W(S) \cap K^\times]}.$$

But the same computation as in sections 6.3.2 and 6.3.3 give $[\mathbb{I}_{K,S} : W(S)] = p^{2s}$ and $[\mathbb{I}_{K,S} \cap K^\times : W(S) \cap K^\times] = p^s$.

We pass to the proof of (b). Let V be an open subgroup of $\mathbb{C}_K$ such that $\mathbb{C}_K/V$ is killed by p and let U be its inverse image in $\mathbb{I}_K$. We want to show that there exists S such that $W(S) \cdot K^\times$ is contained in U . But since U is open in $\mathbb{I}_K$, we know that there exists S such that $\prod_{v \in S} 1 \times \prod_{v \notin S} U_v$ is contained in U . But we also know that $(\cdot)^p$ kills $\mathbb{I}_K/U$ (since it kills $\mathbb{C}_K/V$) so U also contains $\mathbb{I}_K^p$. This proves that $K^\times \cdot W(S) \subset U$, as wanted. $\square$

We can now prove Theorem 4.18:

Theorem 8.8 (Existence theorem). *Let $H \subset \mathbb{C}_K$ be an open subgroup of finite index. Then there exists a unique abelian extension L of K such that $\text{Nm}_{L/K}(\mathbb{C}_L) = H$.*

Proof. The proof is done by induction on the index n of H . When $n = 1$, this is obvious. Assume $n > 1$. There exists a prime number p such that p divides n . Let ζ be a primitive p -th root of 1 and K' be the composite $\mathbf{Q}(\zeta) \cdot K$. If we prove that $\text{Norm}_{K'/K}^{-1}(H) \subset \mathbb{C}_{K'}$ is a norm group then by Lemma 8.6 we also have the result for H . Hence we can assume that K contains a primitive p -th root of 1. Choose $V \subset \mathbb{C}_K$ a subgroup of index p such that H is contained in V . By Theorem 8.7, we know that V is a norm group: there exists M/K of exponent p such that $V = \text{Norm}_{M/K}(\mathbb{C}_M)$. Write $U := \text{Norm}_{M/K}^{-1}(H) \subset \mathbb{C}_M$. We want to apply the induction hypothesis to U , to do that we will show that $[\mathbb{C}_M : U]$ strictly divides $[\mathbb{C}_K : H]$. Consider the map

$$\text{Norm}_{M/K} : \mathbb{C}_M \rightarrow \mathbb{C}_K/H.$$

Its image is V/H and its kernel is U so we have $[\mathbb{C}_M : U] = [V : H] = [\text{Norm}_{M/K}(\mathbb{C}_M) : H]$ and since $\text{Norm}_{M/K}(\mathbb{C}_M)$ is a strict subgroup of $\mathbb{C}_K$ then $[\text{Norm}_{M/K}(\mathbb{C}_M) : H]$ strictly divides $[\mathbb{C}_K : H]$. We obtain that $[\mathbb{C}_M : U]$ strictly divides $[\mathbb{C}_K : H]$, so we can apply the induction hypothesis to get that U is a norm group: there exists L/M such that $U = \text{Norm}_{L/M}(\mathbb{C}_L)$. Then

$$H = \text{Norm}_{M/K}(U) = \text{Norm}_{M/K}(\text{Norm}_{L/M}(\mathbb{C}_L)) = \text{Norm}_{L/K}(\mathbb{C}_L),$$

as wanted. □

Remark 8.9. This concludes the proof of the two main theorems of Global Class Field Theory, namely Reciprocity Law (Theorem 4.17) and Existence Theorem (Theorem 4.18) in terms of idèles. To derive the analogous results for ray class groups (Theorem 2.9 and Theorem 2.10), it suffices to use Proposition 4.12.

9 Density of primes

Recall that the exponential series $\sum_{n \geq 0} \frac{z^n}{n!}$ converges on $\mathbf{C}$ and defines an holomorphic function $\exp$ on $\mathbf{C}$. For n a positive integer we write n^z for $\exp(\log(n) \cdot z)$ where $\log : \mathbf{R}_{>0} \rightarrow \mathbf{R}$ is the usual real logarithm.

9.1 Dirichlet series

We make the following definitions:

(•) A Dirichlet series is a series of the form

$$f(s) = \sum_{n \geq 1} \frac{a(n)}{n^s},$$

for $a(n)$ coefficients in $\mathbf{C}$ and s the variable in $\mathbf{C}$.

(•) Let K be a number field. An Euler product for K is a product of the form

$$g(s) = \prod_{\mathfrak{p} \notin S} \frac{1}{(1 - \theta_1(\mathfrak{p})N(\mathfrak{p})^{-s})(1 - \theta_2(\mathfrak{p})N(\mathfrak{p})^{-s}) \cdots (1 - \theta_d(\mathfrak{p})N(\mathfrak{p})^{-s})}$$

where $d \geq 1$ is an integer, S is a finite set of places of K that contains S_∞ , the $\theta_i(\mathfrak{p}_v)$ are complex numbers and s is the variable in $\mathbf{C}$. Recall also that $N(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}]$.

Example 9.1. We describe here are some classical examples of such objects.

(1) **Riemann zeta function.** It is the Dirichlet series and the Euler product given by

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime number}} \frac{1}{1 - p^{-s}}.$$

(2) **Dedekind zeta function.** If K is a number field, the associated Dirichlet zeta function is the Dirichlet series and the Euler product given by

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

where the sum is over the integral ideals in $\mathcal{O}_K$ and the product over the prime ideals in $\mathcal{O}_K$. If $K = \mathbf{Q}$, we recover the previous example.

(3) **Dirichlet L -series.** Let K be a number field. If $\mathfrak{m}$ is a modulus, we define a Dirichlet character as a group morphism

$$\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$$

such that $\chi(K_{\mathfrak{m},1})$ is trivial. In other words, it is a character $\chi : C_{\mathfrak{m}} \rightarrow \mathbf{C}^\times$ of the ray class group corresponding to $\mathfrak{m}$. The associated Dirichlet L -series is given by

$$L(s, \chi) = \sum_{(\mathfrak{a}, \mathfrak{m})=1} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}},$$

where the sum is over the integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ which are prime to the prime ideals in $S(\mathfrak{m})$ and the product over the prime ideals of $\mathcal{O}_K$ which are prime to the prime ideals in $S(\mathfrak{m})$.

(4) **Hecke L -series.** Let K be a number field. We define a Hecke character as a continuous group morphism

$$\psi : \mathbb{I}_K / K^\times \rightarrow \mathbf{C}^\times$$

such that its image is contained in $\mathbf{S}^1 := \{z \in \mathbf{C} \mid |z| = 1\}$. Using (the proof of) Proposition 4.12, we see that a Dirichlet character corresponds to a Hecke character with discrete image (note that in Proposition 4.12 the group G was discrete, here $\mathbf{C}^\times$ is equipped with its natural topology). Conversely, if the morphism ψ_v induced by ψ on the infinite places v satisfies

$\psi_v(\mathbf{R}_{>0}) = 1$ if v is real and $\psi_v(\mathbf{C}^\times) = 1$ if v is complex, then there exists a modulus $\mathfrak{m}$ such that ψ induces a Dirichlet character $\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$.

If $\psi : \mathbb{I}_K/K^\times \rightarrow \mathbf{C}^\times$ is a Hecke character, since it is continuous, there exists a finite set of places S containing S_∞ such that $\prod_{v \in S} \{1\} \times \prod_{v \notin S} U_v$ is contained in the kernel of ψ . For a place v , we denote by π_v the element of $\mathbb{I}_K$ which has a prime element in the v -position and 1 elsewhere. The Hecke L -series associated to ψ is defined as the product:

$$L_S(s, \psi) = \prod_{v \notin S} \frac{1}{1 - \psi(\pi_v) N(\mathfrak{p}_v^{-s})}.$$

(5) **Artin L -series.** Let K be a number field and let L be a finite Galois extension of K with Galois group G . Let $\rho : G \rightarrow \mathrm{GL}(V)$ be a finite dimensional complex representation of G . Recall that the trace of ρ is the morphism $\mathrm{Tr}(\rho) : G \rightarrow \mathbf{C}$ sending $g \in G$ to the trace of the endomorphism $\rho(g)$ of V . For g in G , we write $P_g(X) \in \mathbf{C}[X]$ the characteristic polynomial of $\rho(g)$, i.e.

$$P_g(X) = \det(1 - \rho(g)X) = \prod_{i=1}^{\dim(V)} (1 - a_i(g)X),$$

where the coefficients $a_i(g)$ are in $\mathbf{C}$. This depends only on the conjugacy class of g so if $\mathfrak{p}$ is a prime of K unramified in L then we can define

$$P_{\mathfrak{p}}(X) := P_{(\mathfrak{q}, L/K)}(X)$$

and we write $a_i(\mathfrak{p})$ for the coefficients $a_i(\mathfrak{q}, L/K)$, where $\mathfrak{q}$ is any prime of L dividing $\mathfrak{p}$. The Artin L -series corresponding to ρ is given by

$$L(s, \rho) := \prod_{\mathfrak{p} \text{ unr.}} \frac{1}{P_{\mathfrak{p}}(N(\mathfrak{p})^{-s})} = \prod_{\mathfrak{p} \text{ unr.}} \frac{1}{(1 - a_1(\mathfrak{p})N(\mathfrak{p})^{-s})(1 - a_2(\mathfrak{p})N(\mathfrak{p})^{-s}) \cdots (1 - a_{\dim(V)}(\mathfrak{p})N(\mathfrak{p})^{-s})},$$

where the product is over the primes of K unramified in L .

9.2 Convergence results

In this section we prove various convergence results for Dirichlet series and Euler products.

9.2.1 Dirichlet series and zeta function

We have the following general convergent result for Dirichlet series:

Proposition 9.2. *Let $f(s) = \sum_{n \geq 1} \frac{a(n)}{n^s}$ be a Dirichlet series and for $x \geq 1$ define $S(x) := \sum_{n \leq x} a(n)$. Assume that there exist positive constants M , a and b such that for all*

$x \geq M$, we have $|S(x)| \leq ax^b$. Then for all $\varepsilon > 0$ and $\delta > 0$, the series $f(s)$ converges uniformly for s in

$$D(b, \delta, \varepsilon) := \{s \in \mathbf{C} \mid \Re(s) \geq b + \delta \text{ and } |\arg(s - b)| \leq \frac{\pi}{2} - \varepsilon\}.$$

In particular, the series $f(s)$ defines an analytic function on the half plane $\Re(s) > b$.

Proof. The second point follows from the first one since every point s with $\Re(s) > b$ admits a neighbourhood of the form $D(b, \delta, \varepsilon)$. We show the uniform convergence using Cauchy criterion. Let $1 \leq n_1 < n_2$ be two integers big enough, we have

$$\begin{aligned} \left| \sum_{n=n_1}^{n_2} \frac{a(n)}{n^s} \right| &= \left| \sum_{n=n_1}^{n_2} \frac{S(n) - S(n-1)}{n^s} \right| \\ &= \left| \sum_{n=n_1}^{n_2} \frac{S(n)}{n^s} - \sum_{n=n_1-1}^{n_2-1} \frac{S(n)}{(n+1)^s} \right| \\ &= \left| \frac{S(n_2)}{n_2^s} - \frac{S(n_1-1)}{n_1^s} + \sum_{n=n_1}^{n_2-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| \\ &\leq \frac{|S(n_2)|}{n_2^{\Re(s)}} + \frac{|S(n_1-1)|}{n_1^{\Re(s)}} + \sum_{n=n_1}^{n_2-1} |S(n)| \cdot |s| \cdot \left| \int_n^{n+1} \frac{dt}{t^{s+1}} \right| \\ &\leq \frac{a}{n_2^{\Re(s)-b}} + \frac{a}{n_1^{\Re(s)-b}} + \sum_{n=n_1}^{n_2-1} |s| \cdot (an^b) \cdot \left| \int_n^{n+1} \frac{dt}{t^{s+1}} \right| \\ &\leq \frac{2a}{n_1^{\Re(s)-b}} + \sum_{n=n_1}^{n_2-1} |s| \cdot a \cdot \left| \int_n^{n+1} \frac{t^b dt}{t^{s+1}} \right| \\ &\leq \frac{2a}{n_1^{\Re(s)-b}} + |s| \cdot a \cdot \int_{n_1}^{\infty} \frac{dt}{t^{\Re(s)-b+1}} \\ &\leq \frac{2a}{n_1^{\Re(s)-b}} + \frac{|s|a}{(\Re(s) - b)n_1^{\Re(s)-b}}. \end{aligned}$$

Write $\theta(s) := \arg(s - b)$. For $s \in D(b, \delta, \varepsilon)$, we have

$$\frac{|s|}{\Re(s) - b} = \frac{|s - b + b|}{\Re(s) - b} \leq \frac{|s - b|}{\Re(s) - b} + \frac{b}{\Re(s) - b} = \frac{1}{\cos(\theta(s))} + \frac{b}{\Re(s) - b} \leq \frac{1}{\cos(\theta(s))} + \frac{b}{\delta}.$$

Since we have assumed that $|\theta(s)|$ is less than $\frac{\pi}{2} - \varepsilon$, this means that the term $\frac{1}{\cos(\theta(s))}$ is bounded by some constant C . We obtain

$$\left| \sum_{n=n_1}^{n_2} \frac{a(n)}{n^s} \right| \leq \frac{2a}{n_1^{\Re(s)-b}} + \frac{(C + \frac{b}{\delta})a}{n_1^{\Re(s)-b}}$$

and we see that when n_1 goes to infinity, the term on the left converges to zero. Hence the uniform convergence follows from Cauchy's criterion. $\square$

Example 9.3. (1) Riemann zeta function. In the case of the series $\zeta(s)$, the sum $S(x)$ is equal to $[x]$, the integral part of x . Hence $b = 1$ and the proposition tells us that $\zeta(s)$ converges for $\mathcal{R}(s) > 1$.

(2) **Dedekind zeta function.** Let K be a number field. For the series $\zeta_K(s)$, the sum $S(x)$ is equal to the number of integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ such that has norm less than x . We can show (see for example Proposition 9.10) that we have an inequality $S(x) \leq ax$ for some constant a . Hence $b = 1$ as well in that case and we deduce from Proposition 9.2 that $\zeta_K(s)$ converges for $\mathcal{R}(s) > 1$.

Note that we also have the following result:

Proposition 9.4. *Let $f(s) = \sum_{n \geq 1} \frac{a(n)}{n^s}$ be a Dirichlet series with $a(n)$ a real number such that $a(n) \geq 0$. Let b be a real number. Assume that $f(s)$ converges for $\mathcal{R}(s) > b$ and there exists $\varepsilon > 0$ such that it can be extended as an holomorphic function for $|s| \leq \varepsilon$. Then $f(s)$ converges on $\mathcal{R}(s) > b - \varepsilon$.*

Proof. Up to changing s by $s - b$, we can assume $b = 0$. Assume that $f(s) = \sum_{n \geq 1} \frac{a(n)}{n^s}$ converges for $\mathcal{R}(s) > 0$ and there exists $\varepsilon > 0$ such that it can be extended as an holomorphic function for $|s| \leq \varepsilon$. Let us write $\tilde{f}(s)$ this holomorphic function.

On the disk $|s| \leq \varepsilon$, we can write $\tilde{f}(s)$ as its Taylor series

$$\tilde{f}(s) = \sum_{k \geq 0} \frac{1}{k!} (s - 1)^k \tilde{f}^{(k)}(1)$$

and in particular for $s = -\varepsilon$, we have

$$\tilde{f}(-\varepsilon) = \sum_{k \geq 0} \frac{1}{k!} (-1)^k (\varepsilon + 1)^k \tilde{f}^{(k)}(1).$$

But we have

$$\tilde{f}^{(k)}(1) = f^{(k)}(1) = (-1)^k \sum_{n \geq 1} \frac{a(n) \log(n)^k}{n}$$

and we obtain

$$\tilde{f}(-\varepsilon) = \sum_{k \geq 0, n \geq 1} \frac{1}{k!} (\varepsilon + 1)^k \frac{a(n) \log(n)^k}{n}$$

(the series converge since both series converge and have positive terms). We can now compute

this series:

$$\begin{aligned}
\tilde{f}(-\varepsilon) &= \sum_{n \geq 1} \frac{a(n)}{n} \sum_{k \geq 0} \frac{1}{k!} (\varepsilon + 1)^k \log(n)^k \\
&= \sum_{n \geq 1} \frac{a(n)}{n} \exp(\log(n)(1 + \varepsilon)) \\
&= \sum_{n \geq 1} \frac{a(n)}{n^{-\varepsilon}} = f(-\varepsilon).
\end{aligned}$$

It follows that the series $f(s)$ converges for $\mathcal{R}(s) > -\varepsilon$. □

Lemma 9.5. *The zeta function $\zeta(s)$ has an analytic continuation to a meromorphic function on the half plane $\mathcal{R}(s) > 0$ with its only possible pole at $s = 1$.*

Proof. Consider the Dirichlet series

$$\zeta_2(s) := \sum_{n \geq 1} \frac{(-1)^{n-1}}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

For this series, the term $S(x) = \sum_{n \leq x} a(n)$ from Proposition 9.2 is equal to 0 or 1. So in that case $b = 0$ and the proposition tells us that $\zeta_2(s)$ is an analytic function for $\mathcal{R}(s) > 0$. Moreover, we have the following formula:

$$\zeta(s) - \frac{2}{2^s} \zeta(s) = \zeta_2(s),$$

equivalently,

$$\zeta(s) = \frac{\zeta_2(s)}{1 - 2^{1-s}}.$$

Hence, we see that $\zeta(s)$ is analytic for $\mathcal{R}(s) > 0$ except possibly at points s such that 2^{s-1} is equal to 1. In other words the only possible problems are for s such that

$$(9.2.1) \quad s = 1 + \frac{2k\pi i}{\log(2)}, \quad \text{for } k \in \mathbf{Z}.$$

Consider now the series $\zeta_3(s) = \sum_{n \geq 1} \frac{a(n)}{n^s}$ where $a(n) = -2$ if n is divisible by 3 and 1 otherwise:

$$\zeta_3(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} \cdots$$

In that case $S(x)$ is equal to 0, 1 or 2, so $b = 0$ and Proposition 9.2 tells us that $\zeta_3(s)$ is analytic on $\mathcal{R}(s) > 0$. In addition, we have:

$$\zeta(s) = \frac{\zeta_3(s)}{1 - 3^{1-s}},$$

and we see that the only possible poles for $\zeta(s)$ are at the points s such that

$$(9.2.2) \quad s = 1 + \frac{2k\pi i}{\log(3)}, \quad \text{for } k \in \mathbf{Z}.$$

Combining (9.2.1) and (9.2.2), we see that if s is a pole of $\zeta(s)$ then we must have

$$\frac{2k\pi i}{\log(2)} = \frac{2k'\pi i}{\log(3)},$$

equivalently,

$$2^{k'} = 3^k.$$

The only solution is $k = k' = 0$, so the only possible pole for $\zeta(s)$ is $s = 1$. □

Lemma 9.6. *Let s be in $\mathbf{R}$ such that $s > 1$, then we have*

$$\frac{1}{s-1} \leq \zeta(s) \leq 1 + \frac{1}{s-1}.$$

In particular, $\zeta(s)$ admits a simple pole at $s = 1$ with residue 1. In other words, in a neighborhood of 1, we can write

$$\zeta(s) = \frac{1}{s-1} + h(s)$$

where $h(s)$ is an holomorphic function.

Proof. Assume that s is in $\mathbf{R}$ and $s > 1$. Then for all $n \geq 1$, we have

$$\int_n^{n+1} \frac{dx}{x^s} \leq \frac{1}{n^s} \leq \int_{n-1}^n \frac{dx}{x^s}$$

and we obtain:

$$\int_1^\infty \frac{dx}{x^s} \leq \zeta(s) \leq 1 + \int_1^\infty \frac{dx}{x^s}.$$

Since $\int_1^\infty \frac{dx}{x^s} = \frac{1}{s-1}$, this gives the inequality from the lemma:

$$(9.2.3) \quad \frac{1}{s-1} \leq \zeta(s) \leq 1 + \frac{1}{s-1}.$$

From Lemma 9.5, we know that ζ is meromorphic at $s = 1$ so in a neighborhood of 1, we can write

$$\zeta(s) = \frac{s_0}{(s-1)^m} + \frac{h(s)}{(s-1)^{m-1}}$$

where m is an integer, s_0 a complex number and $h(s)$ an holomorphic function. Using the inequalities from (9.2.3), we see that for s real, $s > 1$, we have

$$1 \leq \frac{s_0}{(s-1)^{m-1}} + \frac{h(s)}{(s-1)^{m-2}} \leq s.$$

When s tends to 1^+ , we have

$$\frac{s_0}{(s-1)^{m-1}} \rightarrow \begin{cases} s_0 & \text{if } m = 1, \\ \infty & \text{if } m > 1 \text{ and } s_0 \neq 0, \\ 0 & \text{if } s_0 = 0 \text{ or } m < 1, \end{cases} \quad \text{and} \quad \frac{h(s)}{(s-1)^{m-2}} \rightarrow \begin{cases} h(1) & \text{if } m = 2, \\ \infty & \text{if } m > 2 \text{ and } h(1) \neq 0, \\ 0 & \text{if } h(1) = 0 \text{ or } m < 2. \end{cases}$$

It follows that $m = 1$ and $s_0 = 1$. $\square$

Proposition 9.7. *Let $f(s) = \sum_{n \geq 1} \frac{a(n)}{n^s}$ be a Dirichlet series and $S(x)$ as in Proposition 9.2. Assume that there exist positive constants s_0 , a and b with $b < 1$ such that*

$$|S(x) - s_0 x| \leq ax^b.$$

Then $f(s)$ extends to a meromorphic function on $\mathcal{R}(s) > b$ that admits a simple pole at $s = 1$ with residue s_0 . In other words, in a neighborhood of 1, we can write

$$f(s) = \frac{s_0}{s-1} + h(s)$$

where $h(s)$ is an holomorphic function.

Proof. Consider the Dirichlet series $g(s) := f(s) - s_0 \zeta(s)$. For this series, by hypothesis, we have $|S(x)| \leq ax^b$. We can apply Proposition 9.2 and we obtain that $g(s)$ is analytic on $\mathcal{R}(s) > b$. Since $\zeta(s)$ is meromorphic for $\mathcal{R}(s) > 0$ with a simple pole at $s = 1$, we deduce that $f(s) = g(s) + s_0 \zeta(s)$ is meromorphic on $\mathcal{R}(s) > b$ with a simple pole at $s = 1$. $\square$

9.2.2 Euler products

Recall that we say that a product $\prod_{n \geq 1} (1 + a_n)$ with a_n in $\mathbf{C}$ and $a_n \neq 1$ converges is the finite products $\prod_{n=1}^m (1 + a_n)$ converges to a non-zero element in $\mathbf{C}$ when m goes to infinity. We say that $\prod_{n \geq 1} (1 + a_n)$ converges absolutely if the product $\prod_{n \geq 1} (1 + |a_n|)$ converges. If a product $\prod_{n \geq 1} (1 + a_n)$ converges absolutely then it converges. If a product $\prod_{n \geq 1} (1 + a_n)$ converges absolutely, we can change the order of the terms and the product will still converge. absolutely. Moreover, we have the following lemma:

Lemma 9.8. *The product $\prod_{n \geq 1} (1 + a_n)$ converges absolutely if and only if the series $\sum_{n \geq 1} a_n$ converges absolutely.*

Proof. Write $S_n := \sum_{k=1}^n |a_k|$ and $P_n := \prod_{k=1}^n |a_k|$. They are increasing sequences and for all n , we have $P_n \geq S_n$ so if $(P_n)_n$ converges, so does $(S_n)_n$. Conversely, we have

$$\exp(S_n) = \prod_{k=1}^n \exp(|a_k|) \geq \prod_{k=1}^n (1 + |a_k|) = P_n.$$

If $(S_n)_n$ converges, then $(\exp(S_n))_n$ also converges and since $(P_n)_n$ is an increasing sequence, the above inequality tells us that it converges. $\square$

Recall that since any integer can be decomposed uniquely as a product of primes, we have the following (formal) identification:

$$\prod_p \frac{1}{1 - p^{-s}} = \sum_{n \geq 1} \frac{1}{n^s}.$$

More generally, we have

Proposition 9.9. *Let K be a number field and let $\mathfrak{m}$ be a modulus. If $\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$ is a Dirichlet character then for s such that $\mathcal{R}(s) > 1$, the product $L(\chi, s) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}}$ converges.*

Proof. Let s be such that $\mathcal{R}(s) > 1$. Then we have (formally)

$$\frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \sum_{n \geq 0} \frac{\chi(\mathfrak{p}^n)}{N(\mathfrak{p}^n)^s}$$

So if we fix N_0 we have an equality

$$\prod_{(\mathfrak{p}, \mathfrak{m})=1 \text{ s.t. } N(\mathfrak{p}) \leq N_0} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \sum_{(\mathfrak{a}, \mathfrak{m})=1 \text{ s.t. } N(\mathfrak{a}) \leq N_0} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

where the sum in the right hand side term runs over the integral ideal $\mathfrak{a}$ with norm less than N_0 . When N_0 goes to infinity, the right hand side converges absolutely (we use again Proposition 9.2 and the fact that the number of integral ideals with norm less than s is bounded by ax for a some constant). It follows that the left hand side converges absolutely to $L(s, \chi)$. $\square$

9.2.3 The residue formula

Let K be a number field and let $\mathfrak{m}$ be a modulus. For every class $\mathfrak{c}$ in the ray class group $C_{\mathfrak{m}}$, the partial zeta function is defined as:

$$\zeta(s, \mathfrak{c}) = \sum_{\mathfrak{a} \text{ integral s.t. } \mathfrak{a} \in \mathfrak{c}} \frac{1}{N(\mathfrak{a})^s},$$

so that if $\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$ is a Dirichlet character, we have

$$L(s, \chi) = \sum_{\mathfrak{c} \in C_{\mathfrak{m}}} \chi(\mathfrak{c}) \zeta(s, \mathfrak{c})$$

and

$$\zeta_K(s) = \sum_{\mathfrak{c} \in C_{\mathfrak{m}}} \zeta(s, \mathfrak{c}).$$

Hence, in order to understand $L(s, \chi)$ and $\zeta_K(s)$, we are reduced to study the functions $\zeta(s, \mathfrak{c})$ for $\mathfrak{c}$ in the ray class group C_m . To be able to apply Proposition 9.2, we define $S(x, \mathfrak{c})$ as the number of elements of the set

$$\{\mathfrak{a} \in \mathfrak{c} \mid \mathfrak{a} \text{ integral ideal s.t. } N(\mathfrak{a}) \leq x\}.$$

Recall that we have defined

$$K_{m,1} := \{a \in K^\times \mid \begin{cases} a_v > 0 \text{ for all real place } v \text{ dividing } m \\ \text{ord}_{\mathfrak{p}}(a - 1) \geq m(\mathfrak{p}) \text{ for all finite place } \mathfrak{p} \text{ dividing } m \end{cases}\}.$$

and $U_{m,1} := U_K \cap K_{m,1}$. We have seen in the proof of Theorem 2.7 that the index $[U_K : U_{m,1}]$ is finite.

Recall also that we have a morphism (see for example the proof of Proposition 5.16 or Exercise Sheet 3):

$$\lambda : \begin{cases} U_K & \rightarrow \mathbf{R}^{r_1+r_2} \\ u & \mapsto (\log|\sigma_1(u)|, \log|\sigma_2(u)|, \dots, \log|\sigma_{r_1}(u)|, 2\log|\sigma_{r_1+1}(u)|, \dots, 2\log|\sigma_{r_1+r_2}(u)|) \end{cases},$$

where r_1 is the number of real places in K , the morphisms $\sigma_1, \dots, \sigma_{r_1}$ are the corresponding real embeddings, r_2 is the number of complex places and $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ are the corresponding complex embeddings. The kernel of λ is the torsion subgroup of U_K and its image $\lambda(U_K)$ is a lattice of rank $r_1 + r_2 - 1$. The regulator of K , denoted by $\text{reg}(K)$ is defined as

$$\text{reg}(K) = \frac{1}{\sqrt{r_1 + r_2}} \text{covol}(\lambda(U_K)).$$

In practice, we can compute it in the following way: if $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$ are elements in U_K that lift a basis of $U_K/\mu(K)$, then we have

$$\text{reg}(K) = |\det(\log\|\sigma_i(\varepsilon_j)\|)_{i \in I, 1 \leq j \leq r_1+r_2-1}|,$$

where I is the set $\{1, \dots, r_1 + r_2\}$ where we remove one element and we set

$$\|\sigma_i(\cdot)\| = \begin{cases} |\sigma_i(\cdot)| & \text{if } 1 \leq i \leq r_1, \\ |\sigma_i(\cdot)|^2 & \text{if } r_1 + 1 \leq i \leq r_1 + r_2. \end{cases}$$

If m is a modulus we define its regulator $\text{Reg}(m)$ as

$$\text{Reg}(m) = \text{reg}(K)[U_K : U_{m,1}].$$

If K is a number field and $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ is a modulus for K , we write:

$$\begin{aligned} d &= [K : \mathbf{Q}], \\ r_0 &= \text{number of real places in } \mathfrak{m}, \\ r_1 &= \text{number of real places in } K, \\ r_2 &= \text{number of complex places in } K, \\ w_{\mathfrak{m}} &= \text{number of roots of unity in } K_{\mathfrak{m},1}, \\ w_K &= \text{number of roots of unity in } K, \\ N(\mathfrak{m}) &= N(\mathfrak{m}_0) \cdot 2^{r_0}, \\ \Delta_{K/\mathbf{Q}} &= \text{discriminant of } K/\mathbf{Q}. \end{aligned}$$

Moreover, we set

$$g_{\mathfrak{m}} := \frac{2^{r_1} (2\pi)^{r_2} \text{reg}(\mathfrak{m})}{w_{\mathfrak{m}} N(\mathfrak{m}) |\Delta_{K/\mathbf{Q}}|^{\frac{1}{2}}}.$$

Proposition 9.10. *There exists a constant a such that for all $x \geq 1$ and $\mathfrak{c}$ in $C_{\mathfrak{m}}$, we have $|S(x, \mathfrak{c}) - g_{\mathfrak{m}} \cdot x| \leq ax^{1-\frac{1}{d}}$.*

Proof. See for example page 132 sqq of the book *Algebraic Number Theory* of Lang. $\square$

As a consequence, we obtain:

Corollary 9.11. *The partial zeta function $\zeta(s, \mathfrak{c})$ is meromorphic on $\mathcal{R}(s) > 1 - \frac{1}{d}$ with a simple pole at $s = 1$ with residue $g_{\mathfrak{m}}$.*

Proof. This follows immediately from Proposition 9.10 and the general convergence result Proposition 9.7. $\square$

In particular, we see that the residue $g_{\mathfrak{m}}$ of $\zeta(s, \mathfrak{c})$ does not depend on the choice of $\mathfrak{c}$ in $C_{\mathfrak{m}}$. We derive from the analyticity of the partial zeta function, the following convergence results:

Proposition 9.12. *Let K be a number field and $\mathfrak{m}$ a modulus for K .*

(1) *If $\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$ is a Dirichlet character for $\mathfrak{m}$ which is not trivial then $L(s, \chi)$ is analytic on the plane $\mathcal{R}(s) > 1 - \frac{1}{d}$.*

(2) *The Dedekind zeta function $\zeta_K(s)$ is meromorphic on the plane $\mathcal{R}(s) > 1 - \frac{1}{d}$ with a simple pole at $s = 1$ with residue*

$$\frac{2^{r_1} (2\pi)^{r_2} \text{reg}(K)}{w_K |\Delta_{K/\mathbf{Q}}|^{\frac{1}{2}}} h_K.$$

Proof. We need the following general lemma:

Lemma 9.13. *Let A be a finite abelian group and $\chi : A \rightarrow \mathbb{C}^\times$ be a non-trivial morphism of groups. Then*

$$\sum_{a \in A} \chi(a) = 0.$$

Proof of Lemma 9.13. Since the character χ is non trivial, we can find an element a_0 in A such that $\chi(a_0)$ is not 1. Then we have

$$\sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(aa_0) = \left(\sum_{a \in A} \chi(a) \right) \chi(a_0),$$

in other words,

$$(\chi(a_0) - 1) \left(\sum_{a \in A} \chi(a) \right) = 0.$$

The factor $(\chi(a_0) - 1)$ is non zero, so we obtain $\sum_{a \in A} \chi(a) = 0$. □

Let us now prove the proposition. Consider first the function $L(s, \chi)$. We have

$$L(s, \chi) = \sum_{\mathfrak{c} \in C_{\mathfrak{m}}} \chi(\mathfrak{c}) \cdot \zeta(s, \mathfrak{c}),$$

and we know from Corollary 9.11 that $\zeta(s, \mathfrak{c})$ is meromorphic on $\mathcal{R}(s) > 1 - \frac{1}{d}$ with a simple pole at $s = 1$ with residue $g_{\mathfrak{m}}$. So in a neighborhood of $s = 1$, we have

$$L(s, \chi) = \frac{\sum_{\mathfrak{c} \in C_{\mathfrak{m}}} \chi(\mathfrak{c}) g_{\mathfrak{m}}}{s - 1} + h(s)$$

where $h(s)$ is holomorphic. But it follows from the lemma that $\sum_{\mathfrak{c} \in C_{\mathfrak{m}}} \chi(\mathfrak{c}) g_{\mathfrak{m}}$ is zero. Hence, $L(s, \chi)$ is holomorphic everywhere on $\mathcal{R}(s) > 1 - \frac{1}{d}$.

Consider now the function $\zeta_K(s)$. We have

$$\zeta_K(s) = \sum_{\mathfrak{c} \in C_{\mathfrak{m}}} \zeta(s, \mathfrak{c}).$$

Hence, we see that $\zeta_K(s)$ is meromorphic on $\mathcal{R}(s) > 1 - \frac{1}{d}$ with a simple pole at $s = 1$ with residue

$$\sum_{\mathfrak{c} \in C_{\mathfrak{m}}} g_{\mathfrak{m}} = |C_{\mathfrak{m}}| \cdot g_{\mathfrak{m}} = \frac{2^{r_1} (2\pi)^{r_2} \text{reg}(K)}{w_K |\Delta_{K/\mathbb{Q}}|^{\frac{1}{2}}} h_K,$$

using the formula from Theorem 2.7. □

Example 9.14. If K is an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ with discriminant strictly less than -4 , we can deduce from the residue formula in Proposition 9.12, the following equality:

$$h_K = \frac{1}{2 - \chi(2)} \sum_{(n, \Delta_K)=1 \text{ with } 0 < n < \frac{|\Delta_K|}{2}} \chi(n).$$

9.3 Density of splitting primes

Let K be a number field and T a set of places of K . Consider the function

$$\zeta_{K,T}(s) := \prod_{\mathfrak{p} \in T} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

If there exists an integer n such that $\zeta_{K,T}(s)^n$ extends to a meromorphic function in a neighborhood of $s = 1$ with a pole of order m at $s = 1$, we say that the set T has polar density and we define

$$\delta_{\text{pol}}(T) = \frac{m}{n}.$$

Proposition 9.15. *Let K be a number field. Then:*

- (1) *The set of all prime ideals of K has polar density equal to 1.*
- (2) *If T is a set of places with a polar density then $\delta_{\text{pol}}(T) \geq 0$.*
- (3) *If T, T_1, T_2 are three set of places such that $T = T_1 \cup T_2$ (disjoint union) and any two of T, T_1, T_2 have polar densities then the third one also has polar density and $\delta_{\text{pol}}(T) = \delta_{\text{pol}}(T_1) + \delta_{\text{pol}}(T_2)$.*
- (4) *If T_1 and T_2 are two sets of places such that $T_1 \subset T_2$ and such that they have polar density, then $\delta_{\text{pol}}(T_1) \leq \delta_{\text{pol}}(T_2)$.*
- (5) *If T is a finite set then T has polar density and $\delta_{\text{pol}}(T) = 0$.*

Proof. We first prove (1). Assume that T is the set of all finite places of K . Then $\zeta_{K,T}(s)$ is equal to $\zeta_K(s)$ and we know from Proposition 9.12 that it is meromorphic on $\mathcal{R}(s)$ with a simple pole at $s = 1$. Hence its polar density is 1.

If $\delta_{\text{pol}}(T) < 0$, this means that the function $\zeta_{K,T}(s)^{-n}$ is meromorphic with a pole at $s = 1$ for some $n > 0$. In other words, the function $\zeta_{K,T}(s)^n$ is holomorphic and is equal to 0 for $s = 1$. But $\zeta_{K,T}(1) := \prod_{\mathfrak{p} \in T} \frac{1}{1 - N(\mathfrak{p})^{-1}} > 0$. This proves (2).

We now show (3). We can write

$$\zeta_{K,T}(s) = \zeta_{K,T_1}(s) \cdot \zeta_{K,T_2}(s).$$

Assume that there exist n and n_1 such that $\zeta_{K,T}(s)^n$ and $\zeta_{K,T_1}(s)^{n_1}$ are meromorphic functions in a neighborhood of $s = 1$ with poles at $s = 1$ of order m and m_1 respectively. Then we see that the function

$$\zeta_{K,T_2}(s)^{nn_1} = \frac{\zeta_{K,T}(s)^{nn_1}}{\zeta_{K,T_1}(s)^{nn_1}}$$

extends to a meromorphic function in a neighborhood of $s = 1$ with poles at $s = 1$ of order $n_1 m - n m_1$. We obtain

$$\delta_{\text{pol}}(T_2) = \frac{n_1 m - n m_1}{n n_1} = \frac{m}{n} - \frac{m_1}{n_1} = \delta_{\text{pol}}(T) - \delta_{\text{pol}}(T_1).$$

The proof is similar if we exchange the roles of T , T_1 and T_2 .

To prove the fourth point, consider the set $T_0 := T_2 \setminus T_1$. Then T_2 is the disjoint union of T_0 and T_1 and from the previous point we know that $\delta_{\text{pol}}(T_2) = \delta_{\text{pol}}(T_0) + \delta_{\text{pol}}(T_1)$. By (2), we also have that $\delta_{\text{pol}}(T_0) \geq 0$ and it follows that $\delta_{\text{pol}}(T_1) \leq \delta_{\text{pol}}(T_2)$.

The proof of the last point is immediate by definition of the density. $\square$

We also have:

Proposition 9.16. *Let K be a number field. Let us write T_0 the set of prime ideals $\mathfrak{p}$ of K such that $N(\mathfrak{p})$ is a prime number.*

(1) *If T is a set of places such that $T \cap T_0$ is empty, then $\delta_{\text{pol}}(T) = 0$.*

(2) *Assume that T_1 and T_2 are two sets of prime ideals of K such that they differ only by primes which are not in T_0 . Then if one of the two has polar density, the other also has polar density and $\delta_{\text{pol}}(T_1) = \delta_{\text{pol}}(T_2)$.*

Proof. Assume that $T \cap T_0$ is empty. For any $\mathfrak{p}$ in T , we then have $N(\mathfrak{p}) = p^f$ with $f \geq 2$. For a prime number p in $\mathbf{Q}$, there are at most $d := [K : \mathbf{Q}]$ prime ideals of K that divide p . Hence we can write

$$\zeta_{K,T}(s) = \prod_{i=1}^d \prod_{p \text{ prime number}} g_i(p, s) \text{ with } g_i(p, s) = 1 \text{ or } \frac{1}{1 - (p^{f_i})^{-s}}, \text{ where } f_i \geq 2.$$

Let us write $h_i(s) := \prod_{p \text{ prime number}} g_i(p, s)$. We want to show that $h_i(s)$ is holomorphic at 1. But we have

$$h_i(1) \leq \sum_{n \geq 1} \frac{1}{n^2} = \zeta(2),$$

hence the sum is holomorphic. This proves that $\delta_{\text{pol}}(T)$ is zero.

To prove (2), it suffices to apply the first point to the sets $T_{0,1} := T_1 \setminus (T_1 \cap T_2)$ and $T_{0,2} := T_2 \setminus (T_1 \cap T_2)$. We have $\delta_{\text{pol}}(T_{0,1}) = \delta_{\text{pol}}(T_{0,2}) = 0$ and by Proposition 9.15(3),

$$\begin{aligned} \delta_{\text{pol}}(T_1) &= \delta_{\text{pol}}(T_{0,1}) + \delta_{\text{pol}}(T_1 \cap T_2) = \delta_{\text{pol}}(T_1 \cap T_2) \\ \delta_{\text{pol}}(T_2) &= \delta_{\text{pol}}(T_{0,2}) + \delta_{\text{pol}}(T_1 \cap T_2) = \delta_{\text{pol}}(T_1 \cap T_2). \end{aligned}$$

$\square$

We obtain the following theorem:

Theorem 9.17. *Let K be a number field and L be a finite extension of K . Denote by M the Galois closure of L in $\overline{K}$. Then the set of prime ideals of K that splits completely in L has polar density equals to $\frac{1}{[M:K]}$.*

Proof. We first prove the following lemma:

Lemma 9.18. *Let K be a number field and L be a finite extension of K . Denote by M the Galois closure of L in $\overline{K}$. A prime ideal $\mathfrak{p}$ of K splits completely in L if and only if it splits completely in M .*

Proof of Lemma 9.18. Write $L = K[X]/(P(X))$ with P in $K[X]$ irreducible. Then M is defined as the composite of the $L_i := K(\alpha_i)$'s where the elements α_i 's are the roots of P . If $\mathfrak{p}$ is a prime ideal of K that splits completely in one of the L_i , then it splits completely in all of the L_i 's. So to prove the lemma, it suffices to prove that if $\mathfrak{p}$ is a prime ideal of K that splits completely in two field extensions L and L' then it splits completely in the composite $L \cdot L'$. But we know that a prime $\mathfrak{p}$ in K splits completely in L if and only if $L \otimes_K K_{\mathfrak{p}}$ is a product of copies of $K_{\mathfrak{p}}$, and we can see $L \cdot L'$ as a direct factor of $L \otimes_K L'$. $\square$

We now come back to the proof of the proposition. By the lemma, we can assume that L/K is Galois. Let us denote by S the set of all prime ideals of K that split completely in L . We write T for the set of places of L that divide the places in S . By hypothesis, for each prime $\mathfrak{p}$ of S , there exists exactly $[L : K]$ prime ideals $\mathfrak{q}$ in T that divide $\mathfrak{p}$ and we have $\text{Norm}_{L/K}(\mathfrak{q}) = \mathfrak{p}$. Hence $N(\mathfrak{q}) = N(\mathfrak{p})$ and $\zeta_{L,T}(s) = \zeta_{K,S}(s)^{[L:K]}$. To prove the proposition, it remains to show that T has polar density equals to 1.

Consider the set T_1 of all prime ideals of L . We know from Proposition 9.15 that it has density 1. For any $\mathfrak{q}$ in T_1 , we have that $N(\mathfrak{q})$ is equal to $p^{f(\mathfrak{q}/p)}$. If $f(\mathfrak{q}/p)$ is equal to 1, then $f(\mathfrak{q}/\mathfrak{q} \cap \mathcal{O}_K) = 1$ and either $\mathfrak{q}$ is in T or $\mathfrak{q} \cap \mathcal{O}_K$ ramifies in L . Hence $T_1 \setminus T$ can be written as the union of a finite set (corresponding to the primes that ramify) and a set of primes $\mathfrak{q}$ such that $N(\mathfrak{q})$ is not a prime number. By Proposition 9.15 and Proposition 9.16, we obtain that T_1 and T has same density equal to 1. This concludes the proof of the theorem. $\square$

We derive from the theorem the following consequences:

Corollary 9.19. *Let K be a number field and $P(X)$ be a polynomial in $K[X]$. If $P(X)$ splits into linear factors modulo $\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of K , then $P(X)$ itself splits into linear factors in K .*

Proof. Let L be the splitting field of the polynomial $P(X)$. From Theorem 9.17, we know that the set of prime ideals of K that split completely in L has density $\frac{1}{[L:K]}$. But by hypothesis, almost all prime ideals of K split completely in L , so by Proposition 9.15, this set has density 1. Hence $L = K$. $\square$

For K a number field and L a Galois extension of K , we write $\text{Spl}_K(L)$ the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that split completely in L .

Corollary 9.20. *Let K be a number field and let L and M be Galois extensions of K . Then we have,*

$$L \subset M \quad \text{if and only if} \quad \text{Spl}_K(L) \supset \text{Spl}_K(M)$$

and in particular,

$$L = M \quad \text{if and only if} \quad \text{Spl}_K(L) = \text{Spl}_K(M)$$

We obtain an injective map $L \mapsto \text{Spl}_K(L)$ from the set of finite Galois extensions of K (contained in $\overline{K}$) to the set of subsets of $\{\mathfrak{p} \text{ prime ideals of } K\}$.

Proof. We obviously have that if L is a subset of M then any prime of K that is completely split in L is also completely split in M . Let us prove the reverse implication. Recall that sending σ in $\text{Gal}(LM/K)$ to $(\sigma|_L, \sigma|_M)$ defines an injective morphism

$$\text{Gal}(LM/K) \hookrightarrow \text{Gal}(L/K) \times \text{Gal}(M/K),$$

such that if $\mathfrak{q}$ is a prime ideal of LM , then $(\mathfrak{q}, LM/K)$ is sent to $((\mathfrak{q} \cap \mathcal{O}_L, L/K), (\mathfrak{q} \cap \mathcal{O}_M, M/K))$. In particular, we see that

$$\text{Spl}_K(LM) = \text{Spl}_K(L) \cap \text{Spl}_K(M).$$

So if $\text{Spl}_K(L) \supset \text{Spl}_K(M)$, we obtain $\text{Spl}_K(LM) = \text{Spl}_K(M)$. From Theorem 9.17, we know that these two sets have density $\frac{1}{[LM:K]}$ and $\frac{1}{[M:K]}$. Hence $[LM:K] = [M:K]$. This means $L \subset M$, as wanted. $\square$

Finally, we can recover the surjectivity of the Artin map:

Corollary 9.21. *Let K be a number field and let L be an abelian extension of K . Assume that S is a finite set of places of K such that S contains S_∞ and the set of all primes that ramify in L . Then the Artin map*

$$\psi_{L/K} : I_K^S \rightarrow \text{Gal}(L/K)$$

is surjective.

Proof. Let H be the image of $\psi_{L/K}$. If $\mathfrak{p}$ is not in S , then it is unramified in L so it is unramified in L^H and we also have

$$(\mathfrak{p}, L^H/K) = (\mathfrak{p}, L/K)|_{L^H} = 1.$$

In particular, we see that $\mathfrak{p}$ splits completely in L^H .

If we write T the set of primes that split completely in L^H , we know by Theorem 9.17 that this set has polar density equals to $\frac{1}{[L^H:K]}$. But we have just seen that all primes of K except a finite number split completely in L^H . So by Proposition 9.15, we see that the set of primes that do not split completely has density equals to 0 and we obtain that T has density equals to 1. Hence $[L^H:K] = 1$. This proves that $H = \text{Gal}(L/K)$, as wanted. $\square$

9.4 Density of primes in an arithmetic progression

Reminders and notations. Recall that the exponential map $\exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}$ defines an isomorphism from $\{z \in \mathbf{C} \mid -\pi < \mathcal{I}(z) < \pi\}$ onto $\mathbf{C} \setminus \{z \in \mathbf{R} \mid z \leq 0\}$ and we write $\log$ for its inverse. We have

$$\log(z) = \log(|z|) + i \cdot \arg(z) \quad \text{with } -\pi < \arg(z) < \pi.$$

With this definition we also have

$$\log\left(\frac{1}{1-z}\right) = \sum_{n \geq 1} \frac{z^n}{n} \quad \text{for } |z| < 1.$$

If $f(s)$ and $g(s)$ are two functions defined for $\mathcal{R}(s) > 1$ and with values in $\mathbf{R}$, we write $f(s) \sim g(s)$ if there exists $\varepsilon > 0$ such that $f(s) - g(s)$ is bounded when s is real and $1 < s < 1 + \varepsilon$. Note that if there exists a real number δ such that $f(s) \sim \log\left(\frac{1}{s-1}\right)$ then

$$\lim_{s \rightarrow 1^+} \frac{f(s)}{\log\left(\frac{1}{s-1}\right)} = \delta.$$

We also have that if $f(s)$ and $g(s)$ are two meromorphic functions in a neighborhood of $s = 1$ with a (possible) pole at $s = 1$ then $f(s) \sim g(s)$ if and only if $f(s) - g(s)$ is a function that is holomorphic in a neighborhood of 1.

Definition 9.22. Let K be a number field and let T be a set of places of K . We say that T has Dirichlet density δ if there exists δ such that

$$\sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s} \sim \delta \cdot \log \frac{1}{s-1}.$$

We write $\delta_D(T) = \delta$.

We first show the following lemma:

Lemma 9.23. Let $(u_n)_{n \geq 1}$ be a sequence of real numbers that are ≥ 2 and define $f(s) := \prod_{n \geq 1} \frac{1}{1-u_n^{-s}}$. Assume that for all $\varepsilon > 0$ and $\delta > 0$, the function $f(s)$ converges uniformly on

$$D(1, \delta, \varepsilon) := \{s \in \mathbf{C} \mid \mathcal{R}(s) \geq 1 + \delta \text{ and } |\arg(s-1)| \leq \frac{\pi}{2} - \varepsilon\}.$$

Then,

$$\log(f(s)) \sim \sum_{n \geq 1} \frac{1}{u_n^s}.$$

Proof. We have the following equalities:

$$\begin{aligned}
\log(f(s)) &= \sum_{n \geq 1} \log \frac{1}{1 - u_n^{-s}} \\
&= \sum_{n \geq 1} \sum_{m \geq 1} \frac{1}{m u_n^{sm}} \\
&= \sum_{n \geq 1} \frac{1}{u_n^s} + \sum_{n \geq 1} \sum_{m \geq 2} \frac{1}{m u_n^{sm}} \\
&= \sum_{n \geq 1} \frac{1}{u_n^s} + h(s),
\end{aligned}$$

where

$$h(s) := \sum_{n \geq 1} \sum_{m \geq 2} \frac{1}{m u_n^{sm}}.$$

We have

$$|h(s)| \leq \sum_{n \geq 1} \sum_{m \geq 2} \left| \frac{1}{m u_n^{sm}} \right| = \sum_{n \geq 1} \sum_{m \geq 2} \frac{1}{m u_n^{\mathcal{R}(s)m}}$$

and since $u_n \geq 2$ and $\mathcal{R}(s) > 1$,

$$\begin{aligned}
\sum_{m \geq 2} \frac{1}{m u_n^{\mathcal{R}(s)m}} &\leq \sum_{m \geq 2} \frac{1}{2} \left(\frac{1}{u_n^{\mathcal{R}(s)}} \right)^m \\
&= \frac{1}{2} \left(\frac{1}{1 - u_n^{-\mathcal{R}(s)}} - u_n^{-\mathcal{R}(s)} - 1 \right) \\
&= \frac{1}{2} \left(\frac{u_n^{-2\mathcal{R}(s)}}{1 - u_n^{-\mathcal{R}(s)}} \right) \\
&< \frac{1}{u_n^{2\mathcal{R}(s)} - 1},
\end{aligned}$$

where we have used that $2(u_n^{2\mathcal{R}(s)} - u_n^{\mathcal{R}(s)}) > u_n^{2\mathcal{R}(s)} - 1$. It follows

$$|h(s)| \leq \sum_{n \geq 1} \frac{1}{u_n^{2\mathcal{R}(s)} - 1}.$$

Since we have assumed that $f(s) = \prod_{n \geq 1} \frac{1}{1 - u_n^{-s}}$ converges uniformly on $D(1, \delta, \varepsilon)$ for any ε and δ , we know (by Lemma 9.8) that $\sum_{n \geq 1} \frac{1}{u_n^s - 1}$ converges uniformly on $D(1, \delta, \varepsilon)$ for any ε and δ and hence it is holomorphic for $\mathcal{R}(s) > 1$. It follows that $\sum_{n \geq 1} \frac{1}{u_n^{2\mathcal{R}(s)} - 1}$ is holomorphic for $\mathcal{R}(s) > \frac{1}{2}$ and so $h(s)$ is bounded when s tends to 1.

□

We have:

Proposition 9.24. *Let K be a number field and let T be a set of places of K . If the polar density of T exists then its Dirichlet density exists and the two are equal.*

Proof. Assume that $\delta_{\text{pol}}(T)$ exists, we can write

$$\zeta_{K,T}(s)^n = \frac{s_0}{(s-1)^m} + \frac{h(s)}{(s-1)^{m-1}}$$

where $h(s)$ is holomorphic in a neighborhood of $s = 1$. We also know that $s_0 > 0$ since when s is real such that $s > 1$, then $\zeta_{K,T}(s)$ is real and > 0 . From Lemma 9.23, we obtain

$$n \sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s} \sim m \log \frac{1}{s-1}.$$

Hence

$$\delta_D(T) = \frac{m}{n},$$

as wanted. □

Remark 9.25. We also have a notion of *natural density*. We say that T has natural density δ if there exists δ such that

$$\delta = \lim_{x \rightarrow \infty} \frac{|\{\mathfrak{p} \in T \text{ s.t. } N(\mathfrak{p}) \leq x\}|}{|\{\mathfrak{p} \text{ primes of } K \text{ s.t. } N(\mathfrak{p}) \leq x\}|}.$$

We write $\delta_{\text{nat}}(T) = \delta$. It can be showed that if the natural density of T exists then its Dirichlet density exists as well and the two are equal. However, there exist sets T that have a Dirichlet density without having a natural density. Similarly, there exists sets T such that T has a natural density but not a polar one. This comes from the fact that the polar density is a rational numbers and we can construct sets with natural density that is not rational.

Our next goal is to prove the following properties:

Proposition 9.26. *Let K be a number field. Then:*

- (1) *The set of all prime ideals of K has Dirichlet density equal to 1.*
- (2) *If T is a set of places with a Dirichlet density δ then $\delta \geq 0$.*
- (3) *If T, T_1, T_2 are three set of places such that $T = T_1 \cup T_2$ (disjoint union) and any two of T, T_1, T_2 have Dirichlet densities then the third one also has Dirichlet density and $\delta_D(T) = \delta_D(T_1) + \delta_D(T_2)$.*
- (4) *If T_1 and T_2 are two sets of places such that $T_1 \subset T_2$ and such that they have Dirichlet density, then $\delta_D(T_1) \leq \delta_D(T_2)$.*
- (5) *If T is a finite set then T has Dirichlet density and $\delta_D(T) = 0$.*

Proof. The first point follows from Lemma 9.24 and Proposition 9.15. For the second point, assume that we can write

$$\sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s} \sim \delta \log \frac{1}{s-1}$$

i.e.

$$\lim_{s \rightarrow 1^+} \frac{f(s)}{\log\left(\frac{1}{s-1}\right)} = \delta.$$

For $\varepsilon < 1$ and $s = 1 + \varepsilon$, we have that $\log \frac{1}{s-1} = -\log(\varepsilon)$ is positive. Since $\frac{1}{N(\mathfrak{p})^s}$ is also positive, we see that necessarily, δ itself is positive.

To prove (3), note that for $\mathcal{R}(s) > 1$, we have

$$\sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \in T_1} \frac{1}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p} \in T_2} \frac{1}{N(\mathfrak{p})^s}.$$

Assume that $\delta_D(T_1)$ and $\delta_D(T)$ exist and are equal to δ_1 and δ , respectively. Then

$$\sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s} \sim \delta \log \frac{1}{s-1} \quad \text{and} \quad \sum_{\mathfrak{p} \in T_1} \frac{1}{N(\mathfrak{p})^s} \sim \delta_1 \log \frac{1}{s-1}$$

and we obtain

$$\sum_{\mathfrak{p} \in T_2} \frac{1}{N(\mathfrak{p})^s} \sim (\delta - \delta_1) \log \frac{1}{s-1}.$$

So $\delta_D(T_2)$ exists and is equal to $(\delta - \delta_1)$. The argument is similar if we exchange the roles of T , T_1 and T_2 .

Consider now T_1 and T_2 two sets of places such that $T_1 \subset T_2$ and such that $\delta_D(T_1)$ and $\delta_D(T_2)$ exist. Then $\delta_D(T_2 \setminus T_1)$ exists. By (3), we know that $\delta_D(T_2 \setminus T_1) = \delta_D(T_2) - \delta_D(T_1)$ and by (2), we know that $\delta_D(T_2 \setminus T_1)$ is positive. Hence $\delta_D(T_1) \leq \delta_D(T_2)$, as wanted.

Let us prove (5). If T is a finite set, then $\sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s}$ is holomorphic and so it is bounded near $s = 1$. Hence, $\delta_D(T) = 0$.

□

Proposition 9.27. *Let K be a number field and consider T the set of prime ideals $\mathfrak{p}$ of K such that the inertia degree $f(\mathfrak{p}/p)$ of $\mathfrak{p}$ over $\mathbb{Q}$ is equal to 1. Then*

(1) *we have $\delta_D(T) = 1$ and,*

(2) *for any set S of places of K that has a Dirichlet density, $\delta_D(T \cap S) = \delta_D(S)$.*

Proof. Let us first prove (1). We denote by S_0 the set of all finite places of K . We know from Proposition 9.16 that $\delta_{\text{pol}}(S_0 \setminus T)$ is zero. So by Lemma 9.24, we also have $\delta_D(S_0 \setminus T)$ is zero. Since $\delta_D(T) = \delta_D(S_0) - \delta_D(S_0 \setminus T)$, we obtain that $\delta_D(T) = \delta_D(S_0) = 1$.

To prove the second point, let us write $T' := S_0 \setminus T$. Since $S \cap T' \subset T'$ and T' has density equal to zero, it follows from the properties proved above that $\delta_D(S \cap T')$ is zero. Since we can write S as the disjoint union of $S \cap T$ and $S \cap T'$, it follows that $\delta_D(T \cap S) = \delta_D(S)$. $\square$

We can finally prove:

Theorem 9.28. *Let K be a number field and let $\mathfrak{m}$ be a modulus for K . Let H be a subgroups of $I_K^{S(\mathfrak{m})}$ such that H contains $K_{\mathfrak{m},1}$. Then,*

$$\delta_D(\{\mathfrak{p} \in H\}) = \begin{cases} \frac{1}{[I_K^{S(\mathfrak{m})}:H]} & \text{if } L(1, \chi) \text{ is non zero for all non trivial character } \chi \text{ of } I_K^{S(\mathfrak{m})}/H, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We need the following general lemma:

Lemma 9.29. *Let A be a finite abelian group and let a be an element of A . Then*

$$\sum_{\chi \in A^\vee} \chi(a) = \begin{cases} |A| & \text{if } a = 1, \\ 0 & \text{otherwise.} \end{cases}$$

where $A^\vee = \text{Hom}(A, \mathbf{C}^\times)$.

Proof of Lemma 9.29. Since A is abelian and finite, $A^\vee$ has the same number of elements as A . Hence if $a = 1$ is trivial, we have

$$\sum_{\chi \in A^\vee} \chi(a) = \sum_{\chi \in A^\vee} 1 = |A^\vee| = |A|.$$

If a is not trivial, then there exists a character χ_1 such that $\chi_1(a) \neq 1$. We have

$$\sum_{\chi \in A^\vee} \chi(a) = \sum_{\chi \in A^\vee} (\chi_1 \chi)(a) = \sum_{\chi \in A^\vee} \chi_1(a) \chi(a) = \chi_1(a) \sum_{\chi \in A^\vee} \chi(a).$$

Since $\chi_1(a) \neq 1$, we obtain $\sum_{\chi \in A^\vee} \chi(a) = 0$. $\square$

Let us now prove the theorem. Let $\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$ be a character such that $\chi(H)$ is trivial. Consider the L -function

$$L(s, \chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}}.$$

From Lemma 9.23, we know that

$$\log(L(s, \chi)) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

Let us now take the sum over all characters $\chi : I_K^{S(m)}/H \rightarrow \mathbf{C}^\times$. We have

$$\sum_{\chi} \log(L(s, \chi)) \sim \sum_{\chi} \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{N(\mathfrak{p})^s} \sum_{\chi} \chi(\mathfrak{p}),$$

and from the previous lemma,

$$\sum_{\chi} \chi(\mathfrak{p}) = \begin{cases} [I_K^{S(m)} : H] & \text{if } \mathfrak{p} \in H \\ 0 & \text{if } \mathfrak{p} \notin H \end{cases}.$$

Hence,

$$(9.4.1) \quad \sum_{\chi} \log(L(s, \chi)) \sim [I_K^{S(m)} : H] \sum_{\mathfrak{p} \in H} \frac{1}{N(\mathfrak{p})^s}.$$

If χ is non trivial, we know by Proposition 9.12 that $L(s, \chi)$ is holomorphic in a neighborhood of $s = 1$, so we can write $L(s, \chi) = (s - 1)^{m(\chi)} h(s)$ with $m(\chi) \geq 0$ and $h(1) \neq 0$. This gives

$$(9.4.2) \quad \log(L(s, \chi)) \sim m(\chi) \log(s - 1) = -m(\chi) \log \frac{1}{s - 1}.$$

If χ is trivial, then we can write

$$L(s, \chi) = \left(\prod_{\mathfrak{p} \mid \mathfrak{m}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \right)^{-1} \zeta_K(s)$$

and we obtain

$$(9.4.3) \quad \log(L(s, \chi)) \sim \log \zeta_K(s) \sim \log \frac{1}{s - 1}.$$

Combining (9.4.1), (9.4.2) and (9.4.3), we get

$$[I_K^{S(m)} : H] \sum_{\mathfrak{p} \in H} \frac{1}{N(\mathfrak{p})^s} \sim \left(1 - \sum_{\chi \text{ non trivial}} m(\chi) \right) \log \frac{1}{s - 1}.$$

This yields

$$\delta_D(\{\mathfrak{p} \in H\}) = \frac{1 - \sum_{\chi \text{ non trivial}} m(\chi)}{[I_K^{S(m)} : H]}.$$

If $L(1, \chi) \neq 0$, then $m(\chi) = 0$, so we obtain $\delta_D(\{\mathfrak{p} \in H\}) = \frac{1}{[I_K^{S(m)} : H]}$ if $L(1, \chi)$ is non zero for all non trivial character χ . If one of the $m(\chi)$ is non zero, then since $\delta_D(\{\mathfrak{p} \in H\}) \geq 0$, we see that all the other $m(\chi)$'s are zero and the non-zero one is equal to 1. In that case we have $\delta_D(\{\mathfrak{p} \in H\}) = 0$, as claimed. $\square$

9.5 The Second Inequality: alternative proof

In this section we give a new proof of the second inequality using Theorem 9.28.

Theorem 9.30 (Second Inequality). *Let K be a number field and L a Galois extension of K . If $\mathfrak{m}$ is a modulus for K then*

$$[I_K^{S(\mathfrak{m})} : K_{\mathfrak{m},1} \cdot \text{Norm}_{L/K}(I_L^{S(\mathfrak{m})})] \leq [L : K].$$

Proof. Set $H := K_{\mathfrak{m},1} \cdot \text{Norm}_{L/K}(I_L^{S(\mathfrak{m})})$. We can apply Theorem 9.28 to H and we obtain that $\delta_D(\{\mathfrak{p} \in H\})$ is either 0 or $\frac{1}{[I_K^{S(\mathfrak{m})}:H]}$. We claim that it cannot be zero. To see that, note that if $\mathfrak{p}$ is a prime ideal of K which is completely split in L then $f(\mathfrak{q}/\mathfrak{p}) = 1$ for any ideal $\mathfrak{q}$ of L dividing $\mathfrak{p}$ and in particular, $\mathfrak{p} = \text{Norm}_{L/K}(\mathfrak{q})$. So H contains the set of prime ideals of K that split completely in L and that do not divide $\mathfrak{m}$. Since the latter set is finite, we know by Theorem 9.17 that this set has (polar, hence Dirichlet) density equal to $\frac{1}{[L:K]}$. This yields

$$\delta_D(\{\mathfrak{p} \in H\}) \geq \frac{1}{[L : K]},$$

and we see that it cannot be zero. Hence $\delta_D(\{\mathfrak{p} \in H\}) = \frac{1}{[I_K^{S(\mathfrak{m})}:H]}$ and we obtain

$$[I_K^{S(\mathfrak{m})} : H] \leq [L : K].$$

□

Remark 9.31. Note also that in the proof of Theorem 9.30, we have also obtained that for all non trivial character $\chi : I_K^{S(\mathfrak{m})}/K_{\mathfrak{m},1} \cdot \text{Norm}_{L/K}(I_L^{S(\mathfrak{m})}) \rightarrow \mathbf{C}^\times$, we have $L(1, \chi) \neq 0$.

9.6 Chebotarev Density Theorem

We will now use global class field theory to prove Chebotarev's density theorem. Let us first note that we have the following result:

Theorem 9.32. *Let K be a number field and let $\mathfrak{m}$ be a modulus for K . For any non-trivial character $\chi : C_{\mathfrak{m}} \rightarrow \mathbf{C}^\times$, we have $L(1, \chi) \neq 0$.*

Proof. Let $\chi : C_{\mathfrak{m}} \rightarrow \mathbf{C}^\times$ be a non-trivial character. From Existence Theorem (Theorem 2.10) we know that there exists L/K a finite abelian extension such that

$$\ker(\chi) = \text{Norm}_{L/K}(C_{\mathfrak{m},L}).$$

The result then follows from Remark 9.31. □

Theorem 9.33. *Let K be a number field and let $\mathfrak{m}$ be a modulus for K . Let H be a subgroup of $I_K^{S(\mathfrak{m})}$ such that H contains $K_{\mathfrak{m},1}$. For any class $\mathfrak{c}$ in $I_K^{S(\mathfrak{m})}/H$, then the set of prime ideals in $\mathfrak{c}$ has Dirichlet density equal to $\frac{1}{[I_K^{S(\mathfrak{m})}:H]}$.*

Proof. By Theorem 9.28, it suffices to prove that for any non-trivial character $\chi : I_K^{S(\mathfrak{m})} \rightarrow \mathbf{C}^\times$ trivial on $\mathfrak{c}H$, we have $L(1, \chi)$ is non zero. This follows from Theorem 9.32. $\square$

Corollary 9.34. *Let L/K be a finite abelian extension with Galois group G and let g be a fixed element in G . Then the set of prime ideals $\mathfrak{p}$ in K that are unramified in L and for which $(\mathfrak{p}, L/K) = g$ has Dirichlet density equal to $\frac{1}{[L:K]}$.*

Proof. From Reciprocity Law (Theorem 2.9), we know that there exists a modulus $\mathfrak{m}$ of K such that the Artin map induces an isomorphism

$$I_K^{S(\mathfrak{m})}/K_{\mathfrak{m},1} \cdot \text{Norm}_{L/K}(I_L^{S(\mathfrak{m})}) \xrightarrow{\sim} \text{Gal}(L/K).$$

The corollary follows from Theorem 9.33 applied to the group $H = K_{\mathfrak{m},1} \cdot \text{Norm}_{L/K}(I_L^{S(\mathfrak{m})})$ and to $\mathfrak{c}$ equal to the inverse image of the element g . $\square$

Theorem 9.35 (Chebotarev's density theorem). *Let L be a finite Galois extension of a number field K with Galois group G , and let C be a subset of G stable under conjugation. Let T be the set of prime ideals $\mathfrak{p}$ of K such that $\mathfrak{p}$ is unramified in L and $(\mathfrak{p}, L/K)$ is in C . Then,*

$$\delta_D(T) = \frac{\text{number of elements in } C}{\text{number of elements in } G}.$$

Proof. Let us denote by d the degree $[L : K]$ and c the order of C so that we have to show that $\delta_D(T) = \frac{c}{d}$. Note that if $C = \bigcup_i C_i$ is the union of distinct conjugacy classes, then we can write $T = \bigcup_i T_i$ where T_i is the set of prime ideals $\mathfrak{p}$ of K such that $\mathfrak{p}$ is unramified in L and $(\mathfrak{p}, L/K)$ is in C_i . Hence, it suffices to prove the theorem for each one of the C_i . Let us then assume that C is the conjugacy class of an element g of G :

$$C := \{hgh^{-1} \mid h \in G\}.$$

Let us denote by f the order of g in G and let $M := L^{\langle g \rangle}$ so that L is a cyclic extension of M of degree f . From Reciprocity Law (Theorem 2.9), we know that there exists a modulus $\mathfrak{m}$ of M such that the Artin map induces an isomorphism

$$I_M^{S(\mathfrak{m})}/M_{\mathfrak{m},1} \cdot \text{Norm}_{L/M}(I_L^{S(\mathfrak{m})}) \xrightarrow{\sim} \text{Gal}(L/M) \simeq \langle g \rangle.$$

Consider the set

$$T_{M,g} := \{\mathfrak{q}_M \text{ prime ideal of } M \mid \mathfrak{q}_M \nmid \mathfrak{m}, (\mathfrak{q}_L, L/M) = g, f(\mathfrak{q}_M/\mathfrak{q}_M \cap \mathcal{O}_K) = 1\}.$$

Note that when it comes to density problem the condition $\mathfrak{q}_M \nmid \mathfrak{m}$ does not matter since the set of places dividing $\mathfrak{m}$ is finite. Corollary 9.34 states that the set of prime ideals $\mathfrak{q}_M$ such that $(\mathfrak{q}_L, L/M) = g$ has density $\frac{1}{f}$ and reasoning as in the proof of Proposition 9.27, we see that in fact $\delta_D(T_{M,g}) = \frac{1}{f}$. We define also the set:

$$T_{L,g} := \{\mathfrak{q}_L \text{ prime ideal of } L \mid \mathfrak{q}_L \cap \mathcal{O}_M \nmid \mathfrak{m}, (\mathfrak{q}_L, L/K) = g\}.$$

We make the following claim:

Claim 9.36. (1) The map $\mathfrak{q}_L \mapsto \mathfrak{q}_L \cap \mathcal{O}_M$ induces a bijection between $T_{L,g}$ and $T_{M,g}$.

(2) The map $\mathfrak{q}_L \mapsto \mathfrak{q}_L \cap \mathcal{O}_K$ from $T_{L,g}$ to T sends exactly $\frac{d}{cf}$ primes of $T_{L,g}$ to each prime of T .

Assuming that the claim is true, we obtain that the map $\mathfrak{q}_M \mapsto \mathfrak{q}_M \cap \mathcal{O}_K$ is a $(\frac{d}{cf} : 1)$ -map from $T_{M,g}$ to T . For $\mathfrak{q}_M$ in $T_{M,g}$, we have $\text{Norm}_{M/K}(\mathfrak{q}_M) = \mathfrak{q}_M \cap \mathcal{O}_K$ and so $N(\mathfrak{q}_M) = N(\mathfrak{q}_M \cap \mathcal{O}_K)$. Thus, we obtain

$$\sum_{\mathfrak{p} \in T} \frac{1}{N(\mathfrak{p})^s} = \frac{cf}{d} \sum_{\mathfrak{q}_M \in T_{M,g}} \frac{1}{N(\mathfrak{q}_M)^s} \sim \frac{cf}{d} \frac{1}{f} \log \frac{1}{s-1} = \frac{c}{d} \log \frac{1}{s-1},$$

and this proves the theorem.

Proof of Claim 9.36. We first prove (1). We first prove that the map $T_{L,g} \rightarrow T_{M,g}$ is well defined. Let us take $\mathfrak{q}_L$ in $T_{L,g}$ and write $\mathfrak{q}_M := \mathfrak{q}_L \cap \mathcal{O}_M$ and $\mathfrak{p} := \mathfrak{q}_L \cap \mathcal{O}_K$. Since the Galois group of $L_{\mathfrak{q}_L}/K_{\mathfrak{p}}$ is equal to $\langle g \rangle$ (because $\mathfrak{q}_L$ is in $T_{L,g}$) and since g fixes $M_{\mathfrak{q}_M}$, we obtain that $M_{\mathfrak{q}_M} = K_{\mathfrak{p}}$. Thus $f(\mathfrak{q}_M/\mathfrak{p})$ is equal to 1 and $\mathfrak{q}_M$ is in $T_{M,g}$, as wanted.

Let us show that this map is bijective. We have

$$f(\mathfrak{q}_L/\mathfrak{q}_M) = f(\mathfrak{q}_M/\mathfrak{p})^{-1} f(\mathfrak{q}_L/\mathfrak{p}) = f,$$

and we see that $\mathfrak{q}_L$ is the only prime ideal of L dividing $\mathfrak{q}_M$. So the map is injective. For the surjectivity, note that if $\mathfrak{q}_M$ is in $T_{M,g}$, then for any $\mathfrak{q}_L$ dividing it, we have

$$(\mathfrak{q}_L, L/M) = (\mathfrak{q}_L, L/K)^{f(\mathfrak{q}_M/\mathfrak{p})}$$

and since $f(\mathfrak{q}_M/\mathfrak{p}) = 1$, we obtain

$$(\mathfrak{q}_L, L/M) = (\mathfrak{q}_L, L/K).$$

Since $\mathfrak{q}_M$ is in $T_{M,g}$, then $(\mathfrak{q}_L, L/M) = g$ and so $(\mathfrak{q}_L, L/K) = g$. It follows that $\mathfrak{q}_L$ is in $T_{L,g}$, as wanted.

Let us now show the second point. Let $\mathfrak{p}$ be in T . We want to show that there are exactly $\frac{d}{cf}$ primes in $T_{L,g}$ dividing $\mathfrak{p}$. Fix $\mathfrak{q}_{L,0}$ a prime in $T_{L,g}$ dividing $\mathfrak{p}$. Let us write $C_G(g) = \{h \in G \mid hg = gh\}$ the centralizer of g in G . Since

$$(h \cdot \mathfrak{q}_{L,0}, L/K) = h(\mathfrak{q}_{L,0}, L/K)h^{-1},$$

the map $h \mapsto h \cdot \mathfrak{q}_{L,0}$ defines a bijection

$$C_G(g)/G_{\mathfrak{q}_{L,0}} \rightarrow \{\mathfrak{q}_L \in T_{L,g} \mid \mathfrak{q}_L \cap \mathcal{O}_K = \mathfrak{p}\}$$

where $G_{\mathfrak{q}_{L,0}}$ is the decomposition subgroup. But we have $G_{\mathfrak{q}_{L,0}} = \langle g \rangle$, in particular, it has order f . Since $h \mapsto hgh^{-1}$ gives a bijection $G/C_G(g) \xrightarrow{\sim} C$, we also have that $C_G(g)$ has order $\frac{d}{c}$. Hence $C_G(g)/G_{\mathfrak{q}_{L,0}}$ has order $\frac{d}{cf}$. It follows that

$$|\{\mathfrak{q}_L \in T_{L,g} \mid \mathfrak{q}_L \cap \mathcal{O}_K = \mathfrak{p}\}| = \frac{d}{cf},$$

as wanted. □

□

Remark 9.37. It can be proved that the above theorem also holds if we replace Dirichlet densities δ_D by the natural densities δ_{nat} .

10 Restricted ramification

Let K be a number field. For S a (possibly infinite) set of places of K that contains S_∞ , we write K_S/K the maximal extension which is unramified outside of S . We also define $G_S := \text{Gal}(K_S/K)$. If v is a finite place of K and w a place of K_S that divides v (i.e. a prolongation of v to K_S) then we write

$$K_{S,w} := \text{colim}_{K_S/L/K} L_{w_L},$$

where the colimit runs over the subextensions $L \subset K_S$ of K and $w_L := w \cap L$.

From now on, we will specify the field in the notation for the S -units, i.e. we will write

$$U_K(S) := \{x \in K^\times \mid \text{ord}_v(x) = 0 \text{ for all } v \notin S\},$$

$$U_L(S) := \{x \in L^\times \mid \text{ord}_w(x) = 0 \text{ for all } w \text{ such that } w \cap K \notin S\} \text{ for } L/K \text{ finite extension,}$$

$$U_{K_S}(S) := \bigcup_{K_S/L/K} U_L(S).$$

We define the group of S -idèles of K as the restricted product

$$\mathbb{I}_{K,S} := \prod_{v \in S} (K_v^\times, \mathcal{O}_v^\times),$$

i.e. its elements are sequences of the form $(a_v)_{v \in S}$ such that a_v is in $K_v^\times$ for all v in S and a_v is in U_v for almost all v . Recall from Lemma 5.12 that if L/K is a finite Galois extension with Galois group G and v a place of K and $w(v)$ any place of L that divides v , we have:

$$\prod_{w|v} L_w^\times \xrightarrow{\sim} \text{Ind}_{G_{w(v)}}^G (L_{w(v)}^\times) \quad \text{and} \quad \prod_{w|v} U_{L,w} \xrightarrow{\sim} \text{Ind}_{G_{w(v)}}^G (U_{L,w(v)}).$$

Hence, if L/K is finite Galois with Galois group G , we define $\mathbb{I}_{L/K,S}$ as the restricted product:

$$(10.0.1) \quad \mathbb{I}_{L/K,S} := \prod_{v \in S} (\text{Ind}_{G_{w(v)}}^G (L_{w(v)}^\times), \text{Ind}_{G_{w(v)}}^G (U_{L,w(v)})).$$

We define the group of S -idèles of K_S as the colimit

$$\mathbb{I}_{K_S,S} := \text{colim}_{L/K} \mathbb{I}_{L/K,S},$$

where the colimit runs over the subextensions $L \subset K_S$ of K .

Let us consider the following class groups:

$$\mathbb{C}_{K,S} := \mathbb{I}_{K,S}/U_K(S), \quad \text{and} \quad \mathbb{C}_{K_S,S} := \text{colim}_{L/K} \mathbb{C}_{L,S},$$

where the colimits run over the subextensions $L \subset K_S$ of K . Since taking colimit is exact, we have:

$$(10.0.2) \quad 0 \rightarrow U_{K_S}(S) \rightarrow \mathbb{I}_{K_S,S} \rightarrow \mathbb{C}_{K_S,S} \rightarrow 0.$$

We would like this group $\mathbb{C}_{K,S}$ to play the same role as $\mathbb{C}_K$ in the restricted ramification theory, however it does not satisfy Galois descent, i.e. in general it is not true that for L/K finite Galois, the group $\mathbb{C}_{K,S}$ is isomorphic to $(\mathbb{C}_{L,S})^{\text{Gal}(L/K)}$. Instead, we need to consider the following variant:

$$U_{K,S} := \prod_{v \in S} \{1\} \times \prod_{v \notin S} U_v, \quad \text{and} \quad U_{K_S,S} := \text{colim}_{L/K} U_{L,S},$$

$$\mathbb{C}_S(K) := \mathbb{C}_K/U_{K,S} \simeq \mathbb{I}_K/K^\times \cdot U_{K,S}, \quad \text{and} \quad \mathbb{C}_S(K_S) := \text{colim}_{L/K} \mathbb{C}_S(L).$$

We have:

Proposition 10.1. *The group $\mathbb{C}_{K,S}$ is an open subgroup of $\mathbb{C}_S(K)$. Moreover, there is an exact sequence*

$$0 \rightarrow \mathbb{C}_{K,S} \rightarrow \mathbb{C}_S(K) \rightarrow C_{K,S} \rightarrow 0$$

where $C_{K,S}$ is the ideal class group of the ring $\mathcal{O}_{K,S} := \{x \in K \mid \text{ord}_v(x) \geq 0 \text{ for all } v \notin S\}$ (in other words, $C_{K,S}$ is the quotient of the usual ideal class group C_K of K by the subgroup generated by the classes of all places in S). In particular, if S omits only finitely many primes then $C_{K,S}$ is trivial and hence $\mathbb{C}_{K,S} = \mathbb{C}_S(K)$.

Proof. There is a canonical injection $\mathbb{I}_{K,S} \hookrightarrow \mathbb{I}_K$ which induces a morphism

$$j : \mathbb{I}_{K,S} \rightarrow \mathbb{I}_K / K^\times U_{K,S} = \mathbb{C}_S(K)$$

and the set $j(\mathbb{I}_{K,S})$ is closed. We claim that its kernel is equal to

$$(10.0.3) \quad \text{Ker}(j) = U_K(S).$$

Indeed, if we take α an element in $\mathbb{I}_{K,S}$ such that $j(\alpha) = 1$ and if we write $\tilde{\alpha}$ its image in $\mathbb{I}_K$, we can write $\tilde{\alpha} = \lambda \cdot u$ with λ in $K^\times$ and u in $U_{K,S}$. In other words, we have

$$\begin{aligned} \alpha_v &= \tilde{\alpha}_v = \lambda & \text{if } v \in S, \\ 1 &= \tilde{\alpha}_v = \lambda \cdot u_v & \text{if } v \notin S. \end{aligned}$$

So we can write $\alpha = \lambda$ with λ in $U_K(S)$ and this proves (10.0.3). We obtain an injective map with closed image

$$j : \mathbb{C}_{K,S} \hookrightarrow \mathbb{C}_S(K).$$

We need to compute its cokernel. We have

$$\begin{aligned} \mathbb{I}_K / (\mathbb{I}_{K,S} U_{K,S} K^\times) &= \left(\bigoplus_{v \notin S} K_v^\times / U_v \right) / K^\times \\ &= \left(\bigoplus_{v \notin S} \mathbb{Z} \right) / K^\times \\ &\simeq C_{S,K}, \end{aligned}$$

as wanted. Since the ideal class group is finite, we see also that $\mathbb{C}_{K,S}$ has finite index in $\mathbb{C}_K$, so it is open.

When S is almost all places, then $\mathcal{O}_{K,S}$ is a Dedekind ring¹ with only finitely many prime ideals and in particular, it is a principal ideal domain. It follows that $C_{K,S}$ is trivial and $\mathbb{C}_{K,S} = \mathbb{C}_S(K)$. $\square$

Let us write $N(S) := \{n \in \mathbb{N} \mid n \in U_K(S)\}$.

Lemma 10.2. *If n is in $N(S)$, there is an exact sequence of G_S -modules:*

$$(10.0.4) \quad 0 \rightarrow \mu_n \rightarrow U_{K_S}(S) \xrightarrow{n} U_{K_S}(S) \rightarrow 0.$$

Proof. If v is not in S , then $\text{ord}_v(n) = 0$ so $K_v(\mu_n)/K_v$ is unramified. This means that $K(\mu_n) \subset K_S$. Choose x in $U_{K_S}(S)$ and consider the extension $L := K(\mu_n, x)$. If v is not in S then both n and x are units in L_v so the extension $L_v(x^{\frac{1}{n}})/L_v$ is unramified. In other words $L(x^{\frac{1}{n}})/L$ is a subextension of K_S/L and so $x^{\frac{1}{n}}$ is in $U_{K_S}(S)$, as wanted. $\square$

¹If S contains at least one finite place, then $\mathcal{O}_{K,S}$ is always a Dedekind ring. This is because $\mathcal{O}_{K,S}$ is equal to the localization of $\mathcal{O}_K$ with respect to the set of prime $\mathfrak{p}$ which are not in S . The properties of being noetherian and integrally closed are preserved by localization. Since we have assumed that at least one prime ideal survives localization, then we see that the dimension 1 property is also satisfied.

We have the following result:

Proposition 10.3. *There are a natural isomorphisms $\mathbb{C}_S(K_S) \simeq \mathbb{C}_{K_S,S}$ and $\mathbb{C}_{K_S,S}^{G_S} \simeq \mathbb{C}_S(K)$.*

Proof. Let K_0 be the abelian maximal extension of K inside K_S in which all primes of S split completely. Then the Artin map induces an isomorphism between $C_{K,S}$ and $\text{Gal}(K_0/K)$ (see Claim 11.14), in other words, every ideal of $\mathcal{O}_{K,S}$ becomes a principal ideal in K_0/K . Hence

$$\varinjlim_{L/K} C_{S,L} = 0.$$

Passing the colimit in the exact sequence from Proposition 10.1, we obtain

$$(10.0.5) \quad \mathbb{C}_{K_S,S} \simeq \mathbb{C}_S(K_S),$$

as wanted.

For the second part of the statement, consider the exact sequence

$$0 \rightarrow U_{K_S,S} \rightarrow \varinjlim_{L/K} \mathbb{C}_L \rightarrow \mathbb{C}_{K_S,S} \rightarrow 0$$

coming from (10.0.5). Taking the G_S -cohomology, we obtain a long exact sequence:

$$0 \rightarrow U_{K,S} \rightarrow \mathbb{C}_K \rightarrow \mathbb{C}_{K_S,S}^{G_S} \rightarrow H^1(G_S, U_{K_S,S}).$$

But for L/K subextension of K_S/K , a place v not in S and w dividing v , then U_w has no higher cohomology so $H^1(G_S, U_{K_S,S}) = 0$. We obtain $\mathbb{C}_{K_S,S}^{G_S} \simeq \mathbb{C}_K/U_{K,S} = \mathbb{C}_S(K)$. $\square$

If L/K is Galois, there is an exact sequence of $\text{Gal}(L/K)$ -modules,

$$0 \rightarrow U_{L,S} \rightarrow \mathbb{C}_L \rightarrow \mathbb{C}_S(L) \rightarrow 0.$$

If L/K is moreover a subextension of K_S/K and v not in S , then we know that for w dividing v , then U_w is cohomologically trivial². It follows that $U_{L,S}$ itself is cohomologically trivial and we obtain:

Proposition 10.4. *Let L/K be a finite Galois subextension of K_S/K . Then for all i in $\mathbb{Z}$, we have*

$$\widehat{H}^i(\text{Gal}(L/K), \mathbb{C}_S(L)) \simeq \widehat{H}^i(\text{Gal}(L/K), \mathbb{C}_L).$$

We can now compute the cohomology of the S -idèles and the S -class group:

²i.e. the higher cohomology groups $H^i(H, U_w)$ are trivial for any closed subgroup H of G_v .

Proposition 10.5. *Let K be a number field. Then we have,*

$$\begin{aligned} H^0(G_S, \mathbb{I}_{K_S, S}) &= \mathbb{I}_{K, S}, \\ H^1(G_S, \mathbb{I}_{K_S, S}) &= 0, \\ H^2(G_S, \mathbb{I}_{K_S, S})(p) &= \bigoplus_{v \in S} \text{Br}(K_v)(p) \quad \text{for all prime numbers } p \text{ in } N(S), \\ H^3(G_S, \mathbb{I}_{K_S, S}) &= 0, \end{aligned}$$

and,

$$\begin{aligned} H^0(G_S, \mathbb{C}_{K_S, S}) &= \mathbb{C}_S(K), \\ H^1(G_S, \mathbb{C}_{K_S, S}) &= 0, \\ H^2(\text{Gal}(L/K), \mathbb{C}_{L/K, S}) &= \frac{1}{|\text{Gal}(L/K)|} \mathbb{Z}/\mathbb{Z}, \quad \text{for all finite Galois extension } K_S/L/K, \\ H^3(G_S, \mathbb{C}_{K_S, S}) &= 0. \end{aligned}$$

Proof. We only prove the results for i in $\{0, 1, 2\}$.

To compute the cohomology of the idèles, we proceed exactly as in the proofs of Proposition 5.13 and Corollary 5.14 and we get that for L/K a finite Galois subextension of K_S/K , we have

$$\begin{aligned} H^0(\text{Gal}(L/K), \mathbb{I}_{L, S}) &= \mathbb{I}_{K, S}, \\ H^1(\text{Gal}(L/K), \mathbb{I}_{L, S}) &= 0, \\ H^2(\text{Gal}(L/K), \mathbb{I}_{L, S}) &= \bigoplus_{v \in S} \text{Br}(L_{w(v)}/K_v) \simeq \bigoplus_{v \in S} \frac{1}{n_v} \mathbb{Z}/\mathbb{Z} \end{aligned}$$

where we choose some place $w(v)$ above v and $n_v := [L_{w(v)} : K_v]$.

We then take the limit over L/K . The result for $i = 0$ and $i = 1$ immediately follows. If p is a prime number in $N(S)$, then $K(\mu_{p^n})/K$ is contained in K_S/K for all n and so we have

$$\varinjlim_{K_S/L/K} \text{Br}(L_{w(v)}/K_v)(p) \simeq \mathbb{Q}_p/\mathbb{Z}_p$$

when v is non-archimedean (in the colimit the transitive maps are the natural maps

$$\text{Br}(L_{w,1}) = \frac{1}{[L_{w,1} : K_v]} \mathbb{Z}/\mathbb{Z} \rightarrow \frac{1}{[L_{w,2} : K_v]} \mathbb{Z}/\mathbb{Z} = \text{Br}(L_{w,2}) \text{ for } L_{w,2}/L_{w,1}/K_v$$

and we have used that $\mathbb{Q}_p/\mathbb{Z}_p = \text{colim}_{p^n} \frac{1}{p^n} \mathbb{Z}/\mathbb{Z}$).

When v is infinite, the group $H^2(\text{Gal}(L_w/K_v), L_w^\times)$ is either trivial or has order 2. If 2 is in $N(S)$ then $L := K(i)$ is in K_S/K and we have $H^2(\text{Gal}(L_w/K_v), L_w^\times) = \frac{1}{2} \mathbb{Z}/\mathbb{Z}$ when v is real.

In any case we obtain

$$H^2(G_S, \mathbb{I}_{K_S, S})(p) = \bigoplus_{v \in S} \text{Br}(K_v)(p).$$

Let us now compute the cohomology of $\mathbb{C}_{K_S, S}$. The H^0 -group was computed in Proposition 10.3. We have also seen in Proposition 10.3 that $\mathbb{C}_{K_S, S} \simeq \varinjlim_{K_S/L/K} \mathbb{C}_S(L)$ and from Proposition 10.4, we know that for $i \geq 1$,

$$H^i(\text{Gal}(L/K), \mathbb{C}_S(L)) \simeq H^i(\text{Gal}(L/K), \mathbb{C}_L).$$

So the result follows from Theorem 6.1. □

The above proposition together with exact sequence (10.0.2) yields:

Proposition 10.6. *Let K be a number field. Then we have,*

$$\begin{aligned} H^0(G_S, U_{K_S}(S)) &= U_K(S), \\ H^1(G_S, U_{K_S}(S)) &= C_{K, S} \quad \text{where } C_{K, S} \text{ is the ideal class group of } \mathcal{O}_{K, S}, \\ H^2(G_S, U_{K_S}(S))(p) &= \text{Ker}\left(\bigoplus_{v \in S} H^2(\text{Gal}(\overline{K}_v/K_v), \mu_{p^\infty}) \rightarrow H^2(G_S, \mathbb{C}_{K_S, S})(p)\right) \\ &= \begin{cases} \text{Ker}\left(\bigoplus_{v \in S \setminus S_\infty} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\Sigma} \mathbb{Q}_p/\mathbb{Z}_p\right) & \text{if } p \neq 2 \\ \text{Ker}\left(\left(\bigoplus_{v \in S \setminus S_\infty} \mathbb{Q}_2/\mathbb{Z}_2 \oplus \bigoplus_{v \in S_R} \frac{1}{2}\mathbb{Z}/\mathbb{Z}\right) \xrightarrow{\Sigma} \mathbb{Q}_2/\mathbb{Z}_2\right) & \text{if } p = 2 \end{cases}, \\ &\quad \text{for all prime numbers } p \text{ in } N(S), \\ H^3(G_S, U_{K_S}(S))(p) &= 0, \quad \text{for all prime numbers } p \text{ in } N(S), \end{aligned}$$

Proof. We only do the proof for $i \in \{0, 1, 2\}$. The case $i = 0$ is trivial. In higher degree, we use the exact sequence:

$$0 \rightarrow U_{K_S}(S) \rightarrow \mathbb{I}_{K_S, S} \rightarrow \mathbb{C}_{K_S, S} \rightarrow 0$$

and the computations from Proposition 10.5. If $i = 1$, we obtain an exact sequence

$$\mathbb{I}_{K, S} \rightarrow \mathbb{C}_S(K) \rightarrow H^1(G_S, U_{K_S}(S)) \rightarrow 0$$

and we have already seen in the proof of Proposition 10.1 that the quotient $\mathbb{C}_S(K)/\mathbb{I}_{K, S} = \mathbb{I}_K/(\mathbb{I}_{K, S}U_{K, S}K^\times)$ is isomorphic to $C_{K, S}$.

For $i = 2$ and if $p \neq 2$, we have a commutative diagram where the first row is exact:

$$\begin{array}{ccccc} 0 & \longrightarrow & H^2(G_S, U_{K_S}(S))(p) & \longrightarrow & H^2(G_S, \mathbb{C}_{K_S, S})(p) \\ & & \sim \downarrow & & \downarrow \sim \\ & & \bigoplus_{v \in S \setminus S_\infty} \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\Sigma} & \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

If $p = 2$, the above diagram becomes

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(G_S, U_{K_S}(S))(2) & \longrightarrow & H^2(G_S, \mathbb{I}_{K_S, S})(2) & \longrightarrow & H^2(G_S, \mathbb{C}_{K_S, S})(2) . \\
& & & & \downarrow \sim & & \downarrow \sim \\
& & \bigoplus_{v \in S \setminus S_\infty} \mathbb{Q}_2/\mathbb{Z}_2 \oplus \bigoplus_{v \in S_{\mathbb{R}}} \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\Sigma} & \mathbb{Q}_2/\mathbb{Z}_2 & &
\end{array}$$

□

Using Tate's theorem (Theorem 5.1), we obtain the global reciprocity law for restricted ramification.

Theorem 10.7. *Let L/K be a finite Galois extension inside K_S . Then there is a canonical isomorphism*

$$\mathbb{C}_S(K)/\text{Norm}_{L/K}(\mathbb{C}_S(L)) \simeq \text{Gal}(L/K).$$

11 Duality for cohomology of number fields

In this section we investigate duality theorems for number fields. In particular, we prove Poitou-Tate duality, which allows to relate local and global duality results.

11.1 Global duality

The notations are the same as in the previous section: K is a number field and S a (possibly infinite) set of places of K that contains S_∞ . We write K_S/K the maximal extension which is unramified outside of S and $G_S := \text{Gal}(K_S/K)$. If v is a finite place of K and w a place of K_S that divides v (i.e. a prolongation of v to K_S) then we write

$$K_{S,w} := \text{colim}_{K_S/L/K} L_{w_L},$$

where the colimit runs over the subextensions $L \subset K_S$ of K and $w_L := w \cap L$.

11.1.1 General duality result

Let us recall the general duality result for cohomology of profinite groups. Let G be a profinite group and let M be a discrete module for G such that for all open subgroups $V \subset U \subset G$ such V is normal in U ,

(i) there exists an invariant isomorphism $\text{inv}_{U/V} : H^2(U/V, M^V) \xrightarrow{\sim} \frac{1}{[U:V]} \mathbb{Z}/\mathbb{Z}$,

(ii) the group $H^1(U/V, M^V)$ is trivial,

(iii) if $W \subset V$ is an open normal subgroup of U , the invariant morphisms are compatible, i.e. there is a commutative diagram:

$$\begin{array}{ccccc} H^2(U/V, M^V) & \xrightarrow{\text{inf}} & H^2(U/W, M^W) & \xrightarrow{\text{res}} & H^2(V/W, M^W) \\ \text{inv} \downarrow \sim & & \text{inv} \downarrow \sim & & \text{inv} \downarrow \sim \\ \frac{1}{[U:V]} \mathbf{Z}/\mathbf{Z} & \xrightarrow{\text{can}} & \frac{1}{[U:W]} \mathbf{Z}/\mathbf{Z} & \xrightarrow{[U:V]} & \frac{1}{[V:W]} \mathbf{Z}/\mathbf{Z} \end{array}$$

Then, if A is a discrete G -module which is finitely generated and free as a $\mathbf{Z}$ -module, for all $i \in \mathbf{Z}$, the cup-product

$$\widehat{H}^i(G, \text{Hom}(A, M)) \times \widehat{H}^{2-i}(G, A) \xrightarrow{\cup} H^2(G, M),$$

induces a topological isomorphism

$$\widehat{H}^i(G, \text{Hom}(A, M)) \xrightarrow{\sim} \widehat{H}^{2-i}(G, A)^\vee,$$

where the topology on each side is defined in the following way:

- (•) if $i > 0$, the groups $\widehat{H}^i(G, A)$ are equipped with the discrete topology,
- (•) if $i \leq 0$, the groups $\widehat{H}^i(G, A) = \varprojlim_U \widehat{H}^i(G/U, A^U)$ are equipped with the profinite topology,
- (•) if $i > 0$, the groups $\widehat{H}^i(G, \text{Hom}(A, M))$ are equipped with the discrete topology,
- (•) if $i \leq 0$, the groups $\widehat{H}^i(G, \text{Hom}(A, M)) = \varprojlim_U \widehat{H}^i(G/U, \text{Hom}(A, M)^U)$ are equipped with the profinite topology.

Here $(\cdot)^\vee$ denote the Pontryagin dual, i.e. $\text{Hom}(-, \mathbf{Q}/\mathbf{Z})$ equipped with the compact-open topology.

11.1.2 Duality theorem for number fields

Let L/K be a Galois extension of number fields with Galois group G . It can be checked that the conditions (i), (ii) and (iii) from Section 11.1.1 are satisfied by the G -module $\mathbb{C}_S(L)$. Hence, we have the following duality result:

Theorem 11.1. *Let L/K be a Galois extension of number fields, which is unramified outside S . Let G be its Galois group and A be a G -module, which is finitely generated and free as a $\mathbf{Z}$ -module. Then for all i in $\mathbf{Z}$, the cup-product*

$$\widehat{H}^i(G, \text{Hom}(A, \mathbb{C}_S(L))) \times \widehat{H}^{2-i}(G, A) \xrightarrow{\cup} H^2(G, \mathbb{C}_S(L)),$$

induces a topological isomorphism

$$\widehat{H}^i(G, \text{Hom}(A, \mathbb{C}_S(L))) \xrightarrow{\sim} \widehat{H}^{2-i}(G, A)^\vee,$$

11.2 Passage from global to local

Let K be a number field and S be a set (possibly infinite) of places of K .

If v is a place of K , we write G_v for the Galois group $\text{Gal}(\overline{K}_v/K_v)$. If A is a G_v -module, we say that A is unramified if $A^{I_v} = A$, where $I_v := \text{Gal}(\overline{K}_v/K_v^{\text{unr}})$. If A is a G_S -module which is finitely generated as a $\mathbf{Z}$ -module then there exists a finite extension $K_S/K'/K$ such that A is fixed by $\text{Gal}(K^S/K')$. In particular, A is an unramified G_v -module for all primes v which are unramified in K'/K . Hence, A is unramified at v for almost all primes v of K .

We denote by $\text{Mod}_S(G_S)$ the category of discrete G_S -modules A which are finitely generated as $\mathbf{Z}$ -modules and whose torsion has order in $N(S)$.

11.2.1 Case of finite modules

If A is in $\text{Mod}_S(G_S)$ and A finite then we define its dual G_S -module A' by

$$A' := \text{Hom}(A, U_{K_S}(S)) = \text{Hom}(A, \mu(K_S)) \in \text{Mod}_S(G_S).$$

Let us write n the order of A . Note that since n in $N(S)$ by assumption, the field K_S contains all the n -th roots of 1 in $\overline{K}$ (since for v not in S , the extension $K_v(\mu_n)/K_v$ is unramified) and we see that A' is finite of order n . We also have $(A')' = A$.

If A is in $\text{Mod}_S(G_S)$, we set

$$H^i(K_v, A) := \begin{cases} H^i(G_v, A) & \text{if } v \text{ is non-archimedean,} \\ \widehat{H}^i(G_v, A) & \text{if } v \text{ is archimedean.} \end{cases}$$

If v is non-archimedean and A unramified at v , we define the unramified cohomology groups as

$$H_{\text{unr}}^i(K_v, A) := \text{Im}(H^i(G_v/I_v, A) \rightarrow H^i(G_v, A)).$$

If A is finite and unramified at v non-archimedean, then,

$$\begin{aligned} H_{\text{unr}}^0(K_v, A) &\simeq H^0(K_v, A) \\ H_{\text{unr}}^1(K_v, A) &\simeq H^1(\text{Gal}(\overline{k}_v/k_v), A) \\ H_{\text{unr}}^2(K_v, A) &= 0 \\ H_{\text{unr}}^i(K_v, A) &= H^i(K_v, A) = 0 \text{ for all } i \geq 3. \end{aligned}$$

Since in general A is unramified at almost all v , we can define the restricted product:

$$P^i(G_S, A) := \prod_{v \in S} (H^i(K_v, A), H_{\text{unr}}^i(K_v, A)),$$

where the cohomology groups are given the discrete topology (recall that when A is finite, the groups $H^i(K_v, A)$ are finite). In particular, we obtain:

$$\begin{aligned} P^0(G_S, A) &= \prod_{v \in S \setminus S_\infty} H^0(K_v, A) \times \prod_{v \in S_\infty} \widehat{H}^0(K_v, A) \text{ is compact,} \\ P^1(G_S, A) &= \prod_{v \in S} (H^1(K_v, A), H_{\text{unr}}^1(K_v, A)) \text{ is locally compact,} \\ P^2(G_S, A) &= \bigoplus_{v \in S} H^2(K_v, A) \text{ is discrete,} \\ P^i(G_S, A) &= \bigoplus_{v \in S_\infty} H^i(K_v, A) \text{ is finite for all } i \geq 3. \end{aligned}$$

For A in $\text{Mod}_S(G_S)$ finite and v non-archimedean, we know from local duality theorem that for $0 \leq i \leq 2$, the cup-product

$$H^i(K_v, A) \times H^{2-i}(K_v, A') \xrightarrow{\cup} \text{Br}(K_v) \xrightarrow{\text{inv}_v} \mathbf{Q}/\mathbf{Z}$$

induces isomorphisms

$$\Theta_v^i : H^i(K_v, A) \rightarrow H^{2-i}(K_v, A')^\vee$$

We have:

Proposition 11.2. *Let A be in $\text{Mod}_S(G_S)$ and assume that it is finite. Then for $0 \leq i \leq 2$, the maps Θ_v^i induce an isomorphism*

$$\Theta^i : P^i(G_S, A) \xrightarrow{\sim} P^{2-i}(G_S, A')^\vee.$$

Proof. We use the following result about restricted products:

Proposition 11.3. *Let $(X_i)_{i \in I}$ be a family of locally compact topological spaces and let $(U_i)_{i \in I}$ be a family of open subsets $U_i \subset X_i$ such that all but finitely many U_i are compact. Then there is a topological isomorphism:*

$$\left(\prod_{i \in I} (X_i, U_i) \right)^\vee \simeq \prod_{i \in I} (X_i^\vee, (X_i/U_i)^\vee).$$

Proof. Exercise. □

In our case we know from local theory that $H^{2-i}(K_v, A')^\vee \simeq H^i(K_v, A)$. Moreover, if A is an unramified G_v -module which is finitely generated as a $\mathbf{Z}$ -module and assume that the order of the torsion subgroup of A is prime to the characteristic of the residue field of K_v , then the groups $H_{\text{unr}}^{2-i}(K_v, A')$ and $H_{\text{unr}}^i(K_v, A)$ annihilate each other in this pairing and this induces a topological isomorphism

$$H_{\text{unr}}^i(K_v, A) \simeq (H^{2-i}(K_v, A')/H_{\text{unr}}^{2-i}(K_v, A'))^\vee \subset H^{2-i}(K_v, A')^\vee.$$

Hence we deduce from Proposition 11.3 a topological isomorphism:

$$\prod_{v \in S} (H^i(K_v, A), H_{\text{unr}}^i(K_v, A)) = \left(\prod_{v \in S} (H^{2-i}(K_v, A'), H_{\text{unr}}^{2-i}(K_v, A')) \right)^\vee.$$

□

11.2.2 Case of infinite modules

This subsection will not be used in the following of the notes. It can be ignored.

If A is not finite the G_S -dual $A' := \text{Hom}(A, U_{K_S}(S))$ is still defined but it is not in $\text{Mod}_S(G_S)$ anymore and we do not have the identification $(A')' = A$. Instead for any place v of K , we set:

$$H^i(K_v, A') := H^i(K_v, \text{Hom}(A, \overline{K}_v^\times)).$$

Note that when A is finite, this corresponds to the previous definition. As G_v -modules, we have an injective map $A' \hookrightarrow \text{Hom}(A, \overline{K}_v^\times)$, so we obtain a map

$$H^i(G_S, A') \rightarrow H^i(K_v, A').$$

If A is unramified at a place v , we define

$$H_{\text{unr}}^i(K_v, A') := H_{\text{unr}}^i(K_v, \text{Hom}(A, \mathcal{O}_{K_v}^\times)).$$

As before, we define the restricted products:

$$P^i(G_S, A) := \prod_{v \in S} (H^i(K_v, A), H_{\text{unr}}^i(K_v, A)) \quad \text{and} \quad P^i(G_S, A') := \prod_{v \in S} (H^i(K_v, A'), H_{\text{unr}}^i(K_v, A'))$$

where the cohomology groups are all equipped with the discrete topology except for $H^0(K_v, A')$, which is endowed with the topology induced by the compact-open topology on $\text{Hom}(A, \overline{K}_v^\times)$. In particular, $H^0(K_v, A')$ is locally compact and $H_{\text{unr}}^0(K_v, A')$ is compact when A is unramified. Hence, when A and S are infinite, in general only the following groups are locally compact:

- (•) the group $P^1(G_S, A)$, since $H^1(K_v, A)$ is finite,
- (•) the group $P^0(G_S, A')$, since $H_{\text{unr}}^0(K_v, A')$ is compact and $H^0(K_v, A')$ is locally compact,
- (•) the group $P^1(G_S, A')$, since $H^1(K_v, A')$ is finite.

Remark 11.4. If A is free as a $\mathbf{Z}$ -module and unramified at v , then

$$H_{\text{unr}}^1(K_v, A) = H^1(K_v, A) \quad \text{and} \quad H_{\text{unr}}^i(K_v, A') = 0 \text{ for } i \geq 1.$$

We obtain that $P^1(G_S, A)$ is a product of finite groups so it is compact and for $i \geq 1$, the groups $P^i(G_S, A')$ are a direct sum of discrete groups so they are discrete.

Let A be a module in $\text{Mod}_S(G_S)$. In degree $i = 1$, we have an isomorphism of finite groups:

$$H^1(K_v, A') \xrightarrow{\sim} H^1(K_v, A)^\vee.$$

In degree $i = 0$, we have an injective map

$$H^0(K_v, A') \hookrightarrow H^2(K_v, A)^\vee,$$

which has dense image, the group of the left is locally compact and the one on the right is compact.

Passing to the dual, we obtain an isomorphism of finite groups:

$$\Theta_v^1 : H^1(K_v, A) \xrightarrow{\sim} H^1(K_v, A')^\vee,$$

and an injective map:

$$\Theta_v^2 : H^2(K_v, A) \hookrightarrow H^0(K_v, A')^\vee,$$

which has dense image, the group of the left is discrete and the one on the right is locally compact.

We have:

Proposition 11.5. *Let A be in $\text{Mod}_S(G_S)$. For i in $\{1, 2\}$, the map Θ_v^i induces a continuous morphism:*

$$\Theta^i : P^i(G_S, A) \rightarrow P^{2-i}(G_S, A')^\vee.$$

Moreover,

(1) *the map Θ^1 is an isomorphism of locally compact groups,*

(2) *the map Θ^2 is injective with dense image.*

Proof. This follows from the following result for local fields: if A is an unramified G_v -module which is finitely generated as a $\mathbf{Z}$ -module and assume that the order of the torsion subgroup of A is prime to the characteristic of the residue field of K_v , then the groups $H_{\text{unr}}^i(K_v, \text{Hom}(A, \mathcal{O}_{K_v^{\text{unr}}}))$ and $H_{\text{unr}}^{2-i}(K_v, A)$ annihilate each other in the pairing inducing the maps Θ_v^i and we obtain a map

$$H_{\text{unr}}^i(K_v, A) \rightarrow (H^{2-i}(K_v, A')/H_{\text{unr}}^{2-i}(K_v, A'))^\vee$$

which is an isomorphism for $i = 1$. Moreover as before we have

$$\left(\prod_{v \in S} (H^{2-i}(K_v, A'), H_{\text{unr}}^{2-i}(K_v, A')) \right)^\vee = \prod_{v \in S} (H^{2-i}(K_v, A')^\vee, (H^{2-i}(K_v, A')/H_{\text{unr}}^{2-i}(K_v, A'))^\vee).$$

□

11.3 Digression: Ext-groups

In the next subsection, we will prove Poitou-Tate duality and to do so, we need some results about Ext-groups. In this subsection G is a profinite group. All the G -modules are assumed to be discrete but not necessarily finitely generated.

11.3.1 Extensions of G -modules

If M and N are G -modules, we define $\text{Ext}_G^i(M, N)$ as the set of homotopy classes of morphisms $M^\bullet \rightarrow N^\bullet$ of degree i , where $M^\bullet$ is any resolution of M by G -modules and $N^\bullet$ is any resolution of N by injective G -modules.

Hence we see that $\text{Ext}_G^i(M, -)$ is the i -th right derived functor of the functor $N \mapsto \text{Hom}_G(M, N)$ from the category of discrete G -modules Mod_G to the category of abelian groups. In other words, for N a G -module and $N^\bullet$ a resolution of N by injective G -modules, we have

$$\text{Ext}_G^i(M, N) = H^i(\text{Hom}_G(M, N^\bullet)).$$

For $M = \mathbf{Z}$, we recover the group cohomology:

$$\text{Ext}_G^i(\mathbf{Z}, N) = H^i(G, N).$$

There is a canonical product

$$\text{Ext}_G^i(N, P) \times \text{Ext}_G^j(M, N) \rightarrow \text{Ext}_G^{i+j}(M, P)$$

sending a pair (f, g) of extensions to $f \cdot g$ defined in the following way: let $N^\bullet$ and $P^\bullet$ be injective resolutions of N and M respectively and choose $f : N^\bullet \rightarrow P^\bullet$ and $g : M \rightarrow N^\bullet$ representatives of f and g respectively, then $f \cdot g$ is defined as the class represented by $f \circ g$. In degree zero, we recover the usual composition $(f, g) \mapsto f \circ g$:

$$\text{Hom}_G(N, P) \times \text{Hom}_G(M, N) \rightarrow \text{Hom}_G(M, P).$$

When $M = \mathbf{Z}$, we obtain a pairing

$$(11.3.1) \quad \text{Ext}_G^i(N, P) \times H^j(G, N) \rightarrow H^{i+j}(G, P).$$

11.3.2 Spectral sequence

Let M and N be G -modules. In general, the module $\text{Hom}(M, N)$ is not discrete for the action given by

$$(g \cdot \varphi)(x) = g \cdot \varphi(g^{-1} \cdot x) \quad \text{for } g \in G, \varphi \in \text{Hom}(M, N), x \in M.$$

Let H be a closed normal subgroup of G . Consider the discrete G/H -module:

$$\begin{aligned}\underline{\text{Hom}}_H(M, N) &= \bigcup_{H \subset U \subset G \text{ open}} \text{Hom}(M, N)^U \\ &= \{\varphi \in \text{Hom}(M, N) \mid \exists U \text{ s.t. } g \cdot \varphi = \varphi \text{ for all } g \in U\}.\end{aligned}$$

We define $\underline{\text{Ext}}_H^i(M, -)$ the i -th right derived functor of $N \mapsto \underline{\text{Hom}}_H(M, N)$ from Mod_G to $\text{Mod}_{G/H}$. If H is trivial we drop the H from the notation. If M is finitely generated, note that we have

$$\underline{\text{Ext}}_H^i(M, N) = \text{Ext}_H^i(M, N).$$

Theorem 11.6. *Let H be a closed normal subgroup of G and let N and P be G -modules. Let M be a G/H -module such that $\text{Tor}_i^{\mathbf{Z}}(M, N) = 0$ for $i \geq 1$. Then there is a spectral sequence:*

$$\text{Ext}_{G/H}^i(M, \underline{\text{Ext}}_H^j(N, P)) \Rightarrow \text{Ext}_G^{i+j}(M \otimes_{\mathbf{Z}} N, P).$$

In fact, as we will see in the proof below, $\text{Tor}_i^{\mathbf{Z}}(M, N) = 0$ is always zero for $i \geq 2$, so it suffices to assume that $\text{Tor}_1^{\mathbf{Z}}(M, N) = 0$.

To prove the theorem, we first prove the following three lemmas.

Lemma 11.7. *Let H be a closed normal subgroup of G and let N and P be G -modules. Let M be a G/H -module. Then there is a canonical isomorphism:*

$$\text{Hom}_{G/H}(M, \underline{\text{Hom}}_H(N, P)) \xrightarrow{\sim} \text{Hom}_G(M \otimes_{\mathbf{Z}} N, P).$$

Proof. We can check that the map which sends a morphism φ in $\text{Hom}_{G/H}(M, \underline{\text{Hom}}_H(N, P))$ to $x \otimes y \mapsto \varphi(x)(y)$ in $\text{Hom}(M \otimes_{\mathbf{Z}} N, P)$ induces an isomorphism:

$$(11.3.2) \quad \text{Hom}_{G/H}(M, \underline{\text{Hom}}_H(N, P)) \xrightarrow{\sim} \text{Hom}(M \otimes_{\mathbf{Z}} N, P)$$

(its inverse is obtained by sending a morphism ψ from $\text{Hom}(M \otimes_{\mathbf{Z}} N, P)$ to the morphism $x \mapsto (y \mapsto \psi(x \otimes y))$). We then take the G -invariants. We have

$$\begin{aligned}(\text{Hom}_{G/H}(M, \underline{\text{Hom}}_H(N, P)))^G &= \text{Hom}_G(M, \text{Hom}(N, P)) \\ &= \text{Hom}_G(M, \text{Hom}_H(N, P)) \\ &= \text{Hom}_G(M, \underline{\text{Hom}}_H(N, P)),\end{aligned}$$

where in the second equality we use the fact that M is a G/H -module and for the third one, we use the fact that M is a discrete G/H -module.

Taking the G -invariants on the right of (11.3.2) gives $\text{Hom}_G(M \otimes_{\mathbf{Z}} N, P)$, hence the lemma. $\square$

Lemma 11.8. *If I is an injective G -module and N is a torsion-free G -module, then $\underline{\text{Hom}}_H(N, I)$ is an injective G/H -module.*

Proof. To prove that $\underline{\text{Hom}}_H(N, I)$ is injective, it suffices to prove that the functor

$$\text{Hom}_{G/H}(-, \underline{\text{Hom}}_H(N, I)) : \text{Mod}_{G/H} \rightarrow \text{Ab}$$

is exact. But Lemma 11.7 tells us that it is the composite of the functors $-\otimes_{\mathbf{Z}} N$ and $\text{Hom}_G(-, I)$ which are exact (since N is torsion-free and I is injective). $\square$

Lemma 11.9. *Let N and I be G -modules with I injective and let M be a G/H -module. Then there is a canonical isomorphism*

$$\text{Ext}_{G/H}^i(M, \underline{\text{Hom}}_H(N, I)) \xrightarrow{\sim} \text{Hom}_G(\text{Tor}_i^{\mathbf{Z}}(M, N), I).$$

Proof. Choosing a set of generators for N as $\mathbf{Z}[G]$ -modules gives us a resolution of N by torsion-free G -modules:

$$0 \rightarrow N_1 \rightarrow N_0 \rightarrow N \rightarrow 0.$$

We can use this resolution to compute $\text{Tor}_i^{\mathbf{Z}}(M, N)$ and it follows that $\text{Tor}_i^{\mathbf{Z}}(M, N)$ is zero for $i \geq 2$ and the first terms fit into an exact sequence:

$$0 \rightarrow \text{Tor}_1^{\mathbf{Z}}(M, N) \rightarrow M \otimes_{\mathbf{Z}} N_1 \rightarrow M \otimes_{\mathbf{Z}} N_0 \rightarrow \text{Tor}_0^{\mathbf{Z}}(M, N) = M \otimes_{\mathbf{Z}} N \rightarrow 0.$$

For each open subgroup U of G containing H , we have a short exact sequence

$$0 \rightarrow \text{Hom}_U(N, I) \rightarrow \text{Hom}_U(N_0, I) \rightarrow \text{Hom}_U(N_1, I) \rightarrow 0$$

(we have used that I is injective as a G -module, so also as a U -module) and taking the limit, we obtain an injective resolution of $\underline{\text{Hom}}_H(N, I)$ (it is injective by the previous lemma since N_0 and N_1 are torsion-free):

$$0 \rightarrow \underline{\text{Hom}}_H(N, I) \rightarrow \underline{\text{Hom}}_H(N_0, I) \rightarrow \underline{\text{Hom}}_H(N_1, I) \rightarrow 0$$

We use this resolution to compute $\text{Ext}_{G/H}^i(M, \underline{\text{Hom}}_H(N, I))$. Consider the diagram

$$(11.3.3) \quad \begin{array}{ccc} \text{Hom}_{G/H}(M, \underline{\text{Hom}}_H(N_0, I)) & \xrightarrow{\alpha} & \text{Hom}_{G/H}(M, \underline{\text{Hom}}_H(N_1, I)) \\ \sim \downarrow & & \downarrow \sim \\ \text{Hom}_G(M \otimes_{\mathbf{Z}} N_0, I) & \xrightarrow{\beta} & \text{Hom}_G(M \otimes_{\mathbf{Z}} N_1, I) \end{array}$$

where the vertical maps are isomorphisms by Lemma 11.7. We have

$$\text{Ker}(\alpha) = \text{Ext}_{G/H}^0(M, \underline{\text{Hom}}_H(N, I))$$

$$\text{Ker}(\beta) = \text{Hom}_G(\text{Tor}_0^{\mathbf{Z}}(M, N), I)$$

$$\text{CoKer}(\alpha) = \text{Ext}_{G/H}^1(M, \underline{\text{Hom}}_H(N, I))$$

$$\text{CoKer}(\beta) = \text{Hom}_G(\text{Tor}_1^{\mathbf{Z}}(M, N), I).$$

and since the vertical maps in (11.3.3) are isomorphisms, we obtain the isomorphisms from the statement of the lemma. $\square$

We can now prove the theorem.

Proof of Theorem 11.6. From Lemma 11.7, we see that $\text{Hom}_G(M \otimes_{\mathbf{Z}} N, -)$ can be written as the composite of the functors $\underline{\text{Hom}}_H(N, -)$ and $\text{Hom}_{G/H}(M, -)$. Lemma 11.9 shows that the first of these functors maps injective objects to objects that are acyclic for the second functor (since we have assumed $\text{Tor}_i^{\mathbf{Z}}(M, N) = 0$ for $i \geq 1$). Then the spectral sequence of the theorem is the Grothendieck spectral sequence for this composite. $\square$

We derive from the theorem the following consequences.

(•) When $M = N = \mathbf{Z}$, the spectral sequence corresponds to the Hochschild-Serre spectral sequence

$$H^i(G/H, H^j(H, P)) \Rightarrow H^{i+j}(G, P).$$

(•) If $M = \mathbf{Z}$ and $H = \{1\}$, the spectral sequence becomes

$$(11.3.4) \quad H^i(G, \underline{\text{Ext}}^j(N, P)) \Rightarrow \text{Ext}_G^{i+j}(N, P).$$

In particular, we see that when $\underline{\text{Ext}}^j(N, P) = 0$ for $j \geq 1$

$$(11.3.5) \quad H^i(G, \underline{\text{Hom}}(N, P)) = \text{Ext}_G^i(N, P).$$

(•) When $N = \mathbf{Z}$, the spectral sequence becomes

$$(11.3.6) \quad \text{Ext}_{G/H}^i(M, H^j(H, P)) \Rightarrow \text{Ext}_G^{i+j}(M, P).$$

When $i = 0$, the map $\text{Ext}_{G/H}^0(M, P^H) \rightarrow \text{Ext}_G^0(M, P)$ is obviously an isomorphism. If moreover we assume that $H^1(H, P) = 0$, we obtain an isomorphism $\text{Ext}_{G/H}^1(M, P^H) \rightarrow \text{Ext}_G^1(M, P)$. More generally, if $H^i(H, P) = 0$ for all $i > 0$, we have an isomorphism

$$(11.3.7) \quad \text{Ext}_{G/H}^i(M, P^H) \rightarrow \text{Ext}_G^i(M, P),$$

for all $i > 0$.

11.3.3 Shapiro's lemma

We will also use the following generalization of Shapiro's lemma:

Proposition 11.10. *Let G be a group and H be a subgroup of G . Let M be a G -module and N a H -module. Then for all $i \geq 0$,*

$$\text{Ext}_G^i(M, \text{Ind}_H^G(N)) \simeq \text{Ext}_H^i(M, N).$$

Similarly,

$$\text{Ext}_H^i(N, M) \simeq \text{Ext}_G^i(\text{Ind}_H^G(N), M).$$

Proof. Exercise. $\square$

11.4 Poitou-Tate duality

Let us go back to $P^i(G_S, A)$. To simplify the proofs, in the following, we will assume that A is finite.

Let us first prove the following factorization:

Proposition 11.11. *Let A be in $\text{Mod}_S(G_S)$. Assume that A is finite. Then for any $i \geq 0$, the restriction morphism*

$$\text{Res}^i : H^i(G_S, A) \rightarrow \prod_{v \in S} H^i(K_v, A)$$

factors through $P^i(G_S, A)$.

Proof. We need to show that if x is a class in $H^i(G_S, A)$ then for almost all places v of S , the image $x_v := \text{Res}_v(x)$ by the restriction map $\text{Res}_v : H^i(G_S, A) \rightarrow H^i(K_v, A)$ is contained in $H_{\text{unr}}^i(K_v, A)$. Since the inflation maps induce an isomorphism

$$\text{colim}_{K_S/L/K} H^i(\text{Gal}(L/K), A^{\text{Gal}(K_S/L)}) \xrightarrow{\sim} H^i(G_S, A),$$

there exists a subextension L_x/K of K_S/K and y in $H^i(\text{Gal}(L_x/K), A^{\text{Gal}(K_S/L_x)})$ such that $x = \text{Inf}(y)$.

Since A is finitely generated over $\mathbf{Z}$, there exists L_A a finite Galois subextension of K_S/K such that A is fixed by $\text{Gal}(K_S/L_A)$. In particular, A is fixed by $\text{Gal}(K_S/L_x \cdot L_A)$. Assume that v is a place of S such that v is unramified in the composite $L_x \cdot L_A/K$. We obtain that $\text{Res}_v(x)$ is the image by

$$\text{Inf} : H^i(\text{Gal}(K_v^{\text{unr}}/K_v), A) \rightarrow H^i(\text{Gal}(\overline{K}_v/K_v), A)$$

of the element $\tilde{y}_v$, which is the image of $y_v := \text{Res}_v(y)$ via the map

$$H^i(\text{Gal}((L_x \cdot L_A)_v/K_v), A) \rightarrow H^i(\text{Gal}(K_v^{\text{unr}}/K_v), A).$$

Hence x_v is in $H_{\text{unr}}^i(K_v, A)$, as wanted. □

Hence if M is A or A' , we thus obtain localization maps

$$\lambda^i : H^i(G_S, M) \rightarrow P^i(G_S, M).$$

We define

$$\text{III}^i(G_S, M) := \text{Ker}(\lambda^i).$$

Example 11.12. We have the following result:

Lemma 11.13. *If n is in $N(S)$, then there are natural isomorphisms*

$$\begin{aligned} \text{III}^1(G_S, \mathbf{Z}/n\mathbf{Z}) &\simeq \text{Hom}(C_{K,S}, \mathbf{Z}/n\mathbf{Z}) \\ \text{III}^1(G_S, \mathbf{Z}') &\simeq C_{K,S}, \end{aligned}$$

where as before $C_{K,S}$ is the ideal class group of the ring $\mathcal{O}_{K,S}$ and $\mathbf{Z}'$ is the S -dual of $\mathbf{Z}$.

Note that in the above, we are assuming that we have prove Proposition 11.11 in the infinite case as well and that $\text{III}^1(G_S, \mathbf{Z}')$ is well-defined.

Proof. First note that we have the following:

Claim 11.14. Let K_0 be the abelian maximal extension of K inside K_S in which all primes of S split completely. Then the Artin map induces an isomorphism between $C_{K,S}$ and $\text{Gal}(K_0/K)$.

Proof of the claim. Let us recall that the Artin map gives an isomorphism between the ideal class group C_K of K and the Galois group of the Hilbert class field E of K which is the maximal abelian unramified extension of K . Recall also that $C_{K,S}$ is the quotient of C_K by the subgroup generated by all the primes of S , which we will denote by $J_{K,S}$. Hence, to prove the claim, it suffices to show that the image of $J_{K,S}$ by the Artin map is exactly the group $\text{Gal}(E/K_0)$. But if L/K is a finite abelian subextension of E , then the Artin map sends exactly $J_{K,S}$ to the group $D(L/K)$ generated by all the decomposition subgroups $D(\mathfrak{p}, L/K)$ for $\mathfrak{p}$ in S . Since $\text{Gal}(E/K_0) \simeq \varprojlim_{K_0/L/K} D(L/K)$, the result follows. $\square$

Let us go back to the proof of the lemma. For the first point, by definition, we have

$$\text{III}^1(G_S, \mathbf{Z}/n\mathbf{Z}) = \text{Ker}(H^1(G_S, \mathbf{Z}/n\mathbf{Z}) \rightarrow \prod_{v \in S} H^1(K_v, \mathbf{Z}/n\mathbf{Z})),$$

in other words it is the intersection (for v in S) of the kernels of the restriction maps:

$$H^1(G_S, \mathbf{Z}/n\mathbf{Z}) \rightarrow H^1(K_v, \mathbf{Z}/n\mathbf{Z}).$$

By the restriction-inflation exact sequence, we know that each of this kernel is equal to $H^1(G_S/G_v, \mathbf{Z}/n\mathbf{Z}) \simeq \text{Hom}(G_S/G_v, \mathbf{Z}/n\mathbf{Z})$. Hence, taking the intersection, we obtain

$$\text{III}^1(G_S, \mathbf{Z}/n\mathbf{Z}) \simeq \text{Hom}(\text{Gal}(K_0/K), \mathbf{Z}/n\mathbf{Z}) \simeq \text{Hom}(C_{K,S}, \mathbf{Z}/n\mathbf{Z}).$$

For the second point, we have

$$H^1(K_v, \mathbf{Z}') = H^1(G_v, \text{Hom}(\mathbf{Z}, \overline{K}_v^\times)) \simeq H^1(G_v, \overline{K}_v^\times) = 0$$

by Hilbert's Theorem 90. Hence

$$\text{III}^1(G_S, \mathbf{Z}') = H^1(G_S, \mathbf{Z}') = H^1(G_S, \text{Hom}(\mathbf{Z}, U_{K_S}(S))) \simeq H^1(G_S, U_{K_S}(S)) \simeq C_{K,S}$$

by Proposition 10.6. $\square$

In degree 1, the localization map λ^1 has the following property:

Lemma 11.15. *If A is finite then the inverse image of every compact subspace of $P^1(G_S, A)$ by $\lambda^1 : H^1(G_S, A) \rightarrow P^1(G_S, A)$ is finite.*

Proof. Choose L/K a finite subextension of K_S/K such that $\text{Gal}(K_S/L)$ acts trivially on A . Since the inflation maps are continuous, it follows from the commutative diagram:

$$\begin{array}{ccc} H^1(G_S, A) & \xrightarrow{\lambda^1} & P^1(G_S, A) \\ \downarrow & & \downarrow \\ H^1(\text{Gal}(K_S/L), A) & \xrightarrow{\lambda^1} & P^1(\text{Gal}(K_S/L), A) \end{array}$$

that it suffices to prove the result for the map $\lambda^1 : H^1(\text{Gal}(K_S/L), A) \rightarrow P^1(\text{Gal}(K_S/L), A)$. Hence we can assume that G_S acts trivially on A .

Let us then assume that A is a finite module with a trivial G_S -action. By definition of the restricted product, any compact neighborhood of 1 in $P^1(G_S, A)$ is of the form

$$P(T) = \prod_{v \in S \setminus T} H^1(K_v, A) \times \prod_{v \in T} H_{\text{unr}}^1(K_v, A),$$

where T a subset of S such that $S \setminus T$ is finite (note $P(T)$ is indeed compact by Tykhonov's theorem). So it suffices to show that the inverse image of $P(T)$ by λ^1 is finite. Since we have assumed that the action of G_S is trivial, we can identify the group $H^1(G_S, A)$ with $\text{Hom}(G_S, A)$. If an element $f : G_S \rightarrow A$ in $\text{Hom}(G_S, A)$ is sent to an element of $P(T)$ via λ^1 , this means that for all v in T , the morphism f is trivial on $I_v \subset G_v$. In other words, the group I_v is contained in $\text{Ker}(f)$, or equivalently the extension $K_S^{\text{Ker}(f)}$ is unramified at all places v in T . Hence we see that the extension $K_S^{\text{Ker}(f)}$ of K is unramified outside a finite number of places. Note also that its degree $[K_S^{\text{Ker}(f)} : K] = [G_S : \text{Ker}(f)]$ divides the order of A . We can then conclude by applying the following lemma:

Lemma 11.16. *Let L be a number field and S_L a finite set of places of L . For any fixed integer r , there is only a finite number of extensions of L of degree r that are unramified outside of S_L .*

Proof of Lemma (11.16). Exercise. □

□

If A is finite, by duality, we see that the localization maps λ^i for the module A' induce maps

$$\mu^i : P^i(G_S, A) \rightarrow H^{2-i}(G_S, A')^\vee, \quad \text{for } i \in \{0, 1, 2\}.$$

We can now state our main result:

Theorem 11.17 (Poitou-Tate duality). *Let A be in $\text{Mod}_S(G_S)$. Assume that A is finite. Then,*

(1) *The groups $\text{III}^1(G_S, A)$ and $\text{III}^2(G_S, A')$ are finite and there is a perfect pairing of finite groups*

$$\text{III}^1(G_S, A) \times \text{III}^2(G_S, A') \rightarrow \mathbf{Q}/\mathbf{Z}.$$

(2) *The map λ^0 is injective, the map μ^2 is surjective and for i in $\{0, 1, 2\}$, we have*

$$\text{Im}(\lambda^i) = \text{Ker}(\mu^i).$$

(3) *For $i \geq 3$, the map*

$$\text{Res} : H^i(G_S, A) \xrightarrow{\sim} \bigoplus_{v \in S_{\mathbf{R}}} H^i(G_v, A)$$

is an isomorphism.

In other words, there is a canonical exact sequence of locally compact groups (with continuous morphisms):

$$\begin{aligned} 0 \rightarrow H^0(G_S, A) \rightarrow P^0(G_S, A) \rightarrow H^2(G_S, A')^\vee \rightarrow \\ H^1(G_S, A) \rightarrow P^1(G_S, A) \rightarrow H^1(G_S, A')^\vee \rightarrow \\ H^2(G_S, A) \rightarrow P^2(G_S, A) \rightarrow H^0(G_S, A')^\vee \rightarrow 0. \end{aligned}$$

The exact sequence from the theorem is called Poitou-Tate exact sequence. Note that the groups in the sequence have the following topological properties:

$$\begin{aligned} 0 \rightarrow \text{finite} \rightarrow \text{compact} \rightarrow \text{compact} \rightarrow \\ \text{discrete} \rightarrow \text{locally compact} \rightarrow \text{compact} \rightarrow \\ \text{discrete} \rightarrow \text{discrete} \rightarrow \text{finite} \rightarrow 0. \end{aligned}$$

Remark 11.18. In the above, since we have assumed that A is finite, we can replace A by A' and we obtain a perfect pairing of finite groups

$$(11.4.1) \quad \text{III}^1(G_S, A') \times \text{III}^2(G_S, A) \rightarrow \mathbf{Q}/\mathbf{Z}.$$

It can be proved (but it is more complicated) that for any A in $\text{Mod}_S(G_S)$ we still have a perfect pairing of finite groups (11.4.1). However, when A is not finite, we cannot exchange A and A' and it is not necessarily true in general that there is a perfect pairing

$$\text{III}^1(G_S, A) \times \text{III}^2(G_S, A') \rightarrow \mathbf{Q}/\mathbf{Z}.$$

The idea of the proof of Theorem 11.17 is to apply the functor $\text{Hom}_{G_S}(A', -)$ to the exact sequence:

$$0 \rightarrow U_{K_S}(S) \rightarrow \mathbb{I}_{K_S, S} \rightarrow \mathbb{C}_{K_S, S} \rightarrow 0,$$

and to identify the terms $\text{Ext}_{G_S}(A', -)$ of the induced long exact sequence with the terms appearing in the exact sequence from the theorem. Hence, we need to compute the terms $\text{Ext}_{G_S}^i(A', M)$ for $M \in \{U_{K_S}(S), \mathbb{I}_{K_S, S}, \mathbb{C}_{K_S, S}\}$. This is done in the following three lemmas.

Lemma 11.19. *We have:*

(1) *For all $i \geq 0$, we have an equality*

$$\text{Ext}_{G_S}^i(A, U_{K_S}(S)) = H^i(G_S, A').$$

(2) *If v is not in S , then*

$$H^i(\text{Gal}(\bar{k}_v/k_v), A') = \text{Ext}_{\text{Gal}(\bar{k}_v/k_v)}^i(A, \mathcal{O}_v^{\text{unr}, \times})$$

and they are equal to 0 in degree $i \geq 2$.

Proof of Lemma 11.19. The first point is a direct consequence of formula (11.3.5) applied to the group $G = G_S$ and the modules $N = A$ and $P = U_{K_S}(S)$. Note that here we have $\text{Ext}^1(A, U_{K_S}(S)) = 0$ since we have assumed the torsion of A is a unit outside of S and $U_{K_S}(S)$ is divisible by such integers.

The first statement of the second point is again a consequence of (11.3.5): as before we know that the torsion of A is a unit outside of S , so in particular it is a unit in $\mathcal{O}_v^{\text{unr}}$ if v is not in S so $\text{Ext}^1(A, \mathcal{O}_v^{\text{unr}, \times}) = 0$.

Let us now write $g_v := \text{Gal}(\bar{k}_v/k_v)$ and we want to show that the group $\text{Ext}_{g_v}^i(A, \mathcal{O}_v^{\text{unr}, \times})$ is zero in degree $i \geq 2$. We can use the following claim (the proof is left as an exercise, see Sheet 11):

Claim 11.20. Let G be a profinite group such that given any n , there exists only finitely many open normal subgroups of G with index n . Let M be $\mathbf{Z}[G]$ -module which is finitely generated as a $\mathbf{Z}$ -module. Then M is cohomologically trivial³ if and only if there exists an exact sequence

$$0 \rightarrow M \rightarrow I_0 \rightarrow I_1 \rightarrow 0$$

where I_0 and I_1 are injective $\mathbf{Z}[G]$ -modules.

Since we know from local theory that $\mathcal{O}_v^{\text{unr}, \times}$ is cohomologically trivial, it follows that we can write

$$0 \rightarrow \mathcal{O}_v^{\text{unr}, \times} \rightarrow I_0 \rightarrow I_1 \rightarrow 0$$

with I_0 and I_1 injective $\mathbf{Z}[g_v]$ -modules. We obtain $\text{Ext}_{g_v}^i(A, \mathcal{O}_v^{\text{unr}, \times}) = 0$ for $i \geq 2$, as wanted. $\square$

³i.e. the higher cohomology groups vanish for every closed subgroup.

We also have:

Lemma 11.21. *Let A be in $\text{Mod}_S(G_S)$. Assume that A is finite. Then,*

$$\begin{aligned}\text{Hom}_{G_S}(A, \mathbb{I}_{K_S, S}) &= \prod_{v \in S} H^0(G_S, A'), \\ \text{Ext}_{G_S}^i(A, \mathbb{I}_{K_S, S}) &= P^i(G_S, A') \quad \text{for } i \geq 1.\end{aligned}$$

Proof of Lemma 11.21. We consider finite subsets T of S such that T contains all archimedean places of K and all the non-archimedean places at which A is ramified, T is such that the order of A is a T -unit (i.e. it is a unit at all the places not in T). For such a set and L/K finite, we set

$$\mathbb{I}_{L/K, T \subset S} := \prod_{w \text{ dividing elements of } T} L_w^\times \times \prod_{w \text{ dividing elements of } S \setminus T} U_w.$$

Hence we can write

$$\mathbb{I}_{L/K, S} = \varinjlim_{T \subset S} \mathbb{I}_{L/K, T \subset S},$$

where the colimit runs over the subsets T as above and L/K is a subextension of K_T/K (where K_T is the maximal extension of K unramified outside T). Since A is finitely generated the functor $\text{Hom}_{G_S}(A, -)$ commutes with the colimit. We obtain:

$$\text{Ext}_{G_S}^i(A, \mathbb{I}_{K_S, S}) = \varinjlim_{L, T} \text{Ext}_{\text{Gal}(L/K)}^i(A, \mathbb{I}_{L/K, T \subset S}).$$

We need to compute the terms on the right. Fix L/K a finite Galois subextension of K_S/K . Since the functor $\text{Hom}_{\text{Gal}(L/K)}(A, -)$ commutes with the product (and using Proposition 11.10) we have

$$\text{Ext}_{\text{Gal}(L/K)}^i(A, \mathbb{I}_{L/K, T \subset S}) = \left(\prod_{v \in T} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) \right) \times \left(\prod_{v \in S \setminus T} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, U_{w(v)}) \right),$$

where for each place v of K we have fixed $w(v)$ a place of L that divides v . If v is in $S \setminus T$ and w divides v , then L_w is unramified and since $\mathcal{O}_v^{\text{unr}, \times}$ has no cohomology in higher degrees, it follows from (11.3.7), that we have an equality

$$\text{Ext}_{\text{Gal}(L_w/K_v)}^i(A, U_w) = \text{Ext}_{g_v}^i(A, \mathcal{O}_v^{\text{unr}, \times}).$$

Using Lemma 11.19, we obtain

$$(11.4.2) \quad \text{Ext}_{\text{Gal}(L/K)}^i(A, \mathbb{I}_{L/K, T \subset S}) = \left(\prod_{v \in T} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) \right) \times \left(\prod_{v \in S \setminus T} H^i(g_v, A') \right).$$

Assume now that i is in $\{0, 1\}$. In that case, since we know that $H^1(\text{Gal}(\bar{L}_{w(v)}/L_{w(v)}), \bar{L}_{w(v)}^\times)$ is trivial, (11.3.7) gives an equality:

$$\text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) = \text{Ext}_{\text{Gal}(\bar{K}_v/K_v)}^i(A, \bar{K}_v^\times).$$

Moreover, since $\overline{K}_v^\times$ is divisible, we also have $\text{Ext}^1(A, \overline{K}_v^\times) = 0$ and (11.3.5) gives

$$\text{Ext}_{\text{Gal}(\overline{K}_v/K_v)}^i(A, \overline{K}_v^\times) = H^i(\text{Gal}(\overline{K}_v/K_v), A').$$

So we can take the limit of the equations (11.4.2) and if $i = 0$, we obtain (recall that when a module M is unramified at v , we have $H^0(g_v, M) = H^0(G_v, M)$ since the inertia subgroup acts trivially):

$$\text{Ext}_{G_S}^0(A, \mathbb{I}_{K_S, S}) = \prod_{v \in S} H^0(G_v, A')$$

and if $i = 1$,

$$\text{Ext}_{G_S}^1(A, \mathbb{I}_{K_S, S}) = P^1(G_S, A),$$

as wanted.

Assume that $i \geq 2$. We know from Lemma 11.19 that the terms on the right in the equation (11.4.2) are all zero, so we can write

$$\begin{aligned} \text{Ext}_{G_S}^i(A, \mathbb{I}_{K_S, S}) &= \varinjlim_{T, K_T/L/K} \left(\prod_{v \in T} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) \right) \\ &= \varinjlim_{K_S/L/K} \left(\bigoplus_{v \in S} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) \right) \\ &= \bigoplus_{v \in S} \left(\varinjlim_{K_S/L/K} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) \right). \end{aligned}$$

Claim 11.22. We have an isomorphism

$$\varinjlim_{K_S/L/K} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times) \simeq \text{Ext}_{\text{Gal}(\overline{K}_v/K_v)}^i(A, \overline{K}_v^\times).$$

Proof of Claim 11.22. Since A is finite with order in $N(S)$, the groups appearing in the claim are torsion with torsion in $N(S)$, hence it suffices to prove that we have an isomorphism between the p -torsion part

$$\varinjlim_{K_S/L/K} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times)(p) \simeq \text{Ext}_{\text{Gal}(\overline{K}_v/K_v)}^i(A, \overline{K}_v^\times)(p),$$

for any p in $N(S)$.

We use the spectral sequence (11.3.6). In our case, when $K_S/L/K$ is fixed, it becomes:

$$\text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, H^j(\text{Gal}(\overline{K}_v/L_{w(v)}), \overline{K}_v^\times)) \Rightarrow \text{Ext}_{\text{Gal}(\overline{K}_v/K_v)}^{i+j}(A, \overline{K}_v^\times).$$

Taking the colimit, we have

$$(11.4.3) \quad E_2^{i,j} = \varinjlim_{K_S/L/K} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, H^j(\text{Gal}(\overline{K}_v/L_{w(v)}), \overline{K}_v^\times)) \Rightarrow \text{Ext}_{\text{Gal}(\overline{K}_v/K_v)}^{i+j}(A, \overline{K}_v^\times).$$

We also have⁴

$$\varinjlim_{K_S/L/K} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, H^j(\text{Gal}(\overline{K}_v/L_{w(v)}), \overline{K}_v^\times)) = \text{Ext}_{\varprojlim_L \text{Gal}(L_{w(v)}/K_v)}^i(A, \varinjlim_L H^j(\text{Gal}(\overline{K}_v/L_{w(v)}), \overline{K}_v^\times)).$$

From local theory, we know that

$$H^j(\text{Gal}(\overline{K}_v/L_{w(v)}), \overline{K}_v^\times) = \begin{cases} L_{w(v)}^\times & \text{if } j = 0 \\ 0 & \text{if } j = 1 \\ \mathbf{Q}/\mathbf{Z} & \text{if } j = 2 \\ 0 & \text{if } j \geq 3. \end{cases}$$

We claim that for p in $N(S)$

$$\varinjlim_{K_S/L/K} H^2(\text{Gal}(\overline{K}_v/L_{w(v)}), \overline{K}_v^\times)(p) = 0.$$

Indeed, the transition maps in the colimit are given by

$$[L_{w,2} : L_{w,1}] \cdot \text{Res} : H^2(\text{Gal}(\overline{K}_v/L_{w,1}), \overline{K}_v^\times) \rightarrow H^2(\text{Gal}(\overline{K}_v/L_{w,2}), \overline{K}_v^\times), \quad \text{for } K_S/L_2/L_1.$$

But when p is in $N(S)$, the extension $K(\mu_{p^\infty})/K$ is contained in K_S/K so for any $L_{w,1}$ we can find $L_{w,2}/L_{w,1}$ such that p divides $[L_{w,2} : L_{w,1}]$. It follows that the p -torsion part of the colimit is zero, as wanted.

We have then showed that in the spectral sequence (11.4.3), all the rows $(E_2^{i,j})_i$ are zero except for $j = 0$ where we have $E_2^{i,0} = \varinjlim_{K_S/L/K} \text{Ext}_{\text{Gal}(L_{w(v)}/K_v)}^i(A, L_{w(v)}^\times)$. We thus obtained the isomorphism from the claim. □

Since we also have that $\text{Ext}_{\text{Gal}(\overline{K}_v/K_v)}^i(A, \overline{K}_v^\times) = H^i(G_v, A')$ (apply again (11.3.5)), we obtain

$$\text{Ext}_{G_S}^i(A, \mathbb{I}_{K_S, S}) = \bigoplus_{v \in S} H^i(G_v, A') = P^i(G_S, A'),$$

as wanted. □

⁴This follows from (11.3.4): since $\text{Ext}^i(N, P)$ is always zero when $i \geq 2$, if we assume that the modules are finitely generated then the spectral sequence (11.3.4) will induce a long exact sequence:

$$0 \rightarrow H^1(G, \text{Hom}(N, P)) \rightarrow \text{Ext}_G^1(N, P) \rightarrow H^0(G, \text{Ext}^1(N, P)) \rightarrow H^2(G, \text{Hom}(N, P)) \rightarrow \dots$$

So if we assume that G and P can be written compatively as $G = \varprojlim_i G_i$ and $P = \varinjlim_i P_i$ (with P_i a G_i -module) such that the action of G on N factors through each G_i then

$$\text{Ext}_G^j(N, P) = \varinjlim_i \text{Ext}_{G_i}^j(N, P_i).$$

Lemma 11.23. *Let A be a finite G_S -module such that its order is an S -unit. Then, for all $i \geq 1$, there is an isomorphism*

$$\mathrm{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \simeq H^{2-i}(G_S, A)^\vee.$$

Proof. The proof will be done in the next subsection. □

We can now go back to the proof of Theorem 11.17.

Proof of Theorem 11.17. The fact that $\mathrm{III}^1(G_S, A)$ is finite follows immediately from Lemma 11.15, since it is defined as the inverse image of $\{0\}$. Consider the short exact sequence:

$$0 \rightarrow U_{K_S}(S) \rightarrow \mathbb{I}_{K_S, S} \rightarrow \mathbb{C}_{K_S, S} \rightarrow 0,$$

and apply the functor $\mathrm{Hom}_{G_S}(A', -)$. This gives a long exact sequence:

$$\cdots \rightarrow \mathrm{Ext}_{G_S}^{i-1}(A', \mathbb{C}_{K_S, S}) \rightarrow \mathrm{Ext}_{G_S}^i(A', U_{K_S}(S)) \rightarrow \mathrm{Ext}_{G_S}^i(A', \mathbb{I}_{K_S, S}) \rightarrow \mathrm{Ext}_{G_S}^i(A', \mathbb{C}_{K_S, S}) \rightarrow \mathrm{Ext}_{G_S}^{i+1}(A', U_{K_S}(S)) \rightarrow \cdots$$

Using Lemmas 11.19, 11.21 and 11.23 to identify the terms, we obtain an exact sequence:

$$\begin{aligned} 0 \rightarrow H^0(G_S, A) &\rightarrow \prod_{v \in S} H^0(K_v, A) \rightarrow \mathrm{Hom}_{G_S}(A', \mathbb{C}_{K_S, S}) \\ &\rightarrow H^1(G_S, A) \rightarrow P^1(G_S, A) \rightarrow H^1(G_S, A')^\vee \\ &\rightarrow H^2(G_S, A) \rightarrow P^2(G_S, A) \rightarrow H^0(G_S, A')^\vee \\ &\rightarrow H^3(G_S, A) \rightarrow \bigoplus_{v \text{ real}} H^3(G_v, A) \rightarrow 0, \end{aligned}$$

and if $i \geq 4$, isomorphisms:

$$H^i(G_S, A) \xrightarrow{\sim} \bigoplus_{v \text{ real}} H^3(G_v, A).$$

In particular, this proves point (3) of the theorem. Let us prove that the map

$$P^2(G_S, A) \rightarrow H^0(G_S, A')^\vee$$

is surjective. This is the dual of the map

$$H^0(G_S, A') \rightarrow P^0(G_S, A') = \prod_{v \in S \setminus S_\infty} H^0(G_v, A') \times \prod_{v \in S_\infty} \widehat{H}^0(G_v, A'),$$

which is injective (here we need to assume that S contains at least one finite place). In summary, we have obtained the following exact sequence:

$$\begin{aligned} 0 \rightarrow H^0(G_S, A) &\rightarrow \prod_{v \in S} H^0(K_v, A) \rightarrow \mathrm{Hom}_{G_S}(A', \mathbb{C}_{K_S, S}) \\ &\rightarrow H^1(G_S, A) \rightarrow P^1(G_S, A) \rightarrow H^1(G_S, A')^\vee \\ &\rightarrow H^2(G_S, A) \rightarrow P^2(G_S, A) \rightarrow H^0(G_S, A')^\vee \rightarrow 0. \end{aligned}$$

To conclude, we have to show that there is an exact sequence:

$$0 \rightarrow H^0(G_S, A) \rightarrow P^0(G_S, A) \rightarrow H^2(G_S, A')^\vee \rightarrow H^1(G_S, A) \rightarrow P^1(G_S, A).$$

But we can do the same reasoning as above replacing A' by A and taking the dual and this gives an exact sequence:

$$\begin{aligned} 0 \rightarrow H^0(G_S, A) &\rightarrow P^0(G_S, A) \rightarrow H^2(G_S, A')^\vee \\ &\rightarrow H^1(G_S, A) \rightarrow P^1(G_S, A) \rightarrow H^1(G_S, A')^\vee \\ &\rightarrow \dots \end{aligned}$$

The first five terms give the desired sequence. In summary we have obtained a nine terms exact sequence:

$$\begin{aligned} (11.4.4) \quad 0 \rightarrow H^0(G_S, A) &\xrightarrow{\lambda^0} P^0(G_S, A) \xrightarrow{\mu^0} H^2(G_S, A')^\vee \xrightarrow{\delta} \\ &H^1(G_S, A) \xrightarrow{\lambda^1} P^1(G_S, A) \xrightarrow{\mu^1} H^1(G_S, A')^\vee \rightarrow \\ &H^2(G_S, A) \xrightarrow{\lambda^2} P^2(G_S, A) \xrightarrow{\mu^2} H^0(G_S, A')^\vee \rightarrow 0, \end{aligned}$$

and we have proved point (2) of the theorem. It remains to check that there is a perfect pairing:

$$\text{III}^1(G_S, A) \times \text{III}^2(G_S, A') \rightarrow \mathbf{Q}/\mathbf{Z}.$$

and that $\text{III}^2(G_S, A')$ is a finite group. The latter will follow from the perfect pairing. We have:

$$\begin{aligned} \text{III}^1(G_S, A) &= \text{Ker}(\lambda^1 : H^1(G_S, A) \rightarrow P^1(G_S, A)), \\ \text{III}^2(G_S, A')^\vee &= (\text{Ker}(\lambda^2 : H^2(G_S, A') \rightarrow P^2(G_S, A'))^\vee \\ &\simeq \text{CoKer}(\mu^0 : P^0(G_S, A) \rightarrow H^2(G_S, A')^\vee). \end{aligned}$$

But from (11.4.4), we also have

$$\begin{aligned} \text{Ker}(\lambda^1) &= \text{Im}(\delta) \\ \text{CoKer}(\mu^0) &= \text{CoIm}(\delta). \end{aligned}$$

And the duality is induced by the isomorphism:

$$\delta : \text{CoIm}(\delta) \xrightarrow{\sim} \text{Im}(\delta).$$

□

11.5 Proof of Lemma 11.23

In this section we proof the following result:

Theorem 11.24. *Let A be a finite G_S -module such that its order is an S -unit. Then, for all $i \geq 1$ and for any prime number p , there is an isomorphism*

$$\alpha^i(A) : \text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \simeq H^{2-i}(G_S, A)^\vee.$$

We will need the following generalization of Tate's theorem (Theorem 5.1).

Theorem 11.25 (Tate-Nakayama Theorem). *Let G be a finite group and for any prime p , let us fix G_p a p -Sylow of G . Let M be a G -module. We consider an element u of $H^2(G, M)$. Assume that for all primes p , the following assumptions hold:*

(1) *We have $H^1(G_p, M) = 0$.*

(2) *The cohomology group $H^2(G_p, M)$ has order $m_p := |G_p|$ and is generated by the restriction u_p of u to $H^2(G_p, M)$.*

Then for each torsion-free G -module D and each subgroup H of G , the cup-product by $u_H = \text{Res}_H(u) \in H^2(H, M)$ induces isomorphisms

$$- \cup u_H : \hat{H}^i(H, D) \xrightarrow{\sim} \hat{H}^{i+2}(H, M \otimes D), \quad \text{for all } i \in \mathbf{Z}.$$

As a consequence, we obtain:

Proposition 11.26. *Let L/K be a finite Galois subextension of K_S/K . For D any torsion-free $\text{Gal}(L/K)$ -module, if we write $u_{L/K}$ the canonical generator of $\hat{H}^2(\text{Gal}(L/K), \mathbb{C}_S(L)) \simeq \frac{1}{[L:K]} \mathbf{Z}/\mathbf{Z}$, then the cup product with $u_{L/K}$ induces an isomorphism:*

$$- \cup u_{L/K} : \hat{H}^i(\text{Gal}(L/K), D) \xrightarrow{\sim} \hat{H}^{i+2}(\text{Gal}(L/K), \mathbb{C}_S(L) \otimes D), \quad \text{for all } i \in \mathbf{Z}.$$

Proof. This follows from Proposition 10.4 and Theorem 11.25 (using the second inequality (Theorem 6.1) for the computation of the cohomology of $\mathbb{C}_L$). $\square$

We first prove the following lemma:

Lemma 11.27. *Let A be in $\text{Mod}_S(G_S)$. Then for $i \geq 4$, the group $\text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S})$ is zero. If moreover A is torsion free then $\text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S})$ is zero for $i \geq 3$.*

Proof. Since A is a finitely generated, we can find a resolution by finitely generated G_S -modules:

$$0 \rightarrow A_1 \rightarrow A_0 \rightarrow A \rightarrow 0$$

such that A_0 is torsion-free. Hence to prove the lemma, it suffices to show that $\text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) = 0$ for $i \geq 3$ and A torsion-free.

Since A is torsion-free, we have that $\text{Ext}^1(A, \mathbb{C}_{K_S, S}) = 0$ and (11.3.5) gives us

$$\text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \simeq H^i(G_S, \underline{\text{Hom}}(A, \mathbb{C}_{K_S, S})).$$

Let us write $B := \text{Hom}(A, \mathbb{Z})$. We have an isomorphism between the G -modules $B \otimes \mathbb{C}_{K_S, S}$ and $\underline{\text{Hom}}(A, \mathbb{C}_{K_S, S})$ given by

$$\varphi \otimes c \mapsto (a \mapsto \varphi(a)c), \quad \text{for } c \in \mathbb{C}_{K_S, S}, a \in A \text{ and } \varphi \in B.$$

Since B is finitely generated, there exists an open normal subgroup $H \subset G_S$ such that $B^H = B$. Let us write L_H the corresponding subextension of K_S/K . We have

$$\begin{aligned} H^i(G_S, B \otimes \mathbb{C}_{K_S, S}) &= \text{colim}_{H \subset G_S \text{ s.t. } B^H = B} H^i(\text{Gal}(L_H/K), B \otimes (\mathbb{C}_{K_S, S})^H) \\ &= \text{colim}_H H^i(\text{Gal}(L_H/K), B \otimes \mathbb{C}_S(L_H)) \\ &\simeq \text{colim}_H H^{i-2}(\text{Gal}(L_H/K), B), \end{aligned}$$

where the last equality is given by Proposition 11.26 (we have used that $i \geq 3$ to identify Tate's cohomology groups with the usual ones).

We claim that this colimit is zero. This is because the inductive maps are given by

$$[H_1 : H_2] \cdot \text{Inf} : H^{i-2}(G_S/H_1, B) \rightarrow H^{i-2}(G_S/H_2, B), \quad \text{for } H_1 \subset H_2.$$

For α an element in $H^{i-2}(G_S/H_1, B)$, we know that α is torsion with torsion in $N(S)$. So there exists m in $N(S)$ such that $m \cdot \alpha = 0$. But for any prime p in $N(S)$, the extension $K(\mu_{p^\infty})/K$ is in K_S/K so we can find H_2 an open subgroup of H_1 such that $[H_1 : H_2]$ is divisible by m and the image of α in $H^{i-2}(G_S/H_2, B)$ is zero. This concludes the proof of the lemma. $\square$

If A is a G_S -module, using (11.3.1) we obtain a pairing (setting $H^i(G, A) := 0$ if $i \leq 0$):

$$\text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \times H^{2-i}(G_S, A) \rightarrow H^2(G_S, \mathbb{C}_{K_S, S}) \quad \text{for all } i \geq 0$$

and this last group is equal to $\mathbb{Q}/\mathbb{Z}$ by Proposition 10.5. It follows that we can define morphisms for all $i \geq 0$,

$$\alpha^i(A) : \text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \rightarrow H^{2-i}(G_S, A)^\vee.$$

We have the following duality result:

Theorem 11.28. *Let A be in $\text{Mod}_S(G_S)$. For $i \geq 2$, the map*

$$\alpha^i(A) : \text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \rightarrow H^{2-i}(G_S, A)^\vee$$

is an isomorphism. In particular, for $i \geq 3$,

$$\text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) = 0.$$

If moreover A is torsion-free, $\alpha^1(A)$ is also an isomorphism.

Proof. From Lemma 11.27, we know the result is true for $i \geq 4$. Assume that $i \leq 3$.

Step 1: Let us first assume that A has trivial G_S -action. Then we can write A as a direct sum of G_S -module isomorphic to $\mathbf{Z}$ or $\mathbf{Z}/n\mathbf{Z}$ for some n and it is enough to prove that $\alpha^i(\mathbf{Z})$ and $\alpha^i(\mathbf{Z}/n\mathbf{Z})$ are isomorphisms.

Let us first do the case $A = \mathbf{Z}$. For $i = 3$, the result is contained in Lemma 11.27. It remains to prove the isomorphism for $i = 1$ and $i = 2$. For $i = 1$, both source and target of $\alpha^1(A)$ are zero: indeed we have

$$\mathrm{Ext}_{G_S}^1(\mathbf{Z}, \mathbb{C}_{K_S, S}) = H^1(G_S, \mathbb{C}_{K_S, S}) = 0,$$

by Proposition 10.5 and $H^1(G_S, \mathbf{Z}) = \mathrm{Hom}_{\mathrm{cont}}(G_S, \mathbf{Z}) = 0$ since G_S is compact and $\mathbf{Z}$ discrete and torsion-free. When $i = 2$, the map

$$\alpha^2(A) : \mathrm{Ext}_{G_S}^2(\mathbf{Z}, \mathbb{C}_{K_S, S}) = H^2(G_S, \mathbb{C}_{K_S, S}) \rightarrow H^0(G_S, \mathbf{Z})^\vee = \mathbf{Q}/\mathbf{Z}$$

coincides with the usual invariant isomorphism $H^2(G_S, \mathbb{C}_{K_S, S}) \simeq \mathbf{Q}/\mathbf{Z}$.

Assume now that $A = \mathbf{Z}/n\mathbf{Z}$ for some integer n . If $i = 3$, the fact that $\mathrm{Ext}_{G_S}^3(\mathbf{Z}/n\mathbf{Z}, \mathbb{C}_{K_S, S}) = 0$ follows from the exact sequence:

$$0 \rightarrow \mathrm{Ext}_{G_S}^2(\mathbf{Z}, \mathbb{C}_{K_S, S})/n \rightarrow \mathrm{Ext}_{G_S}^3(\mathbf{Z}/n\mathbf{Z}, \mathbb{C}_{K_S, S}) \rightarrow \mathrm{Ext}_{G_S}^3(\mathbf{Z}, \mathbb{C}_{K_S, S}),$$

since we know that $\mathrm{Ext}_{G_S}^3(\mathbf{Z}, \mathbb{C}_{K_S, S}) = 0$ and $\mathrm{Ext}_{G_S}^2(\mathbf{Z}, \mathbb{C}_{K_S, S}) \simeq \mathbf{Q}/\mathbf{Z}$ is divisible. If $i = 2$, using the exact sequence:

$$\mathrm{Ext}_{G_S}^1(\mathbf{Z}, \mathbb{C}_{K_S, S}) \rightarrow \mathrm{Ext}_{G_S}^2(\mathbf{Z}/n\mathbf{Z}, \mathbb{C}_{K_S, S}) \rightarrow \mathrm{Ext}_{G_S}^2(\mathbf{Z}, \mathbb{C}_{K_S, S})[n] \rightarrow 0$$

and the fact that $\mathrm{Ext}_{G_S}^1(\mathbf{Z}, \mathbb{C}_{K_S, S}) = H^1(G_S, \mathbb{C}_{K_S, S}) = 0$, we obtain

$$\mathrm{Ext}_{G_S}^2(\mathbf{Z}/n\mathbf{Z}, \mathbb{C}_{K_S, S}) = \mathrm{Ext}_{G_S}^2(\mathbf{Z}, \mathbb{C}_{K_S, S})[n] = H^2(G_S, \mathbb{C}_{K_S, S})[n].$$

Then we can check that the map

$$\alpha^2(A) : \mathrm{Ext}_{G_S}^2(\mathbf{Z}/n\mathbf{Z}, \mathbb{C}_{K_S, S}) = H^2(G_S, \mathbb{C}_{K_S, S})[n] \rightarrow H^0(G_S, \mathbf{Z}/n\mathbf{Z})^\vee = \frac{1}{n}\mathbf{Z}/\mathbf{Z}$$

actually corresponds to the restriction of the usual invariant isomorphism $H^2(G_S, \mathbb{C}_{K_S, S}) \simeq \mathbf{Q}/\mathbf{Z}$ to the n -torsion parts.

This concludes the proof of the theorem in the case where the module A has trivial action.

Step 2: If A is a finitely generated G_S -module, then we can find H an open normal subgroup of G_S such that $A^H = A$. Consider the exact sequence:

$$0 \rightarrow A \rightarrow \mathrm{Ind}_H^{G_S}(A) \rightarrow A_1 \rightarrow 0$$

where A_1 is the obvious quotient. Shapiro's lemma for cohomology (Lemma 5.11) tells us that $H^i(G, \mathrm{Ind}_H^{G_S}(A)) \simeq H^i(H, A)$ and the one for Ext-groups (Lemma 11.10) that

$\text{Ext}_H^i(A, \mathbb{C}_{K_S, S}) = \text{Ext}_{G_S}^i(\text{Ind}_H^{G_S}(A), \mathbb{C}_{K_S, S})$. We obtain a commutative diagram with exact rows:

(11.5.1)

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \text{Ext}_{G_S}^i(A_1, \mathbb{C}_{K_S, S}) & \longrightarrow & \text{Ext}_H^i(A, \mathbb{C}_{K_S, S}) & \longrightarrow & \text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \longrightarrow \text{Ext}_{G_S}^{i+1}(A_1, \mathbb{C}_{K_S, S}) \longrightarrow \cdots \\ & & \downarrow \alpha_{G_S}^i(A_1) & & \downarrow \alpha_H^i(A) & & \downarrow \alpha_{G_S}^i(A) & & \downarrow \alpha_{G_S}^{i+1}(A_1) \\ \cdots & \longrightarrow & H^{2-i}(G_S, A_1)^\vee & \longrightarrow & H^{2-i}(H, A)^\vee & \longrightarrow & H^{2-i}(G_S, A)^\vee & \longrightarrow & H^{1-i}(G_S, A_1)^\vee \longrightarrow \cdots \end{array}$$

Recall that we want to prove that $\alpha_{G_S}^i(A)$ is an isomorphism for $i \in \{2, 3\}$ and also $i = 1$ when A is torsion-free.

Assume first that $i = 3$. We need to show that $\text{Ext}_{G_S}^3(A, \mathbb{C}_{K_S, S})$ is zero. In the first row of the diagram (11.5.1), we know that the term on the right $\text{Ext}_{G_S}^4(A_1, \mathbb{C}_{K_S, S})$ is zero (we apply Lemma 11.27 to the module A_1). But since the action of H on A is trivial, we also know by **Step 1** that the group $\text{Ext}_H^3(A, \mathbb{C}_{K_S, S})$ is zero. Hence $\text{Ext}_{G_S}^3(A, \mathbb{C}_{K_S, S})$ is zero.

Assume that $i = 2$. From the previous case ($i = 3$) applied to the module A_1 we know that $\alpha_{G_S}^3(A_1) : \text{Ext}_{G_S}^3(A, \mathbb{C}_{K_S, S}) \rightarrow H^{-1}(G_S, A_1)^\vee$ is zero (both source and target are zero). Since the action of H on A is trivial, we also know by **Step 1** that the map $\alpha_H^2(A)$ is an isomorphism. Hence it follows from (11.5.1) (for $i = 2$) that $\alpha_{G_S}^2(A)$ is surjective. Since this is true for any module, this also proves that $\alpha_{G_S}^2(A_1)$ is surjective. We then obtain that $\alpha_{G_S}^2(A)$ is an isomorphism using the five lemma.

Assume that $i = 1$ and A is torsion-free. The previous point gives us that $\alpha_{G_S}^2(A_1)$ is an isomorphism and we also know that $\alpha_H^1(A)$ and $\alpha_H^2(A)$ are isomorphisms from **Step 1**. It follows from (11.5.1) (for $i = 1$) that $\alpha_{G_S}^1(A)$ is surjective. Since this is true for any module which are torsion-free and since A_1 is torsion-free, this also proves that $\alpha_{G_S}^1(A_1)$ is surjective. We then obtain that $\alpha_{G_S}^1(A)$ is an isomorphism using the five lemma.

This concludes the proof of the theorem. $\square$

We can now prove Theorem 11.24.

Proof. Let A be in $\text{Mod}_S(G_S)$ and assume that A is finite. We want to show that the map

$$\alpha^i(A) : \text{Ext}_{G_S}^i(A, \mathbb{C}_{K_S, S}) \simeq H^{2-i}(G_S, A)^\vee$$

is an isomorphism for $i \geq 1$. From the previous theorem, we already know that it is the case for $i \geq 2$. So we are left to prove that if A is finite, then $\alpha^1(A)$ is an isomorphism. Reasoning as in the proof of Theorem 11.28, we see that it suffices to show the result for $A = \mathbb{Z}/p^m\mathbb{Z}$ for p a prime number and $m > 0$.

We apply $\text{Ext}_{G_S}(-, \mathbb{C}_{K_S, S})$ to the exact sequence

$$0 \rightarrow \mathbb{Z} \xrightarrow{p^m} \mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z} \rightarrow 0$$

and using the fact that $\text{Ext}_{G_S}^i(\mathbf{Z}, \mathbb{C}_{K_S, S}) = H^i(G_S, \mathbb{C}_{K_S, S})$, we obtain

$$0 \rightarrow H^0(G_S, \mathbb{C}_{K_S, S})/p^m \rightarrow \text{Ext}_{G_S}^1(\mathbf{Z}/p^m\mathbf{Z}, \mathbb{C}_{K_S, S}) \rightarrow H^1(G_S, \mathbb{C}_{K_S, S})[p^m] \rightarrow 0.$$

But the term on the right is zero and the one on the left is $\mathbb{C}_S(K)/p^m$ by Proposition 10.5. The target of $\alpha^1(\mathbf{Z}/p^m\mathbf{Z})$ is

$$H^1(G_S, \mathbf{Z}/p^m\mathbf{Z})^\vee = \text{Hom}_{\text{cont}}(G_S, \mathbf{Z}/p^m\mathbf{Z})^\vee = G_S^{\text{ab}}/p^m$$

(this last equality comes from the usual Pontryagin duality: the evaluation map $g \mapsto (\chi \mapsto \chi(g))$ induces an isomorphism:

$$G_S^{\text{ab}}/p^m \xrightarrow{\sim} \text{Hom}_{\text{cont}}(\text{Hom}_{\text{cont}}(G_S, \frac{1}{m}\mathbf{Z}/\mathbf{Z}), \mathbf{Q}/\mathbf{Z}).)$$

We can check that the map

$$\alpha^1(A) : \mathbb{C}_S(K)/p^m \rightarrow G_S^{\text{ab}}/p^m$$

corresponds to the reciprocity map of Theorem 10.7 and we will see later that this is an isomorphism. [In fact this will follow from the fact that the kernel of the Artin map

$$\mathbb{C}_S(K) \rightarrow G_S^{\text{ab}}$$

is divisible. Note that without taking the quotient by p^m , the result is not true anymore, so the finiteness hypothesis is needed here.]

This concludes the proof of the theorem. □

The proof of the Poitou-Tate duality result is now complete.

11.6 Some consequences

We collect here some consequences of Theorem 11.17.

Corollary 11.29. *If the set S is finite and A is a finite module in $\text{Mod}_S(G_S)$, then the groups $H^i(G_S, A)$ are finite for all i .*

Proof. If S and A are finite then the groups $H^i(G_v, A)$ are all finite so we directly obtain from point (3) of Theorem 11.17 that $H^i(G_S, A)$ is finite for $i \geq 3$. It also follows that the groups $P^i(G_S, A)$ are finite (they are equal to the finite product of the $H^i(G_v, A)$). Then point (2) of Theorem 11.17 implies that $H^0(G_S, A)$ is finite. For $i \in \{1, 2\}$, we have an exact sequence

$$0 \rightarrow \text{III}^i(G_S, A) \rightarrow H^i(G_S, A) \rightarrow P^i(G_S, A)$$

and we see that $H^i(G_S, A)$ has to be finite. □

Corollary 11.30. *Let A be a finite module in $\text{Mod}_S(G_S)$. Then for any finite subset T of S such that $S \setminus T$ contains at least one finite place, the map*

$$H^2(G_S, A) \rightarrow \bigoplus_{v \in T} H^2(G_v, A)$$

is surjective. In particular, it is the case for the map

$$H^2(G_S, A) \rightarrow \bigoplus_{v \text{ real}} H^2(G_v, A).$$

Proof. Let v_0 be a finite place in $S \setminus T$. Recall that when A is finite, the group $P^2(G_S, A)$ is just the direct sum $\bigoplus_{v \in S} H^2(G_v, A)$. Let us take an element $(a_v)_{v \in T}$ in $\bigoplus_{v \in T} H^2(G_v, A)$ and extend it arbitrarily to an element $a = (a_v)_{v \in S}$ in $\bigoplus_{v \in S} H^2(G_v, A) = P^2(G_S, A)$. We will see that we can modify the component a_{v_0} in such a way that a will be in the image of

$$\lambda^2 : H^2(G_S, A) \rightarrow \bigoplus_{v \in S} H^2(G_v, A).$$

By duality between $P^2(G_S, A)$ and $P^0(G_S, A')$ (Proposition 11.2), we know that a corresponds to a character $\chi_a : P^0(G_S, A') \rightarrow \mathbf{Q}/\mathbf{Z}$ and we still write χ_a its restriction to $H^0(G_S, A')$. The inflation map

$$H^0(G_S, A') \rightarrow H^0(G_{v_0}, A')$$

is injective. So we are in the following situation:

$$\begin{array}{ccc} H^0(G_S, A') & \hookrightarrow & H^0(G_{v_0}, A') \\ \chi_a \downarrow & \swarrow \tilde{\chi}_a & \\ \mathbf{Q}/\mathbf{Z} & & \end{array}$$

and the dotted arrow $\tilde{\chi}_a$ exists since $\mathbf{Q}/\mathbf{Z}$ is a divisible abelian group (so it is injective as an abelian group).

We have obtained a character $\tilde{\chi}_a$ of $H^0(G_{v_0}, A')$. But by local duality such a character corresponds to an element a''_{v_0} of $H^2(G_{v_0}, A)$. Consider the element $(a'_v)_{v \in S}$ of $P^2(G_S, A)$ such that $a'_{v_0} = a_{v_0} - a''_{v_0}$ and $a'_v = a_v$ for any $v \neq v_0$. We claim that this element $(a'_v)_{v \in S}$ is in the image of λ^2 . From the exact sequence (11.4.4), it suffices to prove that $(a'_v)_{v \in S}$ is in the kernel of

$$\mu^2 : P^2(G_S, A) \rightarrow H^0(G_S, A')^\vee.$$

But the image of a' by μ^2 is by construction a character $\chi_{a'} : H^0(G_S, A') \rightarrow \mathbf{Q}/\mathbf{Z}$ making the following diagram commute:

$$\begin{array}{ccc} H^0(G_S, A') & \hookrightarrow & H^0(G_{v_0}, A') \\ \chi_{a'} \downarrow & \swarrow \tilde{\chi}_{a'} & \\ \mathbf{Q}/\mathbf{Z} & & \end{array}$$

where $\tilde{\chi}_{a'}$ corresponds to the element $a''_{v_0} - a'_{v_0} = 0$. Hence $\tilde{\chi}_{a'} = 0$ and $\chi_{a'} = 0$ as wanted. $\square$

Example 11.31. The perfect pairing

$$\text{III}^1(G_S, A) \times \text{III}^2(G_S, A') \rightarrow \mathbf{Q}/\mathbf{Z}$$

can be described explicitly.

Let us denote by $Z^1(G_S, A)$ and $Z^2(G_S, A')$ the corresponding groups of cocycles. For elements a in $\text{III}^1(G_S, A)$ and a' in $\text{III}^2(G_S, A')$ we choose representatives α in $Z^1(G_S, A)$ and α' in $Z^2(G_S, A')$ and for v in S , we write α_v and α'_v their respective restrictions to G_v . By definition of the III-groups, we have that for any v in S , the projections $[\alpha_v]$ and $[\alpha'_v]$ of α_v and α'_v in $H^1(G_v, A)$ and $H^2(G_v, A')$ are zero, so there exist a 0-cochain β_v and a 1-cochain β'_v such that

$$\alpha_v = d(\beta_v) \quad \text{and} \quad \alpha'_v = d(\beta'_v).$$

Moreover, since we have $A \otimes A' \simeq U_{K_S}(S)$, the cup-product $\alpha \cup \alpha'$ gives us an element in $Z^3(G_S, U_{K_S}(S))$. But from Proposition 10.6, we know that $H^3(G_S, U_{K_S}(S))(p) = 0$ for all p in $N(S)$. Recall that we have assumed that the order of A is in $N(S)$. It follows that $\alpha \cup \alpha'$ comes from a 2-cochain γ with coefficients in $U_{K_S}(S)$:

$$\alpha \cup \alpha' = d(\gamma).$$

We have

$$d(\beta_v \cup \alpha'_v) = d(\beta_v) \cup \alpha'_v = \alpha_v \cup \alpha'_v = d(\gamma_v)$$

and similarly

$$d(\alpha_v \cup \beta'_v) = d(\gamma_v).$$

On the other hand, we also have

$$d(\beta_v \cup \beta'_v) = d(\beta_v) \cup \beta'_v - \beta_v \cup d(\beta'_v) = \alpha_v \cup \beta'_v - \beta_v \cup \alpha'_v.$$

Then we see that $\beta_v \cup \alpha'_v - \gamma_v$ and $\alpha_v \cup \beta'_v - \gamma_v$ are cocycles in $Z^2(G_v, \overline{K}_v^\times)$ representing the same class c_v in $H^2(G_v, \overline{K}_v^\times)$.

We define:

$$\langle a, a' \rangle := \sum_{v \in S} \text{inv}_v(c_v).$$

Proposition 11.32. *The pairing $\langle a, a' \rangle$ described above is independant of the choices and it coincides with the perfect pairing from Theorem 11.17.*

Proof. Exercise. $\square$

12 Complements

In this section we first study the connected component of the idèles class group. We then use the previous results to completely determine the $\text{Gal}(\overline{K}/K)$ -cohomology of $\mathbf{Z}$.

12.1 The connected component of $\mathbb{C}_K$

In this section K is a number field.

Proposition 12.1. *Any open subgroup of the idèle class group $\mathbb{C}_K$ has finite index.*

Proof. Let $W \subset \mathbb{C}_K$ be an open subgroup. Then the pre-image of W by the projection $\mathbb{I}_K \rightarrow \mathbb{C}_K$ is open and so it contains an open of the form

$$V = \prod_v V_v$$

with $V_v \subset U_v$ is an open subgroup such that $V_v = U_v$ for almost all v , if v is real, V_v is $\mathbf{R}^{\times,+}$ and if v is complex V_v is $\mathbf{C}^\times$. Since when v is finite all open subgroups of U_v have finite index (because in that case U_v is compact), we see that V has finite index in the group

$$\tilde{U} := \prod_{v \text{ finite}} U_v \times \prod_{v \text{ complex}} \mathbf{C}^\times \times \prod_{v \text{ real}} \mathbf{R}^{\times,+}.$$

Then to prove the proposition, it suffices to show that $\mathbb{I}_K/K^\times \tilde{U}$ is finite. But we see that this $\tilde{U}$ is equal to the open $W_{\mathfrak{m}}$ from (4.1.1) where the modulus $\mathfrak{m}$ is equal to $\mathfrak{m} = \prod_{\mathfrak{p} \text{ real place}} \mathfrak{p}$. Hence from Proposition 4.11, we know that $\mathbb{I}_K/K^\times \tilde{U} \simeq C_{\mathfrak{m}}$ for this modulus. Since we have seen that $C_{\mathfrak{m}}$ is finite (Theorem 2.7), this concludes the proof.

(In fact $\mathbb{I}_K/(K^\times \tilde{U})$ corresponds to the narrow class field of K , see Example 2.5(2)).

□

Let us denote by $\mathbb{D}_K$ the connected component of the identity in the idèle class group $\mathbb{C}_K$.

Proposition 12.2. *Let K be a number field. There is an exact sequence:*

$$0 \rightarrow \mathbb{D}_K \rightarrow \mathbb{C}_K \xrightarrow{\psi_K} G_K^{\text{ab}} \rightarrow 0,$$

where $\psi_K : \mathbb{C}_K \rightarrow G_K^{\text{ab}}$ is induced by the Artin maps

$$\psi_{L/K} : \mathbb{C}_K \rightarrow \text{Gal}(L/K)$$

for L/K finite abelian extension of K .

Proof. By reciprocity law (Theorem 4.17), we know that the Artin map is surjective and that the kernel of $\psi_{L/K}$ is exactly equal to $\text{Norm}_{L/K}(\mathbb{C}_L)$. So it suffices to prove that the kernel of the Artin map is equal to the identity component $\mathbb{D}_K$. The existence theorem (Theorem 4.18) tells us that any open subgroup of $\mathbb{C}_K$ of finite index corresponds to a norm group $\text{Norm}_{L/K}(\mathbb{C}_L) = \ker(\psi_{L/K})$. So the kernel of ψ_K is equal to the intersection of all open subgroups of finite index of $\mathbb{C}_K$, which is the same as all open subgroups by Proposition 12.1. Then we conclude using the following general lemma (the proof is left as an exercise):

Lemma 12.3. *In every locally compact group G , the identity component G_0 is the intersection of all open subgroups of G .*

□

Recall that there is a continuous surjective morphism of groups

$$(12.1.1) \quad |\cdot| : \begin{cases} \mathbb{C}_K & \rightarrow (\mathbf{R}_{>0}, \times) \\ a & \mapsto |a| := \prod_v |a_v|_v. \end{cases}$$

and we denote by $\mathbb{C}_K^1$ the kernel of $|\cdot|$, i.e.

$$\mathbb{C}_K^1 := \{a \in \mathbb{C}_K \mid |a| = 1\}.$$

We also set $\mathbb{D}_K^1 := \mathbb{C}_K^1 \cap \mathbb{D}_K$. Recall also that we have seen in Theorem 4.7 that $\mathbb{C}_K^1$ is compact. Moreover, the morphism (12.1.1) admits a continuous section $s : \mathbf{R}_{>0} \rightarrow \mathbb{C}_K$: in fact, for any infinite prime v of K , the restriction of $|\cdot|$ to the subgroup $\mathbf{R}_{>0}$ of $K_v^\times \subset \mathbb{C}_K$ is an isomorphism and we can define s as its inverse. Since $\mathbf{R}_{>0}$ is connected then the image of s is contained in $\mathbb{D}_K$ and we have compatible decompositions:

$$(12.1.2) \quad \mathbb{C}_K \simeq \mathbb{C}_K^1 \times \mathbf{R}_{>0} \quad \text{and} \quad \mathbb{D}_K \simeq \mathbb{D}_K^1 \times \mathbf{R}_{>0}.$$

Lemma 12.4. *Let K be a number field. Then,*

- (1) *We have $\mathbb{D}_K^1 = \bigcap_{L/K} \text{Norm}_{L/K}(\mathbb{C}_L^1)$,*
- (2) *For any finite extension L/K , the norm maps*

$$\begin{aligned} \text{Norm}_{L/K} : \mathbb{D}_L &\rightarrow \mathbb{D}_K, \\ \text{Norm}_{L/K} : \mathbb{D}_L^1 &\rightarrow \mathbb{D}_K^1, \end{aligned}$$

are surjective.

Proof. We have already seen that $\mathbb{D}_K = \bigcap_{L/K} \text{Norm}_{L/K}(\mathbb{C}_L)$. Let us write

$$\text{Norm}_{\overline{K}/K}(\mathbb{C}) := \bigcap_{L/K} \text{Norm}_{L/K}(\mathbb{C}_L) \quad \text{and} \quad \text{Norm}_{\overline{K}/K}(\mathbb{C}^1) := \bigcap_{L/K} \text{Norm}_{L/K}(\mathbb{C}_L^1).$$

Using the decomposition (12.1.2) (by construction of the section s), we see that for any L/K finite Galois,

$$\mathbb{C}_K^1 / \text{Norm}_{L/K}(\mathbb{C}_L^1) \simeq \mathbb{C}_K / \text{Norm}_{L/K}(\mathbb{C}_L).$$

This implies

$$\text{Norm}_{\overline{K}/K}(\mathbb{C}^1) = \mathbb{C}_K^1 \cap \text{Norm}_{\overline{K}/K}(\mathbb{C}) = \mathbb{C}_K^1 \cap \mathbb{D}_K = \mathbb{D}_K^1,$$

which proves (1).

Let us now prove that the norm maps are surjective on $\mathbb{D}_K$ and $\mathbb{D}_K^1$. Let L/K finite, we want to show that

$$\text{Norm}_{L/K} : \mathbb{D}_L^1 \rightarrow \mathbb{D}_K^1$$

is surjective. Let x in $\mathbb{D}_K^1$. Consider the family of sets

$$\{P_M := \text{Norm}_{M/L}(\mathbb{C}_M^1) \cap \text{Norm}_{L/K}^{-1}(x)\}_{M/L \text{ finite}}.$$

For any M/L finite, since $\mathbb{C}_M^1$ is compact then P_M is also compact. It is non-empty (it contains x). Moreover if P_{M_1} and P_{M_2} are two such sets, they both contain $P_{M_1 \cdot M_2}$ and hence their intersection is non empty. It follows that the intersection $\bigcap_{M/L \text{ finite}} P_M$ is non-empty. But if y is an element of $\bigcap_{M/L \text{ finite}} P_M$, then it is an element of $\mathbb{D}_L^1 = \bigcap_{M/L} \text{Norm}_{M/L}(\mathbb{C}_M^1)$ such that its image by the norm map is x . Hence $\text{Norm}_{L/K}$ is surjective on $\mathbb{D}_K^1$.

The surjectivity of

$$\text{Norm}_{L/K} : \mathbb{D}_L \rightarrow \mathbb{D}_K$$

follows then from the commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{D}_L^1 & \longrightarrow & \mathbb{D}_L & \longrightarrow & \mathbf{R}_{>0} \longrightarrow 0 \\ & & \downarrow \text{Norm}_{L/K} & & \downarrow \text{Norm}_{L/K} & & \downarrow \text{Norm}_{L/K} \\ 0 & \longrightarrow & \mathbb{D}_K^1 & \longrightarrow & \mathbb{D}_K & \longrightarrow & \mathbf{R}_{>0} \longrightarrow 0 \end{array}$$

using the fact that the norm map $\text{Norm}_{L/K} : \mathbf{R}_{>0} \rightarrow \mathbf{R}_{>0}$ is given by $x \mapsto x^{[L:K]}$, which is surjective. $\square$

Proposition 12.5. *Let K be a number field. Then,*

- (1) *The group $\mathbb{D}_K$ is equal to the group of all divisible elements of $\mathbb{C}_K$.*
- (2) *The group $\mathbb{D}_K$ is divisible.*

Proof. For (1), note that $\mathbb{C}_K / \mathbb{D}_K$ is equal to $\mathbb{C}_K^1 / \mathbb{D}_K^1$ and so it is compact, totally disconnected and Hausdorff (i.e. it is a profinite group). Let x be a divisible element of $\mathbb{C}_K$. Then its image in the quotient $\mathbb{C}_K / \mathbb{D}_K$ is contained in every open subgroup, so it is trivial. In other words, x is in $\mathbb{D}_K$.

To prove (2), since the group $(\mathbf{R}_{>0}, \times)$ is divisible, we see from the decomposition (12.1.2) that it suffices to prove that $\mathbb{D}_K^1$ is divisible. Let p be a prime number. For L a finite extension of K that contains a p -th root of unity and S a finite set of places of L , consider the Kummer extension $M := L(U_L(S)^{\frac{1}{p}})$ corresponding to the group $U_L(S) \cdot L^{\times p} / L^{\times p} \simeq U_L(S) / U_L(S) \cap L^{\times p}$. Recall that we have seen in the proof of Theorem 8.7 that for S large enough we have

$$W(S)L^{\times} / L^{\times} = \text{Norm}_{M/L}(\mathbb{C}_M)$$

where

$$W(S) := \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v.$$

So we obtain

$$\mathbb{D}_L \subset W(S)L^{\times} / L^{\times} = (\mathbb{C}_L)^p \cdot (U_{L,S}L^{\times} / L^{\times}),$$

where

$$U_{L,S} = \prod_{v \in S} \{1\} \times \prod_{v \notin S} U_v.$$

Since the morphism $|\cdot|$ is trivial on $(U_{L,S}L^{\times} / L^{\times})$, it follows that we have the inclusion

$$\mathbb{D}_L^1 \subset W(S)L^{\times} / L^{\times} = (\mathbb{C}_L^1)^p \cdot (U_{L,S}L^{\times} / L^{\times}).$$

This is true for all set S large enough, hence

$$\mathbb{D}_L^1 \subset \bigcap_{S \text{ "large enough"}} (\mathbb{C}_L^1)^p \cdot (U_{L,S}L^{\times} / L^{\times}) = (\mathbb{C}_L^1)^p.$$

By the previous lemma we know that $\mathbb{D}_K^1 = \text{Norm}_{L/K}(\mathbb{D}_L^1)$ and we finally obtain

$$(12.1.3) \quad \mathbb{D}_K^1 \subset (\text{Norm}_{L/K}(\mathbb{C}_L^1))^p.$$

Let x be an element of $\mathbb{D}_K^1$, we want to show that there exists y in $\mathbb{D}_K^1$ such that $y^p = x$. Let us write f_p for the map $\mathbb{C}_K^1 \rightarrow \mathbb{C}_K^1, a \mapsto a^p$. Consider the family of sets

$$\{X_L := \text{Norm}_{L/K}(\mathbb{C}_L^1) \cap f_p^{-1}(x)\}_{L/K \text{ s.t. } \zeta_p \in L}$$

The spaces X_L are compact and non-empty by (12.1.3) and any intersection of two of them contains a third. Hence $\bigcap_{L/K} X_L$ is non empty. If y is in $\bigcap_{L/K} X_L$, then by construction, y is an element of $\mathbb{D}_K^1$ such that $y^p = x$. This concludes the proof of the proposition. $\square$

For K be a number field and S be a (possibly infinite) set of places of K , we denote by $\mathbb{D}_S(K)$ the identity component of the group $\mathbb{C}_S(K)$.

Proposition 12.6. *Let K be a number field and S be a set of places of K . Then*

$$\mathbb{D}_S(K) = \mathbb{D}_K U_{K,S} / U_{K,S}$$

and the group $\mathbb{D}_S(K)$ is divisible. Moreover there is an exact sequence:

$$0 \rightarrow \mathbb{D}_S(K) \rightarrow \mathbb{C}_S(K) \xrightarrow{\psi_S} G_S^{\text{ab}} \rightarrow 0,$$

where $\psi_S : \mathbb{C}_S(K) \rightarrow G_K^{\text{ab}}$ is induced by the Artin maps

$$\psi_{L/K} : \mathbb{C}_S(K) \rightarrow \text{Gal}(L/K)$$

for L/K finite abelian extension of K in K_S .

Proof. Recall that the group $\mathbb{C}_S(K)$ is defined as the quotient $\mathbb{C}_K/U_{K,S}$. So the identity component $\mathbb{D}_S(K)$ is equal to the closure of $\mathbb{D}_K$ via the map $\mathbb{C}_K \rightarrow \mathbb{C}_K/U_{K,S} = \mathbb{C}_S(K)$. But $U_{K,S}$ is compact so the projection $\mathbb{C}_K \rightarrow \mathbb{C}_S(K)$ is proper and the image of $\mathbb{D}_K$ is already closed. We have showed

$$\mathbb{D}_S(K) = \mathbb{D}_K U_{K,S} / U_{K,S}$$

as wanted. The fact that $\mathbb{D}_S(K)$ is divisible follows then from the same statement for $\mathbb{D}_K$ (Proposition 12.5(2)).

To obtain the exact sequence from the lemma, first note that the image of the subgroup $U_{K,S} \subset \mathbb{C}_K$ via the Artin map $\mathbb{C}_K \rightarrow G_K^{\text{ab}}$ is equal to the subgroup of G_K^{ab} fixing the subextensions of K_S which are abelian, i.e. the subgroup fixing $K_S \cap K^{\text{ab}}$. But this subgroup is also equal to the kernel of the map

$$G_K^{\text{ab}} \rightarrow G_S^{\text{ab}}.$$

Hence, if we apply the snake lemma to the commutative diagram with exact rows:

$$\begin{array}{ccccccc} U_{K,S} & \longrightarrow & \text{Gal}(K^{\text{ab}}/K_S \cap K^{\text{ab}}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbb{D}_K & \longrightarrow & \mathbb{C}_K & \longrightarrow & \text{Gal}(K^{\text{ab}}/K) \longrightarrow 0, \end{array}$$

we obtain the desired exact sequence. □

12.2 An example: the cohomology of $\mathbb{Z}$

Let us now give an example of a concrete computation of cohomology.

Proposition 12.7. *Let K be a number field and let G_K be its absolute Galois group. Let r be the number of real primes of K . Then,*

$$\begin{aligned} H^0(G_K, \mathbb{Z}) &= \mathbb{Z}, \\ H^1(G_K, \mathbb{Z}) &= 0, \\ H^2(G_K, \mathbb{Z}) &= \text{Hom}(\mathbb{C}_K/\mathbb{D}_K, \mathbb{Q}/\mathbb{Z}), \\ H^{2i}(G_K, \mathbb{Z}) &= (\mathbb{Z}/2\mathbb{Z})^{2r} \quad \text{for } i \geq 2, \\ H^{2i+1}(G_K, \mathbb{Z}) &= 0 \quad \text{for } i \geq 2. \end{aligned}$$

Note that this is also true that $H^3(G_K, \mathbf{Z})$ is trivial but we will not prove it here.

Proof. The result for $i = 0$ is obvious. For $i = 1$, we have

$$H^1(G_K, \mathbf{Z}) = \text{Hom}_{\text{cont}}(G_K, \mathbf{Z}) = 0$$

since G_K is profinite hence compact and $\mathbf{Z}$ is discrete and without torsion. For $i = 2$, consider the exact sequence:

$$0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Q} \rightarrow \mathbf{Q}/\mathbf{Z} \rightarrow 0.$$

Since $H^1(G_K, \mathbf{Q}) = H^2(G_K, \mathbf{Q}) = 0^5$, we obtain

$$H^2(G_K, \mathbf{Z}) = H^1(G_K, \mathbf{Q}/\mathbf{Z}) = \text{Hom}_{\text{cont}}(G_K, \mathbf{Q}/\mathbf{Z}) = \text{Hom}_{\text{cont}}(G_K^{\text{ab}}, \mathbf{Q}/\mathbf{Z}).$$

By Proposition 12.2, we can identify G_K^{ab} with $\mathbb{C}_K/\mathbb{D}_K$ and we obtain the desired formula for $H^2(G_K, \mathbf{Z})$.

Assume that $i \geq 4$. Then we have (using again that $H^j(G_K, \mathbf{Q}) = H^j(G_v, \mathbf{Q}) = 0$ for $j > 0$ and all places v):

$$\begin{aligned} H^i(G_K, \mathbf{Z}) &= H^{i-1}(G_K, \mathbf{Q}/\mathbf{Z}) \\ &= \varinjlim_n H^{i-1}(G_K, \frac{1}{n}\mathbf{Z}/\mathbf{Z}) \\ &= \varinjlim_n \prod_{v \text{ real}} H^{i-1}(G_v, \frac{1}{n}\mathbf{Z}/\mathbf{Z}) \\ &= \prod_{v \text{ real}} \varinjlim_n H^{i-1}(G_v, \frac{1}{n}\mathbf{Z}/\mathbf{Z}) \\ &= \prod_{v \text{ real}} H^{i-1}(G_v, \mathbf{Q}/\mathbf{Z}) \\ &= \prod_{v \text{ real}} H^i(G_v, \mathbf{Z}), \end{aligned}$$

where the third equality is given by Theorem 11.17. But then since $\text{Gal}(\mathbf{C}/\mathbf{R})$ is cyclic, the groups $H^i(G_v, \mathbf{Z})$ can be computed by the usual formulas for cyclic groups. We have

$$H^{i-1}(G_v, \mathbf{Z}) = \begin{cases} \mathbf{Z}/2\mathbf{Z} & \text{if } i \text{ is even,} \\ 0 & \text{if } i \text{ is odd.} \end{cases}$$

□

⁵Recall that if G is a profinite group, then for any G -module V which is a $\mathbf{Q}$ -vector space, the cohomology groups $H^i(G, V)$ are zero for $i > 0$. This follows from the fact that the groups $H^i(G, M)$ are torsion for any G -module M and $i > 0$.

12.3 The global Euler-Poincaré characteristic

Let K be a number field and let S be a finite set of places such that S contains all infinite places of K . As before we write K_S for the maximal extension of K unramified outside of S and $G_S := \text{Gal}(K_S/K)$. Recall that we denote by $U_K(S) \subset K^\times$ (respectively $U_{K_S}(S) \subset K_S^\times$) the group of S -units.

12.3.1 Statement of the main theorem

For A a finite G_S -module such that its order is an S -unit, we know from Corollary 11.29 that the groups $H^i(G_S, A)$ are finite for all $i \geq 0$. We define the Euler-Poincaré characteristic of A as

$$\chi(G_S, A) = \frac{|H^0(G_S, A)| \cdot |H^2(G_S, A)|}{|H^1(G_S, A)|}.$$

Theorem 12.8. *We have:*

$$\chi(G_S, A) = \prod_{v \in S_\infty} \frac{|H^0(G_v, A)|}{|\#A|_v}.$$

Recall that if K_v is a non-archimedean local field and A a finite G_v -module, we also define the Euler-Poincaré characteristic as the quotient

$$\chi(G_v, A) = \frac{|H^0(G_v, A)| \cdot |H^2(G_v, A)|}{|H^1(G_v, A)|}.$$

Then we have the following result:

$$(12.3.1) \quad \chi(G_v, A) = |\#A|_v.$$

When K_v is $\mathbf{R}$ or $\mathbf{C}$ and $G_v = \text{Gal}(\mathbf{C}/K_v)$ then we have

$$(12.3.2) \quad \frac{|H^0(G_v, A)| \cdot |H^0(G_v, A')|}{|H^1(G_v, A)|} = |\#A|_v.$$

In that case we define the Euler-Poincaré characteristic as

$$\chi(G_v, A) = \frac{|\widehat{H}^0(G_v, A)| \cdot |\widehat{H}^2(G_v, A)|}{|\widehat{H}^1(G_v, A)|}.$$

Since the Herbrand quotient of a finite module is equal to 1 (Proposition 5.2(2)), we obtain

$$(12.3.3) \quad \chi(G_v, A) = |\widehat{H}^0(G_v, A)|.$$

12.3.2 Proof of Theorem 12.8

The idea of the proof is similar to the one of the equivalent local result. Recall that we assume that S and A are finite. We define

$$\varphi(A) := \chi(G_S, A) \cdot \left(\prod_{v \in S_\infty} \frac{|H^0(G_v, A)|}{|\#A|_v} \right)^{-1}$$

and our goal is to show that $\varphi(A) = 1$.

Lemma 12.9. *We have $\varphi(A) \cdot \varphi(A') = 1$.*

Proof. Recall (see Exercise Sheet 5) that for M_i with $0 \leq i \leq r$ finite groups such that there is an exact sequence of groups:

$$0 \rightarrow M_0 \rightarrow M_1 \rightarrow \cdots \rightarrow M_{r-1} \rightarrow M_r \rightarrow 0$$

then

$$\prod_{0 \leq i \leq r \text{ s.t. } i \text{ even}} |M_i| = \prod_{0 \leq i \leq r \text{ s.t. } i \text{ odd}} |M_i|.$$

We apply this result to the nine terms exact sequence (11.4.4) and we obtain

$$\chi(G_S, A) \cdot \chi(G_S, A') = \frac{|P^0(G_S, A)| \cdot |P^2(G_S, A)|}{|P^1(G_S, A)|}.$$

But S is finite so

$$\frac{|P^0(G_S, A)| \cdot |P^2(G_S, A)|}{|P^1(G_S, A)|} = \prod_{v \in S} \chi(G_v, A).$$

Formulas (12.3.1) and (12.3.3) then yield

$$\chi(G_S, A) \cdot \chi(G_S, A') = \left(\prod_{v \in S \text{ finite}} |\#A|_v \right) \cdot \left(\prod_{v \in S \text{ infinite}} |\hat{H}^0(G_v, A)| \right).$$

From the product formula and the fact that $|\#A|_v = 1$ when $v \notin S$, we also have

$$\prod_{v \in S \text{ finite}} |\#A|_v = \left(\prod_{v \in S_\infty} |\#A|_v \right)^{-1}.$$

Hence,

$$\chi(G_S, A) \cdot \chi(G_S, A') = \prod_{v \in S_\infty} \frac{|\hat{H}^0(G_v, A)|}{|\#A|_v}.$$

Since A is finite $|\hat{H}^0(G_v, A)| = |\hat{H}^1(G_v, A)| = |H^1(G_v, A)|$ and formula (12.3.2) finally gives us

$$\chi(G_S, A) \cdot \chi(G_S, A') = \prod_{v \in S_\infty} \frac{|H^0(G_v, A)| \cdot |H^0(G_v, A')|}{(|\#A|_v)^2},$$

as wanted. □

Hence, to prove Theorem 12.8, it suffices to prove the following proposition:

Proposition 12.10. *We have $\varphi(A) = \varphi(A')$.*

Let us denote by $\text{Mod}_S^f(G_S)$ the subcategory of $\text{Mod}_S(G_S)$ which consists of finite modules.

Lemma 12.11. *The map $\varphi : \text{Mod}_S^f(G_S) \rightarrow (\mathbf{Q}_{>0}, \times)$ is additive, in the sense that if*

$$0 \rightarrow A_1 \rightarrow A \rightarrow A_2 \rightarrow 0$$

is a short exact sequence of in $\text{Mod}_S^f(G_S)$ then,

$$\varphi(A) = \varphi(A_1)\varphi(A_2).$$

Proof. Applying $H^i(G_S, -)$ to the exact sequence from the lemma and using Theorem 11.17 in degrees $i \geq 3$, we obtain an exact sequence of finite groups:

$$\begin{aligned} 0 &\rightarrow H^0(G_S, A_1) \rightarrow H^0(G_S, A) \rightarrow H^0(G_S, A_2) \\ &\rightarrow H^1(G_S, A_1) \rightarrow \cdots \rightarrow H^2(G_S, A_2) \\ &\rightarrow \bigoplus_{v \text{ real}} H^3(G_v, A_1) \rightarrow \bigoplus_{v \text{ real}} H^3(G_v, A) \rightarrow \bigoplus_{v \text{ real}} H^3(G_v, A_2) \\ &\rightarrow \bigoplus_{v \text{ real}} H^4(G_v, A_1) \rightarrow \bigoplus_{v \text{ real}} H^4(G_v, A) \rightarrow \bigoplus_{v \text{ real}} H^4(G_v, A_2) \\ &\rightarrow \text{Ker}\left(\bigoplus_{v \text{ real}} H^5(G_v, A_1) \rightarrow \bigoplus_{v \text{ real}} H^5(G_v, A)\right) \rightarrow 0. \end{aligned}$$

But since we are assuming that the modules are finite and G_v is cyclic, we have

$$\frac{|H^3(G_v, M)|}{|H^4(G_v, M)|} = 1 \quad \text{and} \quad H^5(G_v, M) = H^1(G_v, M) \quad \text{for } M \in \{A, A_1, A_2\}$$

So the above exact sequence gives

$$\chi(G_S, A_1) \cdot \chi(G_S, A_2) = \chi(G_S, A) \cdot |C|$$

where

$$C := \text{Ker}\left(\bigoplus_{v \text{ real}} H^1(G_v, A_1) \rightarrow \bigoplus_{v \text{ real}} H^1(G_v, A)\right).$$

Then the order of C can be computed using the following exact sequence:

$$0 \rightarrow \bigoplus_{v \text{ real}} H^0(G_v, A_1) \rightarrow \bigoplus_{v \text{ real}} H^0(G_v, A) \rightarrow \bigoplus_{v \text{ real}} H^0(G_v, A_2) \rightarrow C \rightarrow 0.$$

We have

$$|C| = \prod_{v \text{ real}} \frac{|H^0(G_v, A_1)| \cdot |H^0(G_v, A_2)|}{|H^0(G_v, A)|}.$$

Since we also know that $|A_1| \cdot |A_2| = |A|$, we obtain

$$\varphi(A_1) \cdot \varphi(A_2) = \varphi(A),$$

as wanted. $\square$

Before proving our main result, let us recall a few facts about the Grothendieck group of finite dimensional $\mathbf{F}_p[G]$ -modules, where G is a finite group and p a prime number. We denote by $R_{\mathbf{F}_p}(G)$ this group. This is the abelian group generated by isomorphism classes $[M]$ of $\mathbf{F}_p[G]$ -modules where we impose the following relations: if

$$0 \rightarrow M_1 \rightarrow M \rightarrow M_2 \rightarrow 0$$

is an exact sequence then

$$[M] = [M_1] + [M_2].$$

Note that since $\text{Hom}_{\mathbf{F}_p}(-, \mathbf{F}_p)$ is exact, it defines a functor:

$$(-)^* : R_{\mathbf{F}_p}(G) \rightarrow R_{\mathbf{F}_p}(G).$$

Moreover, there is a morphism $\theta : R_{\mathbf{F}_p}(G) \rightarrow \mathbf{Q}_{>0}$ sending the class of a module $[M]$ to the order of M^G .

We can describe generators for this group. More precisely, we have:

Lemma 12.12. *Let G be a finite group and for any subgroup H of G consider*

$$\text{Ind}_H^G : R_{\mathbf{F}_p}(H) \rightarrow R_{\mathbf{F}_p}(G)$$

be the morphism taking the class of an H -module to the class of the corresponding induced G -module. Then $R_{\mathbf{F}_p}(G) \otimes \mathbf{Q}$ is generated by the images of the Ind_H^G as H runs over the set of cyclic subgroups of G of order prime to p .

We can also endow the group $R_{\mathbf{F}_p}(G)$ with a multiplicative structure, setting

$$[M_1] \cdot [M_2] = [M_1 \otimes M_2]$$

where the identity is the class of $\mathbf{F}_p$ (with the trivial action).

Proof of Proposition 12.10 (and hence of Theorem 12.8). Let A be in $\text{Mod}_S^f(G_S)$. Recall that we want to show that $\varphi(A) = \varphi(A')$. From Lemma 12.11, we see that it suffices to prove the result for A killed by a prime p with p a S -unit. Choose L/K a finite Galois subextension of K_S/K such that $\text{Gal}(K_S/L)$ fixes A . Up to changing L by some $L(\zeta_p)$ (since $\text{Gal}(K_S/L(\zeta_p)) \subset \text{Gal}(K_S/L)$), we can assume that L contains a primitive p -th root of 1 (or a primitive 4-th root of 1 if $p = 2$). Write $G := \text{Gal}(L/K)$. The groups A and $H^i(\text{Gal}(K_S/L), A)$ define classes $[A]$ and $[H^i(\text{Gal}(K_S/L), A)]$ in the Grothendieck group $R_{\mathbf{F}_p}(G)$. In view of

Lemma 12.12, let us consider a cyclic subgroup $H \subset G$ of order prime to p and assume that A is equal to $\text{Ind}_H^G(M)$ for some H -module M in $R_{\mathbf{F}_p}(H)$. Let us also denote by $K' = L^H$ the corresponding extension. Since L is a totally imaginary field then it follows from Theorem 11.17 that $H^i(\text{Gal}(K_S/L), M) = 0$ for $i \geq 3$. We obtain that there exists a well-defined morphism

$$\chi' : R_{\mathbf{F}_p}(H) \rightarrow R_{\mathbf{F}_p}(H)$$

sending a class $[M]$ in $R_{\mathbf{F}_p}(H)$ to

$$[H^0(\text{Gal}(K_S/L), M)] - [H^1(\text{Gal}(K_S/L), M)] + [H^2(\text{Gal}(K_S/L), M)].$$

Now recall that we have a map $\theta : R_{\mathbf{F}_p}(H) \rightarrow \mathbf{Q}_{>0}$ sending $[M]$ to the order of M^H .

Claim 12.13. We have $(\theta \circ \chi')(M) = \chi(G_S, A)$.

Proof of Claim 12.13. By definition we have

$$(\theta \circ \chi')(M) = \frac{|H^0(\text{Gal}(K_S/L), M)^H| \cdot |H^2(\text{Gal}(K_S/L), M)^H|}{|H^1(\text{Gal}(K_S/L), M)^H|}.$$

Since H is cyclic of order prime to p and M is killed by p (since A is), we have $H^i(H, H^j(\text{Gal}(K_S/L), M)) = 0$ for $i > 0$ and $j \geq 0$. So the Hochschild-Serre spectral sequence

$$H^i(H, H^j(\text{Gal}(K_S/L), M)) \Rightarrow H^{i+j}(\text{Gal}(K_S/K'), M)$$

induces isomorphisms

$$H^i(\text{Gal}(K_S/K'), M) \simeq H^i(\text{Gal}(K_S/L), M)^H$$

and we obtain

$$(\theta \circ \chi')(M) = \chi(\text{Gal}(K_S/K'), M).$$

Let us write $G'_S := \text{Gal}(K_S/K')$. By Shapiro's lemma, we also have

$$\begin{aligned} H^i(G_S, \text{Res}_G^{G_S}(A)) &= H^i(G_S, \text{Res}_G^{G_S}(\text{Ind}_H^G(M))) \\ &= H^i(G_S, \text{Ind}_{G'_S}^{G_S}(M)) \\ &= H^i(G'_S, M), \end{aligned}$$

which proves that $\chi(G'_S, M) = \chi(G_S, A)$. This concludes the proof of the claim. $\square$

Let us come back to the proof of the proposition. We want to show that $\varphi(A) = \varphi(A')$. We first prove that $\chi(G_S, A) = \chi(G_S, A')$. This will follow from the following computation:

Lemma 12.14. *Let M be a finite $\mathbf{F}_p[H]$ -module. Then*

$$(1) \chi'(M') = [M]^* \cdot \chi'(\mu_p),$$

$$(2) [M] \cdot [\mathbf{F}_p[H]] = \dim_{\mathbf{F}_p}(M) \cdot [\mathbf{F}_p[H]].$$

(Here we are setting $M' := \text{Hom}(M, \mu_p)$, which is consistent with our previous notation).

Proof of Lemma 12.14. We claim that for all $i \geq 0$, there are isomorphisms

$$H^i(\text{Gal}(K_S/L), \mu_p) \otimes \text{Hom}(M, \mathbf{F}_p) \xrightarrow{\sim} H^i(\text{Gal}(K_S/L), M')$$

In degree 0, this isomorphism is induced by the product

$$(\zeta_p, f) \mapsto (x \mapsto \zeta_p^{f(x)}) : \mu_p \times \text{Hom}(M, \mathbf{F}_p) \rightarrow M'$$

(recall that the action of $\text{Gal}(K_S/L)$ on M and μ_p is trivial). In higher degree, note that if we choose a resolution $\mu_p \rightarrow I^\bullet$ by injective modules, then $I^\bullet \otimes \text{Hom}(M, \mathbf{F}_p)$ will then define an injective resolution of M' via the above product. The isomorphism in higher degrees follow and this proves the first point.

For the second point, let us denote M_0 the module M with a trivial H -action. Then the map $g \otimes x \mapsto g \otimes g(x)$ induces an isomorphism of $\mathbf{F}_p[H]$ -modules:

$$\mathbf{F}_p[H] \otimes M_0 \xrightarrow{\sim} \mathbf{F}_p[H] \otimes M.$$

This proves (2). □

Using first (1) then (the dual of) (2) we obtain:

$$\chi'(M') \cdot [\mathbf{F}_p[H]]^* = [M]^* \cdot [\mathbf{F}_p[H]]^* \cdot \chi'(\mu_p) = \dim_{\mathbf{F}_p}(M) \cdot [\mathbf{F}_p[H]]^* \cdot \chi'(\mu_p),$$

and since $\dim_{\mathbf{F}_p}(M) = \dim_{\mathbf{F}_p}(M')$ we also have

$$\chi'(M) \cdot [\mathbf{F}_p[H]]^* = \dim_{\mathbf{F}_p}(M) \cdot [\mathbf{F}_p[H]]^* \cdot \chi'(\mu_p).$$

Applying θ and using Claim 12.13, we obtain

$$\chi(G_S, A') = \chi(G_S, A).$$

To show that $\varphi(A) = \varphi(A')$, it remains to show that for all v real,

$$(12.3.4) \quad \frac{|A^{G_v}|}{|\#A|_v} = \frac{|(A')^{G_v}|}{|\#A'|_v}.$$

For v real, either $G_v \simeq \mathbf{Z}/2\mathbf{Z}$ or G_v is trivial. In the case where G_v is trivial, (12.3.4) is obviously satisfied. Assume $G_v \simeq \mathbf{Z}/2\mathbf{Z} = \langle 1, \sigma \rangle$. Recall that we have also assumed that A is finite and killed by some prime p . If p is not 2 then the norm map $N = 1 + \sigma$ induces an isomorphism

$$A/(\sigma - 1) \xrightarrow{\sim} A^\sigma.$$

(For the surjectivity: we have $x = (1 + \sigma)(\frac{x}{2}) + (1 - \sigma)(\frac{x}{2})$. For the injectivity, if $(1 + \sigma)(x) = 0$ and $(1 - \sigma)(x) = 0$ then $2x = 0$ so $x = 0$.)

We can then check that the duality between A and A' induces a duality between $A/(\sigma - 1)$ and $(A')^\sigma$ and the equality (12.3.4) follows.

Assume now that $p = 2$. Recall that we have assumed that $A = \text{Ind}_H^G M$ where $H = \text{Gal}(L/K')$ is a cyclic group of order prime to 2. For v a real place in S , choose v_0 and w places of K' and L above v . Then $\text{Gal}(L_w/K'_{v_0})$ is trivial so $\text{Gal}(\bar{K}_v/K'_{v_0})$ fixes M . Let us write $G'_v := \text{Gal}(\bar{K}_v/K'_{v_0})$. By Shapiro's lemma, we have $H^0(G'_v, M) = H^0(G_v, A)$ and we see that A is fixed by G_v . Hence A' is also fixed by G_v and equality (12.3.4) follows.

This proves that $\varphi(A) = \varphi(A')$, as wanted. □

12.3.3 Consequences

Recall that in this section we are assuming that both S and A are finite.

Corollary 12.15. *We have:*

$$\chi(G_S, A) = \prod_{v \in S_\infty} \frac{|\hat{H}^0(G_v, A')|}{|H^0(G_v, A)|}.$$

Proof. From Theorem 12.8, we have

$$\chi(G_S, A) = \prod_{v \in S_\infty} \frac{|H^0(G_v, A)|}{|\#A|_v}$$

and replacing $|\#A|_v$ using (12.3.2), we obtain

$$\chi(G_S, A) = \prod_{v \in S_\infty} \frac{|H^1(G_v, A)|}{|H^0(G_v, A')|}.$$

Then the following (local archimedean) duality result gives us that $|H^1(G_v, A)| = |H^1(G_v, A')|$:

Proposition 12.16. *For any finitely generated $\text{Gal}(\mathbf{C}/\mathbf{R})$ -module M with dual $M' := \text{Hom}(M, \mathbf{C}^\times)$, the cup product defines a non degenerate pairing of finite groups*

$$\hat{H}^i(\text{Gal}(\mathbf{C}/\mathbf{R}), M') \times \hat{H}^{2-i}(\text{Gal}(\mathbf{C}/\mathbf{R}), M) \rightarrow H^2(\text{Gal}(\mathbf{C}/\mathbf{R}), \mathbf{C}^\times) \simeq \frac{1}{2}\mathbf{Z}/\mathbf{Z}$$

for all $i \geq 0$.

And since A' is finite, its Herbrand quotients are equal to 1, which implies $|H^1(G_v, A')| = |\hat{H}^0(G_v, A')|$. □

Corollary 12.17. *We have:*

$$\chi(G_S, A) \cdot \chi(G_S, A') = \prod_{v \in S} \chi(G_v, A).$$

Proof. This computation was done in the proof of Lemma 12.9. □

Example 12.18. Theorem 12.8 is often used to compute the order of $H^1(G_S, A)$. In fact from the theorem, we have

$$|H^1(G_S, A)| = |H^0(G_S, A)| \cdot |H^2(G_S, A)| \cdot \prod_{v \text{ arch.}} \frac{|\#A|_v}{|H^0(G_v, A)|}.$$

and from Theorem 11.17, we know that $H^2(G_S, A)$ fits into an exact sequence

$$0 \rightarrow \text{III}^2(G_S, A) \rightarrow H^2(G_S, A) \rightarrow \bigoplus_{v \in S} H^2(K_v, A) \rightarrow H^0(G_S, A')^\vee \rightarrow 0.$$

Since by duality $|\text{III}^2(G_S, A)| = |\text{III}^1(G_S, A')|$ and $|H^0(K_v, A')| = |H^2(K_v, A)|$, we obtain

$$|H^1(G_S, A)| = |\text{III}^1(G_S, A')| \cdot \frac{|H^0(G_S, A)|}{|H^0(G_S, A')|} \cdot \prod_{v \in S} |H^0(K_v, A')| \cdot \prod_{v \text{ arch.}} \frac{|\#A|_v}{|H^0(G_v, A')|}.$$

Remark 12.19. In the above we have assumed that the set S is finite. In fact a similar result can be proved when S is infinite as well. Since in that case the cohomology groups are not necessarily finite, we need to work with Haar measures instead of orders.