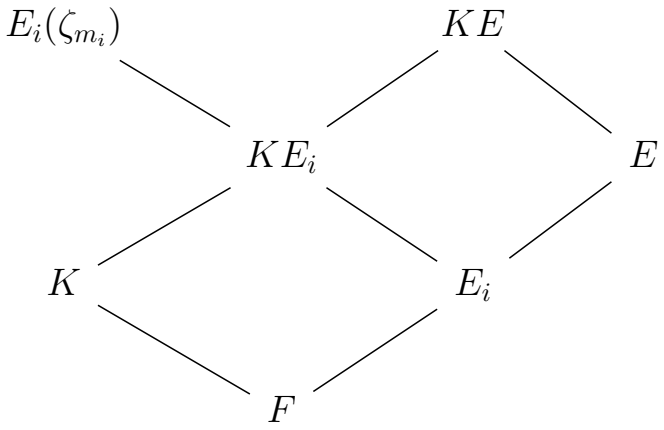
Student Seminar in Pure Mathematics

Class Field Theory

Marilou Bezos
Damien Ganaël Bridel
Kasimir Pierre Rama De Guilhem De Lataillade
Boran Erol
Léo Pierre Karlen
Paul Corentin Mathiot
Raphaël Augustin Parriaux
Sandro Pfammatter
Eva Sophie Terzolo
Tianxiang Xie

Aleksandra Bogdanova
Douglas Christian Clerc
Pierre Emmanuel Augustin Descombes
Eliot Grimont
Junda Long
Louis Romain André Menétrey
Beatrice Pedroni
Loris Alain Alexandre Schirar
Dimitri Wyss



EPFL

EPFL Lausanne, Fall semester 2025–2026

Contents

0 Preface

The present manuscript grew out of the student seminar in pure mathematics at EPFL, organized by Dimitri Wyss as the main organizer and Pierre Emmanuel Augustin Descombes as the teaching assistant, which took place in the fall semester of 2025. The goal was to get familiar with the basics of Class Field Theory following Nancy Childress's book[1]. Unless otherwise stated all the material is taken from there. The seminar consisted of 2 hours of lectures and 2 hours of exercises per week for 14 weeks. The lectures, notes, and solutions were given and written by the students participating in the seminar course. Each chapter ends with a few exercises, the solutions of which can be found at the end of the notes.
We motivated class field theory in two ways. First by the quadratic reciprocity law following Wyman [2], and secondly by Dirichlet's theorem on primes in arithmetic progressions. These well-known theorems can be seen as consequences of Artin reciprocity and the Existence theorem respectively.
After recalling basic properties of number fields and local fields we study idèles, cyclic group cohomology and a bit of analytic number theory to deduce the main theorems of class field theory.
We finish by taking full responsibility for the possible typos and errors that you may find in these notes.

[1] Class field theory. Springer Science and Business Media, 2008.
[2] What is a Reciprocity Law?, The American Mathematical Monthly, Vol. 79, No. 6 (Jun. - Jul., 1972), pp. 571-586.

1 Recollection on number and local fields

In this sections we recall some basic facts about number fields and their completions.

1.1 Number fields

A *number field* F is a finite extension of the rational numbers $\mathbb{Q}$. The integral closure $\mathcal{O}_F$ of $\mathbb{Z}$ inside F is called *the ring of integers* of F.
While $\mathcal{O}_F$ fails in general to be a PID or a UFD, it has the structure of a Dedekind domain i.e. it's a Noetherian, integrally closed domain and every non-zero prime ideal is maximal. As a consequence any ideal in $\mathcal{O}_F$ admits a unique factorization into prime ideals. Hence it make sense to write $\mathfrak{p}|\mathfrak{a}$ whenever $\mathfrak{p}$ is a factor in the decomposition of an ideal $\mathfrak{a} \subset \mathcal{O}_F$.

Example 1.1. In $\mathbb{Z}[\sqrt{-5}]$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

two factorizations into irreducibles. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. But the ideal (6) factors uniquely as $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$. Notice that (2) and (3) are not prime ideals since for example $(1+\sqrt{-5})(1-\sqrt{-5}) \in (3)$ but neither $(1 + \sqrt{-5}) \notin (3)$ and similarly for (2).

A *fractional ideal* of F is a non-zero finitely generated $\mathcal{O}_F$-submodule of F. The set of fractional ideals form an abelian group $\mathcal{I}_F$ under multiplication with identity $\mathcal{O}_F$ and for any $\mathfrak{a} \in \mathcal{I}_F$ its inverse is given by

$$\mathfrak{a}^{-1} = \{x \in F \mid x\mathfrak{a} \subset \mathcal{O}_F\}.$$

It follows from the unique factorization of any ideal into prime ideals, that $\mathcal{I}_F$ is the free abelian group generated by the non-zero prime ideals of $\mathcal{O}_F$.

Example 1.2. Any fractional ideal in $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Q}^\times$. Its inverse is given by $a^{-1}\mathbb{Z}$.

A fractional ideal is *principal* if it's generated by a single element in $F^\times$. Principal fractional ideals form a subgroup $\mathcal{P}_F \subset \mathcal{I}_F$ and the *ideal class group* of F is the quotient

$$\mathcal{C}_F = \mathcal{I}_F/\mathcal{P}_F.$$

One of the first non-trivial theorems in algebraic number theory states that $\mathcal{C}_F$ is a fintie group for any number field F. The *class number* h_F of F is the order of $\mathcal{C}_F$. Essentially by definition $h_F = 1$ if and only if $\mathcal{O}_F$ is a PID.
Given an extension K/F of number fields and an ideal $\mathfrak{p} \subset \mathcal{O}_F$ we may consider the unique factorization of $\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K$:

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Here $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$ and $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ is the *ramification index* of $\mathfrak{P}_i/\mathfrak{p}$.
Since all non-zero prime ideals are maximal we have for any i inclusions of finite fields

$$\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) \subset \mathcal{O}_F/\mathfrak{p} \subset \mathcal{O}_K/\mathfrak{P}_i.$$

The fields $\mathcal{O}_F/\mathfrak{p}$ and $\mathcal{O}_K/\mathfrak{P}_i$ are usually called *residue fields* and the degree

$$f(\mathfrak{P}_i/\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_F/\mathfrak{p}],$$

of their extension is the *residue field degree*. We have the formula

$$\sum_{i=1}^{g} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [K : F].$$

If K/F is Galois, then the Galois group acts transitively on the $\mathfrak{P}_i$ and hence $e_1 = e_2 = \cdots = e_g = e$, $f_1 = f_2 = \cdots = f_g = f$ and the above formula becomes $efg = [K : F]$.

Definition 1.3. Let K/F be an extension of number fields. Then a prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is:

1. *unramified* in K/F if $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ for all i.
2. *ramified* in K/F if $e(\mathfrak{P}_i/\mathfrak{p}) > 1$ for some i.
3. *totally ramified* in K/F if $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$ and $e = [K : F]$.
4. *inert* in K/F if $\mathfrak{p}\mathcal{O}_K$ is prime.
5. *completely split* in K/F if $g = [K : F]$.

1.2 Discriminants

Let K/F be an extension of degree n and $v_1, \dots, v_n$ an F-basis of K. The *discriminant* of the basis is

$$d(v_1, \dots, v_n) = \det\left(\mathrm{Tr}_{K/F}(v_i v_j)\right) = \det(\sigma_i(v_j))^2,$$

where $\sigma_1, \dots, \sigma_n$ denote the n different embeddings $K \hookrightarrow \overline{F} = \overline{\mathbb{Q}}$. If $K = F(\alpha)$, then $1, \alpha, \dots, \alpha^{n-1}$ form an F-basis of K and in this case

$$d(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

In general the discriminant will depend on the chosen basis, but we may consider the ideal generated by all possible discriminants. More generally let $M \subset K$ be an $\mathcal{O}_F$-submodule containing an F-basis of K. We define $d(M)$ to be the $\mathcal{O}_F$ module generated by

$$\{d(v_1, \dots, v_n) \mid v_1, \dots, v_n \in M \text{ is an F-basis of } K\}.$$

If M is fractional so is $d(M)$ and if M is free, say $M = \oplus_{i=1}^n \mathcal{O}_F v_i$, then $d(M)$ is the principal ideal generated by $d(v_1, \dots, v_n)$. The most important case is $M = \mathcal{O}_K$, in which case $d_{K/F} = d(\mathcal{O}_K)$ is the *(relative) discriminant (ideal)*. The *(absolute) discriminant (ideal)* of a number field F is $d_F = d_{F/\mathbb{Q}}$. An important fact about discriminants states that a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is ramified in K/F if and only if $\mathfrak{p} | d_{K/F}$. In particular the set of ramified primes in K/F is finite.

1.3 Exercises week 1

1. Let G be a finite group of automorphisms of a ring A and let

   $$A^G = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in G\},$$

   be the ring of invariants.

   (a) Show that A is integral over A^G.

   (b) Let $\mathfrak{p} \subset A^G$ be a prime ideal and P the set of prime ideals $\mathfrak{q} \subset A$ such that $\mathfrak{q} \cap A^G = \mathfrak{p}$. Show that G acts transitively on P.
   Hint: See exercises 5.12 and 5.13 in Atiyah-Macdonald's Introduction to commutative algebra.

2. Show that the ideal $J = (2, 1 + \sqrt{-5})$ is not principal in $\mathbb{Z}[\sqrt{-5}]$. In particular the ideal class group of $\mathbb{Q}[\sqrt{-5}]$ is non-trivial.

3. Give examples of extensions of number fields K/F and prime ideals $\mathfrak{p} \subset \mathcal{O}_F$ that are unramified, ramified, inert and completely split in K/F.

4. Show that the cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$ factors into distinct linear factors modulo a prime p if any only if $p \equiv 1 \pmod{n}$.

   Hint: $\mathbb{F}_p^\times$ contains a cyclic group of order n if and only if $p \equiv 1 \pmod{n}$.

2 Discriminant, Norm and Decomposition group

Recall: Let K/F be a finite extension of number fields. A prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is decomposed in a unique way: $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where the e_i's are called the *ramification indices* and the $\mathfrak{P}_i$'s are prime ideals which live "over" the prime ideal $\mathfrak{p}$ in the ring $\mathcal{O}_K$.

Definition 2.1. Let K/F be a finite extension of number fields and $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal, the *residue field* of $\mathfrak{p}$ is defined as $\mathbb{F}_\mathfrak{p} := \mathcal{O}_F/\mathfrak{p}$. Moreover, $f_i = f(\mathfrak{P}_i/\mathfrak{p}) = [\mathbb{F}_{\mathfrak{P}_i} : \mathbb{F}_\mathfrak{p}]$ is the *residue field degree*.

To be a little less abstract, we can now consider the following diagram describing inclusions of fields:

$$\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} \qquad \subset \qquad \mathcal{O}_F/\mathfrak{p} \qquad \subset \qquad \mathcal{O}_K/\mathfrak{P}_i$$

In other words, we are looking at every prime ideal of the ring $\mathcal{O}_F$ and count how many prime ideals from the ring $\mathcal{O}_K$ are part of the decomposition of $\mathfrak{p}\mathcal{O}_K$.

Lemma 2.2. $\sum_{i=1}^{g} e_i \cdot f_i = [K : F]$

Remark 2.3. If the extension K/F is Galois, then $\mathrm{Gal}(K/F)$ acts transitively on the prime ideals $\mathfrak{P}_i$ (exercise 1(b) from exercise sheet 1). Hence, $e_1 = e_2 = \cdots = e_g = e$ and $f_1 = f_2 = \cdots = f_g = f$.
In general, we have that the degree of K/F is

$$\sum_{i=1}^{g} e_i \cdot f_i = [K : F]$$

and since K/F is Galois, we conclude that

$$[K : F] = \sum_{i=1}^{g} e \cdot f = e \cdot f \cdot g$$

Definition 2.4. Let K/F an extension of number fields, then a prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is

- *unramified* if $e_i = 1$, for all i.
- *ramified* if $e_i > 1$ for some i.
- *totally ramified* if $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$ and $e = [K : F]$, i.e $f = 1$. This means that nothing happens on the residue field.
- *inert* if $\mathfrak{p}\mathcal{O}_K$ is prime, i.e doesn't split.
- *completely split* if $g = [K : F]$.

2.1 Discriminant

Let K/F be an extension of degree n, let $v_1, ..., v_n$ a F-basis of K.

Definition 2.5. The *discriminant* of the basis $v_1, ..., v_n$ is

$$d(v_1, ..., v_n) = \det(\mathrm{Tr}_{K/F}(v_i \cdot v_j)) = \det(\sigma_i(v_j))^2 \in F,$$

where Tr is the trace map of the extension K/F and $\sigma_1, ..., \sigma_n$ are the n different embeddings of K $\to F$.

If $K = F(\alpha)$ is a degree n extension, then $1, \alpha, ..., \alpha^{n-1}$ form a basis. Then the "classical" definition of the discriminant is

$$d(1, \alpha, \alpha^2, ..., \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

Note that, here, the discriminant depends on the choice of the basis, but can we generalize by not having to define a basis each time ? The answer is the following generalization over modules:

Definition 2.6. Let K/F be an extension, let $\mathcal{O}_F$ be the integral closure of $\mathbb{Z}$ inside F, let M be a $\mathcal{O}_F$-submodule of K containing an F-basis of K. We define the *discriminant* $d(M)$ to be the $\mathcal{O}_F$-module generated by the set of all possible discriminants

$$\{d(v_1, ..., v_n) : v_1, ..., v_n \in M \text{ is an } F\text{-basis of } K\}$$

Remark 2.7. If M is a fractional ideal, i.e a non zero, finitely generated $\mathcal{O}_F$-submodule of F, so is $d(M)$.

Example 2.8.

If M is *free*, i.e if $M = \oplus_{i=1}^{n} \mathcal{O}_F \cdot v_i$, $v_i \in K$. Then, $d(M) = d(v_1, ..., v_n) \cdot \mathcal{O}_F$.

If $M = \mathcal{O}_K$, we write $d_{K/F} = d(\mathcal{O}_K)$. It is called the *relative discriminant of K/F.*

The *(absolute) discriminant* of a number field F is $d_F = d_{F/\mathbb{Q}}$.

Then, we have the following important theorem.

Theorem 2.9. *A prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is ramified in $K/F \iff \mathfrak{p} \mid d_{K/F}$*

In particular, this implies that the set of ramified primes in $(K|F)$ is finite.

2.2 Norm

Recall: for any finite extension K/F, there is a *norm map* $N_{K/F} : K \to F$ such that $x \mapsto \det(f)$, where $f : K \to K$ is defined as $f(y) = x \cdot y$. But can we generalize this definition to ideals ?

Definition 2.10. Let K/F be an extension of number fields, $\mathfrak{P} \subset \mathcal{O}_K$ a prime ideal and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$, then the *norm of* $\mathfrak{P}$ is $N_{K/F}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$. More generally, if $U \subset K$ is a fractional ideal, i.e $U = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_l^{a_l}$, $a_i \in \mathbb{Z}$, then $N_{K/F}(U) = \prod_{i=1}^{l} N_{K/F}(\mathfrak{P}_i)^{a_i} \subset F$.

Proposition 2.11. *Here are some properties of the norm of $\mathfrak{P}$:*

- *If K/F is Galois, then $N_{K/F}(U) = \prod_{\sigma \in Gal(K/F)} \sigma(U) \cap F$*
- *If $\alpha \in K$, $N_{K/F}(\alpha \mathcal{O}_K) = N_{K/F}(\alpha)\mathcal{O}_F$. More generally, $N_{K/F}(U) =$ fractional ideal generated by $\{N_{K/F}(\alpha) : \alpha \in U\}$.*
- *If $F \subset E \subset K$, then $N_{K/F} = N_{E/F} \circ N_{K/E}$.*
- *If $F = \mathbb{Q}$, then $N_{K/\mathbb{Q}}(U) = a\mathbb{Z}$, for some $a \in \mathbb{Q}$.*

One will, for now on, use the following notations: $NU = N_{K/\mathbb{Q}}(U)$ and $NU = |a|$, with a as above. In this case, if $\mathfrak{P} \subset \mathcal{O}_K$ is a prime ideal, then $N\mathfrak{P} = (\mathfrak{P} \cap \mathbb{Z})^{f(\mathfrak{P}/\mathfrak{P} \cap \mathbb{Z})} = (|\mathcal{O}_K/\mathfrak{P}|) = |\mathbb{F}_{\mathfrak{P}}| \subset \mathbb{Z}$.

2.3 Decomposition groups

Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$, let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal and $\mathfrak{P} \subset \mathcal{O}_K$ with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$.

Definition 2.12. The *decomposition group of* $(\mathfrak{p}, \mathfrak{P})$ is $Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\} \subset G$

In other words, the decomposition group of a prime ideal $\mathfrak{P}$ is the subgroup of G that consists of all automorphisms that "fix" the prime $\mathfrak{P}$. But beware of the fact that it's the prime ideal that is invariant and not the elements in it.
By definition, $Z(\mathfrak{P}/\mathfrak{p})$ acts on the finite field $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ and fixes $\mathbb{F}_{\mathfrak{p}}$. Moreover, with the decomposition $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, the stabilizer of a prime ideal $\mathfrak{P}_i$ under the action of the Galois group $\mathrm{Gal}(K/F)$ on the set $\{\mathfrak{P}_1, ..., \mathfrak{P}_g\}$ is given by $\mathrm{Stab}(\mathfrak{P}_i) = \{\sigma \in \mathrm{Gal}(K/F) | \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} =: \mathrm{Z}(\mathfrak{P}_i/\mathfrak{p})$, the decomposition group.
Thus, we have the following homomorphism:

$$Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}). \tag{1}$$

Theorem 2.13.

- *The degree* $[G : Z(\mathfrak{P}/\mathfrak{p})] = |\{\mathfrak{P} \subset \mathcal{O}_K \text{ prime } : \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K\}|$, *since* G *acts transitively on* $\mathfrak{P}$. *Moreover, if* $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}\mathcal{O}_K$, *then the two decomposition groups* $Z(\mathfrak{P}/\mathfrak{p})$ *and* $Z(\mathfrak{P}'/\mathfrak{p})$ *are* G*-conjugate.*
- *The homomorphism* (1) *is surjective, its kernel* $T(\mathfrak{P}/\mathfrak{p})$ *is called the* ***inertia subgroup****. In particular,* $[Z(\mathfrak{P}/\mathfrak{p}) : T(Z(\mathfrak{P}/\mathfrak{p})] = f$ *and* $|T(\mathfrak{P}/\mathfrak{p})| = e$, *i.e is exactly the ramification.*

Remark 2.14. If K/F is an abelian extension (G is abelian), then by the first part of the previous theorem, $Z(\mathfrak{P}/\mathfrak{p}) = Z(\mathfrak{p})$ depends only on $\mathfrak{p}$!

Now consider the following fields extensions:

$$\begin{array}{lll} K & & \\ | & & \\ K^{T(\mathfrak{P}/\mathfrak{p})} & = K_T & \text{(inertia field)} \\ | & & \\ K^{Z(\mathfrak{P}/\mathfrak{p})} & = K_Z & \text{(decomposition field)} \\ | & & \\ F & = K^G & \end{array}$$

Note that $F = K^G$ because the group G is Galois.

Theorem 2.15. *(Layer Theorem) Let* K/F *be an abelian extension, let* $\mathfrak{p} \subset \mathcal{O}_F$ *a prime ideal, then*

- $\mathfrak{p}$ *splits completely in* K_Z/F *(the "first layer" in our diagram above).*
- *The primes above* $\mathfrak{p}$ *remain inert in* K_T/K_Z *and ramify totally in* K/K_T.

2.4 Artin automorphism

This new section is motivated by the quadratic reciprocity.

Definition 2.16. Let K/F be Galois and an unramified prime ideal $\mathfrak{p} \subset \mathcal{O}_F$, by the previous theorem, there exists an isomorphism

$$Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

Thus, if we take a look at the codomain, we see that the Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is generated by one element: $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) =< \varphi_{\mathfrak{p}} >$, where $\varphi_{\mathfrak{p}}(x) = x^{|\mathbb{F}_{\mathfrak{p}}|}, \forall x \in \mathbb{F}_{\mathfrak{P}}$ is the *Frobenius*.
We call the correspondent element of the Frobenius in $Z(\mathfrak{P}/\mathfrak{p})$ the *Frobenius element at* $\mathfrak{P}$ and denote it by $\left(\frac{\mathfrak{P}}{K/F}\right) = (\mathfrak{P}, K/F) \in Z(\mathfrak{P}/\mathfrak{p}) \subset G$.
Furthermore, if the extension K/F is abelian, then the Frobenius element $\left(\frac{\mathfrak{P}}{K/F}\right)$ only depends on $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$. In this case, it is the *Artin automorphism at* $\mathfrak{p}$, denoted $\left(\frac{\mathfrak{p}}{K/F}\right)$. It defines a map

$$\{ \text{ primes of } \mathcal{O}_F \text{ unramified in } K/F\} \to \mathrm{Gal}(K/F)$$

$$\mathfrak{p} \mapsto \left(\frac{\mathfrak{p}}{K/F}\right)$$

Let's look at some examples:

Example 2.17.

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_m)$ a cyclotonic extension, without loss of generality m is either odd or $4 \mid m$, because if $m = 2k$, with k odd then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_k)$.

Then, in the Exercise sheet week 2, exercise 2(a), we prove that $p\mathbb{Z}$ ramifies in $K \iff p \mid m$

If $p \nmid m$, we have $\sigma \in \left(\frac{p\mathbb{Z}}{K/F}\right) \in \mathrm{Gal}(K/F) = (\mathbb{Z}/m\mathbb{Z})^\times$ is exactly $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Example 2.18.

Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$, square-free, then $\mathrm{Gal}(K/F) = \{\pm 1\}$ and

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{if } d \not\equiv 1 \mod 4 \end{cases}$$

If $p \nmid d_K$ unramified and odd, then $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \left(\frac{d_K}{p}\right) \in \{\pm 1\}$, the Legendre symbol of the discriminant d_K (Exercise sheet 2, exercise 4(b)).

Note that writing $\mathrm{Gal}(K/F) = \{\pm 1\}$ means that the elements -1 and 1 are the non-trivial and trivial automorphisms respectively and not integers.

2.5 Exercises week 2

1. Let K/F be a Galois extension of number fields with Galois group G and $\mathfrak{p} \subset \mathcal{O}_F$ a non-zero prime unramified in K/F.

   (a) Let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime dividing $\mathfrak{p}\mathcal{O}_K$. Show that the Frobenius element $\left(\frac{\mathfrak{P}}{K/F}\right)$ at $\mathfrak{P}$ is the unique element $\sigma \in \mathrm{Gal}(K/F)$ with the property $\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \ (mod\ \mathfrak{P})$ for every $\alpha \in \mathcal{O}_K$.

   (b) Assume now that K/F is abelian and let $F \subset L \subset K$ be an intermediate field. Show that

   $$\left(\frac{\mathfrak{p}}{L/F}\right) = \left(\frac{\mathfrak{p}}{K/F}\right)_{|L}.$$

2. Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field and assume without loss of generality that m is odd or divisible by 4.

   (a) Show that $p\mathbb{Z}$ ramifies in K if and only if $p|m$.
   Hint: Consider the action of the inertia group on ζ_m.

   (b) Let $p \in \mathbb{Z}$ be a prime not dividing m and $\mathfrak{P} \subset \mathcal{O}_K$ a prime over $p\mathbb{Z}$. Show that if ζ, ζ' are m-th roots of unity in K such that $\zeta \equiv \zeta' \ (mod\ \mathfrak{P})$ then $\zeta = \zeta'$.
   Hint: Differentiate the polynomial $X^m - 1$.

   (c) Using 1(a), deduce that for any prime p not dividing m, the Artin automorphism $\left(\frac{p\mathbb{Z}}{K/F}\right) \in G \cong (\mathbb{Z}/m\mathbb{Z})^\times$ is given by $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$.

3. For an odd prime p, show that the absolute discriminant of $\mathbb{Q}(\zeta_p)$ is given by $(-1)^{\frac{p-1}{2}} p^{p-2}$.

4. Let d be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$ a quadratic extension of $\mathbb{Q}$.

   (a) Show that the absolute discriminant d_K of K is equal to d if $d \equiv 1 \ mod\ 4$ and equal to $4d$ if $d \equiv 2, 3 \ mod\ 4$.
   Hint: You may use without proof that

   $$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \ mod\ 4 \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \ mod\ 4 \end{cases}$$

   (b) For $p \in \mathbb{Z}$ an odd unramified prime, show that

   $$\left(\frac{p\mathbb{Z}}{K/F}\right) = \left(\frac{d_k}{p}\right),$$

   where $\left(\frac{d_k}{p}\right)$ is the Legendre symbol and we identify $\mathrm{Gal}(K/\mathbb{Q})$ with $\{\pm 1\}$.

   Hint: Use Theorem 1.1 from Childress Book

3 Completion and Ramification theory

3.1 Embeddings and units of number fields

Definition 3.1. Let F be a number field. An *embedding* is an injective homomorphism $F \hookrightarrow \mathbb{C}$.

Let F be a number field. By the primitive element theorem, it can be written as $F = \mathbb{Q}(\alpha)$ for some $\alpha \in F$. Consider the minimal polynomial m_α of α with roots $\alpha = \alpha_1, ..., \alpha_d$ in $\mathbb{C}$ (with $d = [F : \mathbb{Q}]$). Since any field homomorphism φ verifies

$$m_\alpha(\varphi(\alpha)) = \varphi(m_\alpha(\alpha)) = \varphi(0) = 0,$$

the image $\varphi(\alpha)$ must be a conjugate of α.
So an embedding of F in $\mathbb{C}$ is entirely determined by the choice of the image $\varphi(\alpha)$ among the roots of m_α, and there are exactly d distincts embedding.

Now let r be the number of real embeddings and s be the number of pair of complex conjugate embeddings. We have that

$$[F : Q] = r + 2s$$

Remark 3.2. If F is a Galois extension of $\mathbb{Q}$, then we have $r = 0$ or $s = 0$ (since the Galois group cannot swap a real root and a pair of complex conjugate roots).

Theorem 3.3 (Dirichlet's unit theorem)**.** *Let F be a number field and r, s as above. We can find units $\varepsilon_1, ..., \varepsilon_{r+s-1} \in \mathcal{O}_F^\times$ such that*

$$\begin{aligned}\mathcal{O}_F^\times &\cong \mathcal{W}_F \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_{r+s-1} \rangle \\ &\cong \mathcal{W}_F \times \mathbb{Z}^{r+s-1}\end{aligned}$$

where $\mathcal{W}_F$ is the group of roots of unity in F. The ε_k are called a fundamental system of units *for F.*

Example 3.4. Let $F = Q[\sqrt{3}]$. We have two real embeddings, sending $\sqrt{3}$ to $\sqrt{3}, -\sqrt{3}$ respectively. So $r + s - 1 = 1$.
First, let us check that $2 + \sqrt{3}$ is an integer. Its minimal polynomial is

$$x^2 - 4x + 1 = (x - (2 + \sqrt{3}))(x - (2 - \sqrt{3}))$$

which is a monic polynomial with coefficients in $\mathbb{Z}$. Note that $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$, so $2 + \sqrt{3} \in \mathcal{O}_F^\times$. Since F is a subfield of $\mathbb{R}$, the group of roots of unity $\mathcal{W}_F$ is $\{\pm 1\}$. So by the Dirichlet unit theorem

$$\mathcal{O}_F^\times = \{\pm 1\} \times \langle 2 + \sqrt{3} \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

3.2 Completion of number fields

3.2.1 p-adic numbers

First let us recall a few definitions.

Definition 3.5. A *distance* on a field F is a function $d : F \times F \to [0, \infty]$ such that

- $d(x, y) = d(y, x) \quad \forall\, x, y \in F$,
- $d(x, y) = 0$ if and only if $x = y$,
- $d(x, z) \leq d(x, y) + d(y, z) \quad \forall\, x, y, z \in F$ (the so-called *triangle inequality*).

Definition 3.6. A *norm* (also called an *absolute value*) on a field F is a function $|\cdot| : F \to [0, \infty]$ such that

- $|x| = 0$ if and only if $x = 0$,
- $|xy| = |x||y| \quad \forall\, x, y \in F$,
- $|x + y| \leq |x| + |y| \quad \forall\, x, y \in F$ (triangle inequality).

We say that a norm is *non-archimedean* when $|x+y| \leq \max\{|x|,|y|\}$ for all $x, y \in F$. The non-archimedean inequality implies the triangle inequality, so it is a stronger property.

A norm $||\cdot||$ induces a distance $d_{||\cdot||}(x,y) := ||x-y||$.

Definition 3.7 (p-adic valuation)**.** Let $p \in \mathbb{Z}$ be a prime and $a \in \mathbb{Z} \setminus \{0\}$. We define $\mathrm{ord}_p(a)$ to be the greatest integer n so that a can be written as

$$a = p^n b$$

with $b \in \mathbb{Z}$ not divisible by p.

We have that $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$, like a logarithm.

Definition 3.8 (p-adic valuation for rationals)**.** Let $p \in \mathbb{Z}$ be a prime and $x = \frac{a}{b} \in \mathbb{Q}^\times$. We define

$$\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$$

Definition 3.9 (p-adic norm)**.** The p-adic valuation can be used to define a norm as follows :

$$|\cdot|_p : x \mapsto \begin{cases} 0 & \text{if } x = 0 \\ p^{-\mathrm{ord}_p(x)} & \text{otherwise} \end{cases}.$$

Example 3.10.

$$108 = 2^2 3^3$$

$$\mathrm{ord}_2(108) = 2 \quad \mathrm{ord}_3(108) = 3 \quad \mathrm{ord}_5(108) = 0$$

$$|108|_2 = 1/4 \quad |108|_3 = 1/21 \quad |108|_5 = 1$$

Proposition 3.11. *For all primes p, $|\cdot|_p$ is a non-archimedean norm.*

Proof : The first two conditions are easy to verify directly form the definition. We show that the non-archimedean inequality holds.
Let $x = \frac{a}{b}, y = \frac{c}{d} \in \mathbb{Q}$. We have $x + y = \frac{ad+bc}{bd}$. Without loss of generality, we may assume that $x, y, x+y \neq 0$.

$$\mathrm{ord}_p(x+y) = \mathrm{ord}_p(ad-bc) - \mathrm{ord}_p(bd)$$

$$\geq \min\{\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)\} - \mathrm{ord}_p(b) - \mathrm{ord}_p(d)$$

$$= \min\{\mathrm{ord}_p(ad) - \mathrm{ord}_p(d) - ord_p(b), \mathrm{ord}_p(bc) - \mathrm{ord}_p(b) - \mathrm{ord}_p(d)\}$$

$$= \min\{\mathrm{ord}_p(a) - \mathrm{ord}_p(d), \mathrm{ord}_p(c) - \mathrm{ord}_p(b)\} = \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$$

$$\implies |x+y|_p \leq \max\{|x|_p, |y|_p\} \quad \square$$

Recall that two distances are equivalent if they have the same Cauchy sequences, and that two norms are equivalent if they induce equivalent distances.

Theorem 3.12 (Ostrowski)**.** *Every non-trivial norm of $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p or for $p = \infty$.*

Let (a_n) and (b_n) be Cauchy sequences in $(\mathbb{Q}, |\cdot|)$. We say that that they have the same limit if the Cauchy sequence $(a_n - b_n)$ has limit 0.

Definition 3.13 (p-adic completion field)**.** The *field of p-adic numbers* $\mathbb{Q}_p$ is the *completion* of $\mathbb{Q}$ for the p-adic norm, meaning that it consists of all possible limits of Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$. We construct it as follows :

$$\mathbb{Q}_p := \{\text{Cauchy sequences in } (\mathbb{Q}, |\cdot|_p)\}/_\sim$$

where $(a_n) \sim (b_n)$ if they have the same limit.

We can extend the p-adic norm to $\mathbb{Q}_p$ by letting it commute with the limit :

$$|x|_p = |\lim_i x_i|_p := \lim_i |x_i|_p.$$

Remark 3.14. We can take the completion for any norm on $\mathbb{Q}$ in a similar fashion. The completion of the standard norm $|\cdot|$ on $\mathbb{Q}$ is $\mathbb{R}$. Note that, while $|\cdot|$ on $\mathbb{Q}$ takes values in $\mathbb{Q}$, the extended norm $|\cdot|$ on $\mathbb{R}$ takes values in $\mathbb{R}$. In the case of a p-adic norm however, the extended norm $|\cdot|_p$ still takes values in $\mathbb{Q}$. Indeed, it only takes countably many values $\{p^{-n} \mid n \in \mathbb{N}\} \cup \{0\}$, so the only accumulation point is 0.

Remark 3.15. Directly from the definition, $\mathbb{Q}_p$ is complete for the p-adic norm. $\mathbb{Q}_p$ is a field extension of $\mathbb{Q}$, but not a finite extension. In fact, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ (as any number in $\mathbb{Q}_p$ can be approached by a sequence in $\mathbb{Q}$) but we do not prove it.

Definition 3.16 (p-adic integer)**.** The *ring of p-adic integers* is

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Theorem 3.17.

$$\mathbb{Z}_p \approxeq \varprojlim_{p\to\infty} \mathbb{Z}/p^n\mathbb{Z}$$

which means that for $x \in \mathbb{Z}_p$, we can find a unique sequence of integers $(x_i)_{i\in\mathbb{N}}$ such that for all i

$$0 \leq x_i \leq p^i \ ; \qquad x_i \equiv x_{i+1} \pmod{p^i}.$$

Let we write x_i, x_{i+1} in base p :

$$x_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1}p^{i-1}$$

$$x_{i+1} = c_0 + c_1 p + c_2 p^2 + \cdots + c_i p^i$$

(with the digits $0 \leq b_j, c_k \leq p-1$)
The second condition given by Theorem 2.13 implies that for all $j \leq i-1$, $b_j = c_j$, so we can think of x as an infinite p-adic expansion

$$x = \sum_{j=0}^{\infty} b_j \ (p^j)$$

We also have a p-adic expansion for all elements of $\mathbb{Q}_p$, since for all $y \in \mathbb{Q}_p$, there exists some n such that $p^n y$ is a p-adic integer. So we can write the expansion of $p^n y$ and "shifts the digits" n places to the left.

Example 3.18. The p-adic expansion of 1 is

$$1 = 1 + 0 \ (p) + 0 \ (p^2) + \cdots$$

The p-adic expansion of -1 is

$$-1 = p-1 + p-1 \ (p) + p-1 \ (p^2) + \cdots$$

We can verify that

$$1 + \sum_{j=0}^{\infty} (p-1)p^j = 0$$

Example 3.19. Let us find the 5-adic expansion of $\frac{1}{3}$.
We write

$$\frac{1}{3} = a_0 + a_1 \ (5) + a_2 \ (25) + \cdots$$

which translates into the set of conditions :

- $3a_0 \equiv 1 \pmod 5 \implies a_0 = 2$
- $3(2 + 5a_1) \equiv 1 \pmod{25} \implies 15a_1 \equiv 20 \pmod{25}$
  $\implies 3a_1 \equiv 4 \pmod 5 \implies a_1 = 3$
- similarly for $a_2 = 3, a_3 = 1$, etc.

Eventually we find a sequence of digits that repeat. We can guess a pattern, in this case

$$\frac{1}{3} = 2313131313\cdots = 2\overline{31}$$

and then check through direct computation that indeed $3 \times 2\overline{31} = 1$.

3.3 Completion of a general number field

Let F be any number field. We will define a (non-archimedean) norm on F using a prime ideal of $\mathcal{O}_F$, and then use the completion with respect to this norm. This construction preserves some algebraic properties of the number field, and we allow us to study it "locally" in some sense.

Let $\mathfrak{p}$ be an ideal in $\mathcal{O}_F$.

Definition 3.20 ($\mathfrak{p}$-adic valuation, $\mathfrak{p}$-adic norm)**.** Let $x \in F^\times$. We have a prime ideal decomposition

$$x\mathcal{O}_F = \mathfrak{p}^n \mathfrak{p}_1^{n_1} ... \mathfrak{p}_t^{n_t}$$

where the $\mathfrak{p}_i$ are distinct from $\mathfrak{p}$. We set $\mathrm{ord}_\mathfrak{p}(x) := n$ (the highest power of $\mathfrak{p}$ appearing in the decomposition). The $\mathfrak{p}$-*adic norm* on F is

$$|\cdot|_\mathfrak{p} : x \mapsto \begin{cases} 0 & \text{if } x = 0 \\ c^{\mathrm{ord}_\mathfrak{p}(x)} & \text{otherwise} \end{cases}.$$

for some real number $0 < c < 1$. Different choices of c yield equivalent norms.

Remark 3.21. In (2.1) we had the particular case

$$\mathcal{O}_F = \mathbb{Z}, \quad \mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}, \quad c = \frac{1}{p}.$$

We leave the proof that this is a non-archimedean norm as an exercise.
In the archimedean case, Let $\sigma : F \to \mathbb{C}$ be an embedding. Then the pullback norm of the usual norm on $\mathbb{C}$

$$|x|_\sigma = |\sigma(x)|_C$$

is an archimedean norm on F.

Remark 3.22. If $\sigma_1, ..., \sigma_r$ are the real embeddings of F and $\sigma_{r+1}, ..., \sigma_{r+s}$ representants of conjugate pairs of complex embeddings, then :

- the $|\cdot|_{\sigma_i}$ are pairwise inequivalent
- $|\cdot|_\sigma$ and $|\cdot|_{\bar{\sigma}}$ are equivalent

Furthermore, for $\mathfrak{p} \neq \mathfrak{q}$, the norms $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ are inequivalent (see exercise sheet).

Example 3.23. Let $F = \mathbb{Q}[x]/(x^2 - 3)$. Let $\rho, -\rho$ be the roots of 3 in F. We have two non-equivalent absolute values on F:

$$\begin{cases} |a + b\rho|_1 = |a + b\sqrt{3}|_\mathbb{R} & (\sigma_1 : \rho \mapsto \sqrt{3} \in \mathbb{R}) \\ |a + b\rho|_2 = |a - b\sqrt{3}|_\mathbb{R} & (\sigma_2 : \rho \mapsto -\sqrt{3} \in \mathbb{R}) \end{cases}$$

Theorem 3.24 (Ostrowski)**.** *Every non-trivial norm on F is either equivalent to a $\mathfrak{p}$-adic norm for some $\mathfrak{p}$ (if non-archimedean) or to the pullback norm of some embedding $F \to \mathbb{C}$ (if archimedean).*

As before, two Cauchy sequences has the same limit if their difference has limit 0.

Definition 3.25. The completion of F with respect to a norm $||\cdot||$ is the field

$$\{\text{Cauchy sequences in } (F, ||\cdot||)\}/\sim$$

where $(a_n) \sim (b_n)$ if they have the same limit.

The norm $||\cdot||$ extends to the completion by commuting with the limit :

$$||\lim_i x_i|| = \lim_i ||x_i||.$$

Notation :

- if $||\cdot||$ is the $\mathfrak{p}$-adic norm $|\cdot|_\mathfrak{p}$, we will denote the completion $F_\mathfrak{p}$.

- if $||\cdot||$ is an archimedean norm given by an embedding, then the completion will be isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ (via an isometry for the induced distance).

Definition 3.26 ($\mathfrak{p}$-adic ring of integers)**.** The *ring of* $\mathfrak{p}$*-adic integers* $\mathcal{O}_\mathfrak{p}$ is

$$\{x \in F_\mathfrak{p} \mid |x|_\mathfrak{p} \leq 1\}$$

$\mathcal{O}_\mathfrak{p}$ is a local ring. Its group of units is

$$\mathcal{O}_\mathfrak{p}^\times = \{x \in F_\mathfrak{p} \mid |x|_\mathfrak{p} = 1\}$$

and

$$\mathfrak{m}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \setminus \mathcal{O}_\mathfrak{p}^\times$$

is the unique maximal ideal (we have that $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$).

Remark 3.27. We can define the residue field of $F_\mathfrak{p}$ as $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$. The residue field of $F_\mathfrak{p}$ is isomorphic to the residue field of F, so it is often denoted by $\mathbb{F}_\mathfrak{p}$:

$$\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}_F/\mathfrak{p} =: \mathbb{F}_\mathfrak{p},$$

so it is finite and $F_\mathfrak{p}$ is local (complete with finite residue field). In fact, $\mathcal{O}_\mathfrak{p} \cap F$ is exactly the localization of $\mathcal{O}_F$ at the ideal $\mathfrak{p}$.

Proposition 3.28 ($\mathfrak{p}$-adic expansion)**.** *Let* $\mathcal{C} = \{c_0 = 0, c_1, \cdots, c_q\}$ *be a set of representatives of* $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ *and let* $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$*. We call* π *a uniformizer of* $F_\mathfrak{p}$*.*

- $\forall\ x \in \mathcal{O}_\mathfrak{p}$*, we have*
$$x = \sum_{j=0}^{\infty} a_j \pi^j, \quad (a_j \in \mathcal{C} \ \ \forall\ j).$$
- $\forall\ x \in F_\mathfrak{p}$ *we have*
$$x = \sum_{j=-ord_\mathfrak{p}(x)}^{\infty} a_j \pi^j \quad (a_j \in \mathcal{C} \ \ \forall\ j).$$
- $\mathfrak{m}_\mathfrak{p} = \langle \pi \rangle$.

(Idea of a proof : Let $x \in \mathcal{O}_\mathfrak{p}$, take a_0 a rep of the class $x + \mathfrak{m}_\mathfrak{p}$, then set $x_1 = \frac{x - a_0}{\pi} \in \mathcal{O}_\mathfrak{p}$. Iterate the process.)

Theorem 3.29 (Hensel's lemma)**.** *Let* f *be a monic polynomial in* $O_\mathfrak{p}[x]$ *and*$\bar{f}$ *be its class in the residue field* $\mathbb{F}_\mathfrak{p}[x] = \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}[x]$.
If $\bar{g}(x)$ *and* $\bar{h}(x)$ *are monic and coprime in the residue field such that* $\bar{f} = \bar{g}\bar{h}$ *then there exists a lifting of* $\bar{g}$ *and* $\bar{h}$ *to polynomials* $g, h \in \mathcal{O}_\mathfrak{p}[x]$ *such that* $f = gh$ *that preserves their degree (i.e.* $\deg(g) = \deg(\bar{g}), \deg(h) = \deg(\bar{h})$*).*

For a proof, see Theorem 4.6 in [3].
In particular, whenever one of the factors $\bar{g}, \bar{h}$ is linear, we can find a root of f in $\mathcal{O}_\mathfrak{p}[x]$.

Example 3.30. Let $f(x) = x^2 - 2 \in \mathbb{Z}_7[x]$. Then in $\mathbb{F}_7[x]$, $\bar{f}$ factors as

$$\bar{f}(x) = (x - 3)(x - 4)$$

So $\exists\ g, h \in \mathbb{Z}_7[x]$ monic linear such that $f(x) = g(x)h(x)$, and therefore 2 has a square root in $\mathbb{Z}_7$.

3.4 Ramification theory

Take K/F an extension of number fields, $\mathfrak{p}$ a prime ideal in $\mathcal{O}_F$ and consider the prime decomposition

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

where the $\mathfrak{P}_j$ are distincts primes in $\mathcal{O}_K$ and the e_j are positive integers.

The norms $|\cdot|_{\mathfrak{P}_i}$ on K are all pairwise inequivalent, but they all restrict to $|\cdot|_{\mathfrak{p}}$ up to equivalence. In fact, the $\mathfrak{P}_i$ represent all the topologically inequivalent ways to extend $|\cdot|_{\mathfrak{p}}$ to K. At the completion level, we have the following finite extension for each $\mathfrak{P}_i$:

$$K_{\mathfrak{P}_i}/F_{\mathfrak{p}}$$

and conversely if $L/F_{\mathfrak{p}}$ is a finite extension, then $L = K_{\mathfrak{P}}$ for some finite extension K/F and some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$. This is a way of saying that any finite extension of $F_{\mathfrak{p}}$ can be obtained from a prime ideal in a finite extension of F.

For $K_{\mathfrak{P}}/F_{\mathfrak{p}}$, let $\mathcal{O}_{\mathfrak{P}}$ be the ring of integer of $K_{\mathfrak{P}}$. It has a unique maxiaml ideal $\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{P}}$. As with number fields, we have a unique factorization

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{P}} = \mathfrak{p}\mathcal{O}_{\mathfrak{P}} = \mathfrak{m}_{\mathfrak{P}}^e$$

where $e = e(\mathfrak{m}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{p}})$ is the *local ramification index*.
We also have the *local residue field degree* :

$$f = f\left(\mathfrak{m}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{p}}\right) = \left[\mathcal{O}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}; \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}\right]$$

Remark 3.31. In this case, there is a single prime in the factorization of $\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{P}}$ because we "killed" all the other primes by localizing.

Definition 3.32. We say that the extension $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is

- ramified if $e > 1$.
- unramified if $e = 1$.
- totally ramified if $f = 1$.

Remark 3.33. Note that

$$f\left(\mathfrak{m}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{p}}\right) = \left[\mathcal{O}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}; \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}\right] = \left[\mathbb{F}_{\mathfrak{P}}; \mathbb{F}_{\mathfrak{p}}\right] = f\left(\mathfrak{P}/\mathfrak{p}\right).$$

Similarly we can check that $e\left(\mathfrak{m}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{p}}\right) = e\left(\mathfrak{P}/\mathfrak{p}\right)$.
So the local ramification index and residue field degree (for the completions $K_{\mathfrak{P}}, F_{\mathfrak{p}}$) are the same as their global counterpart (for K, F).

If K/F is Galois, then the local extension $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is also Galois, but since there is no splitting (because there is only one prime, see remark 3.31), we have that

$$ef = [K_{\mathfrak{P}} : F_{\mathfrak{p}}]$$

(compare this formula with the non-local case seen in Week 2: $efg = [K : F]$).
This means we have a simpler layer decomposition

$$F_{\mathfrak{p}} \xhookrightarrow{f} K_{\mathfrak{P}}^I \xhookrightarrow{e} K_{\mathfrak{P}}$$

where $K_{\mathfrak{P}}^I/F_{\mathfrak{p}}$ is unramified, and $K_{\mathfrak{P}}/K_{\mathfrak{P}}^I$ is totally ramified (see *Normal extensions* in [4]).

3.5 Finite extensions of $\mathbb{Q}_p$

$\mathbb{Q}_p$ is not algebraically closed, and its closure $\mathbb{Q}_p^{alg}$ is not complete. However, the completion of $\mathbb{Q}_p^{alg}$ is both complete and algebraically closed. We will denote it $\mathbb{C}_p$. There is a unique absolute value on $\mathbb{C}_p$ that extends $|\cdot|_p$ and we also denote it $|\cdot|_p$.
Suppose that $\sigma : F \hookrightarrow \mathbb{Q}_p^{alg}$ is an embedding. For $x \in F$, we define :

$$|x|_\sigma = |\sigma(x)|_p$$

so that $|\cdot|_\sigma$ extends $|\cdot|_p$ on F.
Moreover, we have a one-to-one correspondance :

$$\left\{\text{topologically distinct extensions of } |\cdot|_p \text{ to } F\right\}$$

$$\updownarrow$$

$$\left\{\text{conjugacy classes of continuous embeddings } \ \sigma : F \hookrightarrow \mathbb{Q}_p^{alg}\right\}$$

So the only way to extend an absolute value from $\mathbb{Q}_p$ to F is via an embedding.

Sources

- [1] Nancy Childress, *Class Field Theory*
- [2] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-functions*
- [3] Jürgen Neukrich, *Algebraic Number Theory*
- [4] Frédérique Oggier, *Introduction to Algebraic Number Theory*

3.6 Exercises week 3

1. Let $F = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Compute r and s, the numbers of real embeddings and pairs of conplex conjugate embeddings, respectively, and then give an explicit description of the unit group $\mathcal{O}_F^\times$. Do the same for $F' = \mathbb{Q}(\sqrt{3}, \sqrt{7}, i)$.

2. (a) Find the p-adic expansion of $\frac{1}{6} \in \mathbb{Q}_7$.
   (b) For which $p = 2, 3, 5, 7, 11, 13$ does -1 have a square root in $\mathbb{Q}_p$?

3. Let F be a number field. Let $\mathfrak{p} \neq \mathfrak{q}$ be non-zero prime ideals of $\mathcal{O}_F$. Prove that the norms $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ are not equivalent.

4. Let K/F be a number field extension. And let $\mathfrak{P}, \mathfrak{p}$ be primes of K and F resp. such that $\mathfrak{P}$ is above $\mathfrak{p}$. Then consider the extension of local fields $K_\mathfrak{P}/F_\mathfrak{p}$. Show that for $\pi_\mathfrak{p}$ an uniformizer of $F_\mathfrak{p}$, we have:

   $$|\pi_\mathfrak{p}|_\mathfrak{P} = |\pi_\mathfrak{P}|_\mathfrak{P}^e$$

   Where $\pi_\mathfrak{P}$ is an uniformizer of $K_\mathfrak{P}$ and e is the ramification index $e = e(\mathfrak{P}/\mathfrak{p})$. This means that the ramification index of the field extension and their completion coincides.

4 Dirichlet Characters and Galois correspondence

4.1 Introduction to Character

Definition 4.1. A character χ for a finite abelian group, G, is a group homeomorphism

$$\chi : G \to \mathbb{C}^\times.$$

The product of two characters χ_1, χ_2 is defined for any $g \in G$ as

$$\chi_1 \cdot \chi_2(g) = \chi_1(g) \cdot \chi_2(g).$$

We denote $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ and denote the neutral element χ_0, defined by $\chi_0(g) = 1$, for all $g \in G$.

Lemma 4.2. *$G \cong \widehat{G}$.*

Proof. As G is a finite abelian group we have $G = \bigoplus_n \mathbb{Z}/n\mathbb{Z}$, thus
$\hat{G} = \bigoplus_n \widehat{\mathbb{Z}/n\mathbb{Z}}$.
Any $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$ is uniquely determined by $\chi(1)$, thus $\chi \mapsto \chi(1)$ is an injective map from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{C}^\times$. We notice that set of $\chi(1)$'s correspond to the set of n-th roots of unity, which allows us to conclude that $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$, so $G \cong \widehat{G}$. □

Lemma 4.3. *There is a natural isomorphism $G \cong \widehat{\widehat{G}}$.*

Proof. We define the following map, for any $g \in G$:

$$\begin{aligned} \hat{g} \colon \widehat{G} &\to \mathbb{C}^\times \\ \chi &\mapsto \chi(g). \end{aligned}$$

It follows that the map

$$\begin{aligned} G &\to \widehat{\widehat{G}} \\ g &\to \hat{g} \end{aligned}$$

is clearly an homomorphism (it can be proven as an exercise). As $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, we only need to show injectivity, to get that it is an isomorphism.
If $\hat{g}(\chi) = \chi(g) = 1$, for all $\chi \in \widehat{G}$, we look at the subgroup $H = \langle g \rangle$ of G. Then it is immediate to see that elements of $\widehat{G}$ can be viewed as elements of $\widehat{G/H}$, by the first isomorphism theorem. This implies that $|\widehat{G/H}| = |\widehat{G}| = |G|$, thus $|H| = 1$, so the map is indeed injective, as the only elements sent to $id_{\widehat{G}}$, is 1.

□

We can thus naturally identify G with $\widehat{\widehat{G}}$.

Proposition 4.4. *For $H < G$, we define $H^\perp := \{\chi \in \widehat{G} : \chi(h) = 1 \quad \forall h \in H\}$.*

1. *if $H < G$, then $H^\perp \cong \widehat{G/H}$*
2. *if $H < G$, then $\widehat{H} \cong \widehat{G}/H^\perp$*
3. *$(H^\perp)^\perp = H$, under the identification $\widehat{\widehat{G}} \cong G$.*

Proof. 1. For any $\chi \in H^\perp$, we define $\psi \in \widehat{G/H}$ as $\psi(gH) = \chi(g)$, it is clearly well defined and is actually an isomorphism.

2. Clearly $\chi \mapsto \chi|_H$, is a homomorphism from $\widehat{G}$ to $\widehat{H}$, with kernel $H^\perp$. We also notice that $|H^\perp| = |\widehat{G/H}| = |G|/|H|$, so
$|\widehat{H}| = |H| = |G|/|H^\perp| = |\widehat{G}|/|H^\perp| = |\widehat{G}/H^\perp|$, which allows us to conclude.

3. First we notice that $(H^\perp)^\perp = \{\hat{g} \in \widehat{\widehat{G}} | \hat{g}(\chi) = 1, \quad \forall \chi \in H^\perp\}$. We get for all $h \in H$, $\hat{h}(H^\perp) = \{1\}$, thus we deduce $\widehat{\widehat{H}} = H \subseteq (H^\perp)^\perp$.
We also notice that, by our previous calculations

$$|(H^\perp)^\perp| = |\widehat{G}/H^\perp| = |G|/|G/H| = |H|,$$

which allows us to conclude.

□

Proposition 4.5 (Orthogonality relations)**.** *Let G be a finite abelian group.*

1. *Fix χ a character, then:* $\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ |G| & \text{if } \chi = \chi_0 \end{cases}$
2. *Fix an element $g \in G$, then* $\sum_{\chi\in \widehat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1 \end{cases}$

Proof. 1. We have $\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g)$, for some $h \in G$. This gives us $\sum_{g\in G} \chi(g)(\chi(h) - 1) = 0$.
Either $\chi(h) = 1$, and as we can take any $h \in G$ in the previous calculations, we get that $\chi = \chi_0$, and in particular $\sum_{g\in G} \chi_0(g) = |G|$.
Or $\sum_{g\in G} \chi(g) = 0$, and we are done, in the case $\chi \neq \chi_0$.

2. Noticing that $\chi(g) = \hat{g}(\chi)$, we can conclude using point 1).

□

4.2 Dirichlet Characters

Definition 4.6 (Dirichlet character)**.** A Dirichlet character is a character of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, for some $n \in \mathbb{N}$. For $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$, n is called the modulus of χ.

Example 4.7. 1. if p is an odd prime, the Legendre symbol is a Dirichlet character of modulus p, where the Legendre symbol is $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$, for $a \in \mathbb{Z}/p\mathbb{Z}$.

2. $\chi : (\mathbb{Z}/5\mathbb{Z}) \to \mathbb{C}^\times$, such that $\chi(1) = 1$, $\chi(2) = i$, $\chi(3) = -i$ and $\chi(4) = -1$.

We notice that for if $n|m$ we have a natural homomorphism

$$\varphi : (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

We define $\tilde{\chi} = \chi \circ \varphi$, which is clearly in $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$, for any $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$. In this case we say that $\tilde{\chi}$ is **induced** by χ.
We say that χ is **primitive** if it is not induced by any character of lower modulus. We define f_χ to be the minimal modulus of a Dirichlet character χ, i.e χ is not induced by a character of smaller modulus, and call f_χ the **conductor** of χ.

We notice that any Dirichlet character can be extended to a function $\mathbb{Z} \to \mathbb{C}$, by setting: $\chi(a) = \begin{cases} \chi(a \mod f_\chi) & \text{if } (a, f_\chi) = 1 \\ 0 & \text{if } (a, f_\chi) \neq 1 \end{cases}$.

If we take χ_1, χ_2 two primitive Dirichlet characters, with conductor n and m respectively. We notice that for $l = \operatorname{lgm}(n, m)$, we get a character:

$$\begin{aligned} \eta \colon (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathbb{C}^\times \\ a &\mapsto \chi_1(a)\chi_2(a). \end{aligned}$$

This character need not be irreducible, but we can define $\chi_1\chi_2$ as the irreducible character which induces η. This enables us to define a closed product on the set of primitive Dirichlet characters, that is clearly associative, commutative and with identity χ_0.

Example 4.8.

We take $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$, defined by $\chi(1) = 1$, $\chi(5) = -1$, $\chi(7) = -1$ and $\chi(11) = 1$, and $\varphi : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$, defined by $\varphi(1) = 1$, $\varphi(3) = -1$.
We get $\eta : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$, such that $\eta(1) = \chi(1)\varphi(1) = 1$, $\eta(5) = -1$, $\eta(7) = 1$, $\eta(11) = -1$, which is not primitive.
Indeed, we notice that the primitive character that induces η is:
$\chi\varphi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$, such that $\chi\varphi(1) = 1$, $\chi\varphi(2) = -1$, so $f_{\chi\varphi} = 3$.

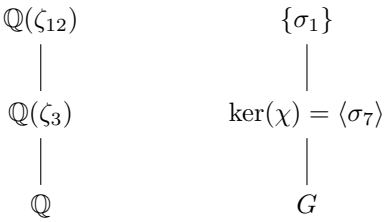
We notice that for any $n \in \mathbb{N}$, $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$, $\bar{\chi} = \chi^{-1}$, as the image of χ is contained in the set of n-th roots of unity. We also notice that $\bar{\chi}$ has to have the same conductor as χ, and $\bar{\chi} \cdot \chi = \chi_0$. Combining this observation with the previous paragraph we get that the Dirichlet characters form a group, as any Dirichlet character can be represented by a primitive Dirichlet character and their product is well defined.
We call **order** of a Dirichlet character its order as a group element, and notice that it is always finite.

In particular we notice that $\chi(-1) = \pm 1$, if $\chi(-1) = 1$ we say that χ is **even** and if $\chi(-1) = -1$ we call χ **odd**. Actually, the set of even characters forms a subgroup of the group of Dirichlet characters.

We can easily notice that the Dirichlet characters with conductor dividing n form a finite subgroup, noticing for instance that the lcm of two of their conductors is always going to be smaller or equal to n.

We define ζ_n to be a primitive n-th root of unity, then we can identify $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times$.
Let $\chi \in \widehat{G}$, and $K = \mathbb{Q}(\zeta_n)^{\ker(\chi)}$ (as clearly $\ker(\chi)$ is a subgroup of G), we call K the **the field associated to** χ.
More generally, we can consider $X < \widehat{G}$ (i.e X is a subgroup that contains characters such that the lcm of their conductors divides n). Let $H = \cap_{\chi \in X} \ker(\chi)$, then H is a subgroup of G, and we call the fixed field by H the **field associated to** X. Furthermore, under the identification $G \cong \widehat{\widehat{G}}$, we notice that $H = X^\perp$, as $\{\hat{g} \in \widehat{\widehat{G}} | \hat{g}(\chi) = 1, \forall \chi \in X\} \cong \{g \in G | \chi(g) = 1, \forall \chi \in X\}$.

Example 4.9. Let $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \to \mathbb{C}^\times$, defined by $\chi(\sigma_1) = 1$, $\chi(\sigma_5) = -1$, $\chi(\sigma_7) = 1$, $\chi(\sigma_{11}) = -1$, where $\sigma_i : \zeta_{12} \mapsto \zeta_{12}^i$. We notice that $\ker(\chi) = \{\sigma_1, \sigma_7\}$.



We notice that $\sigma_7(\zeta_3) = \zeta_3$, so $\ker(\chi)$ fixes elements of $\mathbb{Q}(\zeta_3)$. In particular by Galois theory, we can see that $\mathbb{Q}(\zeta_3)$ is the fixed field of $\mathbb{Q}(\zeta_{12})$ by $\ker(\chi)$, hence it is the field associated to χ. From this we get that χ is a character of $G/\ker(\chi) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^\times$, and $f_\chi = 3$.

Example 4.10. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, and take X to be the subset of even characters in $\widehat{G}$. We actually have that X is a subgroup. We notice that X is a subgroup of index 2. We further have that for any $\chi \in X$, $\chi(-1) = 1$, so $\sigma_{-1} \in \ker(\chi)$, for all $\chi \in X$ (where σ_i is defined as in the previous example). As σ_{-1} is simply the complex conjugation, it allows us to deduce that the field fixed by X has to be real.
We know that $\{\sigma_1, \sigma_{-1}\} \subseteq \cap_{\chi \in X} \ker(\chi)$ and now we will show that it is actually an equality.
Assume we have $\sigma_r \in \cap_{\chi \in X} \ker(\chi)$, where $r \neq 1$. We get that for all $\chi \in X$, $\hat{\sigma}_r(\chi) = \chi(\sigma_r) = 1$ and as $\hat{\sigma}_r$ cannot be trivial, there exist $\psi \in \widehat{G}$, such that $\hat{\sigma}_r(\psi) = \psi(\sigma_r) \neq 1$ (where $\hat{\sigma}$ is defined in the proof of Lemma 4.3). By the definition of X, ψ has to be odd, which implies that ψ^2 is even, so $\psi^2(\sigma_r) = 1$ and thus $\psi(\sigma_r) = -1$.
As X has index 2, any odd character can be written as $\psi\chi$, for some $\chi \in X$. This implies that $\tilde{\sigma}_r$ sends any odd character to -1 and any even character to 1, but in that case $\sigma_r = \sigma_{-1}$, and it allows us to conclude. We will later prove that the field associated to X is actually $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, the maximal real

field of this extension.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & & \{1\} \\ | & & | \\ \mathbb{Q}(\zeta_n+\zeta_n^{-1}) & & \{\sigma_1,\sigma_{-1}\} \\ | & & | \\ \mathbb{Q} & & G \end{array}$$

We will use the following theorem without proof.

Theorem 4.11 (Conductor discriminant formula)**.** *Let X be a finite group of Dirichlet characters and K its associated number field, then*

$$d_{K/\mathbb{Q}} = (-1)^{r_2} \prod_{\chi \in X} f_\chi,$$

where r_2 is the number of pairs of imaginary embeddings.

4.3 Enhanced Galois correspondence

Let $K/\mathbb{Q}$ be an abelian extension. Denote $G = \mathrm{Gal}(K/\mathbb{Q})$. We recall the usual Galois correspondence:

$$\begin{array}{ccc} K & & \{1\} \\ | & & | \\ L = K^H & & H = \mathrm{Gal}(K/L) \\ | & & | \\ \mathbb{Q} & & G \end{array} .$$

Let $X_K := \widehat{\mathrm{Gal}(K/\mathbb{Q})}$.

Remark 4.12. Let $K/\mathbb{Q}$ be an abelian extension.
By Kronecker–Weber theorem, there exists a $n \in \mathbb{N}$, such that $K \subseteq \mathbb{Q}(\zeta_n)$. From Galois theory we know that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$, in particular $K = \mathbb{Q}(\zeta_n)^{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)}$.

We get the following new correspondence (where we identify $\mathrm{Gal}(K/\mathbb{Q})$, with $\widehat{\widehat{\mathrm{Gal}(K/\mathbb{Q})}}$):

$$\begin{aligned} \{\text{Subgroups of } X_K\} &\to \{\text{Subfields of K}\} \\ Y &\mapsto \text{fixed field of } Y^\perp, \text{ denoted } K^{Y^\perp} \\ \mathrm{Gal}(K/L)^\perp = X_L &\hookleftarrow L \end{aligned}$$

To prove the correspondence we first notice that:
$X_L = \widehat{\mathrm{Gal}(L/\mathbb{Q})} = \mathrm{Gal}(\widehat{K/\mathbb{Q}})/\mathrm{Gal}(K/L)) = \mathrm{Gal}(K/L)^\perp$.

Let $Y \leq X_K$, and set $L = K^{Y^\perp}$, by usual Galois correspondence we get $Y^\perp = \mathrm{Gal}(K/L)$. This allows us to conclude one direction as $X_L = \mathrm{Gal}(K/L)^\perp = (Y^\perp)^\perp = Y$.

For the other direction, let $\mathbb{Q} \subseteq L \subseteq K$. As $\left(\mathrm{Gal}(K/L)^\perp\right)^\perp = \mathrm{Gal}(K/L)$ we remark that $K^{\left(\mathrm{Gal}(K/L)^\perp\right)^\perp} = K^{\mathrm{Gal}(K/L)} = L$.
We thus get the following enhanced Galois correspondence:

$$\begin{array}{ccccc} K & & \{1\} & & X_K = \widehat{G} \\ | & & | & & | \\ L = K^H & & H = \mathrm{Gal}(K/L) & & X_L = H^\perp = \widehat{G/H} \\ | & & | & & | \\ \mathbb{Q} & & G & & \{\chi_0\} = G^\perp \end{array}$$

Example 4.13. Let X be the group of even Dirichlet characters, of modulus n. We call K the associated field, and we already know that $K \subseteq \mathbb{Q}(\zeta_n)$ and that K is real.
Let $L \subseteq \mathbb{Q}(\zeta_n)$ be a real subfield, which implies that $\sigma_{-1}|_L = id_L$, i.e $\sigma_{-1} \in X_L^{\perp}$, or equivalently all elements in X_L are even. This tell us that $X_L \subseteq X$, an we can conclude that $L \subseteq K$ using our enhanced Galois correspondence. This implies that in particular K has to be the maximal real subfield of $\mathbb{Q}(\zeta_n)$.

Remark 4.14. Let X_1, X_2 be groups of Dirichlet characters associated to fields L_1, L_2, then the field associated to the group generated by X_1, X_2 is $L_1 L_2$.
The proof is left as an exercise.

4.4 Ramification via Dirichlet characters

Remark 4.15. We can decompose Dirichlet characters.
Let $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ and $n = \prod_{j=1}^n p_j^{a_j}$. From the Chinese reminder theorem we get:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{j=1}^{n} \left(\mathbb{Z}/p_j^{a_j}\mathbb{Z}\right)^\times,$$

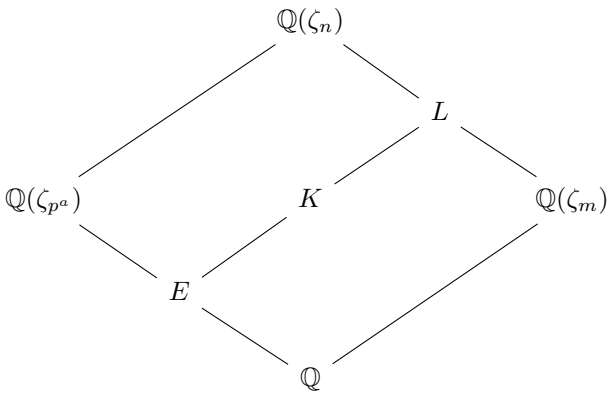
thus we can define χ, by giving a family of $\chi_{p_j} : (\mathbb{Z}/p_j^{a_j}\mathbb{Z})^\times \to \mathbb{C}^\times$.

Definition 4.16. Let X be a group of Dirichlet characters defined modulo n, where $n = \prod_{j=1}^n p_j^{a_j}$. We define $X_{p_j} = \{\chi_{p_j} | \chi \in X\}$.

Theorem 4.17. *Suppose X is a group of Dirichlet characters with associated field K. If $p \in \mathbb{Z}$ is prime, then the ramification index of p in $K/\mathbb{Q}$ is $e = |X_p|$.*

Proof. A reminder from algebraic number theory: let $F \subseteq L \subseteq K$ be an extension of number fields. Let $\mathfrak{p} \subseteq \mathcal{O}_F$, a non zero prime ideal, and take $\mathfrak{P}$ a prime ideal in $\mathcal{O}_L$, $\mathfrak{B}$ a prime ideal in $\mathcal{O}_K$ such that $\mathfrak{p} \cdot \mathcal{O}_L \subseteq \mathfrak{P}$ and $\mathfrak{p} \cdot \mathcal{O}_K \subseteq \mathfrak{B}$, then $e(\mathfrak{B}/\mathfrak{p}) = e(\mathfrak{B}/\mathfrak{P}) \cdot e(\mathfrak{P}/\mathfrak{p})$.
Moreover $d_{K/F} = N_{L/F}(d_{K/L}) \cdot d_{L/F}^{[K:L]}$.
Also recall that if $L_1 \cap L_2 = \mathbb{Q}$, where L_1, L_2 two number fields, then $d_{L_1 L_2/\mathbb{Q}} = d_{L_1/\mathbb{Q}}^{[L_2:\mathbb{Q}]} \cdot d_{L_2/\mathbb{Q}}^{[L_1:\mathbb{Q}]}$.

We can now begin the proof of the theorem. Let $n = \operatorname{lcm}(f_\chi | \chi \in X)$, then $K \subseteq \mathbb{Q}(\zeta_n)$ and write $n = p^a m$, for some $p \nmid m$.
Let $L = K(\zeta_m)$, we clearly have the following field extension $\mathbb{Q}(\zeta_m) \subseteq L \subseteq \mathbb{Q}(\zeta_n)$.
We now look at $X_L = \widehat{\operatorname{Gal}(L/\mathbb{Q})}$. We notice that it is generated by elements from $\widehat{\operatorname{Gal}(K/\mathbb{Q})} = X$ and $\widehat{\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})}$. Since $(p, m) = 1$, $\widehat{\operatorname{Gal}(L/\mathbb{Q})} = X_p \times \widehat{\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})}$, in particular $L = E\mathbb{Q}(\zeta_n)$, where E is the field corresponding to X_p. Moreover $E \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, i.e it is a composition of linearly disjoint fields. We get the following diagram:



We also get the following assertions:

- p is unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, since $p \nmid m$.
- Let $\mathfrak{P}$ be a prime over p in $\mathcal{O}_E$, we know that $d_{L/\mathbb{Q}} = d_{E/\mathbb{Q}}^{[\mathbb{Q}(\zeta_m):\mathbb{Q}]} d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$.
  We also get $d_{L/\mathbb{Q}} = N_{E/\mathbb{Q}}(d_{L/E}) d_{E/\mathbb{Q}}^{[L:E]}$, thus as $[L : E] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$, we have $N_{E/\mathbb{Q}}(d_{L/E}) =$

$d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$.
We assume by contradiction that $\mathfrak{P}$ ramifies in L, which is equivalent to $\mathfrak{P}$ dividing $d_{L/E}$. Then, from the definition of the norm, and as $f(\mathfrak{P}/p) \neq 0$, $p|N_{E/\mathbb{Q}}(d_{L/E})$. Form the previous paragraph we get that $p|d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$, which yields a contradiction as p is not ramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ thus cannot divide $d_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}^{[E:\mathbb{Q}]}$.
We recall that for any finite extensions $N \subseteq P \subseteq Q$, and primes $\mathfrak{n}, \mathfrak{p}, \mathfrak{q}$ in N, P, Q respectively, we have $e(\mathfrak{q}/\mathfrak{n}) = e(\mathfrak{q}/\mathfrak{p})e(\mathfrak{p}/\mathfrak{n})$.
We now notice that for any prime $\mathfrak{B}$ over $\mathfrak{P}$ in L, we get $e(\mathfrak{B}/\mathfrak{P}) = 1$, thus we also get that for any prime over $\mathfrak{P}$ in K the ramification index is 1. It allows us to conclude that the ramification index for p in $E/\mathbb{Q}$ is the same as the ramification index for p in $K/\mathbb{Q}$.

- p is totally ramified in $\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}$, so p is totally ramified in E.

Hence, the ramification index for p is $[E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})| = |X_p|$. □

Corollary 4.18. *Let X be a group of Dirichlet characters, and K the associated field. Then p is unramified in $K/\mathbb{Q}$ if and only if $\chi(p) \neq 0$ for all $\chi \in X$.*

Proof. The prime p is unramified if and only if $|X_p| = 1$, or equivalently if there is no nontrivial character in X with conductor divisible by p, i.e $\chi(p) \neq 0$, for all $\chi \in X$. □

Theorem 4.19. *Let X be a group of Dirichlet characters, and K be the associated field. Let $p \in \mathbb{N}$ be prime. We define*

$$Y = \{\chi \in X : \chi(p) \neq 0\}$$
$$Y_1 = \{\chi \in X : \chi(p) = 1\},$$

and get that

X/Y is isomorphic to the inertia subgroup for p.
X/Y_1 is isomorphic to the decomposition group for p.
X/Y_1 is cyclic of order p.

Example 4.20. Le χ be the generator of $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})}$, let ψ be a generator of $\widehat{\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})}$.
Let K be associated to $\chi^2\psi$ and L to $\langle\chi^2, \psi\rangle$, where we view these characters as elements of $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q})}$. We notice that $\ker(\psi) = \langle\sigma_{13}\rangle$ and $\ker(\chi^2) = \langle\sigma_9, \sigma_{11}\rangle$, so L is the fixed field of $\langle\sigma_9\rangle$. We also notice that $\ker(\psi\chi^2) = \langle\sigma_3\rangle$, so $K = \mathbb{Q}(\zeta_{20})^{\langle\sigma_3\rangle}$. We can compute, using for instance SageMath, that $L = \mathbb{Q}(\sqrt{5}, i)$ and $K = \mathbb{Q}(\sqrt{-5})$.
This implies that L/K is unramified at all primes other than 2 and 5, where we can deduce this result by looking at ramification indices for $L/\mathbb{Q}$ and $K/\mathbb{Q}$ as the extensions are abelian.

- For $K/\mathbb{Q}$, for $p = 2$ or 5, we have $X = \{\chi_0, \chi^2\psi\}$ and $Y = \{\chi_0\}$, thus $e_2 = e_5 = 2$.
- For $L/\mathbb{Q}$, $X = \{\chi_0, \chi^2, \psi, \chi^2\psi\}$.
  for $p = 2$, $Y = \{\chi_0, \chi^2\}$, thus $e_2 = 2$
  for $p = 5$, $Y = \{\chi_0, \psi\}$, thus $e_5 = 2$.

This implies that L/K is actually unramified at every prime: ramification on L/K is $e_{L/\mathbb{Q}}/e_{K/\mathbb{Q}} = 1$.

4.5 Exercises week 4

1. Review the concepts introduced in the lecture by consulting the Jupyter Notebook uploaded on Moodle (you can open it, for example, with CoCalc). The notebook summarizes the key notions from the lecture and demonstrates how they can be computed using SageMath. Run all code cells to observe how the computations are carried out. Experiment by modifying the examples (e.g., changing input values) to strengthen your understanding of the concepts and see how the results change.

2. (a) Let χ and ψ be primitive characters. Show that if $(f_\chi, f_\psi) = 1$, then $f_{\chi\psi} = f_\chi f_\psi$. Find a counterexample in the case where $(f_\chi, f_\psi) \neq 1$.
   (b) Show that the set of all even Dirichlet characters is a subgroup of the group of all Dirichlet characters.

3. Let $p > 2$ be a prime and let $n > 0$ be an integer. Calculate the absolute discriminant of $\mathbb{Q}(\zeta_{p^n})$.
   Hint: Use the Conductor Discriminant Formula

4. Let X_1 and X_2 be the group of Dirichlet characters corresponding to the fields L_1 and L_2, respectively. Show that:
   (a) The group generated by X_1 and X_2 corresponds to the compositum L_1L_2.
   (b) The group $X_1 \cap X_2$ corresponds to $L_1 \cap L_2$.

5. In this exercise we study quadratic Dirichlet characters and their associated fields.
   (a) Let m be an odd positive integer. How many quadratic Dirichlet characters modulo m are there? How many of them are primitive?
   Hint: Consider the decomposition of a quadratic character. What is the group structure of $(\mathbb{Z}/p^a\mathbb{Z})^\times$ *?*
   (b) What does your answer to part (a) tell you about the quadratic subfield(s) of $\mathbb{Q}(\zeta_p)$, where p is an odd prime? Does a quadratic subfield always exist? Is it unique? When is it real? Calculate the quadratic subfield(s) and the discriminant(s).
   Hint: Is the quadratic character even/odd? Use the conductor discriminant formula and [Sh2,Ex4] Exercises week 2.
   (c) Let p be an odd prime. How many quadratic Dirichlet characters modulo $4p$ are there? How many of them are primitive? What does this tell you about the quadratic subfield(s) of $\mathbb{Q}(\zeta_{4p})$, where p is an odd prime? Calculate all quadratic subfield(s).
   (d) Answer similar questions about the quadratic subfield(s) of $\mathbb{Q}(\zeta_8)$.
   (e) Conclude that for any odd prime p, $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_m)$ for $m = p$ or $4p$. Use this to show (without Kronecker–Weber) given any integer d, there is some m such that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_m)$.

5 Dirichlet's Theorem on Arithmetic progressions

5.1 Dirichlet Series

Our goal today is to prove Dirichlet's Theorem on Arithmetic progressions, Theorem 4.1 from Childress' book. Let us state the theorem for motivation.

Theorem 5.1. *Let m be a positive integer and a be an integer such that $\gcd(a, m) = 1$. Then, there are infinitely many primes in the sequence $a, m + a, m + 2a, \ldots$. In other words, there are infinitely many primes p such that $p \equiv a \mod m$.*

Notice that the special case with $a = 1$ is just the statement that there are infinitely many primes. Let us first give another proof of this fact using the Riemann Zeta function to motivate what is to come. 2000 years after Euclid's proof of the infinitude of primes, Euler gave another proof using what we today call Riemann's Zeta function in 1737. Let us now sketch Euler's proof of the infinitude of primes.
We define the Riemann Zeta function by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

We will show later in this lecture that the following formula, called Euler's Product Formula, holds:

$$\zeta(s) = \prod_{p} (1 - \frac{1}{p^s})^{-1}$$

This formula is true since we can write every integer as a product of primes using the fundamental theorem of arithmetic. Since in Dedekind domains we can write every ideal as a product of prime ideals, it's natural to expect a generalization to this to Dedekind domains, which we will call the Dedekind Zeta function.
As $s \to 1$, $\zeta(s)$ approaches the harmonic series, which diverges. Thus, the right-handside of the equation above should also diverge. However, if we had finitely many primes, it would not. In fact, in the same paper, Euler shows that $\sum_p \frac{1}{p}$ also diverges and states informally that the sum over all primes of $1/p$ is $\log \log \infty$, which one can see as a primitive version of the Prime Number Theorem!
Let us now start to generalize by defining Dirichlet series.

Definition 5.2. Let $\{a_n\}$ be a sequence of complex numbers. Then,

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is called a **Dirichlet series**.

Notice that $\zeta(s)$ is a Dirichlet series with the sequence $a_n = 1$ for every $n \geq 1$.
Let us now recall some tools we are going to use from complex analysis.

Definition 5.3. Let

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

We say that $f(s)$ **converges pointwise** at $s_0 \in \mathbb{C}$ if

$$S_N(s_0) = \sum_{n=1}^{N} \frac{a_n}{n^s}$$

converges to some $L \in \mathbb{C}$ as $N \to \infty$.
We say that $f(s)$ **converges absolutely** at $s_0 \in \mathbb{C}$ if

$$\sum_{n=1}^{\infty} |\frac{a_n}{n^s}|$$

converges.
We say that $f(s)$ **converges uniformly on** $U \subseteq \mathbb{C}$ if $f(s)$ converges pointwise and

$$\sup_{z\in U}|S_N(z) - f(z)| \to 0$$

as $N \to \infty$.

Let us now recall Abel's Lemma, which follows from a simple trick with telescoping sums and is used in the proof of Abel's Test in real analysis. We omit the proof.

Lemma 5.4. *Let $\{a_n\}, \{b_n\}$ be sequences of complex numbers. Let $r \geq m$.*
Let $A_{m,r} := \sum_{n=m}^{r} a_n$ and $S_{m,r} := \sum_{n=m}^{r} a_n b_n$.
Then,

$$S_{m,r} = \sum_{n=m}^{r-1} A_{m,n}(b_n - b_{n+1}) + A_{m,r}b_r.$$

Let us also remember the following statement about the convergence of holomorphic functions from complex analysis.

Lemma 5.5. *Let A be an open subset of $\mathbb{C}$ and let $\{f_n\}$ be a sequence of holomorphic functions on A that converge uniformly on every compact subset to f. Then, f is holomorphic on A and $\{f_n'\}$ converges to f' on A.*

The proof is Exercises week 5 exercise 1.
Finally, here is one last lemma, whose proof is Exercises week 5 exercise 2:

Lemma 5.6. *If $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges uniformly in every domain of the form*

$$\{s : Re(s - s_0) \geq 0, |Arg(s - s_0)| \leq \theta\}$$

with $\theta < \frac{\pi}{2}$.

Theorem 5.7. *If $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges for $Re(s) > Re(s_0)$ to a function that is holomorphic there.*

Let us now sketch the proof.

Proof. Apply Lemma 5.6 and Lemma 5.5 to $A = \{s \in \mathbb{C} : Re(s) > Re(s_0)\}$ and $f_N(s) = \sum_{n=1}^{N} \frac{a_n}{n^s}$. □

Let's now explore some corollaries of this theorem.

Corollary 5.8. *Let*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Write $s = \sigma + it$ for $\sigma, t \in \mathbb{R}$.

1. *If the a_n are bounded, then $f(s)$ converges absolutely for $\sigma > 1$.*
2. *If $A_n = a_1 + \cdots + a_n$ is bounded, then $f(s)$ converges (but not necessarily absolutely) for $\sigma > 0$.*
3. *If $f(s)$ converges at $s = s_0$, it converges absolutely for $\sigma > Re(s_0) + 1$.*

Proof. 1. Let $M > 0$ be a real number such that $|a_n| \leq M$ for every $n \geq 0$. Then,

$$\sum_{n=1}^{\infty} |\frac{a_n}{n^s}| \leq \sum_{n=1}^{\infty} \frac{|a_n|}{n^\sigma} \leq M \sum_{n=1}^{\infty} \frac{1}{n^\sigma}.$$

Since the infinite sum on the right-hand side converges for $\sigma > 1$, we have the desired result.

2. For $r \geq m$, let $A_{m,r} := \sum_{n=m}^{r} a_n$ be as in Abel's Lemma.
   Let $M > 0$ be a real number such that $|A_{m,r}| \leq M$ for every $r \geq m \geq 0$.
   Applying Abel's Lemma with $b_n := n^{-s}$, we get

$$\begin{aligned} S_{m,r} &= \left| \sum_{n=m}^{r-1} A_{m,n}\big(n^{-s} - (n+1)^{-s}\big) + A_{m,r} r^{-s} \right| \\ &\leq \sum_{n=m}^{r-1} |A_{m,n}|\,|n^{-s} - (n+1)^{-s}| + |A_{m,r}|\,|r^{-s}| \\ &\leq M \left(\sum_{n=m}^{r-1} |n^{-s} - (n+1)^{-s}| + |r^{-s}| \right). \end{aligned}$$

   By Theorem 3.2, we can assume without loss of generality that $s = \sigma \in \mathbb{R}$. Then, we have that

$$|S_{m,r}| \leq \frac{M}{m^{\sigma}}.$$

   so the partial sums of $f(s)$ are Cauchy when $\sigma > 0$.

3. Let

$$g(s) = f(s + s_0) = \sum_{n=1}^{\infty} \frac{a_n}{n_{s_0}} \frac{1}{n^s}.$$

   Since $f(s_0)$ is convergent, $b_n = \frac{a_n}{n^{s_0}} \to 0$ s $n \to \infty$.
   Thus, by part (i), $g(s)$ is absolutely convergent for $\sigma > 1$, so $f(s) = g(s - s_0)$ is absolutely convergent when $Re(s - s_0) > 1$.

□

We finally have all of the ingredients ready to generalize the Riemann-Zeta function.

Definition 5.9. Let $\chi : (\mathbb{Z}/m\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$. The **Dirichlet L-series associated to** χ is

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Notice that $\zeta(s) = L(s, \chi_0)$.
Assume $\chi \neq \chi_0$.
Let $A_n = \chi(1) + \cdots + \chi(n)$. Let $n = mk + r$ where $0 \leq r \leq m - 1$. Then,

$$\begin{aligned} &[\chi(1) + \ldots + \chi(m)] + [\chi(m+1) + \ldots + \chi(2m)] + \cdots \\ &\quad + [\chi(km+1) + \ldots + \chi(km+r)] \\ &= \chi(km+1) + \ldots + \chi(km+r) \end{aligned}$$

because $\chi(1) + \ldots + \chi(m) = 0$ by the orthogonality relations. Thus, $A_n \leq r < m$ for any $n \geq 0$.
Thus, by part (ii) of Corollary 3.3, $L(s, \chi)$ is analytic for $Re(s) > 0$. By part (iii), $L(s, \chi)$ converges absolutely for $Re(s) > 1$.
Let us now generalize Euler's product formula. Notice that we also obtain Euler's product formula as a special case when $\chi = \chi_0$.

Proposition 5.10. *Let $s = \sigma + it$ with $\sigma > 1$. Then,*

$$L(s, \chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}.$$

Proof. Fix $s = \sigma + it$ with $\sigma > 1$.
We want to show

$$\lim_{N\to\infty} \prod_{p\leq N} (1 - \frac{\chi(p)}{p^s})^{-1} = L(s, \chi).$$

Let $p_1, \ldots, p_k$ be all the primes less than N.
Then,

$$\prod_{i=1}^{k} (1 - \frac{\chi(p_i)}{p_i^s})^{-1} = \prod_{i=1}^{k} (1 + \frac{\chi(p_i)}{p_i^s} + \frac{\chi(p_i)^2}{p_i^{2s}} + \cdots)$$

since

$$|\frac{\chi(p_i)}{p_i^s}| < 1$$

so we can apply the geometric series formula.
By multiplying the product of sums out, we get

$$\prod_{i=1}^{k} (1 + \frac{\chi(p_i)}{p_i^s} + \frac{\chi(p_i)^2}{p_i^{2s}} + \cdots) = \sum_{m_1,\ldots,m_k\geq 0} \frac{\chi(p_1^{m_1} \cdots p_k^{m_k})}{(p_1^{m_1} \cdots p_k^{m_k})^s}.$$

Let

$$\delta_N = \{n \in \mathbb{Z}_{\geq 0} : n \text{ is not divisible by any prime } p > N\}.$$

Then,

$$\sum_{m_1,\ldots,m_k\geq 0} \frac{\chi(p_1^{m_1} \cdots p_k^{m_k})}{(p_1^{m_1} \cdots p_k^{m_k})^s} = \sum_{n\in\delta_N} \frac{\chi(n)}{n^s}.$$

Thus, we have that

$$L(s, \chi) - \prod_{p\leq N} (1 - \frac{\chi(p)}{p^s})^{-1} = \sum_{n\in\mathbb{Z}_{\geq 0}\setminus\delta_N} \frac{\chi(N)}{n^s}.$$

Taking absolute values and applying the triangle inequality,

$$\sum_{n\in\mathbb{Z}_{\geq 0}\setminus\delta_N} \frac{\chi(N)}{n^s} \leq \sum_{n\in\mathbb{Z}_{\geq 0}\setminus\delta_N} \frac{1}{n^\sigma}.$$

As $N \to \infty$, the right hand-side goes to zero for $\sigma > 1$. □

If $Re(s) > 1$, we have that $L(s, \chi) \neq 0$. This is because we showed in section 4 that $\log L(s, \chi)$ is convergent for $Re(s) > 1$, and this implies that the infinite product can't diverge. It also can't converge to zero since otherwise the logarithm would have to diverge to negative infinity. (In general, infinite products are said to converge if the product converges to a non-zero number. If the product converges to zero, the product is said to diverge to zero.)
Let log be the principal branch of the logarithm, so the argument is between $-\pi$ and π.
Taking logarithm and using the Taylor series for $\log(1 - t)$, we obtain

$$\log(L(s, \chi)) = -\sum_p \log(1 - \chi(p)p^{-s}) = \sum_p \sum_{n\geq 1} \frac{\chi(p)^n}{np^{ns}}.$$

Now, notice that

$$\sum_p \sum_{n\geq 1} |\frac{\chi(p)^n}{np^{ns}}| \leq \sum_p \sum_{n\geq 1} \frac{1}{p^{n\sigma}} \leq \sum_{m\geq 1} \frac{1}{m^\sigma}.$$

The last inequality holds because instead of summing over all the numbers of the form p^n, we are summing over all natural numbers, so we are adding positive terms to the series, which can only make it larger. Thus, $\log(L(s, \chi))$ converges absolutely for $\sigma > 1$ so we can rearrange terms to get

$$\log(L(s,\chi)) = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

Let

$$\beta(s,\chi) = \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

Notice that

$$|\sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}| \leq \sum_{n\geq 2} \frac{1}{p^{n\sigma}} = \frac{p^{-2\sigma}}{1-p^{-\sigma}}.$$

Thus,

$$|\sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}| \leq \sum_p \frac{p^{-2\sigma}}{1-p^{-\sigma}}.$$

Since there are finitely many primes with $p^{-\sigma} \geq \frac{1}{2}$, we can ignore them completely and so we can ignore the denominator for the remaining infinitely many primes. Thus, this is essentially

$$\sum_p p^{-2\sigma}$$

which converges absolutely for $\sigma > 1/2$.

5.2 Dirichlet's Theorem on Primes in Arithmetic Progressions

We are now ready to prove Dirichlet's Theorem on Primes in Arithmetic Progressions, Theorem 5.1, which was stated in the beginning of the lecture.
Before diving into the proof, let us state some definitions and results we will use.

Definition 5.11. Let K be an algebraic number field. We define the **Dedekind zeta function of** K to be

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}$$

, as $\mathfrak{a}$ runs over all non-zero integral ideals of $\mathcal{O}_K$.

It is Exercise 3 on Exercises week 5to prove that $\zeta_K(s)$ is absolutely convergent for $\mathrm{Re}(s) > 1$.
By using factorizations of ideals instead of numbers, we have that

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$$

as $\mathfrak{p}$ runs over the prime ideals of $\mathcal{O}_K$. Let

$$\gamma_n = \{\mathfrak{a} : N\mathfrak{a} = n\}.$$

Then,

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\gamma_n}{n^s}.$$

We leave it as an exercise to show that $\zeta_K(s)$ is absolutely convergent for $Re(s) > 1$.
We will also use the following theorem without proof.

Theorem 5.12. *$\zeta_K(s)$ can be analytically continued to $\mathbb{C} - \{1\}$, with a simple pole at $s = 1$, i.e.*

$$\zeta_K(s) = \frac{\rho(K)}{s-1} + \textit{(something entire)}.$$

Moreover,

$$\rho(K) = \frac{2^{r_1}(2\pi)^{r_2} h_K r_K}{w_K \sqrt{|d_{K/\mathbb{Q}}|}}$$

where r_1 is the number of real embeddings of K, r_2 is the number of pairs of conjugate complex embeddings of K, h_K is the class number of K, R_K is the regulator of K, w_K is the number of roots of unity in K and $d_{K/\mathbb{Q}}$ is the discriminant.

We will also use the following lemma whose proof is Exercises week 5 exercise 4:

Lemma 5.13. *Let p, m be natural numbers with p prime such that $p \nmid m$. Let f be the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then,*

$$(1 - T^f)^{\varphi(m)/f} = \prod_{\chi \mod m} (1 - \chi(p)T)$$

where T is a variable.

We can now begin the proof.

Proof. Let $\gcd(m, a) = 1$. Notice that as the sums run over all characters of $(\mathbb{Z}/m\mathbb{Z})^\times$,

$$\begin{aligned}
\sum_\chi \chi(a)^{-1} \log L(s, \chi) &= \sum_\chi \chi(a)^{-1} \left(\sum_p \frac{\chi(p)}{p^s} + \beta(s, \chi) \right) \\
&= \sum_p \frac{1}{p^s} \sum_\chi \chi(a)^{-1}\chi(p) + \sum_\chi \chi(a)^{-1}\beta(s, \chi) \\
&= \sum_p \frac{1}{p^s} \sum_\chi \chi(pa^{-1}) + \sum_\chi \chi(a)^{-1}\beta(s, \chi).
\end{aligned}$$

But, by the orthogonality relations,

$$\sum_\chi \chi(pa^{-1}) = \begin{cases} \varphi(m), & p \equiv a \pmod m, \\ 0, & \text{otherwise}, \end{cases}$$

so

$$\sum_\chi \chi(a)^{-1} \log L(s, \chi) = \varphi(m) \sum_{p \equiv a \pmod m} p^{-s} + G(s), \qquad (*)$$

where $G(s)$ is just some series which is absolutely convergent for $\Re(s) > \frac{1}{2}$.
Let $s \to 1$. For the right-hand side of (*)
we get

$$\lim_{s \to 1} \varphi(m) \sum_{p \equiv a \mod m} p^{-s} + \text{some finite constant}$$

which would be finite if there were finitely many primes with $p \equiv a \mod m$. Thus, the proof will be complete if we can show that the left-hand side is infinite.
We already know that if $\chi = \chi_0$ we have

$$L(s, \chi_0) = \prod_p (1 - \chi_0(p)p^{-s})^{-1} = \zeta(s) \prod_{p \mid m} (1 - p^{-s}) \to \infty$$

as $s \to 1$ so $\log L(s, \chi_0) \to \infty$ as $s \to 1$.

Thus, it suffices to show that the non-trivial characters don't cancel this out. Recall that by the orthogonality relations, the sums over the characters are bounded. Thus, by Corollary 3.3 part (ii), $L(s,\chi)$ is analytic for $Re(s) > 0$. Thus, we only need to show that $L(1,\chi) \neq 0$.
Let $K = \mathbb{Q}(\zeta_m)$. Thus,

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{p}} \left(1 - N\mathfrak{p}^{-s}\right)^{-1} \\ &= \prod_{p} \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)^{-1} \\ &= \left(\prod_{p|m} \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}\right) \left(\prod_{p\nmid m} \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}\right).\end{aligned}$$

Notice that $N\mathfrak{p} = p^f$ where f is residue field degree.
Now, by Lemma 5.13, we have that

$$\prod_{p\nmid m} (1 - p^{-sf})^{-\varphi(m)/f} = \prod_{\chi} \prod_{p\nmid m} (1 - \chi(p)p^{-s})^{-1}.$$

Now, if $p \mid m$, then $\chi(p) = 0$, so they don't contribute, and we have

$$\begin{aligned}\prod_{p\nmid m} (1 - p^{-sf})^{-\varphi(m)/f} &= \prod_{p} (1 - p^{-sf})^{-\varphi(m)/f} \\ &= \prod_{p} \prod_{\chi} (1 - \chi(p)p^{-s})^{-1} \\ &= \prod_{\chi} \prod_{p} (1 - \chi(p)p^{-s})^{-1} \\ &= \prod_{\chi} L(s,\chi).\end{aligned}$$

On the other hand,

$$\prod_{p\nmid m} (1 - p^{-sf})^{-\varphi(m)/f} = \prod_{p\nmid m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1} = \zeta_K(s) \prod_{p|m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1}.$$

Thus,

$$\begin{aligned}\zeta_K(s) &\prod_{p|m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1} \\ &= \prod_{\chi} L(s,\chi) \\ &= L(s,\chi_0) \prod_{\chi\neq\chi_0} L(s,\chi) \\ &= \zeta(s) \prod_{p|m} (1 - p^s) \prod_{\chi\neq\chi_0} L(s,\chi).\end{aligned}$$

Finally, we have

$$\frac{\left(\prod_{p|m} \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)\right) \zeta_K(s)}{\left(\prod_{p|m} (1 - p^{-s})\right) \zeta(s)} = \prod_{\chi\neq\chi_0} L(s,\chi).$$

Notice that both products over $p \mid m$ are non-zero constants. Since both ζ and ζ_K have a simple pole at $s = 1$, we can let $s \to 1$ and the expression on the left approaches a finite constant, so the right-handside does too. We thus conclude the proof. □

5.3 Exercises week 5

1. Let A be an open subset of $\mathbb{C}$ and let (f_n) be a sequence of holomorphic functions on A that converges uniformly on every compact subset to a function f.
   Show that f is holomorphic on A and that the sequence of derivatives (f_n') converges uniformly on all compact subsets to f'.

   Hint: Let D be a closed disk contained in A and let C be its boundary. For s_0 in the interior of D, Cauchy's Formula applies to the $f_n(s_0)$. Let $n \to \infty$ to get a similar formula for $f(s_0)$. For the derivatives, proceed in the same way, using

   $$f'(s_0) = \frac{1}{2\pi i} \int_C \frac{f(s)}{(s-s_0)^2} ds.$$

2. Prove the following Lemma:

   Lemma 5.14. *If $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges uniformly in every domain of the form*

   $$\{s : Re(s - s_0) \geq 0, |Arg(s - s_0)| \leq \theta\}$$

   with $\theta < \frac{\pi}{2}$.

   Hint: Assume $s_0 = 0$. Show that we can replace domains of the form

   $$\{s : Re(s) \geq 0, |Arg(s)| \leq \theta\}$$

   for $\theta < \frac{\pi}{2}$ by domains of the form

   $$\{s : Re(s) \geq 0, \frac{|s|}{Re(s)} \leq M\}$$

   and prove the result on it. To prove the result, start by using Abel's Lemma and then use the following fact to obtain an upper bound to $|S_{m,r}|$ in Abel's Lemma:

   $$|e^{-cs} - e^{-ds}| = |s| \int_c^d e^{-tRe(s)} dt = \frac{|s|}{Re(s)} (e^{-cRe(s)} - e^{-dRe(s)}).$$

3. Show that

   $$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\gamma_n}{n^s}, \qquad \gamma_n = \#\{\mathfrak{a} : N\mathfrak{a} = n\}$$

   is absolutely convergent for $Re(s) > 1$. (Compare this to (i) of Cor.5.8 in the section on Dirichlet series—are the γ_n bounded?)

4. Let $p, m \in \mathbb{N}$ with p prime such that $p \nmid m$. Our goal is to prove that

   $$(1 - T^f)^{\varphi(m)/f} = \prod_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} (1 - \chi(p)T) \quad \forall T \in \mathbb{C}$$

   where $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ and f is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$.

   (a) Let $K = \mathbb{Q}(\zeta_m)$, $G = \mathrm{Gal}(K/\mathbb{Q})$, and $Z = Z(p)$ the decomposition group of p. Show that the restriction map $\widehat{G} \to \widehat{Z}$ is surjective.

   (b) Deduce that

   $$\prod_{\chi \in \widehat{G}} (1 - \chi(p)T) = \Big(\prod_{\psi \in \widehat{Z}} (1 - \psi(p)T) \Big)^g,$$

   where $g = \#\ker(\widehat{G} \to \widehat{Z}) = \varphi(m)/f$.

   (c) Identify $\widehat{Z} \cong \mu_f$ via $\psi \mapsto \psi(p)$ and use

   $$\prod_{\eta \in \mu_f} (1 - \eta T) = 1 - T^f$$

   to conclude.

6 Dirichlet Density and Ray Class Group

6.1 Dirichlet Density

Definition 6.1. Let $f, g : (1;\infty) \to \mathbb{R}$ defined for $s \in \mathbb{R}, s > 1$. We write $f \sim g$ when $f(s) - g(s)$ is bounded as $s \to 1^+$.

Remark 6.2 (reformulation of Dirichlet's Theorem)**.** We take a and m as in Dirichlet's Theorem on primes in arithmetic progressions, i.e., m a positive integer and a such that $(a, m) = 1$.
Recall that for any χ Dirichlet character, we have

$$\begin{aligned}\log L(s,\chi) &= \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + \{ \text{ Dirichlet series converging for } \mathrm{Re}(s) > 1/2\} \\ &\sim \sum_{p \text{ prime}} \frac{\chi(p)}{p^s}.\end{aligned}$$

We assume that $L(1,\chi) \neq 0$ if $\chi \neq \chi_0$ thus we have

$$\begin{aligned}\sum_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} \chi(a)^{-1} \log L(s,\chi) &\sim \sum_{\chi} \chi(a)^{-1} \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} \\ &\sim \sum_{p \equiv a \bmod m} \frac{\varphi(m)}{p^s} \sim \log L(s,\chi_0).\end{aligned}$$

Now

$$L(s,\chi_0) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \left(\prod_{p|m} (1 - p^{-s})\right) \zeta(s),$$

so $\log L(s,\chi_0) \sim \log \zeta(s)$ and

$$\underbrace{\sum_{p \equiv a \bmod m} \frac{1}{p^s}}_{\text{diverges as } s \to 1^+} \sim \frac{1}{\varphi(m)} \log \zeta(s). \tag{2}$$

Since ζ has a pole in $s = 1$ we have that $\log \zeta(s) \xrightarrow{s \to 1^+} \infty$, the sum cannot consist of only finitely many terms, and this gives us Dirichlet's Theorem.
Now that we have reformulated the Theorem, this leads us to the new notion of Dirichlet density. Note that

$$\begin{aligned}\frac{1}{\varphi(m)} \log \zeta(s) &= \frac{1}{\varphi(m)} \left(\underbrace{\log((s-1)\zeta(s))}_{\xrightarrow{s \to 1^+} 1} + \log\left(\frac{1}{s-1}\right) \right) \\ &\sim \frac{1}{\varphi(m)} \log\left(\frac{1}{s-1}\right).\end{aligned}$$

Hence using (2) we have

$$\sum_{p \equiv a \bmod m} p^{-s} \sim \frac{1}{\varphi(m)} \log\left(\frac{1}{s-1}\right).$$

If we reformulate this means that

$$\lim_{s \to 1^+} \frac{\sum_{p \equiv a \bmod m} p^{-s}}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{\varphi(m)}.$$

This motivates the following definition:

Definition 6.3 (Dirichlet density)**.** Let $\mathcal{S}$ be any set of primes. If

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}} p^{-s}}{\log(\frac{1}{s-1})} = \delta \text{ exists.}$$

Then we say that $\mathcal{S}$ has Dirichlet density $\delta = \delta(\mathcal{S})$.

Example 6.4 (Dirichlet Theorem)**.** If $\mathcal{S} = \{\text{primes } p : p \equiv a \bmod m\}$ then $\delta(\mathcal{S}) = \frac{1}{\varphi(m)}$.

Lemma 6.5. *Suppose $\mathcal{S}$ and $\mathcal{T}$ are sets of primes such that $\mathcal{S}\cap\mathcal{T} = \emptyset$, then if any two of $\delta(\mathcal{S}), \delta(\mathcal{T})$ or $\delta(\mathcal{S}\cup\mathcal{T})$ are finite then so is the third, and in that case we have*

$$\delta(\mathcal{S}\cup\mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T}).$$

Proof. Since we assume that $\mathcal{S}\cap\mathcal{T} = \emptyset$, using the definition of the density we have:

$$\begin{aligned}\lim_{s\to 1^+} \frac{\sum_{p\in(\mathcal{S}\cup\mathcal{T})} p^{-s}}{\log(\frac{1}{s-1})} &\underbrace{=}_{\mathcal{S}\cap\mathcal{T}=\emptyset} \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}} p^{-s} + \sum_{p\in\mathcal{T}} p^{-s}}{\log(\frac{1}{s-1})} \\ &= \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}} p^{-s}}{\log(\frac{1}{s-1})} + \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{T}} p^{-s}}{\log(\frac{1}{s-1})}.\end{aligned}$$

Thus, if any two of the three limits exists, the third one exists and we get the equality that we wanted. □

Theorem 6.6. *Let ${}^{K}\!/_{\mathbb{Q}}$ be Galois, and let*

$$\mathcal{S}_K = \{p \in \mathbb{Z} : p \text{ splits completely in } {}^{K}\!/_{\mathbb{Q}}\}.$$

Then $\delta(\mathcal{S}_K) = {}^{1}\!/_{[K:\mathbb{Q}]}$.

Proof. Let $\zeta_K(s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K \text{ prime}} (1 - N_{\mathfrak{p}}^{-s})^{-1}$ for $\mathrm{Re}(s) > 1$, be the Dedekind zeta function for K. We have for $s \in \mathbb{R}, s > 1$:

$$\begin{aligned}\log\zeta_K(s) &= -\sum_{\mathfrak{p}\subset\mathcal{O}_K \text{ prime}} \underbrace{\log(1 - N_{\mathfrak{p}^{-s}})}_{\text{well defined: } {}^{1}\!/_{N_{\mathfrak{p}}}<1} \\ &= \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{n} N_{\mathfrak{p}}^{-ns} \sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s} + \underbrace{\sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n} N_{\mathfrak{p}}^{-ns}}_{(\bullet) \text{ bounded as } s\to 1^+} \\ &\sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s}.\end{aligned}$$

Let us show (•):

$$\begin{aligned}\sum_{n=2}^{\infty} \frac{1}{n} N_{\mathfrak{p}}^{-ns} &\le \frac{N_{\mathfrak{p}}^{-2s}}{1 - N_{\mathfrak{p}}^{-s}} \\ &\le 2N_{\mathfrak{p}}^{-2s}.\end{aligned}$$

Thus we have

$$\sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n} N_{\mathfrak{p}}^{-ns} \le \sum_{\alpha\subset\mathcal{O}_K \text{ ideal}} 2N_{\alpha}^{-2s} = 2\zeta_K(2s) \underbrace{<}_{2s>2>1} \infty.$$

Now see that $\log\zeta_K(s) = \log((s-1)(\zeta_K(s)) + \log(1/(s-1)) \sim \log(1/(s-1))$,thus we have

$$\begin{aligned}\log\zeta_K(s) &\sim \log(1/(s-1)) \sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s} \\ &\sim \sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)=1=e(\mathfrak{p}/p)} p^{-s} + \sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)>1} p^{-f(\mathfrak{p}/p)s} + \sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)=1, e(\mathfrak{p}/p)>1} p^{-s}.\end{aligned}$$

The third series is bounded as the number of ramified primes is finite, now the second one is also bounded since:

$$\sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)>1} p^{-f(\mathfrak{p}/p)s} \leq \sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)>1} p^{-2s} \leq [K:\mathbb{Q}] \sum_{p\in\mathcal{S}_K} p^{-2s}.$$

The last inequality comes from the fact that since the extension is Galois, and we are looking at unramified primes, for such a prime ideal, $\mathfrak{p}$, we have $g(\mathfrak{p}/p) = \frac{1}{f(\mathfrak{p}/p)}[K:\mathbb{Q}]$. Thus since $f(\mathfrak{p}/p) > 1$ we get the inequality. So we are left only with the first series

$$\begin{aligned}\log \zeta_K(s) \sim & \log(1/(s-1)) \sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s} \\ \sim & \sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)=1=e(\mathfrak{p}/p)} p^{-s} \underbrace{=}_{g(\mathfrak{p}/p)=[K:\mathbb{Q}]} [K:\mathbb{Q}] \sum_{p\in\mathcal{S}_K} p^{-s}\end{aligned}$$

Hence

$$\log\left(\frac{1}{s-1}\right) = \sum_{p\in\mathcal{S}_K} [K:\mathbb{Q}]p^{-s} + \underbrace{b(s)}_{\text{bounded as } s\to 1^+}.$$

Thus we can compute $\delta(\mathcal{S}_K)$

$$\begin{aligned}\delta(\mathcal{S}_K) = & \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}_K} p^{-s}}{\log\left(\frac{1}{s-1}\right)} \\ = & \left(\frac{\sum_{p\in\mathcal{S}_K}[K:\mathbb{Q}]p^{-s} + b(s)}{\sum_{p\in\mathcal{S}_K} p^{-s}}\right)^{-1} \\ = & [K:\mathbb{Q}]^{-1}.\end{aligned}$$

□

Remark 6.7 (Notations)**.** Let $\mathcal{S}, \mathcal{T}$ be sets of primes in $\mathcal{O}_K$, where K is a number field. We define the following notations:

- Write $\mathcal{S} \prec \mathcal{T}$ if and only if $\delta(\mathcal{S} - \mathcal{T}) = 0$.
- Write $\mathcal{S} \approx \mathcal{T}$ if and only if $\mathcal{S} \prec \mathcal{T} \prec \mathcal{S}$.

Theorem 6.8. *Let E and K be number fields, both Galois over $\mathbb{Q}$, then*

$$\mathcal{S}_K \prec \mathcal{S}_E \iff E \subseteq K.$$

Proof. The part "$\Longleftarrow$" is clear since if $E \subseteq K$ then $\mathcal{S}_K \subseteq \mathcal{S}_E$.
For "$\Longrightarrow$"suppose that $\mathcal{S}_K \prec \mathcal{S}_E$. We know from exercise 3 sheet 3 that $\mathcal{S}_{KE} = \mathcal{S}_E \cap \mathcal{S}_K$, and since $\delta(\mathcal{S}_K - \mathcal{S}_E) = 0$, using lemma 6.5, we get

$$\delta(\mathcal{S}_{EK}) = \delta(\mathcal{S}_K \cap \mathcal{S}_E) = \delta(\mathcal{S}_K - \mathcal{S}_E) + \delta(\mathcal{S}_E \cap \mathcal{S}_K) = \delta(\mathcal{S}_K).$$

Thus Theorem 6.6 gives us that $[KE:\mathbb{Q}] = [K:\mathbb{Q}]$ hence $KE = K$ and $E \subseteq K$. □

6.2 Introduction of the Ray Class Group

Our goal in this section is to generalize the Dirichlet argument to a prime ideal in the ring of integers of a number field F. The question we will try to answer is "Are there infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_F$ in an arithmetic progression ? " But for that, we need to define what we mean by arithmetic progression in this context.

- We will replace "mod m" for $m \in \mathbb{Z}$ with "mod $\mathfrak{m}$" with $\mathfrak{m}$ an ideal of $\mathcal{O}_F$.
- We will define the ray class group analogously to the ideal class group.
- We will also expand the notion of Dirichlet characters and $\mathcal{L}$-functions.

Theorem 6.9 (Approximation Theorem)**.** *Let $|.|_1, ..., |.|_n$ be non-trivial pairwise inequivalent absolute values on F and let $\beta_1, ..., \beta_n$ be non-zero elements of F . For any $\epsilon > 0$, there is an element $\alpha \in F$ such that*

$$|\alpha - \beta_j|_j < \epsilon$$

for each $j = 1, ..., n$.

Proof. We will first show that $\exists x_1, ..., x_n \in F$ so that $\forall j$ we have $|x_j|_j > 1$ and $|x_j|_i < 1$ for all $i \neq j$. We proceed by induction on n.

- For $n = 2$: We take $j = 1$ And since $|.|_1, |.|_2$ are inequivalent, we can find $y \neq z \in F - \{0\}$ such that $|y|_1 > 1 \geq |z|_1$ and $|y|_2 \leq 1 < |z|_2$. Indeed, consider

  $$\sup_{z \in F, |z|_1 \leq 1} \{|z|_2|\}$$

  then this supremum can't be finite, else if $\exists M$ such that $\forall z \in F$ with$|z|_1 \leq 1$, $|z|_2 \leq M$ we would have, that for all $z \in F$, take $z' = \frac{z}{|z|_1}$ then, $|z'|_1 = 1$ thus $|z'|_2 = \frac{|z|_2}{|z|_1} \leq M$ by homogeneity, which is a contradiction since the two norms are inequivalent. This means that we can find a z as we wanted. For y we simply inverse the two norms and get the same result. Now take $x_1 = \frac{y}{z}$.

- For $n > 1$: Suppose that $\exists x \in F$ such that $|x|_1 > 1$ and $|x|_i < 1$ for all $i = 1, ..., n-1$. by the above, we know that there is a $v \in F$ such that $|v|_1 > 1$ and $|v|_n < 1$. We take x_1 to be :

  $$x_1 = \begin{cases} x & \text{if } |x|_n < 1 \\ x^r v & \text{if } |x|_n = 1 \\ \frac{x^r v}{1+x^r} & \text{if } |x|_n > 1. \end{cases}$$

  For $r \in \mathbb{Z}$ determined as follows:

  - For $|x|_n = 1$ then it suffices to take a sufficiently large r as $|x_1|_i = |x|_i^r |v|_i \xrightarrow{r \to \infty} 0$.
  - For $|x|_n > 1$, we have

    $$|x_1|_i = \frac{|x|_i^r |v|_i}{|1 + x^r|_i} = \frac{|v|_i}{|x^{-r} + 1|_i}.$$

    When $2 \leq i \leq n-1$, since $|x|_i < 1$ we have

    $$\frac{|v|_i}{|x^{-r} + 1|_i} \xrightarrow{r \to \infty} 0.$$

    When $i = 1$, since $|x|_1 > 1$ we have:

    $$\frac{|v|_1}{|x^{-r} + 1|_1} \xrightarrow{r \to \infty} |v|_1 > 1.$$

    When $i = n$, since $|x|_n < 1$ we have:

    $$\frac{|v|_n}{|x^{-r} + 1|_n} \xrightarrow{r \to \infty} |v|_n < 1.$$

  Similarly we can find $x_2, ..., x_n$ such that for all j $|x_j|_j > 1$ and $|x_j|_i < 1$ for all $i \neq j$.

Now we set $\alpha = \sum_{j=1}^{n} \frac{x_j^l \beta_j}{1+x_j^l}$ where $l \in \mathbb{Z}$ is determined as follows:

$$|\alpha\beta_j|_j \leq \underbrace{\left|\frac{\beta_j}{1 + x_j^l}\right|_j}_{\approx \frac{1}{|x_j|_j^l} \xrightarrow{l \to \infty} 0} + \sum_{i \neq j} \underbrace{\left|\frac{x_i^l \beta_i}{1 + x_i^l}\right|_j}_{\approx |x_i|_j^l \xrightarrow{l \to \infty} 0}.$$

Thus it suffices to choose l large enough. □

Remark 6.10. If we apply the Approximation Theorem 6.9 in the case where the absolute values are the $\mathfrak{p}$-adic norm $|.|_{\mathfrak{p}_1}, ..., |.|_{\mathfrak{p}_n}$, all pairwise inequivalent, and take $\beta_1, ..., \beta_n \in F^\times$ such that $\forall j = 1, ..., n$, $\beta_j \in \mathcal{O}_{\mathfrak{p}_j}^\times$, with $\mathcal{O}_{\mathfrak{p}_j}^\times$ the units of the $\mathfrak{p}$-adic integer, then by the Approximation Theorem, $\forall \epsilon > 0, \exists \alpha \in F$ such that $\forall j = 1, ..., n$

$$|\alpha - \beta_j|_{\mathfrak{p}_j} < \epsilon.$$

Now if we take $\epsilon = c^m$ with $c \in (0, 1)$ as in definition of the $\mathfrak{p}_j$-adic norms $|.|_{\mathfrak{p}_j}$ and $m \in \mathbb{Z}$, we have

$$\begin{aligned}
\left|\frac{\alpha}{\beta_j} - 1\right|_{\mathfrak{p}_j} \underbrace{|\beta_j|_{\mathfrak{p}_j}}_{=1} < \epsilon = c^m & \\
\implies & \operatorname{ord}_{\mathfrak{p}_j}\left(\frac{\alpha}{\beta_j} - 1\right) > m \\
\implies & \frac{\alpha}{\beta_j} - 1 \in \mathfrak{p}_j^m \\
\implies & \alpha - \beta_j \in \mathfrak{p}_j^m \\
\implies & \alpha \equiv \beta_j \bmod \mathfrak{p}_j^m.
\end{aligned}$$

Thus if $F = \mathbb{Q}$ and $\mathfrak{p}_j^m = (p_j)$, $p_j \in \mathbb{Z}$ prime we get the Chinese remainder Theorem.

Definition 6.11. Recall that the ideal class group of a number field F is

$$\mathcal{C}_F = \mathcal{I}_F / \mathcal{P}_F$$

Where $\mathcal{I}_F = \{\text{fractional ideals of } F\}$ and $\mathcal{P}_F = \{\text{fractional principal ideals of } F\}$.

Definition 6.12. Let $\alpha \in F$ be such that $\sigma(\alpha) > 0$, for all σ real embeddings of F. Then we say that α is totally positive and we denote it by $\alpha >> 0$.

Definition 6.13. Let $\mathfrak{m} \subset \mathcal{O}_F$ be a non-zero integral prime ideal, we define

$$\mathcal{P}_{F,\mathfrak{m}}^+ = \text{subgroup of } \mathcal{P}_F \text{ generated by } \{< \alpha >, \alpha \in \mathcal{O}_F, \alpha \equiv 1 \bmod \mathfrak{m}\}.$$

We introduce the following notation for $\alpha \in \mathcal{O}_F$ such that $\alpha \equiv 1 \bmod \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(\mathfrak{m})}$ for all $\mathfrak{p}|\mathfrak{m}$ in $F_\mathfrak{p}$ then we write $\alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}$.

Lemma 6.14. *With this notation, we have that*

$$\begin{aligned}
\mathcal{P}_{F,\mathfrak{m}}^+ =& \{< \frac{\alpha}{\beta} > | \alpha, \beta \in \mathcal{O}_F \textit{ prime to } \mathfrak{m}, \frac{\alpha}{\beta} >> 0, \alpha \equiv \beta \bmod \mathfrak{m}\} \\
=& \{< \alpha > | \alpha \in F, \alpha >> 0, \alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}\}.
\end{aligned}$$

Proof. Exercise 4 sheet 6. □

Definition 6.15. Let $\mathcal{I}_{F,\mathfrak{m}} = \{\mathfrak{a} \in \mathcal{I}_F, \operatorname{ord}_\mathfrak{p}(\mathfrak{a}) = 0, \forall \mathfrak{p}|\mathfrak{m}\}$, then we define the strict ray class group of f for $\mathfrak{m} \subset \mathcal{O}_F$ a non-zero integral prime ideal as :

$$\mathcal{R}_{F,\mathfrak{m}}^+ = \mathcal{I}_{F,\mathfrak{m}} / \mathcal{P}_{F,\mathfrak{m}}^+.$$

Example 6.16. Take $F = \mathbb{Q}, \mathfrak{m} = m\mathbb{Z}, m \geq 1$. If $< r > \in \mathcal{I}_{\mathbb{Q},m}$, then $r = \frac{a}{b} > 0$ such that $(a, m) = (b, m) = 1$. Then we define

$$\begin{aligned}
\Phi : \mathcal{I}_{\mathbb{Q},m} &\to \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \\
< r > &\mapsto ab^{-1}.
\end{aligned}$$

One can show that this map is surjective and well-defined, with kernel

$$\begin{aligned}
\ker \Phi =& \{< r > \in \mathcal{I}_{\mathbb{Q},m} | ab^{-1} \equiv 1 \bmod m\} \\
\underbrace{=}_{\text{Lemma 6.14}} & \mathcal{P}_{\mathbb{Q},m}^+ \\
\implies & \mathcal{R}_{\mathbb{Q},m}^+ = \mathcal{I}_{\mathbb{Q},m} / \mathcal{P}_{\mathbb{Q},m^+} \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times.
\end{aligned}$$

6.3 Exercises week 6

1. Let H be a subgroup of $\mathbb{Z}/n\mathbb{Z}$ and define

$$\mathcal{S} = \{\, p \text{ prime in } \mathbb{Z} : p + n\mathbb{Z} \in H \,\}.$$

Compute the density $\delta(\mathcal{S})$ in terms of $\#H$.

2. Let K/F be Galois, and let

$$\mathcal{S}_{K/F} = \{\mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \text{ splits completely in } K/F\}.$$

Prove that

$$\delta_F(\mathcal{S}_{K/F}) = \frac{1}{[K:F]}.$$

3. Let E and K be number fields, each of which is Galois over $\mathbb{Q}$.
Show that for any prime $p \in \mathbb{Z}$, p splits completely in both $E/\mathbb{Q}$ and $K/\mathbb{Q}$ if and only if p splits in their compositum extension $KE/\mathbb{Q}$.

4. Let F be a number field and $\mathfrak{m} \subset \mathcal{O}_F$ a non-zero ideal. Let $P^+_{F,\mathfrak{m}}$ be the subgroup of P_F generated by

$$\{\langle\alpha\rangle : \alpha \in \mathcal{O}_F,\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \text{and } \alpha \gg 0\}.$$

Show the two equalities:

$$P^+_{F,\mathfrak{m}} = \{\langle\alpha\rangle :\ \alpha \in F,\ \alpha \gg 0,\ \alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}\}$$

$$= \{\langle\tfrac{\alpha}{\beta}\rangle :\ \tfrac{\alpha}{\beta} \gg 0,\ \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \pmod{\mathfrak{m}}\}.$$

7 Introduction to Class Fields

7.1 Dirichlet Theorem for algebraic number fields

Previously we proved the **Dirichlet Theorem on primes in Arithmetic progression**.

Theorem 7.1. ***(Dirichlet's Theorem on Primes in Arithmetic Progressions)*** *If m is a positive integer and a is an integer for which $(a, m) = 1$, then there are infinitely many primes p satisfying $p \equiv a \,(mod\, m)$.*

The main goal of this section is to generalize this statement to any algebraic number field F, following the proof of Dirichlet, which involved several useful concepts, such as Dirichlet characters and L-functions. Their definition involved the group $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ which is the Galois group of cyclotomic extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$. We first need to generalize these notions to our new setting, namely when F is an algebraic number field and $\mathfrak{m}$ is a non-zero integral ideal of $\mathcal{O}_F$.

7.2 Ray class groups

We first focus on the Galois group $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. We could work with the ideal class group, but it turns out not to be enough. Instead we introduce a new group, named the *Ray class group(s)* which is a generalization of both the class group and the Galois group.

Recall that if an element $\alpha \in F$ satisfies $\sigma(\alpha) > 0$ for every real embedding $\sigma : F \to \mathbb{R}$, we say that α is *totally positive* and write $\alpha \gg 0$. Given a non-zero integral ideal $\mathfrak{m}$ of $\mathcal{O}_F$, we write

$$\mathcal{I}_F(\mathfrak{m}) = \{\mathfrak{a} \mid ord_\mathfrak{p}(\mathfrak{a}) = 0 \;\forall\; \mathfrak{p}|\mathfrak{m}\} \subseteq \mathcal{I}_F.$$

On the other hand, we set $\mathcal{P}^+_{F,\mathfrak{m}}$ to be the subgroup of $\mathcal{P}_F$ generated by

$$\{\langle\alpha\rangle \mid \alpha \in \mathcal{O}_F,\ \alpha \equiv 1 \,(\mathrm{mod}\, \mathfrak{m}),\ \text{and}\ \ \alpha \gg 0\} \subseteq \mathcal{P}_F.$$

Remark 7.2. We have

$$\begin{aligned}\mathcal{P}^+_{F,\mathfrak{m}} &= \{\langle\alpha\rangle \,|\, \alpha \in F^\times,\ \alpha \gg 0,\ \alpha \overset{\times}{\equiv} 1 \ (\mathrm{mod}\ \mathfrak{m})\} \\ &= \left\{ \left\langle \frac{\alpha}{\beta} \right\rangle \;\middle|\; \frac{\alpha}{\beta} \gg 0,\ \alpha, \beta \in \mathcal{O}_F \ \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \ (\mathrm{mod}\ \mathfrak{m}) \right\}.\end{aligned}$$

The proof of these equalities is left as an exercise in exercise sheet 6.

Similarly, we define the *ray modulo* $\mathfrak{m}$ to be

$$\mathcal{P}_{F,\mathfrak{m}} = \{\langle\alpha\rangle \,|\, \alpha \in F^\times,\ \alpha \overset{\times}{\equiv} 1 \ (\mathrm{mod}\ \mathfrak{m})\}.$$

The total positivity condition of $\mathcal{P}^+_{F,\mathfrak{m}}$ can be interpreted as a congruence condition for the primes at infinity.

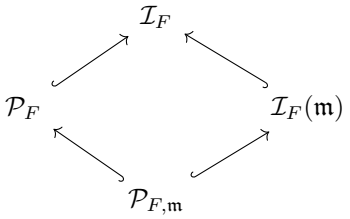
Definition 7.3. (Ray class group) We may finally define the *Ray class group of* F for $\mathfrak{m}$ to be

$$\mathcal{R}_{F,\mathfrak{m}} = \mathcal{I}_F(\mathfrak{m}) \Big/ \mathcal{P}_{F,\mathfrak{m}}.$$

while the *strict (or narrow) ray class group* of F is

$$\mathcal{R}^+_{F,\mathfrak{m}} = \mathcal{I}_F(\mathfrak{m}) \Big/ \mathcal{P}^+_{F,\mathfrak{m}}.$$

The links between those different groups are summed up in the following diagram.



In the base setting, we recover the usual definition, which confirms that this is indeed a generalization of the Galois group.

Example 7.4. Let $F = \mathbb{Q},\ \mathfrak{m} = m\mathbb{Z}$. Using (7.2), we have

$$\mathcal{P}^+_{\mathbb{Q},\mathfrak{m}} = \left\{ \left\langle \frac{a}{b} \right\rangle \middle| \, a, b \equiv 1 \,(\mathrm{mod}\ m),\ \frac{a}{b} > 0 \right\}.$$

An isomorphism $\mathcal{P}^+_{\mathbb{Q},\mathfrak{m}} \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ is given by the map induced by

$$\begin{array}{ccc} \mathcal{I}_{\mathbb{Q}}(m\mathbb{Z}) & \longrightarrow & \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \\ \left\langle \frac{a}{b} \right\rangle & \longmapsto & ab^{-1} \end{array}.$$

Example 7.5. Let $\mathfrak{m} = \mathcal{O}_F$. One has

$$\begin{aligned} \mathcal{R}_{F,\mathfrak{m}} &= \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F, \text{ the ordinary ideal class group} \\ \mathcal{R}^+_{F,\mathfrak{m}} &= \mathcal{I}_F/\mathcal{P}^+_F = \mathcal{C}_F, \text{ the strict (narrow) ideal class group.} \end{aligned}$$

Therefore the ray class groups are indeed generalizations of both the Galois group and the class group.

7.3 Class fields

We now will define the field extension analog to the cyclotomic extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$, named the *class field*.

We first fix some group $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$. Any such group is named an *ideal group mod* $\mathfrak{m}$.

Theorem 7.6. ***(Existence and Definition of Class field)*** *Let $\mathcal{H}$ be an ideal group mod $\mathfrak{m}$. There is a unique Galois extension K/F such that*

$$\begin{aligned} \mathcal{S}_{K/F} &= \{ \textit{primes } \mathfrak{p} \textit{ of } \mathcal{O}_F \mid \mathfrak{p} \textit{ splits completely in } K/F \} \\ &\approx \{ \textit{primes } \mathfrak{p} \textit{ of } \mathcal{O}_F \mid \mathfrak{p} \in \mathcal{H} \}. \end{aligned}$$

We call such an extension the class field of $\mathcal{H}$. (Recall that for two sets $\mathcal{S}, \mathcal{T}$, one writes $\mathcal{S} \approx \mathcal{T}$ if and only if they differ by a set with Dirichlet density zero.)

Proof. The existence part of the theorem is one of the main results of Class Field Theory and will be proven later in the course. For now, we will only prove the uniqueness. Recall that the Dirichlet density of a set $\mathcal{S}$ of primes is

$$\delta_F(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} \frac{1}{N\mathfrak{p}^s}}{\log\left(\frac{1}{s-1}\right)}.$$

We moreover know from exercise sheet 6, exercise 2 that $\delta_F(\mathcal{S}_{K/F}) = [K:F]^{-1}$. Let $K_1, K_2/F$ be two field extensions satisfying the theorem's condition. The composite field $K = K_1K_2$ is also a class field. We know from exercise 3 of Exercises week 6[3] that

$$\mathcal{S}_{K/F} = \mathcal{S}_{K_1/F} \cap \mathcal{S}_{K_2/F} \approx \{\mathfrak{p} \text{ of } F : \ \mathfrak{p} \in \mathcal{H}\}$$

which yields

$$\mathcal{S}_{K/F} \approx \mathcal{S}_{K_1/F} \approx \mathcal{S}_{K_2/F}$$

and thus $[K:F] = [K_1:F] = [K_2:F]$ and $K = K_1 = K_2$.

□

Remark 7.7. Notice that the class field is unique up to *strict* equality, not up to isomorphism.

Example 7.8. Let $F = \mathbb{Q}$ and $\mathfrak{m} = m\mathbb{Z}$. We have

$$\begin{aligned} \{p\mathbb{Z} \mid p\mathbb{Z} \in \mathcal{P}^+_{\mathbb{Q},m\mathbb{Z}}\} &\overset{\text{def}}{=} \{p\mathbb{Z} \mid \ p \cong 1 \,(\mathrm{mod}\ m),\ p > 0\} \\ &= \{p\mathbb{Z} \mid p \text{ splits completely in } \mathbb{Q}(\xi_m)\} \end{aligned}$$

[3]The exercise is with $F = \mathbb{Q}$, but a similar argument holds for the general case.

7.4 Weber characters

We now come to the generalization of the Dirichlet character, which we will name *Weber characters*. It is natural to define a Weber character to be a group character $\chi\colon \mathcal{R}^+_{F,\mathfrak{m}} \to \mathbb{C}^\times$. We also define analogously an L-function for these generalized Dirichlet characters

$$L_{\mathfrak{m}}(s,\chi) = \sum_{\substack{\mathfrak{a}\in\mathcal{I}_F(\mathfrak{m})\\ \mathfrak{a}\text{ integral}}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s}.$$

In the base setting, we used the fact that $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ is finite to get that any character χ must take value in the unit circle, a useful fact to ensure convergence. As it turns out, a similar argument works in our generalized setting, as $\mathcal{R}^+_{F,\mathfrak{m}}$ is also finite.

Theorem 7.9. *$\mathcal{R}^+_{F,\mathfrak{m}}$ is a finite group*

Proof. See Childress, Proposition 3.2.1, p.50 or exercise 1 of the exercise sheet of week 7. An explicit formula for the cardinal of $\mathcal{R}^+_{F,\mathfrak{m}}$ depending on F and $\mathfrak{m}$ is even provided. □

Hence $L_{\mathfrak{m}}(s,\chi)$ is well-defined. The following summarizes these new definitions.

Base case	***General case***
$F = \mathbb{Q}$	F algebraic number field
$\mathfrak{m} = m\mathbb{Z}$	$\mathfrak{m}$ non-zero integral ideal of $\mathcal{O}_F$
Galois group $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$	ray class group $\mathcal{R}^+_{F,\mathfrak{m}}$
of the cycl. extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$	Class field K/F
Dirichlet characters / L-functions.	Weber characters / L-functions.

We are now able to write the desired generalization of theorem (7.1).

Theorem 7.10. ***(Generalization of Dirichlet's theorem on Primes in Arithmetic Progressions)*** *Given $\mathfrak{a} \in \mathcal{I}_{F,\mathfrak{m}}$, the set*

$$\mathcal{S}_{\mathfrak{a},\mathfrak{m}} = \left\{ \textit{primes } \mathfrak{p} \textit{ of } \mathcal{O}_F \mid \mathfrak{p} \equiv \mathfrak{a} \textit{ in } \mathcal{R}^+_{F,\mathfrak{m}} \right\}$$

is infinite.

7.5 Towards the proof of Theorem 7.10

We first enumerate some facts about the newly defined L-functions.

(1.) The Euler product formula holds for $\mathrm{Re}(s) > 1$.

$$L_{\mathfrak{m}}(s,\chi) = \sum_{\substack{\mathfrak{a}\in\mathcal{I}_F(\mathfrak{m})\\ \mathfrak{a}\text{ integral}}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \left(1 - \chi(\mathfrak{p})N\mathfrak{p}^{-s}\right)^{-1}.$$

(2.) For $\chi \neq \chi_0$, $L_{\mathfrak{m}}(s,\chi)$ is analytic.

(3.) $L_{\mathfrak{m}}(s,\chi_0)$ has a simple pole at $s = 1$ and is analytic elsewhere.

The proof of these facts are generalizations of the arguments used to prove their equivalent for Dirichlet L-functions.

Proposition 7.11. *Let $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$ and $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$. If for all Weber characters $\chi \neq \chi_0$ that are trivial on $\mathcal{H}$, we have $L_{\mathfrak{m}}(1,\chi) \neq 0$, then*

$$\delta_F\left(\{\textit{primes } \mathfrak{p} \textit{ of } \mathcal{O}_F \mid \mathfrak{p} \in \mathfrak{a}\mathcal{H}\}\right) = \frac{1}{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}.$$

Proof. Using the Euler product formula for $L_{\mathfrak{m}}(s,\chi)$ and taking the log, we have

$$\log L_{\mathfrak{m}}(s,\chi) = -\sum_{p\nmid\mathfrak{m}} \log\left(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}\right) = \sum_{\mathfrak{p}\nmid\mathfrak{m}}\sum_{n=1}^{\infty}\frac{\chi(\mathfrak{p})^n N\mathfrak{p}^{-ns}}{n}$$

where we took the Taylor expansion of $\log(1-x)$ for the second equality. Splitting the sum yields

$$= \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})N\mathfrak{p}^{-\mathfrak{s}} + \sum_{\mathfrak{p}\nmid\mathfrak{m}}\sum_{n=2}^{\infty}\frac{\chi(\mathfrak{p})^n N\mathfrak{p}^{-ns}}{n} \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}}\chi(\mathfrak{p})N\mathfrak{p}^{-s}.$$

Since χ vanishes on $\mathcal{H}$, it can be seen as a character of $\mathcal{I}_F(\mathfrak{m})\big/_{\mathcal{H}}$. Given a fixed prime $\mathfrak{p}$ of $\mathcal{O}_F$, we have the following orthogonal relation

$$\sum_{\chi}\chi(\mathfrak{a})^{-1}\chi(\mathfrak{p}) = \begin{cases} 0 & \text{if } \mathfrak{p}\notin\mathfrak{a}\mathcal{H} \\ [\mathcal{I}(\mathfrak{m}):\ \mathcal{H}] & \text{if } \mathfrak{p}\in\mathfrak{a}\mathcal{H}\end{cases}$$

where the sum is taken over characters of $\mathcal{I}_F(\mathfrak{m})\big/_{\mathcal{H}}$. Let

$$\beta_\chi(s) = \sum_{\mathfrak{p}\nmid\mathfrak{m}}\sum_{n=2}^{\infty}\frac{\chi(\mathfrak{p})^n N\mathfrak{p}^{-ns}}{n}.$$

Using the definition and the orthogonal relation, we get

$$\sum_{\chi}\chi(\mathfrak{a})^{-1}\log L_{\mathfrak{m}}(s,\chi) = \sum_{\chi}\chi(\mathfrak{a})^{-1}\left[\sum_{\mathfrak{p}\nmid\mathfrak{m}}\chi(\mathfrak{p})N\mathfrak{p}^{-s}+\beta_\chi(s)\right] \tag{3}$$

$$\sum_{\chi}\chi(\mathfrak{a})^{-1}\left[\log L_{\mathfrak{m}}(s,\chi)-\beta_\chi(s)\right] = \sum_{\mathfrak{p}\in\mathfrak{a}\mathcal{H}}\left[\mathcal{I}_F(\mathfrak{m}):\ \mathcal{H}\right]N\mathfrak{p}^{-s}. \tag{4}$$

We write

$$\mathcal{S} = \{\text{primes } \mathfrak{p} \text{ of } \mathcal{O}_F \mid \mathfrak{p}\in\mathfrak{a}\mathcal{H}\}.$$

Our goal is to show that

$$\delta_F(\mathcal{S}) = \lim_{s\to1^+}\frac{\sum_{\mathfrak{p}\in\mathcal{S}}N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{[\mathcal{I}_F(\mathfrak{m}):\ \mathcal{H}]}.$$

Let $h = [\mathcal{I}_F(\mathfrak{m}):\ \mathcal{H}]$. By rearranging (4), we get

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{S}}N\mathfrak{p}^{-s} - \frac{1}{h}\log\left(\frac{1}{s-1}\right) =& \frac{1}{h}\sum_{\chi\neq\chi_0}\chi(\mathfrak{a})^{-1}\left[\log L_{\mathfrak{m}}(s,\chi)-\beta_\xi(s)\right] \\ &+\frac{1}{h}\log\left[(s-1)L_{\mathfrak{m}}(s,\chi_0)\right]-\frac{1}{h}\beta_{\chi_0}(s).\end{aligned}$$

Notice that the RHS is bounded as $s\to1^+$, since by assumption $L_{\mathfrak{m}}(1,\chi)\neq0$ for every Weber characters different from χ_0 vanishing on $\mathcal{H}$, and we know for a fact that $L_{\mathfrak{m}}(s,\chi_0)$ has a simple pole at $s=1$. By dividing by $\log\left(\frac{1}{s-1}\right)$ on both sides and using the fact that $\lim_{s\to1^+}\log\left(\frac{1}{s-1}\right)=\infty$, we get

$$\frac{\sum_{\mathfrak{p}\in\mathcal{S}}N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)} - \frac{1}{h} \to 0 \quad \text{as} \quad s\to1^+.$$

This amounts to $\delta_F(\mathcal{S}) = \frac{1}{h} = \frac{1}{[\mathcal{I}_F(\mathfrak{m}:\ \mathcal{H})]}$, as desired.

□

Remark 7.12. In the same setting as in the proposition, if $\mathcal{H} = \mathcal{P}^+_{F,\mathfrak{m}}$, one has

$$\mathcal{S} = \mathcal{S}_{\mathfrak{a},\mathfrak{m}}, \quad \delta_F(\mathcal{S}) = \frac{1}{|\mathcal{R}^+_{F,\mathfrak{m}}|}.$$

The next step is to show that the assumption are satisfied, namely that $L_{\mathfrak{m}}(1,\chi) \neq 0$ whenever $\chi \neq \chi_0$ vanishes on $\mathcal{H}$. It is nearly accomplished by the next theorem.

Theorem 7.13. *Suppose K/F is a Galois extensions, and $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$. Suppose there is some set of primes $\mathcal{J} \subseteq \mathcal{H}$, with $\delta_{K/F} \approx \mathcal{J}$. Then*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [K : F]$$

and $L_{\mathfrak{m}}(1,\chi) \neq 0$ whenever $\chi \neq \chi_0$ and χ is trivial on $\mathcal{H}$.

Proof. Let $m(\chi) = \operatorname{ord}_{s=1}(L_{\mathfrak{m}}(s,\chi))$. We know that $m(\chi) \geq 0$ for $\chi \neq \chi_0$ and $m(\chi_0) = -1$.

Again, since χ is trivial on $\mathcal{H}$, we may view it as a character of $\mathcal{I}_F(\mathfrak{m})/\mathcal{H}$. There is some non-zero constant $a \in \mathbb{C}$ such that

$$\prod_{\chi} L_{\mathfrak{m}}(s,\chi) = a(s-1)^{\sum_\chi m(\chi)} + \cdots \sim a(s-1)^{\sum_\chi m(\chi)}$$

where the product is taken over characters of $\mathcal{I}_F(\mathfrak{m})/\mathcal{H}$. Taking log of both sides yields

$$\sum_{\chi} \log L_{\mathfrak{m}}(s,\chi) \sim \left(\sum_{\chi} m(\chi)\right) \log(s-1) = -\left(\sum_{\chi} m(\chi)\right) \log\left(\frac{1}{s-1}\right).$$

We have seen in the previous proof that

$$\log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s}.$$

Hence

$$\sum_{\chi} \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p} \in \mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\, N\mathfrak{p}^{-s}$$

which yields

$$\sum_{\mathfrak{p} \in \mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\, N\mathfrak{p}^{-s} \sim -\left(\sum_{\chi} m(\chi)\right) \log\left(\frac{1}{s-1}\right). \tag{5}$$

Splitting the sum on the LHS gives us

$$\sum_{\mathfrak{p} \in \mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\, N\mathfrak{p}^{-s} = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \left(\sum_{\mathfrak{p} \in \mathcal{J}} N\mathfrak{p}^{-s} + \sum_{\mathfrak{p} \in \mathcal{H} \setminus \mathcal{J}} N\mathfrak{p}^{-s}\right)$$

Dividing by $\log\left(\frac{1}{s-1}\right)$ on both sides of (5) and letting $s \to 1^+$, we get

$$-\left(\sum_{\chi} m(\chi)\right) = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\, \delta_F(\mathcal{J}) + [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{H} \setminus \mathcal{J}} N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)}$$

By assumption, $\mathcal{J} \approx \mathcal{S}_{K/F}$. Moreover, since $\delta_F(\mathcal{S}_{K/F})$ exists and the LHS is finite, the limit on the RHS must exist. Hence one has

$$\begin{aligned} -\left(\sum_{\chi} m(\chi)\right) &= [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\, \delta_F(\mathcal{S}_{K/F}) + [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \,(\text{some finite nonnegative constant}) \\ &\geq [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\, \delta_F(\mathcal{S}_{K/F}) = \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]}. \end{aligned}$$

Since $m(\chi) \geq 0$ and $m(\chi_0) = -1$, we get

$$1 \geq 1 - \sum_{\chi \neq \chi_0} m(\chi) \geq \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]} > 0. \tag{6}$$

In particular

$$0 \geq -\sum_{\chi \neq \chi_0} m(\chi) > -1$$

which forces $m(\chi) = 0$ for all $\chi \neq \chi_0$. Hence $-\left(\sum_\chi m(\chi)\right) = 1$ and $L_{\mathfrak{m}}(1, \chi)$ has a non-zero constant term when expanded in powers of $(s-1)$. In particular $L_{\mathfrak{m}}(1, \chi) \neq 0$ for every $\chi \neq \chi_0$. On the other hand, one has from (6) that

$$1 \geq \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]}$$

which gives $[K : F] \geq [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]$, as desired.

□

Remark 7.14. If we assume the class field of $\mathcal{H}$ over F to exist and let

$$\mathcal{J} = \{\text{primes } \mathfrak{p} \text{ in } \mathcal{O}_F \text{ such that } \mathfrak{p} \in \mathcal{H}\} \subseteq \mathcal{H},$$

one has $\mathcal{J} \approx \mathcal{S}_{K/F}$ and we may prove the generalization of the Theorem on Primes in Arithmetic Progressions (Theorem 7.10) using this last result.

7.6 Exercises week 7

1. The explicit formula for the strict ray class number modulo $\mathfrak{m}$ is

$$|\mathcal{R}^+_{F,\mathfrak{m}}| = \frac{h_F 2^{r_1} \varphi(\mathfrak{m})}{[\mathcal{U}_F : \mathcal{U}^+_{F,\mathfrak{m}}]} \tag{7}$$

   where :

   - h_F is the class number
   - r_1 is the number of real embeddings
   - $\varphi(\mathfrak{m})$ is the cardinal of $\left(\mathcal{O}_F \big/ \mathfrak{m}\right)^\times$
   - $\mathcal{U}_F = \mathcal{O}_F^\times$, the units of $\mathcal{O}_F$
   - $\mathcal{U}^+_{F,\mathfrak{m}} = \{\varepsilon \in \mathcal{U}_F \mid \varepsilon \gg 0, \varepsilon \equiv 1 \pmod{\mathfrak{m}}\}$

   (a) Let $F = \mathbb{Q}(\sqrt{3})$ and $\mathfrak{m} = \mathcal{O}_F$. Compute the ray strict ray class number and deduce what the ray class group $\mathcal{R}^+_{\mathbb{Q}(\sqrt{3}),\mathbb{Z}[\sqrt{3}]}$ is up to isomorphism.

   (b) Same question for $F = \mathbb{Q}(i)$, $\mathfrak{m} = \mathcal{O}_F$.

   (c) Compare $\mathcal{R}^+_{\mathbb{Q}(i),\mathbb{Z}[i]}$ and $\mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}$. How are they related ?

2. Let F be a number field and let $\mathfrak{n}, \mathfrak{m}$ be (not necessarily distinct) ideals of $\mathcal{O}_F$. Is it possible to find $\mathcal{H}_1 \neq \mathcal{H}_2$ with $\mathcal{P}^+_{F,\mathfrak{n}} \leq \mathcal{H}_1 < \mathcal{I}_F(\mathfrak{n})$ and $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H}_2 < \mathcal{I}_F(\mathfrak{m})$ such that they have the same class field over F ?

3. Let K be the class field of $\mathcal{H}$ over F where $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$.
   Prove that $[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] = [K : F]$.

4. Let F be a number field. If we take $\mathfrak{m} = \mathcal{O}_F$, then the class field of $\mathcal{P}_{F,\mathfrak{m}}$ over F is called the *Hilbert class field*.

   (a) Find the Hilbert class field of $\mathbb{Q}$.

   (b) Find the Hilbert class field of $\mathbb{Q}(i)$.

5. *(Algebraic bonus !)* Prove that there is an exact sequence

$$0 \longrightarrow \mathcal{O}_F^\times \hookrightarrow F^{\mathfrak{m}} \longrightarrow \mathcal{I}(\mathfrak{m}) \twoheadrightarrow \mathcal{C}_F \longrightarrow 0$$

   where $F^{\mathfrak{m}} := \{a \in F^\times \mid \langle a \rangle \in \mathcal{I}_F(\mathfrak{m})\}$.

   This is lemma 1.1 on page 144 of the book Class Field Theory*, by J. S. Milne. You can refer to it for a proof !*

8 Main theorems of Class Field Theory and Idèles

8.1 Universal Norm Index Inequality

Recall from last chapter :

Corollary 8.1. *Let F be a number field, K/F a class field for $\mathcal{H}$, where $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$. Then*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] = [K : F].$$

We use the following notation:

$$\mathcal{N}_{K/F}(\mathfrak{m}) = \{\mathfrak{p} \in \mathcal{I}_F(\mathfrak{m}) |\ \mathfrak{p} = N_{K/F}(\mathfrak{U}) \text{ for some } \mathfrak{U} \in \mathcal{I}_K\}.$$

Theorem 8.2. *(Universal Norm Index Inequality) Let K/F be a Galois extension of number fields, and $\mathcal{H} = \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})$. Then*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [K : F].$$

Proof. Let $\tau = \mathcal{S}_{K/F} \cap \mathcal{I}_F(\mathfrak{m})$. It is enough to show that τ is a subgroup of $\mathcal{H}$, because then by our previous corollary

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \leq [\mathcal{I}_F(\mathfrak{m}) : \tau] = [K : F].$$

Let $\mathfrak{p} \in \tau$. Since $\mathfrak{p} \in \mathcal{S}_{K/F}$, we have $N_{K/F}(\mathfrak{p}) = \mathfrak{p}^{f(\mathfrak{p}/\mathfrak{p})} = \mathfrak{p}$, which shows $p \in \mathcal{H}$. □

One may ask themselves when the reverse equality holds. The following theorem answers our question, but it uses techniques that will be developed later, so we omit the proof for now.

Theorem 8.3. *(Global Cyclic Norm Index Inequality) Let K/F be a cyclic extension and $\mathfrak{m}$ such that for each ramifying prime $\mathfrak{p}$ of K/F, $\mathfrak{p}^{k_\mathfrak{p}}$ divides $\mathfrak{m}$ for $k_\mathfrak{p}$ large enough. Then*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})] \geq [K : F].$$

8.2 The three main theorems of Class field theory

We now state 3 central theorems in class field theory, for which the proofs will require some theory that will be introduced in the following chapters.

Theorem 8.4. *(Existence) For all $\mathcal{H}$ with $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$, there exists a class field K/F for $\mathcal{H}$.*

In particular, this theorem provides the missing step in a precedent proof to show $\mathcal{L}_\mathfrak{m}(1, \mathcal{X}) \neq 0\ \forall \mathcal{X} \neq \mathcal{X}_0$.

Theorem 8.5. *(Completeness) For any abelian extension K/F, there exists $\mathfrak{m}$ and $\mathcal{H}$ with $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$ such that K is the class field over F for $\mathcal{H}$.*

Theorem 8.6. *(Isomorphy) If K is the class field over F for $\mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$, then*

$$Gal(K/F) \cong \mathcal{I}_F(\mathfrak{m})/\mathcal{H}.$$

The isomorphism is given by the Artin map, which will be introduced later.

Example 8.7. Let $m \in \mathbb{Z}$, and K be the class field over $\mathbb{Q}$ for $\mathcal{H} = \mathcal{P}_{\mathbb{Q},(m)}$. Then by Isomorphy

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{I}_\mathbb{Q}((m))/\mathcal{P}^+_{\mathbb{Q},(m)}.$$

As seen in example 2.8 in week 6, we have

$$\mathcal{I}_\mathbb{Q}((m))/\mathcal{P}^+_{\mathbb{Q},(m)} \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

By unicity this gives $K = \mathbb{Q}(\zeta_m)$, which we already knew.

8.3 Correspondence

The previous 3 theorems allow us to get the following correspondence:

$$\{\text{Finite abelian extentions /F}\} \leftrightarrow \{\mathcal{H} \text{ such that } \mathcal{P}^+_{F,\mathfrak{m}} < \mathcal{H} < \mathcal{I}_F(\mathfrak{m})\}.$$

It is given by :

$$K \xrightarrow{existence} \mathcal{H}_K$$
$$K_{\mathcal{H}} \xleftarrow{completeness} \mathcal{H}.$$

Moreover, it is order-reversing:

$$\begin{array}{ccc} L & \text{———} & \mathcal{H}_L \\ \uparrow & & \downarrow \\ K & \text{———} & \mathcal{H}_K \\ \uparrow & & \downarrow \\ F & \text{———} & \mathcal{I}_F(\mathfrak{m}) \end{array}$$

and we have by Isomorphy

$$\mathrm{Gal}(L/F) \cong \mathcal{I}_F(\mathfrak{m})/\mathcal{H}_L$$

$$\mathrm{Gal}(K/F) \cong \mathcal{I}_F(\mathfrak{m})/\mathcal{H}_K.$$

We get from this correspondence the famous result:

Corollary 8.8. *(Kronecker-Weber) Let $F/\mathbb{Q}$ be abelian. Then $F \subseteq \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}$.*

Proof. By our previous correspondence, we have the following:

$$\begin{array}{ccc} K & \text{———} & \mathcal{P}^+_{\mathbb{Q},(m)} \\ \uparrow & & \downarrow \\ F & \text{———} & \mathcal{H}_F \\ \uparrow & & \downarrow \\ \mathbb{Q} & \text{———} & \mathcal{I}_{\mathbb{Q}}((m)) \end{array}$$

But then,

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{I}_{\mathbb{Q}}((m))/\mathcal{P}^+_{\mathbb{Q},(m)} \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

By unicity of the class field, we get $K = \mathbb{Q}(\zeta_m)$. □

8.4 Hilbert class field:

We finish this by introducing the Hilbert Class field and state a few facts about it.

Definition 8.9. The Hilbert Class field is the ray class field when $\mathfrak{m} = \mathcal{O}_F$. We will write F_1 for the Hilbert Class Field for F.

1) By isomorphy,

$$\mathrm{Gal}(F_1/F) \cong \mathcal{I}_F(\mathcal{O}_F)/\mathcal{P}_{F,\mathcal{O}_F} \cong \mathcal{I}_F/\mathcal{P}_F \cong \mathcal{C}_F.$$

2) The Hilbert class field is the maximal unramified abelian extension over F.

3) Any $\mathfrak{q} \in \mathcal{I}_F$ becomes principal in F_1. This is done in the second problem of this week's exercise sheet.

4) Let F_n be the Hilbert class field over F_{n-1}. Then the tower $F \subseteq F_0 \subseteq F_1 \subseteq ...$ does not necessarily stabilize.

8.5 Idèlic theory

Definition 8.10. An absolute value on a number field F is a map $||.|| \to [0, \infty)$ such that

1. $||0|| = 0$.
2. $||.||_{|_{F^\times}}$ is a multiplicative group homomorphism.
3. $||1 + x|| \leq c$, whenever $||x|| \leq 1$ for some $c \geq 1$.

This induces a metric topology on F.

Remark 8.11. For any such $||.||$, there exists some $\lambda \in \mathbb{R}_+^\times$ such that $||.||^\lambda$ satisfies the triangular inequality. This is problem 3 of this week's exercise sheet.

We say that two norms are equivalent if they induce the same topology. Notice that $||.||$ and $||.||^\lambda$ are equivalent by taking balls of radius $\epsilon^{\pm\lambda}$ to get from one basis to the other.

Definition 8.12. A place of F is an equivalence class (with the notion stated above) of non-trivial absolute values. We denote the set of places on F by V_F.

There are 3 types of places:

1. Finite places: places containing $||\alpha||_\mathfrak{p} = N\mathfrak{p}^{-\mathrm{ord}_\mathfrak{p}(\alpha)}$, for some $\mathfrak{p}$ non-zero prime ideal of $\mathcal{O}_F$ of F. We write $v_\mathfrak{p} := v$ Theses are also sometimes referred to as non-Archimedean places, or discrete places.

   We denote $\mathfrak{p}_v$ the prime associated to it in $\mathcal{O}_F$, and sometimes write ord_v instead of $\mathrm{ord}_{\mathfrak{p}_v}$ to lighten notation.

2. Infinite real places: (or real Archimedean) places such that $||\alpha||_\sigma = |\sigma(\alpha)|_\mathbb{R}$ for some σ a real embedding of F, and in this case we write $v_\sigma := v$.

3. Infinite imaginary places: places containing $||\alpha||_\sigma = |\sigma(\alpha)|_\mathbb{C}^2 = |\sigma(\alpha)|_\mathbb{C} \cdot |\bar{\sigma}(\alpha)|_\mathbb{C}$, for σ an imaginary embedding of F, and again we write $v_\sigma := v$.

   Note that there is a single place for each pair of conjugate embeddings (they are equivalent).

For any $v \in V_F$, we denote $||.||_v$ a representative for the absolute value described in the 3 previous sub-points. Notice that by our previous remark, we can always choose such representative to satisfy the triangular inequality.

Theorem 8.13. *(Product formula) For any $x \in F^\times$, with F a number field:*

$$\prod_{v \in V_F} ||x||_v = 1.$$

A proof an be found in a paper by Keith Conrad: "Ostrowski for number fields".

Example 8.14. Let $F = \mathbb{Q}(\sqrt{3})$. It has two real embeddings:

$$\sigma_1 : \sqrt{3} \mapsto \sqrt{3}$$

$$\sigma_2 : \sqrt{3} \mapsto -\sqrt{3}.$$

The field F has two real places, v_{σ_1} and v_{σ_2}, both real, and no imaginary places.

Example 8.15. Let $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{3})$. It has 4 embeddings:

$$\sigma_{11} : \sqrt{3} \mapsto \sqrt{3},\ i \mapsto i$$

$$\sigma_{12} : \sqrt{3} \mapsto \sqrt{3},\ i \mapsto -i$$

$$\sigma_{21} : \sqrt{3} \mapsto -\sqrt{3},\ i \mapsto i$$

$$\sigma_{22} : \sqrt{3} \mapsto -\sqrt{3},\ i \mapsto -i.$$

The field K has two places: $v_{\sigma_{11}} = v_{\sigma_{12}}$ and $v_{\sigma_{21}} = v_{\sigma_{22}}$, both imaginary. We get the following:

- The prime 3 ramifies in $\mathbb{Q}(\zeta_3)/\mathbb{Q}$. Moreover, theorem 2.2 in chapter 2 of Childress gives us that the ramification index of 3 in $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is $|X_3|$. Recall that X_3 are the characters modulus 3 of $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^\times$, so $|X_3| = |(\mathbb{Z}/3\mathbb{Z})^\times| = 2$ is the ramification index of 3 in $\mathbb{Q}(\zeta_3)/\mathbb{Q}$.
- In $\mathbb{Q}(i)/\mathbb{Q}$, 3 is inert (example 10 page 27 of Childress).
- We get $e = f = 2$ for 3 in $K/\mathbb{Q}$, because $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(i)$. This implies that $p = \sqrt{-3}$ is prime in $\mathcal{O}_K$, because $3 = -p^2$.

We can now do the following computations:

$$||3||_p = N_p^{-\mathrm{ord}_p(3)} = 9^{-2}$$
$$||3||_{\sigma_{11}} = ||3||_{\sigma_{21}} = 9.$$

This agrees with the product formula:

$$\prod_{v \in V_K} ||3||_v = ||3||_p \cdot ||3||_{\sigma_{11}} \cdot ||3||_{\sigma_{21}} = 1.$$

Completion:

Let F be a number field, and $v \in V_F$ a place. We may complete F with respect to v, and we denote this completion F_v.

Remark 8.16. We define $\iota_v : F \hookrightarrow F_v$ an embedding of F into F_v for each place v. Here are a few observations about ι_v:

- The map ι_v is continuous if F is given the topology from $||.||_v$.
- With respect to the previous topology, $\iota_v(F)$ is dense in F_v.
- If $\alpha \neq 0$, $\iota_v(\alpha) \neq 0$ $\forall v \in V_F$.
- For all but finitely many of the places v, $\iota_v(\alpha)$ is a unit of F_v.

Definition 8.17. Units of a place:
For an infinite place v, it is straightforward: it is $F_v^\times$.
For a finite place, the units are $\mathcal{U}_v = \mathcal{O}_{F_v}^\times$, elements of absolute value 1.

8.6 A little (Group) Topology

We make a small detour towards topological groups:

Definition 8.18. A topological group G is a group that is also a topological space, with the multiplication and inverse operations being continuous.

Proposition 8.19. *Let G be a topological group, and fix $g \in G$. Define*

$$f_g : x \mapsto gx.$$

Then f_g is a homeomorphism, with inverse $f_{g^{-1}}$.

Proof. Follows directly from continuity of left multiplication. □

This makes G a homogeneous space, a space where for every two points of the space, there exists a homeomorphism that sends one to the other.
One can get new toplogical spaces from subgroups: for a subgroup $H \leq G$, we get the set G/H with the topology induced by the cosets of H. If H is normal, we have in our hands a topological group.

Example 8.20. Let $p \in \mathbb{Z}$ be prime. Then $(\mathbb{Z}_p, +)$, forms a topological group. Moreover, it is is compact and totally disconnected. (Recall that $\mathbb{Z}_p = \{z \in \mathbb{Q}_p |\ |z|_p \leq 1\}$)

- It is a topological group by usual metric space arguments:

$$|x + y - (a + b)| \leq \max(|x - a|, |y - b|).$$

- Compactness: Metric spaces are compact if and only if they are complete and totally bounded, ie for any $\epsilon > 0$, there exists finitely many open balls of radius ϵ covering $\mathbb{Z}_p$.

  We already know that $\mathbb{Z}_p$ is complete (it is a closed subset of $\mathbb{Q}_p$, which is complete). We show it is totally bounded using the following short exact sequence:

  $$0 \longrightarrow \mathbb{Z}_p \xrightarrow[[\cdot p^n]]{} \mathbb{Z}_p \xrightarrow[[\pi_n]]{} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

  with

  $$\pi_n : (a_0, a_1, ...) \mapsto a_0 + a_1 p + ... + a_{n-1}p^{n-1}.$$

  The exact sequence gives $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, a finite group. This means that there are finitely many cosets of $p^n\mathbb{Z}_p$. Taking $z \in \mathbb{Z}_p$, observe that every coset is a closed ball:

  $$z + p^n\mathbb{Z}_p = \{a \in \mathbb{Z}_p |\ a - z \in p^n\mathbb{Z}_p\} = \{a \in \mathbb{Z}_p |\ |a - z|_p \leq p^{-n}\}.$$

  We can thus finitely cover $\mathbb{Z}_p$ with open balls of radius bigger than p^{-n}. Since n was arbitrary, this shows $\mathbb{Z}_p$ is totally bounded.

- Totally disconnected: We show that $\mathbb{Q}_p$ is totally disconnected instead. Since subspaces of totally disconnected spaces are totally disconnected, the result follows.

  Let $x, y \in \mathbb{Q}_p$, we set $d = d(x, y)$. Notice that $A := \{z \in \mathbb{Q}_p |\ |x - z| < d\}$ is an open ball in $\mathbb{Q}_p$ centered around x, and $y \notin A$. We see that A is open, and because in $\mathbb{Q}_p$ open balls are closed, we conclude that any connected subset of $\mathbb{Q}_p$ must have only one element.

  To see why open balls in $\mathbb{Q}_p$ are closed, notice that for $a \in \mathbb{Q}_p$, $r \in \mathbb{R}_{>0}$,

  $$B(a, r) = \{x \in \mathbb{Q}_p |\ |x - a|_p < r\} = \{x \in \mathbb{Q}_p |\ |x - a|_p < p^{-n}\} = \{x \in \mathbb{Q}_p |\ |x - a|_p \leq p^{-n+1}\}$$

  for n the smallest integer such that $r < p^{-n}$.

We now introduce Idèles:

8.7 Idèles

Definition 8.21. An Idèle of a number field F is an infinite vector $\mathbf{a} = (..., a_v, ...)_{v \in V_F}$ indexed by places, with each a_v an element of the corresponding completion of F by v. Furtheremore, it requires that for infinite places $a_v \in F_v^\times$, and for all but finitely-many finite places v, $a_v \in \mathcal{U}_v$ (recall $\mathcal{U}_v$ are the elements of norm 1 in the completion of F by the place v).

The following set, called the set of Idèles of F, forms a multiplicative group

$$J_F = \underline{\prod_v} F_v^\times$$

but we will not endow it with the product topology ($\underline{\prod}$ indicates that we are not using the standard product topology). More precisely, we will need a special topology making it locally compact, and wish for the following subspace

$$\mathcal{E}_F = \prod_{v \in V_F} \mathcal{U}_v$$

to be a topological subgroup, for which the subspace topology agrees with the standard product topology.

Both theses conditions will determine the topology we need, called the restricted topological product.

Definition 8.22. (Restricted product topology) Let $\{B_i\}_{i \in J}$ be a family of topological spaces, such that for all but finitely many $i \in J$, we are given in advance open sets $A_i \subseteq B_i$. Let

$$B = \{\{x_i\}_{i \in J} |\ x_i \in B_i \ \&\ x_i \in A_i \text{ for all but finitely many } i\}.$$

We define the restricted topological product on B by having the following sets to be a basis for the opens:

$$\{\prod_{i \in J} U_i \mid U_i \text{ open in } B_i \ \&\ U_i = A_i \text{ for all but finitely many } i\}.$$

For our Idèles group J_F, we let the opens A_i to be the $\mathcal{U}_v \subseteq F_v^\times$.

8.8 Exercises week 8

For this exercise sheet, recall that the Hilbert class field over F can be characterized as the maximal unramified abelian extension of F (unramified extension means each *prime* ideal in F is unramified in the extension).

1. Find the Hilbert class field over $\mathbb{Q}(\sqrt{15})$.

2. As mentioned in class, the Principal Ideal Theorem states that any ideal of a number field F becomes principal in its Hilbert class field F_1. This exercise is a partial proof of it, assuming one group theory key fact.

   (I) Let F_2 be the Hilbert class field over F_1. Show that F_2 is Galois over F.

   (II) Let $A := \mathrm{Gal}(F_2/F_1)$ and $G := \mathrm{Gal}(F_2/F)$. Show that $A = G' = [G, G]$ and that

   $$\gamma : \mathcal{I}_F/\mathcal{P}_F \longrightarrow \mathcal{I}_{F_1}/\mathcal{P}_{F_1} : \mathfrak{a}\mathcal{P}_F \mapsto (a\mathcal{O}_{F_1})\mathcal{P}_{F_1}$$

   is a well defined group homomorphism.

   (III) Let $V : G/G' \to G'$ (called the transfer map, ***V**erlagerung* in german) be the map making the following diagram commute.

   $$\begin{array}{ccc} \mathcal{C}_F & \xrightarrow{\cong} & G/G' \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle V} \\ \mathcal{C}_{F_1} & \xrightarrow[\cong]{} & G \end{array}$$

   Prove that the upper and lower morphisms are isomorphisms and show that proving the Principal Ideal Theorem amounts to proving the map V to be trivial.

   (IV) Artin was the one able to reduce our initial statement to the group theoretical problem of showing that V is trivial. Fortunately, there is a result in group theory (also called the Principal Ideal Theorem!) which precisely answers our needs.
   If G is a finite group and G' is its commutator subgroup, then the transfer $V : G/G' \to G'/(G')'$ is the trivial map.
   Using the previous points and this result, conclude.

3. We now recall the definition of *absolute value* on an algebraic number field F. It is a map

   $$\| \bullet \| : F \to [0, \infty)$$

   satisfying $\|0\| = 0$ and such that its restriction to $F^\times$ is an multiplicative group homeomorphism, satisfying

   $$\|1 + x\| \leq c, \quad \text{whenever } \|x\| \leq 1$$

   and some suitable constant c.
   For any such absolute value $\| \bullet \|$, show that there exists $\lambda \in \mathbb{R}_+^\times$ such that $\| \bullet \|^\lambda$ satisfies the triangular inequality, or equivalently $\| \bullet \|^\lambda$ is a standard absolute value, as defined for instance in in Chapter 1. of Childress' book.

4. Let $F = \mathbb{Q}(i)$ and $x = 2 - i$. Compute $\|x\|_v$, for all $v \in V_F$ and verify that the product formula $\prod_{v \in V_F} \|x\| = 1$ holds.

5. Let H be a subgroup of the topological group G. Show the following:

   (a) If H is open in G, then H is also closed.

   (b) If H is closed with finite index in G, then H is also open.

   (c) If G is compact and H is open in G, then $[G : H]$ is finite.

9 The Group of Idèles of a Number Field

9.1 Idèles recall

We recall that for each place v of a number field F, the completion F_v is a local field and $F_v^\times$ denotes its multiplicative group. For finite places v we set $\mathcal{U}_v = \mathcal{O}_v^\times$, while for infinite places we take $\mathcal{U}_v = F_v^\times$.

Definition 9.1. An idèle of a number field F is an infinite vector

$$a = (a_v)_{v \in V_F}$$

where $a_v \in F_v^\times$ for all v, and $a_v \in \mathcal{U}_v$ for all but finitely many v. The set of all idèles is denoted J_F, and it forms a group under componentwise multiplication.

Our goal is to equip J_F with a topology making it a locally compact topological group. This topology will not be the product topology, but the restricted product topology. Two conditions must hold:
1. the multiplication and inversion maps must be continuous;
2. the subspace topology on

$$\mathcal{E}_F := \prod_{v \in V_F} \mathcal{U}_v$$

must coincide with the product topology, where each $\mathcal{U}_v$ carries its usual metric topology.

To begin, note that multiplication by a fixed $a \in J_F$ is continuous: for all $x, y \in \mathcal{E}_F$,

$$|ax - ay|_v = |a|_v \, |x - y|_v,$$

so the map $x \mapsto ax$ is bi-Lipschitz and therefore a homeomorphism.
Moreover, for a finite place v, the set $\mathcal{O}_v^\times$ is an open (and closed) subset of $F_v^\times$. Indeed, since $|\cdot|_v$ is continuous and takes values in a discrete subset of $\mathbb{R}_{>0}$, we have

$$\mathcal{O}_v^\times = \{x \in F_v^\times : |x|_v = 1\} = |\cdot|_v^{-1}(\{1\}),$$

and $\{1\}$ is both open and closed in the image of $|\cdot|_v$.

We now present some general tools that help us analyze the local structure of idèles.

Proposition 9.2. *Let K be a complete field with respect to a discrete absolute value. Let $\mathcal{U}$ be its ring of integers and $\mathfrak{m}$ its maximal ideal. Then $\mathcal{U}$ is compact if and only if $\mathcal{U}/\mathfrak{m}$ is finite.*

Thanks to this proposition (whose proof we omit, since it is similar to the one for the compactness of $\mathbb{Z}_p$ seen in the previous section), we deduce that for a finite place v, the group $\mathcal{U}_v$ is compact.

Corollary 9.3. *Assume $\mathcal{U}/\mathfrak{m}$ is finite. Then $\mathfrak{m}^n$, $1 + \mathfrak{m}^n$, and $\mathcal{U}^\times$ are all compact subsets of $\mathcal{U}$.*

Proof. Each of these sets is closed in the compact set $\mathcal{U}$, hence compact. □

The next lemma describes a basis for the topology on $K^\times$ when K is a local non-Archimedean field. It will be the key ingredient in defining the restricted product topology.

Lemma 9.4. *Let $K/\mathbb{Q}_p$ be a finite extension of local fields, let $\mathcal{U}$ be the ring of integers, and π a uniformizer. Then*

$$\{\, aA : a \in K^\times,\ A \subseteq \mathcal{U}^\times \text{ open} \,\}$$

is a basis of open neighborhoods in $K^\times$.

Proof. The sets $1 + \pi^n\mathcal{U}$ ($n \geq 0$) form a neighborhood basis of 1 in $K^\times$. Because multiplication by $a \in K^\times$ is a homeomorphism, the sets

$$a(1 + \pi^n\mathcal{U})$$

form a neighborhood basis of a. Since each $1 + \pi^n\mathcal{U}$ is an open subset of $\mathcal{U}^\times$, the sets of the form aA with $A \subseteq \mathcal{U}^\times$ open form a basis.

□

This lemma motivates the definition of the restricted topological product. At a global level, it tells us that neighborhoods should locally be of the form $a_v A_v$ for finitely many places, while at all other places the open set should be the whole compact group $\mathcal{U}_v$.
We therefore define the topology on the idèle group

$$J_F = \{\text{idèles of } F\}$$

by declaring that the sets

$$\Big\{ \prod_{v \in V_F} C_v : C_v \text{ open in } F_v^\times \text{ for all } v,\ C_v = \mathcal{U}_v \text{ for all but finitely many } v \Big\}$$

form a basis of open sets.
Since each $\mathcal{U}_v$ is compact for v finite, this construction is the global analogue of taking products of the local bases described in the previous lemma.

Observe that $\mathcal{E}_F := \prod_{v \in V_F} \mathcal{U}_v$ is open in J_F. Let $a \in J_F$ and let $A \subseteq \mathcal{E}_F$ be open. Then aA is open in $\mathcal{E}_F$ because multiplication by a is a homeomorphism in every component.
Now consider a basic open set

$$B = \prod_{v \in V_F} B_v, \qquad B_v \subseteq F_v^\times \text{ open},\ B_v = \mathcal{U}_v \text{ for all but finitely many } v.$$

For each of the finitely many places where $B_v \neq \mathcal{U}_v$, the lemma above ensures that we can find $a_v \in F_v^\times$ and an open $T_v \subseteq \mathcal{O}_v^\times$ such that

$$a_v T_v \subseteq B_v.$$

For all other places, set $a_v = 1$ and $T_v = \mathcal{U}_v$. Let $A = \prod_{v \in V_F} T_v$. Then $aA \subseteq B$. Since this can be done around every point of B, the sets of the form aA form a basis of the restricted product topology.
Intersecting this basis with $\mathcal{E}_F$ we obtain

$$\{\, aA : a \in J_F,\ A \subseteq \mathcal{E}_F \text{ open in the product topology} \,\} = \{\, A : A \subseteq \mathcal{E}_F \text{ open} \,\}.$$

Thus $\mathcal{E}_F$ inherits the product topology.
Finally, note that

$$\mathcal{E}_F = \prod_{v \text{ infinite}} \mathcal{U}_v \times \prod_{v \text{ finite}} \mathcal{U}_v \simeq (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \times \{\text{a compact set}\}.$$

This structure plays a central role in proving the local compactness of J_F.

Proposition 9.5. *J_F is a locally compact topological group.*

Proof. Exercise 1 from week 9 exercise sheet. □

9.2 Idèles class group and its connection with other class groups

Proposition 9.6. *The quotient group $J_F/\mathcal{E}_F$ is isomorphic to $\mathcal{I}_F$, the group of fractional ideals of F.*

Proof. Define a map

$$\eta : J_F \longrightarrow \mathcal{I}_F$$

by

$$\eta\big((a_v)_{v \in V_F}\big) \;=\; \prod_{v \text{ finite}} \mathfrak{p}_v^{\operatorname{ord}_v(a_v)},$$

where $\mathfrak{p}_v$ denotes the prime ideal of $\mathcal{O}_F$ corresponding to the finite place v, and $\operatorname{ord}_v(a_v) \in \mathbb{Z}$ is the usual additive valuation exponent of a_v at v.
The product on the right is finite because for all but finitely many finite places v we have $a_v \in \mathcal{U}_v = \mathcal{O}_v^\times$, hence $\operatorname{ord}_v(a_v) = 0$.
It is immediate that η is a group homomorphism (valuation exponents add under multiplication) and that η is surjective: given a fractional ideal $\prod_{v \text{ finite}} \mathfrak{p}_v^{n_v}$, one can choose an idèle whose finite components have those prescribed valuations and whose infinite components are 1.

Finally, the kernel of η consists precisely of those idèles with trivial finite valuation at every finite place, i.e.

$$\ker \eta = \{(a_v)_{v\in V_F} \in J_F : \mathrm{ord}_v(a_v) = 0 \text{ for all finite } v\} = \mathcal{E}_F.$$

Hence by the first isomorphism theorem

$$J_F/\mathcal{E}_F \cong \mathcal{I}_F,$$

as claimed.

□

We may view each $\alpha \in F^\times$ as the idèle

$$\iota(\alpha) = \big(\iota_v(\alpha)\big)_{v\in V_F} \in J_F,$$

where $\iota_v : F \hookrightarrow F_v$ is the natural embedding into the completion at the place v. The map

$$\iota : F^\times \longrightarrow J_F, \qquad \alpha \mapsto \big(\iota_v(\alpha)\big)_v$$

is called the *diagonal embedding*. From now on we often identify α with $\iota(\alpha)$.
For such a principal idèle $\iota(\alpha)$ we have

$$\eta(\iota(\alpha)) = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\iota_v(\alpha))} = \alpha\mathcal{O}_F,$$

so $\eta(F^\times) = \mathcal{P}_F$ is the subgroup of principal fractional ideals. This yields:

Proposition 9.7. *For a number field F,*

$$J_F/F^\times\mathcal{E}_F \;\cong\; \mathcal{C}_F \;=\; \mathcal{I}_F/\mathcal{P}_F,$$

i.e. the idèle class group $J_F/(F^\times\mathcal{E}_F)$ is isomorphic to the ideal class group $\mathcal{I}_F/\mathcal{P}_F$.

Let $|\cdot|$ denote the usual absolute value on $\mathbb{C}$. For an infinite place v arising from an embedding $\iota_v : F \hookrightarrow \mathbb{C}$ we set

$$\|x\|_v = |\iota_v(x)|^d,$$

where $d = [F_v : \mathbb{R}]$: $d = 1$ if v is real, and $d = 2$ if v is complex. For a finite place v lying above the rational prime p we may view ι_v as an embedding $F \hookrightarrow F_v \subseteq \mathbb{C}_p$ (where $\mathbb{C}_p$ is the completion of an algebraic closure of $\mathbb{Q}_p$); then we set

$$\|x\|_v = |\iota_v(x)|_p^d, \qquad d = [F_v : \mathbb{Q}_p],$$

where $|\cdot|_p$ is the p-adic absolute value on $\mathbb{C}_p$ normalized so that $|p|_p = 1/p$.
These normalizations ensure the product formula holds in the usual way and are compatible with the valuations used in the definition of η.

Example 9.8. Let $F = \mathbb{Q}(i, \sqrt{3})$. For each rational prime p, we describe the completions of F at the primes above p and the corresponding embeddings $\iota_v : F \hookrightarrow F_v$.

We begin with the prime $p = 5$. In $\mathcal{O}_F$ the ideal (5) splits as a product of two distinct prime ideals,

$$(5) = \mathfrak{p}_5\,\mathfrak{p}_5',$$

and each of them has inertia degree 2. To describe the completions, let θ_5 be a root of $X^2 - 3$ in $\mathbb{Q}_5^{\mathrm{alg}}$; the field $\mathbb{Q}_5(\theta_5)$ is then the quadratic extension generated by $\sqrt{3}$, and both completions satisfy

$$F_{\mathfrak{p}_5} \simeq F_{\mathfrak{p}_5'} \simeq \mathbb{Q}_5(\theta_5).$$

The polynomial $X^2 + 1$, which defines i, reduces modulo 5 as

$$X^2 + 1 \equiv (X - 2)(X - 3) \pmod 5,$$

so the residue of i modulo $\mathfrak{p}_5$ must be 2, while modulo $\mathfrak{p}_5'$ it must be 3. By Hensel's lemma these roots lift uniquely to two 5-adic roots $\kappa_5, \tilde{\kappa}_5 \in \mathbb{Q}_5(\theta_5)$ of X^2+1. Assuming $i \equiv 2 \pmod{\mathfrak{p}_5}$ and $i \equiv 3 \pmod{\mathfrak{p}_5'}$, the corresponding embeddings satisfy

$$\iota_{\mathfrak{p}_5}(i) = \kappa_5, \qquad \iota_{\mathfrak{p}_5'}(i) = \tilde{\kappa}_5, \qquad \iota_{\mathfrak{p}_5}(\sqrt{3}) = \iota_{\mathfrak{p}_5'}(\sqrt{3}) = \theta_5.$$

Consider now $p = 3$. In this case the situation is different: both i and $\sqrt{3}$ generate quadratic extensions of $\mathbb{Q}_3$, and these extensions are linearly disjoint. As a consequence there is a single prime $\mathfrak{p}_3$ of F above 3, and the completion is

$$F_{\mathfrak{p}_3} \simeq \mathbb{Q}_3(i, \sqrt{3}), \qquad [F_{\mathfrak{p}_3} : \mathbb{Q}_3] = 4.$$

Let θ_3 be a root of X^2-3 and κ_3 a root of X^2+1 in $\mathbb{Q}_3^{\mathrm{alg}}$. An embedding $\iota_{\mathfrak{p}_3} : F \hookrightarrow F_{\mathfrak{p}_3}$ is then specified by

$$\iota_{\mathfrak{p}_3}(\sqrt{3}) = \theta_3, \qquad \iota_{\mathfrak{p}_3}(i) = \kappa_3.$$

At the infinite places, the field $\mathbb{Q}(\sqrt{3})$ has two real embeddings, which extend to two complex embeddings of F. Let v_1 correspond to the embedding sending $\sqrt{3}$ to $\sqrt{3}$, and v_2 to the one sending $\sqrt{3}$ to $-\sqrt{3}$. Then $F_{v_1} \simeq F_{v_2} \simeq \mathbb{C}$, and we may choose

$$\iota_{v_1}(i) = i, \qquad \iota_{v_2}(i) = -i.$$

If $\alpha = \sqrt{-3}$, the associated principal idèle is the element

$$\iota(\alpha) = \big(\iota_v(\alpha)\big)_{v \in V_F} = (\dots, \iota_{v_1}(\alpha), \iota_{v_2}(\alpha), \iota_{\mathfrak{p}_3}(\alpha), \iota_{\mathfrak{p}_5}(\alpha), \iota_{\mathfrak{p}_5'}(\alpha), \dots).$$

Theorem 9.9. *Let $\mathfrak{m}$ be a non-zero integral ideal of $\mathcal{O}_F$. Define*

$$J_{F,\mathfrak{m}}^+ := \left\{ a \in J_F : a_v > 0 \text{ for all real places } v,\ a_v \equiv 1 \pmod{\mathfrak{p}_v^{ord_v(\mathfrak{m})}} \text{ for all } \mathfrak{p}_v \mid \mathfrak{m} \right\}.$$

Then we have an isomorphism of groups

$$J_F / F^\times \mathcal{E}_{F,\mathfrak{m}}^+ \simeq \mathcal{R}_{F,\mathfrak{m}}^+,$$

where $\mathcal{E}_{F,\mathfrak{m}}^+ := J_{F,\mathfrak{m}}^+ \cap \mathcal{E}_F$.

Proof. First, note that

$$J_{F,\mathfrak{m}}^+ \cap F^\times = \{\alpha \in F^\times : \alpha \gg 0,\ \alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}\} =: F_{\mathfrak{m}}^+.$$

We claim $J_F = F^\times J_{F,\mathfrak{m}}^+$.
Let $a = (a_v)_{v \in V_F} \in J_F$. By the Approximation Theorem and the density of F in each F_v, there exists $\alpha \in F^\times$ such that

$$\|\iota_v(\alpha) - a_v\|_v < \varepsilon$$

for all infinite real places v and for all finite places v dividing $\mathfrak{m}$, where ε is sufficiently small. Then

$$\operatorname{sign}(\iota_v(\alpha)) = \operatorname{sign}(a_v) \text{ for all real } v, \quad \iota_v(\alpha)^{-1} a_v \equiv 1 \pmod{\mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}} \text{ for all } v \mid \mathfrak{m}.$$

Hence $\alpha^{-1} a \in J_{F,\mathfrak{m}}^+$, proving the claim.
It follows that

$$J_{F,\mathfrak{m}}^+ / F_{\mathfrak{m}}^+ = J_{F,\mathfrak{m}}^+ / J_{F,\mathfrak{m}}^+ \cap F^\times \simeq J_{F,\mathfrak{m}}^+ F^\times / F^\times = J_F / F^\times,$$

whence

$$J_{F,\mathfrak{m}}^+ / F_{\mathfrak{m}}^+ \mathcal{E}_{F,\mathfrak{m}}^+ \simeq J_F / F^\times \mathcal{E}_{F,\mathfrak{m}}^+.$$

Now define the natural homomorphism

$$\eta_{\mathfrak{m}} : J_{F,\mathfrak{m}}^+ \longrightarrow I_F(\mathfrak{m}), \qquad a = (a_v)_{v \in V_F} \longmapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}.$$

Then $\eta_{\mathfrak{m}}(J_{F,\mathfrak{m}}^+) = \mathcal{I}_F(\mathfrak{m})$, $\ker(\eta_{\mathfrak{m}}) = \mathcal{E}_{F,\mathfrak{m}}^+$, and $\eta_{\mathfrak{m}}(F_{\mathfrak{m}}^+) = \mathcal{P}_{F,\mathfrak{m}}^+$.

Hence the first isomorphism theorem gives

$$J^+_{F,\mathfrak{m}} \,/\, F^+_{\mathfrak{m}}\, \mathcal{E}^+_{F,\mathfrak{m}} \;\simeq\; \mathcal{I}_F(\mathfrak{m}) \,/\, \mathcal{P}^+_{F,\mathfrak{m}} =: \mathcal{R}^+_{F,\mathfrak{m}}.$$

Combining with the claim above, we obtain the desired result:

$$J_F / F^\times \mathcal{E}^+_{F,\mathfrak{m}} \simeq \mathcal{R}^+_{F,\mathfrak{m}}.$$

□

Corollary 9.10. *The set of subgroups $\mathcal{H} \subset J_F$ with $\mathcal{H} \supseteq F^\times \mathcal{E}^+_{F,\mathfrak{m}}$ for some $\mathfrak{m}$, corresponds to the set of open subgroups of J_F that contain $F^\times$.*

Proof. First we show that $\mathcal{E}^+_{F,\mathfrak{m}}$ is an open subgroup of J_F. Indeed,

$$\mathcal{E}^+_{F,\mathfrak{m}} \;\cong\; \prod_{v \text{ imaginary}} \mathbb{C}^\times \;\times\; \prod_{v \text{ real}} \mathbb{R}^\times_+ \;\times\; \prod_{\mathfrak{p}_v \mid \mathfrak{m}} (1 + \mathfrak{p}_v^{\operatorname{ord}_v(\mathfrak{m})}) \;\times\; \prod_{\mathfrak{p}_v \nmid \mathfrak{m}} \mathcal{U}_v,$$

which is open in $\mathcal{E}_F$, and hence open in J_F. It follows that $F^\times \mathcal{E}^+_{F,\mathfrak{m}}$ is open, and therefore any subgroup $\mathcal{H} \subset J_F$ containing $F^\times \mathcal{E}^+_{F,\mathfrak{m}}$ is open.

Conversely, suppose that $\mathcal{H} \subset J_F$ is an open subgroup containing $F^\times$. Since $1 \in \mathcal{H}$, there exists an open neighbourhood

$$A = \prod_v A_v \subset \mathcal{H}$$

of 1 in J_F, where $A_v = \mathcal{U}_v$ for all but finitely many v, and for the remaining places

$$A_v = \begin{cases} 1 + \mathfrak{p}_v^{n_v}, & v \text{ finite}, \\ \{x \in F_v : \|x - 1\|_v < \varepsilon\}, & v \text{ infinite}. \end{cases}$$

Let $\mathcal{H}_0$ be the subgroup of J_F generated by A. Then $\mathcal{H}_0 \subset \mathcal{H}$. Because $1 + \mathfrak{p}_v^{n_v}$ is already a group, we have

$$\mathcal{H}_0 = \left(\prod_{v \text{ imaginary}} \langle A_v \rangle \right) \times \left(\prod_{v \text{ real}} \langle A_v \rangle \right) \times \prod_{v \text{ finite}} A_v.$$

For real places, $\langle A_v \rangle = \mathbb{R}^\times_+$ or $\mathbb{R}^\times$. For imaginary places, $\langle A_v \rangle = \mathbb{C}^\times$.
Thus,

$$\mathcal{H}_0 = \left(\prod_{v \text{ imaginary}} \mathbb{C}^\times \right) \times \left(\prod_{v \text{ real}} \{\mathbb{R}^\times \text{ or } \mathbb{R}^\times_+\} \right) \times \prod_{v \text{ finite}} A_v,$$

where

$$A_v = \begin{cases} \mathcal{U}_v, & \text{for almost all } v, \\ 1 + \mathfrak{p}_v^{n_v}, & \text{otherwise}. \end{cases}$$

Define the modulus

$$\mathfrak{m} = \prod_{\substack{v \text{ finite} \\ A_v = 1 + \mathfrak{p}_v^{n_v}}} \mathfrak{p}_v^{n_v}.$$

Then by construction

$$\mathcal{H}_0 \supset \mathcal{E}^+_{F,\mathfrak{m}}, \qquad \text{and hence} \qquad \mathcal{H} \supset \mathcal{H}_0 \supset \mathcal{E}^+_{F,\mathfrak{m}}.$$

This proves the claim.

□

We may now reformulate the main theorems of class field theory in terms of idèles. The main idea can be summarized as follows:

Theorem 9.11. *There is an order-reversing bijection*

$$\{\,\textit{finite abelian extensions } K/F\,\} \longleftrightarrow \{\,\textit{open subgroups } \mathcal{H} \subset J_F \textit{ with } F^\times \subset \mathcal{H}\,\},$$

where inclusion of subgroups corresponds to reverse inclusion of fields. Moreover,

$$Gal(K/F) \simeq J_F/\mathcal{H}.$$

Given an open subgroup $\mathcal{H} \subset J_F$ containing $F^\times \mathcal{E}^+_{F,\mathfrak{m}}$, we may consider the induced subgroup

$$\mathcal{H}/F^\times \mathcal{E}^+_{F,\mathfrak{m}} \subset J_F/F^\times \mathcal{E}^+_{F,\mathfrak{m}} \simeq \mathcal{R}^+_{F,\mathfrak{m}}.$$

The nontrivial point is to determine precisely which subgroups of the ray class group $\mathcal{R}^+_{F,\mathfrak{m}}$ arise in this way. This provides a precise link between the formulation idèlic of class field theory and its classical ray class version.

9.3 Exercises week 9

1. Show that J_F is a topological group when equipped with the restricted product topology. Show furthermore that it is a locally compact group.

2. Show that $F^\times$ is a discrete subgroup of J_F. (Recall that we view $F^\times$ as a subgroup of J_F via $\iota(F^\times)$.)

3. In this exercise, you will prove the finiteness of the ideal class group $\mathscr{C}_F$. Before we do so, we introduce the content map as follows:
   For an idèle $\mathbf{a} = (\ldots, a_v, \ldots) \in J_F$, define its content to be

   $$\text{content}(\mathbf{a}) = \prod_{v \in V_F} ||a_v||_v$$

   You may assume that the content map is a continuous homomorphism $J_F \to \mathbb{R}^\times_+$.

   (a) Denote the kernel of the content map on J_F by J^1_F. Show that $F^\times < J^1_F$ and that the quotient $J^1_F/F^\times$ with the quotient topology is compact.

   (b) Let $\eta : J_F \to \mathcal{I}_F$ be the map $\mathbf{a} = (\ldots, a_v, \ldots) \mapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{\text{ord}_v(a_v)}$. Show that if $\mathcal{I}_F$ is given the discrete topology, η is continuous.

   (c) Show that $\eta(J^1_F) = \mathcal{I}_F$.

   (d) Show that $\mathscr{C}_F = \mathcal{I}_F/\mathcal{P}_F$ is compact. Finish the argument by remembering that it is a discrete group.

4. This exercise is to get familiar with idèles, and have some glimpses of concrete computations. Define the map:

   $$\mathbb{Q}^\times \times \mathbb{R}_+ \times \prod_p \mathbb{Z}_p^\times \to J_\mathbb{Q}$$
   $$(r, t, (u_p)_p) \mapsto (rt, ru_2, ru_3, ru_5, \ldots)$$

   (a) Prove that the map is surjective.
   Hint: Given $\mathbf{a} \in J_\mathbb{Q}$, observe the element $a = \text{sign}(a_\infty) \prod_p p^{\text{ord}_p a_p}$.

   (b) Prove that the map is injective.
   Hint: It is enough to show uniqueness of the factorization of $1 = (\ldots, 1, \ldots)$.

   (c) Show that the group on the left is a topological group by exhibiting a fundamental system of neighborhoods of 1.

10 Cohomology of finite groups and Cyclic Galois action on Idèles

10.1 Cohomology of Finite Cyclic Groups and the Herbrand Quotient

Let G be a finite cyclic group, say $G = \langle\sigma\rangle$, and let A be a G-module, so G acts on A and A is a module over the group ring $\mathbb{Z}[G]$.
Define

$$s(G) = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1},$$

where n is the order of G and

$$\begin{aligned} \sigma - 1 : A &\to A \\ a &\mapsto (\sigma - 1)(a) = \sigma(a) - a. \end{aligned}$$

Observe the following:

1. $\ker(\sigma - 1) = A^G$ because

$$\begin{aligned} \ker(\sigma - 1) &= \{a \in A \mid (\sigma - 1)(a) = 0\} \\ &= \{a \in A \mid \sigma(a) - a = 0\} \\ &= A^G. \end{aligned}$$

2. $s(G)A \subseteq A^G = \ker(\sigma - 1)$ because

$$\begin{aligned} (\sigma - 1)(1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}) &= \sigma + \sigma^2 + \cdots + \sigma^n - 1 - \sigma - \sigma^2 - \cdots - \sigma^{n-1} \\ &= \sigma^n - 1 \\ &= 0 \end{aligned}$$

   since G is of order n.

3. $(\sigma - 1)(A) \subseteq \ker(s(G))$ by the same computations as above.

Definition 10.1. We define

$$\mathcal{Q}_G(A) = \frac{[A^G : s(G)A]}{[\ker(s(G)) : (\sigma - 1)A]}$$

when these indices are finite and call this number the *Herbrand quotient* of A for the group G.

Example 10.2. Let $G = \langle\sigma\rangle$ be a cyclic group of order n and let $A = \mathbb{Z}$, with G acting trivially on A. We have

$$A^G = \mathbb{Z},$$

and

$$\begin{aligned} s(G)A &= \{(1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1})(a) \mid a \in A\} \\ &= \{a + \sigma(a) + \sigma^2(a) + \cdots + \sigma^{n-1}(a) \mid a \in A\} \\ &= \{na \mid a \in A\} \\ &= n\mathbb{Z}. \end{aligned}$$

Also, $\ker(s(G)) = \{0\}$ and $(\sigma - 1)A = \{0\}$, so we get

$$\mathcal{Q}_G(A) = \frac{[\mathbb{Z} : n\mathbb{Z}]}{[\{0\} : \{0\}]} = [\mathbb{Z} : n\mathbb{Z}] = n.$$

We now want to study some properties of the Herbrand quotient. To do this, we will use a lemma about the *Tate cohomolgy groups*.

Definition 10.3. We define the *Tate cohomology groups* as follows:

$$\begin{aligned} H^0(A) &= \frac{\ker_A(\sigma - 1)}{s(G)A}, \\ H^1(A) &= \frac{\ker_A(s(G))}{(\sigma - 1)A}, \end{aligned}$$

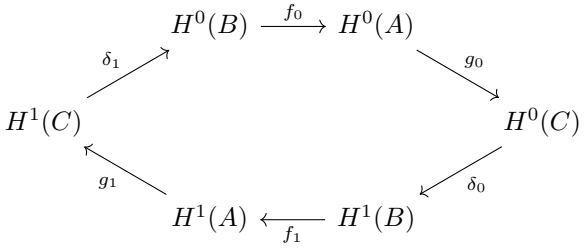
where $\ker_A$ indicates that $\sigma - 1 : A \to A$.

Note that $\frac{\#H^0(A)}{\#H^1(A)} = \mathcal{Q}_G(A)$.

Lemma 10.4 (Exact Hexagon Lemma)**.** *Suppose we have an exact sequence of $\mathbb{Z}[G]$-modules*

$$0 \longrightarrow B \xrightarrow{f} A \xrightarrow{g} C \longrightarrow 0.$$

Then there are $\mathbb{Z}[G]$-homomorphisms $f_0, f_1, g_0, g_1, \delta_0, \delta_1$ such that



is exact.

Proof. Define

$$\begin{aligned}
f_0 &: H^0(B) \to H^0(A) \\
&\quad b + s(G)B \mapsto f(b) + s(G)A, \\
g_0 &: H^0(A) \to H^0(C) \\
&\quad a + s(G)A \mapsto g(a) + s(G)C, \\
f_1 &: H^1(B) \to H^1(A) \\
&\quad b + (\sigma - 1)B \mapsto f(b) + (\sigma - 1)A, \\
g_1 &: H^1(A) \to H^1(C) \\
&\quad a + (\sigma - 1)A \mapsto g(a) + (\sigma - 1)C.
\end{aligned}$$

All are clearly well-defined $\mathbb{Z}[G]$-homomorphisms.
We now construct $\delta_0 : \ H^0(C) \to H^1(B)$ as follows.
Let $c \in \ker_C(\sigma - 1)$. We want to define $\delta_0(c + s(G)C)$. To do that, we make the following observations:

1. Since g is surjective, there exists $a_0 \in A$ such that $g(a_0) = c$.
2. Since $c \in \ker_C(\sigma - 1)$,
$$\begin{aligned}
&(\sigma - 1)(c) = 0 \\
&\Rightarrow (\sigma - 1)(g(a_0)) = 0 \\
&\Rightarrow g((\sigma - 1)(a_0)) = 0 \\
&\Rightarrow (\sigma - 1)(a_0) \in \ker(g) = \mathrm{im}(f).
\end{aligned}$$
3. There exists $b_0 \in B$ such that $f(b_0) = (\sigma - 1)(a_0)$.
4. Since $s(G)(\sigma - 1)$ is the zero map, we have
$$\begin{aligned}
0 &= s(G)(\sigma - 1)(a_0) \\
&= s(G)f(b_0) \\
&= f(s(G)(b_0)).
\end{aligned}$$
5. Since f is injective, we have $s(G)b_0 = 0$, which implies that $b_0 \in \ker_B(s(G))$.

With these observations, we define

$$\delta_0(c + s(G)C) = b_0 + (\sigma - 1)B.$$

To finish the proof, it remains to define

$$\delta_1 : H^1(C) \to H^0(B).$$

Its construction is done in Exercise 1 of week 10. Moreover, this exercise also shows that δ_1 is well-defined and that $\mathrm{im}(\delta_1) = \ker(f_0)$, which allows us to conclude that the hexagon is exact. □

We now use this lemma to prove some properties.

Proposition 10.5 (1^{st} property)**.** *If B is a G-submodule of A, and $C = \frac{A}{B}$, then*

$$\mathcal{Q}_G(A) = \mathcal{Q}_G(B)\mathcal{Q}_G(C).$$

In particular, if any two of these exist, then so does the third.

Proof. We have the exact sequence

$$0 \longrightarrow B \xrightarrow{f} A \xrightarrow{g} C \longrightarrow 0,$$

so we can apply the above Lemma.
Suppose that $\mathcal{Q}_G(A), \mathcal{Q}_G(B), \mathcal{Q}_G(C)$ are defined. Using the hexagon from the lemma and Lagrange's Theorem, we get

$$\begin{aligned}
\#H^0(B) &= \#\ker(f_0)\#\mathrm{im}(f_0),\\
\#H^0(C) &= \#\ker(\delta_0)\#\mathrm{im}(\delta_0),\\
\#H^0(A) &= \#\ker(g_0)\#\mathrm{im}(g_0), \text{ and so on.}
\end{aligned}$$

From the exactness of the hexagon, we get

$$\begin{aligned}
\#H^0(B)\#H^0(C)\#H^1(A) &= \#\ker(f_0)\#\mathrm{im}(f_0)\#\ker(\delta_0)\#\mathrm{im}(\delta_0)\#\ker(g_1)\#\mathrm{im}(g_1)\\
&= \#\mathrm{im}(\delta_1)\#\ker(g_0)\#\mathrm{im}(g_0)\#\ker(f_1)\#\mathrm{im}(f_1)\#\ker(\delta_1)\\
&= \#H^1(C)\#H^0(A)\#H^1(B),
\end{aligned}$$

whence, with some computations, we get

$$\begin{aligned}
\mathcal{Q}_G(B)\mathcal{Q}_G(C) &= \frac{\#H^0(B)\#H^0(C)}{\#H^1(B)\#H^1(C)}\\
&= \frac{\#H^0(A)}{\#H^1(A)}\\
&= \mathcal{Q}_G(A).
\end{aligned}$$

□

Proposition 10.6 (2^{nd} property)**.** *If A is a finite G-module, then $\mathcal{Q}_G(A) = 1$.*

Proof. Using the definition of $\mathcal{Q}_G(A)$ and Lagrange's Theorem, we get

$$\begin{aligned}
\mathcal{Q}_G(A) &= \frac{[A^G : s(G)A]}{[\ker s(G) : \mathrm{im}(\sigma - 1)]}\\
&= \frac{\#\ker(\sigma - 1)}{\#\mathrm{im}(s(G))}\frac{\#\mathrm{im}(\sigma - 1)}{\#\ker s(G)}\\
&= \frac{\#A}{\#A}\\
&= 1.
\end{aligned}$$

□

Corollary 10.7. *If B is a G-submodule of A of finite index, then $Q_G(A) = Q_G(B)$.*

We now state an important proposition without proof.

Proposition 10.8 (Shapiro's Lemma)**.** *Suppose $A = A_1 \oplus \cdots \oplus A_r$, where the A_j are subgroups of A but not submodules, and suppose that G transitively permutes $A_1, \ldots, A_r$. Let*

$$G_j = \{\tau \in G : \tau(A_j) = A_j\}.$$

Then A_j is a G_j-module and $\mathcal{Q}_G(A) = Q_{G_j}(A_j)$.

Example 10.9. Let $F/\mathbb{Q}$ be a cyclic extension of number fields, with $G = \mathrm{Gal}(F/\mathbb{Q}) = \langle\sigma\rangle$ of order n. What is $\mathcal{Q}_G(\mathcal{O}_F)$?
The Normal Basis Theorem gives the existence of an element $a \in F$ such that $\{\sigma^i(a)\}_{0\leq i<n}$ is a $\mathbb{Q}$-basis for F. We may assume that $a \in \mathcal{O}_F$, since otherwise, some multiple of it is. Let

$$B = \mathbb{Z}a + \mathbb{Z}\sigma(a) + \cdots + \mathbb{Z}\sigma^{n-1}(a)$$

Now $\mathrm{rank}_{\mathbb{Z}}(B) = n$ and $[\mathcal{O}_F : B]$ is finite, thus $\mathcal{Q}_G(\mathcal{O}_F) = \mathcal{Q}_G(B)$. Let $A_1 = \mathbb{Z}a$. Then

$$G_1 = \{\tau \in G \mid \tau(A_1) = A_1\} = \{1\}.$$

We have by Shapiro's Lemma

$$\begin{aligned}\mathcal{Q}_G(B) &= \mathcal{Q}_{G_1}(A_1)\\ &= \frac{[A_1^{G_1} : s(G_1)A_1]}{[\ker(s(G_1)) : (\sigma_1 - 1)A_1]}\\ &= \frac{[A_1 : A_1]}{[\{0\} : \{0\}]}\\ &= 1,\end{aligned}$$

where $\sigma_1 : 1 \to 1$.

10.2 Cyclic Galois Action on Idèles

Let K/F be a, not necessarily abelian, Galois extension of number fields.
Recall that we denote by V_K the places of K and by J_K the idèles of K.
Let $G = \mathrm{Gal}(K/F)$. We want to define an action of G on J_K.
We start by defining an action on the places of K and then use it to define an action on the idèles of K.
Let $\sigma \in G$ and $w \in V_K$. We define $\sigma w \in V_K$ by

$$\|\alpha\|_{\sigma w} = \|\sigma^{-1}(\alpha)\|_w$$

for any $\alpha \in K$.
Note that $\tau(\sigma w) = (\tau\sigma)w$ and that

$$\sigma : (K, \|\cdot\|_w) \to (K, \|\cdot\|_{\sigma w})$$

is an isometry. Thus σ induces an isomorphism between the completions that we also denote by σ :

$$\sigma : K_w \xrightarrow{\cong} K_{\sigma w}.$$

Before moving on to the definition of the action of G on the idèles of K, we introduce the following notation:
For all $v \in V_F$, $w \in V_K$, we say that w lies above v if $w|_F = v$.
To define the action of G on the idèles, we are going to range over every place v of F and look at every place w of K lying above this v. Doing this, we will range over every place of K.
Let $a \in J_K$ and $\sigma \in G$. We define for each $v \in V_F$

$$\sigma(a_w)_{w|v} = (b_w)_{w|v}$$

where

$$b_w := \sigma(a_{\sigma^{-1}(w)}).$$

This gives an action of σ on J_K.

Remark 10.10. This action is consistent with the usual action of G on $K^\times$, where we view $K^\times \subseteq J_K$ as before.

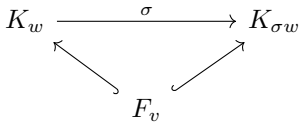
Remark 10.11. We have an obvious embedding $J_F \hookrightarrow J_K$ by sending

$$(b_v)_{v\in V_F} \mapsto ((b_v)_{w|v})_{v\in V_F}.$$

Now we have that J_K is a G-module, we want to know what is J_K^G.

Lemma 10.12. *We have $J_K^G = J_F$.*

Proof. We start by showing the reverse inclusion $J_K^G \supseteq J_F$.
For all $\sigma \in G$, we have a commutative diagram



where σ fixes F_v. Observe that by the commutativity of the diagram, we have that any element of J_F, see as an element of J_K by the above embedding, is fixed by G. Thus $J_F \subseteq J_K^G$.
We will now show the inclusion $J_K^G \subseteq J_F$.
Let $a \in J_K^G$. This means that for all $\sigma \in G$, we have $\sigma(a) = a$ and for all $v \in V_F$, we have $\sigma(a)_{w|v} = a_{w|v}$.
Define

$$G_w = \{\sigma \in G \mid \sigma w = w\} \subseteq G.$$

By Point (c) of Exercise 3 of week 10, we have

$$\begin{aligned} \mathrm{Gal}(K_w/F_v) &\cong G_w \\ \sigma &\mapsto \sigma|_K. \end{aligned}$$

Knowing this, for any element $\sigma \in G_w$, as $\sigma(a_w) = a_w$, we have $a_w \in F_v$ for all $w|v$.
Now, take w_1, w_2 above v. Using that by Point (a) of Exercise 3 of week 10, G acts transitively on the set $\{w|v\}$, we know there exist $\sigma \in G$ such that $w_1 = \sigma^{-1}w_2$. This means that $a_{w_2} = \sigma(a_{w_1})$. Since $a_{w_1} \in F_v$, we have by the first part that $\sigma(a_{w_1}) = a_{w_1}$ and so $a_{w_2} = a_{w_1}$. This shows that a is in the image of the embedding $J_F \to J_K$ and so we conclude. □

Recall the notion of the norm of an idèle.

Definition 10.13. Let K/F be an extension of number fields. We define the norm of an idèle by

$$\begin{aligned} N_{K/F} : J_K &\to J_F \\ (a_w)_{w \in V_K} &\mapsto (b_v)_{v \in V_F} \end{aligned}$$

where $b_v = \prod_{w|v} N_{K_w/F_v}(a_w)$.

Lemma 10.14. *Let G by cyclic of order n. Then*

$$s(G)a = \prod_{\sigma \in G} \sigma(a) = N_{K/F}(a)$$

for all $a \in J_K$ and where we use multiplicative notation for $s(G)$.

Proof. Take $v \in V_F$. We can write

$$\begin{aligned} a_{w|v} &= (a_{w_1}, \dots, a_{w_r}) \\ &= (a_{w_1}, 1, \dots, 1) \cdots (1, \dots, 1, a_{w_r}) \end{aligned}$$

Since $\prod_{\sigma \in G} \sigma(a_{w_1}, 1, \dots, 1) \in J_K^G = J_F$, we have

$$\prod_{\sigma \in G} \sigma(a_{w_1}, 1, \dots, 1) = (c_v, \dots, c_v)$$

for some $c_v \in F_v$. This means that we only need to know what one of the coordinates looks like. Let us work with the first coordinate. Define

$$G_{w_1} = \{\tau \in G \mid \tau w_1 = w_1\} = \mathrm{Gal}(K_{w_1}/F_v).$$

We notice that if $\sigma \notin G_{w_1}$, then the first coordinate of $\sigma(a_{w_1}, 1, \dots, 1)$ is 1. Thus, the first coordinate of $\prod_{\sigma \in G} \sigma(a_{w_1}, 1, \dots, 1)$ can be written as

$$\prod_{\sigma \in G_{w_1}} \sigma(a_{w_1}) = N_{K_{w_1}/F_v}(a_{w_1}).$$

This holds for any other coordinates, so we have

$$\prod_{\sigma\in G_{w_j}} \sigma(a_{w_j}) = N_{K_{w_j}/F_v}(a_{w_j})$$

for any $j \in \{1,\dots,r\}$. Taking the product of, we get

$$\left(\prod_{\sigma\in G}\sigma(a)\right)_{w|v} = \left(\underbrace{\prod_{w|v} N_{K_w/F_v}(a)}_{=b_v}\right)_{v\in V_F}.$$

Since b_v is the v^{th} coordinate of $N_{K/F}(a)$, we get

$$\prod_{\sigma\in G}\sigma(a) = N_{K/F}(a)$$

as we wanted. □

We now may study the Herbrand quotient of J_K for the group G, where $G = \langle\sigma\rangle$ is a finite cyclic group, with $G = \mathrm{Gal}(K/F)$ as before. We want some G-module A such that

$$[A^G : s(G)A] = [J_F : F^\times N_{K/F} J_K].$$

To make this statement more precise, we need to know more about the Herbrand quotient on idèles and on the idèle class group. We have the following lemma.

Lemma 10.15. *Let $C_K = \frac{J_K}{K^\times}$ be the group of idèle classes of K, and similarly let $C_F = \frac{J_F}{F^\times}$. The embedding $J_F \hookrightarrow J_K$ induces an embedding $C_F \hookrightarrow C_K$. Moreover, $C_K^G = C_F$.*

Proof. We have the following diagram:

$$\begin{array}{ccc} J_F & \hookrightarrow & J_K \\ \downarrow & \overset{\varphi}{\searrow} & \\ C_F & \hookrightarrow & C_K \end{array}$$

We have

$$\ker(\varphi) = J_F \cap K^\times = J_K^G \cap K^\times = (K^\times)^G = F^\times$$

where the last equality holds because G is Galois. This implies the existence of the dashed arrow and commutativity of the above diagram. The diagram shows the embedding $C_F \hookrightarrow C_K$.
It remains to show that $C_K^G = C_F$.
For any $a \in J_K$, we denote by $\bar{a}$ its image in $C_K = \frac{J_K}{K^\times}$. We define the action of G on C_K by, $\sigma(\bar{a}) = \overline{\sigma(a)}$ for all $\sigma \in G$.
We start by showing that $C_F \subseteq C_K^G$.
This comes from the following diagram:

$$\begin{array}{ccc} J_F & \hookrightarrow & J_K \\ \downarrow & & \downarrow \\ C_F & \hookrightarrow & C_K \end{array}$$

For the other direction, let $b \in J_K$ and $\bar{b} \in C_K^G$. This means that for all $\sigma \in G$, we have $\sigma(\bar{b}) = \overline{\sigma(b)} = \bar{b}$. This implies that $\overline{\sigma(b)}\bar{b}^{-1} = \bar{1}$, which implies that $\frac{\sigma(b)}{b} \in K^\times$ for all $\sigma \in G$.
Let us define

$$\begin{aligned} \varphi_b : G &\to K^\times \\ \sigma &\mapsto \frac{\sigma(b)}{b}. \end{aligned}$$

and observe that for $\tau, \sigma \in G$, we have

$$\begin{aligned}\tau(\varphi_b(\sigma)) &= \frac{\tau\sigma(b)}{\tau(b)} \\ &= \varphi_b(\tau\sigma)[\varphi_b(\tau)]^{-1}.\end{aligned}$$

To conclude, we use the following theorem without proof:

Theorem 10.16 (Hilbert's Theorem 90)**.** *Let $G = Gal(K/F)$, and let $f : G \to K^\times$ satisfy $f(\tau\sigma) = \tau(f(\sigma))f(\tau)$. Then there is some $\alpha \in K^\times$ such that $f(\sigma) = \frac{\sigma(\alpha)}{\alpha}$ for all $\sigma \in G$.*

As shown above, we can apply it to obtain that there exists $\alpha \in K^\times$ such that for all $\sigma \in G$, $\frac{\sigma(b)}{b} = \frac{\sigma(\alpha)}{\alpha}$. This is equivalent to $\sigma(\alpha^{-1}b) = \alpha^{-1}b$ and implies that $\alpha^{-1}b \in J_K^G = J_F$. Now, since $\alpha \in K^\times$, we know that $\overline{\alpha^{-1}b} = \bar{b} \in C_K$. But as $\alpha^{-1}b \in J_F$, we have $\overline{\alpha^{-1}b} = \bar{b} \in C_F$. □

10.3 Exercises week 10

1. *Looking at the proof of Lemma* 4.1 *in the book of Childress, construct the function δ_1, prove it is well-defined and prove that $im(\delta_1) = ker(f_0)$.*

2. If A, B are G-modules such that their Herbrand quotient exist, show that

$$\mathcal{Q}_G(A \times B) = \mathcal{Q}_G(A)\mathcal{Q}_G(B)$$

3. Let K/F be a Galois extension of number fields with Galois group G.

   (a) Let $v \in V_F$ be a place of F. Prove that G acts transitively on the set $\{w \mid v\}$ of places of K lying above v.

   (b) Check that the action of G on J_K coincides with the usual action of G on $K^\times$.

   (c) Let $v \in V_F$ and fix a place $w \mid v$. Show that the map

$$Gal(K_w/F_v) \longrightarrow G, \qquad \sigma \longmapsto \sigma|_K$$

   is an isomorphism onto the subgroup $G_w = \{\tau \in G \mid \tau(w) = w\}$ of G.

4. Recall Hilbert's Theorem 90 from class: For any cyclic Galois extension of fields K/F with Galois group G and any map $f : G \to K^\times$ satisfying

$$f(\tau\sigma) = \tau(f(\sigma))\, f(\tau),$$

   there exists some $\alpha \in K^\times$ such that

$$f(\sigma) = \frac{\sigma(\alpha)}{\alpha}, \qquad \text{for all } \sigma \in G.$$

   Use this to show:

   (a) There is an exact sequence of abelian groups

$$1 \longrightarrow F^\times \longrightarrow K^\times \longrightarrow ker(N_{K/F}) \longrightarrow 1.$$

   (b) Deduce that the norm map is surjective for an extension of finite fields.

11 Cyclic Galois Action on Idèles

11.1 Cyclic extensions of local fields

Let K/F be an algebraic cyclic extension of number fields and let $C_K = {}^{J_K}\!\big/_{K^\times}$. We recall the results obtained thus far:

1. $J_K^G = J_F$
2. $s(G)J_K = N_{K/F}J_K$
3. $C_F \hookrightarrow C_K$
4. $C_K^G = C_F$.

We also defined the norm $N_{K/F}$ on C_K so that the diagram below commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & J_K & \longrightarrow & C_K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} & & \\ 1 & \longrightarrow & F^\times & \longrightarrow & J_F & \longrightarrow & C_F & \longrightarrow & 1 \end{array}$$

Together these give,

$$\begin{aligned} [C_K^G : s(G)C_K] &= [C_F : N_{K/F}C_K] \\ &= \left[{J_F}\big/{F^\times} : N_{K/F}{J_K}\big/{F^\times \cap N_{K/F}J_K} \right] \\ &= [J_F : F^\times N_{K/F}J_K]. \end{aligned}$$

Later we shall see $[J_F : F^\times N_{K/F}J_K] = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}N_{K/F}(\mathfrak{m})]$ for a suitable modulus $\mathfrak{m}$. Combined with Hilbert Theorem 90, this motivates the study of $\mathcal{Q}_G(C_K)$ for $G = \mathrm{Gal}(K/F)$ cyclic. Recall that

$${J_K}\big/{K^\times \mathcal{E}_K} \cong \mathcal{C}_K$$

where $\mathcal{C}_K$ is the ideal class group of K. Before proceeding, we compute

$$\begin{aligned} \mathcal{Q}_G(C_K) &= \mathcal{Q}_G({K^\times \mathcal{E}_K}\big/{K^\times}) \\ &= \mathcal{Q}_G({\mathcal{E}_K}\big/{K^\times \cap \mathcal{E}_K}) \\ &= \mathcal{Q}_G({\mathcal{E}_K}\big/{\mathcal{U}_K}) \end{aligned}$$

where the first equality is justified by the finiteness of the index $[C_K : {K^\times \mathcal{E}_K}\big/{K^\times}]$ ($[J_K : K^\times \mathcal{E}_K] = |\mathcal{C}_K|$ is itself finite), and the second by the identity $\mathcal{E}_K \cap K^\times = \mathcal{U}_K$. Observe that

$$\mathcal{E}_K = \prod_w \mathcal{U}_w = \prod_{v \in V_F} \prod_{w|v} \mathcal{U}_w.$$

By Shapiro's Lemma,

$$\mathcal{Q}_F(\prod_{w|v} \mathcal{U}_w) = \mathcal{Q}_{G_w}(\mathcal{U}_w)$$

where $G_w = \{\sigma \in G : \sigma w = w\}$. Thus, the cohomology of the global product reduces to the cohomology of its local components, this suggests analyzing the norm index by means of the Herbrand quotient of unit groups in local fields.
We now prove the following lemma, which relates the norm index to the ramification index for cyclic extensions of local fields.

Lemma 11.1. *Let k_2/k_1 be a cyclic extension of local fields (with p such that $k_j/\mathbb{Q}_p$ is finite). Let $G = Gal(k_2/k_1)$ and let U_j denote the units of k_j. Then*

1. $\mathcal{Q}_G(\mathcal{U}_2) = 1$

2. $[\mathcal{U}_2^G : s(G)\mathcal{U}_2] = e(k_1/k_2)$.

Proof. We will prove the lemma in two steps.
Step 1: proving $\mathcal{Q}_G(\mathcal{U}_2) = 1$. Let $D = p^N\mathcal{O}_2$ where $\mathcal{O}_2$ is the ring of integers of k_2. We seek a subgroup $B \subset \mathcal{U}_2$ of finite index with $\mathcal{Q}_G(B) = 1$, since this would imply the desired result, assuming $B \cong D$ as G-modules:

$$\mathcal{Q}_G(\mathcal{U}_2) \overset{\text{finite index}}{=} \mathcal{Q}_G(B) \overset{B \cong_G D}{=} \mathcal{Q}_G(D) = \mathcal{Q}_G(\mathcal{O}_2) \overset{\text{Shapiro}}{=} 1.$$

To show the module isomorphism, consider the two following p-adic power series, allowing the transfer between multiplicative group structure to additive group structure and vice-versa:

$$\exp X = \sum_{i \geq 0} \frac{X^n}{n!}$$

$$\log X = \sum_{i \geq 1} (-1)^{n-1} \frac{(X-1)^n}{n}.$$

We leave it as an exercise (no.1, week 11) to find the radii of convergence of these series. Consider the radii $r = p^{-\frac{1}{p-1}}$: around 0 and 1 (respectively), disks of radius r satisfy the usual identities. This allows us to set $B = \exp(D)$, which is well-defined for N large enough and is open (B is a subgroup and has an obvious open neighbourhood of 1, using log / exp properties). In particular,

$$\exp : (D, +) \xrightarrow{\cong} (B, \cdot)$$

is a group isomorphism, even a G-module isomorphism, since the diagram below commutes.

$$\begin{array}{ccc} D & \xrightarrow[\exp]{} & B \\ {\scriptstyle\sigma}\downarrow & & {\scriptstyle\sigma}\downarrow \\ D & \xrightarrow[\exp]{} & B \end{array}$$

As we have seen, this implies $\mathcal{Q}_G(B) = 1$. There still remains to show B is of finite index in $\mathcal{U}_2$. Since B is open, we can write $\mathcal{U}_2$ as a disjoint union of the cosets of B:

$$\mathcal{U}_2 = \coprod_{i \in I} u_i B.$$

Using compactness of $\mathcal{U}_2$ and the fact that the cosets are disjoint, we obtain that I is a finite set, hence B has finite index in $\mathcal{U}_2$ as wanted and $\mathcal{Q}_G(\mathcal{U}_2) = 1$.
Step 2: computing the index. From $\mathcal{Q}_G(\mathcal{U}_2) = 1$ we obtain

$$[\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2] = [\mathcal{U}_2^G : s(G)\mathcal{U}_2] = [\ker_{\mathcal{U}_2} s(G) : (\sigma - 1)\mathcal{U}_2].$$

Let $A = \ker_{\mathcal{U}_2} s(G)$. For $u \in A$, $N_{k_2/k_1}(u) = 1$. Then, Hilbert's Theorem 90 provides $\alpha \in k_2^\times$ with

$$u = \frac{\sigma(\alpha)}{\alpha}.$$

Write $\alpha = \pi^t\varepsilon$ for $\pi \in k_2$ a uniformiser, $\varepsilon \in \mathcal{U}_2^\times$ and $t \in \mathbb{Z}$. Rewriting the above gives

$$u = \frac{\sigma(\pi^t)}{\pi^t} \cdot \frac{\sigma(\varepsilon)}{\varepsilon} \equiv \frac{\sigma(\pi^t)}{\pi^t} \equiv \left(\frac{\sigma(\pi)}{\pi}\right)^t \mod (\sigma - 1)\mathcal{U}_2.$$

This shows $A/(\sigma - 1)\mathcal{U}_2$ is generated by $\sigma(\pi)/\pi$. Finding the order of this group boils down to finding the order of its generator $\sigma(\pi)/\pi$. Let $d = \operatorname{ord}_\pi(\sigma(\pi)/\pi)$ be its order. We will show $d = e = e(k_2/k_1)$.

- $d \mid e$: write $\pi^e = \delta\rho$ for $\delta \in \mathcal{U}_2^\times$ and $\rho \in k_1$ a uniformiser. Then,

$$\frac{\sigma(\pi^e)}{\pi^e} = \frac{\sigma(\delta\rho)}{\delta\rho} = \frac{\sigma(\delta)}{\delta} \in (\sigma - 1)\mathcal{U}_2 \Rightarrow d|e.$$

- $e \mid d$: by definition of d, we have
$$\frac{\sigma(\pi^d)}{\pi^d} \in (\sigma - 1)\mathcal{U}_2.$$
Then there exists $\eta \in \mathcal{U}_2$ with
$$\frac{\sigma(\pi^d)}{\pi^d} = \frac{\sigma(\eta)}{\eta}, \text{ which implies } \frac{\sigma(\pi^d)}{\sigma(\eta)} = \frac{\pi^d}{\eta}.$$
This means σ fixes ${\pi^d}/{\eta}$. Since σ generates $G = \mathrm{Gal}(k_2/k_1)$, we must have ${\pi^d}/{\eta} \in k_1$. Together with $\gamma \in k_1^\times \Rightarrow e|\mathrm{ord}_\pi(\gamma)$, we conclude $e|d$.

Now that we know $e = e(k_2/k_1)$ is the order of the generator ${\sigma(\pi)}/{\pi}$ in the group ${\ker_{\mathcal{U}_2} s(G)}/{(\sigma-1)\mathcal{U}_2}$, we deduce
$$e = e(k_2/k_1) = [\ker_{\mathcal{U}_2} s(G) : (\sigma - 1)\mathcal{U}_2] = [\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2] = [\mathcal{U}_2 : s(G)\mathcal{U}_2].$$

□

Remark 11.2. Applying this lemma to the case of an unramified local extension k_2/k_1 yields $\mathcal{U}_1 = N_{k_2/k_1}\mathcal{U}_2$ (notice that k_2/k_1 being unramified requires it to be cyclic as well). In particular, we deduce that the norm is surjective on units in unramified local extensions.

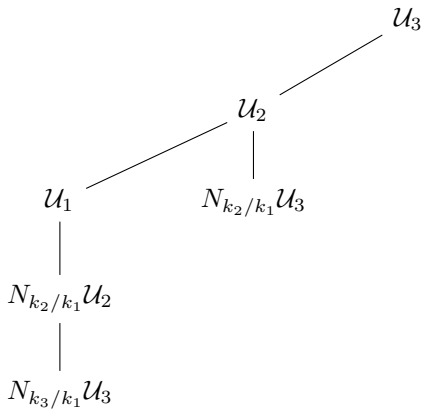
11.2 Ramified extensions of local fields

We now turn to non-cyclic (hence ramified) abelian extensions of local fields. To study them, we will consider a tower of intermediate subfields, so that each step in the tower is an extension with cyclic Galois group.

Lemma 11.3. *Let k_2/k_1 be an extension of local fields, with subgroups $B \leq A \leq U_2$ with $[A : B] = d$. Then,*
$$[N_{k_2/k_1}A : N_{k_2/k_1}B] \mid d.$$

Proof. Reference: Nancy Childress, Class Field Theory, Lemma 5.4., p. 90. □

Proposition 11.4. *Let $k_1 \subseteq k_2 \subseteq k_3$ be a tower of local fields. If $[\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2] \leq e(k_2/k_1)$ and $[\mathcal{U}_2 : N_{k_3/k_2}\mathcal{U}_3] \leq e(k_3/k_2)$ then*
$$[\mathcal{U}_1 : N_{k_3/k_1}\mathcal{U}_3] \leq e(k_3/k_1).$$



Proof. First, we use functoriality of norms, i.e., $N_{k_3/k_1} = N_{k_2/k_1} \circ N_{k_3/k_2}$. This yields
$$\begin{aligned}[\mathcal{U}_1 : N_{k_3/k_1}\mathcal{U}_3] &= [\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2][N_{k_2/k_1}\mathcal{U}_2 : N_{k_3/k_1}\mathcal{U}_3] \\ &= [\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2][N_{k_2/k_1}\mathcal{U}_2 : N_{k_2/k_1}(N_{k_3/k_2}\mathcal{U}_3)]\end{aligned}$$

By the previous lemma, the second factor of the above expression divides $[\mathcal{U}_2 : N_{k_3/k_2}\mathcal{U}_3]$ (in particular, it has to be smaller or equal to it). Therefore,
$$[\mathcal{U}_1 : N_{k_3/k_1}\mathcal{U}_3] \leq [\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2][\mathcal{U}_2 : N_{k_3/k_2}\mathcal{U}_3] \leq e(k_2/k_1)e(k_3/k_2) = e(k_3/k_1).$$

□

Remark 11.5. In particular, observe that if k_2/k_1 is an abelian extension of local fields, then

$$[\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2] \leq e(k_2/k_1).$$

It suffices to apply above knowledge on the control of ramification indices while exploiting the fact that any abelian extension decomposes as a tower of cyclic extension.

Before being able to prove the next proposition, we will need a little fugue to unify results and definitions of maps we might have seen before in other contexts.
Define a map $\eta_{K,\mathfrak{m}} : J^+_{K,\mathfrak{m}} \to \mathcal{I}_K(\mathfrak{m})$ by

$$\eta_{K,\mathfrak{m}} : a \mapsto \prod_{v\nmid\infty} \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}.$$

This extends to idèles via

$$\alpha : J_K \twoheadrightarrow J_K\Big/F^\times \cong J^+_{K,\mathfrak{m}}\Big/F^+_{\mathfrak{m}} \overset{\eta_{K,\mathfrak{m}}}{\to} \mathcal{I}_K(\mathfrak{m})\Big/\mathcal{P}^+_{K,\mathfrak{m}} = \mathcal{R}^+_{K,\mathfrak{m}}$$

where we slightly abuse notation when noting $\eta_{K,\mathfrak{m}}$ above. More explicitly, given $x \in F^\times$ with $xa \in J^+_{F,\mathfrak{m}}$, it is given by

$$\alpha : a \mapsto aF^\times \overset{\cong}{\mapsto} xaF^+_{\mathfrak{m}} \overset{\eta_{K,\mathfrak{m}}}{\mapsto} \Big(\prod_{v\nmid\infty} \mathfrak{p}^{\mathrm{ord}_v(x_v a_v)}\Big)\mathcal{P}^+_{K,\mathfrak{m}}.$$

We leave it as an exercise (no.3, week 11) to show that $\eta_{K,\mathfrak{m}}$ is surjective, that its extension to J_K is well-defined and that α is well defined. The key isomorphism induced by α is

$$J_F\Big/F^\times\mathcal{E}^+_{F,\mathfrak{m}} \cong \mathcal{I}_F(\mathfrak{m})\Big/\mathcal{P}^+_{F,\mathfrak{m}} = \mathcal{R}^+_{F,\mathfrak{m}}.$$

Notice that $\eta_{K,\mathfrak{m}}$ also satisfies

$$\eta_{F,\mathfrak{m}} \circ N_{K/F} = N_{K/F} \circ \eta_{K,\mathfrak{m}}.$$

We will use these results in the proof of the next proposition.

Proposition 11.6. *Let K/F be an abelian extension and let $\mathcal{H} = F^\times N_{K/F}J_K$. Then*

1. *$\mathcal{H}$ is open in J_F ($\Rightarrow \exists\mathfrak{m}$ s.t. $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$)*
2. *$\alpha(\mathcal{H}) = \mathcal{P}^+N_{K/F}\mathcal{I}_K(\mathfrak{m})\Big/\mathcal{P}^+_{F,\mathfrak{m}}$.*

Proof. We prove the two assertions separately.

1. Recall $N_{K/F}\mathcal{E}_K \subseteq N_{K/F}J_K \subseteq \mathcal{H}$ and

$$N_{K/F}\mathcal{E}_K = \prod_v \prod_{w|v} N_{K_w/F_v}\mathcal{U}_w.$$

It is enough to show $N_{K/F}\mathcal{E}_K$ is open, by properties of topological groups. Since $\mathcal{E}_F$ has the product topology, $N_{K/F}\mathcal{E}_K$ will be open in $\mathcal{E}_F$ if we can show $N_{K_w/F_v}\mathcal{U}_w$ is open for any $w \mid v$. This will be our strategy. We separate our first part of the proof in two subcases relying on the nature of v.
Case 1: if v is infinite, then $\mathcal{U}_w = \mathbb{R}^\times$ or $\mathbb{C}^\times$. Therefore, $N_{K_w/F_v}\mathcal{U}_w = \mathbb{C}^\times, \mathbb{R}^\times$ or $\mathbb{R}^\times_+$ which is open in any case.
Case 2: if v is finite, then if $w \mid v$ is unramified, $N_{K_w/F_v}\mathcal{U}_w = \mathcal{U}_v$. If ramified,

$$[\mathcal{U}_v : N_{K_w/F_v}\mathcal{U}_w] \leq e(w/v).$$

Using continuity of the norm, we deduce that $N_{K_w/F_v}\mathcal{U}_w$ is compact, hence open, as a closed subgroup of finite index in the compact group $\mathcal{U}_v$. By the correspondence we have seen, $\mathcal{H}$ being open and $F^\times \subseteq \mathcal{H}$ means there is some $\mathfrak{m}$ for which $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$.

2. 1^{st} inclusion:

$$\alpha(\mathcal{H}) \subseteq \mathcal{P}^+_{F,\mathfrak{m}} N_{K/F}\mathcal{I}_K(\mathfrak{m}) \Big/ \mathcal{P}^+_{F,\mathfrak{m}}.$$

Let $a \in \mathcal{H}$ of the form $a = c \cdot N_{K/F}(y)$ with $c \in F^\times$, $y \in J_K$. Choose $x \in F^\times$ with $xa \in J^+_{F,\mathfrak{m}}$. Then $\alpha(a) = \langle xa \rangle = \langle xc \cdot N_{K/F}(y) \rangle$. First, observe that $\langle xy \rangle \in \mathcal{P}^+_{F,\mathfrak{m}}$ since $xc \in F^\times$ and $xa \in J^+_{F,\mathfrak{m}}$. Secondly,

$$\eta_{F,\mathfrak{m}}(N_{K/F}(y)) = N_{K/F}(\eta_{K,\mathfrak{m}}(y)) \in N_{K/F}(\mathcal{I}_K(\mathfrak{m})).$$

Therefore, $\alpha(a) \in \mathcal{P}^+_{F,\mathfrak{m}} N_{K/F}\mathcal{I}_K(\mathfrak{m})$.
2^{nd} inclusion:

$$\alpha(\mathcal{H}) \supseteq \mathcal{P}^+_{F,\mathfrak{m}} N_{K/F}\mathcal{I}_K(\mathfrak{m}) \Big/ \mathcal{P}^+_{F,\mathfrak{m}}.$$

Let us write an element of the right-hand-side as $\langle B \rangle \cdot N_{K/F}(A)$ with $B \in F^\times$, $A \in \mathcal{I}_K(\mathfrak{m})$. There exists $y \in J_K$ such that $\eta_{K,\mathfrak{m}}(y) = A$, for any $A \in \mathcal{I}_K(\mathfrak{m})$ (exercise).
To conclude the proof, let us define $a := B \cdot N_{K/F}(y) \in \mathcal{H}$. Then,

$$\begin{aligned} \alpha(a) &= \langle B \cdot N_{K/F}(y) \rangle \\ &= \langle B \rangle \eta_{F,\mathfrak{m}}(N_{K/F}(y)) \\ &= \langle B \rangle N_{K/F}(\eta_{K,\mathfrak{m}}(y)) \\ &= \langle B \rangle N_{K/F}(A). \end{aligned}$$

□

Remark 11.7. A consequence of this proposition is the isomorphism

$$J_F \Big/ F^\times N_{K/F} J_K \cong \mathcal{I}_F(\mathfrak{m}) \Big/ \mathcal{P}^+_{F,\mathfrak{m}} N_{K/F}(\mathfrak{m}) \quad \text{for some } \mathfrak{m}.$$

In particular the right hand side does not depend on $\mathfrak{m}$. Naturally, we can ask ourselves: for which $\mathfrak{m}$ does this work? For which $\mathfrak{m}$ do we have $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$? If v is unramified, $v \nmid \mathfrak{m}$. If v is ramified, $v \mid \mathfrak{m}$.

Example 11.8. Let $K = \mathbb{Q}(\zeta_p)$, $F = \mathbb{Q}$ and $\mathcal{H} = \mathbb{Q}^\times N_{K/F} J_K$ ($p \neq 2$). We want to find $\mathfrak{m} = m\mathbb{Z} \subseteq \mathbb{Q}$ with $\mathcal{E}^+_{\mathbb{Q},m\mathbb{Z}} \subseteq \mathcal{H}$. For $q \neq p$ prime, q is unramified in $K/\mathbb{Q}$, so if w is a place of K above q, we have

$$N_{K_w/\mathbb{Q}_q}\mathcal{U}_w = \mathbb{Z}_q^\times \text{ (local norm map surjects on units).}$$

In the other case, p is totally ramified with ramification index $[\mathbb{Z}_p^\times : N_{K_w/\mathbb{Q}_p}\mathcal{U}_w] = p-1$. If w is a place of K above p, using $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ (in particular that it has a unique subgroup of index $p-1$) forces

$$N_{K_w/\mathbb{Q}_p}(\mathcal{U}_w) = 1 + p\mathbb{Z}_p.$$

Therefore,

$$N_{K/\mathbb{Q}} J_K = \mathbb{R}_+^\times \times (1 + p\mathbb{Z}_p) \times \prod_{q \neq p} \mathbb{Z}_q^\times.$$

Hence we may take the modulus $\mathfrak{m} = m\mathbb{Z} = p\mathbb{Z}$.

11.3 Exercises week 11

1. (Convergence of the p-adic Exponential)

   Consider the p-adic exponential power series defined over the field of p-adic numbers $\mathbb{Q}_p$:

   $$\exp X = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

   Let v_p denote the standard p-adic valuation normalized such that $v_p(p) = 1$. By analyzing the p-adic valuation of the coefficients $a_n = \frac{1}{n!}$, prove that the radius of convergence of this power series is $p^{-\frac{1}{p-1}}$. In other words, show that the series converges on the open disc:

   $$D = \left\{ x \in \mathbb{C}_p \;\middle|\; |x|_p < p^{-\frac{1}{p-1}} \right\}$$

2. (Continuity of the Norm Map)

   Let k_2/k_1 be an extension of local fields above $\mathbb{Q}_p$. Show that, with respect to the p-adic topology, the norm map

   $$N_{k_2/k_1} : k_2 \to k_1$$

   is continuous.

3. (The map α)

   The map $\eta_{K,\mathfrak{m}} : \mathcal{J}^+_{K,\mathfrak{m}} \to \mathcal{I}_K(\mathfrak{m})$ is defined by

   $$\eta_{K,\mathfrak{m}} : a \mapsto \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}.$$

   We "extend" $\eta_{K,\mathfrak{m}}$ to all ideals by considering the map

   $$\alpha : \ \mathcal{J}_K \twoheadrightarrow \mathcal{J}_K \big/ K^\times \xrightarrow{\cong} \mathcal{J}^+_{K,\mathfrak{m}} \big/ K^+_{\mathfrak{m}} \xrightarrow{\bar{\eta}_{K,\mathfrak{m}}} \mathcal{I}_K(\mathfrak{m}) \big/ \mathcal{P}^+_{K,\mathfrak{m}} = \mathcal{R}^+_{K,\mathfrak{m}}.$$

   Explicitly, it is given by :

   $$\alpha : \ a \longmapsto aK^\times \xmapsto{\cong} xaK^+_{\mathfrak{m}} \xmapsto{\bar{\eta}_{K,\mathfrak{m}}} \left(\textstyle\prod_{v \nmid \infty} \mathfrak{p}^{\mathrm{ord}_v(x_v a_v)} \right) \mathcal{P}^+_{K,\mathfrak{m}}.$$

   where $x \in K^\times$ is any unit such that $xa \in \mathcal{J}^+_{K,\mathfrak{m}}$.

   (i) Show that $\eta_{K,\mathfrak{m}}$ is surjective (This is the missing step in the proof of the idèle-ideal correspondence).

   (ii) The definition of α depends on the choice of $x \in K^\times$ by weak approximation. Show that α is well-defined.

   (iii) Compute the kernel of α.

4. (A more general case)

   Let E/F be a generic number extension (not necessarily Galois), and let $\mathcal{H} = F^\times \tilde{N}_{E/F} \mathcal{J}_E$. Show that $\mathcal{H}$ is open in $\mathcal{J}_F$.

12 Global Cyclic Norm Index Equality

12.1 Global Cyclic Norm Index Equality

The goal of today's lecture is to prove the Global Cyclic Norm Index Equality (Theorem 12.6), using this we can reformulate the proof of the Completeness Theorem, whose proof we get closer to by preparing Artin reciprocity which will be presented in next chapter.

Proposition 12.1. *Let K/F be a Galois extension of number fields, with cyclic Galois group $G = \langle\sigma\rangle$. Let v be a place of F and w a place of K above v. Then*

1. $\mathcal{Q}_{G_w}(\mathcal{U}_w) = 1$ *if w is finite, if w is real, or if v is imaginary.*
2. $\mathcal{Q}_{G_w}(\mathcal{U}_w) = 2$ *if w is imaginary but v is real.*
3. $\mathcal{Q}_G\left(\prod_{v\notin\mathcal{S}}\prod_{w|v}\mathcal{U}_w\right) = 1$, *where*

$$\mathcal{S} = \{v \in V_F : v \text{ is infinite, or } v \text{ ramifies in } K/F\}$$

Proof. 1. If $\mathcal{U}_w = \begin{cases}\mathbb{R}^\times, & w \text{ real}\\ \mathbb{C}^\times, & v \text{ imaginary}\end{cases}$ then

$$G_w = \{\sigma \in G, \sigma w = w\} = \begin{cases}Gal(\mathbb{R}/\mathbb{R}) = \{1\}, & w \text{ real}\\ Gal(\mathbb{C}/\mathbb{C}) = \{1\}, & v \text{ imaginary}\end{cases}$$

therefore $\mathcal{Q}_{G_w}(\mathcal{U}_w) = 1$. If w is finite, we can apply lemma 11.1 with $k_1 = F_v, k_2 = K_w, \mathcal{U}_2 = \mathcal{U}_w$ and get the result.

2. If w is imaginary and v real, we have that $G_w = Gal(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$ with τ the complex conjugation, $\mathcal{U}_w^{G_w} = (\mathbb{C}^\times)^{G_w} = \mathbb{R}^\times$ and $s(G_w)\mathcal{U}_w = (1+\tau)\mathbb{C}^\times = \{z\bar{z} : z \in \mathbb{C}^\times\} = \mathbb{R}_+^\times$ (for the second equality, note that the additive structure becomes multiplicative). We also have that

$$\ker_{\mathcal{U}_w} s(G_w) = \{z \in \mathbb{C}^\times : z\bar{z} = 1\},$$

is the unit circle group, and

$$(\tau - 1)\mathcal{U}_w = (\tau - 1)\mathbb{C}^\times = \left\{\frac{z}{\bar{z}} : z \in \mathbb{C}^\times\right\}$$

is also the unit circle group. It follows that

$$[\mathcal{U}_w^{G_w} : s(G_w)\mathcal{U}_w] = [\mathbb{R}^\times : \mathbb{R}_+^\times] = 2, \qquad [\ker_{\mathcal{U}_w} s(G_w) : (\tau-1)\mathcal{U}_w] = 1$$

therefore $\mathcal{Q}_{G_w}(\mathcal{U}_w) = 2$.

3. See exercise 12. 1.

□

Note that Proposition 12.1 allows us to compute the Herbrand quotient of $\mathcal{E}_K$:

Lemma 12.2.

$$\mathcal{Q}_G(\mathcal{E}_K) = 2^a$$

with $a = |\{v \in V_F : v \text{ is real on } F \text{ but extends to an imaginary place of } K\}|$.

Proof. Indeed, using the same $\mathcal{S}$ as in Proposition 12.1,

$$\begin{aligned}\mathcal{Q}_G(\mathcal{E}_K) &= \mathcal{Q}_G\Big(\prod_{v\in V_F}\prod_{w|v}\mathcal{U}_w\Big)\\ &= \Big(\prod_{v\in\mathcal{S}}\mathcal{Q}_G\Big(\prod_{w|v}\mathcal{U}_w\Big)\Big)\mathcal{Q}_G\Big(\prod_{v\notin\mathcal{S}}\prod_{w|v}\mathcal{U}_w\Big)\\ &= \Big(\prod_{v\in\mathcal{S}}\mathcal{Q}_{G_{w_v}}(\mathcal{U}_{w_v})\Big)\mathcal{Q}_G\Big(\prod_{v\notin\mathcal{S}}\prod_{w|v}\mathcal{U}_w\Big)\\ &= 2^a \cdot 1\end{aligned}$$

where the second and third equality are due to Exercise 2 of sheet 10 and Shapiro's lemma, a as defined in the statement and w_v denotes any place above v (they either all go to a real place or all to an imaginary one). □

We want to find the Herbrand quotient of $\mathcal{U}_K$, where K/F is cyclic. Once we have done so, we can combine it with the above information to find the Herbrand quotient of the idèle class group C_K. This in turn will lead to a proof of a result on the norm index in the case of a cyclic global extension. We shall need a preliminary lemma which is left as an exercise (ex 2 of exercise sheet 12).

Lemma 12.3. *Let G be a finite group acting on a finite set $\mathcal{S}$. Let $V = \bigoplus_{w\in\mathcal{S}} \mathbb{R}X_w$. Then G acts on V by*

$$\sigma\left(\sum_{w\in S} a_w X_w\right) = \sum_{w\in S} a_w X_{\sigma w}.$$

Let $\mathcal{L} \subseteq V$ be a G-stable lattice (note that it always exists since one can consider the lattice generated by the orbits of X_w under action G for each $w \in \mathcal{S}$). Then there is a basis $\{Y_w\}_{w\in\mathcal{S}}$ of V contained in $\mathcal{L}$ such that $\sigma(Y_w) = Y_{\sigma w}$ for all $\sigma \in G$ and all $w \in \mathcal{S}$.

Proposition 12.4. *Let K/F be a Galois extension of number fields with cyclic Galois group $G = \langle\sigma\rangle$, then*

$$\mathcal{Q}_G(\mathcal{U}_K) = \frac{2^a}{[K:F]},$$

where $a = |\{v \in V_F : v \text{ is real on } F \text{ but extends to an imaginary place in } K\}|$ as previously.

Proof. Let a as above and note that $\mathcal{U}_K = \mathcal{O}_K^\times$. By Dirichlet's Unit Theorem $\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^{r_1+r_2-1}$ with W_K, r_1, r_2 as defined in Dirichlet's Unit Theorem. Let $\mathcal{S} = \{w \in V_K, w \text{ is infinite}\}$ and define

$$\ell : \mathcal{U}_K \longrightarrow V := \mathbb{R}^{r_1+r_2}, \qquad \ell(\varepsilon) = (\dots, \log\|\varepsilon\|_w, \dots)_{w\in\mathcal{S}}$$

The image $\ell(\mathcal{U}_K)$ is a discrete subgroup of V as $\mathcal{U}_K$ is discrete. More precisely $\ell(\mathcal{U}_K)$ is a lattice in

$$V_0 = \left\{(\dots, x_w, \dots) \in V : \sum_w x_w = 0\right\}$$

by the product formula since we know already that for units $u \in \mathcal{U}_K = \mathcal{O}_K^\times$ and finite places w we have $\|u\|_w = 1$. Furthermore we have $\dim_{\mathbb{R}} V_0 = r_1 + r_2 - 1$.

For $w \in \mathcal{S}$ let $X_w = (0, \dots, 0, 1, 0, \dots, 0) \in V$ with the 1 in the w-th coordinate. Then $V = \bigoplus_{w\in\mathcal{S}} \mathbb{R}X_w$. Let G act on V by $\sigma(X_w) = X_{\sigma w}$. Let

$$\ell_0 = \sum_{w\in\mathcal{S}} X_w = (1, \dots, 1) \qquad \text{and} \qquad \mathcal{L} = \ell(\mathcal{U}_K) \oplus \mathbb{Z}\ell_0.$$

Note that $\mathcal{L} \subset V = V_0 \oplus \mathbb{R}\ell_0$. We will compute $\mathcal{Q}_G(\mathcal{U}_K)$ by linking it to $\mathcal{Q}_G(\mathcal{L})$.

By the Dirichlet Unit Theorem, $\ker\ell = W_K$, and we have the exact sequence

$$0 \longrightarrow W_K \longrightarrow \mathcal{U}_K \xrightarrow{\ell} \ell(\mathcal{U}_K) \longrightarrow 0,$$

In particular $\mathcal{U}_K/W_K \cong \ell(\mathcal{U}_K)$. By the multiplicativity of the Herbrand quotient we get

$$\mathcal{Q}_G(\mathcal{U}_K) = \mathcal{Q}_G(W_K)\mathcal{Q}_G(\ell(\mathcal{U}_K)) = \mathcal{Q}_G(\ell(\mathcal{U}_K)),$$

since W_K is finite its Herbrand quotient is 1 by a Proposition from week 10.

Note then that G acts trivially on $\mathbb{Z}\ell_0 \cong \mathbb{Z}$, so $\mathcal{Q}_G(\mathbb{Z}\ell_0) = |G| = [K:F]$. Hence we have

$$\mathcal{Q}_G(\mathcal{L}) = \mathcal{Q}_G(\ell(\mathcal{U}_K))\mathcal{Q}_G(\mathbb{Z}\ell_0) = \mathcal{Q}_G(\mathcal{U}_K)[K:F].$$

We now show that G preserves $\mathcal{L}$. First note that $\sigma(\ell_0) = \sum_{w\in\mathcal{S}} X_{\sigma w} = \ell_0$ and for $\varepsilon \in \mathcal{U}_K$,

$$\begin{aligned}\ell(\sigma(\varepsilon)) &= \sum_{w\in\mathcal{S}} \log\|\sigma(\varepsilon)\|_w\, X_w \\ &= \sum_{w\in\mathcal{S}} \log\|\varepsilon\|_{\sigma^{-1}w}\, X_w \\ &= \sum_{w\in\mathcal{S}} \log\|\varepsilon\|_w\, X_{\sigma w} \\ &= \sigma\left(\sum_{w\in\mathcal{S}} \log\|\varepsilon\|_w\, X_w\right) = \sigma\big(\ell(\varepsilon)\big).\end{aligned}$$

Hence $\sigma(\ell(\mathcal{U}_K)) = \ell(\sigma(\mathcal{U}_K)) = \ell(\mathcal{U}_K)$. Since $\sigma(\ell_0) = \ell_0$ this means $\sigma(\mathcal{L}) = \mathcal{L}$ for all $\sigma \in G$.

We now apply Lemma 12.3 to $\mathcal{L}$: there exists a basis $\{Y_w\}_{w\in\mathcal{S}} \subset \mathcal{L}$ of V such that $\sigma(Y_w) = Y_{\sigma w}$ for all $\sigma \in G$ and all $w \in \mathcal{S}$. Let

$$\mathcal{L}' = \bigoplus_{w\in\mathcal{S}} \mathbb{Z}Y_w \subseteq \mathcal{L}$$

But $\operatorname{rank}_{\mathbb{Z}} \mathcal{L}' = |\mathcal{S}| = \operatorname{rank}_{\mathbb{Z}} \mathcal{L}$ so $\mathcal{L}/\mathcal{L}'$ is finite, therefore $\mathcal{Q}_G(\mathcal{L}) = \mathcal{Q}_G(\mathcal{L}')$.

But we can reorder the infinite places w by grouping those above the same place $v \in V_F$, and write

$$\mathcal{L}' = \bigoplus_{v|\infty} \bigoplus_{w|v} \mathbb{Z}Y_w$$

Each summand $\bigoplus_{w|v} \mathbb{Z}Y_w$ is a G-module on which G transitively permutes the summands. By Shapiro's lemma,

$$\mathcal{Q}_G\Big(\bigoplus_{w|v} \mathbb{Z}Y_w\Big) = \mathcal{Q}_{G_w}(\mathbb{Z}Y_w).$$

But $\mathbb{Z}Y_w \cong \mathbb{Z}$ has trivial G_w-action, so $\mathcal{Q}_{G_w}(\mathbb{Z}Y_w) = |G_w|$. Therefore

$$\mathcal{Q}_G(\mathcal{L}') = \prod_{v|\infty} |G_{w_v}|$$

where w_v is an arbitrary place above v.

Now $|G_w| = [K_w : F_v]$ and by Proposition 12.1,

$$[K_w : F_v] = \begin{cases} 1 & \text{if } w \text{ and } v \text{ are both real, or both complex} \\ 2 & \text{if } v \text{ is real and } w \text{ is complex.}\end{cases}$$

Therefore

$$\mathcal{Q}_G(\mathcal{L}') = 2^a,$$

where $a = |\{v \in V_F : v \text{ real in } F \text{ but becomes complex in } K\}|$. Combining the equalities above yields

$$\mathcal{Q}_G(\mathcal{U}_K) = \frac{\mathcal{Q}_G(\mathcal{L})}{[K:F]} = \frac{\mathcal{Q}_G(\mathcal{L}')}{[K:F]} = \frac{2^a}{[K:F]}$$

□

Corollary 12.5.

$$\mathcal{Q}_G(C_K) = [K : F].$$

Proof. $\mathcal{Q}_G(C_K) = \mathcal{Q}_G(\mathcal{E}_K/\mathcal{U}_K) = 2^a(\frac{2^a}{[K:F]})^{-1}$ □

We can now present the most important result of this first half.

Theorem 12.6 (Global Cyclic Norm Index Equality)**.** *If K/F is a cyclic extension of number fields and $\mathfrak{m}$ is an integral ideal of $\mathcal{O}_F$ that is divisible by a sufficiently high power of every ramified prime in K/F, then*

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})] = [K : F]$$

Proof. Since $\mathcal{Q}_G(C_K) = [K : F]$, we have

$$[C_K^G : s(G)C_K] = [K : F]\,[\ker_{C_K} s(G) : (\sigma - 1)C_K].$$

But from previous section 12 we also know that

$$[C_K^G : s(G)C_K] = [C_F : N_{K/F}C_K] = [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})]$$

whenever $\mathfrak{m}$ satisfies $F^\times N_{K/F}J_K \supseteq \mathcal{E}^+_{F,\mathfrak{m}}$, which is the case here by our choice of $\mathfrak{m}$. Thus

$$[K : F] \mid [\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})]$$

Meanwhile, the Universal Norm Index Inequality gives

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})] \leq [K : F]$$

Hence equality holds. □

We can further generalize this result to abelian extensions K/F. We will prove and use this generalization next chapter to show the Completeness Theorem.

12.2 Introduction on Artin Reciprocity

Given an abelian Galois extension of number fields K/F, we have shown that the subgroup $\mathcal{H} = F^\times N_{K/F}J_K$ of J_F contains $\mathcal{E}^+_{F,\mathfrak{m}}$ for some integral ideal $\mathfrak{m} \in \mathcal{I}_F$ divisible by sufficiently high powers of the primes that ramify in K/F. The ideal $\mathfrak{m}$ is not unique however. Suppose $\mathfrak{n}$ is another ideal of $\mathcal{O}_F$ for which $\mathcal{E}^+_{F,\mathfrak{n}} \subseteq \mathcal{H}$. Let $(\mathfrak{m}, \mathfrak{n})$ denote the g.c.d. of $\mathfrak{m}$ and $\mathfrak{n}$.

Remark 12.7. We can show that $\mathcal{E}^+_{F,\mathfrak{m}}\mathcal{E}^+_{F,\mathfrak{n}} = \mathcal{E}^+_{F,(\mathfrak{m},\mathfrak{n})}$. We do not prove this.

Definition 12.8. By Remark 12.7, we have that there is a minimal ideal $\mathfrak{f}$ of $\mathcal{O}_F$ such that $\mathcal{E}^+_{F,\mathfrak{f}} \subseteq H$. This ideal $\mathfrak{f}$ is called the conductor of $\mathcal{H}$ (or of K/F) and denoted $\mathfrak{f} = \mathfrak{f}(K/F)$. By minimality here, we mean precisely that if $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq \mathcal{H}$ then $\mathfrak{f}|\mathfrak{m}$.

In section 10, we saw that we can find an $\mathfrak{m}$ divisible only by ramified primes such that $\mathcal{E}^+_{F,\mathfrak{m}} \subset \mathcal{H}$, the minimality of $\mathfrak{f}$ means that the conductor cannot be divisible by any unramified prime.

We now use the conductor and the Global Cyclic Norm Index Equality to reformulate the proof of the Completeness Theorem, which is a central theorem and will be seen later in the chapter. The Completeness Theorem states that for any abelian extension K/F, there exists some $\mathfrak{m}$ and some H with $\mathcal{P}^+_{F,\mathfrak{m}} < H < \mathcal{I}_F(\mathfrak{m})$ such that K is the class field of H over F. Recall the set

$$\mathcal{S}_{K/F} = \{\mathfrak{p} \text{ prime of } F \text{ that splits completely in } K/F\}$$

We have seen in section 6 that its Dirichlet density is $\delta_F(\mathcal{S}_{K/F}) = \frac{1}{[K:F]}$. Now let $H = \mathcal{P}^+_{F,\mathfrak{f}}\mathcal{N}_{K/F}(\mathfrak{f})$ where $\mathfrak{f}$ is the conductor of $\mathcal{H}$ as defined previously and consider

$$\mathcal{T}_{K/F} = \{\text{primes } \mathfrak{p} \in H\}.$$

If $\mathfrak{p}$ splits completely in K/F, then $(\mathfrak{p}, \mathfrak{f}) = 1$ and for $\mathfrak{P} \mid \mathfrak{p}$, we have $N_{K/F}\mathfrak{P} = \mathfrak{p}$. Thus $\mathcal{S}_{K/F} \subseteq \mathcal{T}_{K/F}$. Also, by Proposition 2.3 from chapter 2, if we can show $L_\mathfrak{f}(1, \chi) \neq 0$ for all characters $\chi \neq \chi_0$ of $\mathcal{I}_F(\mathfrak{f})$ that are trivial on H, and if we can generalize to abelian extensions the Global Cyclic Norm Index Equality, then

$$\delta_F(\mathcal{T}_{K/F}) = \frac{1}{[\mathcal{I}_F(\mathfrak{f}) : H]} = \frac{1}{[K : F]} = \delta_F(\mathcal{S}_{K/F})$$

so under these assumptions, $\mathcal{S}_{K/F} \approx \mathcal{T}_{K/F}$. By the definition of class field in chapter 2, it would then follow that K is the class field over F of H, and the Completeness Theorem would be established.

We need to work a bit more to get both of the assumptions needed for this result. In particular we need to show Artin reciprocity, for which we need to introduce the Artin symbol and the Artin map.

Let K/F be a Galois extension of number fields with abelian Galois group G. Let $\mathfrak{p}$ be a prime ideal

of $\mathcal{O}_F$ that is unramified in K/F. Then the decomposition group $G_\mathfrak{p} = Z(\mathfrak{p})$ must be cyclic as $\mathfrak{p}$ is unramified with a canonical generator $\sigma_\mathfrak{p} = \left(\frac{\mathfrak{p}}{K/F}\right)$, the Artin automorphism.

Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ that is divisible by all the primes that ramify in the extension K/F and no others. The map $\mathfrak{p} \mapsto \sigma_\mathfrak{p}$ induces a homomorphism $\mathcal{A} = \mathcal{A}_{K/F} : \mathcal{I}_F(\mathfrak{m}) \to G$ given by $\mathfrak{a} \mapsto \sigma_\mathfrak{a} = \left(\frac{\mathfrak{a}}{K/F}\right)$ where, for $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}} \in \mathcal{I}_F(\mathfrak{m})$ with each $\mathfrak{p}$ unramified, we set

$$\sigma_\mathfrak{a} = \prod_\mathfrak{p} \sigma_\mathfrak{p}^{n_\mathfrak{p}} = \left(\frac{\mathfrak{a}}{K/F}\right).$$

(Here $\sigma_\mathfrak{a}$ does not depend on the choice of $\mathfrak{m}$.)

Definition 12.9. The map $\mathcal{A}$ is called the Artin map and $\left(\frac{\mathfrak{a}}{K/F}\right)$ is the Artin symbol.

Proposition 12.10 (Consistency Property)**.** *Let $F \subseteq L \subseteq K$, $F \subseteq E \subseteq K$ be number fields and suppose K/F is an abelian Galois extension of number fields. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ that is unramified in K/F and let $\mathfrak{P}_K$ be a prime ideal of $\mathcal{O}_K$ that divides $\mathfrak{p}$. Let $\mathfrak{P}_L = \mathfrak{P}_K \cap L$, $\mathfrak{P}_E = \mathfrak{P}_K \cap E$ be prime ideals of $\mathcal{O}_L$ and $\mathcal{O}_E$ respectively that each lie above $\mathfrak{p}$. Then*

$$\left(\frac{\mathfrak{P}_E}{K/E}\right)\Bigg|_L = \left(\frac{\mathfrak{p}}{L/F}\right)^f$$

where $f = f(\mathfrak{P}_E/\mathfrak{p})$ is the residue field degree.

Proof. Let $\sigma_\mathfrak{p} = \left(\frac{\mathfrak{p}}{K/F}\right)$. Recall, for $\alpha \in \mathcal{O}_K$, we have

$$\sigma_\mathfrak{p}(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}_K},$$

and this congruence completely characterizes $\sigma_\mathfrak{p}$.

Let $\sigma_{\mathfrak{P}_E} = \left(\frac{\mathfrak{P}_E}{K/E}\right)$. Then $\sigma_{\mathfrak{P}_E}(\alpha) \equiv \alpha^{N\mathfrak{P}_E} \pmod{\mathfrak{P}_K}$ for all $\alpha \in \mathcal{O}_K$ and

$$\sigma_{\mathfrak{P}_E}|_L(\alpha) \equiv \alpha^{N\mathfrak{P}_E} \pmod{\mathfrak{P}_K \cap \mathcal{O}_L} \equiv \alpha^{N\mathfrak{P}_E} \pmod{\mathfrak{P}_L}$$

But $N\mathfrak{P}_E = (N\mathfrak{p})^f$ by definition of f, so

$$\sigma_\mathfrak{p}^f(\alpha) \equiv \alpha^{N\mathfrak{p}^f} \equiv \alpha^{N\mathfrak{P}_E} \pmod{\mathfrak{P}_L}.$$

Hence $\sigma_\mathfrak{p}^f(\alpha) \equiv \sigma_{\mathfrak{P}_E}|_L(\alpha) \pmod{\mathfrak{P}_L}$. It follows that $\sigma_\mathfrak{p}^f = \sigma_{\mathfrak{P}_E}|_L$ as desired. □

We now present a few correlaries that will be useful for Artin reciprocity. By the Consistency Property, we have

$$\left(\frac{\mathfrak{P}_E}{K/E}\right)\Bigg|_L = \left(\frac{\mathfrak{p}}{L/F}\right)^f = \left(\frac{\mathfrak{p}^f}{L/F}\right) = \left(\frac{N_{E/F}\mathfrak{P}_E}{L/F}\right).$$

For $\mathfrak{A} \in \mathcal{I}_E(\mathfrak{m})$ (where $\mathfrak{m}$ is divisible by all the ramified primes, and no others), by decomposing $\mathfrak{A}$ into primes, multiplicativity gives

$$\left(\frac{\mathfrak{A}}{K/E}\right)\Bigg|_L = \left(\frac{N_{E/F}\mathfrak{A}}{L/F}\right)$$

Corollary 12.11. *Let $F \subseteq L \subseteq K$ be number fields, where K/F is abelian Galois. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ that is unramified in K/F. Then*

$$\left(\frac{\mathfrak{p}}{K/F}\right)\Bigg|_L = \left(\frac{\mathfrak{p}}{L/F}\right)$$

Proof. Letting $E = F$ in Proposition 12.10, the corollary follows. □

Corollary 12.12. *Let $F \subseteq E \subseteq K$ be number fields, where K/F is abelian Galois. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ that is unramified in K/F and let $\mathfrak{P}_E$ be a prime of $\mathcal{O}_E$ above $\mathfrak{p}$. Then*

$$\left(\frac{\mathfrak{P}_E}{K/E}\right) = \left(\frac{N_{E/F}\mathfrak{P}_E}{K/F}\right)$$

Proof. Letting $L = K$ in Proposition 12.10 gives the result. □

Corollary 12.13. *Let K/F be an abelian Galois extension of number fields. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ that is divisible by all the primes that ramify in K/F. Then*

$$\mathcal{N}_{K/F}(\mathfrak{m}) \subseteq \ker\left(A : \mathcal{I}_F(\mathfrak{m}) \to G\right)$$

This is essentially the first part of Artin reciprocity which will be shown next week.

Proof. Putting $L = K = E$ in Proposition 12.10 gives

$$\left(\frac{N_{K/F}\mathfrak{P}_K}{K/F}\right) = \left(\frac{\mathfrak{P}_K}{K/K}\right)\Bigg|_K = 1$$

If $\mathfrak{A} \in N_{K/F}(\mathfrak{m})$ then by factoring $\mathfrak{A}$ we have

$$\left(\frac{N_{K/F}\mathfrak{A}}{K/F}\right) = 1$$

□

12.3 Exercise week 12

1. In this exercise you finish the proof of Proposition 12.1.
   Let K/F be a Galois extension of number fields, with cyclic Galois group $G = \langle\sigma\rangle$. Let v be a place of F and w be a place of K above v. We define $\mathcal{S} := \{v \in V_F : v \text{ is infinite, or } v\text{ramifies in } K/F\}$. We want to show that
   $$\mathcal{Q}_G\left(\prod_{v\notin\mathcal{S}}\prod_{w|v}\mathcal{U}_w\right) = 1$$
   .
   (a) Define $A = \prod_{v\notin\mathcal{S}} A_v$, where $A_v = \prod_{w|v}\mathcal{U}_w$, and notice that $\mathcal{S}$ is a finite set. Show that $A_v^G \cong \mathcal{U}_v$ and $s(G)A_v \cong \mathcal{U}_v$.
   (b) Show that $[\ker_{A_v} s(G) : (\sigma - 1)A_v] = 1$.
   (c) Show that $A^G = s(G)A$ and $\ker_A s(G) = (\sigma - 1)A$, and conclude.

2. This exercise will prove lemma 12.3.
   Let G be a finite group acting on a finite set $\mathcal{S}$. Let
   $$V = \bigoplus_{w\in\mathcal{S}} \mathbb{R}X_w$$
   be a vector space. Then G acts on V via
   $$\sigma\left(\sum_{w\in\mathcal{S}} a_w X_w\right) = \sum_{w\in\mathcal{S}} a_w X_{\sigma w}.$$
   Let $\mathcal{L} \subseteq V$ be a lattice preserved by G. You will show in this exercise that there exists a basis $\{Y_w\}_{w\in\mathcal{S}}$ of V contained in $\mathcal{L}$ such that $\sigma(Y_w) = Y_{\sigma w}$, for all $\sigma \in G$, $w \in \mathcal{S}$.

   For any $\sum_{w\in\mathcal{S}} a_w X_w \in V$, define the following norm on V :
   $$||\sum_{w\in\mathcal{S}} a_w X_w||_0 = \max_w\{|a_w| : w \in \mathcal{S}\}.$$
   If we have a set $\{X'_w\}_{w\in\mathcal{S}}$ such that for every $w \in \mathcal{S}$ $||X'_w - X_w||_0 < \frac{1}{\dim_{\mathbb{R}} V}$, then $\{X'_w\}_{w\in\mathcal{S}}$ is also a basis for V.

(a) Let $\{w_1, ..., w_r\}$ to be a complete set of representatives for the orbits of the action of G on $\mathcal{S}$. Show that for $i \in \{1, \dots, r\}$ we can choose elements $X'_{w_i} \in \mathbb{Q}\mathcal{L}$ such that

$$||X'_{w_i} - X_{w_i}||_0 < \frac{1}{\dim_{\mathbb{R}} V}$$

.

(b) Define for all $i \in \{1, \dots, r\}$

$$X''_{w_i} = \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \sigma(X'_{w_i}),$$

where $G_{w_i} := \{\sigma \in G | \sigma(w_i) = w_i\}$, and show that $||X''_{w_i} - X_{w_i}||_0 < \frac{1}{\dim_{\mathbb{R}} V}$.

(c) Show that defining X''_w to be $\sigma(X''_{w_i})$ whenever $\sigma w_i = w$ is a definition that makes sense. In particular a similar definition would not have made sense on the X'_{w_i}'s.

(d) Show that $\{X''_w\}_{w \in \mathcal{S}}$ is a basis of V contained in $\mathbb{Q}\mathcal{L}$ and that we can transform it into a basis contained in $\mathcal{L}$.

(e) Call the basis found in the previous point $\{Y_w\}_{w \in \mathcal{S}}$, and show that $\sigma(Y_w) = Y_{\sigma w}$, for any $\sigma \in G$, $w \in \mathcal{S}$. This will conclude the proof of the lemma.

3. Let K/F be an abelian extension of number fields, and let $\mathfrak{f} = \mathfrak{f}(K/F)$.

(a) Show: if $\mathfrak{m}$ is an ideal of $\mathcal{O}_F$ such that $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K$, then $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$.

(b) Prove or disprove and salvage: If $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K$, then

$$\mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m}) \;=\; \mathcal{P}^+_{F,\mathfrak{f}} \mathcal{N}_{K/F}(\mathfrak{f}) \cap \mathcal{I}_F(\mathfrak{m}).$$

(c) Suppose $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$. Show that there is a natural embedding

$$\mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}} N_{K/F}(\mathfrak{m}) \;\hookrightarrow\; \mathcal{I}_F(\mathfrak{f})/\mathcal{P}^+_{F,\mathfrak{f}} N_{K/F}(\mathfrak{f})$$

induced by inclusion.

(d) Under what circumstances is the embedding of part (c) an isomorphism?

4. Let $K = \mathbb{Q}(\sqrt{5}, i)$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where σ is complex conjugation, while τ fixes i and sends $\sqrt{5} \mapsto -\sqrt{5}$. Suppose $p\mathbb{Z}$ is an unramified prime in $K/\mathbb{Q}$.

(a) Compute

$$\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right),$$

i.e., give congruence conditions on p that determine whether the Artin symbol is 1, σ, τ, or $\sigma\tau$. (Hint: If you can find some cyclotomic field that contains K, then Example 1 of Chapter 1 may be useful.)

(b) Give necessary and sufficient conditions (in terms of congruence) on $p\mathbb{Z}$ to split completely in $K/\mathbb{Q}$. Compare your answer with (a) and Theorem 1.18:

Theorem 12.14. *Let $K \subseteq \mathbb{Q}(\zeta_m)$, then identify $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and let $H < (\mathbb{Z}/m\mathbb{Z})^\times$ be the subgroup corresponding to $Gal(\mathbb{Q}(\zeta_m)/K)$. The primes $p \nmid m$ that split completely in $K/\mathbb{Q}$ are precisely the unramified primes with trivial Artin automorphism.*

(c) Suppose $p\mathbb{Z}$ is inert in $\mathbb{Q}(i)/\mathbb{Q}$. What can you say about

$$\left(\frac{p\mathbb{Z}[i]}{K/\mathbb{Q}(i)}\right)?$$

(d) Suppose $p\mathbb{Z}$ splits in $\mathbb{Q}(i)/\mathbb{Q}$, say $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}'$. What can you say about

$$\left(\frac{p}{K/\mathbb{Q}(i)}\right)?$$

13 Artin Reciprocity and Quadratic Reciprocity

13.1 Artin Reciprocity

Today, we will begin by stating and giving a big sketch of the proof of the Artin reciprocity. For this, let us first recall how the Artin map is defined.

Let K/F be an extension of number fields. Let also $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ that is divisible by all the primes that ramify in K/F and no others. We denote by $\mathfrak{p}$ a prime ideal of $\mathcal{O}_F$ and define

$$\sigma_{\mathfrak{p}} := \left(\frac{\mathfrak{p}}{K/F}\right).$$

This induces the Artin map

$$\mathcal{A} = \mathcal{A}_{K/F} : \mathcal{I}_F(m) \longrightarrow G := \mathrm{Gal}(K/F), \qquad \mathfrak{a} \longmapsto \sigma_{\mathfrak{a}} := \left(\frac{\mathfrak{a}}{K/F}\right),$$

where for

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \in \mathcal{I}_F(\mathfrak{m}),$$

we set

$$\sigma_{\mathfrak{a}} := \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}} = \left(\frac{\mathfrak{a}}{K/F}\right).$$

Now we can state the Artin reciprocity theorem.

Theorem 13.1 (Artin Reciprocity)**.** *Let K/F be an abelian extension of number fields, and assume $\mathfrak{m}$ is an ideal of $\mathcal{O}_F$ divisible by all the ramifying primes. Let*

$$G = Gal(K/F).$$

Then:

(i) $\mathcal{A} : \mathcal{I}_F(m) \to G$ *is surjective.*

(ii) The ideal $\mathfrak{m}$ of $\mathcal{O}_F$ can be chosen so that it is divisible only by the ramified primes and satisfies

$$\mathcal{P}^+_{F,\mathfrak{m}} \subset \ker(\mathcal{A}).$$

(iii) $\mathcal{N}_{K/F}(\mathfrak{m}) \subset \ker(\mathcal{A})$.

Observe that *(ii)* and *(iii)* imply that $\mathcal{A}$ induces a surjective homomorphism

$$\overline{\mathcal{A}} : \mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m}) \longrightarrow G.$$

And since

$$\#\Big(\mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}}\mathcal{N}_{K/F}(\mathfrak{m})\Big) \leq [K:F] = \#G,$$

by the universal norm index inequality, in fact $\overline{\mathcal{A}}$ is an isomorphism.

Proof. Observe first that we have already proved *(iii)* in the previous section 12. Now let us prove *(i)*. Denote by

$$H := \mathcal{A}(\mathcal{I}_F(\mathfrak{m})) \subset G,$$

and let $E = K^H$ be the fixed field of H. Given $\mathfrak{a} \in \mathcal{I}_F(m)$, we have by consistency that

$$\left(\frac{\mathfrak{a}}{E/F}\right) = \left(\frac{\mathfrak{a}}{K/F}\right)\Big|_E.$$

And since $\left(\frac{\mathfrak{a}}{K/F}\right) \in H$ and E is the fixed field of H, we get

$$\left(\frac{\mathfrak{a}}{K/F}\right)\Big|_E = 1 = \left(\frac{\mathfrak{a}}{E/F}\right).$$

In particular, if $\mathfrak{a} = \mathfrak{p}$ is any prime such that $\mathfrak{p} \nmid \mathfrak{m}$, then

$$\left(\frac{\mathfrak{p}}{E/F}\right) = 1,$$

which generates the decomposition group $Z_{E/F}(\mathfrak{p})$. Therefore $\mathfrak{p}$ splits completely in E/F.
Recall the sets

$$\mathcal{S}_F := \{\mathfrak{p} \subset \mathcal{O}_F \text{ prime}\}, \qquad \mathcal{S}_{E/F} := \{\mathfrak{p} \subset \mathcal{O}_F \text{ prime splitting completely in } E/F\}.$$

Thus

$$S_F \setminus S_{E/F} = \{\mathfrak{p} \subset \mathcal{O}_F \text{ prime } \mid \mathfrak{p} \mid m\},$$

which is finite. Hence

$$\frac{1}{[E:F]} = \delta_F(\mathcal{S}_{E/F}) = \delta_F(\mathcal{S}_F) = 1.$$

Thus $E = F$, and it follows that $H = G$. Therefore $\mathcal{A}$ is surjective, as wanted.
It remains now to prove *(ii)*, i.e. there exists $\mathfrak{m}$ such that

$$\mathcal{P}^+_{F,\mathfrak{m}} \subset \ker(\mathcal{A}),$$

and moreover we may take $\mathfrak{m}$ to be divisible only by primes that ramify in K/F.
We will split the proof of *(ii)* into four different steps.

Step 1 : We begin with the special case $F = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity. Let $p \in \mathbb{N}$ be a prime number with $(p, m) = 1$. Then

$$\left(\frac{p\mathbb{Z}}{K/F}\right) = \sigma_p : \zeta_m \longmapsto \zeta_m^p.$$

Let $a \in \mathbb{N}$ with $a = p_1^{e_1} \cdots p_r^{e_r}$, and suppose that all the p_i are coprime with m. Then

$$\left(\frac{a\mathbb{Z}}{K/F}\right) = \prod_{i=1}^{r} \sigma_{p_i}^{e_i} = \sigma_a.$$

Now say $a = \frac{b}{c}$ with $b, c \in \mathbb{N}$. Then

$$\sigma_a = \left(\frac{a\mathbb{Z}}{K/F}\right) = \sigma_b \sigma_c^{-1}.$$

Thus

$$\sigma_a = 1 \iff \sigma_b = \sigma_c \iff b \equiv c \pmod{m} \iff a \overset{\times}{\equiv} 1 \pmod{m}.$$

So we have shown *(ii)* for $F = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta_m)$.

Step 2 : Next suppose that F is any number field and $K = F(\zeta_m)$.
We have for $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$,

$$\left(\frac{\mathfrak{a}}{K/F}\right)\Big|_{\mathbb{Q}(\zeta_m)} = \left(\frac{N\mathfrak{a}}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right),$$

by the consistency property. Note that $\sigma \in G$ is trivial if and only if $\sigma|_{\mathbb{Q}(\zeta_m)} = 1$, because the value of ζ_m by σ defines σ entirely.
Let $\mathfrak{m} = m\mathcal{O}_F$ and suppose $\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}$. Then

$$\mathfrak{a} = \langle \alpha \rangle, \quad \text{where } \alpha \in F,\ \alpha \gg 0,\ \alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}.$$

Thus

$$\left(\frac{\mathfrak{a}}{K/F}\right)\Big|_{\mathbb{Q}(\zeta_m)} = \left(\frac{N\langle\alpha\rangle}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right) = \left(\frac{\langle N\alpha\rangle}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right).$$

Since $\alpha \gg 0$, we get $N\alpha > 0$. And since $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$, we also get $N\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$. From the previous step we thus obtain that

$$\left(\frac{\langle N\alpha\rangle}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right) = 1 = \left(\frac{\mathfrak{a}}{K/F}\right)\Big|_{\mathbb{Q}(\zeta_m)}.$$

So we deduce that

$$\left(\frac{\mathfrak{a}}{K/F}\right) = 1,$$

and we're done.

Step 3 : Next, let K/F be an arbitrary cyclic extension of number fields. Choose $\mathfrak{m}$ admissible so that

$$\mathcal{E}^+_{F,\mathfrak{m}} \subset F^\times N_{K/F} J_K.$$

By the global cyclic norm index equality we have that

$$\big[\mathcal{I}_F(\mathfrak{m}) : \mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m})\big] = [K : F]$$

and since we've proved *(i)*, we also have that

$$\big[\mathcal{I}_F(\mathfrak{m}) : \mathrm{Ker}(\mathcal{A})\big] = [K : F].$$

We'll show later the Proposition 1.3 that tells us that

$$\mathrm{Ker}(\mathcal{A}) \subset \mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m}).$$

So that

$$\mathrm{Ker}(\mathcal{A}) = \mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m}),$$

and hence

$$\mathcal{P}^+_{F,\mathfrak{m}} \subset \mathrm{Ker}(\mathcal{A}).$$

Step 4 : Finally, we suppose that K/F is an arbitrary extension of number fields that is abelian. Let E/F be a cyclic intermediate extension. By the above, there is some $\mathfrak{m}_E$ such that

$$P^+_{F,\mathfrak{m}_E} \subset \mathrm{Ker}\big(\mathcal{A}_{E/F}\big).$$

Let

$$\mathfrak{m} = \prod_{\substack{E/F \text{ cyclic} \\ E \subset K}} \mathfrak{m}_E.$$

Then $\mathcal{P}^+_{F,\mathfrak{m}} \subset \mathcal{P}^+_{F,\mathfrak{m}_E}$ for all such E, so

$$\mathcal{P}^+_{F,\mathfrak{m}} \subset \mathrm{Ker}\big(\mathcal{A}_{E/F}\big).$$

Suppose $\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}$, then

$$\left(\frac{\mathfrak{a}}{E/F}\right) = 1 \qquad \text{for every cyclic subextension } E/F.$$

Denote $\sigma = \left(\frac{\mathfrak{a}}{K/F}\right)$. We have then by consistency property that $\sigma|_E = 1$ for every cyclic E/F. Suppose by contradiction that $\sigma \neq 1$, then there exists a non-trivial character

$$\chi : \langle\sigma\rangle \longrightarrow \mathbb{C}^\times$$

so that $\chi(\sigma) \neq 1$. Extend this character to G, and denote it still χ. Denote also $H = \mathrm{Ker}(\chi)$. Then G/H is cyclic because it's isomorphic to $\mathrm{im}(\chi)$ (which is a finite subgroup of $\mathbb{C}^\times$). In fact we have $H = \langle\chi\rangle^\perp$ so we have an explicit description

$$G/H \;\cong\; \widehat{G/H} \;\cong\; H^\perp \;\cong\; \big(\langle\chi\rangle^\perp\big)^\perp \;\cong\; \langle\chi\rangle.$$

Hence if we take E to be the fixed field of H, $E = K^H$, then E/F is cyclic by the Galois correspondence. So $\sigma|_E = 1$, and then $\sigma \in H = \mathrm{Ker}(\chi)$, which is a contradiction. Thus $\sigma = 1$, and $\mathfrak{a} \in \mathrm{Ker}(\mathcal{A})$ as wanted. □

In order to complete the proof, it remains to show Proposition 13.3that shows the cyclic case for *(ii)* of Artin reciprocity. Thus, until the end of this section, we consider K/F to be cyclic of order n, with

$$G = \mathrm{Gal}(K/F) = \langle \sigma \rangle.$$

We will use an important lemma in order to prove Proposition 13.3.

Lemma 13.2 (Artin's lemma)**.** *Let $\mathcal{S}$ be a finite set of primes of $\mathbb{Z}$, $\mathfrak{p}$ a prime of $\mathcal{O}_F$. Then there is some $m \in \mathbb{N}$ and an extension E/F such that*

1. *$K \cap E = F$,*
2. *$KE \subset K(\zeta_m) = E(\zeta_m)$,*
3. *$K \cap F(\zeta_m) = F$,*
4. *$\mathfrak{p}$ splits completely in E/F,*
5. *m is prime to the elements of S and to $\mathfrak{p}$.*

Proof. This is a long proof using bunch of lemmas, and the exercise 1 of the exercise session of this week gives you steps to prove it using the last lemma needed for it. For more details you can follow the pages 115–127 of the book of Nancy Childress. □

Now let's finally restate and prove the proposition needed.

Proposition 13.3. *Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ sufficiently large so that it is divisible by all the ramifying primes in K/F, and so that*

$$\mathcal{E}^+_{F,\mathfrak{m}} \subset F^\times N_{K/F} J_K,$$

then

$$\mathrm{Ker}(\mathcal{A}) \subset \mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m}).$$

Proof. Let $\mathfrak{a} \in \mathrm{Ker}(\mathcal{A})$,

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\gamma_i}.$$

Let $\mathfrak{m}$ be a multiple of $\mathfrak{f} = \mathfrak{f}(K/F)$, chosen divisible by all the ramified primes and no others. We denote

$$\left(\frac{\mathfrak{p}_i^{\gamma_i}}{K/F}\right) = \sigma^{d_i},$$

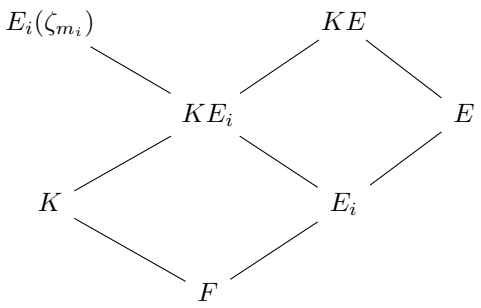
so that

$$1 = \left(\frac{\mathfrak{a}}{K/F}\right) = \sigma^{d_1 + \cdots + d_r} \qquad \Longrightarrow \qquad n \mid (d_1 + \cdots + d_r).$$

By repeatedly applying Artin's lemma and enlarging $\mathcal{S}$, we get $m_1, \ldots, m_r \in \mathbb{N}$ and fields $E_1, \ldots, E_r$. Define $E = E_1 \cdots E_r$, then by 1. and 3. of Artin's lemma we get

$$K \cap E_i = F = K \cap E.$$

We have a diagram of inclusions:



and then isomorphisms

$$G = \mathrm{Gal}(K/F) \;\cong\; \mathrm{Gal}(KE_i/E_i) \;\cong\; \mathrm{Gal}(KE/E),$$

given by restriction maps.
Let $\mathfrak{B}_E \in \mathcal{I}_E(m_1 \cdots m_r\, \mathfrak{m}\mathcal{O}_E)$ such that

$$\sigma = \left(\frac{\mathfrak{B}_E}{KE/E}\right)\Big|_K = \left(\frac{N_{E/F}\mathfrak{B}_E}{K/F}\right),$$

which exists by the consistency property and the surjectivity of the Artin map. Let

$$\mathfrak{b}_F = N_{E/F}\mathfrak{B}_E, \qquad \text{so that} \qquad \left(\frac{\mathfrak{b}_F}{K/F}\right) = \sigma.$$

Then

$$\left(\frac{\mathfrak{p}_i^{\gamma_i}\,\mathfrak{b}_F^{-d_i}}{K/F}\right) = \sigma^{d_i}\sigma^{-d_i} = 1.$$

But since $\mathfrak{p}_i$ splits completely in E_i/F, it is a norm of any prime of E_i lying above it. Thus $\mathfrak{p}_i^{\gamma_i}\mathfrak{b}_F^{-d_i}$ is a norm from E_i because $\mathfrak{b}_F$ is a norm from $E \supset E_i$. Hence

$$\mathfrak{p}_i^{\gamma_i}\,\mathfrak{b}_F^{-d_i} = N_{E_i/F}\,\mathfrak{U}_{E_i}$$

for some fractional ideal

$$\mathfrak{U}_{E_i} \in \mathcal{I}_{E_i}(m_i\,\mathfrak{m}\,\mathcal{O}_{E_i}).$$

The consistency property implies

$$\left(\frac{\mathfrak{U}_{E_i}}{KE_i/E_i}\right)\Big|_K = \left(\frac{\mathfrak{p}_i^{\gamma_i}\mathfrak{b}_F^{-d_i}}{K/F}\right) = 1.$$

And since $\mathrm{Gal}(KE_i/E_i) \cong \mathrm{Gal}(K/F)$, we have

$$\left(\frac{\mathfrak{U}_{E_i}}{KE_i/E_i}\right) = 1.$$

Observe that, thanks to 2. of Artin's Lemma, we have $KE_i \subset E_i(\zeta_{m_i})$. Exercise 2 of the exercise session tells us that Artin reciprocity holds for intermediate extensions of quasi-cyclotomic extensions. Hence Artin reciprocity holds for KE_i/E_i, so we get from the isomorphism $\overline{\mathcal{A}}$:

$$\mathfrak{U}_{E_i} = \langle \alpha_{E_i} \rangle\; N_{KE_i/E_i}\mathfrak{U}_{KE_i},$$

where

$$\alpha_{E_i} \overset{\times}{\equiv} 1 \pmod{m_i\mathfrak{m}\,\mathcal{O}_{E_i}}, \qquad \alpha_{E_i} \gg 0, \qquad \mathfrak{U}_{KE_i} \in \mathcal{I}_{KE_i}(m_i\mathfrak{m}\,\mathcal{O}_{KE_i}).$$

So

$$N_{E_i/F}(\alpha_{E_i}) \gg 0, \qquad N_{E_i/F}(\alpha_{E_i}) \overset{\times}{\equiv} 1 \pmod{m_i\mathfrak{m}}.$$

Thus

$$\begin{aligned}
\mathfrak{p}_i^{\gamma_i}\mathfrak{b}_F^{-d_i} &= N_{E_i/F}\mathfrak{U}_{E_i} \\
&= N_{E_i/F}\big(\langle \alpha_{E_i} \rangle\, N_{KE_i/E_i}\mathfrak{U}_{KE_i}\big) \\
&= \big\langle N_{E_i/F}(\alpha_{E_i}) \big\rangle\; N_{E_i/F}\, N_{KE_i/E_i}\mathfrak{U}_{KE_i} \\
&= \big\langle N_{E_i/F}(\alpha_{E_i}) \big\rangle\; N_{KE_i/F}\mathfrak{U}_{KE_i} \\
&\in \mathcal{P}^+_{F,m_i\mathfrak{m}}\,\mathcal{N}_{K/F}(m_i\mathfrak{m}).
\end{aligned}$$

And hence

$$\prod_{i=1}^{r} \mathfrak{p}_i^{\gamma_i}\mathfrak{b}_F^{-d_i} = \mathfrak{a}\,\mathfrak{b}_F^{-d_1-\cdots-d_r} \in \mathcal{P}^+_{F,\mathfrak{m}}\,\mathcal{N}_{K/F}(\mathfrak{m}).$$

But since $n \mid (d_1 + \cdots + d_r)$, there exists $d \in \mathbb{N}$ such that

$$-(d_1 + \cdots + d_r) = -dn.$$

Then

$$\mathfrak{a}\,(\mathfrak{b}_F^{-d})^{\,n} = \mathfrak{a}\,N_{K/F}(\mathfrak{b}_F^{-d}\mathcal{O}_K) \in \mathcal{P}^+_{F,\mathfrak{m}}\,\mathcal{N}_{K/F}(\mathfrak{m}).$$

But since $\mathfrak{b}_F \in \mathcal{I}_F(\mathfrak{m})$, we have that

$$N_{K/F}(\mathfrak{b}_F^{-d}\mathcal{O}_K) \in \mathcal{P}^+_{F,\mathfrak{m}}\,\mathcal{N}_{K/F}(\mathfrak{m}).$$

And thus

$$\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}\,\mathcal{N}_{K/F}(\mathfrak{m}),$$

as wanted. □

13.2 Idèlic Artin map

Let's try now to find an interpretation of Artin reciprocity in terms of idèles. If $\mathfrak{m}$ is chosen so that

$$\mathcal{E}_{F,\mathfrak{m}}^{+} \subset F^{\times} N_{K/F} J_K,$$

then we have

$$J_F/F^{\times} \;\cong\; J_{F,\mathfrak{m}}^{+}/F_{\mathfrak{m}}^{+} \;\longrightarrow\; \mathcal{I}_F(\mathfrak{m})/\mathcal{P}_{F,\mathfrak{m}}^{+},$$

via

$$\mathbf{a} \longmapsto (\alpha\mathbf{a})F_m^{+} \longmapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\iota_v(\alpha)a_v)},$$

where $\alpha \in F^{\times}$ is chosen so that $\alpha\mathbf{a} \in J_{F,\mathfrak{m}}^{+}$, so:

(i) for any finite place v of F, $\iota_v(\alpha) \in \mathcal{O}_v$, and $\iota_v(\alpha)a_v \equiv 1 \pmod{\mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}}$;

(ii) for any real place v of F, $\iota_v(\alpha)a_v > 0$.

It induces then

$$J_F \longrightarrow J_F/F^{\times}N_{K/F}J_K \;\cong\; \mathcal{I}_F(\mathfrak{m})/\mathcal{P}_{F,\mathfrak{m}}^{+}\mathcal{N}_{K/F}(\mathfrak{m}) \;\overset{\overline{\mathcal{A}}}{\cong}\; G,$$

and we denote the composition

$$\rho_{K/F} : J_F \longrightarrow \mathrm{Gal}(K/F).$$

We call this map the *idèlic Artin map*.

13.3 Quadratic reciprocity

In this section, we suppose that $F = \mathbb{Q}$, and

$$K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}\, p}\right), \qquad p > 2.$$

Then p is the only prime that ramifies in K/F, so the ideal $\mathfrak{m}$ in the statement of Artin reciprocity can be picked to be a power of $p\mathbb{Z}$. Consider the idèlic Artin map

$$\rho_{K/\mathbb{Q}} : J_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\},$$

and by Artin reciprocity

$$\ker(\rho_{K/\mathbb{Q}}) = \mathbb{Q}^{\times} N_{K/\mathbb{Q}} J_K.$$

Now let $q > 2$ be a prime of $\mathbb{Z}$, $p \neq q$, and let v_ℓ be a place of $\mathbb{Q}$. Define

$$\mathbf{b}_\ell = (1, \ldots, 1, q, 1, \ldots, 1) \in J_{\mathbb{Q}},$$

where q is in the component at v_ℓ. Observe that

$$\iota(q) \in \ker(\rho_{K/\mathbb{Q}}) = \mathbb{Q}^{\times} N_{K/\mathbb{Q}} J_K,$$

because

$$q \cdot N_{K/\mathbb{Q}}(\mathbf{1}) = q \cdot \mathbf{1} = \iota(q)$$

so if $q \neq \ell \neq p$,

$$\rho_{K/\mathbb{Q}}(\mathbf{b}_\ell) = \prod_v \left(\frac{\mathfrak{p}_v}{K/\mathbb{Q}}\right)^{\mathrm{ord}_v(b_v)} = 1.$$

Thus

$$1 = \rho_{K/\mathbb{Q}}(\iota(q)) = \prod_{v_\ell \in V_{\mathbb{Q}}} \rho_{K/\mathbb{Q}}(\mathbf{b}_\ell) = \rho_{K/\mathbb{Q}}(\mathbf{b}_p)\, \rho_{K/\mathbb{Q}}(\mathbf{b}_q).$$

Let's compute $\rho_{K/\mathbb{Q}}(\mathbf{b}_p)$ and $\rho_{K/\mathbb{Q}}(\mathbf{b}_q)$.
We have $\alpha\mathbf{b}_p \in J_{\mathbb{Q},\mathfrak{m}}^{+}$ for some $\alpha \in \mathbb{N}$ with

$$\alpha q \equiv 1 \pmod{p^{\mathrm{ord}_p(\mathfrak{m})}}.$$

By Artin reciprocity, we have that $\rho_{K/\mathbb{Q}}(\mathbf{b}_p) = 1$ if and only if

$$\mathbf{b}_p \in \mathbb{Q}^\times N_{K/\mathbb{Q}} J_K,$$

if and only if q is a norm from K_p to $\mathbb{Q}_p$. But $K_p/\mathbb{Q}_p$ is a totally ramified extension of degree 2, so the norm group has index 2 in

$$\mathcal{U}_p = \mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p),$$

where μ_{p-1} denotes the $(p-1)^{\text{th}}$ roots of unity in $\mathbb{Z}_p^\times$. Since p is odd, the only subgroup of index 2 is

$$\mu_{p-1}^2 \times (1 + p\mathbb{Z}_p) = (\mathbb{Z}_p^\times)^2.$$

Thus $\rho_{K/\mathbb{Q}}(\mathbf{b}_p) = 1$ if and only if q is a square modulo p, and since $\mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$ we get

$$\rho_{K/\mathbb{Q}}(\mathbf{b}_p) = \left(\frac{q}{p}\right).$$

Now we have $\alpha \mathbf{b}_q \in J^+_{\mathbb{Q},\mathfrak{m}}$ for $\alpha = 1$, and

$$\rho_{K/\mathbb{Q}}(\mathbf{b}_q) = \prod_v \left(\frac{\mathfrak{p}_v}{K/\mathbb{Q}}\right)^{\mathrm{ord}_v(\alpha(\mathbf{b}_q)_v)} = \left(\frac{q\mathbb{Z}}{K/\mathbb{Q}}\right).$$

Thus

$$\begin{aligned}
\rho_{K/\mathbb{Q}}(\mathbf{b}_q) = 1 &\iff \left(\frac{q\mathbb{Z}}{K/\mathbb{Q}}\right) = 1 \\
&\iff q\mathbb{Z} \text{ splits completely in } K/\mathbb{Q} \\
&\iff (-1)^{\frac{p-1}{2}} p \text{ is a square in } \mathbb{Z}_q \\
&\iff \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = 1 \quad (q \neq 2),
\end{aligned}$$

We used Corollary 5.2.9, P124 in the book of Nancy Childress to get the second equivalence. Since Euler's criterion tells us that

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$$

and that $\mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$, we deduce that

$$\rho_{K/\mathbb{Q}}(\mathbf{b}_q) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

And then we can deduce the quadratic reciprocity law

$$1 = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right),$$

i.e.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

13.4 Exercises week 13

1. In this exercise, you will prove the 'Artin Lemma' that was stated during the lecture. Its proof requires in its entirety multiple technical lemmas that build on each other. To simplify your work, we state here the last of those lemmas which will be the only one you use.

   Lemma 13.4. *Let F be a number field, $\mathcal{S}$ a finite set of primes in $\mathbb{Z}$, $\mathfrak{p}$ a prime of $\mathcal{O}_F$. Then for any integer $n > 1$, there exists $m \in \mathbb{Z}$, prime to $\mathcal{S}$ and to $\mathfrak{p}$, such that if ζ_m is a primitive m^{th}-root of unity, then*

   (a) $Gal(F(\zeta_m)/F) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

(b) $\left(\frac{p}{F(\zeta_m)/F}\right)$ *has order divisible by* n *in* $Gal(F(\zeta_m)/F)$.

(c) There is some $\tau \in Gal(F(\zeta_m)/F)$ *of order divisible by* n*, such that* τ *is independent to* $\left(\frac{p}{F(\zeta_m)/F}\right)$. *Note that this means here that* $\langle\tau\rangle \cap \langle\left(\frac{p}{F(\zeta_m)/F}\right)\rangle = 1$.

We recall here the statement of Artin's Lemma as you will prove it:

Lemma 13.5. *Let* K/F *be a cyclic extension of number fields of degree* n*,* $\mathcal{S}$ *a finite set of primes of* $\mathbb{Z}$*,* $\mathfrak{p}$ *a prime of* $\mathcal{O}_F$*. Then, there is some* $m \in \mathbb{Z}_+$ *prime to the elements of* $\mathcal{S}$ *and to* $\mathfrak{p}$*, and an extension* E/F *such that:*

(a) $K \cap E = F$

(b) $K(\zeta_m) = E(\zeta_m)$*, i.e.* $KE \subseteq K(\zeta_m) = E(\zeta_m)$

(c) $K \cap F(\zeta_m) = F$

(d) $\mathfrak{p}$ *splits completely in* E/F.

With all the setup being clear, we start the exercises:

(a) Use the given lemma to construct an adequate m and to prove *iii.* above, i.e. $K \cap F(\zeta_m) = F$. You may use freely the fact that there does not exist an everywhere unramified extension of $\mathbb{Q}$.

(b) Denote $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$. Describe the Galois group $\mathrm{Gal}(K(\zeta_m)/F)$ in terms of G and $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(F(\zeta_m)/F)$.

(c) Let τ be the morphism as obtained from 1). Define the subgroup H in $\mathrm{Gal}(K(\zeta_m)/F)$ to be the one generated by $\sigma \times \tau$ and $\left(\frac{\mathfrak{p}}{K(\zeta_m)/F}\right)$, and E to be its fixed field.

i. Prove that $\mathfrak{p}$ splits completely in E. (**Hint**: The decomposition group might be useful.)

ii. Prove that $K \cap E = F$, by showing that $\sigma \times 1$ fixes $K \cap E$.

(d) By 2., a generic element of H writes as

$$(\sigma \times \tau)^i \left(\left(\frac{\mathfrak{p}}{K/F}\right) \times \left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)\right)^j$$

and a generic element in $G \times 1$ writes as $\sigma^a \times 1$.

i. Compute the fixed field of $H \cap (G \times 1)$.

ii. Let $b \in H \cap (G \times 1)$. By comparing coordinate-wise, show that $b = 1$.

iii. Conclude.

2. Let $m > 0$. Let E/F be an extension of number fields such that $E \subset F(\zeta_m)$. Prove that Artin reciprocity holds for E assuming that Artin reciprocity holds for quasi-cyclotomic extensions.

3. Let K/F be an Abelian extension of number fields with $\mathrm{Gal}(K/F) = G$. Let $\sigma \in G$. Define

$$\mathcal{S}_\sigma = \left\{\text{primes } \mathfrak{p} \text{ of } \mathcal{O}_F : \ \mathfrak{p} \text{ is unramified in } K/F \text{ and } \left(\frac{\mathfrak{p}}{K/F}\right) = \sigma\right\}.$$

Show that $\delta_F(\mathcal{S}_\sigma) = \frac{1}{[K:F]}$.

(This exercise is one of the ingredients in the proof of the Chebotarev Density Theorem, see Exercise 5.10 for a proof of the Density Theorem and Exercise 5.11 for a nice application.)

4. Let K/F be an Abelian extension of number fields. We showed during lecture that the idelic Artin map is surjective with kernel $F^\times \tilde{N}_{K/F} J_K$.

   Reformulate the idelic Artin map such that the domain becomes $C_F = J_F/F^\times$. In particular, show that the new Artin map $C_F \to \mathrm{Gal}(K/F)$ is still surjective, but the kernel becomes $\tilde{N}_{K/F} C_K$.

14 Existence Theorem

14.1 Recap on basic results on Class Fields

The goal of this section is to prove the long-awaited Existence Theorem for class fields. Together with the results from the courses of the previous weeks, this completes the objectives stated in chapter 8, namely the Existence, Completeness and Isomorphy Theorems.
We begin by recalling some results and definitions from the previous sections. Let K/F be an abelian extension of number fields, and let $\mathfrak{m} \subseteq \mathcal{O}_F$ be an ideal such that

$$\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K.$$

Then we can define the idèlic Artin map $\rho_{K/F}$ as the composition

$$J_F \longrightarrow {}^{J_F}\!/_{F^\times N_{K/F} J_K} \xrightarrow{\cong} {}^{\mathcal{I}_F(\mathfrak{m})}\!/_{\mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m})} \xrightarrow{\cong} \mathrm{Gal}(K/F),$$

where the first homomorphism is the natural quotient map and the last homomorphism is induced by the Artin map. In particular, the kernel of the idèlic Artin map is given by $F^\times N_{K/F} J_K$, and we obtain an isomorphism

$${}^{J_F}\!/_{F^\times N_{K/F} J_K} \cong \mathrm{Gal}(K/F).$$

Recall further that for a tower of abelian extensions of number fields

$$F \subseteq K' \subseteq K,$$

we obtain the following commutative diagram

$$\begin{array}{ccc} J_F & \xrightarrow{\rho_{K/F}} & \mathrm{Gal}(K/F) \\ & \searrow^{\rho_{K'/F}} & \downarrow \\ & & \mathrm{Gal}(K'/F) \end{array} \tag{8}$$

where the vertical map is given by restriction of automorphisms to K'.
We also recall the notion of a class field in the idèlic language, which is the framework in which we will prove the Existence Theorem. Let $\mathcal{H}$ be an open subgroup of J_F containing $F^\times$. If $\mathcal{H} = F^\times N_{K/F} J_K$ for some abelian extension K/F, then K is called the class field of $\mathcal{H}$ over F. In this terminology, we already implicitly use the previously established uniqueness of the class field.
We are now ready to state the Existence Theorem in terms of idèles.

14.2 Existence Theorem

Theorem 14.1 (Existence)**.** *Every open subgroup $\mathcal{H} \subseteq J_F$ with $\mathcal{H} \supseteq F^\times$ is of the form*

$$\mathcal{H} = F^\times N_{K/F} J_K$$

for some (unique) finite abelian extension K/F.

The proof of this theorem is postponed to a later point in this section.
We observe, that using the relationship between the classical, ideal-theoretic formulation and the idèlic formulation of the theory established in the previous weeks, the Existence Theorem also yields the corresponding existence result in the classical theory.
Once this theorem has been proven, we obtain a bijective correspondence

$$\left\{ \begin{array}{c} \text{finite abelian} \\ \text{extensions } K/F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{open subgroups } \mathcal{H} \subseteq J_F \\ \text{with } F^\times \subseteq \mathcal{H} \end{array} \right\} \tag{9}$$

This correspondence is given by sending an extension K/F to the subgroup $F^\times N_{K/F} J_K$, and conversely by sending an open subgroup $\mathcal{H}$ to its class field. Note that we have already seen in Week 8 that class fields (defined in terms of ideals) are unique. We reprove this fact in the following proposition as a consequence of Artin reciprocity. In particular, this establishes part of the bijective correspondence stated above.

Proposition 14.2. *Let Φ be the map from finite abelian extensions K of F to open subgroups $\mathcal{H}$ of J_F containing $F^\times$, defined by*

$$\Phi(K) = F^\times N_{K/F} J_K.$$

Let K and K' be finite abelian extensions of F. Then:

(i) $K \subseteq K'$ *if and only if* $\Phi(K) \subseteq \Phi(K')$;

(ii) $\Phi(KK') = \Phi(K) \cap \Phi(K')$;

(iii) $\Phi(K \cap K') = \Phi(K)\Phi(K')$.

(iv) If $\mathcal{H} = \Phi(E)$ *and* $E \subseteq K$, *then* E *is the fixed field of* $\rho_{K/F}(\mathcal{H})$.

Proof. By Artin reciprocity, we have $\Phi(K) = \ker \rho_{K/F}$ and $\Phi(K') = \ker \rho_{K'/F}$.
We first prove part (ii). Using the commutativity of the diagram (8), we observe that

$$\ker \rho_{KK'/F} \subseteq \ker \rho_{K/F} \quad \text{and} \quad \ker \rho_{KK'/F} \subseteq \ker \rho_{K'/F}.$$

In particular,

$$\Phi(KK') \subseteq \Phi(K) \cap \Phi(K').$$

Conversely, let $\mathbf{a} \in \Phi(K) \cap \Phi(K')$. Then the element

$$\sigma = \left(\frac{\mathbf{a}}{KK'/F}\right) \in \mathrm{Gal}(KK'/F)$$

is trivial on both K and K'. Hence σ is trivial on KK', and we conclude that

$$\mathbf{a} \in \ker \rho_{KK'/F} = \Phi(KK').$$

This proves that $\Phi(KK') = \Phi(K) \cap \Phi(K')$.
Next we prove part (i). If $K \subseteq K'$, then

$$N_{K'/F} J_{K'} = N_{K/F}\big(N_{K'/K} J_{K'}\big) \subseteq N_{K/F} J_K,$$

where we use the compatibility of the norm maps in a tower of extensions and the fact that, by definition, the idèlic norm map $N_{K'/K}$ has image in J_K. This immediately implies

$$\Phi(K') = F^\times N_{K'/F} J_{K'} \subseteq F^\times N_{K/F} J_K = \Phi(K).$$

Conversely, assume that $\Phi(K') \subseteq \Phi(K)$. Then $\Phi(K') \cap \Phi(K) = \Phi(K')$, and by Artin reciprocity together with part (ii), we obtain

$$\begin{aligned}
[K' : F] &= \#\left(J_F / \Phi(K')\right) \\
&= \#\left(J_F / \Phi(K') \cap \Phi(K)\right) \\
&= \#\left(J_F / \Phi(KK')\right) \\
&= [KK' : F].
\end{aligned}$$

It follows that $K' = KK'$, and hence $K \subseteq K'$. This completes the proof of part (i).
The proofs of parts (iii) and (iv) are left as exercises. □

By part (i) of the above proposition, which is often referred to as the Ordering Theorem, we deduce that Φ is injective. Once the Existence Theorem has been established, we will also know that Φ is surjective, and the proof of the bijective correspondence (9) will be complete.
We now turn to a pair of auxiliary results that allow one to deduce the existence of new class fields from known ones.

Corollary 14.3. *Suppose K is the class field of an open subgroup $\mathcal{H} \subseteq J_F$ containing $F^\times$, and let $\mathcal{H}' \supseteq \mathcal{H}$ be an open subgroup of J_F. Then $\mathcal{H}'$ admits a class field over F.*

Proof. Let K' be the fixed field of $\rho_{K/F}(\mathcal{H}')$. We claim that

$$\ker \rho_{K'/F} = \mathcal{H}',$$

i.e., that K' is the class field of $\mathcal{H}'$ over F.
Note that $F \subseteq K' \subseteq K$. Moreover, by the commutativity of the diagram (8), we have for $\mathbf{a} \in J_F$

$$\left(\frac{\mathbf{a}}{K'/F}\right) = \left(\frac{\mathbf{a}}{K/F}\right)\Big|_{K'}.$$

Therefore,

$$\begin{aligned}
\mathbf{a} \in \ker \rho_{K'/F} &\iff \left(\frac{\mathbf{a}}{K/F}\right)\Big|_{K'} = 1 \\
&\iff \left(\frac{\mathbf{a}}{K/F}\right) \in \rho_{K/F}(\mathcal{H}') \\
&\iff \text{there exists } \mathbf{b} \in \mathcal{H}' \text{ with } \left(\frac{\mathbf{a}\mathbf{b}^{-1}}{K/F}\right) = 1 \\
&\iff \text{there exists } \mathbf{b} \in \mathcal{H}' \text{ with } \mathbf{a}\mathbf{b}^{-1} \in \ker \rho_{K/F} = \mathcal{H} \\
&\iff \mathbf{a} \in \mathcal{H}\mathcal{H}' = \mathcal{H}'.
\end{aligned}$$

□

Proposition 14.4 (Reduction Lemma)**.** *Let K/F be a cyclic extension of number fields, and let $\mathcal{H}$ be an open subgroup of J_F containing $F^\times$. Define*

$$\mathcal{H}_K = \{\mathbf{x} \in J_K : N_{K/F}(\mathbf{x}) \in \mathcal{H}\} = N_{K/F}^{-1}(\mathcal{H}).$$

If $\mathcal{H}_K$ has a class field over K, then $\mathcal{H}$ has a class field over F.

Proof. Let E be the class field of $\mathcal{H}_K$ over K. Then $\mathrm{Gal}(E/K)$ is abelian and

$$\mathcal{H}_K = K^\times N_{E/K} J_E = \ker \rho_{E/K}.$$

We first show that E/F is Galois. Let E' be the Galois closure of E/F, i.e., the smallest Galois extension of F containing E. It suffices to show that $E = E'$. Let $\sigma \in \mathrm{Gal}(E'/F)$. Then $\sigma|_K \in \mathrm{Gal}(K/F)$. Since K/F is cyclic, the idèlic norm map coincides with the map

$$s\big(\mathrm{Gal}(K/F)\big) \colon J_K \longrightarrow J_K$$

introduced in the discussion of Herbrand quotients and Tate cohomology. Explicitly, for $\mathbf{a} \in J_K$,

$$s\big(\mathrm{Gal}(K/F)\big)(\mathbf{a}) = \prod_{\tau \in \mathrm{Gal}(K/F)} \tau(\mathbf{a}).$$

It follows that

$$\begin{aligned}
N_{K/F}\big(\sigma(\mathbf{a})\big) &= \prod_{\tau \in \mathrm{Gal}(K/F)} \tau\big(\sigma(\mathbf{a})\big) \\
&= \prod_{\tau' \in \mathrm{Gal}(K/F)} \tau'(\mathbf{a}) = N_{K/F}(\mathbf{a}).
\end{aligned}$$

In particular,

$$\mathbf{a} \in \mathcal{H}_K \iff N_{K/F}(\mathbf{a}) \in \mathcal{H} \iff N_{K/F}\big(\sigma(\mathbf{a})\big) \in \mathcal{H} \iff \sigma(\mathbf{a}) \in \mathcal{H}_K.$$

Hence, one has $\sigma\mathcal{H}_K = \mathcal{H}_K$. We claim that σE is the class field of $\sigma\mathcal{H}_K$. By the uniqueness of the class field, it follows that $\sigma E = E$, and therefore $E = E'$. Thus E/F is Galois. It remains to justify the claim. Since K/F is Galois, every automorphism of E'/F preserves K. We obtain the following commutative diagram

$$\begin{array}{ccc}
J_K & \xrightarrow{\rho_{E/K}} & \mathrm{Gal}(E/K) \\
\Big\downarrow{\scriptstyle \sigma|_K} & & \Big\downarrow{\scriptstyle c_{\sigma|_E}} \\
J_K & \xrightarrow{\rho_{\sigma E/K}} & \mathrm{Gal}(\sigma E/K),
\end{array} \tag{10}$$

where $c_{\sigma|_E}$ denotes conjugation by $\sigma|_E$.
In particular, for $x \in J_K$ we have

$$\begin{aligned} x \in \ker \rho_{E/K} &\iff \rho_{E/K}(x) = 1 \\ &\iff \rho_{\sigma E/K}(\sigma x) = 1 \\ &\iff \sigma x \in \ker \rho_{\sigma E/K}. \end{aligned}$$

Since E is the class field associated to $\mathcal{H}_K$ over K, it follows that σE is the class field associated to $\sigma\mathcal{H}_K$ over K.
Next, we show that E/F is abelian. Let $\sigma \in \mathrm{Gal}(E/F)$ be such that $\sigma|_K$ generates $\mathrm{Gal}(K/F)$. This is possible since K/F is cyclic. Let $\tau \in \mathrm{Gal}(E/K)$. It suffices to show that σ and τ commute. Indeed, by the Galois correspondence we have

$$\mathrm{Gal}(E/F) = \bigsqcup_{i=1}^{[K:F]} \sigma^i \,\mathrm{Gal}(E/K),$$

and since $\mathrm{Gal}(E/K)$ is abelian, commutativity of σ with all elements of $\mathrm{Gal}(E/K)$ implies that $\mathrm{Gal}(E/F)$ is abelian.
As E/K is abelian, the idèlic Artin map $\rho_{E/K}$ exists and is surjective by Artin reciprocity. Thus there exists $\mathbf{b} \in J_K$ such that

$$\tau = \rho_{E/K}(\mathbf{b}).$$

Then by commutativity of diagram (10),

$$\sigma\tau\sigma^{-1} = \left(\frac{\sigma(\mathbf{b})}{\sigma E/\sigma K}\right) = \left(\frac{\sigma(\mathbf{b})}{E/K}\right).$$

As shown above,

$$N_{K/F}\big(\sigma(\mathbf{b})\big) = N_{K/F}(\mathbf{b}),$$

and hence $N_{K/F}\big(\sigma(\mathbf{b})\mathbf{b}^{-1}\big) = 1 \in \mathcal{H}$. Therefore

$$\sigma(\mathbf{b})\mathbf{b}^{-1} \in \mathcal{H}_K = \ker \rho_{E/K}.$$

It follows that

$$\sigma\tau\sigma^{-1} = \left(\frac{\sigma(\mathbf{b})}{E/K}\right) = \left(\frac{\mathbf{b}}{E/K}\right) = \tau.$$

Thus σ and τ commute, and we conclude that E/F is abelian.
Finally, since E is the class field of $\mathcal{H}_K$ over K, we have

$$\mathcal{H}_K = K^\times N_{E/K} J_E.$$

Moreover, by definition, $N_{K/F}\mathcal{H}_K \subseteq \mathcal{H}$. As we have shown that E/F is abelian, E is the class field over F of the subgroup $F^\times N_{E/F} J_E$ of J_F. Combining these observations, we obtain

$$F^\times N_{E/F} J_E \subseteq F^\times N_{K/F}\big(N_{E/K} J_E\big) \subseteq F^\times N_{K/F}\mathcal{H}_K \subseteq F^\times \mathcal{H} = \mathcal{H}.$$

By Corollary 14.3, we conclude that $\mathcal{H}$ has a class field over F, namely the fixed field of $\rho_{E/F}(\mathcal{H})$. □

We continue the reduction of the Existence Theorem by showing that the general case can be reduced to abelian extensions of finite exponent over fields containing the appropriate roots of unity. We then introduce a classification theorem for such extensions.

Definition 14.5. Let n be a positive integer. An abelian group G is said to have exponent n if $g^n = 1$ for every $g \in G$. Similarly, an abelian extension K/F is said to have exponent n if the abelian group $\mathrm{Gal}(K/F)$ has exponent n.

Remark 14.6. The present definition does not impose any minimality condition on n. In much of the literature, the exponent of an abelian group G is defined to be the smallest positive integer n such that $g^n = 1$ for all $g \in G$, provided such an integer exists. Throughout these notes, we will consistently use the above convention.

Let $\mathcal{H}$ be an open subgroup of J_F with $F^\times \subseteq \mathcal{H}$, and suppose that ${}^{J_F}\!/_{\mathcal{H}}$ has exponent n. Note that such an exponent exists since ${}^{J_F}\!/_{\mathcal{H}}$ is a finite group. Our goal is to relate the existence of a class field of $\mathcal{H}$ over F to a simpler existence problem.
Consider the extension $F(\zeta_n)/F$, where ζ_n denotes a primitive n^{th} root of unity. Since $\mathrm{Gal}\left(F(\zeta_n)/F\right)$ is abelian, and hence solvable, we may invoke the equivalent characterization of solvable finite groups to obtain a subnormal series whose successive quotients are cyclic. By Galois correspondence, this yields a tower of intermediate fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = F(\zeta_n)$$

such that each extension F_{i+1}/F_i is cyclic. For each i, define $\mathcal{H}_i = N^{-1}_{F_i/F}(\mathcal{H})$. By the compatibility of norm maps in a tower of extensions, we have

$$\mathcal{H}_i = N^{-1}_{F_i/F_{i-1}}(\mathcal{H}_{i-1}).$$

If we can show that $\mathcal{H}_t$ admits a class field over F_t, then we may apply the Reduction Lemma to the cyclic extension F_t/F_{t-1} to conclude that $\mathcal{H}_{t-1}$ admits a class field. Iterating this argument finitely many times, we ultimately deduce that $\mathcal{H}_0 = \mathcal{H}$ admits a class field over F.
We conclude that if ${}^{J_F}\!/_{\mathcal{H}}$ has exponent n, it suffices to treat the case where F contains μ_n, the group of all n^{th} roots of unity. The study of such extensions has its own terminology.

Definition 14.7. A finite abelian extension K/F is called a Kummer n-extension if $\mathrm{Gal}(K/F)$ has exponent n and F contains all the n^{th} roots of unity.

We now state a central result of Kummer theory, which studies such extensions.

Theorem 14.8. *Let F be a number field containing all the n^{th} roots of unity. There is a bijective correspondence between finite Kummer n-extensions K of F and subgroups W of $F^\times$ such that $(F^\times)^n \subseteq W$ and ${}^{W}\!/_{(F^\times)^n}$ is finite. The correspondence associates to the subgroup W the field $K = F(W^{1/n})$, for which we have $\mathrm{Gal}(K/F) \cong {}^{W}\!/_{(F^\times)^n}$.*

Proof. We first show that the map $W \mapsto F(W^{1/n})$ is well-defined. Let W be a subgroup of $F^\times$ with $(F^\times)^n \subseteq W$ and ${}^{W}\!/_{(F^\times)^n}$ finite. Choose elements $\alpha_1, \ldots, \alpha_r \in W$ whose images generate ${}^{W}\!/_{(F^\times)^n}$, and set

$$K = F(W^{1/n}) = F(\alpha_1^{1/n}, \ldots, \alpha_r^{1/n}).$$

Clearly, K/F is a finite extension. Since F contains all n^{th} roots of unity, it follows that K contains all conjugates of $\alpha_1^{1/n}, \ldots, \alpha_r^{1/n}$. In particular, K/F is Galois. Let $\sigma \in \mathrm{Gal}(K/F)$. Then for each i we have $\sigma(\alpha_i^{1/n}) = \zeta\, \alpha_i^{1/n}$ for some n^{th} root of unity ζ, since all conjugates of $\alpha_i^{1/n}$ are of this form. In particular, since $\zeta \in F$, we have $\sigma^n = 1$, and hence $\mathrm{Gal}(K/F)$ has exponent n. Moreover, the action of σ on the generators shows that $\mathrm{Gal}(K/F)$ is abelian. Thus K/F is a finite Kummer n-extension.
The remaining parts of the proof may be found in Childress, Theorem 7.7.2. □

We now introduce a theorem which, at first sight, concerns a rather special situation, but which will allow us to complete the proof of the Existence Theorem. We begin by fixing some notation.
Let F be a number field, and let $\mathcal{S}$ be a finite set of places of F such that $\mathcal{S}_\infty \subseteq \mathcal{S}$, where $\mathcal{S}_\infty$ denotes the set of infinite places of F. Define

$$J_{F,\mathcal{S}} = \prod_{v \in \mathcal{S}} F_v^\times \times \prod_{v \notin \mathcal{S}} \mathcal{U}_v,$$

which is an open subgroup of J_F, as well as

$$F_{\mathcal{S}} = J_{F,\mathcal{S}} \cap F^\times,$$

the group of $\mathcal{S}$-units of F, a discrete subgroup of $J_{F,\mathcal{S}}$. Note that $F_{\mathcal{S}}$ admits the equivalent description

$$F_{\mathcal{S}} = \left\{\alpha \in F^\times : \text{the factorization of } \langle\alpha\rangle \text{ involves no prime } \mathfrak{p}_v \text{ with } v \notin \mathcal{S}\right\}.$$

Lemma 14.9. *Let F be a number field. There exists a finite set of places $\mathcal{S} \supseteq \mathcal{S}_\infty$ such that*

$$J_F = F^\times J_{F,\mathcal{S}}.$$

Proof. A proof may be found in Childress, Lemma 7.2.2. □

This lemma allows us to formulate the following theorem, which is the key remaining ingredient in the proof of the Existence Theorem.

Theorem 14.10. *Let F be a number field containing all the n^{th} roots of unity. Let $\mathcal{S}$ be a finite set of places of F containing $\mathcal{S}_\infty$, all places v such that $\mathfrak{p}_v \mid n$, and sufficiently many finite places so that $J_F = F^\times J_{F,\mathcal{S}}$. Define*

$$B = \prod_{v\in\mathcal{S}} (F_v^\times)^n \times \prod_{v\notin\mathcal{S}} \mathcal{U}_v.$$

Then $F^\times B$ has class field $F(F_{\mathcal{S}}^{1/n})$ over F.

We postpone the proof of this theorem for the moment and explain how it implies the Existence Theorem.

Proof of Existence Theorem. Let F be a number field, and let $\mathcal{H}$ be an open subgroup of J_F containing $F^\times$. Let ${}^{J_F}\!/_{\mathcal{H}}$ have exponent n. As observed above, we may assume that F contains all the n^{th} roots of unity. Choose a finite set of places $\mathcal{S}$ as in Theorem 14.10, and enlarge $\mathcal{S}$ further so that it contains all places v for which $\mathcal{U}_v \not\subseteq \mathcal{H}$. By the construction of the topology on J_F, only finitely many such places exist.
For this enlarged set $\mathcal{S}$, we have $B \subseteq \mathcal{H}$. As $F^\times B$ admits a class field by Theorem 14.10, and since

$$\mathcal{H} = F^\times \mathcal{H} \supseteq F^\times B,$$

Corollary 14.3 applies. We conclude that $\mathcal{H}$ admits a class field over F. This completes the proof of the Existence Theorem. □

We will spend the remainder of this section proving Theorem 14.10 and discussing some of its consequences. To this end, we first introduce several auxiliary lemmas computing the cardinalities of certain group quotients that will play a central role in the proof.

Lemma 14.11. *If F contains all n^{th} roots of unity and $\mathcal{S} \supseteq \mathcal{S}_\infty$ is a finite set of places of F, then*

$$[F_{\mathcal{S}} : F_{\mathcal{S}}^n] = n^{\#\mathcal{S}}.$$

Proof. A proof of this result can be found in Childress, Corollary 7.2.4. □

Lemma 14.12. *Let v be a finite place of F, and let $n \in \mathbb{Z}_+$. If μ_n denotes the group of all n^{th} roots of unity, then*

(i) $[\mathcal{U}_v : \mathcal{U}_v^n] = \dfrac{1}{\|n\|_v} \#(F_v \cap \mu_n)$,

(ii) $[F_v^\times : (F_v^\times)^n] = \dfrac{n}{\|n\|_v} \#(F_v \cap \mu_n)$.

Proof. A proof of this result can be found in Childress, Lemma 7.2.5. □

With these lemmas at hand, we are now ready to prove Theorem 14.10.

Proof of Theorem 14.10. First observe that $F_{\mathcal{S}} \cap (F^\times)^n = F_{\mathcal{S}}^n$. Moreover,

$${}^{F_{\mathcal{S}}(F^\times)^n}\!/_{(F^\times)^n} \cong {}^{F_{\mathcal{S}}}\!/_{F_{\mathcal{S}} \cap (F^\times)^n} = {}^{F_{\mathcal{S}}}\!/_{F_{\mathcal{S}}^n},$$

which is a finite group of order $n^{\#\mathcal{S}}$ by Lemma 14.11. By Theorem 14.8, the field

$$K = F(F_{\mathcal{S}}^{1/n})$$

is the Kummer n-extension corresponding to the subgroup $F_{\mathcal{S}}(F^\times)^n \subseteq F^\times$, and the group ${}^{F_{\mathcal{S}}(F^\times)^n}\!/_{(F^\times)^n} \cong {}^{F_{\mathcal{S}}}\!/_{F_{\mathcal{S}}^n}$ is isomorphic to $\mathrm{Gal}(K/F)$.
Note that K is obtained by adjoining to F the roots of equations of the form

$$f(X) = X^n - \alpha$$

for $\alpha \in F_{\mathcal{S}}$. Let β be such a root. Then $f'(\beta) = n\beta^{n-1}$ is divisible only by primes corresponding to places in $\mathcal{S}$. Indeed, by assumption all places corresponding to primes dividing n lie in $\mathcal{S}$, and by the alternative description of $F_{\mathcal{S}}$ this property holds for α. Consequently, it also holds for β, since $\beta^n = \alpha$. It follows

that if $v \notin \mathcal{S}$, then the prime $\mathfrak{p}_v$ cannot ramify in K/F. Indeed, a standard result from algebraic number theory asserts that a prime $\mathfrak{p}$ can ramify in an extension $F(\beta)/F$ only if it divides the discriminant of the extension, or equivalently, only if it divides the derivative of the minimal polynomial of β evaluated at β. Since the minimal polynomial of β over F divides $f(X)$, it follows that its derivative evaluated at β divides $f'(\beta)$. Consequently, if $v \notin \mathcal{S}$, the prime $\mathfrak{p}_v$ cannot ramify in $F(\beta)/F$. As the field K is obtained by adjoining finitely many elements of the form β, the claim follows from the transitivity of ramification indices, and hence $\mathfrak{p}_v$ cannot ramify in K/F.
We next show that

$$F^\times B = F^\times N_{K/F} J_K.$$

We first prove the inclusion $F^\times B \subseteq F^\times N_{K/F} J_K$. Since $\mathrm{Gal}(K/F)$ has exponent n, any element $x \in (F_v^\times)^n$ for $v \in \mathcal{S}$ satisfies

$$\varphi_v(x) \in \ker \rho_{K/F} = F^\times N_{K/F} J_K,$$

where φ_v denotes the embedding of $x \in F_v^\times$ into J_F with all components equal to 1 except the v-component, which is equal to x. On the other hand, if $v \notin \mathcal{S}$ and $x \in \mathcal{U}_v$, then x is a local norm, since the norm map is surjective on units in unramified local extensions. By the definition of B, this shows that

$$F^\times B \subseteq F^\times N_{K/F} J_K.$$

It remains to prove the reverse inclusion. Since

$$[J_F : F^\times N_{K/F} J_K] = \#\,\mathrm{Gal}(K/F) = n^{\#\mathcal{S}}$$

by Artin reciprocity, and since we already have $F^\times B \subseteq F^\times N_{K/F} J_K$, it suffices to show that

$$[J_F : F^\times B] = n^{\#\mathcal{S}}.$$

Using the assumption $J_F = F^\times J_{F,\mathcal{S}}$, we compute

$$\begin{aligned}
[J_F : F^\times B] &= [F^\times J_{F,\mathcal{S}} : F^\times B] \\
&= \frac{[J_{F,\mathcal{S}} : B]}{[J_{F,\mathcal{S}} \cap F^\times : B \cap F^\times]} \\
&= \frac{\prod_{v\in\mathcal{S}} [F_v^\times : (F_v^\times)^n]}{[F_\mathcal{S} : B \cap F^\times]} \\
&= \frac{\prod_{v\in\mathcal{S}} \frac{n^2}{\|n\|_v}}{[F_\mathcal{S} : B \cap F^\times]} \qquad \text{by Lemma 14.12} \\
&= \frac{n^{2\#\mathcal{S}}}{[F_\mathcal{S} : B \cap F^\times]} \qquad \text{by the product formula.}
\end{aligned}$$

By Exercise 5 of Week 14, we have $B \cap F^\times = F_\mathcal{S}^n$. Since $[F_\mathcal{S} : F_\mathcal{S}^n] = n^{\#\mathcal{S}}$, by Lemma 14.11, the desired equality follows. This shows that K is the class field of $F^\times B$ over F. □

This completes the proofs of all the theorems announced in Week 8. In particular, we have finally established the generalization of Dirichlet's theorem on primes in arithmetic progressions: the existence of a class field for $\mathcal{P}_\mathfrak{m}^+$ is precisely what is required to show that the Weber L-functions satisfy

$$L_\mathfrak{m}(1, \chi) \neq 0$$

for every non-trivial character χ of $\mathcal{R}_\mathfrak{m}^+$.

14.3 Exercises week 14

Let F be a number field.

1. Let

$$\begin{array}{rccc}
\Phi: & \{\text{finite abelian extension } K \text{ of } F\} & \longrightarrow & \{\text{open subgroups } \mathcal{H} \text{ of } J_F \text{ that contains } F^\times\} \\
& K & \longmapsto & F^\times N_{K/F}\, J_F
\end{array}$$

Let K, K' be finite abelian field extensions of F. Show that Φ has the following properties

iii. $\Phi(K \cap K') = \Phi(K)\Phi(K')$.

iv. If $\mathcal{H} = \Phi(E) = F^\times N_{E/F} J_E$ and $K \supseteq E$, then E is the fixed field of $\rho_{K/F}(\mathcal{H})$.

2. The group of $\mathcal{S}$-idèle classes of F is

$$C_{F,\mathcal{S}} = {}^{C_F}\!/_{F_\mathcal{S}}.$$

We have $J_{F,\mathcal{S}} \subseteq J_F$ and $F_\mathcal{S} \subseteq F^\times$, so there a natural embedding $C_{F,\mathcal{S}} \hookrightarrow C_F$. Show that there is a topological and algebraic isomorphism

$${}^{J_F}\!/_{F^\times J_{F,\mathcal{S}}} \cong {}^{C_F}\!/_{C_{F,\mathcal{S}}}$$

3. Let $\mathcal{S} \subseteq V_F$ be a finite set of places of F, containing all infinite places.

(a) Let $\mathcal{S}_0 = \mathcal{S} - \mathcal{S}_\infty$ and

$$\begin{array}{rccc} \gamma : & F_\mathcal{S} & \longrightarrow & \mathcal{I}_{\mathcal{S}_0} \\ & \alpha & \longmapsto & \langle \alpha \rangle \end{array}$$

where $\mathcal{I}_{\mathcal{S}_0}$ is the group of fractional ideals of F generated by $\{\mathfrak{p}_v : v \in \mathcal{S}_0\}$. Show that there is an exact sequence

$$1 \longrightarrow \mathcal{O}_F^\times \longrightarrow F_\mathcal{S} \xrightarrow{\gamma} \mathcal{I}_{\mathcal{S}_0} \ .$$

(b) Show that $\gamma(F_\mathcal{S})$ is of rank $\#\mathcal{S}_0$.

(c) Show that $F_S \cong \mathcal{O}_F^\times \times \gamma(F_\mathcal{S})$.

(d) Conclude that

$$F_\mathcal{S} \cong \mathcal{W}_F \times \mathbb{Z}^{\#\mathcal{S}-1}$$

where $\mathcal{W}_F$ is the group of roots of unity in F.

4. We look at Kummer extension of some fields.

(a) What are the Kummer 2-extension of $\mathbb{Q}$?

(b) What if we add a third root of unity ? Namely, what are the Kummer 3-extension of $\mathbb{Q}(\zeta_3)$?

5. Let $n > 0$ and $\mathcal{S}$ be a finite set of places of F, where F contains all n-th root of unity. Moreover assume that for every prime $\mathfrak{p}_v$ dividing n, the associated finite place v belongs to $\mathcal{S}$ and that $\mathcal{S}$ contains all infinite places and is large enough so that $J_F = F^\times J_{F,\mathcal{S}}$. Finally let

$$B = \prod_{v \in \mathcal{S}} (F_v^\times)^n \times \prod_{v \notin \mathcal{S}} \mathcal{U}_v.$$

Show that $B \cap F^\times = F_\mathcal{S}^n$.

15 Solutions

15.1 Week 1 solutions by Pierre Emmanuel Augustin Descombes

1. (a) Given $a \in A$, consider the polynomial:

$$f(X) = \prod_{\sigma \in G} (X - \sigma(a))$$

(here one use the fact that G is finite): it is a monic polynomial with root a. As $\sigma(f(X)) = f(\sigma(X))$ for all $\sigma \in G$, $f \in A^G[X]$, hence by definition a is integral over A^G, and furthermore A is integral over A^G.

(b) Consider $\mathfrak{q}_1, \mathfrak{q}_2 \in P$, we will show that $\mathfrak{q}_2 = \sigma(\mathfrak{q}_1)$ for some $\sigma \in G$. Consider $a \in \mathfrak{q}_2$, then

$$b := \prod_{\sigma \in G} \sigma(a) = a \cdot \prod_{\sigma \neq 1} \sigma(a) \in \mathfrak{q}_2$$

but b is by construction G-invariant, i.e.:

$$b \in \mathfrak{q}_2 \cap A^G = \mathfrak{p} = \mathfrak{q}_2 \cap A^G \subset \mathfrak{q}_1$$

but, as $\mathfrak{q}_1$ is prime, there is some $\sigma \in G$ such that $\sigma^{-1}(a) \in \mathfrak{q}_1$, i.e. $a \in \sigma(\mathfrak{q}_1)$. Such a σ exists for any $a \in \mathfrak{q}_2$, hence we have:

$$\mathfrak{q}_2 \subset \bigcup_{\sigma \in G} \sigma(\mathfrak{q}_1)$$

but, if an ideal is contained in a finite union of prime ideals, then it is contained in one of those prime ideal (this is the prime avoidance lemma, which can be proven by induction over n). Then there is some $\sigma \in G$ such that $\mathfrak{q}_2 \subset \sigma(\mathfrak{q}_1)$. Similarly, there is some $\sigma' \in G$ such that $\mathfrak{q}_1 \subset \sigma'(\mathfrak{q}_2)$, such that:

$$\mathfrak{q}_2 \subset \sigma(\mathfrak{q}_1) \subset \sigma'\sigma(\mathfrak{q}_2) \subset \cdots \subset (\sigma'\sigma)^n(\mathfrak{q}_2) \subset$$

but, as G is finite, $\sigma'\sigma$ has finite order, hence this sequence of inclusion is a sequence of equality, and then $\mathfrak{q}_2 = \sigma(\mathfrak{q}_1)$ as claimed.

2. We compute the norm of the given generators of J:

$$\begin{aligned} N(a + b\sqrt{-5}) := (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \\ N(2) = 4 \\ N(1 + \sqrt{-5}) = 6 \end{aligned}$$

Supposing that $J = (\alpha)$ for $\alpha \in \mathbb{Z}[\sqrt{-5}]$, we will raise a contradiction. Then α would divide 2 and $1 + \sqrt{-5}$, hence, by multiplicativity of the norm, α would divide 4 and 6, i.e. $N(\alpha) = 2$ or $N(\alpha) = 1$. There is no element of norm 2, hence $N(\alpha) = 1$, $\alpha = \pm 1$ and $J = \mathbb{Z}[\sqrt{-5}]$. But, reducing modulo 2, one obtains the ideal $\hat{J} \subset \mathbb{F}_2[\sqrt{-5}] = \mathbb{F}_2$ (i.e., 1 is a square root of -5 in $\mathbb{F}_2$). But $\hat{2} = 0 \in \mathbb{F}_2$, and $1 + \hat{\sqrt{-5}} = 1 + 1 = 0 \in \mathbb{F}_2$, hence $\hat{J} = \{0\} \subsetneq \mathbb{F}_2$, hence $J \subsetneq \mathbb{Z}[\sqrt{-5}]$, giving a contradiction. Then J is not principal, i.e. there is a non principal ideal in $\mathbb{Z}[\sqrt{-5}]$, which is the ring of integer in $\mathbb{Q}[\sqrt{-5}]$ (as $-5 \equiv 3 \pmod 4$), hence by definition the ideal class group of $\mathbb{Q}[\sqrt{-5}]$ is not trivial.

3. Consider the extension $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$, we have:

- $(3) = (\sqrt{-3})^2$, i.e. the prime ideal (3) of $\mathbb{Z}$ is ramified in the extension $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$.
- $3 \equiv 4^2 \pmod{13}$, in particular $(13) = (4 - \sqrt{3})(4 + \sqrt{3})$, hence the prime ideal (3) of $\mathbb{Z}$ is completely split in $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$. In particular, it is also unramified.
- 3 is not a prime modulo 5, hence the polynomial $X^2 - 3$ is irreducible modulo 5, i.e. (5) is still prime in $\mathbb{Z}[\sqrt{3}]$, and then 5 is inert in $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$. In particular, it is also unramified.

4. First, we use the recursive definition of the cyclotomic polynomial:

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

as this definition works over any ring: in particular, the reduction $(\Phi_n)_p \in \mathbb{F}_p[X]$ of the cyclotomic polynomial still verify this definition. For any d, $(\Phi_d)_p(X)|X^d - 1$, i.e. a root of $(\Phi_d)_p(X)$ is a d-th root of unity. We prove by induction that the roots of $(\Phi_n)_p(X)$ are exactly the n-th root of unity. For $n = 1$, this is trivial. Assume that we have proven it for any $d|n$ such that d is not n: then, in the decomposition:

$$X^n - 1 = (\Phi_n)_p(X) \times \prod_{d|n, d\neq n} (\Phi_d)_p(X)$$

we have that the roots of the second members are exactly the primitive d-th roots of unity for any d dividing strictly n, hence by definition the roots of $(\Phi_n)_p(X)$ are exactly the primitive n-th roots of unity in $\mathbb{F}_p$.

By definition, the primitive n-th roots of unity in $\mathbb{F}_p$ are the elements of order exactly n in the multiplicative group $\mathbb{F}_p^\times$. Then $(\Phi_n)_p(X)$ is a product of linear factors in $\mathbb{F}_p[X]$, i.e. $\Phi_n(X)$ completely splits modulo p, iff $\mathbb{F}_p^\times$ contains $\varphi(n)$ elements of order n (where we denote by $\varphi(n)$ the numbers of $1 \leq m \leq n-1$ which are prime to n). But $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, hence it contains a cyclic group of order n (which contains then $\varphi(n)$ elements of order n) iff $n|p-1$, i.e. $n \equiv 1 \pmod{p}$. Then $\mathbb{F}_p$ has $\varphi(n)$ distinct primitive n-th roots of unity iff $n \equiv 1 \pmod{p}$.

15.2 Week 2 solutions by Raphaël Augustin Parriaux

1. (a) From the course, we know that $Z(\mathfrak{P}/\mathfrak{p}) \cong Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ and that the Frobenius element

$$\left(\frac{\mathfrak{P}}{K/F}\right) \in Z(\mathfrak{P}/\mathfrak{p}) \subset G$$

is the image by that isomorphism of the generator $\varphi_\mathfrak{p} \in Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ with

$$\varphi_\mathfrak{p}(x) = x^{N\mathfrak{p}} \quad \forall x \in \mathbb{F}_\mathfrak{P}$$

with $N\mathfrak{p} = |\mathbb{F}_\mathfrak{p}|$. From that definition and the fact that the elements of $Z(\mathfrak{P}/\mathfrak{p})$ send $\mathfrak{P}$ to itself, we directly get that

$$\left(\frac{\mathfrak{P}}{K/F}\right)(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_K.$$

To show unicity, we now let $\sigma \in G$ with

$$\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \forall\, \alpha \in \mathcal{O}_K,$$

From that property, it is obvious that σ sends $\mathfrak{P}$ to itself, meaning i.p. that $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$. Through the isomorphism $Z(\mathfrak{P}/\mathfrak{p}) \cong Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, we see that σ induces the same automorphism $\varphi_\mathfrak{p}$ on $\mathbb{F}_\mathfrak{P}$ as $\left(\frac{\mathfrak{P}}{K/F}\right)$, i.e.

$$\sigma = \left(\frac{\mathfrak{P}}{K/F}\right)$$

(b) Let K/F be abelian, $F \subset L \subset K$ some intermediate extension, and $\mathfrak{p} \subset \mathcal{O}_F$ an unramified prime in K. Choose a prime $\mathfrak{P} \subset \mathcal{O}_K$ above $\mathfrak{p}$ and let $\mathfrak{P}_L = \mathfrak{P} \cap \mathcal{O}_L$.
By definition $\left(\frac{\mathfrak{p}}{K/F}\right) \in \mathrm{Gal}(K/F)$ (which is independent of $\mathfrak{P}$ as seen in class) is the unique element inducing the map $x \mapsto x^{N\mathfrak{p}}$ on $\mathbb{F}_\mathfrak{P}$. Its restriction $\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L \in \mathrm{Gal}(L/F)$ stabilizes $\mathfrak{P}_L$ as it stabilizes $\mathfrak{P}$ and therefore induces an automorphism of the residue field $\mathbb{F}_{\mathfrak{P}_L} = \mathcal{O}_L/\mathfrak{P}_L$. But $\mathbb{F}_{\mathfrak{P}_L} \subset \mathbb{F}_\mathfrak{P}$ therefore the map $\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L$ with domain $\mathbb{F}_{\mathfrak{P}_L}$ is defined directly by what $\left(\frac{\mathfrak{p}}{K/F}\right)$ does on $\mathbb{F}_\mathfrak{P}$, i.e.

$$\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L(x) = \left(\frac{\mathfrak{p}}{K/F}\right)(x) = x^{N\mathfrak{p}},$$

for all $x \in \mathbb{F}_{\mathfrak{P}_L}$ so $\left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L$ induces the map $x \mapsto x^{N\mathfrak{p}}$ on $\mathbb{F}_{\mathfrak{P}_L}$ which is exactly the map $\left(\frac{\mathfrak{p}}{L/F}\right)$.

2. (a) Let $K = \mathbb{Q}(\zeta_m),\ \zeta = \zeta_m,\ G = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.
Let a prime $\mathfrak{p}$ and a prime $\mathfrak{P}$ of $\mathcal{O}_K$ above $\mathfrak{p}$. For an element $x \in \mathcal{O}_K$ or O_F, denote by $\overline{x}$ its class in $\mathbb{F}_\mathfrak{P}$ or $\mathbb{F}_\mathfrak{p}$ respectively. Consider the inertia group

$$T := T(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(x) \equiv x \mod \mathfrak{P} \quad \forall x \in \mathcal{O}_K\} \subset Z(\mathfrak{P}/\mathfrak{p})$$

i.e. the kernel of the natural surjection $\varphi : Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$.
We have the following equality for the ramification index: $e = |T|$. In particular, $\mathfrak{p}$ is ramified iff T is non-trivial.
Now note that each $\sigma \in G$ has the form $\sigma_a(\zeta) = \zeta^a$ for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Let $\sigma_a \in T$, then by definition

$$\varphi(\sigma_a) = Id_{\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})}$$

In particular, this is equivalent to $\overline{\zeta^a} = \overline{\zeta}$ in $\mathbb{F}_\mathfrak{P}$

If $p \nmid m$, then by part (b) the reduction map on the set of m-th roots of unity is injective modulo $\mathfrak{P}$. Therefore $\overline{\zeta^a} = \overline{\zeta}$ implies $\zeta^a = \zeta$, hence $a \equiv 1 \pmod m$. Therefore $\sigma_a = \mathrm{id}$, so T is trivial and $\mathfrak{p}$ is unramified.

If $p \mid m$, write $m = p^r m'$ with $r \geq 1$ and $p \nmid m'$.
By the chinese remainder theorem we have

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times.$$

Consider $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that

$$a \equiv 1 \pmod{m'} \quad \text{but} \quad a \not\equiv 1 \pmod{p^r}.$$

Such an a exists since $(\mathbb{Z}/p^r\mathbb{Z})^\times$ contains nontrivial units. Then ζ^{a-1} is a p^r-th root of unity, in particular

$$\overline{\zeta^{a-1}} = 1 \quad \Rightarrow \quad \overline{\zeta^a} = \overline{\zeta}.$$

Therefore $\sigma_a \in T$. But since $a \not\equiv 1 \pmod m$, we have $\sigma_a \neq \mathrm{id}$, hence T is nontrivial and $\mathfrak{p}$ ramifies in K.

(b) Let $p \nmid m$ and $\mathfrak{P} \subset \mathcal{O}_K$ a prime above $\mathfrak{p} = p\mathbb{Z}$. Suppose $\zeta, \zeta' \in \mu_m := \{x \in K : x^m = 1\}$ satisfy

$$\overline{\zeta} = \overline{\zeta'} \quad \text{in } \mathbb{F}_\mathfrak{P}.$$

Note that $\overline{\zeta}^m = \overline{\zeta'}^m = 1$ in $\mathbb{F}_\mathfrak{P}$, i.e. the common reduction is a root of $X^m - 1$ over $\mathbb{F}_\mathfrak{P}$. Since $p \nmid m$ we have

$$\frac{d}{dX}(X^m - 1) = mX^{m-1} \not\equiv 0 \pmod p,$$

so the polynomial $X^m - 1$ is separable modulo p and therefore has exactly m distinct roots in $\overline{\mathbb{F}_\mathfrak{p}}$.
The elements of μ_m are m distinct roots of $X^m - 1$ in K, and their reductions (viewed in $\overline{\mathbb{F}_\mathfrak{P}}$) must therefore be m distinct roots of $X^m - 1$ as well. If two distinct m-th roots of unity in K had the same reduction, this would yield fewer than m distinct roots after reduction, contradicting separability. Hence no two distinct elements of μ_m can have the same reduction, and $\overline{\zeta} = \overline{\zeta'}$ implies $\zeta = \zeta'$.

(c) For $p \nmid m$, the Frobenius automorphism $\left(\frac{\mathfrak{P}}{K/F}\right)$ satisfies $\left(\frac{\mathfrak{P}}{K/F}\right)(\zeta) \equiv \zeta^p \ mod\ \mathfrak{P}$ for all $\zeta \in \mathcal{O}_K$ by 1(a). By 2(b), reduction modulo $\mathfrak{P}$ is injective on m-th roots of unity, hence $\left(\frac{\mathfrak{P}}{K/F}\right)(\zeta) = \zeta^p$. Identifying $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ via $\zeta \mapsto \zeta^a$, the Artin automorphism corresponds to $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$.

3. First, let us clarify the exercise statement. As seen in class, the absolute discriminant of $K = \mathbb{Q}(\zeta_p)$ is a module (ideal) in the principal ring $\mathbb{Z}$ with generator $d(v_1, \ldots, v_n)$ where $\{v_1, \ldots, v_n\}$ is any integral basis of $\mathcal{O}_K$ (a change in $\mathbb{Z}$-basis equates to multiplying by a matrix A with $det(A)^2 = 1$ hence all basis here have the same discriminant). Our goal rather than to compute the module d_K is to compute the discriminant of any integral basis of $\mathcal{O}_K$.

Let $n = [K : \mathbb{Q}] = p - 1$, and consider the integral basis $\{1, \zeta_p, \ldots, \zeta_p^{n-1}\}$ of $\mathcal{O}_K$. As seen in class, the discriminant of this basis is

$$d(1, \zeta_p, \ldots, \zeta_p^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\zeta_p) - \sigma_j(\zeta_p))^2,$$

where σ_k are the embeddings $K \hookrightarrow \mathbb{C}$ given by $\sigma_k(\zeta_p) = \zeta_p^k$. Hence,

$$d(1, \zeta_p, \ldots, \zeta_p^{n-1}) = \prod_{1 \le i < j \le n} (\zeta_p^i - \zeta_p^j)^2.$$

Factor ζ_p^i from each term: $\zeta_p^i - \zeta_p^j = \zeta_p^i(1 - \zeta_p^{j-i})$, so

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

Let us compute these products. For the first product:

$$\Big(\prod_{1 \le i < j \le n} \zeta_p^i \Big)^2 = \zeta_p^{2 \sum_{1 \le i < j \le n} i} = \zeta_p^{2 \sum_{i=1}^{n-1} i(n-i)} = \zeta_p^{\frac{n(n-1)(n+1)}{3}} = \zeta_p^{\frac{p(p-1)(p-2)}{3}}$$

If $p > 3$, then $\frac{(p-1)(p-2)}{3} \in \mathbb{Z}$ and $p \mid \frac{p(p-1)(p-2)}{3}$, meaning that $\left(\prod_{1 \le i < j \le n} \zeta_p^i \right)^2 = 1$.

For $p = 3$ then $\left(\prod_{1 \le i < j \le n} \zeta_p^i \right)^2 = \zeta_3^2$.

For the second product, consider the pairs $1 \le i < j \le n$. For each $k = j - i$, the number of pairs with difference k is $n - k = p - 1 - k$, so

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

Using the equality $1 - \zeta_p^{p-k} = -\zeta_p^{-k}(1 - \zeta_p^k)$ and pairing k with $p - k$ for $k \in \{2, \ldots, \frac{p-1}{2}\}$:

$$\begin{aligned}
&(1 - \zeta_p^k)^{2(p-1-k)} (1 - \zeta_p^{p-k})^{2(p-1-(p-k))} \\
&= (-1)^{2(k-1)} \zeta_p^{-2k(k-1)} (1 - \zeta_p^k)^{2(p-1-k)} (1 - \zeta_p^k)^{2(k-1)} \\
&= \zeta_p^{-2k(k-1)} (1 - \zeta_p^k)^{2(p-2)} \\
&= \zeta_p^{-2k(k-1)} \big(-\zeta_p^k (1 - \zeta_p^k)(1 - \zeta_p^{p-k}) \big)^{p-2} \\
&= (-1)^{p-2} \zeta_p^{-2k^2} \big((1 - \zeta_p^k)(1 - \zeta_p^{p-k}) \big)^{p-2}
\end{aligned}$$

Which allows us to write

$$\begin{aligned}
\Big(\prod_{k=1}^{p-2} (1 - \zeta_p^k)^{p-1-k} \Big)^2 &= (1 - \zeta_p)^{2(p-2)} \Big(\prod_{k=2}^{(p-1)/2} (-1)^{p-2} \zeta_p^{-2k^2} \big((1 - \zeta_p^k)(1 - \zeta_p^{p-k}) \big)^{p-2} \Big) \\
&= (1 - \zeta_p)^{p-2} \Big(\prod_{k=2}^{(p-1)/2} (-1)^{p-2} \zeta_p^{-2k^2} \Big) \Big(\prod_{k=1}^{p-2} (1 - \zeta_p^k) \Big)^{p-2} \\
&= -\zeta_p^{p-2} (1 - \zeta_p^{p-1})^{p-2} \Big(\prod_{k=2}^{(p-1)/2} (-1)^{p-2} \zeta_p^{-2k^2} \Big) \Big(\prod_{k=1}^{p-2} (1 - \zeta_p^k) \Big)^{p-2} \\
&= \zeta_p^{-2} \Big(\prod_{k=1}^{(p-1)/2} (-1)^{p-2} \Big) \Big(\prod_{k=2}^{(p-1)/2} \zeta_p^{-2k^2} \Big) \Big(\prod_{k=1}^{p-1} (1 - \zeta_p^k) \Big)^{p-2} \\
&= \Big(\prod_{k=1}^{(p-1)/2} (-1) \Big) \Big(\prod_{k=1}^{(p-1)/2} \zeta_p^{-2k^2} \Big) \Big(\prod_{k=1}^{p-1} (1 - \zeta_p^k) \Big)^{p-2} \\
&= (-1)^{\frac{p-1}{2}} \zeta_p^{-\frac{p(p-1)(p+1)}{12}} \Big(\prod_{k=1}^{p-1} (1 - \zeta_p^k) \Big)^{p-2}
\end{aligned}$$

Differentiating the equality $X^p - 1 = (X-1)\prod_{k=1}^{p-1}(X-\zeta_p^k)$ and evaluating at $X=1$ gives $\prod_{k=1}^{p-1}(1-\zeta_p^k) = p$. Hence

$$\Big(\prod_{k=1}^{p-2}(1-\zeta_p^k)^{p-1-k}\Big)^2 = (-1)^{\frac{p-1}{2}}\zeta_p^{-\frac{p(p-1)(p+1)}{12}}p^{p-2}.$$

If $p>3$, then $\frac{(p-1)(p+1)}{12} \in \mathbb{Z}$ hence $\zeta_p^{-\frac{p(p-1)(p+1)}{12}} = 1$.

For $p=3$, $\zeta_p^{-\frac{p(p-1)(p+1)}{12}} = \zeta_3$. Remember the equality $\Big(\prod_{1\le i<j\le n}\zeta_p^i\Big)^2 = \zeta_3^2$ for $p=3$, the multiplication of those terms gives us 1, and indeed for any odd prime p, we obtain

$$d(1,\zeta_p,\dots,\zeta_p^{n-1}) = (-1)^{\frac{p-1}{2}}p^{p-2}.$$

4. (a) As in ex. 3, we are looking to compute the discriminant of an integral basis of $K=\mathbb{Q}(\sqrt{d})$. It is clear the the embeddings $\sigma : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ are entirely determined by the image of $\sqrt{d}$. In particular, the image $\sigma(\sqrt{d})$ must also be a zero of the quadratic polynomial x^2-d. This implies that the unique non trivial embedding $\mathbb{K}\hookrightarrow\overline{\mathbb{Q}}$ sends $\sqrt{d}$ to $-\sqrt{d}$. Characterising these embeddings justifies the computations of d_K that we are about to do.

   If $d \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big]$ with integral basis $\Big\{1, \frac{1+\sqrt{d}}{2}\Big\}$. By definition, the discriminant is

$$d_K = \det\begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2}\end{pmatrix}^2 = d.$$

   If $d \equiv 2,3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ with integral basis $\{1,\sqrt{d}\}$. As justified above, the discriminant is

$$d_K = \det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d}\end{pmatrix}^2 = 4d.$$

   (b) Write $\mathfrak{p} = p\mathbb{Z}$ and let $\mathfrak{P}\subset\mathcal{O}_K$ be a prime lying above $\mathfrak{p}$. By definition, p being unramified in $K/\mathbb{Q}$ means $p\nmid d_K$. By part (a) it follows in particular that $p\nmid d$.

   By definition, the Frobenius element $\Big(\frac{\mathfrak{p}}{K/\mathbb{Q}}\Big) \in \mathrm{Gal}(K/\mathbb{Q})$ satisfies

$$\Big(\frac{\mathfrak{p}}{K/\mathbb{Q}}\Big)(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}} \qquad \text{for all } \alpha\in\mathcal{O}_K.$$

   We apply this to $\alpha=\sqrt{d}$. Euler's criterion in the residue field $\mathbb{F}_{\mathfrak{P}}$ gives

$$\sqrt{d}^{\,p-1} = d^{\frac{p-1}{2}} \equiv \Big(\frac{d}{p}\Big) \pmod{\mathfrak{P}},$$

   so multiplying by $\sqrt{d}$ yields

$$\Big(\frac{\mathfrak{p}}{K/\mathbb{Q}}\Big)(\sqrt{d}) \equiv \Big(\frac{d}{p}\Big)\sqrt{d} \pmod{\mathfrak{P}}.$$

   The reductions of $\sqrt{d}$ and $-\sqrt{d}$ are distinct: if $\sqrt{d}\equiv -\sqrt{d} \pmod{\mathfrak{P}}$ then $2\sqrt{d}\in\mathfrak{P}$, which cannot happen because p is odd and $p\nmid d$. Thus reduction modulo $\mathfrak{P}$ distinguishes the two galois images, so the congruence above implies the following equality for the Frobenius element

$$\Big(\frac{\mathfrak{p}}{K/\mathbb{Q}}\Big) = \Big(\frac{d}{p}\Big) \in \mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$$

   Finally, since p is odd and $p\nmid d_K$, we have $(\frac{4}{p})=1$, so $(\frac{d_K}{p}) = (\frac{d}{p})$ and we get the desired result.

15.3 Week 3 solutions by Damien Ganaël Bridel

1. We know that the degree of the extension $F/\mathbb{Q}$ is equal to $[F:\mathbb{Q}] = r + 2s$ where r is the number of real embeddings and s the number of pairs of complex embeddings.
We want to find the embeddings of the field $F = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. First notice that there are embeddings that sends $\sqrt{3} \to \pm\sqrt{3}$ and $\sqrt{7} \to \pm\sqrt{7}$. Choosing every combination of plus and minus makes already 4 different real embeddings.
Notice that $[F:\mathbb{Q}] \geq 4$ since $1, \sqrt{3}, \sqrt{7}$ and $\sqrt{21}$ are linearly independent (where F is seened as a $\mathbb{Q}-$vector space). Hence $r = 4$ and $s = 0$.
Also we know that $\mathcal{O}_F^\times = W_F \times \mathbb{Z}^{r+s-1} = W_F \times \mathbb{Z}^3$ where W_F is the group of unity of F (setwise we have $W_F = \mathcal{U}_1 \cap F$ where $\mathcal{U}_1 \subset \mathbb{C}$ is the unit circle). In this case, $W_F \cong \mathbb{Z}/2\mathbb{Z}$ corresponding to $\pm 1 \subset \mathcal{U}_1$.
To find explicit generators of the free part of $\mathcal{O}_F^\times$, we want to find $a, b \in \mathbb{Z}$ such that $a + b\sqrt{d}$ is of norm 1 for $d = 3, 7, 21$. Such integers would satisfy: $1 = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$. Checking for small values of a and b, we find generators: $\{2 + \sqrt{3}, 8 + 3\sqrt{7}, 55 + 12\sqrt{21}\}$.

   Now the same for $F' = \mathbb{Q}(\sqrt{3}, \sqrt{7}, i)$. There are already 4 pairs of complex embeddings that sends $\sqrt{3} \to \pm\sqrt{3}$, $\sqrt{7} \to \pm\sqrt{7}$ and $i \to \pm i$. Again notice that $[F':\mathbb{Q}] \geq 8$ since $1, \sqrt{3}, \sqrt{7}, \sqrt{21}, i, i\sqrt{3}, i\sqrt{7}$ and $i\sqrt{21}$ are linearly indepedant. Hence $r = 0$ and $s = 4$.
Notice that $F' \cap \mathcal{U}_1 = \{\pm 1, \pm i\}$ so we have that $W_{F'} = \mathbb{Z}/4\mathbb{Z} \implies \mathcal{O}_{F'}^\times = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}^3$.
Using the same logic as for the group $\mathcal{O}_F^\times$, we find generators of the free part of the unit group $\mathcal{O}_K^\times$: $\{i, 2 + \sqrt{3}, 8 + 3\sqrt{7}, 55 + 12\sqrt{21}\}$

2. (a) We want to find integers $a_0, a_1, ...$ with $a_i \in \{0, ..., 6\}$ such that

$$\frac{1}{6} = a_0 + a_1 7 + a_2 7^2 + a_3 7^3 + ...$$

   We begin with a_0, it must satisfy $6a_0 \equiv 1 \pmod 7$. Since $6^2 = 36 \equiv 1 \pmod 7$, we have that $a_0 = 6$.
Next, a_1 must satisfy $6(6+7a_1) \equiv 1 \pmod{49} \iff 36+42a_1 \equiv 1 \pmod{49} \iff 42a_1 \equiv -35 \equiv 14 \pmod{49}$. Dividing by 7 we have

$$6a_1 \equiv 2 \pmod 7 \iff a_1 \equiv 6^{-1} \cdot 2 \equiv 6 \cdot 2 \equiv 5 \pmod 7$$

   Going on we look for a_3 satisfying $6(6 + 7 \cdot 6 + 7^2 a_3) \equiv 1 \pmod{7^3}$ and after the computation we find $a_3 = 5$. We begin to see a pattern and we suggest that $\frac{1}{6} = 6555... = 6\bar{5}$ in 7-addic expansion. Now we can check the result:

$$6555... = 6 + 5 \cdot 7 + 5 \cdot 7^2 + ... = 6 + 5\sum_{k\geq 1}^{\infty} 7^k = 6 + 5\frac{7}{1-7} = 6 - \frac{35}{6} = \frac{36-35}{6} = \frac{1}{6}$$

   (b) Reformulating the question, we want to find for which prime p between 2 and 13 does the polynomial $P(X) = X^2 + 1 \in \mathbb{Z}_p[X]$ have a root in $\mathbb{Q}_p$. A root α of P would be in $\mathbb{Z}_p$ since $1 = |-1|_p = |\alpha^2|_p = |\alpha|_p^2$ by multiplicity of the norm.

   Using Hensel's lemma, if the reduction of P in the ring $\mathbb{Z}/p\mathbb{Z}[X]$ has a root $\bar{\alpha}$ that is simple, then it lifts to a root α of P in $\mathbb{Z}_p[X]$. Hence since $(X+2)(X+3) = X^2 + 1 \pmod 5$ and $(X+5)(X+8) = X^2 + 1 \pmod{13}$ then $\mathbb{Z}_5$ and $\mathbb{Z}_{13}$ have square roots of -1.

   Then notice that if P has a root in $\mathbb{Z}_p$ so that $P(X) = (X-\alpha)(X-\beta)$, with $\alpha, \beta \in \mathbb{Z}_p$ then looking at the reduction modulo p we have that $\bar{P}(X) = (X-\bar{\alpha})(X-\bar{\beta}) \in \mathbb{Z}/p\mathbb{Z}[X]$ has roots in $\mathbb{Z}/p\mathbb{Z}[X]$. For $p = 3, 7, 11$, since $\bar{P}(X) = X^2 + 1$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[X]$ (after quickly checking manually), we find that -1 isn't a square in $\mathbb{Z}_p$.

   Now suppose that P has a root in $\mathbb{Z}_2$, then its reduction in $\mathbb{Z}/p\mathbb{Z}[X]$ but also in $\mathbb{Z}/p^n\mathbb{Z}[X]$ (for any $n \in \mathbb{N}$) should have a root. However the polynomial $\bar{P}(X) = X^2 + 1 \in \mathbb{Z}/4\mathbb{Z}[X]$ is irreducible, contradiction.

   Hence the only p where -1 has a root is 5 and 13.

3. Suppose that the 2 norms are equivalent, i.e that there are real numbers $c, C \in \mathbb{R}$ such that $c|y|_{\mathfrak{p}} \leq |y|_{\mathfrak{q}} \leq C|y|_{\mathfrak{p}}$ for every $y \in F$.
Since $\mathfrak{p} \neq \mathfrak{q}$, there is an element $x \in \mathfrak{p} \backslash \mathfrak{q}$. Then for $\epsilon \in \mathbb{N}, x^n \in \mathfrak{p}^n$, so $|x^n|_{\mathfrak{p}} = \epsilon^n$ and $|x|_{\mathfrak{q}} = \epsilon$ for some $0 \leq \epsilon \leq 1$, therefore:

$$c|x^n|_{\mathfrak{p}} \leq |x^n|_{\mathfrak{q}} \leq C|x^n|_{\mathfrak{p}} \iff c\epsilon^n \leq \epsilon \leq C\epsilon^n$$

And for $n >> 1$ big integer we have that $\epsilon \geq C\epsilon^n$, a contradiction.

4. Let $\mathfrak{p}\mathcal{O}_K = \mathfrak{B}^e {\mathfrak{B}_1}^{e_1} \cdots {\mathfrak{B}_{\mathfrak{g}}}^{e_g}$ with $\mathfrak{B}_i \subset \mathcal{O}_K$ prime ideals the decomposition into prime ideal. We choose uniformizers $\pi_{\mathfrak{p}} \in F, \pi_{\mathfrak{B}} \in K$ such that $\pi_{\mathfrak{p}} \in \mathfrak{p} \backslash \mathfrak{p}^2, \pi_{\mathfrak{B}} \in \mathfrak{B} \backslash \mathfrak{B}^2$.
Therefore there is an ideal $I \subset \mathcal{O}_F$ coprime to $\mathfrak{p}$ such that $\pi_{\mathfrak{p}}\mathcal{O}_F = \mathfrak{p}I$. We then have $\pi_{\mathfrak{p}}\mathcal{O}_K = (\pi_{\mathfrak{p}}\mathcal{O}_F)\mathcal{O}_K = \mathfrak{p}I\mathcal{O}_K \cong (\mathfrak{p}\mathcal{O}_K)(I\mathcal{O}_K) = \mathfrak{B}^e {\mathfrak{B}_1}^{e_1} \cdots {\mathfrak{B}_{\mathfrak{g}}}^{e_g} I\mathcal{O}_K$ with $I\mathcal{O}_K$ coprime to $\mathfrak{B}^e \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$.
Since $\pi_{\mathfrak{B}} \in \mathfrak{B} \backslash \mathfrak{B}^2 \subset \mathcal{O}_K$ is a uniformizer, we have that $\pi_{\mathfrak{B}}\mathcal{O}_K = \mathfrak{B}J$ with J and $\mathfrak{B}$ coprime.
Hence we have that $|\pi_{\mathfrak{B}}|_{\mathfrak{B}}^e = |\pi_{\mathfrak{p}}|_{\mathfrak{B}}$.

15.4 Week 4 solutions by Louis Romain André Menétrey

1. *Review the concepts introduced in the lecture by consulting the Jupyter Notebook uploaded on Moodle (you can open it, for example, with CoCalc). The notebook summarizes the key notions from the lecture and demonstrates how they can be computed using SageMath. Run all code cells to observe how the computations are carried out. Experiment by modifying the examples (e.g., changing input values) to strengthen your understanding of the concepts and see how the results change.*

2. (a) By definition, the Dirichlet character product $\chi\psi$ is the primitive character inducing

$$(\chi\psi)^{\text{pre}} : \left(\mathbb{Z}\Big/ f_\chi f_\psi \mathbb{Z}\right)^\times \to \mathbb{C}^\times : a \mapsto \chi(a)\psi(a).$$

Since the conductors f_χ and f_ψ are coprime, there is an isomorphism

$$\left(\mathbb{Z}\Big/ f_\chi f_\psi \mathbb{Z}\right)^\times \cong (\mathbb{Z}/f_\chi\mathbb{Z})^\times \times (\mathbb{Z}/f_\psi\mathbb{Z})^\times.$$

Under this isomorphism, we can identify χ as $(\chi_m, 1)$ and ψ as $(1, \psi_n)$. Hence, η correspond to (χ_m, ψ_n) and we want to show η is primitive (implying $f_\chi f_\psi = f_{\chi\psi}$). Suppose $\chi\psi$ is a character of modulus $d < mn$ with $d = d_1 d_2$, $d_1 | m$, $d_2 | n$ and $(d_1, d_2) = 1$. We must have

$$\chi\psi(a, 1) = \chi_m(a)\psi_n(1) = \chi_m(a) = 1, \quad \forall a \equiv 1 \mod d_1$$

$$\text{similarly, } \psi_n(b) = 1, \quad \forall b \equiv 1 \mod d_2$$

This directly means χ (resp. ψ) is induced by a character modulo d_1, (resp. d_2). By primality of χ and ψ, we must have $d_1 = m$ and $d_2 = n$, contradicting $d_1 d_2 < mn$.

A counterexample where $(f_\chi, f_\psi) \neq 1$ occurs for

$$\chi = \psi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times : \quad 1 \mapsto 1; \quad 2 \mapsto -1$$

Then,

$$\eta : (\mathbb{Z}/9\mathbb{Z})^\times \to \mathbb{C}^\times : a \mapsto \chi(a)\psi(a)$$

is the principal character. Thus, $f_{\chi\psi} = 1$ while $f_\chi f_\psi = 9$.

(b) Let χ and ψ be even Dirichlet characters (EDC). We check the requirements one by one:

i. $(\chi\chi^{-1})(-1) = \chi(-1)\chi^{-1}(-1) = 1 \Rightarrow \chi^{-1}(-1) = 1$..
ii. $(\chi\psi)(-1) = \chi(-1)\psi(-1) = 1$.
iii. $\chi_0(-1) = 1$.

3. Let $K = \mathbb{Q}(\zeta_{p^n})$ and $G = \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ which is a cyclic group of order $\varphi(p^n) = p^{n-1}(p-1)$. To use the Conductor Discriminant Formula as hinted, we need to find the number of pairs of complex embeddings of K. First, $p^n \neq 2$, so there are no real embeddings. This means the

total number of complex embeddings is the number of embeddings which is $\varphi(p^n)$. So the number of pairs of complex embeddings r_2 is

$$r_2 = \frac{p^{n-1}(p-1)}{2}.$$

Since what is taken into account in the Conductor Discriminant Formula is the parity of r_2, we will use the congruence $r_2 \equiv \frac{p-1}{2} \mod 2$.
Now, we want to be able to compute the products of conductors $\prod_\chi f_\chi$ running over all primitive characters of G. Observe that the characters of $(\mathbb{Z}/p^k\mathbb{Z})^\times$ embed into characters of $(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$: this way, we have $a_{k+1} := \varphi(k+1) - \varphi(k)$ primitive characters of modulus p^{k+1}. Hence, we obtain

$$\prod_\chi f_\chi = \prod_{k=1}^{n} (p^k)^{a_k} = p^{\sum_{k=1}^n k a_k} = p^{\sum_{k=1}^n k\varphi(p^k) - \sum_{k=1}^n k\varphi(p^{k-1})}$$

The sum S in the exponent can be easily worked out through telescopy to obtain

$$S = n\varphi(p^n) + p^{n-1} = p^{n-1}(n(p-1)+1)$$

So, using the Conductor Discriminant Formula:

$$d_K = (-1)^{(p-1)/2} p^{p^n(n(p-1)-1)}.$$

4. (a) Let $K = \mathbb{Q}(\zeta_m)$ be a field containing both L_1 and L_2 (we can use the Kronecker-Weber Theorem) and let $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. By the correspondence seen in class, the compositum L_1L_2 corresponds to

$$K^H, \quad H = \bigcap_{\chi \in X_1, X_2} \ker \chi = H_1 \cap H_2$$

for $H_i = \bigcap_{\chi \in X_i} \ker \chi$. Hence, $K^H = K^{H_1 \cap H_2} = L_1L_2$ by Galois theory (since fixing L_1L_2 is equivalent to fixing both L_1 and L_2).

(b) Using Galois theory again, this follows from the isomorphism

$$\mathrm{Gal}(K/L_1 \cap L_2) \cong H_1H_2.$$

Indeed, this implies that $L_1 \cap L_2$ correspond to

$$(H_1H_2)^\perp \cong H_1^\perp \cap H_2^\perp = X_1 \cap X_2.$$

5. (a) Since m is odd, it decomposes as $m = \prod_{i \in I} p_i^{a_i}$ uniquely, for p_i odd primes. As

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \left(\mathbb{Z}/\prod_{i\in I} p_i^{a_i}\mathbb{Z}\right)^\times \overset{\text{CRT}}{\cong} \prod_{i\in I} \left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right)^\times,$$

we obtain that a quadratic character χ modulo m is the same as a product of quadratic characters $(\chi_i)_{i\in I}$, each modulo $p_i^{a_i}$. Since each factor $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ is cyclic of order $p_i^{a_i-1}(p_i-1)$, which is an even number, we conclude that both $k \mapsto 1$ and $k \mapsto -1$ engender valid quadratic characters, for k a generator. This means that for each prime p_i, there are two quadratic characters modulo $p_i^{a_i}$ (one of which is trivial), so that the total number of quadratic characters modulo m is $2^{|I|}$.
χ is primitive if and only all the χ_i are primitive. Observe that the group of squares in a cyclic group of even order $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ has index 2 and already appears modulo p. In other words, let π be the reduction modulo p. Then, if $a_i > 1$, we have a non-trivial quadratic Dirichlet character modulo p, inducing the χ_i if non-trivial:

$$\left(\frac{\bullet}{p}\right) : (\mathbb{Z}/p_i\mathbb{Z}) \to \mathbb{C}^\times.$$

We conclude that

$$\#\{\text{primitive, quadratic } \chi \mod m\} = \begin{cases} 1 & a_i = 1, \forall i \in I \quad (m \text{ is squarefree}) \\ 0 & \text{else} \end{cases}$$

(b) **Preliminary Observation:** We know that any quadratic subfield corresponds uniquely to some Dirichlet subgroup $X \leq \widehat{G}$. It happens precisely when $|X| = 2 \iff X = \{\chi_0, \chi\}$ for χ non-trivial, quadratic and primitive ($|X| = 2$ since the correspondence preserves the order). If not primitive, two characters could define the same fields, so we should reduce them modulo their conductor and then apply this procedure. Since L is a quadratic subfield, we can write $L = \mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Z}$. By both Sheet 2, Exercise 4 and the conductor discriminant formula, we obtain

$$d_L = \begin{cases} d & d \equiv 1 \mod 4 \\ 4d & \text{else} \end{cases} = (-1)^{r_2} f_\chi$$

If f_χ is not divisible by 4, we directly deduce $|d| = f_\chi$. If it is, then $|d| = f_\chi/4$. To determine whether d is positive or negative, we evaluate χ at -1, since -1 corresponds to complex conjugation $\zeta_p \to \zeta_p^{-1}$. $\chi(-1) = 1$ means complex conjugation on L is trivial, i.e. L is real ($d > 0$). On the other hand, non-trivial complex conjugation on L means it is complex ($d < 0$).

Now, we can return to our original questions and answer them. By part (a), we know that there is one and only one unique non-trivial quadratic Dirichlet character of module p (determined by sending a generator to -1) which also turns out to be primitive and which we have seen, is $(\frac{\bullet}{p})$. Using the quadratic reciprocity, we directly have $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. Therefore, by applying our **observation** above, we directly deduce that $L = \mathbb{Q}(\sqrt{p^*})$ and $d_L = p^*$ where $p^* = (-1)^{\frac{p-1}{2}} p$.

(c) By part (a), there are $2^2 = 4$ Dirichlet characters modulo $4p$ among which only 1 is primitive (not 0, because $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ contains a non-trivial quadratic primitive character modulo 4). Let $L = \mathbb{Q}(\sqrt{d})$ be the corresponding quadratic subfield to this primitive character. Using the **observation** above, we deduce that $d = \pm 4p$. We want to evaluate the primitive Dirichlet character χ at -1 as before, to determine what the sign of $|d|$ is. As a primitive Dirichlet character modulo $4p$ decomposes as two primitive Dirichlet characters ψ, ω (ψ modulo 4, ω modulo p, which we have seen is $\omega = (\frac{\bullet}{p})$). One can easily verify that ψ has to be the character sending -1 to -1. Together,

$$\chi(-1) = \psi(-1)\omega(-1) = (-1)^{\frac{p+1}{2}}.$$

So,

$$L = \mathbb{Q}(\sqrt{4p}) = \mathbb{Q}(\sqrt{p}) \iff p \equiv 3 \mod (4)$$
$$L = \mathbb{Q}(\sqrt{-4p}) = \mathbb{Q}(\sqrt{-p}) \iff p \equiv 1 \mod (4).$$

Now, let's consider the two cases where the characters are not primitive. With the same decomposition notation as above, they are determined by

$$\psi_1\omega_1, \quad \psi_1(-1) = -1, \quad \omega_1 \equiv 1$$

$$\psi_2\omega_2, \quad \psi_2 \equiv 1, \quad \omega_2 = \left(\frac{\bullet}{p}\right)$$

Their primitive reductions χ_1, χ_2 are of module 4, p respectively and are described by sending a generator of their respective domain group to -1. Write $L_1 = \mathbb{Q}(\sqrt{d_1})$, $L_2 = \mathbb{Q}(\sqrt{d_2})$ for their associated subfield. Continuing the procedure of the **observation** above, we directly obtain $d_1 = -1$ (the case $d_1 = 1$ yields a trivial extension, not quadratic) and $d_2 = p^*$.

(d) Recall $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For any non-trivial Dirichlet quadratic character χ modulo 8, one can verify that the possibilities are

	χ_1	χ_2	χ_3
$1 \mapsto$	1	1	1
$3 \mapsto$	-1	-1	1
$5 \mapsto$	-1	1	-1
$7 \mapsto$	1	-1	-1

among which, χ_1 and χ_3 are the primitive ones and χ_2 is induced by the primitive

$$\chi_2' : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times : -1 \mapsto -1.$$

Using the same **observation** as in part (b) and (c), we obtain the three correspond subfields $L_i = \mathbb{Q}(\sqrt{d_i})$ with $d_1 = 8$, $d_2 = -1$ and $d_2 = -8$. Therefore, the quadratic subfields of $\mathbb{Q}(\zeta_8)$ are

$$\mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{\pm 8}) = \mathbb{Q}(\sqrt{\pm 2})$$

(e) By part (b), if $p \equiv 1 \mod (4)$, then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$, and by part (c), if $p \equiv 3 \mod (4)$, then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p})$. In fact, we thus always have $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p})$ for any odd prime p. This is also true for $p = 2$ since part (d) exhibits $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$.
Now let d be any integer. We can assume it is squarefree: $d = p_1...p_r$. Then $\mathbb{Q}(\sqrt{d})$ embeds into the compositum $\mathbb{Q}(\zeta_{4p_1})...\mathbb{Q}(\zeta_{4p_r}) = \mathbb{Q}(\zeta_{4\prod_{i=1}^r p_i}) = \mathbb{Q}(\zeta_{4d})$ as wanted.

15.5 Week 5 solutions by Paul Corentin Mathiot

1. We let D be a closed disk contained in A and $C = \partial D$ be its boundary, oriented counter-clockwise. We may apply Cauchy's integral formula to deduce that given any $s_0 \in D \backslash C$ in the interior of D we get for all $n \in \mathbb{N}$:

$$f_n(s_0) = \frac{1}{2\pi i} \int_C \frac{f_n(s)}{s - s_0} ds$$

Since we have uniform convergence, we may pass to the limit to obtain

$$f(s_0) = \frac{1}{2\pi i} \int_C \frac{f(s)}{s - s_0} ds$$

This shows that f is holomorphic on the interior of D and so it follows that f is holomorphic on U as desired.
Let $K \subset A$ be a compact set, and since $A \neq \mathbb{C}$, we must have $d(K, \partial A) > 0$, say $d(K, \partial A) = d$. Consider $K' = \bigcup_{x \in K} D(x, d/2)$, the union of disks centered at points in K. We have inclusions $K \subset K' \subset A$. The set K' is further bounded, so it remains to how that K' is closed to conclude that it is compact. We do this by proving that the complement is open. Take $p \notin K'$. By compactness of K, there exists $q \in K$ that realises the infimum in the distance of p to K, i.e. $|p - d| = d(p, K)$. Since $p \notin K'$, we must have $d(p, K) > d/2$, and so $D(p, |p - q| - d/2)$ is an open disk around p that does not intersect K' and so K' is closed.
Now, $\{f_n\}$ converges uniformly on K' by assumption. Let $\varepsilon > 0$ and find an N such that $|f_n(s) - f(s)| < \varepsilon$ for all $s \in K'$ and all $n \geq N$. For any $p \in K$, the disc $D = D(p, d/2)$ is fully contained in K' and has boundary in K', and so we may use the Cauchy Formula to obtain:

$$|f_n'(p) - f'(p)| = |\frac{1}{2\pi} \int_{\partial D} \frac{f_n(t)}{(t-p)^2} - \frac{f(t)}{(t-p)^2} dt| \leq \frac{||f_n - f||_D}{(d/2)} \leq \frac{2\varepsilon}{d}$$

and so f_n' converges uniformly to f' on K.

2. We start by stating the following lemma:

Lemma 15.1. *Let $0 < c < d \in \mathbb{R}$. Then $|e^{-cs} - e^{-ds}| \leq \frac{|s|}{\Re(s)}(e^{-c\Re(s)} - e^{-d\Re(s)})$.*

We have

$$e^{-cs} - e^{-ds} = s \int_c^d e^{-ts} dt$$

Taking absolute values yield

$$|e^{-cs} - e^{-ds}| = |s \int_c^d e^{-ts} dt| \leq |s| \int_c^d |e^{-ts}| dt = |s| \int_c^d e^{-t\Re(s)} dt = \frac{|s|}{\Re(s)}(e^{-c\Re(s)} - e^{-d\Re(s)})$$

We prove the statement:
If $g(s)$ converges at $s = s_0$, then $f(s) := g(s - s_0)$ converges at $s = 0$, and so in everything that

follows, we work with $s = s_0$.
Then, $f(0) = \sum_{i=1}^{\infty} a_n$ converges uniformly. We remark that we now wish to prove the uniform convergence of $f(s)$ on any domain

$$\{s : \Re(s) \geq 0, |\operatorname{Arg}(s)|\} \leq \theta$$

for some $\theta < \frac{\pi}{2}$.
We write $s = x + iy$ with $x, y \in \mathbb{R}$. For every s in the above defined domain, we have $x \geq 0$ and so $\operatorname{Arg}(s) = \arctan(\frac{y}{x})$. The second condition thus reads

$$|\operatorname{Arg}(s)| \leq \theta \iff |y| \leq x \tan(\theta)$$

We finish by writing $|s|^2 = x^2 + y^2 \leq x^2 + x^2 \tan(\theta)^2 = x^2(1 + \tan(\theta))^2$. Therefore, the condition on the argument is equivalent to the condition $|s| \leq xM$, with $M = \sqrt{1 + \tan(\theta)}$ and so $\frac{|s|}{\Re(s)} \leq M$ with any $M \geq 0$. Effectively, it remains to show the result on

$$\{s : \Re(s) \geq 0, \frac{|s|}{\Re(s)} \leq M\}$$

As in Abel's Lemma, we introduce for $r, m \in \mathbb{N}, r > m$:

$$A_{m,r} = \sum_{n=m}^{r} a_n$$

By the uniform convergence of $f(0)$, we deduce that there exists $N \in \mathbb{N}$ large enough such that for all $r > m \geq N$, we have $|A_{m,r}| \leq \varepsilon$. We now set $b_n = \frac{1}{n^s}$ (such that $a_n b_n$ is exactly the $n-$th term of the Dirichlet series) to obtain from Abel's Lemma

$$|S_{m,r}| = |\sum_{n=m}^{r-1} A_{m,n}(n^{-s} - (n+1)^{-s}) + A_{m,r} b_r|$$

Using the above lemma with $c = \ln(n), d = \ln(n+1)$ as well as the bound on $|A_{m,r}|$, we conclude

$$\begin{aligned}
|S_{m,r}| &\leq |\sum_{n=m}^{r-1} A_{m,n}(n^{-s} - (n+1)^{-s})| + |A_{m,r} r^{-s}| \\
&\leq \varepsilon \sum_{n=m}^{r-1} \frac{|s|}{\Re(s)}(n^{-\Re(s)} - (n+1)^{-\Re(s)}) + \varepsilon \\
&\leq \varepsilon(1 + \frac{|s|}{\Re(s)}(m^{-\Re(s)} - r^{-\Re(s)}) \\
&\leq \varepsilon(1 + M)
\end{aligned}$$

This shows that $|S_{m,r}| \xrightarrow{m \to \infty} 0$ (in fact $S_{m,r} \to 0$ uniformly on the desired domain) and since $S_{m,r}$ is the expression of the difference of the partial sums, we conclude that the series converges uniformly for all s satisfying $\Re(s) \geq 0$ and $\frac{|s|}{\Re(s)} \leq M$.
Undoing the original translation by s_0, we conclude the proof.

3. We will prove that the Euler Product

$$\prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$$

is absolutely convergent for $\Re(s) > 1$ and will then rearrange this product to prove that it is in fact the Euler product of $\zeta_K(s)$. To start with, we let $s \in \mathbb{R}$, as the previous exercise implies the desired result.
An infinite product of the form $\prod_i (1 + x_n)$ with $|x_i| < 1$ is convergent if the series $\sum_i x_i$ converges.(We omit the proof, but the idea is the monotone convergence theorem and an upper bound

on the product given by the exponential of the sum.)
In our case, we have $x_i = \frac{1}{N\mathfrak{p}_i^s}$ and so we wish to understand the sum

$$\sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s}.$$

For any prime $\mathfrak{p}$ lying over $p = \mathfrak{p} \cap \mathbb{Z}$, the norm satisfies $N\mathfrak{p} \geq p$, and therefore $\frac{1}{p^s} \geq \frac{1}{N\mathfrak{p}^s}$. Furthermore, there is a maximum of $[K : \mathbb{Q}]$ primes $\mathfrak{p}$ lying over a common p, which gives us

$$\sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s} \leq \sum_{p} \frac{[K : \mathbb{Q}]}{p^s} < \infty$$

and the right hand side is a convergent series, since it is bounded by the zeta function at $s > 1$ which is convergent. This shows convergence for all $s \in \mathbb{C}$ satisfying $\Re(s) > 1$.
To retrieve the Zeta function from its product, the heuristic is as follows:
We recall that the Taylor expansion of $(1-x)^{-1}$ is precisely $\sum_n x^n$, and so upon taking the product of, say the primes $\mathfrak{p}$ with norms smaller than N, we get

$$\begin{aligned}\prod_{\mathfrak{p},\ N\mathfrak{p}\leq N} (1 - N\mathfrak{p}^{-s})^{-1} &= \prod_{\mathfrak{p}, N\mathfrak{p}\leq N} (1 + \frac{1}{N\mathfrak{p}^s} + \frac{1}{N\mathfrak{p}^{2s}} + \ldots) \\ &= \sum_{m_1,\ldots,m_k \geq 0} \frac{1}{(N\mathfrak{p}_1^{m_1} \ldots N\mathfrak{p}_k^{m_k})^s}\end{aligned}$$

and we recognize that by unique factorization into primes, the last sum is precisely the sum $\sum_{\mathfrak{a}} N\mathfrak{a}^{-s}$ over the integral ideals $\mathfrak{a}$.

4. (a) We prove the general statement that given G an abelian group and $H < G$, the restriction map $\widehat{G} \to \widehat{H}$ is surjective. It is easy to see that this map is a group homomorphism, and has kernel $H^{\perp}$, hence we obtain an injective homomorphism $\frac{\widehat{G}}{H^{\perp}} \to \widehat{H}$. Finally, counting orders, we get that it is necessarily an isomorphism which implies that the restriction is surjective.
   We finish by recalling that $Z < G$ and $G \simeq \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^{\times}$ is an abelian group.

   (b) We use (a) to split the product as

$$\prod_{\chi \in \widehat{G}} (1 - \chi(p)T) = \prod_{\psi \in \widehat{Z}} \prod_{\substack{\chi \in \widehat{G} \\ \chi_{|Z} = \psi}} (1 - \chi(p)T)$$

   Finally, we note that $\chi(p)$ depends only on the image of χ in $\widehat{Z}$ (via the identification $Z \simeq X/Y_1$) and we may simplify the product to obtain $\prod_{\psi \in \widehat{Z}} (1 - \psi(p)T)^{a_\psi}$. The powers a_ψ that appear in the product is then exactly the cardinality of a coset of $\widehat{Z}$ in $\widehat{G}$ which is given by

$$\begin{aligned}\#\chi\widehat{Z} &= \#\ker(\widehat{G} \to \widehat{Z}) \\ &= \frac{\#\widehat{G}}{\#\widehat{Z}} \\ &= \frac{\varphi(m)}{f} = g\end{aligned}$$

   Therefore,

$$\prod_{\chi \in \widehat{G}} (1 - \chi(p)T) = \prod_{\psi \in \widehat{Z}} (1 - \psi(p)T)^g.$$

(c) Using the stated result and combining with our result from (c), we obtain from the identification $\widehat{Z} \simeq \mu_f$:

$$\begin{aligned}\prod_{\chi \in \widehat{G}} (1 - \chi(p)T) &= \prod_{\psi \in \widehat{Z}} (1 - \psi(p)T)^g \\ &= \prod_{\eta \in \mu_f} (1 - \eta T)^g \\ &= (1 - T^f)^g = (1 - T^f)^{\varphi(m)/f}\end{aligned}$$

as desired.

(d) We prove

$$\prod_{\eta \in \mu_f} (1 - \eta T) = 1 - T^f$$

The classical cyclotomic polynomial reads as $X^f - 1 = \prod_\eta (X - \eta)$. Upon doing the change of variable $X = 1/T$, we obtain $T^{-f} - 1 = \prod_\eta (1/T - \eta)$ hence after multiplying by T^f

$$1 - T^f = \prod_\eta (1 - \eta T)$$

15.6 Week 6 solutions by Tianxiang Xie

1. Let $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ be a subgroup. Each element $h \in H$ corresponds to a residue $a \pmod n$. Then

$$\mathcal{S} = \bigcup_{a \in H} \{p \mid p \equiv a \pmod n\}.$$

Hence it suffices to compute the density of primes in a given residue class $p \equiv a \pmod n$.
For a Dirichlet character $\chi \pmod n$,

$$\log L(s, \chi) = \sum_p \frac{\chi(p)}{p^s} + R(s),$$

where $R(s)$ converges for $\mathrm{Re}(s) > 1/2$. Thus, as $s \to 1^+$,

$$\log L(s, \chi) \sim \sum_p \frac{\chi(p)}{p^s}.$$

Using orthogonality of Dirichlet characters,

$$\frac{1}{\varphi(n)} \sum_{\chi \bmod n} \overline{\chi}(a)\chi(p) = \begin{cases} 1, & p \equiv a \pmod n, \\ 0, & \text{otherwise.} \end{cases}$$

Applying this to $\log L(s, \chi)$, we get

$$\sum_{\chi \bmod n} \overline{\chi}(a) \log L(s, \chi) \sim \sum_{p \equiv a \pmod n} \varphi(n) \frac{1}{p^s}.$$

For the trivial character χ_0,

$$L(s, \chi_0) = \prod_{p \mid n} \left(1 - \frac{1}{p^s}\right) \zeta(s) \sim \zeta(s) \quad \text{as } s \to 1^+.$$

Hence

$$\sum_{p \equiv a \pmod n} \frac{1}{p^s} \sim \frac{1}{\varphi(n)} \log \zeta(s).$$

Summing over all residues $a \in H$ gives

$$\sum_{a \in H} \sum_{p \equiv a \pmod{n}} \frac{1}{p^s} \sim \frac{|H|}{\varphi(n)} \log \zeta(s).$$

By definition,

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{S}} p^{-s}}{\log \frac{1}{s-1}}.$$

Since $\log \zeta(s) \sim \log \frac{1}{s-1}$ as $s \to 1^+$, we conclude

$$\delta(\mathcal{S}) = \frac{|H|}{\varphi(n)}.$$

2. Let $\zeta_K(s) = \prod_{\mathfrak{P} \subset \mathcal{O}_K} (1 - N\mathfrak{P}^{-s})^{-1}$ be the Dedekind zeta function of K, which converges for $\Re(s) > 1$. For $s > 1$ real we have

$$\log \zeta_K(s) \;=\; -\sum_{\mathfrak{P}} \log\bigl(1 - N\mathfrak{P}^{-s}\bigr) \;=\; \sum_{\mathfrak{P}} \sum_{n \geq 1} \frac{1}{n} N\mathfrak{P}^{-ns}.$$

Group the sum over prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ by the prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ below them. For each prime $\mathfrak{p} \subset \mathcal{O}_F$ write $g(\mathfrak{p})$ for the number of primes of $\mathcal{O}_K$ lying above $\mathfrak{p}$ (so $1 \leq g(\mathfrak{p}) \leq d$), and write $N\mathfrak{p}$ for the absolute norm from F to $\mathbb{Q}$. Then

Split the inner n–sum into the $n = 1$ term and the tail $n \geq 2$:

$$\log \zeta_K(s) = \sum_{\mathfrak{P}, f(\mathfrak{P}/\mathfrak{p})=1=e(\mathfrak{P}/\mathfrak{p})} (N\mathfrak{p})^{-s} + \sum_{\mathfrak{P}, n>1} (N\mathfrak{P})^{-ns} + \sum_{\mathfrak{P}, f(\mathfrak{P}/\mathfrak{p})>1} (N\mathfrak{p})^{-f(\mathfrak{P}/\mathfrak{p})s} + \sum_{\mathfrak{P}, f(\mathfrak{P}/\mathfrak{p})=1, e(\mathfrak{P}/\mathfrak{p})>1} (N\mathfrak{p})^{-s}$$

The second term converge when $s \to 1^+$, the forth term is finite as only finite primes ramified, and the third term converges because $f(\mathfrak{P}/\mathfrak{p}) > 1$.

Hence as $s \to 1^+$ the main growth of $\log \zeta_K(s)$ comes from the first term

$$\sum_{\mathfrak{p}} g(\mathfrak{p}) \, (N\mathfrak{p})^{-s}.$$

Now separate the contribution from primes that split completely and the rest. Therefore

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p} \in \mathcal{S}_{K/F}} d \, (N\mathfrak{p})^{-s} \qquad \text{as } s \to 1^+,$$

where "$\sim$" means the difference is bounded as $s \to 1^+$.

On the other hand $\zeta_K(s)$ and $\zeta_F(s)$ both have a simple pole at $s = 1$, hence

$$\log \zeta_K(s) \sim \log \zeta_F(s) \sim \log \frac{1}{s-1} \qquad (s \to 1^+).$$

Combining the two asymptotics yields

$$\log \frac{1}{s-1} \sim d \sum_{\mathfrak{p} \in \mathcal{S}_{K/F}} (N\mathfrak{p})^{-s} \qquad (s \to 1^+).$$

Rearranging and using the definition of Dirichlet density relative to F,

$$\delta_F(\mathcal{S}_{K/F}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}_{K/F}} (N\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} = \frac{1}{d},$$

as desired.

3. Let $L = EK$. Since both $E/\mathbb{Q}$ and $K/\mathbb{Q}$ are Galois, so is $L/\mathbb{Q}$.

   We first recall a simple fact: if $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ restricts to the identity on both E and K, then $\sigma = \mathrm{id}_L$. Indeed, since L is generated by E and K, for any $x = \sum_i e_i k_i$ with $e_i \in E, k_i \in K$, we have
   $$\sigma(x) = \sum_i \sigma(e_i)\sigma(k_i) = \sum_i e_i k_i = x.$$

   ($\Rightarrow$) Suppose p splits completely in $L/\mathbb{Q}$. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ lying above p. Then the residue degree and ramification index of $\mathfrak{P}$ over p are both 1. Let $\mathfrak{p}_E = \mathfrak{P} \cap \mathcal{O}_E$ and $\mathfrak{p}_K = \mathfrak{P} \cap \mathcal{O}_K$. Then $f(\mathfrak{p}_E|p)$ and $f(\mathfrak{p}_K|p)$ must divide $f(\mathfrak{P}|p) = 1$, so they are also 1, and the same holds for ramification indices. Thus p splits completely in both E and K.

   Equivalently, if the Frobenius element $\mathrm{Frob}_{\mathfrak{P}}$ in $\mathrm{Gal}(L/\mathbb{Q})$ is the identity, its images in $\mathrm{Gal}(E/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$ are also identities, so p splits completely in E and K.

   ($\Leftarrow$) Conversely, suppose p splits completely in both $E/\mathbb{Q}$ and $K/\mathbb{Q}$. Then p is unramified in both fields, hence also unramified in L. Let $\mathfrak{P}$ be a prime of L above p, and let $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(L/\mathbb{Q})$ denote its Frobenius element.

   Since p splits completely in E and K, the Frobenius elements in $\mathrm{Gal}(E/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$ are both trivial. Thus the restrictions of $\mathrm{Frob}_{\mathfrak{P}}$ to E and K are both the identity. By the fact noted above, this implies $\mathrm{Frob}_{\mathfrak{P}} = \mathrm{id}_L$. Hence p splits completely in L.

4. We first prove the second equality.

$$\begin{aligned}
P^+_{F,\mathfrak{m}} &= \langle\, \langle\alpha\rangle : \alpha \in \mathcal{O}_F,\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \alpha \gg 0 \,\rangle \\
&= \left\{ \left\langle \prod_i \alpha_i^{\delta_i} \right\rangle \;\middle|\; \alpha_i \in \mathcal{O}_F,\ \alpha_i \equiv 1 \pmod{\mathfrak{m}},\ \alpha_i \gg 0,\ \delta_i = \pm 1 \right\} \\
&\subset \left\{ \left\langle \frac{\prod_{\delta_i>0} \alpha_i}{\prod_{\delta_j<0} \alpha_j} \right\rangle \;\middle|\; \alpha_i, \alpha_j \in \mathcal{O}_F,\ \alpha_i, \alpha_j \equiv 1 \pmod{\mathfrak{m}},\ \frac{\prod_{\delta_i>0} \alpha_i}{\prod_{\delta_j<0} \alpha_j} \gg 0 \right\} \\
&\subset \left\{ \langle \tfrac{\alpha}{\beta} \rangle : \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \pmod{\mathfrak{m}},\ \tfrac{\alpha}{\beta} \gg 0 \right\}.
\end{aligned}$$

   To prove the reverse inclusion, take $\langle \frac{\alpha}{\beta} \rangle$ with $\alpha, \beta \in \mathcal{O}_F$ prime to $\mathfrak{m}$ and $\alpha \equiv \beta \pmod{\mathfrak{m}}$. Then $(\alpha) + \mathfrak{m} = \mathcal{O}_F$, so we can find $\gamma \in \mathcal{O}_F$ such that $\alpha\gamma \equiv 1 \pmod{\mathfrak{m}}$. Hence $\langle \frac{\alpha}{\beta} \rangle = \langle \alpha\gamma \rangle \langle \beta\gamma \rangle^{-1} = \langle (\alpha\gamma)^2 \rangle \langle (\beta\gamma)(\alpha\gamma) \rangle^{-1}$, and both $(\alpha\gamma)^2$ and $(\beta\gamma)(\alpha\gamma)$ satisfy the defining conditions ($(\alpha\gamma)^2 \equiv 1 \pmod{\mathfrak{m}}$ and $(\alpha\gamma)^2 \gg 0$), so the reverse inclusion holds. Thus the second equality is proved.

   Now we prove the first equality. One direction is trivial:

$$\left\{ \langle \tfrac{\alpha}{\beta} \rangle : \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \pmod{\mathfrak{m}},\ \tfrac{\alpha}{\beta} \gg 0 \right\} \subset \{ \langle \alpha \rangle : \alpha \in F^\times,\ \alpha \gg 0,\ \alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}} \}.$$

   Conversely, let $\alpha \in F^\times$ with $\alpha \gg 0$ and $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$. Write $\alpha = \beta/\gamma$ with $\beta, \gamma \in \mathcal{O}_F$. Let
   $$\beta = \prod_{p|\mathfrak{m}} p^{e_p} \prod_{q \nmid \mathfrak{m}} q^{e_q}, \qquad \gamma = \prod_{p|\mathfrak{m}} p^{f_p} \prod_{q \nmid \mathfrak{m}} q^{f_q}.$$

   Since $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$, we have $e_p = f_p$ for all $p \mid \mathfrak{m}$. Choose an element ω satisfying
   $$\begin{cases} v_p(\omega) = -f_p, & \text{for all } p \mid m, \\ v_q(\omega) > 0, & \text{for all } q \nmid m. \end{cases}$$

   Then both $\beta\omega$ and $\gamma\omega$ are in $\mathcal{O}_F$, prime to $\mathfrak{m}$, and $\beta\omega \equiv \gamma\omega \pmod{\mathfrak{m}}$. Hence
   $$\langle \alpha \rangle = \langle \tfrac{\beta}{\gamma} \rangle = \langle \tfrac{\beta\omega}{\gamma\omega} \rangle,$$
   so the reverse inclusion holds. This completes the proof.

15.7 Week 7 solutions by Douglas Christian Clerc

1. (a) We will simply apply the above formula for the strict ray class number.
In our case, as $F = \mathbb{Q}(\sqrt{3})$, we have that $\mathfrak{m} = \mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$ and $r_1 = 2$. Moreover, as $\mathbb{Z}[\sqrt{3}]$ is a PID, we have that $h_F = 1$ and we observe that $\mathcal{O}_F^\times = \{\pm(2+\sqrt{3})^n : n \in \mathbb{Z}\}$. We can also compute

$$\varphi(\mathcal{O}_F) = \left| \left(\frac{\mathcal{O}_F}{\mathcal{O}_F}\right)^\times \right| = 1.$$

The only part missing to use the formula is the denominator

$$[\mathcal{U}_F : \mathcal{U}_{F,\mathfrak{m}}^+].$$

To compute it, recall Theorem 1.9 of the book Class Field Theory by Nancy Childress:

Theorem 15.2 (Dirichlet Unit Theorem)**.** *Let F be a number field and r_1, r_2 represent the number of real embeddings and the number of conjugate pairs of imaginary embeddings of F respectively.*
There are units $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in \mathcal{O}_F^\times$ such that

$$\begin{aligned}\mathcal{O}_F^\times &\cong \mathcal{W}_F \times \langle\varepsilon_1\rangle \times \cdots \times \langle\varepsilon_{r_1+r_2-1}\rangle \\ &\cong \mathcal{W}_F \times \mathbb{Z}^{r_1+r_2-1},\end{aligned}$$

where $\mathcal{W}_F$ is the group of roots of unity in F. The ε_j are called a fundamental system of units for F.

In our case, since $\mathcal{U}_F = \mathcal{O}_F^\times$, $\mathcal{W}_F = \{\pm 1\}$, $r_1 = 2$ and $r_2 = 0$, we get by Dirichlet Unit Theorem that

$$\mathcal{U}_F \cong \{\pm 1\} \times \mathbb{Z} \cong \{\pm 1\} \times \langle\varepsilon\rangle$$

where ε is a fundamental unit. We observe that in our case, the fundamental units for $\mathbb{Q}(\sqrt{3})$ are $\{\pm(2+\sqrt{3})\}$ as $(2+\sqrt{3})^{-1} = 2-\sqrt{3}$. Let us take $\varepsilon = 2+\sqrt{3}$. Then we have $\varepsilon >> 0$ and by definition

$$\mathcal{U}_F^\times = \{u \in \mathcal{U}_F : u >> 0, u \equiv 1 \ mod(\mathcal{O}_F)\} = \langle\varepsilon\rangle,$$

hence

$$[\mathcal{U}_F : \mathcal{U}_{F,\mathfrak{m}}^\times] = 2$$

and by the above formula, we conclude that

$$|\mathcal{R}_{F,\mathfrak{m}}^+| = \frac{1 \cdot 2^2 \cdot 1}{2} = 2.$$

Since $\mathcal{R}_{F,\mathfrak{m}}^+$ is the quotient of abelian groups, this is an abelian group. We know that up to isomorphism, there is only one abelian group of order 2, thus

$$\mathcal{R}_{\mathbb{Q}(\sqrt{3}),\mathbb{Z}[\sqrt{3}]}^+ \cong \mathbb{Z}/2\mathbb{Z}.$$

(b) We have $\mathcal{O}_F = \mathbb{Z}[i]$. Since $\mathbb{Q}(i)$ has no real embeddings and one pair of conjugate embedding, we have $r_1 = 0$ and $r_2 = 1$. As above, $\mathbb{Z}[i]$ is a PID so $h_F = 1$. We again have $\varphi(\mathcal{O}_F) = 1$ and we have

$$\mathcal{U}_F = \mathcal{O}_F^\times = \{\pm 1, \pm i\}.$$

In the definition of $\mathcal{U}_{F,\mathfrak{m}}^+$, we have $u >> 0$, which by definition means that $\sigma(u) > 0$ for all real embeddings, but in our case, as we do not have any real embedding, we get $\mathcal{U}_{F,\mathfrak{m}}^+ = \mathcal{U}_F$ and so $[\mathcal{U}_F : \mathcal{U}_{F,\mathfrak{m}}^+] = 1$. By the above formula for the strict ray class number modulo $\mathfrak{m}$, we get

$$|\mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}^+| = \frac{1 \cdot 2^0 \cdot 1}{1} = 1.$$

Thus $\mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}^+$ is trivial.

(c) By definition,

$$\mathcal{R}^+_{F,\mathfrak{m}} = \frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}} \text{ and } \mathcal{R}_{F,\mathfrak{m}} = \frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}_{F,\mathfrak{m}}}.$$

Moreover, $\mathcal{P}^+_{F,\mathfrak{m}}$ is the subgroup of totally positive element of $\mathcal{P}_{F,\mathfrak{m}}$. Since we do not have any real embedding, $\mathcal{P}_{F,\mathfrak{m}} = \mathcal{P}^+_{F,\mathfrak{m}}$ and so

$$\mathcal{R}^+_{\mathbb{Q}(i),\mathbb{Z}[i]} = \mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}.$$

2. Yes, it is possible.
Let $F = \mathbb{Q}$, $\mathfrak{n} = n\mathbb{Z}$ and $\mathfrak{m} = (2n)\mathbb{Z}$ where n is odd. Let $\mathcal{H}_1 = \mathcal{P}^+_{\mathbb{Q},\mathfrak{n}}$, $\mathcal{H}_2 = \mathcal{P}^+_{\mathbb{Q},\mathfrak{m}}$ and observe that $\mathcal{H}_1 \neq \mathcal{H}_2$. By an example of Section 7, we know that the class field over $\mathbb{Q}$ of $\mathcal{H}_1$ is $K = \mathbb{Q}(\zeta_n)$ and that the class field over $\mathbb{Q}$ of $\mathcal{H}_2$ is $L = \mathbb{Q}(\zeta_{2n})$. Now, since n is odd, we have that $K = L$ and so we found $\mathcal{H}_1 \neq \mathcal{H}_2$ such that they have the same class field over $\mathbb{Q}$.

3. By definition, since K is the class field for $\mathcal{H}$, we have

$$\{\text{primes } \mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \in \mathcal{H}\} \approx S_{K/F} = \{\text{primes } \mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \text{ splits completely in } K/F\}.$$

By definition of $\approx$, we have that $\{\text{primes } \mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \in \mathcal{H}\}$ and $S_{K/F}$ differ by a set with Dirichlet density zero, thus

$$\delta_F(\{\text{primes } \mathfrak{p} \in \mathcal{H}\} \backslash S_{K/F}) = \lim_{s \to 1^+} \sum_{\mathfrak{p} \in \mathcal{H} \backslash S_{K/F}} \frac{N\mathfrak{p}^{-1}}{\log(\frac{1}{s-1})} = 0.$$

With this equality, we redo the proof of Theorem 7.13 to get the result.
Let $m(\chi) = \operatorname{ord}_{s=1}(L_{\mathfrak{m}}(s,\chi))$. For $\chi \neq \chi_0$, we know that $m(\chi) \geq 0$, while $m(\chi_0) = -1$. As in the assumption of Theorem 2.4, we take χ to be trivial on $\mathcal{H}$ and we may view χ as a character of $\frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{H}}$.
There is some constant a such that

$$\prod_{\chi \in \widehat{\frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{H}}}} L_{\mathfrak{m}}(s,\chi) = a(s-1)^{\sum_\chi m(\chi)} + \cdots$$

Taking logs, we get

$$\begin{aligned}\sum_\chi \log L_{\mathfrak{m}}(s,\chi) &\sim \left(\sum_\chi m(\chi)\right) \log(s-1) \\ &= -\left(\sum_\chi m(\chi)\right) \log\left(\frac{1}{s-1}\right).\end{aligned}$$

Now

$$\begin{aligned}\log L_{\mathfrak{m}}(s,\chi) &= \sum_{\mathfrak{p} \nmid \mathfrak{m}} \sum_{n=1}^{\infty} \frac{\chi(\mathfrak{p})^n}{n N\mathfrak{p}^{ns}} \\ &\sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s}\end{aligned}$$

and so as in the proof of Proposition 2.3

$$\sum_\chi \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p} \in \mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] N\mathfrak{p}^{-s}.$$

Hence,

$$\sum_{\mathfrak{p} \in \mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] N\mathfrak{p}^{-s} \sim -\left(\sum_\chi m(\chi)\right) \log\left(\frac{1}{s-1}\right).$$

We can split the LHS, divide by $\log\left(\frac{1}{s-1}\right)$ and let $s \to 1^+$ to obtain

$$\begin{aligned}
-\sum_{\chi} m(\chi) &= \lim_{s\to 1^+} \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \sum_{\mathfrak{p}\in S_{K/F}} N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)} + \lim_{s\to 1^+} \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \sum_{\mathfrak{p}\in \mathcal{H}\backslash S_{K/F}} N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)} \\
&= [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]\delta_f(S_{K/F}) \\
&= \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]}
\end{aligned}$$

as the second term on the right is zero by the equation we got at the start of the exercise. As $m(\chi) \geq 0$ for all $\chi \neq \chi_0$ and $m(\chi_0) = -1$, we have

$$1 \geq 1 - \sum_{\chi\neq\chi_0} m(\chi) = \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]} > 0.$$

This force $m(\chi) = 0$ for all $\chi \neq \chi_0$ and so $-\sum_\chi m(\chi) = 1$. Thus we get

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] = [K : F].$$

4. (a) As $F = \mathbb{Q}$, we have $\mathcal{O}_F = \mathbb{Z}$. By the Isomorphism Theorem, we know that

$$\mathrm{Gal}(K/F) \cong \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F$$

where K is the Hilbert class field of F.
In our case, as $\mathbb{Z}$ is a PID, we have $\mathcal{I}_F = \mathcal{P}_F$, thus $\mathrm{Gal}(K/F)$ is trivial and so $K = F = \mathbb{Q}$.

(b) As $F = \mathbb{Q}(i)$, $\mathcal{O}_F = \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, $\mathcal{P}_F = \mathcal{I}_F$.
By the Isomorphism Theorem

$$\mathrm{Gal}(K/\mathbb{Q}(i)) \cong \{1\},$$

thus $K = F = \mathbb{Q}(i)$.

5. Let S be the set of primes dividing $\mathfrak{m}$ and I^S be the subgroup of $\mathcal{I}_F$ generated by primes not in S. We observe that $\mathcal{I}_F(\mathfrak{m}) = I^S$. Moreover, if we define $i : F^\times \to \mathcal{I}_F$ to be the map sending $a \in F^\times$ to the principal ideal $\langle a\rangle$, we see that $i(F^\times) = \mathcal{P}_F$. With these observations, we can rewrite our exact sequence as

$$0 \longrightarrow \mathcal{O}_F^\times \hookrightarrow F^{\mathfrak{m}} \longrightarrow I^S \twoheadrightarrow C \longrightarrow 0$$

where $C = \mathcal{I}_F/i(F^+)$.
To show that $I^S \to C$ is surjective, we have to show that every ideal class $\mathcal{C}$ of C is represented by an ideal in I^S. Let $\mathfrak{a} \in \mathcal{I}_F$ represents $\mathcal{C}$. By definition of a fractional ideal, we have that there exist a non-zero $\alpha \in F$ such that $\alpha\mathfrak{a} \subseteq \mathcal{O}_F$. Take $\mathfrak{b} = \alpha\mathfrak{a}$ and $\mathfrak{c} = \langle\alpha\rangle$, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals. Now, let $c \in \mathfrak{c}$. We have

$$\mathfrak{a} \cdot \langle c\rangle = \mathfrak{b} \cdot \mathfrak{c}^{-1} \cdot \langle c\rangle,$$

but since $c \in \mathfrak{c}$, we have $\langle c\rangle \subseteq \mathfrak{c}$, thus $\mathfrak{c}^{-1}\langle c\rangle$ is an integral ideal. This give us that $\mathfrak{a} \cdot \langle c\rangle$ is a product of integral ideals and so integral itself. Now, since the class of $\mathfrak{a}$ in C only depends on it up to multiplication by a principal ideal, we may suppose that $\mathfrak{a}$ is an integral ideal. Write

$$\mathfrak{a} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b},$$

where $\mathfrak{b} \in I^S$. For each $\mathfrak{p} \in S$, choose $\pi_\mathfrak{p} \in \mathfrak{p}\backslash\mathfrak{p}^2$ so that $\mathrm{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. By the Chinese Remainder Theorem, there exists an $a \in \mathcal{O}_F$ such that

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} \bmod \mathfrak{p}^{n(\mathfrak{p})+1}$$

for all $\mathfrak{p} \in S$. These congruences imply that $\mathrm{ord}_\mathfrak{p}(a) = n(\mathfrak{p})$ for all $\mathfrak{p} \in S$, so

$$\langle a\rangle = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}'$$

with $\mathfrak{b}' \in I^S$. We get $a^{-1}\mathfrak{a} \in I^S$ and it represents the same class as $\mathfrak{a}$ in C, so $I^S \to C$ is surjective as we wanted.
Let the map $F^{\mathfrak{m}} \to I^S$ be defined by sending a to $\langle a \rangle$. Now, if $\mathfrak{a} \in I^S$ maps to zero in C, then $\mathfrak{a} = \langle a \rangle$ for some $a \in F^{\mathfrak{m}}$, and a is uniquely determined up to a unit. Conversely, $a \in F^{\mathfrak{m}}$ is send to $\langle a \rangle \in \mathcal{P}_F$, thus it is in $\ker(I^S \to C)$.
To conclude, we show that $\ker(F^{\mathfrak{m}} \to I^S)$ is $\mathcal{O}_F^\times$. We see $\mathcal{O}_F^\times \to F^{\mathfrak{m}}$ as the inclusion. If $a \in \mathcal{O}_F^\times$, then $\langle a \rangle = \mathcal{O}_F$. Conversely, if $\langle a \rangle = \mathcal{O}_F$, then a has an inverse in $\mathcal{O}_F$, so it is a unit. This prove that $\ker(F^{\mathfrak{m}} \to I^S) = \mathcal{O}_F^\times$ and prove the exactness of the sequence.

15.8 Week 8 solutions by Sandro Pfammatter

1. We first compute the class number of $F = \mathbb{Q}(\sqrt{15})$. Since the Hilbert class field of F is a Galois extension of F with Galois group isomorphic to $\mathcal{C}_F$ by the Isomorphy Theorem, the degree of the Hilbert class field extension coincides with the class number of F.

   The discriminant of F is $d_{F/\mathbb{Q}} = 60$, by the known results on discriminants of quadratic extensions. Moreover, the degree of the extension over $\mathbb{Q}$ is $n = 2$, and the number of pairs of complex embeddings is $r_2 = 0$. Hence, the Minkowski bound is given by

   $$M_F = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_{F/\mathbb{Q}}|} = \sqrt{15} < 4.$$

   Consequently, every ideal class contains an integral ideal of norm at most 3. To determine the class group, it therefore suffices to examine the prime ideals lying above the rational primes 2 and 3.

   Since 2 and 3 divide the discriminant, they ramify in F. Their norms are 4 and 9, respectively, and hence

   $$(2) = \mathfrak{p}_2^2 \quad \text{and} \quad (3) = \mathfrak{p}_3^2,$$

   where $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are the unique prime ideals of $\mathcal{O}_F$ lying above 2 and 3, with $N_{F/\mathbb{Q}}(\mathfrak{p}_2) = 2$ and $N_{F/\mathbb{Q}}(\mathfrak{p}_3) = 3$.

   Using computational tools such as SageMath, one finds

   $$\mathfrak{p}_2 = (2, 1 + \sqrt{15}) \quad \text{and} \quad \mathfrak{p}_3 = (3, \sqrt{15}).$$

   Both ideals are non-principal. Indeed, suppose that $\mathfrak{p}_2 = (a)$ for some $a \in \mathcal{O}_F = \mathbb{Z}[\sqrt{15}]$. Then

   $$N_{F/\mathbb{Q}}(a) \mid N_{F/\mathbb{Q}}(2) = 4 \quad \text{and} \quad N_{F/\mathbb{Q}}(a) \mid N_{F/\mathbb{Q}}(1 + \sqrt{15}) = -14,$$

   so $N_{F/\mathbb{Q}}(a) \in \{\pm 1, \pm 2\}$. Writing $a = b + c\sqrt{15}$, we have

   $$N_{F/\mathbb{Q}}(a) = b^2 - 15c^2.$$

   If $N_{F/\mathbb{Q}}(a) = 1$, then a is a unit, which is impossible since $\mathfrak{p}_2$ is proper. Moreover, a brief check shows that -1 and ± 2 are not values of $b^2 - 15c^2$ for integers b, c. Hence, $\mathfrak{p}_2$ is non-principal. A similar argument shows that $\mathfrak{p}_3$ is likewise not principal.

   By the Minkowski bound, the ideal class group is generated by the classes of $\mathfrak{p}_2$ and $\mathfrak{p}_3$. We compute their product:

   $$\mathfrak{p}_2\mathfrak{p}_3 = (6, 3 + 3\sqrt{15}, 2\sqrt{15}, \sqrt{15} + 15) = (6, 3 + \sqrt{15}).$$

   This ideal is principal, since

   $$-(3 - \sqrt{15})(3 + \sqrt{15}) = 6.$$

   Hence $[\mathfrak{p}_2] = [\mathfrak{p}_3]^{-1}$. Because $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3^2$, we have

   $$[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = \big[(0)\big].$$

   Thus, $\mathcal{C}_F \cong \mathbb{Z}/2\mathbb{Z}$.

   Now consider $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Since it is the compositum of the linearly disjoint fields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$, its discriminant satisfies

   $$d_{K/\mathbb{Q}} = d_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}^{\left[\mathbb{Q}(\sqrt{5}):\mathbb{Q}\right]} \cdot d_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}^{\left[\mathbb{Q}(\sqrt{3}):\mathbb{Q}\right]} = 12^2 \cdot 5^2 = 60^2.$$

For a tower of field extensions $A \subset B \subset C$, we have

$$d_{C/A} = N_{B/A}(d_{C/B}) \cdot d_{B/A}^{[C:B]}.$$

Applying this to $\mathbb{Q} \subset F \subset K$, we obtain

$$N_{F/\mathbb{Q}}(d_{K/F}) = 1.$$

In particular, the extension $F \subset K$ is unramified. Moreover, $F \subset K$ is abelian, since $\mathbb{Q} \subset K$ is abelian with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Therefore, K is contained in the Hilbert class field of F (by the equivalent characterization of the Hilbert class field).

Since both fields have the same degree, recall that the class number of F is 2, we conclude that they coincide. Hence,

$$K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

is the Hilbert class field of $F = \mathbb{Q}(\sqrt{15})$.

2. Let F be a number field and denote its Hilbert class field by F_1.

   (a) Let F_2 be the Hilbert class field of F_1. We show that F_2/F is Galois. Since extensions of number fields are separable, it suffices to prove normality of F_2/F, i.e. that every F-embedding $\sigma\colon F_2 \hookrightarrow \mathbb{C}$ has image $\sigma(F_2) = F_2$. Let $\sigma\colon F_2 \hookrightarrow \mathbb{C}$ be an F-embedding. Its restriction to F_1 satisfies

   $$\sigma|_{F_1} \in \mathrm{Hom}_F(F_1, \mathbb{C}) = \mathrm{Hom}_F(F_1, F_1),$$

   because F_1/F is Galois. In particular $\sigma(F_1) = F_1$. Now σ induces an isomorphism

   $$\sigma\colon F_2 \xrightarrow{\cong} \sigma(F_2),$$

   Since F_2 is the Hilbert class field of F_1, i.e. the maximal unramified abelian extension of F_1, $\sigma(F_2)$ has to be the maximal unramified abelian extension of $\sigma(F_1) = F_1$. By uniqueness of the Hilbert class field of F_1, we must have $\sigma(F_2) = F_2$. Thus, every F-embedding of F_2 into $\mathbb{C}$ is an F-automorphism of F_2, so F_2/F is normal and hence Galois.

   (b) Set $A = \mathrm{Gal}(F_2/F_1)$ and $G = \mathrm{Gal}(F_2/F)$. Then $A \trianglelefteq G$ and

   $$G/A \cong \mathrm{Gal}(F_1/F).$$

   Since F_2 is the Hilbert class field of F_1, it is unramified over F_1 and hence (by multiplicativity of ramification in towers) also unramified over F. Consequently F_1 is the maximal abelian subextension of F contained in F_2, so G/A is the largest abelian quotient of G. Equivalently, A is the commutator subgroup $G' = [G, G]$ of G.
   Next consider the extension-of-ideals map $\mathcal{I}_F \to \mathcal{I}_{F_1}$, which is a group homomorphism. Composing with the quotient $\mathcal{I}_{F_1} \to \mathcal{I}_{F_1}/\mathcal{P}_{F_1}$ gives

   $$\tilde{\gamma}\colon \mathcal{I}_F \longrightarrow \mathcal{I}_{F_1}/\mathcal{P}_{F_1}.$$

   If $(a) \in \mathcal{P}_F$ is principal in F, then $(a)\mathcal{O}_{F_1}$ is principal in F_1, so $\tilde{\gamma}\big((a)\big)$ is trivial. Hence $\tilde{\gamma}$ factors through the quotient by $\mathcal{P}_F$, yielding a homomorphism of ideal class groups

   $$\gamma\colon \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F \longrightarrow \mathcal{I}_{F_1}/\mathcal{P}_{F_1} = \mathcal{C}_{F_1},$$

   given on classes by $\mathfrak{a}\mathcal{P}_F \mapsto (\mathfrak{a}\mathcal{O}_{F_1})\mathcal{P}_{F_1}$.

   (c) By the Isomorphy Theorem, we obtain

   $$G/G' \cong \mathrm{Gal}(F_1/F) \cong \mathcal{C}_F \quad \text{and} \quad G' = A = \mathrm{Gal}(F_2/F_1) \cong \mathcal{C}_{F_1},$$

   since the Hilbert class field of a number field K is, by definition, the class field associated with $\mathcal{P}_{K,\mathcal{O}_K} = \mathcal{P}_K$, the group of principal ideals of K.
   We thus have the following commutative diagram:

   $$\begin{array}{ccc} \mathcal{C}_F & \xrightarrow{\cong} & G/G' \\ \big\downarrow{\scriptstyle \gamma} & & \big\downarrow{\scriptstyle V} \\ \mathcal{C}_{F_1} & \xrightarrow{\cong} & G'. \end{array}$$

If we can show that the transfer map V is trivial, then by commutativity of the diagram it follows that γ is trivial as well. Triviality of γ means that every ideal of F becomes principal in F_1, i.e. the Principal Ideal Theorem holds for F_1/F.

(d) Finally, observe that $A = G'$ is abelian. Hence its commutator subgroup $(G')'$ is trivial. The hypothesis of the given group-theoretic theorem therefore applies and implies that the transfer map

$$V\colon G/G' \longrightarrow A$$

is trivial. By commutativity of the diagram this yields $\gamma = 0$, so every ideal of $\mathcal{O}_F$ becomes principal in $\mathcal{O}_{F_1}$. This is precisely the Principal Ideal Theorem.

3. Let $\|\cdot\|$ be an absolute value on a number field F. We want to show that there exists a positive real number λ such that $\|\cdot\|^\lambda$ satisfies the triangle inequality.

First, note that by multiplicativity we have $\|1\| = 1$, and by definition $\|0\| = 0$. Suppose that $c = 1$. Then, whenever $\|x\| \leq 1$, we have

$$\|1 + x\| \leq 1.$$

Let $y, z \in F$. We claim that $\|\cdot\|$ already satisfies the triangle inequality. If either y or z is zero, the inequality is trivially verified. Hence, suppose that y and z are both nonzero, and without loss of generality assume that $\|y\| \leq \|z\|$. Set $u = \frac{y}{z}$. By multiplicativity of the absolute value, we obtain

$$\|u\| = \frac{\|y\|}{\|z\|} \leq 1.$$

By assumption, this implies that $\|1 + u\| \leq 1$. Therefore,

$$\|y + z\| = \|z\| \cdot \|1 + u\| \leq \|z\| \leq \|y\| + \|z\|.$$

Hence $\|\cdot\|$ satisfies the triangle inequality. Moreover, we have seen that $\|\cdot\|$ is non-Archimedean.

Suppose now that $c > 1$. Note that by setting $\lambda = \log_c(2)$, we obtain

$$\|1 + x\|^\lambda \leq c^\lambda = 2$$

whenever $\|x\| \leq 1$. We will show that $|\cdot| \coloneqq \|\cdot\|^\lambda$ satisfies the triangle inequality.

Let $x_1, x_2 \in F$. If $0 \neq |x_1| \geq |x_2|$, then

$$|x_1 + x_2| = |x_1| \cdot |x_1^{-1} x_2 + 1| \leq 2|x_1|.$$

Hence,

$$|x_1 + x_2| \leq 2 \max\big\{|x_1|, |x_2|\big\}.$$

We now derive an inequality for general finite sums of elements. We will show by induction that the absolute value of a sum of 2^r elements is bounded by 2^r times the maximal absolute value of the summands.

The case $r = 1$ was established above. Assume the statement holds for $r - 1$. Then,

$$\begin{aligned}\left|\sum_{k=1}^{2^r} x_k\right| &\leq 2 \max\left\{\left|\sum_{k=1}^{2^{r-1}} x_k\right|, \left|\sum_{k=2^{r-1}+1}^{2^r} x_k\right|\right\} \\ &\leq 2 \max\Big\{2^{r-1} \max_{1 \leq k \leq 2^{r-1}} \big\{|x_k|\big\}, 2^{r-1} \max_{2^{r-1}+1 \leq k \leq 2^r} \big\{|x_k|\big\}\Big\} \\ &= 2^r \max\big\{|x_1|, \ldots, |x_{2^r}|\big\},\end{aligned}$$

where $x_1, \ldots, x_{2^r} \in F$.

Next, consider a general $n > 1$. Let $r \in \mathbb{N}$ be such that $2^{r-1} < n \leq 2^r$. We can extend any sum over n elements to a sum over 2^r elements by adding $2^r - n$ zeros. Hence,

$$\left|\sum_{k=1}^{n} x_k\right| \leq 2^r \max\big\{|x_1|, \ldots, |x_n|\big\} \leq 2n \max\big\{|x_1|, \ldots, |x_n|\big\}, \tag{11}$$

for any $x_1, \dots, x_n \in F$.

In particular, this implies that

$$|n| = |\underbrace{1 + \dots + 1}_{n \text{ times}}| \leq 2n \cdot |1| \leq 2n \tag{12}$$

for all $n \in \mathbb{N}$.

Now let $y, z \in F$ and $n \in \mathbb{Z}$. We compute:

$$\begin{aligned}
|y+z|^n = \big|(y+z)^n\big| &= \left|\sum_{k=0}^{n} \binom{n}{k} y^k z^{n-k}\right| \\
&\leq 2(n+1) \max_{k=0,\dots,n} \left|\binom{n}{k} y^k z^{n-k}\right| && \text{by (11)} \\
&\leq 2(n+1) \max_{k=0,\dots,n} 2\binom{n}{k} |y|^k |z|^{n-k} && \text{by (12)} \\
&\leq 4(n+1)\big(|y| + |z|\big)^n.
\end{aligned}$$

In the last inequality, we used the trivial observation that a sum of nonnegative terms is at least as large as its maximal summand.

Taking the n-th root of both sides and noting that the function $x \mapsto \sqrt[n]{x}$ is increasing on $[0, +\infty)$, we obtain

$$|y+z| \leq \sqrt[n]{4(n+1)}\,\big(|y| + |z|\big).$$

Since this inequality holds for all $n \in \mathbb{Z}$, we can pass to the limit as $n \to +\infty$. Because

$$\lim_{n \to +\infty} \sqrt[n]{4(n+1)} = 1,$$

we conclude that

$$|y+z| \leq |y| + |z|.$$

As $y, z \in F$ were arbitrary, it follows that $|\cdot| = \|\cdot\|^\lambda$ satisfies the triangle inequality.

4. Let $F = \mathbb{Q}(i)$ and $x = 2 - i$. We recall that $\mathcal{O}_F = \mathbb{Z}[i]$, which is a PID (indeed, it is even a Euclidean domain). For any element $a + bi \in \mathcal{O}_F$, the norm is given by

$$N_{F/\mathbb{Q}}(a + bi) = a^2 + b^2,$$

and the norm of a principal ideal generated by such an element coincides with this value. Hence, the norm of x is

$$N_{F/\mathbb{Q}}(x) = 2^2 + (-1)^2 = 5.$$

Since 5 is a rational prime, it follows that x is irreducible, and therefore prime, in $\mathcal{O}_F$. Recall that the $\mathfrak{p}$-adic absolute value of x differs from 1 if and only if $\mathfrak{p}$ appears in the factorization of $(x) = x\mathcal{O}_F$. In particular, the only finite prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ for which $\|x\|_\mathfrak{p} \neq 1$ is the ideal $\mathfrak{p} = (x)$. We compute

$$\|x\|_{(x)} = N\big((x)^{-\operatorname{ord}_{(x)}(x)}\big) = N\big((x)\big)^{-1} = 5^{-1}.$$

Since $\mathbb{Q}(i)$ is an imaginary quadratic field, it possesses a single infinite place, corresponding to the complex embedding

$$\sigma \colon \mathbb{Q}(i) \hookrightarrow \mathbb{C}, \quad a + bi \mapsto a + bi.$$

For this embedding, the corresponding absolute value is

$$\|x\|_\sigma = |\sigma(x)|_\mathbb{C}^2 = |2 - i|^2 = 5.$$

There are no real infinite places of F.

Therefore, only two places $v \in V_F$ satisfy $\|x\|_v \neq 1$, namely the finite place corresponding to (x) and the infinite complex place σ. We may now verify the product formula:

$$\prod_{v \in V_F} \|x\|_v = \|x\|_{(x)} \cdot \|x\|_\sigma = 5^{-1} \cdot 5 = 1.$$

Hence, the product formula holds for $x = 2 - i$ in $F = \mathbb{Q}(i)$.

5. Let G be a topological group and H be a subgroup of G

   (a) For all $g \in G$ the map induced by left multiplication with g is a homeomorphism. In particular, since H is open, every left coset of H in G is open. The union of all left cosets different from H is therefore an open set, so its complement H is closed. Thus an open subgroup is closed.

   (b) Conversely, if H is a closed subgroup then each left coset gH is closed. If $[G : H] < \infty$ then there are only finitely many left cosets. The union of finitely many closed sets is closed, so the complement (which is H) is open. Thus a closed subgroup of finite index is open.

   (c) If H is open, then every left coset gH is open. By choosing one representative from each coset, we obtain a disjoint open cover of G. If G is compact, every open cover has a finite subcover. Since the cosets in the cover are pairwise disjoint, the open cover can be finite only if there are finitely many cosets. Therefore, $[G : H]$ is finite.

15.9 Week 9 solutions by Junda Long

1. Let K be a number field. For every place v of K denote by K_v the completion of K at v. For a non-archimedean place v let $\mathcal{O}_v$ be its valuation ring and $\mathcal{O}_v^\times$ its unit group. Each $K_v^\times$ is a topological group for the topology coming from the local field K_v.

   The *idele group* of K is the *restricted direct product*

$$\mathbf{I}_K = \prod_v{}' K_v^\times = \Big\{(x_v)_v \in \prod_v K_v^\times \;\Big|\; x_v \in \mathcal{O}_v^\times \text{ for almost all non-archimedean } v\Big\},$$

   equipped with the *restricted product topology* generated by the basic open sets

$$\mathcal{U} = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v^\times,$$

   where S is any finite set of places containing all archimedean places, and each U_v is an open neighbourhood of a fixed element x_v in $K_v^\times$.

   The goal of this note is to give a detailed proof that $\mathbf{I}_K$ is a topological group; i.e. that multiplication

$$m : \mathbf{I}_K \times \mathbf{I}_K \longrightarrow \mathbf{I}_K, \qquad m((x_v),(y_v)) = (x_v y_v)$$

   and inversion

$$\iota : \mathbf{I}_K \longrightarrow \mathbf{I}_K, \qquad \iota((x_v)) = (x_v^{-1})$$

   are continuous maps (and of course $\mathbf{I}_K$ is a group algebraically because multiplication and inversion are defined coordinatewise).

   Key observations used repeatedly

   - For each place v, the maps

$$m_v : K_v^\times \times K_v^\times \to K_v^\times, \quad (a,b) \mapsto ab, \qquad \iota_v : K_v^\times \to K_v^\times, \quad a \mapsto a^{-1},$$

     are continuous (they are continuous in the topology of the local field K_v).
   - For non-archimedean v, $\mathcal{O}_v^\times$ is a compact open subgroup of $K_v^\times$; in particular $\mathcal{O}_v^\times$ is stable under multiplication and inversion and is open in $K_v^\times$.
   - A basic open set in the restricted product is obtained by choosing a finite S and open sets U_v for $v \in S$ and taking $\prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v^\times$. Equivalently such a basic open set is the intersection with the full product $\prod_v K_v^\times$ of a product-open set that equals $\mathcal{O}_v^\times$ at almost all non-archimedean v.

   Continuity of multiplication:

   Continuity is a local property; we prove m is continuous at an arbitrary point $\big(x,y\big) = \big((x_v)_v,(y_v)_v\big) \in \mathbf{I}_K \times \mathbf{I}_K$.

Let $\mathcal{U} \subset \mathbf{I}_K$ be a basic open neighbourhood of the product $xy = (x_v y_v)_v$. By definition there exists a finite set S of places containing all archimedean places and all non-archimedean places where either x_v or y_v fails to lie in $\mathcal{O}_v^\times$, and open sets $U_v \subset K_v^\times$ for $v \in S$, such that

$$\mathcal{U} = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v^\times$$

and $x_v y_v \in U_v$ for every $v \in S$.

Fix $v \in S$. Since the local multiplication m_v is continuous at (x_v, y_v) there exist open neighbourhoods V_v of x_v and W_v of y_v in $K_v^\times$ such that

$$m_v(V_v \times W_v) = \{ab : a \in V_v, b \in W_v\} \subset U_v.$$

(Explicitly: choose V_v, W_v with $V_v W_v \subset U_v$.)

For $v \notin S$ choose $V_v = W_v = \mathcal{O}_v^\times$. This choice is valid because for $v \notin S$ we have $x_v, y_v \in \mathcal{O}_v^\times$ and $\mathcal{O}_v^\times$ is a subgroup, hence $\mathcal{O}_v^\times \cdot \mathcal{O}_v^\times = \mathcal{O}_v^\times \subset \mathcal{O}_v^\times$.

Now set

$$\mathcal{V} = \prod_{v \in S} V_v \times \prod_{v \notin S} \mathcal{O}_v^\times \qquad \text{and} \qquad \mathcal{W} = \prod_{v \in S} W_v \times \prod_{v \notin S} \mathcal{O}_v^\times.$$

These are basic open neighbourhoods of x and y in $\mathbf{I}_K$, respectively. By construction, for any $(a_v)_v \in \mathcal{V}$ and $(b_v)_v \in \mathcal{W}$ we have for each place v

$$a_v b_v \in \begin{cases} U_v, & v \in S, \\ \mathcal{O}_v^\times, & v \notin S, \end{cases}$$

hence $m\big(\mathcal{V} \times \mathcal{W}\big) \subset \mathcal{U}$.

Since $\mathcal{U}$ was an arbitrary basic open neighbourhood of xy, this proves m is continuous at (x, y). Because (x, y) was arbitrary, m is continuous everywhere on $\mathbf{I}_K \times \mathbf{I}_K$.

Continuity of inversion:

Again we check continuity at an arbitrary point $x = (x_v)_v \in \mathbf{I}_K$. Let $\mathcal{U}$ be a basic open neighbourhood of $x^{-1} = (x_v^{-1})_v$. Choose a finite set S of places (containing all archimedean places and all non-archimedean places where $x_v \notin \mathcal{O}_v^\times$) and open sets $U_v \subset K_v^\times$ for $v \in S$ such that

$$\mathcal{U} = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v^\times$$

and $x_v^{-1} \in U_v$ for each $v \in S$.

For each $v \in S$ the local inversion map ι_v is continuous at x_v, so there exists an open neighbourhood $V_v \subset K_v^\times$ of x_v such that $\iota_v(V_v) = \{a^{-1} : a \in V_v\} \subset U_v$. For $v \notin S$ put $V_v = \mathcal{O}_v^\times$. Note that $\mathcal{O}_v^\times$ is invariant under inversion (it is a subgroup), so $\iota_v(V_v) = \mathcal{O}_v^\times \subset \mathcal{O}_v^\times$.

Define the basic open set

$$\mathcal{V} = \prod_{v \in S} V_v \times \prod_{v \notin S} \mathcal{O}_v^\times,$$

which is an open neighbourhood of x in $\mathbf{I}_K$. By construction $\iota(\mathcal{V}) \subset \mathcal{U}$. As $\mathcal{U}$ was arbitrary, ι is continuous at x, and hence everywhere.

locally compact:

Since $\mathbf{I}_K$ is a topological group, to prove it is locally compact it suffices to find a compact neighbourhood of 1.

For each archimedean (infinite) place v, define

$$A_v = \{\, x \in K_v^\times : |x - 1|_v \leq \tfrac{1}{2} \,\},$$

which is a compact neighbourhood of 1 in $K_v^\times$.

For each non-archimedean (finite) place v, let

$$A_v = \mathcal{O}_v^\times,$$

which is compact and open in $K_v^\times$.

Now set

$$A = \prod_{v \text{ archimedean}} A_v \times \prod_{v \text{ non-archimedean}} \mathcal{O}_v^\times.$$

Let $\{U_i\}_{i\in I}$ be an open cover of A in the restricted product topology. Choose U_1 containing the identity idele $1 \in A$. Since U_1 is open in J_K, it contains a basic neighbourhood of the form

$$V = \Big(\prod_{v\in S} V_v\Big) \times \prod_{v\notin S} \mathcal{O}_v^\times,$$

where S is a finite set of places and each $V_v \subset K_v^\times$ is an open neighbourhood of 1.

Because for every non-archimedean v we have $A_v = \mathcal{O}_v^\times$, it follows that

$$\prod_{v\notin S} A_v \;=\; \prod_{v\notin S} \mathcal{O}_v^\times \;\subseteq\; V \subseteq U_1.$$

Hence U_1 covers all factors of A outside the finite set S.

Thus every element of A lies in U_1 except possibly for its projection to the finite product

$$A_S := \prod_{v\in S\cap\{\text{arch}\}} A_v \;\times \prod_{v\in S\cap\{\text{non-arch}\}} \mathcal{O}_v^\times.$$

Since S is finite and each A_v and $\mathcal{O}_v^\times$ is compact, the set A_S is a finite product of compact spaces, hence compact.

The family $\{U_i \cap A\}_{i\in I}$ covers A_S, so by compactness of A_S there exist

$$U_1,\ U_{i_2}, \ldots, U_{i_m}$$

such that

$$A_S \subset U_1 \cup U_{i_2} \cup \cdots \cup U_{i_m}.$$

Since U_1 already covers all components of A outside S, these finitely many open sets cover all of A.

Therefore $\{U_1, U_{i_2}, \ldots, U_{i_m}\}$ is a finite subcover of the original open cover, and A is compact.
Then A is a compact neighbourhood of 1 in the idele group $\mathbf{I}_K$, proving that $\mathbf{I}_K$ is locally compact.

2. Let K be a number field, and as before write $\mathbf{I}_K = \prod_v' K_v^\times$ for the idele group (restricted product with respect to $\mathcal{O}_v^\times$ at finite places). The diagonal map

$$\Delta : K^\times \longrightarrow \mathbf{I}_K, \qquad \Delta(a) = (a)_v$$

is an injective group homomorphism; we identify $K^\times$ with its image $\Delta(K^\times) \subset \mathbf{I}_K$. We will show this image is a discrete subgroup of $\mathbf{I}_K$.

The subgroup $\Delta(K^\times) \subset \mathbf{I}_K$ is discrete. Equivalently, there exists a neighbourhood U of the identity $1 \in \mathbf{I}_K$ such that $U \cap \Delta(K^\times) = \{1\}$.

We construct an explicit basic neighbourhood U of 1 with the required property.

Choose for each infinite (archimedean) place v a small open neighbourhood $V_v \subset K_v$ of 0; later we will choose these so small that they separate the archimedean image of units. For each finite (non-archimedean) place v put $W_v = \mathcal{O}_v^\times$, the unit group of the valuation ring (which is compact and open). Define a basic neighbourhood of $1 \in \mathbf{I}_K$ by

$$U \;=\; \prod_{v|\infty} (1 + V_v) \;\times \prod_{v\nmid\infty} \mathcal{O}_v^\times,$$

where $1 + V_v = \{1 + x : x \in V_v\} \subset K_v^\times$ (shrinking V_v if necessary we may assume $1 + V_v \subset K_v^\times$).

Suppose $a \in K^\times$ satisfies $\Delta(a) \in U$. Then for every finite place v we have $a \in \mathcal{O}_v^\times$, i.e. $v(a) = 0$. Hence a is an algebraic integer which is a unit at every finite place; consequently $a \in \mathcal{O}_K^\times$ (the global unit group of the ring of integers $\mathcal{O}_K$).

Thus

$$\Delta(K^\times)\cap U \subset \big\{\text{global units } \varepsilon\in\mathcal{O}_K^\times \;\big|\; \varepsilon\in 1+V_v \text{ for every archimedean } v\big\}.$$

Consider the archimedean embedding

$$\iota_\infty : \mathcal{O}_K^\times \longrightarrow \prod_{v|\infty} K_v^\times, \qquad \varepsilon \mapsto (\varepsilon)_{v|\infty}.$$

By Dirichlet's unit theorem (or, equivalently, by passing to the logarithmic embedding) the image of $\mathcal{O}_K^\times$ under the map

$$\varepsilon \longmapsto \big(\log|\varepsilon|_v\big)_{v|\infty}$$

is a full-rank lattice in a hyperplane of $\mathbb{R}^{r+s}$. In particular the archimedean image $\iota_\infty(\mathcal{O}_K^\times)$ is discrete in $\prod_{v|\infty} K_v^\times$ (with the product topology coming from the usual topologies on the archimedean completions).

Therefore we may choose the neighbourhoods V_v small enough so that the only global unit lying in $1+V_v$ for every archimedean v is $\varepsilon = 1$. With such a choice we obtain

$$\Delta(K^\times)\cap U = \{1\}.$$

Hence 1 has a neighbourhood in $\mathbf{I}_K$ meeting the diagonal copy of $K^\times$ only in 1, which proves $\Delta(K^\times)$ is discrete. Since Δ is a group homomorphism, $\Delta(K^\times)$ is a discrete subgroup of $\mathbf{I}_K$.

3. (a) Let F be a number field. For each place v denote by F_v the completion and by $\mathcal{O}_v$ the valuation ring when v is non-archimedean. The idele group is the restricted product

$$J_F = \prod_v{}' F_v^\times,$$

and the adelic norm is

$$|\cdot| : J_F \to \mathbb{R}_{>0}, \qquad |(a_v)_v| = \prod_v |a_v|_v.$$

Put

$$J_F^1 = \ker(|\cdot|) = \{a\in J_F :\ |a| = 1\}.$$

The inclusion $F^\times \subset J_F^1$ is immediate from the product formula: for every $x\in F^\times$ one has $\prod_v |x|_v = 1$, so the diagonal image of $F^\times$ lies in J_F^1.

It remains to show compactness of $J_F^1/F^\times$. Fix some notation and a compact neighbourhood of $1\in J_F$. For each infinite (archimedean) place v choose a compact neighbourhood $U_v\subset F_v^\times$ of 1 (for example $U_v = \{x\in F_v^\times : |x-1|_v \le 1/2\}$). For each finite (non-archimedean) place v take $U_v = \mathcal{O}_v^\times$ (compact and open). Put

$$U := \prod_{v|\infty} U_v \times \prod_{v\nmid\infty} \mathcal{O}_v^\times \subset J_F.$$

Then U is compact (Tychonoff, the first exercise) and is a neighbourhood of 1.

We will show every element of J_F^1 can be moved into U by multiplying by some element of $F^\times$. This implies

$$J_F^1 = F^\times\cdot(U\cap J_F^1),$$

so the image of the compact set $U\cap J_F^1$ in the quotient $J_F^1/F^\times$ is the whole quotient, hence $J_F^1/F^\times$ is compact.

So let $x = (x_v)_v \in J_F^1$ be arbitrary. Define the finite set S to contain all archimedean places and all finite places v for which $x_v\notin\mathcal{O}_v^\times$ (there are only finitely many such finite places by the restricted product condition). For each finite $v\in S$ choose a uniformizer $\pi_v\in F_v$ and let $n_v := \mathrm{ord}_v(x_v)\in\mathbb{Z}$. Define

$$\alpha_0 := \prod_{v\in S,\, v\nmid\infty} \pi_v^{-n_v} \in F^\times.$$

By construction the finite components of $\alpha_0 x$ are units: for every finite v,

$$\mathrm{ord}_v\left((\alpha_0 x)_v\right) = \mathrm{ord}_v(\alpha_0) + \mathrm{ord}_v(x_v) = \begin{cases} 0, & v \notin S, \\ 0, & v \in S \end{cases}$$

so $(\alpha_0 x)_v \in \mathcal{O}_v^\times$ for all finite v. Thus the only obstruction for $\alpha_0 x$ to lie in U is at the archimedean places.

We will now adjust α_0 by multiplying by a second factor $\beta \in F^\times$ which is arbitrarily close to $(\alpha_0 x_v)^{-1}$ at each archimedean v, while at the same time being congruent to 1 to sufficiently high order at each finite $v \in S$, so that the finite valuations are not altered. More precisely, choose for every infinite v an archimedean neighbourhood V_v of $(\alpha_0 x_v)^{-1}$ small enough that if $\beta \in V_v$ then $\beta(\alpha_0 x_v) \in U_v$. For each finite $v \in S$ choose an integer $N_v \geq 1$ so large that if $\beta \equiv 1 \pmod{\pi_v^{N_v}}$ then β is a unit in F_v and multiplication by β does not change the condition $(\alpha_0 x)_v \in \mathcal{O}_v^\times$.

Now apply the (standard) Weak Approximation Theorem: for the finite set of places $T := S \cup \{v \mid \infty\}$ and the prescribed targets

$$\begin{cases} \beta \equiv 1 \pmod{\pi_v^{N_v}} & \text{for each finite } v \in S, \\ \beta \in V_v & \text{for each archimedean } v, \end{cases}$$

there exists $\beta \in F^\times$ satisfying all these local conditions simultaneously. (The congruence conditions at finite places can be realized by requiring β to lie in a specified open coset in $F_v^\times$, so they fit into the local approximation conditions allowed by weak approximation.)

Set $\alpha := \beta\alpha_0 \in F^\times$. By construction:

- For every finite v, $\mathrm{ord}_v((\alpha x)_v) = \mathrm{ord}_v(\beta) + \mathrm{ord}_v(\alpha_0 x_v) = 0$, so $(\alpha x)_v \in \mathcal{O}_v^\times$.
- For every infinite v, $(\alpha x)_v = \beta(\alpha_0 x_v) \in U_v$ by the choice of V_v.

Hence $\alpha x \in U$. Since $x \in J_F^1$ was arbitrary, we have shown that every element of J_F^1 is $F^\times$-equivalent to an element of the compact set $U \cap J_F^1$. Therefore the quotient $J_F^1/F^\times$ is compact, as required.

(b) Let $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}} \in \mathcal{I}_F$ be a fixed fractional ideal. We show that $\eta^{-1}(\{\mathfrak{a}\})$ is open in J_F.

An idele $a = (a_v)_v$ satisfies $\eta(a) = \mathfrak{a}$ exactly when

$$\mathrm{ord}_\mathfrak{p}(a_\mathfrak{p}) = n_\mathfrak{p} \quad \text{for all finite primes } \mathfrak{p}.$$

Since $a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ for all but finitely many $\mathfrak{p}$, only finitely many conditions $\mathrm{ord}_\mathfrak{p}(a_\mathfrak{p}) = n_\mathfrak{p} \neq 0$ are nontrivial.

For each finite $\mathfrak{p}$, the function

$$\mathrm{ord}_\mathfrak{p} : F_\mathfrak{p}^\times \to \mathbb{Z}$$

is locally constant: the subsets

$$U_\mathfrak{p}(m) = \{x \in F_\mathfrak{p}^\times : \mathrm{ord}_\mathfrak{p}(x) = m\} = \pi_\mathfrak{p}^m \mathcal{O}_\mathfrak{p}^\times$$

are open in $F_\mathfrak{p}^\times$.

Hence for the given $\mathfrak{a}$, the set

$$V_\mathfrak{p} = \begin{cases} \pi_\mathfrak{p}^{n_\mathfrak{p}} \mathcal{O}_\mathfrak{p}^\times, & \text{if } \mathfrak{p} \text{ is finite}, \\ F_\mathfrak{p}^\times, & \text{if } \mathfrak{p} \text{ is infinite} \end{cases}$$

is open in $F_\mathfrak{p}^\times$. Then

$$\eta^{-1}(\{\mathfrak{a}\}) = \Big(\prod_\mathfrak{p} V_\mathfrak{p}\Big) \cap J_F$$

is a basic open subset of the restricted product topology on J_F.

Since the preimage of each point $\{\mathfrak{a}\} \subset \mathcal{I}_F$ is open, η is continuous when $\mathcal{I}_F$ has the discrete topology.

(c) Let $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \in \mathcal{I}_F$ be any fractional ideal (only finitely many $n_{\mathfrak{p}} \neq 0$). We construct $a = (a_v)_v \in J_F^1$ with $\eta(a) = \mathfrak{a}$.

Step 1: prescribe finite components. Choose a finite set S of finite primes containing all $\mathfrak{p}$ with $n_{\mathfrak{p}} \neq 0$. For each $\mathfrak{p} \in S$ pick a uniformizer $\pi_{\mathfrak{p}} \in F_{\mathfrak{p}}$ and set

$$a_{\mathfrak{p}} := \pi_{\mathfrak{p}}^{n_{\mathfrak{p}}} \in F_{\mathfrak{p}}^{\times}.$$

For every finite prime $\mathfrak{p} \notin S$ set $a_{\mathfrak{p}} := 1 \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Thus the finite part of the idele a we will build has the desired valuations:

$$\operatorname{ord}_{\mathfrak{p}}(a_{\mathfrak{p}}) = n_{\mathfrak{p}} \qquad (\mathfrak{p} \text{ finite}).$$

Step 2: choose archimedean components and compute the norm. For each archimedean place v choose any nonzero element $a_v \in F_v^{\times}$. The tuple $(a_v)_v$ (with the finite components from Step 1 and these archimedean choices) defines an idele

$$b = (b_v)_v \in J_F$$

whose finite valuations realize $\mathfrak{a}$: $\eta(b) = \mathfrak{a}$. Its adelic norm

$$t := |b| = \prod_v |b_v|_v$$

is some positive real number.

Step 3 : adjust the norm to 1 by changing an archimedean component. Let $b = (b_v)_v \in J_F$ be the idele constructed in Steps 1–2 so that $\eta(b) = \mathfrak{a}$. Set

$$t := |b| = \prod_v |b_v|_v > 0.$$

Choose an archimedean place v_0 of F (there is at least one). Since $F_{v_0} \cong \mathbb{R}$ or $\mathbb{C}$, there exists an element $c \in F_{v_0}^{\times}$ with $|c|_{v_0} = t^{-1}$. (Indeed, any positive real number occurs as the absolute value of some element of $R^{\times}$ or $\mathbb{C}^{\times}$.)

Step 4 (conclude). Define the idele $a = (a_v)_v \in J_F$ by

$$a_v = \begin{cases} c\, b_{v_0}, & v = v_0, \\ b_v, & v \neq v_0. \end{cases}$$

Since c lies in the archimedean completion F_{v_0}, multiplying only the v_0-coordinate does not change any finite valuation, so for every finite prime $\mathfrak{p}$ we still have $\operatorname{ord}_{\mathfrak{p}}(a_{\mathfrak{p}}) = \operatorname{ord}_{\mathfrak{p}}(b_{\mathfrak{p}}) = n_{\mathfrak{p}}$, hence $\eta(a) = \mathfrak{a}$. Moreover

$$|a| = \left|c b_{v_0}\right|_{v_0} \prod_{v \neq v_0} |b_v|_v = |c|_{v_0} \cdot |b| = t^{-1} \cdot t = 1,$$

so $a \in J_F^1$. This proves that every fractional ideal $\mathfrak{a}$ is the content of some idele in J_F^1, i.e. $\eta(J_F^1) = \mathcal{I}_F$.

(d) From part (c) we have $\eta(J_F^1) = \mathcal{I}_F$; moreover η sends principal ideles (diagonal image of $F^{\times}$) to principal ideals, so η factors through the quotient by $F^{\times}$. Concretely, write

$$\bar{\eta} : \; J_F^1/F^{\times} \;\longrightarrow\; \mathcal{I}_F/\mathcal{P}_F = \mathscr{C}_F$$

for the map induced by η. The map $\bar{\eta}$ is continuous because η is continuous (when $\mathcal{I}_F$ is given the discrete topology, as shown in part (b)) and constant on $F^{\times}$-cosets, so it descends to the quotient.

Since $\eta(J_F^1) = \mathcal{I}_F$, the induced map $\bar{\eta}$ is surjective. A continuous image of a compact space is compact, therefore $\mathscr{C}_F = \operatorname{im}(\bar{\eta})$ is compact.

Finally, $\mathscr{C}_F$ carries the discrete topology (it is a quotient of the discrete group $\mathcal{I}_F$); a topological space that is both compact and discrete must be finite (every point is open, so compactness forces finitely many points). Hence $\mathscr{C}_F$ is finite.

4. (a) Surjectivity Let $\mathbf{a} = (a_v)_v \in J_{\mathbb{Q}}$. We must find $r \in \mathbb{Q}^\times$, $t \in \mathbb{R}_{>0}$ and $u_p \in \mathbb{Z}_p^\times$ for all primes p with

$$\mathbf{a} = \Phi\big(r, t, (u_p)_p\big).$$

Write the finite prime factorization of $\mathbf{a}$ at the finite places:

$$\mathrm{ord}_p(a_p) = n_p \in \mathbb{Z}, \qquad \text{with } n_p = 0 \text{ for almost all } p.$$

Define the rational number

$$r := \mathrm{sign}(a_\infty) \prod_p p^{n_p} \in \mathbb{Q}^\times.$$

(Here $\mathrm{sign}(a_\infty) \in \{\pm 1\}$ is the sign of the real component a_∞.)

For each finite prime p put

$$u_p := r^{-1} a_p \in \mathbb{Q}_p^\times.$$

By construction $\mathrm{ord}_p(u_p) = \mathrm{ord}_p(a_p) - \mathrm{ord}_p(r) = n_p - n_p = 0$, hence $u_p \in \mathbb{Z}_p^\times$. At the infinite place set

$$t := r^{-1} a_\infty \in \mathbb{R}^\times.$$

Because we included $\mathrm{sign}(a_\infty)$ in the definition of r, the real number t is positive (indeed $t = |a_\infty|$), so $t \in \mathbb{R}_{>0}$.

Thus $(r, t, (u_p)_p)$ lies in the domain and

$$\Phi\big(r, t, (u_p)_p\big) = (rt,\ ru_2,\ ru_3, \ldots) = (a_\infty, a_2, a_3, \ldots) = \mathbf{a},$$

showing surjectivity.

(b) Injectivity Suppose $\Phi(r, t, (u_p))$ is the identity idele $\mathbf{1} = (1, 1, 1, \ldots)$. Then

$$rt = 1 \quad \text{in } \mathbb{R}, \qquad ru_p = 1 \quad \text{in } \mathbb{Q}_p \text{ for every } p.$$

From $ru_p = 1$ we get $u_p = r^{-1} \in \mathbb{Z}_p^\times$ for every prime p. In particular $\mathrm{ord}_p(r) = 0$ for every p, so r has no prime divisors; hence $r = \pm 1$.

From $rt = 1$ and $t > 0$ we deduce $r > 0$. Combining $r \in \{\pm 1\}$ with $r > 0$ gives $r = 1$. Therefore $t = 1$ and $u_p = 1$ for all p. This shows the only element of the domain mapping to the identity is the trivial triple, so Φ is injective.

(c) Topology: fundamental system of neighborhoods of 1 Endow the left-hand group with the product topology in which $\mathbb{Q}^\times$ is given the discrete topology, $\mathbb{R}_{>0}$ the usual topology (as a topological group under multiplication), and $\prod_p \mathbb{Z}_p^\times$ the product topology (each $\mathbb{Z}_p^\times$ being a compact open subgroup of $\mathbb{Q}_p^\times$). Each factor is a topological group, hence the product is a topological group.

A convenient fundamental system of neighbourhoods of the identity $1 = (1, 1, (1)_p)$ is given by all sets of the form

$$V_{I, \varepsilon, (N_p)} = \{1\} \times \big(1 - \varepsilon, 1 + \varepsilon\big) \times \prod_{p \in I} (1 + p^{N_p} \mathbb{Z}_p) \ \times \ \prod_{p \notin I} \mathbb{Z}_p^\times,$$

where

- I is a finite set of primes,
- each $N_p \geq 1$ is an integer,
- $\varepsilon > 0$.

Here $1 + p^{N_p}\mathbb{Z}_p$ is an open neighbourhood of 1 in $\mathbb{Z}_p^\times$, and $(1 - \varepsilon, 1 + \varepsilon)$ is an open neighbourhood of 1 in $\mathbb{R}_{>0}$ (interpreted multiplicatively). The discrete factor $\mathbb{Q}^\times$ contributes the singleton $\{1\}$ to ensure we describe neighbourhoods of the identity in the product topology.

These sets form a basis at 1 because any product neighbourhood of 1 contains one of these. Multiplication and inversion are continuous in each factor, hence continuous in the product; therefore the product is a topological group.

Finally, Φ is a bijection between the product group (with the product topology above) and $J_{\mathbb{Q}}$. One checks Φ is continuous (it is defined coordinatewise by continuous maps) and open (basic product neighbourhoods map to basic restricted-product neighbourhoods in $J_{\mathbb{Q}}$), so Φ is a topological isomorphism onto $J_{\mathbb{Q}}$. In particular the left-hand group is a topological group and identifies topologically with $J_{\mathbb{Q}}$.

15.10 Week 10 solutions by Eliot Grimont

1. We recall that we have a short exact sequence of G-modules

$$0 \to B \xrightarrow{f} A \xrightarrow{g} C \to 0$$

We also recall the construction of $\delta_1 : H^1(C) \to H^0(B)$ as in the book of Childress. Let $c \in ker_C\ s(G)$. Since g is surjective, there exists $a_1 \in A$ such that $g(a_1) = c$. But since $c \in ker_C\ s(G)$, we have

$$0 = s(G)(g(a_1)) = g(s(G)(a_1))$$

so that $s(G)(a_1) \in ker(g) = im(f)$. Then there exists $b_1 \in B$ with $f(b_1) = s(G)(a_1)$. Now

$$\begin{aligned} 0 &= (\sigma - 1)s(G)(a_1) \\ &= (\sigma - 1)f(b_1) \\ &= f((\sigma - 1)(b_1)) \end{aligned}$$

Hence, by injectivity of f we get $(\sigma - 1)(b_1) = 0$ so that $b_1 \in ker_B\ (\sigma - 1)$. So we may define

$$\delta_1(c + (\sigma - 1)C) = b_1 + s(G)B$$

Let's check that δ_1 is well-defined. Suppose $c + (\sigma - 1)C = c' + (\sigma - 1)C$ in $H^1(C)$. Repeating the abovee for c', we obtain

$$\begin{aligned} &a_1' \in A \text{ with } g(a_1') = c', \text{ and} \\ &b_1' \in B \text{ with } f(b_1') = s(G)(a_1') \end{aligned}$$

It suffices to show that

$$b_1 - b_1' \in s(G)B$$

We have that $c - c' \in (\sigma - 1)C$ and since g is surjective, there exists $a \in A$ such that

$$c - c' = (\sigma - 1)(g(a)) = g((\sigma - 1)(a))$$

Also

$$c - c' = g(a_1) - g(a_1') = g(a_1 - a_1')$$

Thus

$$g(a_1 - a_1' - (\sigma - 1)(a)) = 0$$

So that $a_1 - a_1' - (\sigma - 1)(a) \in ker(g) = im(f)$. But now there exists $b \in B$ with

$$f(b) = a_1 - a_1' - (\sigma - 1)(a)$$

Hence

$$\begin{aligned} s(G)f(b) &= s(G)(a_1 - a_1' - (\sigma - 1)(a)) \\ &= f(b_1) - f(b_1') \end{aligned}$$

So that

$$f(s(G)(b)) = f(b_1 - b_1')$$

And by injectivity of f we get that

$$b_1 - b_1' \in s(G)B$$

as wanted.
Now that we know that δ_1 is well-defined, let's show that $im(\delta_1) = ker(f_0)$. First let $c \in ker_c\ s(G)$, we have

$$\begin{aligned} f_0(\delta_1(c + (\sigma - 1)C)) &= f_0(b_1 + s(G)B) \\ &= f(b_1) + s(G)A \\ &= s(G)a_1 + s(G)A \\ &= s(G)A \end{aligned}$$

So $im(\delta_1) \subseteq ker(f_0)$. Now let $b + s(G)B \in ker(f_0)$, it means that $f(b) \in s(G)A$. Hence there exists $a \in A$ suvh that $f(b) = s(G)(a)$. Define $c = g(a) \in C$, and oberve that

$$s(G)(c) = s(G)(g(a)) = g(s(G)(a)) = g(f(b)) = 0$$

so that $c \in ker_C\ (\sigma - 1)$, and by definition

$$\delta_1(c + (\sigma - 1)C) = b + s(G)B$$

So $ker(f_0) \subseteq im(\delta_1)$ and then

$$im(\delta_1) = ker(f_0)$$

2. Let $x \in \mathbb{Z}[G]$, and denote also by x the left multiplication by x in either A, B or $A \times B$, which is G-module map. Obseve that

$$\begin{aligned} ker_{A\times B}(x) &= \{(a,b) \in A \times B \mid x(a,b) = (0,0)\} \\ &= \{(a,b) \in A \times B \mid xa = 0,\ xb = 0\} \\ &= ker_A(x) \times ker_B(x) \end{aligned}$$

Similarly

$$\begin{aligned} im_{A\times B}(x) &= \{x(a,b) \mid (a,b) \in A \times B\} \\ &= \{(xa, xb) \mid (a,b) \in A \times B\} \\ &= im_A(x) \times im_B(x) \end{aligned}$$

So we get

$$\begin{aligned} \mathcal{Q}_G(A \times B) &= \frac{\left[ker_{A\times B}(\sigma - 1) : im_{A\times B}s(G)\right]}{\left[ker_{A\times B}s(G) : im_{A\times B}(\sigma - 1)\right]} \\ &= \frac{\left[ker_A(\sigma - 1) \times ker_B(\sigma - 1) : im_A s(G) \times im_B s(G)\right]}{\left[ker_A s(G) \times ker_B s(G) : im_A(\sigma - 1) \times im_B(\sigma - 1)\right]} \\ &= \frac{\left[ker_A(\sigma - 1) : im_A s(G)\right]\ \left[ker_B(\sigma - 1) : im_B s(G)\right]}{\left[ker_A s(G) : im_A(\sigma - 1)\right]\ \left[ker_B s(G) : im_B(\sigma - 1)\right]} \\ &= \mathcal{Q}_G(A)\ \mathcal{Q}_G(B). \end{aligned}$$

3. (a) Assume for contradiction that the action is not transitive. Then there exist two places $w, w' \mid v$ lying in distinct G-orbits. Thus the sets

$$\{\sigma(w) : \sigma \in G\}, \qquad \{\sigma(w') : \sigma \in G\}$$

are disjoint.
By the Approximation Theorem, we may choose an element $\alpha \in K^\times$ satisfying

$$||\sigma(\alpha)||_w < 1 \qquad \text{and} \qquad ||\sigma(\alpha)||_{w'} > 1 \qquad \text{for all } \sigma \in G.$$

But then

$$||N_{K/F}(\alpha)||_w < 1 < ||N_{K/F}(\alpha)||_{w'}$$

which is absurd because $N_{K/F}(\alpha) \in F$ and $w|_F = v = w'|_F$. Therefore, the assumption that w and w' lie in distinct orbits is impossible, and the action of G on the places above v must be transitive.

(b) Let $\iota : K^\times \to J_K$ be the inclusion given by $\iota(\alpha) = (\alpha)_{w\in V_K}$. Then for $v \in V_F$ $\iota(\alpha)_{w|v} = (\alpha)_{w|v}$ and the action by $\sigma \in G$ is given by

$$\sigma \cdot (\alpha)_{w|v} = (\sigma(\alpha))_{w|v}$$

So we get

$$\sigma \cdot \iota(\alpha) = \iota(\sigma(\alpha))$$

as wanted.

(c) Let $v \in V_F$ and fix a place $w \mid v$ of K. Consider the map

$$Gal(K_w/F_v) \longrightarrow G, \qquad \tau \longmapsto \tau|_K,$$

where $Gal(K_w/F_v)$ denotes the group of F_v-automorphisms of the local field K_w. By definition, these automorphisms fix F_v. Moreover, since K_w/F_v is a finite extension of complete fields, every automorphism is automatically continuous with respect to the w-adic topology: this is because any field automorphism fixing the base field F_v is F_v-linear and linear maps on finite-dimensional normed vector spaces are continuous.
If $\tau \in Gal(K_w/F_v)$, then $\tau|_K$ is an automorphism of K fixing F, hence an element of $G = Gal(K/F)$. Since τ is continuous and preserves the w-adic valuation, we have

$$w(\tau(x)) = w(x) \qquad \text{for all } x \in K_w^\times.$$

This shows that $\tau|_K$ fixes the place w, because a place is determined by the valuation it induces. Hence

$$\tau|_K \in G_w := \{\sigma \in G : \sigma(w) = w\},$$

and the restriction map lands in G_w.
Suppose $\tau \in Gal(K_w/F_v)$ restricts to the identity on K. Since K is dense in K_w and τ is continuous, τ must act trivially on all of K_w. Hence $\tau = id$, so the map is injective.
Let $\sigma \in G_w$. Then σ is a field automorphism of K fixing F and satisfying $\sigma(w) = w$. Because σ preserves the valuation corresponding to w, it is continuous for the w-adic topology on K. Since K is dense in K_w, any continuous map from K extends uniquely to a continuous automorphism of the completion K_w. Thus σ extends to an element $\widetilde{\sigma} \in Gal(K_w/F_v)$ whose restriction to K is σ, which proves surjectivity.
Since the map is injective with image G_w, we conclude that

$$Gal(K_w/F_v) \;\cong\; G_w.$$

4. (a) Assume K/F is cyclic with generator $\sigma \in Gal(K/F)$ of order n. Observe firstly that $F^\times \to K^\times$ is clearly injective since it is just the inclusion of $F^\times$ into $K^\times$. We define

$$\varphi : K^\times \to ker(N_{K/F}), \quad \varphi(\alpha) = \frac{\alpha}{\sigma(\alpha)}$$

We have for any $\alpha \in K^\times$ that

$$N_{K/F}\left(\frac{\alpha}{\sigma(\alpha)}\right) = \prod_{i=0}^{n-1} \sigma^i\left(\frac{\alpha}{\sigma(\alpha)}\right) = \frac{\prod_{i=0}^{n-1}\sigma^i(\alpha)}{\prod_{i=0}^{n-1}\sigma^{i+1}(\alpha)} = 1$$

because G is cyclic. So φ is well defined, and clearly it is a group morphism because σ is a group morphism.
It remains to show that $ker(\varphi) = F^\times$ and that φ is surjective.
If $\varphi(\alpha) = 1$ it means that $\alpha = \sigma(\alpha)$, so α is fixed by σ and hence by the whole Galois group since it is a generator, so $\alpha \in F^\times$. Conversely any $\alpha \in F^\times$ is fixed by σ, so $\varphi(\alpha) = 1$. Thus $ker(\varphi) = F^\times$.
Let $b \in K^\times$ such that $N_{K/F}(b) = 1$. Define a map

$$f : G \longrightarrow K^\times, \qquad f(\sigma^i) = \prod_{j=0}^{i-1} \sigma^j(b),$$

with the convention that the empty product $f(1)$ is equal to 1. We check that f is a 1-cocycle. For any $i, k \in \{0, \ldots, n-1\}$ we have

$$f(\sigma^{i+k}) = \prod_{j=0}^{i+k-1} \sigma^j(b) = \Big(\prod_{j=0}^{i-1}\sigma^j(b)\Big)\Big(\prod_{j=i}^{i+k-1}\sigma^j(b)\Big) = f(\sigma^i)\,\sigma^i\big(f(\sigma^k)\big),$$

so $f(\tau\sigma) = \tau(f(\sigma))\,f(\tau)$ for all $\tau, \sigma \in G$. Thus Hilbert's Theorem 90 applies, and there exists $\alpha \in K^\times$ such that

$$f(\tau) = \frac{\tau(\alpha)}{\alpha}, \qquad \text{for all } \tau \in G.$$

But $f(\sigma) = b$, so $b = \sigma(\alpha)/\alpha = \varphi(\alpha^{-1})$. Therefore b lies in the image of φ, proving that φ is surjective.
We have shown that $\ker(\varphi) = F^\times$ and that φ is surjective onto $\ker(N_{K/F})$. This yields the desired short exact sequence

$$1 \longrightarrow F^\times \longrightarrow K^\times \xrightarrow{\varphi} ker(N_{K/F}) \longrightarrow 1.$$

(b) Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite extension of finite fields. This extension is Galois with cyclic Galois group generated by the Frobenius automorphism

$$\sigma : x \mapsto x^q.$$

By the previous result, for any cyclic Galois extension K/F we have the short exact sequence

$$1 \longrightarrow F^\times \longrightarrow K^\times \xrightarrow{\varphi} ker(N_{K/F}) \longrightarrow 1,$$

where $\varphi(\alpha) = \alpha/\sigma(\alpha)$ and $N_{K/F}$ is the field norm.
Applying this to $K = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_q$, we obtain that φ is surjective onto $\ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})$. Since $K^\times$ is a finite group, the exactness of the sequence implies

$$|\ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})| = \frac{|K^\times|}{|F^\times|} = \frac{q^n - 1}{q - 1}.$$

But the image of the norm is a subgroup of $F^\times$, and we have

$$|F^\times| = q - 1.$$

Since $|K^\times| = |ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})| \cdot |im(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})|$, we obtain

$$|im(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})| = \frac{q^n - 1}{|\ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})|} = q - 1 = |F^\times|.$$

Hence $im(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}) = F^\times$. In other words, the norm map

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$$

is surjective.

15.11 Week 11 solutions by Damien Ganaël Bridel

1. We first want to find the valuation $v_p(n!)$ for any number $n \in \mathbb{N}$. First, notice that if $n < p$, then $v_p(n!) = 0$. Now if $n \geq p$, then we have contributions of powers of p in $n!$:

$$p, 2p, \ldots, \lfloor \frac{n}{p} \rfloor p$$

but also (if $n \geq p^2$) contributions given by

$$p^2, 2p^2, \ldots, \lfloor \frac{n}{p^2} \rfloor p^2$$

and so on with powers of p.
Hence, the numbers of powers of p in the decomposition in prime number of $n!$ is given by

$$v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

where this sum is finite since after some large $k \in \mathbb{N}$, $\lfloor \frac{n}{p^k} \rfloor = 0$. Notice that since $\lfloor \frac{n}{p^k} \rfloor \leq \frac{n}{p^k}$ for any $k \in \mathbb{N}$,

$$v_p(n!) \leq \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1}$$

since it's a geometric serie. Hence,

$$|\frac{1}{n!}|_p = p^{-v_p(\frac{1}{n!})} = p^{v_p(n!)} \leq p^{\frac{n}{p-1}}$$

By real analysis, the radius of convergence $R \in \mathbb{Q}$ satisfies

$$\frac{1}{R} = \limsup_{n\to\infty} |\frac{1}{n!}|^{\frac{1}{n}} \leq \limsup_{n\to\infty} (p^{\frac{n}{p-1}})^{\frac{1}{n}} = p^{\frac{1}{p-1}}$$

So $R \geq p^{-\frac{1}{p-1}}$.

Now consider $x = p^{\frac{1}{p-1}}$ as a p-adic number in $\mathbb{C}_p$, so that $v_p(x) = \frac{1}{p-1}$. We want to show that $\exp(x)$ doesn't converge. First, for $i \in \mathbb{N}$, notice that

$$v_p(p^i!) = \sum_{k=1}^{\infty} \lfloor \frac{p^i}{p^k} \rfloor = \sum_{k=1}^{i} \frac{p^i}{p^k} = p^i \sum_{k=1}^{i} p^{-k} = p^i \frac{1-p^{-i}}{p-1} = \frac{p^i - 1}{p-1}$$

Hence,

$$v_p(\frac{x^{p^i}}{p^i!}) = p^i v_p(x) - v_p(p^i!) = \frac{p^i}{p-1} - \frac{p^i-1}{p-1} = \frac{1}{p-1}$$

Then, $|\frac{x^{p^i}}{p^i!}|_p = p^{\frac{1}{p-1}}$ is a constant for any $i \in \mathbb{N}$, which shows that $\lim_{n\to\infty} \frac{x^n}{n!} \neq 0$, so the serie cannot converge. Finally since $|x|_p = p^{-\frac{1}{p-1}}$, $R = p^{-\frac{1}{p-1}}$.

2. We can view k_2 as a k_1-vector space, and we choose $\{e_1, \ldots, e_n\}$ to be a basis, where $n = [k_2 : k_1]$. Recall that the norm map $N_{k_2/k_1} : k_2 \to k_1$ is defined as $N_{k_2/k_1}(x) = \det(M_x)$ the determinant of the map $M_x : k_2 \to k_2$ that sends $y \mapsto xy$, seen as linear map. In particular, if for $x \in k_2$ we write $x = x_1e_1 + \cdots + x_ne_n$ with $x_i \in k_1$, notice that $N_{k_2/k_1}(x) = P(x_1, \ldots, x_n)$ where P is a polynomial in $k_1[X_1, \ldots, X_n]$. Hence, $N_{k_2/k_1}(x)$ is the composition of a projection function, addition and multiplication in k_1. We just need to show that addition and multiplication are continuous with respect to the p-adic topology.

   Without loss of generality, we show continuity aroud 0. The set $B(0,\epsilon) = \{x \in k_1 \mid |x|_p < \epsilon\}$ give a basis of the open set around 0 in k_1. Let $+ : k_1 \times k_1 \to k_1$ be the addition map and $\cdot : k_1 \times k_1 \to k_1$ be the multiplication.

   Take $(x, y) \in B(0,\epsilon) \times B(0,\epsilon)$. Since $|\cdot|_p$ is a non archimedean norm,

$$|x + y|_p = \max\{|x|_p, |y|_p\} < \epsilon$$

   which shows that $B(0,\epsilon) \times B(0,\epsilon)$ is contained in the preimage of $B(0,\epsilon)$ by $+$, hence $+$ is continuous.

   Take $(x, y) \in B(0,\sqrt{\epsilon}) \times B(0,\sqrt{\epsilon})$. Then

$$|xy|_p = |x|_p|y|_p \leq \sqrt{\epsilon}\sqrt{\epsilon} = \epsilon$$

   so $B(0,\sqrt{\epsilon}) \times B(0,\sqrt{\epsilon})$ is contained in the preimage of $B(0,\epsilon)$ by $\cdot$, hence $\cdot$ is continuous.

3. (i) Recall that we have

$$\mathcal{I}_K(\mathfrak{m}) = \{\mathfrak{a} \in \mathcal{I}_K : \mathrm{ord}_{\mathfrak{p}}\mathfrak{a} = 0 \text{ for all } \mathfrak{p}|\mathfrak{m}\}$$

$$\mathcal{J}^+_{K,\mathfrak{m}} = \{\mathbf{a} \in \mathcal{J}_K : a_v > 0 \text{ for all real } v \text{ and } a_v \equiv 1 \pmod{\mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}} \text{ for all } \mathfrak{p}_v|\mathfrak{m}\}$$

   Take $\mathfrak{a} \in \mathcal{I}_K(\mathfrak{m})$ and let

$$\mathfrak{a} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v\mathfrak{a}} = \prod_{v \text{ finite},\ \mathfrak{p}_v \nmid \mathfrak{m}} \mathfrak{p}_v^{\mathrm{ord}_v\mathfrak{a}}$$

be its decomposition in primes, since $\mathrm{ord}_{\mathfrak{p}}\mathfrak{a} = 0$ for all $\mathfrak{p}|\mathfrak{m}$. For every $v \in V_K$ such that $\mathfrak{p}_v \nmid \mathfrak{m}$, choose $a_v \in K_v^\times$ such that $\mathrm{ord}_v(a_v) = \mathrm{ord}_v(\mathfrak{a})$ and take $a_v = 1$ for the $v \in V_K$ such that $\mathfrak{p}_v|\mathfrak{m}$. By taking

$$\mathbf{a} = (\dots, a_v, \dots)_{v \in V_K}$$

$\eta_{K,\mathfrak{m}}(\mathbf{a}) = \mathfrak{a}$.

(ii)-iii) Let $x, y \in K^\times$ two units such that $x\mathbf{a}, y\mathbf{a} \in \mathcal{J}^+_{K,\mathfrak{m}}$. Consider $\frac{x}{y} \in K^\times$. Notice the following:

(a) For any real place $v \in V_K$, $ya_v > 0$, $xa_v > 0$ by definition of $\mathcal{J}^+_{K,\mathfrak{m}}$, so $\frac{x}{y} = \frac{xa_v}{ya_v} > 0$

(b) For any place $v \in V_K$ such that $\mathfrak{p}_v|\mathfrak{m}$,

$$1 \equiv xa_v \equiv \frac{x}{y} ya_v \equiv \frac{x}{y} \pmod{\mathfrak{p}_v^{\mathrm{ord}_v \mathfrak{m}}}$$

by definition of $\mathcal{J}^+_{K,\mathfrak{m}}$.

Together, we have that $\frac{x}{y} \in \mathcal{J}^+_{K,\mathfrak{m}}$, and so $(\frac{x}{y}) \in \mathcal{P}^+_{K,\mathfrak{m}}$. Now

$$\alpha(\mathbf{a}) = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(xa_v)} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\frac{x}{y} ya_v)} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\frac{x}{y}) + \mathrm{ord}_v(ya_v)}$$

$$= \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(ya_v)} \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\frac{x}{y})} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(ya_v)}(\frac{x}{y})$$

Hence it is well defined in the quotient.

(iv) From Theorem 9.7, the kernel of α is

$$\ker(\alpha) = K^\times \mathcal{E}^+_{K,\mathfrak{m}}$$

4. This exercise is a generalization of Prop11.6 for arbitrary (non necessarily Galois) finite extension of field. The only part of this proof that uses the Galois assumption is that for a finite place $v \in V_F$, and if $w \mid v$ is ramified, then $[\, \mathcal{U}_v : \ N_{K_w/F_v}(\mathcal{U}_w)\,] \leq e(v/w)$ (from 11.5). We want to prove that this index is always finite even for non Galois extension, and the rest of the proof is the same.

Let $\mathcal{U}_v^{(n)} = 1 + \mathfrak{p}_v^n \subseteq \mathcal{U}_v$ be the n-th higher unit group. Notice that we have a tower of groups

$$\cdots \subset \mathcal{U}_v^{(n+1)} \subset \mathcal{U}_v^{(n)} \subset \cdots \subset \mathcal{U}_v^{(1)} \subset \mathcal{U}_v^{(0)} = \mathcal{U}_v$$

Since K_w/F_v is a finite extension, there is a number $n \in \mathbb{N}$ such that

$$[\, \mathcal{U}_v^{(n)} : N_{K_w/F_v}(\mathcal{U}_w)\,] < +\infty$$

Moreover, we have that

$$\mathcal{U}_v^{(i)} / \, \mathcal{U}_v^{(i+1)} \cong \mathcal{O}_v/\mathfrak{p}_v$$

which is a finite field. Hence $[\, \mathcal{U}_v^{(i)} : \ \mathcal{U}_v^{(i+1)}\,] < +\infty$ for every $i \in \mathbb{N}$. Finally we have that

$$[\, \mathcal{U}_v : \ N_{K_w/F_v}(\mathcal{U}_w)\,] = [\, \mathcal{U}_v : \ \mathcal{U}_v^{(1)}\,][\, \mathcal{U}_v^{(1)} : \ \mathcal{U}_v^{(2)}\,] \cdots [\, \mathcal{U}_v^{(n-1)} : \ \mathcal{U}_v^{(n)}\,][\, \mathcal{U}_v^{(n)} : \ N_{K_w/F_v}(\mathcal{U}_w)\,] < +\infty$$

15.12 Week 12 solutions by Tianxiang Xie

1. *a)* Since $v \notin S$, the extension K/F is unramified at v.
   - The invariants are $A_v^G = A_v \cap F_v = \mathcal{U}_v$.
   - The map $s(G)$ acts as the norm $N_{K/F}$. A key property of unramified extensions of local fields is that the norm map on units is surjective, i.e., $N_{K_w/F_v}(\mathcal{U}_w) = \mathcal{U}_v$.

   Thus, $s(G)A_v = \mathcal{U}_v = A_v^G$, which implies $\hat{H}^0(G, A_v) = 1$.

b) The index $[\ker_{A_v} s(G) : (\sigma - 1)A_v]$ represents the order of the cohomology group $H^1(G, A_v)$. By Shapiro's Lemma, $H^1(G, A_v) \cong H^1(G_w, \mathcal{U}_w)$, where G_w is the decomposition group. Consider the cohomology sequence derived from $1 \to \mathcal{U}_w \to K_w^\times \xrightarrow{v} \mathbb{Z} \to 0$. Since the extension is unramified, the valuation map on invariants $F_v^\times \to \mathbb{Z}$ is surjective. Combined with Hilbert's Theorem 90 ($H^1(G_w, K_w^\times) = 1$), the exact sequence implies that $H^1(G_w, \mathcal{U}_w) = 1$. Therefore, the index is 1.

c) Let $A = \prod_{v \notin S} A_v$. Cohomology commutes with direct products. From parts (a) and (b), we have $\hat{H}^0(G, A_v) = 1$ and $H^1(G, A_v) = 1$ for all $v \notin S$. It follows that:

$$A^G/s(G)A \cong \prod(\hat{H}^0) = 1 \implies A^G = s(G)A$$

$$\ker_A s(G)/(\sigma - 1)A \cong \prod(H^1) = 1 \implies \ker_A s(G) = (\sigma - 1)A$$

Consequently, the Herbrand quotient is $\mathcal{Q}_G(A) = 1$.

2. *a)* Since $\mathcal{L}$ is a lattice in V, the $\mathbb{Q}$-span $\mathbb{Q}\mathcal{L}$ is dense in $V \cong \mathbb{R}^n$. Let $\{w_1, \ldots, w_r\}$ be a complete set of representatives for the orbits of S. For each i, since $\mathbb{Q}\mathcal{L}$ is dense, we can choose an element $X'_{w_i} \in \mathbb{Q}\mathcal{L}$ arbitrarily close to the basis vector X_{w_i}. Specifically, we choose X'_{w_i} such that:

$$\left\|X'_{w_i} - X_{w_i}\right\|_0 < \frac{1}{\dim V}.$$

b) First, observe that the norm $\|\cdot\|_0$ is G-invariant. That is, for any $v \in V$ and $\sigma \in G$, $\|\sigma v\|_0 = \|v\|_0$, because σ merely permutes the coefficients corresponding to the basis $\{X_w\}$.
Also, note that for any $\sigma \in G_{w_i}$, we have $\sigma(X_{w_i}) = X_{\sigma w_i} = X_{w_i}$. Now, we estimate the distance:

$$\begin{aligned}
\left\|X''_{w_i} - X_{w_i}\right\|_0 &= \left\| \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \sigma(X'_{w_i}) - X_{w_i} \right\|_0 \\
&= \left\| \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} (\sigma(X'_{w_i}) - \sigma(X_{w_i})) \right\|_0 \\
&\leq \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \left\|\sigma(X'_{w_i} - X_{w_i})\right\|_0 \\
&= \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \left\|X'_{w_i} - X_{w_i}\right\|_0 \quad \text{(by } G\text{-invariance)} \\
&< \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \frac{1}{\dim V} = \frac{1}{\dim V}.
\end{aligned}$$

c) **Well-definedness:** We need to ensure that the definition $X''_w = \sigma(X''_{w_i})$ does not depend on the choice of σ. Suppose $\sigma w_i = \tau w_i = w$. Then $\tau^{-1}\sigma w_i = w_i$, so $\rho := \tau^{-1}\sigma \in G_{w_i}$.
We must show that X''_{w_i} is invariant under G_{w_i}. Let $\rho \in G_{w_i}$:

$$\rho(X''_{w_i}) = \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \rho\sigma(X'_{w_i}) = \frac{1}{|G_{w_i}|} \sum_{\mu \in G_{w_i}} \mu(X'_{w_i}) = X''_{w_i}.$$

Thus, $\tau^{-1}\sigma X''_{w_i} = X''_{w_i} \implies \sigma X''_{w_i} = \tau X''_{w_i}$. So X''_w is well-defined.
Why it fails for X': The element X'_{w_i} was chosen arbitrarily in $\mathbb{Q}\mathcal{L}$ near X_{w_i} and is not necessarily fixed by G_{w_i}. Thus, $\sigma X'_{w_i}$ could differ from $\tau X'_{w_i}$, making the definition ambiguous.

d) First, we show $\{X''_w\}_{w \in S}$ is a basis. For any $w \in S$, let $w = \sigma w_i$. Then:

$$\|X''_w - X_w\|_0 = \left\|\sigma(X''_{w_i}) - \sigma(X_{w_i})\right\|_0 = \left\|X''_{w_i} - X_{w_i}\right\|_0 < \frac{1}{\dim V}.$$

Since this holds for all $w \in S$, by Lemma 5.8, $\{X''_w\}_{w \in S}$ is a basis for V.

Next, regarding containment: Since $\mathcal{L}$ is preserved by G and $X'_{w_i} \in \mathbb{Q}\mathcal{L}$, any linear combination/action by G keeps the element in $\mathbb{Q}\mathcal{L}$. Thus $X''_w \in \mathbb{Q}\mathcal{L}$. To find a basis in $\mathcal{L}$, let m be the common denominator of the coefficients of all X''_w expressed in a basis of $\mathcal{L}$. Then let $Y_w = mX''_w$. Then $\{Y_w\}_{w\in S}$ is a basis for V contained in $\mathcal{L}$.

e) Let $\{Y_w\}_{w\in S}$ be the basis found in (d) (where $Y_w = mX''_w$ for some scalar m). For any $\sigma \in G$ and $w \in S$, let $w = \tau w_i$. Then $\sigma w = \sigma\tau w_i$. Using the definition from (c):

$$\sigma(Y_w) = \sigma(mX''_w) = m\sigma(\tau(X''_{w_i})) = m(\sigma\tau)(X''_{w_i}).$$

By definition, $Y_{\sigma w} = mX''_{\sigma w} = m(\sigma\tau)(X''_{w_i})$. Hence, $\sigma(Y_w) = Y_{\sigma w}$. This concludes the proof.

3. *a)* The condition $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K$ implies that $\mathfrak{m}$ is a defining modulus for the abelian extension K/F. By the definition of the conductor $\mathfrak{f}$ (as the greatest common divisor of all such moduli), we must have $\mathfrak{f} \mid \mathfrak{m}$.

Since $\mathfrak{f} \mid \mathfrak{m}$, any prime ideal $\mathfrak{p}$ that divides $\mathfrak{f}$ must also divide $\mathfrak{m}$. Consequently, if an ideal $\mathfrak{a}$ is coprime to $\mathfrak{m}$ (i.e., $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$), it is coprime to any factor of $\mathfrak{m}$, and thus coprime to $\mathfrak{f}$. Therefore, $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$.

b) The statement is true. We utilize the Artin map from Class Field Theory. Let $\psi_\mathfrak{m} : \mathcal{I}_F(\mathfrak{m}) \to \mathrm{Gal}(K/F)$ be the Artin map defined modulo $\mathfrak{m}$. By the main theorems of Class Field Theory, the kernel of this map is:

$$\ker(\psi_\mathfrak{m}) = \mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m}).$$

Similarly, for the conductor $\mathfrak{f}$, the kernel of $\psi_\mathfrak{f} : \mathcal{I}_F(\mathfrak{f}) \to \mathrm{Gal}(K/F)$ is:

$$\ker(\psi_\mathfrak{f}) = \mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f}).$$

Since $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$, the map $\psi_\mathfrak{m}$ is simply the restriction of $\psi_\mathfrak{f}$ to the subgroup $\mathcal{I}_F(\mathfrak{m})$. Therefore, the kernel of $\psi_\mathfrak{m}$ must be exactly the intersection of the kernel of $\psi_\mathfrak{f}$ with the domain $\mathcal{I}_F(\mathfrak{m})$:

$$\ker(\psi_\mathfrak{m}) = \ker(\psi_\mathfrak{f}) \cap \mathcal{I}_F(\mathfrak{m}).$$

Substituting the explicit forms of the kernels gives the desired equality:

$$\mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m}) = \mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f}) \cap \mathcal{I}_F(\mathfrak{m}).$$

c) Let $H_\mathfrak{m} = \mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m})$ and $H_\mathfrak{f} = \mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f})$. Consider the inclusion map $i : \mathcal{I}_F(\mathfrak{m}) \hookrightarrow \mathcal{I}_F(\mathfrak{f})$. From part (b), we established that $H_\mathfrak{m} = H_\mathfrak{f} \cap \mathcal{I}_F(\mathfrak{m})$. This implies that $H_\mathfrak{m} \subseteq H_\mathfrak{f}$.

Since $H_\mathfrak{m}$ maps to the identity in the quotient $\mathcal{I}_F(\mathfrak{f})/H_\mathfrak{f}$, the inclusion map induces a well-defined homomorphism between the quotients:

$$\varphi : \mathcal{I}_F(\mathfrak{m})/H_\mathfrak{m} \hookrightarrow \mathcal{I}_F(\mathfrak{f})/H_\mathfrak{f}.$$

The map is injective because the kernel of the map from $\mathcal{I}_F(\mathfrak{m})$ to the quotient $\mathcal{I}_F(\mathfrak{f})/H_\mathfrak{f}$ is exactly $H_\mathfrak{f} \cap \mathcal{I}_F(\mathfrak{m})$, which equals $H_\mathfrak{m}$.

d) The embedding in part (c) is **always an isomorphism** (under the assumption from (a) that $\mathfrak{m}$ is a valid modulus, i.e., $\mathfrak{f} \mid \mathfrak{m}$).

Reasoning: The Artin map $\psi_\mathfrak{f}$ induces an isomorphism:

$$\mathcal{I}_F(\mathfrak{f})/\mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f}) \xrightarrow{\sim} \mathrm{Gal}(K/F).$$

Similarly, since $\mathfrak{f} \mid \mathfrak{m}$, the Artin map $\psi_\mathfrak{m}$ is surjective (by Chebotarev's Density Theorem, every conjugacy class in the Galois group contains infinitely many primes, so we can always find primes coprime to $\mathfrak{m}$ representing any $\sigma \in \mathrm{Gal}(K/F)$). Thus, it induces an isomorphism:

$$\mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(K/F).$$

Since both the domain and codomain of the embedding φ are finite groups isomorphic to $\mathrm{Gal}(K/F)$, they have the same order. An injective homomorphism between two finite groups of the same order must be an isomorphism.

4. *a)* We determine the Artin symbol $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)$ by analyzing the action of p on i and $\sqrt{5}$.
The action on i is determined by $p \pmod 4$:

$$\sigma_p(i) = i \iff p \equiv 1 \pmod 4, \quad \sigma_p(i) = -i \iff p \equiv 3 \pmod 4.$$

The action on $\sqrt{5}$ is determined by the Legendre symbol $\left(\frac{p}{5}\right)$:

$$\sigma_p(\sqrt{5}) = \sqrt{5} \iff p \equiv 1, 4 \pmod 5, \quad \sigma_p(\sqrt{5}) = -\sqrt{5} \iff p \equiv 2, 3 \pmod 5.$$

Combining these congruences modulo 20:

- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = 1 \iff \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1, 4 \pmod 5 \end{cases} \implies p \equiv 1, 9 \pmod{20}.$
- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \tau \iff \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 2, 3 \pmod 5 \end{cases} \implies p \equiv 13, 17 \pmod{20}.$
- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \sigma \iff \begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 1, 4 \pmod 5 \end{cases} \implies p \equiv 11, 19 \pmod{20}.$
- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \sigma\tau \iff \begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 2, 3 \pmod 5 \end{cases} \implies p \equiv 3, 7 \pmod{20}.$

b) A prime p splits completely in $K/\mathbb{Q}$ if and only if its Artin symbol is the identity. From part (a), this corresponds to:

$$p \equiv 1, 9 \pmod{20}.$$

This matches the condition from Theorem 0.1, as these are precisely the primes p such that $p \equiv 1 \pmod m$ for the subfield $\mathbb{Q}(\zeta_m)$ containing K. Wait, specifically, $K \subset \mathbb{Q}(\zeta_{20})$. Primes splitting completely in $\mathbb{Q}(\zeta_{20})$ are $p \equiv 1 \pmod{20}$. However, K is a proper subfield. The primes splitting in K form the subgroup of $(\mathbb{Z}/20\mathbb{Z})^\times$ corresponding to $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/K)$, which is $\{1, 9\}$.

c) Suppose $p\mathbb{Z}$ is inert in $\mathbb{Q}(i)/\mathbb{Q}$. This implies $p \equiv 3 \pmod 4$. Let $\mathfrak{P} = p\mathbb{Z}[i]$. The residue degree of $\mathfrak{P}$ over p is $f = 2$. Using the property of the Artin symbol under restriction/lifting:

$$\left(\frac{p\mathbb{Z}[i]}{K/\mathbb{Q}(i)}\right) = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)^f = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)^2.$$

From part (a), if $p \equiv 3 \pmod 4$, the symbol $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)$ is either σ or $\sigma\tau$. Since $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$, the square of any element is the identity.

$$\sigma^2 = 1, \quad (\sigma\tau)^2 = 1.$$

Thus, the Artin symbol is trivial:

$$\left(\frac{p\mathbb{Z}[i]}{K/\mathbb{Q}(i)}\right) = 1.$$

(This implies $p\mathbb{Z}[i]$ splits completely in $K/\mathbb{Q}(i)$).

d) Suppose $p\mathbb{Z}$ splits in $\mathbb{Q}(i)/\mathbb{Q}$, so $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}'$. This implies $p \equiv 1 \pmod 4$. The residue degree is $f = 1$. Thus:

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}(i)}\right) = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)^1 = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right).$$

Since $p \equiv 1 \pmod 4$, we know from part (a) that the symbol is either 1 or τ. We distinguish the cases using the Legendre symbol $\left(\frac{p}{5}\right)$:

- If $\left(\frac{p}{5}\right) = 1$ (i.e., $p \equiv 1, 4 \pmod 5$), then the symbol is 1.
- If $\left(\frac{p}{5}\right) = -1$ (i.e., $p \equiv 2, 3 \pmod 5$), then the symbol is τ.

In terms of mod 20 congruences:

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}(i)}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 9 \pmod{20} \\ \tau & \text{if } p \equiv 13, 17 \pmod{20} \end{cases}$$

15.13 Week 13 solutions by Beatrice Pedroni

1. Let K/F be a cyclic extension of number fields of degree n, let $\mathcal{S}$ be a finite set of rational primes, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_F$. We follow the four steps of the exercise sheet.

   (a) Construction of m and proof of (iii): $K \cap F(\zeta_m) = F$.
   Enlarge $\mathcal{S}$ so that it contains all rational primes that ramify in $F/\mathbb{Q}$ and in $K/\mathbb{Q}$, and also the rational prime below $\mathfrak{p}$. We now apply Lemma 0.1 with this $\mathcal{S}$ and $n = [K : F]$ and obtain an integer $m > 1$, prime to every element of $\mathcal{S}$ and to $\mathfrak{p}$, such that:
   (i) $\mathrm{Gal}(F(\zeta_m)/F) \cong (\mathbb{Z}/m\mathbb{Z})^\times$;
   (ii) $\left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)$ has order divisible by n;
   (iii) there exists $\tau \in \mathrm{Gal}(F(\zeta_m)/F)$ of order divisible by n independent from $\left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)$.
   Since every rational prime ramifying in $F/\mathbb{Q}$ lies in $\mathcal{S}$ and m is prime to $\mathcal{S}$, no prime dividing m ramifies in $F/\mathbb{Q}$. Conversely, a rational prime $q \nmid m$ cannot ramify in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Hence $F \cap \mathbb{Q}(\zeta_m)$ is everywhere unramified over $\mathbb{Q}$, and by the given fact that $\mathbb{Q}$ has no nontrivial everywhere unramified extensions,
   $$F \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$
   The same argument (using that $\mathcal{S}$ contains the primes ramifying in $K/\mathbb{Q}$) gives
   $$K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$
   Set $L := K \cap F(\zeta_m)$. A standard degree identity yields
   $$[F(\zeta_m) : L] = [K(\zeta_m) : K].$$
   Moreover, thanks to the same identity we have
   $$[F(\zeta_m) : F] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m), \qquad [K(\zeta_m) : K] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m).$$
   Therefore
   $$\varphi(m) = [F(\zeta_m) : F] = [F(\zeta_m) : L][L : F] = [K(\zeta_m) : K][L : F] = \varphi(m)[L : F],$$
   so $[L : F] = 1$ and hence
   $$K \cap F(\zeta_m) = F,$$
   which proves (iii).

   (b) Description of $\mathrm{Gal}(K(\zeta_m)/F)$.
   Let $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$. Since $K \cap F(\zeta_m) = F$, the extensions K/F and $F(\zeta_m)/F$ are linearly disjoint over F, and restriction induces an isomorphism
   $$\mathrm{Gal}(K(\zeta_m)/F) \;\cong\; G \times \mathrm{Gal}(F(\zeta_m)/F).$$
   Under this identification,
   $$\left(\frac{\mathfrak{p}}{K(\zeta_m)/F}\right) = \left(\frac{\mathfrak{p}}{K/F}\right) \times \left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right).$$

   (c) Definition of H and E, proofs of (iv) and (i).
   Assume $\mathfrak{p}$ is unramified in K/F (so Frobenius elements are defined); since $\mathfrak{p} \nmid m$, it is also unramified in $F(\zeta_m)/F$ and in $K(\zeta_m)/F$. Let τ be as in (1) and define
   $$H := \left\langle\, \sigma \times \tau,\ \left(\frac{\mathfrak{p}}{K(\zeta_m)/F}\right)\right\rangle \subseteq \mathrm{Gal}(K(\zeta_m)/F), \qquad E := K(\zeta_m)^H.$$
   (iv) Since $\mathfrak{p}$ is unramified in $K(\zeta_m)/F$, its decomposition group is cyclic generated by the Frobenius element $\left(\frac{\mathfrak{p}}{K(\zeta_m)/F}\right)$, which lies in H. Hence the decomposition group of $\mathfrak{p}$ in E/F is trivial, so $\mathfrak{p}$ splits completely in E/F.
   (i) Notice that $\sigma \times \tau \in H$ fixes E and $1 \times \tau \in G \times \mathrm{Gal}(F(\zeta_m)/F)$ fixes K. Therefore, the element
   $$\sigma \times 1 = (\sigma \times \tau)(1 \times \tau)^{-1}$$
   fixes $K \cap E$. As σ generates $G = \mathrm{Gal}(K/F)$, this implies $K \cap E = F$.

(d) $K(\zeta_m) = E(\zeta_m)$.
We have $\mathrm{Gal}(K(\zeta_m)/F(\zeta_m)) \cong G \times 1$. The fixed field of $H \cap (G \times 1)$ is therefore

$$K(\zeta_m)^{H\cap(G\times 1)} = E(\zeta_m).$$

Let $b \in H \cap (G \times 1)$. Since $b \in G \times 1$, we can write $b = \sigma^a \times 1$ for some $a \in \mathbb{Z}$. On the other hand, since $H = \langle\, \sigma \times \tau,\ \big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\big)\rangle$, there exist integers i, j such that

$$b = (\sigma \times \tau)^i \Big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\Big)^j.$$

Using the identification of (2),

$$\Big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\Big) = \Big(\frac{\mathfrak{p}}{K/F}\Big) \times \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big),$$

we obtain

$$b = \Big(\sigma^i \Big(\frac{\mathfrak{p}}{K/F}\Big)^j\Big) \times \Big(\tau^i \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big)^j\Big).$$

Comparing second coordinates (since $b = \sigma^a \times 1$) gives

$$\tau^i \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big)^j = 1.$$

By Lemma 0.1(iii) the subgroups $\langle\tau\rangle$ and $\Big\langle\big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\big)\Big\rangle$ intersect trivially, hence the equality above forces $\tau^i = 1$ and $\big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\big)^j = 1$. Since both τ and $\big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\big)$ have order divisible by n, we conclude

$$n \mid i \qquad \text{and} \qquad n \mid j.$$

Now compare first coordinates:

$$\sigma^i \Big(\frac{\mathfrak{p}}{K/F}\Big)^j = \sigma^a.$$

Because $G = \langle\sigma\rangle$ has order n, from $n \mid i$ we get $\sigma^i = 1$, and from $n \mid j$ we get $\big(\frac{\mathfrak{p}}{K/F}\big)^j = 1$. Hence $\sigma^a = 1$ and therefore $b = 1$. Thus $H \cap (G \times 1) = \{1\}$, and consequently

$$K(\zeta_m)^{H\cap(G\times 1)} = K(\zeta_m).$$

But the fixed field of $H \cap (G \times 1)$ is $E(\zeta_m)$, so we obtain

$$K(\zeta_m) = E(\zeta_m),$$

which proves (ii). All four properties are proved.

2. Let F be a number field and let E be an intermediate field

$$F \subseteq E \subseteq F(\zeta_m),$$

with E/F abelian. We prove that statement (ii) of Artin Reciprocity holds for the extension E/F.
For the cyclotomic extension $F(\zeta_m)/F$, Artin Reciprocity has already been proved. In particular, there exists an ideal $\mathfrak{m}$ of $\mathcal{O}_F$, divisible only by the primes that ramify in $F(\zeta_m)/F$, such that

$$\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \ker\big(\mathcal{A}_{F(\zeta_m)/F} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow \mathrm{Gal}(F(\zeta_m)/F)\big)\,.$$

Since E is an intermediate field of $F(\zeta_m)/F$, every prime of F that ramifies in E/F also ramifies in $F(\zeta_m)/F$. Hence the same ideal $\mathfrak{m}$ is admissible for the extension E/F.
Let $\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}$. By the choice of $\mathfrak{m}$, the Artin symbol of $\mathfrak{a}$ in $F(\zeta_m)/F$ is trivial:

$$\Big(\frac{\mathfrak{a}}{F(\zeta_m)/F}\Big) = 1.$$

By the Consistency Property of the Artin symbol, the Artin symbol of $\mathfrak{a}$ in E/F is the restriction of its Artin symbol in $F(\zeta_m)/F$. Therefore

$$\left(\frac{\mathfrak{a}}{E/F}\right) = \left(\frac{\mathfrak{a}}{F(\zeta_m)/F}\right)\Big|_E = 1.$$

This shows that $\mathfrak{a}$ lies in the kernel of the Artin map for E/F, and hence

$$\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \ker\big(\mathcal{A}_{E/F} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow \mathrm{Gal}(E/F)\big).$$

Thus statement (ii) of Artin Reciprocity holds for the extension E/F, as required.

3. Let K/F be an abelian extension with Galois group G, and fix an element $\sigma \in G$. Let $\mathfrak{m}$ be a modulus divisible only by the primes that ramify in K/F. The Artin map

$$\mathcal{A} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow G$$

is surjective, and its kernel is

$$H := \mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}\mathcal{I}_K(\mathfrak{m}), \qquad \mathcal{I}_F(\mathfrak{m})/H \cong G.$$

Choose an ideal $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$ such that $\mathcal{A}(\mathfrak{a}) = \sigma$. Since only finitely many primes divide $\mathfrak{m}$, removing them does not change Dirichlet density, so it suffices to consider primes $\mathfrak{p} \nmid \mathfrak{m}$. For a prime ideal $\mathfrak{p} \nmid \mathfrak{m}$ we have

$$\left(\frac{\mathfrak{p}}{K/F}\right) = \sigma \quad \Longleftrightarrow \quad \mathcal{A}(\mathfrak{p}) = \mathcal{A}(\mathfrak{a}) \quad \Longleftrightarrow \quad \mathfrak{p}\mathfrak{a}^{-1} \in H.$$

Thus the set S_σ of primes of $\mathcal{O}_F$ whose Frobenius equals σ is precisely the set of primes contained in the coset $\mathfrak{a}H$.

Since $\mathcal{P}^+_{F,\mathfrak{m}} \subset H$, the hypotheses of Proposition 2.3 of chapter 3 are satisfied. Applying this proposition to the coset $\mathfrak{a}H$, we obtain

$$\delta_F(S_\sigma) = \frac{1}{[\mathcal{I}_F(\mathfrak{m}) : H]}.$$

Finally, because $\mathcal{I}_F(\mathfrak{m})/H \cong G$, we have $[\mathcal{I}_F(\mathfrak{m}) : H] = |G| = [K : F]$, and therefore

$$\delta_F(S_\sigma) = \frac{1}{[K : F]}.$$

4. Let K/F be an abelian extension of number fields. By Artin reciprocity, the idelic Artin map

$$\mathcal{A} : J_F \longrightarrow \mathrm{Gal}(K/F)$$

is surjective and has kernel

$$\ker(\mathcal{A}) = F^\times N_{K/F} J_K.$$

Recall that the idèle class group of F is defined by

$$C_F := J_F/F^\times.$$

Since $\mathcal{A}(f) = 1$ for every $f \in F^\times$, we have $F^\times \subseteq \ker(\mathcal{A})$. Therefore $\mathcal{A}$ is constant on cosets of $F^\times$ and factors through the quotient C_F, inducing a map

$$\overline{\mathcal{A}} : C_F \longrightarrow \mathrm{Gal}(K/F), \qquad \overline{\mathcal{A}}(xF^\times) := \mathcal{A}(x).$$

This map is well defined: if $xF^\times = yF^\times$, then $y = xf$ for some $f \in F^\times$, and hence

$$\mathcal{A}(y) = \mathcal{A}(x)\mathcal{A}(f) = \mathcal{A}(x),$$

because $f \in \ker(\mathcal{A})$. Moreover, $\overline{\mathcal{A}}$ is surjective, since $\mathcal{A}$ is surjective and the natural projection $J_F \twoheadrightarrow C_F$ is surjective.

By definition, the kernel of $\overline{\mathcal{A}}$ is

$$\ker(\overline{\mathcal{A}}) = \{\, xF^\times \in C_F : \mathcal{A}(x) = 1 \,\} = \frac{\ker(\mathcal{A})}{F^\times} = \frac{F^\times N_{K/F} J_K}{F^\times}.$$

The idelic norm map

$$N_{K/F} : J_K \longrightarrow J_F$$

sends principal idèles of $K^\times$ to principal idèles of $F^\times$ and thus induces a homomorphism on idèle class groups,

$$N_{K/F} : C_K = J_K/K^\times \longrightarrow C_F = J_F/F^\times, \qquad jK^\times \longmapsto N_{K/F}(j)F^\times.$$

Its image is

$$N_{K/F}C_K = \{\, N_{K/F}(j)F^\times : j \in J_K \,\} \subseteq C_F.$$

By construction, this image coincides with the image of $N_{K/F}J_K$ in C_F, and therefore

$$N_{K/F}C_K = \frac{F^\times N_{K/F} J_K}{F^\times} = \ker(\overline{\mathcal{A}}).$$

Thus the induced Artin map

$$\overline{\mathcal{A}} : C_F \longrightarrow \mathrm{Gal}(K/F)$$

is surjective with kernel $N_{K/F}C_K$, and by the First Isomorphism Theorem we obtain

$$\frac{C_F}{N_{K/F}C_K} \;\cong\; \mathrm{Gal}(K/F).$$

This gives the desired reformulation of the idelic Artin map.

15.14 Week 14 solutions by Marilou Bezos

1. We will start with (4) as we will use it to prove (3).

   - (4) Let $\mathcal{H} = \Phi(E) = F^\times N_{E/F} J_E$ and $K \supseteq E$. First we show $\rho_{K/F}(\mathcal{H})$ fixes E.
     By Artin Reciprocity, we have that $\mathcal{H} = \ker\rho_{E/F}$. Let $a \in \mathcal{H}$, we have:

     $$\rho_{K/F}(a)|_E = \left(\frac{a}{K/F}\right)|_E \overset{*}{=} \left(\frac{a}{E/F}\right) = \rho_{E/F}(a) = 1.$$

     Where $*$ comes from the consistency property for idèles.
     Now let $x \in K$ fixed by $\rho_{K/F}(\mathcal{H})$, let's show that $x \in E$. Since E is fixed by $\rho_{K/F}(\mathcal{H})$ then so is $E(x)$. Then as before by the consistency property we have for any $a \in \mathcal{H}$

     $$\left(\frac{a}{K/F}\right)|_{E(x)} = \left(\frac{a}{E(x)/F}\right) = 1.$$

     Thus

     $$\Phi(E) = \mathcal{H} = F^\times N_{E/F} J_E \subseteq \ker\rho_{E(x)/F} = F^\times N_{E(x)/F} J_{E(x)} = \Phi(E(x))$$

     Since we have shown $\Phi(E) \subseteq \Phi(E(x))$, then by the ordering theorem we have that $E(x) \subseteq E$ hence $x \in E$.

   - (3) We will proceed by double inclusion:
     (a) $\supseteq$: This just follows from the ordering theorem, since $K \cap K' \subseteq K$ and $K \cap K' \subseteq K'$ and thus it means that $\Phi(K) \subseteq \Phi(K \cap K')$, $\Phi(K') \subseteq \Phi(K \cap K')$.

(b) $\subseteq$: By *iv.* we have that K is the fixed field of $\rho_{KK'/F}(\Phi(K))$ and K' is the fixed field of $\rho_{KK'/F}(\Phi(K'))$. Let E be the fixed field of $\rho_{KK'/F}(\Phi(K)\Phi(K'))$. Now since $\Phi(K) \subseteq \Phi(K)\Phi(K')$, we have $\rho_{KK'/F}(\Phi(K)) \subseteq \rho_{KK'/F}(\Phi(K)\Phi(K'))$, so we must have $E \subseteq K$ and as for K', we get that $E \subseteq K \cap K'$.
Now if $a \in \Phi(K)$ and $a' \in \Phi(K)$, we get :

$$\left(\frac{aa'}{KK'/F}\right)|_{K\cap K'} = \left(\frac{a}{KK'/F}\right)|_{K\cap K'}\left(\frac{a'}{KK'/F}\right)|_{K\cap K'} = 1.$$

Which means that $\rho_{KK'/F}(\Phi(K)\Phi(K'))$ fixes $K \cap K'$ thus

$$E = K \cap K'.$$

But by *iv.* we know that E is the fixed field of $\rho_{KK'/F}(\Phi(E))$ and by injectivity of the Galois correspondance we have that

$$\rho_{KK'/F}(\Phi(E)) = \rho_{KK'/F}(\Phi(K)\Phi(K')).$$

Now if $a \in \Phi(K \cap K') = \Phi(E)$, $\exists b \in \Phi(K)$ and $b' \in \Phi(K')$ such that $\rho_{KK'/F}(a) = \rho_{KK'/F}(bb')$. Then $\rho_{KK'/F}(a(bb')^{-1}) = 1$ thus $a(bb')^{-1} \in \ker\rho_{KK'/F} = \Phi(KK') = \Phi(K) \cap \Phi(K')$ using point *ii.* of the ordering theorem. So $a(bb')^{-1} = x$ with $x \in \Phi(K) \cap \Phi(K')$ thus

$$a = \underbrace{xb}_{\in\Phi(K)}\ \underbrace{b'}_{\in\Phi(K')} \in \Phi(K)\Phi(K').$$

Hence the claim follows.

2. Recall that

$$C_F = {}^{J_F}\!/_{F^\times} \text{ and } C_{F,S} = {}^{J_{F,S}}\!/_{F_S},$$

Since $J_{F,S} \subset J_F$ and $F_S \subset F^\times$, we have a map

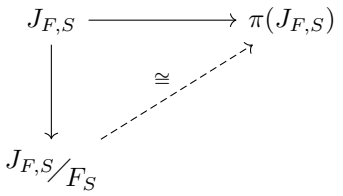
$$\iota : C_{F,S} = {}^{J_{F,S}}\!/_{F_S} \longrightarrow {}^{J_F}\!/_{F^\times} = C_F.$$

This is clear that ι is injective an thus we can see $C_{F,S}$ as a subgroup of C_F.

Let π be the quotient map

$$\pi : J_F \longrightarrow C_F.$$

We want to show that $\pi(J_{F,S}) \cong C_{F,S}$: It's easy to see that $\ker(\pi|_{J_{F,S}}) = J_{F,S} \cap F^\times = F_S$, so by simply using the first isomorphism theorem we get



And thus as we claim:

$$\pi(J_{F,S}) \cong {}^{J_{F,S}}\!/_{F_S} = C_{F,S}.$$

Now we define

$$\varphi : \ J_F \xrightarrow{\pi} C_F \xrightarrow{q} {}^{C_F}\!/_{C_{F,S}}.$$

The map is clearly surjective and, we will show by double inclusion that its kernel is $F^\times J_{F,S}$:
First, let $x \in \ker(\varphi)$, then $\pi(x) \in C_{F,S} \cong \pi(J_{F,S})$. So $\exists\, y \in J_{F,S}$ such that $\pi(x) = \pi(y)$ thus $xy^{-1} \in F^\times$ and $\exists z \in F^\times$ such that $x = zy \in F^\times J_{F,S}$.
Now, let $x \in F^\times J_{F,S}$, then $\exists z \in F^\times, y \in J_{F,S}$ such that $x = zy$, thus $\varphi(x) = \varphi(zy) = q \circ \pi(zy) = q(\pi(y)) = 1$. Thus $\ker\varphi = F^\times J_{F,S}$ and applying the first isomorphism theorem:

$${}^{J_F}\!/_{F^\times J_{F,S}} \cong {}^{C_F}\!/_{C_{F,S}}.$$

This gives us the algebraic isomorphism. For the topological part, we have to show that φ is a homeomorphism. All maps involved are quotient, thus continuous. Now since J_F is a locally compact topological group and $F^\times$ is discrete, π is also an open map. Then since $J_{f,S}$ is an open subgroup and π is an open map, we have that $\pi(J_{F,S}) = C_{F,S}$ is also open, hence closed in C_F hence the quotient map q is also open. As φ is the composition of continuous open maps, φ is also a continuous open map which is bijective, thus this is a homeomorphism.

3. (a) We show that there is an exact sequence

$$1 \longrightarrow \mathcal{O}_F^\times \longrightarrow F_S \xrightarrow{\gamma} I_{S_0}.$$

We check that this is well defined, let $\alpha \in F_S$, by definition of F_S, $v(\alpha) = 0, \forall v \notin S_0$ hence $< \alpha > \in I_{S_0}$.
To show exactness we have to show that $\ker\gamma = \mathcal{O}_F^\times$ (since the injectivity of the first map is obvious) :
If $\alpha \in \mathcal{O}_F^\times$, then $< \alpha >= \mathcal{O}_F$, so $\gamma(\alpha) = 1$. Hence $\mathcal{O}_F^\times \subset \ker\gamma$.
Now if $\alpha \in \ker\gamma$, then $< \alpha >= \mathcal{O}_F$, thus $\alpha \in \mathcal{O}_F^\times$ so $\ker\gamma = \mathcal{O}_F^\times$. This proves exactness.

(b) Let $h = \#\mathcal{C}_F$. For$v \in S_0$, the ideal $\mathfrak{p}_v^h$ is clearly principal, so this means that $\exists \alpha_v \in F^\times$ such that

$$< \alpha_v >= \mathfrak{p}_v^h.$$

Then it's easy to see that $\alpha_v \in F_S$, thus $\mathfrak{p}_v^h \in \gamma(F_S)$. So:

$$I_{S_0}^h \subset \gamma(F_S) \subset I_{S_0}.$$

Since both I_{S_0} and $I_{S_0}^h$ are free Abelian of rank $\#S_0$ so is $\gamma(F_S)$.

(c) From part a) we have the s.e.s

$$1 \longrightarrow \mathcal{O}_F^\times \longrightarrow F_S \xrightarrow{\gamma} \gamma(F_S) \longrightarrow 1.$$

from part b), the group $\gamma(F_S)$ is free Abelian. So this tells us that the sequence splits, and it follows that

$$F_S \cong \mathcal{O}_F^\times \times \gamma(F_S).$$

(d) Dirichlet's Unit Theorem tells us that

$$\mathcal{O}_F^\times \cong W_F \times \mathbb{Z}^{r_1+r_2-1},$$

And from part c):

$$F_S \cong W_F \times \mathbb{Z}^{r_1+r_2-1} \times \gamma(F_S).$$

From part b) $\gamma(F_S) \cong \mathbb{Z}^{\#S_0}$

$$F_S \cong W_F \times \mathbb{Z}^{r_1+r_2-1+\#S_0}.$$

as $\#S_\infty = r_1 + r_2$ and $\#S_0 = \#S - \#S_\infty$ we compute and conclude that:

$$F_S \cong W_F \times \mathbb{Z}^{\#S-1}.$$

4. (a) Since $\mu_2 = \{\pm 1\} \subset \mathbb{Q}$, we may apply Kummer theory for $n = 2$ over $\mathbb{Q}$. Let $a \in \mathbb{Q}^\times$ and look at the field $K = \mathbb{Q}(\sqrt{a})$. If $a \in (\mathbb{Q}^\times)^2$, then $\sqrt{a} \in \mathbb{Q}$ and $K = \mathbb{Q}$. Otherwise, $K/\mathbb{Q}$ is a quadratic extension, so it is cyclic of degree 2 and $\mathrm{Gal}(K/\mathbb{Q})$ has exponent 2.
Conversely, any cyclic extension of $\mathbb{Q}$ of degree 2 is of the form $K = \mathbb{Q}(\sqrt{a})$ for some $a \in \mathbb{Q}^\times$, with a determined up to squares. This shows that quadratic extensions of $\mathbb{Q}$ correspond to nontrivial elements of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.
Now, let $a_1, \ldots, a_r \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ and consider

$$K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r}).$$

This extension is Abelian. An automorphism is determined by choosing the sign of each $\sqrt{a_i}$, so the Galois group has exponent 2. If the classes of the a_i are linearly independent modulo squares, then

$$(Gal)(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

Thus the Kummer 2-extensions of $\mathbb{Q}$ are exactly of the form $K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r})$ whith $a_1, \ldots, a_r \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ linearly independent.

(b) Let $F = \mathbb{Q}(\zeta_3)$. Since $\mu_3 \subset F$, we can apply Kummer theory for $n = 3$. Let $\alpha \in F^\times$ and $K = F(\sqrt[3]{\alpha})$. If $\alpha \in (F^\times)^3$, then $\sqrt[3]{\alpha} \in F$ and $K = F$. Otherwise, K/F is a cyclic extension of degree 3, and Gal$l(K/F)$ has exponent 3. Thus using the same argumentation as for a) , the cyclic extensions of degree 3 over F are classified by the nontrivial classes in $F^\times/(F^\times)^3$. Now let $\alpha_1, \ldots, \alpha_r \in F^\times - (F^\times)^3$ and consider

$$K = F(\sqrt[3]{\alpha_1}, \ldots, \sqrt[3]{\alpha_r}).$$

The extension K/F is Abelian, and each automorphism sends $\sqrt[3]{\alpha_i} \mapsto \zeta_3^k \sqrt[3]{\alpha_i}$ with $k = 1, 2, 3$. So the Galois group has exponent 3and if the classes of the $\alpha_i's$ are linearly independent, we get

$$\mathrm{Gal}(K/F) \cong (\mathbb{Z}/3\mathbb{Z})^r.$$

So the Kummer 3-extensions of $\mathbb{Q}(\zeta_3)$ are of the form $K = F(\sqrt[3]{\alpha_1}, \ldots, \sqrt[3]{\alpha_r})$ with $\alpha_1, \ldots, \alpha_r \in F^\times - (F^\times)^3$.

5. We will do a double inclusion:

(a) $\supseteq$ This is the easy inclusion: Pick $x \in F_S^n$, then $\exists y \in F_S$ such that $x = y^n$. Since $y \in F_S$, we have $y \in U_v$ for all $v \notin S$, hence $x = y^n \in U_v$. For $v \in S$, $x \in (F_v^\times)^n$. Thus $x \in B$ by definition of B, and since $x \in F^\times$, $x \in B \cap F^\times$.

(b) $\subseteq$ Let $x \in B \cap F^\times$. Then $x \in (F_v^\times)^n$ for all $v \in S$, so this means that:

$$[F_v(x^{1/n}) : F_v] = 1 \text{ for all } v \in S.$$

this shows that $\mathfrak{p}_v$ splits completely in $F(x^{1/n})/F$ for all $v \in S$.
If $v \notin S$, we get that $x \in U_v$, moreover since $v \nmid n$ and $\mu_n \subset F$,then $\mathfrak{p}_v$ is unramified in $F(x^{1/n})$. Recall that

$$J_{F,S} = \prod_{v \in S} F_v^\times \times \prod_{v \notin S} U_v$$

For $v \in S$ pick w a place above v then the local norm map $N_{F(x^{1/n})_w/F_v}$ is the identity and thus $F_v^\times \subset N_{F(x^{1/n})/F}(J_{F(x^{1/n})})$ and for $v \notin S$ and w a place above v, since S contains all infinite places, then the local extension $F(x^{1/n})_w/F_v$ is a finite extension. Then we know from exercises 4, sheet 10 that the norm map is surjective for finite extension of fields, thus the local norm map is surjective and we get $N_{F(x^{1/n})_w/F_v}(U_w) = U_v$ hence every units in F_v is the image of a norm of $F_w^\times$. Thus $U_v \subset N_{F(x^{1/n})/F}(J_{F(x^{1/n})})$ and so we have that :

$$J_{F,S} \subset N_{F(x^{1/n})/F}(J_{F(x^{1/n})}).$$

And since $J_F = F^\times J_{F,S}$, we get

$$J_F = F^\times J_{F,S} \subset F^\times N_{F(x^{1/n})/F}(J_{F(x^{1/n})}).$$

By Artin reciprocity, the kernel of the Artin map

$$\rho_{F(x^{1/n})/F} : J_F \longrightarrow \mathrm{Gal}\left(F(x^{1/n})/F\right)$$

is equal to $F^\times N_{F(x^{1/n})/F}(J_{F(x^{1/n})})$. So this means that $\ker \rho_{F(x^{1/n})/F} = J_F$, and thus

$$\mathrm{Gal}\left(F(x^{1/n})/F\right) \cong {}^{J_F}\!\diagup_{N_{F(x^{1/n})/F}(J_{F(x^{1/n})})} = {}^{J_F}\!\diagup_{J_F} = 1.$$

Hence $F(x^{1/n}) = F$ and $x^{1/n} \in F$.
Since $x \in B$, we also have $x \in U_v$ for all $v \notin S$, and therefore $x \in F_S$ thus $x \in F_S^n$.

This concludes the proof.