Number theory II

Yiwen Ding

June 28, 2021

Contents

Chapter 1

Lubin-Tate formal groups

1.1 Introduction

Let K be a number field or a finite extension of $\mathbb{Q}_p$. The class field theory for K gives an "automorphic" characterization of the maximal abelian extension K^{ab} of K. For example, when K is a finite extension of $\mathbb{Q}_p$, we have the following (non-precise) statement:

Theorem 1.1.1. *Let K be a finite extension of $\mathbb{Q}_p$, then there exists a natural continuous injection $K^\times \hookrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$, and the image is dense.*

The global class field theory is a bit more involved to state for general K, while we have the following theorem in the case $K = \mathbb{Q}$.

Theorem 1.1.2 (Kronecker-Weber). *We have $\mathbb{Q}^{\mathrm{ab}} = \cup_n \mathbb{Q}(\zeta_n)$, and hence an isomorphism*

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times.$$

Here is a short and non-complete timeline on the development of the class field theory

- (1853) Kronecker-Weber theorem.
- (1927) Global class field theory on an arbitrary number fields.
- (1930's) Local class field theory (global proof).
- (1940's) Local class field theory (local proof).

We look back to Theorem 1.1.1. Let $\mathcal{O}_K$ be the ring of integers in K. By a choice of a uniformizer ϖ of K, we have an isomorphism $\mathcal{O}_K^\times \times \mathbb{Z} \xrightarrow{sim} K^\times$, $(\alpha, n) \mapsto \alpha\varpi^n$. By Theorem 1.1.1, we see $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$. In particular, we have a projection $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathcal{O}_K^\times$ (depending on ϖ). By (infinite) Galois theory, K admits an abelian extension K_ϖ such that $\mathrm{Gal}(K_\varpi/K) \cong \mathcal{O}_K^\times$. A natural problem is to find an explicit construction of K_ϖ.

Example 1.1.3. $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$ *where* $\mathbb{Q}_p(\zeta_{p^\infty}) := \cup_n \mathbb{Q}_p(\zeta_{p^n})$.

- (1965) Lubin-Tate formal group (constructing K_ϖ explicitly).

1.2 Formal group laws

Definition 1.2.1. *Let A be a commutative ring (with 1). An one-parameter commutative formal group law is a power series $F(X,Y) \in A[[X,Y]]$ such that*

1. *$F(X,Y) = X + Y +$ terms of degree ≥ 2,*
2. *$F(X, F(Y,Z)) = F(F(X,Y), Z)$,*
3. *there exists a unique $i_F(X) \in A[[X]]$ such that $F(X, i_F(X)) = 0$,*
4. *$F(X,Y) = F(Y,X)$.*

Remark 1.2.2. *(1) From the exercise, we will see Condition (3) can be implied by (1)(2)(4) and $F(X,Y)$ has the following form:*

$$F(X,Y) = X + Y + \sum_{\substack{1 \leq i < \infty \\ 1 \leq j < \infty}} a_{i,j} X^i Y^j.$$

(2) One can similarly define n-parameter formal group laws.

(3) When A is the ring $\mathcal{O}_K$ of integers of a finite extension K of $\mathbb{Q}_p$, a formal group law F defines a group structure on $\mathfrak{m}_K$: For any $a, b \in \mathfrak{m}_K$, the power series $F(a,b)$ converges in $\mathfrak{m}_K$. One checks by definition the map

$$\mathfrak{m}_K \times \mathfrak{m}_K \to \mathfrak{m}_K, \ (a,b) \mapsto F(a,b)$$

defines a group structure "$+_F$" on $\mathfrak{m}_K$.

Example 1.2.3. *(1) $F(X,Y) = X + Y$ is a formal group law (with $i_F(X) = -X$). If $A = \mathcal{O}_K$, then $+_F = +$.*

(2) $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ is a formal group with $i_F(X) = -X\sum_{i=0}^\infty (-1)^i X^i$. In fact, one can find $i_F(X)$ by solving the equation:

$$F(X, i_F(X)) = 0 \Rightarrow X + i_F(X) + X i_F(X) = 0 \Rightarrow i_F(X) = -(1+X)^{-1}X.$$

If $A = \mathcal{O}_K$, consider the following map

$$\mathfrak{m}_K \xrightarrow{\sim} 1 + \mathfrak{m}_K, \ a \mapsto 1 + a.$$

One easily checks this is a group isomorphism if the left hand side is equipped with the group operation $+_F$ and the right hand side is equipped with the standard multiplicative structure.

(3) One may associate one parameter formal group laws to elliptic curves.

Now we define morphisms of formal group laws.

Definition 1.2.4. *Let $F(X,Y)$, $G(X,Y)$ be formal group laws over A. A morphism $h : F \to G$ is a power series $h(T) \in TA[[T]]$ such that*

$$h(F(X,Y)) = G(h(X), h(Y)).$$

Example 1.2.5. *(1) If $F = G$, then $h = T \in \mathrm{End}(F)$.*

(2) Suppose $F = X + Y$, and $h \in \mathrm{End}(F)$. By definition, $h(X+Y) = h(X) + h(Y)$. By comparing the coefficients, we see if A has torsion free over $\mathbb{Z}$, then $h = aT$ for $a \in A$. However, if $p = 0$ in A then $h(T) = T^p \in \mathrm{End}(F)$.

(3) Suppose $F = X + Y + XY = (1+X)(1+Y) - 1$, and $\mathbb{Z}_p \hookrightarrow A$. For $a \in \mathbb{Z}_p$, put $[a](T) := (1+T)^a - 1 := \sum_{i=0}^{\infty} \binom{a}{i} T^i - 1$. Then

$$[a](F(X,Y)) = (1+X)^a(1+Y)^a - 1 = F([a](X), [a](Y)).$$

In particular, we get a map of sets $\mathbb{Z}_p \hookrightarrow \mathrm{End}(F)$, $a \mapsto (1+T)^a - 1$.

Lemma 1.2.6. *Let F, G, H be formal groups over A, let $f : F \to G$, $g : G \to H$ be morphisms. Then $g \circ f := g(f(T)) \in TA[[T]]$ is a morphism from F to H.*

Proof. $g(f(F(X,Y))) = g(G(f(X), f(Y))) = H(g(f(X)), g(f(Y)))$. □

Remark 1.2.7. *As in Exercise 1(b), the morphism g is invertible if and only if $g \equiv aT \pmod{T^2}$ for a certain $a \in A^\times$. If so, we denote by $g^{-1} \in TA[[T]]$ the element such that $g \circ g^{-1}(T) = g^{-1} \circ g(T) = T$.*

Let F be a formal group law over A. Then

$$TA[[T]] \times TA[[T]] \to TA[[T]], (f,g) \mapsto F(f(T), g(T)) =: f +_F g$$

defines an abelian group structure on $TA[[T]]$.

Lemma 1.2.8. *The set $\mathrm{End}(F) \subset TA[[T]]$ is stable under "$+_F$". Moreover, $\mathrm{End}(F)$ has a ring structure with the identity element T, multiplication given by composition and addition given by "$+_F$".*

Proof. Let $f, g \in \mathrm{End}(F)$. Then

$$\begin{aligned}(f +_F g)(F(X,Y)) &= F(f(F(X,Y)), g(F(X,Y))) = F(F(f(X), f(Y)), F(g(X), g(Y))) \\ &= F(F(f(X), g(X)), F(F(f(Y), g(Y)))) = F((f +_F g)(X), (f +_F g)(Y)),\end{aligned}$$

where the third equality uses the associativity and commutativity of F. We see thus $f +_F g \in \mathrm{End}(F)$. For $f, g, h \in \mathrm{End}(F)$, we have

$$h(f +_F g) = h(F(f(T), g(T))) = F(h(f(T)), h(g(T)) = (h \circ f) +_F (h \circ g).$$

The lemma follows. □

1.3 Lubin-Tate group laws

Let K be a finite extension of $\mathbb{Q}_p$, ϖ be a uniformizer of K and $q := |\mathcal{O}_K/\varpi|$. Let

$$\mathcal{F}_\varpi := \left\{ f(T) \in \mathcal{O}_K[[T]] \mid f(T) \equiv \varpi T \pmod{T^2},\ f(T) \equiv T^q \pmod{\varpi} \right\}$$

Example 1.3.1. *If $f(T) = T^q + \cdots \varpi T$ is an Eisenstein polynomial, then $f(T) \in \mathcal{F}_\varpi$.*

Lemma 1.3.2. *Let $f, g \in \mathcal{F}_\varpi$, and $\Phi_1(X_1, \cdots, X_n) = \sum_{i=1}^n a_i X_i$ be a linear form with coefficients in $\mathcal{O}_K$. Then there exists a unique $\Phi \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ such that*

$$\begin{cases} \Phi(X_1, \cdots, X_n) = \Phi_1 + \text{terms of degree} \geq 2 \\ f(\Phi(X_1, \cdots, X_n)) = \Phi(g(X_1), \cdots, g(X_n)). \end{cases}$$

Proof. By induction, it suffices to show that for any $r \in \mathbb{Z}_{\geq 1}$, there exists a unique $\Phi_r(X_1, \cdots, X_n) \in \mathcal{O}_K[X_1, \cdots, X_n]$ of degree r such that

$$\begin{cases} \Phi_r(X_1, \cdots, X_n) = \Phi_1 + \text{terms of degree} \geq 2 \\ f(\Phi_r(X_1, \cdots, X_n)) = \Phi_r(g(X_1), \cdots, g(X_n)) + \text{terms of degree} \geq r+1. \end{cases} \tag{1.1}$$

Indeed, if such $\{\Phi_r\}$ are uniquely constructed, then we see by uniqueness $\Phi_{r+1} = \Phi_r +$ terms of degree $\geq r+1$. Then one check $\Phi := \lim_r \Phi_r \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ satisfies the property.

First note Φ_1 is the unique linear form satisfying the conditions in (1.1) (noting $f \equiv g \pmod{T^2}$).

Assume the unique existence of Φ_r, and let $\Phi_{r+1} := \Phi_r + Q$ where Q is a homogeneous polynomial of degree $r+1$. We want to find Q such that

$$\begin{aligned} f(\Phi_r(X_1, \cdots, X_n) + Q(X_1, \cdots, X_n)) = \Phi_r(g(X_1), \cdots, g(X_n)) \\ + Q(g(X_1), \cdots, g(X_n)) + \text{terms of degree} \geq r+2 \end{aligned}$$

We have

$$\begin{aligned} & f(\Phi_r(X_1, \cdots, X_n) + Q(X_1, \cdots, X_n)) \\ & \qquad \equiv f(\Phi_r(X_1, \cdots, X_n)) + \varpi Q(X_1, \cdots, X_n) \pmod{\deg \geq r+2} \end{aligned}$$

$\big($noting for $h(T) \in T^2\mathcal{O}_K[[T]]$, $h(\Phi_r(X_1, \cdots, X_n) + Q(X_1, \cdots, X_n)) \equiv h(\Phi_r(X_1, \cdots, X_n)) \pmod{\deg \geq r+2}\big)$. On the other hand we have

$$\begin{aligned} \Phi_r(g(X_1), \cdots, g(X_n)) + Q(g(X_1), \cdots, g(X_n)) &\equiv \Phi_r(g(X_1), \cdots, g(X_n)) + Q(\varpi X_1, \cdots, \varpi X_n) \\ &= \Phi_r(g(X_1), \cdots, g(X_n)) + \varpi^{r+1} Q(X_1, \cdots, X_n) \pmod{\deg \geq r+2} \end{aligned}$$

So the equality holds if and only if (where $(\cdot)_{r+1}$ signifies the degree $r+1$ term)

$$Q(X_1, \cdots, X_n) = \frac{1}{\varpi^{r+1} - \varpi} \big(f(\Phi_r(X_1, \cdots, X_n)) - \Phi_r(g(X_1), \cdots, g(X_n)) \big)_{r+1}. \tag{1.2}$$

The only problem left is that the right hand side lies *a priori* in $K[[X_1, \cdots, X_n]]$. We have

$$\begin{cases} f(\Phi_r(X_1, \cdots, X_n)) \equiv \Phi_r(X_1, \cdots, X_n)^q \pmod{\varpi} \\ \Phi_r(g(X_1), \cdots, g(X_n)) \equiv \Phi_r(X_1^q, \cdots, X_n^q) \pmod{\varpi}, \end{cases}$$

and $\Psi(X_1^q, \cdots, X_n^q) \equiv \Psi(X_1, \cdots, X_n)^q \pmod{p}$ for any $\Psi \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ with constant term equal to 0. We deduce hence the right hand side of (1.2) lies in $\mathcal{O}_K[[X_1, \cdots, X_n]]$. The lemma follows. □

Remark 1.3.3. *By the proof, the statement still holds if one replaces $\mathcal{O}_K$ everywhere by any $\mathcal{O}_K$-algebra A with injective structure morphism $\mathcal{O}_K \hookrightarrow A$.*

Proposition 1.3.4. *For any $f \in \mathcal{F}_\varpi$, there exists a unique formal group law $F_f \in \mathcal{O}_K[[X, Y]]$ such that $f \in \mathrm{End}(F_f)$.*

Proof. Applying the previous lemma to $\Phi_1 = X + Y$ and $g = f$, we obtain $F_f := \Phi(X, Y) \in \mathcal{O}_K[[X, Y]]$. We need to show F_f is a formal group law. By definition $F_f(X, Y) = X + Y +$ terms of deg ≥ 2.

•$F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$: Let $\Phi^1 := F_f(X, F_f(Y, Z))$ and $\Phi^2 := F_f(F_f(X, Y), Z)$. Then the both have the form $X + Y + Z + \deg \geq 2$. One can check

$$f(F_f(X, F_f(Y, Z))) = F_f(f(X), f(F_f(Y, Z))) = F_f(f(X), F_f(f(Y), f(Z))),$$

i.e $f(\Phi^1(X, Y, Z)) = \Phi^1(f(X), f(Y), f(Z))$. Similarly, we have

$$f(\Phi^2(X, Y, Z)) = \Phi^2(f(X), f(Y), f(Z)).$$

By the uniqueness in Lemma 1.3.2, we see $\Phi^1 = \Phi^2$.

•$F_f(X, Y) = F_f(Y, X)$: by Lemma 1.3.2 and $F_f(X, Y) \equiv F_f(Y, X) \pmod{\deg \geq 2}$.

As in Exercise, the existence of i_{F_f} follows from the other conditions. So F_f is a formal group law, and it is clear $f \in \mathrm{End}(F_f)$. If there exists another formal group law F such that $f \in \mathrm{End}(F)$, the uniqueness in Lemma 1.3.2 implies $F = F_f$. □

Example 1.3.5. *Suppose $f(T) = (1 + T)^p - 1 \in \mathcal{F}_p$ (with $K = \mathbb{Q}_p$), recall $f \in \mathrm{End}(F)$ with $F(X, Y) = X + Y + XY$. Thus in this case $F_f = F = X + Y + XY$.*

Let $f, g \in \mathcal{F}_\varpi$, and $a \in \mathcal{O}_K$. Put $\Phi_1(X) = aX$. By Lemma 1.3.2, there exists a unique $[a]_{g,f}(T) \in \mathcal{O}_K[[T]]$ such that

$$\begin{cases} [a]_{g,f}(T) \equiv aT \pmod{\deg \geq 2} \\ [a]_{g,f}(f(T)) = g([a]_{g,f}(T)). \end{cases}$$

Proposition 1.3.6. *$[a]_{g,f}(T)$ is a morphism from F_f to F_g.*

Proof. We need to show $\Phi^1(X,Y) := [a]_{g,f}(F_f(X,Y)) = F_g([a]_{g,f}(X),[a]_{g,f}(Y)) =: \Phi^2(X,Y)$. It is clear that $\Phi^1(X,Y) \equiv \Phi^2(X,Y) \pmod{\deg \geq 2}$. We have

$$\begin{aligned}\Phi^1(f(X),f(Y)) = [a]_{g,f}(F_f(f(X),f(Y))) = [a]_{g,f}(f(F_f(X,Y)))\\ = g([a]_{g,f}(F_f(X,Y))) = g(\Phi^1(X,Y)).\end{aligned}$$

Similarly, we have $\Phi^2(f(X),f(Y)) = g(\Phi^2(X,Y))$. By Lemma 1.3.2, we deduce $\Phi^1 = \Phi^2$. The proposition follows. □

Proposition 1.3.7. *(1)* $[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$.

(2) $[ab]_{h,f} = [a]_{h,g} \circ [g]_{g,f}$ *(as a morphism from* F_f *to* F_h*).*

Proof. (1) $[a+b]_{g,f}(T) \equiv (a+b)T \pmod{\deg \geq 2} \equiv [a]_{g,f} +_{F_g} [b]_{g,f}$. We have $[a+b]_{g,f}(f(T)) = g \circ [a+b]_{g,f}(T)$, and

$$\begin{aligned}([a]_{g,f} +_{F_g} [b]_{g,f})(f(T)) = F_g([a]_{g,f}(f(T)),[b]_{g,f}(f(T)))\\ = F_g(g \circ [a]_{g,f}(T), g \circ [b]_{g,f}(T)) = g([a]_{g,f} +_{F_g} [b]_{g,f}). \quad (1.3)\end{aligned}$$

By Lemma 1.3.2, we deduce $[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$.

(2) We have $[ab]_{h,f} \equiv abT \equiv [a]_{h,g} \circ [b]_{g,f} \pmod{\deg \geq 2}$. We have $[ab]_{h,f}(f(T)) = h([ab]_{h,f}(T))$, and

$$([a]_{h,g} \circ [b]_{g,f})(f(T)) = [a]_{h,g}(g([b]_{g,f}(T))) = h([a]_{h,g} \circ [b]_{g,f}(T)).$$

By Lemma 1.3.2, $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$. □

Corollary 1.3.8. *For* $f, g \in \mathcal{F}_\varpi$*, we have* $F_f \cong F_g$*.*

Proof. Let $u \in \mathcal{O}_K^\times$, then $[u]_{g,f}$ defines a morphism from F_f to F_g. By (2) of the above proposition, we have $[u^{-1}]_{f,g} \circ [u_{g,f}] = [1]_{f,f}$. By Lemma 1.3.2, one easily sees $[1]_{f,f} = T$. Hence $[u^{-1}]_{f,g} = [u_{g,f}]^{-1}$. The corollary follows. □

If $f = g$, we denote by $[a]_f := [a]_{f,f}$ for $a \in \mathcal{O}_K$. By Proposition 1.3.7, we see:

Corollary 1.3.9. *The map* $\mathcal{O}_K \to \mathrm{End}(F_f)$*,* $a \mapsto [a]_f$ *is an injective ring homomorphism.*

Remark 1.3.10. *The formal group* F_f *may be called a formal* $\mathcal{O}_K$*-module.*

Example 1.3.11. *Suppose* $K = \mathbb{Q}_p$*,* $f(T) = (1+T)^p - 1 \in \mathcal{F}_p$ *hence* $F_f = X + Y + XY$*. For* $a \in \mathbb{Z}_p$*, we have* $[a]_f(T) = (1+T)^a - 1$*. The corollary (re)proves Exercise 5.6 (3).*

Lemma 1.3.12. $[\varpi]_f(T) = f(T)$.

Proof. We have $f \equiv \varpi T \equiv [\varpi]_f(T) \pmod{\deg \geq 2}$, and $f(f(T)) = f(f(T))$. By Lemma 1.3.2, the lemma follows. □

1.4 Lubin-Tate extensions

We use the notation of the last section: K, $\mathcal{O}_K$, ϖ, q. Let $f(T) \in \mathcal{F}_\varpi$, and F_f be the associated Lubin-Tate formal group. Let $\overline{K}$ be an algebraic closure of K, $\mathcal{O}_{\overline{K}} := \cup_{[L:K]<+\infty} \supset \mathfrak{m}_{\mathcal{O}_{\overline{K}}}$. Let val_K be the additive valuation on K, normalized with $\mathrm{val}_K(\varpi) = 1$. Recall val_K can uniquely extend to a valuation (still denoted by val_K) on $\overline{K}$. We have thus $\mathcal{O}_{\overline{K}} = \{x \in \overline{K} \mid \mathrm{val}_K(x) \geq 0\}$, and $\mathfrak{m}_{\mathcal{O}_{\overline{K}}} = \{x \in \overline{K} \mid \mathrm{val}_K(x) > 0\}$.

The formal group law F_f defines an operation $\mathfrak{m}_{\mathcal{O}_{\overline{K}}} \times \mathfrak{m}_{\mathcal{O}_{\overline{K}}} \to \mathfrak{m}_{\mathcal{O}_{\overline{K}}}$, $(a, b) \mapsto F_f(a, b)$. This equips with $\mathfrak{m}_{\mathcal{O}_{\overline{K}}}$ an abelian group structure. Similarly, for $\lambda \in \mathcal{O}_K$, $[\alpha]_f(T)$ defines an operator $\mathfrak{m}_{\mathcal{O}_{\overline{K}}} \to \mathfrak{m}_{\mathcal{O}_{\overline{K}}}$, $a \mapsto [\lambda]_f(a)$. The following lemma follows directly from 1.3.9.

Lemma 1.4.1. *The abelian group $\mathfrak{m}_{\mathcal{O}_{\overline{K}}}$ is an $\mathcal{O}_K$-module, where $\mathcal{O}_K$-action is given by $\{[\alpha]_f\}_{\alpha \in \mathcal{O}_K}$ (and the abelian group structure is given by F_f).*

We denote by Λ_f the $\mathcal{O}_K$-module $\mathfrak{m}_{\mathcal{O}_{\overline{K}}}$ in the above lemma.

Lemma 1.4.2. *For f, $g \in \mathcal{F}_\varpi$, $u \in \mathcal{O}_K^\times$, then the map $\Lambda_f \to \Lambda_g$, $a \mapsto [u]_{g,f}(a)$ is an isomorphism of $\mathcal{O}_K$-modules.*

Proof. We have $[u]_{g,f}(a +_{F_f} b) = [u]_{g,f}(a) +_{F_g} [u]_{g,f}(b)$, and $[u]_{g,f}([\alpha]_f(a)) = [u\alpha]_{g,f}(a) = [\alpha u]_{g,f}(a) = [\alpha]_g([u]_{g,f}(a))$. We see the morphism in the lemma is $\mathcal{O}_K$-linear, with the inverse given by $\Lambda_g \to \Lambda_f$, $a \mapsto [u^{-1}]_{f,g}(a)$. The lemma follows. □

Let $\Lambda_f[\varpi^n] \subset \Lambda_f$ be the $\mathcal{O}_K$ submodule of Λ_f $(= \mathfrak{m}_{\overline{K}})$ annihilated by ϖ^n:

$$\Lambda_f[\varpi^n] = \{a \in \mathfrak{m}_{\mathcal{O}_{\overline{K}}} \mid [\varpi^n]_f(a) = \underbrace{f \circ f \cdots \circ f}_{n}(a) = 0\}.$$

Let $K_{\varpi,n} := K(\Lambda_f[\varpi^n])$ be the algebraic extension of K generated by elements in $\Lambda_f[\varpi^n]$.

Lemma 1.4.3. *The extension $K_{\varpi,n}$ is independent of the choice of $f \in \mathcal{F}_\varpi$, in particular, $K_{\varpi,n}$ is finite over K.*

Proof. Let $f, g \in \mathcal{F}_\varpi$, and $u \in \mathcal{O}_K^\times$. We have seen that $[u]_{g,f} : \Lambda_f \xrightarrow{\sim} \Lambda_g$ as $\mathcal{O}_K$-modules. Thus $[u]_{g,f}$ induces an isomorphism $\Lambda_f[\varpi^n] \cong \Lambda_g[\varpi_n]$ with an inverse given by $[u^{-1}]_{f,g}$. Since $[u]_{g,f}(T) \in \mathcal{O}_K[[T]]$ (resp. $[u^{-1}]_{f,g}(T) \in \mathcal{O}_K[[T]]$), we deduce $K(\Lambda_g) \subset K(\Lambda_f)$ (resp. $K(\Lambda_f) \subset K(\Lambda_g)$). The first part follows. Choosing $f \in \mathcal{F}_\varpi$ to be a polynomial, we see $K_{\varpi,n}$ is generated by the roots of the polynomial $[\varpi^n]_f$ hence finite over K. □

Remark 1.4.4. *We have $[\varpi^n]_f(T) \equiv T^{q^n} \pmod{\varpi}$. We deduce $\Lambda_f[\varpi_n] = \{x \in \overline{K} \mid [\varpi^n]_f(T) = 0\}$. By the proof of the above lemma, we see the same holds if f is replaced by any $g \in \mathcal{F}_\varpi$.*

In the sequel, without loss of generality we assume $f(T)$ has the form $T^q + \cdots \varpi T$ (so f is a monic polynomial). And we write $\Lambda_n := \Lambda_f[\varpi^n]$ for simplicity.

Example 1.4.5. *Suppose $K = \mathbb{Q}_p$, and $f(T) = (1+T)^p - 1$. We have*

$$\Lambda_n = \{x \in \overline{\mathbb{Q}_p} \mid (1+x)^{p^n} - 1 = 0\} = \{\zeta_{p^n}^i - 1\}_{1 \le i \le p^n - 1},$$

and hence $\mathbb{Q}_p(\Lambda_n) = \mathbb{Q}_p(\zeta_{p^n})$.

Lemma 1.4.6. *$K_{\varpi,1}$ is a totally ramified extension of K of degree $(q-1)$.*

Proof. By definition, $f(T)/T = T^{q-1} + \cdots + \varpi$ is an Eisenstein polynomial, the lemma follows. □

Proposition 1.4.7. *We have $\Lambda_n \cong \mathcal{O}_K/\varpi^n$ as $\mathcal{O}_K$-module.*

Proof. It is clear that Λ_n is annihilated by ϖ^n and $|\Lambda_n| \le q^n$. Together with the above lemma, we see $|\Lambda_1| = q$ and the morphism $\mathcal{O}_K/\varpi \to \Lambda_1$, $x \mapsto x\alpha_1$ for any non-zero $\alpha_1 \in \Lambda_1$ is an isomorphism.

Now we use induction on n. Suppose we have an isomorphism $\mathcal{O}_K/\varpi^{n+1} \cong \Lambda_{n-1}$, sending 1 to $\alpha_{n-1} \in \Lambda_{n-1}$. Let $a_n \in \Lambda_n$ such that $\varpi a_n = \alpha_{n-1}$ (i.e. $a_n \in \overline{K}$ such that $f(a_n) = \alpha_{n-1}$). Consider $\mathcal{O}_K/\varpi^n \to \Lambda_n$, $x \mapsto xa_n$. Since $\varpi^{n-1}a_n = \varpi^{n-2}\alpha_{n-1} \neq 0$, we deduce the map is injective, hence is bijective by comparing the cardinality. The proposition follows. □

Let $\alpha_n \in \Lambda_n$ be a generator. For any $\alpha \in \Lambda_n$, there exists $\lambda \in \mathcal{O}_k$ such that $\alpha = [\lambda]_f(\alpha_n) \in K(\alpha_n)$. This implies $K_{\varpi,n} = K(\alpha_n)$

Proposition 1.4.8. *α_n is a uniformizer of $K_{\varpi,n}$, and $K_{\varpi,n}$ is totally ramified over K of degree $q^{n-1}(q-1)$.*

Proof. We use induction on n. The polynomial $f(T)/T = T^{q-1} + \cdots + \varpi$ is an Eisenstein polynomial over K, we deduce hence $K_{\varpi,1} = K(\alpha_1)$ is totally ramified over K of degree $q-1$, and α_1 is a uniformizer of $K_{\varpi,1}$.

Suppose this holds for $n-1$. We have $K_{\varpi,n} = K_{\varpi,n-1}(\alpha_n)$. Let $\alpha_{n-1} := [\varpi]_f(\alpha_n) = f(\alpha_n)$. Then α_{n-1} is a generator of Λ_{n-1}. By induction hypothesis, α_{n-1} is a uniformizer of $K_{\varpi,n-1}$. The polynomial $f(T) - \alpha_{n-1}$ is Eisenstein, we deduce that K_{α_n} is totally ramified of degree q over $K_{\alpha_{n-1}}$ hence (again by induction hypothesis) is totally ramified over K of degree $q^{n-1}(q-1)$, and that α_n is a uniformizer of $K_{\varpi,n}$. □

Proposition 1.4.9. *$K_{\varpi,n}$ is Galois over K, and $\mathrm{Gal}(K_{\varpi,n}/K) \cong (\mathcal{O}_K/\varpi^n)^\times$.*

Proof. By definition, $K_{\varpi,n}$ is the splitting field of $[\varpi^n]_f(T) \in K[T]$, hence is Galois over K. The minimal polynomial $p_n(T)$ of α_n over K is of degree $[K_{\varpi,n} : K] = q^{n-1}(q-1) = |(\mathcal{O}_K/\varpi^n)^\times|$. Then it is easy to see $p_n(T) = (f/T) \circ \underbrace{f \circ f \cdots \circ f}_{n-1}$. For $\alpha \in \Lambda_n$ with $p_n(\alpha) = 0$, we see $[\varpi^{f-1}](\alpha) \neq 0$ (as $p_n(T)$ is irreducible) hence $\alpha \notin K_{\varpi,n-1}$ and $\alpha \notin \Lambda_{n-1}$.

By comparing cardinality, we see the roots of $p_n(x)$ are exactly given by $\Lambda_n \setminus \Lambda_{n-1}$. For any $\lambda \in (\mathcal{O}_K/\varpi^n)^\times$, $\alpha_n \mapsto [\lambda]_f(\alpha_n)$ defines an element in $\sigma_\lambda \in \mathrm{Gal}(K_{\varpi,n}/K)$:

$$K_{\varpi,n} \to K_{\varpi,n},\ h(\alpha_n) \mapsto h([\lambda]_f(\alpha_n)).$$

We deduce hence a map

$$\iota_n : (\mathcal{O}_K/\varpi^n)^\times \longrightarrow \mathrm{Gal}(K_{\varpi,n}/K),\ a \mapsto \sigma_\lambda. \tag{1.4}$$

The map is surjective, as for any root α of $p_n(T)$, $\alpha \in \Lambda_n \setminus \Lambda_{n-1}$ hence there exists $\lambda \in \mathcal{O}_K^\times$ such that $[\lambda]_f(\alpha_n) = \alpha$. We have $\iota_n(\lambda_1\lambda_2)(\alpha_n) = [\lambda_1\lambda_2]_f(\alpha_n)$, and

$$\iota_n(\lambda_1)(\iota_n(\lambda_2)(\alpha_n)) = \iota_n(\lambda_1)([\lambda_2]_f(\alpha_n)) = [\lambda_2]_f(\iota_n(\lambda_1)(\alpha_n)) = [\lambda_2]_f([\lambda_1]_f(\alpha_n)) = [\lambda_1\lambda_2]_f(\alpha_n),$$

where the second equality follows from the continuity of the Galois action. We see ι_n is a group morphism. Finally since $|\mathrm{Gal}(K_{\varpi_n}/K)| = [K_{\varpi,n} : K] = q^{n-1}(q-1)$, we see (1.4) is an isomorphism. □

Proposition 1.4.10. *(1) The map (1.4) is independent of the choice of α_n.*

(2) The following diagram commutes

$$\begin{array}{ccc} (\mathcal{O}_K/\varpi^n)^\times & \xrightarrow{\iota_n} & \mathrm{Gal}(K_{\varpi,n}/K) \\ \downarrow & & \downarrow \\ (\mathcal{O}_K/\varpi^{n-1})^\times & \xrightarrow{\iota_{n-1}} & \mathrm{Gal}(K_{\varpi,n-1}/K) \end{array}$$

where the vertial maps are natural projections.

Proof. Let α_n' be another generator of Λ_n, and $\mu \in (\mathcal{O}_K/\varpi^n)^\times$ such that $\alpha_n' = [\mu]_f(\alpha_n)$. Let ι_n (resp. ι_n') be the map in (1.4) associated to α_n (resp. α_n'), i.e. for $\lambda \in (\mathcal{O}_K/\varpi_n)^\times$, $\iota_n(\lambda)(\alpha_n) = [\lambda]_f(\alpha_n)$ (resp. $\iota_n'(\lambda)(\alpha_n') = [\lambda]_f(\alpha_n')$). We have

$$\begin{aligned}\iota_n(\lambda)(\alpha_n') = \iota_n(\lambda)([\mu]_f(\alpha_n)) = [\mu]_f(\iota_n(\lambda)(\alpha_n)) \\ = [\mu]_f([\lambda]_f(\alpha_n) = [\mu\lambda]_f(\alpha_n) = [\lambda]_f(\alpha_n')\iota_n'(\lambda)(\alpha_n'),\end{aligned}$$

where the second equality follows from the continuity of the action of $\mathrm{Gal}(K_{\varpi,n}/K)$ on K_ϖ. (1) follows. Similarly we have

$$\iota_n(\lambda)([\varpi]_f(\alpha_n)) = [\lambda\varpi]_f(\alpha_n) = [\lambda]_f([\varpi_f](\alpha_n)) = \iota_{n-1}(\lambda)(\alpha_{n-1}),$$

and (2) follows. □

Let $K_\varpi := \varinjlim_n K_{\varpi,n}$. We see $\mathrm{Gal}(K_\varpi/K) \cong \varprojlim_n (\mathcal{O}_K/\varpi^n)^\times \cong \mathcal{O}_K^\times$.

Proposition 1.4.11. *For $n \geq 1$, there exists $\alpha \in K_{\varpi,n}$ such that $N_{K_{\varpi,n}/K}(\alpha) = \varpi$.*

Proof. Let $\alpha_n \in \Lambda_n$ be a generator. The minimal polynomial $r(x)$ of α_n has the form $x^{(q-1)q^{n-1}} + \cdots + \varpi$. Thus $N_{K_{\varpi,n}/K}(\alpha) = (-1)^{(q-1)q^{n-1}}\varpi$. The proposition follows for $q \neq 2^d$ or $n \neq 1$. However if $n = 1$, $q = 2^d$, $-1 = (-1)^{(q-1)} = N_{K_{\varpi,1}/K}(-1)$, hence $N_{K_\varpi/K}(-\alpha) = \varpi$. □

1.5 Local reciprocity map

Recall $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \mathrm{Gal}(\bar{k}/k)$, and we fix an isomorphism $\widehat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(\bar{k}/k)$, $1 \mapsto \mathrm{Frob}_q := [x \mapsto x^q]$. We also use σ to denote the element in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ corresponding to Frob_q, i.e. the element such that $\sigma(x) \equiv x^q \pmod{\mathfrak{m}_{K^{\mathrm{ur}}}}$.

Theorem 1.5.1. *There exists a unique homomorphism (called the local Artin map)*

$$\rho_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following properties:

(a) for any uniformizer $\varpi \in K^\times$, and any finite unramified extension L over K, $\rho_K(\varpi)|_L = \sigma$,

(b) for any finite abelian extension L of K, $N_{L/K}(L^\times)$ is contained in the kernel $a \mapsto \rho_K(a)$, and ρ_K induces an isomorphism

$$K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Remark 1.5.2. *By the property (b), one deduces that ρ_K has dense image.*

Theorem 1.5.3. *A subgroup H of $K^\times$ is an open subgroup of finite index if and only if it is a norm group, i.e. there exists a finite extension L over K such that $N_{L/K}(L^\times) = H$.*

Corollary 1.5.4. *The morphism ρ_K is continuous and injective.*

Proof. By Theorem 1.5.1 (b), $\rho_K^{-1}(\mathrm{Gal}(K^{\mathrm{ab}}/L)) = N_{L/K}(L^\times)$ that is open by Theorem 1.5.3. Hence ρ_K is continuous. By Theorem 1.5.3, $\mathrm{Ker}\,\rho_K$ is contained in any open subgroup of finite index. It is straightforward to check $\mathrm{Ker}\,\rho_K = \{1\}$. □

One direction of Theorem 1.5.3 is fairly easy

Proposition 1.5.5. *A norm group is an open subgroup of $K^\times$ of finite index.*

Proof. Let L be a finite extension of K of degree d, then $N_{L/K}(L^\times) \supset (K^\times)^d$. We show $(K^\times)^d$ (hence $N_{L/K}(L^\times)$) is an open subgroup of finite index in $K^\times$. Using $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$, it sufficies to $(\mathcal{O}_K^\times)^d$ is open of finite index in $\mathcal{O}_K^\times$. However, let m be sufficiently large (depending on d) such that $\sum_{i=0}^\infty \binom{1/d}{i}(-1)^i(x-1)^i$ converges for any $x \in 1 + \mathfrak{m}_K^m$. Then $1 + \mathfrak{m}_K^m \subset (\mathcal{O}_K^\times)^d$. The proposition follows. □

In this section, using the theory of Lubin-Tate formal groups, we prove a weaker version of Theorem 1.5.1. Recall for each uniformizer ϖ of K, we have constructed a totally ramified extension K_ϖ over K such that $\mathrm{Gal}(K_\varpi/K) \cong \mathcal{O}_K^\times$. We have a decomposition $\mathcal{O}_K^\times \times \mathbb{Z} \xrightarrow{\sim} K^\times$, $(\lambda, n) \mapsto \lambda\varpi^n$. We define a morphism $\rho_\varpi : K^\times \to \mathrm{Gal}(K_\varpi K^{\mathrm{ur}}/K)$ such that

- for $\lambda \in \mathcal{O}_K^\times$, $\rho_\varpi(\lambda)$ is trivial on K^{ur} and $\rho_\varpi(\lambda)|_{K_\varpi} = \sigma_\lambda^{-1} = [\lambda^{-1}]_f$,

- $\rho_\varpi(\varpi)|_{K_\varpi} = 1$ and $\rho_\varpi|_{K^{\mathrm{ur}}} = \sigma$.

The field K^{ur} is not p-adically complete. Indeed, write $\overline{\mathbb{F}_q} = \cup_n F_n$ where F_n are finite extensions of $\mathbb{F}_q$ such that $F_{n-1} \subsetneq F_{n_1}$, and let $a_n \in F_n \setminus F_{n-1}$ and put $a := \sum_{n=1}^{\infty} \varpi^n [a_n]$ (where $[a_n]$ denotes the Teichmuller lifting of a_n in the unramified extension K_n^{ur} of K of residue field F_n), then $a \notin K^{\mathrm{ur}}$: for any m, $\varpi^{-(m+1)}(a - \sum_{n=1}^{m} \varpi^n [a_n]) \equiv a_{m+1} \pmod{\varpi}$; we have $a_{m+1} \notin F_m$ and hence $a - \sum_{n=1}^{m} \varpi^n [a_n] \notin K_m^{\mathrm{ur}}$ that implies $a \notin K_m^{\mathrm{ur}}$ as $\sum_{n=1}^{m} \varpi^n [a_n] \in K_m^{\mathrm{ur}}$. We put $\breve{K}$ to be the completion of K^{ur}.

Theorem 1.5.6. *$K^{\mathrm{unr}} K_\varpi$ and ρ_ϖ are both independent of the choice of ϖ.*

In the rest of the section, we prove the theorem. Let ϖ_1, ϖ_2 be two uniformizers of K. Let $f \in \mathcal{F}_{\varpi_1}$ and $g \in \mathcal{F}_{\varpi_2}$. We want to show $K_{\varpi_1} K^{\mathrm{ur}} = K_{\varpi_2} K^{\mathrm{ur}}$ and $\phi_{\varpi_1} = \phi_{\varpi_2}$. Let $u \in \mathcal{O}_K^\times$ such that $\varpi_2 = \varpi_1 u$. A natural idea is to compare the formal groups F_f and F_g over $\mathcal{O}_{\breve{K}}$.

Lemma 1.5.7. *There exists $\theta(T) \in T\mathcal{O}_{\breve{K}}[[T]] \setminus T^2 \mathcal{O}_{\breve{T}}[[T]]$ such that*

$$\sigma(\theta) = \theta \circ [u]_f, \tag{1.5}$$

$$\theta \circ [u]_f \circ f \circ \theta^{-1} = g, \tag{1.6}$$

where $\sigma(r)(T) := \sum_i \sigma(a_i) T^i$ for $r = \sum_i a_i T \in \mathcal{O}_{\breve{K}}[[T]]$.

Proof of Theorem 1.5.6. We explain how to deduce Theorem 1.5.6 from the above lemma. By (1.6), we have

$$[u^n]_f \circ \underbrace{f \circ \cdots \circ f}_{n} \circ \theta^{-1} = \theta^{-1} \circ \underbrace{g \circ \cdots \circ g}_{n}.$$

So if $\alpha_n \in \Lambda_{g,n}$ then $\theta^{-1}(\alpha_n) \in \Lambda_{f,n}$. The map $a_n \mapsto \theta^{-1}(a_n)$ defines a bijection between $\Lambda_{g,n}$ and $\Lambda_{f,n}$. We then deduce

$$\breve{K} K_{\varpi_1,n} = \breve{K} K_{\varpi_2,n}. \tag{1.7}$$

We show $K'_n = \breve{K} K_{\varpi_i} \cap \overline{K} = K^{\mathrm{ur}} K_{\varpi_i,n}$. It is clear $K^{\mathrm{ur}} K_{\varpi_i,n} \subset K'_n$. For any $\tau \in \mathrm{Gal}(\overline{K}/K^{\mathrm{ur}} K_{\varpi_i,n})$, by the continuity of the Galois action, we see τ fixes K'. By (infinite) Galois theory, we have $K' \subset K^{\mathrm{ur}} K_{\varpi_i,n}$. (1.7) then implies $K^{\mathrm{ur}} K_{\varpi_1,n} = K^{\mathrm{ur}} K_{\varpi_2,n}$ hence $K^{\mathrm{ur}} K_{\varpi_1} = K^{\mathrm{ur}} K_{\varpi_2}$.

Now we compare the "local artin maps" ϕ_{ϖ_1} and ϕ_{ϖ_2}. By definition, we are led to compare the power series $[\lambda]_f$ and $[\lambda]_g$ for $\lambda \in \mathcal{O}_K$.

Claim: For $\lambda \in \mathcal{O}_K$, we have $\theta \circ [\lambda]_f \circ \theta^{-1} = [\lambda]_g$.

We prove the claim. We first show $\theta \circ [\lambda]_f \circ \theta^{-1} \in \mathcal{O}_K[[T]]$: we have

$$\begin{aligned} \sigma(\theta \circ [\lambda]_f \circ \theta^{-1}(T)) &= \sigma(\theta) \circ [\lambda_f] \circ \sigma(\theta^{-1})(T) \\ &= \theta \circ [u]_f \circ [\lambda]_f \circ [u^{-1}]_f \circ \theta^{-1}(T) = \theta \circ [\lambda]_f \circ \theta^{-1}(T). \end{aligned}$$

Now we can apply (again!) Lemma 1.3.2. We have:

- $\theta \circ [\lambda]_f \circ \theta^{-1}(T) \equiv \lambda T \pmod{T^2}$,
- $\theta \circ [\lambda]_f \circ \theta^{-1}(g(T)) = \theta \circ [\lambda]_f \circ [u_f] \circ f \circ \theta^{-1} = g \circ \theta \circ f \circ \theta^{-1}$.

The claim then follows from Lemma 1.3.2.

We have

$$\phi_{\varpi_1}(\varpi_2) = \phi_{\varpi_1}(\varpi_1 u) = \begin{cases} \sigma & \text{on } K^{\mathrm{ur}} \\ [u^{-1}]_f & \text{on } K_{\varpi_1,n} \end{cases}, \ \phi_{\varpi_2}(\varpi_2) = \begin{cases} \sigma & \text{on } K^{\mathrm{ur}} \\ 1 & \text{on } K_{\varpi_2,n} \end{cases},$$

Let $\alpha_n \in \Lambda_{f,n} \subset \breve{K}K_{\varpi_1,n} = \breve{K}K_{\varpi_2 n}$, and let $\beta_n := \lambda_{g,n}$ such that $\alpha_n = \theta^{-1}(\beta_n)$. Then

$$\phi_{\varpi_2}(\varpi_2)(\alpha_n) = \phi_{\varpi_2}(\varpi_2)(\theta^{-1}(\beta_n)) = \sigma(\theta)^{-1}(\beta_n) = [u^{-1}]_f \circ \theta^{-1} \circ \theta(\beta_n) = [u^{-1}]_f(\alpha_n),$$

hence $\phi_{\varpi_1}(\varpi_2) = \phi_{\varpi_2}(\varpi_2)$. Let $\lambda \in \mathcal{O}_K^\times$, we have

$$\phi_{\varpi_1}(\lambda) == \begin{cases} 1 & \text{on } K^{\mathrm{ur}} \\ [\lambda^{-1}]_f & \text{on } K_{\varpi_1,n} \end{cases}, \ \phi_{\varpi_2}(\lambda) = \begin{cases} 1 & \text{on } K^{\mathrm{ur}} \\ [\lambda^{-1}]_g & \text{on } K_{\varpi_2,n} \end{cases}.$$

By the claim, for any $\beta_n \in \Lambda_{g,n}$, we see $\theta \circ [\lambda^{-1}]_f \circ \theta^{-1}(\beta_n) = [\lambda^{-1}]_g(\beta_n)$ hence (the last equality uses $\theta_{\varpi_2}(\lambda) = 1$ on $\breve{K}$)

$$\begin{aligned} \phi_{\varpi_1}(\lambda)(\theta^{-1}(\beta_n)) = [\lambda^{-1}]_f(\theta^{-1}(\beta_n)) = \theta^{-1} \circ [\lambda^{-1}]_g(\beta_n) \\ = \theta^{-1}(\phi_{\varpi_2}(\lambda)(\beta_n)) = \phi_{\varpi_2}(\lambda)(\theta^{-1}(\beta_n)). \end{aligned}$$

Thus $\phi_{\varpi_1}(\lambda) = \phi_{\varpi_2}(\lambda)$. This concludes the proof. □

Remark 1.5.8. *In fact θ induces an isomorphism of F_f and F_g over $\mathcal{O}_{\breve{K}}$, i.e.*

$$\theta(F_f(X,Y)) = F_g(\theta(X), \theta(Y)). \tag{1.8}$$

We leave it as an exercise.

Proof of Lemma 1.5.7. We use induction to construct $\theta(T)$. We need to find $\theta_1(T) = \varepsilon T$ such that (1.5) (1.6) hold modulo terms of degree ≥ 2. One sees this is equivalent to $\sigma(\varepsilon) = \varepsilon u$. The existence of such $\theta_1(T)$ then follows from the following claim.

Claim: The map $\mathcal{O}_{\breve{K}}^\times \to \mathcal{O}_{\breve{K}}^\times$, $x \mapsto \frac{\sigma(x)}{x}$ is surjective.

We prove the claim. Let τ be the map $x \mapsto \frac{\sigma(x)}{x}$. We have $\mathcal{O}_{\breve{K}}/\varpi \cong \mathcal{O}_{K^{\mathrm{ur}}}/\varpi \cong \overline{k}$. Thus the induced map $(\mathcal{O}_{\breve{K}}/\varpi)^\times \to (\mathcal{O}_{\breve{K}}/\varpi)^\times$ is given by $x \mapsto x^{q-1}$ and is surjective. The map τ induces $\tau_n : (\mathcal{O}_{\breve{K}}/\varpi^n)^\times \to (\mathcal{O}_{\breve{K}}/\varpi^n)^\times$. We use induction to show τ_n is surjective. We have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 + \varpi^{n-1}\mathcal{O}_{\breve{K}}/1 + \varpi^n\mathcal{O}_{\breve{K}} & \longrightarrow & (\mathcal{O}_{\breve{K}}/\varpi^n)^\times & \longrightarrow & (\mathcal{O}_{\breve{K}}/\varpi^{n-1})^\times & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \tau_{n-1}} & & \downarrow{\scriptstyle \tau_n} & & \\ 1 & \longrightarrow & 1 + \varpi^{n-1}\mathcal{O}_{\breve{K}}/1 + \varpi^n\mathcal{O}_{\breve{K}} & \longrightarrow & (\mathcal{O}_{\breve{K}}/\varpi^n)^\times & \longrightarrow & (\mathcal{O}_{\breve{K}}/\varpi^{n-1})^\times & \longrightarrow & 0 \end{array}$$

where the left vertical map is given by $1+\varpi^{n-1}\mathcal{O}_{\breve{K}}/1+\varpi^n\mathcal{O}_{\breve{K}} \cong \overline{k} \xrightarrow{a\mapsto a^q-a} \overline{k} \cong 1+\varpi^{n-1}\mathcal{O}_{\breve{K}}/1+\varpi^n\mathcal{O}_{\breve{K}}$ and is surjective. By induction hypothesis, the right vertical map is also surjective, so is the middle one. We also see the natural projection $(\mathcal{O}_{\breve{K}}/\varpi^n)^\times \twoheadrightarrow (\mathcal{O}_{\breve{K}}/\varpi^{n-1})^\times$ induces a surjective map $\operatorname{Ker}\tau_n \twoheadrightarrow \operatorname{Ker}\tau_{n-1}$. Now for any $x \in \mathcal{O}_{\breve{K}}^\times$, there exists $y_n \in (\mathcal{O}_{\breve{K}}/\varpi^n)^\times$ such that $\tau_n(y_n) = x \pmod{\varpi^n}$. By multiplying a certain element in $\operatorname{Ker}\tau_n$, we can and do assume $y_n \equiv y_{n-1} \pmod{\varpi^{n-1}}$. The elements $\{y_n\}$ then give an element $y \in \mathcal{O}_{\breve{K}}^\times$ such that $\tau(y) = x$. (This also explains why we work with $\breve{K}$ rather than K^{ur}.)

We use induction to show there exists a polynomial θ_r of degree at most r such that

$$\begin{cases}\theta_r \equiv \theta_{r-1} \pmod{T^r} \\ \sigma(\theta_r) \equiv \theta_r \circ [u]_f \pmod{T^{r+1}}\end{cases} \tag{1.9}$$

We have constructed $\theta_1(T) = \varepsilon T$. Suppose we have θ_{r-1} satisfying the properties in (1.9) and we put $\theta_r(T) = \theta_r(T) + a_r T^r$. We have $\sigma(\theta_r)(T) = \sigma(\theta_{r-1})(T) + \sigma(a_r)T^r$, and $\theta_r \circ [u]_f(T) = \theta_{r-1} \circ [u]_f(T) + a_r([u]_f)^r \equiv \theta_{r-1} \circ [u]_f(T) + u^r a_r T$. Let $b \in \mathcal{O}_{\breve{K}}$ such that $\sigma(\theta_{r-1})(T) - \theta_r \circ [u]_f(T) \equiv bT^{r+1} \pmod{T^{r+2}}$. Thus to have the second equation in (1.9), we need $b = u^r a_r - \sigma(a_r)$. Let $\varepsilon' \in \mathcal{O}_{\breve{K}}$ such that $u^r = \varepsilon'/\sigma(\varepsilon')$ (where the existence follows from the claim), then we need

$$b\sigma(\varepsilon') = (\varepsilon' a_r) - \sigma(\varepsilon' a_r). \tag{1.10}$$

By similar arguments as in the proof of the claim, $\sigma - 1 : \mathcal{O}_{\breve{K}} \to \mathcal{O}_{\breve{K}}$ is surjective. The existence of a_r satisfying (1.10) follows.

By taking limit, we see there exists θ such that (1.5) holds. Now we want to modify θ such that (1.6) also holds (noting in the above induction argument, a_r is not unique).

Consider $h := \theta \circ [u]_f \circ f \circ \theta^{-1} \in \mathcal{O}_{\breve{K}}[[T]]$. The we have

$$\begin{aligned}\sigma(h)(T) = \sigma(\theta) \circ [u]_f \circ f \circ \sigma(\theta^{-1})(T) &= \sigma(\theta) \circ f \circ [u]_f \circ \sigma(\theta)^{-1} \\ &= \sigma(\theta) \circ f \circ \theta^{-1}(T) = \theta \circ [u]_f \circ f \circ \theta^{-1}(T) = h(T).\end{aligned} \tag{1.11}$$

Hence $h \in \mathcal{O}_K[[T]]$, we also have $h(T) \equiv \varpi_2 T \pmod{T}^2$. Since $\theta^{-1} = \varepsilon^{-1}T + \cdots$, $f \circ \theta^{-1}(T) \equiv (\theta^{-1})^q(T) \pmod{\varpi_1}$, we see $\sigma(\theta) \circ f \circ \theta^{-1}(T) \equiv \sigma(\sigma) \circ (\theta^{-1})^q \pmod{\varpi_1}$. Using $\sigma(\theta)(T^q) \equiv \theta^q \pmod{\varpi_1}$, we deduce $\sigma(\theta) \circ (\theta^{-1})^q(T) \equiv T^q \pmod{\varpi_1}$. In particular, we deduce $h \in \mathcal{F}_{\varpi_2}$. Replacing θ by $[1]_{g,h} \circ \theta$, one can check both of ((1.5) (1.6) hold. This concludes the proof. □

Chapter 2

Group cohomology

2.1 Group cohomology: abstract formalism

Let G be a finite group, $(M, +)$ be an abelian group eauipped with a (left) action of G:

$$\begin{cases} 1_G(m) = m, \\ g(m_1 + m_2) = g(m_1) + g(m_2), \\ (hg)(m) = h(g(m)), \end{cases}$$

for $m, m_1, m_2 \in M$, $g, h \in G$. We call M a G-module. Denote by $\mathbb{Z}[G]$ the group algebra associated to G, i.e. $\mathbb{Z}[G]$ is a free $\mathbb{Z}$-module with a basis $\{e_g\}_{g \in G}$, and is equipped with a ring structure that is induced by the relation $e_g e_h = e_{gh}$. So we see a (left) G-module is the same as a (left) $\mathbb{Z}[G]$-module.

Let M_1, M_2 be G-modules. A map $f : M_1 \to M_2$ is called a morphism of G-modules if f is a group homomorphism satisfying $f(g(m)) = g(f(m))$ for all $m \in M_1$ and $g \in G$. In other words, f is a morphism of $\mathbb{Z}[G]$-modules. We denote by $\mathcal{M}\mathrm{od}_G$ the category of left G-modules.

Example 2.1.1. *(1) Let $G = \{1\}$, then $\mathcal{M}\mathrm{od}_G$ is the same as the category of abelian groups.*

(2) A G-module M is called a trivial G-module if for any $g \in G$ and $m \in M$, $g(m) = m$.

(3) Let L/K be a finite Galois extension of fields. Then $(L, +)$, $(L, \times)$ are both $\mathrm{Gal}(L/K)$-modules

A G-module I is called injective (resp. projective) if for any injective (resp. surjective) morphism $M_1 \to M_2$ in $\mathcal{M}\mathrm{od}_G$, the induced map $\mathrm{Hom}_G(M_2, I) \to \mathrm{Hom}_G(M_1, I)$ (resp. $\mathrm{Hom}_G(P, M_1) \to \mathrm{Hom}_G(P, M_2)$) is surjective. Equivalently, the functor $\mathcal{M}\mathrm{od}_G \to \{Sets\}$, $M \to \mathrm{Hom}_G(M, I)$ (resp. $M \to \mathrm{Hom}_G(P, M)$) is exact.

Example 2.1.2. *Let $G = \{1\}$, then $\mathbb{Q}/\mathbb{Z}$ is an injective G-module (that is an injective object in the category of abelian groups). In fact, let $M \hookrightarrow N$, and $f : M \to \mathbb{Q}/\mathbb{Z}$. Let S be the set consisting of $(M', f_{M'})$ where $M' \supset M$ is a submodule of N, and $f_{M'} : M \to \mathbb{Q}/\mathbb{Z}$*

is a morphism such that $f_{M'}|_M = f$. The set S has an obvious partial order. By Zorn's lemma, there exists a maximal element $(N', f_{N'})$. Suppose $N' \neq N$, and let $\beta \in N \backslash N'$. The set $\{r \in \mathbb{Z} \mid r\beta \in N'\}$ is an ideal of $\mathbb{Z}$ and is equal to (a) for $a \in \mathbb{Z}_{\geq 0}$. Let $N'' = N' + \mathbb{Z}\beta$. If $a = 0$, then $N' \oplus \mathbb{Z}\beta \hookrightarrow N$, and it is easy to see one can extend $f_{N'}$ to $N'' \cong N' \oplus \mathbb{Z}\beta$ (by sending β to any element in $\mathbb{Q}/\mathbb{Z}$). If $a > 0$, we extend $f_{N'}$ to N" by sending β to $\frac{1}{a} f_{N'}(a\beta)$. The both cases contradict that N' is maximal.

We leave the following lemma as an exercise:

Lemma 2.1.3. *An abelian group Λ is injective if and only if Λ is divisible, i.e. $n : \Lambda \to \Lambda$ is surjective for any $n \in \mathbb{Z}_{>0}$.*

The following proposition will be proved later.

Proposition 2.1.4. *The category $\mathcal{M}\mathrm{od}_G$ has enough injective objects, i.e. for any $M \in \mathcal{M}\mathrm{od}_G$, there exists an injective object I such that $M \hookrightarrow I$.*

Example 2.1.5. *Suppose $G = \{1\}$, for any abelian group M, let F be a free abelian group such that $F \twoheadrightarrow M$, and let N be the kernel of the projection. Then we have*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N & \longrightarrow & F \otimes_{\mathbb{Z}} \mathbb{Q} & \longrightarrow & (F \otimes_{\mathbb{Z}} \mathbb{Q})/N & \longrightarrow & 0 \end{array}.$$

We deduce $M \hookrightarrow (F \otimes_{\mathbb{Z}} \mathbb{Q})/N$, where the latter is injective by Lemma 2.1.3. So $\mathcal{M}\mathrm{od}_{\{1\}} = \mathcal{A}\mathrm{b}$ has enough injective objects.

Let $M \in \mathcal{M}\mathrm{od}_G$, an exact sequence

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

(or the associated sequence $I^\bullet(M) := 0 \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} \cdots$) is called an injective resolution of M. By Proposition 2.1.4, any M admits an injective resolution: first pick an injective I^0 such that $M \hookrightarrow I^0$, then pick an injective I^1 such that $I^0/M \hookrightarrow I^1$, then continue the arguments....

Consider the functor $\mathcal{M}\mathrm{od}_G \to \mathcal{A}\mathrm{b}$, $M \mapsto M^G := \{x \in M \mid gx = x,\ \forall g \in G\}$.

Lemma 2.1.6. *The functor is left exact, i.e. given an exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ in $\mathcal{M}\mathrm{od}_G$, then $0 \to M_1^G \to M_2^G \to M_3^G$ is exact.*

Proof. It is clear that $M_1^G \hookrightarrow M_2^G$. Let $x \in M_2^G$, and suppose x is sent to 0 in M_3, by the given exact sequence we see $x \in M_1$. However, we have $M_2^G \cap M_1 = M_1^G$. The lemma follows. □

Apply the functor to an injective resolution $I^\bullet(M)$ of M, we obtain a sequence of abelian groups

$$0 \to (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d_1} \cdots$$

We put $H^i(G, M) := \mathrm{Ker}(d^i)/\,\mathrm{Im}(d^{i-1})$ $(d^{-1} := 0)$, called the i-th cohomology of the G-module M. It is clear that $H^0(G, M) = M^G$.

Lemma 2.1.7. *Let $f : M \to N$ be a morphism of G-modules, $0 \to M \to I^\bullet$ be an exact sequence of G-modules $I^\bullet$, and $J^\bullet$ be an injective resolution of N. Then there exists a commutative diagram (of morphisms in $\mathcal{M}\mathrm{od}_G$):*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & I^0 & \xrightarrow{d^0} & I^1 & \xrightarrow{d^1} & I^2 & \longrightarrow & \cdots \\ & & {\scriptstyle f}\big\downarrow & & {\scriptstyle f^0}\big\downarrow & & {\scriptstyle f^1}\big\downarrow & & {\scriptstyle f^2}\big\downarrow & & \\ 0 & \longrightarrow & N & \longrightarrow & J^0 & \xrightarrow{d^0} & J^1 & \xrightarrow{d^1} & J^2 & \longrightarrow & \cdots \end{array} \quad . \tag{2.1}$$

Proof. We inductively construct f^i. The existence of f^0 follows from the injectivity of J^0. Now suppose the maps $\{f^j\}_{j \le i}$ have been constructed. In particular, we have

$$\begin{array}{ccc} I^i/\,\mathrm{Im}\,d^{i-1} & \overset{d^i}{\hookrightarrow} & I^{i+1} \\ \big\downarrow{\scriptstyle f^i} & & \vdots\,{\scriptstyle f^{i+1}?} \\ J^i/\,\mathrm{Im}\,d^{i-1} & \overset{d^i}{\hookrightarrow} & J^{i+1} \end{array}$$

As J^{i+1} is an injective object, the existence of $f^{i+1} : I^{i+1} \to J^{i+1}$ follows. This concludes the proof. □

One can view the set of the morphisms $\{f^i\}$ as a morphism from the complex $I^\bullet$ to $J^\bullet$. Appyling $(\bullet)^G$ to both of the complexes, it is straightforward to see (2.1) induces $H^i(f) : H^i(G, M) \to H^i(G, N)$.

Lemma 2.1.8. *The maps $H^i(f)$ are independent of the choice of f_i.*

Proof. It suffices to show if $f = 0$, then $H^i(f) = 0$ for any choice of f_i. We claim there exists $g^i : I^{i+1} \to J^i$ such that $f^i = d_J^{i-1} \circ g^{i-1} + g^i \circ d_I^i$ $(g^{-1} = 0)$:

$$\begin{array}{ccccccccc} 0 & \xrightarrow{d_I^{-1}} & I^0 & \xrightarrow{d_I^0} & I^1 & \xrightarrow{d_I^1} & I^2 & \xrightarrow{d_I^2} & \cdots \\ & \swarrow{\scriptstyle 0=g^{-1}} & \big\downarrow{\scriptstyle f^0} & \swarrow{\scriptstyle g^0} & \big\downarrow{\scriptstyle f^1} & \swarrow{\scriptstyle g^1} & \big\downarrow{\scriptstyle f^2} & & \\ 0 & \xrightarrow{d_J^{-1}} & J^0 & \xrightarrow{d_J^0} & J^1 & \xrightarrow{d_I^1} & J^2 & \xrightarrow{d_J^2} & \cdots \end{array}$$

Since $f = 0$, f_0 factors through I^0/M. Then by the injectivity of J^0, we deduce the existence of g^0:

$$\begin{array}{ccc} J^0 & \overset{g^0}{\longleftarrow} & \\ \big\uparrow{\scriptstyle f^0} & \nwarrow & \\ I^0/M & \overset{d_I^0}{\hookrightarrow} & I^1 \end{array} \quad .$$

Suppose $\{g^j\}_{j\leq i-1}$ have been constructed. For $x \in \operatorname{Ker} d_I^i = \operatorname{Im} d_I^{i-1} \subset I^i$, writing $x = d_I^{i-1}(y)$ we have $f^i(x) = d_J^{i-1} \circ f^{i-1}(y) = d_J^{i-1} \circ (d_J^{i-2} \circ g^{i-2} + g^{i-1} \circ d_I^{i-1}) = d_J^{i-1} \circ g^{i-1}(x)$. So $f^i - d_J^{i-1} \circ g^{i-1} = 0$. Using the injectivity of J^i, we have g^{i+1} such that the following diagram commutes:

$$\begin{tikzcd} J^i & \\ I^i/\operatorname{Ker} d_I^i \arrow[u, "f^i - d_J^{i-1}\circ g^{i-1}"] \arrow[r, hook, "d_I^i"] & I^{i+1}. \arrow[ul, "g^{i+1}"'] \end{tikzcd}$$

The claim follows. Applying $(\bullet)^G$, we get

$$\begin{tikzcd} 0 \arrow[r, "d_I^{-1}"] & (I^0)^G \arrow[r, "d_I^0"] \arrow[d, "f^0"] \arrow[dl, "g^{-1}"'] & (I^1)^G \arrow[r, "d_I^1"] \arrow[d, "f^1"] \arrow[dl, "g^0"'] & (I^2)^G \arrow[r, "d_I^2"] \arrow[d, "f^2"] \arrow[dl, "g^1"'] & \cdots \\ 0 \arrow[r, "d_J^{-1}"] & (J^0)^G \arrow[r, "d_J^0"] & (J^1)^G \arrow[r, "d_I^1"] & (J^2)^G \arrow[r, "d_J^2"] & \cdots \end{tikzcd}$$

For $x \in \operatorname{Ker}[d_I^i : (I^i)^G \to (I^{i+1})^G]$, we see $f^i(x) \in \operatorname{Im} d_J^{i-1}$, thus $H^i(f)(x) = 0$. The lemma follows. □

Corollary 2.1.9. *(1) For $M \in \mathcal{M}\mathrm{od}_G$, $H^i(G, M)$ is independent of the choice of the injective resolution $I^\bullet$ of M.*

(2) For a morphism $f : M \to N$ in $\mathcal{M}\mathrm{od}_G$, the induced morphism $H^i(f) : H^i(G, M) \to H^i(G, N)$ is independent of the choice of the injective resolutions of M and N.

Proof. (1) Let $I^\bullet$, $J^\bullet$ be two resolutions of M, let H_I^i and H_J^i be the cohomology group of $(I^\bullet)^G$ and $(J^\bullet)^G$ respectively. The identity map on M induces $\alpha : H_I^i \to H_J^i$ and $\beta : H_J^i \to H_I^i$. By the above lemma, $\alpha \circ \beta = \mathrm{id}$, and $\beta \circ \alpha = \mathrm{id}$. (1) follows.

(2) follows by similar arguments. □

Example 2.1.10. *(1) Suppose M is injective, then $I^0 = M$, $I^i = 0$ for $i < 0$ give an injective resolution of M. We then deduce $H^i(G, M) = 0$ for all $i > 0$.*

(2) Suppose $G = \{1\}$, by definition $(I^\bullet)^G = I^\bullet$, we deduce then $H^i(G, M) = 0$ for all $i > 0$.

Proposition 2.1.11. *A short exact sequence in $\mathcal{M}\mathrm{od}_G$:*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0,$$

naturally induces a long exact sequence

$$0 \to H^0(G, M_1) \xrightarrow{H^0(f)} H^0(G, M_2) \xrightarrow{H^0(g)} H^0(G, M_3)$$
$$\xrightarrow{\delta^0} H^1(G, M_1) \xrightarrow{H^1(f)} H^1(G, M_2) \xrightarrow{H^1(g)} H^1(G, M_3) \xrightarrow{\delta^1} \cdots$$

Proof. Let $I_1^\bullet$ (resp. $I_3^\bullet$) be an injective resolution of M_1 (resp. M_3). Let $I_2^i := I_1^i \oplus I_3^i$. We use $\{I_2^i\}_i$ to construct an injective resolution of M_2 such that the diagram commutes:

$$
\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & {\scriptstyle d_1^i}\uparrow & & {\scriptstyle d_2^i}\uparrow & & {\scriptstyle d_3^i}\uparrow & & \\
0 & \longrightarrow & I_1^i & \longrightarrow & I_1^i \oplus I_3^i & \longrightarrow & I_3^i & \longrightarrow & 0 \\
 & & {\scriptstyle d_1^{i-1}}\uparrow & & {\scriptstyle d_2^{i-1}}\uparrow & & {\scriptstyle d_3^{i-1}}\uparrow & & \\
0 & \longrightarrow & I_1^{i-1} & \longrightarrow & I_1^{i-1} \oplus I_3^{i-1} & \longrightarrow & I_3^{i-1} & \longrightarrow & 0 \\
 & & {\scriptstyle d_1^{i-2}}\uparrow & & {\scriptstyle d_2^{i-2}}\uparrow & & {\scriptstyle d_3^{i-2}}\uparrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & {\scriptstyle d_1^1}\uparrow & & {\scriptstyle d_2^1}\uparrow & & {\scriptstyle d_3^1}\uparrow & & \\
0 & \longrightarrow & I_1^1 & \longrightarrow & I_1^1 \oplus I_3^1 & \longrightarrow & I_3^1 & \longrightarrow & 0 \\
 & & {\scriptstyle d_1^0}\uparrow & & {\scriptstyle d_2^0}\uparrow & & {\scriptstyle d_3^0}\uparrow & & \\
0 & \longrightarrow & I_1^0 & \longrightarrow & I_1^0 \oplus I_3^0 & \longrightarrow & I_3^0 & \longrightarrow & 0 \\
 & & {\scriptstyle h_1}\uparrow & & {\scriptstyle h_2}\uparrow & & {\scriptstyle h_3}\uparrow & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
\tag{2.2}
$$

where the horizontal maps are natural maps. We use induction to construct the maps h_2 and $\{d_2^i\}$ such that the above diagram commutes and that the induced sequences

$$
\begin{gathered}
0 \to \operatorname{Ker} d_1^i \to \operatorname{Ker} d_2^i \to \operatorname{Ker} d_3^i \to 0 \\
0 \to \operatorname{Coker} d_1^i \to \operatorname{Coker} d_2^i \to \operatorname{Coker} d_3^i \to 0
\end{gathered}
$$

are exact (also for h_j).

First, since I_1^0 is injective, there exists a morphism $h_1' : M_2 \to I_1^0$ whose composition with f is equal to the morphism $M_1 \hookrightarrow I_1^0$. Let h_3' be the natural composition $M_2 \to M_3 \to I_3^0$, we then obtain a morphism $h_2 = (h_1', h_3') : M_2 \to I_2^0$. One easily checks that this morphism is injective. By snake lemma, we have

$$0 \to \operatorname{Coker} h_1 \to \operatorname{Coker} h_2 \to \operatorname{Coker} h_3 \to 0.$$

Suppose $\{d_2^j\}_{j \leq i}$ have been constructed. We need to construct d_2^{i+1} such that the following diagram commutes

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & I_1^{i+2} & \longrightarrow & I_1^{i+2} \oplus I_3^{i+2} & \longrightarrow & I_3^{i+2} & \longrightarrow & 0 \\
 & & {\scriptstyle d_1^{i+1}}\uparrow & & {\scriptstyle d_2^{i+1}?}\uparrow & & {\scriptstyle d_3^{i+1}}\uparrow & & \\
0 & \longrightarrow & \operatorname{Coker} d_1^i & \longrightarrow & \operatorname{Coker} d_2^i & \longrightarrow & \operatorname{Coker} d_3^i & \longrightarrow & 0
\end{array}
$$

However, by similar arguments as for h_2, the existence of d_2^{i+1} follows. there exists a morphism d_2^{i+1}. By snake lemma,

$$0 \to \operatorname{Coker} d_1^{i+1} \to \operatorname{Coker} d_2^{i+1} \to \operatorname{Coker} d_3^{i+1} \to 0.$$

We write $0 \to I_1 \bullet \to I_2^\bullet \to I_3^\bullet \; ra0$ to denote (2.2). Applying the functor $(\bullet)^G$, we obtain $0 \to (I_1^\bullet)^G \to (I_2^\bullet)^G \to (I_3^\bullet)^G \to 0$ that is exact, i.e. all the horizontal sequences $0 \to (I_1^i)^G \to (I_2^i)^G \to (I_3^i)^G \to 0$ are exact. The commuative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (I_1^{i+1})^G & \longrightarrow & (I_2^{i+1})^G & \longrightarrow & (I_3^{i+1})^G & \longrightarrow & 0 \\
 & & {\scriptstyle d_1^i}\big\uparrow & & {\scriptstyle d_2^i}\big\uparrow & & {\scriptstyle d_3^i}\big\uparrow & & \\
0 & \longrightarrow & (I_1^i)^G & \longrightarrow & (I_2^i)^G & \longrightarrow & (I_3^i)^G & \longrightarrow & 0
\end{array}$$

induces by snake lemma

$$0 \to \operatorname{Ker} d_1^i \to \operatorname{Ker} d_2^i \to \operatorname{Ker} d_3^i \to \operatorname{Coker} d_1^i \to \operatorname{Coker} d_2^i \to \operatorname{Coker} d_3^i \to 0.$$

Finally the commutative diagram

$$\begin{array}{ccccccccc}
 & & \operatorname{Coker} d_1^i & \longrightarrow & \operatorname{Coker} d_2^i & \longrightarrow & \operatorname{Coker} d_3^i & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\
0 & \longrightarrow & \operatorname{Ker} d_1^{i+1} & \longrightarrow & \operatorname{Ker} d_2^{i+1} & \longrightarrow & \operatorname{Ker} d_3^{i+1} & &
\end{array}$$

induces by snake lemma an exact sequence

$$H^i(G, M_1) \to H^i(G, M_2) \to H^i(G, M_3) \to H^{i+1}(G, M_1) \to H^{i+1}(G, M_2) \to H^{i+1}(G, M_3).$$

This concludes the proof. □

A G-module M is called acyclic if $H^i(G, M) = 0$ for all $i > 0$. By Example 2.1.10, any injective G-module is acyclic and if $G = \{1\}$, then any G-module is acyclic.

Proposition 2.1.12. *Let $I^\bullet$ be an acyclic resolution of M, i.e. there is an exact sequence $0 \to M \to I^0 \to I^1 \cdots$ with I^i all acyclic. Then $H^i((I^\bullet)^G) \cong H^i(G, M)$ for all i.*

Proof. Let $M_0 := M$, and we inductively construct $M_i := I^{i-1}/M_{i-1} \hookrightarrow I^i$. We have thus an exact sequence $0 \to M_i \to I^i \to M_{i+1} \to 0$, that induces $0 \to H^0(G, M_i) \to H^0(G, I^i) \to H^0(G, M_{i+1}) \to H^1(G, M_i) \to 0$ and $H^j(G, M_{i+1}) \xrightarrow{\sim} H^{j+1}(G, M_i)$ for $j \geq 1$. By definition, $H^0(G, M_{i+1}) = \operatorname{Ker}[d^{i+1} : I^{i+1} \to I^{i+2}]$ and hence $H^1(G, M_i) \cong H^{i+1}((I^\bullet)^G)$. We then deduce $H^i(G, M) \cong H^i(G, M_0) \cong H^{i-1}(G, M_1) \cong \cdots \cong H^1(G, M_{i-1}) \cong H^i((I^\bullet)^G)$. □

Remark 2.1.13. *Let $I^\bullet$ be an acyclic resolution of M, and $J^\bullet$ be an injective resolution of M. By Lemma 2.1.7, the identity map on M induces a morphism of complexes of G-modules: $I^\bullet \to J^\bullet$. By an induction argument as in the above proof, one can show that the morphism $I^\bullet \to J^\bullet$ induces an isomorphism $H^i((I^\bullet)^G) \cong H^i((J^\bullet)^G)$ for $i \geq 0$.*

2.2 Change of groups

Let $H \subset G$ be a subgroup. Note that a G-module is naturally an H-module by restriction. The injection $H \hookrightarrow$ induces an injection of $\mathbb{Z}$-algebra $\mathbb{Z}[H] \hookrightarrow \mathbb{Z}[G]$. For $M \in \mathcal{M}\mathrm{od}(H)$, $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ is a left $\mathbb{Z}[G]$-module (where $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ is the quotient of $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ modulo the $\mathbb{Z}[G]$-submodule generated by $e_g e_h \otimes m - e_g \otimes hm$). There is a natural morphism of $\mathbb{Z}[H]$-modules: $\iota : M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$, $m \mapsto 1 \otimes m$.

Lemma 2.2.1. *$\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module, and consequently, the functor $\mathcal{M}\mathrm{od}_H \to \mathcal{M}\mathrm{od}_G$, $M \mapsto \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ is exact.*

Proof. Let R be a set of representatives of the right cosets H in G, then $\mathbb{Z}_G \cong \oplus_{g \in R} \mathbb{Z}[H] e_g$. □

For $M \in \mathcal{M}\mathrm{od}_H$, we put $\mathrm{Ind}_H^G M := \{f : G \to M \mid f(hg) = h(f(g)),\ \forall h \in H\}$. We equip $\mathrm{Ind}_H^G M$ a left G-action by $(gf)(g') = f(g'g)$ hence $\mathrm{Ind}_H^G M \in \mathcal{M}\mathrm{od}_H$. There is a natural morphism of $\mathbb{Z}[H]$-modules: $\jmath : \mathrm{Ind}_H^G M \to M$, $f \mapsto f(1)$.

Lemma 2.2.2. *(1) There is a natural isomorphism $M^H \xrightarrow{\sim} (\mathrm{Ind}_H^G M)^H$.*

(2) (Frobenius reciprocity) Let $M \in \mathcal{M}\mathrm{od}_G$, $N \in \mathcal{M}\mathrm{od}_H$, then there are natural bijections:

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G N) \xrightarrow{\sim} \mathrm{Hom}_H(M, N)$$
$$\mathrm{Hom}_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N, M) \xrightarrow{\sim} \mathrm{Hom}_H(N, M).$$

Proof. (1) We have a natural map $M^H \hookrightarrow \mathrm{Ind}_H^G M$, $m \mapsto [g \mapsto m]$. It is clear the image is contained in $(\mathrm{Ind}_H^G M)^G$. Let $f \in (\mathrm{Ind}_H^G M)^G$, we deduce $f(g) = (gf)(1) = f(1) =: m \in M$ for all $g \in G$. Since $f(h) = hf(1) = hm = m$, we deduce $m \in M^H$. (1) follows.

(2) We have a natural map

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G N) \to \mathrm{Hom}_H(M, N),\ \ F \mapsto \jmath \circ F. \tag{2.3}$$

One can check the following map is well-defined and gives an inverse of (2.3): $\mathrm{Hom}_H(M, N) \to \mathrm{Hom}_G(M, \mathrm{Ind}_H^G N)$, $F \mapsto [m \mapsto [g \mapsto F(gm)]]$. Similarly, we have the following pair of maps, that are inverse to each other,

$$\mathrm{Hom}_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N, M) \to \mathrm{Hom}_H(N, M), F \mapsto F \circ \iota,$$

$$\mathrm{Hom}_H(N, M) \to \mathrm{Hom}_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N, M), F \to [e_g \otimes m \mapsto gF(M)].$$

(2) follows. □

Lemma 2.2.3. *We have $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \cong \mathrm{Ind}_H^G M$, in particular, we have*

$$\begin{aligned} \mathrm{Hom}_H(N, M) &\cong \mathrm{Hom}_G(\mathrm{Ind}_H^G N, M), \\ \mathrm{Hom}_G(M, \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N) &\cong \mathrm{Hom}_H(M, N), \end{aligned}$$

for $N \in \mathcal{M}\mathrm{od}_H$ and $M \in \mathcal{M}\mathrm{od}_G$.

Proof. For $e_g \otimes m \in \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$, consider the induced map

$$G \to M,\ g' \mapsto \begin{cases} g'gm & g'g \in H \\ 0 & \text{otherwise} \end{cases}.$$

One can check the map lies in $\operatorname{Ind}_H^G M$. One can also check this construction induces a morphism of G-modules $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \to \operatorname{Ind}_H^G M$. The map admits an inverse given by

$$\operatorname{Ind}_H^G M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M, f \mapsto \sum_{g \in R} e_g \otimes f(g^{-1}),$$

where R denotes a set of representatives of left cosets of H in G (note the term on the right hand side does not depend on the choice of R. The lemma follows. □

Remark 2.2.4. *Let* $(\operatorname{Ind}_H^G M)' := \{f : G \to M \mid f(gh^{-1}) = hf(g)\}$*, and we equip* $(\operatorname{Ind}_H^G M)'$ *with a left* G*-action given by* $(gf)(g') = f(g^{-1}g')$*. One can easily check that*

$$\operatorname{Ind}_H^G M \to (\operatorname{Ind}_H^G M)',\ f \mapsto [g \mapsto f(g^{-1})$$

is an isomorphism of G*-modules.*

Proposition 2.2.5. *If* $M \in \mathcal{M}\mathrm{od}_H$ *is injective, then* $\operatorname{Ind}_H^G M$ *(hence* $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$*) is injective in* $\mathcal{M}\mathrm{od}_G$*.*

Proof. Let $M_1 \hookrightarrow M_2$ be an injection in $\mathcal{M}\mathrm{od}_G$, and I_H be an injective H-module. Then we have

$$\begin{array}{ccc} \operatorname{Hom}_G(M_2, \operatorname{Ind}_H^G I_H) & \longrightarrow & \operatorname{Hom}_G(M_1, \operatorname{Ind}_H^G I_H) \\ \downarrow \sim & & \downarrow \sim \\ \operatorname{Hom}_H(M_2, I_H) & \twoheadrightarrow & \operatorname{Hom}_H(M_1, H) \end{array}$$

hence the top map is surjective. The proposition follows. □

Corollary 2.2.6. *The category* $\mathcal{M}\mathrm{od}_G$ *has enough injective objects.*

Proof. Let $M \in \mathcal{M}\mathrm{od}_G$. Forgetting the G-action, we view M as an object in $\mathcal{A}\mathrm{b} = \mathcal{M}\mathrm{od}_{\{1\}}$. Let $I \in \mathcal{A}\mathrm{b}$ be an injective object such that $f : M \hookrightarrow I$ (in $\mathcal{A}\mathrm{b}$). By Frobenius reciprocity, this map induces a morphism of G-modules: $M \to \operatorname{Ind}_{\{1\}}^G I$ ($m \mapsto [g \mapsto f(gm)]$), that one can check is injective (using f is injective). Since $\operatorname{Ind}_{\{1\}}^G I$ is injective in $\mathcal{M}\mathrm{od}_G$, the corollary follows. □

Corollary 2.2.7 (Shapiro's lemma)**.** *Let* $H \subset G$ *and* $N \in \mathcal{M}\mathrm{od}_H$*. There is a canonical isomorphism*

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

Proof. Let $0 \to N \to I^\bullet$ be an injective resolution of N in $\mathcal{M}\mathrm{od}_H$. Then by Proposition 2.2.5 and the fact $\operatorname{Ind}_H^G -$ is exact, we see $0 \to \operatorname{Ind}_H^G N \to (\operatorname{Ind}_N^G I^\bullet)$ is an injective resolution of $\operatorname{Ind}_H^G N$ in $\mathcal{M}\mathrm{od}_G$. We deduce $H^i(H, N) \cong H^i((I^\bullet)^H) \cong H^i((\operatorname{Ind}_H^G I^\bullet)^G) \cong H^i(G, N)$. □

As an immediate consequence of Shapiro's lemma, we have

Corollary 2.2.8. *Let $H \subset G$ and $N \in \mathcal{M}\mathrm{od}_H$. If N is acyclic for $(-)^H$, then $\operatorname{Ind}_H^G N$ is acyclic for $(-)^G$. In particular, for any abelian group M, $\operatorname{Ind}_{\{1\}}^G M$ is acyclic (for $(-)^G$).*

Corollary 2.2.9. *Let $M \in \mathcal{M}\mathrm{od}_G$. If M is a finitely generated abelian group, then $H^i(G, M)$ is a finitely generated abelian group.*

Proof. We have an injection $M \hookrightarrow \operatorname{Ind}_{\{1\}}^G M$. As M is finitely generated, we see $\operatorname{Ind}_{\{1\}}^G M$ is also finitely generated. We then deduce that M admits an acyclic resolution $I^\bullet$ consisting of G-modules that are finitely generated as abelian groups. Hence $H^i(G, M) \cong H^i((I^\bullet)^G)$ is a finitely generated abelian group. □

Corollary 2.2.10. *Let L/K be a finite Galois extension. Then $H^i(\mathrm{Gal}(L/K), L) = 0$, for all $i > 0$.*

Proof. By the normal basis theorem, there exists $\alpha \in L$ such that $\{g(\alpha)\}_{g\in \mathrm{Gal}(L/K)}$ form a basis of L over K. We see as $\mathrm{Gal}(L/K)$-module, $\mathbb{Z}[\mathrm{Gal}(L/K)] \otimes_Z K \xrightarrow{sim}$ Ł $\oplus_{g\in\mathrm{Gal}(L/K)} Kg(\alpha) = L$, $e_g \otimes a \mapsto ag(\alpha)$. Hence $H^i(\mathrm{Gal}(L/K), L) \cong H^i(\{1\}, K)$, and the corollary follows. □

Corollary 2.2.11. *Let $H \subset G$, $M \in \mathcal{M}\mathrm{od}_G$. There are natural morphisms* $\mathrm{Res} : H^i(G, M) \to H^i(H, M)$ *(called restrictions) and* $\mathrm{Cor} : H^i(H, M) \to H^i(G, M)$ *(called corestrictions). Moreover,* $\mathrm{Cor} \circ \mathrm{Res} = [G : H]$.

Proof. By Frobeinus reciprocty, we have a natural G-equivariant morphism $\iota : M \to \operatorname{Ind}_H^G M$, $m \mapsto [g \mapsto gm]$, that induces $\mathrm{Res} : H^i(G, M) \to H^i(G, \operatorname{Ind}_H^G M) \cong H^i(H, M)$. Similarly, by Frobenius reciprocity, we also have a G-equivariant morphism $\kappa : \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \cong \operatorname{Ind}_H^G M \to M$, $g \otimes m \mapsto gm$, that induces $\mathrm{Cor} : H^i(H, M) \cong H^i(G, \operatorname{Ind}_H^G M) \to H^i(G, M)$.

One checks $\kappa \circ \iota : M \to M$, $m \mapsto [G : H]m$, hence $\mathrm{Cor} \circ \mathrm{Res} = [G : H]$ (since the both are induced from $\kappa \circ \iota = [G : H]$, hence are equal by Corollary 2.1.9 (2)). □

Corollary 2.2.12. *Let M be a finite G-module, if $(|M|, |G|) = 1$, then $H^i(G, M) = 0$ for all $i > 0$.*

Proof. As $(|M|, |G|) = 1$, multiplying $|G|$ is an isomorphism on M hence is an isomorphism on $H^i(G, M)$ for all i. Applying the above corollary to $H = \{1\}$, $\mathrm{Cor} \circ \mathrm{Res} = |G| : H^i(G, M) \to H^i(G, M)$. However, we have $H^i(\{1\}, M) = 0$ for all $i > 0$, hence $\mathrm{Cor} \circ \mathrm{Res} = 0$ on $H^i(G, M)$ when $i > 0$. As $|G|$ is an isomorphism $H^i(G, M)$, we deduce $H^i(G, M) = 0$ for all $i > 0$. □

The restrictions are actually special cases of the following functorial property of the group cohomology. Let G_1, G_2 be two finite groups, and $\alpha : G_1 \to G_2$ be a morphism. The morphism α naturally induces a functor $\mathcal{M}\mathrm{od}_{G_2} \to \mathcal{M}\mathrm{od}_{G_1}$: for each $M \in \mathcal{M}\mathrm{od}_{G_2}$, we equip M with a G_1-action via α.

Proposition 2.2.13. *Let $M_1 \in \mathcal{M}\mathrm{od}_{G_1}$, and $M_2 \in \mathcal{M}\mathrm{od}_{G_2}$. Let $f : M_2 \to M_1$ be a morphism in $\mathcal{M}\mathrm{od}_{G_1}$. Then f induces natural morphisms*

$$H^i(G_2, M_2) \to H^i(G_1, M_1), \ \forall i \geq 0. \tag{2.4}$$

Proof. First for any $N \in \mathcal{M}\mathrm{od}_{G_2}$, as the G_1-action on N factors through G_2, there is a natural injection

$$N^{G_2} \longrightarrow N^{G_1}.$$

Let $I^\bullet_{G_2}$ be an injective resolution of M_2 in $\mathcal{M}\mathrm{od}_{G_2}$. Let $I^\bullet_{G_1}$ be an injective resolution of M_2 in $\mathcal{M}\mathrm{od}_{G_1}$. As the sequence $0 \to M_2 \to I^\bullet_{G_2}$ is also G_1-equivariant , by the same argument as in Lemma 2.1.7 (using $I^i_{G_1}$ are injective in $\mathcal{M}\mathrm{od}_{G_1}$), there is a morphism $\alpha : I^\bullet_{G_2} \to I^\bullet_{G_1}$ in the category of complexes of G_1-modules. Applying $(-)^{G_1}$, we get $(I^\bullet_{G_2})^{G_1} \to (I^\bullet_{G_1})^{G_1}$. By the above discussion, we have another morphism $(I^\bullet_{G_2})^{G_2} \to (I^\bullet_{G_2})^{G_1}$. The composition $(I^\bullet_{G_2})^{G_2} \to (I^\bullet_{G_1})^{G_1}$ then induces $H^i(G_2, M_2) \to H^i(G_1, M_2)$. The morphism f induces $H^i(G_1, M_2) \to H^i(G_1, M_1)$. By taking composition, the lemma follows. □

Remark 2.2.14. *(1) By Corollary 2.1.9 (and the proof), one can show the maps $H^i(G_2, M_2) \to H^i(G_1, M_2)$ are independent of choices of injection resolutions of M (in either $\mathcal{M}\mathrm{od}_{G_1}$ or $\mathcal{M}\mathrm{od}_{G_2}$).*

(2) Taking $G_2 = G$, $G_1 = H \hookrightarrow G$, and $M \in \mathcal{M}\mathrm{od}_G$, the proposition can recover (check it!) the restriction maps $\mathrm{Res} : H^i(G, M) \to H^i(H, M)$.

Let H be a normal subgroup of G, and $M \in \mathcal{M}\mathrm{od}_G$. Then M^H inherits a natural G/H-action. Applying the proposition to the case $G_1 = G$, $G_2 = G/H$, $M_2 = M^H$ and $M_1 = M$, we deduce natural morphisms $\inf : H^i(G/H, M^H) \to H^i(G, M)$ called inflations.

Proposition 2.2.15 (Inflation-Restriction)**.** *The following sequence is exact*

$$0 \to H^1(G/H, M^H) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M). \tag{2.5}$$

Suppose if $H^l(H, M) = 0$ for $1 \leq l \leq i-1$, then the following sequence is exact

$$0 \to H^i(G/H, M^H) \xrightarrow{\inf} H^i(G, M) \xrightarrow{\mathrm{Res}} H^i(H, M). \tag{2.6}$$

Proof. One can use cochains to directly prove (2.5) (that we will leave as an exercise for the next section). Assume now (2.5) holds. Recall we have a natural G-equivariant injection $M \to \mathrm{Ind}^G_{\{1\}} M$, $m \mapsto [g \mapsto gm]$, and let $N := \mathrm{Ind}^G_{\{1\}} M/M$ so that we have an exact sequence in $\mathcal{M}\mathrm{od}_G$:

$$0 \to M \to \mathrm{Ind}^G_{\{1\}} M \to N \to 0. \tag{2.7}$$

We have hence $H^l(G, N) \cong H^{l+1}(G, N)$ for $l \geq 1$. For $H' \leq G$, $\mathrm{Ind}^G_{\{1\}} M \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \cong \mathbb{Z}[H'] \otimes_{\mathbb{Z}} (\oplus_{H'g \in H' \backslash G} e_g M)$, hence is an induced module for H'. As $H^1(H, M) = 0$, we deduce from (2.7) $H^l(H, N) \cong H^{l+1}(H, N)$ for $l \geq 1$ and an exact sequence (of G/H-modules)

$$0 \to M^H \to (\mathrm{Ind}^G_{\{1\}} M)^H \to N^H \to 0. \tag{2.8}$$

Now we use induction on i: suppose the proposition holds for $k \leq i-1$, and suppose now $H^l(G, M) = 0$ for $1 \leq l \leq i-1$. By the above discussion, $H^l(G, N) = 0$ for $1 \leq l \leq i-2$ so we can apply the induction hypothesis to N and obtain an exact sequence as in (2.6) with M replaced by N and i replaced by $i-1$. Since $(\operatorname{Ind}_{\{1\}}^G M)^H \cong \mathbb{Z}[G/H] \otimes \mathbb{Z}M$, we deduce from (2.8) $H^l(G/H, N^H) \cong H^{l+1}(G, M^H)$ for $l \geq 1$. We finally obtain the following commutative diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & H^{i-1}(G/H, N^H) & \xrightarrow{\text{inf}} & H^{i-1}(G, N) & \xrightarrow{\text{Res}} & H^{i-1}(H, N) & \\ & \sim\downarrow & & \sim\downarrow & & \sim\downarrow & . \\ & H^i(G/H, M^H) & \xrightarrow{\text{inf}} & H^i(G, M) & \xrightarrow{\text{Res}} & H^i(H, N) & \end{array}$$

The proposition follows. ☐

Remark 2.2.16. *The proposition is a special case of the so-called Hochschild-Serre spectral sequences (concerning about the composition of the functors* $(-)^G = ((-)^H)^{G/H}$.

2.3 Group cohomology via cochains

We use Corollary 2.2.8 to construct an explicit acyclic resolution of a G-module M so that we can calculate $H^i(G, M)$ in an explicit way. We put

$$N^i := \{\phi : G^{i+1} := \underbrace{G \times \cdots \times G}_{i+1} \to M\}$$

and we equip N^i with a (left) G-action by

$$(g\phi)(g_0, \cdots, g_i) = g(\phi(g^{-1}g_0, \cdots, g^{-1}g_i)).$$

We put $N_0^i := \{\phi : G^i \to M\}$.

Lemma 2.3.1. *We have* $N^i \cong \operatorname{Ind}_{\{1\}}^G N_0^i$ *as* G*-module.*

Proof. Recall $\operatorname{Ind}_{\{1\}}^G N_0^i$ is isomorphic to $\{f : G \to N_0^i\}$ with the G-action given by $(gf)(g') := f(g^{-1}g')$. Consider the map

$$\{f : G \to N_0^i\} \longrightarrow N^i, \; f \mapsto \big[(g_0, \cdots, g_i) \mapsto g_0\big(f(g_0)(g_0^{-1}g_1, \cdots, g_0^{-1}g_i)\big)\big].$$

It is straightforward to check this map is G-equivariant. This map is clearly bijective with the inverse given by $\phi \mapsto [g \mapsto [(g_1, \cdots, g_i) \mapsto g^{-1}\phi(g, gg_1, \cdots, gg_i)]]$. The lemma follows. ☐

Put

$$d_1^i : N^i \to N^{i+1}, \; \phi \mapsto \big[(g_0, \cdots, g_{i+1}) \mapsto \sum_{j=0}^{i+1}(-1)^j \phi(g_0, \cdots, \hat{g}_j, \cdots, g_{i+1})\big]$$

where $\hat{g}_j$ means omitting the term g_j. One can check the morphism is G-equivariant. There is also a natural morphism $\iota : M \hookrightarrow N^0$, $m \mapsto [g \mapsto m]$. One can directly verify the following lemma (for example, if $d_1^i(\phi) = 0$, then $\phi(g_0, \cdots, g_i) = (-1)^i \sum_{j=0}^i \phi(g_0, \cdots, \hat{g}_j, \cdots, g_i, 1) = d_1^{-1}(\psi) \in \operatorname{Im} d_1^{i-1}$ with $\psi(g_0, \cdots, g_{i-1}) := \phi(g_0, \cdots, g_{i-1}, 1)$).

Lemma 2.3.2. *We have an exact sequence of G-modules*

$$0 \to M \xrightarrow{\iota} N^0 \xrightarrow{d_1^0} N^1 \to \cdots N^i \xrightarrow{d_1^i} N^{i+1} \to \cdots \tag{2.9}$$

Together with Lemma 2.3.1, we see (2.9) gives an acyclic resolution of M. Now we apply the functor $(-)^G$ to the resolution. We have $C^i(G, M) := \{G^i \to M\} \xrightarrow[\sim]{\jmath_i} (N^i)^G$, $\phi \mapsto [(g_0, \cdots, g_i) \mapsto g_0(\phi(g_0^{-1}g_1, g_1^{-1}g_2, \cdots, g_{i-1}^{-1}g_i))]$ with the inverse given by

$$\Phi \mapsto [(g_1, \cdots, g_i) \mapsto \Phi(1, g_1, g_1g_2, \cdots, g_1 \cdots g_i)].$$

One can check the composition $d^i : C^i(G, M) \xrightarrow{\jmath_i} (N^i)^G \xrightarrow{d_1^i} (N^{i+1})^G \xrightarrow{\jmath_{i+1}^{-1}} C^{i+1}(G, M)$ is given by

$$\phi_i \mapsto \Big[(g_1, \cdots, g_{i+1}) \mapsto g_1\phi_i(g_2, \cdots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j \phi_i(g_1, \cdots, g_jg_{j+1}, \cdots, g_{i+1}) + (-1)^{i+1}\phi_i(g_1, \cdots, g_i)\Big]. \tag{2.10}$$

Put $B^i(G, M) := \operatorname{Im} d^{i-1} \subset C^i(G, M)$ called the set of i-th coboundaries, and

$$Z^i(G, M) := \operatorname{Ker} d^i = \Big\{\phi \in C^i(G, M) \mid \forall (g_1, \cdots, g_{i+1}) \in G^{i+1}, \\ g_1\phi_i(g_2, \cdots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j \phi_i(g_1, \cdots, g_jg_{j+1}, \cdots, g_{i+1}) + (-1)^{i+1}\phi_i(g_1, \cdots, g_i) = 0\Big\},$$

called the set of i-th cocycles. Then

$$H^i(G, M) \cong Z^i(G, M)/B^i(G, M).$$

Example 2.3.3. *We have*

$$H^1(G, M) \cong \frac{\{f : G \to M \mid f(g_1g_2) = g_1f(g_2) + f(g_1)\}}{\{f : G \to M \mid f(g) = g(m) - m\}}.$$

If G acts trivially on M, then $Z^1(G, M) = \operatorname{Hom}(G, M)$ (Hom denotes group homomorphisms), and $B^1(G, M) = 0$. We see in this case $H^1(G, M) = \operatorname{Hom}(G, M) = \operatorname{Hom}(G^{\mathrm{ab}}, M)$.

For $\alpha : G_1 \to G_2$, $M_i \in \mathcal{M}\mathrm{od}_{G_i}$. Let $N_i^\bullet$ be the acyclic resolution of M_i in $\mathcal{M}\mathrm{od}_{G_i}$ as in (2.9). Given a morphism $f : M_2 \to M_1$ in $\mathcal{M}\mathrm{od}_{G_1}$, f induces G_1-equivariant maps

$N_2^i \to N_1^i$, $\phi \mapsto [(g_0, \cdots, g_i) \mapsto f(\phi(\alpha(g_0), \cdots, \alpha(g_i)))]$ for all i. These maps form a G_1-equivariant morphism $N_2^\bullet \to N_1^\bullet$. We have thus $(N_2^\bullet)^{G_2} \to (N_2^\bullet)^{G_1} \to (N_1^\bullet)^{G_1}$, that induces for $i \geq 0$:

$$H^i(G_2, M_2) \to H^i(G_1, M_1),\ \phi \mapsto [(g_1, \cdots, g_i) \mapsto f(\phi(\alpha(g_1), \cdots, \alpha(g_i)))]. \tag{2.11}$$

We remark that these (explicit) maps coincide with those given in Proposition 2.2.13. Indeed, let $I_i^\bullet$ be an injective resolution of M_i in $\mathcal{M}\mathrm{od}_{G_i}$. By Lemma 2.1.7, we can obtain a morphism of complexes in $\mathcal{M}\mathrm{od}_{G_i}$: $N_i^\bullet \to I_i^\bullet$ (extending identity map on M_i). Again by similar arguments, there exists a G_1-equivariant morphism $I_2^\bullet \to I_1^\bullet$ such that the following diagram commutes

$$\begin{array}{ccc} N_2^\bullet & \longrightarrow & I_2^\bullet \\ \downarrow & & \downarrow \\ N_1^\bullet & \longrightarrow & I_1^\bullet \end{array}$$

where the left vertical map is given by previous discussions (induced by f). Applying $(-)^{G_i}$ and taking cohomology, we then deduce (2.11) coincides with (2.4).

Proposition 2.3.4 (Hilbert's theorem 90)**.** *Let L/K be a finite Galois extension, then $H^1(\mathrm{Gal}(L/K), L^\times) = \{1\}$.*

Proof. Let $c : \mathrm{Gal}(L/K) \to L^\times$ be a cocycle, i.e. $c(g_1g_2) = g_1(c(g_2))/c(g_1)$. For $x \in L$, consider $a_x := \sum_{g\in\mathrm{Gal}(L/K)} c(g)g(x)$. Then

$$h(a_x) = \sum_{g\in\mathrm{Gal}(L/K)} h(c(g))(hg)(x) = c(h) \sum_{g\in\mathrm{Gal}(L/K)} c(hg)(hg)(x) = c(h)a_x.$$

If $a_x \neq 0$, then $c(h) = h(a_x)/a_x \in B^1(\mathrm{Gal}(L/K), L^\times)$ and the proposition will follow. The existence of non-zero a_x follows from the following claim (called Dedekind's linear independence of automorphisms):

claim: Let $a_g \in L$ for $g \in \mathrm{Gal}(L/K)$, if

$$\sum_{g\in\mathrm{Gal}(L/K)} a_g g(x) = 0,\ \forall x \in L, \tag{2.12}$$

then $a_g = 0$ for all $g \in \mathrm{Gal}(L/K)$.

Suppose there exist non-zero $\{a_g\}$ such that (2.12) holds. We can and do take one such that $S = \{g\ |a_g \neq 0\}$ has minimal elements. It is easy to see $|S| > 1$. Let $g_1, g_2 \in S$, and pick $\alpha \in L^\times$ such that $g_1(\alpha) \neq g_2(\alpha)$. Then $\sum_{g\in\mathrm{Gal}(L/K)} a_g g(\alpha x) = \sum_{g\in S} a_g g(\alpha x) = \sum_{g\in S} a_g g(\alpha)g(x) = 0$, and we deduce $\sum_{g\in S\setminus\{g_1\}} a_g(g(\alpha) - g_1(\alpha))g(x) = 0$ for all x, contradicting $|S|$ is minimal. ☐

Cohomology of profinite groups

Let G be a profinite group, M is called a (topological) G-module if M is a topological abelian group equipped with a (left) G-action such that $G \times M \to M$, $(g, m) \mapsto gm$ is continuous. We call M a discrete G-module if M is a G-module and M is equipped with the discrete topology. We see M is a discrete G-module, if and only if for any $m \in M$, the subgroup $\{g \in G \mid gm = m\}$ is a open subgroup of G. Denote by $\mathcal{M}\mathrm{od}_G$ the category of discrete G-modules.

Example 2.3.5. *Let K be a field, $\overline{K}$ be an algebraic closure of K, then $\overline{K}$, $\overline{K}^{\times}$ are discrete $\mathrm{Gal}(\overline{K}/K)$-modules.*

We summarize some facts on cohomology of profinite groups.

Fact 2.3.6. *(1) The category $\mathcal{M}\mathrm{od}_G$ has enough injective objects, in particular, we can define $H^i(G, M)$ as derived functors of the functor $M \mapsto M^G$.*

(2) We have $M = \varinjlim_{\substack{H \triangleleft G \\ H \text{ open}}} M^H$, and $H^i(G, M) \cong \varinjlim_{\substack{H \triangleleft G \\ H \text{ open}}} H^i(G/H, M^H)$, where $H^i(G/H, M^H) \to H^i(G/H', M^{H'})$ is the inflation map.

(3) Let $M \in \mathcal{M}\mathrm{od}_G$, then $H^i(G, M)$ can also be calculated using continuous cochains. Namely, let $\mathcal{C}^i(G, M) := \{f : G^i \to M \mid f \text{ continuous}\}$, and we define a complex exactly as the finite group case:

$$\xrightarrow{d^{i-1}} \mathcal{C}^i(G, M) \xrightarrow{d^i} \mathcal{C}^{i+1}(G, M) \xrightarrow{d^{i+1}} \cdots$$

where d^i are given as in (2.10). Then we have $H^i(G, M) = \mathrm{Ker}\, d^i / \mathrm{Im}\, d^{i-1}$. For example,

$$H^1(G, M) = \frac{\{f : G \to M \text{ continuous} \mid f(g_1g_2) = f(g_1) + g_1f(g_2)\}}{\{f : G \to M \mid \exists a \in M \text{ s.t. } f(g) = ga - a\}}.$$

Corollary 2.3.7. *Let K be a field, then $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^{\times}) = 1$.*

2.4 Group homology

Let G be a finite group. We introduce the group homology of a G-module M. Most of the theory is parallel to the group cohomology. We first define a functor $\mathcal{M}\mathrm{od}_G \to \mathcal{A}\mathrm{b}$, $M \mapsto M_G := M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. Let $I_G := \ker[\mathbb{Z}[G] \to \mathbb{Z}, e_g \mapsto 1]$. Then I_G is a left ideal of $\mathbb{Z}[G]$, called the ideal of augmentation. Then $M_G \cong M \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G]/I_G) \cong M/I_GM$.

Lemma 2.4.1. *$I_G \cong \oplus_{g \in G \setminus \{1\}} \mathbb{Z}(e_g - 1)$ (note $1 = e_1 \in \mathbb{Z}[G]$).*

Proof. Let $\alpha = \sum_{g \in G} a_g e_g \in I_G$ with $a_g \in \mathbb{Z}$, by definition we have $\sum_{g \in G} a_g = 0$. Hence $\alpha = \sum_{g \in G} a_g(e_g - 1)$. Together with the fact $\{e_g\}$ is a basis of $\mathbb{Z}[G]$ over $\mathbb{Z}$, the lemma follows. □

As taking tensor product is right exact, the functor $M \mapsto M_G$ is right exact.

Lemma 2.4.2. *The category $\mathcal{M}\mathrm{od}_G$ has enough projectives, i.e. for any $M \in \mathcal{M}\mathrm{od}_G$, there exists a projective object $P \in \mathcal{M}\mathrm{od}_G$ such that $P \twoheadrightarrow M$.*

Proof. Any free $\mathbb{Z}[G]$-module is projective. For any $M \in \mathcal{M}\mathrm{od}_G$, we have a surjective morphism $\oplus_{m\in M}\mathbb{Z}[G]_m \twoheadrightarrow M$, where $\mathbb{Z}[G]_m \cong \mathbb{Z}[G]$ and the map consists of $\mathbb{Z}[G]_m \to M$, $e_g \mapsto gm$. The lemma follows. □

Consequently, any $M \in \mathcal{M}\mathrm{od}_G$ admits a projective resolution

$$P_\bullet \to M : \cdots P_{i+1} \xrightarrow{d_i} P_i \xrightarrow{d_{i-1}} \cdots \xrightarrow{d_0} P_0 \to M \to 0.$$

We deduce then a sequence $\cdots (P_{i+1})_G \xrightarrow{d_i} (P_i)_G \xrightarrow{d_{i-1}} \cdots \xrightarrow{d_0} (P_0)_G \to M_G \to 0$, and we put $H_i(G, M) := \operatorname{Ker} d_{i-1}/\operatorname{Im} d_i$.

Example 2.4.3. *Suppose $G = \{1\}$, then $M_G = M$. We see* $H_i(G, M) = \begin{cases} M & i = 0 \\ 0 & i > 0 \end{cases}$.

Proposition 2.4.4. *(1) $H_i(G, M)$ is independent of the choice of the projective resolution of M.*

(2) A morphism $f : M_1 \to M_2$ of G-modules induces naturally morphisms $H_i(f) : H_i(G, M_1) \to H_i(G, M_2)$ for $i \in \mathbb{Z}_{\geq 0}$. Moreover, a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ induces a long exact sequence

$$\begin{aligned}\cdots \to H_i(G, M_1) \to H_i(G, M_2) \to H_i(G, M_3)& \\ \to H_{i-1}(G, M_1) \to H_{i-1}(G, M_2) \to H_{i-1}(G, M_3) \to& \\ \cdots \to H_0(G, M_1) \to H_0(G, M_2) \to H_0(G, M_3) \to 0.&\end{aligned}$$

*(3) (**Shapiro's lemma**) Let $H \subset G$, then $H_i(G, \operatorname{Ind}_H^G M) \cong H_i(H, M)$ for any $M \in \mathcal{M}\mathrm{od}_H$, and $i \in \mathbb{Z}_{\geq 0}$.*

(4) Let $G_1 \to G_2$ be a group homomorphism, $M_i \in \mathcal{M}\mathrm{od}_{G_i}$, and $f : M_1 \to M_2$ be a G_1-equivaraint morphism. Then f induces natural morphisms

$$H_i(G_1, M_1) \to H_i(G_2, M_2).$$

Sketch of proof. (1) & (2) Let $f : M_1 \to M_2$ be a morphism of G-modules, and let $P_\bullet$, $Q_\bullet$ be a projective resolution of M_1, M_2 respectively. Using the projectivity of P_i, there exists a morphism of complexes of G-modules $f_\bullet : P_\bullet \to Q_\bullet$ such that the following diagram commutes.

$$\begin{array}{ccc} P_\bullet & \longrightarrow & M_1 \\ {\scriptstyle f_\bullet}\downarrow & & {\scriptstyle f}\downarrow \\ Q_\bullet & \longrightarrow & M_2 \end{array}.$$

Moreover, different choices of $f_\bullet$ satisfy a homotopy equivalence as in the proof of Lemma 2.1.8. (1) and the first part of (2) follow. Given a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$, one can construct as in the proof of Proposition 2.1.11 an exact sequence $0 \to (P_1)_\bullet \to (P_2)_\bullet \to (P_3)_\bullet \to 0$ of complexes of G-modules with $(P_i)_\bullet$ certain projective resolution of M_i. Applying the functor $(-)_G$ and taking cohomology, we deduce the long exact sequence.

(3) For any projective $\mathbb{Z}[H]$-module, $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} N$ is a projective $\mathbb{Z}[G]$-module. For any $M'\in \mathcal{M}\mathrm{od}_H$, $(\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} M')_G \xrightarrow{\sim} M'_H$. Now let $P_\bullet \to M$ be a projective resolution. Then $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} P_\bullet \to \mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} M$ is a projective resolution of $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} M$ (recalling $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} -$ is exact). Since $(\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} P_\bullet)_G \cong (P_\bullet)_H$, (3) follows.

(4) The morphism $G_1\to G_2$ induces $\mathbb{Z}[G_1]\to\mathbb{Z}[G_2]$ that sends I_{G_1} to I_{G_2}. Thus for a G_2-module M, there is a natural map $M_{G_1}\to M_{G_2}$. Similarly as in the proof of Proposition 2.2.13, we deduce natural morphisms $H_i(G_1,M)\to H_i(G_2,M)$. Applying this to $M=M_2$, then composing with the natural morphisms $H_i(G_1,M_1)\to H_i(G_1,M_2)$, (4) follows. □

Let $H\subset G$, by Proposition 2.4.4 (4), we have natural corestriction maps:

$$\mathrm{Cor}: H_i(H,M)\to H_i(G,M).$$

The maps can also be obtained by applying $H_i(G,-)$ to the G-equivariant morphism $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} M \to M$, $e_g\otimes m\mapsto gm$. The G-equivariant morphism $M\to \mathrm{Ind}_H^G M$, $m\mapsto [g\mapsto gm]$ induces restriction maps:

$$\mathrm{Res}: H_i(G,M)\to H_i(G,\mathrm{Ind}_H^G M)\cong H_i(H,M).$$

Similarly as in Corollary 2.2.11, we have

Proposition 2.4.5. $\mathrm{Cor}\circ\mathrm{Res}=[G:H]$.

Suppose H is a normal subgroup of G. For $M\in\mathcal{M}\mathrm{od}_G$, $M_H\cong M\otimes_{\mathbb{Z}[H]}\mathbb{Z}$ inherits from M a natural G-action that factors through G/H. By Proposition 2.4.4(4), the G-equivariant morphism $M\to M_H$ induces $\mathrm{Coinf}: H_i(G,M)\to H_i(G/H,M_H)$, called coinflation maps. Similarly as in Proposition 2.2.15, we have

Proposition 2.4.6. *The following sequence is exact*

$$H_1(H,M)\xrightarrow{\mathrm{Cor}} H_1(G,M)\xrightarrow{\mathrm{Coinf}} H_1(G/H,M_H)\to 0.$$

We end this section by a discussion on $H_1(G,\mathbb{Z})$. We have an exact sequence $0\to I_G\to \mathbb{Z}[G]\to\mathbb{Z}\to 0$, that induces ($H_1(G,\mathbb{Z}[G])=0$ as $\mathbb{Z}[G]$ is projective):

$$0\to H_1(G,\mathbb{Z})\to H_0(G,I_G)\to \mathbb{Z}[G]/I_G\to\mathbb{Z}\to 0.$$

The morphism $\mathbb{Z}[G]/I_G\to\mathbb{Z}$ is an isomorphism, hence $H_1(G,\mathbb{Z})\xrightarrow{\sim} H_0(G,I_G)\cong I_G/I_G^2$.

Lemma 2.4.7. *The map $\kappa: G\to I_G/I_G^2$, $g\mapsto e_g-1$ is a group homomorphism, and induces an isomorphism $G^{\mathrm{ab}}\xrightarrow{\sim} I_G/I_G^2$.*

Proof. We have $e_{gh}-1-(e_g-1+e_h-1)=e_{gh}-e_g-(e_h-1)=(e_g-1)(e_h-1)\in I_G^2$, for $g,h\in G$. Hence κ is a group homomoprhism. It is also clear that κ is surjective. As

I_G/I_G^2 is abelian, the morphism factors through $G^{\mathrm{ab}} \twoheadrightarrow I_G/I_G^2$. We construct an inverse: $\alpha : I_G/I_G^2 \to G^{\mathrm{ab}}$, $n(e_g - 1) \mapsto g^n$. Indeed, as I_G is generated by $e_g - 1$ over $\mathbb{Z}$, we see I_G^2 is generated by $(e_g - 1)(e_h - 1)$ over $\mathbb{Z}$. We see $(e_g - 1)(e_h - 1) = e_{gh} - 1 - (e_g - 1) - (e_h - 1)$ is sent to $ghg^{-1}h^{-1}$, so the map α is well-defined. It is straightforward to check α gives an inverse of κ. The lemma follows. □

Corollary 2.4.8. *We have a natural isomorphism $H_1(G, \mathbb{Z}) \xrightarrow{\sim} G^{\mathrm{ab}}$.*

Lemma 2.4.9. *Let $H \subset G$ be a subgroup, then* Cor : $H_1(H, \mathbb{Z}) \to H_1(G, \mathbb{Z})$ *coincides with the natural map $H^{\mathrm{ab}} \to G^{ab}$ and* Res : $H_1(G, \mathbb{Z}) \to H_1(H, \mathbb{Z})$ *coincides with the transfer map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.*

Proof. By the G-equivariant exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, we have a commutative diagram

$$\begin{array}{ccccccccc} H_1(H,\mathbb{Z}) & \longrightarrow & H_0(H, I_G) & \longrightarrow & \mathbb{Z}[G]/I_H & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} & & \| & & \\ H_1(G,\mathbb{Z}) & \xrightarrow{\sim} & H_0(G, I_G) & \longrightarrow & \mathbb{Z}[G]/I_G & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array} . \tag{2.13}$$

We have an H-equivariant commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_H & \longrightarrow & \mathbb{Z}[H] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & I_G & \longrightarrow & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

that induces

$$\begin{array}{ccccc} H_1(H,\mathbb{Z}) & \xrightarrow{\sim} & H_0(H, I_H) & & \\ \| & & \downarrow & & \\ H_1(H,\mathbb{Z}) & \longrightarrow & H_0(H, I_G) & \longrightarrow & \mathbb{Z}[G]/I_H \end{array} . \tag{2.14}$$

The composition $H_0(H, I_H) \to H_0(H, I_G) \to H_0(G, I_G)$ coincides with $H^{\mathrm{ab}} \to G^{\mathrm{ab}}$. Together with (2.13) (2.14), the first part of the lemma follows. We leave the second part as an exercise. □

2.5 Tate cohomology

Let G be a finite group. For $M \in \mathcal{M}\mathrm{od}_G$, denote by $\mathcal{N}_G : M \to M$, $m \mapsto \sum_{g \in G} gm$

Lemma 2.5.1. *The map $\mathcal{N}_G$ is a morphism of G-modules, and $\mathrm{Im}(\mathcal{N}_G) \subset M^G$, $I_G M \subset \mathrm{Ker}(\mathcal{N}_G)$.*

Proof. For $m \in M$, $h \in G$, $\mathcal{N}_G(hm) = \sum_{g \in G} ghm = h \sum_{g \in G} (h^{-1}gh)m = h \sum_{g \in G} gm = h\mathcal{N}_G(m)$. For $\alpha = \sum_{g \in M} gm \in \mathrm{Im}(\mathcal{N}_G)$, $h(\alpha) = \sum_{g \in M} hgm = \sum_{g \in M} gm = \alpha$ so $\alpha \in M^G$. As $I_G M$ is generated by $(e_g - 1)m = gm - m$ and $\mathcal{N}_G(gm - m)$ is zero, $I_G M \subset \mathrm{Ker}(\mathcal{N}_G)$. □

In particular we see $\mathcal{N}_G$ induces a map $H_0(G,M) \xrightarrow{\mathcal{N}_G} H^0(G,M)$. We put

$$H_T^i(G,M) := \begin{cases} H^i(G,M) & i \geq 1, \\ H^0(G,M)/\mathcal{N}_G(M) \cong M^G/\mathcal{N}_G(M) & i = 0 \\ \mathrm{Ker}(\mathcal{N}_G|_{H_0(G,M)}) & i = -1 \\ H_{-i-1}(G,M) & i \leq -2 \end{cases}.$$

The groups $H_T^i(G,M)$ are called Tate cohomology of M. Note $H_T^i(G,-)$ are functors on $\mathcal{M}\mathrm{od}_G$: a morphism $M \to N$ in $\mathcal{M}\mathrm{od}_G$ induces natural maps $H_i^T(G,M) \to H_i^T(G,N)$ for all $i \in \mathbb{Z}$.

Example 2.5.2. *If $G = \{1\}$, we see $H_T^i(G,M) = 0$ for all i.*

Proposition 2.5.3. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence in $\mathcal{M}\mathrm{od}_G$. Then there is a natural long exact sequence*

$$\begin{aligned} \cdots \to H_T^{-2}(G,M_1) \to H_T^{-2}(G,M_2) \to H_T^{-2}(G,M_3) \to \\ H_T^{-1}(G,M_1) \to H_T^{-1}(G,M_2) \to H_T^{-1}(G,M_3) \to H_T^0(G,M_1) \to H_T^0(G,M_2) \\ \to H_T^0(G,M_3) \to H_T^1(G,M_1) \to H_T^1(G,M_2) \to H_T^1(G,M_3) \to \cdots \end{aligned}$$

Proof. We have a commutative diagram (for example, to see $H_1(G,M_3) \to H_0(G,M_1) \xrightarrow{\mathcal{N}_G} H^0(G,M_1)$ is zero, one uses the fact $H^0(G,M_1) \to H^0(G,M_2)$ is injective, and $H_1(G,M_3) \to H_0(G,M_1) \to H_0(G,M_2)$ is zero).

$$\begin{array}{ccccccccc} H_1(G,M_3) & \longrightarrow & H_0(G,M_1) & \longrightarrow & H_0(G,M_2) & \longrightarrow & H_0(G,M_3) & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle \mathcal{N}_G} & & \downarrow{\scriptstyle \mathcal{N}_G} & & \downarrow{\scriptstyle \mathcal{N}_G} & & \downarrow \\ 0 & \longrightarrow & H^0(G,M_1) & \longrightarrow & H^0(G,M_2) & \longrightarrow & H^0(G,M_3) & \longrightarrow & H^1(G,M_1) \end{array}.$$

Consequently, the morphism $H_1(G,M_3) \to H_0(G,M_1)$ (resp. $H^0(G,M_3) \to H^1(G,M_1)$) factors through $H_T^{-1}(G,M_1)$ (resp. $H_T^0(G,M_3)$). Moreover, by snake lemma, we deduce an exact sequence

$$H_T^{-1}(G,M_1) \to H_T^{-1}(G,M_2) \to H_T^{-1}(G,M_3) \to H_T^0(G,M_1) \to H_T^0(G,M_2) \to H_T^0(G,M_3).$$

Together with Proposition 2.1.11 and Proposition 2.4.4 (2), the proposition follows. □

Remark 2.5.4. *Tate cohomology can also be constructed by using the so-called complete resolutions.*

Proposition 2.5.5. *Let H be a subgroup of G and $M \in \mathcal{M}\mathrm{od}_H$, then $H_T^i(G, \mathrm{Ind}_H^G M) \cong H_T^i(H,M)$. In particular, $H_T^i(G, \mathrm{Ind}_{\{1\}}^G M) = 0$.*

Proof. We only need to show the isomorphism for $i = -1, 0$. Recall the isomorphism $\iota^0 : H^0(H,M) \to H^0(G, \mathrm{Ind}_H^G M)$ is induced by the H-equivariant morphism $\mathrm{Ind}_H^G M \to M$, $f \mapsto f(1)$; $\iota_0 : H_0(H,M) \to H_0(G, \mathrm{Ind}_H^G M)$ is induced by $M \to \mathrm{Ind}_H^G M \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$,

$m \mapsto 1 \otimes m$. One can then directly check the following diagram commutes (using the isomorphism $\operatorname{Ind}_H^G M \xrightarrow{\sim} \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$, $f \mapsto \sum_{g \in G} g \otimes f(g^{-1})$)

$$\begin{array}{ccc} H_0(H, M) & \xrightarrow{\iota_0} & H_0(G, \operatorname{Ind}_H^G M) \\ {\scriptstyle \mathcal{N}_H}\downarrow & & {\scriptstyle \mathcal{N}_G}\downarrow \\ H^0(H, M) & \xrightarrow{\iota^0} & H^0(G, \operatorname{Ind}_H^G M) \end{array}.$$

The proposition follows. □

Similarly as for group cohomology and group homology, for $M \in \mathcal{M}\mathrm{od}_G$, we have restriction and corestriction maps for Tate's cohomology (induced by the natural G-equivariant morphisms $M \to \operatorname{Ind}_H^G M$, $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \to M$ respectively)

$$\operatorname{Res} : H_T^i(G, M) \to H_T^i(G, \operatorname{Ind}_H^G M) \cong H_T^i(H, M),$$

$$\operatorname{Cor} : H_T^i(H, M) \cong H_T^i(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M) \to H_T^i(G, M).$$

By the same argument as in the proof of Corollary 2.2.11, we have

Proposition 2.5.6. $\operatorname{Cor} \circ \operatorname{Res} = [G : H]$.

Theorem 2.5.7. *Let G be a finite cyclic group, $M \in \mathcal{M}\mathrm{od}_G$. Then there is a canonical (up to the choice of a generator of G) functorial isomoprhism $H_T^i(G, M) \xrightarrow{\sim} H_T^{i+2}(G, M)$.*

Proof. Let h be a generator of G, we have an exact sequence (of G-modules)

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

where$\mathbb{Z} \to \mathbb{Z}[G]$ sends $1 \to \sum_{g \in G} e_g$, and $\mathbb{Z}[G] \to \mathbb{Z}[G]$, $e_g \mapsto e_{gh} - e_g$, and $\mathbb{Z}[G] \to \mathbb{Z}$ sends e_g to 1. Taking $- \otimes_{\mathbb{Z}} M$, we have an exact sequence of G-modules (with $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ equipped with the diagonal G-action: $g(\alpha \otimes \beta) = g(\alpha) \otimes g(\beta)$):

$$0 \to M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to M \to 0. \tag{2.15}$$

Claim: The map $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$, $g \otimes m \mapsto e_g \otimes gm$ is an isomorphism of G-modules, where the left hand side is equipped with the induced G-action: $g(\alpha \otimes \beta) = g(\alpha) \otimes \beta$, and the right hand side is equipped with the diagonal G-action.

We prove the claim. We see $g \otimes g^{-1} m$ is sent to $e_g \otimes m$, hence the map is surjective. If $\sum e_{g_i} \otimes m_i$ is sent to zero, then $\sum e_{g_i} \otimes g_i(m_i) = 0 \Rightarrow g_i(m_i) = 0 \Rightarrow m_i = 0$ so the map is injective. It is straightforward to check it is G-equivariant.

By the claim, (2.15) induces

$$0 \to M \to \operatorname{Ind}_{\{1\}}^G M \to \operatorname{Ind}_{\{1\}}^G M \to M \to 0.$$

As $H_T^i(G, \operatorname{Ind}_{\{1\}}^G M) = 0$ for all i, we deduce $H_T^i(G, M) \xrightarrow{\sim} H_T^{i+2}(G, M)$. □

Remark 2.5.8. *From the proof, (with a fixed generator of G) the isomorphisms $H_T^i(G,M) \xrightarrow{\sim} H_T^{i+1}(G,M)$ are functorial on M, i.e. if we have a morphism $M \to N$, then the following diagram commutes*

$$\begin{array}{ccc} H_T^i(G,M) & \longrightarrow & H_T^{i+2}(G,M) \\ \downarrow & & \downarrow \\ H_T^i(G,N) & \longrightarrow & H_T^{i+2}(G,N) \end{array}.$$

Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence in $\mathcal{M}\mathrm{od}_G$ (with G cyclic), then the exact sequence in Proposition 2.5.3 becomes:

$$\begin{array}{ccccc} & H_T^{-1}(G,M_2) & \longrightarrow & H_T^{-1}(G,M_3) & \\ \nearrow & & & & \searrow \\ H_T^{-1}(G,M_1) & & & & H_T^0(G,M_1) \\ \nwarrow & & & & \swarrow \\ & H_T^0(G,M_3) & \longleftarrow & H_T^0(G,M_2) & \end{array}.$$

For $M \in \mathcal{M}\mathrm{od}_G$, if $H_T^i(G,M)$ is finite, then we put $h(M) := \frac{|H_T^0(G,M)|}{|H_T^{-1}(G,M)|}$, called the Herbrant quotient of M. By the above discussion, we have

Corollary 2.5.9. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence, if two of M_i have Herbrand quotients, so does the third. And if so, $h(M_2) = h(M_1)h(M_3)$.*

Lemma 2.5.10. *Suppose G is finite cyclic, and $M \in \mathcal{M}\mathrm{od}_G$ has finite cardinality. Then $h(M) = 1$.*

Proof. Let $h \in G$ be a generator, we have an exact sequence (of finite abelian groups)

$$0 \to M^G \to M \xrightarrow{m \mapsto hm-m} M \to M_G \to 0.$$

We deduce hence $|M^G| = |M_G|$. On the other hand, we have by definition an exact sequence (of finite abelian groups)

$$0 \to H_T^{-1}(G,M) \to M_G \xrightarrow{N_G} M^G \to H_T^0(G,M) \to 0$$

and hence $h(M) = \frac{|M^G|}{|M_G|} = 1$. $\square$

2.6 Cup products

Let $M, N \in \mathcal{M}\mathrm{od}_G$, then $M \otimes_{\mathbb{Z}} N$ equipped with the diagonal G-action: $g(a \otimes b) = ga \otimes gb$, is a G-module. The operation can induce operations on (co)homology groups. For example, there is a natural map $M^G \otimes_{\mathbb{Z}} N^G \to (M \otimes_{\mathbb{Z}} N)^G$. In general, we first construct $\mathcal{C}^i(G,M) \otimes_{\mathbb{Z}} \mathcal{C}^j(G,N) \xrightarrow{\cup} \mathcal{C}^{i+j}(G, M \otimes_{\mathbb{Z}} N)$, $f \otimes f' \mapsto [(g_1, \cdots, g_{i+j}) \mapsto f(g_1, \cdots, g_i) \otimes (g_1 \cdots g_i) f(g_{i+1}, \cdots, g_{i+j})]$.

Lemma 2.6.1. $d^{i+j}_{M\otimes_{\mathbb{Z}}N}(f\cup f') = d^i_M(f)\cup f' + (-1)^i f\cup d^j_N f'$.

Proof. We have

$$\begin{aligned}
& d^{i+j}_{M\otimes_{\mathbb{Z}}N}(f\cup f')(g_0,\cdots,g_{i+j}) \\
= \ & g_0((f\cup f')(g_1,\cdots,g_{i+j})) + \sum_{k=1}^{i+j}(f\cup f')(g_0,\cdots,g_{k-1}g_k,\cdots,g_{i+j}) \\
& +(-1)^{i+j+1}(f\cup f')(g_0,\cdots,g_{i+j-1}) \\
= \ & g_0 f(g_1,\cdots,g_i)\otimes(g_0\cdots g_i)f(g_{i+1},\cdots,g_{i+j}) \\
& +\sum_{k=1}^{i}(-1)^k f(g_1,\cdots,g_{k-1}g_k,g_i)\otimes(g_0\cdots g_i)f'(g_{i+1},\cdots,g_{i+j}) \\
& +\sum_{k=i+1}^{i+j}(-1)^k f(g_0,\cdots,g_{i-1})\otimes(g_0\cdots g_{i-1})f'(g_i,\cdots,g_{k-1}g_k,\cdots,g_{i+j}) \\
& +(-1)^{i+j+1} f(g_1,\cdots,g_{i-1})\otimes(g_0\cdots g_{i-1})f'(g_i,\cdots,g_{i+j-1}) \\
= \ & (d^i_M f)\cup f' - (-1)^{i+1} f(g_0,\cdots,g_{i-1})\otimes(g_0\cdots g_i)f'(g_{i+1},\cdots,g_{i+j}) \\
& +(-1)^i f\cup d^j_N(f') + (-1)^{i+1} f(g_0,\cdots,g_{i-1})\otimes(g_0\cdots g_i)f'(g_{i+1},\cdots,g_{i+j}) \\
= \ & d^i_M(f)\cup f' + (-1)^i f\cup d^j_N(f').
\end{aligned}$$

□

By the lemma, $\cup$ induces

$$Z^i(G,M)\otimes Z^i(G,N)\xrightarrow{\cup} Z^{i+j}(G,M\otimes_{\mathbb{Z}}N)$$

$$B^i(G,M)\otimes Z^j(G,N)+Z^i(G,M)\otimes B^j(G,N)\xrightarrow{\cup} B^{i+j}(G,M\otimes_{\mathbb{Z}}N).$$

We deduce hence:

Proposition 2.6.2. *The maps $\cup$ induce $H^i(G,M)\otimes_{\mathbb{Z}} H^j(G,N)\overset{\cup}{\to} H^{i+j}(G,M\otimes_{\mathbb{Z}}N)$ for $i,j\in\mathbb{Z}_{\geq 0}$, called cup-products.*

It is easy to see the cup-products are functorial on G-modules.

Theorem 2.6.3. *The collection of maps*

$$\{H^i(G,M)\otimes_{\mathbb{Z}} H^j(G,N)\overset{\cup}{\to} H^{i+j}(G,M\otimes_{\mathbb{Z}}N)\}_{\substack{i,j\in\mathbb{Z}_{\geq 0}\\ M,N\in\mathcal{M}\mathrm{od}_G}}$$

is the unique one satisfying the following properties

1. *if $i=j=0$, $H^0(G,M)\otimes H^0(G,N)\to H^0(G,M\otimes_{\mathbb{Z}}N)$ is induced by the identity map on $M\otimes_{\mathbb{Z}}N$: $M^G\otimes_{\mathbb{Z}}N^G\to(M\otimes_{\mathbb{Z}}N)^G$;*

2. *if* $0 \to M_1 \to M \to M_2$ *is an exact sequence in* $\mathcal{M}\mathrm{od}_G$*, and* $N \in \mathcal{M}\mathrm{od}_G$ *such that* $0 \to M_1 \otimes_{\mathbb{Z}} N \to M \otimes_{\mathbb{Z}} N \to M_2 \otimes_{\mathbb{Z}} N \to 0$ *is exact, then*

$$\delta(\alpha_2) \cup \beta = \delta(\alpha_2 \cup \beta) \in H^{i+j+1}(G, M \otimes_{\mathbb{Z}} N)$$

for all $\alpha_2 \in H^i(G, M_2)$ *(so* $\delta(\alpha_2) \in H^{i+1}(G, M_1)$*) and* $\beta \in H^j(G, N)$*;*

3. *if* $0 \to N_1 \to N \to N_2 \to 0$ *is an exact sequence in* $\mathcal{M}\mathrm{od}_G$*, and* $M \in \mathcal{M}\mathrm{od}_G$ *such that* $0 \to M \otimes_{\mathbb{Z}} N_1 \to M \otimes_{\mathbb{Z}} N \to M \otimes_{\mathbb{Z}} N_2 \to 0$*, then*

$$\alpha \cup \delta(\beta_2) = (-1)^i \delta(\alpha \cup \beta_2) \in H^{i+j+1}(G, M \otimes_{\mathbb{Z}} N)$$

for all $\alpha \in H^i(G, M)$ *and* $\beta_2 \in H^j(G, N_2)$*.*

Sketch of proof. One can directly check these conditions, using the following description of the δ-maps in term of cochains. If we have an exact sequence $0 \to M_1 \to M \to M_2 \to 0$ in $\mathcal{M}\mathrm{od}_G$, then we naturally get exact sequences

$$0 \to \mathcal{C}^i(G, M_1) \to \mathcal{C}^i(G, M) \to \mathcal{C}^i(G, M_2) \to 0,$$

for all $i \geq 0$. We deduce a commutative diagram

$$\begin{array}{ccccccc} & & \frac{\mathcal{C}^i(G,M_1)}{B^i(G,M_1)} & \longrightarrow & \frac{\mathcal{C}^i(G,M)}{B^i(G,M)} & \longrightarrow & \frac{\mathcal{C}^i(G,M_2)}{B^i(G,M_2)} & \longrightarrow & 0 \\ & & {\scriptstyle d^i_{A_1}}\downarrow & & {\scriptstyle d^i_{A}}\downarrow & & {\scriptstyle d^i_{A_2}}\downarrow & & \\ 0 & \longrightarrow & Z^{i+1}(G, M_1) & \longrightarrow & Z^{i+1}(G, M) & \longrightarrow & Z^{i+1}(G, M_2) & & \end{array}$$

and the δ-map $H^i(G, M_2) \to H^{i+1}(G, M_1)$ is induced by the snake lemma. Explicitly, for $f : G^i \to A_2$ such that $d^i_{A_2}(f) = 0$. We lift f to a map $\tilde{f} : G^i \to A$, then $d^i_A \tilde{f} : G^{i+1} \to A$ has image in A_1. Then $[d^i_A \tilde{f}] = \delta(f)$.

We now explain the uniqueness. When $i = j = 0$, the uniqueness is clear. For $M \in \mathcal{M}\mathrm{od}_G$, we have an exact sequence in $\mathcal{M}\mathrm{od}_G$:

$$0 \to M \to \mathrm{Ind}_{\{1\}}^G M \to M' \to 0, \tag{2.16}$$

that induces $H^0(G, M') \twoheadrightarrow H^1(G, M)$. Note that the exact sequence splits in the category of abelian groups: $\mathrm{Ind}_{\{1\}}^G M \to M$, $f \mapsto M$. Hence for any $N \in \mathcal{M}\mathrm{od}_G$, we obtain an exact sequence

$$0 \to M \otimes_{\mathbb{Z}} N \to (\mathrm{Ind}_{\{1\}}^G M) \otimes_{\mathbb{Z}} N \to M' \otimes_{\mathbb{Z}} N \to 0.$$

By Condition 2, the following diagram should commute

$$\begin{array}{ccc} H^0(G, M') \otimes H^0(G, N) & \longrightarrow & H^0(G, M' \otimes_{\mathbb{Z}} N) \\ \downarrow & & \downarrow \\ H^1(G, M) \otimes H^0(G, N) & \longrightarrow & H^1(G, M \otimes_{\mathbb{Z}} N) \end{array}.$$

As the left map is surjective, the bottom cup-product map is fixed (for any $M, N \in \mathcal{M}\mathrm{od}_G$). This proves the case $i = 1$, $j = 0$. Using similar arguments and induction on i, we obtain the uniqueness of $H^i(G,M)\otimes H^0(G,N)\xrightarrow{\cup}H^i(G,M\otimes_{\mathbb{Z}}N)$ for all $M,N\in\mathcal{M}\mathrm{od}_G$ and $i\in\mathbb{Z}_{\geq 0}$. Using similar arguments with M replaced by N and induction on j, we then deduce the uniqueness of $H^i(G,M)\otimes H^j(G,N)\xrightarrow{\cup}H^{i+j}(G,M\otimes_{\mathbb{Z}}N)$ for all $M,N\in\mathcal{M}\mathrm{od}_G$, $i,j\in\mathbb{Z}_{\geq 0}$. □

We have a G-equivariant isomorphism $s: M\otimes_{\mathbb{Z}}N\to N\otimes_{\mathbb{Z}}M$, $a\otimes b\mapsto b\otimes a$, that induces isomorphisms $s: H^i(G,M\otimes_{\mathbb{Z}}N)\xrightarrow{\sim}H^i(G,N\otimes_{\mathbb{Z}}M)$.

Proposition 2.6.4. *We have a commutative diagram*

$$\begin{array}{ccc} H^i(G,M)\otimes H^j(G,N) & \xrightarrow{\cup} & H^{i+j}(G,M\otimes_{\mathbb{Z}}N) \\ \Big\downarrow s & & \Big\downarrow s \\ H^j(G,N)\otimes H^i(G,M) & \xrightarrow{(-1)^{ij}\cup} & H^{i+j}(G,N\otimes_{\mathbb{Z}}M) \end{array}. \tag{2.17}$$

Proof. We use induction on i,j. The case $i=j=0$ is clear. Suppose it holds for i,j. Using the exact sequence in (2.16), we deduce a surjective δ-map $H^i(G,M')\twoheadrightarrow H^{i+1}(G,M)$. We have commutative diagrams

$$\begin{array}{ccc} H^i(G,M')\otimes H^j(G,N) & \xrightarrow{\cup} & H^{i+j}(G,M'\otimes_{\mathbb{Z}}N) \\ \delta\Big\downarrow \quad \Big\| & & \Big\downarrow\delta \\ H^{i+1}(G,M)\otimes H^j(G,N) & \xrightarrow{\cup} & H^{i+j+1}(G,M\otimes_{\mathbb{Z}}N) \end{array},$$

$$\begin{array}{ccc} H^j(G,N)\otimes H^i(G,M') & \xrightarrow{\cup} & H^{i+j}(G,N\otimes_{\mathbb{Z}}M') \\ \delta\Big\downarrow \quad \Big\| & & \Big\downarrow\delta \\ H^j(G,N)\otimes H^{i+1}(G,M) & \xrightarrow{(-1)^j\cup} & H^{i+j+1}(G,N\otimes_{\mathbb{Z}}M) \end{array}.$$

Together with the assumption hypothesis, we deduce (2.17) holds for $i+1,j$. The proposition follows. □

Proposition 2.6.5. *Let $M_1,M_2,M_3\in\mathcal{M}\mathrm{od}_G$, $\alpha\in H^i(G,M_1)$, $\beta\in H^j(G,M_2)$, $\gamma\in H^k(G,M_3)$, then*

$$(\alpha\cup\beta)\cup\gamma=\alpha\cup(\beta\cup\gamma)\in H^{i+j+k}(G,M_1\otimes_{\mathbb{Z}}M_2\otimes_{\mathbb{Z}}M_3).$$

Proof. The proposition follows from the uniqueness in Theorem 2.6.3. □

Notation 2.6.6. *Suppose we have a G-equivariant morphism $M\otimes_{\mathbb{Z}}N\to E$, then we also denote by $\cup$ the composition:*

$$H^i(G,M)\otimes H^j(G,N)\xrightarrow{\cup}H^{i+j}(G,M\otimes_{\mathbb{Z}}N)\to H^{i+j}(G,E).$$

Proposition 2.6.7. *Let $M, N \in \mathcal{M}\mathrm{od}_G$.*

(1) Let H be a subgroup of G, $\alpha \in H^i(G, M)$, $\beta \in H^j(G, N)$, then

$$\mathrm{Res}(\alpha \cup \beta) = \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta).$$

(2) Let H be a nomral subgroup of G, $\alpha \in H^i(G/H, M^H)$, $\beta \in H^j(G/H, N^H)$, then

$$\inf(\alpha \cup \beta) = \inf(\alpha) \cup \inf(\beta) \in H^{i+j}(G, M \otimes_{\mathbb{Z}} N).$$

(3) Let H be a subgroup of G, $\alpha \in H^i(H, M)$, $\beta \in H^i(G, N)$, then

$$(\mathrm{Cor}\,\alpha) \cup \beta = \mathrm{Cor}(\alpha \cup \mathrm{Res}\,\beta) \in H^{i+j}(G, M \otimes_{\mathbb{Z}} N),$$

in other words, the following diagram commutes:

$$\begin{array}{ccc} H^i(H, M) \otimes H^j(H, N) & \longrightarrow & H^{i+j}(H, M \otimes_{\mathbb{Z}} N) \\ \mathrm{Cor}\downarrow \qquad \mathrm{Res}\uparrow & & \mathrm{Cor}\downarrow \\ H^i(G, M) \otimes H^j(G, N) & \longrightarrow & H^{i+j}(G, M \otimes_{\mathbb{Z}} N) \end{array}.$$

Proof. (1) (2) follow by explicit formulas (or induction on degrees as for (3)). (3) follows by induction on degrees: one first checks it holds for $i = j = 0$, then uses (2.16) and induction on i to prove it holds for $i \geq 0$ and $j = 0$ (as in the proof of Theorem 2.6.3); finally one uses (2.16) with M replaced by N and induction on j to prove it holds for all $i, j \geq 0$. □

For $M, N \in \mathcal{M}\mathrm{od}_G$, we also have a natural morphism $M_G \otimes_{\mathbb{Z}} N^G \to (M \otimes_{\mathbb{Z}} N)_G$, $\bar{m} \otimes n \mapsto m \mathbin{\bar{\otimes}} n$ (as $n \in N^G$, the morphism is well-defined). This can induce the so-called cap-products: $H_{i+j}(G, M) \otimes H^i(G, N) \to H_j(G, M \otimes_{\mathbb{Z}} N)$. We omit further discussion the theory. Finally we have for Tate cohomology:

Theorem 2.6.8. *There is a unique collection of maps*

$$\{H^i_T(G, M) \otimes_{\mathbb{Z}} H^j_T(G, N) \xrightarrow{\cup} H^{i+j}_T(G, M \otimes_{\mathbb{Z}} N)\}_{\substack{i,j \in \mathbb{Z} \\ M,N \in \mathcal{M}\mathrm{od}_G}}$$

satisfying

(1) $H^0_T(G, M) \otimes H^0_T(G, N) \to H^0_T(G, M \otimes_{\mathbb{Z}} N)$ is induced by the identity map on $M \otimes_{\mathbb{Z}} N$,

(2) the maps are compatible with δ-maps.

Proof. The existence and uniqueness can follow by a dimension shifting argument, similarly as in the proof of Theorem 2.6.3. □

Example 2.6.9. *The map $H^0_T(G, M) \otimes H^{-1}_T(G, N) \xrightarrow{\cup} H^{-1}_T(G, M \otimes_{\mathbb{Z}} N)$ is given by $(a, b) \mapsto a \otimes b$. Indeed, as $a \in M^G$, and $\mathcal{N}_G(b) = 0$, we see $\mathcal{N}_G(a \otimes b) = 0$ (so that the map is well-defined).*

By the same argument as in proof of Proposition 2.6.4, we have:

Proposition 2.6.10. *We have a commutative diagram*

$$\begin{array}{ccc} H_T^i(G,M)\otimes H_T^j(G,N) & \xrightarrow{\cup} & H_T^{i+j}(G,M\otimes_{\mathbb{Z}} N) \\ {\scriptstyle s}\downarrow & & {\scriptstyle s}\downarrow \\ H_T^j(G,N)\otimes H_T^i(G,M) & \xrightarrow{(-1)^{ij}\cup} & H_T^{i+j}(G,N\otimes_{\mathbb{Z}} M) \end{array}. \tag{2.18}$$

We have as in Proposition 2.6.7 (1) (3):

Proposition 2.6.11. *Let $M, N \in \mathcal{M}\mathrm{od}_G$.*

(1) Let H be a subgroup of G, $\alpha \in H_T^i(G,M)$, $\beta \in H_T^j(G,N)$, then

$$\mathrm{Res}(\alpha\cup\beta) = \mathrm{Res}(\alpha)\cup\mathrm{Res}(\beta).$$

(2) Let H be a subgroup of G, $\alpha \in H_T^i(H,M)$, $\beta \in H_T^i(G,N)$, then

$$(\mathrm{Cor}\,\alpha)\cup\beta = \mathrm{Cor}(\alpha\cup\mathrm{Res}\,\beta) \in H_T^{i+j}(G,M\otimes_{\mathbb{Z}} N),$$

in other words, the following diagram commutes:

$$\begin{array}{ccc} H_T^i(H,M)\otimes H_T^j(H,N) & \longrightarrow & H_T^{i+j}(H,M\otimes_{\mathbb{Z}} N) \\ {\scriptstyle \mathrm{Cor}}\downarrow \quad {\scriptstyle \mathrm{Res}}\uparrow & & {\scriptstyle \mathrm{Cor}}\downarrow \\ H_T^i(G,M)\otimes H_T^j(G,N) & \longrightarrow & H_T^{i+j}(G,M\otimes_{\mathbb{Z}} N) \end{array}.$$

Chapter 3

Local class field theory

In this chapter, we finish the proof of Theorem 1.5.1 and Theorem 1.5.3. We will also prove

Theorem 3.0.1. *Let L/K be a finite Galois extension, and M be the maximal abelian subextension of L/K. Then $N_{L/K}L^\times = N_{M/K}M^\times$.*

The key ingredient is the following theorem in terms of Galois cohomology.

Theorem 3.0.2. *For any finite Galois extension L/K, there exists a canonical isomorphism*

$$H_T^i(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} H_T^{i+2}(\mathrm{Gal}(L/K), L^\times). \tag{3.1}$$

Remark 3.0.3. *(1) Let $i := -2$, then $H_T^i(\mathrm{Gal}(L/K), \mathbb{Z}) \cong H_1(\mathrm{Gal}(L/K), \mathbb{Z}) \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}$, and $H_T^0(\mathrm{Gal}(L/K), L^\times) \cong K^\times / \mathrm{Norm}_{L/K}(L^\times)$. The induced isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} K^\times / \mathrm{Norm}_{L/K}(L^\times)$ will finally induce the local artin reciprocity map (the "canonical" in the theorem will ensure the compatibility of the isomorphisms when L varies).*

(2) The morphism (3.1) is in fact given by the cup-product with a certain element in $H^2(\mathrm{Gal}(L/K), L^\times)$, that will be a central object to study in this section. The group $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \cong \varinjlim_L H^2(\mathrm{Gal}(L/K), L^\times)$ is the so-called Brauer group of K.

3.1 Tate's theorem

Theorem 3.1.1 (Tate)**.** *Let G be a finite group and let M be a G-module. Suppose for any subgroup H of G, $H^1(H, M) = 0$ and $H^2(H, M)$ is cyclic of order $\#H$. Then there are isomorphisms*

$$\iota_\phi : H_T^i(G, \mathbb{Z}) \xrightarrow{\sim} H_T^{i+2}(G, M) \tag{3.2}$$

that are canonical up to the choice of generators of $H^2(G, M)$.

Lemma 3.1.2. *Keep the assumption of the theorem, then the restriction map $H^2(G, M) \to H^2(H, M)$ is surjective for $H \leq G$.*

Proof. The lemma follows easily from the fact $\mathrm{Cor} \circ \mathrm{Res} = [G : H]$, $H^2(G, M)$ (resp. $H^2(H, M)$) is cyclic of order $|G|$ (resp. $|H|$). □

We introduce the so-called splitting module for $\phi \in H^2(G,M)$. Recall $\phi \in H^2(G,M)$ is represented by a 2-cocycle: $\phi : G^2 \to M$ satisfying $g_1\phi(g_2,g_3) + \phi(g_1,g_2g_3) = \phi(g_1g_2,g_3) + \phi(g_1g_2)$. We put $M[\phi] := M \oplus \oplus_{g\in G\setminus\{1\}} \mathbb{Z}x_g$, and denote by $x_1 := \phi(1,1) \in M$. We define the following G-action on $M[\phi]$ extending the G-action on M:

$$hx_g := x_{hg} - x_h + \phi(h,g) \in M[\phi].$$

Indeed, for $g', g, h \in G$, we have $1(x_g) = x_g - x_1 + \phi(1,g) = x_g$ (using $\phi(1,g) = \phi(1,1)$)

$$\begin{aligned} g'(h(x_g)) &= g'(x_{hg} - x_h + \phi(h,g)) \\ &= x_{g'hg} - x_{g'} + \phi(g',hg) - (x_{g'h} - x_{g'} + \phi(g',h)) + g'\phi(h,g) \\ &= x_{g'hg} - x_{g'h} + \phi(g'h,g) = (g'h)(x_g). \end{aligned}$$

The G-equivariant morphism $M \hookrightarrow M[\phi]$ induces $H^2(G,M) \to H^2(G,M[\phi])$. By the construction, we see ϕ is sent to zero via the map (as ϕ is a 2-coboundary in $M[\phi]$). We have an exact sequence

$$0 \to M \to M[\phi] \to \mathbb{Z}[G]$$

where the last map sends M to zero and x_g to $e_g - 1$ (so $h(x_g) = x_{hg} - x_h + \phi(h,g)$ is sent to $e_{hg} - 1 - e_h + 1 = h(e_g - 1)$). We deduce hence a G-equivariant exact sequence

$$0 \to M \to M[\phi] \to I_G \to 0 \tag{3.3}$$

Remark 3.1.3. *We have the following conceptual explanation for splitting modules of ϕ. We have $\phi \in H^2(G,M) \cong \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z},M)$. Applying $\mathrm{Hom}_{\mathbb{Z}[G]}(-,M)$ to the exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, we deduce $\mathrm{Ext}^1_{\mathbb{Z}[G]}(I_G,M) \xrightarrow{\sim} \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z},M)$. Then $M[\phi]$ is actually the premiage of ϕ via this isomorphism.*

Recall the exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, induces $H^i_T(G,\mathbb{Z}) \xrightarrow{\sim} H^{i+1}_T(G,I_G)$ for all i.

Claim: $H^i_T(G,M[\phi]) = 0$ for all i.

Assume the claim, we deduce from (3.3):

$$H^{i-1}_T(G,\mathbb{Z}) \xrightarrow{\sim} H^i_T(G,I_G) \xrightarrow{\sim} H^{i+1}_T(G,M),$$

and the theorem follows (noting the last map depends on the choice of ϕ).

For the rest of the section, we prove the claim. First note that $\mathbb{Z}[G]$ is an induced module for any subgroup H of G: $\mathbb{Z}[G] \cong \mathbb{Z}[H]^{|G:H|}$ as H-module. Hence we have $H^i_T(H,\mathbb{Z}[G]) = 0$ for all i. We deduce by (3.3):

$$\begin{aligned} 0 = H^1(H,M) \to H^1(H,M[\phi]) \to H^1(H,I_G) \to H^2(H,M) \\ \to H^2(H,M[\phi]) \to H^2(H,I_G) \to \cdots \end{aligned}$$

Using the commutative diagram

$$\begin{array}{ccc} H^2(G,M) & \longrightarrow & H^2(G,M[\phi]) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ H^2(H,M) & \longrightarrow & H^2(H,M[\phi]) \end{array}$$

and Lemma 3.1.2, we see the natural morphism $H^2(H,M) \to H^2(H,M[\phi])$ is zero. We have $H^1(H,I_G) \cong H^0_T(H,\mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z}$. Using cocycles, we easily see $H^1(H,\mathbb{Z}) = 0$ hence $H^2(H,I_G) = 0$ (for all $H \leq G$). We then deduce that $H^1(H,M[\phi]) = H^2(H,M[\phi]) = 0$ for all $H \leq G$. The claim then follows from the following lemma.

Lemma 3.1.4. *Let G be a finite group, $N \in \mathcal{M}\mathrm{od}_G$. Suppose*

$$H^1(H,N) = H^2(H,N) = 0 \text{ for all } H \leq G, \tag{3.4}$$

then $H^i_T(G,N) = 0$ for all i.

Proof. (1) Suppose first G is cyclic, then $H^i_T(G,N) \cong H^{i+2}_T(G,N)$. By (3.4), we deduce $H^i_T(G,N) = 0$ for all i.

(2) Suppose G is solvable, and we use induction on the order of G.

Induction hypothesis: if $|G| < r$, then for any $N \in \mathcal{M}\mathrm{od}_G$, if (3.4)holds, then $H^i_T(G,N) = 0$ for all i.

Assume $|G| = r$. By induction hypothesis, for any proper subgroup H' of G, we have $H^i_T(H',N) = 0$. Since G is solvable, there exists a normal (proper) subgroup H of G such that G/H is cyclic (and $H^i_T(H,N) = 0$ for all i). By restriction-inflation sequence

$$0 \to H^1(G/H,N^H) \to H^1(G,N) \to H^1(H,N)$$

we deduce hence $H^1(G/H,N^H) = 0$. Similarly, using $H^1(H,N) = 0$, we have an exact sequence

$$0 \to H^2(G/H,N^H) \to H^2(G,N) \to H^2(H,N)$$

that implies $H^2(G/H,N^H) = 0$. Since G/H is cyclic, we deduce $H^i_T(G/H,N^H) = 0$ for all i. Since $H^{i-1}(H,N) = 0$, the following sequence is exact

$$0 \to H^i(G/H,N^H) \to H^i(G,N) \to H^i(H,N).$$

Together with the fact $H^i(G/H,N^H) = 0$ for all $i \geq 1$, we deduce $H^i(G,N) = 0$ for all i. Hence $H^i_T(G,N) = H^i(G,N) = 0$ for all $i > 0$. We have $H^0_T(G,N) = N^G/\mathcal{N}_G(N)$. As $H^0_T(G/N,N^H) = H^0_T(H,N) = 0$, for any $x \in N^G$, there exists $y \in N^H$ such that $\mathcal{N}_{G/H} y = x$; and for such y, there exists $z \in N$ such that $\mathcal{N}_H z = y$. We deduce $\mathcal{N}_G(z) = x$ hence $H^0_T(G,N) = 0$.

Let N' be the kernel of $\mathbb{Z}[G] \otimes_{\mathbb{Z}} N \to N$, $g \otimes n \mapsto gn$. Taking Tate cohomology, we deduce $H^i_T(H',N) \xrightarrow{\sim} H^{i+1}_T(H',N')$ for all i and for any $H' \leq G$. In particular, $H^0_T(H',N) = 0$ (resp. $H^1(H',N) = 0$) implies $H^1(H',N') = 0$ (resp. $H^2(H',N') = 0$) for all $H' \leq G$. Thus N' satisfies the condition in (3.4). By the above argument (and the induction hypothesis applied to N') we deduce hence $H^i_T(G,N') = 0$ for $i \geq 0$, hence $H^i_T(G,N) = 0$ for $i \geq -1$. Continue with the argument, we see $H^i_T(G,N) = 0$ for all i.

(3) Now we consider the general case. Let $G_p \subset G$ be a p-Sylow subgroup. The composition $\mathrm{Cor} \circ \mathrm{Res} : H^i_T(G,N) \to H^i_T(G_p,N) \to H^i_T(G,N)$ is equal to $[G : G_p]$. As $(p,[G : G_p]) = 1$, we see $H^i_T(G,N)[p^\infty] := \cup H^i_T(G,N)[p^n] \hookrightarrow H^i_T(G_p,N)$. By (2), $H^i_T(G,N)[p^\infty] = 0$ for all i (and all p). Since $H^i_T(G,N)$ is annihilated by $|G|$, we deduce $H^i_T(G,N) = 0$ for all i. This concludes the proof. □

Remark 3.1.5. *We show the (3.2) is given by* $\alpha \mapsto \alpha \cup \phi$*. Denote by* $\delta_1 : H^1(G, I_G) \xrightarrow{\sim} H^2(G, M)$ *the isomorphism induced by (3.3) (so depending on* ϕ*), and* $\delta_2 : H^0_T(G, \mathbb{Z}) \xrightarrow{\sim} H^1(G, I_G)$ *the canonical isomorphism. We first show* $\delta_1 \circ \delta_2(1) = \phi$*. Indeed, the map* δ_2 *sends 1 to the 1-cocycle (see the proof of Theorem 2.6.3 for the description of* δ*-maps in terms of cochains):* $c_1 : g \mapsto g(e_1) - e_1 = e_g - e_1$*. Similarly (recall* x_g *is a lifting of* $e_g - 1$ *in* $M[\phi]$*)* δ_2 *sends* c_1 *to the 2-cocycle:* $c_2 : (g_1, g_2) \mapsto g_1(x_{g_2}) - x_{g_1g_2} + x_{g_1} = \phi(g_1, g_2)$*. Taking cup-product with* $1 \in H^0_T(G, \mathbb{Z})$ *gives the identity map* $H^{i+2}_T(G, M) \xrightarrow{\sim} H^{i+2}_T(G, M)$*,* $\beta \mapsto \beta \cup 1$*. For* $\alpha \in H^i_T(G, M)$*, we have*

$$\iota_\phi(\alpha) \cup 1 = (\delta_{1,i} \circ \delta_{2,i})(\alpha) \cup 1 = \alpha \cup (\delta_1 \circ \delta_2)(1) = \alpha \cup \phi,$$

where $\delta_{1,i} : H^{i+1}_T(G, I_G) \xrightarrow{\sim} H^{i+2}_T(G, M)$ *(induced by (3.3)) and* $\delta_{2,i} : H^i_T(G, Z) \xrightarrow{\sim} H^{i+1}_T(G, I_G)$ *(so* $\delta_{1,0} = \delta_1$ *and* $\delta_{2,0} = \delta_2$*).*

3.2 Brauer group of local fields

Let L/K be a finite Galois extension. We want to apply Tate's theorem to $G = \mathrm{Gal}(L/K)$ and $M = L^\times$. By Hilbert's theorem 90, we know already $H^1(\mathrm{Gal}(L/K), L^\times) = \{1\}$. In this section we study $H^2(\mathrm{Gal}(L/K), L^\times)$.[1] Note the natural exact sequence

$$1 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$$

is $\mathrm{Gal}(L/K)$-equivariant (so that we can study the Galois cohomology of $L^\times$ via that of $\mathcal{O}_L^\times$ and $\mathbb{Z}$).

We first consider the case L is unramified over K. Note in this case $\mathrm{Gal}(L/K)$ is cyclic, and hence $H^2(\mathrm{Gal}(L/K), L^\times) \cong H^2_T(\mathrm{Gal}(L/K), L^\times) \cong H^0_T(\mathrm{Gal}(L/K), L^\times) \cong K^\times/N_{L/K}(L^\times)$.

Lemma 3.2.1. $H^0_T(\mathrm{Gal}(k_L/k), k_L^\times) = \{1\}$.

Proof. One can directly prove $N_{k_L/k}(k_L^\times) = k^\times$, or use the fact $h(k_L^\times) = 1$ ($k_L^\times$ is finite) and $H^1_T(\mathrm{Gal}(k_L/k), k_L^\times) = \{1\}$. □

Lemma 3.2.2. *We have* $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$*.*

Proof. By the above lemma, for $x \in \mathcal{O}_K^\times$, there exists $y_1 \in \mathcal{O}_L^\times$ such that $N_{L/K}(y_1) \equiv x \pmod{\varpi_K}$, or equivalently, $N_{L/K}(y_1)/x \equiv 1 \pmod{\varpi_K}$. We use induction to show there exists $y_i \in \mathcal{O}_L^\times$ such that $y_i \equiv y_{i-1} \pmod{\varpi_K^{i-1}}$ and $N_{L/K}(y_i)/x \equiv 1 \pmod{\varpi_K^i}$. Let $y_i = y_{i-1}(1 + \varpi_K^{i-1}a)$, then $N_{L/K}(y_i) \equiv N_{L/K}(y_{i-1})(1 + \mathrm{tr}_{k_L/k}(a)\varpi_K^{i-1}) \pmod{\varpi_K^i}$. As $\mathrm{tr}_{k_L/k} : k_L \to k$ is surjective, the existence of y_i follows. □

Lemma 3.2.3. *We have* $H^1_T(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = \{1\}$*.*

Proof. As $H^1_T(\mathrm{Gal}(L/K), L^\times) = \{1\}$, for any $f \in Z^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) \subset Z^1(\mathrm{Gal}(L/K), L^\times)$ there exists $\alpha \in L^\times$ such that $f(g) = g(\alpha)/\alpha$ for all $g \in \mathrm{Gal}(L/K)$. Let $\alpha_0 \in \mathcal{O}_L^\times$ such that $\alpha = \varpi_K^i \alpha_0$ (note ϖ_K is also a uniformizer in L), then $f(g) = g(\alpha_0)/\alpha_0$. The lemma follows. □

[1] The group $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \cong \varinjlim_L H^2(\mathrm{Gal}(L/K), L^\times)$ is called the *Brauer group* of K.

We see $H_T^i(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = 0$ for all i, hence $H_T^i(\mathrm{Gal}(L/K), L^\times) \cong H_T^i(\mathrm{Gal}(L/K), \mathbb{Z})$ for all i. We see:

Proposition 3.2.4. *If L/K is finite unramified, then $H_T^0(\mathrm{Gal}(L/K), L^\times)$ is a cyclic group of order $[L : K]$. Moreover, $N_{L/K}^\times(L^\times)$ is generated by $\varpi_K^{|L:K|}$ (where $\varpi_K^\times$ is an arbitrary uniformizer of K) and $\mathcal{O}_K^\times$, and (hence) $H_T^0(\mathrm{Gal}(L/K), L^\times)$ is generated by ϖ_K.*

Now we assume L/K is a general finite Galois extension.

Lemma 3.2.5. *There exists a finite free $\mathcal{O}_K$-submodule V of $\mathcal{O}_L$ of rank $[L : K]$, stable by $\mathrm{Gal}(L/K)$, such that $H^i(\mathrm{Gal}(L/K), V) = 0$ for all $i > 0$.*

Proof. Recall there exists $\alpha \in L$ such that $L = \oplus_{\sigma \in \mathrm{Gal}(L/K)} K\sigma(\alpha)$. Multiplying α be a certain power of ϖ_K, we can and do assume $\alpha \in \mathcal{O}_L$. Put $V := \oplus_{\sigma \in \mathrm{Gal}(L/K)} \mathcal{O}_K \sigma(\alpha) \subset \mathcal{O}_L$. Then V is an induced $\mathrm{Gal}(L/K)$-module. The lemma follows. □

Lemma 3.2.6. *There exists an open subgroup $W \subset \mathcal{O}_L^\times$, stable by $\mathrm{Gal}(L/K)$ such that $H^i(\mathrm{Gal}(L/K), W) = 1$ for all $i > 0$.*

Proof. We use the notation in the proof of the above lemma. Multiplying α by a certain power of ϖ_K, we can and do assume that for all $x \in V$, the power series $\exp(x) := \sum_{i=0}^{\infty} \frac{x^i}{n!}$ converges. Let W be the image of $\exp : V \to \mathcal{O}_L^\times$, that is clearly stable by $\mathrm{Gal}(L/K)$. Moreover, as $\varpi^m \mathcal{O}_L \subset V$ for m sufficiently large, we see (using the log map) $1 + \varpi_K^n \mathcal{O}_L \subset W$ for n sufficiently large, so W is open. Finally, as the map $\exp : V \to W$ is an isomorphism of $\mathrm{Gal}(L/K)$-modules, we see $H^i(\mathrm{Gal}(L/K), W) = 1$ for all $i > 0$. □

Corollary 3.2.7. *Suppose L/K is cyclic. We have $h(L^\times) = [L : K]$, consequently, the group $H^2(\mathrm{Gal}(L/K), L^\times)$ is finite of order $[L : K]$.*

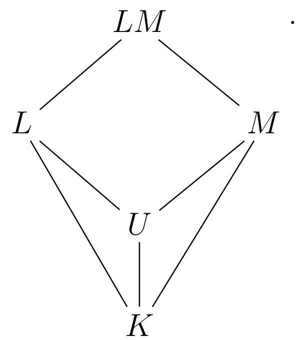
Proof. By the above lemma, we deduce $h(\mathcal{O}_K^\times) = h(W)h(\mathcal{O}_K^\times/W) = 1$. We also have $h(\mathbb{Z}) = |H_T^0(\mathrm{Gal}(L/K), \mathbb{Z})| = [L : K]$. The corollary follows from the fact $h(L^\times) = h(\mathcal{O}_K^\times)h(\mathbb{Z})$. □

Corollary 3.2.8. *Let L be a finite Galois extension of K, we have $|H^2(\mathrm{Gal}(L/K), L^\times)| \leq [L : K]$.*

Proof. Recall $\mathrm{Gal}(L/K)$ is solvable (by ramification theory). By Hilbert's theorem 90, $H^1(\mathrm{Gal}(L/K'), L^\times) = 0$ for any subextension K'/K. The corollary then follows from the above lemma by using restriction-inflation sequence (for H^2). □

Theorem 3.2.9. *Let L be a finite Galois extension of K, then $H^2(\mathrm{Gal}(L/K), L^\times)$ is cyclic of order $[L : K]$.*

Proof. Let $d := [L : K]$ and let M be the unramified extension of K of degree d. Put $U := M \cap L$, that is the maximal unramified subextension in L. We have the following picture:



By construction, LM/L is unramified, LM/M and L/U are totally ramified. We have moreover $\mathrm{Gal}(LM/L) \xrightarrow{\sim} \mathrm{Gal}(M/U)$, $\mathrm{Gal}(LM/M) \xrightarrow{\sim} \mathrm{Gal}(L/U)$. Consider the restriction-inflation sequences

$$\begin{array}{ccccccc} 1 \longrightarrow & H^2(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\inf_L} & H^2(\mathrm{Gal}(LM/K), (LM)^\times) & \xrightarrow{\mathrm{Res}_L} & H^2(\mathrm{Gal}(LM/L), (LM)^\times) & \cdot \\ & \uparrow \vdots & \overset{\inf_M}{\nearrow} & \sim \uparrow & & & \\ 1 \longrightarrow & H^2(\mathrm{Gal}(M/K), M^\times) & \xrightarrow{\inf_M} & H^2(\mathrm{Gal}(LM/K), (LM)^\times) & \xrightarrow{\mathrm{Res}_M} & H^2(\mathrm{Gal}(LM/M), (LM)^\times) & \end{array}$$

As $|H^2(\mathrm{Gal}(L/K), L^\times)| \leq d$, and $H^2(\mathrm{Gal}(M/K), M^\times)$ is cyclic of order d, it is sufficient to show $\mathrm{Res}_L \circ \inf_M = 0$ (that will imply the injection $\inf_M$ factors through $H^2(\mathrm{Gal}(L/K), L^\times)$). First we claim $\mathrm{Res}_L \circ \inf_M$ is equal to the following composition

$$H^2(\mathrm{Gal}(M/K), M^\times) \xrightarrow{\mathrm{Res}} H^2(\mathrm{Gal}(M/U), M^\times) \to H^2(\mathrm{Gal}(LM/L), (LM)^\times),$$

where the second morphism is induced by the $H := \mathrm{Gal}(M/U) \cong \mathrm{Gal}(LM/L)$-equivariant injection $M^\times \to (LM)^\times$. Actually, this follows easily by translating the maps in terms of cochains. Recall as in the proof of Theorem 2.5.7 for a fixed generator σ of $G := \mathrm{Gal}(M/K)$, we have an associated exact sequence of G-modules

$$0 \to M \to \mathrm{Ind}_{\{1\}}^G M \to \mathrm{Ind}_{\{1\}}^G M \to M \to 0 \tag{3.5}$$

that induces isomorphisms

$$\iota_\sigma : H_T^i(G, M^\times) \xrightarrow{\sim} H_T^{i+2}(G, M^\times). \tag{3.6}$$

As $\mathrm{Ind}_{\{1\}}^G M$ is also induced module for H, we deduce from (3.5) also isomorphisms

$$\iota_\sigma : H_T^i(H, M^\times) \xrightarrow{\sim} H_T^{i+2}(G, M^\times) \tag{3.7}$$

that are compatible with (3.6) and the restriction maps. More generally, for any H-modules N, tensoring the sequence (3.5) by N induces an exact sequence in $\mathcal{M}\mathrm{od}_H$

$$0 \to N \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} N \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} N \to N \to 0 \tag{3.8}$$

where $\mathbb{Z}[G] \otimes_{\mathbb{Z}} N$ is equipped with the diagonal H-action. Using the isomorphism $\mathbb{Z}[G] \cong \oplus_{g \in H\backslash G} \mathbb{Z}[H] e_g$, we deduce by the claim in the proof of Theorem 2.5.7 that $\mathbb{Z}[G] \otimes_{\mathbb{Z}} N$ is isomorphic to an induced H-module, and hence the sequence (3.8) induces

$$\iota_\sigma : H_T^i(H, N) \xrightarrow{\sim} H_T^{i+2}(H, N)$$

(that gives the maps (3.7) when $N \cong M^\times$). It is clear that the isomorphisms are functorial on N. In particular, the following diagram commutes

$$\begin{array}{ccc} H_T^0(H, M^\times) & \longrightarrow & H_T^0(H, (LM)^\times) \\ \iota_\sigma \downarrow & & \iota_\sigma \downarrow \\ H_T^2(H, M^\times) & \longrightarrow & H_T^2(H, (LM)^\times) \end{array}.$$

We finally deduce a commutative diagram

$$\begin{array}{ccccc} H_T^0(G, M^\times) & \xrightarrow{\text{Res}} & H_T^0(H, M^\times) & \longrightarrow & H_T^0(H, (LM)^\times) \\ \iota_\sigma \downarrow \wr & & \iota_\sigma \downarrow \wr & & \iota_\sigma \downarrow \wr \\ H^2(G, M^\times) & \xrightarrow{\text{Res}} & H^2(H, M^\times) & \longrightarrow & H^2(H, (LM)^\times) \end{array}.$$

It is sufficient to show the top composition is zero. By Proposition 3.2.4, we only need to show it sends ϖ_K to 1. Let ϖ_L be a uniformizer of L, thus $\varpi_K = \varpi_L^e \alpha$ for $\alpha \in \mathcal{O}_L^\times$. The composition sends ϖ_K to $\varpi_L^e \alpha$. However, as LM is unramified of degree e over L, we see (again) by Proposition 3.2.4: $\varpi_L^e \alpha \equiv 1 \in H_T^0(H, (LM)^\times)$. This concludes the proof . □

Corollary 3.2.10. *Let L/K be a finite Galois extension, taking cup-product with a generator of $H^2(\mathrm{Gal}(L/K), L^\times)$ induces a canonical isomorphism*

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} K^\times / N_{L/K}(L^\times).$$

Corollary 3.2.11. *Let L/K be a finite Galois extension, and M be the maximal abelian subextension of L/K. Then $N_{L/K}(L^\times) = N_{M/K}(M^\times)$*

Proof. It is clear $N_{L/K}(L^\times) \subset N_{M/K}(M^\times)$. By the above corollary, we have $K^\times / N_{L/K}(L^\times) \cong K^\times / N_{M/K}(M^\times)$. The corollary follows. □

We now study the compatibility of isomorphisms $H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathbb{Z}/[L : K] \cong (1/[L : K])\mathbb{Z}/\mathbb{Z}$. We begin with one (more!) easy fact on group cohomology.

Lemma 3.2.12. *Let G be finite group, there are canonical isomorphisms $H^i(G, \mathbb{Q}/\mathbb{Z}) \to H^{i+1}(G, \mathbb{Z})$ for $i \geq 1$.*

Proof. Consider the exact sequence of (trivial) G-modules:

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0. \tag{3.9}$$

By the same argument as in the proof of Corollary 2.2.12 (using restriction and corestriction), we see $H^i(G, \mathbb{Q}) = 0$ for all $i > 0$. The lemma follows (by looking at the long exact sequence induced by (3.9)). □

Remark 3.2.13. *For a finite abelian group G, $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is called the Pontryagain dual of G.*

Assume first we have unramified extensions $M \supset L \supset K$. We have a commutative diagram (where the top objects are the $\mathrm{Gal}(M/L)$-invariant sub objects of the bottom ones)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_L^\times & \longrightarrow & L^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathcal{O}_M^\times & \longrightarrow & M^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}.$$

We deduce (using also the above lemma)

$$\begin{array}{ccccc} H^2(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\sim} & H^2(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\sim} & H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \\ \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} \\ H^2(\mathrm{Gal}(M/K), M^\times) & \xrightarrow{\sim} & H^2(\mathrm{Gal}(M/K), \mathbb{Z}) & \xrightarrow{\sim} & H^1(\mathrm{Gal}(M/K), \mathbb{Q}/\mathbb{Z}) \end{array} \tag{3.10}$$

We fix a Frobenius $\sigma_K \in \mathrm{Gal}(K^{\mathrm{unr}}/K)$ (such that $\sigma_K|_{L'}$ is a generator of $\mathrm{Gal}(L'/K)$ for any finite unramified extension L'/K). Then σ_K induces an isomorphism

$$\iota_{\sigma_K} : H^1(\mathrm{Gal}(L'/K), \mathbb{Q}/Z) \xrightarrow{\sim} \mathbb{Q}/Z, \ \chi \mapsto \chi(\sigma_K|_{L'}),$$

for any finite unramified extension L'/K. Moreover, it is easy to see such isomorphisms (with L' varying) are compatible with inflations. In particular, the following diagram commutes

$$\begin{array}{ccc} H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\iota_{\sigma_K}} & \mathbb{Q}/Z \\ \downarrow{\scriptstyle \inf} & & \| \\ H^1(\mathrm{Gal}(M/K), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\iota_{\sigma_K}} & \mathbb{Q}/Z \end{array}. \tag{3.11}$$

For L' finite unramified over K, denote by

$$\mathrm{inv}_{L'/K} : H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\sim} H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\iota_{\sigma_K}} \mathbb{Q}/Z.$$

Note $\mathrm{Im}(\mathrm{inv}_{L'/K}) = (1/[L' : K])\mathbb{Z}/\mathbb{Z}$. By (3.10)(3.11), we see

$$\begin{array}{ccc} H^2(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\mathrm{inv}_{L/K}} & \mathbb{Q}/Z \\ \downarrow{\scriptstyle \inf} & & \| \\ H^2(\mathrm{Gal}(M/K), M^\times) & \xrightarrow{\mathrm{inv}_{M/K}} & \mathbb{Q}/Z \end{array}.$$

We deduce hence a map $\mathrm{inv}_{K^{\mathrm{ur}}/K} : H^2(\mathrm{Gal}(K^{\mathrm{ur}}/K), (K^{\mathrm{ur}})^\times) \to \mathbb{Q}/Z$. As $\mathrm{inv}_{L'/K}$ is injective and has image equal to $(1/[L' : K])\mathbb{Z}/\mathbb{Z}$, we easily deduce $\mathrm{inv}_{K^{ur}/K}$ is bijective. By the proof of Theorem 3.2.9, we have $H^2(\mathrm{Gal}(K^{\mathrm{ur}}/K), (K^{\mathrm{ur}})^\times) \xrightarrow{\sim} H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$. We finally deduce:

Theorem 3.2.14. *There is a canonical isomorphism (depending on the choice of Frobenius σ_K):*

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Proposition 3.2.15. *Let L be a finite extension of K, $\sigma_L := \sigma_K^{[k_L:k]}$, then (*$\mathrm{inv}_L$ *is defined with respect to σ_L)*

$$\mathrm{inv}_L \circ \mathrm{Res} = [L:K]\,\mathrm{inv}_K : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Proof. The unramified case is clear. As both sides of the equality respect the composition of finite extensions, it suffices to consider the case where L is totally ramified over K. Let $e := [L:K]$, $M \supset L$ be a finite Galois extension over K (hence M is also Galois over L), $d := [M:K]$ (hence $e|d$). It suffices to show $\mathrm{inv}_{M/L} \circ \mathrm{Res} = [L:K]\,\mathrm{inv}_{M/K} : H^2(\mathrm{Gal}(M/K), M^\times) \to \mathbb{Q}/\mathbb{Z}$. Let M_0 be the unramified extension of K of degree d. As L is totally ramified over K, we see LM_0 is unramified over L of degree d. Let $L_1 \subset LM_0$ be the unramified extension of L of degree $d/e = [M:L]$. It is not difficult to see the following diagram commutes

$$\begin{array}{ccc} H^2(\mathrm{Gal}(M/K), M^\times) & \xrightarrow{\mathrm{inf}} & H^2(\mathrm{Gal}(MM_0/K), (MM_0)^\times) \\ {\scriptstyle\mathrm{Res}}\downarrow & & {\scriptstyle\mathrm{Res}}\downarrow \\ H^2(\mathrm{Gal}(M/L), M^\times) & \xrightarrow{\mathrm{inf}} & H^2(\mathrm{Gal}(MM_0/L), (MM_0)^\times) \end{array}.$$

As the top (resp. bottom) horizontal morphism factors through an (fixed) isomorphism $H^2(\mathrm{Gal}(M/K), M^\times) \xrightarrow{\sim} H^2(\mathrm{Gal}(M_0/K), M_0^\times)$ (resp. $H^2(\mathrm{Gal}(M/L), M^\times) \xrightarrow{\sim} H^2(\mathrm{Gal}(L_1/L), L_1^\times)$), it is suffices to show the composition

$$H^2(\mathrm{Gal}(M_0/K), M_0^\times) \hookrightarrow H^2(\mathrm{Gal}(MM_0/K), (MM_0)^\times) \xrightarrow{\mathrm{Res}} H^2(\mathrm{Gal}(MM_0/L), (MM_0)^\times) \xrightarrow{\mathrm{inv}_{MM_0/L}} \mathbb{Q}/\mathbb{Z}$$

is equal to $[L:K]$ times the composition

$$H^2(\mathrm{Gal}(L_1/L), L_1^\times) \xrightarrow{\mathrm{inf}} H^2(\mathrm{Gal}(LM_0/L), (LM_0)^\times) \xrightarrow{\mathrm{inf}} H^2(\mathrm{Gal}(MM_0/L), (MM_0)^\times) \xrightarrow{\mathrm{inv}_{MM_0/L}} \mathbb{Q}/\mathbb{Z}.$$

It is straightforward to check the following diagram commutes

$$\begin{array}{ccc} H^2(\mathrm{Gal}(M_0/K), M_0^\times) & \xrightarrow{\mathrm{inf}} & H^2(\mathrm{Gal}(MM_0/K), (MM_0)^\times) \\ {\scriptstyle\iota}\downarrow & & {\scriptstyle\mathrm{Res}}\downarrow \\ H^2(\mathrm{Gal}(LM_0/K), (LM_0)^\times) & \xrightarrow{\mathrm{inf}} & H^2(\mathrm{Gal}(MM_0/L), (MM_0)^\times) \end{array}$$

where ι is induced by the $\mathrm{Gal}(M_0/K) \cong \mathrm{Gal}(LM_0/K)$-equivariant injection $M_0^\times \hookrightarrow (LM_0)^\times$. We finally reduce to show $[L:K]\,\mathrm{inv}_{M_0/K} = \mathrm{inv}_{LM_0/L} \circ \iota$. However, this follows from the following commutative diagram (by our choice of σ_L):

$$\begin{array}{ccccccc} H^2(\mathrm{Gal}(M_0/K), M_0^\times) & \longrightarrow & H^2(\mathrm{Gal}(M_0/K), \mathbb{Z}) & \longrightarrow & H^1(\mathrm{Gal}(M_0/K), \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle\iota}\downarrow & & {\scriptstyle[L:K]}\downarrow & & {\scriptstyle[L:K]}\downarrow & & \downarrow \\ H^2(\mathrm{Gal}(LM_0/L), (LM_0)^\times) & \longrightarrow & H^2(\mathrm{Gal}(LM_0/L), \mathbb{Z}) & \longrightarrow & H^1(\mathrm{Gal}(LM_0/L), \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

This concludes the proof. □

3.3 Local reciprocity

We fix a Frobinus element σ_K as in the previous section. Correspondingly, we fix an isomorphism

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

hence fix isomorphisms $\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\sim} (1/[L:K])\mathbb{Z}/\mathbb{Z}$ for any finite Galois extension L of K, we put $\phi_{L/K} := \mathrm{inv}_{L/K}^{-1}(\frac{1}{[L:K]})$. Denote by $\rho_{L/K} : K^\times \to K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$ the morphism induced by (3.2.10), i.e. the inverse (of the second morphism) is given by cup-product with $\phi_{L/K}$. In this section, we show $\{\rho_{L/K}\}$ (with L varying) can glue to a morphism $\rho_K : K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$. In particular, for abelian extensions $M \supset L \supset K$, we show $\rho_{M/K}(a)|_L = \rho_{L/K}(a)$.

Example 3.3.1. *We may try to understand $\rho_{L/K}$ in the case L/K is unramified. In this case, $K^\times/N_{L/K}(L^\times)$ is generated by an arbitrary uniformizer ϖ_K of K, and we want to describe the element $\rho_{L/K}(\varpi_K)$. We have a commutative diagram*

$$\begin{array}{ccccc}
H_T^{-2}(\mathrm{Gal}(L/K),\mathbb{Z})\times & H_T^2(\mathrm{Gal}(L/K),L^\times) & \xrightarrow{\cup} & H_T^0(\mathrm{Gal}(L/K),L^\times) \\
\| & \sim\downarrow & & \sim\downarrow \\
H_T^{-2}(\mathrm{Gal}(L/K),\mathbb{Z})\times & H_T^2(\mathrm{Gal}(L/K),\mathbb{Z}) & \xrightarrow{\cup} & H_T^0(\mathrm{Gal}(L/K),\mathbb{Z}) \\
\downarrow & \delta^{-1}\downarrow\sim & & \delta^{-1}\downarrow\sim \\
H_T^{-2}(\mathrm{Gal}(L/K),\mathbb{Z})\times & H_T^1(\mathrm{Gal}(L/K),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\cup} & H_T^{-1}(\mathrm{Gal}(L/K),\mathbb{Q}/\mathbb{Z}) \\
 & \sim\downarrow \chi\mapsto\chi(\sigma_K) & & \sim\downarrow \\
 & (1/[L:K])\mathbb{Z}/\mathbb{Z} & & (1/[L:K])\mathbb{Z}/\mathbb{Z}
\end{array} \quad . \tag{3.12}$$

The composition of the second column is equal to $\mathrm{inv}_{L/K}$, and the composition of the third column sends ϖ_K to $1/[L:K]$. Let $\chi \in H_T^1(\mathrm{Gal}(L/K), \mathbb{Q}/Z)$ be the element corresponding to $\phi_{L/K}$, so $\chi(\sigma_K) = 1/[L:K]$. As $\rho_{L/K}(\varpi_K) \cup \phi_{L/K} = \varpi_K$, we see $\rho_{L/K}(\varpi_K) \cup \chi = 1/[L:K]$. If $\rho_{L/K}(\varpi_K) \cup \chi = \chi(\rho_{L/K}(\varpi_K))$, one can deduce $\rho_{L/K}(\varpi_K) = \sigma_K$. In summary, we need to understand the cup-product in the third row.

Lemma 3.3.2. *Let G be a finite group, $\sigma \in G$ with $\bar{\sigma}$ its image in $G^{\mathrm{ab}} \cong H_T^{-2}(G, \mathbb{Z})$, and $\chi : G \to \mathbb{Q}/\mathbb{Z} \in H^1(G, \mathbb{Q}/\mathbb{Z})$. Then $\bar{\sigma} \cup \chi = \chi(\sigma) \in (\frac{1}{|G|}\mathbb{Z})/\mathbb{Z} \cong H_T^{-1}(G, \mathbb{Q}/\mathbb{Z})$.*

Proof. Applying $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ to the exact sequence of G-modules (that splits as abelian groups)

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0, \tag{3.13}$$

we obtain an exact sequence of G-modules

$$0 \to \mathbb{Q}/\mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z}) \to 0, \tag{3.14}$$

where G acts on $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ via $(gf)(m) = f(g^{-1}m)$ for a left G-module M. Both of the exact sequences split as abelian groups, we deduce hence exact sequences of G-modules (with diagonal G-action):

$$0 \to I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/Z \to 0, \tag{3.15}$$

$$0 \to I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) \to I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z}) \to 0. \tag{3.16}$$

We claim $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z})$ is an induced G-module. Indeed, by definition, we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Ind}_{\{1\}}^{G} \mathbb{Q}/\mathbb{Z}$. By the same argument as in the proof of Theorem **??**, we see $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Q}/Z$, $I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z})$ are all induced G-modules.

We have commutative diagrams (where we use δ_1 (resp. δ_2) to denote the δ-maps induced by (3.13) and (3.15) (resp. by (3.14) and (3.16)):

$$\begin{array}{ccccc}
H_T^{-2}(G, \mathbb{Z}) & \times H^1(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\cup} & H_T^{-1}(G, \mathbb{Q}/Z) \\
\delta_1 \downarrow \wr & \| & & \delta_1 \downarrow \wr \\
H_T^{-1}(G, I_G) & \times H^1(G, \mathbb{Q}/Z) & \xrightarrow{\cup} & H_T^{0}(G, I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})
\end{array}$$

$$\begin{array}{ccccc}
H_T^{-1}(G, I_G) \times & H_T^{0}\big(G, \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z})\big) & \xrightarrow{\cup} & H_T^{-1}\big(G, I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z})\big) \\
\| & \delta_2 \downarrow \wr & & \delta_2 \downarrow \wr \\
H_T^{-1}(G, I_G) \times & H_T^{1}(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{(-1)\cup} & H_T^{-1}(G, I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})
\end{array}$$

Let $f \in H_T^0(G, \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z}))$ such that $\delta_2(f) = \chi$, then

$$\delta_1(\bar{\sigma} \cup \chi) = \delta_1(\bar{\sigma}) \cup \chi = \delta_1(\bar{\sigma}) \cup \delta_2(f) = (-1)\delta_2(\delta_1(\bar{\sigma}) \cup f).$$

Recall we have $\delta_1(\bar{\sigma}) = e_\sigma - 1$. We can also directly check f satisfies $f(e_\tau - 1) = \chi(\tau)$ for $\tau \in G$. Denote by j the natural morphism $H_T^{-1}(G, I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z})) \to H_T^{-1}(G, \mathbb{Q}/Z)$ induced by the G-equivariant morphism $I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$, $a \otimes \alpha \mapsto \alpha(a)$. Then we have $j(\delta_1(\bar{\sigma} \cup f) = j((e_\sigma - 1) \otimes f) = f(e_\sigma - 1) = \chi(\bar{\sigma})$. It then suffices to show $\delta_1 \circ j = \delta_2$. One can check the following diagram commutes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} & \longrightarrow & I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) & \longrightarrow & I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & 0 \\
 & & \| & & \theta \downarrow & & j \downarrow & & \\
0 & \longrightarrow & I_G \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} & \longrightarrow & \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0,
\end{array}$$

where θ is given by $I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}) \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$, $\alpha \otimes f \mapsto \alpha \otimes f(\alpha)$. We deduce hence $\delta_1 \circ j = \delta_2$. This concludes the proof. □

By the lemma and the discussions in Example 3.3.1, we have

Corollary 3.3.3. *Suppose L is finite unramified over K, then $\rho_{L/K}(\varpi_K) = \sigma_K$.*

For general case, we have:

Proposition 3.3.4. *Let L be a finite Galois extension of K, $\chi \in \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z} \in H^1_T(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2_T(\mathrm{Gal}(L/K), \mathbb{Z})$, then*

$$\mathrm{inv}_{L/K}(a \cup \delta(\chi)) = \chi(\rho_{L/K}(a)) \in \mathbb{Q}/\mathbb{Z}.$$

for all $a \in K^\times$.

Proof. Denote by $d := [L : K]$. Recall $\phi_{L/K} \in H^2(\mathrm{Gal}(L/K), L^\times)$ satisfies $\mathrm{inv}_{L/K}(\phi_{L/K}) = \frac{1}{d}$. We have by Theorem 2.6.8 and Proposition 2.6.10 a commutative diagram:

$$\begin{array}{ccccccc}
H^0_T(\mathrm{Gal}(L/K), L^\times) \times & H^2_T(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\cup} & H^2_T(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\mathrm{inv}_{L/K}} & (1/d)\mathbb{Z}/\mathbb{Z} \\
{\scriptstyle \cup\phi_{L/K}}\uparrow & \| & & {\scriptstyle \cup\phi_{L/K}}\uparrow & & {\scriptstyle \frac{1}{d}}\uparrow \\
H^{-2}_T(\mathrm{Gal}(L/K), \mathbb{Z}) \times & H^2_T(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\cup} & H^0_T(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z}/d\mathbb{Z} \\
\| & {\scriptstyle \delta}\uparrow{\scriptstyle \sim} & & {\scriptstyle \delta}\uparrow{\scriptstyle \sim} & & {\scriptstyle d}\uparrow \\
H^{-2}_T(\mathrm{Gal}(L/K), \mathbb{Z}) \times & H^1_T(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\cup} & H^{-1}_T(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & (1/d)\mathbb{Z}/\mathbb{Z}
\end{array} . \tag{3.17}$$

We can now calculate:

$$\begin{aligned}
\mathrm{inv}_{L/K}(a \cup \delta(\chi)) = \mathrm{inv}_{L/K}(\phi_{L/K} \cup \rho_{L/K}(a) \cup \delta(\chi)) &= \mathrm{inv}_{L/K}(\phi_{L/K} \cup (\delta(\rho_{L/K}(a) \cup \chi))) \\
= \mathrm{inv}_{L/K}\left(\phi_{L/K} \cup \delta(\chi(\rho_{L/K}(a)))\right) &= \mathrm{inv}_{L/K}\left((d\chi(\rho_{L/K}(a)))\phi_{L/K}\right) \\
&= (d\chi(\rho_{L/K}(a)))\,\mathrm{inv}_{L/K}(\phi) = \chi(\rho_{L/K}(a)),
\end{aligned}$$

where the first two equalities follow from standard properties of cup-product, the third equality follows from the previous lemma, the fourth uses the canonical isomorphisms $H^{-1}_T(\mathrm{Gal}(L/K), \mathbb{Q}/Z) \cong \frac{1}{d}\mathbb{Z}/\mathbb{Z}$, $H^0_T(\mathrm{Gal}(L/K), \mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$ and the right bottom corner in (3.17), the last equality uses the fact $\mathrm{inv}_{L/K}(\phi_{L/K}) = 1/d$. The proposition follows. ☐

Corollary 3.3.5. *Let $M \supset L \supset K$ be finite abelian extensions, then $\rho_{M/K}(a)|_L = \rho_{L/K}(a)$ for all $a \in K^\times$.*

Proof. By Pontryagain duality, it suffices to show for any $\chi \in H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$, we have $\chi(\rho_{L/K}(a)) = \chi(\rho_{M/K}(a)|_L)$. By the previous proposition, we have $\chi(\rho_{L/K}(a)) = \mathrm{inv}_{L/K}(a \cup \delta(\chi))$. By definition, we have $\mathrm{inv}_{M/K} \circ \inf = \mathrm{inv}_{L/K}$. We have a commutative diagram

$$\begin{array}{ccccc}
H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \times & H^0(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\cup} & H^2(\mathrm{Gal}(L/K), L^\times) \\
{\scriptstyle \inf}\downarrow & {\scriptstyle \inf}\downarrow & & {\scriptstyle \inf}\downarrow \\
H^2(\mathrm{Gal}(M/K), \mathbb{Z}) \times & H^0(\mathrm{Gal}(M/K), M^\times) & \xrightarrow{\cup} & H^2(\mathrm{Gal}(M/K), M^\times)
\end{array}$$

and note taht the middle inflation map is the identity map on $K^\times$. We have thus $\mathrm{inv}_{L/K}(a \cup \delta(\chi)) = \mathrm{inv}_{M/K}(\inf(a \cup \delta(\chi))) = \mathrm{inv}_{M/K}(a \cup \delta(\inf(\chi))) = (\inf(\chi))(\rho_{M/K}(a)) = \chi(\rho_{M/K}(a)|L)$. The corollary follows. ☐

Corollary 3.3.6. *There exists a homomorphism (called the local Artin map)*

$$\rho_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following properties:

(a) for any uniformizer $\varpi \in K^\times$, and any finite unramified extension L over K, $\rho_K(\varpi)|_L = \sigma_K$,

(b) for any finite abelian extension L of K, $N_{L/K}(L^\times)$ is contained in the kernel $a \mapsto \rho_K(a)$, and ρ_K induces an isomorphism

$$K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Next we show the uniqueness of ρ_K and that any compact open subgroup of $K^\times$ is a norm group. Recall by Lubin-Tate theory, we have constructed a continuous morphism

$$\rho_{\mathrm{LT}} : K^\times \to \mathrm{Gal}(K_\varpi K^{\mathrm{ur}}/K)$$

that satisfies that $\rho_{\mathrm{LT}}(\varpi)$ fixes K_ϖ and that $\rho_{\mathrm{LT}}(\varpi)$ is equal to σ_K on K^{ur}, $\rho_{\mathrm{LT}}(1+\varpi^n\mathcal{O}_K) = 1$ on $K_{\varpi,n}$. Recall also $\varpi \in N_{K_{\varpi,n}/K}(K_{\varpi,n}^\times)$ for all n.

Lemma 3.3.7. *For $a \in K^\times$, $\rho_K(a)|_{K_\varpi K^{\mathrm{ur}}} = \rho_{\mathrm{LT}}(a)$.*

Proof. It suffices to show the equality for all uniformizers ϖ' of K (since they generate $K^\times$). Recall we have $\rho_{\mathrm{LT}}(\varpi') = \begin{cases} \mathrm{id} & \text{on } K_{\varpi'} \\ \sigma_K & \text{on } K^{\mathrm{ur}} \end{cases}$. As $\varpi' \in N_{K_{\varpi',n}/K}K_{\varpi',n}^\times$ for all n, $\rho_K\varpi') = \mathrm{id}$ on $K_{\varpi'}$. It is clear that $\rho_K\varpi') = \sigma_K$ on K^{ur}. The lemma follows. □

Theorem 3.3.8. *(1) We have $K_\varpi K^{\mathrm{ur}} = K^{\mathrm{ab}}$, and ρ_K is unique satisfying the given properties in Corollary 3.3.6.*

(2) Any open subgroup of finite index of $K^\times$ is a norm group.

Proof. We put $K_{n,m} := K_{\varpi,n}K_m^{\mathrm{ur}}$, where K_m^{ur} denotes the unramified extension of K of degree m. We see $(1+\varpi^n\mathcal{O}_K)\langle\varpi^m\rangle \subset K^\times$ fixes $K_{n,m}$ (via $\phi = \rho_{\mathrm{LT}}$). Indeed, $(1+\varpi^n\mathcal{O}_K) \subset N_{K_m^{\mathrm{ur}}/K}((K_m^{\mathrm{ur}})^\times)$ hence fixes K_m^{ur}, and it also fixes $K_{\varpi,n}$ by Lubin-Tate theory; $\varpi^m \in N_{K_{n,m}/K}(K_{n,m}^\times)$ hence fixes $K_{n,m}$. We deduce hence $(1+\varpi^n\mathcal{O}_K)\langle\varpi^m\rangle \subset K^\times \subset N_{K_{n,m}/K}(K_{n,m}^\times)$. The map ρ_K induces hence a projection

$$K^\times/(1+\varpi^n\mathcal{O}_K)\langle\varpi^m\rangle \twoheadrightarrow \mathrm{Gal}(K_{n,m}/K)$$

that has to be an isomorphism by comparing the order of the both sides. For any finite abelian extension L of K, $N_{L/K}(L^\times)$ is open of finite index in $K^\times$. We deduce hence there exists m, n such that $(1+\varpi^n\mathcal{O}_K)\langle\varpi^m\rangle \subset N_{L/K}L^\times$. Let $L_{n,m}$ be the composition of L and $K_{n,m}$. The map ρ_K induces

$$K^\times/N_{L_{n,m}/K}(L_{n,m}^\times) \xrightarrow{\sim} \mathrm{Gal}(L_{n,m}/K).$$

For $a \in K^\times$, if $\rho_K(a)$ fixes L, then $a \in N_{L/K}(L^\times) \subset N_{K_{n,m}/K}(K_{n,m}^\times)$ hence $\rho_K(a)$ fixes $K_{n,m}$. This implies $L \subset K_{n,m}$. So $K_\varpi K^{\mathrm{ur}} = K^{\mathrm{ab}}$. The uniqueness of ρ_K then follows from Lemma 3.3.7.

For any open subgroup U of finite index in $K^\times$, there exists m, n such that $(1 + \varpi^n \mathcal{O}_K)\langle \varpi^m \rangle \subset U$. Using the isomorphism $\rho_K : K^\times/(1+\varpi^n\mathcal{O}_K)\langle\varpi^m\rangle \cong \mathrm{Gal}(K_{n,m}/K)$, we see there exists a subextension L of $K_{n,m}$ such that ρ_K induces $\mathrm{Gal}(L/K) \cong K^\times/U$, implying $U = N_{L/K}(L^\times)$. □

The following proposition gives the functoriality of the reciprocity law.

Proposition 3.3.9. *Let L be a finite extension of K. Then we have the following commutative diagrams (where ϕ_L sends uniformizers to $\sigma_L = \sigma_K^{[k_L:k]} \in \mathrm{Gal}(L^{\mathrm{unr}}/L)$):*

$$\begin{array}{ccc} L^\times & \xrightarrow{\phi_L} & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle r} \\ K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \end{array}$$

where r denotes the natural injection of restriction;

$$\begin{array}{ccc} K^\times & \longrightarrow & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle V_{L/K}} \\ L^\times & \longrightarrow & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \end{array}$$

where $V_{L/K}$ denotes the transfer map, j the natural injection;

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ \sigma(L)^\times & \longrightarrow & \mathrm{Gal}(\overline{K}/\sigma(L))^{\mathrm{ab}} \end{array}$$

where $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and $\sigma^*(g) = \sigma g \sigma^{-1}$ for $g \in \mathrm{Gal}(\overline{K}/L)$.

Proof. We prove the first commutative diagram leaving the other two as exercises. Let $M \supset L$ be a finite Galois extension of K, it suffices to show the following diagram commutes

$$\begin{array}{ccc} L^\times/N_{M/L}(M^\times) & \xrightarrow{\rho_{M/L}} & \mathrm{Gal}(M/L)^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ K^\times/N_{M/K}(M^\times) & \xrightarrow{\rho_{M/K}} & \mathrm{Gal}(M/K)^{\mathrm{ab}} \end{array}.$$

However, this follows from the following commutative diagram

$$\begin{array}{ccc} H_T^{-2}(\mathrm{Gal}(M/L), \mathbb{Z}) & \xrightarrow{\cup\phi_{M/L}} & H_T^0(\mathrm{Gal}(M/L), M^\times) \\ {\scriptstyle \mathrm{Cor}}\downarrow & & \downarrow{\scriptstyle \mathrm{Cor}} \\ H_T^{-2}(\mathrm{Gal}(M/K), \mathbb{Z}) & \xrightarrow{\cup\phi_{M/K}} & H_T^0(\mathrm{Gal}(M/K), M^\times) \end{array}$$

where $\phi_{M/L} = \mathrm{Res}(\phi_{M/K})$ by Proposition 2.6.11 (2) and Lemma 2.4.9. □

Chapter 4

Class formation

4.1 Reciprocity maps

Definition 4.1.1. *Let K be a field. A class formation (A, inv) for K is a discrete $\mathrm{Gal}(\overline{K}/K)$-module A such that for all finite separable extension L/K, $H^1(\mathrm{Gal}(\overline{K}/K), A) = 0$, and*

$$\mathrm{inv}_L : H^2(\mathrm{Gal}(\overline{K}/L), A) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

satisfying $\mathrm{inv}_L \circ \mathrm{Res}_{E/L} = [L : E]\,\mathrm{inv}_E$ for any separable subextension E of L over K:

$$\begin{array}{ccc} H^2(\mathrm{Gal}(\overline{K}/E), A) & \xrightarrow{\mathrm{inv}_E} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle [L:E]} \\ H^2(\mathrm{Gal}(\overline{K}/L), A) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \end{array}.$$

Denote by $A_L := A^{\mathrm{Gal}(\overline{K}/L)}$. Suppose L/E is a moreover a finite Galois extension, it is easy to see the kernel of $H^2(\mathrm{Gal}(\overline{K}/E), A) \to H^2(\mathrm{Gal}(\overline{K}/L), A)$ is exactly $H^2(\mathrm{Gal}(L/K), A_L)$ (via restriction-inflation sequence), we deduce hence an isomorphism

$$\mathrm{inv}_{L/E} : H^2(\mathrm{Gal}(L/E), A_L) \xrightarrow{\sim} \frac{1}{[L : E]}\mathbb{Z}/\mathbb{Z}. \tag{4.1}$$

If we have finite Galois extensions $M \supset L \supset E$, we see the following diagram commutes:

$$\begin{array}{ccccc} H^1(\mathrm{Gal}(L/E), A_L) & \xrightarrow{\mathrm{inv}_{L/E}} & \frac{1}{[L:E]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{inf}}\downarrow & & & & \| \\ H^1(\mathrm{Gal}(M/E), A_E) & \xrightarrow{\mathrm{inv}_{M/E}} & \frac{1}{[M:E]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}.$$

For $L \supset E \supset K$, we have the restriction map $A_E \to A_L$, and we denote by $N_{L/E} : A_L \to A_E$ the corestriction map.

Example 4.1.2. *If K is a finite extension of $\mathbb{Q}_p$, we see $(K^\times, \mathrm{inv}_K)$ is a class formation.*

Let (A, inv) be a class formation. Let L/K be a finite Galois extension, $\alpha_{L/K} := \mathrm{inv}_{L/K}^{-1}(1/[L:K]) \in H^2(\mathrm{Gal}(L/K), A_L)$. By Tate's theorem, there is a canonical isomorphism

$$\theta_{L/K} : H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\cup \alpha_{L/K}} H_T^0(\mathrm{Gal}(L/K), A_L) \cong A_K/N_{L/K}A_L.$$

Denote by $\rho_{L/K} : A_K \twoheadrightarrow A_K/N_{L/K}A_L \xrightarrow{\theta_{L/K}^{-1}} \mathrm{Gal}(L/K)^{\mathrm{ab}}$. By exactly the same argument as in the proof of Proposition 3.3.4 (with $L^\times$ replaced by A_L), we deduce

Proposition 4.1.3. *Let L be a finite Galois extension of K, $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z} \in H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$, δ be the connecting homomorphism for the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ of (trivial) $\mathrm{Gal}(L/K)$-modules. Then we have*

$$\mathrm{inv}_{L/K}(a \cup \delta(\chi)) = \chi(\rho_{L/K}(a))$$

for all $a \in A_K$.

We deduce as in Corollary 3.3.5.

Corollary 4.1.4. *Let $L \subset M$ be finite Galois extensions of K, then $\rho_{M/K}(a)|_L = \rho_{L/K}(a)$ for all $a \in A_K$.*

We see the maps $\{\rho_{L/K}\}$ form a map $\rho_K : A_K \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, called the reciprocity map for K with respect to the class formation (A, inv):

Theorem 4.1.5 (Reciprocity law for class formations)**.** *Let K be a field and (A, inv) a class formation for K, and ρ_K the associated reciprocity map. For any finite Galois extension L/K, the composition ρ_K with restriction induces a surjective map $\rho_{L/K} : K^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$ with kernel $N_{L/K}L^\times$.*

Proposition 4.1.6. *Let (A, inv) be a class formation for K and let L be a finite separable extension of K. Then we have the following commutative diagrams:*

$$\begin{array}{ccc} A_L & \xrightarrow{\rho_L} & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle r} \\ A_K & \xrightarrow{\rho_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \end{array}$$

where r denotes the natural injection of restriction;

$$\begin{array}{ccc} A_K & \xrightarrow{\rho_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle V_{L/K}} \\ A_L & \xrightarrow{\rho_L} & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \end{array}$$

where $V_{L/K}$ denotes the transfer map, j the natural injection;

$$\begin{array}{ccc} A_L & \longrightarrow & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ \sigma(A_L) & \longrightarrow & \mathrm{Gal}(\overline{K}/\sigma(L))^{\mathrm{ab}} \end{array}$$

where $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and $\sigma^*(g) = \sigma g \sigma^{-1}$ for $g \in \mathrm{Gal}(\overline{K}/L)$.

4.2 Norm groups

Let (A, inv) be a class formation for K.

Definition 4.2.1. *A subgreoup $\mathscr{N}$ of A_K is called a norm group, if there exists a finite separable extension L over K such that $\mathscr{N} = N_{L/K}A_L := \mathscr{N}_L$.*

Lemma 4.2.2. *Let $M \supset L \supset K$ be finite separable extensions, then $\mathscr{N}_M \subset \mathscr{N}_L$.*

Lemma 4.2.3. *Let L/K be a finite separable extension of K, and let E be the maximal abelian extension of K in L, then $\mathscr{N}_L = \mathscr{N}_E$.*

Proof. It suffices to show $\mathscr{N}_E \subset \mathscr{N}_L$. Let $a \in \mathscr{N}_E$. Let M be a finite Galois extension of K containing L, $G := \mathrm{Gal}(M/K)$, $H := \mathrm{Gal}(M/L)$, and let M^{ab} be the maximal abelian extension of K in M (so $M^{\mathrm{ab}} \supset E$). We have $\rho_{M/K}(a)$ acts trivially on E. As E is maximal abelian over K, we see $[G,G]H = \mathrm{Gal}(M/E)$ and hence the morphism $H \hookrightarrow \mathrm{Gal}(M/E) \twoheadrightarrow \mathrm{Gal}(M^{ab}/E)$ is surjective. Note the composition factors through H^{ab}. In summary, for $\rho_{M/K}(a)$ there exists $\sigma \in H^{\mathrm{ab}}$ such that $\rho_{M/K}(a) = \sigma$. Let $b \in A_L$ such that $\sigma = \rho_{M/L}(b)$. By Proposition 4.1.6, we see $\rho_{M/K}(N_{L/K}(b)) = \rho_{M/K}(a)$. Hence there exists $c \in A_M$ such that $N_{L/K}(b) - a = N_{M/K}(c)$. So $a = N_{L/K}(b - N_{M/L}(c))$. The lemma follows. □

Remark 4.2.4. *Note the statement is stronger than Lemma 3.2.11.*

Corollary 4.2.5. *Every norm group $\mathscr{N}$ has finite index in A_K, with $[A_K : \mathscr{N}] \leq [L : K]$ for $\mathscr{N} = \mathscr{N}_L$, and the equality holds if and only if L/K is abelian.*

Proposition 4.2.6. *For any finite abelian extensions L, M of K, the followings hold.*

(1) $\mathscr{N}_L \cap \mathscr{N}_M = \mathscr{N}_{LM}$.

(2) $\mathscr{N}_L + \mathscr{N}_M = \mathscr{N}_{L\cap M}$.

(3) $\mathscr{N}_M \subset \mathscr{N}_L$ if and only if $L \subset M$.

(4) For any subgroup $\mathscr{N}$ of A_K containing $\mathscr{N}_L$, there exists an intermediate field E in L/K with $\mathscr{N} = \mathscr{N}_E$.

Proof. (1) $\supset$ is clear. We have

$$\begin{array}{ccc} A_K/\mathscr{N}_{LM} & \xrightarrow{\sim} & \mathrm{Gal}(LM/K) \\ \downarrow & & \downarrow \\ A_K/\mathscr{N}_L \times A_K/\mathscr{N}_M & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \end{array}$$

hence $\mathscr{N}_L \cap \mathscr{N}_M = \mathscr{N}_{LM}$.

(3) The "if" part is clear. If $\mathscr{N}_M \subset \mathscr{N}_L$, then $\mathscr{N}_{LM} = \mathscr{N}_M$ by (1). By reciprocity law, we see $LM = M$.

(4) Let $E := L^{\rho_{L/K}(\mathscr{N})}$. We have a commutative diagram

$$\begin{array}{ccc} A_E/N_{L/E}(A_L) & \xrightarrow[\sim]{\rho_{L/E}} & \mathrm{Gal}(L/E) \\ {\scriptstyle N_{E/K}}\downarrow & & \downarrow \\ A_K/N_{L/K}(A_L) & \xrightarrow[\sim]{\rho_{L/K}} & \mathrm{Gal}(L/K), \\ \uparrow & & \uparrow \\ \mathscr{N}/N_{L/K}(A_L) & \xrightarrow{\sim} & \mathrm{Gal}(L/E) \end{array}$$

and we deduce $N_{E/K}(A_E) = \mathscr{N}$.

(2) $\subset$ is clear. By (4), there exists an intermediate field E of L/K such that $\mathscr{N}_E = \mathscr{N}_L + \mathscr{N}_M$. As $\mathscr{N}_E \supset \mathscr{N}_M$, we see by (3) $E \subset M$ hence $E \subset L \cap M$ and $\mathscr{N}_E \supset \mathscr{N}_{L \cap M}$. □

Corollary 4.2.7. *For a norm subgroup $\mathscr{N}$ of A_K, there exists a unique finite abelian extension L/K such that $\mathscr{N} = \mathscr{N}_L$.*

For a finite separable extension L of K, we set $D_L = \ker \rho_L$.

Lemma 4.2.8. *Let L be a finite separable extension of K. We have*

$$D_L = \cap_M N_{M/L}(A_M),$$

where M runs through finite abelian (or separable) extensions of L.

Definition 4.2.9. *We say that a class formation (A, inv) for K is topological if each A_L is given an additional Hausdorff topology such that if L/K is Galois, A_L is a topological $\mathrm{Gal}(L/K)$-module, and for $M \subset L \subset K$, the topology on A_L coincides with the induced topology from A_M via $A_L \hookrightarrow A_M$, and moreover the following properties are satisfied:*

1. *the norm map $N_{M/L} : A_M \to A_L$ has closed image and compact kernel for each finite extension M/L of finite separable extensions of K,*

2. *for each prime p, there exists a finite separable extension K_p over K such that for all finite separable extensions L of K_p, the kernel of $\phi_p : A_L \to A_L$, $a \mapsto pa$ is compact and the image of ϕ_p contains D_L,*

3. *for each finite separable extension L of K there exists a compact subgroup U_L of A_L such that every closed subgroup of finite index in A_L that contains U_L is a norm group.*

Remark 4.2.10. *Let L be a finite separable extension of K, and M be a finite Galois extension of K containing L. Then A_M is a topological $\mathrm{Gal}(M/K)$-module, and we deduce $A_K \cong A_M^{\mathrm{Gal}(M/K)}$ is closed in $A_L \cong A_M^{\mathrm{Gal}(M/L)}$, that is closed in A_M. The property 1 implies D_K is closed in A_K. The property 2 implies $\ker[\phi_p : A_K \to A_K]$ is compact.*

Example 4.2.11. *Let K be a finite extension of $\mathbb{Q}_p$, we show $(\overline{K}^\times, \mathrm{inv})$ is a topological class formation where $\overline{K}^\times$ is equipped with the p-adic topology. Condition (1) is clear. For (3), one can take $U_L := \mathcal{O}_L^\times$, then (3) follows by considering unramified extensions of L. For (2), the map $L^\times \to L^\times$, $x \mapsto x^p$ has compact kernel. As we knew $D_L = 1$, the second part of (2) is also clear (recalling our proof of $D_L = 1$ used the Lubin-Tate theory). But in fact, the second part can also follow from (the much eaiser) Kummer theory, that we leave as an exercise.*

Theorem 4.2.12. *Suppose (A, inv) is a topological class formation for K, then a subgroup $\mathscr{M}$ of A_K is a norm group if and only if $\mathscr{M}$ is closed of finite index in A_K.*

Corollary 4.2.13. *Let (A, inv) be a topological class formation for K, then there is a canonical isomorphism (induced by the reciprocity map):*

$$\rho_K : \widehat{A_K} := \varprojlim_{\mathscr{M}} A_K/\mathscr{M} \xrightarrow{\sim} \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}},$$

where $\mathscr{M}$ runs through open subgroups of finite index of A_K.

We prove the theorem in the rest of the section. We will frequently use the finite intersection property of compact spaces: let X be a compact space, $\{Z_i\}$ be a set of closed subsets, if any finite Z_i have non-empty intersection, then $\cap Z_i \neq \emptyset$. Now let (A, inv) be a topological class formation, we first prove:

Lemma 4.2.14. *Let L be a finite separable extension of K, then $N_{L/K} D_L = D_K$.*

Proof. It is clear that $N_{L/K} D_L \subset D_K$. Let $a \in D_K$, and consider $N_{L/K}^{-1}(a)$, that is a compact subset of A_L by Property 1. For any finite separable extension M/L, as $a \in N_{M/K}(A_M)$, we deduce $N_{M/L}(A_M) \cap N_{L/K}^{-1}(a) \neq \emptyset$. Using the finite intersection property (and Proposition **??** (1)), we deduce $\emptyset \neq \cap_M (N_{M/L}(A_M) \cap N_{L/K}^{-1}(a)) = D_L \cap N_{L/K}^{-1}(a)$. The lemma follows. □

Proposition 4.2.15. *The group D_K is divisible, and $D_K = \cap_n n A_K$.*

Proof. To show D_K is divisible, it suffices to show $\phi_p : D_K \to D_K$, $x \mapsto px$ is surjective for any prime number p. For any $x \in D_K$, $\phi_p^{-1}(x)$ is closed hence compact. For any finite separable extension L/K, there exists $y \in D_L$ such that $N_{L/K}(y) = x$. Enlarging L, we assume L contains K_p, by property 2, we have $y \in pA_L$ hence $\phi_p^{-1}(x) \cap N_{L/K}(A_L) \neq \emptyset$ (for any finite separable L over K_p). Using finite intersection property, we deduce $\phi_p^{-1}(x) \cap D_K \neq \emptyset$, in other words, ϕ_p is surjective. We have $D_K = \cap_n n D_K \subset \cap_n n A_K$. If $x \in \cap_n n A_K$, for any finite separable M/K, $x = N_{M/K}(1/[M:K]x)$ hence $x \in D_K$. □

Proof of Theorem 4.2.12. The "only if" part follows from the reciprocity law ($\Rightarrow$ finite index) and the property 1. Let $\mathscr{M}$ be a closed subgroup of finite index in A_K. To show it is a norm group, by Proposition 4.2.6 (4) it suffices to show it contains a norm group. First by the precedent proposition, we have $\mathscr{M} \supset D_K$ as $\mathscr{M} \supset nA_K$ using $\mathscr{M}$ has finite index. Now we (finally) use the property 3. Since $\mathscr{M} + U_K$ is obviously of finite index and open hence closed, $\mathscr{M} + U_K$ is a norm group. We first claim there exists a norm group $\mathscr{N}$ such that $\mathscr{N} \cap U_K \subset \mathscr{M}$. Indeed, if not, $\emptyset \neq (\mathscr{N} \cap U_K) \cap (A_K \setminus \mathscr{M}) = (U_K \cap (A_K \setminus \mathscr{M})) \cap \mathscr{N}$ for any $\mathscr{N}$, which implies, using finite intersection property for the compact set $U_K \cap (A_K \setminus \mathscr{M})$, $(U_K \cap (A_K \setminus \mathscr{M})) \cap D_K \neq \emptyset$ contradicting $D_K \subset \mathscr{M}$. Let $\mathscr{N}$ be a norm group such that $\mathscr{N} \cap U_K \subset \mathscr{M}$. Then $\mathscr{M} \cap \mathscr{N}$ is also closed of finite index, implying $\mathscr{M} \cap \mathscr{N} + U_K \supset U_K$ is closed of finite index hence a norm group. We can check $\mathscr{N} \cap (\mathscr{M} \cap \mathscr{N} + U_K) \subset \mathscr{M}$ (for $x = y + z$ with $x \in \mathscr{N}$, $y \in \mathscr{M} \cap \mathscr{N}$, $z \in U_K$, $z = x - y \in U_K \cap \mathscr{N} \subset \mathscr{M}$, hence $y + z \in \mathscr{M}$). So $\mathscr{M}$ is a norm group. $\square$

Chapter 5

Global class field theory

5.1 Adeles and Ideles (revisited)

Let K be a finite extension of $\mathbb{Q}$, $\mathbb{A}_K := \prod'_v K_v$ be the ring of adeles (where v run though the places of K and $\prod'$ denotes the restricted product with respect to $\{\mathcal{O}_{K_v}\}_{v\nmid\infty}$), and $I_K = \prod'_v K_v^\times$ be the group of ideles. Let S_∞ be the set of archimedean places of K. For a finite set $S \supset S_\infty$ of places of K, put $\mathbb{A}_{K,S} := \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v}$, and $I_{K,S} := \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times$. Recall that $(\mathbb{A}_K, +)$ and $(I_K, \times)$ are locally compact groups, and $\{\mathbb{A}_{K,S}\}$ (resp. $\{I_{K,S}\}$) form a topological basis of $\mathbb{A}_K$ (resp. I_K).

For a place v of K, we normalize the associated valuation $|\cdot|_v$ on K_v in the following way:

$$|\alpha|_v = \begin{cases} |\alpha| & K_v = \mathbb{R}, \\ |\alpha|^2 & K_v = \mathbb{C}, \\ q_v^{-\operatorname{ord}_v(\alpha)} & v \nmid \infty \end{cases}$$

where q_v is the cardinality of the residue field k_v of K_v and $\operatorname{ord}_v : K_v \to \mathbb{Z}$ is the additive valuation normalized by sending uniformizers to 1. We then deduce a valuation on I_K (noting $|\alpha_v|_v = 1$ for all but finitely many v. :

$$|\cdot|_{I_K} : I_K \longrightarrow \mathbb{R}_{>0},\ (\alpha_v) \mapsto \prod_v |\alpha_v|_v.$$

Let $I_K^1 := \{\alpha \in I_K \mid |\alpha|_{I_K} = 1\}$, which is a closed subgroup in I_K. Recall

Fact 5.1.1. *(1) $K^\times \hookrightarrow I_K$ is contained in I_K^1.*

(2) The image of $K^\times$ in I_K^1 is discrete and $I_K^1/K^\times$ is compact Hausdorff.

Let J_K denote the group of fractional ideals in K. Consider the natural morphism

$$\iota : I_K \to J_K,\ (\alpha_v)_v \mapsto \prod_v \mathfrak{p}_v^{\operatorname{ord}_v(\alpha_v)}$$

which is surjective and continuous if J_K is equipped with the discrete topology. Recall ι induces $I_K^1/K^\times \twoheadrightarrow J_K/P_K = C_K$ (P_K denoting the group of principal fractional ideals in K, and recall this proves J_K/P_K is finite since it is discrete and compact). Let $\mathbb{C}_K := I_K/K^\times$, called the idele class group. As a topological group, we have $\mathbb{C}_K \cong \mathbb{R}_{>0} \times I_K^1/K^\times$.

Now let L be a finite extension of K, then we have $\mathbb{A}_L \cong \mathbb{A}_K \otimes_K L$. We have the following natural maps

$$\mathrm{Tr}_{L/K} : \mathbb{A}_L \to \mathbb{A}_K,\ (\alpha_w)_w \mapsto \big(\sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha_w)\big)_v,$$

$$N_{L/K} : I_L \to I_K,\ (\alpha_w)_w \mapsto \big(\prod_{w|v} N_{L_w/K_v}(\alpha_w)\big)_v.$$

Note when restricted to L and $L^\times$ respectively, we get the standard trace and norm maps.

Suppose L/K is Galois. Using $\mathbb{A}_K \otimes_K L \cong \mathbb{A}_L$ (resp. $K_v \otimes_K L \cong \prod_{w|v} L_w$), we see $\mathbb{A}_L$ (resp. $K_v \otimes_K L \cong \prod_{w|v} L_w$) is equipped with a natural action of $\mathrm{Gal}(L/K)$. In fact, each place w of L corresponds to an embedding $\iota_w : L \hookrightarrow L_w$. For $g \in \mathrm{Gal}(L/K)$, there exists a unique place $g^{-1}(w)$ of L such that the composition $L \xrightarrow{g} L \xrightarrow{\iota_w} L_w$ factors through $\iota_{g^{-1}(w)} : L \hookrightarrow L_{g^{-1}(w)}$, i.e. we have a commutative diagram:

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

Using the density of L in L_w and in $L_{g^{-1}(w)}$, $g : L_{g^{-1}(w)} \to L_w$ is an isomorphism. As g is identity on K, for a place v of K, $v|w$ if and only if $v|g^{-1}(w)$. In particular, we get an action of $\mathrm{Gal}(L/K)$ on the set $\{w|v\}$. Denote by $D_w := \{g \in \mathrm{Gal}(L/K) \mid g^{-1}(w) = w\}$, then we have a natural injection $D_w \hookrightarrow \mathrm{Gal}(L_w/K_v)$. Denote by $S_w := \{g(w)\}$, then $|D_w||S_w| = [L : K]$. As $\sum_{w'|v}[L'_w : K_v] = [L : K]$, it is not difficult to deduce $D_w \xrightarrow{\sim} \mathrm{Gal}(L_w/K_v)$ and $S_w = \{w'|v\}$, i.e. the $\mathrm{Gal}(L/K)$-action on $\{w|v\}$ is transitive.

When w is a finite place with $\mathfrak{p}_w$ the associated prime ideal of $\mathcal{O}_L$, then $\mathfrak{p}_{g^{-1}(w)} = g^{-1}\mathfrak{p}_w$. So $D_{\mathfrak{p}_w} = D_w$.

Lemma 5.1.2. *Let $g \in \mathrm{Gal}(L/K)$, then g sends $L_w \hookrightarrow K_v \otimes_K L \cong \prod_{w|v} L_w$ to $L_{g(w)}$ (where L_w is viewed as a K_v vector subspace of $\prod_{w|v} L_w$ with 0 for factors at $w' \neq w$).*

Proof. Let $x = \sum_i a_i \otimes \alpha_i \in K_v \otimes_K L$, and suppose x is sent to $L_w \hookrightarrow \prod_{w|v} L_w$. Thus $\sum_i a_i \iota_{w'}(\alpha_i) = 0$ for all $w' \neq w$, $w'|v$. We have $g(x) = \sum_i a_i \otimes g(\alpha_i)$, so we see

$$\sum_i a_i \iota_{g(w')}(g(\alpha_i)) = g(\sum_i a_i \iota_{w'}(\alpha_i)) = 0$$

for $w' \neq w$ (or equivalently $g(w') \neq g(w)$). Hence $g(x) \in L_{g(w)}$. The lemma follows. □

The induced $\mathrm{Gal}(L/K)$-action on $K_v \otimes_K L$ is continuous, that implies $\prod_{w|v} \mathcal{O}_w^\times$ is stable by the $\mathrm{Gal}(L/K)$-action. We then deduce that I_L inherits from $\mathbb{A}_L$ an action of $\mathrm{Gal}(L/K)$.

Lemma 5.1.3. *We have* $\mathbb{A}_L^{\mathrm{Gal}(L/K)} = \mathbb{A}_K$ *and* $I_L^{\mathrm{Gal}(L/K)} = I_K$.

Proof. As $I_L \cap \mathbb{A}_K = I_K$, it suffices to prove the statement for $\mathbb{A}_L$. We first show $(K_v \otimes_K L)^{\mathrm{Gal}(L/K)} = K_v$ for any place v of K. The direction "$\supset$" is clear. As $\mathrm{Gal}(L_w/K_v)$ fixes the factor L_w and $L_w^{\mathrm{Gal}(L_w/K_v)} = K_v$, we see $(\prod_{w|v} L_w)^{\mathrm{Gal}(L/K)} \subset \prod_{w|v} K_v$. By the above lemma, the $\mathrm{Gal}(L/K)$-action on $\prod_{w|v} K_v \hookrightarrow \prod_{w|v} L_w$ is transitive, hence $(\prod_{w|v} K_v)^{\mathrm{Gal}(L/K)} \subset K_v$.

If w is a finite place, by Lemma 5.1.2 (and the discussions above it) it is easy to see $\prod_{w|v} \mathcal{O}_{L_w} \subset \prod_{w|v} L_w$ is stable under the action of $\mathrm{Gal}(L/K)$. We deduce hence $\mathbb{A}_L^{\mathrm{Gal}(L/K)} = \mathbb{A}_K$. □

Corollary 5.1.4. $H^0(\mathrm{Gal}(L/K), \mathbb{C}_L) \cong \mathbb{C}_K$.

Proof. Consider the exact sequence $1 \to L^\times \to I_L \to \mathbb{C}_L \to 1$. Taking $\mathrm{Gal}(L/K)$-cohomology (and using the above lemma), we obtain

$$1 \to K^\times \to I_K \to \mathbb{C}_L^{\mathrm{Gal}(L/K)} \to H^1(\mathrm{Gal}(L/K), L^\times) = 1.$$

The lemma follows. □

Finally we remark that, the norm map $N_{L/K} : I_L \to I_K$ induces $N_{L/K} : \mathbb{C}_L \to \mathbb{C}_K$.

5.2 Global class field theory (statements)

We first discuss more relation between local Galois group and global Galois group. Let $K/\mathbb{Q}$ be a finite extension, v be a place of K, L/K be a finite abelian extension, $w|v$ be a place of L, and $\mathcal{L} := L_w$. Note it is possible that we obtain the same $\mathcal{L}$ for different w. Indeed, fixing a place $w'|v$ such that $L_{w'} \cong \mathcal{L}$ is the same as fixing an embedding $\iota_{w'} : L \hookrightarrow \mathcal{L}$ that extends $\iota_v : K \hookrightarrow K_v$.

Lemma 5.2.1. *The composition* $\jmath_w : \mathrm{Gal}(\mathcal{L}/K_v) \xrightarrow{\sim} \mathrm{Gal}(L_w/K_v) \longrightarrow \mathrm{Gal}(L/K)$ *is independent of the choice of* w.

Proof. Let w' be another place of L dividing v, $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(w) = w'$. For $g \in \mathrm{Gal}(\mathcal{L}/K_v)$, $\jmath_w(g) : L \to L$ is the map satisfying the following commutative diagram

$$\begin{array}{ccc} L & \xrightarrow{\iota_w} & \mathcal{L} \\ {\scriptstyle \jmath_w(g)}\downarrow & & \downarrow{\scriptstyle g} \\ L & \xrightarrow{\iota_w} & \mathcal{L} \end{array}.$$

We deduce $\jmath_{\sigma(w)}(g) = \sigma(\jmath_w(g))\sigma^{-1} = \jmath_w(g)$ (using $\mathrm{Gal}(L/K)$ is abelian). □

We have $\mathrm{Gal}(\overline{K}_v/K_v)^{\mathrm{ab}} \cong \varprojlim_{\substack{M/K_v \\ \text{finite ablian}}} \mathrm{Gal}(M/K_v)$. For each finite abelian extension L/K, we choose a place $w|v$ of L such that if $L_1 \subset L_2$ are finite abelian over K, then the fixed places w_i of L_i satisfy $w_1|w_2$. Consider the composition (recalling for any finite extension M of K_v, there exists a finite extension M_0 of K such that M is isomorphic to the completion of M_0 at a certain place)

$$\mathrm{Gal}(\overline{K_v}/K_v)^{\mathrm{ab}} \cong \varprojlim_{\substack{M/K_v \\ \text{finite ablian}}} \mathrm{Gal}(M/K_v) \xrightarrow{\sim} \varprojlim_{\substack{L/K \\ \text{finite abelian}}} \mathrm{Gal}(L_w/K_v) \hookrightarrow \varprojlim_{\substack{L/K \\ \text{finite abelian}}} \mathrm{Gal}(L/K) \cong \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}. \tag{5.1}$$

If v is a finite place of K, we have defined the local artin recriprocity map $\rho_{K_v} : K_v^\times \to \mathrm{Gal}(\overline{K_v}/K_v)^{\mathrm{ab}}$. We briefly discuss the local artin reciprocity for archimedean fields. If $K_v = \mathbb{R}$, we put $\rho_{K_v} : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ the unique non-trivial group homomorphism, which factors through $\mathbb{R}^\times/\mathbb{R}_{>0} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{C}/bR)$, $-1 \mapsto [x \mapsto \bar{x}]$; if $K_v = \mathbb{C}$, put ρ_{K_v} to be the trivial map $\mathbb{C}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{1\}$.

Together with (5.1), for $\alpha_v \in K_v^\times$, we have $\rho_{K_v}(\alpha_v) \in \mathrm{Gal}(\overline{K_v}/K_v)^{\mathrm{ab}} \hookrightarrow \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$. Neext, we show that this map can glue together to a reciprocity map on the group of ideles.

Lemma 5.2.2. *Let L/K be finite abelian, $\alpha = (\alpha_v) \in I_K$, then $\rho_{L_w/K_v}(\alpha_v) = 1$ for all but finitely many places v of K.*

Proof. We only need to consider the non-archemedean places. However, for all but finitely many non-archimedean places v, we have $\alpha_v \in \mathcal{O}_{K_v}^\times$ and L_w/K_v is unramified. Hence $\alpha_v \in N_{L_w/K_v}(L_w^\times)$ and $\rho_{L_w/K_v}(\alpha_v) = 1$. □

For L/K finite abelian, we put

$$\phi_{L/K} : I_K \to \mathrm{Gal}(L/K),\ (\alpha_v) \mapsto \prod_v \rho_{L_w/K_v}(\alpha_v)|_L$$

where for each places v of K, we choose a place $w|v$ of L in the above product.

Lemma 5.2.3. *Let $L \subset M$ be finite abelian extensions of K, $\alpha \in I_K$, then $\Phi_{L/K}(\alpha) = \Phi_{M/K}(\alpha)|_L$.*

Proof. For any place v of K, let $w|v$ be a place of L and $\tilde{w}|w$ a place of M. By the local artin reciprocity law, we have $\rho_{M_{\tilde{w}}/K_v}(\alpha_v)|_{L_w} = \rho_{L_w/K_v}(\alpha_v)$ (that obviously holds also for archimedean places). The lemma follows. □

We deduce hence $\Phi_K := (\Phi_{L/K}) : I_K \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$. It is straightforward to check $\Phi_K(\alpha) = \prod_v \phi_{K_v}(\alpha_v)|_{K^{\mathrm{ab}}}$.

Theorem 5.2.4. *(1) For any $\alpha \in K^\times$, $\Phi_K(\alpha) = 1$.*

(2) For any finite abelian extension L/K, $\Phi_{L/K}$ is surjective with kernel $K^\times N_{L/K}(I_L)$.

By the theorem, we can define the so-called global reciprocity maps $\phi_K : \mathbb{C}_K \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, and $\Phi_{L/K} : \mathbb{C}_K \to \mathrm{Gal}(L/K)$ for L/K finite abelian. We also deduce:

Theorem 5.2.5. *For any finite abelian extension L/K, $\Phi_{L/K}$ induces an isomorphism*

$$\big(I_K^\times/K^\times N_{L_K} I_L^\times = \big)\mathbb{C}_K/N_{L/K}\mathbb{C}_L \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

The following proposition follows from the definition of Φ_K and the corresponding facts on local artin reciprocity law:

Proposition 5.2.6. *Let L/K be a finite extension. Then the following diagram commutes*

$$\begin{array}{ccc} I_L & \xrightarrow{\Phi_L} & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ I_K & \xrightarrow{\Phi_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} I_K & \xrightarrow{\Phi_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ \downarrow & & \downarrow{\scriptstyle V_{L/K}} \\ I_L & \xrightarrow{\Phi_L} & \mathrm{Gal}(\overline{K}/L) \end{array},$$

and for $\sigma : L \to \overline{K}$,

$$\begin{array}{ccc} I_L & \xrightarrow{\Phi_L} & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ I_{\sigma(L)} & \xrightarrow{\Phi_{\sigma(L)}} & \mathrm{Gal}(\overline{K}/\sigma(L))^{\mathrm{ab}} \end{array}.$$

Proof. Exercise. □

Finally we have

Theorem 5.2.7 (Existence theorem)**.** *The open subgroup of finite index of $\mathbb{C}_K$ are exactly the norm subgroups $N_{L/K}\mathbb{C}_L$ with Lfinite abelian extensions of K. Moreover, let L, M be finite abelian extensions over K, then $N_{M/K}\mathbb{C}_M \subset N_{L/K}\mathbb{C}_L$ if and only if $L \subset M$.*

We will establish the theorems in the following sections. A rough idea is to show

$$(\mathrm{Gal}(\overline{K}/K), \mathbb{C}_{\overline{K}} := \varinjlim_{L} \mathbb{C}_L)$$

is a topological class formation and is compatible with the local class formations. We end this section by the following proposition.

Proposition 5.2.8. *Let L/K be a finite extension, then $N_{L/K}I_L$ is an open subgroup of I_K.*

Proof. Let S be a finite set of places of K containing all the archimedean places and those that ramify in L, and $S_L := \{w|v, v \in S\}$. By Lemma 4.2.3, $N_{L/K}I_{L,S_L} = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v^\times$. The proposition follows. □

5.3 Cohomology of idele class group: first inequality

Let L be a finite extension of K, and let S be a finite set of places containing all the archimedean places of L. Recall

Lemma 5.3.1. *Suppose S contains a finite set S_0 of finite places w of L such that $\{\mathfrak{p}_w\}_{w\in S_0}$ can generate the ideal class group of L, then $I_L = L^\times I_{L,S}$.*

Proof. Recall we have $I_L/\big(L^\times(\prod_{w|\infty} L_w^\times \times \prod_{w\nmid\infty} \mathcal{O}_{L_w}^\times)\big) \xrightarrow{\sim} \mathrm{Cl}_L$. By the assumption on S, the induced map

$$L^\times I_{L,S}/\big(L^\times(\prod_{w|\infty} L_w^\times \times \prod_{w\nmid\infty} \mathcal{O}_{L_w}^\times)\big) \longrightarrow \mathrm{Cl}_L$$

is surjective hence is also an isomorphism. The lemma follows. □

We deduce then $\mathbb{C}_L = I_L/L^\times \xleftarrow{\sim} I_{L,S}/(L^\times \cap I_{L,S})$. Recall $\mathcal{O}_{L,S}^\times := L^\times \cap I_{L,S}$ is the group of S-units in L. Denote by $S_f \subset S$ the subset of finite places, then we have an exact sequence:

$$1 \to \mathcal{O}_L^\times \to \mathcal{O}_{L,S}^\times \xrightarrow{\sum_{w\in S_f} \mathrm{val}_w} \oplus_{w\in S_f}\mathbb{Z} \tag{5.2}$$

The image of the last map contains $\oplus_{w\in S_f} N\mathbb{Z}$ for some N sufficiently large: indeed, let $N \in \mathbb{Z}_{\geq 1}$ such that $\mathfrak{p}_w^N$ is principal for all $w \in S_f$, and let $\alpha_w \in \mathcal{O}_L$ such that $\mathfrak{p}_w^N = \alpha_w$, then $\alpha_w \in \mathcal{O}_{L,S}^\times$ is sent to N at w and 0 at other places. By Dirichlet's unit theorem, we see $\mathcal{O}_{L,S}^\times$ is a finitely generated group of rank $|S| - 1$.

Now suppose L is finite Galois over K, and let v be a place of K. Let $w|v$ be a place of L.

Lemma 5.3.2. *We have* $(L \otimes_K K_v)^\times \cong \mathrm{Ind}_{D_w}^{\mathrm{Gal}(L/K)} L_w^\times$ *and* $\prod_{w'|v} \mathcal{O}_{w'}^\times \cong \mathrm{Ind}_{D_w}^{\mathrm{Gal}(L/K)} \mathcal{O}_w^\times$.

Proof. The natural D_w-equivariant injection $L_w^\times \hookrightarrow \prod_{w'|v} L_{w'}^\times$ (resp. $\mathcal{O}_w^\times \hookrightarrow \prod_{w'|v} \mathcal{O}_{w'}^\times$) induces a $\mathrm{Gal}(L/K)$-equivariant map

$$\mathbb{Z}[\mathrm{Gal}(L/K)] \otimes_{\mathbb{Z}[D_w]} L_w^\times \to \prod_{w'|v} L_{w'}^\times \text{ (resp. } \mathbb{Z}[\mathrm{Gal}(L/K)] \otimes_{\mathbb{Z}[D_w]} \mathcal{O}_w^\times \to \prod_{w'|v} \mathcal{O}_{w'}^\times).$$

Using Lemma 5.1.2, one directly checks the induced maps are isomorphisms. □

We deduce hence

$$\begin{aligned} H_T^i(D_w, L_w^\times) &\cong H_T^i(\mathrm{Gal}(L/K), (L \otimes_K K_v)^\times) \\ H_T^i(D_w, \mathcal{O}_w^\times) &\cong H_T^i(\mathrm{Gal}(L/K), \prod_{w'|v} \mathcal{O}_{w'}^\times) \end{aligned}$$

Notation 5.3.3. *Let S be a finite set of places of K, we denote by* $I_{L,S} := \prod_{v\in S}\prod_{w|v} L_w^\times \times \prod_{v\notin S}\prod_{w|v} \mathcal{O}_w^\times$.

Proposition 5.3.4. *Let S be a finite set of places of K containing all the archimedean places and the places that ramify in L/K. Then we have for all $i \in \mathbb{Z}$:*

$$H_T^i(\mathrm{Gal}(L/K), I_{L,S}) \cong \oplus_{v\in S} H_T^i(D_w, L_w^\times)$$

where for each place of K, we choose a place w of L dividing v.

Proof. First group cohomology commutes with product (one can see this using cochains, or using the fact that a direct product of injective objects is still injective): $H^i(G, \prod_i M_i) \cong \prod_i H^i(G, M_i)$. We also have $\mathrm{Ind}_H^G(\prod_i M_i) \cong \prod_i \mathrm{Ind}_H^G M_i$. By dimension shifting, we deduce $H_T^i(G, \prod_i M_i) \cong \prod_i H_T^i(G, M_i)$. We have then

$$\begin{aligned} H_T^i(\mathrm{Gal}(L/K), I_{L,S}) &\cong \prod_{v \in S} H_T^i(\mathrm{Gal}(L/K), \prod_{w|v} L_w^\times) \times \prod_{v \notin S} H_T^i(\mathrm{Gal}(L/K), \prod_{w|v} \mathcal{O}_w^\times) \\ &\cong \prod_{v \in S} H_T^i(D_w, L_w^\times) \times \prod_{v \notin S} H_T^i(D_w, \mathcal{O}_{L_w}^\times) \cong \prod_{v \in S} H_T^i(D_w, L_w^\times), \end{aligned}$$

where the last isomorphism follows from Lemma 3.2.2, 3.2.3 (and our assumption on S). □

Corollary 5.3.5. *Let S be a finite set of places of K containing all the archimedean places and places that ramify in L. Then $|H_T^0(\mathrm{Gal}(L/K), I_{L,S})| = \prod_{v \in S} |D_w^{\mathrm{ab}}|$, $H_T^1(\mathrm{Gal}(L/K), I_{L,S}) = 1$ and $H_T^2(\mathrm{Gal}(L/K), I_{L,S}) \cong \oplus_{v \in S} \frac{1}{|D_w|}\mathbb{Z}/Z$.*

Proposition 5.3.6. *W have $H_T^i(\mathrm{Gal}(L/K), I_L) \cong \oplus_v H_T^i(D_w, L_w^\times)$.*

Proof. We have $I_L = \varinjlim_S I_{L,S}$ where S runs through finite set of places of K satisfying the condition in Proposition 5.3.4. The proposition then follows from Proposition 5.3.4 and the fact that Tate cohomology commutes with direct limit: taking (finite) group cohomology commutes with direct limit+direct limit of induced module is induced+dimension shifting. □

Corollary 5.3.7. *We have $H^1(\mathrm{Gal}(L/K), I_L) = 1$ and $H^2(\mathrm{Gal}(L/K), I_L) \cong \oplus_v \frac{1}{|D_w|}\mathbb{Z}/\mathbb{Z}$.*

Theorem 5.3.8. *If L/K is cyclic, then $h(\mathrm{Gal}(L/K), \mathbb{C}_L) = [L : K]$.*

Proof. Let S be a finite set of places of K containing all the archimedean places, places that ramify in L such that $\mathfrak{p}_w$ for $w|v$, and $v \in S_f$ generate Cl_L. Denote by $S_L : \{w|v, v \in S\}$. We have thus a $\mathrm{Gal}(L/K)$-equivariant exact sequence

$$1 \to \mathcal{O}_{L,S_L}^\times \to I_{L,S} \to \mathbb{C}_L \to 1.$$

We then need to calculate $H_T^i(\mathrm{Gal}(L/K), \mathcal{O}_{L,S_L}^\times)$. The following sequence is also $\mathrm{Gal}(L/K)$-equivariant:

$$1 \to \mathcal{O}_L^\times \to \mathcal{O}_{L,S_L}^\times \xrightarrow{\nu := \sum_{w \in S_{L,f}}} \oplus_{w \in S_{L,f}} \mathbb{Z}.$$

We have

$$\begin{aligned} H_T^i(\mathrm{Gal}(L/K), \oplus_{w \in S_{L,f}} \mathbb{Z}) &\cong \oplus_{v \in S_f} H_T^i(\mathrm{Gal}(L/K), \mathrm{Ind}_{D_w}^{\mathrm{Gal}(L/K)} \mathbb{Z}) \\ &\cong \oplus_{v \in S_f} H_T^i(D_w, \mathbb{Z}) \cong \begin{cases} \oplus_{v \in S_f} \mathbb{Z}/|D_w|\mathbb{Z}, & i = 0 \\ 0 & i = 1 \end{cases}. \end{aligned}$$

As $\mathrm{Im}\,\nu$ has finite index in $\oplus_{w \in S_{L,f}} \mathbb{Z}$,

$$h(\mathrm{Gal}(L/K), \mathrm{Im}\,\nu) = h(\mathrm{Gal}(L/K), \oplus_{w \in S_{L,f}} \mathbb{Z}) = \prod_{v \in S_f} |D_w|.$$

Now we calculate $H_T^i(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)$. We have

$$\mathcal{O}_L^\times \xrightarrow{j} \oplus_{w\in S_{L,\infty}}\mathbb{R} =: V,\ \alpha \mapsto (\log|\alpha|_w)_{w\in S_{L,\infty}}.$$

The map j is moreover $\mathrm{Gal}(L/K)$-equivariant, if we equip $\oplus_{w\in S_{L,\infty}}\mathbb{R}$ with the $\mathrm{Gal}(L/K)$-action by $g(a_w) = (b_w)$ where $b_w = a_{g(w)}$. Recall $\mathrm{Im}\, j$ is a lattice of rank $|S_{L,\infty}| - 1$, and $\mathrm{Ker}\, j$ is the finite group of roots of unity in L in particular $h(\mathrm{Gal}(L/K), \mathrm{Ker}\, j) = 1$. Let $\Lambda := \oplus_{w\in S_{L,\infty}}\mathbb{Z}$ be the standard full lattice of V. Then

$$H_T^i(\mathrm{Gal}(L/K), \Lambda) \cong \begin{cases} \oplus_{v\in S_\infty}\mathbb{Z}/|D_w|\mathbb{Z} & i = 0 \\ 0 & i = 1 \end{cases}.$$

Let $e := (1, \cdots, 1) \in V$, then $\mathrm{Im}\, j + \mathbb{Z}e = \mathrm{Im}\, j \oplus \mathbb{Z}e$ is a lattice in V. By the lemma below, we have $h(\mathrm{Gal}(L/K), \mathrm{Im}\, j+\mathbb{Z}e) = h(\mathrm{Gal}(L/K), \Lambda) = \prod_{v\in S_\infty}|D_w|$. As the $\mathrm{Gal}(L/K)$-action on $\mathbb{Z}e$ is trivial, we have $h(\mathrm{Gal}(L/K), \mathbb{Z}e) = |\mathrm{Gal}(L/K)|$. We deduce hence $h(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = h(\mathrm{Gal}(L/K), \mathrm{Im}\, j) = \frac{1}{|\mathrm{Gal}(L/K)|}\prod_{v\in S_\infty}|D_w|$. So $h(\mathrm{Gal}(L/K), \mathcal{O}_{L,S_L}^\times) = \frac{1}{|\mathrm{Gal}(L/K)|}\prod_{v\in S}|D_w|$ and $h(\mathrm{Gal}(L/K), \mathbb{C}_L) = [L : K]$. □

Lemma 5.3.9. *Let V be an $\mathbb{R}$-vector space equipped with an $\mathbb{R}$-linear action of a finite group G, and let Λ_1, Λ_2 be two G-equivariant lattices in V. Then $\Lambda_1 \otimes_\mathbb{Z} \mathbb{Q} \cong \Lambda_2 \otimes_\mathbb{Z} \mathbb{Q}$ as G-modules over $\mathbb{Q}$. Consequently, $h(G, \Lambda_1) = h(G, \lambda_2)$.*

Proof. Let $n := \dim_\mathbb{R} V$. For a characteristic 0 field k, se have a natural isomorphism of k-vector spaces (of dimension n^2)

$$\mathrm{Hom}_\mathbb{Z}(\Lambda_1, \Lambda_2) \otimes_\mathbb{Z} k \cong \mathrm{Hom}_k(\Lambda_1 \otimes_\mathbb{Z} k, \Lambda_2 \otimes_\mathbb{Z} k),$$

which is moreover G-equivariant if we equip the both with the G-action given by $gf(v) := gf(g^{-1}v)$. For $f \in \mathrm{Hom}_\mathbb{R}(\Lambda_1\otimes_\mathbb{Z} k, \Lambda_2\otimes_\mathbb{Z} k)$, f is G-equivariant if and only if $f \in \mathrm{Hom}_k(\Lambda_1\otimes_\mathbb{Z} k, \Lambda_2 \otimes_\mathbb{Z} k)^G$. Let f_i be a basis $\mathrm{Hom}_\mathbb{Z}(\Lambda_1, \Lambda_2)$. For $g \in G$, let $A_g := (a_{i,j}(g)) \in M_{n^2}(\mathbb{Z})$ such that $gf_i = \sum_j a_{i,j}(g)f_j$. Let $f \in \mathrm{Hom}_\mathbb{R}(\Lambda_1 \otimes_\mathbb{Z} k, \Lambda_2 \otimes_\mathbb{Z} k)$, and let $b_i \in \mathbb{R}$ for $i = 1, \cdots, n^2$ such that $f = \sum_i f_i \otimes b_i$. Then f is G-equivariant if and only if $\sum_i(\sum_j(a_{ij}(g)f_j) \otimes b_i) = \sum_i f_i \otimes b_i$ for all g if and only if $A_g^T \begin{pmatrix} b_1 \\ \vdots \\ b_{n^2} \end{pmatrix} = 0$ for all g. Let $W_k := \{b = (b_1, \cdots, b_{n^2})^T \in k^{n^2} \mid A_g^T b = 0,\ \forall g \in G\}$. By the above discussion, we have $\mathrm{Hom}_k(\Lambda_1 \otimes_\mathbb{Z} k, \Lambda_2 \otimes_\mathbb{Z} k)^G \cong W_k$ sending f to the coefficients under the basis f_i. As it is clear that $W_\mathbb{Q} \otimes_\mathbb{Q} \mathbb{R} \cong W_\mathbb{R}$, we deduce

$$\mathrm{Hom}_\mathbb{Q}(\Lambda_1 \otimes_\mathbb{Z} \mathbb{Q}, \Lambda_2 \otimes_\mathbb{Z} \mathbb{Q})^G \otimes_\mathbb{Q} \mathbb{R} \xrightarrow{\sim} \mathrm{Hom}_\mathbb{R}(\Lambda_1 \otimes_\mathbb{Z} \mathbb{R}, \Lambda_2 \otimes_\mathbb{Z} \mathbb{R})^G.$$

Now we need to find a bijection in $\mathrm{Hom}_\mathbb{Q}(\Lambda_1 \otimes_\mathbb{Z} \mathbb{Q}, \Lambda_2 \otimes_\mathbb{Z} \mathbb{Q})^G$. Let α_i be a basis of this $\mathbb{Q}$-vector space, which we view as elements in $M_n(\mathbb{Q})$ by identifying $\mathrm{Hom}_\mathbb{Q}(\Lambda_1 \otimes_\mathbb{Z} \mathbb{Q}, \Lambda_2 \otimes_\mathbb{Z} \mathbb{Q})$ with $M_n(\mathbb{Q})$ (with respect to a basis of Λ_1 and Λ_2). We need to show there exist $a_i \in \mathbb{Q}$ such that $\det(\sum a_i\alpha_i) \neq 0$. However, by assumption, there exists $a_i' \in \mathbb{Q}$ such that $\det(\sum a_i'\alpha_i) \neq 0$. We deduce the map $(a_i) \mapsto \det(\sum a_i\alpha_i)$ is given by a *non-zero* $\mathbb{Q}$-coefficient polynomial (of multi-variables), hence can not be constantly zero for (a_i) (in $\mathbb{Q}$). The first part of the lemma follows.

Put $V_{\mathbb{Q}} := \Lambda_1 \otimes_{\mathbb{Z}} \mathbb{Q} \cong \Lambda_2 \otimes_{\mathbb{Z}} \mathbb{Q}$, and we view Λ_i as $\mathbb{Z}$-submodules of $V_{\mathbb{Q}}$. There exist thus $m_1, m_2 \in \mathbb{Z}_{\geq 1}$ such that $m_1\Lambda_2 \subset \Lambda_1 \subset \frac{1}{m_2}\Lambda_2$. We see the quotient $\Lambda_1/m_1\Lambda_2$ is finite, hence $h(G, \Lambda_1) = h(G, m_1\Lambda_2) = h(G, \Lambda_2)$ $(m_1\Lambda_2 \cong \Lambda_2)$. □

Corollary 5.3.10 (First inequality)**.** *If L/K is cyclic, then* $[\mathbb{C}_K : N_{L/K}\mathbb{C}_L] = [I_K : K^\times N_{L_K} I_L] \geq [L : K]$.

Corollary 5.3.11. *Let L/K be a finite abelian extension. Then there exists infinitely many places of K that do not split completely in L.*

Proof. It is easy to reduce to the cyclic case. Assume hence L/K cyclic. Suppose the statement does not holds. Let S be the finite set of places of K containing S_∞, the places that ramify in L and the places that do not split. For any $v \notin S$, $w|v$, we have $L_w \cong K_v$ hence $N_{L_w/K_v}(L_w^\times) = K_v^\times$. Let $I^S := \{(x_v) \in I_K \mid x_v = 1,\ \forall v \in S\}$, then $I^S \subset N_{L/K}I_L$. Recall $K^\times$ is dense in $\prod_{v \in S} K_v^\times$. We deduce $K^\times I^S$ is dense in I_K hence $K^\times N_{L/K}I_L$ is dense in I_K. However $N_{L/K}I_L$ is open in $I_K \Rightarrow K^\times N_{L/K}I_L$ is open $\Rightarrow K^\times N_{L/K}I_L$ is closed $\Rightarrow$ $K^\times N_{L/K}I_L = I_K$. By the first inequality, $L = K$. □

Let L/K be a finite abelian extension, and v be a finite place of K that is unramified in L. For $w|v$, we have $\mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$, and we denote by Frob_v the image of the arithemetic Frobenius element in $\mathrm{Gal}(L_w/K_v)$. Recall the injection hence Frob_v do not depend on the choice for $w|v$.

Corollary 5.3.12. *Let L/K be a finite abelian extension, S be a finite set of places of K containing S_∞ and those that ramify in L. Then $\{\mathrm{Frob}_v\}_{v\notin S}$ generated* $\mathrm{Gal}(L/K)$.

Proof. Let H be the subgroup generated by $\{\mathrm{Frob}_v\}_{v\notin S}$, and $M := L^H$. By assumption, for all $v \notin S$, and $w|v$ a place in M, we have $M_w = K_v$. Thus any $v \notin S$ splits in M. By the above corollary, $M = K$ hence $H = \mathrm{Gal}(L/K)$. □

Corollary 5.3.13. *Let $L_1, \cdots, L_t$ be cyclic extensions of K of prime degree p, such that each L_i is disjoint from the composition of L_j for $j \neq i$. Then there are infinitely many places of K that are inert in L_1 and splits completely in L_i for $i \geq 2$.*

Proof. Let $L := L_1 \cdots L_t$ and $L' := L_2 \cdots L_t$, then $\mathrm{Gal}(L/L') \cong \mathbb{Z}/p\mathbb{Z}$. By the above corollary, there exists infinitely many finite places w of L' such that w is unramified in L and $\langle \mathrm{Frob}_w \rangle = \mathrm{Gal}(L/L')$. Such w is inert in L. Let v be the place of K divided w. Removing finitely many w, we can and do assume v is unramified in L. The local Galois group $\mathrm{Gal}(L_w/K_v)$ has to be cyclic. But $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus t}$, hence $\mathrm{Gal}(L_w/K_v) \cong \mathbb{Z}/p\mathbb{Z}$ and v splits in L'. We have $L^{\mathrm{Frob}_v} \supset L'$ hence an equality. Thus v has to be non-split hence inert in L_1 (since otherwise $L_1 \subset L^{\mathrm{Frob}_v}$). The lemma follows. □

5.4 Cohomology of idele class group: second inequality

Theorem 5.4.1. *Let L/K be a finite Galois extension, then*

(1) $[\mathbb{C}_K : N_{L/K}\mathbb{C}_L] \leq [L:K]$,

(2) $H^1_T(\mathrm{Gal}(L/K), \mathbb{C}_L) = 1$,

(3) $\# H^2_T(\mathrm{Gal}(L/K), \mathbb{C}_L) \leq [L:K]$.

Remark 5.4.2. *By the first equality, (1) ⇔ (2) ⇔ (3) in the cyclic case.*

We first reduce to the case where L/K is cyclic of order p.

Lemma 5.4.3. *Suppose the statements in the theorem hold in the case where L/K is cyclic of prime order, then they hold in general.*

Proof. Assume first L/K is solvable, and we use induction on the degree $[L:K]$. Let M be an intermediate extension. We have restriction-inflation sequence

$$0 \to H^1_T(\mathrm{Gal}(M/K), \mathbb{C}_M) \to H^1_T(\mathrm{Gal}(L/K), \mathbb{C}_L) \to H^1_T(\mathrm{Gal}(L/M), \mathbb{C}_L)$$

By induction hypothesis, we easily deduce $H^1_T(\mathrm{Gal}(L/K), \mathbb{C}_L) = 1$. This allows to obtain the restriction-inflation sequence for H^2:

$$0 \to H^2_T(\mathrm{Gal}(M/K), \mathbb{C}_M) \to H^2_T(\mathrm{Gal}(L/K), \mathbb{C}_L) \to H^2_T(\mathrm{Gal}(L/M), \mathbb{C}_L).$$

Using again induction hypothesis, we deduce $\# H^2_T(\mathrm{Gal}(L/K), \mathbb{C}_L) \leq [L:K]$. We have

$$\begin{aligned} [\mathbb{C}_K : N_{L/K}\mathbb{C}_L] = \left|\frac{I_K}{K^\times N_{L/K} I_L}\right| &= \left|\frac{I_K}{K^\times N_{M/K}(N_{L/M} I_L)}\right| \\ &= \left|\frac{I_K}{K^\times N_{M/K} I_M}\right| \left|\frac{K^\times N_{M/K} I_M}{K^\times N_{L/K} I_L}\right| \leq [M:K] \left|\frac{K^\times N_{M/K} I_M}{K^\times N_{L/K} I_L}\right|. \end{aligned}$$

The (surjective) norm map $I_M \xrightarrow{N_{M/K}} N_{M/K} I_M$ induces

$$N_{M/K} : \frac{I_M}{M^\times N_{L/M} I_L} \longrightarrow \frac{N_{M/K} I_M}{(K^\times N_{L/K} I_L) \cap N_{M/K} I_M} \twoheadrightarrow \frac{K^\times N_{M/K} I_M}{K^\times N_{L/K} I_L}.$$

Hence $\left|\frac{K^\times N_{M/K} I_M}{K^\times N_{L/K} I_L}\right| \leq \left|\frac{I_M}{M^\times N_{L/M} I_L}\right| \leq [L:M]$ by induction hypothesis. We then deduce $[\mathbb{C}_K : N_{L/K}\mathbb{C}_L] \leq [L:K]$.

Now assume L/K is finite Galois. Let $\mathrm{Gal}(L/K)_p \subset \mathrm{Gal}(L/K)$ be the p-Sylow subgroup (that is solvable). We have $H^i_T(\mathrm{Gal}(L/K), \mathbb{C}_L)[p^\infty] \hookrightarrow H^i_T(\mathrm{Gal}(L/K)_p, \mathbb{C}_L)[p^\infty]$. The general case then follows (from the solvable case). □

We reduce furthermore to the case where $\zeta_p \in K$.

Lemma 5.4.4. *Let L/K be cyclic of order p, suppose the statements in Theorem holds for the extension $L(\zeta_p)/K(\zeta_p)$, then they hold for L/K.*

Proof. As $p \nmid [K(\zeta_p) : K] =: d$, $[L(\zeta_p) : K(\zeta_p)] = p$ and $\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)) \xrightarrow{\sim} \mathrm{Gal}(L/K)$. We prove the natural map

$$\begin{aligned} I_K/(K^\times N_{L/K} I_L) &\cong H^0_T(\mathrm{Gal}(L/K), \mathbb{C}_L) \\ &\longrightarrow H^0_T(\mathrm{Gal}(L(\zeta_p)/K(\zeta_p)), \mathbb{C}_{L(\zeta_p)}) \cong I_{K(\zeta_p)}/(K(\zeta_p)^\times N_{L(\zeta_p)/K(\zeta_p)} I_{L(\zeta_p)}) \end{aligned}$$

is injective. Let $x \in I_K$ and suppose there exist $y \in K(\zeta_p)$, $z \in I_{L(\zeta_p)}$ such that $x = y N_{L(\zeta_p)/K(\zeta_p)}(z)$. Then $x^d = N_{K(\zeta_p)/K}(y) N_{L(\zeta_p)/K}(z) \in K^\times N_{L/K} I_L$, hence $x^d = 1 \in H^0_T(\mathrm{Gal}(L/K), \mathbb{C}_L)$. As $H^0_T(\mathrm{Gal}(L/K), \mathbb{C}_L)$ is p-torsion, we deduce $x = 1 \in H^0_T(\mathrm{Gal}(L/K), \mathbb{C}_L)$. The lemma follows. □

Now suppose we have L/K cyclic of order p and $\zeta_p \in K$. An upshot is we can apply Kummer theory. As shown in the Exercise 5.6, we have an isomorphism:

$$K^\times/(K^\times)^p \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_p),$$

sending α to $g \mapsto g(\alpha^{\frac{1}{p}})/\alpha^{\frac{1}{p}}$. We have the following easy fact:

Lemma 5.4.5. *Let $\alpha \in K^\times$ and v be an archimedean place of K. Then $K_v(\alpha^{\frac{1}{p}})$ is unramified over K_v if and only if there exist $x_v \in \mathcal{O}_v^\times$, $y_v \in (K_v^\times)^p$ such that $\alpha = x_v y_v$.*

Proof. The "if" part follows by Hensel's lemma. Suppose $K_v(\alpha^{\frac{1}{p}})$ is unramified over K_v, then $\mathrm{val}_{K_v}(\alpha) = \mathrm{val}_{K_v(\alpha^{\frac{1}{p}})}(\alpha) = p\,\mathrm{val}_{K_v(\alpha^{\frac{1}{p}})}(\alpha^{\frac{1}{p}}) \in p\mathbb{Z}$. The "only if" part follows. □

We let $\Delta_0 := (L^\times)^p \cap K^\times$, then $L = K(\Delta_0^{\frac{1}{p}}) = K(\{\alpha^{\frac{1}{p}}\}_{\alpha \in \Delta_0})$. We want to understand $N_{L/K}\mathbb{C}_L$. Let S be a finite set of places of K containing $\{v|\infty\}$, $\{v|p\}$, those that ramify in L such that $\{\mathfrak{p}_v\}_{v \in S_f}$ generate Cl_K (so $I_{K,S}K^\times = I_K$).

Lemma 5.4.6. *Let $\Delta := (L^\times)^p \cap O_{K,S}^\times$. Then $L = K(\Delta^{\frac{1}{p}})$.*

Proof. Let $x \in (L^\times)^p \cap K^\times$ such that $L = K(x^{\frac{1}{p}})$. For $v \notin S$, $K_v(x^{\frac{1}{p}})$ is unramified over K_v. So $\mathrm{val}_{K_v}(x) = \mathrm{val}_{K_v(x^{\frac{1}{p}})}(x) = p\,\mathrm{val}_{K_v(x^{\frac{1}{p}})}(x^{\frac{1}{p}}) \in p\mathbb{Z}$. There exist thus $u_v \in \mathcal{O}_{K_v}^\times$, $y_v \in K_v^\times$ such that $x = u_v y_v^p$. Put $y_v := 1$ for $v \in S$, and $y := (y_v)_{v \notin S} \times (y_v)_{v \in S} \in I_K$. There exist $z \in K^\times$, $w \in I_{K,S}$ such that $y = zw$. Then $x/z^p \in I_{K,S} \cap K^\times = O_{K,S}^\times$, and it is clear $L = K((x/z)^{\frac{1}{p}})$. □

Lemma 5.4.7. *There is a set T of $|S| - 1$ places of K, disjoint from S, such that the following sequence is exact:*

$$1 \to \Delta/(\mathcal{O}_{K,S}^\times)^p \to (\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \to \prod_{v \in T} K_v^\times/(K_v^\times)^p \to 1.$$

Proof. By (generalized) Dirichlet's unit theorem, we have $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus|S|}$ (noting $\mu_K/(\mu_K)^p \cong \mathbb{Z}/p\mathbb{Z}$ as $\zeta_p \in K$). We have (noting $\mathcal{O}_{K,S}^\times \cap (K^\times)^p = (\mathcal{O}_{K,S}^\times)^p$)

$$\Delta/(\mathcal{O}_{K,S}^\times)^p \hookrightarrow \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \hookrightarrow K^\times/(K^\times)^p \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_p).$$

Let K_S be the finite extension of K generated by $\alpha^{\frac{1}{p}}$, $\alpha \in \mathcal{O}_{K,S}^\times$. We have $L \subset K_S$, and by Kummer theory, $\mathrm{Gal}(K_S/K) \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus|S|}$. Let $g_1, \cdots, g_{|S|-1} \in \mathrm{Gal}(K_S/K)$ be a basis of $\mathrm{Gal}(K_S/L) \cong (\mathbb{Z}/p\mathbb{Z})^{|S|-1}$. For each g_i, let $L_i := K_S^{g_i}$. By Corollary 5.3.13, there exists $v_i \notin S$ such that v_i is not completely split in K_S and v_i is completely splits in L_i (one can just pick a place w_i of L_i such that w_i is inert in K_S and the underlying place v_i in K does not belong to S). As $L = \cap L_i$, v_i are all split in L. So for any $\alpha \in \Delta$, $\alpha \in (\mathcal{O}_{K_{v_i}}^\times)^p \subset (K_{v_i}^\times)^p$. The composition

$$\Delta/(\mathcal{O}_{K,S}^\times)^p \hookrightarrow \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \to \prod_{v_i} \mathcal{O}_{K_{v_i}}^\times/(\mathcal{O}_{K_{v_i}}^\times)^p \tag{5.3}$$

is zero. If $x \in \mathrm{Ker}(\mathcal{O}_{K,S} \to \prod_{v_i} \mathcal{O}_{K_{v_i}}^\times/(\mathcal{O}_{K_{v_i}}^\times)^p)$, then $K(x^{\frac{1}{p}}) \subset K_S$ is split at all v_i hence $K(x^{\frac{1}{p}}) \subset \cap_i L_i = L$ so $x \in \Delta$. We deduce (5.3) is exact and the lemma follows with $T = \{v_i\}$. □

Let $J_{K,S,T} := \prod_{v\in S}(K_v^\times)^p \times \prod_{v\in T} K_v^\times \times \prod_{v\notin S\cup T} \mathcal{O}_{K_v}^\times$. The following lemma is clear (since $v \in T$ splits in L).

Lemma 5.4.8. *We have* $N_{L/K}(I_L) \supset J_{K,S,T}$.

Lemma 5.4.9. *We have* $[I_K : K^\times J_{K,S,T}] = p$.

Proof. Note $I_K = K^\times I_{K,S\cup T}$. We have an exact sequence

$$1 \to \frac{I_{K,S\cup T} \cap (K^\times J_{K,S,T})}{J_{K,S,T}} \to \frac{I_{K,S\cup T}}{J_{K,S,T}} \to \frac{K^\times I_{K,S\cup T}}{K^\times J_{K,S,T}} \to 1,$$

and isomorphisms:

$$\frac{\mathcal{O}_{K,S\cup T}^\times}{J_{K,S,T} \cap K^\times} \cong \frac{I_{K,S\cup T} \cap K^\times}{J_{K,S,T} \cap K^\times} \xrightarrow{\sim} \frac{I_{K,S\cup T} \cap (K^\times J_{K,S,T})}{J_{K,S,T}}.$$

Now $I_{K,S\cup T}/J_{K,S\cup T} \cong \prod_{v\in S} K_v^\times/(K_v^\times)^p$. If $v|\ell$, $K_v^\times \cong \mathbb{Z} \times \mu(K_v) \times \mathbb{Z}_\ell^{[K_v:\mathbb{Q}_\ell]}$, then (recalling $\zeta_p \in \mu(K_v)$)

$$|K_v^\times/(K_v^\times)^p| = p^2|p|_v^{-1}. \tag{5.4}$$

If $v|\infty$, we also have (5.4) (noting if $p > 2$, then $K_v \cong \mathbb{C}$). We deduce hence

$$|I_{K,S\cup T}/J_{K,S\cup T}| = p^{2|S|} \prod_{v\in S} |p|_v^{-1} p^{2|S|} \prod_{v} |p|_v^{-1} = p^{2|S|}. \tag{5.5}$$

By the following lemma, we have $J_{K,S,T} \cap K^\times = (O_{K,S\cup T}^\times)^p$, hence

$$\left|\frac{\mathcal{O}_{K,S\cup T}^\times}{J_{K,S,T} \cap K^\times}\right| = \left|\frac{\mathcal{O}_{K,S\cup T}^\times}{(\mathcal{O}_{K,S\cup T}^\times)^p}\right| = p^{2|S|-1}.$$

The lemma follows. □

Lemma 5.4.10. *We have $J_{K,S,T} \cap K^\times = (O_{K,S\cup T}^\times)^p$.*

Proof. "$\supset$" is clear. Now let $x \in J_{K,S,T} \cap K^\times$, and consider $M = K(x^{\frac{1}{p}})$. Then M/K is unramified for $v \notin S \cup T$ and split at $v \in S$. Thus

$$N_{M/K} I_M \supset \prod_{v\in S} K_v^\times \times \prod_{v\notin S\cup T} \mathcal{O}_v^\times \times \prod_{v\in T} (K_v^\times)^p \supset \prod_{v\in S} K_v^\times \times \prod_{v\notin S\cup T} \mathcal{O}_v^\times \times \prod_{v\in T} (\mathcal{O}_v^\times)^p.$$

As $\mathcal{O}_{K,S}^\times \twoheadrightarrow \prod_{v\in T} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^p$, we deduce $\mathcal{O}_{K,S} N_{M/K} I_M \supset \prod_{v\in S} K_v^\times \times \prod_{v\in S\cup T} \mathcal{O}_{K_v}^\times \times \prod_{v\in T} \mathcal{O}_{K_v}^\times$. Then $K^\times N_{M/K} I_M \supset K^\times I_{K,S} = I_K$. By the first inequality, $M = K$. ☐

Proof of Theorem 5.4.1. By Lemma 5.4.3, Lemma 5.4.4, we reduce to the case L/K is cyclic of order p and $\zeta_p \in K$. By Lemma 5.4.8, Lemma 5.4.9, $[I_K : K^\times N_{L/K} I_L] \leq p$. This concludes the proof. ☐

5.5 Global reciprocity law

Let L/K be a finite Galois extension of number fields. Consider the exact sequence $1 \to L^\times \to I_L \to \mathbb{C}_L \to 1$. Since $H^1(\mathrm{Gal}(L/K), \mathbb{C}_L) = 1$, we deduce

$$H^2(\mathrm{Gal}(L/K), L^\times) \hookrightarrow H^2(\mathrm{Gal}(L/K), I_L) \cong \oplus_v H^2(\mathrm{Gal}(L_w/K_v), L_w^\times).$$

For each K_v, let $\mathrm{inv}_{K_v} : H^2(\mathrm{Gal}(L_w/K_v), L_w^\times) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ be the local invariant mapj, that is associated to the Frobenius $x \mapsto x^{q_v}$ when v is non-archimedean. Denote by inv_v the composition $H^2(\mathrm{Gal}(L/K), I_L) \to H^2(\mathrm{Gal}(L_w/K_v), L_w) \xrightarrow{\mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z}$, and $\tilde{\mathrm{inv}}_{L/K} := \sum_v \mathrm{inv}_v$. Taking direct limit, we get

$$H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \hookrightarrow H^2(\mathrm{Gal}(\overline{K}/K), I_{\overline{K}}) \cong \oplus_v H^2(\mathrm{Gal}(\overline{K_v}/K_v), \overline{K_v}^\times)$$

and $\tilde{\mathrm{inv}}_K : H^2(\mathrm{Gal}(\overline{K}/K), I_{\overline{K}}) \to \mathbb{Q}/\mathbb{Z}$.

Lemma 5.5.1. *For $\alpha \in I_K$, $\chi \in \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(\mathrm{Gal}(L/K), \mathbb{Z})$, we have*

$$\tilde{\mathrm{inv}}_{L/K}(\overline{\alpha} \cup \delta(\chi)) = \sum_v \mathrm{inv}_v(\overline{\alpha} \cup \delta(\chi)) = \chi(\Phi_{L/K}(\alpha)) \in \mathbb{Q}/\mathbb{Z},$$

where $\overline{\alpha}$ is the image of α in $H_T^0(\mathrm{Gal}(L/K), I_L)$.

Proof. For a place v of K and $w|v$, we have commutative diagrams

$$\begin{array}{ccccc}
H^0_T(\mathrm{Gal}(L/K), I_L) & \times & H^2_T(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\cup} & H^2_T(\mathrm{Gal}(L/K), I_L) \\
\downarrow & & \downarrow & & \downarrow \\
H^0_T(\mathrm{Gal}(L/K), \prod_{w'|v} L^\times_{w'}) & \times & H^2_T(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\cup} & H^2_T(\mathrm{Gal}(L/K), \prod_{w'|v} L^\times_{w'}) \\
\downarrow & & \downarrow & & \downarrow \\
H^0_T(\mathrm{Gal}(L_w/K_v), \prod_{w'|v} L^\times_{w'}) & \times & H^2_T(\mathrm{Gal}(L_w/K_v), \mathbb{Z}) & \xrightarrow{\cup} & H^2_T(\mathrm{Gal}(L_w/K_v), \prod_{w'|v} L^\times_{w'}) \\
\downarrow & & \downarrow & & \downarrow \\
H^0_T(\mathrm{Gal}(L_w/K_v), L^\times_w) & \times & H^2_T(\mathrm{Gal}(L_w/K_v), \mathbb{Z}) & \xrightarrow{\cup} & H^2_T(\mathrm{Gal}(L_w/K_v), L^\times_w)
\end{array} \tag{5.6}$$

and

$$\begin{array}{ccc}
H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta} & H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \\
\downarrow & & \downarrow \\
H^1(\mathrm{Gal}(L_w/K_v), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta} & H^2(\mathrm{Gal}(L_w/K_v), \mathbb{Z})
\end{array}.$$

We deduce $\mathrm{inv}_v(\overline{\alpha} \cup \delta(\chi)) = \mathrm{inv}_{K_v}(\overline{\alpha_v} \cup \delta(\chi_v)) = \chi_v(\rho_{L_w/K_v}(\alpha_v))$ where $\chi_v := \chi|_{\mathrm{Gal}(L_w/K_v)}(= \mathrm{Res}(\chi))$, and the last equality follows from Proposition 3.3.4. We deduce hence

$$\begin{aligned}
\sum_v \mathrm{inv}_v(\overline{\alpha} \cup \delta(\chi)) &= \sum_v \chi_v(\rho_{L_w/K_v}(\overline{\alpha_v}) \\
&= \sum_v \chi(\rho_{L_w}/K_v(\overline{\alpha_v})) = \chi(\prod_v \rho_{L_w/K_v}(\alpha_v)) = \chi(\Phi_{L/K}(\alpha)).
\end{aligned}$$

□

Lemma 5.5.2. *For any $n \in \mathbb{Z}_{\geq 1}$, $a \in \mathbb{Q}^\times$, we have $\Phi_{\mathbb{Q}}(a)(\zeta_n) = \zeta_n$.*

Proof. It sufficient to prove the case where a is a prime number q or -1, and $n = p^k$. First suppose $q \neq p$:

- for a prime number ℓ different from p and q, the extension $\mathbb{Q}_\ell(\zeta_{p^k})$ is unramified, and $q \in \mathbb{Z}_\ell^\times$ hence $\rho_{\mathbb{Q}_\ell}(q)(\zeta_{p^k}) = \zeta_{p^k}$;
- $\mathbb{Q}_q(\zeta_{p^k})$ is unramified, hence $\rho_{\mathbb{Q}_q}(q)$ acts on $\mathbb{Q}_q(\zeta_{p^k})$ via the Frobenius: $\rho_{\mathbb{Q}_q}(q)(\zeta_{p^k}) = \zeta_{p^k}^q$;
- as $q \in \mathbb{Z}_p^\times$, $\rho_{\mathbb{Q}_p}(q)(\zeta_{p^k}) = \zeta_{p^k}^{1/q}$;
- $\rho_{\mathbb{R}}(q)(\zeta_{p^k}) = \zeta_{p^k}$.

We see $\Phi_{\mathbb{Q}}(q)(\zeta_{p^k}) = \zeta_{p^k}$. If $q = p$, then

$$\begin{cases} \rho_{\mathbb{Q}_\ell}(p)(\zeta_{p^k}) = \zeta_{p^k}, & \ell \neq p, \\ \rho_{\mathbb{Q}_p}(p)(\zeta_{p^k}) = \zeta_{p^k}, \\ \rho_{\mathbb{R}}(p)(\zeta_{p^k}) = \zeta_{p^k}. \end{cases}$$

Finally, we have

$$\begin{cases} \rho_{\mathbb{Q}_\ell}(-1)(\zeta_{p^k}) = \zeta_{p^k} & \ell \neq p, \\ \rho_{\mathbb{Q}_p}(-1)(\zeta_{p^k}) = \zeta_{p^k}^{-1} \\ \rho_{\mathbb{R}}(-1)(\zeta_{p^k}) = \zeta_{p^k}^{-1} \end{cases}$$

The lemma follows. □

Lemma 5.5.3. *Suppose $L \subset K(\zeta_n)$, then $\Phi_{L/K}(a) = 1$ for all $a \in K^\times$.*

Proof. By Proposition 5.2.6, we have $\Phi_{K(\zeta_n)/K}(a)|_{\mathbb{Q}(\zeta_n)} = \Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(N_{K/\mathbb{Q}}(a))$. □

Before going further, we give/recall some facts on Tate cohomology.

Lemma 5.5.4. *Let G be a finite cyclic group of order n, $\chi : G \to \mathbb{Q}/Z$, and δ be the connecting map for $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Let g be a generator of G, viewed as an element, denote by u_g, in $H_T^{-2}(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$. Let $\tilde{\chi}$ be the composition $G \to \frac{1}{\mathbb{Z}}/\mathbb{Z} \xrightarrow{n} \mathbb{Z}/n\mathbb{Z}$. Then $u_g \cup \delta(\chi) = \tilde{\chi}(g) \in H_T^0(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. The lemma follows from Lemma 3.3.2 and the following commutative diagram:

$$\begin{array}{ccccc} H_T^{-2}(G,\mathbb{Z}) \times H_T^2(G,\mathbb{Z}) & \xrightarrow{\cup} & H_T^0(G,\mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z}/n\mathbb{Z} \\ \| \quad\quad \delta\downarrow\sim & & \delta\downarrow\sim & & n\downarrow \\ H_T^{-2}(G,\mathbb{Z}) \times H_T^1(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\cup} & H_T^{-1}(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & (1/n)\mathbb{Z}/\mathbb{Z} \end{array}$$

□

Corollary 5.5.5. *Keep the situation as in the above lemma, and suppose χ is injective. Let A be a G-module, then the map*

$$H_T^i(G, A) \to H_T^{i+2}(G, A), \; c \mapsto \delta(\chi) \cup c$$

is an isomorphism.

Proof. The composition $H_T^{i+2}(G, A) \xrightarrow{\cup u_g} H_T^i(G, A) \xrightarrow{\cup\delta(\chi)} H_T^{i+2}(G, A)$ is given by $c \mapsto c\cup(u_g \cup \delta(\chi)) = \tilde{\chi}(g)c$, hence is an isomorphism. Similarly, $H_T^i(G, A) \xrightarrow{\cup\delta(\chi)} H_T^{i+2}(G, A) \xrightarrow{\cup u_g} H_T^i(G, A)$ is also an isomorphism. The corollary follows. □

The following lemma will allow us to use cyclotomic extensions to study Brauer groups on number fields in general.

Lemma 5.5.6. *Let S be a finite set of places of K containing all archimedean places. For $n \in \mathbb{Z}_{\geq 1}$, there exists a cyclic extension L of K contained in $K(\zeta_N)$ for some $N \geq 1$ such that $[L_w : K_v]$ is divisible by n for $v \in S_f$, and $[L_w : K_v] = 2$ for all real places of K.*

Proof. We can and do assume n is even, and write $n = \prod_i p_i^{e_i}$. For each odd p_i, consider $\tilde{L}_i := \varinjlim_m K(\zeta_{p_i^m})_{p_i}$, where $K(\zeta_{p_i^m})_{p_i}$ denotes the maximal subextension in $K(\zeta_{p_i^m})$ of p-th power degree over K. For $p_i = 2$, let $\tilde{L}_i := \varinjlim_m K(\zeta_{2^m} - \zeta_{2^m}^{-1})$ (noting $\mathbb{Q}(\zeta_{2^m} - \zeta_{2^m}^{-1})$ is totally imaginary). Put $\tilde{L}$ to be the composition of $\tilde{L}_i$. Then $\tilde{L}$ is a procyclic extension of K. Let L_i be the subfield of $\tilde{L}_i$ such that $p_i^{e_i} | [L_{i,w} : K_v]$ for $v \in S_f$, and L be the composition of L_i (that is a subextension of $\tilde{L}$). Then L satisfies the properties in the lemma. □

Proposition 5.5.7. *The map $\tilde{\mathrm{inv}}_K = \sum_v \mathrm{inv}_v : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \to \mathbb{Q}/\mathbb{Z}$ is trivial.*

Proof. Let $\beta \in H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$, and S be the set of places such that $\mathrm{inv}_v(\beta) \neq 0$. Let n be the least common multiple of the orders of the elements $\mathrm{inv}_v(\beta)$. By Lemma 5.5.6, let $L \subset K(\zeta_N)$ (with N sufficiently large) be a cyclic extension of K such that L_w/K_v is divisible by n for all $v \in S_f$ and $L_w = \mathbb{C}$ for all $w|\infty$. In particular, $n|\#H^2(\mathrm{Gal}(L_w/K_v), L_w^\times)$ for $v \in S_f$. We have $\mathrm{inv}_v(\beta) \in \mathrm{inv}_v\left(H^2(\mathrm{Gal}(L/K), \overline{K}^\times)\right)$ for all $v \in S$. We have a commutative diagram

$$\begin{array}{ccc} H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) & \longrightarrow & \oplus_v \mathbb{Q}/Z \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow \\ H^2(\mathrm{Gal}(\overline{K}/L), \overline{K}^\times) & \longrightarrow & \oplus_w \mathbb{Q}/\mathbb{Z} \end{array}$$

where the right vertical map sends (a_v) to $(([L_w : K_v]a_v)_{w|v})$. As $H^1(\mathrm{Gal}(\overline{K}/L), \overline{K}^\times) = 1$, the kernal of the left vertical map is $H^2(\mathrm{Gal}(L/K), L^\times)$. We deduce $\beta \in H^2(\mathrm{Gal}(L/K), L^\times)$. Let $\chi : \mathrm{Gal}(L/K) \hookrightarrow \mathbb{Q}/\mathbb{Z}$, then there exists $b \in H_T^0(\mathrm{Gal}(L/K), L^\times)$ such that $\beta = b \cup \delta(\chi)$ We have $\Phi(L/K)(b) = 1$ hence $\chi(\Phi_{L/K}(b)) = 1$. Thus $\sum_v \mathrm{inv}_v(b \cup \delta(\chi)) = \chi(\Phi_{L/K}(b)) = 1$. □

Corollary 5.5.8. $\Phi_K(a) = 1$ *for all* $a \in K^\times$.

Proof. Let L be a finite abelian extension of K. We have $\chi(\Phi_{L/K}(a)) = \sum_v \mathrm{inv}_v(a \cup \delta(\chi)) = 0$ for any character $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/Z$. Hence $\Phi_{L/K}(a) = 1$ (for all L). The corollary follows. □

Proposition 5.5.9. *Let L/K be a finite cyclic extension, then $\tilde{\mathrm{inv}}_{L/K}$ induces an isomorphism $\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \xrightarrow{\sim} \frac{1}{|\mathrm{Gal}(L/K)|}\mathbb{Z}/\mathbb{Z}$.*

Proof. The exact sequence $1 \to L^\times \to I_L \to \mathbb{C}_L \to 1$ induces

$$1 \to H^2(\mathrm{Gal}(L/K), L^\times) \to H^2(\mathrm{Gal}(L/K), I_L) \to H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \to 1$$

By Corollary 5.3.12, for each $p|[L : K]$ with $e = \mathrm{val}_p([L : K])$, there exist places v of K such that $[L_w : K_v] = p^e$. We then deduce $\tilde{\mathrm{inv}}_{L/K} = \sum_v \mathrm{inv}_v : H^2(\mathrm{Gal}(L/K), I_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$

is surjective. By Proposition 5.5.7 and the above exact sequence, $\tilde{\mathrm{inv}}_{L/K}$ induces $\mathrm{inv}_{L/K}$: $H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \twoheadrightarrow \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, which has to be surjective hence bijective by the second inequality. □

Let $\mathcal{E}_K$ be the set of finite cyclic extensions of K which are contained in $K(\zeta_N)$ for certain N. By Proposition 5.5.9 and taking limit, we get:

Corollary 5.5.10. *The natural morphism*

$$\varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), I_L) \longrightarrow \varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)$$

is surjective, and $\tilde{\mathrm{inv}}_K$ *on* $\varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), I_L)$ *factors through a bijection*

$$\mathrm{inv}_K : \varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}. \tag{5.7}$$

Lemma 5.5.11. *Let $L \supset E \supset K$ be finite Galois extensions, then the following diagram commutes*

$$\begin{array}{ccc} H^2(\mathrm{Gal}(L/K), I_L) & \xrightarrow{\tilde{\mathrm{inv}}_{L/K}} & \frac{1}{|\mathrm{Gal}(L/K)|}\mathbb{Z}/\mathbb{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & {\scriptstyle [E:K]}\downarrow \\ H^2(\mathrm{Gal}(L/E), I_L) & \xrightarrow{\tilde{\mathrm{inv}}_{L/E}} & \frac{1}{|\mathrm{Gal}(L/E)|}\mathbb{Z}/\mathbb{Z} \end{array}.$$

Proof. Let v be a place of K, and w be a place of L dividing v. For each place $u|v$ of E, there exists $\sigma_u \in \mathrm{Gal}(L/K)$ such that $\sigma_u(w)|u$. Recall σ_u induces an isomorphism $\sigma_u : L_w^\times \xrightarrow{\sim} L_{\sigma_u(w)}^\times$, that is compatible with the group homomorphism $D_w \to D_{\sigma_u(w)}$, $g \mapsto \sigma_u g \sigma_u^{-1}$. Denote by ι_u the following composition

$$H^2(D_w, L_w^\times) \underset{\sim}{\xrightarrow{\sigma_u^*}} H^2(D_{\sigma_u(w)}, L_{\sigma_u(w)}^\times) \xrightarrow{\mathrm{Res}} H^2(\mathrm{Gal}(L_{\sigma_u(w)}/E_u), L_{\sigma_u(w)}^\times).$$

To prove the lemma, it is sufficient to show the following diagram commutes:

$$\begin{array}{ccccc} H^2(\mathrm{Gal}(L/K), \prod_{w|v} L_w^\times) & \xrightarrow{\sim} & H^2(D_w, L_w^\times) & \xrightarrow{\mathrm{inv}_v} & \frac{1}{|\mathrm{Gal}(L/K)|}\mathbb{Z}/\mathbb{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & {\scriptstyle \iota=(\iota_u)}\downarrow & & {\scriptstyle [E:K]}\downarrow \\ H^2(\mathrm{Gal}(L/E), \prod_{w|v} L_w^\times) & \xrightarrow{\sim} & \oplus_{u|v} H^2(\mathrm{Gal}(L_{\sigma_u(w)}/E_u), L_{\sigma_u(w)}^\times) & \xrightarrow{\sum_u \mathrm{inv}_u} & \frac{1}{|\mathrm{Gal}(L/E)|}\mathbb{Z}/\mathbb{Z} \end{array}.$$

However, we have (using $\mathrm{inv}_{L_{\sigma_u(w)}/K_v} \circ \sigma_u^* = \mathrm{inv}_{L_w/K_v}$ for the third equation)

$$\begin{aligned} \sum_{u|v} \mathrm{inv}_{L_{\sigma_u(w)}/E_u} \circ \iota_u &= \sum_{u|v} [E_u : K_v] \, \mathrm{inv}_{L_{\sigma_u(w)}/K_v} \circ \sigma_u^* \\ &= \sum_{u|v} [E_u : K_v] \, \mathrm{inv}_{L_w/K_v} = [E : K] \, \mathrm{inv}_{L_w/K_v} . \end{aligned}$$

The lemma follows. □

Proposition 5.5.12. *Let L/K be a finite Galois extension, then $H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)$ is cyclic of order $[L : K]$.*

Proof. For any finite Galois extension M/K, denote by

$$H^2(\mathrm{Gal}(M/K), \mathbb{C}_M)_0 \subset H^2(\mathrm{Gal}(M/K), \mathbb{C}_M)$$

the image of the natural map $H^2(\mathrm{Gal}(M/K), I_M) \to H^2(\mathrm{Gal}(M/K), \mathbb{C}_M)$. The map $\tilde{\mathrm{inv}}_{M/K}$ then induces a map $\mathrm{inv}_{M/K} : H^2(\mathrm{Gal}(M/K), \mathbb{C}_M)_0 \to \mathbb{Q}/Z$. Note if M/K is cyclic, we have by Proposition 5.5.9: $H^2(\mathrm{Gal}(M/K), \mathbb{C}_M)_0 = H^2(\mathrm{Gal}(M/K), \mathbb{C}_M)$. We have an exact sequence

$$\begin{array}{ccccc}
1 \to H^2(\mathrm{Gal}(L/K), I_L) & \longrightarrow & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), I_{LM}) & \longrightarrow & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/L), I_{LM}) \\
\downarrow & & \downarrow & & \downarrow \\
1 \to H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) & \longrightarrow & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM}) & \longrightarrow & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/L), \mathbb{C}_{LM})
\end{array} \tag{5.8}$$

which induces an exact sequence

$$1 \to H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)'_0 \to \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM})_0 \to \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/L), \mathbb{C}_{LM})$$

where $H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)'_0 := H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \cap \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM})_0$ (that contains $H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)_0$).

By Lemma 5.5.11, we can deduce a commutative diagram

$$\begin{array}{ccc}
\varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM})_0 & \xrightarrow{\mathrm{Res}} & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/L), \mathbb{C}_{LM}) \\
{\scriptstyle \mathrm{inv}'_K}\downarrow & & {\scriptstyle \mathrm{inv}_L}\downarrow\wr \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z}
\end{array}.$$

We also have a commutative diagram

$$\begin{array}{ccc}
\varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(M/K), \mathbb{C}_M) & \xrightarrow{\mathrm{inf}} & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM})_0 \\
{\scriptstyle \mathrm{inv}_K}\downarrow\wr & & {\scriptstyle \mathrm{inv}'_K}\downarrow \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Q}/\mathbb{Z}
\end{array}.$$

We let $\iota := \mathrm{inf} \circ \mathrm{inv}_K^{-1} : \mathbb{Q}/Z \hookrightarrow \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM})_0$. We have thus

$$\begin{array}{ccccc}
 & & \mathbb{Q}/Z & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \\
 & & {\scriptstyle \mathrm{inv}'_K}\uparrow & & {\scriptstyle \mathrm{inv}_K}\uparrow\wr \\
0 \to H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)'_0 & \longrightarrow & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/K), \mathbb{C}_{LM})_0 & \longrightarrow & \varinjlim_{M\in\mathcal{E}_K} H^2(\mathrm{Gal}(LM/L), \mathbb{C}_{LM}) \\
 & & {\scriptstyle \iota}\uparrow & & {\scriptstyle \mathrm{inv}_L^{-1}}\uparrow\wr \\
 & & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z}
\end{array}. \tag{5.9}$$

The map ι induces $\iota : \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)'_0 \hookrightarrow H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)$, and the composition has to be bijective by the second inequality. In particular, $H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)$ is cyclic of order $[L : K]$. □

Corollary 5.5.13. *The morphism $\varinjlim_L H^2(\mathrm{Gal}(L/K), I_L) \to \varinjlim_L H^2(\mathrm{Gal}(L/K), \mathbb{C}_L)$ is surjective, and $\widetilde{\mathrm{inv}}_K$ factors through a bijection*

$$\mathrm{inv}_K : \varinjlim_L H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}. \tag{5.10}$$

Proof. We have by Corollary 5.5.10 (where the injection is induced by inflation)

$$\mathbb{Q}/\mathbb{Z} \xrightarrow[\sim]{\mathrm{inv}_K^{-1}} \varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \to \varinjlim_{\substack{L/K \\ \text{finite Galois}}} H^2(\mathrm{Gal}(L/K), \mathbb{C}_L).$$

By the precedent proposition, we see the map is in fact bijective. We have a commutative diagram

$$\begin{array}{ccc} \varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), I_L) & \longrightarrow & \varinjlim_{\substack{L/K \\ \text{finite Galois}}} H^2(\mathrm{Gal}(L/K), I_L) \\ \downarrow & & \downarrow \\ \varinjlim_{L\in\mathcal{E}_K} H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) & \xrightarrow{\sim} & \varinjlim_{\substack{L/K \\ \text{finite Galois}}} H^2(\mathrm{Gal}(L/K), \mathbb{C}_L) \end{array}.$$

The first part then follows from Corollary 5.5.10. Together with Proposition 5.5.7 (and an obvious exact sequence), the second part also follows. □

Theorem 5.5.14. *Let K be a number field. Then $(\mathbb{C}_{\overline{K}} := \varinjlim_L \mathbb{C}_L, \mathrm{inv})$ is a class formation. Moreover, the induced reciprocity map $\mathbb{C}_K \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ coincides with Φ_K.*

Proof. Let L be a finite extension of K. We have $H^1(\mathrm{Gal}(\overline{K}/L), \mathbb{C}_L) = 1$, and $\mathrm{inv}_L : H^2(\mathrm{Gal}(\overline{K}/L), \mathbb{C}_L) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Moreover, by Lemma 5.5.11 (and taking limit), for a finite subextension E of L over K, we have $\mathrm{inv}_L \circ \mathrm{Res}_{E/L} = [L : E]\,\mathrm{inv}_E$. So $(\mathbb{C}_{\overline{K}}, \mathrm{inv})$ is a class formation. Let $\Phi'_K : \mathbb{C}_K \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ be the induced reciprocity map. Then for a finite abelian extension L/K, and $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/Z$, we have $\mathrm{inv}_{L/K}(\overline{a} \cup \delta(\chi)) = \chi(\Phi'_{L/K}(a))$. However, by definition, we also have $\mathrm{inv}_{L/K}(\overline{a} \cup \delta(\chi)) = \chi(\Phi_{L/K}(a))$. By Pontryagain duality, this implies $\Phi'_{L/K} = \Phi_{L/K}$ hence $\Phi'_K = \Phi_K$. □

Let L be a finite extension of K. Then $L^\times$ is a closed and discrete subgroup of I_L. We deduce $\mathbb{C}_L$, equipped with the quotient topology, is Hausdorff. If L/K is moreover Galois, it is clear that $\mathbb{C}_L$ is a topological $\mathrm{Gal}(L/K)$-module.

Lemma 5.5.15. *We have an isomorphism of topological groups $\mathbb{C}_K \cong I_K^1/K^\times \times \mathbb{R}_{>0}$.*

Proof. We have an exact sequence $1 \to I_K^1/K^\times \to \mathbb{C}_K \xrightarrow{|\cdot|_{I_K}} \mathbb{R}_{>0} \to 1$. Let v be an archimedean place of K, then $K_v \xrightarrow{|\cdot|_v} \mathbb{R}_{>0}$ admits a section, i.e. there exists a continuous map $\iota_v : \mathbb{R}_{>0} \hookrightarrow K_v$ such that $|\cdot|_v \circ \iota_v = \mathrm{id}$. We deduce $|\cdot|_{I_K}$ admits a section ι that is equal to ι_v at v and to 1 for places different from v. The lemma follows. □

Proposition 5.5.16. *With the above natural topology on* $\mathbb{C}_L$*,* $(\varinjlim_L \mathbb{C}_L, \mathrm{inv})$ *becomes a topological class formation.*

Proof. We check the three conditions in Definition 4.2.9.

(1) Let $M \supset L$ be finite extensions of K. By Proposition 5.2.8, we easily deduce $N_{M/L}(\mathbb{C}_M)$ is open hence closed in $\mathbb{C}_L$. We have $\mathrm{Ker}(N_{M/L})$ is closed and contained in the compact set $I_L^1/K^\times$. Hence $\mathrm{Ker}(N_{M/L})$ is compact.

(3) For a finite extension L over K, we take $U_L := I_L^1/L^\times \subset \mathbb{C}_L$. Then any closed subgroup of finite index in $I_L/L^\times$ containing I_L^1 has to be $I_L/L^\times$ hence is a norm group.

(2) Let $K_p := K(\zeta_p)$. Let L be a finite extension of $K(\zeta_p)$. We have $\ker[\phi_p : \mathbb{C}_L \to \mathbb{C}_L, x \mapsto x^p]$ is closed in $I_L^1/L^\times$ hence compact. We construct certain norm groups. Let S be a finite set of places of L containing all archimedean places, places dividing p, that is sufficiently large such that $\{\mathfrak{p}_v\}_{v\in S_f}$ generates Cl_L. So $\mathbb{C}_L \cong I_{L,S}/\mathcal{O}_{L,S}^\times$. For a finite set $S \supset S$ of places of L, put $J_{L,S} := \prod_{v\in S}(L_v^\times)^p \times \prod_{v\notin S}\mathcal{O}_v^\times \supset I_{L,S}^p$. Let $L_S := L((\mathcal{O}_{L,S}^\times)^{\frac{1}{p}})$. By Kummer's theory, L_S is an abelian extension over L of degree $|\mathcal{O}_{L,S}^\times/(\mathcal{O}_{L,S}^\times)^p| = p^{|S|}$ (see the proof of Lemma 5.4.7). It is clear that $J_{L,S} \subset N_{L_S/L}(I_{L_S})$. By similar arguments as in Lemma 5.4.10, we have $J_{L,S} \cap L^\times = (\mathcal{O}_{L,S}^\times)^p$: for $x \in J_{L,S} \cap L^\times$, $L(x^{\frac{1}{p}})$ is split at $v \in S$ at unramified at $v \notin S$, thence $N_{L(x^{\frac{1}{p}})/L}(I_{L(x^{\frac{1}{p}})}) \supset I_{L,S}$ implying $L(x^{\frac{1}{p}}) = L$. Then by the proof of Lemma 5.4.9, we deduce

$$[I_L : L^\times J_{L,S}] = p^{|S|} = [L_S : L].$$

As $\# H_T^0(\mathrm{Gal}(L_S/L), \mathbb{C}_{L_S}) = p^{|S|}$, we deduce $N_{L_S/L}(\mathbb{C}_{L_S}) = L^\times J_{L,S}/L^\times$.

Next we show $(L^\times I_L^p)/L^\times$ is an intersection of certain norm groups (which concludes the proof). Recall we have $L^\times I_{L,S}/L^\times \cong I_L^1/L^\times \times \mathbb{R}_{>0}$, we deduce $(L^\times I_{L,S}^p)/L^\times \cong (I_L^1/L^\times)^p \times \mathbb{R}_{>0}$. As the map ϕ_p is continuous and $I_L^1/L^\times$ is compact, we see $(I_L^1/L^\times)^p$ is also compact and hence closed (noting $I_L/L^\times$ is Hausdorff). So $(L^\times I_{L,S}^p)/L^\times \cong (I_L^1/L^\times)^p \times \mathbb{R}_{>0}$ is also a closed subgroup of $\mathbb{C}_L$. As $I_L^1/L^\times$ is compact, it is not difficult to show the closed subgroup $(I_L^1/L^\times)^p$ is equal to the intersection of open subgroups (of finite index) which contain $(I_L^1/L^\times)^p$. We deduce $(L^\times I_L^p)/L^\times$ is also equal to the intersection of open subgroups H of finite index in $\mathbb{C}_L$ which contain $(L^\times I_L^p)/L^\times$. For such a group H, denote by U the premage in I_L (then $L^\times \subset U$ and $I_L/U \cong \mathbb{C}_L/H$). Note $\mathbb{C}_L/H$ is p-torsion. As U is open, there exists S sufficiently large such that $U \supset \prod_{v\in S} 1 \times \prod_{v\notin S}\mathcal{O}_v^\times$. As $I_L^p \subset U$, we have $\prod_{v\in S}(K_v^\times)^p \times \prod_{v\notin S}\mathcal{O}_v^\times \subset U$ hence $U \supset L^\times J_{L,S}$. We deduce $H = U/L^\times$ is a norm group. This finishes the proof. □

Corollary 5.5.17. *A subgroup* H *of* $\mathbb{C}_K$ *is a norm group if and only if* H *is open of finite index.*

Let $K_\infty := \prod_{v|\infty} K_v$ and K_∞^0 be the connected component of $1 \in K_\infty^\times$. The reciprocity map $\Phi_K : I_K/K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ factors through $I_K/K^\times K_\infty^o$ hence factors through $I_K/\overline{K^\times K_\infty^o}$ where $\overline{K^\times K_\infty^o}$ denotes the closure. As $I_K/\overline{K^\times K_\infty^o}$ is profinite, we finally deduce:

Corollary 5.5.18. *The reciprocity map Φ_K induces an isomorphism*

$$I_K/\overline{K^\times K_\infty^o} \xrightarrow{\sim} \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}. \tag{5.11}$$

Corollary 5.5.19 (Kronecker-Weber theorem)**.** *We have* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}} \cong \widehat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times$ *and any finite abelian extension of* $\mathbb{Q}$ *is contained in a certain cyclotomic field.*

Proof. We have $I_\mathbb{Q} \cong \mathbb{Q}^\times(\mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times$. Hence the natural injection $\prod_p \mathbb{Z}_p^\times \hookrightarrow I_\mathbb{Q}$ induces an isomorphism $\prod_p \mathbb{Z}_p^\times \xrightarrow{\sim} I_\mathbb{Q}/\overline{\mathbb{Q}^\times \mathbb{R}_{>0}}$. Hence we have $\mathrm{Gal}(\overline{\mathbb{Q}}/Q)^{\mathrm{ab}} \cong \widehat{\mathbb{Z}}^\times$. We write κ the induced map $\mathbb{C}_\mathbb{Q} \twoheadleftarrow \widehat{\mathbb{Z}}^\times$. Let K be a finite abelian extension of $\mathbb{Q}$, to show $K \subset \mathbb{Q}(\zeta_N)$ for a sufficiently large N, it suffices to show $\kappa\big(N_{K/\mathbb{Q}}(\mathbb{C}_K)\big)$ contains $\kappa\big(N_{K/\mathbb{Q}}(\mathbb{C}_{\mathbb{Q}(\zeta_N)})\big)$. Writing $N = \prod p_i^{e_i}$, we have $N_{\mathbb{C}_{\mathbb{Q}(\zeta_N)}/\mathbb{Q}}(\mathbb{C}_{\mathbb{Q}(\zeta_N)}) = \cap N_{\mathbb{Q}(\zeta_{p_i^{e_i}})/\mathbb{Q}}(\mathbb{C}_{\mathbb{Q}(\zeta_{p_i^{e_i}})})$. We calculate hence $N_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}}(\mathbb{C}_{\mathbb{Q}(\zeta_{p^e})})$ for a prime number e. We have $[\mathbb{Q}(\zeta_{p^e}) : \mathbb{Q}] = p^{e-1}(p-1)$. For $\ell \neq p$, $\mathbb{Q}_\ell(\zeta_{p^e})$ is unramfied, hence $N_{\mathbb{Q}_\ell(\zeta_{p^e})/\mathbb{Q}_\ell}(\mathbb{Q}_\ell(\zeta_{p^e})^\times) \supset \mathbb{Z}_\ell^\times$. At p, we have $N_{\mathbb{Q}_p(\zeta_{p^e})/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_{p^e})^\times) \supset 1 + p^e\mathbb{Z}_p$. We deduce $N_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}}(I_{\mathbb{Q}(\zeta_{p_i^{e_i}})}) \supset \mathbb{R}_{>0} \times (1 + p^e\mathbb{Z}_p) \times \prod_{\ell\neq p} \mathbb{Z}_\ell^\times$. By comparing the order, we deduce $\kappa\big(N_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}}(\mathbb{C}_{\mathbb{Q}(\zeta_{p_i^{e_i}})})\big) = (1+p^e\mathbb{Z}_p) \times \prod_{\ell\neq p} \mathbb{Z}_\ell^\times)$. Let $H := \kappa(N_{K/\mathbb{Q}}(\mathbb{C}_K))$ (that is open of finite index in $\widehat{\mathbb{Z}}^\times$), it is clear that there exist $p_i^{e_i}$ such that $H \supset \prod_i (1 + p_i^{e_i}\mathbb{Z}_{p_i}) \times \prod_{\ell \neq p_i} \mathbb{Z}_\ell^\times$. Hence $K \subset \mathbb{Q}(\zeta_N)$ with $N = \prod p_i^{e_i}$. □

5.6 Global class field theory via ideals

Recall a modulus $\mathfrak{m}$ of K is a formal product $\mathfrak{m}^\infty \mathfrak{m}_\infty$ where $\mathfrak{m}^\infty = \prod_v \mathfrak{p}_v^{e_v}$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a subset of $\{\sigma : K \hookrightarrow \mathbb{R}\}$. For a place v of K, we write $v|\mathfrak{m}$ if $\mathfrak{p}_v|\mathfrak{m}^\infty$ when v is non-archimedean, and if $v \in \mathfrak{m}_\infty$ when v is archimedean. For $v|\mathfrak{m}$, define

$$U_v(\mathfrak{m}) := \begin{cases} \mathbb{R}_{>0} & v|\infty \\ 1 + \mathfrak{p}_v^{e_v}\mathcal{O}_{K_v} & v \nmid \infty \end{cases}.$$

Define $J_K(\mathfrak{m}) \subset J_K$ to be the group of fractional ideals that are relatively prime to $\mathfrak{m}^\infty$ (i.e. that do not have $\mathfrak{p}_v$-factor in the prime decomposition for all $\mathfrak{p}_v|\mathfrak{m}^\infty$). Put $P_K(\mathfrak{m}) = \{(\alpha) \mid \alpha \in K^\times, \alpha \in U_v(\mathfrak{m}) \ \forall v|\mathfrak{m}\}$. The quotient $J_K(\mathfrak{m})/P_K(\mathfrak{m})$ is finite and called a Ray class group of K.

Let $I_{K,\infty} := \prod_{v|\infty} K_v^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$. Put $I_K(\mathfrak{m}) := I_K \cap \prod_{v|\mathfrak{m}} U_v(\mathfrak{m}) \times \prod_{v\nmid\mathfrak{m}} K_v^\times$, $W_K(\mathfrak{m}) := I_K(\mathfrak{m}) \cap I_{K\infty}$ that is a open subgroup of $I_K(\mathfrak{m})$. Consider the natural morphism

$$I_K(\mathfrak{m}) \longrightarrow J_K(\mathfrak{m}),\ (x_v) \mapsto \prod_v \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}.$$

It is clear that this map is surjective, with the kernel equal to $W_K(\mathfrak{m})$. We deduce then an isomorphism

$$I_K(\mathfrak{m})/W_K(\mathfrak{m})(K^\times \cap I_K(\mathfrak{m})) \xrightarrow{\sim} I_K(\mathfrak{m})/P_K(\mathfrak{m}), \tag{5.12}$$

which gives an adelic description of the ray class group. Recall the natural injection $I_K(\mathfrak{m}) \hookrightarrow I_K$ induces an isomorphism $I_K(\mathfrak{m})/(I_K(\mathfrak{m}) \cap K^\times) \xrightarrow{\sim} I_K/K^\times$.

Let L/K be a finite abelian extension. Let $\mathfrak{m}$ be a modulus divisible by all ramified primes (including infinite primes) of K in the extension L/K. For $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{p} \nmid \mathfrak{m}$, recall we have the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$: $\left(\frac{L/K}{\mathfrak{p}}\right)(x) \equiv x^{N(\mathfrak{p})} \equiv \mathfrak{P}$ for all $x \in \mathcal{O}_L$, and for $\mathfrak{P}$ a (or any) prime ideal of $\mathcal{O}_L$ dividing $\mathfrak{p}$. We have then a morphism

$$J_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K),\ \prod \mathfrak{p}^{e_\mathfrak{p}} \mapsto \prod \left(\frac{L/K}{\mathfrak{p}}\right)^{e_\mathfrak{p}}. \tag{5.13}$$

Theorem 5.6.1. *There exists a modulus $\mathfrak{m}$ divisible exactly by all ramified primes of K in L/K such that the induced map $I_K(\mathfrak{m}) \to J_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ coincides with Φ_K. Moreover, in this case, the morphism (5.13) factors through a surjective map*

$$J_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K).$$

Proof. Let $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}^\infty$ be a modulus divisible exactly by all ramified primes of K in L/K such that $W_K(\mathfrak{m}) \subset N_{L/K}(I_L)$. Then we have a surjective map $I_K(\mathfrak{m})/((I_K(\mathfrak{m}) \cap K^\times)W_K(\mathfrak{m})) \twoheadrightarrow \mathrm{Gal}(L/K)$. Together with the isomorphism (5.12), we obtain $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K)$, which by definition coincides with (5.13). The theorem follows. □

Recall we have $I_K/(K^\times I_{K,\infty}) \xrightarrow{\sim} J_K/P_K \cong \mathrm{Cl}_K$. By Corollary 5.5.17, there is an abelian extension H/K such that $I_K/(K^\times I_{K,\infty}) \xrightarrow{\sim} \mathrm{Gal}(H/K)$, that is called the Hilbert class field of K.

Proposition 5.6.2. *H is the maximal unramified abelian extension of K.*

Proof. By the local-global compatibility of class field theory, we have for any place v of K:

$$\begin{array}{ccc} I_K/(K^\times I_{K,\infty}) & \xrightarrow{\Phi_{H/K}} & \mathrm{Gal}(H/K) \\ \uparrow & & \uparrow \\ K_v^\times & \xrightarrow{\rho_{H_w/K_v}} & \mathrm{Gal}(H_w/K_v) \end{array}.$$

We see $\rho_{H_w/K_v}(\mathcal{O}_v^\times) = 1$ hence H_w/K_v is unramified. Let L be a finite unramified abelian extension of K. Then $I_{K,\infty} \subset N_{L/K} I_L$. We deduce $N_{L/K}(\mathbb{C}_L) \supset N_{H/K}(\mathbb{C}_H)$ hence $L \subset H$. □

We end the section by the so-called principal ideal theorem.

Theorem 5.6.3. *Let H be the Hilbert class field of K. For any fractional ideal $\mathfrak{a}$ in K, $\mathfrak{a}\mathcal{O}_H$ is principal in H.*

Proof. Let H' be the Hilbert class field of H, then we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Cl}_K \cong I_K/(K^\times I_{K,\infty}) & \longrightarrow & I_H/(H^\times I_{H,\infty}) \cong I_H \\ \Phi_K \downarrow & & \Phi_H \downarrow \\ \mathrm{Gal}(H/K) \cong \mathrm{Gal}(H'/K)^{\mathrm{ab}} & \xrightarrow{V} & \mathrm{Gal}(H'/H) \cong \mathrm{Gal}(H'/H)^{\mathrm{ab}} \end{array}.$$

The theorem amounts to say that the top map is trivial, which follows from the following lemma. □

Lemma 5.6.4. *Let G be a finite group, G' be the commutator subgroup. Then the transfer map $G^{\mathrm{ab}} \to G'^{\,\mathrm{ab}}$ is trivial.*

Proof. See Theorem VI.7.6 of *Algebraic number theory* by Neukirch. □

Exercises

Exercise 1. (**Formal groups**) Let A be a commutative ring with 1.

(1) (1a) Let $f(T) \in A[[T]]$ with $f(T) \equiv aT \pmod{T^2}$, $a \in A^\times$. Show that there exists a unique $g(T) \in TA[[T]]$ such that $f(g(T)) = T$. Moreover, prove $g(f(T)) = T$.

(1b) Let F, G be (one-parameter commutative) formal group laws, and $h : F \to G$ be a morphism. Show that h admits an inverse if and only if $h(T) \equiv aT \pmod{T^2}$ with $a \in A^\times$.

(2) Let $f(T) = a_0 + a_1 T + \cdots \in A[[T]]$ with $a_0 \in A^\times$, show that there exists $g(T) \in A[[T]]$ such that $f(T)g(T) = 1$.

(3) Let $F(X,Y) \in A[[X,Y]]$ with $F(X,Y) \equiv X+Y+$terms of degree ≥ 2, and $F(X, F(Y,Z)) = F(F(X,Y), Z)$. Prove that $F(X,0) = X = F(0,X)$.

(4) Keep the situation as in (3), prove that there exists a unique $i_F(X) \in A[[X]]$ such that $F(X, i_F(X)) = 0$.

(5) Suppose $\mathbb{Q} \hookrightarrow A$, prove that the formal groups over A: $F(X,Y) = X + Y$ and $G(X,Y) = X + Y + XY$ are isomorphic (hint: consider $\exp(T) = \sum_{n=0}^{\infty} \frac{T^n}{n}$).

(6) Suppose $\mathbb{Q} \hookrightarrow A$, we show that any formal group $F(X,Y)$ over A is isomorphic to the (trivial) additive formal group $X + Y$:

(6a) Let $f(X) := \frac{\partial F}{\partial Y}(X,Y)|_{Y=0} \in A[[X]]$. Prove

$$\frac{\partial F}{\partial Y}(X,Y) f(X) = f(F(X,Y)).$$

(6b) Let $h(X) \in A[[X]]$ such that $h'(X) = \frac{1}{f(X)}$ which is called the **logarithm** for F (here we use $\mathbb{Q} \hookrightarrow A$!). Prove

$$h(F(X,Y)) = h(X) + h(Y).$$

(hint: consider differentiating with respect to X.)

Exercise 2. (1) Prove that $p|\binom{p^n}{i}$ for $n \geq 1$, and $1 \leq i \leq p^n - 1$.

(2) Let $i \geq 0$, for $a \in \mathbb{Z}_p$, show that ($\binom{a}{0} := 1$)

$$\binom{a}{i} = \frac{a(a-1)\cdots(a-i+1)}{i!} \in \mathbb{Z}_p.$$

Moreover, show that the map $\mathbb{Z}_p \to \mathbb{Z}_p$, $a \mapsto \binom{a}{i}$ is continuous.
(3) For $a \in \mathbb{Z}_p$, show that $[a](T) := (1+T)^a - 1 := \sum_{i=0}^{\infty} \binom{a}{i} T^i - 1$ is a endomorphism of the formal group $F(X,Y) = X + Y + XY$ (over $\mathbb{Z}_p$). Moverover, show the morphism $\mathbb{Z}_p \hookrightarrow \mathrm{End}(F)$, $a \mapsto [a](T)$ is a ring homomorphism.

Exercise 3. Let K be a finite extension of $\mathbb{Q}_p$. Let F be a finite unramified extension of F. Let $d := [F : K]$, q be the cardinality of the residue field of K, let $\sigma \in \mathrm{Gal}(F/K)$ be the arithmetic Frobenius, i.e. $\sigma(x) \equiv x^q \pmod{\mathfrak{m}_F}$ for $x \in \mathcal{O}_F$.

(1) Let $a \in \mathfrak{m}_F$, $b \in \mathcal{O}_F$, prove that the equation $a\sigma(x) - x = b$ has a unique solution in $\mathcal{O}_F$.

We assume the following facts: for π, $\pi' \in \mathfrak{m}_F \setminus \mathfrak{m}_F^2$ with $N_{F/K}(\pi) = N_{F/K}(\pi')$, there exists $\delta \in \mathcal{O}_F$ such that $\frac{\pi}{\pi'} = \frac{\sigma(\delta)}{\delta}$.

For $F(X_1, \cdots, X_m) = \sum a_{i_1,\cdots,i_m} X_1^{i_1} \cdots X_m^{i_m} \in \mathcal{O}_F[[X_1, \cdots, X_m]]$, denote by

$$F^\sigma(X_1, \cdots, X_m) := \sum \sigma(a_{i_1,\cdots,i_m}) X_1^{i_1} \cdots X_m^{i_m} \in \mathcal{O}_F[[X_1, \cdots, X_m]].$$

Let $\alpha \in \mathfrak{m}_F^d \setminus \mathfrak{m}_F^{d+1}$ (where $\mathfrak{m}_F$ denotes the maximal ideal of $\mathcal{O}_F$), put

$$\begin{aligned} \mathcal{F}_\alpha := \big\{ f(X) \in \mathcal{O}_F[[X]] \mid\ & f(X) \equiv X^q \pmod{\mathfrak{m}_F}, \\ & f(X) \equiv \pi X \pmod{X^2} \text{ for some } \pi \in \mathcal{O}_F \text{ such that } N_{F/K}(\pi) = \alpha \big\}. \end{aligned}$$

(3) Let $f(X) = \pi X + \cdots$, $g(X) = \pi' X + \cdots$ be two element in $\mathcal{F}_\alpha$. Let $F_1(X_1, \cdots, X_n) = \sum_{i=1}^m a_i X_i$ be a linear polynomial in $\mathcal{O}_F[X_1, \cdots, X_n]$ such that $\frac{\pi}{\pi'} = \frac{\sigma(a_i)}{a_i}$ for all i. Prove that there exists a unique $F(X_1, \cdots, X_n) \in \mathcal{O}_F[[X_1, \cdots, X_n]]$ such that

- $F(X_1, \cdots, X_n) = F_1(X_1, \cdots, X_n) +$ terms of higher degree,
- $F^\sigma(g(X_1), \cdots, g(X_n)) = f(F(X_1, \cdots, X_n))$.

(4.1) For $f \in \mathcal{F}_\alpha$, show that there exists a unique one dimensional formal group law $F_f(X,Y) \in \mathcal{O}_F[[X,Y]]$ such that $F_f^\sigma(f(X), f(Y)) = f(F_f(X,Y))$.

(4.2) For $f \in \mathcal{F}_\alpha$ and $a \in \mathcal{O}_K$, show that there exists a unique $[a](X) \in \mathcal{O}_F[[X]]$ such that $[a](X) \equiv aX \pmod{X)^2}$, and $[a]^\sigma \circ f = f \circ [a]$.

(5) Show that for $f, g \in \mathcal{F}_\alpha$, $F_f \cong F_g$ (as formal group laws over $\mathcal{O}_F$).

(6) For $n \in \mathbb{Z}_{\geq 1}$, let

$$\Lambda_n = \{x \in \overline{F} \mid f^{\sigma^{n-1}} \circ \cdots f^\sigma \circ f(x) = 0\}.$$

Show that $\Lambda_n \cong \mathcal{O}_K/\mathfrak{m}_K^n$ where the $\mathcal{O}_K$-action is given by $x \mapsto [a](x)$.

(7) Show that $F_n := F(\Lambda_n)$ is independent of the choice of $f \in \mathcal{F}_\alpha$ (and only depends on α). And prove that $\mathrm{Gal}(F_n/F) \cong (\mathcal{O}_K/\mathfrak{m}_K^n)^\times$.

Exercise 4. Let θ be as in Lemma 1.5.7, prove θ induces an isomorphism of the formal groups $F_f \xrightarrow{\sim} F_g$ over $\mathcal{O}_{\breve{K}}$.

Exercise 5. Let σ be as in the § 1.5, show $\sigma - 1 : \mathcal{O}_{\breve{K}} \to \mathcal{O}_{\breve{K}}$ is surjective.

Exercise 6. Show that an abelian group Λ is injective (in the category of abelian groups) if and only if Λ is divisible, i.e. $n : \Lambda \to \Lambda$ is surjective for any $n \in \mathbb{Z}_{>0}$.

Exercise 7. Let G be a finite group. Let $N := \sum_{g \in G} e_g \in \mathbb{Z}_G$.

(1) Prove that N is a central element of G and $N^2 = |G|N$.

(2) Prove $\mathbb{Z}[G]^G = \mathbb{Z}N$.

Exercise 8. Prove the restriction-inflation sequence (2.5) in Proposition 2.2.15 is exact.

Exercise 9. Let G be a finite group, $M \in \mathcal{M}\mathrm{od}_G$. A group E is called an extension of G by M, if E sits in an exact sequence of groups

$$0 \to M \to E \xrightarrow{\kappa} G \to 1 \tag{5.14}$$

such that the induced conjugate action of $G \cong E/M$ on M (noting M is abelian) coincides with the given G-action on M. Two extensions E, E' are called isomorphic if we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0 \end{array}.$$

Let E be an extension as in (5.14). For $g \in G$, let $s(g) \in E$ be a preimage of g via κ. For $g_1,\ g_2 \in G$, we have $\kappa(s(g_1g_2)) = \kappa(s(g_1)s(g_2))$ and hence we get $c(g_1, g_2) := s(g_1)s(g_2)s(g_1g_2)^{-1} \in M$.

(1) Show that the map $c : G \times G \to M,\ g_1, g_2 \mapsto c(g_1, g_2)$ is a 2-cocylce, i.e.

$$g_1c(g_2, g_3) - c(g_1g_2, g_3) + c(g_1, g_2g_3) - c(g_1, g_2) = 0.$$

(hint: consider the associativity of the group operation in E.)

(2) Prove the above construction gives a bijection between the isomorphism class of extensions of G by M and $H^2(G, M)$.

Exercise 10. Let G be a finite cyclic group, $h \in G$ be a generator. For $M \in \mathcal{M}\mathrm{od}_G$, recall there is a canonical isomorphism $H_T^{-1}(G, M) \to H_T^1(G, M)$. For $\alpha \in \mathrm{Ker}(\mathcal{N}_G : H_0(G, M) \to H^0(G, M))$, describe the 1-cocycle corresponding to α via the isomorphism.

Exercise 11. Let $K = \mathbb{Q}_p(\sqrt{p})$. Compute the Herbrand quotient of K^* as a $\mathrm{Gal}(K/\mathbb{Q})$-module.

Exercise 12. Let H be a subgroup of G. Let M be a G-module, N be an H-submodule of M. For $\sigma \in G$, put $H^\sigma := \sigma H \sigma^{-1}$.

(1) Show that $\sigma(N)$ is a H^σ-module.

Show that the morphism $N \to \sigma(N),\ n \mapsto \sigma n$ is compatible with the group homomorphism $H^\sigma \to H,\ h \mapsto \sigma^{-1}h\sigma$ and induces isomorphisms $\sigma_* : H^i(H, N) \to H^i(H^\sigma, \sigma(N))$ for all $i \geq 0$.

(2) Show that if M' is a G-module, then we have for all $\alpha \in H^i(H, M),\ \beta \in H^j(H, M')$:

$$\sigma_*(\alpha \cup \beta) = \sigma_*\alpha \cup \sigma_*\gamma.$$

Exercise 13. Let H be a subgroup of G. Show that the restriction $\mathrm{Res} : H_T^{-2}(G, \mathbb{Z}) \to H_T^{-2}(H, \mathbb{Z})$ corresponds to the transfer (Verlagerung) map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

Exercise 14. Let K be a finite extension of $\mathbb{Q}_p$. Construct a finite Galois extension L over K, such that $H_T^i(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)$ is not trivial (for all i).

Exercise 15. We use the notation of Theorem 3.2.14. Let L be a finite extension of K, $\sigma_L := \sigma_K^{[k_L:k]}$. Show that

$$\mathrm{inv}_L \circ \mathrm{Res} = [L : K]\, \mathrm{inv}_K : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

where inv_L is defined as inv_K with σ_K replaced by σ_L. (hint: divide into two cases: L/K unramified or L/K totally ramified.)

Exercise 16. Let K be a finite extension of $\mathbb{Q}_p$, L_1, L_2 be finite abelian extensions of K, and $L := L_1L_2$. Show $N_{L/K}(L^\times) = N_{L_1/K}(L_1^\times) \cap N_{L_2/K}(L_2^\times)$.

Exercise 17. Let K be a finite extension of $\mathbb{Q}_p$, L be a finite extension of K, $f := [k_L : k]$. Let $\sigma_K \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ be the fixed Frobenius as in Corollary 3.3.6, $\sigma_L := \sigma_K^f \in \mathrm{Gal}(L^{ur}/L)$, and ρ_K, ϕ_L be associated the local Artin map respectively. Show that the following diagram commutes:

$$\begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ \Big\downarrow & & \Big\downarrow \quad V \\ L^\times & \xrightarrow{\phi_L} & \mathrm{Gal}(\overline{K}/L)^{\mathrm{ab}} \end{array}$$

where the left vertical map is the natural injection and the right vertical map is the Verlagerung map. (hint: use Exercise 13)

Exercise 18. (**Kummer theory**) Let K be a field, L be a finite Galois extension of K. Let $n \geq 2$, $(n, \mathrm{char}\, K) = 1$.

(1) Suppose $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, and $\zeta_n \in K$ (where ζ_n is a primitive n-th root of unity). Prove that there exists $\alpha \in K$ such that $L = K(\alpha^{\frac{1}{n}})$, where $\alpha^{\frac{1}{n}}$ denotes an n-th root of α (note that different choices of such root differ by n-th roots of unity (contained in K)). [Hint: consider the 1-cocycle on $\mathrm{Gal}(L/K)$ induced by $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(L/K) \to K^\times$, $i \mapsto \zeta_n^i$.]

We define Kummer pairing. Let $\mu_n := \{a \in \overline{K} \mid a^n = 1\}$. Suppose $\mu_n \subset K$. For $\alpha \in K^\times$, let $\alpha^{\frac{1}{n}} \in \overline{K}$ be an n-th root of α. For $g \in \mathrm{Gal}(\overline{K}/K)$, we have $\kappa_\alpha(g) := g(\alpha^{\frac{1}{n}})/\alpha^{\frac{1}{n}} \in \mu_n$. Let $(K^\times)^n := \{x^n, x \in K^\times\}$.

(2) Check that κ_α is independent of the choice of n-th root of α, and we obtain a morphism of groups

$$\kappa : K^\times/(K^\times)^n \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n),$$

or equivalently, a pairing

$$K^\times/(K^\times)^n \times \mathrm{Gal}(\overline{K}/K) \to \mu_n.$$

(3) Prove the map κ is bijective.

Now suppose moreover K is a finite extension of $\mathbb{Q}_p$ (containing μ_n), $\rho_K : K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ the reciprocity map. We can define the so-called n-th norm residue symbol:

$$(\ ,\ )_{n,K} : K^\times \times K^\times \to \mu_n$$

with $(\alpha, \beta)_{n,K} = \rho_K(\beta)(\alpha^{\frac{1}{n}})/\alpha^{\frac{1}{n}}$.

(4) Prove $(\ ,\ )$ is bimultiplicative

(5) Prove $(\alpha, 1-\alpha)_{n,K} = 1$ for all $\alpha \in K \setminus \{0,1\}$. [hint: show $1-\alpha \in N_{K(\alpha^{\frac{1}{n}})/K}$.]

(6) Prove $(\alpha, -\alpha)_{n,K} = 1$ for $\alpha \in K^\times$.

(7) Prove $(\alpha, \beta)_{n,K} = (\beta, \alpha)_{n,K}^{-1}$ for $\alpha, \beta \in K^\times$. [hint: consider $(\alpha\beta, -\alpha\beta)_{n,K}$]

(8) Prove $(\ , \ )_{n,K}$ induces a perfect pairing $K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \mu_n$.

(9) Deduce directly $\cap_{L/K} N_{L/K}(L^\times) \subset (K^\times)^n$ where L runs through finite extensions of K (without using $\cap_{L/K} N_{L/K}(L^\times) = 1$).

Exercise 19. Show (at least one of) the diagrams in Proposition 5.2.6 commute.

Exercise 20. Keep the situation as in Lemma 5.4.7 and let K_S be the extension of K as in the proof of Lemma 5.4.7. Prove $[I_K : K^\times N_{K_S/K} I_{K_S}] = p^{|S|}$.

Exercise 21. Let L/K be a cyclic extension of number fields. Let $a \in K^\times$ and suppose $a \in N_{L_w/K_v} L_w^\times$ for some $w|v$ for all places v of K. Prove that $a \in N_{L/K} L^\times$.