Mathematical Tripos, Part III Essay

Title: Local Class Field Theory

Contents

1 Introduction

This is an essay about class field theory. Roughly speaking, the subject relates intrinsic properties of a local field or a global field to its abelian extensions. In this essay, we will mainly consider abelian extensions of local fields. A local field will always be non-archimedean here (the theory for the archimedean cases, namely $\mathbb{R}$ and $\mathbb{C}$, are trivial). As we shall see below, we can classify their abelian extensions intrinsically using open multiplicative subgroups.

First, we introduce some notations. For a local field K, we write K^{al} for a fixed separable algebraic closure of K. An extension of K will always mean a subfield of K^{al} containing K. The composite of two finite abelian extensions of K is again a finite abelian extension of K (since the Galois group would embed into the direct product of the two abelian Galois groups via restrictions). Therefore, the union of all finite abelian extensions of K is also an abelian extension, denoted by K^{ab}. If k_K is the residue field of K where $|k_K| = q$, then Frob denotes the Frobenius map $x \mapsto x^q$. The main theorems we will prove are as follows.

Theorem 1.1 (Reciprocity Law) *For any local field K, there is a unique homomorphism*

$$\phi_K : K^\times \to \mathrm{Gal}(K^{\text{ab}}/K)$$

with the following properties.

(a) For any uniformiser π of K and any finite unramified extension L of K, $\phi_K(\pi)|_L = \mathrm{Frob}_{L/K}$.

(b) For any finite abelian extension L of K, $N_{L/K}(L^\times)$ is contained in the kernel of $a \mapsto \phi_K(a)|_L$, and ϕ_K induces an isomorphism

$$\phi_{L/K} : K^\times / N_{L/K}(L^\times) \to \mathrm{Gal}(L/K).$$

(b) says that for any finite abelian extension L of K, we have the following commutative diagram.

$$\begin{tikzcd}
K^\times \arrow[r, "\phi_K"] \arrow[d] & \mathrm{Gal}(K^{\text{ab}}/K) \arrow[d, "\tau \mapsto \tau|_L"] \\
K^\times / N_{L/K}(L^\times) \arrow[r, "\phi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

where $\phi_{L/K}$ is an isomorphism. So, L corresponds to the multiplicative subgroup $N_{L/K}(L^\times)$ of $K^\times$ via ϕ_K. We call a group of this form a norm group. Norm groups can be classified by the following.

Theorem 1.2 (Existence Theorem) *Let K be a local field. A subgroup N of $K^\times$ is of the form $N_{L/K}(L^\times)$ for some finite abelian extension L of K iff it is of finite index and open.*

There are several different approaches to the subject. We will follow the group cohomology approach, mostly based on the treatments in [5], with some proofs taken from [3] and [1]. We will develop the theory of cohomology in section 2. The results will then be applied to local fields in section 3 which will enable us to prove the existence in theorem 1.1. In section 4, we introduce the notion of formal groups and prove theorem 1.2 and the uniqueness in theorem 1.1. Finally, in section 5, we will state without proofs how the theory is generalised to global fields.

I would like to thank Dr Tim Dokchitser for suggesting the topic and his helpful comments. I would also like to thank Alex Chmelnitkzi and Stefan Patrikis for the inspiring discussions on the subject during our preparation for the part III seminar series at the end of Lent term.

2 Group Cohomology

Group cohomology will prove to be a very powerful tool in this essay. To develop the theory we need, we will assume familiarity of the language of category theory, eg functor, exactness, left/right exact, etc. Most of the definitions can be found in [4].

2.1 Definition of Cohomology

Ab denotes the category of abelian groups (or $\mathbb{Z}$-modules). Given an abelian group G, we define a contravariant functor $\mathrm{Hom}(-, G)$:**Ab**$\to$**Ab** as follows. For a homomorphism $f : G_1 \to G_2$, let f_* be the map from $\mathrm{Hom}(G_2, G)$ to $\mathrm{Hom}(G_1, G)$ given by $f_*(\theta) = \theta \circ f$. It is easy to see that $f_* f'_* = (f'f)_*$ and $\mathrm{id}_* = \mathrm{id}$. Similarly, we can define the functor $\mathrm{Hom}(G, -)$.

Lemma 2.1 $\mathrm{Hom}(-, G)$ *is a left exact contravariant functor.*

Proof Assume $G_1 \xrightarrow{f} G_2 \xrightarrow{f'} G_3 \to 0$ is exact. We need to show that the sequence $0 \to \mathrm{Hom}(G_3, G) \xrightarrow{f'_*} \mathrm{Hom}(G_2, G) \xrightarrow{f_*} \mathrm{Hom}(G_1, G)$ is exact. Since $f'f = 0$, $f_* f'_* = 0$, ie $\mathrm{Im} f'_* \subseteq \ker f_*$.
If $\phi \in \ker f_*$, then $\phi \circ f = 0$, so $\ker f' = \mathrm{Im} f \subseteq \ker \phi$. Therefore, we have

$$\forall g, h \in G_2,\ f'(g) = f'(h) \Rightarrow \phi(g) = \phi(h) \tag{1}$$

Since f' is surjective, we can define $\psi : G_3 \to G$ by $\psi(g) = \phi(g')$ where $g' \in G_2$ is such that $f'(g') = g$. This is well-defined by (1). We have $f'_*(\psi) = \psi \circ f' = \phi$ and $\phi \in \mathrm{Im} f'_*$.

$$\begin{tikzcd} G_1 \arrow[r, "f"] & G_2 \arrow[r, "f'"] \arrow[d, "\phi"] & G_3 \arrow[r] \arrow[dl, "\psi"] & 0 \\ & G & & \end{tikzcd}$$

Therefore, $\ker f_* \subseteq \mathrm{Im} f'_*$ and so $\ker f_* = \mathrm{Im} f'_*$. Hence, this gives the exactness at $\mathrm{Hom}(G_2, G)$.
If $\theta \in \ker f'_*$, then $\theta \circ f' = 0$, so $\mathrm{Im} f' \subseteq \ker \theta$. But f' is surjective, so $\theta = 0$. Hence f'_* is injective and so the sequence is exact at $\mathrm{Hom}(G_3, G)$. □

Similarly, one can show that the functor $\mathrm{Hom}(G, -)$ is a left exact functor.

Definition 2.2 *An abelian group is said to be* ***injective*** *if* $\mathrm{Hom}(-, G)$ *is exact. An* ***injective resolution*** *of* G *is a long exact sequence*

$$0 \to G \to I^0 \to I^1 \to \cdots$$

where the I^r*'s are injective abelian groups. We abbreviate this complex to* $G \to I^\cdot$.

In particular, by lemma 2.1, G is injective iff given any injective $f : G_1 \to G_2$, $f_* : \mathrm{Hom}(G_2, G) \to \mathrm{Hom}(G_1, G)$ is surjective, ie for any abelian groups $G_1 \leq G_2$, a homomorphism $G_1 \to G$ always extends to G_2. The following equivalent condition will allow us to show the existence of injective resolutions.

Lemma 2.3 *G is injective iff it is divisible, ie for any non-zero integer n and $g \in G$, there exists $h \in G$ s.t. $g = nh$.*

Proof ($\Rightarrow$) Let n be a non-zero integer and $g \in G$. Define $f : n\mathbb{Z} \to G$ by $n \mapsto g$. Then f extends to $\mathbb{Z}$, say $f(1) = h$. So $f(n) = nh = g$.
($\Leftarrow$) Suppose $G_1 \leq G_2$ are abelian groups and $f : G_1 \to G$ is a homomorphism. Consider the poset of (H, f') where $G_1 \leq H \leq G_2$ and f' extends f to H, ordered by inclusion. By Zorn's lemma, there is a maximal element, (H', F) say. If $H' \neq G_2$, let $h \in G_2 - H'$ and define $I = \{m \in \mathbb{Z} | mh \in H'\}$. This is an ideal of $\mathbb{Z}$, hence $I = n\mathbb{Z}$ for some n. The map $I \to G$ where $m \mapsto F(mh)$ extends to $\mathbb{Z}$ as G is divisible. Hence F extends to $H' + \mathbb{Z}h$, contradicting the maximality. So f extends to G_2. □

Example 2.4 *$\mathbb{Q}$ is clearly divisible, hence injective. In fact, any quotients of a divisble abelian group are divisible, eg $\mathbb{Q}/\mathbb{Z}$ is injective. The same is true for quotients of $\mathbb{Q}^X$ where X is any set.*

Corollary 2.5 *Any abelian group G can be embedded in an injective abelian group.*

Proof If X is a generating set for G, let $f : \mathbb{Z}^X \to G$ be the natural surjection. Then $G \cong \mathbb{Z}^X / \ker f \leq \mathbb{Q}^X / \ker f$ which is divisible, so injective by lemma 2.3. Hence the result. □

Given a group G, a G-module is an abelian group together with an action of G. This is an important notion for class field theory since a Galois extension L of K is naturally a $\mathrm{Gal}(L/K)$-module. The category of G-modules is denoted by $\mathbf{Mod}_G$. For a G-module M, we write M^G for the submodule on which G acts trivially, ie $M^G = \{m \in M : gm = m \ \forall g \in G\}$. If M and N are G-modules, then $\mathrm{Hom}_G(M, N)$ denotes the set of G-homomorphisms from M to N, ie $f(gm) = gf(m)$ for all $g \in G$ and $m \in M$.

As with injective abelian groups, we say that a G-module M is injective if $\mathrm{Hom}_G(-, M)$ is exact. We can define injective resolutions of G-modules as in definition 2.2. Note that these definitions agree with 2.2 when we take $G = \mathbb{Z}$. As in representation theory, we can define induced modules as follows.

Definition 2.6 *Let $H \leq G$ be groups, M an H-module. Define* $\mathrm{Ind}_H^G(M) = \{\theta : G \to M | \theta(hg) = h\theta(g) \ \forall h \in H, g \in G\}$. *This is a G-module with* $(g\theta)(x) = \theta(xg)$.

If $f : M_1 \to M_2$ is an H-module map, define f_* :$\mathrm{Ind}_H^G(M_1) \to \mathrm{Ind}_H^G(M_2)$ by $f_*(\theta) = f \circ \theta$. From representation theory, this gives an exact functor from $\mathbf{Mod}_H$ to $\mathbf{Mod}_G$.

Lemma 2.7 *Given a group G. If A is an injective abelian group, the G-module* $\mathrm{Ind}_1^G A$ *is injective.*

Proof Recall Frobenius reciprocity says that if H is a subgroup of G, for any G-module M_1 (which is naturally an H-module) and any H-module M_2, there is a canonial isomorphism as follows.

$$\mathrm{Hom}_G(M_1, \mathrm{Ind}_H^G(M_2)) \to \mathrm{Hom}_H(M_1, M_2)$$

Hence, we have $\mathrm{Hom}_G(-, \mathrm{Ind}_1^G A) \cong \mathrm{Hom}_1(-, A) = \mathrm{Hom}(-, A)$. But $\mathrm{Hom}(-, A)$ is exact as A is injective. Hence, $\mathrm{Ind}_1^G A$ is an injective G-module. □

Proposition 2.8 *An injective resolution exists for any G-module M.*

Proof Note that M is an abelian group, so there exists an injective abelian group A s.t. $M \hookrightarrow A$ by corollary 2.5. So, we have $\mathrm{Ind}_1^G(M) \hookrightarrow \mathrm{Ind}_1^G(A)$ as G-modules. $\mathrm{Ind}_1^G A$ is injective by lemma 2.7. But M embeds into $\mathrm{Ind}_1^G(M)$ by the map $m \mapsto (g \mapsto gm)$, so M embeds into an injective G-module I^0.
Let B^1 be the cokernel of the embedding, then we have an inclusion of G-modules $B^1 \hookrightarrow I^1$ where I^1 is injective. So, $0 \to M \to I^0 \to I^1$ is exact. Continue recursively, we obtain an injective resolution. □

Dually, we define projective modules and projective resolutions as follows.

Definition 2.9 *A G-module M is projective if* $\mathrm{Hom}_G(M, -)$ *is exact. A projective resolution of M is an exact sequence*

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

where the P_r's are projective. The complex is abbreviated to $P. \to M$.

Lemma 2.10 *$M \mapsto M^G$ gives a left exact functor from the category of G-modules to the category of abelian groups.*

Proof Note that $\mathrm{Hom}_G(M,N) = (\mathrm{Hom}(M,N))^G$ where G acts on $\mathrm{Hom}(M,N)$ by $(g\theta)(m) = g\cdot\theta(g^{-1}m)$. In particular, if G acts on $\mathbb{Z}$ trivially, $\mathrm{Hom}_G(\mathbb{Z},M) = (\mathrm{Hom}(\mathbb{Z},M))^G = M^G$. Hence, the left exactness of Hom gives the result. □

Remark 2.11 *We can now give the definition of cohomology. The idea is to measure the failure of $-^G$ from being exact. We will see how it works exactly later.*

Definition 2.12 *Let M be a G-module and choose an injective resolution*

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

Consider the following complex.

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \xrightarrow{d^2} \cdots$$

The r^{th} ***cohomology group*** *of G with coefficients in M is defined to be the abelian group $H^r(G,M) = \ker(d^r)/\mathrm{Im}(d^{r-1})$.*

It is not clear whether the H^r's are independent of the choice of $I^{\cdot}$. We will show that they are well-defined by verifying that these groups are uniquely determined by some elementary properties.

Lemma 2.13 *For any G-module M, $H^0(G,M) \cong M^G$*

Proof As noted in the proof of lemma 2.10, $\mathrm{Hom}_G(\mathbb{Z},M) \cong M^G$. On the other hand, $0 \to M \to I^0 \to I^1$ is exact implies $0 \to M^G \to (I^0)^G \to (I^1)^G$ is exact by lemma 2.10. Hence, $\ker d^0 \cong M^G$. But $d^{-1} = 0$, so we have $H^0(G,M) = \ker d^0/\mathrm{Im}\ d^{-1} = \ker d^0 \cong M^G$. □

Lemma 2.14 *If M is injective, then $H^r(G,M) = 0$ for $r > 0$.*

Proof Note that if M is injective, $0 \to M \to M \to 0 \to 0 \to \cdots$ is an injective resolution. So, the complex in the definition of the cohomology groups becomes $0 \to M^G \to 0 \to \cdots$. Hence the result. □

Lemma 2.15 *For any $\{1\}$-module M, $H^r(1,M) = 0$ for all $r > 0$.*

Proof An $\{1\}$-module is just an abelian group. Under the notations in the proof of proposition 2.8, M is embedded in an injective (or divisible) abelian group I^0. As remarked in example 2.4, $B^1 = I^0/M$ is also injective. Hence, the following is an injective resolution.

$$0 \to M \to I^0 \to I^0/M \to 0 \to 0 \to \cdots$$

$G = \{1\}$ acts trivially, so the complex in the definition of the cohomology groups becomes $0 \to I^0 \to I^0/M \to 0 \to \cdots$. Hence the result. □

We saw in lemma 2.7 that $\mathrm{Ind}_1^G(A)$ is injective if A is an injective abelian group. Hence $H^r = 0$ for $r > 0$. In fact, this is true for any abelian group A. To prove this, we will make use of Shapiro's Lemma.

Lemma 2.16 (Shapiro) *Let H be a subgroup of G. For any H-module N, there is a canonical isomorphism $H^r(G, \mathrm{Ind}_H^G N) \to H^r(H, N)$.*

Proof Let $N \to I^\cdot$ be an injective resolution. Since Ind_H^G is an exact functor that preserves injectivity, $\mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G I^\cdot$ is an injective resolution.
If $f \in (\mathrm{Ind}_H^G I^r)^G$, then $f(x) = gf(x) = f(xg) \forall\ x, g \in G$. Hence, f is a constant map, say $f(x) \equiv m$. But $f(hx) = hf(x)$, so $m \in (I^r)^H$. We have $(\mathrm{Ind}_H^G I^r)^G = (I^r)^H$.
Therefore, we obtain the same complex when we take the H-invariants of $N \to I^\cdot$ and the G-invariants of $\mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G I^\cdot$. Hence, $H^r(G, \mathrm{Ind}_H^G N) \cong H^r(H, N)$ canonically for all r. $\square$

Corollary 2.17 *For any abelian group A, $H^r(G, \mathrm{Ind}_1^G A) = 0$ for all $r > 0$.*

Proof By Shapiro's lemma, $H^r(G,\mathrm{Ind}_1^G A) \cong H^r(1, A)$. But the RHS is 0 for $r > 0$ by lemma 2.15, hence the result. $\square$

Remark 2.18 *Note that $\mathrm{Ind}_1^G \mathbb{Z} = \mathbb{Z}[G]$, so $H^r(G, \mathbb{Z}[G]) = 0$ for all $r > 0$ by above. Moreover, since direct sum preserves exactness, we have $H^r(G, M_1 \oplus M_2) \cong H^r(G, M_1) \times H^r(G, M_2)$. Therefore, $H^r(G, M) = 0$ for all $r > 0$ if M is a free $\mathbb{Z}[G]$-module.*

Proposition 2.19 *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact, then there is a long exact sequence as follows.*

$$0 \to H^0(G, M_1) \to \cdots \to H^r(G, M_2) \to H^r(G, M_3) \to H^{r+1}(G, M_1) \to \cdots$$

Moreover, the association is functorial.

Proof (Sketch) Given a homomorphism $\alpha : M \to N$ of G-modules, if we have injective resolutions $M \to I^\cdot$ and $N \to J^\cdot$, α extends to a morphism of complexes from $I^\cdot$ to $J^\cdot$. We have the following commutative diagram.

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M_1 \arrow[r] \arrow[d] & I^0 \arrow[r] \arrow[d] & I^1 \arrow[r] \arrow[d] & I^2 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & M_2 \arrow[r] \arrow[d] & J^0 \arrow[r] \arrow[d] & J^1 \arrow[r] \arrow[d] & J^2 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & M_3 \arrow[r] \arrow[d] & K^0 \arrow[r] \arrow[d] & K^1 \arrow[r] \arrow[d] & K^2 \arrow[r] \arrow[d] & \cdots \\
& 0 & 0 & 0 & 0 &
\end{tikzcd}$$

$-^G$ is a left exact functor by lemma 2.10, the construction of the long exact sequence is then by diagram chasing. $\square$

In particular, by combining lemma 2.13 and above, we have the following exact sequence.

$$0 \to M_1^G \to M_2^G \to M_3^G \to H^1(G, M_1) \to \cdots$$

This is what we meant by measuring the failure of $-^G$ from being exact in remark 2.11. Continue with the long exact sequence, H^2 then measures how far H^1 is from resolving this failure and so on.

Theorem 2.20 *The H^r's are uniquely determined by 2.13, 2.17 and 2.19.*

Proof Let M be a G-module, $M' = \mathrm{Ind}_1^G(M)$ and $M'' = M'/M$ with M embedded in M' as in the proof of proposition 2.8. Hence, we have a short exact sequence $0 \to M \to M' \to M'' \to 0$. So, we have a long exact sequence of cohomology by proposition 2.19.

$$0 \to M^G \to M'^G \to M''^G \to H^1(G, M) \to H^1(G, M') \to \cdots \tag{2}$$

By corollary 2.17, $H^r(G, M') = 0$ for all $r > 0$. Hence, $M'^G \to M''^G \to H^1(G, M) \to 0$ is exact. Hence, $H^1(G, M) \cong \mathrm{coker}(M'^G \to M''^G)$. That means the H^1's are uniquely determined. The long exact sequence also gives $H^r(G, M'') \cong H^{r+1}(G, M)$ for $r \geq 1$, hence all H^r's are uniquely determined by induction. □

Remark 2.21 *The isomorphism $H^r(G, M'') \cong H^{r+1}(G, M)$ relates properties of cohomology in different dimensions which makes the induction work. This technique is called dimension shifting and will be used again later.*

2.2 Properties of Cohomology

We will now describe the cohomology groups in terms of cochains. This will enable us to carry out explicit calculations. For $r \geq 0$, let P_r be the free $\mathbb{Z}$-module with basis the $(r+1)$-tuples $(g_0, \ldots, g_r)$ of elements of G. G acts on P_r via $g(g_0, \ldots, g_r) = (gg_0, \ldots, gg_r)$. Therefore, P_r is also a free $\mathbb{Z}[G]$-module with basis $\{(1, g_1, \ldots, g_r) | g_i \in G\}$. Now, consider the following complex.

$$\cdots \to P_r \xrightarrow{d_r} P_{r-1} \to \cdots P_0 \xrightarrow{\epsilon} \mathbb{Z} \tag{3}$$

where $d_r(g_0, \ldots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_r)$ and ϵ sends each $g \in G$ to 1. It is not hard to check that $d_r \circ d_{r+1} = 0$.

Lemma 2.22 *The complex in (3) is exact.*

Proof Fix $x \in G$ and define $k_r : P_r \to P_{r+1}$ by $k_r(g_0, \ldots, g_r) = (x, g_0, \ldots, g_r)$.

$$\begin{aligned} d_{r+1} \circ k_r(g_0, \ldots, g_r) &= d_{r+1}(x, g_0, \ldots, g_r) \\ &= (g_0, \ldots, g_r) - (x, g_1, \ldots, g_r) + (x, g_0, g_2, \ldots, g_r) - \cdots \\ &= (g_0, \ldots, g_r) - k_{r-1}((g_1, \ldots, g_r) - (g_0, g_2, \ldots, g_r) + \cdots) \\ &= (g_0, \ldots, g_r) - k_{r-1}(d_r(g_0, \ldots, g_r)) \end{aligned}$$

Hence, $d_{r+1} \circ k_r + k_{r-1} \circ d_r = 1$. If $v \in \ker d_r$, then $v = d_{r+1}(k_r(v)) \in$Im d_{r+1}. Hence the exactness at P_r for $r > 0$.
If $v = \sum n_g g \in \ker \epsilon$, then $\sum n_g = 0$. So $v = \sum n_g(g-1) = \sum n_g d_1(1,g) \in$Im d_1. Hence the exactness at P_0. □

For a fixed G-module M, we can take $\mathrm{Hom}_G(-, M)$ on (3). We obtain a complex

$$0 \xrightarrow{\delta_0} \mathrm{Hom}_G(P_0, M) \xrightarrow{\delta_1} \mathrm{Hom}_G(P_1, M) \xrightarrow{\delta_2} \cdots \tag{4}$$

where $\delta_r : \mathrm{Hom}_G(P_{r-1}, M) \to \mathrm{Hom}_G(P_r, M)$ is given by the composition with d_r, ie given $f \in \mathrm{Hom}_G(P_{r-1}, M)$, we have $\delta_r(f) = f \circ d_r$.

Proposition 2.23 *With the notations above, $H^r(G, M) \cong \ker\delta_{r+1}/\mathrm{Im}\delta_r$.*

Proof We verify the RHS satisfies the properties in theorem 2.20. The construction of long exact sequences is the same and is omitted here.
Note that $P_0 = \mathbb{Z}[G]$. If $f \in \mathrm{Hom}_G(P_0, M)$, f is uniquely determined by $f(1)$. By definition, $(\delta_1(f))(g,h) = f(h) - f(g) = hf(1) - gf(1)$. So, $\delta_1(f) = 0$ iff $f(1) \in M^G$. We have $\ker\delta_1 \cong M^G$. Since $\delta_0 = 0$, the RHS is M^G for $r = 0$.
If $M = \mathrm{Ind}_1^G N$, then $\mathrm{Hom}_G(P_r, M) \cong \mathrm{Hom}(P_r, N)$ by Frobenius reciprocity. So, (4) becomes the following.

$$0 \xrightarrow{\delta_0} \mathrm{Hom}(P_0, N) \xrightarrow{\delta_1} \mathrm{Hom}(P_1, N) \xrightarrow{\delta_2} \mathrm{Hom}(P_2, N) \to \cdots$$

But each P_r is a free abelian group, so $\mathrm{Hom}(P_r, N) = N^{\mathrm{rk}(P_r)}$. The complex above is exact at every place after the first by the same agrument as in the proof of lemma 2.22. Therefore, the RHS is 0 if $M = \mathrm{Ind}_1^G N$ for $r > 0$. Hence we are done by theorem 2.20. □

Note that $\theta \in \mathrm{Hom}(P_r, M)$ can be identified with a function $\theta' : G^{r+1} \to M$ since θ is uniquely determined by the values taken on the basis. If in addition $\theta \in \mathrm{Hom}_G(P_r, M)$, then we have the following additional condition.

$$\theta'(gg_0, \ldots, gg_r) = g(\theta'(g_0, \ldots, g_r)) \text{ for all } g, g_0, \ldots g_r \in G \tag{5}$$

This leads us to give the following definition in order to simplify (4).

Definition 2.24 *$\tilde{C}^r(G, M) := \{f : G^{r+1} \to M | f$ satisfies condition (5)$\}$, this is called the set of **homogeneous** r**-cochians** of G with values in M.*

If we identify $\mathrm{Hom}_G(P_r, M)$ with $\tilde{C}^r(G, M)$, the boundary map becomes $\tilde{d}^r : \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M)$ with

$$(\tilde{d}^{r+1} f)(g_0, \ldots, g_{r+1}) = \sum_{i=0}^{r+1} (-1)^i f(g_0, \ldots, \hat{g}_i \ldots, g_{r+1})$$

We have $H^r(G, M) = \ker \tilde{d}^{r+1}/\mathrm{Im}\ \tilde{d}^r$. In fact, we can simplify further by the following definition.

Definition 2.25 *Let $C^r(G,M)$ be the set of functions from G^r to M with $G^0 = 1$. This is called the group of **inhomogeneous** r**-cochains** of G with values in M. Define $d^{r+1} : C^r(G,M) \to C^{r+1}(G,M)$ by $(d^{r+1}f)(g_1,\dots,g_{r+1}) =$*

$$g_1 f(g_2,\dots,g_{r+1}) + \sum_{i=1}^{r}(-1)^i f(g_1,\dots,g_i g_{i+1},\dots,g_{r+1}) + (-1)^{r+1} f(g_1,\dots,g_r)$$

Proposition 2.26 $0 \xrightarrow{d^0} C^0(G,M) \xrightarrow{d^1} C^1(G,M) \xrightarrow{d^2} C^2(G,M) \to \cdots$ *is a complex and $H^r(G,M) \cong \ker d^{r+1}/\mathrm{Im} d^r$.*

Proof Define $\theta : \tilde{C}^r(G,M) \to C^r(G,M)$ by

$$(\theta f)(g_1,\dots,g_r) = f(1, g_1, g_1 g_2, \dots, g_1 \dots g_r)$$

Note that for $f \in \tilde{C}^r(G,M)$, $f(g_0,\dots,g_r) = g_0 f(1, g_0^{-1}g_1, \dots, g_0^{-1}g_r)$. If we let $h_1 = g_0^{-1}g_1$, $h_2 = g_1^{-1}g_2$,…,$h_r = g_{r-1}^{-1}g_r$, then the above expression becomes $g_0 f(1, h_1, h_1 h_2, \dots, h_1 \dots h_r)$. So f is uniquely determined by the values $f(1, g_1, g_1 g_2, \dots, g_1 \dots g_r)$. Hence θ is a bijection. Moreover, $d^r(\theta(f)) = \theta(\tilde{d}^r(f))$. So, the sequence of $C^r(G,M)$ stated above is the same as the complex of $\tilde{C}^r(G,M)$, hence the result. □

We can now describe H^1 explicitly.

Definition 2.27 *A map $f : G \to M$ is called a **crossed homomorphism** if $f(gh) = gf(h) + f(g)$. A map of the form $g \mapsto gm - m$ for some fixed $m \in M$ is called a **principal crossed homomorphism**.*

Note that $(d^1 f)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1)$, so $f \in \ker d^1$ iff f is a crossed homomorphism. If $f \in C^0(G,M)$, then $f(1) = m$ some $m \in M$. So $(d^0 f)(g) = gm - m$. Hence Im d^0 is the set of principal crossed homomorphism. In particular, $H^1(G,M) = \{\text{crossed homos}\}/\{\text{principal crossed homos}\}$.

Remark 2.28 *In particular, if G acts on M trivially, a crossed homomorphism is just a homomorphism from G to M and a principal crossed homomorphism is just the zero map. Therefore, $H^1(G,M) = \mathrm{Hom}(G,M)$ in this case.*

We will now construct some maps in cohomology between different modules. This will enable us to derive some basic properties of H^r's. First, we need the following definition.

Definition 2.29 *Let M be a G-module and M' a G'-module. Homomorphisms $\alpha : G' \to G$ and $\beta : M \to M'$ are said to be **compatible** if $\beta(\alpha(g)m) = g(\beta(m))$*

Remark 2.30 *If (α, β) is compatible, then we have a homomorphism from $C^r(G,M) \to C^r(G',M')$ defined by $f \mapsto \beta \circ f \circ \alpha^r$ where α^r is the natural homomorphism from $(G')^r$ to G^r defined by α. In fact, this gives a homomorphism of complexes, hence homomorphisms from $H^r(G,M)$ to $H^r(G',M')$.*

Given a G-module M and H a normal subgroup of G, M^H is a G/H-submodule. Indeed, if $m \in M^H$, $g \in G$, $h \in H$, then $h \cdot gm = g(g^{-1}hg)m = gm$ since $g^{-1}hg \in H$. We have $gm \in M^H$ also. So, G/H acts on M^H naturally. This leads to the following definitions.

Definition 2.31 *Let H be a subgroup of G, α the inclusion $H \hookrightarrow G$, β the identity map on a G-module M. The homomorphisms obtained as in remark 2.30 are called **restriction homomorphisms**,* $\mathrm{Res} : H^r(G, M) \to H^r(H, M)$. *If H is a normal subgroup, α the quotient map $G \to G/H$, β the inclusion $M^H \hookrightarrow M$, the homomorphisms obtained are called **inflation homomorphisms**,* $\mathrm{Inf} : H^r(G/H, M^H) \to H^r(G, M)$.

If H is a subgroup of G of finite index, let S be a set of coset representatives. Let $\alpha : G \to G$ be the identity map. For a G-module M, define a homomorphism $\beta : \mathrm{Ind}_H^G M \to M$ by $f \mapsto \sum_{s \in S} sf(s^{-1})$. This gives a map on cohomology Cor : $H^r(G, \mathrm{Ind}_H^G M) \to H^r(G, M)$. If we identify $H^r(H, M)$ with $H^r(G, \mathrm{Ind}_H^G M)$ by Shapiro's lemma, this gives a map from $H^r(H, M)$ to $H^r(G, M)$.

Definition 2.32 *The homomorphisms* $\mathrm{Cor} : H^r(H, M) \to H^r(G, M)$ *constructed above are called **corestriction homomorphisms**.*

Similarly, we can give an alternative definition of Res. Let $M \to \mathrm{Ind}_H^G(M)$ be the homomorphism sending m to f_m where $f_m(g) = gm$. This defines a homomorphism $H^r(G, M) \to H^r(G, \mathrm{Ind}_H^G M)$. It turns out to be the restriction map if we identify $H^r(G, \mathrm{Ind}_H^G M)$ with $H^r(H, M)$.

Lemma 2.33 *Let H be a subgroup of G of finite index, then* $\mathrm{Cor} \circ \mathrm{Res}$ *is the multiplication by* $(G : H)$.

Proof The map on cohomology

$$H^r(G, M) \xrightarrow{\mathrm{Res}} H^r(H, M) \cong H^r(G, \mathrm{Ind}_H^G M) \xrightarrow{\mathrm{Cor}} H^r(G, M)$$

is induced from the map $M \to \mathrm{Ind}_H^G M \to M$ with $m \mapsto f_m \mapsto \sum_{s \in S} sf_m(s^{-1}) = \sum_{s \in S} m = (G : H)m$. Hence the result. □

Corollary 2.34 *If $|G| = m < \infty$, then $mH^r(G, M) = 0$ for any $r > 0$.*

Proof $H^r(1, M) = 0$ for $r > 0$ by lemma 2.15. So, Cor∘Res=0 if we take $H = \{1\}$. But this is multiplication by m by lemma 2.33, hence the result. □

Corollary 2.35 *Let G be a finite group, M a G-module, p a prime. If G_p is a Sylow p-subgroup of G. Then* $\mathrm{Res} : H^r(G, M) \to H^r(G_p, M)$ *is an injection on the set of elements of G whose orders are powers of p.*

Proof $(G : G_p)$ is not divisble by p and Cor∘Res is the multiplication by $(G : G_p)$, hence the result. □

Lemma 2.36 *Let H be a normal subgroup of G, and M a G-module. Then the sequence*

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M)$$

is exact.

Proof $H^1 = \{\text{crossed homos}\}/\{\text{principal crossed homos}\}$. $\mathrm{Res}\circ\mathrm{Inf} = 0$ is clear (even true on the level of cochains). So, $\mathrm{Im(Inf)} \subseteq \ker(\mathrm{Res})$.
If $f \in \ker(\mathrm{Res})$, then $f : G \to M$ is a crossed homomorphism whose restriction to H is principal, so there exists $m \in M$ s.t. $f(h) = hm - m$ for $h \in H$. Define $f' : G \to M$ by $f'(g) = f(g) - gm + m$. Then f' and f are in the same class of $H^1(G, M)$.
But $f'|_H = 0$, so f' factors through G/H. Since f' is a crossed homomorphism, $f'(hg) = hf'(g) + f'(h) = hf'(g)$ for any $h \in H, g \in G$. We have

$$\begin{aligned} hf'(g) &= f'(hg) \\ &= f'(g \cdot g^{-1}hg) \\ &= gf'(g^{-1}hg) + f'(g) \text{ (f' is a crossed homomorphism)} \\ &= f'(g) \text{ (H is normal in G, so $g^{-1}hg \in H$)} \end{aligned}$$

Hence, f' takes values in M^H. Therefore, f' comes from a crossed homomorphism $G/H \to M^H$ by inflation. We have $\ker(\mathrm{Res}) \subseteq \mathrm{Im(Inf)}$. This shows the exactness at $H^1(G, M)$. It is clear that Inf is injective by considering cochains, ie we have the exactness at $H^1(G/H, M^H)$ also. □

We see from the proof above how the description of H^1 using crossed homomorphisms enables us to carry out explicit calculations. The result can be generalised as follows.

Proposition 2.37 (Inflation-Restriction Exact Sequence) *Let H be a normal subgroup of G, and M a G-module. If $r > 0$ is s.t. $H^i(H, M) = 0$ for all $0 < i < r$, then the sequence*

$$0 \to H^r(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^r(G, M) \xrightarrow{\mathrm{Res}} H^r(H, M)$$

is exact.

Proof We proceed by induction on r. $r = 1$ is just the lemma above.
For $r > 1$, assume the result for $r - 1$. As in the proof of theorem 2.20, $0 \to M \to M' \to M'/M \to 0$ is exact (either as G-modules or H-modules since the action of G or H has nothing to do with exactness) where $M' = \mathrm{Ind}_1^G M$, so we have $H^i(H, M'/M) \cong H^{i+1}(H, M)$ for $i > 0$. Hence, $H^i(H, M'/M) = 0$ for $0 < i < r - 1$. Our inductive hypothesis says that

$$0 \to H^{r-1}(G/H, (M'/M)^H) \xrightarrow{\mathrm{Inf}} H^{r-1}(G, M'/M) \xrightarrow{\mathrm{Res}} H^{r-1}(H, M'/M)$$

is exact. But we also have the following commutative diagram.

$$\begin{tikzcd} 0 \arrow[r] & H^{r-1}(G/H, (M'/M)^H) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\wr"] & H^{r-1}(G, M'/M) \arrow[r, "\mathrm{Res}"] \arrow[d, "\wr"] & H^{r-1}(H, M'/M) \arrow[d, "\wr"] \\ 0 \arrow[r] & H^r(G/H, M'/M) \arrow[r, "\mathrm{Inf}"] & H^r(G, M) \arrow[r, "\mathrm{Res}"] & H^r(H, M) \end{tikzcd}$$

Hence the result. □

Remark 2.38 *Once again, we have used the technique of dimension shifting mentioned in remark 2.21. This technique can in fact be generalised as follows. If we have an exact sequence*

$$0 \to M \to J^1 \to \cdots \to J^s \to N \to 0$$

where $H^r(G, J^i) = 0$ *for all* $r, i > 0$*, we can break the sequence up into short exact sequences*

$$0 \to M \to J^1 \to N^1 \to 0$$

$$0 \to N^1 \to J^2 \to N^3 \to 0$$

$$\cdots$$

$$0 \to N^{s-1} \to J^s \to N \to 0$$

So, long exact sequences of cohomology give $H^r(G, N) \cong H^{r+1}(G, N^{s-1}) \cong \cdots \cong H^{r+s}(G, M)$ *for* $r > 0$*.*

2.3 Homology

Let G be a group and M a G-module. M_G denotes the quotient of M by the subgroup generated by elements of the form $gm - m$, ie M_G is the largest quotient of M on which G acts trivially. It is not hard to check that the functor $M \mapsto M_G$ is right exact. Similar to cohomology, homology is defined so as to to measure the failure of $-_G$ from being exact.

Definition 2.39 *Let* M *be a* G*-module and* $P. \to M$ *a projective resolution. Consider the following complex.*

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \xrightarrow{d_0} 0$$

The r^{th} ***homology group*** *of* G *with coefficients in* M *is defined to be* $H_r(G, M) = \ker d_r / \mathrm{Im} d_{r+1}$.

Lemma 2.40 *For any* G*-module* M*,* $H_0(G, M) = M_G$*.*

Proof If $\cdots \to P_1 \to P_0 \to M \to 0$ is a projective resolution, then by right exactness, $(P_1)_G \xrightarrow{d_1} (P_0)_G \xrightarrow{\epsilon} M_G \to 0$ is exact. Hence ϵ is surjective, $M_G = (P_0)_G / \ker \epsilon = (P_0)_G / \mathrm{Im}\ d_1$. But this is $H_0(G, M)$ because $(P_0)_G = \ker d_0$. Hence the result. □

Remark 2.41 *If* $0 \to M_1 \to M_2 \to M_3 \to 0$ *is a short exact sequence of* G*-modules, it gives rise to a long exact sequence of homology.*

$$\cdots \to H_r(G, M_2) \to H_r(G, M_3) \to H_{r-1}(G, M_1) \to \cdots \to H_0(G, M_3) \to 0$$

Remark 2.42 *Also, we have* $H_r(G, M) = 0$ *for all* $r > 0$ *if* M *is of the form* $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ *for some abeian group* A*.*

Analogous to cohomology, homology is uniquely determined by properties 2.40, 2.41 and 2.42.

Similar to lemma 2.14, if M itself is projective, then $H_r(G, M) = 0$ for $r > 0$. The following lemma gives a condition for determining whether a G-module is projective or not.

Lemma 2.43 *M is projective iff it is a summand of a free $\mathbb{Z}[G]$-module.*

Proof Note that to say M is projective, it means that $\mathrm{Hom}_G(M, -)$ is exact, ie given a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$, the sequence $0 \to \mathrm{Hom}_G(M, M_1) \to \mathrm{Hom}_G(M, M_2) \to \mathrm{Hom}_G(M, M_3) \to 0$ is exact also. But $0 \to \mathrm{Hom}_G(M, M_1) \to \mathrm{Hom}_G(M, M_2) \to \mathrm{Hom}_G(M, M_3)$ is always exact. So, M is projective iff for any surjective $f : M_2 \to M_3$ and any $g : M \to M_3$, there exists $h : M \to M_2$ s.t. $g = fh$. Pictorially, we have:

$$\begin{tikzcd} & M \arrow[dl, "h"'] \arrow[d, "g"] & \\ M_2 \arrow[r, "f"] & M_3 \arrow[r] & 0 \end{tikzcd}$$

($\Rightarrow$) Assume M is projective. Let A be a generating set for M and F is the free G-module on A. Then there is a natural surjection f from F to M. Hence, by the above remarks, there exists $h : M \to F$ s.t. $fh = \mathrm{id}_M$. In particular, h is injective. Hence, we can identify M as a submodule of F and we have $F = \ker f \oplus M$.
($\Leftarrow$) Conversely, suppose M is a summand of a free G-module. First, we assume M itself is free (on a set A say). Let $f : M_2 \to M_3$ be surjective and $g : M \to M_3$. We can define a function $h : A \to M_2$ by $h(a) = f^{-1}(g(a))$ for some choice of f^{-1} (exists since f surjective). By the definition of freeness, h extends to M and $g = fh$.
In general, assume $F = M \oplus N$ is free. Let $f : M_2 \to M_3$ be surjective and $g : M \to M_3$, we can extend g to F. By above, there exists $h : F \to M_2$ s.t. $g = fh$. We can then restrict h to M and hence the result. □

Note that this shows the sequence (3) is a projective resolution of $\mathbb{Z}$. In fact, we could have replaced (3) by any projective resolutions of $\mathbb{Z}$ and proposition 2.23 would still hold.

Definition 2.44 *The* ***augmentation map*** *is defined to be $\mathbb{Z}[G] \to \mathbb{Z}$ with $\sum n_g g \mapsto \sum n_g$. The kernel is called the* ***augmentation ideal****, denoted by I_G.*

Remark 2.45 *It's not hard to see that I_G is a free $\mathbb{Z}$-module with basis $\{g - 1 | g \in G\}$. Using I_G, we can describe H_0 as $M/I_G M = M_G = H_0(G, M)$.*

If G acts of $\mathbb{Z}$ trivially, it turns out that $H_1(G, \mathbb{Z})$ is just the abelianisation of G. We will show this in two steps.

Lemma 2.46 *There is a canonical isomorphism* $H_1(G,\mathbb{Z}) \xrightarrow{\sim} I_G/I_G^2$*. Also, we have* $\mathbb{Z}[G]_G \cong \mathbb{Z}$*.*

Proof Note that $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ is exact. $\mathbb{Z}[G]$ is a free $\mathbb{Z}[G]$-module, hence projective by lemma 2.43. So $H_1(G,\mathbb{Z}[G]) = 0$. The long exact sequence arisen is as follows.

$$0 = H_1(G,\mathbb{Z}[G]) \to H_1(G,\mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G\mathbb{Z}[G] \to \mathbb{Z}/I_G\mathbb{Z} \to 0$$

But $I_G \hookrightarrow \mathbb{Z}[G]$ induces a zero map $I_G/I_G^2 \to \mathbb{Z}[G]/I_G\mathbb{Z}[G]$. Hence the sequence above gives $0 \to H_1(G,\mathbb{Z}) \to I_G/I_G^2 \to 0$ is exact. Hence, $H_1(G,\mathbb{Z}) \cong I_G/I_G^2$. It also gives $0 \to \mathbb{Z}[G]/I_G\mathbb{Z}[G] \to \mathbb{Z}/I_G\mathbb{Z} \to 0$ is exact, so $\mathbb{Z}[G]_G = \mathbb{Z}[G]/I_G\mathbb{Z}[G] \cong \mathbb{Z}/I_G\mathbb{Z} \cong \mathbb{Z}$ (as G acts on $\mathbb{Z}$ trivially). □

Lemma 2.47 *There is a canonical isomorphism* $G/G^c \to I_G/I_G^2$ *where* G^c *is the commutator subgroup of* G *(so* $G^{\mathrm{ab}} = G/G^c$*).*

Proof Define $\theta : G \to I_G/I_G^2$ by $\theta(g) = (g-1) + I_G^2$. Note that

$$\theta(gh) = gh - 1 + I_G^2 = (g-1)(h-1) + (g-1) + (h-1) + I_G^2 = \theta(g) + \theta(h)$$

since $(g-1)(h-1) \in I_g^2$. So θ is a homomorphism. I_G/I_G^2 is abelian, so θ factors through G^{ab}.
Let $\phi : I_G \to G^{\mathrm{ab}}$ be the map that sends $g-1$ to the class of g.

$$\phi((g-1)(h-1)) = \phi((gh-1) - (g-1) - (h-1)) = gh \cdot g^{-1} \cdot h^{-1}G^c = 1$$

Therefore, ϕ factors through I_G/I_G^2. ϕ and θ are inverse of each other. Hence the result. □

Corollary 2.48 *There is a canonical isomorphism* $H_1(G,\mathbb{Z}) \to G^{\mathrm{ab}}$*.*

Proof Combine the two lemmas above. □

2.4 The Tate Groups

In this section, we will assume G is a finite group throughout. For a G-module, define the norm map $N_G : M \to M$ by $m \mapsto \sum_{g\in G} gm$. It is clear that $N_G(gm) = gN_G(m) = N_G(m)$. Hence $\mathrm{Im}N_G \subseteq M^G$. It's also clear that $N_G(m - gm) = 0$, so $I_GM \subseteq \ker N_G$. Recall $H_0(G,M) = M/I_GM$ and $H^0(G,M) = M^G$ by remark 2.45 and lemma 2.13. Therefore, N_G factors through I_GM and it defines a homomorphism $N'_G : H_0(G,M) \to H^0(G,M)$. So, we can relate the cohomology groups and the homology groups as follows.

Definition 2.49 *For* G *and* M *as above, the* r^{th} ***Tate group*** *of* G *with coefficients in* M *is defined to be:*

$$H_T^r(G,M) = \begin{cases} H^r(G,M) & r > 0 \\ M^G/N_G(M) = \mathrm{coker}(N'_G) & r = 0 \\ \ker N_G/I_GM = \ker(N'_G) & r = -1 \\ H_{-r-1}(G,M) & r < -1 \end{cases}$$

Given a short exact sequence of G-modules $0 \to M_1 \to M_2 \to M_3 \to 0$, we have a commutative diagram as follows.

$$\begin{tikzcd}
\cdots \arrow[r] & H_0(G,M_1) \arrow[r] \arrow[d, "N'_{G,1}"] & H_0(G,M_2) \arrow[r] \arrow[d, "N'_{G,2}"] & H_0(G,M_3) \arrow[r] \arrow[d, "N'_{G,3}"] & 0 \\
0 \arrow[r] & H^0(G,M_1) \arrow[r] & H^0(G,M_2) \arrow[r] & H^0(G,M_3) \arrow[r] & \cdots
\end{tikzcd}$$

By snake lemma, we have an exact sequence $\mathrm{coker}(N'_{G,1}) \to \mathrm{coker}(N'_{G,2}) \to \mathrm{coker}(N'_{G,3}) \to \ker(N'_{G,1}) \to \ker(N'_{G,2}) \to \ker(N'_{G,3})$. So the norm map enables us to combine the long exact sequences of cohomology and homology to obtain the following long exact sequence.

$$\cdots H^r_T(G,M_1) \to H^r_T(G,M_2) \to H^r_T(G,M_3) \to H^{r+1}_T(G,M_1) \to \cdots$$

Remark 2.50 *Most of the results for H^r are still true for H^r_T. For example, Shapiro's lemma and its consequences are true.* Res, Cor *and* Inf *are defined for H^r_T and* $\mathrm{Res} \circ \mathrm{Cor}$ *is the mulitplication by $(G:H)$ and $H^r_T(G,M)$ is killed by $|G|$. Since we assume G is finite, $\mathrm{Ind}_1^G(M) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$. We have $H^r_T(G, \mathrm{Ind}_1^G(M)) = 0$ for all $r \in \mathbb{Z}$. In particular, the technique of dimension shifting as mentioned in remarks 2.21 and 2.38 can be extended to all $r \in \mathbb{Z}$.*

Sometimes we will drop the subscript T for simplicity. Although H^0 is not the same as H^0_T, we might abuse notations and write H^0 for H^0_T. We will write N_G for N'_G too. Below are some explicit calculations of Tate groups.

Lemma 2.51 *If we regard $\mathbb{Q}$ as a G-module where G acts trivially and consider $\mathbb{Z}$ as a submodule of $\mathbb{Q}$, we have the following.*

(a) $H^r_T(G,\mathbb{Q}) = 0$ for all r;

(b) $H^0_T(G,\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ and $H^1(G,\mathbb{Z}) = 0$;

(c) There is a canonical isomorphism from $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ *to $H^2(G,\mathbb{Z})$.*

Proof (a) For a non-zero integer m, the multiplication by m on $\mathbb{Q}$ is an isomorphism. This induces an isomorphism from $H^r_T(G,\mathbb{Q})$ onto itself, given by multiplication by m. By corollary 2.34, multiplication by $|G|$ is the zero map. But this map is an isomorphism, so $H^r_T(G,\mathbb{Q}) = 0$.
(b) Since G acts trivially on $\mathbb{Z}$, $\mathbb{Z}^G = \mathbb{Z}$ and N_G is the multiplication by $|G|$. Hence $H^0_T(G,\mathbb{Z}) = \mathbb{Z}^G/N_G(\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$.
By remark 2.28, $H^1(G,\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Z})$. But G is a finite group and the only finite subgroup of $\mathbb{Z}$ is 0, so the image of G in $\mathbb{Z}$ is always 0. Hence, $\mathrm{Hom}(G,\mathbb{Z}) = H^1(G,\mathbb{Z}) = 0$.
(c) Consider the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, the corresponding long exact sequence gives

$$H^1(G,\mathbb{Q}) \to H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z}) \to H^2(G,\mathbb{Q})$$

where the first and last term are 0 by (a). So we have an isomomrphism from $H^1(G, \mathbb{Q}/\mathbb{Z})$ to $H^2(G, \mathbb{Z})$. As in (b), we have G acting on $\mathbb{Q}/\mathbb{Z}$ trivially, so $H^1(G, \mathbb{Q}/\mathbb{Z})$ =Hom$(G, \mathbb{Q}/\mathbb{Z})$, hence we have the isomorphism as claimed. $\square$

Proposition 2.52 *If G is cyclic, then for any G-module M, there is an isomorphism $H_T^r(G, M) \to H_T^{r+2}(G, M)$ for all r.*

Proof Let g be a generator of G. Then the sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\alpha} \mathbb{Z} \to 0$$

is exact where α is the augmentation map. The groups above are free $\mathbb{Z}$-modules and so is the kernel of α, ie the augmentation ideal. Hence, the sequence is still exact when tensored with M. We have the following exact sequence of G-modules.

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

But $H_T^r(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} M) = 0$ for all $r \in \mathbb{Z}$ by remark 2.50. By dimension shifting, we have the isomorphisms claimed. $\square$

Therefore, for a cyclic group G, if we know what H_T^0 and H_T^1 are, we know everything about the Tate groups. This leads us to give the following definition.

Definition 2.53 *Let G be a finite cyclic group, M a G-module. If $H_T^r(G, M)$ are finite for $r = 0, 1$, the* ***Herbrand quotient*** *is defined to be $h(M) = \dfrac{|H_T^0(G, M)|}{|H_T^1(G, M)|}$.*

Lemma 2.54 *Let $0 \to A_1 \to A_2 \to \cdots \to A_r \to 0$ be an exact sequence of finite groups, then $|A_1| \times |A_3| \times \cdots = |A_2| \times |A_4| \times \cdots$.*

Proof We can break up the sequence into short exact sequences $0 \to A_0 \to A_1 \to C_1 \to 0$, $0 \to C_1 \to A_2 \to C_2 \to 0$,. . .,$0 \to C_{r-1} \to A_{r-1} \to A_r \to 0$ where C_i =coker$(A_{i-1} \to A_i)$ = ker$(A_{i+1} \to A_{i+2})$. Hence $|A_0||C_1| = |A_1|$, $|C_1||C_2| = |A_2|$, etc. Cancelling the $|C_i|$'s gives the result. $\square$

Proposition 2.55 *Let G be a cyclic group and $0 \to M_1 \to M_2 \to M_3 \to 0$ an exact sequence of G-modules. If any two of the Herbrand quotients $h(M_1)$, $h(M_2)$ and $h(M_3)$ are defined, then so is the third and $h(M_2) = h(M_1)h(M_3)$.*

Proof We truncate the long exact sequence of Tate groups into the following. $0 \to K \to H^0(M_1) \to H^0(M_2) \to H^0(M_3) \to H^1(M_1) \to H^1(M_2) \to H^1(M_3) \to K' \to 0$ where we dropped the G's in our notation for simplicity and K =coker$(H^{-1}(M_2) \to H^{-1}(M_3))$, K' =coker$(H^1(M_2) \to H^1(M_3))$. Hence, by exactness, if two pairs of the H^0's and H^1's are finite, so are the other terms. Hence the first part of the statement. By proposition 2.52, $K \cong K'$ since G is cyclic. We obtain the second part of the statement by lemma 2.54. $\square$

Proposition 2.56 *If G is a finite cyclic group, M a finite G-module, then $h(M) = 1$.*

Proof Since M is finite, so are M^G and M_G. Let g be a generator of G, then we have an exact sequence $0 \to M^G \to M \xrightarrow{g-1} M \to M_G \to 0$. Hence $|M^G| = |M_G|$ by lemma 2.54. Recall $H^0(G, M) = \text{coker}(N_G)$ and $H^{-1}(G, M) = \ker(N_G)$. So, we have

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

is exact. Agian, by lemma 2.54, we have $|H^0(G, M)| = |H^{-1}(G, M)|$. By proposition 2.52, $|H^{-1}(G, M)| = |H^1(G, M)|$. Therefore, we have $|H^0(M)| = |H^1(M)|$, hence the result. $\Box$

Corollary 2.57 *Let $\alpha : M \to N$ be a homomorphism of G-modules with finite kernel and cokernel. If either $h(M)$ or $h(N)$ is defined, then so is the other and they are equal*

Proof Consider the following exact sequences.

$$0 \to \alpha(M) \to N \to \text{coker}(\alpha) \to 0 \quad \text{and} \quad 0 \to \ker(\alpha) \to M \to \alpha(M) \to 0$$

By proposition 2.56, $h(\text{coker}\alpha) = h(\ker \alpha) = 1$. If $h(N)$ is defined, proposition 2.55 applied to the first sequence shows that $h(\alpha M)$ is defined and equals $h(N)$. Consider the second sequence, we have $h(M) = h(\alpha M)$, again by proposition 2.55. So $h(M) = h(N)$.
Similary, if $h(M)$ is defined, then $h(\alpha M) = h(M)$ from the second sequence and $h(N) = h(\alpha M)$ from the first sequence. $\Box$

We will make use of Herbrand quotients to prove results on cyclic extensions later. Now, we will prove Tate's theorem. The version we use here is slightly weaker than the one in [3]. Nevertheless, it is a very powerful result because it relates the Tate groups of $\mathbb{Z}$ to a large class of G-modules which we will consider later.

Theorem 2.58 *If M is a G-module and $H^1(H, M) = H^2(H, M) = 0$ for all subgroup H of G, then $H^r(G, M) = 0$ for all $r \in \mathbb{Z}$.*

Proof We consider three cases.
Case 0: G is cyclic. The result follows immediately from the isomorphisms in proposition 2.52.
Case 1: G is soluble. Let H be a proper normal subgroup s.t. G/H is cyclic. $|H| < |G|$, so by induction $H^r(H, M) = 0$ for all r. Hence, for $r > 0$, we have the inflation-restriction exact sequence:

$$0 \to H^r(G/H, M^H) \xrightarrow{\text{Inf}} H^r(G, M) \xrightarrow{\text{Res}} H^r(H, M)$$

$H^1(G, M) = H^2(G, M) = 0$, so $H^1(G/H, M^H) = H^2(G/H, M^H) = 0$. But G/H is cyclic, so $H^r(G/H, M^H) = 0$ for all r by case 0. Hence the exact sequence above implies $H^r(G, M) = 0$ for $r > 0$.

By remark 2.50, we have $H^r(H, M) \cong H^{r-1}(H, \mathrm{Ind}_1^G M/M)$ for all r and H. Hence by the results for $r > 0$ applied to $\mathrm{Ind}_1^G M/M$, we have $H^0(G, M) \cong H^1(G, \mathrm{Ind}_1^G M/M) = 0$. Using the same argument, we can show $H^r(G, M) = 0$ for all $r < 0$ inductively.
Case 2: G any finite group. Fix a prime p. Let G_p be a Sylow p-subgroup of G. Then G_p is soluble. Case 1 implies that $H^r(G_p, M) = 0$ for all r. By corollary 2.35, elements in $H^r(G, M)$ of order of prime powers must be 0, so $H^r(G, M)$ itself is 0. □

Theorem 2.59 (Tate) *Let M be a G-module. Suppose that for all subgroups H of G, we have*

(a) $H^1(H, M) = 0$, and

(b) $H^2(H, M)$ is a cyclic group of order $|H|$.

Then there is an isomorphism from $H^r(G, \mathbb{Z})$ to $H^{r+2}(G, M)$.

Proof The idea is to extend M to another G-module M' which satisfies the condtions of theorem 2.58. Then $H_T^r(G, M') = 0$ for all r and we will then use dimension shifting to relate $H^{r+2}(G, M)$ and $H^r(G, \mathbb{Z})$.
By (b), $H^2(G, M)$ is cyclic of order $|G|$. Let γ be a generator of $H^2(G, M)$. For a subgroup H of G, Cor∘Res$= (G : H) = |G|/|H|$. But $H^2(H, M)$ is cyclic of order $|H|$, so $\mathrm{Res}(\gamma)$ generates $H^2(H, M)$.
Let f be a 2-cochain in $\ker d^3$ as in definition 2.25 representing the class of γ in $H^2(G, M)$. Let $M' = M \oplus \mathbb{Z}[X]$ where $X = \{x_g | g \in G - \{1\}\}$. The action of G on M extends to M' by setting $g \cdot x_h = x_{gh} - x_g + f(g, h)$ with $x_1 = f(1, 1)$. It is not hard to check that this does define an action on M' using the condition on $f \in \ker d^3$.
The inclusion $M \hookrightarrow M'$ induces a homomorphism $H^2(G, M) \to H^2(G, M')$. Let f' be the 1-cochain which sends g to x_g. Then $(d^2 f')(g, h) = gf'(h) - f'(gh) + f'(g) = gx_h - x_{gh} + x_g = f(g, h)$. Hence $f : G^2 \to M \hookrightarrow M'$ is in Im d^2. So γ is mapped to zero in $H^2(G, M')$.
Claim $H^1(H, M') = H^2(H, M') = 0$ for all subgroups H of G.
Proof of claim Recall we have an exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \tag{6}$$

But $H^r(H, \mathbb{Z}[G]) = 0$ for all r by remark 2.50, so the long exact sequence of Tate groups gives isomorphisms $H^1(H, I_G) \cong H^0(H, \mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z}$ and $H^2(H, I_G) \cong H^1(H, \mathbb{Z}) = 0$ $(*)$ by lemma 2.51. In particular, $|H^1(H, I_G)| = |H|$ (†).
Define $\alpha : M' \to \mathbb{Z}[G]$ by $\alpha(m) = 0$ for $m \in M$ and $\alpha(x_g) = g - 1$. Then we have a short exact sequence of G-modules as follows.

$$0 \to M \to M' \xrightarrow{\alpha} I_G \to 0 \tag{7}$$

But $H^1(H, M) = H^2(H, I_G) = 0$ by (a) and $(*)$, so the long exact sequence arisen gives

$$0 \to H^1(H, M') \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M') \to 0$$

is exact. As noted above, $H^2(H, M)$ is generated by $\text{Res}(\gamma)$, but γ is mapped to 0 in $H^2(G, M')$. So, the map $H^2(H, M) \to H^2(H, M')$ is 0 also. Hence $H^1(H, I_G) \to H^2(H, M)$ is onto. Hypothesis (b) says that $|H^2(H, M)| = |H|$. But we have $|H^1(H, I_G)| = |H|$ by (†). So this map is an isomorphism. Hence the kernel ($H^1(H, M')$) and the cokernel ($H^2(H, M')$) are both 0. Hence the claim.
With this claim, we can apply theorem 2.58 and get $H^r(H, M') = 0$ for all r. Now, if we combine the exact sequences (6) and (7), we have an exact sequence

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

with $H^r(G, M') = H^r(G, \mathbb{Z}[G]) = 0$ for all r. Hence, we have the isomorphisms claimed by dimension shifting on Tate groups. □

2.5 Profinite Groups

It turns out that considering finite groups alone isn't enough. For example, $\text{Gal}(\bar{K}/K)$ is in general not a finite group. However, it can be constructed from finite Galois groups since $\bar{K} = \cup L$ where L runs through the finite Galois extensions of K. We will make this idea precise below.

Definition 2.60 *Let I be a directed partially ordered set. Assume $\{G_i | i \in I\}$ is a set of groups together with homomorphisms $\alpha_{ij} : G_j \to G_i$ for all $i \leq j$ satisfying*

(a) $\alpha_{ii} = \text{id}\ \forall i \in I$, and

(b) $\alpha_{ij} \circ \alpha_{jk} = \alpha_{ik}$ whenever $i \leq j \leq k$.

The family (G_i, α_{ij}) is called a ***inverse system****.*

Let (G_i, α_{ij}) be a inverse system. We would like to in some sense glue the G_i's together. To be precise, we define the inverse limit of the inverse system to be $\{(g_i) \in \prod_{i \in I} G_i | \alpha_{ij}(g_j) = g_i \forall i \leq j\}$, denoted by $\varprojlim G_i$. If each G_i has a topology and all α_{ij} are continuous, then the inverse limit is a closed subspace in the product space. In fact, we can always give a discrete topology on the G_i's. This is of particular importance if they are finite since each G_i will be compact Hausdorff, and so will be the inverse limit. We give the following definition.

Definition 2.61 *A topological group is called a* ***profinite group*** *if it is the inverse limit of an inverse system of finite groups (each equipped with discrete topology).*

Lemma 2.62 *If G is a profinite group, then the open normal subgroups of G form a fundamental system of neighbourhoods of* 1.

Proof Let $G = \varprojlim G_i$. If $\pi_i : G \to G_i$ is the natural projection of the product space restricted to G, π_i is a continuous homomorphism. Hence, $\ker \pi_i$ is an open normal subgroup of G. But the topology of G is induced from the discrete topology on the G_i's, so an open neighbourhood of 1 contains a finite intersection of $\ker \pi_i$. Hence the result. $\square$

Example 2.63 *If K is a local field, then the ring of integers $\mathcal{O}_K$ is a profinite group since it is isomorphic to $\varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ $(x \mapsto (x + \pi^n\mathcal{O}_K)_n)$ where π is a uniformiser. In particular, from the proof above, $\pi^n\mathcal{O}_K$ form a fundamental system of neighbourhoods of* 0.

Conversely, if G is any topological group and $\{N_i | i \in I\}$ is a set of normal subgroups of finite index, the profinite group $\varprojlim G/N$ is the completion of G where the N_i's are ordered by reverse inclusion.

Back to $\mathrm{Gal}(\bar{K}/K)$. Let $K \leq L_1 \leq L_2$ be a tower of finite Galois extensions. There is a natural map from $\mathrm{Gal}(L_2/K)$ to $\mathrm{Gal}(L_1/K)$ by restriction. This gives an inverse system of finite Galois groups. Let G be the corresponding inverse limit. Moreover, $\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L) \cong \mathrm{Gal}(L/K)$, this gives an isomorphism $G \cong \mathrm{Gal}(\bar{K}/K)$. Therefore, $\mathrm{Gal}(\bar{K}/K)$ is a profinite group.

Analogously, we define direct system and direct limit as follows.

Definition 2.64 *Let I be a directed partially ordered set. Assume $\{G_i | i \in I\}$ is a set of abelian groups together with homomorphisms $\alpha_{ji} : G_i \to G_j$ for all $i \leq j$ satisfying*

(a) $\alpha_{ii} = \mathrm{id}\ \forall i \in I$, *and*

(b) $\alpha_{kj} \circ \alpha_{ji} = \alpha_{ki}$ *whenever* $i \leq j \leq k$.

The family (G_i, α_{ij}) is called a ***direct system****.*

Given a direct system (G_i, α_{ij}), define an equivalence relation on $\sqcup G_i$ so that $g_i \in G_i$ is equivalent to $g_j \in G_j$ iff $\alpha_{ki}(g_i) = \alpha_{kj}(g_j)$ for some $k \geq i, j$. The corresponding quotient set is called the *direct limit* of G_i, denoted by $\varinjlim G_i$. Given two direct systems (G_i, α_{ij}) and (H_i, β_{ij}), with homomorphisms $f_i : G_i \to H_i$ s.t. $f_j\alpha_{ji} = \beta_{ji}f_i$ for all $i \leq j$, these f_i's define a homomorphism $f : \varinjlim G_i \to \varinjlim G_i$.

Let (G_i, α_{ij}), (H_i, β_{ij}), (K_i, γ_{ij}) be direct systems with $G_i \xrightarrow{f_i} H_i \xrightarrow{g_i} K_i$ exact for all $i \in I$. Then we can define $\varinjlim G_i \xrightarrow{f} \varinjlim H_i \xrightarrow{g} \varinjlim K_i$. It turns out to be exact. A similar statement can be made about inverse limits.

Remark 2.65 *Therefore, the formation of direct limits commutes with the passage to cohomology in complexes.*

We refine our definition of G-modules for a profinite group as follows.

Definition 2.66 *Let G be a profinite group. A G-**module** M is an abelian group equipped with the discrete topology, together with a continuous action of G on M.*

We can define cohomology groups $H^r_{\text{cts}}(G, M)$ by taking injective resolutions, just as before. The groups can be calculated using continuous cochains, ie continuous maps from G^r to M. We denote the set of such cochains by $C^r_{\text{cts}}(G, M)$. We have $d^{r+1} : C^r_{\text{cts}}(G, M) \to C^{r+1}_{\text{cts}}(G, M)$ as before. It turns out that the cohomology of profinite groups is just the direct limit of the cohomology of finite groups. It can be shown by the following lemma.

Lemma 2.67 *Let f be a continuous r-cochain, then f arises from an element in $C^r(G/H, M^H)$ for some open normal subgroup H of G by inflation.*

Proof Let $f : G^r \to M$ be a continuous r-cochain. Then $f(G^r)$ is compact because G^r is. But M is discrete, hence $f(G^r)$ is finite. The stabliser of a point in M is an open normal subgroup of G. So $f(G^r)$ is contained in M^{H_0} where H_0 is the intersection of the stablisers of elements of $f(G^r)$. Note that H_0 is open normal in G.
$f^{-1}(m)$ is open for each $m \in f(G^r)$, hence contains the translation of some H^r_m, where H_m is an open normal subgroup of G. Let H_1 be the intersection of these H_m's. Then H_1 is open normal and f factors through $(G/H_1)^r$. If $H = H_0 \cap H_1$, then f arises by inflation from an r-cochain on G/H with values in M^H. $\square$

Proposition 2.68 *The maps* $\mathrm{Inf} : H^r(G/H, M^H) \to H^r_{\text{cts}}(G, M)$ *realise the group $H^r_{\text{cts}}(G, M)$ as the direct limit of the groups $H^r(G/H, M^H)$ as H runs through the open normal subgroups H of G.*

Proof If $H_1 \leq H_2$ are open normal subgroups, we have the natural map $G/H_1 \to G/H_2$ and inflation map $C^r(G/H_2, M_2^H) \to C^r(G/H_1, M_1^H)$ since $(G/H_1)/(H_2/H_1) \cong G/H_2$. So, we get a direct system. Lemma 2.67 implies that the corresponding direct limit is indeed $C^r_{\text{cts}}(G, M)$. Now, take cohomology and we obtain the result by remark 2.65. $\square$

We sometimes drop the cts subscript for simplicity. What the proposition says is that $H^r(\lim\limits_{\leftarrow} G_i, M) = \lim\limits_{\rightarrow} H^r(G_i, M^{G_i})$. If M itself is a direct limit, we have the following.

Proposition 2.69 *Let G be a profinite group, and let M be a G-module. If $M = \varinjlim M_i$ where M_i are submodules of M ordered by inclusion, then we have $H^r(G, M) = \varinjlim H^r(G, M_i)$.*

Proof As before, if f is a continuous r-cochain, its image is finite. Hence it's contained in some M_i as the M_i's form a direct system ordered by inclusion (for any $M_{i_1}, M_{i_2}, \ldots, M_{i_k}$, there is M_j containing all $M_{i_1}, M_{i_2}, \ldots, M_{i_k}$ by induction).

Therefore, $C^r(G,M) = \varinjlim C^r(G,M_i)$. Hence by remark 2.65, we have the result. $\square$

Finally, we introduce a result on cohomology triviality. The idea is that we can show a G-module has trivial cohomology via filtration. We will use this result later on.

Proposition 2.70 *Let G be a finite group, M a G-module, $M^i, i \geq 0$ a descending chain of submodules s.t. $M^0 = M$ and $M = \varprojlim M/M^i$. If $r > 0$ and $H^r(G, M^i/M^{i+1}) = 0$ for all i, then $H^r(G,M) = 0$.*

Proof If f is a r-cochain $\in \ker d^{r+1}$ with values in M, there is a $(r-1)$-cochain g_1 s.t. $f = d^r g_1 + f_1$ where f_1 takes values in M^1 since $H^r(G, M/M^1) = 0$. Inductively, we construct f_n, g_n s.t. $f_n = d^r g_{n+1} + f_{n+1}$ where $f_n \in \ker d^{r+1}$ with values in M^n and g_n is a $(r-1)$-cochain with values in M^{n-1}. Let $g = g_1 + g_2 + \cdots$, this converges by the assumption on the inverse limit. It defines a $(r-1)$-cochain with values in M and $f = d^r g$ by continuity. Hence $f \in \mathrm{Im} d^r$, so $H^r(G,M) = 0$ $\square$

3 Reciprocity Law

In this section, we will use cohomology to prove the existence in theorem 1.1. Throughout this section, unless otherwise stated, K will always be a fixed local field. $\mathcal{O}_K$ denotes the ring of integers and $\mathfrak{M}_K$ denotes the unique maximal ideal of $\mathcal{O}_K$. Results on local fields can be found in [2].

Given a finite Galois extension L of K, if $G = \mathrm{Gal}(L/K)$, G acts on L and $L^\times$. So, L and $L^\times$ are natuarally G-modules. Note that the norm map N_G we used in the last section to define the Tate groups now become $Tr_{L/K}$ and $(N_{L/K})|_{L^\times}$ respectively. We will see that $H^1(G, L^\times)$ is always trivial, so we will be more interested in $H^2(G, L^\times)$. To simplify notations, we write $H^2(L/K)$ for $H^2(G, L^\times)$.

3.1 Cohomology of Local Fields

Using the description of H^1 by crossed homomorphisms in the previous sections, we can show that $H^1(G, L^\times) = 0$ as claimed above.

Theorem 3.1 (Hilbert's Theorem 90) *Let L/K be a finite Galois extension with Galois group G, then $H^1(G, L^\times) = 0$.*

Proof Recall $H^1(G, L^\times) = \{\text{crossed homos}\}/\{\text{principal crossed homos}\}$. Let $f : G \to L^\times$ be a crossed homomorphism, ie $f(g'g) = (g'f(g))f(g')$ for all $g, g' \in G$.

For $a \in L^\times$, let $b = \sum_{g\in G} f(g)^{-1}(ga)$. For a fixed $g' \in G$, we have

$$\begin{aligned} g'b &= \sum_{g\in G}(g'f(g))^{-1}(g'ga) \\ &= f(g')\sum_{g\in G} f(g'g)^{-1}(g'ga) \text{ (since } f \text{ is a crossed homo)} \\ &= f(g')b \end{aligned}$$

By the independence of characters, there exists a s.t. $b \neq 0$. Hence $f(g) = g{\cdot}b/b$, ie f is principal. Therefore, $H^1(G, L^\times) = 0$. □

This is a very useful result as we will see later on. Our first application is to apply it to he inflation-restriction sequence to say something about H^2.

Lemma 3.2 *If $E \supseteq L \supseteq K$ is a tower of Galois extension, then there is an exact sequence $0 \to H^2(L/K) \xrightarrow{\text{Inf}} H^2(E/K) \xrightarrow{\text{Res}} H^2(E/L)$.*

Proof By the fundamental theorem of Galois theory, $H = \mathrm{Gal}(E/L)$ is a normal subgroup of $G = \mathrm{Gal}(E/K)$ and $G/H = \mathrm{Gal}(L/K)$. By theorem 3.1, $H^1(H, E^\times) = 0$. Hence, by proposition 2.37, there is an exact sequence $0 \to H^2(G/H, (E^\times)^H) \to H^2(G, E^\times) \to H^2(H, E^\times)$. This gives the exact sequence claimed since $(E^\times)^H = L^\times$ by the Galois correspondence. □

In fact, the cohomology of L is even simplier than that of $L^\times$. $H^0(G, L) = L^G = K$ as usual. For cohomology in positive dimensions, we have the following.

Proposition 3.3 *Let L/K be a finite Galois extension of a local field with Galois group G, then $H^r(G, L) = 0$ for all $r > 0$.*

Proof By the normal basis theorem, there exists $\alpha \in L$ s.t. $\{g\alpha | g \in G\}$ gives a basis of L over K. So $L \cong K[G]$ as a G-module. But we have $K[G] = \mathrm{Ind}_1^G K$, so $H^r(G, L) = H^r(1, K) = 0$ for $r > 0$ by Shapiro's lemma and lemma 2.15. □

We now turn our attention to unramified extensions. Recall from local fields, we have the following.

Theorem 3.4 *If L/K is a finite unramified extension, then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for any α s.t. $\bar{\alpha}$ generates k_L over k_K.*

Lemma 3.5 *Let L/K be a finite unramified extension, then L/K is Galois iff k_L/k_K is Galois. Moreover, in this case,* $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$.

If L/K is a finite unramified extension inside K^{al} (recall K^{al} is a fixed separable algebraic closure of K), then L/K is Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$. Since k_K is finite, and k_L/k_K is a finite extension, $G = \mathrm{Gal}(L/K)$ is cyclic, generated by the Frobenius map $x \mapsto x^q$ where $q = |k_K|$. We denote this element by $\mathrm{Frob}_{L/K}$.

We write U_L for the group of units in L and $U_L^{(m)} = 1 + \mathfrak{M}_L^m$. Recall from local fields that we have $U_L/U_L^{(1)} \cong k_L^\times$ and $U_L^{(m)}/U_L^{(m+1)} \cong k_L$ as G-modules. As shown below, both have trivial Tate groups.

Lemma 3.6 *With the above notations, $H_T^r(G, k_L^\times) = 0$ for all r. In particular, the norm map $k_L^\times \to k_K^\times$ is surjective.*

Proof By theorem 3.1, $H_T^1(G, k_L^\times) = 0$. Note that G is cyclic. By proposition 2.56, $h(k_L^\times) = 1$. So $H_T^0(G, k_L^\times) = 0$ too. Hence, by proposition 2.52, all the H_T^r's are 0.
$H_T^0(G, k_L^\times) = (k_L^\times)^G / N_{L/K}(k_L^\times)$ by definition. But $(k_L^\times)^G = k_K^\times$. So $H_T^0(G, k_L^\times) = 0$ implies $N_{L/K} : k_L^\times \to k_K^\times$ is surjective. □

Lemma 3.7 *With the above notations, $H_T^r(G, k_L) = 0$ for all r. In particular, the trace map $k_L \to k_K$ is surjective.*

Proof As in the proof of proposition 3.3, we can show that $H^r(G, k_L) = 0$ for all $r > 0$. Hence proposition 2.52 proves the first statement. Similar to the proof of lemma above, $H_T^0 = 0$ implies the surjectivity claimed. □

Using these two results, we can show that U_L itself has trivial cohomology in positive dimensions by proposition 2.70. In fact, all Tate groups are trivial. We prove this in two steps.

Proposition 3.8 *For any finite unramified extension L/K, the norm map restricted to U_L, $N_{L/K} : U_L \to U_K$ is surjective.*

Proof Let $u \in U_K$. Then by lemma 3.6 and $U_K/U_K^{(1)} \cong k_K^\times$, there exists $v_0 \in U_L$ s.t. $N_{L/K}(v_0) \equiv u \bmod U_K^{(1)}$.
Note that under the isomorphism $U_L^{(m)}/U_L^{(m+1)} \cong k_L$, multiplication on the left corresponds to addition on the right. So the norm map on the left corresponds to the trace map on the right, which is surjective by lemma 3.7. Hence, there exists $v_1 \in U_L^{(1)}$ s.t. $N_{L/K} \equiv u/N_{L/K}(v_0) \bmod U_K^{(2)}$. Continue inductively, we have a sequence (v_n) where $v_n \in U_L^{(n)}$ and $u/N_{L/K}(v_0 \cdots v_n) \in U_K^{(n+1)}$. Let $v = \lim_{n\to\infty} \prod_{i=1}^{n} v_i$. Then $u/N_{L/K}(v) \in U_K^{(n)}$ for all n, hence it can only be 1. So $N_{L/K}(v) = u$. □

Proposition 3.9 *Let L/K be a finite unramified extension with Galois group G. Then $H_T^r(G, U_L) = 0$ for all r.*

Proof If π is a uniformiser of K, it's also a uniformiser of L. So, $L^\times \cong U_L \times \pi^{\mathbb{Z}}$ and G acts trivially on $\pi^{\mathbb{Z}} \cong \mathbb{Z}$. By remark 2.18, $H^r(G, L^\times) = H^r(G, U_L) \times H^r(G, \pi^{\mathbb{Z}})$. By theorem 3.1, $H^1(G, L^\times) = 0$, so $H^1(G, U_L) = 0$. By proposition 3.8, $H_T^0(G, U_L) = U_K/N_{L/K}(U_L) = 0$. But G is cyclic, hence the result by proposition 2.52. □

Remark 3.10 *If L/K is an infinite unramified extension, $H^r(G, U_L) = 0$ for all $r > 0$ by taking direct limit in proposition 3.9. This enables us to work out $H^r(G, L^\times)$ as below.*

Lemma 3.11 *Let L be an unramified extension of K (possibly infinite), $G = \mathrm{Gal}(L/K)$, then $H^r(G, L^\times) \cong H^r(G, \mathbb{Z})$ for all $r > 0$.*

Proof As above, $H^r(G, L^\times) = H^r(G, U_L) \times H^r(G, \pi^{\mathbb{Z}})$. But we have shown that $H^r(G, U_L) = 0$ for all $r > 0$, hence the isomorphisms claimed. □

3.2 The Invariant Map

We will now define the invariant map for an unramified extension which we will extend to a general extension later. It will eventually enable us to define a map which satisfies the conditions in theorem 1.1 proving the existence of ϕ_K as claimed.

We noted in the proof of lemma 2.51 that $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$ for any G acting on $\mathbb{Q}$ trivially. For L/K an unramified extension, with $G = \mathrm{Gal}(L/K)$, G is generated by σ =Frob_K, the Frobenius map. Hence, we have a homomorphism from $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ to $\mathbb{Q}/\mathbb{Z}$ by sending f to $f(\sigma)$. On the other hand, we showed that $H^r(G, \mathbb{Q}) = 0$ for all r, so the long exact sequence arises from the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ gives an isomorphism $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$. Finally, we have an isomorphism $\theta : H^2(L/K) \to H^2(G, \mathbb{Z})$ induced by ord_L by lemma 3.11. Putting all these together, we have the following definition.

Definition 3.12 *The composition map from $H^2(L/K)$ to $\mathbb{Q}/\mathbb{Z}$ defined below is called the **invariant map** of L/K.*

$$H^2(L/K) \xrightarrow{\theta} H^2(G, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}$$

We denote this map by $\mathrm{inv}_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$.

Since G is cyclic of order $n := [L : K]$, generated by σ, the valuation map $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ is injective with image $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Since δ and θ are both isomorphisms, $\mathrm{inv}_{L/K}$ defines an injective homomorphism with the same image.

Note that the composite of two finite unramified extensions of K is again unramified (as the value group will stay the same). Hence, the union of all finite unramified extensions of K is an infinite unramified extension of K. We denote this field by K^{un}. Now, consider the corresponding residue field $k_{K^{\mathrm{un}}}$. It is the union of all the finite extensions of k_K, hence it's just $\bar{k}_K$. Moreover, $\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \mathrm{Gal}(\bar{k}_K/k_K) \cong (\mathrm{Frob}_K)^{\hat{\mathbb{Z}}}$ where $\mathrm{Frob}_K : x \mapsto x^q$.

Remark 3.13 *Explicitly, we have $K^{\mathrm{un}} = \cup_{p \nmid m} K(\mu_m)$ where $p = \mathrm{char}(k_K)$. By the following lemma, we can in fact extend the invariant maps of finite unramified extensions to K^{un}*

Lemma 3.14 *There is a canonical isomorphism* $\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$.

Proof Let $E \supseteq L \supseteq K$ be a tower of unramified extensions. Since all the maps in the definition of inv are compatible with Inf, the following diagram commutes.

$$\begin{tikzcd}
H^2(L/K) \arrow[r, "\mathrm{inv}_{L/K}"] \arrow[d, "\mathrm{Inf}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\mathrm{id}"] \\
H^2(E/K) \arrow[r, "\mathrm{inv}_{E/K}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

As remarked above, if $[L : K] = n$, then $H^2(L/K)$ is isomorphic to its image under $\mathrm{inv}_{L/K}$, $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ inside $\mathbb{Q}/\mathbb{Z}$. So, by taking direct limit, we have the isomorphism claimed. $\square$

Definition 3.15 *The map* inv_K *defined above is called the* ***invariant map*** *of* K.

Given an extension L/K, we can relate the two invariant maps inv_K and inv_L as follows.

Proposition 3.16 *Let* L *be a finite extension of* K *of degree* n*. There is a commutative diagram as shown below.*

$$\begin{tikzcd}
H^2(K^{\mathrm{un}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(L^{\mathrm{un}}/L) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "n"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Proof Since K^{un} and L^{un} are obtained from adjoining roots of unity, we have $L^{\mathrm{un}} = L \cdot K^{\mathrm{un}}$. Hence $\tau \mapsto \tau|_{K^{\mathrm{un}}}$ defines an injection from $\mathrm{Gal}(L^{\mathrm{un}}/L)$ to $\mathrm{Gal}(K^{\mathrm{un}}/K)$. This gives the homomorphism Res in the diagram.
For simplicity, write $G_K = \mathrm{Gal}(K^{\mathrm{un}}/K)$ and $G_L = \mathrm{Gal}(L^{\mathrm{un}}/L)$. Let e and f be the ramification index and the residue degree of L/K respectively. Consider the following diagram where the horizontal rows are just the invariant maps inv_K and inv_L respectively.

$$\begin{tikzcd}
H^2(K^{\mathrm{un}}/K) \arrow[r, "\theta"] \arrow[d, "\mathrm{Res}"] & H^2(G_K, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "e\mathrm{Res}"] & H^1(G_K, \mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "e\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n"] \\
H^2(L^{\mathrm{un}}/L) \arrow[r, "\theta"] & H^2(G_L, \mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(G_L, \mathbb{Q}/\mathbb{Z}) \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

The first square commutes because it can be obtained from the following commutative diagram.

$$\begin{tikzcd}
(K^{\mathrm{un}})^{\times} \arrow[r, "\mathrm{ord}_K"] \arrow[d] & \mathbb{Z} \arrow[d, "e"] \\
(L^{\mathrm{un}})^{\times} \arrow[r, "\mathrm{ord}_L"] & \mathbb{Z}
\end{tikzcd}$$

The second square commutes because the restriction map commutes with the boundary map (ie δ) in the long exact sequence. For the third square, consider the following.

$$\begin{tikzcd} \mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\phi\mapsto\phi(\sigma)"] \arrow[d, "\phi\mapsto\phi|_{G_L}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "f"] \\ \mathrm{Hom}(G_L, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\phi\mapsto\phi(\sigma)"] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

where σ denotes both the Frobenius map of K and L. Since $|k_L| = |k_K|^f$, $(\mathrm{Frob}_L)|_K = \mathrm{Frob}_K^f$. The above diagram commutes. By multiplying e, we have the third square commutes as well. This proves the proposition. $\Box$

3.3 Extending the Invariant Map

In this section, we will extend the invariant map $\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ defined above to $H^2(K^{\mathrm{al}}/K)$. To do this, we show that $H^2(L/K)$ lies inside $H^2(K^{\mathrm{un}}/K)$ for any finite Galois extension L/K. In other words, $H^2(K^{\mathrm{un}}/K)$ is in fact $H^2(K^{\mathrm{al}}/K)$. We establish this embedding in several steps.

Lemma 3.17 *If L/K is Galois of degree n, then $H^2(L/K)$ has a subgroup of order n.*

Proof Consider the following diagram.

$$\begin{tikzcd} 0 \arrow[r] & \ker(\mathrm{Res}) \arrow[r] \arrow[d] & H^2(K^{\mathrm{un}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{Inf}"] & H^2(L^{\mathrm{un}}/L) \arrow[d, "\mathrm{Inf}"] \\ 0 \arrow[r] & H^2(L/K) \arrow[r] & H^2(K^{\mathrm{al}}/K) \arrow[r, "\mathrm{Res}"] & H^2(K^{\mathrm{al}}/L) \end{tikzcd}$$

Since the two vertical inflation maps are injective (by considering continuous cochains), the first vertical map is injective also. Consider the commutative diagram in proposition 3.16. inv_K and inv_L are both isomorphisms, so $\ker(\mathrm{Res}) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. But it is embedded in $H^2(L/K)$. This proves the lemma. $\Box$

Lemma 3.18 *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then there exists an open subgroup V of U_L which is also a G-module s.t. $H^r(G,V) = 0$ for all $r > 0$.*

Proof Let $x \in L$ be s.t. $\{gx|g \in G\}$ gives a basis for L over K. If d is a common denominator of these gx's, then we can replace x by dx, ie we may assume this basis is in $\mathcal{O}_L$. Let $A = \sum \mathcal{O}_K(gx)$. It is stable under the action of G and is open in $\mathcal{O}_L$. $0 \in A$, so there exists n s.t. $\pi_L^n\mathcal{O}_L \subseteq A$ by example 2.63. Hence, $\pi_K^n\mathcal{O}_L \subseteq A$ as $\mathrm{ord}_L(\pi_K) \geq 1$. Let $M = \pi_K^{n+1}A$, then $V := 1 + M$ is an open subgroup of U_L which is stable under G.
It remains to show that $H^r(G,V) = 0$ for $r > 0$. The strategy is to apply proposition 2.70, so we define a filtration by $V^i := 1 + \pi_K^i M$ for $i \geq 0$ and we

need to show V^i/V^{i+1} has trivial cohomology. Define $\theta : V^i \to M/\pi_K M$ by $\theta(1+\pi_K^i\beta) = \beta + \pi_K M$ where $\beta \in M$.
Claim θ is a homomorphism.
Proof of claim If $\beta_1, \beta_2 \in M = \pi_K^{n+1}A \subseteq \pi_K^{n+1}\mathcal{O}_L$, then $\beta_1\beta_2 \in \pi_K^{2n+2}\mathcal{O}_L \subseteq \pi_K^{n+2}A = \pi_K M$. Hence, we have:

$$\begin{aligned}
\theta(1+\pi_K^i\beta_1)(1+\pi_K^i\beta_2) &= \theta(1+\pi_K^i(\beta_1+\beta_2+\pi_K^i\beta_1\beta_2)) \\
&= \beta_1+\beta_2+\pi_K^i\beta_1\beta_2+\pi_K M \\
&= \beta_1+\beta_2+\pi_K M \\
&= \theta(1+\pi_K^i\beta_1)+\theta(1+\pi_K^i\beta_2)
\end{aligned}$$

Hence the claim.
Note that $\theta(1+\pi_K^i\beta) = 0$ iff $\beta \in \pi_K M$ iff $1+\pi_K^i\beta \in V^{i+1}$, so $\ker\theta = V^{i+1}$. Hence, $V^i/V^{i+1} \cong M/\pi_K M$.
But $M = \pi_K^{n+1}A$, so $M \cong A$ and $M/\pi_K M \cong A/\pi_K A$ as G-modules. $A = \sum \mathcal{O}_K(gx)$, so $A/\pi_K A = \sum k_K(gx) \cong k_K[G] \cong \mathrm{Ind}_1^G(k_K)$. Therefore, we have $H^r(G, M/\pi_K M) = H^r(G, V^i/V^{i+1}) = 0$ for all $r > 0$ by corollary 2.17. Hence, we are done by proposition 2.70. □

Lemma 3.19 *Let L/K be a cyclic extension of degree n, then $h(U_L) = 1$ and $h(L^\times) = n$.*

Proof Let V be an open subgroup of U_L given by lemma 3.18. So, $H_T^1(G,V) = H_T^2(G,V) = 0$. But G is cyclic, so $H_T^0(G,V) = H_T^2(G,V) = 0$ by proposition 2.52. Hence, $h(V)$ is defined and is equal to 1. Since U_L is compact, U_L/V is finite. Apply corollary 2.57 to the inclusion $V \hookrightarrow U_L$, we get $h(U_L) = h(V) = 1$, ie first half of the lemma.
Consider the exact sequence $0 \to U_L \to L^\times \xrightarrow{\mathrm{ord_L}} \mathbb{Z} \to 0$, we have $h(L^\times) = h(U_L)h(\mathbb{Z})$ by proposition 2.55. By lemma 2.51(b), we have $h(\mathbb{Z}) = n$. Hence, $h(L^\times) = n$. □

Lemma 3.20 *Let L be a finite Galois extension of K of order n, then $H^2(L/K)$ has order n.*

Proof If G is cyclic, then by proposition 2.52, $H^2(L/K) \cong H_T^0(G, L^\times)$. Lemma 3.19 says that $h(L^\times) = |H_T^0(G,L^\times)|/|H_T^1(G,L^\times)| = n$. Theorem 3.1 says that $H_T^1(G,L^\times) = 0$, hence $|H_T^0(G,L^\times)| = |H^2(L/K)| = n$.
For a general G, we proceed by induction. Since K is a local field, $\mathrm{Gal}(L/K)$ is soluble. If L/K is not cyclic, there exists a tower of Galois extensions $L \supsetneq K' \supsetneq K$. By lemma 3.2, we have an exact sequence

$$0 \to H^2(K'/K) \to H^2(L/K) \to H^2(L/K')$$

Hence $|H^2(L/K)| \leq |H^2(K'/K)||H^2(L/K')| = [K' : K][L : K'] = n$ by induction. By lemma 3.17, $H^2(L/K)$ has a subgroup of order n. Hence equality holds. □

Remark 3.21 *In particular, the subgroup of order n of $H^2(L/K)$obtained in lemma 3.17 is in fact the whole group. So, $H^2(L/K) \subseteq H^2(K^{\mathrm{un}}/K)$ as we claimed earlier. We can now extend inv_K as follows.*

Theorem 3.22 *There exists a canonical isomorphism $\mathrm{inv}_K : H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}$.*

Proof If L/K is a finite extension, the subgroup $H^2(L/K)$ of $H^2(K^{\mathrm{al}}/K)$ is contained in $H^2(K^{\mathrm{un}}/K)$ by remark 3.21. But $H^2(K^{\mathrm{al}}/K) = \cup H^2(L/K)$ where L runs through all finite extensions of K, so the inflation map $H^2(K^{\mathrm{un}}/K) \to H^2(K^{\mathrm{al}}/K)$ is an isomorphism. Hence the invariant map extends as required. $\square$

Remark 3.23 *By the diagrams in lemma 3.17 and lemma 3.16, if $[L : K] = n$, the following diagram commutes.*

$$\begin{tikzcd}
0 \arrow[r] & H^2(L/K) \arrow[r] \arrow[d, "\mathrm{inv}_{L/K}"] & H^2(K^{\mathrm{al}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(K^{\mathrm{al}}/L) \arrow[d, "\mathrm{inv}_L"] \\
0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "n"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

3.4 Reciprocity Law

We have seen that if L/K is a Galois extension of degree n, $H^2(L/K)$ is cyclic of order n. It is identified with $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ inside $\mathbb{Q}/\mathbb{Z}$ via $\mathrm{inv}_{L/K}$. We will look into how the generators for a tower of extensions are related to each other.

Definition 3.24 *With the notations above, we write $u_{L/K}$ for the element in $H^2(L/K)$ corresponding to $\frac{1}{n}\mathrm{mod}\ \mathbb{Z}$. This element is called the* ***fundamental class*** *of the extension L/K.*

Lemma 3.25 *Let $E \supseteq L \supseteq K$ be a tower of finite Galois extensions. Then $\mathrm{Res}(u_{E/K}) = u_{E/L}$ and $\mathrm{Inf}(u_{L/K}) = [E : L]u_{E/K}$.*

Proof Recall we have an exact sequence

$$0 \to H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(E/K) \xrightarrow{\mathrm{Res}} H^2(E/L)$$

from lemma 3.2. If we combine this with the commutative diagram in the proof of lemma 3.14 and the second square in the diagram of remark 3.23, we have the following commutes.

$$\begin{tikzcd}
0 \arrow[r] & H^2(L/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_{L/K}"] & H^2(E/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_{E/K}"] & H^2(E/L) \arrow[d, "\mathrm{inv}_{E/L}"] \\
0 \arrow[r] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, "\mathrm{id}"] & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \frac{1}{[E:L]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

But $[L:K] \cdot \dfrac{1}{[E:K]} = \dfrac{1}{[E:L]}$ and $\dfrac{1}{[L:K]} = [E:L] \cdot \dfrac{1}{[E:K]}$ by the tower law, so $\mathrm{Res}(u_{E/K}) = u_{E/L}$ and $\mathrm{Inf}(u_{L/K}) = [E:L]u_{E/K}$. □

In lemma 3.11, we described the cohomology of $L^\times$ by that of $\mathbb{Z}$ if L/K is an unramified extension. In fact, the same can be done for a general finite Galois extension as shown below.

Lemma 3.26 *Let L/K be a finite Galois extension with Galois group G. For all r there exists a canonical isomorphism $H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G,L^\times)$.*

Proof If H is a subgroup of G, then $H^1(H,L^\times) = 0$ by theorem 3.1. The isomorphism $\mathrm{inv}_{L/K}$ shows that $H^2(L/L^H) = H^2(H,L^\times)$ is cyclic of order $|H|$. Hence, by theorem 2.59, for all r, there is a canonical isomorphism $H_T^r(G,\mathbb{Z})$ to $H_T^{r+2}(G,L^\times)$.

Corollary 3.27 *There is a canonical isomorphism $G^{\mathrm{ab}} \to K^\times/N_{L/K}(L^\times)$.*

Proof Take $r = -2$ above. By corollary 2.48, there is a canonical isomorphism from $H_T^{-2}(G,\mathbb{Z})$ to G^{ab}. By definition, $H_T^0(G,L^\times) = K^\times/N_{L/K}(L^\times)$. Hence the result. □

In particular, if G itself is abelian, G^{ab} is just G. The map above gives the isomorphism stated in theorem 1.1(b).

Definition 3.28 *For a finite abelian extension L/K, define the* ***local Artin map*** *$\varphi_{L/K} : K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$ to be the inverse of the isomorphism in corollary 3.27.*

Proposition 3.29 *If $E \supseteq L \supseteq K$ is a tower of finite abelian extensions of K, then $\varphi_{E/K}(a)|_L = \varphi_{L/K}(a)$ for all $a \in K^\times$.*

Proof This can be checked directly from the definition of the local Artin maps. Note that the map $\varphi_{E/K}(\cdot)|_L$ corresponds to inflation from $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)$ to $\mathrm{Gal}(E/K)$ in cohomology. The Galois group is just H^{-2} which is isomorphic to H^2, a cyclic group as in definition 3.24. We have $\mathrm{Inf}(u_{L/K}) = [E:L]u_{E/K}$ by lemma 3.25, so $\varphi_{E/K}(\cdot)|_L$ identifies $\mathrm{Gal}(E/K)$ inside $\mathrm{Gal}(L/K)$ as required. □

This enables us to give the following definition.

Definition 3.30 *Define $\varphi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ to be the homomorphism s.t. for every finite abelian extension L/K, $\varphi_K(a)|_L = \varphi_{L/K}(a)$ for all $a \in K^\times$.*

When L/K is unramified, $\varphi_{L/K}$ maps every uniformiser of K to $\mathrm{Frob}_{L/K}$ by the definition of the invariant map. So, this together with corollary 3.27 proves the existence of theorem 1.1.

4 The Local Artin Map

In this section, we will define formal group laws and use them to construct the local Artin map in a different way. This will enable us to prove theorem 1.2 and the uniqueness in theorem 1.1.

4.1 Power Series

Let R be a commutative ring with 1. Given two power series $f, g \in R[[T]]$, $f \circ g(T)$ is in general not defined because we might not have convergence when adding infinitely many elements. However, if the constant term of g is 0, we don't have this problem anymore and $f \circ g(T)$ is well-defined.

Lemma 4.1 *For all $f \in R[[T]]$ and $g, h \in TR[[T]]$, $f \circ (g \circ h) = (f \circ g) \circ h$.*

Proof It is clear that $(f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)$ for any $f_1, f_2 \in R[[T]]$. So $g^n \circ h = (g \circ h)^n$ for any n. Therefore, the statement is true for $f = T^n$. By linearity, it is true in general. □

Lemma 4.2 *If $f = \sum_{i \geq 1} a_i T^i$, then there exists $g \in TR[[T]]$ s.t. $f \circ g = T$ iff a_1 is a unit. In this case, g is unique and $g \circ f = T$.*

Proof If $g = \sum_{i \geq 1} b_i T^i$, then the coefficients of $f \circ g$ are given by $a_1 b_1$, $a_1 b_2 + a_2 b_1$, etc, the n^{th} one is given by $a_1 b_n + (\text{poly in } a_2, \ldots, a_n, b_1 \ldots, b_{n-1})$. Hence there is a g with $f \circ g(T) = T$ iff a_1 is a unit. If this is the case, all the b_i's are uniquely determined recursively. In particular, $a_1 b_1 = 1$ and b_1 is a unit. So, there exists h s.t. $g \circ h(T) = T$. But then

$$f(T) = f \circ T = f \circ (g \circ h(T)) = (f \circ g)(h(T)) = h(T)$$

Hence, $g \circ f(T) = T$. □

In general, if $f \in R[[X_1, \ldots, X_n]]$ and $g_1, \ldots g_n \in R[[Y_1, \ldots, Y_m]]$, then, as in the one-dimensional case, $f(g_1, \ldots, g_n)$ is well-defined if the constant terms of all the g_i's are zero. We would like to define abelian groups with operations given by substitutions into symmetric power series in two variables. Explicitly, we have the following.

Definition 4.3 *Let R be a ring, a **formal group law** is a power series $F \in R[[X, Y]]$ s.t.*

(a) $F(X, Y) = X + Y +$terms of degree ≥ 2;

(b) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

(c) $F(X, Y) = F(Y, X)$.

Lemma 4.4 *If F is a foraml group law, then it's of the form $F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j$.*

Proof Take $Y = 0$ in (a), write $f(X) = F(X, 0) = X + \deg \geq 2$. $f(0) = F(0, 0) = 0$. Put $Y = Z = 0$ in (b), we have $F(X, F(0, 0)) = F(F(X, 0), 0)$ or $f = F(X, 0) = F(f, 0) = f \circ f$. By lemma 4.2, there is a g s.t. $f \circ g(X) = X$. Therefore, $f \circ f \circ g = f \circ g$ and hence $f(X) = X$. $F(X, 0) = X$ and $F(0, Y) = Y$ similarly. Therefore, F is of the form claimed. □

Given the conditions we have so far, we can construct an inverse series as shown below.

Lemma 4.5 *If F is a formal group law, then there exists a unique $i_F(X) \in XR[[X]]$ s.t. $F(X, i_F(X)) = 0$.*

Proof By lemma 4.4, we have $F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j$. Set $i_F(X) = -X + \sum_{k \geq 2} b_k X^k$, then $F(X, i_F(X)) = \sum_{k \geq 2} b_k X^k + \sum_{i,j \geq 1} a_{ij} X^i (-X + \sum_{k \geq 2} b_k X^k)^j$. The cofficient of X^k is $b_k +$ (poly in $a_{ij}, b_2, \ldots, b_{k-1}$). So we can solve for b_k uniquely and get $F(X, i_F(X)) = 0$. □

Let K be a local field. Take $R = \mathcal{O}_K$. If $F(X, Y) = \sum a_{ij} X^i Y^j \in \mathcal{O}_K[[X, Y]]$, then $a_{ij} x^i y^j \to 0$ as $i, j \to \infty$ for any $x, y \in \mathfrak{M}_K$. So, $F(x, y)$ converges by completeness. Therefore, if we define $x +_F y = F(x, y)$, $(\mathfrak{M}_K, +_F)$ is an abelian group (by axiom (b), (c) and lemma 4.5). Also, F turns $XR[[X]]$ into an abelian group by setting $f +_F g = F(f, g)$. Roughly speaking, a formal group law defines a group by substitutions.

Definition 4.6 *Let F and G be two formal group laws, a **homomorphism** from F to G is a power series $h \in TR[[T]]$ s.t. $h(F(X, Y)) = G(h(X), H(Y))$. If in addition, there exists a homomorphism $h' : G \to F$ s.t. $h \circ h'(T) = h' \circ h(T) = T$, we say h is an **isomorphism**. A homomorphism $h : F \to F$ is called an **endomorphism**.*

Note that the above definitions agree with the ordinary notions of morphisms when the formal group laws actually define groups concretely by substitutions. In fact, such homomorphisms form a group also.

Lemma 4.7 *Let F and G be formal group laws. Hom(F, G) is an abelian group with addition $f +_G g$. Moreover, End(F) is a ring with multiplication $f \circ g$.*

Proof Let $f, g \in$Hom(F, G) and $h = f +_G g$.

$$\begin{aligned}
h(F(X, Y)) &= (f +_G g)(F(X, Y)) \\
&= G(f(F(X, Y)), g(F(X, Y))) \text{ (definition of } +_G) \\
&= G(G(f(X), f(Y)), G(g(X), g(Y))) \text{ } (f,\ g \text{ are homomorphisms)} \\
&= (f(X) +_G f(Y)) +_G (g(X) +_G g(Y)) \text{ (definition of } +_G) \\
&= (f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) \text{ } (+_G \text{ abelian, associative)} \\
&= h(X) +_G h(Y) \text{ (definition of } h) \\
&= G(h(X), h(Y)) \text{ (definition of } +_G)
\end{aligned}$$

Hence, $h \in \mathrm{Hom}(F, G)$. Similarly, one can show that $i_G \circ f \in \mathrm{Hom}(F, G)$, which is the inverse of f. So we have the first part of the lemma.
To show the second part, we need to show that the distributitive law holds. Let $f, g, h \in \mathrm{End}(F)$.

$$\begin{aligned} f \circ (g +_F h)(X) &= f(F(g(X), h(X))) \text{ (definition of } +_F) \\ &= F(f(g(X)), f(h(X))) \text{ (} f \text{ is an endomorphism)} \\ &= F(f \circ g(X), f \circ h(X)) \\ &= (f \circ g +_F f \circ h)(X) \text{ (definition of } +_F) \end{aligned}$$

Hence the distributivity. Finally, X is the identity. □

4.2 Lubin-Tate Group Laws

We now fix a uniformiser π of K and let $q = |k_K|$. We will define a formal group law using π. This will eventually enable us to give the alternative definition of the local Artin map we mentioned earlier.

Definition 4.8 *$\mathcal{F}_\pi$ is defined to be the set $\{f \in \mathcal{O}_K[[X]] \mid f(X) = \pi X + \deg \geq 2,\ f(X) \equiv X^q \mathrm{mod}\ \pi\}$.*

Lemma 4.9 *Let $f, g \in \mathcal{F}_\pi$ and $\phi_1(X_1, \ldots, X_n)$ a linear form with coefficients in $\mathcal{O}_K$. Then there is a unique $\phi \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ s.t.*

(a) $\phi = \phi_1 + \deg \geq 2$;

(b) $f(\phi(X_1, \ldots, X_n)) = \phi(g(X_1), \ldots, g(X_n))$.

Proof We will show by induction that for any $r \geq 1$, there is a unique polynomial $\phi_r(X_1, \ldots, X_n)$ of degree at most r s.t.

(a) $\phi_r = \phi_1 + \deg \geq 2$;

(b) $f(\phi_r(X_1, \ldots, X_n)) = \phi_r(g(X_1), \ldots, g(X_n)) + \deg \geq r + 1$.

For $r = 1$, it is clear that ϕ_1 satisfies these conditions since f and g agree on the linear terms.
Suppose we have defined ϕ_r. By the unqiueness of ϕ_r, ϕ_{r+1} must be of the form $\phi_r + Q$ where Q is homogeneous of degree $r + 1$. Now, we only need to consider condition (b) for $r + 1$. LHS is given by

$$f(\phi_{r+1}(X_1, \ldots, X_n)) = f(\phi_r(X_1, \ldots, X_n)) + \pi Q(X_1, \ldots, X_n) + \deg \geq r + 2$$

Similarly, the RHS of condition (b) is given by

$$\phi_r(g(X_1), \ldots, g(X_n)) + Q(\pi X_1, \ldots, \pi X_n) + \deg \geq r + 2$$

Q is homogeneous of degree $r+1$, hence $Q(\pi X_1, \ldots, \pi X_n) = \pi^{r+1} Q(X_1, \ldots, X_n)$. So in order for (b) to hold, it is necessary that

$$\frac{f(\phi_r(X_1, \ldots, X_n)) - \phi_r(g(X_1), \ldots, g(X_n))}{\pi^{r+1} - \pi} = Q + \deg \geq r + 2$$

Hence Q is uniquely determined. However, we have to make sure Q has coefficients in $\mathcal{O}_K$. First note that $\pi^r - 1 \in U_K$, so we only need to show the numerator above is divisble by π. By the definition of $\mathcal{F}_\pi$, we have on one hand,

$$f(\phi_r(X_1, \ldots, X_n)) \equiv \phi_r(X_1 \ldots, X_n)^q \mathrm{mod}\pi$$

On the other hand, we have

$$\begin{aligned}\phi_r(g(X_1), \ldots, g(X_n)) &\equiv \phi_r(X_1^q, \ldots, X_n^q)\mathrm{mod}\pi \\ &\equiv \phi_r(X_1 \ldots, X_n)^q \mathrm{mod}\pi \text{ } (k_K \text{ is a finite field of order } q)\end{aligned}$$

Hence, Q is indeed defined over $\mathcal{O}_K$. To finish the proof, we take ϕ to be the power series given uniquely by $\phi = \phi_r + \deg \geq (r+1)$. ϕ clearly satisfies the conditions of the lemma and ϕ is unique because the ϕ_r's are. □

We will see throughout this section that the uniqueness above is a very useful tool to prove two power series to be equal.

Proposition 4.10 *For any $f \in \mathcal{F}_\pi$, there is a unique formal group law $F_f \in \mathcal{O}_K[[X,Y]]$ s.t. $f \in \mathrm{End}F_f$.*

Proof By taking $f = g$ in lemma 4.9, there is a unique power series F_f s.t.

(a) $F_f(X,Y) = X + Y + \deg \geq 2$;

(b) $f(F_f(X,Y)) = F_f(f(X), f(Y))$.

So we only need to check this F_f is a formal group law.
Let $G(X,Y) = F_f(Y,X)$, then $G(X,Y) = X+Y+\deg \geq 2$. On the other hand, $f(G(X,Y)) = f(F_f(Y,X)) = F_f(f(Y), f(X))$ by (b). But $G(f(X), f(Y)) = F_f(f(Y), f(X))$ by the definition of G. So, $f(G(X,Y)) = G(f(X), f(Y))$. By the uniqueness of F_f, we have $G = F_f$, ie $F_f(X,Y) = F_f(Y,X)$.
Let $G_1(X,Y,Z) = F_f(X, F_f(Y,Z))$ and $G_2(X,Y,Z) = F_f(F_f(X,Y),Z)$. Again, we can use the uniqueness of lemma 4.9 to show that $G_1 = G_2$. Hence F_f satisfies the conditions in definition 4.3. □

Definition 4.11 *A power series is called a* ***Lubin-Tate formal group law*** *if it's of the form F_f for some $f \in \mathcal{F}_\pi$ where π is a uniformiser of K.*

In fact, there is only one Lubin-Tate formal group law up to isomorphism. Given $f, g \in \mathcal{F}_\pi$, we can construct an isomorphism using the following two results.

Proposition 4.12 *For $f, g \in \mathcal{F}_\pi$ and $x \in \mathcal{O}_K$, let $[x]_{f,g}$ be the unique element of $\mathcal{O}_K[[T]]$ given by lemma 4.9 s.t.*

(a) $[x]_{f,g}(T) = xT + \deg \geq 2$;

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

Then $[x]_{f,g}$ is a homomorphism from F_g to F_f.

Proof If we write $h = [x]_{f,g}$, we need to show $h(F_g(X,Y)) = F_f(h(X), h(Y))$. We will again use the uniqueness of lemma 4.9. It's clear that both sides equal $xX + xY + \deg \geq 2$, so condition (a) in the lemma is satisfied.

$$\begin{aligned} f(h(F_g(X,Y)) &= f \circ h(F_g(X,Y)) \\ &= h \circ g(F_g(X,Y)) \text{ (by the definition of } h = [x]_{f,g}) \\ &= h(g(F_g(X,Y))) \\ &= h(F_g(g(X), g(Y))) \text{ (by the definition of } F_g) \end{aligned}$$

Hence, this gives the condition (b) for $h(F_g(X,Y))$. Similarly, we have

$$\begin{aligned} f(F_f(h(X), h(Y))) &= F_f(f(h(X)), f(h(Y))) \text{ (definition of } F_f) \\ &= F_f(f \circ h(X), f \circ h(Y)) \\ &= F_f(h \circ g(X), h \circ g(Y)) \text{ (definition of } h = [x]_{f,g}) \\ &= F_f(h(g(X)), h(g(Y))) \end{aligned}$$

Hence condition (b) for $F_f(h(X), H(Y))$. □

Proposition 4.13 *For any $x, y \in \mathcal{O}_K$, $f, g, h \in \mathcal{F}_\pi$, we have $[x+y]_{f,g} = [x]_{f,g} +_{F_f} [y]_{f,g}$ and $[xy]_{f,h} = [x]_{f,g} \circ [y]_{g,h}$.*

Proof In each case, the power series on the right satisfies the conditions characterising the power series on the left. □

Corollary 4.14 *For $f, g \in \mathcal{F}_\pi$, we have $\mathcal{F}_f \cong \mathcal{F}_g$.*

Proof If we take $x = 1$ in proposition 4.12, by proposition 4.13, we have $[1]_{f,g} \circ [1]_{g,f} = [1]_{f,f}$. In fact, $[1]_{f,f}(T) = T$ by the uniqueness in proposition 4.12. Similarly, $[1]_{g,f} \circ [1]_{f,g}(T) = [1]_{g,g}(T) = T$. Hence $[1]_{f,g}$ and $[1]_{g,f}$ are isomorphisms. □

As claimed above, a uniformiser π of K determines a unique Lubin-Tate formal group law up to isomorphism. In fact, $\mathcal{O}_K$ acts on such a group law by the following.

Corollary 4.15 *Fix $x \in \mathcal{O}_K$ and F_f a Lubin-Tate group law, there is a unique endomorphism $[x]_f : F_f \to F_f$ s.t. $[x]_f(T) = xT + \deg \geq 2$ and $[x]_f$ commutes with f. The map $x \mapsto [x]_f$ gives a ring homomorphism from $\mathcal{O}_K$ to $\mathrm{End}(F_f)$.*

Proof Take $g = f$ in proposition 4.12, then $[x]_f := [x]_{f,f}$ has the properties claimed. This gives a ring homomorphism by proposition 4.13 and $[1]_f$ acts as the identity. □

4.3 Construction of K_π

As we have seen before, K^{un} is fairly easy to understand via extensions of the residue field. In order to study K^{ab}, we will have to consider ramified extensions also. To do this, we will construct a totally ramified extension K_π (π a fixed uniformiser of K) using Lubin-Tate group laws. It turns out that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$, so we only need to understand the structure of K_π in order to understand that of K^{ab}.

The valuation $|\cdot|$ of K extends uniquely to any finite extenstion L of K, hence it extends uniquely to K^{al}. We write $\mathcal{O}_K^{\mathrm{al}}$ for the set $\{x \in K^{\mathrm{al}} |\ |x| \le 1\}$ and $\mathfrak{M}_K^{\mathrm{al}}$ for the set $\{x \in K^{\mathrm{al}} |\ |x| < 1\}$. Fix a uniformiser π of K. For any $f \in \mathcal{F}_\pi$, we have an $\mathcal{O}_K$-module structure on $\mathfrak{M}_K^{\mathrm{al}}$ with addition $+_{F_f}$ and $x \cdot \alpha = [x]_f(\alpha)$. We denote this module by Λ_f and define Λ_n to be the submodule killed by $[\pi]_f^n$. It's not hard to see that on taking $f = g$ and $x = \pi$ in proposition 4.12, f satisfies conditions (a) and (b), so $[\pi]_f = f$ by uniqueness. Hence Λ_n consists of the roots of $f^{(n)} = \underbrace{f \circ \cdots \circ f}_{n}$. K_π is defined to be $\cup_n K(\Lambda_n)$. We will now derive some properties of K_π.

Lemma 4.16 *Let M be an $\mathcal{O}_K$-module, and let $M_n = \ker(\pi^n : M \to M)$. Assume M_1 has $q = |k_K|$ elements and $\pi : M \to M$ is surjective. Then $M_n \cong \mathcal{O}_K/(\pi^n)$.*

Proof We proceed by induction on n. The assumption on M_1 implies the result for $n = 1$ by the isomorphism theorem.
Note that $M_1 \subseteq M_n$ so we have an inclusion $M_1 \hookrightarrow M_n$. If $\alpha \in M_{n-1}$, then $\pi^{n-1} \cdot \alpha = 0$. By the surjectivity of π, there exists β s.t. $\pi \cdot \beta = \alpha$. Hence $\pi^n \cdot \beta = 0$, ie $\beta \in M_n$. Hence $\pi : M_n \to M_{n-1}$ is surjective. Therefore, the sequence $0 \to M_1 \to M_n \xrightarrow{\pi} M_{n-1} \to 0$ is exact.
By induction, $M_{n-1} \cong \mathcal{O}_K/(\pi^{n-1})$, hence it has q^{n-1} elements. By the exact sequence above, $M_n/M_1 \cong M_{n-1}$ and M_n has q^n elements. Since $\mathcal{O}_K$ is a principal ideal domain with only one prime ideal, every finitely generated torsion $\mathcal{O}_K$-module is of the form $\mathcal{O}_K/(\pi^{n_1}) \oplus \cdots \oplus \mathcal{O}_K/(\pi^{n_r})$. Since each summand of M_n contains a non-trivial element of M_1, in order for M_1 to be cyclic, M_n must be cyclic itself. So $M_n \cong \mathcal{O}_K/(\pi^n)$. $\square$

Recall from local fields, we have the following.

Theorem 4.17 *If $f \in \mathcal{O}_K[X]$ is an Eisenstein polynomial, then $L = K[X]/(f)$ is totally ramified over K, and the root of f in L is a uniformiser of L.*

We can now derive the structures of Λ_n.

Proposition 4.18 *$\Lambda_n \cong \mathcal{O}_K/(\pi^n)$, hence we have* $\mathrm{End}_{\mathcal{O}_K}(\Lambda_n) = \mathcal{O}_K/(\pi^n)$ *and* $\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) = (\mathcal{O}_K/(\pi^n))^\times$.

Proof We will show Λ_n satisfies the condition of lemma 4.16. Note that any two F_f and F_g are isomorphic by corollary 4.14, wlog, we may take $f(X) = \pi X + X^q$. $f(X)/X$ is an Eisenstein polynomial of degree $q-1$, so $f(X)/X$ is separable by theorem 4.17. Hence, $f(X)/X$ has $q-1$ distinct non-zero roots in $\mathfrak{M}_K^{\mathrm{al}}$ and f itself has q distinct roots in $\mathfrak{M}_K^{\mathrm{al}}$, ie $|\Lambda_1| = q$.

It remains to show that the multiplication by π is surjective. Note that for any $\alpha \in \mathfrak{M}_K^{\mathrm{al}}$, there exists $\beta \in K^{\mathrm{al}}$ s.t. $[\pi]_f(\beta) = f(\beta) = \alpha$.
Claim $\beta \in \mathfrak{M}_K^{\mathrm{al}}$
Proof of claim $1 > |\alpha| = |\beta^q + \pi\beta|$. If $|\beta^q| = |\pi\beta|$, then $|\beta|^{q-1} < 1$, so $|\beta| < 1$. Otherwise, $|\beta^q + \pi\beta| = \max(|\beta^q|, |\pi\beta|) < 1$, so $|\beta| < 1$. Either way, $|\beta| < 1$, hence the claim. $\square$

We will need the following general result to derive further properties of $K(\Lambda_n)$ we want.

Lemma 4.19 *Let L/K be a finite Galois extension, with $G = \mathrm{Gal}(L/K)$. For any $F \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ and $\alpha_1 \ldots, \alpha_n \in \mathfrak{M}_L$, we have $F(\sigma\alpha_1, \ldots, \sigma\alpha_n) = \sigma F(\alpha_1, \ldots, \alpha_n)$ for all $\sigma \in G$.*

Proof Since $|\alpha_i| < 1$, $F(\alpha_1, \ldots, \alpha_n)$ converges as L is complete. Note that σ perserves norm, so $F(\sigma\alpha_1, \ldots, \sigma\alpha_n)$ converges in L also. The lemma is trivial when F is a polynomial. But σ is continuous since it preserves norm. Hence the lemma is true by taking limit. $\square$

Theorem 4.20 *Let $K_{\pi,n} = K(\Lambda_n)$, we have the following.*

(a) $K_{\pi,n}/K$ is totally ramified of degree $(q-1)q^{n-1}$.

(b) The action of $\mathcal{O}_K$ on Λ_n defines an isomorphism from $\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) = (\mathcal{O}_K/\mathfrak{M}^n)^\times$ to $\mathrm{Gal}(K_{\pi,n}/K)$.

Proof We may let $f(X) = \pi X + X^q$ as above. Since Λ_n is set of roots of $f^{(n)}$, $K(\Lambda_n)$ is the splitting field of $f^{(n)}$ over K. Note that $[\pi]_f^r \cdot \alpha = 0$ where $r \leq n$ implies $[\pi]_f^n \cdot \alpha = 0$, so we have inclusions $\Lambda_n \supseteq \Lambda_{n-1} \supseteq \cdots \supseteq \Lambda_1$.
As stated above, $f(X)/X$ is an Eisenstein polynomial over K. So, if α_1 is a root of $f(X)/X$, then $K(\alpha_1)/K$ is a totally ramified extension of degree $q-1$ with uniformiser α_1 by theorem 4.17. Now, $f(X) - \alpha_1$ is an Eisenstein polynomial over $K(\alpha_1)$, so $K(\alpha_1, \alpha_2)/K(\alpha_1)$ is a totally ramified extension of degree q with uniformiser α_2. Continue similarly, we have $K(\Lambda_n) \supseteq K' \supseteq K$ where $K' = K(\alpha_1, \ldots, \alpha_n)$ is a totally ramified extension of degree $(q-1)q^{n-1}$ over K and $f(\alpha_i) = \alpha_{i-1}$ for $i = 2, \ldots, n$. In particular, $[K(\Lambda_n) : K] \geq [K' : K] = (q-1)q^{n-1}$.
On the other hand, $\mathrm{Gal}(K(\Lambda_n)/K)$ can be identified as a subset of $\mathrm{Sym}(\Lambda_n)$. Under this identification, an element in the Galois group will correspond to an element of $\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n)$ in $\mathrm{Sym}(\Lambda_n)$ by lemma 4.19. But $\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) \cong (\mathcal{O}_K/(\pi^n))^\times$ by proposition 4.18. Hence $|\mathrm{Gal}(K(\Lambda_n)/K)| \leq |(\mathcal{O}_K/(\pi^n))^\times| = (q-1)q^{n-1}$.
Therefore, we must have equality since $|\mathrm{Gal}(K(\Lambda_n)/K)| = [K(\Lambda_n) : K]$. So, (a) is true. We have equality throughout, hence the isomorphism in (b). $\square$

Corollary 4.21 *With the notations above, $\pi \in N_{K(\Lambda_n)/K}(K(\Lambda_n)^\times)$.*

Proof Let $g(X) = f(X)/X$ and $f^{[n]} = g \circ \underbrace{f \circ \cdots \circ f}_{n-1} = \pi + \cdots + X^{(q-1)q^{n-1}}$.
With the notations in the proof above, we have $f^{[n]}(\alpha_n) = f^{[n-1]}(\alpha_{n-1}) = \cdots =$

$f^{[1]}(\alpha_1) = 0$. $K' = K(\alpha_n)$ as K'/K is totally ramified and α_n is a uniformiser of K'. So, $[K(\alpha_n) : K] = (q-1)q^{n-1}$ and $f^{[n]}$ is the minimal polynomial of α_n over K, hence $N_{K(\Lambda_n)/K}(\alpha_n) = (-1)^{(q-1)q^{n-1}}\pi$. This is just π unless $q = 2$ and $n = 1$. The case $n = 1$ is trivial. Hence the claim. □

Corollary 4.22 *The action of $\mathcal{O}_K$ on Λ_n induces an isomorphism from $\mathcal{O}_K^\times$ to* $\mathrm{Gal}(K_\pi/K)$.

Proof By theorem 4.20, the action induces an isomorphism from $(\mathcal{O}_K/(\pi^n))^\times$ to $\mathrm{Gal}(K(\Lambda_n)/K)$. But $K_\pi = \cup_n K(\Lambda_n)$, so $\mathrm{Gal}(K_\pi/K) = \varprojlim \mathrm{Gal}(K(\Lambda_n)/K)$. On the other hand, $\mathcal{O}_K = \varprojlim \mathcal{O}_K/(\pi^n)$ and $\mathcal{O}_K^\times = \varprojlim (\mathcal{O}_K/(\pi^n))^\times$, hence the result. □

Example 4.23 *If $K = \mathbb{Q}_p$ with $\pi = p$, then we have $f(X) = (X+1)^p - 1 \in \mathcal{F}_p$. $f^{(n)}(X) = (X+1)^{p^n} - 1$, so K_π in this case is just $\mathbb{Q}_p(\mu_{p^\infty}) = \cup_n \mathbb{Q}_p(\mu_{p^n})$.*

4.4 Construction of ϕ_π

For a uniformiser π of K, we want to define a map $\phi_\pi : K^\times \to \mathrm{Gal}(K_\pi \cdot K^{\mathrm{un}}/K)$ to establish our alternative definition of the local Artin map. Since $K_\pi \cap K^{\mathrm{un}} = K$, for $a \in K^\times$, it suffices to describe the actions of $\phi_\pi(a)$ on K_π and K^{un} separately. If $a = \pi^n u$ where $n \in \mathbb{Z}$ and u is a unit, we let $\phi_\pi(a)$ act on K^{un} as Frob_K^n and it acts on K_π with $\phi_\pi(a)(\alpha) = [u^{-1}]_f(\alpha)$. We will show that $K_\pi \cdot K^{\mathrm{un}} = K^{\mathrm{ab}}$ and this definition of ϕ_π is independent of the choice of π. To do this, we will relate $\mathcal{F}_\pi$ and $\mathcal{F}_{\pi'}$ for two uniformisers π and π' of K via the completion of K^{un}.

We write $\hat{K}^{\mathrm{un}}$ for the completion of K^{un}. $|\cdot|$ extends to $\hat{K}^{\mathrm{un}}$ and we write $\mathfrak{O}$ for its ring of integers. Note that Frob_K extends to $\hat{K}^{\mathrm{un}}$, denoted by σ.

Lemma 4.24 *Define a homomorphism from $\mathfrak{O}$ to itself by $x \mapsto \sigma x - x$. This is surjective with kernel $\mathcal{O}_K$. Similarly, the homomorphism from $\mathfrak{O}^\times$ with $x \mapsto \sigma x/x$ is surjective with kernel $\mathcal{O}_K^\times$.*

Proof Let R be the ring of integers in K^{un} with maximal ideal $\mathfrak{n}$. Then $\varprojlim R/\mathfrak{n}^n = \mathfrak{O}$. The residue field $R/\mathfrak{n} \cong \bar{k}_K$.

<u>Claim</u> $0 \to \mathcal{O}_K/\mathfrak{M}_K^n \to R/\mathfrak{n}^n \xrightarrow{\sigma-1} R/\mathfrak{n}^n \to 0$ is exact.
<u>Proof of claim</u> We proceed by induction on n. For $n = 1$, it's clear since $(\sigma - 1)(x) = x^q - x$ and this charactrises k_K in $\bar{k}_K$. So assume the sequence is exact for $n-1$. Consider the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & R/\mathfrak{n} \arrow[r] \arrow[d, "\sigma-1"] & R/\mathfrak{n}^n \arrow[r] \arrow[d, "\sigma-1"] & R/\mathfrak{n}^{n-1} \arrow[r] \arrow[d, "\sigma-1"] & 0 \\
0 \arrow[r] & R/\mathfrak{n} \arrow[r] & R/\mathfrak{n}^n \arrow[r] & R/\mathfrak{n}^{n-1} \arrow[r] & 0
\end{tikzcd}$$

where the first and third vertical maps are surjective with kernels $\mathcal{O}_K/\mathfrak{M}_K$ and $\mathcal{O}_K/\mathfrak{M}_K^{n-1}$ respectively. By the snake lemma, we have an exact sequence

$$0 \to \mathcal{O}_K/\mathfrak{M}_K \to \ker(\gamma_n) \to \mathcal{O}_K/\mathfrak{M}_K^{n-1} \to 0 \to \mathrm{coker}(\gamma_n) \to 0$$

where γ_n denotes the map $\sigma - 1 : R/\mathfrak{n}^n \to R/\mathfrak{n}^n$. So γ_n is surjective and the kernel has q^n elements. But $\mathcal{O}_K/\mathfrak{M}_K^n$ lies inside the kernel and $|\mathcal{O}_K/\mathfrak{M}_K^n| = q^n$, so in fact $\ker(\gamma_n) = \mathcal{O}_K/\mathfrak{M}_K^n$. Hence we have the exactness for $R/\mathfrak{n}^n$. This proves the claim.
We obtain the result for $\sigma - 1$ by taking inverse limit. The proof for the second half of the lemma is similar. □

Using this lemma, we can relate elements in $\mathcal{F}_\pi$ and $\mathcal{F}_{\pi'}$ for two uniformisers π and π'. We will do it in several steps.

Proposition 4.25 *Let π and π' be uniformisers of K with $\pi' = u\pi$. If $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_{\pi'}$, then there exists $\epsilon \in \mathfrak{O}^\times$ s.t. $\sigma\epsilon = u\epsilon$ and there exists $\theta(T) \in \mathfrak{O}[[T]]$ s.t.*

(a) $\theta(T) = \epsilon T + \deg \geq 2$;

(b) $\sigma\theta = \theta \circ [u]_f$.

Proof By lemma 4.24, there exists $\epsilon \in \mathfrak{O}^\times$ s.t. $\sigma\epsilon/\epsilon = u$, ie $\sigma\epsilon = \epsilon u$. We construct a sequence of polynomials θ_r satisfying the following.

(1) If $r > 1$, then $\theta_r(T) = \theta_{r-1}(T) + bT^r$ for some $b \in \mathfrak{O}$;

(2) $\sigma\theta_r = \theta_r \circ [u]_f + \deg \geq r + 1$.

Let $\theta_1(T) = \epsilon T$. Then $\sigma\theta_1(T) = \epsilon u T = \epsilon(uT + \cdots) + \deg \geq 2$, so condition (2) is satisfied. Now, assume θ_r has been chosen. Let $\theta_{r+1}(T) = \theta_r(T) + a\epsilon^{r+1}T^{r+1}$ for some $a \in \mathfrak{O}$. Thus, condition (2) says the following.

$$\sigma\theta_r(T) + (\sigma a)(\sigma\epsilon T)^{r+1} = \theta_r \circ [u]_f(T) + a(\epsilon u T)^{r+1} + \deg \geq r + 2$$

So, for this to be true, we need $(\sigma a - a)(\epsilon u)^{r+1} = c$ where c is the coefficient of T^{r+1} in $\theta_r \circ [u]_f - \sigma\theta_r$. Such an a exists by the surjectivity of $\sigma - 1$ from lemma 4.24. Hence, we can take θ to be the power series defined by these θ_r's. □

Note that ϵ is a unit in $\mathfrak{O}$. By lemma 4.2, these exists $\theta^{-1} \in T\mathfrak{O}[[T]]$ s.t. $\theta \circ \theta^{-1}(T) = \theta^{-1} \circ \theta(T) = T$. This enable us to choose θ to be an isomorphism from F_f to F_g as shown below.

Proposition 4.26 *With the notations above, θ can be chosen so that we have the following.*

(a) $\theta(F_f(X, Y)) = F_g(\theta(X), \theta(Y))$;

(b) $\theta \circ [a]_f = [a]_g \circ \theta$.

Proof Let θ be any power series with the properties in proposition 4.25. Let $h = \sigma\theta \circ f \circ \theta^{-1}$.
Claim h has coefficients in $\mathcal{O}_K$.
Proof of claim Proposition 4.25(b) says that $\sigma\theta = \theta \circ [u]_f$, so $h = \theta \circ [u]_f \circ f \circ \theta^{-1}$. By the definition of $[u]_f$, $[u]_f$ commutes with f. Hence, $h = \theta \circ f \circ [u]_f \circ \theta^{-1}$. Note that f and $[u]_f$ have coefficients in $\mathcal{O}_K$, so they are fixed by σ. Hence $\sigma h = \sigma\theta \circ f \circ [u]_f \circ \sigma\theta^{-1}$.
On the other hand, $\theta \circ [u]_f \circ \sigma\theta^{-1}(T) = \sigma\theta \circ \sigma\theta^{-1}(T) = T$, so $\theta^{-1} = [u]_f \circ \sigma\theta^{-1}$. Substituting this into the equaion for σh, we have $\sigma h = \sigma\theta \circ f \circ \theta^{-1} = h$. Hence the claim.
Recall $\sigma\epsilon/\epsilon = u$, we have $h(T) = \sigma\epsilon \cdot \pi \cdot \epsilon^{-1} T + \cdots = u\pi T + \deg \geq 2 = \pi' T + \deg \geq 2$. Furthermore, we have

$$\begin{aligned} h(T) &= \sigma\theta \circ f \circ \theta^{-1}(T) \\ &\equiv \sigma\theta \circ (\theta^{-1})^q(T) \bmod \mathfrak{M}_K \text{ (since } f \in \mathcal{F}_\pi) \\ &\equiv \sigma\theta(\sigma\theta^{-1}(T^q)) \bmod \mathfrak{M}_K \text{ (by definition, } \sigma : x \mapsto x^q) \\ &\equiv T^q \bmod \mathfrak{M}_K \end{aligned}$$

Therefore, $h \in \mathcal{F}_{\pi'}$. We can then relate f and g as follows.
Take $\theta' = [1]_{g,h} \circ \theta$, then clearly it satisfies the conditions of the previous proposition since $[1]_{g,h}$ has coefficients in $\mathcal{O}_K$. So, we can replace θ by θ' and $\sigma\theta' \circ f \circ \theta'^{-1} = [1]_{g,h} \circ h \circ [1]_{g,h}^{-1} = g$.
$\theta'(F_f(\theta'^{-1}(X), \theta'^{-1}(Y)) = F_g(X, Y)$ since the LHS satisfies the conditions characterising F_g in proposition 4.10. Hence, on replacing (X, Y) by $(\theta'(X), \theta'(Y))$, we have (a). Similarly, we can show that $\theta' \circ [a]_f \circ \theta'^{-1}$ has the properties characterising $[a]_g$, hence (b). □

Corollary 4.27 *With the notations above, $\theta : F_f \to F_g$ is an isomorphism.*

Proof Condition (b) in proposition 4.26 says that θ is a homomorphism. As noted before, condion (a) in proposition 4.25 implies $\theta^{-1} \in \mathfrak{O}$ and so θ is an isomorphism. □

Finally, we can prove that $K_\pi \cdot K^{\mathrm{un}}$ and ϕ_π are independent of the choice of π as claimed earlier.

Theorem 4.28 *$K_\pi \cdot K^{\mathrm{un}}$ is independent of the choice of π.*

Proof We use the notations above. Recall that $[\pi]_f = f$ and $[\pi']_g = g$. We have:

$$\begin{aligned} (\sigma\theta) \circ f &= (\sigma\theta) \circ [\pi]_f \\ &= \theta \circ [u]_f \circ [\pi]_f \text{ (property (b) of proposition 4.25)} \\ &= \theta \circ [\pi']_f \text{ (proposition 4.13)} \\ &= [\pi']_g \circ \theta \text{ (property (b) of proposition 4.26)} \\ &= g \circ \theta \end{aligned}$$

Therefore, $f(\alpha) = 0$ implies $g(\theta\alpha) = 0$ and $g(\alpha) = 0$ implies $f(\theta^{-1}(\alpha)) = 0$. Recall $\Lambda_{f,1}$ and $\Lambda_{g,1}$ are the sets of zeros of f and g respectively. Hence we have:

$$\hat{K}^{\mathrm{un}}(\Lambda_{g,1}) = \hat{K}^{\mathrm{un}}(\theta(\Lambda_{f,1})) \subseteq \hat{K}^{\mathrm{un}}(\Lambda_{f,1}) = \hat{K}^{\mathrm{un}}(\theta^{-1}\Lambda_{g,1}) \subseteq \hat{K}^{\mathrm{un}}(\Lambda_{g,1})$$

So we have equality $\hat{K}^{\mathrm{un}}(\Lambda_{f,1}) = \hat{K}^{\mathrm{un}}(\Lambda_{g,1})$. By taking intersection with K^{al}, we have $K^{\mathrm{un}}(\Lambda_{f,1}) = K^{\mathrm{un}}(\Lambda_{g,1})$. Similarly, $K^{\mathrm{un}}(\Lambda_{f,n}) = K^{\mathrm{un}}(\Lambda_{g,n})$ for all n. Hence, $K^{\mathrm{un}} \cdot K_\pi = K^{\mathrm{un}} \cdot K_{\pi'}$. □

Theorem 4.29 *ϕ_π defined in the beginning of this section is indepedent of the choice of π.*

Proof Again, we use the notations as above. $\phi_\pi(\pi')$ and $\phi_{\pi'}(\pi')$ both act as Frob on K^{un}. Now consider their actions on $K_{\pi'}$.
By definition, $\phi_{\pi'}(\pi')$ acts as the identity on $K_{\pi'}$. Let θ be the isomorphism from F_f to F_g in propositions 4.25 and 4.26. We have $\phi_\pi(\pi') = \phi_\pi(u)\phi_\pi(\pi)$, $\phi_\pi(u)$ acts as the identity on K^{un} and it acts as $[u^{-1}]_f$ on K_π whereas $\phi_\pi(\pi)$ acts as Frob$= \sigma$ on K^{un} and as the identity on K_π. Therefore, if $\alpha \in K_\pi$, we have:

$$\begin{aligned}
\phi_\pi(\pi')(\theta\alpha) &= \phi_\pi(u)\phi_\pi(\pi)(\theta\alpha) \\
&= \sigma\theta(\phi_\pi(u)(\alpha)) \text{ (since } \theta \text{ has coefficients in } \hat{K}^{\mathrm{un}}) \\
&= \sigma\theta([u^{-1}]_f(\alpha)) \\
&= \theta\alpha \text{ (by property (b) of proposition 4.25)}
\end{aligned}$$

Therefore, $\phi_{\pi'}(\pi')$ and $\phi_\pi(\pi')$ agree on $K_{\pi'}$. Hence they are equal. But π' is arbitrary, so given any uniformisers π_1 and π_2, ϕ_{π_1} and ϕ_{π_2} take the same values on any uniformisers, hence they take the same values everywhere. □

4.5 Existence Theorem

Fix a uniformiser π_0 of K. Write K' for $K_{\pi_0} \cdot K^{\mathrm{un}}$, and let $\phi' = \phi_{\pi_0}$. We have seen that they are indepedent of the choice of π_0. Let $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ be the map constructed in definition 3.30. We will show that it coincides with ϕ'.

Lemma 4.30 *For all $a \in K^\times$, $\phi(a)|_{K'} = \phi'(a)$.*

Proof Let π be a uniformiser of K. By corollary 4.21, π is a norm from $K_{\pi,n}$, so by property (b) of ϕ in theorem 1.1, $\phi(\pi)$ acts trivially on $K_{\pi,n}$. By definition, $\phi'(\pi) = \phi_\pi(\pi)$ acts trivially on $K_{\pi,n}$. On the other hand, both $\phi(\pi)$ and $\phi'(\pi)$ act as Frob on K^{un}. But π is arbitrary. Hence the claim since $K' = \cup K_{\pi,n} \cdot K^{\mathrm{un}}$. □

To prove the Existence Theorem, we will need to derive some properties of the norm subgroups. First, we introduce some notations.

If we write K_m for the unramified extension K of degree m, then we have $\phi_{\pi_0}(a)|_{K_{\pi_0,n}\cdot K_m}$ =id for $a \in (1+\mathfrak{M}_K^n)\cdot <\pi_0^m>$. Let $K_{n,m} = K_{\pi_0,n}\cdot K_m$ and $U_{n,m} = (1+\mathfrak{M}_K^n)\cdot <\pi_0^m>$.

Lemma 4.31 *With the above notations, $U_{n,m} = N_{K_{n,m}/K}(K_{n,m}^\times)$.*

Proof Since $\phi_{\pi_0}(a)|_{K_{n,m}} = \mathrm{id}$ for all $a \in U_{n,m}$. We have $\phi(a)|_{K_{n,m}} = \mathrm{id}$ for all $a \in U_{n,m}$ by lemma 4.30, hence $U_{n,m} \subseteq N_{K_{n,m}/K}(K_{n,m}^\times)$ by property (b) of theorem 1.1.

$$\begin{aligned}
(K^\times : U_{n,m}) &= (U : 1+\mathfrak{M}_K^n)(<\pi_0>:<\pi_0^m>)\\
&= (q-1)q^{n-1}\cdot m\\
&= [K_{\pi_0,n}:K][K_m:K] \text{ (by theorem 4.20 and definition of } K_m)\\
&= [K_{n,m}:K] \text{ (as } K_{\pi_0,n}\cap K_m = K)\\
&= |\mathrm{Gal}(K_{n,m}/K)|\\
&= (K^\times : N_{K_{n,m}/K}(K_{n,m}^\times)) \text{ (by property (b) of theorem 1.1)}
\end{aligned}$$

Hence we have equality. □

For a general norm group, we have the following.

Lemma 4.32 *Let L be a finite Galois extension of K, and assume $N_{L/K}(L^\times)$ is of finite index in $K^\times$. Then $N_{L/K}(L^\times)$ open in $K^\times$.*

Proof U_L is compact, $N_{L/K}$ is continuous, so $N_{L/K}(U_L)$ is closed in $K^\times$. Note that the norm of a unit is a unit and that of a non-unit is a non-unit, so we have an embedding $U_K/N_{L/K}(U_L) \hookrightarrow K^\times/N_{L/K}(L^\times)$ which is finite by assumption. Hence $N_{L/K}(U_L)$ is closed of finite index in U_K, so its complement in U_K is a finite union of closed subsets. Therefore, $N_{L/K}(U_L)$ is open in U_K, hence in $K^\times$. There is an open neigbourhood of 1 inside $N_{L/K}(L^\times)$, hence it's open by translation. □

Corollary 4.33 $K^{\mathrm{ab}} = K_{\pi_0}\cdot K^{\mathrm{un}}$ *and* $\phi' = \phi$.

Proof If L/K is an abelian extension, $(K^\times : N_{L/K}(L^\times)) = [L:K]$ by property (b) of theorem 1.1. By lemma 4.32, $N_{L/K}(L^\times)$ is open in $K^\times$. So, it contains $U_{n,m}$ for some $n,m \geq 0$. For $a \in K^\times$, we have the following by theorem 1.1(b).

$$\begin{aligned}
\phi(a) \text{ fixes the elements of } L \quad &\Leftrightarrow \quad a \in N_{L/K}(L^\times)\\
\phi(a) \text{ fixes the elements of } K_{n,m} \quad &\Leftrightarrow \quad a \in N_{L/K}(K_{n,m}^\times) = U_{n,m}
\end{aligned}$$

But $N_{L/K}(L^\times) \supseteq U_{n,m}$, so $\phi(a)$ fixes $K_{n,m}$ implies $\phi(a)$ fixes L. Note that $\phi|_{L\cdot K_{n,m}} : K^\times \to \mathrm{Gal}(L\cdot K_{n,m}/K)$ is onto, hence $L \subseteq K_{n,m}$.
Therefore, for any abelian extension L of K, we have $L \subseteq K_{n,m} \subseteq K_{\pi_0}\cdot K^{\mathrm{un}} \subseteq K^{\mathrm{ab}}$. But L is arbitrary, hence we have $K^{\mathrm{ab}} = \cup L = K_{\pi_0}\cdot K^{\mathrm{un}}$. Lemma 4.30 shows that for all $a \in K^\times$, $\phi(a)$ and $\phi'(a)$ act as the same map on this field,

hence they are equal. □

Finally, we can finish off our proofs for the main theorems.

Proof of the Existence Theorem

We have to show that every open subgroup H of $K^\times$ of finite index is a norm group. As we have observed, every such group contains $U_{n,m}$ for some n and m, and $U_{n,m} = N_{K_{n,m}/K}(K_{n,m}^\times)$. Let L be the subfield of $K_{n,m}$ fixed by $\phi_{K_{n,m}/K}(H)$. Then H is the kernel of $\phi : K^\times \to \mathrm{Gal}(L/K)$, and so equals $N_{L/K}(L^\times)$ by the property (b) of theorem 1.1.

Uniqueness of ϕ

Let π be a uniformiser of K. For any n, we have $\pi \in N_{K_{\pi,n}/K}(K_{\pi,n}^\times)$ by corollary 4.21. So condition (b) implies that $\phi(\pi)$ acts as the identity on $K_{\pi,n}$. Therefore, $\phi(\pi)$ acts as the identity on K_π. $\phi(\pi)$ acts as Frob on K^{un} by condition (a). $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$, so $\phi(\pi)$ is uniquely determined. But π is arbitrary, hence the claim.

4.6 Consequences

Using the main theorems we proved, we can now translate results from Galois theory into statements on intrinsic properties of the local field.

Corollary 4.34 *The map $L \mapsto N_{L/K}(L^\times)$ is a bijection from the set of finite abelian extensions of K to the set of open subgroups of finite index in $K^\times$. Moreover, we have the following correspondence.*

$$\begin{aligned} L_1 \subseteq L_2 \quad &\Leftrightarrow \quad N_{L_1/K}(L_1^\times) \supseteq N_{L_2/K}(L_2^\times); \\ N_{L_1 \cdot L_2/K}(L_1 \cdot L_2) \quad &= \quad N_{L_1/K}(L_1) \cap N_{L_2/K}(L_2); \\ N_{L_1 \cap L_2/K}(L_1 \cap L_2) \quad &= \quad N_{L_1/K}(L_1) \cdot N_{L_2/K}(L_2). \end{aligned}$$

for any finite abelian extensions L_1 and L_2 of K.

Proof By theorem 1.2, every open subgroup of $K^\times$ of finite index is of the form $N_{L/K}(L^\times)$ where L/K is a finite abelian extension. Given a finite abelian extension L of K, $\mathrm{Gal}(L/K)$ is identified with $K^\times/N_{L/K}(L^\times)$ via ϕ_K. Moreover, if L' is an intermediate field, then L' is the fixed field of $\mathrm{Gal}(L/L')$. By theorem 1.1, we have for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \in \mathrm{Gal}(L/L')$ iff $\phi_K(\sigma)|L' = \mathrm{id}$ iff σ corresponds to an element in $N_{L'/L}(L'^\times)$. Hence, we have the inclusion reversing correspondence claimed.
The last two equalities follow immediately from the Galois correspondence. □

Recall K_m denotes the unramified extension of K of degree m. Using the local Artin map, we can describe $N_{K_m/K}(K_m^\times)$ as follows.

Lemma 4.35 $N_{K_m/K}(K_m^\times) = U_K \cdot \pi^{m\mathbb{Z}}$ *where π is a uniformiser of K and U_K is the set of units in K.*

Proof Let $u \in U_K$. Note that $\phi_K(\pi)|_{K^{\mathrm{un}}}$ is the Frobenius map. But πu is also a uniformiser of K, so $\phi_K(\pi u)|_{K^{\mathrm{un}}} = \phi_K(\pi)|_{K^{\mathrm{un}}}$. We have $\phi_K(u)|_{K^{\mathrm{un}}} = \mathrm{id}$. Hence, $\phi_{K^{\mathrm{un}}/K}(\pi^n u) = \mathrm{Frob}^n$. Therefore, $\ker(\phi_{K_m/K}) = U_K \cdot \pi^{m\mathbb{Z}}$ which equals $N_{K_m/K}(K_m^\times)$ by theorem 1.1. □

We can also say something about $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Define an alternative topology of $K^\times$ by its open subgroups of finite index. These are just subgroups of the form $N_{L/K}(L^\times)$ where L is an abelian extension of K. Then the completion of $K^\times$ wrt this topology is just $\hat{K^\times} = \varprojlim K^\times/N_{L/K}(L^\times)$. However, we have isomorphism $\phi_{L/K} : K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$. On passing to inverse limits, we have $\hat{K^\times} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Finally, we can prove the Local Kronecker-Weber Theorem using what we have got so far.

Theorem 4.36 (Local Kronecker-Weber) *Let L be a finite abelian extension of $\mathbb{Q}_p$, then L is contained in a cyclotomic extension of $\mathbb{Q}_p$.*

Proof Let $K = \mathbb{Q}_p$, then p is a uniformiser. We have $L \subseteq K^{\mathrm{ab}} = K_p \cdot K^{\mathrm{un}}$ by corollary 4.33. But $K^{\mathrm{un}} = \cup_{p \nmid n} \mathbb{Q}_p(\mu_n)$ by remark 3.13 and $K_p = \mathbb{Q}_p(\mu_{p^\infty})$ by example 4.23. Hence we are done. □

5 Global Class Field Theory

We will state without proof the main theorems in global class field theory here. Throughout this section, K denotes a number field for simplicity although some of the results we state will hold for finite extensions of $\mathbb{F}_p(T)$ also.
Given a number field K, the localisation of $\mathcal{O}_K$ at a prime ideal induces a discrete valuation on K. An embedding of K into $\mathbb{C}$ gives a non-discrete valuation of K. To simplify terminology, we have the following definition.

Definition 5.1 *A **prime** of K is an equivalence class of non-trivial valuations of K. Those identified with prime ideals of $\mathcal{O}_K$ are called **finite primes**, whereas those identified with embeddings into $\mathbb{C}$ are called **infinite primes**. We say that an infinite prime is **real** if it can be identified with an embedding into $\mathbb{R}$ and say it is **complex** if it is identified with a conjugate pair of embeddings into $\mathbb{C}$.*

The completion of K with respect to a prime v is denoted by K_v. The embedding $K \hookrightarrow K_v$ is denoted by $a \mapsto a_v$. Sometimes we write $\mathfrak{p}$ instead of v. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, $\mathbb{N}\mathfrak{a}$ denotes the numerical norm of $\mathfrak{a}$, namely $(\mathcal{O}_K : \mathfrak{a})$.

5.1 Ray Class Groups

To make sense of the statements of the main theorems in global class field theory, we need the notion of ray class groups. First, we introduce some notations. Let

I be the group of fractional ideals in K and C the ideal class group of K. For a finite set S of primes of K, I^S denotes the subgroup of I generated by the prime ideals not in S. K^S denotes the set $\{a \in K^\times | (a) \in I^S\}$, ie it's the set of elements in $K^\times$ with 0 valuation at the finite primes of S. There is a natural map $i : K^S \to I^S$ with $a \mapsto (a) = a\mathcal{O}_K$. From now on, i will always denote the map that sends a to (a).

Lemma 5.2 *With the notations above, the following sequence is exact.*

$$0 \to U_K \to K^S \to I^S \to C \to 0$$

where U_K denotes the set of units in $\mathcal{O}_K$.

Definition 5.3 *A* ***modulus*** *for K is a function $m : \{primes\ of\ K\} \to \mathbb{Z}$ s.t.*

(a) $m(\mathfrak{p}) \geq 0$ for all primes $\mathfrak{p}$, and $m(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$;

(b) if $\mathfrak{p}$ is real, then $m(\mathfrak{p}) = 0$ or 1;

(c) if $\mathfrak{p}$ is complex, then $m(\mathfrak{p}) = 0$.

We write $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$. We say a modulus $\mathfrak{m}$ ***divides*** *another modulus $\mathfrak{n}$ if $m(\mathfrak{p}) \leq n(\mathfrak{p})$ for all $\mathfrak{p}$.*

We can write $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$ where $\mathfrak{m}_\infty$ is a product of real primes and $\mathfrak{m}_0$ is a product of powers of prime ideals. Let $S(\mathfrak{m}) = \{$primes dividing $\mathfrak{m}\}$, ie the set of primes $\mathfrak{p}$ with $m(\mathfrak{p}) \geq 1$, or just the support of m.

Let $K_{\mathfrak{m},1} = \{a \in K^\times | \mathrm{ord}_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) \forall \mathfrak{p} \in S(\mathfrak{m}_0)$ and $a_\mathfrak{p} > 0 \forall \mathfrak{p} \in S(\mathfrak{m}_\infty)\}$. If $a \in K_{\mathfrak{m},1}$ and $\mathfrak{p} \in S(\mathfrak{m}_0)$, then $\mathrm{ord}_\mathfrak{p}(a-1) > 0 = \mathrm{ord}_\mathfrak{p}(1)$. If $\mathrm{ord}_\mathfrak{p}(a) \neq 0$, then $\mathrm{ord}_\mathfrak{p}(a-1) = \min(\mathrm{ord}_\mathfrak{p}(a), 0) > 0$ which is impossible. So, $\mathrm{ord}_\mathfrak{p}(a) = 0$. Note that the definition of $I^{S(\mathfrak{m})}$ ignores the infinite places, we have $a \in K_{\mathfrak{m},1}$ implies $i(a) = (a) \in I^{S(\mathfrak{m})}$. This enables us to give the following definition.

Definition 5.4 *Given a modulus $\mathfrak{m}$, the* ***ray class group modulo*** *$\mathfrak{m}$ is given by $C_\mathfrak{m} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$.*

We write $U_{\mathfrak{m},1} = U_K \cap K_{\mathfrak{m},1}$ and $K_\mathfrak{m} = K^{S(\mathfrak{m})}$. Then, we have the following theorem.

Theorem 5.5 *For any modulus $\mathfrak{m}$, there is an exact sequence*

$$0 \to U_K/U_{\mathfrak{m},1} \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to C_\mathfrak{m} \to C \to 0$$

and canonical isomorphisms

$$K_\mathfrak{m}/K_{\mathfrak{m},1} \cong \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \{\pm\} \times \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \cong \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times.$$

Corollary 5.6 *$C_{\mathfrak{m}}$ is a finite group of order*

$$h_{\mathfrak{m}} = \frac{2^{r_0} h \mathbb{N}(\mathfrak{m}_0)}{(U : U_{\mathfrak{m},1})} \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 - \frac{1}{\mathbb{N}\mathfrak{p}})$$

where r_0 is the number of real primes dividing $\mathfrak{m}$ and h is the class number of K.

Definition 5.7 *Let L/K be a finite Galois extension with Galois group G. If $\mathfrak{p}$ is an ideal of K, and let $\mathfrak{P}$ be an ideal of L lying over it, ie $\mathfrak{P}|\mathfrak{p}$. The* ***decomposition group*** *$D(\mathfrak{P})$ is defined to be $\{\sigma \in G | \sigma\mathfrak{P} = \mathfrak{P}\}$.*

There is an isomorphism $D(\mathfrak{P}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. If $\mathfrak{P}$ is unramified over $\mathfrak{p}$, then the action of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ on $\mathcal{O}_L$ induces an isomorphism on the Galois groups $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(k_{L_{\mathfrak{P}}}/k_{K_{\mathfrak{p}}})$. The group on the RHS is cyclic, generated by the Frobenius element $x \mapsto x^q$ where $q = |k_{K_{\mathfrak{p}}}|$. The corresponding element on LHS is called the Frobenius element $(\mathfrak{P}, L/K)$ at $\mathfrak{P}$. In fact, it is the unique element of $\sigma \in \mathrm{Gal}(L/K)$ s.t.

(a) $\sigma \in D(\mathfrak{P})$, ie $\sigma\mathfrak{P} = \mathfrak{P}$;

(b) for all $\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^q \mathrm{mod}\mathfrak{P}$, where q is the number of elements of the residue field $\mathcal{O}_K/\mathfrak{p} = k_{K_{\mathfrak{p}}}$, $\mathfrak{p} = \mathfrak{P} \cap K$.

We will now give some properties of the Frobenius element.

Lemma 5.8 *With the above notations, let $g \in \mathrm{Gal}(L/K)$ with $g\mathfrak{P}$ be a second prime dividing $\mathfrak{p}$. Then $D(g\mathfrak{P}) = gD(\mathfrak{P})g^{-1}$ and $(g\mathfrak{P}, L/K) = g(\mathfrak{P}, L/K)g^{-1}$.*

With the notations above. Given two primes $\mathfrak{P}_1$, $\mathfrak{P}_2$ of L dividing $\mathfrak{p}$, there exists $g \in G$ s.t. $g\mathfrak{P}_1 = \mathfrak{P}_2$. So, $\{(\mathfrak{P}, L/K) | \ \mathfrak{P}|\mathfrak{p}\}$ is a conjugacy class in G, denoted by $(\mathfrak{p}, L/K)$. When L/K is abeian, this class has one element only. We will regard this as an element of G.

Lemma 5.9 *Consider a tower of fields*

$$\begin{array}{cc} M & \mathfrak{Q} \\ | & \\ L & \mathfrak{P} \\ | & \\ K & \mathfrak{p} \end{array}$$

where $\mathfrak{Q}$ is unramified over $\mathfrak{p}$. We have $(\mathfrak{Q}, M/L) = (\mathfrak{Q}, M/K)^{f(\mathfrak{P}/\mathfrak{p})}$ where f denotes the residue degree. Moreover, if L/K is Galois, then $(\mathfrak{Q}, M/K)|_L = (\mathfrak{P}, L/K)$.

5.2 Statements of Main Theorems

Definition 5.10 *Let L/K be an abelian extension, let S be a finite set of primes of K containing all primes that ramify in L. Define a homomorphism $\psi_{L/K} : I^S \to \mathrm{Gal}(L/K)$ by $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} \mapsto \prod(\mathfrak{p}_i, L/K)^{n_i}$. This is called the* ***global Artin map****.*

Proposition 5.11 *Let L be an abelian extension of K, and let K' be an intermediate field. Assume S is a finite set of prime ideals of K containing all those that ramify in L and the set of primes of K' lying over a prime in S. Then the following diagram commutes.*

$$\begin{tikzcd} I_{K'}^S \arrow[r, "\psi_{L/K'}"] \arrow[d, "N_{K'/K}"'] & \mathrm{Gal}(L/K') \arrow[d, "\text{inclusion}"] \\ I_K^S \arrow[r, "\psi_{L/K}"] & \mathrm{Gal}(L/K) \end{tikzcd}$$

where $N_{K'/K}$ is the norm map from I'_K to I_K (this is defined to be the unique homomorphism s.t. for any prime $\mathfrak{P}$ of K', $N_{K'/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$ where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$).

Corollary 5.12 *For any abelian extension L of K, $N_{L/K}(I_L^S) \subseteq \ker \psi_{L/K}$.*

Therefore, the Artin map factors through $\psi_{L/K} : I_K^S / N_{L/K}(I_L^S) \to \mathrm{Gal}(L/K)$ by an abuse of notations.

Definition 5.13 *Let S be a finite set of primes of K, G any group. We say that a homomorphism $\psi : I^S \to G$* ***admits a modulus*** *if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \subseteq S$ s.t. $\psi(i(K_{\mathfrak{m},1})) = 0$.*

Theorem 5.14 (Reciprocity Law) *Let L be a finite abelian extension of K, and let S be the set of primes of K ramifying in L. Then the Artin map $\psi : I^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, and it defines an isomorphism*

$$I_K^{S(\mathfrak{m})} / i(K_{\mathfrak{m},1}) \cdot N_{L/K}(I_L^S(\mathfrak{m})) \to \mathrm{Gal}(L/K).$$

Definition 5.15 *With the notations as in the theorem above, we call the modulus $\mathfrak{m}$ a* ***defining modulus*** *for L.*

We write $I_K^{\mathfrak{m}}$ for the group of $S(\mathfrak{m})$-ideals in K, and $I_L^{\mathfrak{m}}$ for the group of $S(\mathfrak{m})'$-ideals in L, where $S(\mathfrak{m})'$ contains the primes of L lying over a prime in S.

Definition 5.16 *We say a subgroup H of $I_K^{\mathfrak{m}}$ is a* ***congruence subgroup modulo*** *$\mathfrak{m}$ if $I_K^{\mathfrak{m}} \supseteq H \supseteq i(K_{\mathfrak{m},1})$.*

Theorem 5.17 (Existence Theorem) *For any congruence subgroup H modulo $\mathfrak{m}$, there exists an abelian extension L/K s.t. $H = i(K_{\mathfrak{m},1}) \cdot N_{L/K}(I_L^{\mathfrak{m}})$.*

For H and L as above, by the Reciprocity Law, the Artin map induces an isomorphism $I^{S(\mathfrak{m})}/H \to \mathrm{Gal}(L/K)$. Therefore, for a fixed $\mathfrak{m}$, there is a field $L_{\mathfrak{m}}$, s.t. $C_{\mathfrak{m}} \cong \mathrm{Gal}(L_{\mathfrak{m}}/K)$ via the Artin map.

Definition 5.18 *With the above notations, $L_{\mathfrak{m}}$ is called the **ray class field modulo** $\mathfrak{m}$.*

5.3 Examples

We will now give some examples to illustrate some of the theory in the previous section.

(1) Let $K = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt{m}]$ where m is a sqaure-free integer. Let S be the set of finite primes of K that ramify in L. So S consists of the primes dividing m if $m \equiv 1(\mathrm{mod}4)$ and the primes dividing m together with 2 otherwise. $\mathrm{Gal}(L/K) = \{1, \sigma\}$ where $\sigma\sqrt{m} = -\sqrt{m}$. If $p \in I^S$, $\psi_{L/K}(p) = (p, L/K)$.
To find $(p, L/K)$, we can take $\mathfrak{P} = (p)$ in the definition. We have $(p, L/K)\alpha \equiv \alpha^p \mathrm{mod} p$ for all $\alpha \in \mathcal{O}_L$. But $\mathcal{O}_L = \mathbb{Z}[(1+\sqrt{m})/2]$ if $m \equiv 1(\mathrm{mod}4)$ and $\mathbb{Z}[\sqrt{m}]$ otherwise. Therefore, we have $(p, L/K) = \sigma$ if m is not a square mod$p$ and 1 otherwise. If we identify σ with -1, $\psi_{L/K}(p)$ is just $(\frac{m}{p})$, the Legendre symbol. In general, by multiplicativity, $\psi_{L/K}$ is just the Jacobi symbol.

(2) Let $K = \mathbb{Q}$, $L = \mathbb{Q}[\zeta]$ where ζ is a p^{th} root of unity and p is a rational prime. Then the only prime ramifying in L is p itself. $\mathrm{Gal}(L/K)$ is identified with $(\mathbb{Z}/p\mathbb{Z})^\times$. Similar to above, for any rational prime q other than p, we have $(q, L/K) = (\zeta \mapsto \zeta^q)$, corresponding to $q(\mathrm{mod}p)$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. The Artin map is just $I^S \to (\mathbb{Z}/p\mathbb{Z})^\times$ with $(r/s) \mapsto rs^{-1}(\mathrm{mod}p)$.

(3) Let $\mathfrak{m}$ be a modulus and L a subfield of $L_{\mathfrak{m}}$. If we write $N(C_{L,\mathfrak{m}}) = i(K_{\mathfrak{m},1}) \cdot N_{L/K}(I_L^{\mathfrak{m}}) \mathrm{mod} i(K_{\mathfrak{m},1})$, similar to local class field theory, we have a corollary to the Existence Theorem which relates the abelian extensions of K to the norm groups.

Corollary 5.19 *Fix a modulus $\mathfrak{m}$. Then the map $L \mapsto N(C_{L,\mathfrak{m}})$ is a bijection from the set of abelian extensions of K contained in $L_{\mathfrak{m}}$ to the set of subgroups $C_{\mathfrak{m}}$. Moreover, the correspondence is inclusion-reversing and we have:*

$$\begin{aligned} N(C_{L_1 \cdot L_2,\mathfrak{m}}) &= N(C_{L_1,\mathfrak{m}}) \cap N(C_{L_2,\mathfrak{m}}); \\ N(C_{L_1 \cap L_2,\mathfrak{m}}) &= N(C_{L_1,\mathfrak{m}}) \cdot N(C_{L_2,\mathfrak{m}}). \end{aligned}$$

for any intermediate subfields L_1 and L_2.

(4) Let L/K be an abelian extension with Galois group G. By the Reciprocity Law, there is a modulus $\mathfrak{m}$ with support the set of primes of K ramifying in L s.t. the Artin map $\psi_{L/K}$ takes the value 1 on $i(K_{\mathfrak{m},1})$. Consider the map in theorem 5.5

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

There will be a smallest integer $f(\mathfrak{p}) \leq m(\mathfrak{p})$ s.t. the map factors through $(\mathcal{O}_K/\mathfrak{p}^{f(\mathfrak{p})})^\times$. The modulus $\mathfrak{f}(L/K) = \mathfrak{m}_\infty \prod \mathfrak{p}^{f(\mathfrak{p})}$ is then the smallest modulus s.t. $\psi_{L/K}$ factors through $C_\mathfrak{f}$. We call this the conductor of L/K. The conductor $\mathfrak{f}(L/K)$ is divisible exactly by the primes ramifying in L.

The subfields of the ray class field $L_\mathfrak{m}$ containing K are those conductor $\mathfrak{f}|\mathfrak{m}$. Every abelian extension of K is contained in $L_\mathfrak{m}$ for some $\mathfrak{m}$.

Take $K = \mathbb{Q}$. Let m be a positive integer which is odd or divisble by 4. We have a modulus $\mathfrak{m}$ which is just the factorisation of (m) into prime ideals of $\mathbb{Z}$. The ray class field for (m) is $\mathbb{Q}[\zeta_m + \bar{\zeta_m}]$, and the ray class field for $\infty(m)$ is $\mathbb{Q}[\zeta_m]$ where ∞ denotes the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$. Thus the Reciprocity Law implies the Kronecker-Weber theorem: every abelian extension of $\mathbb{Q}$ has conductor dividing $\infty(m)$ for some m of this form, and therefore is contained in a cyclotomic field.

References

[1] F.W. Anderson and K.R. Fuller: *Rings and Categories of Modules*, Springer-Verlag (1974).

[2] J.W.S. Cassels: *Local Fields*, Cambridge University Press (1986).

[3] J.W.S. Cassels and A. Fröhlich (Eds): *Algebraic Number Theory*, Academic Press (1967).

[4] S. Mac Lane: *Categories for the Working Mathematician*, Springer-Verlag (1998).

[5] J. Milne: *Class Field Theory*, http://www.jmilne.org/ (1997).