1 Group Cohomology

1.1 Definitions

Let $G$ be a group.

Definition 1.2. A $G$-module $A$ is a $\mathbb{Z}[G]$-module, that is, an abelian group $A$ together with a homomorphism of groups $G \to \text{Aut} A$. A morphism of $G$-modules is a morphism as $\mathbb{Z}[G]$-modules.

This is an abelian category since the category of $R$-modules is, for any commutative ring $R$. For this reason, the category of $G$-modules has enough injectives and enough projectives. If $A^G = \{a \in A : ga = a\}$ and $A_G = A/\{ga - a : g \in G, \ a \in A\}$ then for any morphism $A \to B$ we obtain morphisms $A^G \to B^G$ and $A_G \to B_G$, so $A \to A^G$ and $B \to B^G$ are functors from $G$-modules to $G$-modules. The functor $A \to A^G$ is left exact while the functor $A \to A_G$ is right exact.

Definition 1.3. The cohomology group $H^r(G, A)$ is the $r$th right derived functor of $A \to A^G$, and the homology group $H_r(G, A)$ is the $r$th left derived functor of $A \to A_G$.

Remark 1.4. Give $\mathbb{Z}$ the trivial $G$-action and define $\mathbb{Z}[G] \to \mathbb{Z}$ by $g \mapsto 1$ for all $g \in G$. Then $A^G = \text{Hom}(\mathbb{Z}, A)$ and $A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ so we can identify $H^r(G, A) = \text{Ext}^r(\mathbb{Z}, A)$ and $H_r(G, A) = \text{Tor}_r(\mathbb{Z}, A)$.

1.5 Functoriality

The $H^r$ and $H_r$ are cohomological functors in the sense of Grothendieck, that is for any exact sequence

$$0 \to A' \to A \to A'' \to 0$$

(1)

one obtains a long exact sequences

$$0 \to H^0(G, A') \to \cdots \to H^r(G, A) \to H^r(G, A'') \xrightarrow{\delta} H^{r+1}(G, A') \to \cdots$$

and

$$\cdots H_r(G, A) \to H_r(G, A'') \xrightarrow{\delta} H_{r-1}(G, A') \to \cdots \to H_0(G, A'') \to 0$$

that are functorial in the exact sequence (1). Moreover, $H^0(G, A) = A^G$ and $H_0(G, A) = A_G$ since the functors $A \to A^G$ and $A \to A_G$ are left exact and right exact respectively.

Now let $A$ (resp. $A'$) be a $G$ (resp. $G'$) module, and suppose we have a homomorphism of groups $\psi : G' \to G$ and a $G'$-modphism $\varphi : A \to A'$. Then we obtain an inclusion $A^G \hookrightarrow A^{G'}$ and a $G'$-morphism $A^{G'} \to A^{G''}$, and hence morphisms

$$(\psi, \varphi) : H^r(G, A) \to H^r(G', A').$$

for $r \geq 0$.

Similarly, if $\psi : G \to G'$ is a homomorphism of groups, and $\varphi : A \to A'$ is a $G$-morphism, then we have induced maps $A_G \to A_G' \to A^{G'}_G$, and hence morphisms

$$(\psi, \varphi) : H_r(G, A) \to H_r(G', A')$$

for $r \geq 0$.

If we only consider a morphism $G' \to G$, we obtain induced maps $A_{G'} \to A_G$ and $A^G \to A^{G'}$ and thus maps $H^r(G, A) \to H^r(G', A)$ and $H_r(G', A) \to H_r(G, A)$. 

1
2 Local Class Field Theory

Theorem 2.1. Let $K$ be a local nonarchimedean field. Then there is a continuous homomorphism

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

such that:

1. If $L/K$ is an unramified extension and $\pi \in K$ is any prime element, then $\phi_K(\pi)|_L = \text{Frob}_{L/K}$.

2. For any finite abelian extension $L/K$, the map $a \mapsto \phi_K(a)|_L$ induces an isomorphism

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

Theorem 2.2. A subgroup $N$ of $K^\times$ is of the form $\text{Nm}(L^\times)$ for some finite abelian extension $L/L$ iff it is of finite index and open. That is, the map $L \mapsto \text{Nm}(L^\times)$ is a bijection between the finite abelian extensions of $K$ and the open subgroups of finite index in $K^\times$.

Remark 2.3. If $\text{char } K = 0$ then every subgroup of finite index is open.

Example 2.4. We consider the specific case $K = Q_p$. The isomorphisms $Q_p^\times / \text{Nm}(L^\times) \simeq \text{Gal}(L/Q_p)$ for $L/Q_p$ abelian give an isomorphism

$$\lim\limits_{\rightarrow} Q_p^\times / \text{Nm}(L^\times) \simeq \text{Gal}(Q_p^{ab}/Q_p).$$

The left hand side is the completion of $Q_p^\times \simeq Z_p^\times \times Z$ with respect to the norm topology, which is isomorphic to $Z_p^\times \times \hat{Z}$. Thus $Q_p^{ab}$ is the compositum of the fixed fields of $\phi(Z_p^\times)$ and $\phi(\hat{Z})$. The left hand side is the local artin map. But we know that $\phi(p)|_{Q_p^{nr}} = \text{Frob}_p$ and that $Z_p^\times$ is the kernel of $Q_p^\times \xrightarrow{\sim} \text{Gal}(Q_p^{nr}/Q_p)$. Thus $Q_p^{nr}$ is the fixed field of $Z_p^\times$, and in our notes on local field extensions we explicitly describe this field and the action of the galois group $\hat{Z}$ on it.

Now let $L/Q_p$ be a finite field extension fixed by $\phi(\hat{Z})$, i.e. fixed by Frob$_p$. Then as $\phi(p)$ acts trivially on $L$, we must have $p \in \text{Nm}(L^\times)$ by the reciprocity isomorphism. The only abelian extensions of $Q_p$ that satisfy this requirement are the extensions $L_n := Q_p(\zeta_{p^n})$ (see local fields notes). Thus, the fixed field of $\langle \phi(p) \rangle$ is $Q_p(\zeta^\infty_p)$; it is totally ramified over $Q_p$ with galois group $Z_p^\times$.

We conclude that $Q_p^{ab} = Q_p(\zeta_{p^n}) \cdot Q_p^{nr}$, where $Q_p^{nr} = \lim\limits_{\rightarrow} Q_p(\zeta_n)$.

Example 2.5. We describe the map $\phi : Q_p^\times \to \text{Gal}(Q_p(\zeta)/Q_p)$ for a primitive $n$ th root of unity $\zeta$. Let $a = up^t \in Q_p^\times$ with $u \in Z_p^\times$ and write $n = mp$ with $p \nmid m$, so $Q_p(\zeta_n)$ is the compositum $Q_p(\zeta_{p^r}) \cdot Q_p(\zeta_m)$. Then $\phi(a)$ acts on $Q_p(\zeta_n)$ by $\zeta_m \mapsto \text{Frob}_p(\zeta_m) = \zeta_p^m$ and on $Q_p(\zeta_{p^r})$ by $\zeta_{p^r} \mapsto \zeta_{p^r}^{(u \mod p^r)^{-1}}$.

We now sketch the construction of the local Artin map $\phi_K$.

Proposition 2.6. For any local field, there is a canonical isomorphism

$$\text{inv}_K : H^2(K^{ab}/K) := H^2(\text{Gal}(K^{ab}/K), K^{ab^\times}) \simeq Q/Z.$$

Proof. Let $L/K$ be an unramified extension of $K$ and set $G = \text{Gal}(L/K)$ and $U_L = \mathfrak{O}_L^\times$. From the long exact cohomology sequence of the exact sequence of $G$-modules

$$1 \to U_L \to L^\times \xrightarrow{\text{ord}_L} Z \to 0$$

we obtain an isomorphism $H^2(G, L^\times) \xrightarrow{\sim} H^2(G, Z)$, where we have used the fact that $H^1(G, U_L) = 0$. Similarly, from

$$0 \to Z \to Q \to Q/Z \to 0$$

we obtain an isomorphism $H^1(G, Z) \xrightarrow{\sim} H^1(G, Q/Z)$, where we have used the fact that $H^1(G, Q) = 0$. Thus, we have the isomorphism $H^2(K^{ab}/K) \xrightarrow{\sim} H^2(\text{Gal}(K^{ab}/K), K^{ab^\times})$ given by

$$\text{inv}_K : H^2(K^{ab}/K) \xrightarrow{\sim} H^2(\text{Gal}(K^{ab}/K), K^{ab^\times}) \simeq Q/Z.$$


we obtain an isomorphism $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$, where we have used that $H^r(G, \mathbb{Q}) = 0$ for all $r \geq 1$ (because multiplication by $m$ on $\mathbb{Q}$, and hence on $H^r(G, \mathbb{Q})$, is an isomorphism, but since $G$ is finite, $H^r(G, \mathbb{Q})$ is torsion).

Finally, the map $H^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ given by $f \mapsto f(\text{Frob}_{L/K})$ is an isomorphism from $H^1(G, \mathbb{Q}/\mathbb{Z})$ to the subgroup of $\mathbb{Q}/\mathbb{Z}$ generated by $1/n$, where $n = \# G$ (it i here that we use the unramified hypothesis on $L/K$).

We define $\text{inv}_{L/K}$ to be the composite

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

One checks that all the maps above are compatible with $\text{Inf} : H^2(L/K) \to H^2(E/K)$ for any tower of fields $E \supset L \supset K$ with $E, L$ unramified over $K$, i.e. that $\text{inv}_{L/K} = \text{inv}_{E/K} \circ \text{Inf}$, so the maps $\text{inv}_{L/K}$ form an inverse system allowing us to define $\text{inv}_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$. This must be an isomorphism since its image contains $1/n$ for all $n$ (as there is a unique unramified degree $n$ extension of $K$ for every $n$).

The whole point of this is to be able to make the following definition and conclude the next two propositions:

**Definition 2.7.** The fundamental class $u_{L/K} \in H^2(L/K)$ is the element corresponding to $1/[L : K]$ in $\mathbb{Q}/\mathbb{Z}$ under $\text{inv}_{L/K}$.

**Proposition 2.8.** Let $E \supset L \supset K$ be a tower of fields. Then $\text{Inf}(u_{L/K}) = [E : L]u_{E/K}$ and $\text{Res}(u_{E/K}) = u_{E/L}$.

Along with Hilbert’s Theorem 90, this allows one to conclude:

**Proposition 2.9.** Let $L/K$ be a finite extension of local fields with $G = \text{Gal}(L/K)$. For any subgroup $H \subset G$ we have $H^1(H, L^\times) = 0$ and $H^2(H, L^\times)$ is cyclic of order $\# H$, generated by $\text{Res}(u_{L/K})$.

One can then apply Tate’s Theorem:

**Theorem 2.10.** Let $G$ be a finite group and $C$ a $G$-module. Suppose that for every subgroup $H$ of $G$ that $H^1(H, C) = 0$ and $H^2(H, C)$ is cyclic of order $\# H$. Then for all $r$ there is an isomorphism

$$H^r_T(G, \mathbb{Z}) \cong H^{r+2}(G, C).$$

**Corollary 2.11.** There is an isomorphism

$$G^{ab} = H^2_T(G, \mathbb{Z}) \cong H^0_T(G, L^\times) = K^\times / \text{Nm}(L^\times).$$

**Proof:** Set $r = -2$ above. We must show that $G^{ab} = H^{-2}_T(G, \mathbb{Z})$ and $H^2_T(G, L^\times) = K^\times / \text{Nm}(L^\times)$. Recall that the Tate cohomology groups are defined as:

$$H^r_T(G, M) = \begin{cases} H^r(G, M) & r > 0 \\ M^{G}/\text{Nm}_G(M) & r = 0 \\ \ker \text{Nm}_G / I_G M & r = -1 \\ H_{-r-1}(G, M) & r < -1 \end{cases}$$

where $I_G$ is the augmentation ideal, that is, the kernel of $\mathbb{Z}[G] \overset{g \mapsto 1}{\longrightarrow} \mathbb{Z}$ (It is a free $\mathbb{Z}$-module generated by $(g-1)$ for $g \in G$) and $\text{Nm}_G(m) = \sum_{g \in G} g m$. Thus, $H^2_T(G, L^\times) = K^\times / \text{Nm}_G(L^\times) = K^\times / \text{Nm}(L^\times)$ on remembering that $L^\times$ is a $G$-module under multiplication, so $\text{Nm}_G = \text{Nm}_{L/K}$. Now $H^{-2}_T(G, \mathbb{Z}) = H_1(G, \mathbb{Z})$. Using the exact sequence

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

3
we obtain

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

where we have used the fact that \( \mathbb{Z}[G] \) is projective as a \( \mathbb{Z}[G] \)-module (since it is free). Since \( M_G := \frac{M}{\{gm-M\}} = M/I_GM \) is the largest quotient on which \( G \) acts trivially, we see that \( \mathbb{Z}_G = \mathbb{Z}, \mathbb{Z}[G]/G \mathbb{Z}[G] \) and \( (I_G)_G = I_G/I_G^2 \), and since \( I_G \to \mathbb{Z}[G] \) is the inclusion map, the map \( I_G/I_G^2 \to \mathbb{Z}[G]/I_G \mathbb{Z}[G] \) is the zero map. Hence we have an isomorphism \( H_1(G, \mathbb{Z}) \cong I_G/I_G^2 \).

Now consider the map \( G \to I_G/I_G^2 \) defined by \( g \mapsto (g-1)+I_G^2 \). Since \( gg'-1 \equiv g-1+g'-1 \mod I_G^2 \), this is a homomorphism, and since \( I_G/I_G^2 \) is commutative, it factors through \( G^{ab} \). Define a homomorphism \( I_G \to G \) by \( g-1 \mapsto g \) (free \( \mathbb{Z} \)-module!). Again, \( (g-1)(g'-1) = gg'-1 + g-1 + g'-1 \) maps to \( gg' \cdot g'^{-1} \cdot g^{-1} = 1 \) so this map factors through \( I_G/I_G^2 \) and is obviously inverse to the map in the other direction. Thus we have an isomorphism \( H_1(G, \mathbb{Z}) \cong I_G/I_G^2 \cong G^{ab} \).

\[ \square \]

### 3 Global Class Field Theory: Ideles

Let \( K \) be a global field and for any valuation \( v \) of \( K \) let \( K_v \) denote the completion of \( K \) with respect to \( | \cdot |_v \) and \( \mathcal{O}_v = \{ x \in K_v : |x|_v \leq 1 \} \) the ring of integers. We will denote by \( p_v \) the prime ideal of \( \mathcal{O}_K \) corresponding to \( v \) when \( v \) is finite, or its expansion under the map \( \mathcal{O}_K \hookrightarrow \mathcal{O}_v \).

**Definition 3.1.** The ideles \( I_K \) are the topological group with underlying set

\[ I_K = \{(a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for almost all } v\} \]

under component-wise multiplication with a base of opens given by the sets \( \prod U_v \) with \( U_v \subseteq K_v^\times \) open and \( U_v = \mathcal{O}_v^\times \) for almost all \( v \). In particular, the sets

\[ U(S, \epsilon) := \{(a_v) : |a_v - 1| < \epsilon \quad v \in S, \quad |a_v|_v = 1 \quad \forall v \notin S\} \]

form a base of opens of the identity.

We have an injection \( K^\times \hookrightarrow I_K : a \mapsto (a, a, a, \cdots) \) and the image is discrete: indeed, if \( \epsilon < 1 \) and \( S \) is any finite set containing the infinite places, the set \( U(S, \epsilon) \) is a nbd. of the identity with \( U(S, \epsilon) \cap K^\times = \{ a \in K^\times : |a - 1|_v < \epsilon, \quad v \in S, \quad |a|_v = 1, \quad \forall v \notin S\} \), which only contains \( a = 1 \) since by the product formula \( \prod |a|_v = 1 \).

**Definition 3.2.** The idele class group is the quotient \( C_K = I_K/K^\times \).

Now let \( L/K \) be a finite extension.

**Definition 3.3.** Define the map \( \text{Nm} : I_L \to I_K \) by \( \text{Nm}(b_w) = (\prod_{v|w} \text{Nm}_{L_v/K_v} b_w) \). For \( \alpha \in L \) we have \( \text{Nm}_{L/K} \alpha = \prod_{w|\alpha} \text{Nm}_{L_w/K_w}(\alpha) \) so the map \( \text{Nm} \) restricts to \( \text{Nm}_{L/K} \) on the image of \( L^\times \).

**Theorem 3.4.** There exists a unique continuous homomorphism \( \phi_K : I_K \to \text{Gal}(K^{ab}/K) \) with the following properties:

1. (Compatibility) Let \( L/K \) be a finite extension. If \( \phi_v : K_v \to \text{Gal}(L_v/K_v) \simeq D(v) \subseteq \text{Gal}(L/K) \) is the local Artin map then the diagram

\[ \begin{array}{ccc}
K_v & \xrightarrow{\phi_v} & \text{Gal}(L_v/K_v) \\
\downarrow & & \downarrow \\
I_K & \xrightarrow{\phi_K} & \text{Gal}(L/K)
\end{array} \]

commutes.
2. (Artin Reciprocity) We have $\phi_K(K^\times) = 1$ and for every finite abelian extension $L/K$ an isomorphism

$$\phi_{L/K} : I_K/(K^\times \cdot \text{Nm}(I_L)) \xrightarrow{\sim} \text{Gal}(L/K).$$

Observe that $C_K/\text{Nm}(C_L) \simeq I_K/(K^\times \cdot \text{Nm}(I_L))$ so item 2 can be rephrased as an isomorphism $\phi_K : C_K/\text{Nm}(C_L) \xrightarrow{\sim} \text{Gal}(L/K)$.

**Theorem 3.5.** Let $N \subseteq C_K$ be an open subgroup of finite index. Then there exists a unique abelian extension $L/K$ with $\text{Nm}(C_L) = N$.

**Definition 3.7.** A modulus $m$ is a formal product of places $m = \prod_{p} p^{m(p)}$ where for $p$ infinite complex we set $m(p) = 0$ and for $p$ infinite real we stipulate $m(p) \leq 1$, and for all but finitely many $p$ we have $m(p) = 0$.

**Definition 3.8.** For any modulus $m$ let

$$W_m(p) = \begin{cases} R_{>0} & p \text{ real} \\ 1 + p^{m(p)} & p \text{ finite} \end{cases},$$

and observe that $W_m(p)$ is a nbd. of 1 and an open subgroup of $K_p^\times$. We put

$$W_m = \prod_{p|m} K_p^\times \times \prod_{p|m} W_m(p) \times \prod_{p|m} \mathcal{O}_p^\times.$$ 

It is an open subgroup of

$$I_m := \left( \prod_{p|m} K_p^\times \times \prod_{p|m} W_m(p) \right) \cap I.$$ 

We put $K_{m,1} := K^\times \cap I_m$; it is the subgroup of all $a \in K^\times$ with $\text{ord}_p(a - 1) \geq m(p)$ for $p$ finite and $a > 0$ in every real embedding $K \hookrightarrow \bar{K}$, i.e. totally positive.

**Proposition 3.9.** The inclusion $I_m \hookrightarrow I$ gives an isomorphism $I_m/K_{m,1} \simeq I/K^\times$.

**Proof.** By the definition of $K_{m,1}$, it is the kernel of $I_m \rightarrow \mathcal{O}/K^\times$, thus there is an injection $I_m/K_{m,1} \hookrightarrow I/K^\times$. Surjectivity follows from the weak approximation theorem. ■
4 Global Class Field Theory: Ideal-theoretic

In this section we derive the ideal-theoretic formulation of class field theory from the previous section. Throughout we fix the base field $K$.

**Definition 4.1.** Let $m$ be a modulus. Then $I^m$ is the group of fractional ideals of $\mathcal{O}_K$ relatively prime to $m$; i.e. the free abelian group on the (finite) primes of $\mathcal{O}_K$ not dividing $m$. Observe that $K_{m,1} \hookrightarrow I^m$ via $a \mapsto a\mathcal{O}_K$. We define the ray class group $C_m := I^m/K_{m,1}$.

**Proposition 4.2.** The natural map $I^m \to C_m$ defined by $(a_p) \mapsto \prod_{p \text{ finite}} p^{\text{ord}_p(a_p)}$ gives an isomorphism $I_m/(K_{m,1} \cdot W_m) \cong C_m$.

**Proof.** This is just the kernel-cokernel sequence from $0 \to K_{m,1} \to I^m \to \text{coker } f \to 0$.

**Theorem 4.3.** Let $G$ be a finite abelian group with the discrete topology and $\phi : I \to G$ a continuous homomorphism such that $\phi(K^\times) = 1$. Then there exists a modulus $m$ such that $\phi$ factors through $C_m$ and thus defines a map $I^m \to G$ killing $K_{m,1}$.

**Proof.** By propositions 3.9, 4.2, it will suffice to show that $\phi$ kills $W_m$ for some $m$. Since $\phi$ is continuous, the kernel is an open subgroup, and so contains a basic nbd. of the identity. The components of this nbd. at the infinite places must be the connected component of the identity of $\mathbb{R}^\times$ or $\mathbb{C}^\times$, so by the definition of the $W_m$ and the fact that the sets $U(S, \varepsilon)$ form a system of nbds. of the identity, we see that $\phi$ kills $W_m$ for some $m$. ■

**Theorem 4.4.** Let $L/K$ be a finite abelian extension. Then there exists a modulus $m$ such that $\phi_K$ induces an isomorphism $I^m_K/(K_{m,1} \cdot \text{Nm}(I^m_L)) \cong \text{Gal}(L/K)$.

**Proof.** We have a map $a \mapsto \phi_K(a)|_L$ from $I \to \text{Gal}(L/K)$ which by Theorem 4.3 induces a map $I^m \to \text{Gal}(L/K)$ for some $m$ that kills $K_{m,1}$. The entire kernel of this map, by Theorem 3.4 (2), must be the image of the coset $K^\times \cdot \text{Nm}(I_L)$ under the map $I_K \to I_K/K^\times \cong I_m/K_{m,1} \to I^m_K/K_{m,1}$, where $I_m \to I^m_K$ is given by $(a_v) \mapsto \prod_{v \text{ finite}} p_v^{\text{ord}_v(a_v)}$. It is not hard to see that this image is $K_{m,1} \cdot \text{Nm}(I_L)$.

In a similar spirit, the next theorem follows from Theorem 3.5:

**Theorem 4.5.** For any subgroup $H \subset I^m_K$ that contains $K_{m,1}$ there exists a unique abelian extension $L/K$ with $H = K_{m,1} \cdot \text{Nm}(I^m_L)$. Equivalently, for every subgroup $H'$ of $C_m$, there exists an abelian extension $L/K$ such that $\phi_K$ induces (as above) an isomorphism $C_m/H' \cong \text{Gal}(L/K)$. 

6
Remark 4.6. The minimal modulus $m$ for which $\phi_K$ induces an isomorphism $I^m_K/(K_{m,1} \cdot \text{Nm}(I^m_L)) \sim \text{Gal}(L/K)$ is the conductor of $L/K$. It is divisible by precisely those primes of $K$ ramifying in $L$.

Remark 4.7. From the definition of $\phi_K(a_v)$ as the product $\prod \phi_v(a_v)$ of all the local Artin maps, it is immediate that the induced map $I^m_K \to \text{Gal}(L/K)$ takes a prime $p$ to the Frobenius element $\text{Frob}_p \in D(p) \subseteq \text{Gal}(L/K)$, and we see that this description determines the map completely.

Example 4.8. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$. Then $\text{Gal}(L/K) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$, with $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ acting on $\zeta_m \mapsto \zeta_m^a$. If $p$ is any prime of $\mathbb{Q}$ not ramifying in $L$ (equiv. not dividing $m\infty$) then $\text{Frob}_p \in (\mathbb{Z}/m\mathbb{Z})^\times$ must satisfy $\text{Frob}_p(\zeta_m) \equiv \zeta_m^p \mod p$ for a prime $p$ above $p$. But $\text{Frob}_p(\zeta_m) = \zeta_m^r$ for some $r$ and if $p | (\zeta_m^r - \zeta_m)$, then $p \mid \lim_{x \to 1} \prod_{0 < a < m} (x - \zeta_m^a) = m$,

which is not the case. Hence $\text{Frob}_p = p \in (\mathbb{Z}/m\mathbb{Z})^\times$, and it follows that the Artin map $I^\infty_Q \to (\mathbb{Z}/m\mathbb{Z})^\times$ is given by $(a/b)\mathbb{Z} \mapsto [a][b]^{-1}$, and hence that the kernel is

$$\{a/b \in \mathbb{Q} : (a, m) = (b, m) = 1, a \equiv b \mod m, a/b > 0\} = \mathbb{Q}_{m,1},$$

so $L = \mathbb{Q}(\zeta_m)$ is the ray class field $C_{m\infty}$.

**Corollary 4.9 (Kronecker-Weber Theorem).** Let $L$ be an abelian extension of $\mathbb{Q}$. Then $L \subseteq \mathbb{Q}(\zeta_m)$ for some $m$.

**Proof.** By Theorem 4.4, there exists a modulus $m$ with the artin map $I^m_Q \to \text{Gal}(L/K)$ defining an isomorphism $I^m_Q/(Q_{m,1} \cdot \text{Nm}(I^m_L)) \simeq \text{Gal}(L/Q)$. We may as well assume that $m = m\infty$, so by the above example we have an isomorphism $I^m_Q/Q_{m,1} \simeq \text{Gal}(Q(\zeta_m)/Q) := G$. Letting $H$ be the subgroup of $I^m_Q/Q_{m,1}$ corresponding to $\text{Nm}(Q_{m,1} \cdot I^m_L)$, we see that $H$ is a normal subgroup of $G$ and $G/H \simeq \text{Gal}(L/Q)$. Now using the Galois correspondence and the uniqueness statement of Theorem 4.5, we see that $L$ is a subfield of $Q(\zeta_m)$ (namely the fixed field of $H$).

### 5 Quadratic Reciprocity

We give a proof of Quadratic Reciprocity using the theory sketched above.

**Theorem 5.1.** Let $p, q$ be distinct odd primes and define $(\frac{p}{q})_Q$ by $\phi_{Q(\sqrt{p})/Q}(\sqrt{p}) = (\frac{p}{q})_Q \sqrt{p}$. Then

$$\left(\frac{p}{q}\right)_Q \left(\frac{q}{p}\right)_Q = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

**Proof.** Let $p^* = (-1)^{\frac{p-1}{2}} p$, so the unique quadratic subfield of $K = Q(\zeta_p)$ is $Q(\sqrt{p^*})$. There is a unique subgroup $H \subseteq G := \text{Gal}(K/Q) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ if index 2, namely the squares modulo $p$, so $\text{Gal}(Q(\sqrt{p^*})/Q) = G/H$. The artin reciprocity map $\phi_{K/Q} : I^m_Q \to \{a/b \in Q^\times : a/b > 0, \text{ord}_p(a/b) = 0\} \to G$ is given by $q \mapsto \text{Frob}_q$, which acts as $\zeta_p \mapsto \zeta_p^a \mod 1 - \zeta_p$, and since $(p, q) = 1$, this implies that $\text{Frob}_q(\zeta_p) = \zeta_p^q$. Hence, the artin map $\phi : I^m_Q \to (\mathbb{Z}/p\mathbb{Z})^\times$ is $a/b \mapsto [a][b]^{-1}$. On one hand, $\text{Frob}_q$ is trivial on $Q(\sqrt{p^*})$ iff $[q] \in H$, i.e. iff $(\frac{q}{p}) = 1$. On the other hand, $\text{Frob}_q \mid Q(\sqrt{p^*})$ is trivial iff the residual degree of $\mathbb{Z}[\sqrt{p^*}]/\mathbb{F}_p$ is 1, for any $Q$ above 1. This is the case iff $q$ splits in $Q(\sqrt{p^*})$, iff $x^2 - p^*$ splits in $\mathbb{F}_q[x]$, that is, iff $p^*$ is a square mod $q$. To conclude, we have shown that $(\frac{q}{p}) = 1$ iff $(\frac{q}{p})^2 = 1$ or equivalently $(\frac{q^2}{p}) = 1$. We need only show that $(\frac{-1}{q}) = (-1)^{\frac{q-1}{2}}$, but this is classical.
\section{Artin L-series}

Let $L/K$ be a galois extension of number fields and put $G = \text{Gal}(L/K)$. Let $(\rho, V)$ be a (complex) finite dimensional representation of $G$. For any prime $p$ of $K$ and $\mathfrak{p}$ above $p$ in $L$, the group $D_{\mathfrak{p}}/I_{\mathfrak{p}}$ acts on $V^{I_{\mathfrak{p}}} = \{v \in V : \sigma v = v, \ \sigma \in I_{\mathfrak{p}}\}$, where $D_{\mathfrak{p}} \subseteq G$ is the decomposition group at $\mathfrak{p}$ and $I_{\mathfrak{p}}$ is the inertia group at $\mathfrak{p}$. Thus, we obtain a representation $(\rho_{\mathfrak{p}}, V^{I_{\mathfrak{p}}})$ of $D_{\mathfrak{p}}/I_{\mathfrak{p}} \simeq \text{Gal}(l/k)$, where $l, k$ are the residue fields $k = K/\mathfrak{p}$ and $L = L/\mathfrak{p}$. As usual, $\text{Frob}_{\mathfrak{p}}$ is an element of $D_{\mathfrak{p}}$ whose image under the surjective map $D_{\mathfrak{p}} \to \text{Gal}(l/k)$ is a generator. As we know, the conjugacy class $\text{Frob}_{\mathfrak{p}} := \{\text{Frob}_{\mathfrak{p}}, \ \mathfrak{p} \cap K = p\} \subseteq G$ depends only on $p$, and moreover, for any $\mathfrak{p}_1, \mathfrak{p}_2$ above $p$, the groups $D_{\mathfrak{p}_1}, D_{\mathfrak{p}_2}$ and $I_{\mathfrak{p}_1}, I_{\mathfrak{p}_2}$ are simultaneously conjugate.

Thus, the characteristic polynomial
\[
\det(1 - t \rho(\text{Frob}_{\mathfrak{p}}))
\]
of the endomorphism $\rho(\text{Frob}_{\mathfrak{p}})$ acting on $V^{I_{\mathfrak{p}}}$ depends only on $p$.

\begin{definition}
Let $L/K$ be a Galois extension as above with $\text{Gal}(L/K) = G$, and let $(\rho, V)$ be a finite dimensional representation of $G$. Then the Artin $L$-series is
\[
\mathcal{L}(L/K, \rho, s) := \prod_{p \in \text{Spec } \mathcal{O}_K} \det(1 - N_{K/Q}(p)^{-s} \cdot \rho(\text{Frob}_p))^{-1},
\]
and where for each $p \in \text{Spec } \mathcal{O}_K$ we make an arbitrary choice of $\mathfrak{p} \in \text{Spec } \mathcal{O}_L$ lying over $p$.
\end{definition}

\begin{proposition}
The Artin $L$-series $\mathcal{L}(L/K, \rho, s)$ converges absolutely and uniformly for $\Re(s) > 1$.\end{proposition}

\begin{proof}[sketch of proof] The endomorphism $\rho(\text{Frob}_p)$ has finite order, so the roots of the characteristic polynomial are roots of unity; i.e. we have
\[
\det(1 - N_{K/Q}(p)^{-s} \cdot \rho(\text{Frob}_p)) = \prod_{i=1}^{d}(1 - \epsilon_i N_{K/Q}(p)^{-s}),
\]
with $d = \dim V^{I_{\mathfrak{p}}} < n = \dim V$. Thus, we wish to investigate the convergence of
\[
\sum_{p} \sum_{i=1}^{d} \epsilon_i q^s,
\]
where $q = N_{K/Q}(p)$. Convergence for $\Re(s) > 1$ is not obvious.\end{proof}

\begin{example}
If $\rho$ is the trivial representation, then we have
\[
\mathcal{L}(L/K, \rho, s) = \prod_{p \in \text{Spec } \mathcal{O}_K} (1 - N_{K/Q}(p)^{-1})^{-1} = \zeta_K(s),
\]
which evidently does not depend on $L$.
\end{example}

\begin{example}
Suppose now that $G$ is abelian, and let $\rho$ be an irreducible (hence 1-dimensional) representation of $G$. Then we have an isomorphism $C_K/\text{Nm}(C_L) \xrightarrow{\sim} G$ by CFT, so we can interpret $\rho$ as a character of $C_K$ that is trivial on $\text{Nm}(C_L)$, and is hence continuous. Or, using the ideal-theoretic version of CFT, there is a modulus $m$ and a surjective homomorphism $I_K^m \to G$ that is trivial on $K_{m,1}$, so we may think of $\rho$ as a (continuous) character of the ray class group $I_K^m/K_{m,1}$. In either case, we recover the Artin $L$-series recovers a generalized Dirichlet series associated to a Hecke character.
\end{example}

\begin{definition}
A Hecke character is a continuous homomorphism $\chi : I_K \to \mathbb{C}^\times$ that is trivial on $K^\times$. Equivalently, it is a continuous character of the idele class group $C_K$.
\end{definition}

\begin{proposition}
For any Hecke character $\chi$, there exists a modulus $m$ such that $\chi$ induces a character $\overline{\chi} : C_m \to \mathbb{C}^\times$.
\end{proposition}
Indeed, referring to Prop. 4.2, it is enough to show that \( \chi \) kills some \( W_m \). But \( \chi \) is continuous, so the kernel contains an open set, which must contain some \( W_m \). Alternately, the image of \( \prod_{p \mid \infty} O_p^\times \) is a compact totally disconnected subgroup of \( C^\times \), hence finite, and this implies that the kernel contains \( W_m \) for some \( m \).

We now summarize some basic properties of Artin L-series.

**Proposition 6.7.**

Let \( E \supset L \supset K \) be a tower of fields, with \( E/L \) and \( L/K \) Galois. Any representation \( \rho \) of \( G(L/K) \) can be pulled back to a representation, also denoted \( \rho \), of \( G(E/K) \) via the surjective homomorphism \( G(E/K) \to G(L/K) \).

Then

\[
\mathcal{L}(E/K, \rho, s) = \mathcal{L}(L/K, \rho, s).
\]

If \( \rho, \rho' \) are two representations of \( G(L/K) \), then

\[
\mathcal{L}(L/K, \rho \oplus \rho', s) = \mathcal{L}(L/K, \rho, s) \mathcal{L}(L/K, \rho', s).
\]

If \( M \) is an intermediate field \( L \supset M \supset K \) and \( \rho \) is a representation of \( H = G(L/M) \) and we denote the induced representation of \( G = G(L/K) \) by \( \text{Ind}_H^G \rho \), then

\[
\mathcal{L}(L/M, \rho, s) = \mathcal{L}(L/K, \text{Ind}_H^G \rho, s).
\]

**Sketch of proof.** Observe that under the surjective map \( D_p/I_p \to D_p/I_p \) for \( p \) a prime of \( E \) over \( p \in \text{Spec} \, O_L \), the Frobenius \( \text{Frob}_p \) maps to \( \text{Frob}_p \). Now (1) follows from the definitions. As for (2), we remark that the charpoly of \( \text{Frob}_p \) acting on \( V_{I_p} \oplus V'_{I_p} \) is the product of the characteristic polynomials of the same operator on each of \( V_{I_p} \) and \( V'_{I_p} \) (think block matrices). The last item is a bit tricky, and we refer to Neukirch or Lang. ■

**Theorem 6.8.** For an infinite prime \( p \) put

\[
\mathcal{L}_p(L/K, \rho, s) = \begin{cases} 
  L_C(s)^{\text{Tr} \rho(1)} & \text{p real} \\
  L_R(s)^{n^+} L_R(s + 1)^{n^-} & \text{p real}
\end{cases}
\]

where

\[
L_C(s) = 2(2\pi)^{-s} \Gamma(s), \quad L_R(s) = \pi^{-s/2} \Gamma(s/2),
\]

and for real \( p \), we notice that \( \text{Frob}_p \) is of order 2, so we get an eigenspace decomposition \( V = V^+ \oplus V^- \), and we put \( n^+ = \dim V^+ \) and \( n^- = \dim V^- \). Set \( \mathcal{L}_\infty(L/K, \rho, s) = \prod_{p \mid \infty} \mathcal{L}_p(L/K, \rho, s) \). Then there exists a certain constant \( c(L/K, \rho) \), such that the function

\[
\Lambda(L/K, \rho, s) := c(L/K, \rho)^{s/2} \mathcal{L}_\infty(L/K, \rho, s) \mathcal{L}(L/K, \rho, s)
\]

meromorphically continues to all of \( C \) via the functional equation

\[
\Lambda(L/K, \rho, s) = W(\rho) \Lambda(L/K, \overline{\rho}, 1 - s)
\]

where \( \overline{\rho} \) is the the composition of \( \rho \) with complex conjugation and \( W(\rho) \in C^\times \) has absolute value 1.

We do not prove this, but remark that the proof first establishes the result in the case that \( \rho \) is one-dimensional using the correspondence with Hecke characters alluded to above (there is a good theory in this case), and then uses the properties of the \( L \)-functions above and the Brauer Theorem (every character of a finite group \( G \) is a \( Z \)-linear combination of one-dimensional characters induced from subgroups of \( G \)) to handle the general case.
7 Chebotarev Density Theorem

Proposition 7.1. Let $L/K$ be a galois extension of number fields. Then

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq 1} \mathcal{L}(L/K, \chi, s)^{\chi(1)},$$

where the product ranges over all nontrivial irreducible characters of $\text{Gal}(L/K)$.

Proof. This follows from property 3 of the Artin $L$-functions, after observing that for a tower of fields $E \supset L \supset K$ with $G = \text{Gal}(E/K)$ and $H = \text{Gal}(E/L)$, the character of the induced representation $\text{Ind}_H^G \text{id}$ is $\sum \chi(1)\chi$, the sum being over all irreducible characters of $G$. ■

Corollary 7.2. For nontrivial $\chi$, we have $\zeta_L(L/K, \chi, 1) \neq 0$.

Proof. One shows that $\mathcal{L}(L/K, \chi, s)$ does not have a pole at $s = 1$ when $\chi \neq 1$, and then that both $\zeta_K$ and $\zeta_L$ have simple poles at $s = 1$. ■

Proposition 7.3. Let $K$ be a number field, and $m$ a modulus. Let $H_m \subseteq I^K_m$ be a subgroup containing $K_{m,1}$ (i.e. a subgroup of $C_m$) of index $h_m = [I^K_m : H_m]$. Then for any ideal class $\kappa$ in $I^K_m/H_m$, the set of prime ideals in $\kappa$ has Dirichlet density $1/h_m$.

Proof. Let $L$ be the ray class field of conductor $m$. Then the Artin $L$ function $\mathcal{L}(L/K, \chi, s)$ differs from the Hecke $L$-series

$$L(s, \chi) := \prod_p \frac{1}{1 - \chi(p)N_{K/Q}(p)^{-s}}$$

(where $\chi$ is a character of $I^K_m$ via the surjection $I^K_m \rightarrow G$) by finitely many factors that are nonzero at 1, so $L(1, \chi) \neq 0$. One uses this and the asymptotic relation

$$\log L(s, \chi) \sim \sum_{\kappa \in I^K_m/H_m} \sum_{p \in \kappa} \frac{\chi(p)}{N_{K/Q}(p)^s}$$

with the character orthogonality relations to complete the proof; it is a direct generalization of the proof of Dirichlet’s Theorem on primes in arithmetic progression. ■

Observe that as a corollary, we obtain Dirichlet’s Theorem by letting $L/K = Q(\zeta_m/\zeta)$ so $G = (Z/mZ)^\kappa \simeq I_Q^{m\infty}/K_{m\infty,1}$ and $h_m = [L : K] = \varphi(m)$.

Theorem 7.4. Let $L/K$ be a galois extension with galois group $G$. For each conjugacy class $c$ of $G$, let $S(c)$ denote the set of unramified primes $p \in \mathcal{O}_K$ whose image under the map $I_K \rightarrow G$ given by $p \mapsto \text{Frob}_p$ is $c$ (recall that $\text{Frob}_p$ is the conjugacy class of all $\text{Frob}_p$ with $p \in \text{Spec} \mathcal{O}_L$ lying over $p$). Then $S(c)$ has Dirichlet density $\#c/\#G$. 

10