1 Group Cohomology

1.1 Definitions

Let G be a group.

Definition 1.2. A G-module A is a $\mathbf{Z}[G]$-module, that is, an abelian group A together with a homomorphism of groups $G \to \operatorname{Aut} A$. A morphism of G-modules is a morphism as $\mathbf{Z}[G]$-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 $\mathbf{Z}$ the trivial G-action and define $\mathbf{Z}[G] \to \mathbf{Z}$ by $g \mapsto 1$ for all $g \in G$. Then $A^G = \operatorname{Hom}(Z, A)$ and $A_G = \mathbf{Z} \otimes_{\mathbf{Z}[G]} A$ so we can identify $H^r(G, A) = \operatorname{Ext}^r(\mathbf{Z}, A)$ and $H_r(G, A) = \operatorname{Tor}_r(\mathbf{Z}, A)$.

1.5 Functoriality

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

$$0 \to A' \to A \to A'' \to 0 \tag{1}$$

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 $A_G \to A'_G \to A'_{G'}$ 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 $H_r(G', A) \to H_r(G, A)$.

2 Local Class Field Theory

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

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

such that:

1. *If L/K is an unramified extension and $\pi \in K$ is any prime element, then $\phi_K(\pi)\big|_L = \mathrm{Frob}_{L/K}$.*
2. *For any finite abelian extension L/K, the map $a \mapsto \phi_K(a)\big|_L$ induces an isomorphism*

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

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

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

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

$$\varprojlim \mathbf{Q}_p^\times / \mathrm{Nm}(L^\times) \simeq \mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ab}}/\mathbf{Q}_p).$$

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

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

We conclude that $\mathbf{Q}_p^{\mathrm{ab}} = \mathbf{Q}_p(\zeta_{p^\infty}) \cdot \mathbf{Q}_p^{\mathrm{nr}}$, where $\mathbf{Q}_p^{\mathrm{nr}} = \varinjlim_{p \nmid n} \mathbf{Q}_p(\zeta_n)$

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

We now sketch the construction of the local Artin map ϕ_K.

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

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

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

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

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

Similarly, from

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

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

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

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

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

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

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

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 $G = \mathrm{Gal}(L/K)$. 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* $\mathrm{Res}(u_{L/K})$.

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*

$$H_T^r(G, \mathbf{Z}) \xrightarrow{\sim} H_T^{r+2}(G, C).$$

Corollary 2.11. *There is an isomorphism*

$$G^{\mathrm{ab}} = H_T^{-2}(G, \mathbf{Z}) \simeq H_T^0(G, L^\times) = K^\times / \mathrm{Nm}(L^\times).$$

Proof. Set $r = -2$ above. We must show that $G^{\mathrm{ab}} = H_T^{-2}(G, \mathbf{Z})$ and $H_T^0(G, L^\times) = K^\times / \mathrm{Nm}(L^\times)$. Recall that the Tate cohomology groups are defined as:

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

where I_G is the *augmentation ideal*, that is, the kernel of $\mathbf{Z}[G] \xrightarrow{g \mapsto 1} \mathbf{Z}$ (It is a free $\mathbf{Z}$-module generated by $(g-1)$ for $g \in G$) and $\mathrm{Nm}_G(m) = \sum_{g \in G} gm$. Thus, $H_T^0(G, L^\times) = K^\times / \mathrm{Nm}_G(L^\times) = K^\times / \mathrm{Nm}(L^\times)$ on remembering that $L^\times$ is a G-module under multiplication, so $\mathrm{Nm}_G = \mathrm{Nm}_{L/K}$. Now $H_T^{-2}(G, \mathbf{Z}) = H_1(G, \mathbf{Z})$. Using the exact sequence

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

we obtain

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

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

Now consider the map $G \to I_G/I_G^2$ defined by $g \mapsto (g-1)+I_G^2$. Since $gg'-1 \equiv g-1+g'-1 \bmod I_G^2$ 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 $\mathbf{Z}$-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 $H_1(G, \mathbf{Z}) \simeq I_G/I_G^2 \simeq G^{\mathrm{ab}}$. ■

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 $\mathbf{I}_K$ are the topological group with underlying set

$$\mathbf{I}_K = \{(a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for almost all } v\}$$

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

$$U(S, \epsilon) := \{(a_v) : |a_v - 1| < \epsilon \;\; v \in S,\; |a_v|_v = 1 \; v \notin S\}$$

form a base of opens of the identity.

We have an injection $K^\times \hookrightarrow \mathbf{I}_K : a \mapsto (a, a, a, \cdots)$ 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 $U(S, \epsilon) \cap K^\times = \{a \in K^\times : |a-1|_v < \epsilon,\; v \in S,\; |a|_v = 1,\; v \notin S\}$, which only contains $a = 1$ since by the product formula $\prod |a|_v = 1$.

Definition 3.2. The idele class group is the quotient $\mathbf{C}_K = \mathbf{I}_K/K^\times$.

Now let L/K be a finite extension.

Definition 3.3. Define the map $\mathrm{Nm} : \mathbf{I}_L \to \mathbf{I}_K$ by $\mathrm{Nm}((b_w)) = (\prod_{w|v} \mathrm{Nm}_{L_w/K_v} b_w)$. For $\alpha \in L$ we have $\mathrm{Nm}_{L/K} \alpha = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(\alpha)$ so the map Nm restricts to $\mathrm{Nm}_{L/K}$ on the image of $L^\times$.

Theorem 3.4. *There exists a unique continuous homomorphism $\phi_K : \mathbf{I}_K \to \mathrm{Gal}(K^{ab}/K)$ with the following properties:*

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

$$\begin{tikzcd} K_v \arrow[r, "\phi_v"] \arrow[d] & \mathrm{Gal}(L_w/K_v) \arrow[d, hook] \\ \mathbf{I}_K \arrow[r, "\phi_K|_L"] & \mathrm{Gal}(L/K) \end{tikzcd}$$

commutes.

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

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

Observe that $\mathbf{C}_K/\mathrm{Nm}(\mathbf{C}_L) \simeq \mathbf{I}_K/(K^\times \cdot \mathrm{Nm}(\mathbf{I}_L))$ so item 2 can be rephrased as an isomorphism $\phi_K : \mathbf{C}_K/\mathrm{Nm}(\mathbf{C}_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.

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

Remark 3.6. When K is a number field, every subgroup of $\mathbf{I}_K$ of finite index is open.

Proof sketch of Theorem 3.4. Let L/K be a finite abelian extension. Then when L_w/K_v is unramified and $a_v \in \mathcal{O}_v^\times$, we have $\phi_v(a_v) = 1$ (a little tricky to show this) so the product $\phi_{L/K}((a_v)) := \prod_v \phi_v(a_v)$ makes sense. Observe that requiring $\phi_{L/K}$ to be a continuous homomorphism with the compatibility condition in item 1 forces this definition on us. The properties of the local Artin maps show that when $L' \supseteq L$ we have $\phi_L = \phi_{L'}\big|_L$, so the maps $\phi_{L/K}$ are compatible with the inverse system L_α/L of all finite abelian extensions of K, and we obtain ϕ_K is the inverse limit of the $\phi_{L/K}$. The properties of the local Artin maps show that the diagram

$$\begin{tikzcd}
\mathbf{I}_{K'} \arrow[r, "\phi_{L/K'}"] \arrow[d, "\mathrm{Nm}"'] & \mathrm{Gal}(L/K') \arrow[d, hook] \\
\mathbf{I}_K \arrow[r, "\phi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

commutes for any $K^{ab} \supset L \supset K' \supset K$, so taking $K' = L$ shows that $\ker \phi_{L/K} \supset \mathrm{Nm}(\mathbf{I}_L)$, which contains an open subgroup of $\mathbf{I}_K$, so ϕ_K is continuous. This handles existence and continuity of ϕ_K. Proving item 2 is harder. ∎

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

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

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

$$W_m = \prod_{\substack{p \nmid m \\ p \text{ infinite}}} K_p^\times \times \prod_{p \mid m} W_m(p) \times \prod_{\substack{p \nmid m \\ p \text{ finite}}} \mathcal{O}_p^\times.$$

It is an open subgroup of

$$\mathbf{I}_m := \left(\prod_{p \nmid m} K_p^\times \times \prod_{p \mid m} W_m(p) \right) \cap \mathbf{I}.$$

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

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

Proof. By the definition of $K_{m,1}$, it is the kernel of $\mathbf{I}_m \to \mathbf{I}/K^\times$, thus there is an injection $\mathbf{I}_m/K_{m,1} \hookrightarrow \mathbf{I}/K^\times$. 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 $\mathbf{I}_m \to I^m \to C_m$ defined by*

$$(a_p) \mapsto \left[\prod_{p \text{ finite}} p^{\mathrm{ord}_p(a_p)} \right]$$

gives an isomorphism

$$\mathbf{I}_m/(K_{m,1} \cdot W_m) \simeq C_m.$$

Proof. This is just the kernel-cokernel sequence from

$$\begin{tikzcd} 0 \arrow[r] & K_{m,1} \arrow[r, "f"] & \mathbf{I}^m \arrow[r] \arrow[d] & \operatorname{coker} f \arrow[r] & 0 \\ 0 \arrow[r] & \ker g \arrow[r] & \mathbf{I}^m \arrow[r, "g"] & I^m \arrow[r] & 0 \end{tikzcd}$$

where one notes that $\ker g = W_m$. ■

Theorem 4.3. *Let G be a finite abelian group with the discrete topology and $\phi : \mathbf{I} \to G$ a continuous homomorphism such that $\phi(K^\times) = 1$. Then there exists a modulus m such that ϕ 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 ϕ kills W_m for some m. Since ϕ 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 $\mathbf{R}^\times$ or $\mathbf{C}^\times$, so by the definition of the W_m and the fact that the sets $U(S, \epsilon)$ form a system of nbds. of the identity, we see that ϕ 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 ϕ_K induces an isomorphism*

$$I_K^m/(K_{m,1} \cdot \mathrm{Nm}(I_L^m)) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Proof. We have a map $a \mapsto \phi_K(a)\big|_L$ from $\mathbf{I} \to \mathrm{Gal}(L/K)$ which by Theorem 4.3 induces a map $I^m \to \mathrm{Gal}(L/K)$ 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 $K^\times \cdot \mathrm{Nm}(\mathbf{I}_L)$ under the map

$$\mathbf{I}_K \to \mathbf{I}_K/K^\times \xrightarrow{\sim} \mathbf{I}_m/K_{m,1} \to I_K^m/K_{m,1},$$

where $\mathbf{I}_m \to I_K^m$ is given by $(a_v) \mapsto \prod_{v \text{ finite}} p_v^{\mathrm{ord}_v(a_v)}$. It is not hard to see that this image is $K_{m,1} \cdot \mathrm{Nm}(I_L^m)$. ■

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

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

Remark 4.6. The minimal modulus m for which ϕ_K induces an isomorphism $I_K^m/(K_{m,1}\cdot \mathrm{Nm}(I_L^m)) \xrightarrow{\sim} \mathrm{Gal}(L/K)$ 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 $I_K^m \to \mathrm{Gal}(L/K)$ takes a prime p to the Frobenius element $\mathrm{Frob}_p \in D(p) \subseteq \mathrm{Gal}(L/K)$, and we see that this description determines the map completely.

Example 4.8. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\zeta_m)$. Then $\mathrm{Gal}(L/K) \simeq (\mathbf{Z}/m\mathbf{Z})^\times$, with $a \in (\mathbf{Z}/m\mathbf{Z})^\times$ acting on ζ_m by $\zeta_m \mapsto \zeta_m^a$. If p is any prime of $\mathbf{Q}$ not ramifying in L (equiv. not dividing $m\infty$) then $\mathrm{Frob}_p \in (\mathbf{Z}/m\mathbf{Z})^\times$ must satisfy $\mathrm{Frob}_p(\zeta_m) \equiv \zeta_m^p \bmod \mathfrak{p}$ for a prime $\mathfrak{p}$ above p. But $\mathrm{Frob}_p(\zeta_m) = \zeta_m^r$ for some r and if $\mathfrak{p}|(\zeta_m^r - \zeta_m)$, then

$$p| \lim_{x\to 1} \prod_{0<a<m} (x - \zeta_m^a) = m,$$

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

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

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

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

Proof. By Theorem 4.4, there exists a modulus m with the artin map $I_{\mathbf{Q}}^m \to \mathrm{Gal}(L/K)$ definining an isomorphism $I_{\mathbf{Q}}^m/(\mathbf{Q}_{m,1}\cdot \mathrm{Nm}(I_L^m)) \simeq \mathrm{Gal}(L/\mathbf{Q})$. We may as well assume that $m = m\infty$, so by the above example we have an isomorphism $I_{\mathbf{Q}}^m/\mathbf{Q}_{m,1} \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) := G$. Letting H be the subgroup of $I_{\mathbf{Q}}^m/\mathbf{Q}_{m,1}$ corresponding to $\mathrm{Nm}(\mathbf{Q}_{m,1}\cdot I_L^m)$, we see that H is a normal subgroup of G and $G/H \simeq \mathrm{Gal}(L/\mathbf{Q})$. Now using the Galois correspondence and the uniqueness statement of Theorem 4.5, we see that L is a subfield of $\mathbf{Q}(\zeta_m)$ (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 $\left(\frac{p}{q}\right)$ by $\phi_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}}(q)(\sqrt{p}) = \left(\frac{p}{q}\right)\sqrt{p}$. Then*

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

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

6 Artin L-series

Let L/K be a galois extension of number fields and put $G = \mathrm{Gal}(L/K)$. Let (ρ, 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 $D_\mathfrak{p}/I_\mathfrak{p} \simeq \mathrm{Gal}(l/k)$, where l, k are the residue fields $k = K/p$ and $L = L/\mathfrak{p}$. As usual, Frob_p is an element of $D_\mathfrak{p}$ whose image under the surjective map $D_\mathfrak{p} \to \mathrm{Gal}(l/k)$ is a generator. As we know, the conjugacy class $\mathrm{Frob}_p := \{\mathrm{Frob}_\mathfrak{p},\ \mathfrak{p} \cap K = p\} \subseteq G$ 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

$$\det(1 - t\rho(\mathrm{Frob}_\mathfrak{p}))$$

of the endomorphism $\rho(\mathrm{Frob}_\mathfrak{p})$ acting on $V^{I_\mathfrak{p}}$ depends only on p.

Definition 6.1. Let L/K be a Galois extension as above with $\mathrm{Gal}(L/K) = G$, and let (ρ, V) be a finite dimensional representation of G. Then the Artin L-series is

$$\mathcal{L}(L/K, \rho, s) := \prod_{p \in \mathrm{Spec}\, \mathcal{O}_K} \det\left(1 - N_{K/\mathbf{Q}}(p)^{-s} \cdot \rho(\mathrm{Frob}_\mathfrak{p})\right)^{-1},$$

and where for each $p \in \mathrm{Spec}\, \mathcal{O}_K$ we make an arbitrary choice of $\mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_L$ lying over p.

Proposition 6.2. *The Artin L-series $\mathcal{L}(L/K, \rho, s)$ converges absolutely and uniformly for $\Re(s) > 1$.*

sketch of proof. The endomorphism $\rho(\mathrm{Frob}_\mathfrak{p})$ has finite order, so the roots of the characteristic polynomial are roots of unity; i.e. we have

$$\det\left(1 - N_{K/\mathbf{Q}}(p)^{-s} \cdot \rho(\mathrm{Frob}_\mathfrak{p})\right) = \prod_{i=1}^{d} (1 - \epsilon_i N_{K/Q}(p)^{-s}),$$

with $d = \dim V^{I_\mathfrak{p}} < n = \dim V$. Thus, we wish to investigate the convergence of

$$\sum_p \sum_{i=1^d} \frac{\epsilon_i}{q^s},$$

where $q = N_{K/\mathbf{Q}}(p)$. Convergence for $\Re(s) > 1$ is nor obvious. ■

Example 6.3. If ρ is the trivial representation, then we have

$$\mathcal{L}(L/K, \rho, s) = \prod_{p \in \mathrm{Spec}\, \mathcal{O}_K} \left(1 - N_{K/\mathbf{Q}}(p)^{-1}\right)^{-1} = \zeta_K(s),$$

which evidently does not depend on L.

Example 6.4. Suppose now that G is abelian, and let ρ be an irreducible (hence 1-dimensional) representation of G. Then we have an isomorphism $\mathbf{C}_K/\mathrm{Nm}(\mathbf{C}_L) \xrightarrow{\sim} G$ by CFT, so we can interpret ρ as a character of $\mathbf{C}_K$ that is trivial on $\mathrm{Nm}(C_L)$, 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 ρ 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.

Definition 6.5. A Hecke character is a continuous homomorphism $\chi : \mathbf{I}_K \to \mathbf{C}^\times$ that is trivial on $K^\times$. Equivalently, it is a continuous character of the idele class group $\mathbf{C}_K$.

Proposition 6.6. *For any Hecke character χ, there exists a modulus m such that χ induces a character $\overline{\chi} : C_m \to \mathbf{C}^\times$*

Indeed, referring to Prop. 4.2, it is enough to show that χ kills some W_m. But χ is continuous, so the kernel contains an open set, which must contain some W_m. Alternately, the image of $\prod_{p\nmid\infty} \mathcal{O}_p^\times$ is a compact totally disconnected subgroup of $\mathbf{C}^\times$, 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 ρ of $G(L/K)$ can be pulled back to a representation, also deonote ρ, 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 ρ, ρ' 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 ρ is a representation of $H = G(L/M)$ and we denote the induced representation of $G = G(L/K)$ by $\operatorname{Ind}_H^G \rho$, then

$$\mathcal{L}(L/M, \rho, s) = \mathcal{L}(L/K, \operatorname{Ind}_H^G \rho, s).$$

sketch of proof. Observe that under the surjective map $D_\mathfrak{p}/I_\mathfrak{p} \to D_p/I_p$ for $\mathfrak{p}$ a prime of E over $p \in \operatorname{Spec} \mathcal{O}_L$, the frobenius $\operatorname{Frob}_\mathfrak{p}$ maps to Frob_p. Now (1) follows from the definitions. As for (2), we remark that the charpoly of $\operatorname{Frob}_\mathfrak{p}$ acting on $V^{I_\mathfrak{p}} \oplus V'^{I_\mathfrak{p}}$ is the product of the characteristic polynomials of the same operator on each of $V^{I_\mathfrak{p}}$ and $V'^{I_\mathfrak{p}}$ (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*

$$\mathcal{L}_p(L/K, \rho, s) = \begin{cases} L_\mathbf{C}(s)^{\operatorname{Tr}\rho(1)} & p \text{ real} \\ L_\mathbf{R}(s)^{n^+} L_\mathbf{R}(s+1)^{n^-} & p \text{ real} \end{cases},$$

where

$$L_\mathbf{C}(s) = 2(2\pi)^{-s}\Gamma(s), \qquad L_\mathbf{R}(s) = \pi^{-s/2}\Gamma(s/2),$$

and for real p, we notice that $\operatorname{Frob}_\mathfrak{p}$ 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 $\mathcal{L}_\infty(L/K, \rho, s) = \prod_{p|\infty} \mathcal{L}_p(L/K, \rho, s)$. Then there esists 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 $\mathbf{C}$ 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 ρ with complex conjugation and $W(\rho) \in \mathbf{C}^\times$ has absolute value 1.

We do not prove this, but remark that the proof first establishes the result in the case that ρ 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 $\mathbf{Z}$-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 $\mathrm{Gal}(L/K)$.

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 $G = \mathrm{Gal}(E/K)$ and $H = \mathrm{Gal}(E/L)$, the character of the induced representation $\mathrm{Ind}_H^G \mathrm{id}$ is $\sum_\chi \chi(1)\chi$, the sum being over all irreducible characters of G. ■

Corollary 7.2. *For nontrivial χ, we have $\mathcal{L}(L/K, \chi, 1) \neq 0$.*

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 ζ_K and ζ_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 κ in I_K^m/H_m, the set of prime ideals in κ 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

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

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

$$\log L(s, \chi) \sim \sum_{\kappa \in I_K^m . K_{m,1}} \sum_{p \in \kappa} \frac{\chi(p)}{N_{K/\mathbf{Q}}(p)^s}$$

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 $L/K = \mathbf{Q}(\zeta_m/\zeta)$ so G is $(\mathbf{Z}/m\mathbf{Z})^\times \simeq I_{\mathbf{Q}}^{m\infty}/K_{m\infty,1}$ 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 $S(s)$ denote the set of unramified primes $p \in \mathcal{O}_K$ whose image under the map $I_K \to G$ given by $p \mapsto \mathrm{Frob}_p$ is c (recall that Frob_p is the conjugacy class of all $\mathrm{Frob}_\mathfrak{p}$ with $\mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_L$ lying over p). Then $S(c)$ has Dirichlet density $\#c/\#G$.*