24 Artin reciprocity in the unramified case

Let L/K be an abelian extension of number fields. In Lecture 22 we defined the norm group $T^{\mathfrak{m}}_{L/K} \coloneqq N_{L/K}(\mathcal{I}^{\mathfrak{m}}_L)\mathcal{R}^{\mathfrak{m}}_K$ (see Definition 22.27) that we claim is equal to the kernel of the Artin map $\psi^{\mathfrak{m}}_{L/K}\colon \mathcal{I}^{\mathfrak{m}}_K \to \mathrm{Gal}(L/K)$, provided that the modulus $\mathfrak{m}$ is divisible by the conductor of L (see Definition 22.24). In Theorem 22.29 we proved the inequality

$$[\mathcal{I}^{\mathfrak{m}}_K\colon T^{\mathfrak{m}}_{L/K}] \;\le\; [L:K] = [\mathcal{I}^{\mathfrak{m}}_K : \ker \psi^{\mathfrak{m}}_{L/K}] \tag{1}$$

(the equality follows from the surjectivity of the Artin map proved in Theorem 21.19). We now want to prove the reverse inequality

$$[\mathcal{I}^{\mathfrak{m}}_K\colon T^{\mathfrak{m}}_{L/K}] \ge [L:K]. \tag{2}$$

Which will show that the subgroups $T^{\mathfrak{m}}_{L/K}$ and $\ker \psi^{\mathfrak{m}}_{L/K}$ have the same index in $\mathcal{I}^{\mathfrak{m}}_K$. One can then apply an argument due to Artin (see [2, V.5.6]) to show that these equal index subgroups are in fact equal, yielding isomorphisms

$$\mathcal{I}^{\mathfrak{m}}_K/T^{\mathfrak{m}}_{L/K} \xrightarrow{\sim} \mathcal{I}^{\mathfrak{m}}/\ker^{\mathfrak{m}}_{L/K} \xrightarrow{\sim} \mathrm{Gal}(L/K). \tag{3}$$

This result is known as the *Artin reciprocity law*. Note that $T^{m}_{L/K}$ contains $\mathcal{R}^{\mathfrak{m}}_K$, so $\mathcal{I}^{\mathfrak{m}}_K/T^{\mathfrak{m}}_{L/K}$ is a quotient of the ray class group $\mathrm{Cl}^{\mathfrak{m}}_K \coloneqq \mathcal{I}^{\mathfrak{m}}_K/\mathcal{R}^{\mathfrak{m}}_K$, thus the Artin reciprocity law implies that for every finite abelian extension L/K, the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to a quotient of $\mathrm{Cl}^{\mathfrak{m}}_K$, for any modulus $\mathfrak{m}$ divisible by the conductor of L. Moreover, it tells us exactly which quotient: the one induced by the image of the norm map $\mathcal{I}^{\mathfrak{m}}_L \to \mathcal{I}^{\mathfrak{m}}_K$

In this lecture we will prove (2) for cyclic extensions L/K when the modulus $\mathfrak{m}$ is trivial (which forces L/K to be unramified).

24.1 Some cohomological calculations

If L/K is a finite Galois extension of global fields with Galois group G, then we can naturally view any of the abelian groups L, $L^\times$, $\mathcal{O}_L$, $\mathcal{O}_L^\times$, $\mathcal{I}_L$, $\mathcal{P}_L$ as G-modules.

When $G = \langle\sigma\rangle$ is cyclic we can compute the Tate cohomology groups of any of these G-modules A, and their associated Herbrand quotients $h(A)$. The Herbrand quotient is defined as the ratio of the cardinalities of

$$\hat{H}^0(A) \coloneqq \hat{H}^0(G,A) \coloneqq \operatorname{coker} \hat{N}_G = A^G/\operatorname{im}\hat{N}_G = \frac{A[\sigma-1]}{N_G(A)},$$
$$\hat{H}_0(A) \coloneqq \hat{H}_0(G,A) \coloneqq \ker \hat{N}_G = A_G[\hat{N}_G] = \frac{A[N_G]}{(\sigma-1)(A)},$$

if both are finite. We can also compute $\hat{H}_0(A) = \hat{H}^{-1}(A) \simeq \hat{H}^1(A) = H^1(A)$ as 1-cocycles modulo 1-coboundaries whenever it is convenient to do so. In the interest of simplifying the notation we omit G from our notation whenever it is clear from context.

For the multiplicative groups $\mathcal{O}_L^\times, L^\times, \mathcal{I}_L, \mathcal{P}_L$, the norm element $N_G \coloneqq \sum_{i=1}^n \sigma^i$ corresponds to the action of the field norm $\mathrm{N}_{L/K}$ and ideal norm $N_{L/K}$ that we have previously defined, provided that we identify the codomain of the norm map with a subgroup of its domain. For the groups $L^\times$ and $\mathcal{O}_L^\times$ this simply means identifying $K^\times$ and $\mathcal{O}_K^\times$ as subgroups via inclusion. For the ideal group $\mathcal{I}_K$ we have a natural extension map $\mathcal{I}_K \hookrightarrow \mathcal{I}_L$ defined by

Lecture by Andrew V. Sutherland

$I \mapsto I\mathcal{O}_L$ that restricts to a map $\mathcal{P}_K \hookrightarrow \mathcal{P}_L$.[1] Under this convention taking the norm of an element of $\mathcal{I}_L$ that is (the extension of) an element of $\mathcal{I}_K$ corresponds to the map $I \mapsto I^{\#G}$, as it should, and $\mathcal{I}_K$ is a subgroup of the G-invariants $\mathcal{I}_L^G$.[2]

When A is multiplicative, the action of $\sigma - 1$ on $a \in A$ is $(\sigma-1)(a) = \sigma(a)/a$, but we will continue to use the notation $(\sigma-1)(A)$ and $A[\sigma-1]$ to denote the image and kernel of this action. Conversely, when A is additive, the action of N_G corresponds to the trace map, not the norm map. In order to lighten the notation, in this lecture we use N to denote both the (relative) field norm $\mathrm{N}_{L/K}$ and the ideal norm $N_{L/K}$.

Theorem 24.1. *Let L/K be a cyclic Galois extension with Galois group $G \coloneqq \mathrm{Gal}(L/K)$.*

(i) *$\hat{H}^0(L)$ and $\hat{H}_0(L)$ are both trivial.*

(ii) *$\hat{H}^0(L^\times) \simeq K^\times/N(L^\times)$ and $\hat{H}_0(L^\times)$ is trivial.*

Proof. (i) The trace map from L to K is not identically zero (by Theorem 5.20, since L/K is separable), so it must be surjective, since it is a K-linear transformation whose codomain has dimension 1. Thus $N_G(L) = T(L) = K$ and $\hat{H}^0(L) = L^G/N_G(L) = K/K$ is trivial. By the normal basis theorem, we can fix $\gamma \in L$ so that $(\gamma, \sigma(\gamma), \ldots, \sigma^{n-1}(\gamma))$ is a K-basis for $L \simeq K^n$ on which σ acts on vectors in K^n as a cyclic shift. For any $a \in K^n$ with trace zero, we may define $b \in K^n$ by $b_i = -\sum_{j\le i} a_j$ so that $\sigma(b) - b = (b_n - b_1, b_1 - b_2, \ldots, b_{n-1} - b_n) = a$. It follows that $L[N_G] = (\sigma-1)(L)$ and $\hat{H}_0(L)$ is trivial.

(ii) We have $\hat{H}^0(L^\times) = (L^\times)^G/N_G(L^\times) = K^\times/N(L^\times)$. The argument that $\hat{H}_0(L^\times)$ is trivial is as in (i): given $a \in K^n$ with norm one we define $b \in K^n$ by $b_i \coloneqq (\prod_{j\le i} a_i)^{-1}$ so that $\sigma(b)/b = a$. It follows that $L^\times[N_G] = (\sigma-1)(L^\times)$ and $\hat{H}_0(L^\times)$ is trivial. □

Remark 24.2. If one replaces $\hat{H}_0$ with H^1 in Theorem 24.1 (note that $\hat{H}_0 = H^1$ in the cyclic case by Theorem 23.37) the result holds for arbitrary Galois extensions, as shown by Noether [4], but the proof then involves showing that every 1-cocycle is a 1-coboundary.

Corollary 24.3 (Hilbert Theorem 90). *Let L/K be a finite cyclic extension with Galois group $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Then $N(\alpha) = 1$ if and only if $\alpha = \beta/\sigma(\beta)$ for some $\beta \in L^\times$.*

Our next goal is to compute the Herbrand quotient of $\mathcal{O}_L^\times$ (in the case that L/K is a finite cyclic extension of number fields). For this we will apply a variant of Dirichlet's unit theorem due to Herbrand, but first we need to discuss infinite places of number fields.

If L/K is a Galois extension of global fields, the Galois group $\mathrm{Gal}(L/K)$ acts on the set of places w of L via the action $w \mapsto \sigma(w)$, where $\sigma(w)$ is the equivalence class of the absolute value defined by $\|\alpha\|_{\sigma(w)} \coloneqq \|\sigma(\alpha)\|_w$. This action permutes the places w lying above a given place v of K; if v is a finite place corresponding to a prime $\mathfrak{p}$ of K, this is just the usual action of the Galois group on the set $\{\mathfrak{q}|\mathfrak{p}\}$.

Definition 24.4. Let L/K be a Galois extension of global fields and let w be a place of L. The *decomposition group* of w is its stabilizer in $\mathrm{Gal}(L/K)$:

$$D_w \coloneqq \{\sigma \in \mathrm{Gal}(L/K) : \sigma(w) = w\}.$$

If w corresponds to a prime $\mathfrak{q}$ of $\mathcal{O}_L$ then $D_w = D_{\mathfrak{q}}$ is also the decomposition group of $\mathfrak{q}$.

[1] The induced map $\mathrm{Cl}_K \to \mathrm{Cl}_L$ need not be injective; extensions of non-principal ideals may be principal. Indeed, when L is the Hilbert class field every $\mathcal{O}_K$-ideal extends to a principal $\mathcal{O}_L$-ideal; this was conjectured by Hilbert and took over 30 years to prove. You will get a chance to prove it on Problem Set 10.

[2] Note that $\mathcal{I}_L^G = \mathcal{I}_K$ only when L/K is unramified; see Lemma 24.9 below.

Now let L/K be a Galois extension of number fields. If we write $L \simeq \mathbb{Q}[x]/(f)$ then we have a one-to-one correspondence between embeddings of L into $\mathbb{C}$ and roots of f in $\mathbb{C}$. Each embedding of L into $\mathbb{C}$ restricts to an embedding of K into $\mathbb{C}$, and this induces a map that sends each infinite place w of L to the infinite place v of K that w extends. This map may send a complex place to a real place; this occurs when a pair of distinct complex conjugate embeddings of L restrict to the same embedding of K (which must be a real embedding). In this case we say that the place v (and w) is *ramified* in the extension L/K, and define the *ramification index* $e_v := 2$ when this holds (and put $e_v := 1$ otherwise). This notation is consistent with our notation $e_v := e_{\mathfrak{p}}$ for finite places v corresponding to primes $\mathfrak{p}$ of K. Let us also define $f_v := 1$ for $v|\infty$ and put $g_v := \#\{w|v\}$ so that the following formula generalizing Corollary 7.5 holds for all places v of K:

$$e_v f_v g_v = [L : K].$$

Definition 24.5. For a Galois extension of number fields L/K we define the integers

$$e_0(L/K) := \prod_{v\nmid\infty} e_v, \qquad e_\infty(L/K) := \prod_{v|\infty} e_v, \qquad e(L/K) := e_0(L/K)e_\infty(L/K).$$

Let us now write $L \simeq K[x]/(g)$. Each embedding of K into $\mathbb{C}$ gives rise to $[L : K]$ distinct embeddings of L into $\mathbb{C}$ that extend it, one for each root of g (use the embedding of K to view g as a polynomial in $\mathbb{C}[x]$, then pick a root of g in $\mathbb{C}$). The transitive action of $\mathrm{Gal}(L/K)$ on the roots of g induces a transitive action on these embeddings and their corresponding places. Thus for each infinite place v of K the Galois group acts transitively on $\{w|v\}$, and either every place w above v is ramified (this can occur only when v is real and $[L : K]$ is divisible by 2), or none are. It follows that each unramified place v of K has $[L : K]$ places w lying above it, each with trivial decomposition group D_w, while each ramified (real) place v of K has $[L : K]/2$ (complex) places w lying above it, each with decomposition group D_w of order 2 (its non-trivial element corresponds to complex conjugation in the corresponding embeddings), and the D_w are all conjugate.

Theorem 24.6 (Herbrand unit theorem)**.** *Let L/K be a Galois extension of number fields. Let $w_1, \ldots w_{r+s}$ be the archimedean places of L, where r and s are the number of real and complex places of L, respectively. There exist units $\varepsilon_1, \ldots, \varepsilon_{r+s} \in \mathcal{O}_L^\times$ such that*

(i) *$\sigma(\varepsilon_i) = \varepsilon_j$ if and only if $\sigma(w_i) = w_j$, for all $\sigma \in \mathrm{Gal}(L/K)$;*

(ii) *The set $\{\varepsilon_1, \ldots, \varepsilon_{r+s}\}$ generates a finite index subgroup of $\mathcal{O}_L^\times$;*

(iii) *$\prod_i \varepsilon_i = 1$, and every relation among the ε_i is a multiple of this one.*

Proof. The theorem holds with $\varepsilon = 1$ if $r+s = 1$ so assume $r+s > 1$. Pick $u_1, \ldots, u_{r+s} \in \mathcal{O}_L^\times$ such that $\|u_i\|_{w_j} < 1$ for $i \neq j$ and $\|u_i\|_{w_i} > 1$. Such u_i may be constructed as in the proof of Dirichlet's unit theorem: fix $B > (\frac{2}{\pi})^s\sqrt{|D_L|}$, fix generators γ_k for the principal $\mathcal{O}_L$ ideals of absolute norm at most B, let $M = (r+s)\max_{j\neq i,k} \|\gamma_k\|_{w_j}$, define an Arakelov divisor c of size B with $c_v = 1$ for $v \nmid \infty$ and $c_{w_j} = 1/M$ for $j \neq i$, use Proposition 15.9 to obtain $a_i \in \mathcal{O}_L$ with $\|a_i\|_{w_j} \leq 1/M$ for $j \neq i$ and $N(a_i) \leq B$, and take $u_i = a_i/\gamma \in \mathcal{O}_L^\times$, where γ is our chosen generator for (a_i).

Now let $\alpha_i := \prod_{\sigma\in D_{w_i}} \sigma(u_i) \in \mathcal{O}_L^\times$. We have

$$\|\alpha_i\|_{w_i} = \prod_{\sigma\in D_{w_i}} \|\sigma(u_i)\|_{w_i} = \prod_{\sigma\in D_{w_i}} \|u_i\|_{\sigma(w_i)} = \prod_{\sigma\in D_{w_i}} \|u_i\|_{w_i} > 1,$$

and for $j \neq i$ we have

$$\|\alpha_i\|_{w_j} = \prod_{\sigma\in D_{w_i}} \|\sigma(u_i)\|_{w_j} = \prod_{\sigma\in D_{w_i}} \|u_i\|_{\sigma(w_j)} < 1,$$

since $\sigma \in D_{w_i}$ fixes w_i and permutes the w_j with $j \neq i$; note that α_i is fixed by $\sigma \in D_{w_i}$.

The Galois group $G := \mathrm{Gal}(L/K)$ partitions the w_i into m orbits, where m is the number of archimedean place of v. Let us index the w_i and α_i so that $w_1, \ldots, w_m$ lie in distinct orbits. We then have $w_j = \sigma_j(w_{i(j)})$ for a unique $i(j) \leq m$, with σ_j in a unique coset of $D_{w_{i(j)}}$; let us fix a choice of $\sigma_j \in \sigma_j D_{w_{i(j)}}$. We now define $\beta_j := \sigma_j(\alpha_{i(j)})$; the value of β_j does not depend on our choice of σ_j because α_i is fixed by D_{w_i}. The β_j satisfy (i), and Lemma 24.7 below implies that they also satisfy (ii), since they are a permutation of the α_i.

We must have $\prod_i \beta_i^{n_i} = 1$ for some tuple $(n_1, \ldots, n_{r+s}) \in \mathbb{Z}^{r+s}$, since $\mathcal{O}_L^\times$ has rank $r+s-1$. The set of all such tuples spans a rank-1 submodule of $\mathbb{Z}^{r+s}$ from which we may choose a generator $(n_1, \ldots, n_{r+s})$. If now put $\varepsilon_i := \beta_i^{n_i}$ then the ε_i satisfy (iii). The ε_i also satisfy (ii), since the ε_i generate a finite index subgroup of the group generated by the β_i. We must have $n_i = n_j$ whenever w_i and w_j lie in the same Galois orbit (otherwise applying some $\sigma \in G$ to $\prod_i \beta_i^{n_i} = 1$ would yield a relation that is not a multiple of the one we have). It follows that the ε_i satisfy (i), since the β_i do. □

Lemma 24.7. *Let K be a number field with archimedean places $v_1, \ldots, v_{r+s}$. Any units $u_1, \ldots u_{r+s} \in \mathcal{O}_L^\times$ that satisfy $\|u_i\|_{v_j} < 1$ for $j \neq i$ generate a finite index subgroup of $\mathcal{O}_K^\times$.*

Proof. Recall $\mathrm{Log}\colon K_\mathbb{R}^\times \to \mathbb{R}^{r+s}$ given by $(\alpha_v) \mapsto (\log \|\alpha_v\|_v)$ from the proof of Dirichlet's Unit Theorem (see Proposition 15.11). The restriction to $\mathcal{O}_K^\times \subseteq K^\times \hookrightarrow K_\mathbb{R}$ has finite kernel, so it suffices to to show $\mathrm{Log}(\{u_i\})$ generates a finite index subgroup of $\mathrm{Log}(\mathcal{O}_K^\times) \simeq \mathbb{Z}^{r+s-1}$.

Let $e_i = (e_{i1}, e_{i2}, \ldots, e_{i(r+s)}) = \mathrm{Log}(u_i)$. It suffices to show that $e_1, \ldots, e_{r+s-1}$ are $\mathbb{R}$-linearly independent; they then span a free $\mathbb{Z}$-module of rank $r+s-1$ in $\mathrm{Log}(\mathcal{O}_K^\times) \simeq \mathbb{Z}^{r+s-1}$, which must have finite index. Consider the $(r+s-1)\times(r+s-1)$ matrix $M = (e_{ij})$. It has positive diagonal entries, negative nondiagonal entries, and positive row sums ($\sum_{j=1}^{r+s} e_{ij} = 0$ and $e_{i(r+s)} < 0$ imply $\sum_{j=1}^{r+s-1} e_{ij} > 0$). Suppose that $Mx = 0$ has a nonzero solution with $x_1 \geq \max_j |x_j| > 0$ (such a solution can be obtained from any nonzero solution by re-indexing columns and negating x if needed). We have

$$\sum_j m_{1j}x_j = m_{11}x_1 - \sum_{j>1} |m_{1j}|x_j \geq m_{11}x_1 - \sum_{j>1} |m_{1j}|x_1 = x_1 \sum_j m_{1j} > 0,$$

since $\sum_j m_{1j} > 0$, but this contradicts $Mx = 0$. □

Theorem 24.8. *Let L/K be an extension of number fields with cyclic Galois group $G = \langle\sigma\rangle$. The Herbrand quotient of the G-module $\mathcal{O}_L^\times$ is*

$$h(\mathcal{O}_L^\times) = \frac{e_\infty(L/K)}{[L:K]}.$$

Proof. Let $\varepsilon_1, \ldots, \varepsilon_{r+s} \in \mathcal{O}_L^\times$ be as in Theorem 24.6, and let A be the subgroup of $\mathcal{O}_L^\times$ they generate, viewed as a G-module. By Corollary 23.48, $h(A) = h(\mathcal{O}_L^\times)$ if either is defined, since A has finite index in $\mathcal{O}_L^\times$, so we will compute $h(A)$.

For each field embedding $\phi\colon K \hookrightarrow \mathbb{C}$, let E_ϕ be the free $\mathbb{Z}$-module with basis $\{\varphi|\phi\}$ consisting of the $n := [L:K]$ embeddings $\varphi\colon L \hookrightarrow \mathbb{C}$ with $\varphi_{|_K} = \phi$, equipped with the

G-action given by $\sigma(\varphi) := \varphi \circ \sigma$. Let v be the infinite place of K corresponding to ϕ, and let A_v be the free $\mathbb{Z}$-module with basis $\{w|v\}$ consisting of places of L that extend v, equipped with the G-action given by the action of G on $\{w|v\}$. Let $\pi\colon E_\phi \to A_v$ be the G-module morphism sending each embedding $\varphi|\phi$ to the corresponding place $w|v$. Let $m := \#\{w|v\}$ and define $\tau := \sigma^m$; then τ is either trivial or has order 2, and in either case generates the decomposition group D_w for all $w|v$ (since G is abelian). We have an exact sequence

$$0 \to \ker\pi \longrightarrow E_\phi \xrightarrow{\pi} A_v \to 0,$$

with $\ker\pi = (\tau - 1)E_\phi$. If v is unramified then $\ker\pi = 0$ and $h(A_v) = h(E_\phi) = 1$, since $E_\phi \simeq \mathbb{Z}[G] \simeq \mathrm{Ind}^G(\mathbb{Z})$, by Lemma 23.43. Otherwise, order $\{w|v\} = \{w_0, \ldots, w_{m-1}\}$ and $\{\varphi|\phi\} = \{\varphi_0, \ldots, \varphi_{n-1}\}$ so that $w_i = \{\varphi_i, \varphi_{m+i}\}$. We then have

$$\ker\pi = (\tau - 1)E_\phi = \left\{\sum_{0\le i<m} a_i(\varphi_i - \varphi_{m+i}) : a_i \in \mathbb{Z}\right\},$$

which is annihilated by N_G, and $\ker\pi[\sigma - 1] = (\ker\pi)^G = 0$, since $\tau = \sigma^m$ acts as -1, so $h^0(\ker\pi) = 1$. Now $(\sigma - 1)(\ker\pi) = \{\sum a_i(\varphi_i - \varphi_{m+i}) : a_i \in \mathbb{Z} \text{ with } \sum a_i \equiv 0 \bmod 2\}$ has index 2 in $\ker\pi[N_G] = \ker\pi$, so $h_0(\ker\pi) = 2$ and $h(\ker\pi) = 1/2$. Corollary 23.41 implies $h(A_v) = h(E_\phi)/h(\ker\pi) = 2$, and in every case we have $h(A_v) = e_v$, where $e_v \in \{1, 2\}$ is the ramification index of v.

Now consider the exact sequence of G-modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow \bigoplus_{v|\infty} A_v \xrightarrow{\psi} A \longrightarrow 1$$

where ψ sends each infinite place $w_1, \ldots, w_{r+s}$ of L to the corresponding $\varepsilon_1, \ldots, \varepsilon_{r+s} \in A$ given by Theorem 24.6. The kernel of ψ is the trivial G-module $(\sum_i w_i)\mathbb{Z} \simeq \mathbb{Z}$, since we have $\psi(\sum_i w_i) = \prod_i \varepsilon_i = 1$ and no other relations among the ε_i, by Theorem 24.6. We have $h(\mathbb{Z}) = \#G = [L : K]$, by Corollary 23.46, and $h(\bigoplus A_v) = \prod h(A_v) = \prod e_v$, by Corollary 23.42, so $h(A) = e_\infty(L/K)/[L : K]$. ∎

Lemma 24.9. *Let L/K be a cyclic extension of global fields with Galois group $\langle\sigma\rangle$. We have $h_0(\mathcal{I}_L) = 1$ and $h(\mathcal{I}_L) = h^0(\mathcal{I}_L) = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$.*

Proof. Let $I \in \mathcal{I}_L$ and suppose $N(I) = O_K$. For each prime $\mathfrak{q}|\mathfrak{p}$ we have $N(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{p}}$ (by Theorem 6.10), and $N(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{v_\mathfrak{q}(I)}) = \mathfrak{p}^{f_\mathfrak{p}\sum_{\mathfrak{q}|\mathfrak{p}} v_\mathfrak{q}(I)} = \mathcal{O}_K$, equivalently, $\sum_{\mathfrak{q}|\mathfrak{p}} v_\mathfrak{q}(I) = 0$. Order $\{\mathfrak{q}|\mathfrak{p}\}$ as $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ so that $\mathfrak{q}_{i+1} = \sigma(\mathfrak{q}_i)$ and $\mathfrak{q}_1 = \sigma(\mathfrak{q}_g)$. Let $n_i := v_{\mathfrak{q}_i}(I)$ and define $m_i := -\sum_{j\le i} n_j$ and $J_\mathfrak{p} := \prod \mathfrak{q}_i^{m_i}$ so that

$$\sigma(J_\mathfrak{p})/J_\mathfrak{p} = \mathfrak{q}_1^{m_g - m_1}\mathfrak{q}_2^{m_1 - m_2}\cdots\mathfrak{q}_g^{m_{g-1} - m_g} = \mathfrak{q}_1^{n_1}\cdots\mathfrak{q}_g^{n_g} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{v_\mathfrak{q}(I)}.$$

It follows that $I = \sigma(J)/J$ where $J := \prod_\mathfrak{p} J_\mathfrak{p}$, thus $\mathcal{I}_L[N_G] = (\sigma - 1)(\mathcal{I}_L)$ and $h_0(\mathcal{I}_L) = 1$.

We have $I \in \mathcal{I}_L^G \Leftrightarrow v_{\sigma(\mathfrak{q})}(I) = v_\mathfrak{q}(I)$ for all primes $\mathfrak{q} \in \mathcal{I}_L$. If we put $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K$, then $I \in \mathcal{I}_L^G$ if and only if $v_\mathfrak{q}(I)$ is constant on $\{\mathfrak{q}|\mathfrak{p}\}$ for all primes $\mathfrak{p} \in \mathcal{I}_K$. It follows that $\mathcal{I}_L^G$ consists of all products of ideals of the form $(\mathfrak{p}\mathcal{O}_L)^{1/e_\mathfrak{p}}$. Therefore $[\mathcal{I}_L^G : \mathcal{I}_K] = e_0(L/K)$ and $h(\mathcal{I}_L) = h^0(\mathcal{I}_L) = [\mathcal{I}_L^G : N(\mathcal{I}_L)] = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$ as claimed. ∎

Recall that for a modulus $\mathfrak{m}$ of K and an extension of global fields L/K we use $\mathcal{I}_L^{\mathfrak{m}}$ to denote the group of fractional ideals coprime to $\mathfrak{m}\mathcal{O}_L$.

Corollary 24.10. *Let L/K be a cyclic extension of global fields and let $\mathfrak{m}$ be a modulus for K divisible by all the primes that ramify in L. Then $h(\mathcal{I}_L^{\mathfrak{m}}) = [\mathcal{I}_K^{\mathfrak{m}} : N(\mathcal{I}_L^{\mathfrak{m}})]$.*

Proof. The proof of Lemma 24.9 still applies if we replace $\mathcal{I}_L$ with $\mathcal{I}_L^{\mathfrak{m}}$ and $\mathcal{I}_K$ with $\mathcal{I}_K^{\mathfrak{m}}$. □

Theorem 24.11 (Ambiguous class number formula). *Let L/K be a cyclic extension of number fields with Galois group G. The G-invariant subgroup of the G-module Cl_L has cardinality*

$$\#\mathrm{Cl}_L^G = \frac{e(L/K)\#\mathrm{Cl}_K}{n(L/K)\,[L:K]},$$

where $n(L/K) := [\mathcal{O}_K^\times : N(L^\times)\cap\mathcal{O}_K^\times] \in \mathbb{Z}_{\geq 1}$.

Proof. The ideal class group Cl_L is the quotient of $\mathcal{I}_L$ by its subgroup $\mathcal{P}_L$ of principal fractional ideals. We thus have a short exact sequence of G-modules

$$1 \longrightarrow \mathcal{P}_L \longrightarrow \mathcal{I}_L \longrightarrow \mathrm{Cl}_L \longrightarrow 1.$$

The corresponding long exact sequence in (standard) cohomology begins

$$1 \longrightarrow \mathcal{P}_L^G \longrightarrow \mathcal{I}_L^G \longrightarrow \mathrm{Cl}_L^G \longrightarrow H^1(\mathcal{P}_L) \longrightarrow 1,$$

since $H^1(\mathcal{I}_L) \simeq \hat{H}_0(\mathcal{I}_L)$ is trivial, by Lemma 24.9. Therefore

$$\#\mathrm{Cl}_L^G = [\mathcal{I}_L^G : \mathcal{P}_L^G]\; h_0(\mathcal{P}_L). \tag{4}$$

Using the inclusions $\mathcal{P}_K \subseteq \mathcal{P}_L^G \subseteq \mathcal{I}_L^G$ we can rewrite the first factor on the RHS as

$$[\mathcal{I}_L^G : \mathcal{P}_L^G] = \frac{[\mathcal{I}_L^G : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{[\mathcal{I}_L^G : \mathcal{I}_K][\mathcal{I}_K : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{e_0(L/K)\#\mathrm{Cl}_K}{[\mathcal{P}_L^G : \mathcal{P}_K]}, \tag{5}$$

where $[\mathcal{I}_L^G : \mathcal{I}_K] = e_0(L/K)$ follows from the proof of Lemma 24.9.

We now consider the short exact sequence

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{\alpha\mapsto(\alpha)} \mathcal{P}_L \longrightarrow 1.$$

The corresponding long exact sequence in cohomology begins

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow \mathcal{P}_L^G \longrightarrow H^1(\mathcal{O}_L^\times) \longrightarrow 1 \longrightarrow H^1(\mathcal{P}_L) \longrightarrow H^2(\mathcal{O}_L^\times) \longrightarrow H^2(L^\times), \tag{6}$$

since $H^1(L^\times) \simeq \hat{H}_0(L^\times)$ is trivial, by Lemma 24.9. We have $K^\times/\mathcal{O}_K^\times \simeq \mathcal{P}_K$, thus

$$[\mathcal{P}_L^G : \mathcal{P}_K] = h_0(\mathcal{O}_L^\times) = \frac{h^0(\mathcal{O}_L^\times)}{h(\mathcal{O}_L^\times)} = \frac{h^0(\mathcal{O}_L^\times)\,[L:K]}{e_\infty(L/K)},$$

by Theorem 24.8. Combining this identity with (4) and (5) yields

$$\#\mathrm{Cl}_L^G = \frac{e(L/K)\#\mathrm{Cl}_K}{[L:K]} \cdot \frac{h_0(\mathcal{P}_L)}{h^0(\mathcal{O}_L^\times)}. \tag{7}$$

We can write the second factor on the RHS using the second part of the long exact sequence in (6). Recall that $H^2(\bullet) = \hat{H}^2(\bullet) = \hat{H}^0(\bullet)$, by Theorem 23.37, thus

$$H^1(\mathcal{P}_L) \simeq \ker\Big(\hat{H}^0(\mathcal{O}_L^\times) \to \hat{H}^0(L^\times)\Big) \simeq \ker\big(\mathcal{O}_K^\times/N(\mathcal{O}_L^\times) \to K^\times/N(L^\times)\big),$$

so $h_0(\mathcal{P}_L) = [\mathcal{O}_K^\times \cap N(L^\times) : N(\mathcal{O}_L^\times)]$. We have $h^0(\mathcal{O}_L^\times) = [\mathcal{O}_K^\times : N(\mathcal{O}_L^\times)]$, thus

$$\frac{h^0(\mathcal{O}_L^\times)}{h_0(\mathcal{P}_L)} = [\mathcal{O}_K^\times : N(L^\times) \cap \mathcal{O}_K^\times] = n(L/K),$$

and plugging this into (7) yields the desired formula. □

Remark 24.12. If L/K is a quadratic extension then $\mathrm{Cl}_L^G = \mathrm{Cl}_K[2]$. To see this, note that if $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ has order 2 then $I\sigma(I) = N(I) \in \mathcal{P}_K$ for all $I \in \mathcal{I}_K$, thus $[I]^{-1} = [\sigma(I)] = \sigma([I])$ in Cl_K, and we have $\sigma([I]) = [I]^{-1} = [I]$ if and only if $[I] \in \mathrm{Cl}_K[2]$. This fact can be used to prove quadratic reciprocity [3, §9].

Remark 24.13. When $K = \mathbb{Q}$ and L is an imaginary quadratic field of discriminant D, the ambiguous class number formula implies that the rank of the 2-Sylow subgroup of the class group of L is one less than the number of prime divisors of D: we have $\#\mathrm{Cl}_L^G = e_0(L/K)/2$, since $\#\mathrm{Cl}_\mathbb{Q} = 1$ and $e_\infty(L/K) = [L:K] = n(L/K) = 2$.

24.2 Norm index equality for unramified extensions

We first record an elementary lemma.

Lemma 24.14. *Let $f : A \to C$ be a homomorphism of abelian groups and let B be a subgroup of A containing the kernel of f. Then $A/B \simeq f(A)/f(B)$.*

Proof. Apply the snake lemma to the commutative diagram and consider the cokernels.

$$\begin{array}{ccccccccc} & & \ker f & \hookrightarrow & B & \xrightarrow{f} & f(B) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker f & \hookrightarrow & A & \xrightarrow{f} & f(A) & \longrightarrow & 0. \end{array}$$

□

In the following theorem it is crucial that the extension L/K is completely unramified, including at all infinite places of K; to emphasize this, let us say that an extension of number fields L/K is *totally unramified* if $e(L/K) = 1$.

Theorem 24.15. *Let L/K be a totally unramified cyclic extension of number fields. Then*

$$[\mathcal{I}_K : N(\mathcal{I}_L)\mathcal{P}_K] \geq [L : K].$$

Proof. We have

$$[\mathcal{I}_K : N(\mathcal{I}_L)\mathcal{P}_K] = \frac{[\mathcal{I}_K : \mathcal{P}_K]}{[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K]} = \frac{\#\mathrm{Cl}_K}{[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K]}.$$

The denominator on the RHS can be rewritten as

$$\begin{aligned}
[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K] &= [N(\mathcal{I}_L) : N(\mathcal{I}_L)\cap\mathcal{P}_K] && \text{(2nd isomorphism theorem)}\\
&= [\mathcal{I}_L : N^{-1}(\mathcal{P}_K)] && \text{(Lemma 24.14)}\\
&= [\mathcal{I}_L/\mathcal{P}_L : N^{-1}(\mathcal{P}_K)/\mathcal{P}_L] && \text{(3rd isomorphism theorem)}\\
&= [\mathrm{Cl}_L : \mathrm{Cl}_L[N_G]]\\
&= \#N_G(\mathrm{Cl}_L).
\end{aligned}$$

Now $h^0(\mathrm{Cl}_L) = [\mathrm{Cl}_L^G : N_G(\mathrm{Cl}_L)]$, and applying Theorem 24.11 yields

$$[\mathcal{I}_K : N(\mathcal{I}_L)\mathcal{P}_K] = \frac{\#\mathrm{Cl}_K \cdot h^0(\mathrm{Cl}_L)}{\#\mathrm{Cl}_L^G} = \frac{h^0(\mathrm{Cl}_L)n(L/K)[L:K]}{e(L/K)} \geq [L:K], \tag{8}$$

since $e(L/K)=1$, and $h^0(\mathrm{Cl}_L)$, $n(L/K)\geq 1$. □

The norm index inequality Theorem 22.29 implies that for totally unramified cyclic extensions of number fields L/K we have the equality

$$[\mathcal{I}_K : N(\mathcal{I}_L)\mathcal{P}_K] = [L:K],$$

so we must have $n(L/K) = [\mathcal{O}_K^\times : N(L^\times)\cap\mathcal{O}_K^\times] = 1$ and $h^0(\mathrm{Cl}_L)=1$, since (8) is an equality with $e(L/K)=1$.

Corollary 24.16. *Let L/K be a totally unramified cyclic extension of number fields. Then $\#\mathrm{Cl}_L^G = \#\mathrm{Cl}_K/[L:K]$ and the Tate cohomology groups of Cl_L are all trivial.*

Proof. We have $n(L/K) = h^0(\mathrm{Cl}_L) = e(L/K) = 1$, so $\#\mathrm{Cl}_L^G = \#\mathrm{Cl}_K/[L:K]$ by Theorem 24.11. We also have $h(\mathrm{Cl}_L) = h^0(\mathrm{Cl}_L)/h_0(\mathrm{Cl}_L) = 1$, since Cl_L is finite, by Lemma 23.43, so $h_0(\mathrm{Cl}_L)=1$. Thus $\hat{H}^0(\mathrm{Cl}_L)$ and $\hat{H}_0(\mathrm{Cl}_L)$ are both trivial, and this implies that all the Tate cohomology groups are trivial, by Theorem 23.37. □

Corollary 24.17. *Let L/K be a totally unramified cyclic extension of number fields. Then every unit in $\mathcal{O}_K^\times$ is the norm of an element of L.*

Proof. We have $n(L/K) = [\mathcal{O}_K^\times : N(L^\times)\cap\mathcal{O}_K^\times] = 1$, so $\mathcal{O}_K^\times = N(L^\times)\cap\mathcal{O}_K^\times$. □

References

[1] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung **4** (1897), 175–546.

[2] Gerald J. Janusz, *Algebraic number fields*, 2nd ed., AMS, 1992.

[3] F. Lemmermeyer, *Quadratic number fields*, Springer, 2021.

[4] E. Noether, *Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper*, Math. Annalen **108** (1933), 411–419.

18.785 Number Theory I
Fall 2021