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 $T^{\mathfrak{m}}_{L/K} := N_{L/K}(\mathcal{I}^{\mathfrak{m}}_L)\mathcal{R}^{\mathfrak{m}}_K$ (see Definition 22.27) that we claim is equal to the kernel of the Artin map $\psi^{\mathfrak{m}}_{L/K}\colon \mathcal{I}^{\mathfrak{m}}_K \to \operatorname{Gal}(L/K)$, provided that the modulus $\mathfrak{m}$ is divisible by the conductor of L (see Definition 22.24). We showed that $T^{\mathfrak{m}}_{L/K}$ contains $\ker\psi^{\mathfrak{m}}_{L/K}$ (Proposition 22.28), and 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). It only remains to prove the reverse inequality

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

which then yields an isomorphism

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

induced by the Artin map. This result is known as the *Artin reciprocity law.*

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), and then show that this implies the Artin reciprocity law for all unramified abelian extensions.

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

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

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 $N_G := \sum_{i=1}^n \sigma^i$ 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 $I \mapsto I\mathcal{O}_L$ that restricts to a map $\mathcal{P}_K \hookrightarrow \mathcal{P}_L$.[1] Under this convention taking the norm of an

[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.

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 finite Galois extension with Galois group $G := \mathrm{Gal}(L/K)$, and for any G-module A, let $\hat{H}^n(A)$ denote $\hat{H}^n(G, A)$ and let N denote the norm map $\mathrm{N}_{L/K}$.*

(i) *$\hat{H}^0(L)$ and $\hat{H}^1(L)$ are both trivial.*

(ii) *$\hat{H}^0(L^\times) \simeq K^\times/\mathrm{N}(L^\times)$ and $\hat{H}^1(L^\times)$ is trivial.*

Proof. (i) We have $L^G = K$ (by definition). The trace map $\mathrm{T}\colon L \to K$ is not identically zero (by Theorem 5.20, since L/K is separable), so it must be surjective, since it is K-linear. Thus $N_G(L) = \mathrm{T}(L) = K$ and $\hat{H}^0(L) = K/K = 0$.

Now fix $\alpha \in L$ with $\mathrm{T}(\alpha) = \sum_{\tau \in G} \tau(\alpha) = 1$, consider a 1-cocycle $f\colon G \to L$ (this means $f(\sigma\tau) = f(\sigma) + \sigma(f(\tau))$), and put $\beta := \sum_{\tau \in G} f(\tau)\tau(\alpha)$. For all $\sigma \in G$ we have

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau \in G} (f(\sigma\tau) - f(\sigma))(\sigma\tau)(\alpha) = \sum_{\tau \in G} (f(\tau) - f(\sigma))\tau(\alpha) = \beta - f(\sigma),$$

so $f(\sigma) = \beta - \sigma(\beta)$. This implies f is a 1-coboundary, so $\hat{H}^1(L) = H^1(L)$ is trivial.

(ii) We have $(L^\times)^G = K^\times$, so $\hat{H}^0(L^\times) = K^\times/N_G L^\times = K^\times/\mathrm{N}(L^\times)$. Consider any nonzero 1-cocycle $f\colon G \to L^\times$ (now this means $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$). By Lemma 20.6, $\alpha \mapsto \sum_{\tau \in G} f(\tau)\tau(\alpha)$ is not the zero map. Let $\beta = \sum_{\tau \in G} f(\tau)\tau(\alpha) \in L^\times$ be a nonzero element in its image. For all $\sigma \in G$ we have

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau \in G} f(\sigma\tau)f(\sigma)^{-1}(\sigma\tau)(x) = f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau(\alpha) = f(\sigma)^{-1}\beta,$$

so $f(\sigma) = \beta/\sigma(\beta)$. This implies f is a coboundary, so $\hat{H}^1(L^\times) = H^1(L^\times)$ is trivial. □

Corollary 24.2 (Hilbert Theorem 90)**.** *Let L/K be a finite cyclic extension with Galois group* $\mathrm{Gal}(L/K) = \langle\sigma\rangle$*. Then $\mathrm{N}(\alpha) = 1$ if and only if $\alpha = \beta/\sigma(\beta)$ for some $\beta \in L^\times$.*

Proof. By Theorem 23.37, $\hat{H}^1(L^\times) \simeq \hat{H}^{-1}(L^\times) = \hat{H}_0(L^\times) = L^\times[N_G]/(\sigma - 1)(L^\times)$, and Theorem 24.1 implies $L^\times[N_G] = (\sigma - 1)(L^\times)$. The corollary follows. □

Remark 24.3. "Hilbert Theorem 90" refers to Hilbert's text on algebraic number theory [1], although the result is due to Kummer. The result $H^1(\mathrm{Gal}(L/K), L^\times) = 0$ implied by Theorem 24.1 is also often called Hilbert Theorem 90; it is due to Noether [2].

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 $\|\alpha\|_{\sigma(w)} := \|\sigma(\alpha)\|_w$. 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 $\{\mathfrak{q}|\mathfrak{p}\}$.

[2] Note that $\mathcal{I}_L^G = \mathcal{I}_K$ only when L/K is unramified; see Lemma 24.8 below.

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 $\operatorname{Gal}(L/K)$:

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

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

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* $e_v \coloneqq 2$ when this holds (and put $e_v \coloneqq 1$ otherwise). This notation is consistent with our notation $e_v \coloneqq e_{\mathfrak{p}}$ for finite places v corresponding to primes $\mathfrak{p}$ of K. Let us also define $f_v \coloneqq 1$ for $v|\infty$ and put $g_v \coloneqq \#\{w|v\}$ 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

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

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 $\operatorname{Gal}(L/K)$ 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 $w_1,\ldots,w_r$ be the real places of L, let $w_{r+1},\ldots,w_{r+s}$ be the complex places of L. There exist $\varepsilon_1,\ldots,\varepsilon_{r+s} \in \mathcal{O}_L^\times$ such that*

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

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

(iii) *$\varepsilon_1\varepsilon_2\cdots\varepsilon_{r+s} = 1$, and every relation among the ε_i is generated by this one.*

Proof. Pick $\epsilon_1,\ldots,\epsilon_{r+s} \in \mathcal{O}_L^\times$ such that $\|\epsilon_i\|_{w_j} < 1$ for $i \neq j$; the existence of such ϵ_i follows from the strong approximation theorem that we will prove in the next lecture; the product formula then implies $\|\epsilon_i\|_{w_i} > 1$. Now let $\alpha_i \coloneqq \prod_{\sigma\in D_{w_i}} \sigma(\epsilon_i) \in \mathcal{O}_L^\times$. We have

$\|\alpha_i\|_{w_i} = \prod_{\sigma\in D_{w_i}} \|\epsilon_i\|_{w_i} > 1$ and $\|\alpha_i\|_{w_j} = \prod_{\sigma\in D_{w_i}} \|\epsilon_i\|_{\sigma(w_j)} < 1$, since $\sigma \in D_{w_i}$ fixes w_i and permutes the w_j with $j \neq i$. Each α_i is fixed by D_{w_i}.

Let $G \coloneqq \mathrm{Gal}(L/K)$. For $i = 1, \ldots, r{+}s$, let $r(i) \coloneqq \min\{j : \sigma(w_i) = w_j \text{ for some } \sigma \in G\}$, so that $w_{r(i)}$ is a distinguished representative of the G-orbit of w_i. For $i = 1, \ldots, r + s$ let $\beta_i \coloneqq \sigma(\alpha_{r(i)})$, where σ is any element of G such that $\sigma(w_{r(i)}) = w_i$. The value of $\sigma(\alpha_{r(i)})$ does not depend on the choice of σ because $\sigma_1(w_{r(i)}) = \sigma_2(w_{r(i)})$ if and only if $\sigma_2^{-1}\sigma_1 \in D_{w_{r(i)}}$ and $\alpha_{r(i)}$ is fixed by $D_{w_{r(i)}}$. The β_i then satisfy (i).

The β_i also satisfy (ii): a product $\gamma_j \coloneqq \prod_{i\neq j} \beta_i^{n_i}$ cannot be trivial because $\|\gamma_j\|_{w_j} < 1$; in particular, $\beta_1, \ldots, \beta_{r+s-1}$ generate a subgroup of $\mathcal{O}_L^\times$ isomorphic to $\mathbb{Z}^{r+s-1}$ which necessarily has finite index in $\mathcal{O}_L^\times \simeq \mathbb{Z}^{r+s-1} \times \mu_L$ (see Theorem 15.12). But we must have $\prod_i \beta_i^{n_i} = 1$ for some tuple $(n_1, \ldots, n_{r+s}) \in \mathbb{Z}^{r+s}$ (with $n_i = n_j$ whenever w_i and w_j lie in the same G-orbit, since every $\sigma \in G$ fixes 1). The set of such tuples spans a rank-1 submodule of $\mathbb{Z}^{r+s}$ from which we choose a generator $(n_1, \ldots, n_{r+s})$ (by inverting some β_i if necessary, we can make all the n_i positive if we wish). Then $\varepsilon_i \coloneqq \beta_i^{n_i}$ satisfy (i), (ii), (iii) as desired. □

Theorem 24.7. *Let L/K be a cyclic extension of number fields with 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 $n \coloneqq [L : K]$ embeddings $\varphi\colon L \hookrightarrow \mathbb{C}$ with $\varphi_{|_K} = \phi$, equipped with the G-action given by $\sigma(\varphi) \coloneqq \varphi\circ\sigma$. 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 $m \coloneqq \#\{w|v\}$ and define $\tau \coloneqq \sigma^m$; 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 $\{w|v\} = \{w_0, \ldots, w_{m-1}\}$ so

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

and observe that $(\ker\pi)^G = 0$, since τ acts on π as negation, and $(\ker\pi)_G \simeq \mathbb{Z}/2\mathbb{Z}$, since $(\sigma-1)\ker\pi = \{\sum a_i(w_i - w_{m+i}) : a_i \in \mathbb{Z} \text{ with } \sum a_i \equiv 0 \bmod 2\}$ (which is killed by N_G). So in this case $h(\ker\pi) = 1/2$, and therefore $h(A_v) = h(E_\phi)/h(\ker\pi) = 2$, by Corollary 23.41, 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 (each A_v contains either n or $n/2$ of the w_i in its $\mathbb{Z}$-basis). 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 24.8. *Let L/K be a cyclic extension of number fields with Galois group G. For the G-module $\mathcal{I}_L$ we have $h_0(\mathcal{I}_L)=1$ and $h^0(\mathcal{I}_L)=e_0(L/K)[\mathcal{I}_K:N(\mathcal{I}_L)]$.*

Proof. It is clear that $I\in\mathcal{I}_L^G\Leftrightarrow v_{\sigma(\mathfrak{q})}(I)=v_{\mathfrak{q}}(I)$ for all primes $\mathfrak{q}\in\mathcal{I}_L$. If we put $\mathfrak{p}:=\mathfrak{q}\cap\mathcal{O}_K$, then for $I\in\mathcal{I}_L^G$ the value of $v_{\mathfrak{q}}(I)$ is constant on $\{\mathfrak{q}|\mathfrak{p}\}$, since G acts transitively on this set. 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 $h^0(\mathcal{I}_L)=[\mathcal{I}_L^G:N(\mathcal{I}_L)]=e_0(L/K)[\mathcal{I}_K:N(\mathcal{I}_L)]$ as claimed.

For each prime $\mathfrak{q}|\mathfrak{p}$ we have $N(\mathfrak{q})=\mathfrak{p}^{f_{\mathfrak{p}}}$ (by Theorem 6.10). Thus if $N(I)=\mathcal{O}_K$ then $N(\prod_{\mathfrak{q}|\mathfrak{p}}\mathfrak{q}^{v_{\mathfrak{q}}(I)})=\mathfrak{p}^{f_{\mathfrak{p}}\sum_{\mathfrak{q}|\mathfrak{p}}v_{\mathfrak{q}}(I)}=\mathcal{O}_K$, equivalently, $\sum_{\mathfrak{q}|\mathfrak{p}}v_{\mathfrak{q}}(I)=0$, for every prime $\mathfrak{p}$ of K. Order $\{\mathfrak{q}|\mathfrak{p}\}$ as $\mathfrak{q}_1,\ldots,\mathfrak{q}_r$ so that $\mathfrak{q}_{i+1}=\sigma(\mathfrak{q}_i)$ and $\mathfrak{q}_1=\sigma(\mathfrak{q}_r)$, let $n_i:=v_{\mathfrak{q}_i}(I)$, and define

$$J_{\mathfrak{p}}:=\mathfrak{q}_1^{n_1}\mathfrak{q}_2^{n_1-n_2}\mathfrak{q}_3^{n_1-n_2-n_3}\cdots\mathfrak{q}_r^{n_1-n_2-\cdots-n_r}.$$

Then

$$\begin{aligned}\sigma(J_{\mathfrak{p}})/J_{\mathfrak{p}}&=\mathfrak{q}_2^{n_1-(n_1-n_2)}\mathfrak{q}_3^{n_1-n_2-(n_1-n_2-n_3)}\cdots\mathfrak{q}_r^{n_1-\cdots-n_{r-1}-(n_1-\cdots-n_r)}\mathfrak{q}_1^{n_1-\cdots-n_r-n_1}\\&=\mathfrak{q}_2^{n_2}\mathfrak{q}_3^{n_3}\cdots\mathfrak{q}_r^{n_r}\mathfrak{q}_1^{-n_2-\cdots-n_r}=\mathfrak{q}_2^{n_2}\mathfrak{q}_3^{n_3}\cdots\mathfrak{q}_r^{n_r}\mathfrak{q}_1^{n_1}=\prod_{\mathfrak{q}|\mathfrak{p}}\mathfrak{q}^{v_{\mathfrak{q}}(I)},\end{aligned}$$

since $n_1+\cdots+n_r=0$ implies $n_1=-n_2-\cdots-n_r$. It follows that $I=\sigma(J)/J$ where $J:=\prod_{\mathfrak{p}\nmid\mathfrak{m}}J_{\mathfrak{p}}$, thus $I_L[N_G]=(\sigma-1)(I_L)$ and $h_0(\mathcal{I}_L)=1$. □

Theorem 24.9 (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 $n(L/K):=[\mathcal{O}_K^\times:N(L^\times)\cap\mathcal{O}_K^\times]\in\mathbb{Z}_{\geq1}$.

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

$$1\longrightarrow\mathcal{P}_L\longrightarrow\mathcal{I}_L\longrightarrow\mathrm{Cl}_L\longrightarrow1.$$

The corresponding long exact sequence in (standard) cohomology begins

$$1\longrightarrow\mathcal{P}_L^G\longrightarrow\mathcal{I}_L^G\longrightarrow\mathrm{Cl}_L^G\longrightarrow H^1(\mathcal{P}_L)\longrightarrow1,$$

since $H^1(\mathcal{I}_L)\simeq\hat{H}_0(\mathcal{I}_L)$ is trivial, by Lemma 24.8. Therefore

$$\#\mathrm{Cl}_L^G=[\mathcal{I}_L^G:\mathcal{P}_L^G]\;h^1(\mathcal{P}_L).\tag{4}$$

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 24.8.

We now consider the short exact sequence

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

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 $H^1(L^\times)$ is trivial, by Hilbert 90 (Corollary 24.2). We have $K^\times/\mathcal{O}_K^\times \simeq \mathcal{P}_K$, thus

$$[\mathcal{P}_L^G : \mathcal{P}_K] = h^1(\mathcal{O}_L^\times) = \frac{h^0(\mathcal{O}_L^\times)}{h(\mathcal{O}_L^\times)} = \frac{h^0(\mathcal{O}_L^\times)\,[L:K]}{e_\infty(L/K)},$$

by Theorem 24.7. Combining this identity with (4) and (5) yields

$$\#\mathrm{Cl}_L^G = \frac{e(L/K)\#\mathrm{Cl}_K}{[L:K]} \cdot \frac{h^1(\mathcal{P}_L)}{h^0(\mathcal{O}_L^\times)}. \tag{7}$$

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

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

so $h^1(\mathcal{P}_L) = [\mathcal{O}_K^\times \cap N(L^\times) : N(\mathcal{O}_L^\times)]$. We have $h^0(\mathcal{O}_L^\times) = [\mathcal{O}_K^\times : N(\mathcal{O}_L^\times)]$, thus

$$\frac{h^0(\mathcal{O}_L^\times)}{h^1(\mathcal{P}_L)} = [\mathcal{O}_K^\times : N(L^\times) \cap \mathcal{O}_K^\times] = n(L/K),$$

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

24.2 Proof of Artin reciprocity

We now have the essential ingredients in place to prove our desired inequality for unramified cyclic extensions of number fields. We first record an elementary lemma.

Lemma 24.10. *Let $f : A \to G$ 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.

$$\begin{tikzcd}
& \ker f \arrow[r, hook] \arrow[d, equal] & B \arrow[r, "f"] \arrow[d, hook] & f(B) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \ker f \arrow[r, hook] & A \arrow[r, "f"] & f(A) \arrow[r] & 0.
\end{tikzcd}$$

□

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 24.11. *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

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

The denominator on the RHS can be rewritten as

$$\begin{aligned}[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K] &= [N(\mathcal{I}_L) : N(\mathcal{I}_L) \cap \mathcal{P}_K] && \text{(2nd isomorphism theorem)}\\ &= [\mathcal{I}_L : N^{-1}(\mathcal{P}_K)] && \text{(Lemma 24.10)}\\ &= [\mathcal{I}_L/\mathcal{P}_L : N^{-1}(\mathcal{P}_K)/\mathcal{P}_L] && \text{(3rd isomorphism theorem)}\\ &= [\mathrm{Cl}_L : \mathrm{Cl}_L[N_G]]\\ &= \#N_G(\mathrm{Cl}_L).\end{aligned}$$

Now $h^0(\mathrm{Cl}_L) = [\mathrm{Cl}_L^G : N_G(\mathrm{Cl}_L)]$, and applying Theorem 24.9 yields

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

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

For a totally unramified extension of number fields L/K, let $T_{L/K} \coloneqq T_{L/K}^{(1)} = N(\mathcal{I}_L)\mathcal{P}_K$.

Corollary 24.12 (Artin reciprocity law)**.** *Let L/K be a totally unramified cyclic extension of number fields. Then $[\mathcal{I}_K : T_{L/K}] = [L : K]$ and the Artin map induces an isomorphism $\mathcal{I}_K/T_{L/K} \simeq \mathrm{Gal}(L/K)$.*

Proof. Theorems 22.29 and 24.11 imply $[\mathcal{I}_K : T_{L/K}] = [L : K]$. We have $\ker \psi_{L/K} \subseteq T_{L/K}$ (Proposition 22.28), and $[\mathcal{I}_K : \ker \psi_{L/K}] = \#\mathrm{Gal}(L/K) = [L : K] = [\mathcal{I}_K : T_{L/K}]$, since $\psi_{L/K}$ is surjective (Theorem 21.19). Therefore $\ker \psi_{L/K} = T_{L/K}$, and the Corollary follows. □

Corollary 24.13. *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. By the previous corollary and the proof of Theorem 24.11: we have $n(L/K) = 1$ and $h^0(\mathrm{Cl}_L) = 1$, and $e(L/K) = 1$, so $\#\mathrm{Cl}_L^G = \#\mathrm{Cl}_L/[L : K]$ by Theorem 24.9. We also have $h(\mathrm{Cl}_K) = h^0(\mathrm{Cl}_L)/h_0(\mathrm{Cl}_L) = 1$, since Cl_L is finite, by Lemma 23.43, so $h_0(\mathrm{Cl}_L) = 1$. Thus $\hat{H}^{-1}(\mathrm{Cl}_L)$ 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 24.14. *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 $\mathcal{O}_K^\times = N(L^\times) \cap \mathcal{O}_K^\times$. □

24.3 Generalizing to the non-cyclic case

Corollaries 24.13 and 24.14 are specific to unramified cyclic extensions, but Corollary 24.12 (Artin reciprocity) extends to all abelian extensions. Our goal in this section is to show that for any modulus $\mathfrak{m}$ for a number field K, if the Artin reciprocity law holds for all finite cyclic extensions L/K with conductor dividing $\mathfrak{m}$, then it holds for all finite abelian extensions L/K with conductor dividing $\mathfrak{m}$.

Definition 24.15. Let $\mathfrak{m}$ be a modulus for a number field K and let L/K be a finite abelian extension ramified only at primes $\mathfrak{p}|\mathfrak{m}$. We say that L is a *class field* for $\mathfrak{m}$ if $\ker\psi^{\mathfrak{m}}_{L/K} = T^{\mathfrak{m}}_{L/K}$, where $\psi^{\mathfrak{m}}_{L/K}\colon \mathcal{I}^{\mathfrak{m}}_K \to \operatorname{Gal}(L/K)$ is the Artin map.

Remark 24.16. This definition is stated more strongly than is typical, but it is convenient for our purposes; we have already proved the surjectivity of the Artin map and that $T^{\mathfrak{m}}_{L/K}$ contains $\ker\psi^{\mathfrak{m}}_{L/K}$ so there is no reason to use an (apparently) weaker definition.

Lemma 24.17. *Let $\mathfrak{m}$ be a modulus for a number field K. If L_1 and L_2 are class fields for $\mathfrak{m}$ then so is their compositum $L \coloneqq L_1L_2$.*

Proof. We first note that $L = L_1L_2$ is ramified only at primes ramified in either L_1 or L_2 (since ramification indices are multiplicative in towers), so L is ramified only at primes $\mathfrak{p}|\mathfrak{m}$. As in the proof of Theorem 21.18, a prime $\mathfrak{p} \nmid \mathfrak{m}$ splits completely in L if and only if it splits completely in L_1 and L_2, which implies $\ker\psi^{\mathfrak{m}}_{L/K} = \ker\psi^{\mathfrak{m}}_{L_1/K} \cap \ker\psi^{\mathfrak{m}}_{L_2/K}$. The norm map is transitive in towers, so if $I = N_{L/K}(J)$ then $I = N_{L_1/K}(N_{L/L_1}(J))$ and $I = N_{L_2/K}(N_{L/L_2}(J))$, thus $N(\mathcal{I}^{\mathfrak{m}}_L) \subseteq N(\mathcal{I}^{\mathfrak{m}}_{L_1}) \cap N(\mathcal{I}^{\mathfrak{m}}_{L_2})$ and therefore $T^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L_1/K} \cap T^{\mathfrak{m}}_{L_2/K}$. If L_1 and L_2 are class fields for $\mathfrak{m}$, then

$$T^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L_1/K} \cap T^{\mathfrak{m}}_{L_2/K} = \ker\psi^{\mathfrak{m}}_{L_1/K} \cap \ker\psi^{\mathfrak{m}}_{L_2} = \ker\psi^{\mathfrak{m}}_{L/K},$$

and $\ker^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L/K}$ by Proposition 22.28, so $T^{\mathfrak{m}}_{L/K} = \ker\psi^{\mathfrak{m}}_{L/K}$ and the lemma follows. □

Corollary 24.18. *Let $\mathfrak{m}$ be a modulus for a number field K. If every finite cyclic extension of K with conductor dividing $\mathfrak{m}$ is a class field for $\mathfrak{m}$ then so is every abelian extension of K with conductor dividing $\mathfrak{m}$.*

Proof. Let L/K be a finite abelian extension of conductor $\mathfrak{c}|\mathfrak{m}$. The conductor of any subextension of L divides $\mathfrak{c}$ and therefore $\mathfrak{m}$, by Lemma 22.26.

If we write $G \coloneqq \operatorname{Gal}(L/K) \simeq H_1 \times \cdots H_r$ as a product of cyclic groups and define $L_i = L^{\bar{H}_i}$ where $\bar{H}_i = \prod_{j\neq i} H_j \subseteq G$ so that $\operatorname{Gal}(L_i/K) \simeq G/\bar{H}_i \simeq H_i$ is cyclic, then $L = L_1 \cdots L_r$ is a composition of linearly disjoint cyclic extensions of K, and it follows from Lemma 24.17 that if the L_i are all class fields for $\mathfrak{m}$, so is L. □

24.4 Class field theory for unramified abelian extensions

For the trivial modulus $\mathfrak{m} = (1)$, the three main theorems of class field theory stated in Lecture 22 state that the following hold for every number field K:

- **Existence**: The ray class field $K(1)$ exists.
- **Completeness**: Every unramified abelian extension of K is a subfield of $K(1)$.
- **Artin reciprocity**: For every subextension L/K of $K(1)$ we have $\ker\psi_{L/K} = T_{L/K}$ and a canonical isomorphism $\mathcal{I}_K/T_{L/K} \simeq \operatorname{Gal}(L/K)$.

We can now prove all of this, except for the existence of $K(1)$. But if we replace $K(1)$ with the Hilbert class field H of K (the maximal unramified abelian extension of K) we can prove an analogous series of statements, including that H is a finite extension of K and that if $K(1)$ exists it must be equal to H.

Theorem 24.19. *Let K be a number field with Hilbert class field H. The following hold:*

- *H/K is a finite extension with $\mathrm{Gal}(H/K)$ isomorphic to a quotient of Cl_K.*
- *$K(1)$ exists if and only if $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$, in which case $K(1) = H$.*
- *Every unramified abelian extension of K is a subfield of H* (**Completeness**)*.*
- *For every unramified abelian extension of K we have $\ker \psi_{L/K} = T_{L/K}$ and a canonical isomorphism $\mathcal{I}_K/T_{L/K} \simeq \mathrm{Gal}(L/K)$* (**Artin reciprocity**)*.*

Proof. Corollaries 24.12 and 24.18 together imply the Artin reciprocity law for every unramified abelian extension of K. In particular, every such extension L has $\mathrm{Gal}(L/K)$ isomorphic to a quotient of Cl_K (since $T_{L/K}$ contains $\mathcal{P}_K$). Moreover, distinct unramified abelian extensions L/K correspond to distinct quotients of Cl_K, since the primes that split completely in K are precisely those that lie in the kernel of the Artin map, and this set of primes uniquely determines L, by Theorem 21.18. It follows that there is a unique quotient of Cl_K that corresponds to H, the compositum of all such fields. The theorem follows. □

References

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

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

18.785 Number Theory I
Fall 2019