Mathematics GR6657 Algebraic Number Theory
Final Exam

Benjamin Church

September 24, 2019

1

Let K be a number field and let S be a finite set of prime ideals in $\mathcal{O}_K$. We will assume that all extensions of K lie inside a fixed algebraic closure $\bar{K}$.

(a)

Suppose that L, L' are finite extensions of K which are unramified outside S. Let E be the Galois closure of $L \cdot L'$ which is also a finite extension of K because it is the splitting field of the product of minimal polynomials of the generators of L and L'. Let $\mathfrak{p} \subset K$ be a prime ideal. Consider the splitting of the prime $\mathfrak{p}$ in the Galois closure E,

$$\mathfrak{p}\mathcal{O}_E = \prod_{i=1}^{g} \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}}$$

and the inertial group of this splitting,

$$1 \longrightarrow I(\mathfrak{P}_i) \longrightarrow D(\mathfrak{P}_i) \longrightarrow Gal(k(E)/k(K)) \longrightarrow 1$$

which has order $|I(\mathfrak{P})| = e_{\mathfrak{P}|\mathfrak{p}} = e_{E/K}$ because E/K is Galois. I claim that any intermediate field $K \subset F \subset E$ satisfies $F \subset E^{I(\mathfrak{P})}$ if and only if $\mathfrak{p}$ is unramified in F. Suppose that $F \subset E^{I(\mathfrak{P})}$ then we know that E/F is Galois (because E/K is and $K \subset F \subset E$) such that $I(\mathfrak{P}) \subset Gal(E/F)$. We can decompose,

$$\mathfrak{p}\mathcal{O}_F = \prod_{i=1}^{g_F} \mathfrak{q}^{e_{\mathfrak{q}_i|\mathfrak{p}}}$$

and each $\mathfrak{q}$ splits into $\mathfrak{P}_i$ such that,

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{q}} e_{\mathfrak{q}|\mathfrak{p}}$$

However, the inertial group $I(\mathfrak{P})$ of the extension L/K is contained in $Gal(E/F)$ so,

$$I_{E/F}(\mathfrak{P}) = \{\sigma \in Gal(E/F) \mid \forall \alpha \in \mathcal{O}_E : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\} = I(\mathfrak{P}) \cap Gal(E/F) = I(\mathfrak{P})$$

Therefore, $e_{\mathfrak{P}|\mathfrak{q}} = e_{\mathfrak{P}|\mathfrak{p}}$ and thus $e_{\mathfrak{q}|\mathfrak{p}} = 1$ so $\mathfrak{p}$ is unramified in F.

Conversely, if $\mathfrak{p}$ is unramified in F then for each $\mathfrak{q}$ above $\mathfrak{p}$ we have $e_{\mathfrak{q}|\mathfrak{p}} = 1$ and thus,

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{q}} e_{\mathfrak{q}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{q}}$$

Since E/K is Galois we know that E/F is Galois. We know that $I_{E/F}(\mathfrak{P}) \subset I_{E/K}(\mathfrak{P})$ but the orders of these groups are $e_{\mathfrak{P}|\mathfrak{q}}$ and $e_{\mathfrak{P}|\mathfrak{p}}$ which are equal. Therefore, $I_{E/K}(\mathfrak{P}) = I_{E/F}(\mathfrak{P}) \subset Gal(E/F)$ so by Galois theory $F \subset E^{I(\mathfrak{P})}$.

Back to the original problem. Since $\mathfrak{p}$ is unramified in both L and L' we know that $L, L' \subset E^{I(\mathfrak{P})}$. Therefore, $L \cdot L' \subset E^{I(\mathfrak{P})}$ which implies that $\mathfrak{p}$ is unramified in $L \cdot L'$ proving the proposition.

(b)

Let L/K be finite extension unramified outside of S. By the primitive element theorem, there exists some $\alpha \in L$ such that $L = K(\alpha)$. Let $p \in K[X]$ be the minimal polynomial of α. Let E be the splitting field of p which is the Galois closure of L. Therefore, if p has roots $\alpha_1, \cdots, \alpha_n \in \bar{K}$ then $E = K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1) \cdots K(\alpha_n)$. However, basic field theory tells us that since α_i and α_j have the same minimal polynomial then $K(\alpha_i) \cong K(\alpha_j)$ by a K-isomorphism so if $\mathfrak{p}$ is unramified in $L = K(\alpha)$ then $\mathfrak{p}$ is unramified in $K(\alpha_i)$ for each i and thus by the previous problem, $\mathfrak{p}$ is unramified in the compositum, $E = K(\alpha_1) \cdots K(\alpha_n)$.

(c)

Define the maximal S-unramified extension K^S of K as the union of all extensions L/K such that L is unramified outside S. For each L/K in the union, we can replace L with its Galois closure E/K which is still unramified outside S and therefore appears in the union containing L. Therefore,

$$K^S = \bigcup_{L/K} L = \bigcup_{E/K} E$$

However, each extension E/K is finite Galois so K^S/K is Galois because it is the direct limit of finite Galois extensions. The extension K^S/K has a profinite Galois group,

$$\Gamma_S = Gal(K^S/K) = \varprojlim_{E/K} Gal(E/K)$$

where the projective limit runs over finite galois extensions E/K which are unramified outside S.

2

Let K be a number field and M be a finite abelian group of order N with a continuous action of the absolute Galois group, $Gal(\bar{K}/K)$.

(a)

Consider the action $\phi : Gal(\bar{K}/K) \to \mathrm{Aut}\,(M)$. Since ϕ is continuous, the sugbroup $\ker \phi = \phi^{-1}(1)$ is open since M is discrete. By infinite Galois theory, the fixed field $L = \bar{K}^H$ is a finite extension of K if and only if $H \subset Gal(\bar{K}/K)$ is an open subgroup. Therefore, $L = \bar{K}^{\ker \phi}$ is a finite extension of K with $Gal(\bar{K}/L) = \ker \phi$. Furthermore, $\ker \phi$ is normal so L/K is Galois with $Gal(L/K) = Gal(\bar{K}/K)/Gal(\bar{K}/L)$. Since L/K is a finite extension, L is a number field so a finite set of primes $S \subset \mathcal{O}_K$ ramify in L/K. Thus, $K \subset L \subset K^S \subset \bar{K}$. However, K^S is Galois over K and thus over L

so $Gal(\bar{K}/K^S)$ is a normal subgroup of both $Gal(\bar{K}/K)$ and $Gal(\bar{K}/L)$. By the third isomorphism theorem,

$$Gal(L/K) \cong (Gal(\bar{K}/K)/Gal(\bar{K}/K^S))/(Gal(\bar{K}/L)/Gal(\bar{K}/K^S)) \cong Gal(K^S/K)/Gal(K^S/L) \cong \Gamma_S/H$$

where $H = Gal(K^S/L)$. Then, the action $\phi : Gal(\bar{K}/K) \to \mathrm{Aut}\,(M)$ factors through its kernel,

$$Gal(\bar{K}/K) \twoheadrightarrow Gal(\bar{K}/K)/\ker\phi \xrightarrow{\sim} \Gamma_S/H \longrightarrow \mathrm{Aut}\,(M)$$

(b)

Consider the cohomology group $H^1(H, M)$ where $H = Gal(K^S/L)$ is the kernel of the action $\Gamma_S \to \mathrm{Aut}\,(M)$. Therefore, H acts trivially on M so,

$$H^1(H, M) = \mathrm{Hom}\,(H, M)$$

because the crossed homomorphisms are just normal homomorphisms and principal homomorphisms are trivial. Since M is an abelian group, any map $\phi : H \to M$ factors through the abelianization $\phi' : H^{ab} \to M$. Therefore,

$$\mathrm{Hom}\,(H, M) = \mathrm{Hom}\,\big(H^{\mathrm{ab}}, M\big)$$

Consider the commutator subgroup[1] $C = [H, H] \triangleleft H$. Since C is normal in H we know that the intermediate field $L \subset (K^S)^C \subset K^S$ is a galois extension of L. Call $L_S^{\mathrm{ab}} = (K^S)^C$ which I claim is the maximal abelian extension of L still contained in K^S. Since L_S^{ab}/K is Galois,

$$Gal(L_S^{\mathrm{ab}}/L) \cong (Gal(K^S/L))/(Gal(K^S/L_S^{\mathrm{ab}})) = H/C = H^{\mathrm{ab}}$$

Therefore, L_S^{ab}/L is abelian. Furthermore, if $L \subset F \subset K^S$ is an abelian extension of L then $Gal(K^S/F) \triangleleft H$ with abelian quotient. Therefore this subgroup contains the commutator subgroup,

$$Gal(K^S/L_S^{\mathrm{ab}}) = C \subset Gal(K^S/F)$$

and thus by the Galois correspondence, $F \subset L_S^{\mathrm{ab}}$ proving my claim.

By the above argument, we need to study the group,

$$H^1(H, M) = \mathrm{Hom}\,\big(Gal(L_S^{\mathrm{ab}}/L), M\big)$$

Since this profinite Galois group is a topological group it is important that we only consider continuous homomorphisms by the definition of the group cohomology. Let $\mathcal{G} = Gal(L_S^{\mathrm{ab}}/L)$. We need to consider the continuous homomorphisms,

$$\begin{tikzcd} \mathcal{G} \arrow[r, "\phi"] \arrow[d] & M \\ \mathcal{G}/\ker\phi \arrow[ur, hook] & \end{tikzcd}$$

[1]Technically we need to take the closure of the usual commutator subgroup such that the quotient is still profinite and the associated field extension is Galois.

Since ϕ is continuous, $\ker \phi = \phi^{-1}(1)$ is open (since M is discrete) so $\ker \phi$ corresponds to a finite abelian extension $L \subset L^{\ker \phi} \subset L_S^{\text{ab}}$. Also $\ker \phi$ is normal so $L^{\ker \phi}/L$ is a Galois extension with $Gal(L^{\ker \phi}/L) \cong \mathcal{G}/\ker \phi \cong \text{Im}(\phi) \subset M$. Write $F = L^{\ker \phi}$ then we know that $Gal(F/L)$ is isomorphic to a subgroup of M and thus has exponent dividing N, the order of M.

Since $\mathcal{G}$ is a profinite group, we can write the entire set of continuous homomorphisms as a direct limit over open normal subgroups $H \triangleleft \mathcal{G}$,

$$\text{Hom}\,(\mathcal{G}, M) = \varinjlim_{H \triangleleft \mathcal{G}} \text{Hom}\,(\mathcal{G}/H, M)$$

However, each continuous homomorphism $\phi : \mathcal{G} \to M$ is contained in the inclusion of $\text{Hom}\,(\mathcal{G}/\ker \phi, M)$ so we can restrict this direct limit to only such open normal subgroups which appear as kernels of homomorphisms. Therefore,

$$\text{Hom}\,(\mathcal{G}, M) = \varinjlim_{H \triangleleft \mathcal{G}} \text{Hom}\,(Gal(F/L), M)$$

where $L \subset F \subset L_S^{\text{ab}}$ runs over all intermediate finite abelian extension of L which are unramified outside S and appear as fixed fields of the kernels and consequently have degree dividing N.

I claim that there are finitely many abelian extensions F/L with degree dividing N which are unramified outside S. This is a consequence of the classical result known as the Hermite-Minkowski theorem that there are only finitely many extensions with a given discriminant. This theorem was proven using the Minkowski bound and geometry of numbers (see Milne ANT Thm. 8.42). Instead, I will attempt a proof in the abelian case using class field theory.

Theorem 2.1. *Let S be a finite set of primes of a number field K. There are only finitely many abelian extensions of K with degree dividing N which are unramified outside S.*

Proof. Let L/K be an abelian extension of number fields of degree dividing N. For each $\mathfrak{p} \in S$ consider the extension of local fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. This extension is Galois with,

$$Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = D(\mathfrak{P}) \subset Gal(L/K)$$

Thus, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is an abelian extension of degree dividing N. However, a local field of characteristic zero with a finite residue field has only finitely many extensions of fixed degree (see Milne ANT Prop. 7.64). Therefore, we may take the maximum local conductor of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ over all such L/K with degree dividing N since there only finitely many possibilities for the extension of the local field at $\mathfrak{p}$. Call this maximum conductor, $f_N(K_{\mathfrak{p}}) = \max\limits_{L/K} f(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ where L runs over all abelian extensions of K with degree dividing N which are unramified outside S. Define a modulus of K,

$$\mathfrak{m} = \mathfrak{m}_\infty \prod_{\mathfrak{p} \in S} \mathfrak{p}^{f_N(K_{\mathfrak{p}})}$$

where $\mathfrak{m}_\infty$ is the product of all archimedean primes of K. By global class field theory, there is a correspondence between subgroups of the ray class group $C_{\mathfrak{m}}$ and abelian intermediate extensions $K \subset L \subset L_{\mathfrak{m}}$ where $L_{\mathfrak{m}}$ is the ray class field associated with the modulus $\mathfrak{m}$. Consider any extension L/K with degree dividing N which is unramified outside S. The conductor of this extension can be written in terms of the local conductors as,

$$\mathfrak{f}_0(L/K) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{f(L_{\mathfrak{P}}/K_{\mathfrak{p}})}$$

where the product can be restricted to run over primes in S because a prime appears in the factorization of the conductor if and only if it is ramified in L/K and L/K is unramified outside S. Furthermore, since L/K has degree dividing N its local conductors are bounded by the maximum local conductors $f_N(K_\mathfrak{p})$. Therefore,

$$\mathfrak{f}_0(L/K) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{f(L_\mathfrak{P}/K_\mathfrak{p})} \supset \prod_{\mathfrak{p} \in S} \mathfrak{p}^{f_N(K_\mathfrak{p})} = \mathfrak{m}_0$$

and thus including any infinite primes ramifying in L/K we have, $\mathfrak{f}(L/K) \mid \mathfrak{m}$. Therefore, the global Artin map $\theta_{L/K} : I^S \to Gal(L/K)$ factors through $C_\mathfrak{m}$ so L is contained in the ray class field, $K \subset L \subset L_\mathfrak{m}$. Therefore, L corresponds the kernel of the global Artin map $\theta_{L/K} : C_\mathfrak{m} \to Gal(L/K)$. However, the ray class group $C_\mathfrak{m}$ is finite and thus has finitely many subgroups. By the main theorem of class field theory, there are only finitely many abelian extensions of K contained in the ray class field $L_\mathfrak{m}$ and thus finitely many such L/K. □

Given this theorem, we can complete the proof. We have shown that,

$$H^1(H, M) = \mathrm{Hom}\,(H, M) = \mathrm{Hom}\left(Gal(L_S^{\mathrm{ab}}), M\right) = \varinjlim \mathrm{Hom}\,(Gal(F/L), M)$$

where F runs over finite abelian extensions of degree dividing N which are unramified outside S. However, I have shown that there are only finitely many such F/L. Furthermore, since $Gal(F/L)$ and M are finite, $\mathrm{Hom}\,(Gal(F/L), M)$ is finite. Thus, $H^1(H, M)$ is the direct limit of a finite set of finite groups which is finite.

(c)

Consider the inflation-restriction sequence for the group $\Gamma_S = Gal(K^S/K)$ with $H \triangleleft \Gamma_S$,

$$1 \longrightarrow H^r(\Gamma_S/H, M^H) \xrightarrow{\mathrm{inf}} H^r(\Gamma_S, M) \xrightarrow{\mathrm{res}} H^r(H, M)$$

However, we have shown above that $H^1(H, M)$ is finite. Furthermore, $\Gamma_S/H \cong Gal(L/K)$ and M^H are finite groups which implies that $H^1(\Gamma_S/H, M^H)$ is finite since there is a finite number of crossed homomorphisms. Thus, we get the following exact sequence,

$$1 \longrightarrow H^1(\Gamma_S/H, M^H) \xrightarrow{\mathrm{inf}} H^1(\Gamma_S, M) \xrightarrow{\mathrm{res}} H^1(H, M)$$

and thus,

$$H^1(\Gamma_S, M)/H^1(\Gamma_S/H, M^H) \cong \mathrm{Im}(\mathrm{res})$$

Which implies that,

$$|H^1(\Gamma_S, M)| = |H^1(\Gamma_S/H, M^H)| \cdot |\mathrm{Im}(\mathrm{res})| \leq |H^1(\Gamma_S/H, M^H)| \cdot |H^1(H, M)|$$

In particular, since $H^1(\Gamma_S/H, M^H)$ and $H^1(H, M)$ are finite we have that $H^1(\Gamma_S, M)$ is finite.

3

Let K be a number field containing the N^{th} roots of unity and M a finite abelian group.

(a)

Let S be a finite set of primes of $\mathcal{O}_K$ and let $U_{K,S} \subset K^\times$ be the subgroup of S-units. Let $u \in U_{K,S}$ and consider the extension $K_u = K(\sqrt[N]{u})$. I claim that without loss of generality, we may assume that $u \in \mathcal{O}_K$ is an algebraic integer. Otherwise, because u is an S-unit, it generates the fractional ideal,

$$(u) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where $e_i \in \mathbb{Z}$. Because the class group $C\ell(K)$ is finite, for each $\mathfrak{p}_i$ there exits a positive integer n_i such that $\mathfrak{P}_i^{n_i}$ is principal. Therefore, $\mathfrak{p}_1^{n_1|e_1|} \cdots \mathfrak{p}_g^{n_g|e_g|} = (v)$ is a principal ideal of $\mathcal{O}_K$. Furthermore,

$$(uv^N) = (u)(v)^N = \mathfrak{p}_1^{n_1 N|e_1| + e_1} \cdots \mathfrak{p}_g^{n_g N|e_g| + e_g}$$

and thus each exponent is positive. Therefore, uv^N generate a true integral ideal of $\mathcal{O}_K$ with only primes in S so $uv^N \in \mathcal{O}_K \cap U_{K,S}$. Finally, $K(\sqrt{N}u) = K(\frac{1}{v}\sqrt{N}uv^N) = K(\sqrt{N}uv^N)$ so we may assume that the S-unit u generating $K(\sqrt{N}u)$ is, in fact, integral.

Under this assumption, since $(\sqrt[N]{u})^N = u \in K$ and K contains all N^{th} roots of unity, by the cyclic extension theorem, the extension L/K is cyclic and thus abelian. Take the polynomial $f \in K[X]$ given by $f(X) = X^N - u$ and let $\alpha = \sqrt[N]{u}$. Let $p \in K[X]$ be the minimal polynomial of α and $m = \deg p$. Then since $f(\alpha) = 0$ we know that $p \mid f$ and thus,

$$D(1, \alpha, \alpha^2, \ldots, \alpha^{m-1}) = \mathrm{disc}\,(p) \mid \mathrm{disc}\,(f)$$

Let $\Delta_{L/K}$ be the relative discriminant of L/K then $D(1, \alpha, \alpha^2, \ldots, \alpha^{m-1}) \in \Delta_{L/K}$ because it is an integral basis of L since $X^N - u$ is monic and $u\mathcal{O}_K$. Because $\Delta_{L/K}$ is an ideal we know that $\mathrm{disc}\,(f) \in \Delta_{L/K}$. However, we can calculate the discriminant of f,

$$|\mathrm{disc}\,(f)\,| = \mathrm{N}_K^L\,(f'(\alpha)) = \mathrm{N}_K^L\left(N\alpha^{N-1}\right) = N^m u^{N-1}$$

Since $\mathrm{disc}\,(f) \in \Delta_{L/K}$ we know that as ideals,

$$\Delta_{L/K} \supset (\mathrm{disc}\,(f)) = (N^m u^{m-1}) = (N)^m (u)^{m-1}$$

Therefore if a prime $\mathfrak{p}$ in $\mathcal{O}_K$ is ramified then $\mathfrak{p}$ lies above $\Delta_{L/K}$ and thus $\mathfrak{p}$ lies above $(N)^m(u)^{m-1}$. By the uniqueness of Dedekind prime factorization, $\mathfrak{p}$ must appear in either the factorization of either the ideal (N) or the ideal (u). However, by assumption, u is a S-unit so (u) factors as a product of primes in S. Thus, if $\mathfrak{p}$ is a prime outside S which does not not divide (N) then $\mathfrak{p}$ must be unramified.

(b)

From problem 2, we know that to prove $H^1(\Gamma_{S(N)}, M)$ is finite it suffices to show that $H^1(H, M) = \mathrm{Hom}\left(Gal(L_{S(N)}^{\mathrm{ab}}/L), M\right)$ is finite which gives the required result via the inflation-restriction sequence.

Let $\mathcal{G} = Gal(L_{S(N)}^{\mathrm{ab}}/L)$. We need to consider the continuous homomorphisms,

$$\begin{tikzcd}
\mathcal{G} \arrow[r, "\phi"] \arrow[d] & M \\
\mathcal{G}/\ker\phi \arrow[ur, hook] &
\end{tikzcd}$$

Since ϕ is continuous, $\ker\phi = \phi^{-1}(1)$ is open (since M is discrete) so $\ker\phi$ corresponds to a finite abelian extension $L \subset L^{\ker\phi} \subset L^{\text{ab}}_{S(N)}$ and $\ker\psi$ is normal so $Gal(L^{\ker\phi}/L) \cong \mathcal{G}/\ker\phi \cong \text{Im}(\phi) \subset M$. Write $F = L^{\ker\phi}$ then we know that $Gal(F/L)$ is isomorphic to a subgroup of M and thus has exponent dividing N, the order of M.

Since $\mathcal{G}$ is a profinite group, we can write the entire set of continuous homomorphisms as a direct limit over open normal subgroups $H \lhd \mathcal{G}$,

$$\text{Hom}\,(\mathcal{G}, M) = \varinjlim_{H \lhd \mathcal{G}} \text{Hom}\,(\mathcal{G}/H, M)$$

However, since each continuous homomorphism $\phi : \mathcal{G} \to M$ is contained in the inclusion of $\text{Hom}\,(\mathcal{G}/\ker\phi, M)$ we can restrict this direct limit to only such open normal subgroups which appear as kernels of such homomorphisms. Therefore,

$$\text{Hom}\,(\mathcal{G}, M) = \varinjlim_{H \lhd \mathcal{G}} \text{Hom}\,(Gal(F/L), M)$$

where $L \subset F \subset L^{\text{ab}}_{S(N)}$ runs over all intermediate finite extensions of L which are unramified outside $S(N)$ and appear as fixed fields of the kernels and consequently are finite abelian extensions of exponent dividing N. Since $K \subset L$ contain all N^{th} roots of unity, by Kummer theory, there is a correspondence between finite abelian extensions of L with exponent dividing N and finite subgroups of $L^\times/(L^\times)^N$. In particular,

$$F/L \mapsto \Delta = \frac{L^\times \cap (F^\times)^N}{(L^\times)^N} \subset \frac{L^\times}{(L^\times)^N} \quad \text{and} \quad \Delta \subset \frac{L^\times}{(L^\times)^N} \mapsto L[\Delta^{1/N}]/L$$

Given an intermediate Galois extension $L \subset F \subset L^{\text{ab}}_{S(N)}$ with exponent dividing N we know that F/L is abelian and F/K is unramified outside $S(N)$ since $F \subset L^{\text{ab}}_{S(N)} \subset K^{S(N)}$. Take any $u \in \Delta$. The fractional ideal $u\mathcal{O}_L$ must factor into primes lying above $S(N)$ since in F, the ideal $(u) = u\mathcal{O}_F$ can decompose as $(u) = (\sqrt[N]{u})^N$ and thus each prime factor of the fractional ideal $u\mathcal{O}_L$ totally ramifies in the extension F/L since they are relatively prime and their product is a power. However, F/K is unramified outside $S(N)$ so any prime which ramifies in F/L must lie above a prime in $S(N)$. By lemma 5.3, the image of the S-units inside $L^\times/(L^\times)^N$ is finite. However, $\Delta \subset U_{L,S}$ so there are finitely many possible subgroups Δ and thus finitely many finite abelian extensions of L with exponent dividing N which are unramified outside $S(N)$. Furthermore, each $\text{Hom}\,(Gal(F/L), M)$ is a finite group because each F/L is a finite extension and thus both $Gal(L/K)$ and M are finite groups so there are a finite number of maps between them. Thus,

$$H^1(H, M) = \text{Hom}\,(\mathcal{G}, M) = \varinjlim_{H \lhd \mathcal{G}} \text{Hom}\,(Gal(F/L), M)$$

is contained in the union of finitely many finite groups and is therefore finite.

4

Let K be a number field. Take any finite Galois extension L/K and consider the commutative diagram with exact rows and columns,

$$
\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathcal{O}_L \arrow[r] \arrow[d] & L^\times \arrow[r] \arrow[d] & P_L \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{I}_{L,S_\infty} \arrow[r] & \mathbb{I}_L \arrow[r] & I_L \arrow[r] & 1
\end{tikzcd}
$$

where P_L is the group of principal fractional ideals of L and I_L is the group of all fractional ideals of L. The downward maps are inclusions. Let $G = Gal(L/K)$. Now we take the long exact sequence of cohomology of each of the short exact rows. Since cohomology is natural, we get a morphism of long exact sequences. The downward maps remain injective because $(-)^G$ is left-exact,

$$
\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & (\mathcal{O}_L^\times)^G \arrow[r] \arrow[d] & (L^\times)^G \arrow[r] \arrow[d] & (P_L)^G \arrow[r] \arrow[d] & H^1(G, \mathcal{O}_L^\times) \arrow[r] \arrow[d] & H^1(G, L^\times) \arrow[d] \\
1 \arrow[r] & (\mathbb{I}_{L,S_\infty})^G \arrow[r] & (\mathbb{I}_L)^G \arrow[r] & (I_L)^G \arrow[r] & H^1(G, \mathbb{I}_{L,S_\infty}) \arrow[r] & H^1(G, \mathbb{I}_L)
\end{tikzcd}
$$

By Galois theory, $(\mathcal{O}_L^\times)^G = \mathcal{O}_K$ and $(L^\times)^G = K^\times$. Furthermore, by Lemma 5.9, we also have $(\mathbb{I}_{L,S_\infty})^G = \mathbb{I}_{L,S_\infty}$ and $(\mathbb{I}_L)^G = \mathbb{I}_K$. By Hilbert's theorem 90, $H^1(G, L^\times) = 1$ and by Lemma 5.9, $H^1(G, \mathbb{I}_L) = 1$. Therefore, extending the sequence through the image of the maps $K^\times \to (P_L)^G$ and $\mathbb{I}_K \to (I_L)^G$ we get the commutative diagram with exact rows,

$$
\begin{tikzcd}
 & & 1 \arrow[dr] & & 1 & & \\
 & & & P_K \arrow[ur] \arrow[dr] \arrow[ddd, hook] & & & \\
1 \arrow[r] & \mathcal{O}_K \arrow[r] \arrow[d, hook] & K^\times \arrow[ur] \arrow[d, hook] & & (P_L)^G \arrow[r] \arrow[d, hook] & H^1(G, \mathcal{O}_L^\times) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{I}_{K,S_\infty} \arrow[r] & \mathbb{I}_K \arrow[dr] & & (I_L)^G \arrow[r] & H^1(G, \mathbb{I}_{L,S_\infty}) \arrow[r] & 1 \\
 & & & I_K \arrow[ur] \arrow[dr] & & & \\
 & & 1 \arrow[ur] & & 1 & &
\end{tikzcd}
$$

This gives a commutative diagram with exact rows and columns,

$$
\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & P_K \arrow[r] \arrow[d] & (P_L)^G \arrow[r] \arrow[d] & H^1(G, \mathcal{O}_L^\times) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I_K \arrow[r] & (I_L)^G \arrow[r] & H^1(G, \mathbb{I}_{L,S_\infty}) \arrow[r] & 1
\end{tikzcd}
$$

The direct limit is an exact functor so applying the direct limit over all finite Galois extensions L/K gives rise to a commutative diagram with exact rows and columns,

$$
\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & \varinjlim_{L/K} P_K \arrow[r] \arrow[d] & \varinjlim_{L/K} (P_L)^{G_{L/K}} \arrow[r] \arrow[d] & \varinjlim_{L/K} H^1(G_{L/K}, \mathcal{O}_L^\times) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \varinjlim_{L/K} I_K \arrow[r] & \varinjlim_{L/K} (I_L)^{G_{L/K}} \arrow[r] & \varinjlim_{L/K} H^1(G_{L/K}, \mathbb{I}_{L,S_\infty}) \arrow[r] & 1
\end{tikzcd}
$$

However, $\varinjlim_{L/K} P_K = P_K$ and $\varinjlim_{L/K} I_K = I_K$ because the directed systems are constant. Furthermore, let $\bar{G} = Gal(\bar{K}/K)$ be the absolute Galois group. By Lemma 5.5, we know that,

$$H^r(\bar{G}, \mathcal{O}_{\bar{K}}^\times) = \varinjlim H^r(\bar{G}/H, (\mathcal{O}_{\bar{K}}^\times)^H)$$

where the direct limit runs over all open normal subgroups. However, the open normal subgroups correspond exactly to finite Galois extensions L/K. Given an open normal subgroup H we get an intermediate field $K \subset \bar{K}^H \subset \bar{K}$ with galois group $Gal(\bar{K}/\bar{K}^H)$. Since H is normal, the extension $\bar{K}^H/K$ is galois and $Gal(\bar{K}^H/K) \cong \bar{G}/H$. Furthermore, let $L = \bar{K}^H$ then $(\mathcal{O}_{\bar{K}}^\times)^H = \mathcal{O}_{\bar{K}}^\times \cap L = \mathcal{O}_L^\times$. Therefore, the cohomology of the absolute Galois group can be identified with the direct limit of the cohomology of finite Galois extensions of K,

$$H^r(\bar{G}, \mathcal{O}_{\bar{K}}^\times) = \varinjlim_{L/K} H^r(Gal(L/K), \mathcal{O}_L^\times)$$

Furthermore, let K_v be the completion of K at the non-archimedean prime v and let $\bar{K}_v$ be its algebraic closure. Let $\bar{G}_v = Gal(\bar{K}_v/K)$. As before,

$$H^r(\bar{G}_v, \mathcal{O}_{\bar{K}_v}^\times) = \varinjlim H^r(\bar{G}_v/H, (\mathcal{O}_{\bar{K}_v}^\times)^H)$$

over open normal subgroups which correspond to finite Galois extensions $K_v \subset \bar{K}_v^H \subset \bar{K}_v$ of the local field at v. Since H is open $\bar{K}_v^H/K_v$ is finite and since H is normal $\bar{K}_v^H/K_v$ is galois with $Gal(\bar{K}_v^H/K_v) \cong \bar{G}_v/H$. Therefore, we can write the Galois group of the local algebraic closure as the direct limit of the Galois groups of all finite galois extensions of the local field K_v,

$$H^r(\bar{G}_v, \mathcal{O}_{\bar{K}_v}^\times) = \varinjlim_{L_w/K_v} H^r(Gal(L_w/K_v), \mathcal{O}_w^\times)$$

By Lemma 5.8,

$$H^r(G_{L/K}, \mathbb{I}_{L,S_\infty}) = \prod_{v \nmid \infty} H^r(G_w, \mathcal{O}_w^\times) \times \prod_{v \mid \infty} H^r(G_w, L_w^\times)$$

and thus, applying Hilbert's theorem 90,

$$H^1(G_{L/K}, \mathbb{I}_{L,S_\infty}) = \prod_{v \nmid \infty} H^1(G_w, \mathcal{O}_w^\times)$$

Finally,

$$\varinjlim_{L/K} H^1(G_{L/K}, \mathbb{I}_{L,S_\infty}) = \prod_{v \nmid \infty} \varinjlim_{L/K} H^1(G_w, \mathcal{O}_w^\times) = \prod_{v \nmid \infty} H^1(\bar{G}_v, \mathcal{O}_{\bar{K}_v}^\times)$$

Now we define the space $Ш_K$ as the kernel of the induced map,

$$H^1(\bar{G}, \mathcal{O}_{\bar{K}}^\times) \longrightarrow \prod_{v \nmid \infty} H^1(\bar{G}_v, \mathcal{O}_{\bar{K}_v}^\times)$$

Putting everything together, we get a commutative diagram with exact rows and columns,

$$\begin{tikzcd}
 & 1 \arrow[r] \arrow[d] & 1 \arrow[r] \arrow[d] & Ш_K \arrow[d] \arrow[dddll, dashed] & \\
1 \arrow[r] & P_K \arrow[r] \arrow[d] & \varinjlim(P_L^{G_{L/K}}) \arrow[r] \arrow[d] & H^1(\bar{G}, \mathcal{O}_{\bar{K}}^\times) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I_K \arrow[r] \arrow[d] & \varinjlim(I_L^{G_{L/K}}) \arrow[r] \arrow[d] & \prod H^1(\bar{G}_v, \mathcal{O}_{\bar{K}_v}^\times) \arrow[r] \arrow[d] & 1 \\
 & C\ell(K) \arrow[r] & \text{coker} \arrow[r] & \text{coker} &
\end{tikzcd}$$

and by the snake lemma we get a connecting map forming an exact sequence of the kernels and cokernels. However, consider an ideal class $[J] \in C\ell(K)$. This ideal class is in the image of $J \in I_K$ under the quotient map. The map $I_K \to I_L^{G_{L/K}}$ takes $I \mapsto I\mathcal{O}_L$ which is clearly fixed by $G_{L/K}$. However, by Lemma 5.4, there exists a finite Galois extension L/K such that for any ideal I in $\mathcal{O}_K$ the ideal $I\mathcal{O}_L$ is principal. In fact, every ideal of K is principal in the Hilbert class field H_K. Furthermore, if F is a field extension of L then I is also principal in F since $F \supset L$ contains an element which generates I. Thus, $I\mathcal{O}_L$ is principal in the direct limit, $\varinjlim(I_L^{G_{L/K}})$. Therefore, $I\mathcal{O}_L$ is in the image of the principal ideals and thus maps to zero in the cokernel. By commutativity of the diagram, the map $C\ell(K) \to$ coker is the zero map. Therefore, the kernel-cokernel exact sequence reduces to,

$$1 \longrightarrow Ш_K \longrightarrow C\ell(K) \longrightarrow 1$$

and thus the connecting map $Ш_K \xrightarrow{\sim} C\ell(K)$ is an isomorphism.

5 Lemmata

Lemma 5.1. *If $f : A \to F$ is a surjective map of abelian groups and F is free then $A \cong \ker f \oplus F$.*

Proof. Let $f : A \to F$ be a surjective map of abelian groups where F is a free abelian group. Since F is free, it is a projective object in the category of abelian groups so we have a commutative diagram which I have extended to an exact sequence,

$$\begin{tikzcd}
 & & & F \arrow[dl, dashed, "h"'] \arrow[d, "\mathrm{id}_F"] & \\
0 \arrow[r] & \ker f \arrow[r, hook] & A \arrow[r, two heads, "f"] & F \arrow[r] & 0
\end{tikzcd}$$

Since f is surjective and F is projective there exits a map $h : F \to A$ such that the diagram commutes. Thus, $f \circ h = \mathrm{id}_F$ so the exact sequence splits on the right. Therefore, $A \cong \ker f \oplus F$. $\square$

Lemma 5.2. *In a number field K, the group $U_{K,S}$ of S-units is a finitely generated abelian group. In particular, $U_{K,S} \cong \mathcal{O}_K^\times \oplus F$ where F is the free abelian group on $k \le |S|$ generators.*

Proof. Let S be a finite set of primes in $\mathcal{O}_K$. Consider the map, $\Phi : U_{K,S} \to \mathbb{Z}^S$ defined by,

$$u \mapsto (\mathrm{ord}_{\mathfrak{p}_1}(u), \dots, \mathrm{ord}_{\mathfrak{p}_k}(u))$$

where $\mathfrak{p}_i$ enumerates the primes in S. This map is clearly a homomorphism because the order map is a valuation. The image of this map is a subgroup of the free abelian group $\mathbb{Z}^S$ and therefore the image $F = \mathrm{Im}(\Phi)$ is itself free abelian. Suppose that $u \in \ker \Phi$ then we know that $\mathrm{ord}_{\mathfrak{p}}(u) = 0$ for each $\mathfrak{p} \in S$. Thus, no prime in S appears in the factorization of (u) but u is an S unit so no prime can appear in its factorization at all. Thus, $(u) = \mathcal{O}_K$ so $u \in \mathcal{O}_K^\times$ is a unit. Therefore, $\ker \Phi = \mathcal{O}_K^\times$. By the previous lemma, since $\Phi : U_{K,S} \to F$ is a surjective map of abelian groups with F free, we know that $U_{K,S} \cong \mathcal{O}_K^\times \oplus F$. Therefore $U_{K,S}$ is finitely generated by Dirichlet's unit theorem and the fact that $F \subset \mathbb{Z}^S$ is finitely generated since S is finite. $\square$

Lemma 5.3. *Let K be a number field. The set of S-units for a finite set of primes of K modulo n^{th} powers is finite. That is, the group, $U_{K,S}/(U_{K,S} \cap (K^\times)^n)$ is finite.*

Proof. This is immediate from the previous lemma. Since $U_{K,S}$ is finitely generated as an abelian group its quotient by the image of the n^{th} power map is torsion but also finitely generated and thus finite. $\square$

Lemma 5.4. *Let K be a number field. Then there exists a finite galois extension L/K such that every ideal of $\mathcal{O}_K$ is principal in $\mathcal{O}_L$. Explicitly, for any ideal $I \subset \mathcal{O}_K$ the ideal $I\mathcal{O}_L$ is principal.*

Proof. Let $C\ell(K)$ be the class group of K with order h_K. Let $[J_1], \cdots, [J_h]$ enumerate the elements of $C\ell(K)$ with chosen representatives. Since the class group is finite, it has exponent dividing its order. Thus, $J_k^h = (a_k)$ is a principal ideal in K for each k. Consider the field L which is the galois closure of $K(\sqrt[h]{a_1}, \cdots, \sqrt[h]{a_h})$. Consider the $\mathcal{O}_L$-ideals $J_k\mathcal{O}_L$ and $(\sqrt[h]{a_k})$. We know that $(J_k\mathcal{O}_L)^h = a_k\mathcal{O}_L = (a_k)$ and $(\sqrt[h]{a_k})^h = (a_k)$. Thus, $(J_k\mathcal{O}_L)^h = (\sqrt[h]{a_k})^h$ so by the uniqueness of Dedekind prime factorization,

$$J_k\mathcal{O}_L = (\sqrt[h]{a_k})$$

and thus each J_k are principal in $\mathcal{O}_L$. Take any ideal $I \subset \mathcal{O}_K$. Consider the image $[I] \in C\ell(K)$. Since $C\ell(K)$ is finite, $I \sim J_k$ for some k. Therefore, there exist constants $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha I = \beta J_k$. Therefore, $\alpha I\mathcal{O}_L = \beta J_k\mathcal{O}_L = \beta(\sqrt[h]{a_k})$ so $I\mathcal{O}_L$ is itself principal. $\square$

Lemma 5.5. *Let G be a profinite group and M a G-module. Then,*

$$\varinjlim H^r(G/H, M^H) = H^r(G, M)$$

where H runs over open normal subgroups.

Proof. The groups $H^r(G/H, M^H)$ form a directed system where $H_1 \subset H_2$ gives maps $G/H_1 \to G/H_2$ and $M^{H_2} \to M^{H_1}$ which induce a map $H^r(G/H_1, M^{H_1}) \to H^r(G/H_2, M^{H_2})$. Furthermore, for the normal subgroups $H \triangleleft G$ the inflation maps,

$$\inf : H^r(G/H, M^H) \to H^r(G, M)$$

give inclusions of each $H^r(G/H, M^H)$ into $H^r(G, M)$. Since G is profinite, if we restrict to the open subgroups then $H^r(G, M)$ with the inflation maps is universal with respect to cocones over the directed system.

$\square$

Lemma 5.6. *Let L/K be a finite Galois extension of number fields with Galois group $G = Gal(L/K)$. Let v be a prime of K with a prime w in L such that $w \mid v$. Let $G_w = Gal(L_w/L_v)$ be the decomposition group at $w \mid v$ then,*

$$H^r(G, \prod_{w|v} L_w^\times) \cong H^r(G_w, L_w^\times)$$

and likewise,

$$H^r(G, \prod_{w|v} \mathcal{O}_w^\times) \cong H^r(G_w, \mathcal{O}_w^\times)$$

Proof. We use the fact that,

$$\prod_{w|v} L_w^\times = \mathrm{Ind}_{G_w}^G L_w^\times$$

and similarly, that,

$$\prod_{w|v} \mathcal{O}_w^\times = \mathrm{Ind}_{G_w}^G \mathcal{O}_w^\times$$

Therefore, by Shapiro's Lemma,

$$H^r(G, \prod_{w|v} L_w^\times) = H^r(G, \mathrm{Ind}_{G_w}^G L_w^\times) = H^r(G_w, L_w^\times)$$

and similarly,

$$H^r(G, \prod_{w|v} \mathcal{O}_w^\times) = H^r(G, \mathrm{Ind}_{G_w}^G \mathcal{O}_w^\times) = H^r(G_w, \mathcal{O}_w^\times)$$

$\square$

Lemma 5.7. *Let L/K be a finite Galois extension of number fields. Let $\mathfrak{p}$ be a finite prime in K and $\mathfrak{P}$ a prime of L lying above v with ramification index $e_{\mathfrak{P}|\mathfrak{p}}$ and decomposition group $D(\mathfrak{P}) = Gal(L_\mathfrak{P}/K_\mathfrak{p})$. Then,*

$$H^1(D(\mathfrak{P}), \mathcal{O}_\mathfrak{P}^\times) \cong \mathbb{Z}/e_{\mathfrak{P}|\mathfrak{p}}\mathbb{Z}$$

Proof. Let $D = Gal(L_\mathfrak{P}/K_\mathfrak{p})$. Consider the short exact sequence associated to a local field L_w,

$$1 \longrightarrow \mathcal{O}_\mathfrak{P}^\times \longrightarrow L_\mathfrak{P}^\times \xrightarrow{\mathrm{ord}_\mathfrak{P}} \mathbb{Z} \longrightarrow 1$$

This short exact sequence gives rise to a long exact sequence of cohomology,

$$1 \longrightarrow (\mathcal{O}_\mathfrak{P}^\times)^D \longrightarrow (L_\mathfrak{P}^\times)^D \xrightarrow{\mathrm{ord}_\mathfrak{P}} \mathbb{Z}^D \longrightarrow H^1(D, \mathcal{O}_\mathfrak{P}^\times) \longrightarrow H^1(D, L_\mathfrak{P}^\times) \longrightarrow \cdots$$

However, by Hilbert's Theorem 90, $H^1(D, L_\mathfrak{P}^\times) = 1$ the exact sequence becomes,

$$1 \longrightarrow \mathcal{O}_\mathfrak{p}^\times \longrightarrow K_\mathfrak{p}^\times \xrightarrow{\mathrm{ord}_\mathfrak{P}} \mathbb{Z} \xrightarrow{\varphi} H^1(D, \mathcal{O}_\mathfrak{P}^\times) \longrightarrow 1$$

However, the image of $\mathrm{ord}_\mathfrak{P}$ on $K_\mathfrak{p}^\times$ is determined by,

$$\mathrm{ord}_\mathfrak{P}(\mathfrak{p}) = \mathrm{ord}_\mathfrak{P}\left(\prod_{\mathfrak{P}'|\mathfrak{p}} \mathfrak{P}'^e\right) = \mathrm{ord}_\mathfrak{P}(\mathfrak{P}^e) = e$$

By exactness, $\ker\varphi = \mathrm{Im}(\mathrm{ord}_{\mathfrak{P}}) = e\mathbb{Z}$ so by the first isomorphism theorem,

$$H^1(D, \mathcal{O}_{\mathfrak{P}}^\times) = \mathbb{Z}/e\mathbb{Z}$$

□

Lemma 5.8. *Let L/K be a finite Galois extension of number fields with $G = Gal(L/K)$. Let S be a finite set of primes in K with T the set of primes in L lying above some prime in S. Let $G_v = Gal(L_w/L_v)$ be the decomposition group at $w \mid v$ then,*

$$H^r(G, \mathbb{I}_{L,T}) = \prod_{v\notin S} H^r(G_w, \mathcal{O}_w^\times) \times \prod_{v\in S} H^r(G_w, L_w^\times)$$

Proof. By definition,

$$\mathbb{I}_{L,T} = \prod_{w\notin T} \mathcal{O}_w^\times \times \prod_{w\in T} L_w^\times = \prod_{v\notin S}\prod_{w|v} \mathcal{O}_w^\times \times \prod_{v\in S}\prod_{w|v} L_w^\times$$

which is a decomposition as a product of G-modules. Therefore, by the fact that cohomology commutes with products,

$$H^r(G, \mathbb{I}_{L,T}) = \prod_{v\notin S} H^r(G, \prod_{w|v} \mathcal{O}_w^\times) \times \prod_{v\in S} H^r(G, \prod_{w|v} L_w^\times)$$

Thus, by the previous lemma,

$$H^r(G, \mathbb{I}_{L,T}) = \prod_{v\notin S} H^r(G_w, \mathcal{O}_w^\times) \times \prod_{v\in S} H^r(G_w, L_w^\times)$$

□

Lemma 5.9. *Let L/K be a finite Galois extension of number fields with $G = Gal(L/K)$ then,*

$$(\mathbb{I}_L)^G = H^0(G, \mathbb{I}_L) = \mathbb{I}_K \quad \textit{and} \quad H^1(G, \mathbb{I}_L) = 1$$

Proof. We can write,

$$\mathbb{I}_L = \varinjlim_{T_0 \subset T} \mathbb{I}_{L,T}$$

where if $T \subset T'$ then $\mathbb{I}_{L,T} \subset \mathbb{I}_{L,T'}$. Thus, we can choose S_0 to contain the set of ramified primes (since there are finitely many) and T_0 to be all such primes lying over T_0. Thus,

$$H^r(G, \mathbb{I}_L) = \varinjlim_{T_0\subset T} H^r(G, \mathbb{I}_{L,T}) = \varinjlim_{S_0\subset S} \prod_{v\notin S} H^r(G_w, \mathcal{O}_w^\times) \times \prod_{v\in S} H^r(G_w, L_w^\times)$$

However, by assumption, all the ramified primes are in S so by Lemma 5.7,

$$H^1(G_w, \mathcal{O}_w^\times) = 0$$

Furthermore, by Hilbert's theorem 90,

$$H^1(G_w, L_w^\times) = 0$$

Thus, each cohomology group in the product is zero so the limit of these groups is zero as well and therefore,

$$H^1(G, \mathbb{I}_L) = 0$$

Furthermore,

$$\begin{aligned} H^0(G, \mathbb{I}_L T) &= \varinjlim_{T_0 \subset T} H^r(G, \mathbb{I}_{L,T}) = \varinjlim_{S_0 \subset S} \prod_{v \notin S} H^0(G_w, \mathcal{O}_w^\times) \times \prod_{v \in S} H^0(G_w, L_w^\times) \\ &= \varinjlim_{S_0 \subset S} \prod_{v \notin S} (\mathcal{O}_w^\times)^{G_w} \times \prod_{v \in S} (L_w^\times)^{G_w} = \varinjlim_{S_0 \subset S} \prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} L_v^\times = \mathbb{I}_K \end{aligned}$$

□