1 Innequalities of Class Field Theory

Theorem 1.1 (First Innequality)**.** Let L/K be a finite extension of number fields and $C_K = \mathbb{I}_K/K^\times$ and $C_L = \mathbb{I}_K/K^\times$. There is a norm map $N_{L/K} : C_L \to C_K$ then,

- the group $CK/N_{L/K}$ is finite.
- Let $h = |CK/N_{L/K}|$, we have $h \leq [L : S]$
- If L/K is abelian then $h \geq [LK]$

Theorem 1.2 (Second Innequality)**.** If L/K is abelian, then $h \leq [L : K]$

2 Artin Reciprocity Existence April (16)

Theorem 2.1. The theorem has two parts,

(a) Let $r : \mathbf{A}^\times \to Gal(L/K)$ be denoted by $r((a_v)) = \prod_v r_v(a_v)$ then $r(a) = 1$ for all $a = (a) \in K^\times \subset \mathbf{A}^\times$.

(b) Let $\alpha \in Br(L/K) = H^2(Gal(L/K), L^\times)$ then $\sum_v inv_v(\alpha) = 0$.

Lemma 2.2. Let $(a_v) \in \mathbf{A}_K^\times$ and $G = Gal(L/K)$ for L/K abelian, let $\chi \in \hat{G} = H_m(G, \mathbb{Q}/\mathbb{Z}) = \hat{H}^1(G, \mathbb{Z}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z})$. Then,

$$\sum_v inv_v(\bar{a}_v, \delta(x)) = \chi(r_{L/K}((a_v)))$$

Where $(\bar{a}_v) \in \hat{H}^0(G, \mathbf{A}_K^\times)$ and $\delta(x) \in \hat{H}^2(G, \mathbb{Z})$ is mapped to,

$$\bar{a}_v \cup \delta(x) \in \hat{H}^2(G, \mathbf{A}_K^\times) \hookrightarrow \bigoplus_v H^2(G^\nu, (L^\nu)^\times)$$

Corollary 2.3. Let L/K be a cyclic cyclotomic extension. Suppose that (a) of reciprocity theorem holds for K then part (b) holds fror any $\alpha \in Br(L/K)$. In particular, $(a) \implies (b)$.

Proof. Since L/K is cyclic, we may take $\chi \in \hat{G}$ injective then,

$$\cup\delta\chi : \hat{H}^0(G, A) \to \hat{H}^2(G, A) = \hat{H}^2(G, A \otimes \mathbb{Z})$$

is an isomorphism. Apply this to $K^\times$ so we have,

$$K^\times/N_{L/K}L^\times = \hat{H}^0(G, L^\times) \xrightarrow{\cup\delta\chi} Br(L/K) = H^2(G, L^\times)$$

which is an isomorphism. Take $\alpha = \bar{a} \cup \delta\chi$ for some $a \in K^\times$ and $\bar{a}$ is the image of a in $\hat{H}^0$. The lemma above then yields,

$$\sum_v inv_v(\alpha) = \sum_v inv_v(\bar{a} \cup \delta\chi) = \chi(r_{L/K}(a))$$

Assuming (a) we then have $r_{L/K}(a) = 1$ so $\chi(r_{L/K}(a)) = 1$ so $\sum_v inv_v(\alpha_v) = 0$. Thus, $(a) \implies (b)$.

□

Summary of Proof.

Proof. We have shown that,

1. $(a) \implies (b)$ for α split by a cyclic extension for which (a) holds.
2. Every α is split by some cyclic extension for which (a) holds.
3. We know $a)$ if L/K is cyclotomic.
4. Therefore, we have proven (b) in generality.
5. Finally, $(b) \implies (a)$.

□

$(b) \implies (a)$. It suffices to show that $\forall \chi \in \hat{G}$ that $\chi(r_{L/K}(a)) = 1$. Let $a \in K^\times$ for a^* the image of a in $K^\times/N_{L/k}L^\times = \hat{H}^2(G, L^\times)$. Then, using the fact that the cup product is natural,

$$\begin{array}{ccc} \hat{H}^0(G, L^\times) & \xrightarrow{\cup\delta\chi} & \hat{H}^2(G, L^\times) \\ \downarrow & & \downarrow \\ \hat{H}^0(G, \mathbb{A}_L^\times) & \xrightarrow{\cup\delta\chi} & \hat{H}^2(G, \mathbb{A}^t \times_L) \end{array}$$

we see that,

$$\begin{array}{ccc} a^* \cup \delta\chi \in & & \hat{H}^2(G, L^\times) \subset Br(K) \\ \downarrow & & \downarrow \\ \bar{a} \cup \delta\chi \in & & \hat{H}^2(G, \mathbb{A}_L^\times) \end{array}$$

By part (b), we know that,

$$\sum_v inv_v(a^* \cup \delta\chi) = \sum_v inv_v(\bar{a} \cup \delta\chi) = \chi(r_{L/K}(a))$$

Therefore, $\chi(r_{L/K}(a)) = 1$ for each $\chi \in \hat{G}$. □

Corollary 2.4. Suppose $F \subset F' \subset E$ is a tower of abelian extensions of p-adic fields. Let $G = Gal(E/K) \supset H = Gal(E/F)$. Suppose that,

$$\chi' \in \operatorname{Hom}(G/H, \mathbb{Q}/\mathbb{Z}) = \widehat{G/H} = H^1(G/H, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G/H, \mathbb{Z})$$

is mapped to,

$$\chi \in \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z})$$

with $inf^G_{G/H}(\delta(\chi')) = \delta(inf^G_{G/H}(\chi') = \delta(\chi)$. Suppose $a \in F^\times$ then $\chi(r_{E/F}(a)) = \chi^1(r_{F'/F}(a))$.

Proof. $\chi(r_{E/F}(a)) = inv_F(\bar{a} \cup \delta(\chi)) = inv_F(\bar{a} \cup \delta(\chi')) = \chi'(r_{F'/F}(a))$ then $\bar{a} \in \hat{H}^0(G, E^\times)$ and $a \in \hat{H}^0(G/H, F'^\times)$.

$$\begin{array}{ccccc} F^\times & \xrightarrow{r_{F^{ab}/F}} & W_F & \longrightarrow & Gal(F^{ab}/F) \\ & & \downarrow & & \downarrow \\ & & Frob^{\mathbb{Z}} & \hookrightarrow & Gal(F^{un}/F) = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} \end{array}$$

∎

Theorem 2.5 (Artin Existence Theorem)**.** Let K be a number field let $C_K = \mathbb{A}_K^\times / K^\times$ let $U \subset C_K$ be an open subgroup of finite index. Then, there is an ablian extension L/K such that $U = N_{L/K} C_L$. We call U a norm subgroup.

Lemma 2.6. Suppose $V \subset U$ and V is a norm subgroup then U is a norm sugbgroup.

Proof. Let $V = N_{E/K} C_E$ thus $r : C_K / N_{E/K} C_E \xrightarrow{\sim} Gal(E/K)$ maps $U/V \xrightarrow{r} H = r(V)$. Let $L = E^H$. Thus, $C_K/U \xrightarrow{\sim} (C_K/V)/(U/V) = Gal(E/K)/Gal(E/L) = Gal(L/K)$. By the corollary, $\forall a \in C_k$ then $r_{E/K}(a)|_L = r_{L/K}(a)$. Therefore, $\ker r_{L/K} = U$ but by the reciprocity law, $\ker r_{L/K} = N_{L/K} C_L$ so U is a norm subgroup. ∎

Proposition 2.7. Suppose that $\zeta_n \in K$ let $S \supset S_\infty$ be a sufficiently large set of primes containing all primes dividing n and generators of $Cl(K)$. Suppose $a \in K^\times$ satisfies,

$$[a] \forall v \in S, a \in (K_n^\times)^n \quad [b] \forall v \notin S, a \in \mathcal{O}_v^\times$$

then $a \in (K^\times)^n$.

Proof. Let $L = K(\sqrt[n]{a})$. We know that H^1 is abelian over K by hypothesis, and we show $L = K$. y $[a]$, every $v \in S$ splits completely in L. On the other hand, every $v \notin S$ is unramified in L because $a \in \mathcal{O}_v^\times$ and $K_v(\sqrt[n]{a})$. If $a \in 1 + m_v$ then it is already an n^{th} root. $\bar{a} \in (\mathcal{O}_v/m_v)^\times$ which implies $K_v(\sqrt[n]{a}) = K_v(\sqrt[n]{\omega(\bar{a})})$ is unramified. However, $K_v^\times = N_{Lw/K_v} L_w^\times$ for $v \in S$ which implies that $\mathcal{O}_v^\times = N_{L_w/K_v} \mathcal{O}_w^\times \subset N_{L_w/K} L_w^\times$ for all $n \notin S$. Thus, $N_{L/K} \mathbb{A}_L^\times \supset \mathbb{A}_{K,S}^\times$ However, S has been chosen to contain a set of generators of $CL(K)$ so we see that $\mathbb{A}_{K,S}^\times \cdot K^\times = \mathbb{A}_K^\times$ so $N_{L/K} C_L = C_K$. So $[L : K] = C_K / N_{L/K} C_L = 1$ so $\sqrt[n]{a} \in K$. ∎

Lemma 2.8. LEt p be a prime, $\zeta_p \in K$. Let $\bar{V} \subset C_K$ be an open subgroup (the image of $V \subset \mathbb{A}_K^\times$) such that C_K/V is anihilated by p. Then $\bar{V}$ is a norm subgroup.

3 April 18

Lemma 3.1. Let p be a prime, $\zeta_p \in K$, and $V \subset \mathbb{A}_K^\times$ open with $\delta = V \cdot K^\times / K^\times$ such that $(C_K)^p \subset \bar{V}$ i.e. $p \cdot D_K/\bar{V} = 0$ then $\bar{V}$ is a norm subgroup.

Proof. Let S be a set of places as in the proposition $\mathbb{A}_{K,S}^\times \cdot K^\times / K^\times = C_K$ such that $S \supset S_\infty$. Let $\mathcal{U} = U_{K,S}$ be the groups of S-units of K then $\mathcal{U}/T(\mathcal{U}) = \mathbb{Z}^{|S|-1}$ by the unit theorem. Let $L = K(\sqrt[p]{u}) = K(u^{1/p}, u \in \mathcal{U})$ This a finite extension. Let,

$$W = W_S = \prod_{v \in S} (K_v^\times)^p \times \prod_{v \notin S} \mathcal{O}_v^\times \subset \mathbb{A}_{K,S}^\times$$

We prove that $\bar{W} = W \cdot K^\times / K^\times \subset C_K = N_{L/K}(C_L)$. In particular we need to prove two facts,

1. $W \subset N_{L/K} \mathbb{A}_L^\times$
2. $[C_K : \bar{W}] = [C_K : N_{L/K} C_L] = p^| S|$

The proof of the first fact is purely local. For any v, we have $N_{L/K} L_v^\times \supset (K_v^\times)^p$ and $L_v = K_v(\sqrt[p]{u})$. By the local Artin map, $K_v^\times / N_{L_w^\times / K_v^\times} L_w^\times \cong Gal(L_w^\times / K_n^\times) \cong (\mathbb{Z}/p\mathbb{Z})^r$ so $K_v^\times / N_{L_w^\times / K_v^\times} L_w^\times$ has exponent p and thus $(K_v^\times)^p \subset N_{L/K} L_w^\times$. For $n \notin S$, L is unramified at v so the local units are contained in the image of the local norm.

To prove 2, we know that,

$$[C_K : N_{L/K} C_L] = |Gal(L/K)| = [\mathcal{U} \cdot (K^\times)^p : (K^\times)^p]$$

by local reciprocity and kummer theory. To see this, consider the short exact sequence,

$$1 \longrightarrow \mu_p \longrightarrow \bar{K}^\times \xrightarrow{u \mapsto u^p} \bar{K}^\times \longrightarrow 1$$

Appllying the functor $H^1(Gal(L/K), -)$ by Kummer theory,

$$K^\times / (K^\times)^p \cong \operatorname{Hom}\big(Gal(\bar{K}/K), \mu_p\big)$$

since $\mu_p \subset K$. It suffices to show that,

$$[C_K : \bar{W}] = [\mathcal{U} \cdot (K^\times)^p : (K^\times)^p] = |\mathcal{U}/\mathcal{U}^p| = p^{|S|-1} \cdot p$$

from the torsion-free and torsion groups respectively. However, $\mathcal{U} \cap (K^\times)^p = \mathcal{U}^p$. Now,

$$[C_K : \bar{W}] = [\mathbb{A}_{K,S}^\times \cdot K^\times : W \cdot K^\times] = \frac{[\mathbb{A}_{K,S}^\times : W]}{[\mathbb{A}_{K,S}^\times \cap K^\times : W \cap K^\times]} = \frac{[\mathbb{A}_{K,S}^\times : W]}{[\mathcal{U} : \mathcal{U}^p]}$$

because $K^\times \cap W \subset (K^\times)^p$ by rhe proposition. However,

$$\mathbb{A}_{K,S}^\times / W = \prod_{v \in S} K_v^\times / (K_v^\times)^p$$

But if F is a local field containing ζ_p then $[F^\times : (F^\times)^p] = \frac{p^2}{||p||_F}$ thus,

$$|\mathbb{A}_{K,S}^\times / W| = \prod_{v \in S} \frac{p^2}{||p||_v} - \prod_{v \in S} p^2 = p^{2|S|}$$

since $\prod_{v \in S} ||p||_v = \prod_v ||p||_v = 1$ since $||p||_v = 1$ for $v \notin S$. Similarly,

$$[\mathcal{U} : \mathcal{U}^p] = p^{|S|}$$

which implies that,

$$[C_K : \bar{W}] = \frac{p^{2|S|}}{p^{|S|}} = p^{|S|}$$

as required. We have shown that $\bar{\mathcal{U}}$ is an open subgroup. Furthermore, $\bar{V} \supset C_K^p$ and V also contains $\prod_{v \notin S} \mathcal{O}_v^\times$ for some S. Therefore, $\bar{V} \supset \bar{W}$ for some sufficiently large S. Thus $\bar{V}$ is a norm subgroup. $\square$

Lemma 3.2. Let $U \subset C - k$ be an open subgroup of finite index. Suppose there exists a finite cyclic extension K'/K such that $U' = N_{K'/K}^{-1}(U)$ is a norm subgroup of $C_{K'}$. Then U is a norm subgroup.

Corollary 3.3. The lemma holds for K such that $\zeta_p \notin K$.

Proof. Let $K' = K(\zeta_p)$ this is cyclic and $\bar{V}' = N_{K'/K}^{-1}(\bar{V})$ satisfies the hypothesis of the above lemma. Thus,

$$N_{K'/K} : C_{K'}/\bar{V}' \hookrightarrow C_K/\bar{V}$$

Therefore $C_{K'}/\bar{V}'$ is p-torsio. Thus, we reduce to the case of K'. $\square$

Theorem 3.4 (Global Existence)**.** Let $U \subset C_K$ be an open subgroup of finite index then U is a norm subgroup.

Proof. Let $D = [C_K : V]$ and let p be a prime dividing D. Take $K' = K(\zeta_p)$. It suffies, by the above lemma, to prove that $U' = N_{K'/K}^{-1}(U) \subset C_{K'}$ is a norm subgroup. Let $D' = [C_{K'} : U']$ we have $D' \mid D$. By inductin on D, we may assume $D' = D$. Let $C_{K'} \supset V \supset V'$ with $[C_{K'} : V] = p$. By the lemma, V is a norm subgroup corresponding to the cyclic extension L/K'. Let $U'' = N_{L/K'}^{-1}(U')$ if can show $U'' \subset C_L$ is a norm subgroup then we are done by the lemma. It suffices, by induction, to show that $[C_L : U''] < [C_{K'} : U'] = D$. However, we have the injection,

$$N_{L/K} : C_L/U'' \hookrightarrow C_{K'}/U'$$

With $N_{L/K}(C_L) = V$ and the image is V/U' of order $D/p < D$. $\square$

Theorem 3.5 (Kronecker-Weber)**.** Any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Proof. Consider $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times = \left(\mathbb{A}_{\mathbb{Q},\infty}^\times \cdot \mathbb{Q}^\times\right)/\mathbb{Q}^\times$ where $\mathbb{A}_{\mathbb{Q},\infty}^\times = \mathbb{R}_+^\times \times \prod_p \mathbb{Z}_p^\times$. Let $L/\mathbb{Q}$ be an abelian extension and $\bar{U} \subset C_{\mathbb{Q}}$ the corresponding norm subgroup $U \subset \mathbb{A}_{\mathbb{Q}}^\times$ so the map $\prod_p \mathbb{Z}_p^\times \to Gal(L/\mathbb{Q})$ is surjective. The kernel contains U_m for some m where

$$U_m = \{(x_n) \in \prod_p \mathbb{Z}_p^\times \mid (x_v) \equiv 1 \pmod{m}\}$$

so it suffices to show that $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} C_{\mathbb{Q}(\zeta_m)} \supset (\mathbb{R}_+^\times \times U_m) \cdot \mathbb{Q}^\times/\mathbb{Q}^\times$ which implies that $L \subset \mathbb{Q}(\zeta_m)$. We reduce to the case $m = q^r$ for a prime q then the norm at p is surjective on units $p \neq q$. At q,

$$N_{\mathbb{Q}_q(\zeta_{q^r})/\mathbb{Q}_q} \mathbb{Q}_q(\zeta_{q^r})^\times$$

□

4 April 23: Proofs of Local Class Field Theory

Lemma 4.1. Any subgroup $U \subset K^\times$ containing $N(L^\times)$ for some L is a norm subgroup.

Remark 4.2. For $\pi \in K^\times$ a uniformizer. Let $K_{\pi,n}^{Art.}/K$ be the finite abelian extension such that $N((K_{\pi,n}^{Art.})^\times) = \pi^{\mathbb{Z}} \times (1 + \pi^n \mathcal{O}_K)$ if $n \geq 1$. This exists by local existence.

5 Hilbert Theorem 90

Theorem 5.1. Let L/K be a finite Galois extension then $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.

Proof. Let $\varphi \in Z^1(G, L^\times)$. We need to show that $\varphi \in B^1(G, L^\times)$ i.e. there exists some $m \in L^\times$ such that $\varphi(g) = (g \cdot m)m^{-1}$. Pick $a \in L^\times$. Construct,

$$m = \sum_{g \in G} \varphi(g) \cdot g(a)$$

We may ensure that $m \neq 0$ because the characters $g : L^\times \to L^\times$ are linearly independent the linear combination,

$$\sum_{g \in G} \varphi(g) g$$

is a nonzero character and thus does not vanish at some $a \in L^\times$. Now take,

$$g \cdot m = \sum_{h \in G} g\left(\varphi(h) \cdot h(a)\right) = \sum_{h \in G} g(\varphi(h)) \cdot gh(a)$$

However, since $\varphi \in Z^1(G, L^\times)$ then $g\varphi(h) = \varphi(gh)\varphi(g)^{-1}$ which implies that,

$$g \cdot m = \varphi(g)^{-1} \sum_{h \in G} \varphi(gh) \cdot gh(a) = \varphi(g)^{-1} m$$

Therefore,

$$\varphi(g) = \frac{m}{g \cdot m} = \frac{g(m^{-1})}{m^{-1}} \in B^1(G, L^\times)$$

$\square$

Example 5.2. Assume that L/K is cyclic then,

$$H^1(G, L^\times) = \hat{H}^{-1}(G, L^\times) = \ker \mathrm{Nm}_G / \mathrm{Im}((\sigma - 1)) = 0$$

Therefore, for any $a \in L^\times$ such that $\mathrm{Nm}_{L/K}(a) = 1$ then $\exists b \in L^\times$ such that

$$a = (\sigma b) b^{-1}$$

Example 5.3. For $L/K = \mathbb{Q}(i)/\mathbb{Q}$ let $a = x + iy$ and $b = m + in$ for $x, y \in \mathbb{Q}$. Then $\mathrm{Nm}_{L/K}(a) = x^2 + y^2 = 1$ implies that,

$$a = \bar{b} b^{-1} = \frac{m - in}{m + in} = \frac{m^2 - n^2}{m^2 + n^2} + \frac{2mn}{m^2 + n^2} i$$

i.e.

$$x = \frac{m^2 - n^2}{m^2 + n^2} \qquad y = \frac{2mn}{m^2 + n^2} \quad \text{for} \quad m, n \in \mathbb{Q}$$

Remark 5.4. We may also consider L/K infinite Galois. Then, over the finite subextensions $K \subset L' \subset L$,

$$\mathrm{Gal}(L/K) = \varprojlim_{L' \subset L} \mathrm{Gal}(L'/K)$$

is a profinite group. Then we define the continuous group cohomology,

$$H^r_{\text{cts}}(\mathrm{Gal}(L/K), L^\times) = \varinjlim_{L' \subset L} H^r(\mathrm{Gal}(L'/K), (L')^\times)$$

and more generally, if G is a profinite group,

$$G = \varprojlim_{H} G/H$$

then,

$$H^r_{\text{cts}}(G, M) = \varinjlim_{H} H^r(G/H, M^H)$$

This can be computed using continuous cochains under the profinite topology.

6 H^2 of Unramifield Extensions

Let L/K be a finite unramified extension of local fields. Recall that the Galois groups is computed on the residue fields, $\mathrm{Gal}(L/K) = \mathrm{Gal}(\ell/k) = \langle \mathrm{Frob}_{L/K} \rangle$ which is cyclic. We need to prove that,

$$H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathbb{Z}/n\mathbb{Z}$$

Definition: Let $U_K = \mathcal{O}_K^\times$ be the units and,

$$U_K^{(i)} = 1 + \mathfrak{m}_K^i$$

be the i-units. Therefore, we have a filtration,

$$U_k \supset U_K^{(1)} \supset U_K^{(2)} \supset U_K^{(3)} \supset \cdots$$

Proposition 6.1. There are exact sequences.

$$1 \longrightarrow U_K^{(1)} \longrightarrow U_K \longrightarrow k^\times \longrightarrow 1$$

and similarly

$$1 \longrightarrow U_K^{(i+1)} \longrightarrow U_K^{(i)} \longrightarrow k \longrightarrow 0$$

via $1 + a\pi_K^n \mapsto a \in k$.

Lemma 6.2. Let $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(\ell/k)$. Then,

$$\hat{H}^r(G, \ell^\times) = \hat{H}^r(G, \ell) = 0$$

Proof. By Hilbert's theorem 90, $H^1(G, \ell^\times) = 0$. Since G is cylic and $\ell^\times$ is finite, we know its Herbrand quotient $h(\ell^\times) = 1$ and thus $H^2(G, \ell^\times) = 0$. Since G is cylic the entire cohomology is determined by these two terms. □

Corollary 6.3. The maps $\mathrm{Nm} : \ell^\times \to k^\times$ and $\mathrm{Tr} : \ell \to k$ are surjective.

Proof. This follows from the vanishing of Tate cohomology via,

$$\hat{H}^0(G, \ell^\times) = \frac{k^\times}{\mathrm{Nm}\ell^\times} = 0$$
$$\hat{H}^0(G, \ell) = \frac{k}{\mathrm{Tr}\ell} = 0$$

□

Lemma 6.4. The norm map $\mathrm{Nm} : U_L \to U_K$ is surjective.

Proof. Consider the diagrams,

$$\begin{tikzcd} U_L \arrow[r, "\mathrm{Nm}"] \arrow[d] & U_K \arrow[d] \\ \ell^\times \arrow[r, "\mathrm{Nm}"] & k^\times \end{tikzcd}$$

$$\begin{tikzcd} U_L^{(i)} \arrow[r, "\mathrm{Nm}"] \arrow[d] & U_K^{(i)} \arrow[d] \\ \ell \arrow[r, "\mathrm{Tr}"] & k \end{tikzcd}$$

Given $a \in U_K$. We want $b \in U_L$ such that $a \in \mathrm{Nm}(b)$. Since $\mathrm{Nm} : \ell^\times \to k^\times$ is surjective we way find $b_0 \in U_L$ such that $\mathrm{Nm}(b_0) \equiv a$ modulo $\mathfrak{m}_k$. Lt $a_1 = a(\mathrm{Nm}(b_0))^{-1} \in U_K^{(1)}$. Since $\mathrm{Tr} : \ell \to k$ is surjective we may find $b_1 \in U_L$ such that $a_2 = a_1(\mathrm{Nm}(b_1)) \in U_K^{(2)}$. Continue this way and let,

$$b = \prod_{i=0}^{\infty} b_i$$

Then,

$$\frac{a}{\mathrm{Nm}(b)} \in \bigcap_{i=1}^{\infty} U_K^{(i)} = 1$$

□

Corollary 6.5. $\hat{H}^r(G, U_L) = 0$ for each $r \in \mathbb{Z}$.

Proof. The lemma implies that $\hat{H}^0(G, U_L) = 0$. By Hilbert 90, $H^1(G, L^\times) = 0$. Furthermore, $L^\times = U_L \oplus \mathbb{Z}$ and thus,

$$H^1(G, L^\times) = H^1(G, U_L) \oplus H^1(G, \mathbb{Z})$$

which implies that $H^1(G, U_L) = 0$. Therefore, $\hat{H}^r(G, U_L) = 0$ for all $r \geq 0$ by the periodicity. □

Lemma 6.6. We may identify cohomology of the trivial module $\mathbb{Z}$ with homs to the trivial module $\mathbb{Q}/\mathbb{Z}$,

$$H^2(G, \mathbb{Z}) \cong \mathrm{Hom}\,(G, \mathbb{Q}/\mathbb{Z})$$

Proof. Consider the exact sequence of trivial G-modules,

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

which gives rise to a long exact sequence of cohomology. □

Theorem 6.7.

$$H^2(G, L^\times) \cong \mathrm{Hom}\,(G, \mathbb{Q}/\mathbb{Z})$$

Proof.

$$H^2(G, L^\times) = H^2(G, U_L) \oplus H^2(G, \mathbb{Z})$$

Furthermore, $H^2(G, U_L) = 0$ and $H^2(G, \mathbb{Z}) = \mathrm{Hom}\,(H, \mathbb{Q}/\mathbb{Z})$. □

Definition: Let L/K be a finite unramified extension. The *invariant map* is the above isomorphism,

$$\mathrm{inv}_{L/K} : H^2(G, L^2) \xrightarrow{\sim} \mathrm{Hom}\,(G, \mathbb{Q}/\mathbb{Z})$$

Furthermore, G is cyclic of degree n so,

$$\mathrm{Hom}\,(G, \mathbb{Q}/\mathbb{Z}) \subset \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$$

Taking the direct limit we obtain,

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(K^{\mathrm{un}}/K), (K^{\mathrm{un}})^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

7 March 11

Today's Goal:
$$\mathrm{inv}_K : H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times) \cong \mathbb{Q}/\mathbb{Z}$$

Remark 7.1. For any Galois extension of fields L/K, we use the shorthand notation,
$$H^2(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$$

Lemma 7.2. Let L/K be a finite extension of local fields of degree $n = [L : K]$. Then the following diagram commutes,
$$\begin{tikzcd}
H^2(K^{\mathrm{ur}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(L^{\mathrm{ur}}/L) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\times n"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Remark 7.3. Note that $L^{\mathrm{un}} = L \cdot K^{\mathrm{ur}}$ by adjoining all coprime to p power roots of unity. So we may view,
$$\mathrm{Gal}(L^{\mathrm{un}}/L) \subset \mathrm{Gal}(K^{\mathrm{ur}}/K)$$
which is compatible with $(K^{\mathrm{un}})^\times \subset (L^{\mathrm{un}})^\times$ which give a map,
$$\mathrm{Res} : H^2(K^{\mathrm{ur}}/K) \to H^2(L^{\mathrm{ur}}/L)$$

Proof. Consider the valuation map $\mathrm{val}_K : (K^{\mathrm{ur}})^\times \to \mathbb{Z}$ via $\varpi_K^n \mapsto n$ which gives a diagram with isomorphisms in the columns,
$$\begin{tikzcd}
H^2(K^{\mathrm{ur}}/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{val}_K"] & H^2(L^{\mathrm{ur}}/L) \arrow[d, "\mathrm{val}_L"] \\
H^2(K^{\mathrm{ur}}/K, \mathbb{Z}) \arrow[r, dashed] \arrow[d] & H^2(L^{\mathrm{ur}}/L, \mathbb{Z}) \arrow[d] \\
H^1(K^{\mathrm{ur}}/K, \mathbb{Q}/\mathbb{Z}) \arrow[r, dashed] \arrow[d] & H^1(L^{\mathrm{ur}}/L, \mathbb{Q}/\mathbb{Z}) \arrow[d] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, dashed] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

The valuation maps give isomorphisms because the units have trivial cohomology. Let $e = e(L/K)$ be the ramification index, $f = f(L/K)$ the residue degree and chose $\varpi_K = \varpi_L^e$. We have diagrams,
$$\begin{tikzcd}
(K^{\mathrm{ur}})^\times \arrow[r, "\mathrm{val}_K"] \arrow[d] & \mathbb{Z} \arrow[d, "\times e"] \\
(L^{\mathrm{ur}})^\times \arrow[r, "\mathrm{val}_L"] & \mathbb{Z}
\end{tikzcd}$$

Since $\mathrm{Frob}_L = \mathrm{Frob}_K^f$ then $\mathrm{Res}(\varphi)(\mathrm{Frob}_L) = f\varphi(\mathrm{Frob}_K)$. Therefore, the final map fives multiplication by $ef = n$. $\square$

Corollary 7.4. Let L/K be a finite Galois extension of degree $n = [L : K]$. Then, $H^2(L/K)$ contains a cyclic subgroup of order n.

Proof. By Hilbert 90, we can apply the inflation-restriction sequence to get,

$$\begin{tikzcd} 0 \arrow[r] & H^2(L/K) \arrow[r, "\text{inf}"] & H^2(K^{\text{sep}}/K) \arrow[r, "\text{Res}"] & H^2(L^{\text{sep}}/L) \\ 0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] \arrow[u, hook, dashed] & H^2(K^{\text{ur}}/K) \arrow[r, "\text{Res}"] \arrow[u, hook, "\text{Inf}"] & H^2(L^{\text{ur}}/L) \arrow[u, hook, "\text{Inf}"] \\ & & 0 \arrow[u] & 0 \arrow[u] \end{tikzcd}$$

Because the inflation map is injective then the induced map $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \to H^2(L/K)$ is also injetive. □

Proposition 7.5. $|H^2(L/K)| \le [L : K]$.

Proof. If L/K is cyclic, then the Herbrand quotient,

$$h(L^\times) = [L : K]$$

However, by Hilbert 90, $H^1(L/K) = 0$ and thus $|H^2(L/K)| = [L : K]$. Otherwise, if L/K is not cyclic, we use, the fact that $\text{Gal}(L/K)$ for local fields is always solvable. Therefore, we may induct on the degree of the extension. Choose a nontrivial tower, $K \subset K' \subset L$ with K'/K cyclic. Then by inflation-restriction,

$$0 \longrightarrow H^2(K'/K) \xrightarrow{\text{Inf}} H^2(L/K) \xrightarrow{\text{Res}} H^2(L/K')$$

However, K'/K is cyclic and thus $|H^2(K'/K)| = [K' : K]$. Furthermore, by the induction hypothesis, $|H^2(L/K')| \le [L; K']$. Thus,

$$|H^2(L/K)| \le [L : K'][K' : K] = [L : K]$$

□

Theorem 7.6. Let L/K be an extension of local fields. Then $H^2(L/K) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Furthermore, the following diagram commutes,

$$\begin{tikzcd} 0 \arrow[r] & H^2(L/K) \arrow[r, "\text{inf}"] & H^2(K^{\text{sep}}/K) \arrow[r, "\text{Res}"] & H^2(L^{\text{sep}}/L) \\ 0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] \arrow[u, "\sim"] & H^2(K^{\text{ur}}/K) \arrow[r, "\text{Res}"] \arrow[u, hook, "\text{Inf}"] & H^2(L^{\text{ur}}/L) \arrow[u, hook, "\text{Inf}"] \end{tikzcd}$$

Proof. This follows immediately from the previous two propositions. □

Remark 7.7. In particular, we may view $H^2(L/K) \subset H^2(K^{\text{ur}}/K)$ since is is isomorphic to a subgroup of $H^2(K^{\text{ur}}/K)$ which inflates to $H^2(L/K)$.

Theorem 7.8. There exists an isomorphism,

$$H^2(K^{\text{sep}}/K) \xrightarrow{\sim} H^2(K^{\text{ur}}/K)$$

Proof. Notice $H^2(L/K) \subset H^2(K^{\text{ur}}/K) \subset H^2(K^{\text{sep}}/K)$. Taking the direct limit over finite L/K we find that,

$$H^2(K^{\text{sep}}/K) \hookrightarrow H^2(K^{\text{ur}}/K) \hookrightarrow H^2(K^{\text{sep}}/K)$$

since the composition of these surjections is the identity, each must be surjective and thus an isomorphism. □

Definition: Composing with $\text{inv}_K : H^2(K^{\text{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ we obtain an *invariant map*:

$$\text{inv}_K : H^2(K^{\text{sep}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

defined on all seperable extensions.

Definition: We call the element $u_{L/K} \in H^2(L/K)$ with

$$\text{inv}_K(u_{L/K}) = \frac{1}{[L:K]} \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$$

the *fundamental class.*

Remark 7.9. For any field K, the group

$$\text{Br}(K) = H^2(K^{\text{sep}}/K, (K^{\text{sep}})^\times)$$

is known as the *Brouer Group* of K. It is the group of central simple algebras under Brouer equivalence. We have shown,

$$\text{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$$

for any local field. For example, on the quaternion algebra, this map acts as, $\mathbb{H}_K \mapsto \frac{1}{2}$.

Remark 7.10. The notion of a Brouer group generalizes to any scheme X:

$$\text{Br}(X) := H^2_{\text{ét}}(X, \mathbb{G}_m)$$

Remark 7.11. The local Artin reciprocity map, is defined to be the inverse of,

$$\begin{array}{ccc} \hat{H}^{-2}(G,\mathbb{Z}) & \xrightarrow{\sim} & \hat{H}^0(G,L^\times) \\ \downarrow\wr & & \downarrow\wr \\ G^{\text{ab}} & \xrightarrow{\sim} & K^\times/\text{Nm}(L^\times) \end{array}$$

This can be described explicitly in terms of $u_{L/K}$. Thre is a cup product pairing:

$$\hat{H}^{-2}(G,\mathbb{Z}) \times H^2(G,L) \xrightarrow{\smile} \hat{H}^0(G,L^\times)$$

However, $H^2(G,L^\times) = H^2(L/K) = \langle u_{L/K} \rangle$ so the fundamental class induces the map: $\hat{H}^{-2}(G,\mathbb{Z}) \to \hat{H}^0(G,L^\times)$

8 March 27

Remark 8.1. Our goal is to construct the global Artin map,

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

Definition: Let L/K be a finite Galois extension and v be a place of K and $w \mid v$ a place of L. The decomposition group,

$$D(w) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(w) = w\} \cong \mathrm{Gal}(L_w/K_v)$$

Remark 8.2. For a different $w' \mid v$ with $w' = \tau(w)$ we have $D(w') = \tau D(w) \tau^{-1}$. In particular, if L/K is abelian then $D(w) = D(w')$ so the decomposition group of a place v is well-defined.

Remark 8.3. Therefore, for abelian L/K at each place v of K the local Artin map gives a canonical map,

$$\phi_v : K_v^\times \to \mathrm{Gal}(L_w/K_v) = D(v) \subset \mathrm{Gal}(L/K)$$

which is independent of the choice of $w \mid v$.

Proposition 8.4. There exists a continuous homomorphism,

$$\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that for any finite abelian extension L/K and any place v of K the following diagram commutes,

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \big\downarrow & & \big\downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Proof. Let $a = (a_v)_v \in \mathbb{I}_K$ if $a_v \in \mathcal{O}_v^\times$ and L_w/K_v is unramified then $\phi_v(a_v) = 1$. Therfore, $\phi_{L/K}(a)$ is uniquely determined locally by,

$$\phi_{L/K}(a) = \prod_v \phi_v(a_v)$$

since the product is finite and thus well-defined since all but finitely many places are unramifield. Furthermore, varying L we recover the map $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. It remains to show that ϕ_K is continuous i.e. that $\ker \phi_{L/K}$ is an open subgroup of $\mathbb{I}_K$. Take S to be the ramified places of L/K. By the compatibility of local Artin maps,

$$\begin{array}{ccc} \mathbb{I}_{L,S} & \xrightarrow{\phi_{L/L}} & \mathrm{Gal}(L/L) \\ \big\downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \big\downarrow \\ \mathbb{I}_{K,S} & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Therfore, $\ker \phi_{L/K} \supset \mathrm{Nm}_{L/K}\mathbb{I}_{L,S}$ which contains an open subgroup of $\mathbb{I}_{K,S}$ and thus $\ker \phi_{L/K}$ is an open subgroup. $\square$

Theorem 8.5 (Global CFT)**.** Let K be a number field. Then,

1. The homomorphism $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfies,
   (a) $\phi_K(K^\times) = 1$ thus it descends to $\phi_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$
   (b) for any finite abelian L/K the Artin map induces an isomorphism,
$$\phi_{L/K} : C_K/\mathrm{Nm}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$
2. For any finite index open subgroup $N \subset C_K$ there exists a finite abelian extension L/K such that $\mathrm{Nm}(C_L) = N$.

Corollary 8.6. The map $L \mapsto \mathrm{Nm}_{L/K}(C_L)$ gives a bijection between finite abelian extensions of K and finite index open subgroups of C_K. Furthermore,

1. $L_1 \subset L_2 \iff \mathrm{Nm}(C_{L_1}) \supset \mathrm{Nm}(C_{L_2})$
2. $\mathrm{Nm}(C_{L_1 \cdot L_2}) = \mathrm{Nm}C_{L_1)} \cap \mathrm{Nm}C_{L_2}$
3. $\mathrm{Nm}(C_{L_1 \cap L_2}) = \mathrm{Nm}(C_{L_1}) \cdot \mathrm{Nm}(C_{L_2})$

8.1 Ray Class Fields

Definition: A *modulus* of K is a function $m : \{\text{places of } K\} \to \mathbb{Z}_{\geq 0}$ such that,

1. $m(v) = 0$ for all but finitely many v
2. $m(v) \in \{0, 1\}$ if v is a real place
3. $m(v) = 0$ if v is a complex place

Definition: Associated to a modulus m we have the *principal congruence subgroup*,

$$\mathbb{I}_K^m = \prod_{v \nmid \infty} U_{v,m(v)} \times \prod_{v \mid \infty} K_{v,m(v)}^\times$$

where, $U_{v,0} = \mathcal{O}_v^\times$ and $U_{v,i} = 1 + \mathrm{p}_v^i$ and $K_{v,0}^\times = K_v^\times$ and $K_{v,1}^\times = \mathbb{R}_{\geq 0}$.

Definition: Define $C_K^m = (\mathbb{I}_K^m \cdot K^\times)/K^\times \subset C_K$ which is an open subgroup of C_K of finite index. And define the *ray class group*,

$$C\ell_m = C_K/C_K^m$$

which is a finite abelian group.

Remark 8.7. Write formally,

$$\mathfrak{m} = \prod_v \mathrm{p}_v^{m(v)} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$$

where $m_0 \subset \mathcal{O}_K$ can be viewed as an ideal. Then,

$$C\ell_m \cong \frac{\{\text{fractional ideals coprime to } m_0\}}{\{x \in K^\times \mid \forall v \mid \mathfrak{m}_0 : x \in U_{v,m(v)} \text{ and } \forall v \mid \mathfrak{m}_\infty : x \in \mathbb{R}_{v,>0}\}}$$

Example 8.8. Let $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$ for $m \in \mathbb{Z}$. Then,

$$C\ell_\mathfrak{m} = \frac{\{\left(\frac{r}{s}\right) \mid (r,m) = (s,m) = 1\}}{\{\frac{r}{s} \in \mathbb{Q}^\times \mid r \equiv_m s\}} \cong (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$$

Furthermore, for $\mathfrak{m} = (m) \cdot \infty$ we find,

$$C\ell_\mathfrak{m} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

Definition: The abelian extension L_m/K corresponding to $C\ell_m$ via global class field theory with $\mathrm{Nm}(L_\mathfrak{m}) = C_K^m$ and thus $\mathrm{Gal}(L_m/K) \cong C\ell_m$ is called the *ray class field* for m. When $m = 1$ is trivial then $C\ell_m = C\ell_K$ and the corresponding ray class field is called the Hilbert class field H.

Remark 8.9. By local CFT, the ramified places of the ray class field are contained in m. Therefore, H is the maximal unramified abelian extension. An infinite place $v \mid \infty$ is unramified if $L_w/K_v = \mathbb{R}/\mathbb{R}$ or $\mathbb{C}/\mathbb{C}$.

Definition: When the modulus,

$$\mathfrak{m} = \prod_{v \mid \infty} \mathrm{p}_v$$

over only real places the corresponding ray class field is the *narrow* Hilbert class field H^+ which is the maximal abelian extension of K unramified at finite places.

Example 8.10. For $K = \mathbb{Q}$ we have $H = H^+ = \mathbb{Q}$. However, for $K = \mathbb{Q}(\sqrt{3})$ then $H = K$ since $C\ell_K = 1$ but $H^+ = K(i)$ since $(C\ell_K^+ = Z/2\mathbb{Z})$ as $2 + \sqrt{3} > 0$ and $2 - \sqrt{3} > 0$.

Example 8.11. For $K = \mathbb{Q}$ and $\mathfrak{m} = (m) \cdot \infty$ then $C\ell_\mathfrak{m} = (\mathbb{Z}/m\mathbb{Z})^\times$ and thus $L_\mathfrak{m} = \mathbb{Q}(\zeta_m)$. For $\mathfrak{m} = (m)$ then $C\ell_m = (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$ and thus $L_\mathfrak{m} = \mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \overline{\zeta_m})$.

Corollary 8.12 (Kronecker-Weber)**.**

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{m \geq 1} \mathbb{Q}(\zeta_m)$$

Proof. For $K = \mathbb{Q}$ every modulus takes the form,

$$\mathfrak{m} = \prod_{p \in \mathbb{Q}} (p)^{m(p)} \cdot \infty \text{ or } \mathfrak{m} = \prod_{p \in \mathbb{Q}} (p)^{m(p)}$$

However this is simply $\mathfrak{m} = (m) \cdot \infty$ or $\mathfrak{m} = (m)$ where, $m \in \mathbb{Z}$ is,

$$m = \prod_{p \in \mathbb{Q}} p^{m(p)}$$

We have seen that both possible moduli give abelian extensions contained in some cyclotomic field.

□

9 April 3

9.1 Cohomology of Units

Let L/K be a Galois extension of number fields and $S \supset S_\infty$ a finite set containing all infinite places of K and $T = \{w : w \mid v : v \in S\}$ a finite set of places of L.

Definition: The group of T-units of L is defined to be,

$$U(T) = \{\alpha \in L^\times \mid \forall \omega \notin T : \alpha \in U_\omega\} = L^\times \cap \mathbb{I}_{L,T}$$

Proposition 9.1. Assume L/K is cyclic then the Herbrand quotient is given by,

$$h(U(T)) = \frac{\prod_{v \in S} [L_v : K_v]}{[L : K]}$$

Proof. Consider $V = \mathbb{R}^T = \operatorname{Hom}(T, \mathbb{R})$ and $N = \operatorname{Hom}(T, \mathbb{Z}) \subset V$ a G-stable lattice. Then,

$$N \cong \bigoplus_{v \in S} \operatorname{Hom}(G/D(v), \mathbb{Z}) \cong \bigoplus_{v \in S} \operatorname{Ind}_{D(v)}^{G} \mathbb{Z}$$

Therefore, by Shapiro,

$$h(N) = \prod_{v \in S} h(\operatorname{Ind}_{D(v)}^{G} \mathbb{Z}) = \prod_{v \in S} h_{D(v)}(\mathbb{Z}) = \prod_{v \in S} = \prod_{v \in S} |D(v)| = \prod_{v \in S} [L_v : K_v]$$

Consider $\lambda : U(T) \to V$ given by, $\alpha \mapsto (\log |\alpha|_w)_{\omega \in T}$. Let $M^0 = \operatorname{Im}(\lambda) \subset V$. Dirichlet's unit theorem for T-units gives M^0 a lattice in the hyperplane,

$$\{\sum_{\omega \in T} X_\omega = 0\} \subset V$$

Consider $M = M^0 \oplus \mathbb{Z}(1, \cdots, 1) \subset V$ a G-stable lattice in V. Therefore, because $\ker \lambda$ is finite its Herbrand quotient vanishes and thus $h(U(T)) = h(M^0)$ because there is an exact sequence,

$$0 \longrightarrow \ker\lambda \longrightarrow U(T) \longrightarrow M^0 \longrightarrow 0$$

Furthermore,

$$h(M) = h(\mathbb{Z})h(M^0) = |G|h(U(T)$$

Therefore, the following lemma gives the desired conclusion,

$$h(U(T)) = \frac{h(M^0)}{[L:K]} = \frac{h(N)}{[L:K]} = \frac{\prod_{v\in S}[L_v : K_v]}{[L:K]}$$

□

Lemma 9.2. Let G be a finite cyclic group and V a $\mathbb{R}[G]$-module i.e. a G-module and $\mathbb{R}$-vectorspace. Let M and N be two G-stable lattices in V then $h(M) = h(N)$.

9.2 Cohomology of Idele Class Group

Lemma 9.3. $H^0(G, C_L) = C_K$

Proof. Consider the short exact sequence,

$$1 \longrightarrow L^\times \longrightarrow \mathbb{I}_L \longrightarrow C_L \longrightarrow 1$$

Then the long exact sequence of cohomology gives,

$$1 \longrightarrow H^0(G, L^\times) \longrightarrow H^0(G, \mathbb{I}_L) \longrightarrow H^0(G, C_L) \longrightarrow H^1(G, L^\times)$$

However $H^1(G, L^\times) = 0$ and $H^0(G, L^\times) = 0$ and $H^0(G, \mathbb{I}_L) = \mathbb{I}_K$. Therefore we have a short exact sequence,

$$1 \longrightarrow K^\times \longrightarrow \mathbb{I}_K \longrightarrow H^0(G, C_L) \longrightarrow 0$$

showing that,

$$H^0(G, C_L) = \mathbb{I}_K / K^\times = C_K$$

□

Lemma 9.4. Let $S \supset S_\infty$ contain a generating set of primes for $C\ell_K$ then,

$$\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$$

Proof. There is a surjection $\mathbb{I}_K \to I_K$ given by sending,

$$(a_v)_v \mapsto \prod_v \mathrm{p}_v^{v_v(a_v)}$$

which has kernel $\mathbb{I}_{K,S_\infty}$. Therefore,

$$C\ell_K = \frac{I_K}{K^\times} = \frac{\mathbb{I}_K}{K^\times \cdot \mathbb{I}_{K,S_\infty}}$$

Since $C\ell_K$ is finite, by a choice of S I can set,

$$\frac{\mathbb{I}_K}{K^\times \cdot \mathbb{I}_{K,S}} = 0$$

by quotienting $\{\mathrm{p}_v\}_{v\in S}$. □

Theorem 9.5. Let L/K be a finite cyclic extension then $h(C_L) = [L : K]$.

Proof. Let $S \supset S_\infty$ be a finite set of places of K such that T contains a generating set of primes of $C\ell_L$ and all ramified places. Then,

$$C_L = \frac{\mathbb{I}_L}{L^\times} = \frac{L^\times \mathbb{I}_{L,T}}{L^\times} = \frac{\mathbb{I}_{L,T}}{L^\times \cap \mathbb{I}_L T} = \frac{\mathbb{I}_{L,T}}{U(T)}$$

Therefore,

$$h(C_L) = \frac{h(\mathbb{I}_{L,T})}{h(U(T))} = \frac{\prod\limits_{v \in S} n_v}{\left(\frac{\prod_{v \in S} [L_v : K_v]}{[L:K]} \right)} = [L : K]$$

$\square$

Corollary 9.6. $[C_K : \mathrm{Nm}(C_L)] \geq [L : K]$.

Lemma 9.7. Assume L/K is solvable. If $\exists D \supset \mathbb{I}_K$ subgroup such that $D \subset \mathrm{Nm}(I_L)$ and $K^\times D$ is dense in $\mathbb{I}_K$ then $L = K$.

Proof. If not then since L/K is solvable there exists a nontrivial cyclic subextension K'/K. Then $D \subset \mathrm{Nm}(\mathbb{I}_L) \subset \mathrm{Nm}(\mathbb{I}_{K'})$. By local class field theory, $\mathrm{Nm}(\mathbb{I}_{K'})$ is an open subgroup of $\mathbb{I}_K$ which implies that $K^\times \cdot \mathrm{Nm}(\mathbb{I}_{K'})$ is an open subgroup and hence closed. However, $K^\times D$ is dense if $\mathbb{I}_K$ and thus $K^\times \mathrm{Nm}(\mathbb{I}_{K'}) = \mathbb{I}_K$. Therefore, $[C_K : \mathrm{Nm}(C_{K'})] = 1$ and thus by the first innequality $[K' : K] = 1$ contradicting the fact that K'/K is nontrivial. $\square$

Proposition 9.8. Let L/K be a nontrivial solvable extension. Then there exist infinitely many places v of K such that v does not split completely in L.

Proof. If not, let $S \supset S_\infty$ contain all such v which would then be finite. Consider the subgroup $D = \{(a_v) \in \mathbb{I}_K \mid \forall v \in S : a_v = 1\}$. Then $D \subset \mathrm{Nm}(\mathbb{I}_L)$ since if $v \notin S$ then $L_v = K_v$ because v splits completely. However, any $(a_v)_{v \in S}$con be approximated by a global element $a \in K^\times$ (as S is finite). Therefore $K^\times \cdot D$ is dense in $\mathbb{I}_K$. By the previous lemma then extension L/K must be trivial. $\square$

Proposition 9.9. Assume L/K is solvable then $\{\mathrm{Frob}_{w/v} \mid w/v \text{ is unramified}\}$ generate $\mathrm{Gal}(L/K)$.

Proof. Let H be the group generated by the Frobenius elements and $E = L^H$. Then if v is unramified so v splits completely in E/K because the Frobenius acts trivially. Thus $E = K$ by the lemma so $H = G$. $\square$

Corollary 9.10. Let L/K be an abelian extension. Then the Artin map,

$$\phi_K : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

is surjective.

Proof. Since $\phi_K(\varpi_v) = \mathrm{Frob}_{w/v}$ the image of ϕ_K contains all Frobenius elements and thus generates $\mathrm{Gal}(L/K)$. $\square$

10 Second Innequality

Theorem 10.1. Let L/K be a finite abelian extension of number fields then,

$$[C_K : \mathrm{Nm}(C_L)] \leq [L : K]$$

Proof. Equivalently, we need to show that,

$$\frac{1}{[L : K]} \leq \frac{1}{[C_K : \mathrm{Nm}(C_L)]}$$

which we may interprete as relating the density of a set of primes of K. since $1/[L : K]$ is the density of completely split primes of L/K. Let $\mathfrak{m}$ be a modulus of K and let $I_K^{\mathfrak{m}}$ be the group of fractional ideals of K coprime to $\mathfrak{m}$. Let

$$K^{\mathfrak{m}} = \{a \in K^\times \mid \forall v \mid m_0 a \in U_{v,m(v)} \text{ and } \forall v \mid \mathfrak{m}_\infty : a \in K_{v,m(v)}^\times = \mathbb{R}_{>0}\}$$

Then,

$$C\ell_{\mathfrak{m}} \cong \frac{I_K^{\mathfrak{m}}}{K^{\mathfrak{m}}}$$

□

Theorem 10.2. Let $K^{\mathfrak{m}} \subset H \subset I_K^{\mathfrak{m}}$ let $A \in I_K^{\mathfrak{m}}/H$ which is a quotient of $C\ell_{\mathfrak{m}}$. Then,

$$\delta(\mathrm{p} \in A) = \frac{1}{[I_K^{\mathfrak{m}} : K]}$$

Proof. Let χ be any character of $I^{\mathfrak{m}}/H$ then construct the Weber L-function $L(s, \chi)$. Consider,

$$\log L(s, \chi) \sim \sum_{\mathrm{p} \nmid \mathfrak{m}} \frac{\chi(\mathrm{p})}{N(\mathrm{p}^s)} = \sum_{B \in I^{\mathfrak{m}}/H} \chi(B) \sum_{\mathrm{p} \in B} \frac{1}{N\mathrm{p}^s}$$

Recall that if G is a finite abelian group $g \in G$ then,

$$\sum_{\chi \in \mathrm{Hom}(G, \mathbb{C}^\times)} \chi(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

Therefore, consider,

$$\sum_{\chi} \chi(A^{-1}) \log L(s, \chi) \sim \sum_{\chi} \sum_{B \in I_K^{\mathfrak{m}}/H} \chi(A^{-1}B) \sum_{\mathrm{p} \in B} \frac{1}{N\mathrm{p}^s} = [I_K^{\mathfrak{m}} : H] \sum_{\mathrm{p} \in A} \frac{1}{N\mathrm{p}^s}$$

□

Since the sum over all characters picks out the element $A^{-1}B = 1$. Furthermore, for $\chi \neq \chi_0$ we know that $L(s, \chi)$ is finite for $s \to 1$ but,

$$\log L(s, \chi_0) \sim \log \zeta_K(s) \sim \log \frac{1}{s - 1}$$

which implies that,

$$\log \frac{1}{s-1} \sim [I_K^{\mathfrak{m}} : H] \sum_{\mathfrak{p} \in A} \frac{1}{N\mathfrak{p}^s}$$

Therefore,

$$\delta(\mathfrak{p} \in A) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in A} \frac{1}{N\mathfrak{p}^s}}{\log \frac{1}{s-1}} = \frac{1}{[I_K^{\mathfrak{m}} : H]}$$

Theorem 10.3. Let L/K be a finite abelian extension of number fields then,

$$[C_K : \mathrm{Nm}(C_L)] \leq [L : K]$$

Proof. Apply the previous theorem to $H = K^{\mathfrak{m}} \cdot \mathrm{Nm}(I_L^{\mathfrak{m}})$ and $A = 0 \in I_K^{\mathfrak{m}}/K)$. Then,

$$\delta(\mathfrak{p} \in A) = \frac{1}{[I_K^{\mathfrak{m}} : H]}$$

However, if $\mathfrak{p}$ is a prime of K that splits completely in L then $\mathfrak{p} \in \mathrm{Nm}(I_L^{\mathfrak{m}})$ since the Galois group permutes the factors of $\mathfrak{p}$ exactly once. This holds if $\mathfrak{p}$ is coprime to $\mathfrak{m}$ which only removes a finite number of primes from the set of all completely split primes. Therefore, the density of completely split primes is less than the density of primes $\mathfrak{p} \in \mathrm{Nm}(I_L^{\mathfrak{m}})$ i.e. $\mathfrak{p} \in A$. Therfore,

$$\frac{1}{[L : K]} \leq \frac{1}{[I_K^{\mathfrak{m}} : H]}$$

□

Corollary 10.4. If L/K is finite Galois then,

$$H^1(\mathrm{Gal}(L/K), C_L) = 0$$

Proof. When $G = \mathrm{Gal}(L/K)$ is cyclic then the first innequality gives,

$$h(C_L) = \frac{[C_K : \mathrm{Nm}(C_L)]}{|H^1(G, C_L)} = [L : K]$$

However,

$$[C_K : \mathrm{Nm}(C_L)] \leq [L : K]$$

and thus $[C_K : \mathrm{Nm}(C_L)] = [L : K]$ and therefore $H^1(G, C_L) = 0$. If G is not cyclic, then consider G solvable. Take normal $H \triangleleft G$ such that G/H is cyclic. By inflation-restriction, there is an exact sequence,

$$0 \longrightarrow H^1(G/H, C_L^H) \longrightarrow H^1(G, C_L) \longrightarrow H^1(H, C_L)$$

By induction we have $H^1(H, C_L) = 0$ and $H^1(G/H, C_L^H) = 0$ since G/H is cyclic. Therefore, $H^1(G, C_L) = 0$. Finally, for a generaly group G, use the embedding,

$$H^1(G, C_L) \hookrightarrow \prod_{p||G|} H^1(G_p, C_L)$$

where G_p is a p-Sylow subgroup of G which is solvable so $H^1(G_p, C_L) = 0$. Therefore, $H^1(G, C_L) = 0$. $\square$

Theorem 10.5 (Chebotarev Density)**.** Let L/K be a finite Galois extension of number fields. Let $\sigma \in G = \mathrm{Gal}(L/K)$ and $C_\sigma \subset G$ its conjugacy class. Then,

$$\delta(\{\mathrm{p} \subset \mathcal{O}_K \mid \mathrm{Frob}_\mathrm{p} \in C_\sigma\}) = \frac{|C_\sigma|}{|G|}$$

Example 10.6. For $\sigma = 1$ then $C_\sigma = \{1\}$. Furthermore, $\mathrm{Frob}_\mathrm{p} = 1$ exactly when p splits completely. Then the Chebotarev Density theorem gives,

$$\delta(\{\mathrm{p} \subset \mathcal{O}_K \mid \mathrm{Frob}_\mathrm{p} = 1\}) = \frac{1}{|G|}$$

which implies that,

$$\delta(\{\mathrm{p \text{ splits completely}}\}) = \frac{1}{[L:K]}$$

Example 10.7. Take $K = \mathbb{Q}$ and L/K abelian. In particular, take $L = \mathbb{Q}(\zeta_N)$ then $\mathrm{Gal}(L/K) = (\mathbb{Z}/N\mathbb{Z})^\times$ and consider $\sigma = a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then the Chebotarev Density theorem states that,

$$\delta(\{p \mid \mathrm{Frob}_p = a\}) = \frac{1}{|G|}$$

However, if $\mathrm{Frob}_p = a$ then the actions on ζ_N are equal meaning that $\zeta_N^p = \zeta_N^a$ and thus $p \equiv_N a$. Therefore,

$$\delta(\{p \equiv_N a\}) = \frac{1}{\phi(N)}$$

Example 10.8. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ a nonabelian Galois number field which is the splitting field of $x^3 - 2$. Then $G = S_3$. There are three conjugacy classes, $C_1 = \{1\}$, $C_2 = \{(1\,2), (2\,3), (3\,4)\}$, and $C_3 = \{(1\,2\,3), (1\,3\,2)\}$. $\mathrm{Frob}_p \in C_1$ iff p splits completely iff $x^3 - 2$ splits completely in $\mathbb{F}_p$. $\mathrm{Frob}_p \in C_2$ iff $x^3 - 2$ has one linear factor in $\mathbb{F}_p$. Finally, $\mathrm{Frob}_p \in C_3$ iff $x^3 - 2$ is irreducible in $\mathbb{F}_p$. Then the Chebotarev Density theorem tells us that these three conditions occur with frequency $\frac{1}{6}, \frac{1}{2}, \frac{1}{3}$ respectivly.

Remark 10.9. There is <u>no</u> simple congruence condition on p to determine what conjugacy class p lies in.