Mathematics GR6657 Algebraic Number Theory
Assignment # 6

Benjamin Church

October 25, 2018

1

Theorem 1.1. *Let L/K be galois with group $G = Gal(L/K)$. Given $\alpha \in K^\times$ write the Frobenius $s_\alpha = (\alpha, L/K) \in G^{ab}$. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^2(G, \mathbb{Z})$ be a continuous character of degree 1 and let $\delta_\chi \in H^2(G, \mathbb{Z})$ be the image of χ by the coboundary map $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$. Let $\bar{\alpha} \in K^\times / N_{L/K}(L^\times) = \hat{H}^0(G, L^\times)$ be the image of α. Then,*

$$inv_K(\bar{\alpha} \smile \delta\chi) = \chi(s_\alpha)$$

The proof of this theorem and some associated lemmata will require the following properties of the cup product:

1. Associativity: $x \smile (y \smile z) = (x \smile y) \smile z$.
2. For $x \in H^r(G, M)$ and $y \in H^s(G, N)$ we have $x \smile y = (-1)^{rs}(y \smile x)$.
3. Given a short exact sequence of G-modules, $1 \to A \to B \to C \to 1$ and N a flat module consider the short exact sequence,

   $$1 \longrightarrow A \otimes N \longrightarrow B \otimes N \longrightarrow C \otimes N \longrightarrow 1$$

   Each short exact sequence gives rise to a very long exact sequence of Tate cohomology. Let $\delta : \hat{H}^r(G, C) \to \hat{H}^{r+1}(G, A)$ and $\delta' : \hat{H}^r(G, C \otimes N) \to \hat{H}^{r+1}(G, A \otimes N)$ be the boundary maps for these two very long exact seqences. Then, for $x \in \hat{H}^r(G, C)$ and $y \in \hat{H}^s(G, N)$, the cup product satisfies,

   $$\delta(x) \smile y = \delta'(x \smile y)$$

4. The inflation map commutes with cup products,

   $$\inf(x \smile y) = \inf(x) \smile \inf(y)$$

Now we need to prove three lemmata from the appendix to Serre's book. I will state the first two and prove lemma 3.

Remark 1.2. *Given $a \in A^G$ I will use the notation $a^0 \in \hat{H}^0(G, A) = A^G / Nm_G(A)$ for its image. Furthermore, for aA if $Nm_G(a) = 0$ then write $a_0 \in \hat{H}^{-1}(G, A)$ for its image.*

Lemma 1.3. *Given $a \in A^G$ let $f_a : \mathbb{Z} \to A$ be the unique G-morphis such that $f_a(1) = a$. If $x \in \hat{H}^n(G, B)$ then,*

$$a^0 \smile x \in \hat{H}^n(G, A \otimes B)$$

is the image of x under the map $f_a \otimes I : \mathbb{Z} \otimes B \to A \otimes B$.

Lemma 1.4. *Given $a \in A$ such that $Nm_G(a) = 0$ and f a 1-cocycle of G to B, take $\bar{f} \in H^1(G, B)$. Then in $\hat{H}^1(G, A \otimes B)$ we have,*

$$a_0 \smile \bar{f} = c^0$$

where,

$$c = -\sum_{t \in G} ta \otimes f(t)$$

Lemma 1.5. *Let B be a G-module and $f : G \to B^1$ a 1-cocycle with image $\bar{f} \in H^1(G, B)$. Then for each $s \in G$ we have $\bar{s} \smile \bar{f} = \overline{f(s)_0}$ in $\hat{H}^{-1}(G, B)$.*

Proof. First, some notation. Let I_G be the augmentation ideal and for any $s \in G$ let $i_s = s - 1 \in I_G$. Note that f is a 1-cocycle and therefore a crossed homomorphism $f(\sigma\tau) = f(\sigma) + \sigma \cdot f(\tau)$. Thus, consider,

$$\sum_{\sigma \in G} \sigma \cdot f(\tau) = \sum_{\sigma \in G} (f(\sigma\tau) - f(\sigma)) = \sum_{\sigma' \in G} f(\sigma') - \sum_{\sigma \in G} f(\sigma) = 0$$

Thus, $Nm_G f(\tau) = 0$ for any τ so $f(\tau)_0 \in \hat{H}^{-1}(G, B)$ is well-defined. Furthermore, $Nm_G(i_s) = 0$ so $(i_s)_0 \in \hat{H}^{-1}(G, I_G)$ is also well defined. Let $\delta : \hat{H}^{-2}(G, \mathbb{Z}) \to \hat{H}^{-1}(G, I_G)$ be the boundary map induced by the exact sequence,

$$1 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

However,

$$\hat{H}^{-2}(G, \mathbb{Z}) \cong G^{ab} \cong I_G / I_G^2 \cong \ker(Nm_G) / I_G^2 \cong \hat{H}^{-1}(G, I_G)$$

so δ is an isomorphism and if s, s' lie in the same coset of G^{ab} then $(i_s)_0 = (i_{s'})_0$. Tensoring with B we get a map,

$$\delta' : \hat{H}^r(G, \mathbb{Z} \otimes B) \to \hat{H}^r(G, I_G \otimes B)$$

which is also an isomorphism because δ is. First, consider,

$$d'(\bar{s} \smile \bar{f}) = i_s \smile f = (i_s)_0 \smile f$$

By lemma 1.4,

$$(i_s)_0 \smile f = \left[-\sum_{t \in G} (t i_s) \otimes f(t) \right]^0$$

However, using the fact that $f(ts) = f(t) + t \cdot f(s)$ because f is a crossed homomorphism, we can rewrite

$$\begin{aligned}
\sum_{t\in G}(ti_s)\otimes f(t) &= \sum_{t\in G}(t-ts)\otimes f(t) = \sum_{t\in G} t\otimes f(t) ts\otimes f(t) \\
&= \sum_{t\in G} t\otimes f(t) - ts\otimes (t(ts) - t\cdot f(s)) \\
&= \sum_{t\in G} t\otimes t(f0 - ts\otimes f(ts) + ts\otimes t\cdot f(s) \\
&= \sum_{t\in G} t\otimes f(t) - t\otimes f(t) + ts\otimes t\cdot f(s) \\
&= \sum_{t\in G} ts\otimes t\cdot f(s)
\end{aligned}$$

where I have reindexed the second sum. Thus,

$$\sum_{t\in G}(ti_s)\otimes f(t) = \sum_{t\in G} ts\otimes t\ cdot f(s)$$

Now we consider how d' acts,

$$d'(f(s)_0) = \left[\sum_{t\in G}(t\otimes t\cdot f(s))\right]^0$$

Comparing these results gives,

$$\begin{aligned}
d'(f(s)_0) - d'(\bar{s}\smile \bar{f}) &= \left[\sum_{t\in G}(t\otimes t\cdot f(s)) \sum_{t\in G} ts\otimes t\ cdot f(s)\right]^0 \\
&= \left[\sum_{t\in G} t(s-1)\otimes t\cdot f(s)\right]^0 \\
&= \left[\sum_{t\in G} t\cdot [(s-1)\otimes f(s)]\right]^0 \\
&= [Nm_G[(s-1)\otimes f(s)]]^0 = 0
\end{aligned}$$

The image of the norm map is zero in $\hat{H}^0(G, I\otimes B)$ because $\hat{H}^0(G, I\otimes B)$ is the cokernel of Nm_G be definition. Therefore, $d'(f(s)_0) = d'(\bar{s}\smile \bar{f})$ proving the claim. □

Now, we give the proof of the main theorem.

Proof. Let $u_{L/K}$ be a generator of the cyclic group $\hat{H}^2(G, L^\times)$. The map $x \mapsto x \smile u_{L/K}$ induces an isomorphism $\hat{H}^{-2}(G, \mathbb{Z}) \to \hat{H}^0(G, L^\times)$. However, we know that $\hat{H}^{-2}(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$ and $(L^\times)^G = K^\times$. Thus,

$$G^{\mathrm{ab}} \cong \hat{H}^{-2}(G, \mathbb{Z}) \cong \hat{H}^0(G, L^\times) \cong K^\times / Nm_G(L^\times)$$

I will denote the inverse of this isomorphism by,

$$\theta_{L/K} : K^\times / Nm_G(L^\times) \xrightarrow{\sim} \hat{H}^{-2}(G, \mathbb{Z})$$

There is an exact sequence of trivial G modules,

$$1 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 1$$

Taking the long exact chomology sequence gives an isomorphism $\delta : \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^2(G, \mathbb{Z})$ because $\hat{H}^1(G, \mathbb{Q}) = \hat{H}^2(G, \mathbb{Q}) = 0$. Because these are trivial G-modules, the first cohomolgy is identified with the set of homs. Thus, we have an isomorphism,

$$\delta : \mathrm{Hom}\,(G, \mathbb{Q}/\mathbb{Z}) \to \hat{H}^2(G, \mathbb{Z})$$

Take a character $\chi \in HomG\mathbb{Q}/\mathbb{Z}$ and define $s_\alpha = \theta_{L/K}(\alpha)$. Then,

$$\alpha \smile u_{L/K} = \alpha$$

where $\alpha \in K^\times / Nm_G(L^\times)$. Furthermore,

$$\alpha \smile \delta(\chi) = (s_\alpha \smile u_{L/K}) \smile \delta(\chi)$$

since the grading of these elements in the chomology ring is even, the cup product is commutative and (is always) associative. Thus,

$$\alpha \smile \delta(\chi) = u_{L/K} \smile (s_\alpha \smile \delta(\chi)) = u_{L/K} \smile \delta'(s_\alpha \smile \chi) = u_{L/K} \smile \delta'(\chi(s_\alpha))$$

by Lemma 1.5. If the degree of L/K is $[L : K] = n$ then $\chi(s_\alpha) = b/n$ for some $b \in \mathbb{Z}$ and $\delta'(b/n) = b$. thus, $\alpha \smile \delta(\chi) = u_{L/K} \smile b$. Applying the invariant map,

$$inv_{L/K}(\alpha \smile \delta(\chi)) = inv_{L/K}(u_{L/K} \smile b) = b/n = \chi(s_\alpha)$$

$\square$

2

Suppose that $K \subset K' \subset L$ is a sequence of p-adic fields with L/K abelian. Let,

$$r_{L/K} : K^\times \to Gal(L/K) \quad r_{K'/K} : K^\times \to Gal(K'/K)$$

be the reciprocity maps. Take any $a \in K^\times$. We need to show that $r_{L/K}(a)|_{K'} = r_{K'/K}(a)$.

I claim that the following diagram commutes,

$$\begin{tikzcd}
H^1(G_{K'/K}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\delta"] \arrow[d, "\inf"] & H^2(G_{K'/K}, \mathbb{Z}) \arrow[r, "\bar{\alpha}\smile"] \arrow[d, "\inf"] & H^2(G_{K'/K}, (K')^\times) \arrow[r, "inv_{K'/K}"] \arrow[d, "\inf"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\mathrm{id}"] \\
H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\delta"] & H^2(G_{L/K}, \mathbb{Z}) \arrow[r, "\inf\bar{\alpha}\smile"] & H^2(G_{L/K}, (K')^\times) \arrow[r, "inv_{L/K}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

To show this we use the definition of the invariant map and the fact that the inflation map commutes with cup products. Take any $\chi \in \mathrm{Hom}\left(G_{K'/K}, \mathbb{Q}/\mathbb{Z}\right)$ and its image $\chi' = \inf \chi$ under the inflation map. Using the theorem in problem 1, for any $\alpha \in K^\times$,

$$\chi(r_{K'/K}(\alpha)) = inv_{K'/K}(\bar{\alpha} \smile \delta\chi)$$

Using the fact that the above diagram commutes,

$$inv_{K'/K}(\bar{\alpha} \smile \delta\chi) = inv_{L/K}(\inf\bar{\alpha} \smile \delta \inf \chi) = inv_{L/K}(\inf\bar{\alpha} \smile \delta\chi') = \chi'(r_{L/K}(\alpha)) = \chi(r_{L/K}(\alpha)|_{K'})$$

Thus, it suffices to show that if all characters agree on g_1 and g_2 then $g_1 = g_2$. That is,

$$\left(\forall \chi \in \text{Hom}\left(G_{K'/K}, \mathbb{Q}/\mathbb{Z}\right) : \chi(g_1) = \chi(g_2)\right) \implies g_1 = g_2$$

Suppose that $\chi(g_1) = \chi(g_2)$ and thus $\chi(g_1 g_2^{-1}) = 1$ for each character χ. However, $G_{K'/K}$ is a locally compact hausdorff topological group and thus the canonical map $ev_G : G \to \hat{\hat{G}}$ is an isomorphism. However, $ev_G(g_1 g_2^{-1})(\chi) = \chi(g_1 g_2^{-1}) = 1$ and thus $g_1 g_2 - 1 = 1$ since ev_G is an injection. Since, all characters agree on $r_{K'/K}(\alpha)$ and $r_{L/K}(\alpha)|_{K'}$ we have the desired result that,

$$r_{L/K}(\alpha)|_{K'} = r_{K'/K}(\alpha)$$

3

There is a one-to-one correspondence between index two subgroups and surjective homomorphisms to $\{\pm 1\}$. To see this, suppose $\phi : G \to \{\pm 1\}$ is a surjective homomorphism then $G/\ker \phi \cong \{\pm 1\}$ so $\ker \phi$ has index 2. Conversely, suppose that $[G : H] = 2$ then H is normal so $G/H \cong \{\pm 1\}$ and thus $\pi : G \to G/H$ is a surjective homomorphism to $\{\pm 1\}$ with kernel H. We will use this fact to find all the index 2 open subgroups of $C_{\mathbb{Q}} = \mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times$.

We can write the idele class group as,

$$C_{\mathbb{Q}} = \frac{\mathbb{I}_{\mathbb{Q}}}{\mathbb{Q}^\times} = \mathbb{R}^\times_{>0} \times \prod_p \mathbb{Z}_p^\times$$

For each odd prime p we can take the reciprocity map,

$$f_p : C_{\mathbb{Q}} \to \mathbb{Z}_p^\times \xrightarrow{\pi} \mathbb{F}_p^\times \xrightarrow{\left(\frac{-}{p}\right)} \{\pm 1\}$$

Furthermore, for $p = 2$ we need to consider the elements modulo 8. Since $(\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^3$ we can take three different nontrivial homomorphisms. For odd δ,

$$f_{2,\delta}(x) = \begin{cases} 1 & x \equiv 1, \delta \pmod 8 \\ -1 & \text{else} \end{cases}$$

These are clearly homomorphisms $\mathbb{Z}_2^\times \to \{\pm 1\}$. For $p \neq 2$ any quadratic residue lifts to a square in $\mathbb{Z}_p^\times$ by Hensel's Lemma. Furthermore any two nonresidues always differ by a quadratic residue so any homomorphism $f : \mathbb{Z}_p^\times \to \{\pm 1\}$ must take all residues to 1 and must be constant on the set of nonresidues. However, this does not hold for $p = 2$ which is why we must consider the elements modulo 8 which determines the class of lifts in $\mathbb{Z}_2^\times$ since only elements 1 modulo 8 lift to squares in $\mathbb{Z}_2^\times$. Furthermore, if S is a finite set of primes then,

$$f_S = \prod_{p \in S} f_p : C_{\mathbb{Q}} \to \{\pm 1\}$$

Clearly these maps are surjective so their kernels are index 2 subgroups. The prime 2 needs special attention in S. Take a quadratic extension $K/\mathbb{Q}$ and consider the global Artin map which extends to each local Artin map via,

$$\begin{array}{ccc} \mathbb{Q}_v^\times & \xrightarrow{\phi_v} & Gal(K_v/\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ \mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times & \xrightarrow{\phi_K} & Gal(K/\mathbb{Q}) \end{array}$$

By properties of the local Artin map, if v is unramified then ϕ_v takes any unit $u_v \in \mathbb{Z}_v^\times$ to the identity. By the global existence theorem, any open index 2 subgroup of $C_{\mathbb{Q}}$ the image under the norm map of some quadratic field $K/\mathbb{Q}$. Thus, each f_S must have a norm subgroup as its kernel so it factors through the global Artin map for $K/\mathbb{Q}$. However, for any prime p we know that $\mathbb{Z}_p^\times$ is not contained in the kernel of f_S if and only if $p \in S$. Thus, S must be the set of ramified primes in $K/\mathbb{Q}$. However, we have classified all quadratic extensions of $\mathbb{Q}$ which are of the form $K = \mathbb{Q}(\sqrt{\pm p_1 \cdots p_r})$ for distinct primes $p_1, \dots, p_r$ which has discriminant,

$$\Delta_K = \begin{cases} \pm p_1 \cdots p_r & \pm p_1 \cdots p_r \equiv 1 \pmod 4 \\ \pm 4 p_1 \cdots p_r & \text{else} \end{cases}$$

Therefore, the set of ramified primes in $K/\mathbb{Q}$ is, $p_1, \dots, p_r$ if $\pm p_1 \cdots p_r \equiv 1 \pmod 4$ and otherwise, $2, p_1, \dots, p_r$ when all these primes are odd. For $K = \mathbb{Q}(\sqrt{d})$ let $\alpha \equiv d \pmod 8$ be the reduction modulo 8. Given a set of odd primes $p_1, \dots, p_r$, I claim that Artin reciprocity gives the following correspondence,

$$\begin{aligned} S = \{p_1, \dots, p_r\} &\iff K = \mathbb{Q}(\sqrt{\pm p_1 \dots p_r}) \quad \text{for} \quad \alpha = 1, 5 \\ S = \{(2,5), p_1, \dots, p_r\} &\iff K = \mathbb{Q}(\sqrt{\pm p_1 \dots p_r}) \quad \text{for} \quad \alpha = 3, 7 \\ S = \{(2, 1-\alpha), p_1, \dots, p_r\} &\iff K = \mathbb{Q}(\sqrt{\pm 2 p_1 \dots p_r}) \end{aligned}$$

We have already shown that S must contain exactly the ramified primes of K which are exactly the prime factors of Δ_K modulo annoyances at $p = 2$. In the first case, $d \equiv 1 \pmod 4$ so 2 is unramified and we have $S = \{p_1, \dots, p_r\}$ as required. To establish which residues we will need in $\mathbb{Z}_2^\times$ we need to check the norm map explicitly. Using just elements in $\mathbb{Z}_2^\times$, the image of the norm map for the field $K = \mathbb{Q}(\sqrt{d})$ will contain the residues,

$$x^2 - dy^2 \equiv x^2 - \alpha y^2 \pmod 8$$

In the second case, it is easy to see that 5 is in the image of $x^2 - \alpha y^2$ modulo 8. However, 2 is ramified so the kernel must be nontrivial and thus correspond to the map $f_{2,5}$. Finally, in the last case , α is even but not a multiple of 4 so for $(x, y) = (1, 1)$,

$$x^2 - \alpha y^2 \equiv 1 - \alpha \pmod 8$$

and $1 - \alpha$ is an odd residue not equal to one modulo 8 because $8 \not| \alpha$. Therefore, the norm map has elements with residue $1 - \alpha$ in its image and thus it corresponds to the kernel of $f_{2,1-\alpha}$.

Since we have classified all quadratic extensions $K/\mathbb{Q}$ by Artin reciprocity and the global existence theorem, we have also found all open subgroups of index 2 of $C_{\mathbb{Q}}$. In summary, the open index 2 subgroups of $C_{\mathbb{Q}}$ are exactly, $\ker f_S$ for any set of primes (remembering that 2 comes with three options) with the correspondence between the set S and the associated quadratic field whose norm image is $\ker f_S$.

4

First, let K be a number field such that $K/\mathbb{Q}$ is a finite Galois extension with Galois group $G = Gal(K/\mathbb{Q})$. We will restrict to the case in which K is a quadratic field. However, first we will consider some general background results.

Consider the exact sequence,

$$1 \longrightarrow \tfrac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times} \longrightarrow C_K \longrightarrow Cl(K) \longrightarrow 1$$

obtained by applying the third isomorphism theorem to lemma 5.1 where the subgroup,

$$\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times} \subset C_K = \frac{\mathbb{I}_K \cdot K^\times}{K^\times}$$

is the norm subgroup of the idele class group corresponding to the Hilbert class field of K under the Artin reciprocity map. Let $G = Gal(K/\mathbb{Q})$. This short exact sequence gives rise to a long exact sequence of cohomology,

$$1 \longrightarrow \left(\tfrac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G \longrightarrow C_K^G \longrightarrow Cl(K)^G \longrightarrow H^1(G, (\mathbb{I}_{K,S_\infty} \cdot K^\times)/K^\times) \longrightarrow 1$$

Where I have used the fact that $H^1(G, C_K) = 1$ by Lemma 5.2. Using Lemmata 5.3 and 5.7 this exact sequence becomes,

$$1 \longrightarrow C_\mathbb{Q} \longrightarrow\!\!\!\!\!\rightarrow C_\mathbb{Q} \longrightarrow Cl(K)^G \longrightarrow H^1(G, (\mathbb{I}_{K,S_\infty} \cdot K^\times)/K^\times) \longrightarrow 1$$

where the map $C_\mathbb{Q} \to C_\mathbb{Q}$ is surjective because it is simply the restriction of the inclusion map,

$$1 \longrightarrow \tfrac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times} \longrightarrow C_K$$

which clearly takes the subgroup $C_\mathbb{Q} \mapsto \mathbb{C}_\mathbb{Q}$. Therefore, the map $C_\mathbb{Q} \to Cl(K)^G$ in the previous exact sequence is the zero map since the map $C_\mathbb{Q} \to C_\mathbb{Q}$ has full image. Thus, we get an exact sequence,

$$1 \longrightarrow Cl(K)^G \longrightarrow H^1(G, (\mathbb{I}_{K,S_\infty} \cdot K^\times)/K^\times) \longrightarrow 1$$

which gives a canonical isomorphism $Cl(K)^G \cong H^1(G, (\mathbb{I}_{K,S_\infty} \cdot K^\times)/K^\times)$. However, by the second isomorphism theorem,

$$\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times} \cong \frac{\mathbb{I}_{K,S_\infty}}{\mathbb{I}_{K,S_\infty} \cap K^\times} = \frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}$$

where $\mathbb{I}_{K,S_\infty} \cap K^\times$ are the elements of $K^\times$ which are units in every local field and thus factor into no primes i.e. elements of $\mathcal{O}_K^\times$. Therefore,

$$Cl(K)^G \cong H^1\left(G, \frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right) \cong H^1\left(G, \frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}\right)$$

Now, consider the short exact sequence,

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow \mathbb{I}_{K,S_\infty} \longrightarrow \frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times} \longrightarrow 1$$

which gives rise to a long exact sequence of cohomology,

$$\begin{tikzcd}
1 \arrow[r] & (\mathcal{O}_K^\times)^G \arrow[r] & (\mathbb{I}_{K,S_\infty})^G \arrow[r, two heads] & \left(\frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}\right)^G \arrow[r] \arrow[dll, rounded corners] & 1 \\
1 \arrow[r] & H^1(G,\mathcal{O}_K^\times) \arrow[r] & H^1(G,\mathbb{I}_{K,S_\infty}) \arrow[r] & H^1(G,\mathbb{I}_{K,S_\infty}/\mathcal{O}_K^\times) \arrow[r] & H^2(G,\mathcal{O}_K^\times) \arrow[r] & H^2(G,\mathbb{I}_{K,S_\infty})
\end{tikzcd}$$

By Lemma 5.7, the top row becomes,

$$1 \longrightarrow \mathcal{O}_\mathbb{Q}^\times \longrightarrow \mathbb{I}_{\mathbb{Q},S_\infty} \longrightarrow\!\!\!\!\!\rightarrow \frac{\mathbb{I}_{\mathbb{Q},S_\infty}}{\mathcal{O}_\mathbb{Q}^\times} \longrightarrow 1$$

which can be extended to 1 because the map $\mathbb{I}_{\mathbb{Q},S_\infty} \to \frac{\mathbb{I}_{\mathbb{Q},S_\infty}}{\mathcal{O}_\mathbb{Q}^\times}$ is the restriction of the projection map to a subgroup and its corresponding sub-quotient which is still a surjective map.

Thus, if we can show that the map $H^2(G,\mathcal{O}_K^\times) \to H^2(G,\mathbb{I}_{K,S_\infty})$ is injective then we have a short exact sequence,

$$1 \longrightarrow H^1(G,\mathcal{O}_K^\times) \longrightarrow H^1(G,\mathbb{I}_{K,S_\infty}) \longrightarrow H^1(G,\mathbb{I}_{K,S_\infty}/\mathcal{O}_K^\times) \longrightarrow 1$$

which implies that,

$$Cl(K)^G \cong H^1\left(G,\mathbb{I}_{K,S_\infty}/\mathcal{O}_K^\times\right) \cong H^1(G,\mathbb{I}_{K,S_\infty})/H^1(G,\mathcal{O}_K^\times)$$

(a)

Now we restrict to the case of an imaginary quadratic extension $K/\mathbb{Q}$. Since $G = Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ is finite cyclic, there is a natural isomorphism $\hat{H}^0(G,M) \xrightarrow{\sim} \hat{H}^2(G,M) = H^2(G,M)$. In particular, consider the map,

$$\hat{H}^0(G,\mathcal{O}_K^\times) \to \hat{H}^0(G,\mathbb{I}_{K,S_\infty})$$

We will exclude the cases $K \neq \mathbb{Q}(i)$ and $K \neq \mathbb{Q}(\zeta_3)$ such that $\mathcal{O}_K^\times = \{\pm 1\}$[1]. Therefore, $\mathcal{O}_K^\times$ is a trivial G-module. In particular,

$$H^0(G,\mathcal{O}_K^\times) = (\mathcal{O}_K^\times)^G = \mathcal{O}_K^\times \text{ and } \hat{H}^0(G,\mathcal{O}_K^\times) = H^0(G,\mathcal{O}_K^\times)/\mathrm{Nm_G}(\mathcal{O}_K^\times) = \mathcal{O}_K^\times$$

However, at the ramified places of $\mathbb{I}_{K,S_\infty}$, the image of the norm map cannot contain -1 so the image of -1 inside the group $\hat{H}^0(G,\mathbb{I}_{K,S_\infty})$ is nontrivial. The map, $H^2(G,\mathcal{O}_K^\times) \to H^2(G,\mathbb{I}_{K,S_\infty})$ is nontrivial by naturality of the shift by two isomorphism. However,

$$H^2(G,M) = \hat{H}^2(G,M) \cong \hat{H}^0(G,M) \cong \mathcal{O}_K$$

which has size two. Thus, any nontrivial map is injective. By the theory above, we have that,

$$Cl(K)^G \cong H^1\left(G,\mathbb{I}_{K,S_\infty}/\mathcal{O}_K^\times\right) \cong H^1(G,\mathbb{I}_{K,S_\infty})/H^1(G,\mathcal{O}_K^\times)$$

[1] This is not much of a restriction since we know that the class numbers of the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$ are both 1.

Furthermore, since $\mathcal{O}_K^\times$ is a trivial G-module,

$$H^1(G, \mathcal{O}_K^\times) = \mathrm{Hom}\left(G, \mathcal{O}_K^\times\right) \cong \mathbb{Z}/2\mathbb{Z}$$

and using Lemma 5.6 we find that,

$$Cl(K)^G \cong \left(\prod_{p \text{ ram.}} (\mathbb{Z}/e_p\mathbb{Z})\right) / (\mathbb{Z}/2\mathbb{Z})$$

However, since $n = 2$ for a quadratic field and $efg = 2$ we know that if a prime p is ramified then $e_p = 2$. Thus,

$$Cl(K)^G \cong (\mathbb{Z}/2\mathbb{Z})^{r-1}$$

where r is the number of ramified primes in K. In particular, this implies that the class number h_K of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p_1 \cdots p_k})$ for distinct primes p_i has a fast growing lower bound, [2]

$$h_K \geq 2^{k-1}$$

This gives an affirmative answer to Gauss' conjecture that the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$ goes to infinity as d goes to infinity.

(b)

I give up. Please have mercy.

(c)

If $K/\mathbb{Q}$ is a real quadratic extension rather than an imaginary one then vital steps in our proof break down. First, the map $H^2(G, \mathcal{O}_K^\times) \to H^2(G, \mathbb{I}_{K,S_\infty})$ will not be generically be surjective. Since the group of units will be infinite by Dirichlet's theorem, $H^1(G, \mathcal{O}_K^\times)$ will be much more complicated. However, the identification,

$$Cl(K)^G \cong H^1\left(G, \frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right) \cong H^1\left(G, \frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}\right)$$

does still hold. However, rather than moding by torsion, we are now moding this idele group by an infinite abelian group. The resulting cohomology is much more difficult to calculate. I certianlly don't know how to do it in general.

[2] The prime 2 may ramify even if $p_i \neq 2$ for any i. This occurs when $p_1 \cdots p_k \equiv 1 \pmod 4$ and only increases the exponent by one thus not altering the result.

5 Lemmata

Lemma 5.1. *There is an exact sequence,*

$$1 \longrightarrow \mathbb{I}_{K,S_\infty} \cdot K^\times \longrightarrow \mathbb{I}_K \longrightarrow Cl(K) \longrightarrow 1$$

In particular, if $Cl(K) = 1$ then the exact sequence reduces to,

$$1 \longrightarrow \mathbb{I}_{K,S_\infty} \cdot K^\times \longrightarrow \mathbb{I}_K \longrightarrow 1$$

and thus $\mathbb{I}_K \cong \mathbb{I}_{K,S_\infty} \cdot K^\times$.

Proof. Define a map $\Phi : \mathbb{I}_K \to Cl(K)$ via,

$$(a_v) \mapsto \prod_{v \notin S_\infty} \mathfrak{p}_v^{\mathrm{ord}_\mathfrak{p}(a_v)}$$

which is clearly surjective. The kernel of this map is exactly elements of the form $(a_v) \in \mathbb{I}_K$ such that $\Phi((a_v)) = k\mathcal{O}_K$ is a principal ideal. Then, at each non-archimedean place, by Dedekind factorization,

$$\mathrm{ord}_{\mathfrak{p}_v}(k) = \mathrm{ord}_{\mathfrak{p}_v}\left(\prod_{v \notin S_\infty} \mathfrak{p}_v^{\mathrm{ord}_\mathfrak{p}(a_v)}\right) = \mathrm{ord}_{\mathfrak{p}_v}(a_v)$$

Thus, $a_v = ku_v$ where $u_v \in \mathcal{O}_v^\times$ since a_v and k generate the same ideal in $\mathcal{O}_v$. Thus, $(a_v) \in \mathbb{I}_{K,S_\infty} \cdot K^\times$. Clearly, any element of $\mathbb{I}_{K,S_\infty} \cdot K^\times$ is principal and thus in the kernel of Φ. Thus, $\ker \Phi = \mathbb{I}_{K,S_\infty} \cdot K^\times$ and the required exact sequence follows immediately. ☐

Lemma 5.2. *Let L/K be a galois extension of global fields with $G = Gal(L/K)$. Let C_L is the idele class group of L, then $H^1(G, C_L) = 1$.*

Proof. See Milne Section VII, Theorem 5.1. ☐

Lemma 5.3. *Let L/K be a finite galois extensions with $G = Gal(L/K)$. Then $C_L^G = C_K$.*

Proof. Consider the short exact sequence,

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

which gives rise to a long exact sequence of cohomology,

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

where $H^1(G, L^\times) = 1$ by Hilbert's theorem 90. However, $(L^\times)^G = K^\times$ and $(\mathbb{I}_L)^G = \mathbb{I}_K$ by Galois theory. Therefore, we have a short exact sequence,

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

Thus, under the natural inclusions,

$$(C_L)^G = \frac{\mathbb{I}_K}{K^\times} = C_K$$

☐

Lemma 5.4. *Let L/K be a finite galois extensions. 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, $H^1(D, \mathcal{O}_{\mathfrak{P}}^\times) = 1$ so we get he exact sequence,

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

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,

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

$\square$

Lemma 5.5. *Let L/K be a finite galois extension with Galois group $G = Gal(L/K)$. Let v be a prime of K with a prime w_0 in L such that $w_0 \mid v$. Then,*

$$H^r(G, \prod_{w|v} L_w^\times) \cong H^r(D(w_0), L_{w_0}^\times)$$

and likewise,

$$H^r(G, \prod_{w|v} \mathcal{O}_w^\times) \cong H^r(D(w_0), \mathcal{O}_{w_0}^\times)$$

Proof. We use the fact that,

$$\prod_{w|v} L_w^\times = \mathrm{Ind}_{D(w_0)}^G L_{w_0}^\times$$

and similarly, that,

$$\prod_{w|v} \mathcal{O}_w^\times = \mathrm{Ind}_{D(w_0)}^G \mathcal{O}_{w_0}^\times$$

Therefore, by Shapiro's Lemma,

$$H^r(G, \prod_{w|v} L_w^\times) = H^r(G, \mathrm{Ind}_{D(w_0)}^G L_{w_0}^\times) = H^r(D(w_0), L_{w_0}^\times)$$

and similarly,

$$H^r(G, \prod_{w|v} \mathcal{O}_w^\times) = H^r(G, \mathrm{Ind}_{D(w_0)}^G \mathcal{O}_{w_0}^\times) = H^r(D(w_0), \mathcal{O}_{w_0}^\times)$$

$\square$

Lemma 5.6. *Let L/K be finite galois 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. Then,*

$$H^r(G, \mathbb{I}_{L,T}) = \prod_{v \notin S} H^r(D(w_0), \mathcal{O}_{w_0}^\times) \times \prod_{v \in S} H^r(D(w_0), L_{w_0}^\times)$$

In particular, $(\mathbb{I}_L)^G = H^0(G, \mathbb{I}_L) = \mathbb{I}_K$ and $H^1(G, \mathbb{I}_L) = 1$ and last but not least,

$$H^1(G, \mathbb{I}_{L,T_\infty}) = \prod_{v \ ram.} (\mathbb{Z}/e_{w_0|v}\mathbb{Z})$$

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,

$$H^r(G, \mathbb{I}_{L,T}) = \prod_{v \notin S} H^r(D(w_0), \mathcal{O}_{w_0}^\times) \times \prod_{v \in S} H^r(D(w_0), L_{w_0}^\times)$$

In particular,

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

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,

$$H^r(G, \mathbb{I}_L) = \varinjlim_{T_0 \subset T} H^r(G, \mathbb{I}_{L,T}) = \varinjlim_{S_0 \subset S} \prod_{v \notin S} H^r(D(w_0), \mathcal{O}_{w_0}^\times) \times \prod_{v \in S} H^r(D(w_0), L_{w_0}^\times)$$

However, by assumption, all the ramified primes are in S so by a previous lemma,

$$H^1(D(w_0), \mathcal{O}_{w_0}^\times) = 0$$

Furthermore, by Hilbert's theorem 90,

$$H^1(D(w_0), L_{w_0}^\times) = 0$$

Therefore,

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

Furthermore,

$$\begin{aligned} H^0(G, \mathbb{I}_L) &= \varinjlim_{T_0 \subset T} H^r(G, \mathbb{I}_{L,T}) = \varinjlim_{S_0 \subset S} \prod_{v \notin S} H^0(D(w_0), \mathcal{O}_{w_0}^\times) \times \prod_{v \in S} H^0(D(w_0), L_{w_0}^\times) \\ &= \varinjlim_{S_0 \subset S} \prod_{v \notin S} (\mathcal{O}_{w_0}^\times)^{D(w_0)} \times \prod_{v \in S} (L_{w_0}^\times)^{D(w_0)} = \varinjlim_{S_0 \subset S} \prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} L_v^\times = \mathbb{I}_K \end{aligned}$$

Likewise, using Hilbert's Theorem 90 and Lemma 5.4,

$$\begin{aligned} H^1(G, \mathbb{I}_{L,T_\infty}) &= \prod_{v \notin S_\infty} H^1(D(w_0), \mathcal{O}_{w_0}^\times) \times \prod_{v \in S_\infty} H^1(D(w_0), L_{w_0}^\times) \\ &= \prod_{v \notin S_\infty} (\mathbb{Z}/e_{w_0|v}\mathbb{Z}) = \prod_{v \text{ ram.}} (\mathbb{Z}/e_{w_0|v}\mathbb{Z}) \end{aligned}$$

□

Lemma 5.7.

$$\left(\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G = \frac{\mathbb{I}_{\mathbb{Q},S_\infty} \cdot \mathbb{Q}^\times}{\mathbb{Q}^\times} = \frac{\mathbb{I}_{\mathbb{Q}}}{\mathbb{Q}^\times} = C_{\mathbb{Q}}$$

and similarly,

$$\left(\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G = \left(\frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}\right)^G = \frac{\mathbb{I}_{\mathbb{Q},S_\infty}}{\mathcal{O}_{\mathbb{Q}}^\times} = C_{\mathbb{Q}}$$

Proof. Let $G = Gal(K/\mathbb{Q})$ where $K/\mathbb{Q}$ is finite galois. Note that $\mathbb{Q}$ has class number 1 so by Lemma 5.3 we know that $\mathbb{I}_{\mathbb{Q}} = \mathbb{I}_{\mathbb{Q},S_\infty} \cdot \mathbb{Q}^\times$. Now, consider the exact sequence,

$$1 \longrightarrow K^\times \longrightarrow \mathbb{I}_{K,S_\infty} \cdot K^\times \longrightarrow \tfrac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times} \longrightarrow 1$$

which gives rise to a long exact sequence of cohomology,

$$1 \longrightarrow (K^\times)^G \longrightarrow (\mathbb{I}_{K,S_\infty} \cdot K^\times)^G \longrightarrow \left(\tfrac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G \longrightarrow H^1(G, K^\times) = 1$$

where $H^1(G, K^\times) = 1$ by Hilbert's Theorem 90. However,

$$\mathbb{I}_{\mathbb{Q}} = \mathbb{I}_{\mathbb{Q},S_\infty} \cdot \mathbb{Q}^\times \subset (\mathbb{I}_{K,S_\infty} \cdot K^\times)^G \subset (\mathbb{I}_K)^G = \mathbb{I}_{\mathbb{Q}}$$

and thus, $(\mathbb{I}_{K,S_\infty} \cdot K^\times)^G = \mathbb{I}_Q$. Therefore, the long exact sequence reduces to a short exact sequence,

$$1 \longrightarrow \mathbb{Q}^\times \longrightarrow \mathbb{I}_{\mathbb{Q}} \longrightarrow \left(\tfrac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G \longrightarrow 1$$

Therefore,

$$\left(\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G = \mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^\times = C_{\mathbb{Q}}$$

Furthermore, by the second isomorphism theorem,

$$\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times} = \frac{\mathbb{I}_{K,S_\infty}}{K^\times \cap \mathbb{I}_{K,S_\infty}} = \frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}$$

And thus, again by the second isomorphism theorem,

$$\left(\frac{\mathbb{I}_{K,S_\infty} \cdot K^\times}{K^\times}\right)^G = \left(\frac{\mathbb{I}_{K,S_\infty}}{\mathcal{O}_K^\times}\right)^G = C_{\mathbb{Q}} = \frac{\mathbb{I}_{\mathbb{Q}}}{\mathbb{Q}^\times} = \frac{\mathbb{I}_{\mathbb{Q},S_\infty} \cdot \mathbb{Q}^\times}{\mathbb{Q}^\times} = \frac{\mathbb{I}_{\mathbb{Q},S_\infty}}{\mathcal{O}_{\mathbb{Q}}^\times}$$

□