LECTURE 23

Proof of the Second Inequality

Our goal for this lecture is to prove the “second inequality”: that for all extensions E/F of global fields, we have $H^1(G, C_E) = 0$, where $C_E := \mathbb{A}_E^\times/E^\times$ is the “idèle class group” of E. Our main case is when E/F is cyclic of order p, and $\zeta_p \in F$ for some primitive pth root of unity ζ_p, and we will reduce to this case at the end of the lecture (note that $\mathrm{char}(F) = 0$ as we are assuming that F is a number field). In this case, it suffices to show that

$$\#\hat{H}^0(C_E) = \#(C_F/\mathrm{N}C_E) = \#(\mathbb{A}_F^\times/F^\times \cdot \mathrm{N}(\mathbb{A}_E^\times)) \leq p.$$

Indeed, by the “first inequality,” we know that

$$\frac{\#\hat{H}^0(C_E)}{\#\hat{H}^1(C_E)} = p,$$

hence $p \cdot \#\hat{H}^1(C_E) = \#\hat{H}^0(C_E) \leq p$ implies $\#H^1(C_E) = 1$, as desired. Our approach will be one of “trial and error”—that is, we’ll try something, which won’t quite be good enough, and then we’ll correct it.

Fix, once and for all, a finite set S of places of F such that

(1) if $v \mid \infty$, then $v \in S$;
(2) if $v \mid p$, then $v \in S$;
(3) $\mathbb{A}_F^\times = F^\times \cdot \mathbb{A}_{F,S}^\times$, where we recall that

$$\mathbb{A}_{F,S}^\times := \prod_{v \in S} F_v^\times \times \prod_{v \notin S} \mathcal{O}_{F_v}^\times$$

and that this is possible by Lemma 20.12;
(4) $E = F(\sqrt[p]{u})$, for some $u \in \mathcal{O}_{F,S}^\times := F^\times \cap \mathbb{A}_{F,S}^\times$ are the “S-units” of F. This is possible by Kummer Theory.

Note that this last condition implies that E is unramified outside of S, as u is an integral element in any place $v \notin S$, and since p is prime to the order of the residue field of F_v as all places dividing p are in S by assumption, $F_v(\sqrt[p]{u})/F_v$ is an unramified extension.

An important claim, to be proved later in a slightly more refined form, is the following:

Claim 23.1. *$u \in \mathcal{O}_{F,S}^\times$ is a pth power if and only if its image in $F_v^\times$ is a pth power for each $v \in S$.*

Let

$$\Gamma := \prod_{v \in S} (F_v^\times)^p \times \prod_{v \notin S} \mathcal{O}_{F_v}^\times \subseteq \mathbb{A}_{F,S}^\times.$$

Then we have the following claims:

Claim 23.2. $\mathcal{O}_{F,S}^\times \cap \Gamma = (\mathcal{O}_{F,S}^\times)^p$.

Proof. This follows trivially from the previous claim. □

Claim 23.3. $\Gamma \subseteq \mathrm{N}(\mathbb{A}_E^\times)$.

Proof. The extension E/F is unramified at each $v \notin S$, hence the factor $\prod_{v \notin S} \mathcal{O}_{F_v}^\times \subseteq \mathrm{N}(\mathbb{A}_E^\times)$. Since p kills $\hat{H}^0(E_w^\times)$, for a choice of $w \mid v$, it follows that the factor $\prod_{v \in S} (F_v^\times)^p \subseteq \mathrm{N}(\mathbb{A}_E^\times)$ as well. □

Thus,

$$\#(\mathbb{A}_F^\times / F^\times \cdot \mathrm{N}(\mathbb{A}_E^\times)) \leq \#(\mathbb{A}_F^\times / F^\times \cdot \Gamma),$$

and we have a short exact sequence

$$1 \to \mathcal{O}_{F,S}^\times / (\mathcal{O}_{F,S}^\times \cap \Gamma) \to \mathbb{A}_{F,S}^\times / \Gamma \to \mathbb{A}_F^\times / (F^\times \cdot \Gamma) \to 1.$$

Indeed, the third map is surjective by property (3) of S above, the second map is injective as $\mathcal{O}_{F,S}^\times \subseteq F^\times$, and exactness at $\mathbb{A}_{F,S}^\times/\Gamma$ holds by definition. Thus,

$$\#(\mathbb{A}_F^\times / F^\times \cdot \Gamma) = \frac{\#(\mathbb{A}_{F,S}^\times / \Gamma)}{\#(\mathcal{O}_{F,S}^\times / \mathcal{O}_{F,S}^\times \cap \Gamma)},$$

and it remains to compute both the numerator and denominator of this expression. We have

$$\mathbb{A}_{F,S}^\times / \Gamma = \prod_{p \in S} F_v^\times / (F_v^\times)^p,$$

and we recall from (6.3) that

$$\#(F_v^\times / (F_v^\times)^p) = \frac{p \cdot \#\mu_p(F_v)}{|p|_v} = \frac{p^2}{|p|_v}$$

as $\zeta_p \in F$ by assumption. Thus,

$$\prod_{v \in S} \frac{p^2}{|p|_v} = p^{2 \cdot \# S}$$

by the product rule, as $|p|_v = 1$ for $v \notin S$ by assumption. Now we'd like to compute

$$\#(\mathcal{O}_{F,S}^\times / \mathcal{O}_{F,S}^\times \cap \Gamma) = \#(\mathcal{O}_{F,S}^\times / (\mathcal{O}_{F,S}^\times)^p).$$

Recall that, by the S-unit theorem,

$$\mathcal{O}_{F,S}^\times \simeq \mathbb{Z}^{\# S - 1} \times (\mathcal{O}_{F,S}^\times)_{\mathrm{tors}}.$$

The latter is cyclic, and has order divisible by p, hence

$$\#(\mathcal{O}_{F,S}^\times / (\mathcal{O}_{F,S}^\times)^p) = p^{\# S - 1} \cdot p = p^{\# S}.$$

Combining these two results, we obtain

$$\#\hat{H}^0(C_E) \leq \frac{p^{2 \cdot \# S}}{p^{\# S}} = p^{\# S},$$

which is unfortunately not good enough.

Here is how we will improve on this result:

Claim 23.4. *Given such a set $S \subseteq M_F$, there exists a set $T \subseteq M_F$ such that*

(1) $\# T = \# S - 1$;
(2) $S \cap T = \varnothing$;
(3) every $v \in T$ is split in E, i.e., $E_w = F_v$ for all $w \mid v$;

(4) any $u \in \mathcal{O}_{F,S\cup T}^\times$ is a pth power if and only if $u \in F_v^\times$ is a pth power for all $v \in S$.

Note the key difference here from earlier: in property (4), we do not require that $u \in (F_v^\times)^p$ for all $v \in S \cup T$, merely for all $v \in S$. Given such a T, we redefine Γ by

$$\Gamma := \prod_{v\in S} (F_v^\times)^p \times \prod_{v \in T} F_v^\times \times \prod_{v \notin S\cup T} \mathcal{O}_{F_v^\times}.$$

Claim 23.5. *$\Gamma \subseteq \mathrm{N}(\mathbb{A}_E^\times)$.*

Proof. Property (3) implies the claim for the second factor; the first and third follow as before. □

Redoing our calculations with $\mathbb{A}_{F,S\cup T}^\times$ instead of $\mathbb{A}_{F,S}^\times$, we obtain

$$\#(\mathbb{A}_{F,S\cup T}^\times/\Gamma) = p^{2\cdot \#S}$$

as before by property (4), and

$$\#(\mathcal{O}_{F,S\cup T}^\times/(\mathcal{O}_{F,S\cup T}^\times \cap \Gamma)) = p^{\#(S\cup T)} = p^{2\cdot\#S-1},$$

again as before, hence their quotient is p, as desired! Thus, it suffices to prove the claim above.

Claim 23.6. *For any abelian extension F'/F of global fields, the Frobenius elements for $v \notin S$ generate* $\mathrm{Gal}(F'/F)$.

We'd like to prove this purely algebraically, without the Chebotarev density theorem (which, anyhow, gives a slightly different statement).

Proof. Let H be the subgroup generated by all Frobenii for $v \notin S$, and let $F'' := (F')^H$ be the fixed field. We'd like to show that $F'' = F$. Note that Frob_v is trivial in $\mathrm{Gal}(F'/F)/H = \mathrm{Gal}(F''/F)$ for all $v \notin S$, hence every $v \notin S$ splits in F''/F (as they are unramified by assumption). Thus, $F''_w = F_v$ for all $w \mid v$ and $v \notin S$, and we claim that this is impossible.

We may assume that F''/F is a degree-n cyclic extension (replacing it by a smaller extension if necessary). By the first inequality, $\chi(C_{F''}) = n$, which gives

$$\#(\mathbb{A}_F^\times/\mathrm{N}(\mathbb{A}_{F''}^\times)\cdot F^\times) = \#\hat{H}^0(C_{F''}) \geq n.$$

But because this extension is split for all $v \notin S$, we have $\mathrm{N}((F''_v)^\times) = F_v^\times$ trivially, and therefore $\prod_{v\notin S} F_v^\times \subseteq \mathrm{N}(\mathbb{A}_{F''}^\times)$, where this is the restricted direct product. Strong approximation then gives that $F^\times \cdot \prod_{v \notin S} F_v^\times$ is dense in $\mathbb{A}_F^\times$, and since it is also open, this is a contradiction unless $n = 1$, as desired. □

We'd like to apply this claim for $F' := F(\{\sqrt[p]{u} : u \in \mathcal{O}_{F,S}^\times\})$. First, a claim:

Claim 23.7. $\mathrm{Gal}(F'/F) = (\mathbb{Z}/p\mathbb{Z})^{\#S}$*, for F' as above.*

Proof. This is, in essence, Kummer theory, as $\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^p \subseteq F^\times/(F^\times)^p$. We know that all exponent-p extensions of F are given by adjoining pth roots of elements of $F^\times$. The Galois group must be a product of copies of $\mathbb{Z}/p\mathbb{Z}$, but some of these subgroups may coincide—iterated application of Kummer theory gives the statement. □

Now, we have $F'/E/F$, as E/F was assumed to be obtained by adjoining the pth root of some S-unit. Choose places $w_1, \dots, w_{\#S-1}$ of E that do not divide any places of S, whose Frobenii give a basis for $\mathrm{Gal}(F'/E) \simeq (\mathbb{Z}/p\mathbb{Z})^{\#S-1}$, which is possible by the argument of Claim 23.6. Then let $T := \{v_1, \dots, v_{\#S-1}\}$ be the restrictions of the w_i to F.

Claim 23.8. *Each $v \in T$ is split in E.*

Proof. Since $\mathrm{Frob}_v \in \mathrm{Gal}(F'/E)$, it acts trivially on E, so $\mathrm{Gal}(E_w/F_v)$ is trivial for any $w \mid v$, as desired. □

This establishes condition (3) for T; it remains to show condition (4), as conditions (1) and (2) are implicit in the construction of T.

Claim 23.9. *An element $x \in \mathcal{O}_{F,S\cup T}^\times$ is a pth power if and only if $x \in (F_v^\times)^p$ for every $v \in S$.*

Proof. **Step 1.** We claim that

$$\mathcal{O}_{F,S}^\times \cap (E^\times)^p = \{x \in \mathcal{O}_{F,S}^\times : x \in (F_v^\times)^p \text{ for all } v \in T\}.$$

The forward inclusion is trivial as $(F_v^\times)^p = (E_w^\times)^p$ by the previous claim. For the converse, note that for any $x \in \mathcal{O}_{F,S}^\times$, we have an extension $F'/E(\sqrt[p]{x})/E$. If $x \in (E_w^\times)^p$ for each $w \mid v$ and $v \in T$, then this extension is split at w, so Frob_w acts trivially on $E(\sqrt[p]{x})$, hence $\mathrm{Gal}(F'/E)$ acts trivially on $E(\sqrt[p]{x})$ as it is generated by these Frobenii, hence $E(\sqrt[p]{x}) = E$ and $x \in (E^\times)^p$ as desired.

Step 2. Now we claim that the canonical map

$$\mathcal{O}_{F,S}^\times \xrightarrow{\varphi} \prod_{v\in T} \mathcal{O}_{F_v}^\times/(\mathcal{O}_{F_v}^\times)^p$$

is surjective. This is the step that really establishes the limit on the size of T from which the second inequality falls out perfectly. We will proceed by computing the orders of both sides. By Step 1, we have

$$\mathrm{Ker}(\varphi) = \{x \in \mathcal{O}_{F,S}^\times : x \in (E^\times)^p\}.$$

Then $\mathcal{O}_{F,S}^\times/\mathrm{Ker}(\varphi)$ has order $p^{\#S-1}$. Indeed, we computed earlier that $\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^p$ has order $p^{\#S}$, and since

$$(\mathcal{O}_{F,S}^\times)^p = \{x \in \mathcal{O}_{F,S}^\times : x \in (F^\times)^p\}$$

and E/F is a degree-p extension obtained by adjoining the pth root of some S-unit, it follows that $[\mathrm{Ker}(\varphi) : (\mathcal{O}_{F,S}^\times)^p] = p$. Now, using the version of our earlier formula for $\mathcal{O}_{F_v}^\times$ (rather than $F_v^\times$), the right-hand side has order

$$\prod_{v\in T} \frac{\#\mu_p(F_v)}{|p|_v} = p^{\#T} = p^{\#S-1},$$

so the map is indeed surjective.

Step 3. We'd now like to establish the claim: that if $x \in (F_v^\times)^p$ for all $v \in S$, then $x \in (\mathcal{O}_{F,S\cup T}^\times)^p$ (the converse is trivial). We'd like to show that $F(\sqrt[p]{x}) = F$. Set

$$\Gamma := \prod_{v\in S} F_v^\times \times \prod_{v\in T} (\mathcal{O}_{F_v}^\times)^p \times \prod_{v\notin S\cup T} \mathcal{O}_{F_v}^\times \subseteq \mathbb{A}_{F,S}^\times,$$

where this is again a different Γ from earlier. Then in fact,

$$\Gamma \subseteq \mathrm{N}(\mathbb{A}^\times_{F(\sqrt[p]{x})}) \subseteq \mathbb{A}^\times_F,$$

where the third term is because $F(\sqrt[p]{x})/F$ is unramified outside of $S \cup T$, the second because $[F(\sqrt[p]{x}) : F] \leq p$, and the first because the extension is split at all places of S by assumption. Now, we want to show that $F^\times \cdot \Gamma = \mathbb{A}^\times_F$, because the first inequality then implies the result as in Claim 23.6. By Step 2, we have

$$\mathcal{O}^\times_{F,S} \twoheadrightarrow \prod_{v \in T} \mathcal{O}^\times_{F_v}/(\mathcal{O}^\times_{F_v})^p = \mathbb{A}^\times_{F,S}/\Gamma,$$

hence $\mathcal{O}^\times_{F,S} \cdot \Gamma = \mathbb{A}^\times_{F,S}$. This implies that

$$F^\times \cdot \Gamma = F^\times \cdot \mathbb{A}^\times_{F,S} = \mathbb{A}^\times_F$$

by assumption on S. □

Now we'd like to infer the general case of the second inequality from the specific case proven above. The first step is as follows:

Claim 23.10. *If the second inequality holds for any cyclic order-p extension for which the base field contains a pth root of unity, then it holds for any cyclic order-p extension.*

Proof. Let E/F be a degree-p cyclic extension of global fields. Recall that the second inequality for E/F is equivalent to the existence of a canonical injection

$$\mathrm{Br}(F/E) \hookrightarrow \bigoplus_{v \in M_F} \mathrm{Br}(F_v).$$

Indeed, we have an short exact sequence

$$0 \to E^\times \to \mathbb{A}^\times_E \to C_E \to 0,$$

and the long exact sequence on cohomology then gives

$$\underbrace{H^1(G, \mathbb{A}^\times_E)}_{\bigoplus H^1(E^\times_w)=0} \to H^1(G, C_E) \to \mathrm{Br}(F/E) \to \bigoplus_v \mathrm{Br}(F_v/E_w) \subseteq \bigoplus_v \mathrm{Br}(F_v)$$

for some choice of $w \mid v$, where the first equality is by Hilbert's Theorem 90. In order to show the vanishing of $H^1(G, C_E)$, it suffices to show that the final map is injective. Now, the field extensions

$$\begin{tikzcd}
& E(\zeta_p) \arrow[dl, no head] \arrow[dr, no head] & \\
E \arrow[dr, no head] & & F(\zeta_p) \arrow[dl, no head] \\
& F &
\end{tikzcd}$$

induce a commutative diagram

$$\begin{tikzcd}
\mathrm{Br}(F/E) \arrow[r, hook, "\alpha"] \arrow[d, hook, "\gamma"] \arrow[dd, bend right=60, "\times[F(\zeta_p):F]"'] & \bigoplus_v \mathrm{Br}(F_v/E_w) \arrow[d, "\delta"] \\
\mathrm{Br}(F(\zeta_p)/E(\zeta_p)) \arrow[r, hook, "\beta"] \arrow[d] & \bigoplus_v \mathrm{Br}(F(\zeta_p)_w) \\
\mathrm{Br}(F/E), &
\end{tikzcd}$$

where the left-most maps are the restriction and inflation maps on cohomology, respectively, using the cohomological interpretation of the Brauer group (see Problem 2 of Problem Set 7). Moreover, the composition is injective on $\mathrm{Br}(F/E)$, as it is p-torsion (by Problem 2(c)), and $[F(\zeta_p) : F] \mid (p-1)$. Thus, γ is injective as well. Since the second equality holds for $E(\zeta_p)/F(\zeta_p)$ by assumption, β is injective, hence α is injective as well. □

Claim 23.11. *If the second inequality holds for any cyclic order-p extension of number fields, then it holds for any extension.*

Proof. We'd like to show that $H^1(G, C_E) = 0$. As for any Tate cohomology group of a finite group, we have an injection

$$H^1(G, C_E) \hookrightarrow \bigoplus_p H^1(G_p, C_E),$$

where G_p is the p-Sylow subgroup of G. Thus, we may assume that G is a p-group. Since every p-group G contains a normal subgroup H isomorphic to $\mathbb{Z}/p\mathbb{Z}$, we may assume that we have field extensions $E_2/E_1/F$, where $\mathrm{Gal}(E_2/E_1) \simeq H$ and $\mathrm{Gal}(E_1/F) \simeq G/H$. We may assume that the theorem holds for H acting on E_2 and G/H acting on E_1, so we may simply repeat the sort of argument showing injectivity on Brauer groups in the proof of the previous claim.

First, we claim that $C_{E_2}^H = C_{E_1}$. Indeed, we have a short exact sequence

$$0 \to E_2^\times \to \mathbb{A}_{E_2}^\times \to C_{E_2} \to 0,$$

and the long exact sequence on cohomology then gives

$$0 \to \underbrace{H^0(H, E_2^\times)}_{E_1^\times} \to \underbrace{H^0(H, \mathbb{A}_{E_2}^\times)}_{\mathbb{A}_{E_1}^\times} \to \underbrace{H^0(H, C_{E_2})}_{C_{E_2}^H} \to \underbrace{H^1(H, E_2^\times)}_{0}$$

by Hilbert's theorem 90. Note that $\mathbb{A}_{E_2}^{\times, H} = \mathbb{A}_{E_1}^\times$ as taking invariants by a finite group commutes with direct limits and products in the definition of the adèles.

Then we have

$$\mathrm{hKer}\left(C_{E_2}^{\mathrm{h}G} = (C_{E_2}^{\mathrm{h}H})^{\mathrm{h}G/H} \to (\tau^{\geq 2} C_{E_2}^{\mathrm{h}H})^{\mathrm{h}G/H}\right) \simeq \left(\tau^{\leq 0} C_{E_2}^{\mathrm{h}H}\right)^{\mathrm{h}G/H} = (C_{E_1})^{\mathrm{h}G/H},$$

where the first equality is by Problem 3 of Problem Set 6, the map follows by definition of truncation, the quasi-isomorphism is because $H^1(H, C_{E_2})$ vanishes by assumption, and finally, the second expression is simply the naive H-invariants of C_{E_2}, as the truncation kills all cohomologies in degrees greater than 0, so the previous claim gives the equality. The long exact sequence on cohomology then gives

$$\underbrace{H^1\big((C_{E_1})^{\mathrm{h}G/H}\big)}_{H^1(G/H, C_{E_1})=0} \to \underbrace{H^1\big((C_{E_2})^{\mathrm{h}G}\big)}_{H^1(G, C_{E_2})} \to \underbrace{H^1\big((\tau^{\geq 2} C_{E_2}^{\mathrm{h}H})^{\mathrm{h}G/H}\big)}_{0}$$

as the rightmost complex is in degrees at least 2. Thus, $H^1(G, C_{E_2}) = 0$, as desired. □

18.786 Number Theory II: Class Field Theory
Spring 2016