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 \( p \)-th root of unity \( \zeta_p \), and we will reduce to this case at the end of the lecture (note that \( \text{char}(F) = 0 \) as we are assuming that \( F \) is a number field).

In this case, it suffices to show that
\[
\# \hat{H}^0(C_E) = \#(C_F/NC_E) = \#(\mathbb{A}_F^\times / F^\times \cdot N(\mathbb{A}_E^\times)) \leq p.
\]
Indeed, by the “first inequality,” we know that
\[
\# \hat{H}^0(C_E) = \#(C_F/NC_E) = p,
\]
hence \( p \cdot \# \hat{H}^1(C_E) = \# \hat{H}^0(C_E) \leq p \) implies \( \# \hat{H}^1(C_E) = 1 \), 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
\[
\mathbb{A}_{F,S}^\times := \prod_{v \in S} F_v^\times \times \prod_{v \notin S} O_{F,v}^\times
\]
and that this is possible by Lemma 20.12;
4. \( E = F(\sqrt[p]{u}) \), for some \( u \in O_{F,S}^\times := F^\times \cap \mathbb{A}_{F,S}^\times \) 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.** \( u \in O_{F,S}^\times \) is a \( p \)-th power if and only if its image in \( F_v^\times \) is a \( p \)-th power for each \( v \in S \).

Let
\[
\Gamma := \prod_{v \in S} (F_v^\times)^p \times \prod_{v \notin S} O_{F,v}^\times \subseteq \mathbb{A}_{F,S}^\times.
\]
Then we have the following claims:

**Claim 23.2.** \( O_{F,S}^\times \cap \Gamma = (O_{F,S}^\times)^p \).
Proof. This follows trivially from the previous claim.

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

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

Thus,

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

and we have a short exact sequence

$$1 \to \mathcal{O}_{F,S}^\times / (\mathcal{O}_{F,S}^\times \cap \Gamma) \to \mathcal{A}_F^\times / \Gamma \to \mathcal{A}_F^\times / (F^\times \cdot \Gamma) \to 1.$$
(4) any $u \in \mathcal{O}_{F,S,T}^\times$ is a $p$th power if and only if $u \in F_v^\times$ is a $p$th 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 $\Gamma$ 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.** $\Gamma \subseteq N(\mathbb{A}_E^\times)$.

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

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

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

as before by property (4), and

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

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 $\text{Gal}(F'/F)$.

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 Frobenius is trivial in $\text{Gal}(F'/F)/H = \text{Gal}(F''/F)$ 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 $w | v$ 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

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

But because this extension is split for all $v \notin S$, we have $N((F_v'')^\times) = F_v^\times$ trivially, and therefore $\prod_{v \notin S} F_v^\times \subseteq N(\mathbb{A}_{F''}^\times)$, 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.** $\text{Gal}(F'/F) = (\mathbb{Z}/p\mathbb{Z})^{#S}$, 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 $p$th 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 $p$th root of some $S$-unit. Choose places $w_1,\ldots,w_{#S-1}$ of $E$ that do not divide any places of $S$, whose Frobenius give a basis for $\text{Gal}(F'/E) \simeq (\mathbb{Z}/p\mathbb{Z})^{#S-1}$, which is possible by the argument of Claim 23.6. Then let $T := \{v_1,\ldots,v_{#S-1}\}$ be the restrictions of the $w_i$ to $F$.

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

**Proof.** Since $\text{Frob}_v \in \text{Gal}(F'/E)$, it acts trivially on $E$, so $\text{Gal}(E_w/F_v)$ 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 $x \in \mathcal{O}_{F,S,T}^\times$ is a $p$th 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 $F'/E(\sqrt[p]{\mathcal{O}})/E$. If $x \in (E^\times)_p$ for each $w \mid v$ and $v \in T$, then this extension is split at $w$, so $\text{Frob}_w$ acts trivially on $E(\sqrt[p]{\mathcal{O}})$, hence $\text{Gal}(F'/E)$ acts trivially on $E(\sqrt[p]{\mathcal{O}})$ as it is generated by these Frobenius, hence $E(\sqrt[p]{\mathcal{O}}) = E$ 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

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

Then $\mathcal{O}_{F,S}^\times/\text{Ker}(\varphi)$ 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 $p$th root of some $S$-unit, it follows that $[\text{Ker}(\varphi) : (\mathcal{O}_{F,S}^\times)_p] = p$. 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

$$\prod_{v \in T} \frac{\#\mathcal{O}_{F_v}}{|p|_v} = \frac{p^{#T}}{p^{#S-1}},$$

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 $x \in (\mathcal{O}_{F,S,T}^\times)_p$ (the converse is trivial). We’d like to show that $F(\sqrt[p]{\mathcal{O}}) = F$.

Set

$$\Gamma := \prod_{v \in S} F_v^\times \times \prod_{v \in T} (\mathcal{O}_{F_v}^\times)_p \times \prod_{v \in S \cup T} \mathcal{O}_{F_v}^\times \subseteq \mathcal{A}_{F,S}^\times,$$
where this is again a different $\Gamma$ from earlier. Then in fact,
\[ \Gamma \subseteq N(A_F^\times) \subseteq A_F^\times, \]
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 $F^\times \cdot \Gamma = \hat{A}_F^\times$, because the first inequality then implies the result as in Claim 23.6. By Step 2, we have
\[ \mathcal{O}_{F,S}^\times \rightarrow \prod_{v \in T} \mathcal{O}_{F_v}^\times / (\mathcal{O}_{F_v}^\times)^p = \hat{A}_{F,S}^\times / \Gamma, \]
and hence $\mathcal{O}_{F,S}^\times \cdot \Gamma = \hat{A}_{F,S}^\times$. This implies that
\[ F^\times \cdot \Gamma = F^\times \cdot \hat{A}_{F,S}^\times = \hat{A}_F^\times \]
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 $p$th 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
\[ Br(F/E) \hookrightarrow \bigoplus_{v \in M_F} Br(F_v). \]
Indeed, we have an short exact sequence
\[ 0 \rightarrow E^\times \rightarrow \hat{A}_E^\times \rightarrow C_E \rightarrow 0, \]
and the long exact sequence on cohomology then gives
\[ H^1(G, \hat{A}_E^\times) \rightarrow H^1(G, C_E) \rightarrow Br(F/E) \rightarrow \bigoplus_{v} Br(F_v/E_w) \subseteq \bigoplus_{v} Br(F_v) \]
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
\[
\begin{array}{ccc}
E(\zeta_p) & \rightarrow & F(\zeta_p) \\
\downarrow & & \downarrow \\
E & \rightarrow & F(\zeta_p)
\end{array}
\]
induce a commutative diagram

\[
\begin{array}{ccc}
Br(F/E) & \xrightarrow{\alpha} & \bigoplus_v Br(F_v/E_v) \\
\downarrow \gamma & & \downarrow \delta \\
\times [F(\zeta_p):F] Br(F(\zeta_p)/E(\zeta_p)) & \xrightarrow{\beta} & \bigoplus_v Br(F(\zeta_p)_w) \\
\downarrow & & \downarrow \\
Br(F/E),
\end{array}
\]

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 $Br(F/E)$, as it is $p$-torsion (by Problem 2(c)), and $[F(\zeta_p):F] \mid (p-1)$. Thus, $\gamma$ is injective as well. Since the second equality holds for $E(\zeta_p)/F(\zeta_p)$ by assumption, $\beta$ is injective, hence $\alpha$ 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 $\text{Gal}(E_2/E_1) \simeq H$ and $\text{Gal}(E_1/F) \simeq G/H$. 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 $C^H_{E_2} = C_{E_1}$. 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

\[0 \to H^0(H, E_2^\times) \to H^0(H, \mathbb{A}_{E_2}^\times) \to H^0(H, C_{E_2}) \to H^1(H, E_2^\times) \to 0,
\]

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

\[\text{hKer} \left( C^{hG}_{E_2} = (C^{hH}_{E_2})^H \to (\tau^{\leq 2} C^{hH}_{E_2})^H \right) \simeq \left( \tau^{\leq 0} C^{hH}_{E_2} \right)^{hG/H} = (C_{E_1})^{hG/H},
\]

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

\[ H^1((C_{E_1})^{hG/H}) \rightarrow H^1((C_{E_2})^{hG}) \rightarrow H^1((\tau^{\geq 2}C_{E_2}^{hG/H})^{hG/H}) \]

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