LECTURE 20

Proof of the First Inequality

We begin by fulfilling our promise from the last lecture. Let $K^{\mathrm{sep}} = \overline{K}/L/K$ be an extension of nonarchimedean local fields.

Claim 20.1. *There is an exact sequence*

$$0 \to \mathrm{Br}^{\mathrm{coh}}(K/L) \to \mathrm{Br}^{\mathrm{coh}}(K) \to \mathrm{Br}^{\mathrm{coh}}(L).$$

Recall that $\mathrm{Br}^{\mathrm{coh}}(K/L)$ essentially encodes division algebras over K that split over L, and $\mathrm{Br}^{\mathrm{coh}}(K)$ and $\mathrm{Br}^{\mathrm{coh}}(L)$ encode division algebras over K and L, respectively. The kernel of the map $\mathrm{Br}^{\mathrm{coh}}(K) \to \mathrm{Br}^{\mathrm{coh}}(L)$ is essentially division algebras over K that split over L, but we'll make this precise from the cohomological side. One can do this with spectral sequences (which are a bit annoying), but our focus on chain complexes will allow for the proofs to come out much more conceptually. We will need the following construction:

Definition 20.2. Let X be a chain complex of A-modules. Then $\tau^{\leq n}X$ is the "truncated" chain complex

$$\cdots \to X^{n-2} \xrightarrow{d^{n-2}} X^{n-1} \xrightarrow{d^{n-1}} \mathrm{Ker}(d^n) \to 0 \to 0 \to \cdots$$

Lemma 20.3. *The identity map $\tau^{\leq n}X \to X$ is a map of complexes, and this gives an isomorphism $H^i(\tau^{\leq n}X) \xrightarrow{\sim} H^i(X)$ for all $i \leq n$.*

Proof. It suffices to note that the two central squares below commute by the definition of a chain complex:

$$\begin{tikzcd}
\cdots \arrow[r] & X^{n-2} \arrow[r] \arrow[d] & X^{n-1} \arrow[r] \arrow[d] & \mathrm{Ker}(d^n) \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & X^{n-2} \arrow[r] & X^{n-1} \arrow[r] & X^n \arrow[r] & X^{n+1} \arrow[r] & X^{n+1} \arrow[r] & \cdots .
\end{tikzcd}$$

□

Corollary 20.4. *If $X \xrightarrow{\mathrm{qis}} Y$, then the induced map $\tau^{\leq n}X \to \tau^{\leq n}Y$ is also a quasi-isomorphism.*

Remark 20.5. Truncation, $\tau^{\leq n}$, is the one operation that does *not* commute with cones.

Definition 20.6. $\tau^{\geq n+1}X := \mathrm{hCoker}(\tau^{\leq n}X \to X)$.

Lemma 20.7. *$H^iX \xrightarrow{\sim} H^i\tau^{\geq n+1}X$ for all $i \geq n+1$.*

Proof. A simple application of the long exact sequence on cohomology suffices. □

For the application to Brauer groups, we first introduce some notation:

$$\begin{aligned} G_K &:= \mathrm{Gal}(\overline{K}/K) \\ G_L &:= \mathrm{Gal}(\overline{K}/L) \\ H &:= \mathrm{Gal}(L/K), \end{aligned}$$

where we note that L/K must be Galois for $\mathrm{Br}^{\mathrm{coh}}(K/L)$ to be defined. Recall that

$$\begin{aligned} \mathrm{Br}^{\mathrm{coh}}(K) &:= H^2(G_K, \overline{K}^\times) \\ \mathrm{Br}^{\mathrm{coh}}(L) &:= H^2(G_L, \overline{K}^\times) \\ \mathrm{Br}^{\mathrm{coh}}(K/L) &:= H^2(H, \overline{L}^\times). \end{aligned}$$

The main observation is that

$$\left[(\overline{K}^\times)^{\mathrm{h}G_L}\right]^{\mathrm{h}H} = (\overline{K}^\times)^{\mathrm{h}G_K}$$

by Problem 3 on Problem Set 6, since we have a short exact sequence

$$1 \to G_L \to G_K \to H \to 1.$$

Proof (of Claim 20.1). Note that $L^\times = \tau^{\leq 0}(\overline{K}^\times)^{\mathrm{h}G_L}$ as complexes of H-modules. Then by definition,

$$\mathrm{hCoker}\big(L^\times \to (\overline{K}^\times)^{\mathrm{h}G_L}\big) = \tau^{\geq 1}(\overline{K}^\times)^{\mathrm{h}G_L} \simeq \tau^{\geq 2}(\overline{K}^\times)^{\mathrm{h}G_L},$$

since this is equivalent to asserting that $H^1(G_L, \overline{K}^\times) = 0$, which is just Hilbert's Theorem 90. Thus,

$$\mathrm{hCoker}\big((L^\times)^{\mathrm{h}H} \to (\overline{K}^\times)^{\mathrm{h}G_K}\big) = \big(\tau^{\geq 2}(\overline{K}^\times)^{\mathrm{h}G_L}\big)^{\mathrm{h}H}.$$

Finally, the long exact sequence on cohomology gives

$$\underbrace{H^1\big(\tau^{\geq 2}(\overline{K}^\times)^{\mathrm{h}G_L}\big)^{\mathrm{h}H}}_{0} \to \underbrace{H^2(H, L^\times)}_{\mathrm{Br}^{\mathrm{coh}}(K/L)} \to \underbrace{H^2(G_K, \overline{K}^\times)}_{\mathrm{Br}^{\mathrm{coh}}(K)} \to \underbrace{H^2(G_L, \overline{K}^\times)^H}_{\mathrm{Br}^{\mathrm{coh}}(L)^H} \hookrightarrow \mathrm{Br}^{\mathrm{coh}}(L)$$

since for the first term, taking group cohomology can only increase the degrees of a complex, therefore cannot introduce a non-trivial degree-1 cohomology, and for the last, group cohomology is equivalent to taking invariants in the lowest non-zero degree of a complex. □

Now we turn to global class field theory, which is in many ways less beautiful than local class field theory; our treatment will be commensurately less thorough.

Theorem 20.8 (Main Theorems of GCFT). *Let F be a global field. Then*

$$\mathrm{Gal}^{\mathrm{ab}}(G) \simeq (\widehat{\mathbb{A}_F^\times/F^\times}),$$

and moreover, for all finite Galois extensions E/F, we have

$$\mathrm{Gal}(E/F)^{\mathrm{ab}} \simeq \mathrm{N}(\mathbb{A}_E^\times)\backslash\mathbb{A}_F^\times/F^\times.$$

Note that here $\widehat{\cdot}$ denotes profinite completion as usual, and in the second equation we are taking the quotient of $\mathbb{A}_F^\times$ by two separate objects.

The "motto" of GCFT is that $C_F := \mathbb{A}_F^\times/F^\times$, the *idèle class group of F*, plays the role of $K^\times$ in LCFT, and they exhibit very similar behaviors (there's a theory of "class formations" to make this analogy tighter). Thus, we will be importing many of the methods of LCFT for our proofs of GCFT; for instance, we would expect that some sort of "existence theorem" along with Kummer theory would allow us to prove the former statement of Theorem 20.8 from the latter. We likely won't have time to show this implication in class, so instead we'll focus on showing this second assertion.

Our main "inputs" are the following:

THEOREM 20.9 (Inequalities of GCFT). *(1) Let E/F be a degree-n cyclic extension of global fields. Then $\chi(C_E) = n$ (i.e., the Herbrand quotient of C_E).*
(2) For all finite G-Galois extensions E/F of global fields, $H^1(G, C_E) = 0$.

The second statement is analogous to Hilbert's Theorem 90, but is *much* harder to show. These two statements are variously called the "first inequality" and "second inequality" of GCFT; our (arbitrarily) preferred convention is indicated. Indeed, the first inequality gives

$$\#\hat{H}^0(\mathbb{Z}/n\mathbb{Z}, C_E) = n \cdot \#H^1(\mathbb{Z}/n\mathbb{Z}, C_E) \geq n,$$

and the second inequality gives $\#H^0(\mathbb{Z}/n\mathbb{Z}, C_E) \leq n$, hence it is precisely n.

In this lecture, we will prove the first inequality. Throughout, we let E/F be a degree-n cyclic extension of global fields. To do this, we will compute $\chi(E^\times)$ and $\chi(\mathbb{A}_E^\times)$, or at least their quotient, which will give us $\chi(C_E)$ via the exact sequence

$$0 \to E^\times \to \mathbb{A}_E^\times \to C_E \to 0.$$

A slight problem is that both Herbrand quotients are infinite.

First, a general comment on the structure of the group cohomology of $\mathbb{A}_E^\times$:

CLAIM 20.10. *For a G-Galois extension E/F of global fields, we have*

$$\hat{H}^i(G, \mathbb{A}_E^\times) = \bigoplus_{v \in M_F} \hat{H}^i\big(G, (E \otimes_F F_v)^\times\big)$$

for each i, where M_F denotes the set of places (i.e., equivalence classes of valuations) of F.

To be clear, this claim is entirely local, using the structure of the adèles as amalgamating all local information about a global field; we do not make use of the diagonal embedding of $E^\times$, which allows us to treat a field globally within the adèles. Note that $E \otimes_F F_v$ is like the completion of E at v.

PROOF. Recall that

$$\mathbb{A}_E^\times = \varinjlim_{\substack{S \subset M_F \\ \#S < \infty}} \left(\prod_{v \in S} (E \otimes_F F_v)^\times \times \prod_{v \notin S} (\underbrace{\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}}_{\mathcal{O}_{E \otimes_F F_v}})^\times \right),$$

where S contains all ramified primes and infinite places (the set of which we henceforth denote by M_F^∞). Note that usually we take $S \subset M_E$; this alternate formulation instead expresses such places of E in terms of which places of F they lie over. By Problem 6(h) of Problem Set 6, $\hat{H}^i(G, -)$ commutes with direct limits bounded uniformly from below, and also with direct products. This implies that

$$\hat{H}^i(G, \mathbb{A}_E^\times) = \varinjlim_{\substack{S \subset M_F \\ \#S < \infty}} \left(\bigoplus_{v \in S} \hat{H}^i\big(G, (E \otimes_F F_v)^\times\big) \times \prod_{v \notin S} \hat{H}^i\big(G, (\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v})^\times\big) \right)$$

$$= \varinjlim_{\substack{S \subset M_F \\ \#S < \infty}} \bigoplus_{v \in S} \hat{H}^i\big(G, (E \otimes_F F_v)^\times\big).$$

Indeed, because S was assumed to contain all ramified primes, the extension E_w/F_v of local fields is unramified for any place $w \mid v$ of E with $v \notin S$, hence it has Galois group the decomposition group G_w. Then we have

$$\hat{H}^i\big(G, (\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v})^\times\big) = \hat{H}^i(G_w, \mathcal{O}_{E_w}^\times) = 0$$

for any $v \notin S$ and $w \mid v$ by Problem 1(d) on Problem Set 7, since

$$(\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_k)^\times = \prod_{w \mid v} \mathcal{O}_{E_w}^\times = \mathbb{Z}[G] \otimes_{\mathbb{Z}[G_w]} \mathcal{O}_{E,w}^\times$$

is an induced G-module, and the latter expression vanishes as noted in Example 14.3. $\square$

Now we attempt to circumvent the infinite-ness of the Herbrand quotients.

Definition 20.11. For any finite $M_F^\infty \subseteq S \subset M_F$, let

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

denote the *ring of S-adèles*, and similarly for the *group of S-idèles* $\mathbb{A}_{F,S}^\times$.

Lemma 20.12. *There exists a finite $S \subset M_F$ with $\mathbb{A}_{F,S}^\times \cdot F^\times = \mathbb{A}_F^\times$.*

Proof. This identity is equivalent to asserting that the map

$$\mathbb{A}_{F,S}^\times \to \mathbb{A}_{F,M_F^\infty}^\times \backslash \mathbb{A}_F^\times / F^\times = \mathrm{Cl}(F)$$

to the class group of F is surjective, where we may also take the quotient by $\mathbb{A}_{F,M_F^\infty}$ since it is contained in $\mathbb{A}_{F,S}$ by assumption, and the final canonical isomorphism is by Problem 1(b) of Problem Set 2. Under this isomorphism, a uniformizer $\mathfrak{p} \subseteq \mathcal{O}_K$ of $F_{\mathfrak{p}}$ maps to $[\mathfrak{p}] \in \mathrm{Cl}(F)$. Since $\mathrm{Cl}(F)$ is finite, we may simply take S to be M_F^∞ along with a set of places, each associated to a distinct element of $\mathrm{Cl}(F)$. $\square$

Now let us return to the case where E/F is cyclic, and choose a finite set $S \subset M_F$ containing the infinite and ramified places of S and satisfying $\mathbb{A}_{E,S}^\times \cdot E^\times = \mathbb{A}_E^\times$, which is possible by the lemma (note that $\mathbb{A}_{E,S}^\times := \mathbb{A}_{E,T}^\times$, where T is the set of places of E lying above the places of F in S; thus, we are really applying the lemma to E, and projecting the set of places obtained down to F).

Claim 20.13. *We have a short exact sequence*

$$0 \to E_S^\times \to \mathbb{A}_{E,S}^\times \to C_E \to 0,$$

where $E_S^\times := E^\times \cap \mathbb{A}_{E,S}^\times$.

Proof. We have the following commutative diagram:

$$\begin{tikzcd}
 & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[d] \arrow[dddll, dashed, bend left] & \\
0 \arrow[r] & E_S^\times \arrow[r] \arrow[d] & \mathbb{A}_{E,S}^\times \arrow[r] \arrow[d] & \mathbb{A}_{E,S}^\times/E_S^\times \arrow[r] \arrow[d, "\psi"] & 0 \\
0 \arrow[r] & E_S^\times \arrow[r] \arrow[d] & \mathbb{A}_E^\times \arrow[r] \arrow[d] & C_E \arrow[r] \arrow[d] & 0 \\
 & E^\times/E_S^\times \arrow[r, hook, two heads, "\varphi"] & \mathbb{A}_E^\times/\mathbb{A}_{E,S}^\times \arrow[r] & 0, &
\end{tikzcd}$$

where the map φ is surjective by our choice of S and is also injective by the definition of $E_S^\times$ (i.e., $\varphi(x) \in \mathbb{A}_{E,S}^\times$ implies $x \in E_S^\times$). The snake lemma then implies that the map ψ is an isomorphism, as desired. □

By Claim 20.10, we have

$$\hat{H}^i(E, \mathbb{A}_{E,S}^\times) = \bigoplus_{v \in S} \hat{H}^\times\big(G, (E \otimes_F F_v)^\times\big),$$

so

$$\chi(\mathbb{A}_{E,S}^\times) = \prod_{v \in S} \chi\big((E \otimes_F F_v)^\times\big) = \prod_{v \in S} \chi\Big(\prod_{w \mid v} E_w^\times\Big) = \prod_{v \in S} \chi(E_w^\times) = \prod_{v \in S} [E_w : F_v]$$

for some choice of $w \mid v$ by Claim 7.8 and since

$$\Big(\prod_{w \mid v} E_w^\times\Big)^{\mathrm{t}G} \simeq (E_w^\times)^{\mathrm{t}G_w}$$

as before. Now we'd like to compute $\chi(E_S^\times)$, and we want it to satisfy

$$n \cdot \chi(E_S^\times) = \prod_{v \in S} [E_w : F_v],$$

again for some $w \mid v$. By Dirichlet's unit theorem, $E_S^\times$ is finitely generated, and therefore

$$E_S^\times \simeq (E_S^\times)_{\mathrm{tors}} \times \mathbb{Z}^r,$$

where r is the rank of $E_S^\times$. Thus, up to its torsion, $E_S^\times$ is an r-dimensional lattice.

Lemma 20.14. *If a cyclic group G acts on an $\mathbb{R}$-vector space V, and $\Lambda_1, \Lambda_2 \subseteq V$ are two lattices fixed under the G-action, then $\chi(\Lambda_1) = \chi(\Lambda_2)$ (where we are regarding both lattices as G-modules).*

We defer the proof to the next lecture for the sake of time. Now, recall the map used in the proof of the unit theorem:

$$\begin{aligned} E_S^\times &\to \prod_{w \in T} \mathbb{R} \\ x &\mapsto (\log |x|_w)_w, \end{aligned}$$

with T the primes of E lying above those in S, as before. The proof of the unit theorem shows that this map has finite kernel, and its image is a lattice in the hyperplane $\{(y_w)_w : \sum_w y_w = 0\}$. Thus,

$$\mathrm{Im}(E_S^\times) \cup \mathbb{Z} \cdot (1, 1, \ldots, 1)$$

is a lattice in $\prod_{w \in T} \mathbb{R}$, and so

$$\chi(E_S^\times) = \chi(\mathrm{Im}(E_S^\times)) = \frac{\chi(\Lambda)}{\chi(\mathbb{Z})} = \frac{\chi(\Lambda)}{n},$$

where Λ is any G-fixed lattice. Now,

$$\Lambda := \prod_{w \in T} \mathbb{Z} \subseteq \prod_{w \in T} \mathbb{R}$$

is one such lattice. The Galois group G acts on $\prod_{w|v} \mathbb{Z}$, hence

$$\chi(\Lambda) = \chi\Big(\prod_{v \in S} \prod_{w|v} \mathbb{Z}\Big) = \prod_{v \in S} \chi\Big(\prod_{w|v} \mathbb{Z}\Big) = \prod_{v \in S} \# G_w = \prod_{v \in S} [E_w : F_v]$$

for a choice of w, as desired. This completes the proof of the first inequality.

18.786 Number Theory II: Class Field Theory
Spring 2016