LECTURE 22

Artin and Brauer Reciprocity, Part II

In this lecture, our goal is to prove both the Artin and Brauer reciprocity laws, modulo the second inequality. Recall the statement of Artin reciprocity: for a number field F and place v, LCFT gives a map

$$\theta_v\colon F_v^\times \to \mathrm{Gal}^{\mathrm{ab}}(F),$$

and we claim that the induced map

$$\theta\colon \mathbb{A}_F^\times \to \mathrm{Gal}^{\mathrm{ab}}(F)$$

is trivial when restricted to $F^\times$. This is an enormous generalization of quadratic reciprocity: if $F = \mathbb{Q}$, then for any quadratic extension $\mathbb{Q}(\ell)$, we have $\theta_v(\cdot) = (\cdot, \ell)_v$, i.e., the Hilbert symbol over F_v, for v a prime or ∞. However, here we assert that this is true for the entire abelianized Galois group, and not just this particular quotient, which is a copy of $\mathbb{Z}/2\mathbb{Z}$.

Proof (of Artin Reciprocity). First note that for any abelian extension E/F, we obtain a map $\theta\colon \mathbb{A}_F^\times \to \mathrm{Gal}(E/F)$; clearly, it suffices to show vanishing in each such quotient.

Case 1. Let $F := \mathbb{Q}$ and $E := \mathbb{Q}(\zeta_{\ell^r})$ for some prime ℓ. We must show that $\theta(p) = 1$ for every prime p, and $\theta(-1) = 1$, as these elements generate $\mathbb{Q}^\times$ and θ is a group homomorphism. We proceed by explicit calculation using Dwork's theorem.

First suppose $p \neq \ell$. Then

$$\begin{cases} \theta_q(p) = 1, \\ \theta_\infty(p) = 1 \\ \theta_p(p) = p, \\ \theta_\ell(p) = p^{-1}, \end{cases}$$

for $q \neq p, \ell$. For the first equality, note that the cyclotomic extension E/F is unramified at q as long as $q \neq \ell$, and the local Artin map kills every element of $(\mathbb{Z}/q\mathbb{Z})^\times$ for an unramified extension at q (see the proof of Claim 21.5). For the second equality, note that each θ_v factors through the decomposition group at v, which in this case is $\mathbb{Z}/2\mathbb{Z}$, and it is not hard to see explicitly that $\theta_\infty\colon \mathbb{R}^\times \to \mathbb{Z}/2\mathbb{Z}$ corresponds to the sign function. For the third equality, note that E/F is unramified at p because $p \neq \ell$. By Dwork's theorem, the uniformizer p maps to its Frobenius element in $\mathrm{Gal}(E/F) = (\mathbb{Z}/\ell^r\mathbb{Z})^\times$, which is just p. Finally, the extension E/F is totally ramified at ℓ, and $p \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, so Dwork's theorem gives $\theta_\ell(p) = p^{-1}$.

Now suppose $p = \ell$. Then

$$\begin{cases} \theta_q(\ell) = 1, \\ \theta_\infty(\ell) = 1 \\ \theta_\ell(\ell) = 1, \end{cases}$$

for $q \neq \ell$. The final equality is by Dwork's theorem, as ℓ acts trivially on the totally ramified factor of the extension (and as its Frobenius element on the unramified factor).

Finally, we check $\theta(-1)$:

$$\begin{cases} \theta_q(-1) = 1, \\ \theta_\infty(-1) = -1 \\ \theta_\ell(-1) = (-1)^{-1}, \end{cases}$$

for $q \neq \infty, \ell$. Since $-1 \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, Dwork's theorem applies as before in the final case.

Case 2. Let $F := \mathbb{Q}$ as before and $E := \mathbb{Q}(\zeta_n)$, for any integer n. Then

$$n = \prod_{i=1}^{m} p_i^{r_i}$$

for primes p_i, and therefore

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{r_1}}) \cdots \mathbb{Q}(\zeta_{p_m^{r_m}})$$

is the compositum over its prime-power factors, hence

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \prod_{i=1}^{m} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{r_i}})/\mathbb{Q}).$$

Then the Artin map

$$\theta\colon \mathbb{A}_\mathbb{Q}^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

is given by the product over the Artin maps for $\mathbb{Q}(\zeta_{p_i^{r_i}})/\mathbb{Q}$ by LCFT, so it suffices to note the general claim that Artin reciprocity for linearly disjoint extensions implies Artin reciprocity for their compositum. That is, $\mathbb{Q}^\times$ is killed as each of its coordinates are killed by the previous case.

Case 3. Let F be a general number field, and $E := F(\zeta_n)$ for some integer n. By LCFT (at the level of multiplicative groups os local fields), we have the following commutative diagram:

$$\begin{array}{ccccc} F^\times & \hookrightarrow & \mathbb{A}_F^\times & \xrightarrow{\theta} & \mathrm{Gal}(F(\zeta_n)/F) \\ \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{A}_\mathbb{Q}^\times & \xrightarrow{\theta} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \end{array}$$

where θ denotes the Artin map. Since the rightmost map is an injection, it suffices to show that $\mathrm{N}(F^\times) \subseteq \mathbb{Q}^\times$ vanishes in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, but this is just the previous case.

Case 4. Let E/F be a cyclotomic extension of number fields, i.e., $E \subseteq F(\zeta_n)$, for some n. Then by LCFT, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{A}_F & \xrightarrow{\theta} & \mathrm{Gal}(F(\zeta_n)/F) \\ & \searrow^{\theta} & \downarrow \\ & & \mathrm{Gal}(E/F), \end{array}$$

and since θ kills $F^\times$ in the upper Galois group, it also does so in the lower one.

We have established that Artin reciprocity holds for all cyclotomic extensions of number fields; for the general case, we'll use Brauer reciprocity, to which we now turn. □

As a note, Sam is likely the only person in the world to call it "Brauer reciprocity"; usually, it is referred to as "calculation of Brauer groups from GCFT" or the like.

Let E/F be a G-Galois extension of global fields. We have a short exact sequence of G-modules

$$1 \to E^\times \to \mathbb{A}_E^\times \to C_E \to 1,$$

giving a composition

$$\underbrace{\mathrm{Br}(F/E)}_{H^2(G,E^\times)} \to \underbrace{\bigoplus_v \mathrm{Br}(F_v/E_w)}_{H^2(G,\mathbb{A}_E^\times)} \hookrightarrow \bigoplus_v \mathrm{Br}(F_v) \xrightarrow{(x_v)_{v\in M_F} \mapsto \sum_{v \in M_F \setminus M_F^\infty} x_v} \mathbb{Q}/\mathbb{Z},$$

where we recall that $\mathrm{Br}(F/E)$ denotes the group of division algebras over F that become matrix algebras when tensored with E; w is some choice of place lying over v; we recall that

$$\mathrm{Br}(F_v) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } v \text{ is finite,} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } v \text{ is real,} \\ 0 & \text{if } v \text{ is complex;} \end{cases}$$

and the rightmost map is referred to as the "invariants" map, as it is a sum over the "local invariants," which classify local division algebras. This composition corresponds to tensoring central simple algebras over division algebras over local places, taking the invariants at each such place, and adding them up. The direct sum tells us (automatically) that we obtain a matrix algebra over a field at all but finitely many places. Brauer reciprocity states that this composition is zero. So for instance, there is no central simple algebra over $\mathbb{Q}$, or any number field, with the property that it is a matrix algebra (splits) over a field at all places but one. Note that in the case when this composition is applied to a Hamiltonian algebra (associated to two rational numbers), then this simply records the Hilbert reciprocity law.

Claim 22.1. *Let E/F be a cyclic extension of global fields. Then Artin reciprocity is equivalent to Brauer reciprocity.*

Proof. Choosing some generator, we have $\mathrm{Gal}(E/F) = G \simeq \mathbb{Z}/n\mathbb{Z}$. Since G is cyclic, it is its own abelianization and Tate cohomology is 2-periodic, so we have the following commutative diagram:

$$\begin{array}{ccccc} \hat{H}^0(G,E^\times) = F^\times/\mathrm{N}(E^\times) & \longrightarrow & \hat{H}^0(G,\mathbb{A}_E^\times) = \mathbb{A}_F^\times/\mathrm{N}(\mathbb{A}_E^\times) & \xrightarrow{\theta} & G = \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\ \| & & \| & & \downarrow \\ \mathrm{Br}(F/E) = \hat{H}^2(G,E^\times) & \longrightarrow & \hat{H}^2(G,\mathbb{A}_E^\times) & \xrightarrow{\iota} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

where ι denotes the invariants map. Now, the left-hand square commutes trivially, and the right-hand square commutes by LCFT for cyclic extensions. The claim then follows by an easy diagram chase. □

CLAIM 22.2. *For any global field F and every $\beta \in \mathrm{Br}(F)$, there exists a cyclic cyclotomic extension E/F such that $\beta \in \mathrm{Br}(F/E)$, that is, β also lies in the relative Brauer group.*

Let us assume this claim for the moment. Then we can deduce the Brauer reciprocity law in general: since the extension E/F is cyclic, we know that Brauer reciprocity is equivalent to Brauer reciprocity, and moreover, we know Artin reciprocity holds as it is cyclotomic.

This claim is easy to check for local fields: given a division algebra over a local field K, then it is split over a field L/K if the square root of its degree divides $[L : K]$. Indeed, recall that if $\beta \subseteq \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subseteq \mathrm{Br}(K)$, i.e., β is a degree-n^2 division algebra, then $\beta \in \mathrm{Br}(K/L)$ if and only if $n \mid [L : K]$ because

$$\mathbb{Q}/\mathbb{Z} = \mathrm{Br}(K) \xrightarrow{\times[L:K]} \mathrm{Br}(L) = \mathbb{Q}/\mathbb{Z}.$$

Recall now the following theorem, which we will prove in the next lecture:

THEOREM 22.3. *For all extensions E/F of global fields, $H^1(G, C_E) = 0$.*

This is a sort of analog of Hilbert's Theorem 90, and proving this is the hardest part of GCFT; we'll assume it for now. The short exact sequence

$$1 \to E^\times \to \mathbb{A}_E^\times \to C_E \to 1$$

then gives an exact sequence

$$\underbrace{H^1(\mathbb{A}_E^\times)}_{0} \to \underbrace{H^1(C_E)}_{0} \to H^2(E) = \mathrm{Br}(F/E) \to H^2(\mathbb{A}_E^\times) = \bigoplus_v \mathrm{Br}(F_v/E_w)$$

where the vanishing is by the previous theorem and Hilbert's Theorem 90 (as the cohomology of the adèles is simply a direct sum over local cohomologies). Passing to direct limits, we obtain the following corollary:

COROLLARY 22.4. *For any global field F, there is a canonical injection*

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

In other words, any central simple algebra over a number field F is a matrix algebra if and only if it is a matrix algebra at each completion of F. This is definitely not an obvious statement!

The upshot is that, to prove Claim 22.2, it suffices to show the following:

CLAIM 22.5. *Given a finite set of places S of a global field F, and positive integers m_v for all $v \in S$ (such that $m_v = 1$ is v is complex, $m_v = 1, 2$ if v is real, and m_v is arbitrary if v is finite), then there exists a cyclic cyclotomic extension E/F such that E_w/F_v has degree divisible by m_v (for any choice of $w \mid v$).*

PROOF (CLAIM 22.5 $\Longrightarrow$ CLAIM 22.2). By Corollary 22.4, a central simple algebra over F splits if and only if it splits at every local field F_v, which is true if and only if the square root of its degree divides $[E_w : F_v]$ for some extension E/F and place $w \mid v$. Thus, choosing m_v to be the square root of its degree over F_v for each place v (alternatively, the denominator of its local invariant at v), which will necessarily be 1 or 2 if v is real and 1 if v is complex, this claim implies that our CSA splits over the extension E that it provides. Moreover, as noted previously, such a CSA will split over F_v for all but finitely many places v, which implies that we may take S to be the set of only those places at which our CSA does not split. □

Before beginning the proof, let us take a moment to note that there certainly exist cyclotomic extensions which are not cyclic! Indeed, we have $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, where ζ_n is a primitive nth root of unity, so for instance, if $n = 15$, then

$$(\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

is not cyclic!

Proof (of Claim 22.5). First note that we may assume $F = \mathbb{Q}$, as we may replace each local factor m_v by $[F_v : \mathbb{Q}_p] \cdot m_v$ (where p is the place of $\mathbb{Q}$ lying below v), apply the claim over $\mathbb{Q}$, and then replace E by the compositum $E \cdot F$, which is also a cyclic cyclotomic extension of F (as subgroups of cyclic groups are cyclic).

Case 1. Suppose that, for every local place $v \in S$, we have $m_v = p^{r_v}$ for some odd prime p (independent of v). For any r, we have a cyclotomic extension $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ with Galois group $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Note that $\#(\mathbb{Z}/p^r\mathbb{Z})^\times = (p-1)p^{r-1}$, so we may let $\mathbb{Q}(\zeta_{p^r})/E_r/\mathbb{Q}$ be a cyclic subextension with $\mathrm{Gal}(E_r/\mathbb{Q}) \simeq \mathbb{Z}/p^{r-1}\mathbb{Z}$. Then for each $v \in S$ and any choice of $w \mid v$, we claim that $[E_{r,w} : \mathbb{Q}_v] \to \infty$ as $r \to \infty$. Indeed, any local field aside from $\mathbb{C}$ only contains finitely many roots of unity, so these extensions must be increasing in degree. Now, $[E_{r,w} : \mathbb{Q}_v] = [\mathbb{Q}_v(\zeta_{p^r}/\mathbb{Q}_v] \mid (p-1)p^\infty$, hence the p-power factor of this degree diverges, proving the claim in this case as S is finite. Let us note that these extensions are totally complex (i.e., every infinite place is complex), so we need not worry about real places v for which $m_v = 2$.

Case 2. Now suppose that $m_v = 2^{r_v}$ for each $v \in S$. This case is similar, aside from the fact that $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where this isomorphism may be obtained by checking the easy identity

$$\mathbb{Z}/2^{r-2}\mathbb{Z} \simeq \{x \in (\mathbb{Z}/2^r\mathbb{Z})^\times : x \equiv 1 \bmod 4\}$$

(so show that it is cyclic by computing its 2-torsion and then verifying that it contains only 2 elements, etc.) and noting that $\mathbb{Z}/2\mathbb{Z} \simeq \{1, 2^{r-1} - 1\}$. Then we may let $\mathbb{Q}(\zeta_{2^r})/E_r/\mathbb{Q}$ be a cyclotomic degree-2^{r-2} extension whose Galois group is $(\mathbb{Z}/2^{r-2}\mathbb{Z})^\times$, realized as a quotient of $(\mathbb{Z}/2^r\mathbb{Z})^\times$.

We claim that $E_r/\mathbb{Q}$ is a totally complex extension. Since it is an abelian extension, it suffices to show that complex conjugation, which corresponds to $-1 \in (\mathbb{Z}/2^r\mathbb{Z})^\times$, acts on it non-trivially. For sufficiently large r, $-1 \not\equiv 1 \bmod 4$, hence its projection to $(\mathbb{Z}/2^{r-2}\mathbb{Z})^\times$ is given by $1 - 2^{r-1} \neq 1$ via the explicit isomorphism above (note $2^{r-1} - 1 \equiv 3 \bmod 4$ is the only nontrivial element of either factor with this property). Thus, the extension $E_r/\mathbb{Q}$ suffices by an argument similar to that in the previous case.

Case 3. Finally, for the general case, take the compositum over all prime factors of the m_v's of the extensions we constructed in the previous two cases. Moreover, no "interference" can occur (causing the compositum not to be cyclic) as the Galois group of each extension has distinct prime-power order. □

Thus, assuming our analog of Hilbert's Theorem 90, every element of the Brauer group of a global field F is split by a cyclic cyclotomic extension, which implies Brauer reciprocity for all elements of $\mathrm{Br}(F)$. This implies Artin reciprocity for cyclic extensions, because the two reciprocity laws are equivalent for cyclic extensions. Finally, since any abelian group is a product of cyclic groups, every abelian extension E/F is the compositum of cyclic extensions, implying Artin reciprocity in general (we've already seen that Artin reciprocity for a set of linearly disjoint extensions implies that it holds for their compositum).