LECTURE 4

GCFT and Quadratic Reciprocity

Last time, we reduced non-degeneracy and bimultiplicativity of the Hilbert symbol $(\cdot,\cdot)$ to showing that for all quadratic extensions L/K, with K a local field, $\mathrm{N}L^\times \subseteq K^\times$ is a subgroup of index 2. We showed that this holds for unramified extensions and when $p = \mathrm{char}(\mathcal{O}_K/\mathfrak{p})$ is odd (the case when $p = 2$ was more-or-less shown in Problem 1 of Problem Set 1). In this lecture, we will perform a similar analysis in the global setting, that is, for $F = \mathbb{Q}$.

We compare the following two facts: first, that

$$\mathrm{Gal}^{\mathrm{ab}}(\mathbb{Q})/2 \simeq \mathrm{Hom}(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \{1,-1\}) = \mathrm{Hom}(\mathbb{Q}^\times, \{1,-1\}),$$

where the set of primes and -1 form a basis for this group as an $\mathbb{F}_2$-vector space. And second, that CFT predicts that

$$\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times \simeq \mathrm{Gal}^{\mathrm{ab}}(\mathbb{Q})$$

as a canonical isomorphism of profinite completions. Thus, we expect

$$\mathrm{Hom}(\mathbb{Q}^\times, \{1,-1\}) = \mathrm{Gal}^{\mathrm{ab}}(\mathbb{Q})/2 \simeq \mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2. \tag{4.1}$$

Recall the following definition:

Definition 4.1. The *ring of adèles* is defined as

$$\mathbb{A}_\mathbb{Q} := \varinjlim_S \prod_{p\notin S} \mathbb{Z}_p \times \prod_{p\in S} \mathbb{Q}_p,$$

where the S are finite sets of places (primes and ∞) of $\mathbb{Q}$, ordered by inclusion, and $\mathbb{Q}_\infty = \mathbb{R}$. The *group of idèles* is the multiplicative group of the ring of adèles,

$$\mathbb{A}_\mathbb{Q}^\times = \varinjlim_S \prod_{p\in S} \mathbb{Z}_p^\times \times \prod_{p\in S} \mathbb{Q}_p^\times,$$

with S as before.

Example 4.2. We have $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, where p ranges over all primes, and $\widehat{\mathbb{Z}}\times\mathbb{R} \subseteq \mathbb{A}_\mathbb{Q}$ embedded as a subring, in which we may diagonally embed any $n \neq 0$. Similarly, $\widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$, and $\widehat{\mathbb{Z}}^\times \times \mathbb{R}^\times \subseteq \mathbb{A}_\mathbb{Q}^\times$. However, 2 and $1/2$ won't be in $\widehat{\mathbb{Z}}^\times \times \mathbb{R}^\times$ as they aren't in $\mathbb{Z}_2^\times$, and the same holds for any rational number. If we add the rationals in to compensate, i.e., $\widehat{\mathbb{Z}}^\times \times \mathbb{Q}^\times \times \mathbb{R}^\times \to \mathbb{A}_\mathbb{Q}^\times$, then -1 is repeated in $\mathbb{Q}^\times$ and $\mathbb{R}^\times$, so we must replace $\mathbb{R}^\times$ with $\mathbb{R}_{>0}$ (see Problem 1 of Problem Set 2).

We'd like a pairing $\mathbb{A}_{\mathbb{Q}}^{\times} \times \mathbb{Q}^{\times} \to \{1, -1\}$ from the idèles and rationals to $\mathbb{Z}/2\mathbb{Z}$, that should factor through the squares:

$$\begin{array}{ccc} \mathbb{A}_{\mathbb{Q}}^{\times} \times \mathbb{Q}^{\times} & \longrightarrow & \{1, -1\} \\ \downarrow & \nearrow & \\ \mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} / (\mathbb{A}_{\mathbb{Q}}^{\times})^2 \times \mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^2. & & \end{array}$$

Here the copy of $\mathbb{Q}^{\times}$ in the left term of the product is the diagonally embedded "principal idèles," through which this pairing should also factor in order to realize (4.1). This map should induce an isomorphism (which is, in a sense, "non-degeneracy")

$$\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} / (\mathbb{A}_{\mathbb{Q}}^{\times})^2 \xrightarrow{\sim} \mathrm{Hom}(\mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^2, \{1, -1\}),$$

that is, the map shouldn't be identically one or "anything crazy like that."

So fix

$$x = (x_p)_p \in \mathbb{A}_{\mathbb{Q}}^{\times},$$

where p may be either prime or ∞, and define the desired pairing by

$$y \mapsto \prod_p (x_p, y)_p,$$

where we are regarding y as a p-adic unit, and $(\cdot, \cdot)_p$ denotes the Hilbert symbol at p, i.e., on $\mathbb{Q}_p$. Now, it's not even clear *a priori* that this infinite product is well-defined, and for this we introduce the following lemma:

LEMMA 4.3. *$(x_p, y)_p = 1$ for all but finitely many p.*

PROOF. Indeed, for all but finitely many p, we have $p \neq 2, \infty$, $x_p \in \mathbb{Z}_p^{\times}$, and $y \in \mathbb{Z}_p^{\times}$, which imply that $(x_p, y)_p = 1$ by the identities shown with the tame symbol (since the valuations of x_p and y are both 0). □

Now, this map is definitely bimultiplicatives, as each term is, and similarly definitely factors modulo squares, i.e., it is a map

$$\mathbb{A}_{\mathbb{Q}}^{\times} / (\mathbb{A}_{\mathbb{Q}}^{\times})^2 \to \{1, -1\}$$

since if we multiply by squares on either side, the Hilbert symbols don't change. Thus, this map factors modulo $\mathbb{Q}^{\times}$ on the first factor if and only if the following claim holds:

CLAIM 4.4. *For all $x, y \in \mathbb{Q}^{\times}$, we have $\prod_p (x, y)_p = 1$ (that is, this map is invariant by multiplying by a factor of $\mathbb{Q}^{\times}$ in the first factor, which by bimultiplicativity, means we pick up such a factor).*

REMARK 4.5. This is true for all number fields (using general places). In this lecture, we will see how this represents (approximately) a repackaging of quadratic reciprocity. This property is a sort of "conspiring" between the primes: "the p-adic fields are talking to each other behind the scenes; even though they are separate, they ensure that the product is 1." The word for such "conspiracies" is "reciprocity law."

PROOF (OF CLAIM). First of all, since the map is invariant under multiplication by squares, we can assume $x = \pm p_1 \cdots p_r$ and $y = \pm q_1 \cdots q_s$. Then bimultiplicativity implies that we can take $x \in \{-1, 2, p\}$ and $y \in \{-1, 2, q\}$, where p and

q denote odd primes. We prove the claim for the case were p and q are distinct odd primes.

We'd like to show that

$$(p,q)_\infty \times \prod_\ell (p,q)_\ell = 1,$$

where ℓ ranges over all primes. The first term is 1 since both p and q are positive, and we can likewise ignore ℓ on odd primes distinct from p and q, so this reduces to showing that

$$(p,q)_2 \cdot (p,q)_p \cdot (p,q)_q = 1.$$

Now, as shown on Problem 2(b) of Problem Set 1,

$$(p,q)_p = \left(\frac{(-1)^{v_p(p)v_p(q)} \frac{q^{v_p(p)}}{p^{v_p(q)}}}{p} \right) = \left(\frac{q}{p}\right),$$

and similarly, $(p,q)_q = \left(\frac{p}{q}\right)$, where we recall that

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{if } n \text{ is a square mod } p, \\ -1 & \text{otherwise,} \end{cases}$$

where n is prime to p. Furthermore,

$$(p,q)_2 := (-1)^{\varepsilon(p)\varepsilon(q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

which is equal to 1 unless $p \equiv q \equiv 3 \bmod 4$. Thus, we have reduced to elementary congruence conditions, and this is precisely the statement of quadratic reciprocity. □

Remark 4.6. Quadratic reciprocity allows for efficient computation of Legendre symbols via successive reduction.

Proof (of Quadratic Reciprocity). Regard the Legendre symbol as a map

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{1,-1\},$$

and reinterpret $\mathbb{F}_p^\times$ as $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, so that this is the unique nontrivial quadratic character of the Galois group. This character is encoded in a unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ (over $\mathbb{Q}$). We'd like to write this field as $\mathbb{Q}(\sqrt{d})$ for some d. We want some

$$x = \sum_{n=1}^{p-1} x_n \zeta_p^n \in \mathbb{Q}(\zeta_p)$$

such that for all $m \in (\mathbb{Z}/p\mathbb{Z})^\times$,

$$\sum_{n=1}^{p-1} x_n \zeta_p^{mn} = m \cdot x = \left(\frac{m}{p}\right) \cdot x = \sum_{n=1}^{p-1} \left(\frac{m}{p}\right) x_n \zeta_p^n,$$

as a Galois action, since $x_n \in \mathbb{Q}$ is fixed and the action is $\zeta_p \mapsto \zeta_p^m$. That is, the Galois group translates x by ± 1, implying that $x \in \mathbb{Q}(\zeta_d)$, our quadratic subfield.

This equality implies that $x_{mn} = \left(\frac{m}{p}\right) \cdot x_m$. By repeatedly solving this equation, we end up with this element (called a "Gauss sum")

$$x = G := \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n.$$

We know by design that $G^2 \in \mathbb{Q}$, but now we'd like to know which (in fact, we will see that it is either p or $-p$).

Suppose that $\chi\colon k^\times \to \mathbb{C}^\times$ is a multiplicative character, and $\psi\colon k \to \mathbb{C}^\times$ is an additive character, where K is any finite field. Let

$$G_{\chi,\psi} := \sum_{x \in k^\times} \chi(x)\psi(x).$$

REMARK 4.7. As a fun analogy, the gamma function is defined by

$$\Gamma(\chi_s) := \int_{\mathbb{R}_{>0}} e^{-t} t^s \, \frac{dt}{t},$$

and this is like a Gauss sum with $\psi(t) := e^{-t}$ and $\chi_s(t) := t^s$.

We need the following lemma:

LEMMA 4.8. *$G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} = \#k$ if χ and ψ are both not the identity.*

PROOF. We have

$$\begin{aligned} G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} &= \sum_{x,y \in k^\times} \chi(x)\psi(x)\chi^{-1}(y)\psi^{-1}(y) \\ &= \sum_{x,y \in k^\times} \chi(x/y)\psi(x-y) \\ &= \sum_{z,y \in k^\times} \chi(z)\psi(y(z-1)), \end{aligned}$$

where we have made the change of variables $z := x/y$, so that $x = zy$. Now, if $z \neq 1$, then $y(z-1)$ assumes all values in $k^\times$, so the fact that $\sum_{w \in k} \psi(w) = 0$ holds (by non-degeneracy). Thus, we obtain

$$\begin{aligned} G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} &= \sum_{z \in k^\times} \chi(z) \sum_{y \in k^\times} \psi(y(z-1)) \\ &= \sum_{z \in k^\times \setminus \{1\}} \chi(z)(-\psi(0)) + \chi(1) \sum_{y \in k^\times} \psi(0) \\ &= \chi(1) + 1 \cdot \sum_{y \in k^\times} 1 \\ &= 1 + \#k^\times \\ &= \#k, \end{aligned}$$

since $\sum_{w \in k^\times} \chi(w) = 0$ similarly. □

Now, we'd like to know what $G_{\chi^{-1},\psi^{-1}}$ is for ψ corresponding to a power of ζ_p and χ the multiplicative Legendre character. We have

$$G_{\chi^{-1},\psi^{-1}} = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{-n}$$

$$\begin{aligned}
&= \sum_{n=1}^{p-1} \left(\frac{-n}{p}\right) \zeta_p^n \\
&= \left(\frac{-1}{p}\right) \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n \\
&= \left(\frac{-1}{p}\right) G.
\end{aligned}$$

Thus,

$$G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} = G \cdot \left(\frac{-1}{p}\right) G = p,$$

and so

$$G^2 = \left(\frac{-1}{p}\right) \cdot p = (-1)^{(p-1)/2} \cdot p,$$

and G is the square root of either p of $-p$, depending on the condition.

Now, recall that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is unramified at $q \neq p$, and that we have an isomorphism

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) &\simeq (\mathbb{Z}/p\mathbb{Z})^\times, \\
\mathrm{Frob}_q &\mapsto q \bmod p.
\end{aligned}$$

Thus, $\left(\frac{q}{p}\right) = 1$ if and only if Frob_q fixes G; in fact,

$$\begin{aligned}
\mathrm{Frob}_q(G) = \mathrm{Frob}_q \left(\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n\right) &= \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{qn} = \sum_{n=1}^{p-1} \left(\frac{n/q}{p}\right) \zeta_p^n \\
&= \sum_{n=1}^{p-1} \left(\frac{qn}{p}\right) \zeta_p^n = \sum_{n=1}^{p-1} \left(\frac{q}{p}\right)\left(\frac{n}{p}\right) \zeta_p^n \\
&= \left(\frac{q}{p}\right) G.
\end{aligned}$$

Moreover,

$$G^{q-1} = (G^2)^{(q-1)/2} = ((-1)^{(p-1)/2} \cdot p)^{(q-1)/2} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \bmod q,$$

so

$$\left(\frac{q}{p}\right) G^2 = G^{q+1} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G^2 \bmod q.$$

After dividing through by $G^2 = (-1)^{(p-1)/2} \cdot p$ (which is invertible modulo q), we have

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \bmod q,$$

that is,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

as desired. □

18.786 Number Theory II: Class Field Theory

Spring 2016