LECTURE 5

Non-Degeneracy of the Adèle Pairing and Exact Sequences

Recall that we wanted a non-degenerate pairing, for which

$$\begin{aligned} \mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 &\to \{1, -1\} \\ ((x_p), r) &\mapsto \prod_p (x_p, r)_p \end{aligned} \tag{5.1}$$

was a candidate (as before, p ranges over all primes and ∞). Well-definedness of this pairing reduced to the reciprocity law

$$\prod_p (x, y)_p = 1 \quad \text{for} \quad x, y \in \mathbb{Q}^\times.$$

We saw that when $x = p$ and $y = q$ were odd primes, this reduced to quadratic reciprocity,

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

which we proved by considering the character

$$\chi \colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\left(\frac{\cdot}{p}\right)} \{1, -1\}.$$

We saw that this corresponded to a unique quadratic subextension of $\mathbb{Q}(\zeta_p)$,

$$\mathbb{Q}(\sqrt{\pm p}) = \mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right),$$

where the key point was that the Gauss sum

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

More generally, if $F/\mathbb{Q}$ is Galois with Galois group G, and a prime q of $\mathbb{Q}$ is unramified, then $[\mathrm{Frob}_q] \mapsto [1] \in G$ (where these are conjugacy classes) if and only if q splits in F. Thus,

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

since the right side is equivalent to the splitting of q in the extension $\mathbb{Q}(\sqrt{\pm p})$, which implies that

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

which yields the desired result.

Similarly, we may obtain the reciprocity result in other cases, such as:

PROPOSITION 5.1. *We have*

$$\prod_p (2,\ell)_p = 1,$$

where ℓ is an odd prime and p ranges over all primes (note that $(2,\ell)_\infty = 1$ trivially).

PROOF. As before, $(2,\ell)_p = 1$ if $p \neq 2, \ell$, and using the tame symbol,

$$(2,\ell)_\ell = \left(\frac{(-1)^{v(\ell)v(2)} \frac{2^{v(\ell)}}{\ell^{v(2)}}}{\ell} \right) = \left(\frac{2}{\ell} \right).$$

By the formula obtained in Problem 2(d) of Problem Set 1, we have

$$(2,\ell)_2 = (-1)^{\epsilon(1)\epsilon(\ell)+v(2)\theta(\ell)+v(\ell)\theta(1)} = (-1)^{\theta(\ell)},$$

where

$$(-1)^{\theta(\ell)} := \begin{cases} 1 & \text{if } \ell \equiv 1, -1 \bmod 8, \\ -1 & \text{if } \ell \equiv 3, -3 \bmod 8, \end{cases}$$

which corresponds to the canonical isomorphism from ℓ^2 in $\mathbb{Z}/16\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$. Thus, we'd like to show that

$$\left(\frac{2}{\ell} \right) = (-1)^{\theta(\ell)}.$$

To know whether or not 2 is a square modulo ℓ, we'd like a convenient expression for $\sqrt{2}$, i.e., a cyclotomic embedding of $\mathbb{Q}(\sqrt{2})$ (in which ℓ splits if and only if $\left(\frac{2}{\ell}\right) = 1$). Recall that if ζ_8 is a primitive eighth root of unity, then we may take $\zeta_8 = \sqrt{2}/2 + i\sqrt{2}/2$, and so

$$\zeta_8 + \zeta_8^{-1} = \zeta_8 + \bar{\zeta}_8 = 2\,\mathrm{Re}(\zeta_8) = \sqrt{2}.$$

Algebraically, we may show this identity by noting that

$$(\zeta_8 + \zeta_8^{-1})^2 + 2 + \zeta_8^2 + \zeta_8^{-2} = 2 + \zeta_4 + \zeta + 4^{-1} = 2,$$

since ζ_4 and ζ_4^{-1} are precisely i and $-i$. This gives $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$, and a character

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)) = (\mathbb{Z}/8\mathbb{Z})^\times \xrightarrow{\chi} \{1, -1\}.$$

We claim that $\left(\frac{2}{\cdot}\right) = \chi = (-1)^{\theta(\cdot)}$. Clearly $\mathrm{Ker}\left((-1)^{\theta(\cdot)}\right) = \{1, -1\}$, and an element $n \in (\mathbb{Z}/8\mathbb{Z})^\times$ is in $\mathrm{Ker}(\chi)$ if and only if it fixes $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, i.e.

$$\zeta_8 + \zeta_8^{-1} \mapsto \zeta_8^n + \zeta_8^{-n} = \zeta_8 + \zeta_8^{-1},$$

which only holds when $n = 1$ (both terms are fixed) or $n = -1$ (the terms are switched). Thus, the two kernels are the same, and therefore the two functions are equal. □

Note that we could also argue without using Galois groups. If we suppose that $\zeta_8 + \zeta_8^{-1} \in \overline{\mathbb{F}}_\ell$, then so show that $\zeta_8 + \zeta_8^{-1} \in \mathbb{F}_\ell$, we must simply check that $\zeta_8 + \zeta_8^{-1} = (\zeta_8 + \zeta_8^{-1})^\ell = \zeta_8^\ell + \zeta_8^{-\ell}$, i.e., it is fixed under the action of the Frobenius element, and thus we obtain the same conditions as before.

Other symbols are relatively tedious to check, for instance, $\prod_p (2,2)_p = 1$ is simple as $(2,2)_2 = 1$ as shown in Problem 2(d) of Problem Set 1, and $\prod_p (-1,\ell)_p = 1$ is

solved by noting that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Thus, we have checked the well-definedness of our initial pairing (5.1). We'd now like to check that our pairing is non-degenerate. Note that we don't really need reciprocity for this, as the arguments are easier.

PROPOSITION 5.2. *The map*

$$\chi\colon \mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2 \xrightarrow{\sim} \mathrm{Hom}(\mathbb{Q}^\times, \{1,-1\}) \simeq \mathrm{Gal}_2(\mathbb{Q})$$

defined in (5.1) is an isomorphism (note that it does not matter that the pairing defines maps from $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ as the homomorphisms on the right absorb squares).

PROOF. In Problem 1(a) of Problem Set 2, we showed that

$$\mathbb{A}_\mathbb{Q}^\times = \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0} \times \mathbb{Q}^\times,$$

where the first two terms are embedded via local places and the last term is embedded diagonally. Modding out by $\mathbb{Q}^\times$ removes the last term, and modding out by squares removes the second term, so we obtain

$$\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2 = \prod_p \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \tag{5.2}$$

by the Chinese Remainder Theorem, where p ranges over all primes; when p is odd, $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ is an order-2 group generated by any quadratic non-residue, and $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \simeq (\mathbb{Z}/8\mathbb{Z})^\times$ has order 4 and is generated by -1 and 5. Also,

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 = \{\pm p_1\cdots p_r : p_i \text{ primes}\} = \mathbb{Z}/2\mathbb{Z} \times \bigoplus_p \mathbb{Z}/2\mathbb{Z}$$

with p as before, where the first copy of $\mathbb{Z}/2\mathbb{Z}$ corresponds to sign. We will see that, dualizing, these copies of $\mathbb{Z}/2\mathbb{Z}$ all (nearly) match up.

Suppose p is an odd prime, and let r be a quadratic non-residue at p, i.e., a non-trivial element of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. Then

$$(\chi(r)(\pm q))_p = (r, \pm q)_p = \left(\frac{r^{v(\pm q)}/(\pm q)^{v(r)}}{p}\right) = \begin{cases} 1 & \text{if } q \neq p, \\ -1 & \text{if } q = p, \end{cases}$$

is the value of χ on the pth term of $\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2$, where q is a prime. For the last basis element, we have $\chi(r)(-1) = 1 = (r,-1)_p$. Thus, the obvious (topological) basis elements at p match up; now we must ask what happens at $p = 2$. A natural guess is the idèle defined by $r = -1$ or $r = 5$ at 2 and $r = 1$ elsewhere, since 5 corresponds to the unique unramified quadratic extension of $\mathbb{Q}_2$ by Problem 2(b) of Problem Set 2. Computing yields

$$\begin{aligned} \chi(5,1,1,\ldots)(q) &= (5,q)_2 = 1, \\ \chi(5,1,1,\ldots)(-1) &= (5,-1)_2 = 1, \\ \chi(5,1,1,\ldots)(2) &= (5,2)_2 = (-1)^{\theta(5)} = -1, \end{aligned}$$

so indeed, this basis element perfectly matches up to the basis element at 2. Here we have denoted idèles by tuples whose coordinates are taken with respect to the isomorphism (5.2), with primes ordered as usual. Then

$$\chi(-1,1,1,\ldots)(-1) = -1 = (-1,-1)_2$$

completes the proof. Now, the bases actually don't perfectly match up, since pairing with another odd prime p yields symbols corresponding to whether or not -1 is

a square modulo p, but we can easily express one basis in terms of the other by correcting for the $(-1,1,1,\ldots)$ basis element, using "upper triangular matrices" (essentially, we have an infinite matrix with ones along the diagonal, except at $(-1,1,1,\ldots)$, which corresponds to a more complicated element in the basis given for $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$).

Here's a slightly more serious argument. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \prod_{p\neq 2} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / (\mathbb{A}_{\mathbb{Q}}^\times)^2 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow & & \downarrow \simeq & & \\ 0 & \longrightarrow & \{\varphi \colon \mathbb{Q}^\times \to \mathbb{Z}/2\mathbb{Z} \mid \varphi(-1) = 1\} & \longrightarrow & \mathrm{Hom}(\mathbb{Q}^\times, \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{\varphi \mapsto \varphi(-1)} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0. \end{array}$$

The first copy of $\mathbb{Z}/2\mathbb{Z}$ corresponds to the idèle $(5,1,1,\ldots)$, and the other copies correspond to quadratic non-residues at each p; in the rightmost copy of $\mathbb{Z}/2\mathbb{Z}$, we obtain the image of $(-1,1,1,\ldots)$. The maps into $\mathbb{Z}/2\mathbb{Z}$ are both quotients, and the vertical map on the right is an isomorphism because it is non-trivial; the vertical map on the left is an isomorphism because everything matches up perfectly as we saw earlier. Thus, the map in the middle is an isomorphism, as desired. □

Now we return to the problem of showing that for any quadratic extension of local fields L/K, we have $\#(K^\times/\mathrm{N}L^\times) = 2$. Recall that this statement is equivalent to the bimultiplicativity and non-degeneracy of the Hilbert symbol, and that we've proved this in the case of odd primes and unramified and tamely ramified extensions, but we couldn't prove it for wildly ramified extensions or for extensions over $\mathbb{Q}_2$, aside from $\mathbb{Q}_2$ itself. Our present goal will be to prove this more generally: that is, to show that if L/K is a cyclic extension of degree n, i.e., that it is Galois with group $\mathbb{Z}/n\mathbb{Z}$, then $\#(K^\times/\mathrm{N}L^\times) = n$. To further place this in a more general context, if L/K is a finite abelian extension, then we actually expect

$$\mathrm{Gal}(L/K) \simeq K^\times/\mathrm{N}L^\times$$

canonically, so we expect more than an equality of numbers. We will show this using the methods of exact sequences and homological algebra, to which we now turn.

As it turns out, short exact sequences are really great tools for determining the orders of finite abelian groups. Suppose we have the short exact sequence

$$0 \to M \overset{g}{\hookrightarrow} E \overset{f}{\twoheadrightarrow} N \to 0.$$

Then $M = \mathrm{Ker}(f)$ and $N = \mathrm{Coker}(g) = E/M$; in terms of filtrations, M and N are like the associated graded terms. Indeed, we can think of M and N as the "atoms" and E as a "molecule," whose fine structure determines its "reactions". It's clear that if M and N are finite, then so is E, and $\#E = \#M\#N$. The problem with wild ramification is that we don't have a filtration on $L^\times$.

One problem is that many operations don't preserve short exact sequences. For instance, if $n \geq 1$ is an integer, modding out by n does not preserve $\#(E/nE)$.

Example 5.3. (1) If we have the exact sequence

$$0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{x \mapsto (x,0)} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{(x,y) \mapsto y} \mathbb{Z}/n\mathbb{Z} \to 0,$$

then modding out by n preserves it.

(2) If we have the exact sequence

$$0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{x \mapsto xn} \mathbb{Z}/n^2\mathbb{Z} \xrightarrow{1 \mapsto 1} \mathbb{Z}/n\mathbb{Z} \to 0,$$

then modding out by n changes the exact sequence to

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z}/n\mathbb{Z} \to 0.$$

We have the same "atoms," but they form a different "molecule." In the last case, the order was n^2 after modding out, whereas here it is n.

A central thesis of homological algebra is that we can correct this by extending exact sequences. Poetically, the altered exact sequence is like visible light; it's missing the infrared spectrum, which we will be able to see by extending the exact sequences. Specifically, this corresponds to n-torsion: $\mathbb{Z}/n^2\mathbb{Z}$ does not has as much n-torsion as $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which is all n-torsion.

For a module M, let $M[n] \subseteq M$ denote $\mathrm{Ker}(n\colon M \to M)$. Then we obtain a longer exact sequence

$$0 \to M[n] \to E[n] \to N[n] \xrightarrow{\delta} M/n \to E/n \to N/n \to 0,$$

where for $x \in N[n]$, $\delta(x) = ny$ for any $y \in E$ with $f(y) = x$; note that $f(ny) = nx = 0$, so $\delta(x) \in M \subseteq E$ as desired. We will show that this is an exact sequence in the next lecture.

18.786 Number Theory II: Class Field Theory

Spring 2016