Algebraic Number Theory – Lecture 10

Sandro Bettin

"You know that I write slowly. This is chiefly because I am never satisfied until I have said as much as possible in a few words, and writing briefly takes far more time than writing at length."

– Carl Friedrich Gauss

The goal of the lecture is to prove Gauss's reciprocity law, using methods related to what we have done in the past. Firstly, let's introduce the Legendre symbol.

Definition. For every integer a coprime to p, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 \text{ otherwise.} \end{cases}$$

Elementary properties of group theory show us that the Legendre symbol is multiplicative and that one has

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

and this gives

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

for any odd prime p. Gauss's reciprocity law gives us what's left for a full understanding of the Legendre symbol.

Theorem (Gauss's reciprocity law)**.** *For two distinct odd prime numbers p and q, the following identity holds:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

To prove this we need to state some other new results from ramification theory.

Proposition 1. *Let L/K be a Galois extension, $\mathfrak{B}$ an ideal of O_L with ramification index e and inertia degree f, and $Z_{\mathcal{B}}$ the decomposition field of $\mathcal{B}$ over K. Let $\mathcal{B}_Z = \mathcal{B} \cap Z_{\mathcal{B}}$ be the prime ideal of $Z_{\mathcal{B}}$ below $\mathcal{B}$. Then*

i) *$\mathcal{B}_Z$ is nonsplit in L, i.e. $\mathcal{B}$ is the only prime ideal of L above $\mathcal{B}_Z$.*
ii) *$\mathcal{B}$ over $Z_{\mathcal{B}}$ has ramification index e and inertia degree f.*
iii) *The ramification index and the inertia degree of $\mathcal{B}_Z$ over K both equal 1.*

Definition. Let $K \subseteq L = K(\theta)$ be number fields with $\theta \in O_L$ and let $p(x) \in O_K[x]$ be the minimal polynomial of θ. The conductor of the ring $O_K[\theta]$ is the biggest ideal $\mathcal{F}$ of O_L which is contained in $O_K[\theta]$, i.e.

$$\mathcal{F} = \{\alpha \in O_L \mid \alpha O_L \subseteq O_K[\theta]\}.$$

Proposition 2. *Let $\mathfrak{p} \subseteq O_K$ be a prime ideal, coprime with the conductor $\mathcal{F}$ of $O_K[\theta]$, and let*

$$\overline{p}(x) = \overline{p}_1(x)^{e_1} \cdots \overline{p}_r(x)^{e_r}$$

be the factorization of the polynomial $\overline{p}(x) = p(x) \pmod{\mathfrak{p}}$ into irreducibles $\overline{p}_i(x) = p_i(x) \pmod{\mathfrak{p}}$ over the residue class field $O_k/\mathfrak{p}$, with all $p_i \in O_K[x]$. Then

$$\mathcal{B}_i = pO_L + p_i(\theta)O_L, \qquad i = 1, \ldots, r,$$

are the different prime ideals of O_L above $\mathfrak{p}$. The inertia degree f_i of $\mathcal{B}_i$ is the degree of $\overline{p}_i(x)$, and one has

$$\mathfrak{p} = \mathcal{B}_1^{e_1} \cdots \mathcal{B}_r^{e_r}.$$

Proof. See Neukirch. □

Corollary 2.1. *For squarefree a and $(p, 2a) = 1$, we have that $\left(\frac{a}{p}\right) = 1$ if and only if p is totally split in $\mathbb{Q}(\sqrt{a})$.*

Proof. $\left(\frac{a}{p}\right) = 1$ signifies that

$$x^2 - a \equiv (x - \alpha)(x + \alpha) \pmod{p}$$

for some $\alpha \in \mathbb{Z}$. Since $O_{Q(\sqrt{a})} \subseteq \mathbb{Z}[\frac{\sqrt{a}}{2}]$, the conductor of $\mathbb{Z}[\sqrt{a}]$ is a divisor of 2 and so we can apply the previous proposition. □

Now we need to now something about the factorization of primes in the cyclotomic fields.

Proposition 3. *Let ζ_n be a primitive nth root of unity with $n = \prod_p p^{\nu_p}$ the prime factorization of n. Moreover, let f_p be the smallest positive integer such that*

$$p^{f_p} \equiv 1 \pmod{n/p^{\nu_p}}.$$

Then one has in $\mathbb{Q}(\zeta_n)$ the factorization

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p^{\nu_p})},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct prime ideals, all of degree f_p.

Proof. See Neukirch (it's a consequence of Proposition 2). □

Proposition 4. *Let q and p be odd primes, $q^* = (-1)^{\frac{q-1}{2}} q$ and ζ_q a primitive qth root of unity. Then p is totally split in $\mathbb{Q}(\sqrt{q^*})$ if and only if p splits in $\mathbb{Q}(\zeta_q)$ into an even number of prime ideals.*

Proof. A little computation shows that

$$q^* = \tau^2,$$

where τ is the Gauss sum

$$\tau = \sum_{a \in F_q^*} \left(\frac{a}{q}\right) {\zeta_q}^a.$$

Therefore $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q)$. Let's assume p is totally split in $\mathbb{Q}(\sqrt{q^*})$, say $p = \mathfrak{p}_1\mathfrak{p}_2$. Since all the extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q)$ are Galois extension, the number of ideals above $\mathfrak{p}_1$ is equal to the number of ideals above $\mathfrak{p}_2$ and so p splits in $\mathbb{Q}(\zeta_q)$ into an even number of prime ideals. By the previous proposition these ideals must be distinct since for $n = q$ we have $\nu_p = 0$.

Conversely, assume

$$pO_{\mathbb{Q}(\zeta_q)} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

with r even. Since $G = \mathrm{Gal}(Q(\zeta_q)/\mathbb{Q})$ is cyclic and therefore abelian, we have that all the decomposition groups $G_{\mathfrak{p}_i}$ are equal to a (normal) subgroup $G_{\mathfrak{p}}$ of G of even index. Therefore there exists a subgroup H of G of index 2 that contains $G_{\mathfrak{p}}$. But also $\mathrm{Gal}(Q(\zeta_q)/\mathbb{Q}(\sqrt{q^*}))$ is a subgroup of index 2 and so, since G is cyclic, H and $\mathrm{Gal}(Q(\zeta_q)/\mathbb{Q}(\sqrt{q^*}))$ must be equal. Thus

$$\mathrm{Gal}(Q(\zeta_q)/\mathbb{Q}(\sqrt{q^*})) \geqslant G_{\mathfrak{p}}$$

and so

$$Z_{\mathfrak{p}} \geqslant \mathbb{Q}(\sqrt{q^*}).$$

By Proposition 1, we have that the inertia degree and ramification index of $\mathfrak{p}_i \cap O_{Z_{\mathfrak{p}}}$ is 1 and so the same must hold for $\mathfrak{p}_i \cap O_{Q(\sqrt{q^*})}$, since e and f are multiplicative (easy exercise). □

We are now ready for the proof of Gauss's theorem.

Proof of Gauss's Reciprocity Law. By Corollary 3 we have that $\left(\frac{q^*}{p}\right) = 1$ if and only if p is totally split in $\mathbb{Q}(\sqrt{q^*})$ and by the previous proposition this happens if and only if p splits completely in $\mathbb{Q}(\zeta_q)$ into an even number of prime ideals (and by proposition 4 each of them has inertia degree f_p, so $r \cdot f_p \cdot 1 = q - 1$). Finally, this is equivalent to $f_p | \frac{q-1}{2}$ and so to $p^{\frac{q-1}{2}} \equiv 1 \pmod{q}$ and to $\left(\frac{p}{q}\right) = 1$. Thus

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

□