A.7 Proof of the Law of Quadratic Reciprocity

Now for the proof of the law of quadratic reciprocity. In the literature we find many different proofs. We adapt one that uses the theory of finite fields and follows ideas by Zolotarev (Nouvelles Annales de Mathematiques 11 (1872), 354–362) and Swan (Pacific J. Math. 12 (1962), 1099–1106).

Lemma 16 *Let p an odd prime, and a and p be coprime. Then the following statements are equivalent:*

(i) *a is a quadratic residue* $\bmod p$.

(ii) *Multiplication by a is an even permutation of $\mathbb{F}_p$.*

Proof. Denote the multiplication by $\mu_a : \mathbb{F}_p \longrightarrow \mathbb{F}_p$, $x \mapsto ax \bmod p$. Then $a \mapsto \mu_a$ is an injective group homomorphism $\mu : \mathbb{F}_p^\times \longrightarrow \mathfrak{S}_p$ to the full permutation group on p elements. If a is primitive, then μ_a has exactly two cycles: $\{0\}$ and $\mathbb{F}_p^\times$. Since p is odd, the sign of μ_a is $\sigma(\mu_a) = (-1)^{p-2} = -1$, hence μ_a is an odd permutation.

Since a generates the group $\mathbb{F}_p^\times$, the two homomorphisms

$$\left(\frac{\bullet}{p}\right) \quad \text{and} \quad \sigma \circ \mu : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}$$

must be identical, and this was the assertion. ◇

As another tool we use the **discriminant** of a polynomial $f = a_n T^n + \cdots + a_0 \in K[T]$. We can compute it in any extension field $L \supseteq K$ that contains all the zeroes $t_1, \ldots, t_n$ of f by the formula

$$D(f) = a_n^{2n-2} \cdot \prod_{1 \le i < j \le n} (t_i - t_j)^2.$$

> The discriminant is invariant under all permutations of the zeroes. Hence it is in K. In our case this will also follow from the explicit computation.

The ususal method of computing the discriminant from the coefficients consists in comparing it with the resultant of f and its derivative f'. For the cyclotomic polynomial $f = T^n - 1$ the computation is outstandingly simple:

Lemma 17 *Assume that* $\operatorname{char} K$ *doesn't divide n. Then the polynomial $f = T^n - 1 \in K[T]$ has discriminant*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot n^n.$$

Proof. Let ζ be a primitive n-th root of unity (in some suitable extension field). Then

$$\begin{aligned}
f &= \prod_{i=0}^{n-1}(T-\zeta^i), \\
D(f) &= \prod_{0\le i<j\le n-1}(\zeta^i-\zeta^j)^2 = (-1)^{\frac{n(n-1)}{2}}\cdot\prod_{i\ne j}(\zeta^i-\zeta^j) \\
&= (-1)^{\frac{n(n-1)}{2}}\cdot\prod_{i=0}^{n-1}\left[\zeta^i\cdot\prod_{k=1}^{n-1}(1-\zeta^k)\right].
\end{aligned}$$

The polynomial

$$g = T^{n-1}+\cdots+1 = \prod_{k=1}^{n-1}(T-\zeta^k)\in K[T]$$

satisfies $g(1)=n$. Hence

$$D(f) = (-1)^{\frac{n(n-1)}{2}}\cdot\prod_{i=0}^{n-1}[\zeta^i\cdot n] = (-1)^{\frac{n(n-1)}{2}}\cdot n^n,$$

as claimed. $\diamond$

Lemma 18 *Let p be an odd prime and n an odd integer, coprime with p. Then the following statements are equivalent:*

(i) *The discriminant of $T^n-1\in\mathbb{F}_p[T]$ is a quadratic residue* mod p.

(ii) $l=(-1)^{(n-1)/2}\cdot n$ *is a quadratic residue* mod p.

Proof. By Lemma 17 the discriminant is $D(f)=l^n$. Let $n=2k+1$. Then $D(f)$ is the product of l with the quadratic residue l^{2k}. $\diamond$

The discriminant of a polynomial $f\in K[T]$ is a square in an extension field $L\supseteq K$ that contains the zeroes of f:

$$D(f)=\Delta(f)^2 \quad\text{with}\quad \Delta(f)=a_n^{n-1}\cdot\prod_{i<j}(t_i-t_j).$$

But $\Delta(f)$ inherits the sign of a permutation of the zeroes. Thus is not invariant, and therefore in general is not contained in K.

Proof of the theorem. Because of Lemma 15 (i) it suffices to prove the quadratic reciprocity law for two different odd primes p and q.

Let $K = \mathbb{F}_p$, ζ be a primitive q-th root of unity, $L = K(\zeta)$, and $f = T^q - 1$. Then $\zeta \mapsto \zeta^p$ defines a permutation μ_p of the roots of unity, and an automorphism of L over K. Thus:

$$\sigma(\mu_p) \cdot \Delta(f) = \prod_{i<j} (\zeta^{pi} - \zeta^{pj}) = \Delta(f)^p.$$

This yields a chain of equivalent statements:

$$(-1)^{\frac{q-1}{2}} \cdot q \text{ quadratic residue } \bmod p \Longleftrightarrow D(f) \text{ quadratic residue } \bmod p$$

$$\Longleftrightarrow \Delta(f) \in \mathbb{F}_p \Longleftrightarrow \Delta(f) = \Delta(f)^p \Longleftrightarrow \sigma(\mu_p) = 1$$

$$\Longleftrightarrow p \text{ quadratic residue } \bmod q.$$

From Proposition 20 (i) we get

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

as claimed. $\diamondsuit$