QUADRATIC RECIPROCITY : A SPECIAL CASE OF ARTIN RECIPROCITY

Atharva Korde

In 1801, C.F.Gauss in his book *Disquisitiones Arithmeticae*, published the first two proofs of the law of quadratic reciprocity, which states that for distinct odd primes p and q,

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

or equivalently

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$$

where $q^* = (-1)^{\frac{q-1}{2}} q$.
Consequently, laws for higher powers like cubic and quartic reciprocity were investigated and proved which led to Hilbert asking if a general reciprocity law exists for algebraic number fields. Hilbert's question, numbered 9th on his list of 23 problems, was answered partially by E.Artin in the 1920s when he proved his reciprocity theorem. In this note, we shall explain Artin's reciprocity theorem and show that quadratic reciprocity follows as a special case.

1 Preliminaries : The Legendre Symbol and Gauss Sums

Definition 1.1. Fix an odd prime p. The Legendre symbol,

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

is defined as follows: For $a \in \mathbb{F}_p^\times$, $(\frac{a}{p})$ is 1 if a is a square in $\mathbb{F}_p^\times$ and -1 otherwise. This definition is extended to the integers by setting $(\frac{n}{p}) := 0$ if $p \mid n$ and $(\frac{n}{p})$ is defined to be the Legendre symbol evaluated at $n \pmod p$ if $p \nmid n$.

Proposition 1.2. (1) $(\frac{\cdot}{p})$ is a group homomorphism.
(2) For $p \nmid n$, $(\frac{n}{p}) \equiv n^{\frac{p-1}{2}} \pmod p$ and hence $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Let ζ_p be a primitive p-th root of unity. The next Gauss sum was computed in class.

Proposition 1.3. For an odd prime p, if

$$g = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^a$$

then $g^2 = p^*$. Thus $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$.

2 Frobenius Elements and the Artin Map

Let K be a number field and L/K a finite Galois extension of degree n with Galois group $G = \mathrm{Gal}(L/K)$. Let $\mathcal{O}_K$, resp. $\mathcal{O}_L$ be the rings of integers in K, resp L. Let $\mathfrak{p}$ be a nonzero prime ideal in $\mathcal{O}_K$ and let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_g$ be the primes in $\mathcal{O}_L$ lying over $\mathfrak{p}$. Recall the following facts:

(1) G acts transitively on the set $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_g\}$ and the decomposition group $D(\mathcal{P}_i/\mathfrak{p})$ is defined to be the stabilizer of $\mathcal{P}_i$.

(2) The ramification indices, $e(\mathcal{P}_1/\mathfrak{p}) = \cdots = e(\mathcal{P}_g/\mathfrak{p}) = e$ are all equal and so are the residue field degrees, $f(\mathcal{P}_1/\mathfrak{p}) = \cdots = f(\mathcal{P}_g/\mathfrak{p}) = f$. In $\mathcal{O}_L$, $\mathfrak{p}$ factorizes as $\mathfrak{p}\mathcal{O}_L = (\mathcal{P}_1 \cdots \mathcal{P}_g)^e$ and $n = efg$.

(3) For each $i = 1, 2, \ldots, g$, we have the natural map

$$\epsilon_i : D(\mathcal{P}_i/\mathfrak{p}) \to \mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_i}/_{\mathcal{O}_K/\mathfrak{p}})$$

$\epsilon_i(\sigma) = \bar{\sigma}$ defined by $\bar{\sigma}(\bar{x}) := \overline{\sigma(x)}$ for all $\bar{x} = x + \mathcal{P}_i \in \mathcal{O}_L/\mathcal{P}_i$. ϵ_i is a surjective group homomorphism with kernel equal to the inertia group $T(\mathcal{P}_i/\mathfrak{p})$ and $|T(\mathcal{P}_i/\mathfrak{p})| = e$.

Now assume $\mathfrak{p}$ is unramified, so that $e = 1$. Then ϵ_i is an isomorphism. For two primes $\mathcal{P}_i, \mathcal{P}_j$ over $\mathfrak{p}$, let $\tau \in G$ be such that $\tau(\mathcal{P}_i) = \mathcal{P}_j$. The decomposition groups $D(\mathcal{P}_i/\mathfrak{p})$ and $D(\mathcal{P}_j/\mathfrak{p})$ are conjugate with the map $c_\tau : D(\mathcal{P}_i/\mathfrak{p}) \to D(\mathcal{P}_j/\mathfrak{p})$, $c_\tau(\sigma) := \tau\sigma\tau^{-1}$ being an isomorphsim. τ also induces the natural map $\bar{\tau} : \mathcal{O}_L/\mathcal{P}_i \to \mathcal{O}_L/\mathcal{P}_j$, $\bar{\tau}(y + \mathcal{P}_i) := \tau(y) + \mathcal{P}_j$. $\bar{\tau}$ is a ring homomorphism which fixes $\mathcal{O}_K/\mathfrak{p}$ pointwise and is infact an isomorphism with inverse given by $\overline{\tau^{-1}}$. Thus, $\bar{\tau}$ induces an isomorphism between $\mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_i}/_{\mathcal{O}_K/\mathfrak{p}})$ and $\mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_j}/_{\mathcal{O}_K/\mathfrak{p}})$ via the map $c_{\bar{\tau}}$ which sends $\bar{\sigma} \in \mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_i}/_{\mathcal{O}_K/\mathfrak{p}})$ to $\bar{\tau}\bar{\sigma}\bar{\tau}^{-1} \in \mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_j}/_{\mathcal{O}_K/\mathfrak{p}})$. We then have a commutative diagram.

Lemma 2.1. The following diagram commutes, where all arrows are isomorphisms.

$$\begin{array}{ccc} D(\mathcal{P}_i/\mathfrak{p}) & \xrightarrow{\epsilon_i} & \mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_i}/_{\mathcal{O}_K/\mathfrak{p}}) \\ \Big\downarrow{\scriptstyle c_\tau} & & \Big\downarrow{\scriptstyle c_{\bar{\tau}}} \\ D(\mathcal{P}_j/\mathfrak{p}) & \xrightarrow[\epsilon_j]{} & \mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_i}/_{\mathcal{O}_K/\mathfrak{p}}) \end{array}$$

Proof. For $\sigma \in D(\mathcal{P}_i/\mathfrak{p})$, we wish to show that $\overline{\tau\sigma\tau^{-1}} = \bar{\tau}\bar{\sigma}\bar{\tau}^{-1}$. But this is obvious as for $\bar{y} = y + \mathcal{P}_j \in \mathcal{O}_L/\mathcal{P}_j$, $\overline{\tau\sigma\tau^{-1}}(\bar{y}) = \tau\sigma\tau^{-1}(y) + \mathcal{P}_j$ and

$$\bar{\tau}\bar{\sigma}\bar{\tau}^{-1}(\bar{y}) = \bar{\tau}\bar{\sigma}\overline{\tau^{-1}}(\bar{y}) = \bar{\tau}\bar{\sigma}(\tau^{-1}(y) + \mathcal{P}_i) = \bar{\tau}(\sigma\tau^{-1}(y) + \mathcal{P}_i) = \tau\sigma\tau^{-1}(y) + \mathcal{P}_j$$

proving the claim. □

$\mathcal{O}_L/\mathcal{P}_i$ and $\mathcal{O}_K/\mathfrak{p}$ are finite fields so let $N\mathfrak{p} := |\mathcal{O}_K/\mathfrak{p}|$. Then the Galois group $\mathrm{Gal}(^{\mathcal{O}_L/\mathcal{P}_i}/_{\mathcal{O}_K/\mathfrak{p}})$ has the Frobenius map $F_i : a \to a^{N\mathfrak{p}}$.

Definition 2.2. The element $\mathrm{Frob}(\mathcal{P}_i/\mathfrak{p})$ is defined to be the pulback of F_i via ϵ_i. In other words, $\mathrm{Frob}(\mathcal{P}_i/\mathfrak{p})$ is the unique element σ in $D(\mathcal{P}_i/\mathfrak{p})$ satisfying $\sigma(x) \equiv x^{N\mathfrak{p}} \pmod{\mathcal{P}_i}$ for all $x \in \mathcal{O}_L$.

Lemma 2.3. $\{\mathrm{Frob}(\mathcal{P}_1/\mathfrak{p}), \mathrm{Frob}(\mathcal{P}_2/\mathfrak{p}) \cdots, \mathrm{Frob}(\mathcal{P}_g/\mathfrak{p})\}$ is a conjugacy class in $G = \mathrm{Gal}(L/K)$. Denote this by $\mathrm{Frob}(\mathfrak{p})$.

Proof. In view of the commutative diagram in lemma 2.1, it suffices to show that F_i and F_j map to each other under the right vertical isomorphism. This is verified by the following computation:

$$\bar{\tau}F_i\overline{\tau^{-1}}(\bar{y}) = \bar{\tau}F_i(\overline{\tau^{-1}(y)}) = \bar{\tau}(\overline{\tau^{-1}(y)})^{N\mathfrak{p}} = \bar{\tau}(\overline{\tau^{-1}(y^{N\mathfrak{p}})}) = \overline{\tau\tau^{-1}(y^{N\mathfrak{p}})} = \bar{y}^{N\mathfrak{p}}$$

and hence $\bar{\tau}F_i\overline{\tau^{-1}} = F_j$. □

From here, suppose L/K is Abelian and let $\mathfrak{p}$ be unramified, as before. By lemma 2.3, the conjugacy class $\mathrm{Frob}(\mathfrak{p})$ is a singleton set, whose only element will again be called $\mathrm{Frob}(\mathfrak{p})$ by minor abuse of notation.

Definition 2.4. The Artin symbol $(\mathfrak{p}, L/K)$ is defined to be $\mathrm{Frob}(\mathfrak{p}) \in \mathrm{Gal}(L/K)$. Concretely, $(\mathfrak{p}, L/K)$ is the unique element $\sigma \in G$ satisfying $\sigma(x) \equiv x^{N\mathfrak{p}} \pmod{\mathcal{P}}$ for some prime (and hence for all primes) $\mathcal{P}$ over $\mathfrak{p}$.

Lemma 2.5. Let $K, L, \mathfrak{p}$ as before and let E be a subextension of L/K (So that E/K is Abelian as well and $\mathfrak{p}$ is unramified in E). Then,

$$\mathrm{res}_E(\mathfrak{p}, L/K) = (\mathfrak{p}, E/K)$$

where res_E is restriction to E.

Proof. Let $\sigma = (\mathfrak{p}, L/K)$. Let $\mathfrak{a}$ be a prime in E over $\mathfrak{p}$ and $\mathcal{P}$ be a prime in L over $\mathfrak{a}$. Then by the definitions, $\sigma(x) \equiv x^{N\mathfrak{p}} \pmod{\mathcal{P}}$ for all $x \in \mathcal{O}_L$. In particular, $\sigma(x) \equiv x^{N\mathfrak{p}} \pmod{\mathcal{P}}$ for all $x \in \mathcal{O}_E$. But for $x \in \mathcal{O}_E$, $\sigma(x)$ and $x^{N\mathfrak{p}} \in \mathcal{O}_E$ as well, hence $\sigma(x) - x^{N\mathfrak{p}} \in \mathcal{P} \cap \mathcal{O}_E = \mathfrak{a}$, proving that $\mathrm{res}_E\sigma = (\mathfrak{p}, E/K)$. □

Let $\mathfrak{c}$ be a cycle in $\mathcal{O}_K$ i.e., $\mathfrak{c}$ is a formal product $\mathfrak{c}_\infty \cdot \mathfrak{c}_0$ where $\mathfrak{c}_0$ is an integral ideal of $\mathcal{O}_K$ and $\mathfrak{c}_\infty$ is a formal product of the real primes, with the exponent of each real prime being 0 or 1. Define $I(\mathfrak{c})$ to be the subgroup of I_K consisting of those fractional ideals coprime to $\mathfrak{c}_0$. It is clear that $I(\mathfrak{c})$ is the free Abelian group generated by the prime ideals not dividing $\mathfrak{c}_0$. If $\mathfrak{c}$ is divisible by the ramified primes, the Artin symbol is defined for all the primes in $I(\mathfrak{c})$. In that case, we get a map

$$\mathrm{Ar}_\mathfrak{c} : I(\mathfrak{c}) \to \mathrm{Gal}(L/K)$$

by extending the definition $\mathfrak{p} \to (\mathfrak{p}, L/K)$ multiplicatively. This is the Artin map corresponding to $\mathfrak{c}$.

There are two subgroups of $I(\mathfrak{c})$ of main interest:
(1) Define $P_{\mathfrak{c}}$ to be the subgroup consisting of principal ideals J such that $J = (\alpha)$ with $\alpha \equiv 1 \pmod{\mathfrak{c}}$. The meaning of $\alpha \equiv 1 \pmod{\mathfrak{c}}$ is $\eta(\alpha) > 0$ for all real primes $\eta \mid \mathfrak{c}_\infty$ and $v_{\mathfrak{q}}(\alpha - 1) \geq v_{\mathfrak{q}}(\mathfrak{c}_0)$ for every $\mathfrak{q} \mid \mathfrak{c}_0$.
(2) Define

$$\mathcal{N}(\mathfrak{c}) := \{N_K^L \beta \mid \beta \text{ an ideal of } \mathcal{O}_L, (\beta, \mathfrak{c}_0 \mathcal{O}_L) = (1)\}$$

This is the subgroup of norms of ideals which are coprime to $\mathfrak{c}_0$. The norm $N_K^L \beta := \prod_{\sigma \in G} \sigma(\beta)$ is an ideal in $\mathcal{O}_K$.

We can now state the main theorem of this note:

Theorem 2.6. (Artin Reciprocity Theorem) Let L/K be an Abelian extension of number fields. Then, for any cycle $\mathfrak{c}$ divisible by the ramified primes, the Artin map $\mathrm{Ar}_{\mathfrak{c}}$ is surjective. Further there exists a cycle $\mathfrak{f}$ in $\mathcal{O}_K$ (called admissible) such that $\mathrm{Ar}_{\mathfrak{f}}$ has kernel equal to $P_{\mathfrak{f}}\mathcal{N}(\mathfrak{f})$, i.e.,

$$I(\mathfrak{f})/P_{\mathfrak{f}}\mathcal{N}(\mathfrak{f}) \cong \mathrm{Gal}(L/K)$$

3 Proof of Quadratic Reciprocity

Lemma 3.1. Let q be an odd prime and $p \neq q$ any other prime. Then $(p, \mathbb{Q}(\zeta_q)/\mathbb{Q})$ is the map $\zeta_q \to \zeta_q^p$.

Proof. Let σ_p be the map on the RHS. Let $L = \mathbb{Q}(\zeta_q)$ and $x \in \mathcal{O}_L$. Write $x = a_0 + a_1\zeta_q + \cdots + a_{q-2}\zeta_q^{q-2}$ and let $\mathcal{P}$ lie over p. Then $p\mathcal{O}_L \subseteq \mathcal{P}$ and modulo $p\mathcal{O}_L$,

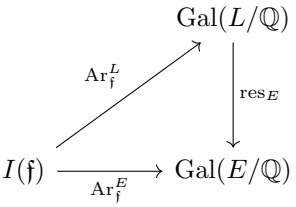
$$x^p = a_0^p + a_1^p\zeta_q^p + \cdots + a_{q-2}\zeta_q^{(q-2)p} = a_0 + a_1\zeta_q^p + \cdots + a_{q-2}\zeta_q^{(q-2)p} = \sigma_p(x)$$

so $\sigma_p(x) \equiv x^p \pmod{\mathcal{P}}$. By the defining property of $(p, \mathbb{Q}(\zeta_q)/\mathbb{Q})$, this symbol must be equal to σ_p. □

Corollary 3.2. The cycle $\mathfrak{f} = q\infty$ is an admissible cycle for $\mathbb{Q}(\zeta_q)/\mathbb{Q}$. (Here ∞ is the usual absolute value on $\mathbb{R}$)

Proof. By Artin reciprocity, $\mathrm{Ar}_{q\infty}$ is surjective and by Lemma 3.1, we see that $\mathrm{Ar}_{q\infty}$ sends a fractional ideal $J = (\frac{a}{b})$ (coprime to $q\infty$) to the map $\sigma_b^{-1}\sigma_a$. So J is in the kernel of the Artin map $\iff \sigma_a = \sigma_b \iff a \equiv b \pmod{q}$. The last congruence holds iff $v_q(\frac{a}{b} - 1) \geq 1$ because $q \nmid b$. Hence $I(q\infty)/P_{q\infty} \cong \mathrm{Gal}(L/\mathbb{Q})$. □

We know that $E = \mathbb{Q}(\sqrt{q^*})$ is a subfield of L (proposition 1.3) and $\mathrm{Gal}(E/\mathbb{Q})$ is identified with $\{\pm 1\}$ by $\phi : \eta \to \frac{\eta(\sqrt{q^*})}{\sqrt{q^*}}$. The only ramified finite prime in E is $q\mathbb{Z}$. Let $\mathrm{Ar}_{\mathfrak{f}}^L$ and $\mathrm{Ar}_{\mathfrak{f}}^E$ be the Artin maps to $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(E/\mathbb{Q})$ respectively. By Artin reciprocity and Lemma 2.4, we have a commutative diagram in which the two maps from $I(\mathfrak{f})$ are surjective.



With the above identification, let $\psi = \phi \circ \mathrm{Ar}_{\mathfrak{f}}^E$.

Lemma 3.3. For p an odd prime, $\psi(p\mathbb{Z}) = \left(\frac{q^*}{p}\right)$.

Proof. Let $(p, E/\mathbb{Q}) = \eta$ and $\mathfrak{a}$ a prime in E above p. By the definitions and Proposition 1.2 (2),

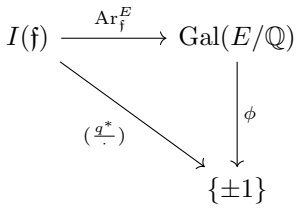
$$\eta(\sqrt{q^*}) \equiv (\sqrt{q^*})^p \equiv (q^*)^{\frac{p-1}{2}}\sqrt{q^*} \equiv \left(\frac{q^*}{p}\right)\sqrt{q^*} \pmod{\mathfrak{a}}$$

as $p\mathcal{O}_E \subseteq \mathfrak{a}$. This implies

$$\sqrt{q^*}\left(\frac{\eta(\sqrt{q^*})}{\sqrt{q^*}} - \left(\frac{q^*}{p}\right)\right) \in \mathfrak{a}$$

but $\sqrt{q^*}$ is not in $\mathfrak{a}$ (If it was, then $(\sqrt{q^*})^2 = q^* \in \mathfrak{a} \implies p, q \in \mathfrak{a}$, a contradiction as then $\mathfrak{a}$ would generate the entire ring). So $\frac{\eta(\sqrt{q^*})}{\sqrt{q^*}} - \left(\frac{q^*}{p}\right) \in \mathfrak{a}$. This number is either ± 2 or 0 and the same argument shows that it can't be ± 2, proving the lemma. □

Lemma 3.3 gives us a formula for ψ and the following commutative diagram:



But putting together the two commutative diagrams, we get $\psi = \phi \circ \mathrm{res}_E \circ \mathrm{Ar}_{\mathfrak{f}}^{L}$. For the final step, observe that $\phi \circ \mathrm{res}_E(\sigma_p) = (\frac{p}{q})$ because σ_p maps to 1 $\iff$ $\sigma_p \in \mathrm{Gal}(L/E) \cong (\mathbb{F}_q^\times)^2$ $\iff$ p is a square in $\mathbb{F}_q^\times$. Hence, $\psi(p\mathbb{Z}) = (\frac{p}{q})$. By computing ψ in two ways we have obtained

$$\psi(p\mathbb{Z}) = \left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$$

completing the proof of quadratic reciprocity.

References

[1] Serge Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1986.

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, John Wiley and Sons, New Jersey, 2011.