Galois Actions and Quadratic Reciprocity

Ignacio Darago

Abstract. In these notes we will give a brief overview of the influence of the action of the Galois group in the prime decomposition, and then we will give a proof of the quadratic reciprocity law, following [Mar77] and [Neu99].

1. Galois Actions

Given a finite extension of number fields $L|k$, one may consider the rings of integers $\mathcal{O}_k \subseteq \mathcal{O}_L$. Then, given a prime ideal $p$ of $\mathcal{O}_k$ it is natural to consider the set of prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ such that $\mathfrak{P} \cap \mathcal{O}_k = p$. Indeed, since $p\mathcal{O}_L$ is an ideal in a Dedekind domain, it must decompose in a unique way into a product of prime ideals $p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. From here on, we will simply write $p$ instead of $p\mathcal{O}_L$ in a slight abuse of notation. One may clearly see that the set of primes in $\mathcal{O}_L$ which lie over $p$ is precisely the set of primes $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ that appear in the prime factorization of $p$. The exponent $e_i$ is called the ramification index and the degree of the field extension $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_k/p]$ is called the inertia degree of $\mathfrak{P}_i$ over $p$. When the extension $L|k$ is separable, the ramification index and the inertia degree are linked by the following theorem.

Theorem 1 (Fundamental Identity). Let $L|k$ be a separable extension of degree $n$. For any prime $p$ of $\mathcal{O}_k$ we have

$$\sum_{i=1}^r e_if_i = n.$$  

Proof. For a proof see [Neu99, p. 46]. □

We say that a prime $p$ is totally split in $L$ if in the decomposition $p = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ we have that $e_i = f_i = 1$ for all $i = 1, \ldots, r$ and $r = [L:k]$. On the other extreme, if $r = 1$ we will say that $p$ is non-split. The fundamental identity thus tells us that if the inertia degree is small, the ideal $p$ is likely to split, that is, factor into different prime ideals.

If $L|k$ is a separable extension, by the primitive element theorem there is some element $\theta \in \mathcal{O}_L$ such that $L = k(\theta)$ (however it may happen that $\mathcal{O}_k[\theta] \subsetneq \mathcal{O}_L$ is properly contained). The decomposition of a prime $p$ of $\mathcal{O}_k$ in $\mathcal{O}_L$ is closely related to the decomposition of the minimal polynomial of $\theta \in \mathcal{O}_k[x]$ over the residue class field $\mathcal{O}_k/p$. However, there is a technical consideration to be taken into account. The conductor of the ring $\mathcal{O}_k[\theta]$ is defined to be the biggest ideal $\mathfrak{f}$ of $\mathcal{O}_L$ which is contained in $\mathcal{O}_k[\theta]$, or in other words

$$\mathfrak{f} = \{a \in \mathcal{O}_L : a\mathcal{O}_L \subseteq \mathcal{O}_k[\theta]\}.$$

Theorem 2 (Dedekind). Let $L|k$ be a separable extension of number fields and $p$ be a prime ideal of $\mathcal{O}_k$ which is relatively prime to the conductor of $\mathcal{O}_k[\theta]$ where $\theta \in \mathcal{O}_L$ is a primitive element of $L|k$. If $f \in \mathcal{O}_k[x]$ is the minimal polynomial of $\theta$ and

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}$$

is the factorization of $f$ into irreducibles $f_i$ over $\mathcal{O}_k/p$. Then $\mathfrak{P}_i = p + (f_i(\theta))$ are the different prime ideals of $\mathcal{O}_L$ lying over $p$. Moreover, the inertia degree of $\mathfrak{P}_i$ is the degree of $f_i(x)$ and we have

$$p = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$
Proof. See [Neu99, p. 48].

A classical problem in number theory is the question of taking square roots modulo a prime \( p \in \mathbb{Z} \). That is, we ask for \( a \in \mathbb{F}_p \) if there exists some \( x \in \mathbb{F}_p \) such that \( x^2 = a \). This is equivalent to finding integer solutions to the diophantine equation \( x^2 + py = a \). We may consider the (multiplicative) group morphism \( \mathbb{F}_p^* \to \mathbb{F}_p^* \), \( x \mapsto x^2 \) and we ask if \( a \in \mathbb{F}_p \) is in the image of this morphism. By noticing that the kernel of that morphism is \( \{ -1, +1 \} \), the image \((\mathbb{F}_p^*)^2\) is a subgroup of index 2. Because \( \mathbb{F}_p^* \) is a cyclic group, one may easily verify that \( a \) is a square modulo \( p \) if and only if \( a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \) and thus we may define the Legendre symbol as \( \left( \frac{a}{p} \right) \) to be \( a^{\frac{p-1}{2}} \pmod{p} \) and it will be 1 if \( a \) is a quadratic residue and \(-1\) if not. The symbol is multiplicative and therefore is the unique character of order 2 in \( \mathbb{F}_p^* \).

Now, let us see that the condition of being a quadratic residue may be translated into terms of the prime decomposition. Consider the extension \( \mathbb{Q}(\sqrt{a})/\mathbb{Q} \). We know that the ring of integers of a quadratic extension is \( \mathbb{Z}[\sqrt{a}] \) if \( a \equiv 2, 3 \pmod{4} \) and \( \mathbb{Z}\left[ \frac{1+\sqrt{a}}{2} \right] \) if \( a \equiv 1 \pmod{4} \) and then it is clear that the conductor of \( \mathbb{Z}[\sqrt{a}] \) is a divisor of 2. The minimal polynomial of \( \sqrt{a} \) is \( x^2 - a \), and reducing modulo \( p \), it remains irreducible if and only if \( a \) is not a quadratic residue, and in the case it is a quadratic residue it splits as \( x^2 - a = (x - b)(x + b) \) for some \( b \in \mathbb{F}_p \). Therefore, Dedekind’s theorem shows that \( \left( \frac{a}{p} \right) = 1 \) if and only if \( (p) \) is totally split in \( \mathbb{Q}(\sqrt{a}) \). We will pursue this link further on in section 2.

When \( L/k \) is a Galois extension, we may understand more thoroughly the problem of prime factorization since we now have an action of the Galois group \( \text{Gal}(L/k) \) on the set of prime factors of \( p \). Indeed, clearly the action of the Galois group \( \text{Gal}(L/k) \) on \( L \) restricts to an action on \( \mathcal{O}_L \) and if \( \mathfrak{P} \) is a prime lying over \( p \) then \( \sigma(\mathfrak{P}) \) is also a prime and we have

\[ \sigma(\mathfrak{P}) \cap \mathcal{O}_k = \sigma(\mathfrak{P} \cap \mathcal{O}_k) = \sigma(p) = p. \]

Let us prove that this action is transitive. Given primes \( \mathfrak{P}_1, \mathfrak{P}_2 \) which lie over \( p \) we shall suppose that \( \mathfrak{P}_2 \neq \sigma(\mathfrak{P}_1) \) for every \( \sigma \in \text{Gal}(L/k) \) and via the Chinese remainder theorem there exists \( x \in \mathcal{O}_L \) such that \( x \equiv 0 \pmod{\mathfrak{P}_2} \) and \( x \equiv 1 \pmod{\sigma(\mathfrak{P}_1)} \) for every \( \sigma \in \text{Gal}(L/k) \). Then, the norm \( N_{L/k}(x) = \prod_{\sigma \in \text{Gal}(L/k)} \sigma(x) \) belongs to \( \mathfrak{P}_2 \cap \mathcal{O}_k = p \) but it does not belong to \( \mathfrak{P}_1 \) because \( \sigma(x) \notin \mathfrak{P}_1 \) for every \( \sigma \in \text{Gal}(L/k) \), which yields a contradiction.

Because of the transitivity of the Galois action, given a prime \( \mathfrak{P} \) lying over \( p \) we obtain every prime ideal lying over \( p \) simply by considering the orbit \( \{ \sigma(\mathfrak{P}) : \sigma \in \text{Gal}(L/k) \} \). Thus, the stabilizer \( G_{\mathfrak{P}} = \{ \sigma \in \text{Gal}(L/k) : \sigma(\mathfrak{P}) = \mathfrak{P} \} \) encodes the number of different prime ideals into which a prime decomposes, for the orbit-stabilizer theorem tells us that the orbit has \( (\text{Gal}(L/k) : G_{\mathfrak{P}}) \) elements. We will call \( G_{\mathfrak{P}} \) the decomposition group of \( \mathfrak{P} \) over \( K \). By the previous discussion, it is clear that \( G_{\mathfrak{P}} = 1 \) if and only if \( p \) is totally split and \( G_{\mathfrak{P}} = \text{Gal}(L/k) \) if and only if \( p \) is nonsplit.

Also, the transitivity of the Galois action forces the ramification index and inertia degree to be independent of the prime in the factorization and will be denoted \( e \) and \( f \) respectively. Indeed, if we write \( p = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \) then considering for each \( i \) some \( \sigma_i \in \text{Gal}(L/k) \) such that \( \sigma_i(\mathfrak{P}_1) = \mathfrak{P}_i \), we have an isomorphism \( \mathcal{O}_L/\mathfrak{P}_1 \isom \mathcal{O}_L/\mathfrak{P}_i \) via \( a \mod \mathfrak{P}_1 \mapsto \sigma_i(a) \mod \mathfrak{P}_i \) and thus the inertia degrees \( f_i = f_1 \) must be equal. Also, applying \( \sigma \) gives us a permutation of the prime factors

\[ p = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r} = \mathfrak{P}_1^{e_{\tau(1)}} \cdots \mathfrak{P}_r^{e_{\tau(r)}} \]

where \( \tau \) is the permutation associated with the action of \( \sigma^{-1} \) on the set \( \{ \mathfrak{P}_1, \ldots, \mathfrak{P}_r \} \). Therefore, \( e_{\tau(i)} = e_i \) for every \( i \) and the transitivity tells us that it must be independent of \( i \).

Consider the fixed field of the decomposition group, that is, \( \mathcal{Z}_{\mathfrak{P}} = \{ x \in L : \sigma(x) = x \ \forall \sigma \in G_{\mathfrak{P}} \} \). This field will be called the decomposition field of \( \mathfrak{P} \) over \( K \). Then, the prime decomposition may be
understood in two steps, first by decomposing in the extension \( Z_q \mid k \) and second by decomposing in the extension \( L \mid Z_q \).

**Proposition 3.** Let \( \mathfrak{P}_Z = \mathfrak{P} \cap Z_q \) be the prime ideal of \( Z_q \) below \( \mathfrak{P} \). Then we have:

1. \( \mathfrak{P}_Z \) is nonsplit in \( L \), that is \( \mathfrak{P} \) is the only prime ideal of \( L \) above \( \mathfrak{P}_Z \).
2. \( \mathfrak{P} \) over \( Z_q \) has ramification index \( e \) and inertia degree \( f \).
3. The ramification index and the inertia degree of \( \mathfrak{P}_Z \) over \( k \) both equal 1.

**Proof.** The main theorem of Galois theory tells us that \( \text{Gal}(L \mid Z_q) = G_q \) and therefore the prime ideals above \( \mathfrak{P}_Z \) are the \( \sigma(\mathfrak{P}_Z) \) for \( \sigma \in G_q \), and they are all equal to \( \mathfrak{P} \).

In the Galois case, the fundamental identity reads \( n = efr \) where \( n = [L : k] = \sharp \text{Gal}(L \mid k) \) and \( r = (\text{Gal}(L \mid k) : G_q) \). Therefore it is clear that \( \sharp \text{Gal}(L \mid Z_q) = \sharp G_q = ef \). Suppose that \( e', e'' \) and \( f', f'' \) are the ramification indices and inertia degrees of \( \mathfrak{P} \) over \( Z_q \) and of \( \mathfrak{P}_Z \) over \( k \) respectively. It is then clear that \( e = e'e'' \) and \( f = f'f'' \) and the fundamental identity for \( \mathfrak{P}_Z \) in \( L \) tells us that \( \sharp \text{Gal}(L \mid Z_q) = e'f' = ef \). Then, \( e''f'' = 1 \) and then \( e'' \) is always divisible by \( d \) as desired.

### 2. Quadratic Reciprocity

In this section we will provide a proof of the law of quadratic reciprocity by understanding first the law of decomposition in cyclotomic fields.

Recall that if \( p \) is a prime number and \( \zeta_p \) is a primitive \( p \)-th root of unity, then \( \mathbb{Q}(\zeta_p) \mid \mathbb{Q} \) is called the \( p \)-th cyclotomic extension. One may prove that the ring of integers of the cyclotomic extension is \( \mathbb{Z}[\zeta_p] \). Also, recall that \( \text{Gal}(\mathbb{Q}(\zeta_p) \mid \mathbb{Q}) = \mathbb{F}_p^\times \) and so, by the main theorem of Galois theory, there exists for each \( d \mid p \) a unique subextension \( F_d \) of \( \mathbb{Q}(\zeta_p) \mid \mathbb{Q} \) of degree \( d \) over \( \mathbb{Q} \) and moreover \( d_1 \mid d_2 \) if and only if \( F_{d_1} \subseteq F_{d_2} \). The following theorem extends the relationship between being a power modulo \( p \) and the prime factorization in certain extensions, as we have outlined in section 1.

**Theorem 4.** Let \( p, q \) be odd primes and suppose that \( d \mid p - 1 \). Then \( q \) is a \( d \)-th power modulo \( p \) if and only if \( q \) totally splits in \( F_d \) the only subextension of \( \mathbb{Q}(\zeta_p) \mid \mathbb{Q} \) of degree \( d \).

**Proof.** Suppose that the order of \( q \) in the multiplicative group \( \mathbb{F}_p^\times \) is \( \frac{p-1}{d} \). We claim that \( q \) is always totally split in \( F_d \). Indeed, we must only prove, by virtue of Dedekind’s theorem, that \( \Phi_p(x) \) factors as the product of \( r \) irreducible polynomials over \( \mathbb{F}_q \). This may be done by considering \( \omega \) a primitive \( p \)-th root of unity in \( \overline{\mathbb{F}_q} \) and considering the polynomial \( (x-\omega)(x-\omega^q)\cdots(x-\omega^{q^{\frac{p-1}{r}}-1}) \) and all of the \( r \) factors will be of this form.

Take \( q \) a prime in \( \mathbb{Z}[\zeta_p] \) lying over \( q \) and consider the decomposition field \( Z_q \). Notice that \( [Z_q : \mathbb{Q}] = \sharp \text{Gal}(\mathbb{Q}(\zeta_p) \mid \mathbb{Q}) : G_q \) is the number of elements in the orbit of \( q \) in the Galois action, that is, the number of primes over \( q \) which is precisely \( r \). Then, \( Z_q \) is the only degree \( r \) subextension of \( \mathbb{Q}(\zeta_p) \mid \mathbb{Q} \).

Since \( \mathbb{F}_p^\times \) is cyclic, it follows that \( q \) is a \( d \)-th power modulo \( p \) if and only if \( d \mid r \), which in turn happens if and only if \( F_d \subseteq F_r \). Therefore, if \( q \) is a \( d \)-th power modulo \( p \) we have that \( F_d \subseteq F_r \) and as \( q \) is totally split over \( F_r \), the same holds for \( F_d \) as the inertia degree of \( q \cap Z_q \) over \( Q \) is 1 by Proposition 3. Conversely, if \( q \) is totally split over \( F_d \) write \( q = p_1 \cdots p_d \) with \( p_i \) primes in \( F_d \). Because of the transitivity of the Galois action there is \( \sigma \) such that \( \sigma(p_1) = p_1 \) and extending \( \sigma \in \text{Gal}(F_d \mid \mathbb{Q}) \) to \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta_p) \mid \mathbb{Q}) \) we obtain a bijection of the primes above \( p_1 \) and the primes above \( p_1 \). This implies that the number of prime ideals \( r \) in the decomposition of \( q \) over \( \mathbb{Q}(\zeta_p) \mid \mathbb{Q} \) is divisible by \( d \) and we are done.
Finally, in order to prove the quadratic reciprocity law we will characterize the only quadratic subextension of $\mathbb{Q}(\xi_p)|\mathbb{Q}$. The Gauss sum will be the key for understanding this. It is defined as
\[ \tau = \sum_{a \in \mathbb{F}_p} \left( \frac{a}{p} \right) \xi_p^a. \]
It is clear that $\tau \in \mathbb{Q}(\xi_p)$ and $\tau \notin \mathbb{Q}$, so if we prove that $\tau^2 \in \mathbb{Q}$ the only subextension of $\mathbb{Q}(\xi_p)|\mathbb{Q}$ of degree 2 will be $\mathbb{Q}(\tau)$. Moreover, it holds that $\tau^2 = \left( \frac{-1}{p} \right) p = (-1)^{p-1} \frac{p^*}{p} = p^*$. For a proof of this, see [IR90].

The previous discussion allows us to reformulate Theorem 4 for the case $d = 2$: given odd primes $p, q$ then $q$ is a quadratic residue modulo $p$ if and only if $q$ totally splits in $\mathbb{Q}(\sqrt{p^*})$. We are in conditions to prove:

**Theorem 5** (Gauss reciprocity law). Let $p, q$ be odd distinct primes. Then
\[ \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} + \frac{q-1}{2}}. \]

**Proof.** We know from section 1 that $\left( \frac{p^*}{q} \right) = 1$ if and only if $q$ is totally split in $\mathbb{Q}(\sqrt{p^*})$, and by the previous discussion this is equivalent to $\left( \frac{q}{p} \right) = 1$. Therefore, we have proved that $\left( \frac{p^*}{q} \right) = \left( \frac{q}{p} \right)$ and a simple manipulation of terms gives us the desired result.

**REFERENCES**

