Reciprocity Law

Diaa Al Saleh

July 17, 2026

One of the central questions in algebraic number theory is understanding how prime numbers factor in extensions of number fields. In Galois extensions, the splitting behavior of a prime is encoded by its Frobenius element, and in the special case of abelian extensions of $\mathbb{Q}$, this information can be described using one-dimensional representations of the Galois group.

The goal of this paper is to explain how the splitting of prime ideals in finite abelian Galois extensions of $\mathbb{Q}$ can be understood through Dirichlet characters. These characters arise naturally as one-dimensional representations of certain finite abelian groups and provide an explicit bridge between arithmetic properties of primes and the structure of abelian extensions. We begin by introducing Dirichlet characters.

Definition 1. A *Dirichlet character modulo q* is a character of the abelian group $(\mathbb{Z}/q\mathbb{Z})^\times$, i.e a multiplcative homomorphism

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$$

We say that q is the *modulus* of χ.

Definition 2. The minimum modulus of the Dirichlet character is called the conductor and we denote it by f_χ. A Dirichlet character with modulus f_χ is called *primitive*

Example 1.

1. Define $\chi : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}^\times$ by $\chi(1) = 1$, $\chi(2) = i$, $\chi(3) = -i$, $\chi(4) = -1$.
2. If p is an odd prime then the quadratic character $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ is the Legendre symbol mod p.
3. Let $(\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$ be given by $\chi(1) = 1, \chi(5) = -1, \chi(7) = 1, \chi(11) = -1$. Observe that $\chi(a + 3k) = \chi(a)$ so χ is induced by the character $\psi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$, where $\psi(1) = 1, \psi(2) = -1$. ψ is primitive so $f_\chi = 3$.

Now let's take an abelian Galois extension $K/\mathbb{Q}$, we want to study $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$, that is the 1-dimensional Galois representations. We will see that χ will play a central role in describing these represetations. Recall that if $K = \mathbb{Q}(\zeta_n)$ then $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ so in this case the 1-dim dimensional Galois representations can be realized as Dirichlet characters.

Theorem 1. (Kronecker Weber). Every Abelian extension over $\mathbb{Q}$ lies in a cyclotomic extension.

Now suppose $L/\mathbb{Q}$ is abelian with conductor n then by Kronecker-Weber we get a surjective homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(L/\mathbb{Q})$$

Now suppose p is a prime with $p \nmid n$ so that $L/\mathbb{Q}$ is unramified above p. From algebraic number theory we know that we have a decomposition group $G_p \subseteq \mathrm{Gal}(L/\mathbb{Q})$ and since there is no ramification G_p is generated by Frob_p. Now we can take the map $p \mapsto \mathrm{Frob}_p$ and extend it to a homomorphism from I_m to $\mathrm{Gal}(L/\mathbb{Q})$ where I_m is the subgroup of $\mathbb{Q}*$ generated by all primes not dividing n. The map $\theta_{L/\mathbb{Q}} : I_n \to \mathrm{Gal}(L/\mathbb{Q})$ is called the *Artin* map.

Really the main potato of this is that θ factors through the map $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$ so in the end we obtain the following diagram:

$$\begin{array}{ccc} I_n & \xrightarrow{\quad\theta\quad} & \mathrm{Gal}(L/\mathbb{Q}) \\ \downarrow & & \downarrow \rho \\ (\mathbb{Z}/n\mathbb{Z})^\times & \xrightarrow[\quad\chi\quad]{} & \mathbb{C}^\times \end{array}$$

Finally we get the reciprocity law $\boxed{\chi(p) = \rho(\mathrm{Frob}_p)}$.

Now we look at some applications of this result. As a habit of me I like to start any examples with my favorite ring i.e $\mathbb{Z}[i]$.

Example 2. Let $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$ given by $\chi(1) = 1, \chi(3) = -1$. Now the reciprocity law tells us that when $p \equiv 1 \pmod 4$ then $\chi(p) = \rho(\mathrm{Frob}_p) = 1$ so it is split in this case. Similarly for $p \equiv 3 \pmod 4$ we get that it is inert.

Theorem 2. Let $K = \mathbb{Q}(\zeta_n)$. The Artin map induces an isomorphism

$$I_n/P_n^+ \cong \mathrm{Gal}(K/\mathbb{Q})$$

where

$$P_n^+ = \{(a/b) \in I_n | a \equiv b \pmod m, a/b > 0\}$$

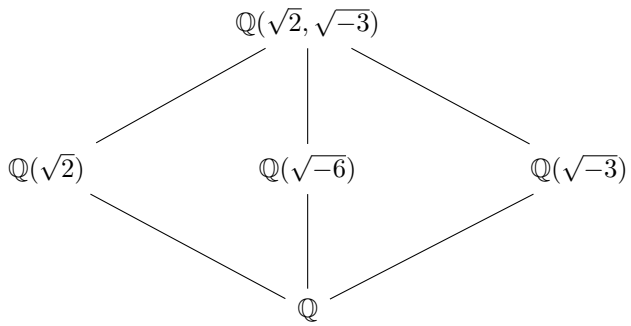
Corollary 1. Let K be as above and let E be a subfield of K. Then there exists a group H with $P_n^+ \leq H \leq I_n$ such that the Artin map induces an isomorphism

$$I_n/H \cong \mathrm{Gal}(E/\mathbb{Q})$$

Now we can give a fun example which makes use of the theorems above. The above example gives an answer to when $x^2 + y^2 = p$ has solutions. We try now to do it for $x^2 + 6y^2 = p$

Proposition 1. Let p be a prime with $p \nmid 6$. The equation $x^2 + 6y^2 = p$ has solutions if and only if $p \equiv 1$ or $p \equiv 7 \pmod{24}$

Proof. The natural field to consider is $K = \mathbb{Q}(\sqrt{-6})$. This way the answer will lie in the norm equation since a solution produces a principle ideal $(x + y\sqrt{-6})$ with norm p. However, the ideal class group is not trivial. Let L be the maximal unramified abelian extension of K. Consider the following diagram:



By discriminant considerations, $\mathbb{Q}(\sqrt{2},\sqrt{-3})$ is ramified at $p = 2, 3$. Now for $p = 2$, it ramifies with index 2 in $\mathbb{Q}(\sqrt{-6})$ and $\mathbb{Q}(\sqrt{2})$ but it is inert with index 2 in $\mathbb{Q}(\sqrt{-3})$ so we must have $e \geq 2, f \geq 2$ in $\mathbb{Q}(\sqrt{2},\sqrt{-3})$. Since this field is Galois, $efg = 4$ forces $e = 2$ in $\mathbb{Q}(\sqrt{2},\sqrt{-3})$ Similarly for $p = 3$ we get that the ramification index is 2 so $\mathbb{Q}(\sqrt{2},\sqrt{-3})$ is unramified over K. By class field theory we know that $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$ so in fact we have $L = \mathbb{Q}(\sqrt{2},\sqrt{-3})$.

The kernel of the Artin map $\theta_{L/K}$ is the group of principal ideals in K. This means a prime ideal $\mathfrak{p}$ lying over p is principal iff $\theta_{L/K}(\mathfrak{p}) = 1$ and this is true iff $\mathfrak{p}$ splits completely in L. Notice that $L/\mathbb{Q}$ is Galois so the condition that p splits completely in K and the primes lying above p splits completely in L is equivalent to saying that p splits completely in L by the tower law. The problem now just reduces to finding which primes in $\mathbb{Q}$ split completely in L.

Note that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ so it is in fact a cyclotomic field and $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$ so L is in their compositum that is $\mathbb{Q}(\zeta_{24})$. and in fact the subgroup corresponding to it is $\{1, 7\}$ (you can check here that at $p = 7$ the primes above p split completely). $\square$