From Quadratic Reciprocity, to Artin's Reciprocity, to Langland's Reciprocity

This article assumes the reader has knowledge of some algebraic number theory, namely knowledge of concepts such as quadratic reciprocity, Frobenius automorphism, Galois groups, and similar concepts. The Kronecker-Weber Theorem will be mentioned in this article, so for the reader who is unaware of this result, it states that all abelian extensions of $\mathbb{Q}$ can be embedded in a Cyclotomic extension of $\mathbb{Q}$, namely that all abelian extensions of $\mathbb{Q}$ are Cyclotomic of $\mathbb{Q}$.

When looking for solutions or irreducibility of integer polynomials, it is natural to want to find as much information as possible about the polynomial. One strategy is to find the solutions of a polynomial mod primes, and trying to piece together this information. As Galois groups hold information about the relation between the roots of polynomials, it would be nice if the "local" information provided by solving after modding can be linked to the "global" information provided by the Galois group. The Artin reciprocity can be interpreted as one part in achieving this result.

To demonstrate this, recall that p is a quadratic residue mod q ($n^2 \equiv p \mod q$) if and only if $\left(\frac{p}{q}\right) = 1$ where $\left(\frac{p}{q}\right)$ is the Legendre symbol. This symbol satisfies the following equation:

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

This is known as the *Quadratic Reciprocity law*. Notice that we can consider the image of the Legendre symbol to be isomorphic to $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))$ (they are both $\cong \mathbb{Z}/2\mathbb{Z}$). It would be more interesting if there is a function from the primes of $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ to the Galois group that commutes with the Legendre symbol:

$$\begin{array}{ccc} \{\text{primes of } \mathbb{Q}(\sqrt{q})/\mathbb{Q}\} & \xrightarrow{\left(\frac{p}{q}\right)} & \{-1,1\} \\ \downarrow \text{id} & & \downarrow \cong \\ \{\text{primes of } \mathbb{Q}(\sqrt{q})/\mathbb{Q}\} & \xrightarrow{?} & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q})) \end{array}$$

It would then be not too much a stretch to ask if we can replace the domain of these functions with the collection of all ideals of $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$:

$$\begin{array}{ccc} \mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} & \xrightarrow{\prod_p \left(\frac{p}{q}\right)} & \{-1,1\} \\ \downarrow \text{id} & & \downarrow \cong \\ \mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} & \xrightarrow{?} & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q})) \end{array}$$

In fact, there is a connection: as $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))$ is abelian, then the Frobenius automorphism (see EYNTKA Algebra) is exactly the map we can place at position "?", where the original condition of "$\left(\frac{p}{q}\right) = 1$ if and only if there is a quadratic residue" becomes "if and only if p splits completely":

$$\begin{array}{ccc} \mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} & \xrightarrow{\prod_p \left(\frac{p}{q}\right)} & \{-1,1\} \\ \downarrow = & & \downarrow \cong \\ \mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} & \xrightarrow{\mathrm{Frob}_{\mathfrak{p}}} & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q})) \end{array}$$

As nice as an observation this is, as we are working with such small sets, the question becomes whether this is an accident or a pattern; can $\mathrm{Gal}_{\mathbb{Q}}(K)$ (or even $\mathrm{Gal}_K(L)$) be replaced with another abelian Galois

group, where the abelian condition is necessary for the Frobenius automorphism to be well-defined, and we can find a corresponding "Legendre symbol" and a group in the codomain that would make the above diagram commute? Does this generalize when looking at cubic reciprocity, biquadratic reciprocity, and so forth (with the appropriate replacement of the Legendre symbol and its image)? Phrased differently, for different polynomial equations, when taking the mod by different primes and finding the relations between primes given by the polynomial, are these relations related to the Galois group? This was a major endeavour in the 20th century, notably Hilbert's 23rd problem was:

> Find a proof of the most general reciprocity law for an arbitrary number field

As it turns out, such a law exists! The group that replaces $\{-1, 1\}$ will be the *ideal class group* $\mathrm{Cl}(K)$ (or more specifically, the *ray class group*)[1], and the Legendre symbol shall be generalized to the Artin symbol! The result is called *Artin Reciprocity*. Exactly how this replacement happens is the goal of a first course in class field theory, and so hopefully this is enough to convince the reader it is a topic worth learning.

One interesting result from this generalization is that most groups will not be isomorphic to the class group, but the *quotient* of the class group. The reader may rightfully wonder if there is a maximal extension L/K where $\mathrm{Gal}_K(L)$ is isomorphic to the class group. As it will again turn out, the answer is yes and results from a generalization of Kronecker Weber's theorem! Thus, the commutative diagram presented above would be extended to a commutative diagram:

$$\begin{array}{ccc} \{\text{primes of } K\} & \longrightarrow & \mathrm{Gal}_K(L) \\ \Big| \text{id} & & \Big| \cong \\ \{\text{primes of } K\} & \longrightarrow & \mathrm{Cl}(K)/T_K \end{array}$$

and if $L = K_H$ is an appropriate "maximal" abelian field extension, then:

$$\mathrm{Cl}(K) \cong \mathrm{Gal}_K(K_H)$$

This incredible unification of the properties of primes and the polynomial relationships that can be put to associate them can be thought of as a crowning achievement of number theory in the 20th century.

One important caveat that must be mentioned is that this reciprocity works with *abelian* Galois groups. Intuitively, the reader can think of this as a consequence of the ideal group being abelian, having its multiplication structure on principal ideal mirror that of the multiplication structure from the group of units of a field. Is there an interesting suitable replacement or generalization of the ideal group or class groups that will allow for the reciprocity to generalize to all Galois groups? Such questions are the beginnings of Langlands' program.

Towards Langland's Reciprocity

In the process of developing class field theory, it will come out that there are two approaches to the problem: one done by focusing on primes along with "infinite primes" (i.e. places) which leads to the ray class group. The other focuses on *local fields* and putting together the information of local fields to find global results. This approach is preferable to the approach given by Ray class groups as it allows us to consider the behaviour of all local fields, and hence all primes, at once. Considering the behaviour of all the primes at once can be thought of as the starting point for looking into objects should replace the class groups in the generalization of Artin's Reciprocity.

An incredible observation in the 20th century was that we can capture the information given by primes by a generating function, and these shall be the appropriate replacement. To illuminate a bit with a special case, take a subset of polynomials $p(x, y)$ that are elliptic curves (polynomials of the form

[1]The ray class group is similar to the ideal class group but it ignores ramifying primes; If we considered the ideal class group, we get cases where the ideal class group is trivial while the Galois group is non-trivial, ex. consider $x^4 + 1$

$y^2 = x^3 + ax + b$). We can take the solution of such a polynomial mod primes, count the number of solutions, normalize them[2], and make them the coefficients of a generating function. For example, for the elliptic curve $y^2 = x^3 - x$ is:

$$f(q) = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37} + \cdots$$

This generating function will exhibit incredible symmetries, namely it is invariant under certain group actions[3]. Generating functions that exhibit these nice properties are called *modular form*. These are good candidates for replacing the class group. Furthermore, instead of working directly with non-abelian groups, we shall work with Galois representations. One-dimensional representations shall correspond to the Galois group and recover the the Artin Reciprocity.

One of the great achievements of the end of the 20th century is that this has been solved for two-dimensional representations! These correspond to elliptic curves, and it was shown that all elliptic curves correspond to a modular form, that is, all elliptic curves are *modular*[4]. One consequence of this is that Fermat's last theorem was shown to be true: that for $n \geq 3$ the equation $x^n + y^n = z^n$ has no integer solutions. This is because this statement can be shown to be equivalent to the following:

If $a, b, c \in \mathbb{N}$ is a non-trivial solution to $a^p + b^p = c^p$ for odd prime, then

$$y^2 = x(x - a^p)(x + b^p)$$

will be an elliptic curve without a modular form

However, It was shown that all elliptic curves have a modular form, and hence the statement is indeed false!

The hunt is now on for pushing further the Langlands Correspondence! Recently, the *Geometric Langlands correspondence* was proven, where instead of working with number fields, the mathematicians worked over function fields (which have very similar properties to number fields). There is still a lot of work for the higher-dimensional versions of Langlands' correspondence, and though daunting to understand, it is fascinating to see it come together!

[2]In particular, take $p - \#\,\mathrm{Sol}$ to normalize the solution-set so that these hover around 0

[3]This symmetry can be seen by writing this function in terms of eta functions, something that would be covered in great depth while studying modular forms

[4]Weil in his seminal paper showed that all semi-stable elliptic curves are modular, and this was generalized to work for all elliptic curves over a period of a few years