Class Field Theory:Some Classical Reciprocity Laws

Yujia Yin

Abstract

We revisit some of the classical reciprocity laws from the point of view of class field theory.

Contents

1 Primes of the Forms $X^2 + Y^2$

Recommended reference: Chapter VI of [3] for the historical perspective.

We study the following classical question solved by Fermat:“Which prime numbers are sums of two squares?”

Clearly, 2 is a sum of squares. For odd primes, the answer is given in terms of congruence information:

Theorem 1.1 (Fermat)**.** *An odd prime number p is a sum of square iff $p \equiv 1(mod\ 4)$.*

This result has many proofs, some are more sophisticated than others. We present a proof which translates the question into a question about the splittings of rational primes in $\mathbb{Q}(i)$. For more proofs, see [1].

Proof of Theorem 1.1.
Equivalence to the splitting of an integral monic:

Consider the integral monic $f(x) = x^2 + 1$, whose splitting field is $\mathbb{Q}(i)$. If an odd prime p is a sum of squares, then the mod-p reduction $\bar{f}$ of f necessarily has a solution in $\mathbb{F}_p$. In other words, $\bar{f}$ splits in $\mathbb{F}_p[x]$ if p is a sum of squares.

Conversely, if $\bar{f}$ splits in $\mathbb{F}_p[x]$, then we know p splits into product of two primes in $\mathbb{Z}[i]$, which we denote by α and β. Taking norm of $p\mathbb{Z}[i]$, we see $p^2 = N(\alpha)N(\beta)$. Moreover, $N(\alpha) = N(\beta)$ because the extension is Galois. We can then conclude that p is a sum of squares since both $N(\alpha)$ and $N(\beta)$ are sums of two squares and equal p.

Therefore, p is a sum of squares iff p splits in $\mathbb{Q}(i)$ iff $\bar{f}$ has a root in $\mathbb{F}_p$.

Characterization of splitting of $\bar{f}$ in terms of arithmetic of $\mathbb{Q}$:

Now, $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$. It follows that α is a root of $\bar{f}$ iff it is an element of order 4 in $\mathbb{F}_p^\times$. Such element exists iff $p \equiv 1(\text{mod } 4)$. This completes the proof.

□

2 Artin Reciprocity for $\mathbb{Q}(i)/\mathbb{Q}$

We are now in the position to compute the Artin symbol $(, \mathbb{Q}(i)/\mathbb{Q})$.

First of all, recall the only two prime places ramified in $\mathbb{Q}(i)$ are ∞ and (2). Therefore, the map $(, \mathbb{Q}(i)/\mathbb{Q})$ goes from $\mathcal{I}_{\mathbb{Q},\infty(2)}$ to $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

By arguments similar to those of example 3.3 and example 3.4 in the first note and theorem 1.1 in section 1, we see the prime ideals generated by primes congruent to 1 modulo 4 go to the identity, while the prime ideals generated by primes congruent to 3 modulo 4 go to conjugation. Hence, the kernel is generated by (p) where p is a prime congruent to 1 modulo 4 and $(p)^2$ where p is a prime congruent to 3 modulo 4.

The conductor $\mathfrak{f}(\mathbb{Q}(i)/\mathbb{Q})$ is not $\infty(2)$ but $\infty(2)^2$. This is not hard to verify. Since the support of $\mathfrak{f}$ is necessarily $\infty(2)$, it is necessarily of the form $\infty(2)^k$ for some positive intger k. k can't be 1 because $\mathcal{I}_{\mathbb{Q},\infty(2)} = \mathcal{P}_{\mathbb{Q},\infty(2)}$ and the extension is non-trivial. For any k above 2, $\mathcal{P}_{\mathbb{Q},\infty(2)^2} N_{\mathbb{Q}(i)/\mathbb{Q}}(\infty(2)^2) = \mathcal{P}_{\mathbb{Q},\infty(2)^k} N_{\mathbb{Q}(i)/\mathbb{Q}}(\infty(2)^k)$. Therefore $\mathfrak{f} = \infty(2)^2$.

The above analysis shows $\frac{\mathcal{I}_{\mathbb{Q},\infty(2)^2}}{\mathcal{P}_{\mathbb{Q},\infty(2)^2} N_{\mathbb{Q}(i)/\mathbb{Q}}(\infty(2)^2)} \overset{(,\mathbb{Q}(i)/\mathbb{Q})}{\cong} \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, confirming Artin reciprocity.

3 Quadratic Reciprocity

We now turn to the famous quadratic reciprocity law.

Recall the Legendre symbol $(\frac{a}{p})$ for a prime p is defined to be the mod-p image of $a^{\frac{p-1}{2}}$ into the residue system $\{-\frac{p-1}{2}, ..., 0, ..., \frac{p-1}{2}\}$, and has only three possibilities:

$$(\tfrac{a}{p}) = \begin{cases} -1 & \text{if } x^2 \equiv a \text{ does not have solutions in } \mathbb{Z}, \\ 0 & \text{if } p|a, \\ 1 & \text{if } x^2 \equiv a \text{ has a solution in } \mathbb{Z}. \end{cases}$$

(Verify $(\frac{-}{p})$ is a Dirichlet character.)

The result in the previous section is now a tautology:$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

For odd primes p and q, we have the quadratic reciprocity law for pairs of odd primes:

Theorem 3.1 (The Quadratic Reciprocity Law for Pairs of Odd Primes)**.** *If p and q are distinct odd primes, then $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

The reciprocity is between the splitting of p in $\mathbb{Q}(\sqrt{q})$ and the splitting of q in $\mathbb{Q}(\sqrt{p})$, which is related by the arithmetic of $\mathbb{Q}$.

The quadratic residue and non-residue of the exceptional prime 2 modulo an odd prime p can also be characterized in terms of arithmetic of $\mathbb{Q}$:

Theorem 3.2 (Quadratic Reciprocity for 2)**.** *For an odd prime p,$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.*

This can be interpreted as a splitting law of odd primes in $\mathbb{Q}(\sqrt{2})$ in terms of mod-8 congruence information.

The strategy is to embed the quadratic extension $L/\mathbb{Q}$ of interest in some cyclotomic field $\mathbb{Q}(\zeta_n)$, whose Galois group and ramifications are known, and then determine the conditions under which Frob_p lies in the fix group of L, in which case p splits in L.

Proof of Theorem 3.1.

Consider the following tower of Galois extensions:

$$\begin{tikzcd} \mathbb{Q}(\zeta_q) \\ \mathbb{Q}(\sqrt{q^*}) \arrow[u] \\ \mathbb{Q} \arrow[u] \end{tikzcd},$$

where $q^* = (-1)^{\frac{q-1}{2}}q$.

$\mathbb{Q}_{\zeta_q}/\mathbb{Q}$ is cyclic with $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong \mathbb{F}_q^{\times}$. Any element is determined by extending $\zeta_q \to \zeta_q^k$, where $k \in \{1, ..., p-1\}$.

By Galois correspondence, $\mathbb{Q}(\sqrt{q^*})$ is the unique quadratic extension of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_q)$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{q^*}))$ consists of those elements in $\mathbb{F}_q^\times$ which are squares.

Since Frob_p acts on ζ_q by sending it to ζ_q^p, we see $(\frac{p}{q}) = 1 \iff p$ splits in $\mathbb{Q}(\sqrt{q^*})$.

On the other hand, p splits in $\mathbb{Q}(\sqrt{q^*}) \iff$ the mod-p reduction of $x^2 - q^*$ splits in $\mathbb{F}_p \iff (\frac{q^*}{p}) = 1$.

Therefore, $(\frac{q^*}{p}) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}(\frac{q}{p}) = (\frac{p}{q}) \iff (\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Remark 3.1. *Notice how the reciprocity about two rational primes was deduced from the reciprocity law of a single abelian extension in this proof.*

$(\frac{2}{p})$ has a different pattern because we will embed $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ into the cyclotomic field $\mathbb{Q}(\zeta_8)$ which is not a cyclic extension of $\mathbb{Q}$.

Proof of Theorem 3.2.

Consider this time the tower

$$\begin{tikzcd} \mathbb{Q}(\zeta_8) \\ \mathbb{Q}(\sqrt{2}) \arrow[u] \\ \mathbb{Q} \arrow[u] \end{tikzcd}$$

The only two elements fixing $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are given by $\zeta_8 \to \zeta_8^1$(the identity) and $\zeta_8 \to \zeta_8^7$.

Now, $1^2 - 1 \equiv 7^2 - 1 \equiv 0(\mathrm{mod} 16)$. Therefore, by arguments similar to the proof of Theorem 3.1, we have $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

□

4 Artin Reciprocity for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

We now study the Artin reciprocity of the quadratic extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. $\mathbb{Q}(\sqrt{2})$ is different from $\mathbb{Q}(i)$ because it is totally real while $\mathbb{Q}(i)$ is purely imaginary.

Once again, by discriminant computation, we see the only rational prime ramified in $\mathbb{Q}(\sqrt{2})$ is 2. Moreover, using the fact that $\mathbb{Q}(\sqrt{2})$ is totally real, we have seen that the unique Archimedean place ∞ of $\mathbb{Q}$ does not ramify in $\mathbb{Q}(\sqrt{2})$. Therefore, the support of the conductor $\mathfrak{f}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is (2). It follows that $\mathfrak{f}$ is necessarily a power of (2).

$\mathfrak{f}$ can't be (2) because $\mathcal{I}_{\mathbb{Q},(2)} = \mathcal{P}_{\mathbb{Q},(2)}$, and the extension is non-trivial. Nor can it be $(2)^2$, because $(5) \in \mathcal{P}_{\mathbb{Q},(2)^2}$ but $\mathrm{Frob}_{(5)}$ is non-trivial. This also proves the Artin symbol is surjective for this extension.

We will show the next power, $(2)^3$, is the conductor(minimality is trivial because the previous two powers aren't even admissible). $\mathcal{P}_{\mathbb{Q},(2)^3}$ is generated by the prime ideals whose generators have residue 1 modulo 8, which we know split by quadratic reciprocity law for 2. Since the extension is quadratic, a prime either splits or is inert. Moreover, an odd rational prime p splits in $\mathbb{Q}(\sqrt{2})$, i.e. , $(p) = Q_1Q_2$, if and only if p is a norm of an ideal of $\mathbb{Q}(\sqrt{2})$(in fact, it is the norm either of the two factors). Finally, since $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is a cyclic group of order two, the square of any Frobenius given by an odd prime is necessarily the identity. The norm of the extension of an inert prime is its square, which gets sent to the identity by the Artin reciprocity map.

We therefore conclude $\frac{\mathcal{I}_{\mathbb{Q},(2)^3}}{\mathcal{P}_{\mathbb{Q},(2)^3}N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}((2)^3)} \overset{(,\mathbb{Q}(\sqrt{2})/\mathbb{Q})}{\cong} \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, confirming Artin reciprocity.

5 Quadratic Extensions of $\mathbb{Q}$

Now that we know the square root of any element in the set $\{-1\}\bigcup\{p : p \text{ is a prime}\}$ lies in a cyclotomic field, we can conclude any quadratic field $\mathbb{Q}(\sqrt{d})$(d is a square-free integer) lies in a cyclotomic field, obtained by taking compositum of the cyclotomic fields containing the squre-roots of the divisors of d.

6 Where Are We Heading?

6.1 The Kronecker-Weber Theorem

It is not a coincidence that any quadratic extension is the intermediate field of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ for some positive integer n. It was proved by Kronecker and Weber that any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Theorem 6.1 (Kronecker-Weber)**.** *If $K/\mathbb{Q}$ is a finite abelian extension, then we have a tower of extensions $\mathbb{Q}(\zeta_n) \supset K \supset \mathbb{Q}$ for some positive integer n.*

6.2 Arithmetic of Quadratic Forms

We can connect the problem of representing primes as sums of squares to the arithmetic of quadratic forms. Indeed, $x^2 + y^2$ is a binary quadratic form over $\mathbb{Q}$ and $\mathbb{Z}$.

More generally, let K be a number field, $\mathfrak{B}$ be a bilinear form on the 2-dimensional K-vector space $V = K^2$, we can form a Clifford algebra $(V, \mathfrak{B})$[1]. We can then ask whether the equation $v^2 = k$ has solution in

[1] This is the symmetric product(as K-module) $\mathrm{Sym}V = \bigoplus_{i\geq 0}\mathrm{Sym}^iV$ modulo the relations $vw + wv = 2\mathfrak{B}(v, w)$.

the Clifford algebra when v is restricted to some subsets(say $(K^{\times})^2$ or $\mathbb{Z}_K^2$) of K^2 for different $k \in K$.

$(V, \mathfrak{B})$ is a non-commutative K-algebra produced out of commutative data V and $\mathfrak{B}$. The translation from $x^2 + y^2 = p$ to $v^2 = p$ is a translation of a two-variable equation over a commutative K-algebra(K itself) to a one-variable equation over a non-commutative K-algebra $(V, \mathfrak{B})$.

6.3 Diophantine Geometry

In addition to the algebraic enrichment by introducing Galois groups, and the arithmetic enhancement from considerations of Clifford algebra, we can also augment the study of Diophantine equations to Diophantine geometry by studying the geometries of varieties and schemes defined by Diophantine equations.

7 Higher Reciprocity Laws

Recommended references:[9],[6].

8 Appendix: Useful Lemmas about Cyclotomic Fields

Recommended references:[7], [10], [4].

As far as the proof of Kronecker-Weber's Theorem is concerned, we need only a couple of structural theorems about the cyclotomic fields and their ramification data, which can be determined explicitly.

1.$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$.

2.$\mathbb{Z}_{\mathbb{Q}[\zeta_n]} \cong \mathbb{Z}[\zeta_n]$.

3.$\mathrm{disc}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (-1)^{\frac{\phi(n)}{2}} n^{\phi(n)} \prod_{p|n} p^{-\frac{\phi(n)}{p-1}}$. In particular, $\mathrm{disc}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

4.Composites of cyclotomic fields are also cyclotomic.

The importance of cyclotomic fields $\mathbb{Q}(\zeta_p)$ with p prime was first recognized in the early attempts to prove the Fermat's last theorem.

Starting with the identity $x^p + y^p = \prod_{1 \le k \le p-1} (x + \zeta_p^k y)$, it can be shown that the nonexistence of non-trivial integral solutions of the Diophantine equation $x^p + y^p = z^p$ subjected to the condition $(xyz, p) = 1$ follows from the p-indivisibility of the class number h_p of the cyclotomic field $\mathbb{Q}(\zeta_p)$. A prime p which does not divide h_p is called regular.

The computation of h_p is tricky. In fact, Fermat's last theorem would have followed if $h_p = 1$ for any prime p, which is not true in general but requires climbing up to the prime 23 to find out. Even the p-divisibility of

h_p is not completely known. As of the year 2021, it is not known whether there are infinitely many regular primes. On the other hand, there are many results about infinitudes of irregular primes of various types(c.f. [2],[5],and [8]). An example of irregular prime is 37, with $h_{37} = 37$.

References

[1] Oswald Baumgart. *The Quadratic Reciprocity Law: A Collection of Classical Proofs.* Birkhäuser, 2015.

[2] Leonard Carlitz. Note on irregular primes. *Proceedings of the American Mathematical Society*, 5(2):329–331, 1954.

[3] Leonard Eugene Dickson. *History of the theory of numbers: Diophantine Analysis*, volume 2. Courier Corporation, 2013.

[4] Harold M Edwards. *Fermat's last theorem: a genetic introduction to algebraic number theory*, volume 50. Springer Science & Business Media, 1996.

[5] Kaj Løchte Jensen. Om talteoretiske egenskaber ved de bernoulliske tal. *Nyt tidsskrift for matematik*, 26:73–83, 1915.

[6] Franz Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein.* Springer Science & Business Media, 2013.

[7] Daniel A Marcus. *Number Fields.* Springer, 2018.

[8] Tauno Metsänkylä. Distribution of irregular prime numbers. *Journal für die reine und angewandte Mathematik*, Issue 282, 1976.

[9] Richard A Mollin. *Algebraic number theory.* CRC press, 1999.

[10] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.