AN OVERVIEW OF CLASS FIELD THEORY

THOMAS R. SHEMANSKE

1. Introduction

In these notes, we try to give a reasonably simple exposition on the question of what is Class Field Theory. We strive more for an intuitive discussion rather than complete accuracy on all points. A great deal of what follows has been lifted without proper reference from the two very informative papers by Garbanati and Wyman [**?**],[**?**]. The questions which we shall pose and try to answer in the next section are:

1. What is Class Field Theory?
2. What are the goals of Class Field Theory?
3. What are the main results of Class Field Theory over $\mathbb{Q}$?

2. The Origins of Class Field Theory

In examining the work of Abel, Kronecker (1821 – 1891) observed that certain abelian extensions of imaginary quadratic number fields are generated by the adjunction of special values of automorphic functions arising from elliptic curves. For example, if K is an imaginary quadratic number field and $\mathfrak{A} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is an ideal of K with $\mathrm{Im}(\omega_1/\omega_2) > 0$, then $K(j(\omega_1/\omega_2))$ is an abelian extension of K, where j is the modular function.

Kronecker wondered whether all abelian extensions of K could be obtained in this manner (Kronecker's Jugendtraum). This leads to the question of "finding" all abelian extensions of number fields. Kronecker conjectured and Weber (1842 – 1913) proved:

Theorem (Kronecker–Weber (1886–1887))**.** *Every abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic extension of* $\mathbb{Q}$*.*

To Kronecker and Weber, Class Field Theory was the task of finding all abelian extensions, and of finding a generalization of Dirichlet's theorem on primes in arithmetic progressions which is valid in number fields.

Hilbert saw that Class Field Theory is much more — that it is the theory of abelian extensions. In his famous address to the ICM in Paris in 1900, Hilbert posed numerous questions two of which are the focus of the endeavors in Class Field Theory.

Date: August 2, 2000.

Hilbert's 9th: To develop the most general reciprocity law in an arbitrary number field, generalizing Gauss' law of quadratic reciprocity.
- — For abelian extensions, this is the Artin reciprocity law
- — For non-abelian extensions, the question is still open and one cannot expect an answer similar to the one in the abelian case. In particular, "congruence conditions will not suffice".

Hilbert's 12th: Generalize Kronecker's Jugendtraum.

2.1. **What is a reciprocity law?** Let $f \in \mathbb{Z}[X]$ be monic and irreducible, and let K_f be the splitting field of f over $\mathbb{Q}$. Then $K_f/\mathbb{Q}$ is a finite Galois extension. Let $p \in \mathbb{Z}$ be a prime and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Reducing f mod p gives a polynomial $f_p \in \mathbb{F}_p[X]$. If f_p factors into distinct linear factors over $\mathbb{F}_p$ then we say that f *splits completely modulo* p. Define $Spl(f) = \{\, p \in \mathbb{Z} \mid f \text{ splits completely modulo } p \,\}$. With finite exceptions, $Spl(f) = \{\, p \in \mathbb{Z} \mid p \text{ splits completely in } K_f \,\}$ via the Dedekind-Kummer theorem (see §4).

By a reciprocity law, we intend a means by which to describe the factorization of f_p as a function of p, or somewhat less demanding, a "rule" which determines which primes belong to $Spl(f)$. First, why is this of interest? In response, we have the Inclusion theorem:

Theorem (Inclusion Theorem)**.** *Let f, g be irreducible polynomials in $\mathbb{Z}[X]$ with splitting fields K_f, K_g respectively. Then $K_f \supset K_g$ if and only if $Spl(f) \subset^* Spl(g)$.*

Here $\subset^*$ means with finitely many exceptions. Thus $K_f = K_g$ if and only if $Spl(f) =^* Spl(g)$, that is the set $Spl(f)$ captures the Galois extension.

Proof. ($\Rightarrow$) This direction is straightforward. If $p \in Spl(f)$ then $e(K_f/\mathbb{Q}) = 1$ and $f(K_f/\mathbb{Q}) = 1$. Since $K_f \supset K_g$ and e and f are multiplicative in towers, we have $e(K_g/\mathbb{Q}) = 1$ and $f(K_g/\mathbb{Q}) = 1$, and hence $p \in Spl(g)$.
($\Leftarrow$) This direction follows from the Tchebotarev density theorem. □

We give an example.

Example. Let p be a prime $p \equiv 1 \pmod 4$, $f(X) = X^2 - p$, and $g(X) = X^p - 1$. Then $K_f = \mathbb{Q}(\sqrt{p})$ and $K_g = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity. Since $p \equiv 1 \pmod 4$, we have $K_f \subset K_g$. We must show that $Spl(f) \supset^* Spl(g)$. It is well-known that a prime $q \in Spl(g)$ (i.e., q splits completely in $\mathbb{Q}(\zeta_p)$) iff $q \equiv 1 \pmod p$ and $q \in Spl(f)$ (i.e., q splits completely in $\mathbb{Q}(\sqrt{p})$) iff $\left(\frac{q}{p}\right) = 1$ (via the Dedekind-Kummer theorem). Clearly any prime q satisfying $q \equiv 1 \pmod p$ satisfies $\left(\frac{q}{p}\right) = 1$, hence $Spl(f) \supset Spl(g)$.

Another theorem of great importance is the

Theorem (Abelian Polynomial Theorem)**.** *The set $Spl(f)$ can be described by congruences with respect to a modulus depending only on f (K_f) if and only if K_f is an abelian extension of $\mathbb{Q}$.*

The Artin reciprocity law is a precise version of ($\Leftarrow$), and ($\Rightarrow$) says that "congruence conditions" will not suffice to characterize a reciprocity law for non-abelian extensions.

Examples:

1. Let $p \in \mathbb{Z}$ be an odd prime, and consider the quadratic polynomial $f(X) = X^2 - q$ where q is an odd prime. Then modulo p, three things can happen:
   (a) $f_p(X) = l(X)^2$, linear $l(X)$
   (b) $f_p(X) = l_1(X)l_2(X)$ distinct linear factors (f splits completely modulo p)
   (c) f_p is irreducible.
   (a) occurs iff $x^2 \equiv q \pmod{p}$ has one solution iff $p = q$.
   (b) occurs iff $x^2 \equiv q \pmod{p}$ has two solutions iff $\left(\frac{q}{p}\right) = +1$.
   (c) occurs iff $x^2 \equiv q \pmod{p}$ has no solutions iff $\left(\frac{q}{p}\right) = -1$.

   To determine for which p the congruence $x^2 \equiv q \pmod{p}$ is solvable, is apriori an infinite problem. On the other hand, it is one from which the traditional form of quadratic reciprocity rescues us.

   Suppose $q = 17$ in the above example. Then $\left(\frac{17}{p}\right) = +1$ iff $\left(\frac{p}{17}\right) = +1$ iff $p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$. Thus $p \in Spl(x^2 - 17)$ iff (with finite exceptions) $p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$.
2. Next consider the cyclotomic polynomials, Φ_n. Let ζ be a primitive n^{th} root of unity and Φ_n the irreducible polynomial of ζ over $\mathbb{Q}$. We know that the degree of Φ_n is $\phi(n)$ and that $x^n - 1 = \prod_{d|n} \Phi_d$. To describe $Spl(\Phi_n)$ we need to answer which primes split completely in $K_{\Phi_n} = \mathbb{Q}(\zeta)$. If $p \nmid n$ then for any prime of K_{Φ_n} lying above p, we know $e = 1$ and $fg = \phi(n)$. Moreover, f is determined by the relation that it is the smallest positive integer such that $p^f \equiv 1 \pmod{n}$. Thus p splits completely in K_{Φ_n} iff $f = 1$, hence $p \in Spl(\Phi_n)$ iff (wfe) $p \equiv 1 \pmod{n}$, characterizing $Spl(\Phi_n)$ by congruence conditions.

Let us loosely define the *arithmetic of a number field K* to be the study of the ideals of K and the quotient rings determined by the ideals of K as well as the study of the ideal class group and groups isomorphic to subgroups or quotient groups of the ideal class group.

Goals of Class Field Theory:

1. Describe all finite abelian extensions of K in terms of the arithmetic of K.
2. Canonically realize $Gal(L/K)$ in terms of the arithmetic of K whenever $Gal(L/K)$ is abelian.
3. Describe the decomposition of a prime ideal from K to L in terms of the arithmetic of K whenever L/K is abelian (i.e., provide a reciprocity law).

2.2. **Summary of Class Field Theory over $\mathbb{Q}$.** Notation: $\mathbb{Q}_m = \mathbb{Q}(e^{2\pi i/m})$. We may assume that $m \not\equiv 2(4)$. For if $m \equiv 2 \pmod 4$ with $m = 2m_0$, then we easily observe that $-e^{2\pi i/m_0}$ is a primitive mth root of unity, and hence that $\mathbb{Q}_m = \mathbb{Q}_{m_0}$. Over $\mathbb{Q}$, the Kronecker-Weber Theorem motiviates the following definition:

Definition . Let $L/\mathbb{Q}$ be a finite abelian extension. A positive integer m is called a *defining modulus* or an *admissible modulus of* L if $L \subset \mathbb{Q}_m$. Such an m exists by the Kronecker-Weber theorem. The *conductor* of L, $\mathfrak{f}_L$, is the smallest admissible modulus of L.

Examples:

1. $L = \mathbb{Q}_m$. Then $\mathfrak{f}_L = m$, since $\mathbb{Q}_m \subset \mathbb{Q}_n$ implies that $\mathbb{Q}_m = \mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_{(m,n)}$ implies that $m \mid n$.
2. Let L be the maximal real subfield of $\mathbb{Q}_m$. Then $L = \mathbb{Q}(\zeta+\zeta^{-1})$ where $\zeta = e^{2\pi i/m}$ (it is the fixed field of complex conjugation). Note that if $m = 3, 4$, then $L = \mathbb{Q}$. For $m \geq 5$, $\mathfrak{f}_L = m$. For $m = 3, 4$, $\mathfrak{f}_L = 1$.
3. $L = \mathbb{Q}(\sqrt{d})$, d square-free integer, $|d| > 1$. Then

$$\mathfrak{f}_L = |\mathrm{disc}(L)| = \begin{cases} |d| & \text{if } d \equiv 1 \pmod 4 \\ |4d| & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

To gain some feeling for why the last example holds, recall that if $L = \mathbb{Q}_p$ (p an odd prime), then $\mathrm{disc}(L) = (-1)^{\frac{p-1}{2}} p^{p-2}$ is the square of an integer in $\mathcal{O}_L$, thus

$$\mathbb{Q}\Big(\sqrt{(-1)^{\frac{p-1}{2}} p}\Big) \subset \mathbb{Q}_p.$$

It follows that for a prime p

$$\mathbb{Q}(\sqrt{p}) \subset \begin{cases} \mathbb{Q}_p & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}_{4p} & \text{if } p \equiv 3 \pmod 4 \\ \mathbb{Q}_8 & \text{if } p = 2. \end{cases}$$

Moreover, if $d = \pm 2^\nu p_1 p_2 \cdots p_r$ is squarefree, then $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{2^\nu}, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_r}) \subset \mathbb{Q}(\zeta_{4\cdot 2^\nu})\mathbb{Q}(\zeta_{p_1}, \zeta_{p_2}, \ldots, \zeta_{p_r}, \zeta_4) = \mathbb{Q}(\zeta_{4d})$.

Theorem . *Let $L/\mathbb{Q}$ be a finite abelian extension, and m an admissible modulus of L. Then $\mathfrak{f}_L \mid m$.*

Proof. $L \subset \mathbb{Q}_m \cap \mathbb{Q}_{\mathfrak{f}_L} = \mathbb{Q}_{(\mathfrak{f}_L, m)}$ which implies $\mathfrak{f}_L \mid m$. □

Let L be an abelian extension of $\mathbb{Q}$, and let m be an admissible modulus of L. Then $L \subset \mathbb{Q}_m$. Let $a \in \mathbb{Z}$ with $(a, m) = 1$, and denote by $\left(\dfrac{L}{a}\right)$ the Artin symbol,

the automorphism of L obtained by restricting to the field L the automorphism of $\mathbb{Q}_m$ determined by $(\zeta \mapsto \zeta^a)$. Then the Artin map is the homomorphism

$$\left(\frac{L}{*}\right) : (\mathbb{Z}/m\mathbb{Z})^\times \to Gal(L/\mathbb{Q}).$$

The Artin map is onto since every automorphism of L extends to one of $\mathbb{Q}_m$ which has the above form. Denote the kernel of $\left(\frac{L}{*}\right)$ by $I_{L,m}$. Identifying $(\mathbb{Z}/m\mathbb{Z})^\times$ with $Gal(\mathbb{Q}_m/\mathbb{Q})$, we see that $I_{L,m}$ is identified with $Gal(\mathbb{Q}_m/L)$, so under the Galois correspondence (see diagram below), L is the fixed field of the subgroup $I_{L,m}$ of $(\mathbb{Z}/m\mathbb{Z})^\times$.

$$\begin{array}{ccc}
\mathbb{Q}_m & \longleftarrow & \{1\} \\
\Big| & & \Big| \\
L & \longleftarrow & I_{L,m} \\
\Big| & & \Big| \\
\mathbb{Q} & \longleftarrow & (\mathbb{Z}/m\mathbb{Z})^\times
\end{array}$$

This information is summarized in the

Theorem (Artin Reciprocity)**.** *Let $L/\mathbb{Q}$ be a finite abelian extension with defining modulus m. Then the following sequence is exact:*

$$1 \to I_{L,m} \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \to Gal(L/\mathbb{Q}) \to 1.$$

Thus, the Artin map induces an isomorphism between $Gal(L/\mathbb{Q})$ and $(\mathbb{Z}/m\mathbb{Z})^\times/I_{L,m}$ thus canonically realizing $Gal(L/\mathbb{Q})$ in terms of the arithmetic of $\mathbb{Q}$. In particular, this says that every abelian extension is given in terms of the arithmetic of $\mathbb{Q}$, and so realizes one of the primary goals of Class Field Theory.

As a special case, if L is a quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}_m$, then $Gal(L/\mathbb{Q})$ is isomorphic to $\{\pm 1\}$, and identifying the isomorphic groups, the Artin map essentially can be defined by $\left(\frac{L}{\cdot}\right) a = \left(\frac{a}{m}\right)$. To make clearer what we mean, we examine some typical cases in the examples below.

Examples:

1. Let p be an prime $p \equiv 1 \pmod 4$. Then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}_p$. If $L = \mathbb{Q}(\sqrt{p})$, then since $[L : \mathbb{Q}] = 2$, $I_{L,p}$ is a subgroup of index two in $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic,

there is a unique such subgroup, namely the squares (or quadratic residues) mod p. For any a prime to p, $\left(\frac{L}{a}\right) = \pm 1$, and $I_{L,p}$ is the kernel of $\left(\frac{L}{*}\right)$. With $I_{L,p}$ identified as the group of squares mod p and $Gal(L/\mathbb{Q})$ identified with $\{\pm 1\}$, it is clear that $\left(\frac{L}{a}\right) = \left(\frac{a}{p}\right)$.

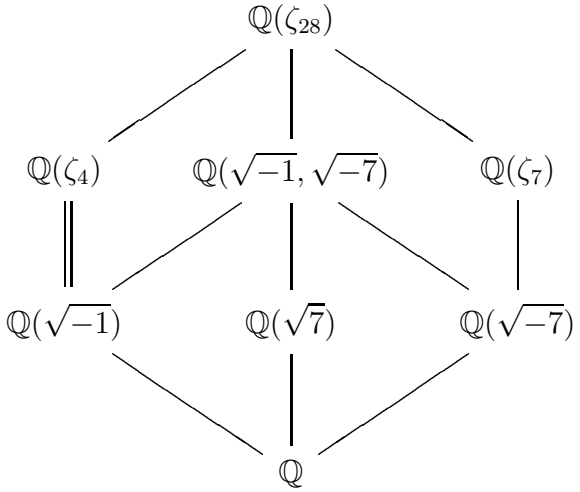
2. A considerably more complicated example is $L = \mathbb{Q}(\sqrt{7})$. Clearly the conductor of L is 28, so take $m = 28$ in the setup above. Here we will see that $\left(\frac{L}{a}\right)$ is almost $\left(\frac{a}{28}\right)$. The only real difficulty in interpreting the quadratic residue symbol $\left(\frac{a}{2}\right)$, so we digress for a moment.

   Recall that $\left(\frac{a}{2}\right)$ is defined by

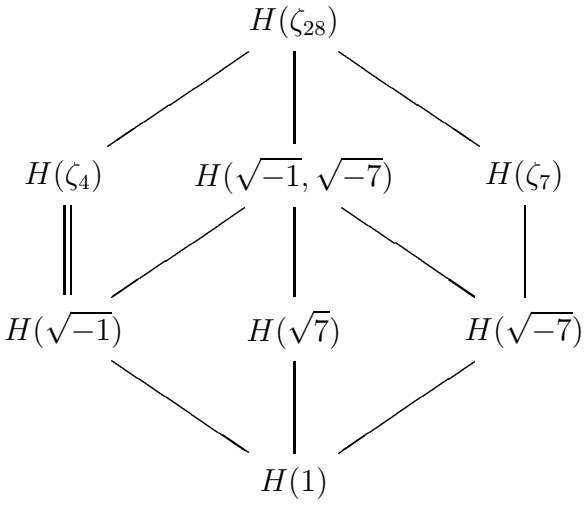
$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8 \\ -1 & \text{if } a \equiv 5 \pmod 8 \\ 0 & \text{otherwise.} \end{cases}$$

   In particular, if a is squarefree and p is any prime, then $\left(\frac{a}{p}\right)$ is 1, -1 or 0 depending upon whether p splits, is inert, or ramifies in $\mathbb{Q}(\sqrt{a})$. The difficulty we encounter is that if $a \equiv 3 \pmod 4$, then $\left(\frac{a}{4}\right) = \left(\frac{a}{2}\right)^2 \neq \left(\frac{a^2}{2}\right)$, the first expression equalling zero, while the last equals 1.

   To continue, let $\zeta_m = e^{2\pi i/m}$, and consider the tower of fields below.



   By the Galois correspondence, there is a corresponding lattice of groups.



Here we set the notation by putting $H(1) = (\mathbb{Z}/28\mathbb{Z})^\times$ (and $H(\zeta_{28}) = \{1\}$). Then for example, $H(\sqrt{-7})$ is the subgroup of $(\mathbb{Z}/28\mathbb{Z})^\times$ corresponding to $Gal(\mathbb{Q}(\zeta_{28})/\mathbb{Q}(\sqrt{-7}))$.

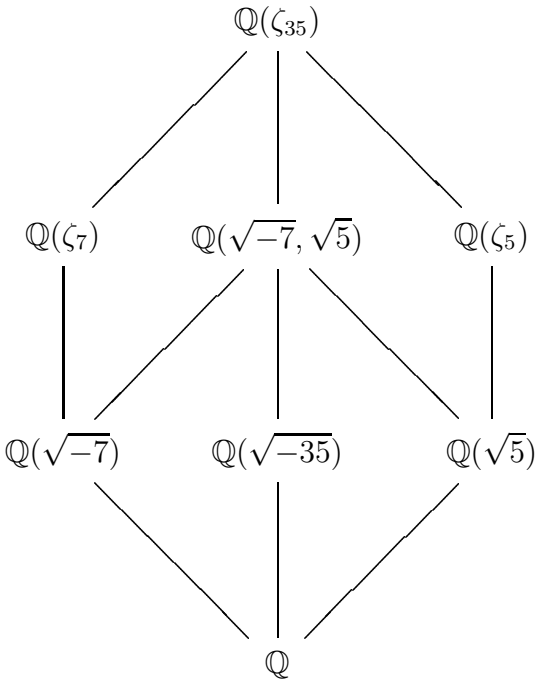
Our purpose is to calculate $I_{L,28}$ where $L = \mathbb{Q}(\sqrt{7})$, and to compare the values of $\left(\frac{L}{a}\right)$ with those of $\left(\frac{a}{28}\right)$. The subgroup $I_{L,28}$ will simply be $H(\sqrt{7})$.

If we consider the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$, then as a subgroup of $(\mathbb{Z}/7\mathbb{Z})^\times$, $\mathbb{Q}(\sqrt{-7})$ corresponds to the subgroup of quadratic residues mod 7 (as in example 1), that is to $\{1, 2, 4\}$. Modulo 28 (i.e. $a \equiv 1, 2, 4 \pmod 7$ and $a \equiv 1, 3 \pmod 4$), this yields $H(\sqrt{-7}) = \{1, 9, 11, 15, 25, 23\} \subset (\mathbb{Z}/28\mathbb{Z})^\times$. The tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ is degenerate yielding the trivial subgroup of $(\mathbb{Z}/4\mathbb{Z})^\times$ corresponding to $\mathbb{Q}(\sqrt{-1})$, or $\{a | a \equiv 1 \pmod 4\}$. Modulo 28 (i.e., $a \equiv 1 \pmod 4$ and $a \not\equiv 0 \pmod 7$), this yields $H(\sqrt{-1}) = \{1, 5, 9, 13, 17, 25\}$.

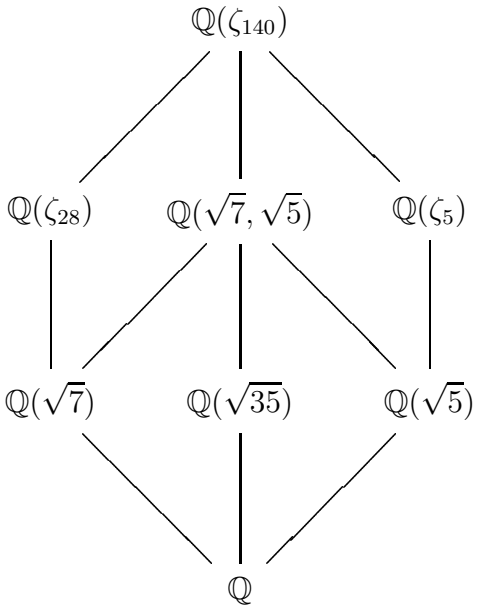
As $\mathbb{Q}(\sqrt{-1}, \sqrt{-7})$ is the compositum of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-7})$, Galois theory tells us that $H(\sqrt{-1}, \sqrt{-7}) = H(\sqrt{-1}) \cap H(\sqrt{-7}) = \{1, 9, 25\}$. For the record, we note that $\left(\frac{a}{28}\right) = +1$ if and only if $(a, 28) = 1$ and $\left(\frac{a}{7}\right) = \left(\frac{a}{4}\right)$, which is true if and only if $a \equiv 1, 2, 4 \pmod 7$ and $a \equiv 1 \pmod 4$. Note that since $\left(\frac{a}{4}\right) = \left(\frac{a}{2}\right)^2$, $\left(\frac{a}{4}\right)$ is never equal to -1. Thus $\{a | \left(\frac{a}{28}\right) = 1\} = \{1, 9, 25\}$, and is not equal to $H(\sqrt{7}) = I_{L,28}$ which has order 6. It is now a trivial matter to deduce that $H(\sqrt{7}) = \{1, 3, 9, 19, 25, 27\}$.

3. To handle more general examples like $L = \mathbb{Q}(\sqrt{\pm 35})$, we need only consider one of the two tower of fields below and use the techniques of the preceding examples.

   If $L = \mathbb{Q}(\sqrt{-35})$, we consider the tower



whereas if $L = \mathbb{Q}(\sqrt{35})$, we consider the tower



and proceed as in the previous examples.

To continue our investigation of class fields, we have the following theorem which gives information about the conductor of an abelian extension.

Theorem (Conductor–Ramification Theorem)**.** *If L is a finite abelian extension of $\mathbb{Q}$, then a prime p of $\mathbb{Q}$ ramifies in L if and only if $p \mid \mathfrak{f}_L$.*

Corollary . *If $L \neq \mathbb{Q}$ is a finite abelian extension of $\mathbb{Q}$, then at least one prime p ramifies in L.*

Proof. Since $L \neq \mathbb{Q}$, $L \nsubseteq \mathbb{Q}_1 = \mathbb{Q}$, hence $\mathfrak{f}_L > 1$, and so is divisible by at least one prime. □

For contrast, we have the result of Minkowski that a prime p of $\mathbb{Q}$ ramifies in a number field L if and only of $p \mid \mathrm{disc}(L)$. This says that for abelian extensions, there should be a connection between the conductor and the discriminant (see the conductor-discriminant formula below).

Theorem (Decomposition Theorem)**.** *Let m be a defining modulus of L. If $p \nmid m$ (in particular p is unramified) then the order of $pI_{L,m}$ in $(\mathbb{Z}/m\mathbb{Z})^\times/I_{L,m}$ is f, the residue class degree.*

Notice that this generalizes the theorem about the decomposition of primes in cyclotomic fields. If we choose $L = \mathbb{Q}_m$, then $I_{L,m} = 1$, and we are reduced to talking about the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$.
Let $m = \mathfrak{f}_L$ in the above theorem. Since $efg = [L : \mathbb{Q}]$,

$$\begin{aligned} p \in Spl(L/\mathbb{Q}) &\Leftrightarrow e = 1,\ f = 1 \\ &\Leftrightarrow p \nmid \mathfrak{f}_L,\ p \in I_{L,\mathfrak{f}_L} \end{aligned}$$

the first condition because $e = 1$ and the second because $f = 1$ via the Decomposition theorem.

If $I_{L,\mathfrak{f}_L} = \{a_1, \ldots a_s\}$ with $a_i \in \mathbb{Z}$ and $(a_i, \mathfrak{f}_L) = 1$, then $p \in Spl(L/\mathbb{Q}) \Leftrightarrow p \equiv a_i \pmod{\mathfrak{f}_L}$ for some i. This acomplishes the goal of describing $Spl(L/\mathbb{Q})$ in terms of congruence conditions, and hence the decomposition of primes in terms of the arithmetic of $\mathbb{Q}$.

2.3. **Duality.** Let X_m denote the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$. That is $\chi \in X_m$ implies that $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ is a homomorphism.

Definition . We say that d is a *defining modulus* for χ if $a \equiv 1 \pmod{d}$ implies that $\chi(a) = 1$. The *conductor* of χ, denoted $\mathfrak{f}_\chi$, is the smallest defining modulus for χ.

If m is a defining modulus for a finite abelian extension L, let

$$X_{L,m} = \{\chi \in X_m | \chi(h) = 1 \text{ for all } h \in I_{L,m}\}$$

Recall that $I_{L,m}$ is the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times \cong Gal(\mathbb{Q}_m/\mathbb{Q})$ corresponding to the subfield $L \subset \mathbb{Q}_m$ via the Galois correspondence. That is, $I_{L,m} \cong Gal(\mathbb{Q}_m/L)$, and from duality we see that

$$X_{L,m} \cong Gal(\mathbb{Q}_m/L)^\perp \cong Gal(\mathbb{Q}_m/\widehat{\mathbb{Q})/Gal}(\mathbb{Q}_m/L) \cong \widehat{Gal(L/\mathbb{Q})}.$$

Finally, we have the

Theorem (Conductor–Discriminant Formula)**.** *Let m be an admissible modulus for a finite abelian extension L of $\mathbb{Q}$. Then*

$$\mathfrak{f}_L = lcm\{\mathfrak{f}_\chi | \chi \in X_{L,m}\}$$

and

$$|disc(L)| = \prod_{\chi \in X_{L,m}} \mathfrak{f}_\chi.$$

In particular, $\mathfrak{f}_L \mid \text{disc}(L)$, and so we always have the tower of fields:

$$\mathbb{Q} \subset L \subset \mathbb{Q}_{\mathfrak{f}_L} \subset \mathbb{Q}_{|\text{disc}(L)|}.$$

3. **Global Class Field Theory**

In order to generalize Class Field Theory to ground fields other than $\mathbb{Q}$, several issues need to be addressed:

1. The Kronecker-Weber theorem is valid only for ground field $\mathbb{Q}$, so we need a new notion of admissible modulus (a very deep theorem).
2. We need to handle all the infinite primes.
3. We need a generalized notion of congruence.
4. With what shall we replace $(\mathbb{Z}/m\mathbb{Z})^\times$ and $\mathbb{Q}_m$?

Let $\mathfrak{M}$ be a modulus and let $\mathfrak{M}_0$ denote its finite part. For a number field K, let $I_K^{\mathfrak{M}}$ denote the group of fractional ideals of K relatively prime to $\mathfrak{M}_0$. Let

$$K_{\mathfrak{M},1} = \{\, \alpha \in K^\times \mid \alpha \equiv 1 \pmod{{}^*\mathfrak{M}} \,\}.$$

Recall that $\alpha \equiv 1 \pmod{{}^*\mathfrak{M}}$ means that

$$\begin{aligned} \text{ord}_{\mathfrak{p}}(\alpha - 1) \geq \text{ord}_{\mathfrak{p}}(\mathfrak{M}_0) \quad &\text{for all } \mathfrak{p} \mid \mathfrak{M}_0 \quad \text{and} \\ \alpha > 0 &\text{ at each real prime dividing } \mathfrak{M} \end{aligned}$$

Let $R_{\mathfrak{M}} = \{\alpha\mathcal{O}_K \mid \alpha \in K_{\mathfrak{M},1}\}$. $R_{\mathfrak{M}}$ is called the *ray mod* $\mathfrak{M}$. Let $C_{\mathfrak{M}} = I_K^{\mathfrak{M}}/R_{\mathfrak{M}}$, the *ray class group*. Special cases are familiar. If $\mathfrak{M} = 1$, then the ray class group C_1 is just the ideal class group of the field K. If $K = \mathbb{Q}$ and $\mathfrak{M} = mp_\infty$, where m is a positive integer, then $C_{\mathfrak{M}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Let L/K be a Galois extension and let $\mathfrak{M}$ be a K-modulus. Define $I_L^{\mathfrak{M}} = I_L^{\mathfrak{M}_0\mathcal{O}_L}$ and

$$L_{\mathfrak{M},1} = \{\, \alpha \in L^\times \mid \alpha \equiv 1 \pmod{{}^*\mathfrak{M}_0\mathcal{O}_L} \text{ and where } \alpha > 0 \text{ at each real prime of } L \text{ dividing a real prime occuring in } \mathfrak{M} \,\}.$$

Finally let $R_{L,\mathfrak{M}} = \{\alpha\mathcal{O}_L \mid \alpha \in L_{\mathfrak{M},1}\}$, and $C_{L,\mathfrak{M}} = I_L^{\mathfrak{M}}/R_{L,\mathfrak{M}}$.

Recall that the norm of an ideal relative to a Galois extension L/K is defined as follows: If $\mathfrak{p}$ is a prime of K and $\mathfrak{P}$ is a prime of L lying above $\mathfrak{p}$ with inertial degree f, then we define the norm of $\mathfrak{P}$ to be $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$. We extend the definition of the norm to the group of fractional ideals by multiplicativity. Note that when $K = \mathbb{Q}$, $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f = p^f\mathbb{Z}$ for the prime $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$, while the absolute norm of $\mathfrak{P}$ is equal the cardinality of the residue class field $\mathcal{O}_L/\mathfrak{P}$ which is p^f, so this definition provides a natural generalization of the absolute norm.

One can show that $N_{L/K}(R_{L,\mathfrak{M}}) \subset R_{\mathfrak{M}}$, and so the definition of the norm can be extended to $C_{L,\mathfrak{M}}$ by defining $N_{L/K}(\mathfrak{A}R_{L,\mathfrak{M}}) = N_{L/K}(\mathfrak{A})R_{\mathfrak{M}}$. Put

$$I_{L/K,\mathfrak{M}} = N_{L/K}(C_{L,\mathfrak{M}}) < C_{\mathfrak{M}}.$$

For example, if $K = \mathbb{Q}$ and $L \subset \mathbb{Q}_m$ (i.e. m is an admissible modulus of L), then we have the diagram:

$$\begin{array}{ccc} \mathbb{Q}_m & \longleftarrow & \{1\} \\ | & & | \\ L & \longleftarrow & I_{L,m} \\ | & & | \\ \mathbb{Q} & \longleftarrow & (\mathbb{Z}/m\mathbb{Z})^\times \end{array}$$

If we let $\mathfrak{M} = mp_\infty$, then it can be shown that $I_{L/K,\mathfrak{M}} \cong I_{L,m}$. Notice also that $C_{\mathfrak{M}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and that $[C_{\mathfrak{M}} : I_{L/\mathbb{Q},\mathfrak{M}}] = [L : \mathbb{Q}]$ by the Galois correspondence. Generalizing this fact, we have the deep theorem:

Theorem . *Let $\mathfrak{M}$ be a K-modulus and L/K an abelian extension of number fields. Then there exists a unique K-modulus $\mathfrak{f}_{L/K}$ such that $[C_{\mathfrak{M}} : I_{L/K,\mathfrak{M}}] = [L : K]$ iff $\mathfrak{f}_{L/K} \mid \mathfrak{M}$.*

The unique modulus $\mathfrak{f}_{L/K}$ is called the *conductor* of L/K and any K-modulus divisible by $\mathfrak{f}_{L/K}$ is called an *admissible* modulus of L/K.

This is not a very intuitive theorem because we don't have something natural like the Kronecker-Weber theorem with which to define the conductor. The theorem is proved in two steps. The first inequality to be established was that $[C_{\mathfrak{M}} : I_{L/K,\mathfrak{M}}] \leq [L : K]$ for all moduli $\mathfrak{M}$. This was done by Weber (1897-8). It is now known as the "second inequality". In 1920, Tagaki showed that $[C_{\mathfrak{M}} : I_{L/K,\mathfrak{M}}] \geq [L : K]$ for some modulus $\mathfrak{M}$, now known as the "first inequality".
One can also show that

$$\mathfrak{f}_{L/\mathbb{Q}} = \begin{cases} (f_L) & \text{if } L \subset \mathbb{R} \\ (f_L)p_\infty & \text{if } L \not\subset \mathbb{R} \end{cases}$$

Now we need an analog of the cyclotomic fields and the Kronecker-Weber theorem.

Theorem (Existence)**.** *Given a K-modulus $\mathfrak{M}$ and a subgroup $I_{\mathfrak{M}}$ of the ray class group $C_{\mathfrak{M}}$, there exists a unique abelian extension L/K such that*

1. *$\mathfrak{M}$ is an admissible modulus of L/K*
2. *$I_{L/K,\mathfrak{M}} = N_{L/K}(C_{L,\mathfrak{M}}) = I_{\mathfrak{M}}$ or*
3. *The kernel of the Artin map $I_K^{\mathfrak{M}} \to Gal(L/K)$ is $H_{\mathfrak{M}}$ where $I_{\mathfrak{M}} = H_{\mathfrak{M}}/R_{\mathfrak{M}}$.*

L is called the *class field* of the subgroup $I_{\mathfrak{M}}$. When $I_{\mathfrak{M}} = R_{\mathfrak{M}}$, the trivial subgroup, the class field L is called the *ray class field* and is denoted $K(R_{\mathfrak{M}})$. If $K = \mathbb{Q}$ and $\mathfrak{M} = mp_\infty$, then $K(R_{\mathfrak{M}}) = \mathbb{Q}_m$, that is the cyclotomic fields are the ray class fields for the moduli $\mathfrak{M} = mp_\infty$. The ray class field for the modulus $\mathfrak{M} = m$ is the maximal real subfield of $\mathbb{Q}_m$.

We have two more important theorems:

Theorem . *Given an abelian extension L/K, there exists a K-modulus $\mathfrak{M}$ so that $L \subset K(R_{\mathfrak{M}})$.*

As a consequence, we recover the Kronecker-Weber theorem.

Theorem . *Given an abelian extension L/K, the conductor $\mathfrak{f}_{L/K}$ is the "smallest" K-modulus $\mathfrak{M}$ such that $L \subset K(R_{\mathfrak{M}})$. Moreover, $\mathfrak{M}$ is an admissible modulus of L/K iff $L \subset K(R_{\mathfrak{M}})$.*

Thus it follows that every abelian extension of K is a subfield of a ray class field for K. We have classified the abelian extensions, but we have not constructed them. More later.

We have the following generalization of Dirichlet's theorem on primes in arithmetic progressions.

Theorem . *Let $I_{\mathfrak{M}}$ be a subgroup of the ray class group $C_{\mathfrak{M}}$. Then $I_{\mathfrak{M}} = H_{\mathfrak{M}}/R_{\mathfrak{M}}$ where $R_{\mathfrak{M}} \subset H_{\mathfrak{M}} \subset I_K^{\mathfrak{M}}$. Then there are an infinite number of primes in each coset of $I_K^{\mathfrak{M}}/H_{\mathfrak{M}}$. In fact, the primes in the coset have density $1/[I_K^{\mathfrak{M}} : H_{\mathfrak{M}}]$.*

If $K = \mathbb{Q}$ and $\mathfrak{M} = mp_\infty$, then $C_{\mathfrak{M}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$. If we choose $H_{\mathfrak{M}} = R_{\mathfrak{M}}$, then $I_K^{\mathfrak{M}}/H_{\mathfrak{M}} = C_{\mathfrak{M}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$, and we have recovered the Dirichlet theorem over $\mathbb{Q}$.

It can be shown that if $\mathfrak{M}$ is an admissible modulus for an abelian extension of number fields L/K, then the Artin map, $\left(\frac{L/K}{*}\right)$, is trivial on the ray mod $\mathfrak{M}$, $R_{\mathfrak{M}}$, and so the definition of the Artin map can be extended to the ray class group, $C_{\mathfrak{M}}$.

In 1927, Artin proved

Theorem (Artin Reciprocity)**.** *Let L/K be an abelian extension of number fields, and let $\mathfrak{M}$ be an admissible modulus of L/K. Then the following sequence is exact:*

$$1 \to I_{L/K,\mathfrak{M}} = N_{L/K}(C_{L/K,\mathfrak{M}}) \hookrightarrow C_{\mathfrak{M}} \to Gal(L/K) \to 1.$$

Corollary . *Let $\mathfrak{M}$ be an admissible modulus of the abelian extension L/K. Then $L \subset K(R_{\mathfrak{M}})$, $Gal(K(R_{\mathfrak{M}})/K) \cong C_{\mathfrak{M}}$ and $Gal(K(R_{\mathfrak{M}})/L) \cong I_{L/K,\mathfrak{M}}$.*

Definition . The Hilbert class field of a number field K is the ray class field $K(R_1)$, and will be denoted $\tilde{K}$.

From above we see that $Gal(\tilde{K}/K) \cong C_1$, the ideal class group of K. Thus much work is done in trying to understand subfields of $\tilde{K}$ to help understand the structure of the ideal class group.

Theorem . *A K-prime $\mathfrak{p}$ ramifies in L iff $\mathfrak{p} \mid \mathfrak{f}_{L/K}$.*

Theorem . *The Hilbert class field $\tilde{K}$ is the maximal abelian unramified extension of K.*

Proof. Since $\tilde{K} = K(R_1)$, $\mathfrak{f}_{\tilde{K}/K} = (1)$. If L is an unramified extension of K, then $\mathfrak{f}_{L/K} = (1)$ by the above theorem. Since (1) is an admissible modulus for L/K, we have $L \subset K(R_1) = \tilde{K}$. □

Theorem . *Each fractional ideal of K becomes principal in $\tilde{K}$.*

This does not say that $\tilde{K}$ has class number one. Instead it suggests the "class tower problem". Let $K_0 = K$ and $K_i = \tilde{K}_{i-1}$ for $i \geq 1$. Does there exist a j such that $K_j = K_{j-1}$? This would imply that the class number of K_{j-1} equals 1. Golod and Shafarevich (1964) showed that any imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ where d is a positive integer divisible by at least six primes has an infinite class field tower.

4. **Equivalence of the reciprocity laws.**

We consider the case of a prime p, $p \equiv 1 \pmod 4$, and q an odd prime, $q \neq p$.

Gauss' law says that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Wyman asks for a rule which describes the primes q which split completely in $\mathbb{Q}(\sqrt{p})$.

Artin says that

$$1 \to H \hookrightarrow I_{\mathbb{Q}}^{pp^\infty} \to Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \to 1$$

for an appropriately defined subgroup H is exact where the map $I_{\mathbb{Q}}^{pp^\infty} \to Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$ is the Artin map.
Consider the diagram:

$$\begin{array}{ccc} L = \mathbb{Q}_p & \longleftarrow & \{1\} \\ \Big| & & \Big| \\ K = \mathbb{Q}(\sqrt{p}) & \longleftarrow & Gal(\mathbb{Q}_p/\mathbb{Q}(\sqrt{p})) \\ \Big| & & \Big| \\ \mathbb{Q} & \longleftarrow & Gal(\mathbb{Q}_p/\mathbb{Q}) \end{array}$$

The Artin map which we need to consider is $\left(\frac{K/\mathbb{Q}}{*}\right)$. However, from the properties of the Frobenius automorphism, we know that $\left(\frac{K/\mathbb{Q}}{*}\right) = \left(\frac{L/\mathbb{Q}}{*}\right)\Big|_K$, so we compute $\left(\frac{L/\mathbb{Q}}{*}\right)$ instead.

Lemma . *Let $m > 0$, q a prime with $q \nmid m$, and $\mathcal{Q}$ a prime of $\mathbb{Q}_m$ lying above q. Then the m-th roots of unity are distinct modulo $\mathcal{Q}$.*

Proof. Let ζ_m be a primitve m-th root of unity. Then

$$X^m - 1 = \prod_{j=0}^{m-1}(X - \zeta_m^j)$$

implies

$$X^{m-1} + \cdots + X + 1 = \prod_{j=1}^{m-1}(X - \zeta_m^j)$$

and hence

$$m = \prod_{j=1}^{m-1}(1 - \zeta_m^j).$$

If $\zeta_m^j \equiv \zeta_m^k \pmod{\mathcal{Q}}$, then $(1 - \zeta_m^l) \equiv 0 \pmod{\mathcal{Q}}$ for some l, hence $(m, \mathcal{Q}) \neq 1$. Since $\mathcal{Q}$ is prime, we have $\mathcal{Q} \mid m\mathcal{O}$ and hence $m\mathcal{O} \subset \mathcal{Q}$. Thus $m \in \mathcal{Q} \cap \mathbb{Z} = q\mathbb{Z}$ which implies $q \mid m$, a contradiction. □

Now let $\sigma : I_{\mathbb{Q}}^{mp^\infty} \to Gal(\mathbb{Q}_m/\mathbb{Q})$ be the Artin map, and denote by σ_a the automorphism $\sigma(a) \in Gal(\mathbb{Q}_m/\mathbb{Q})$ characterized by $\sigma_a(\zeta_m) = \zeta_m^a$. σ_q is the element of the Galois group, $Gal(\mathbb{Q}_m/\mathbb{Q})$, which satisfies $\sigma_q(x) \equiv x^q \pmod{\mathcal{Q}}$ for all $x \in \mathbb{Z}[\zeta_m]$. In

particular, $\sigma_q(\zeta_m) \equiv \zeta_m^q \pmod{\mathcal{Q}}$, and since every automorphism of $Gal(\mathbb{Q}_m/\mathbb{Q})$ is characterized by $\tau(\zeta_m) = \zeta_m^a$ for some a, we have by the lemma that $\sigma_q(\zeta_m) = \zeta_m^q$.

Theorem . *The following are equivalent:*

1. $\left(\frac{p}{q}\right) = 1$.
2. $X^2 - X + \dfrac{1-p}{4} \equiv 0 \pmod{q}$ *is solvable.*
3. q *splits in* $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}\Big(\dfrac{1+\sqrt{p}}{2}\Big)$.
4. $\left(\frac{K/\mathbb{Q}}{q}\right) = 1$.
5. $\left(\frac{q}{p}\right) = 1$.

Proof. The equivalence of (1) and (2) can be seen directly. If $\left(\frac{p}{q}\right) = 1$, then $p \equiv \alpha^2 \pmod{q}$ for some $\alpha \in \mathbb{Z}$. $X \equiv \dfrac{1+\alpha}{2} \pmod{q}$ solves $X^2 - X + \dfrac{1-p}{4} \equiv 0 \pmod{q}$. Conversely, if $X^2 - X + \dfrac{1-p}{4} \equiv (X-\alpha)(X-\beta) \pmod{q}$, then $(\alpha-\beta)^2 \equiv p \pmod{q}$, hence $\left(\frac{p}{q}\right) = 1$. Note that this is really pretty obvious if we think of $\alpha, \beta \equiv \frac{1\pm\sqrt{p}}{2}$, the real roots of the quadratic.

The equivalence of (2) and (3) is a consequence of the Dedekind-Kummer theorem.

Theorem (Dedekind-Kummer)**.** *Let A be a Dedekind domain with quotient field K, let E/K be a finite separable extension, and let B be the integral closure of A in E. Suppose that $B = A[\alpha]$ for some $\alpha \in E$ and let $f(X)$ be the irreducible polynomial for α over K. Let $\mathfrak{p}$ be a prime ideal of A. Let $\overline{f(X)}$ denote the reduction of $f(X)$ modulo $\mathfrak{p}$. Suppose*

$$\overline{f(X)} = \overline{P_1(X)}^{e_1} \cdots \overline{P_g(X)}^{e_g}$$

is the factorization of $f(X)$ modulo $\mathfrak{p}$ into powers of distinct monic irreducible polynomials in $(A/\mathfrak{p})[X]$. Let $P_i(X) \in A[X]$ be a monic polynomial in $A[X]$ which reduces mod $\mathfrak{p}$ to $\overline{P_i(X)}$. Let $\mathfrak{P}_i$ be the ideal of B generated by $\mathfrak{p}$ and $P_i(\alpha)$. Then $\mathfrak{P}_i$ is a prime ideal of B lying above $\mathfrak{p}$, e_i is the ramification index, the $\mathfrak{P}_i$'s are distinct, and

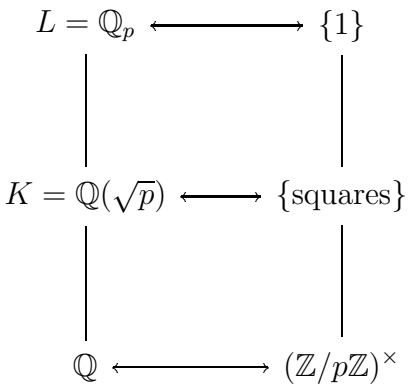
$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

is the factorization of $\mathfrak{p}$ in B.

We merely note that the roots of $X^2 - X + \frac{1-p}{4}$ are $\frac{1\pm\sqrt{p}}{2}$ which generate the ring of integers of $\mathbb{Q}(\sqrt{p})$. For the converse, observe that if $X^2 - X + \frac{1-p}{4}$ was irreducible mod q, then q would be inert in $\mathbb{Q}(\sqrt{p})$.

The equivalence of (3) and (4) is an elementary property of the Frobenius automorphism.

The equivalence of (4) and (5) is where the fun is. Recall that for any integer a not divisible by p, we denote by σ_a the automorphism $\left(\frac{L/\mathbb{Q}}{a}\right)$ of $Gal(\mathbb{Q}_p/\mathbb{Q})$. From above, we know that $\sigma_a(\zeta_p) = \zeta_p^a$, and from elementary properties of the Frobenius that $\sigma_a|_K = \left(\frac{K/\mathbb{Q}}{a}\right)$. The map $a \leftrightarrow \sigma_a$ gives the isomorphism between $(\mathbb{Z}/p\mathbb{Z})^\times$ and $Gal(\mathbb{Q}_p/\mathbb{Q})$. Consider the diagram modified from above:



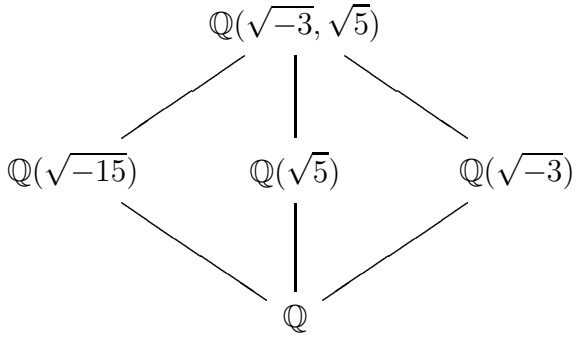
By the Galois correspondence,

$$Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \cong Gal(\mathbb{Q}_p/\mathbb{Q})/Gal(\mathbb{Q}_p/\mathbb{Q}(\sqrt{p})) \cong (\mathbb{Z}/p\mathbb{Z})^\times/\{\text{squares}\}$$

Now (4) is true if and only if $\sigma_q|_K = 1$ in $Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$, hence if and only if $\sigma_q \in Gal(\mathbb{Q}_p/\mathbb{Q}(\sqrt{p}))$, hence under the correspondence above if and only if $q \in \{\text{squares}\}$ if and only if (5). □

5. **Examples of Hilbert Class Fields**

1. $K = \mathbb{Q}$. Then $\tilde{K} = \mathbb{Q}$ since any proper extension of $\mathbb{Q}$ is ramified (as a consequence of Minkowski's bound on the discriminant).
2. $K = \mathbb{Q}(\sqrt{-15})$. Then $\tilde{K} = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$. To see this we need to do a little work. Let $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ and consider the tower of fields:



First, we show that L/K is an unramified extension of fields. Consider the infinite primes first. Since both primes of K are complex, there can be no ramification from K to L at the infinite places. Observe that $\Delta_{K/\mathbb{Q}} = -15$ hence 3 and 5 are the only primes which ramifiy in K. It is then clear that 3 and 5 ramify in L. Moreover, these are the only finite primes p of $\mathbb{Q}$ which ramify in L, since if $p \neq 3, 5$ is prime, then (by checking discriminants) p is unramified in both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$, and hence in the compositum L. Thus the only primes which can ramify from K to L are the primes in K lying above 3 and 5.

Consider a prime $\mathfrak{P}$ of L lying above 3. Note that since $L/\mathbb{Q}$ is Galois (it is the compositum of Galois extensions), it doesn't really matter which prime $\mathfrak{P}$ we choose. Let $\mathfrak{p} = \mathfrak{P} \cap K$, and $\mathfrak{p}' = \mathfrak{P} \cap \mathbb{Q}(\sqrt{5})$. We know that

$$e(\mathfrak{P}/3) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/3) = e(\mathfrak{P}/\mathfrak{p}')e(\mathfrak{p}'/3)$$

and that $e(\mathfrak{p}'/3) = 1$, $e(\mathfrak{p}/3) = 2$, and that $e(\mathfrak{P}/\mathfrak{p}') \leq [L : \mathbb{Q}(\sqrt{5})] = 2$. This implies that $e(\mathfrak{P}/\mathfrak{p}) = 1$. This together with an analogous argument for the prime 5 shows us that L/K is an unramified (necessarily abelian) extension. Thus $L \subset \tilde{K}$.

Out of the study of Dirichlet L-series come various analytic formulae for the class number of number fields (see Borevich and Shafarevich for example). The significance is that $Gal(\tilde{K}/K)$ is isomorphic to the ideal class group of K, and hence $[\tilde{K} : K] = h_K$.

If $K = \mathbb{Q}(\sqrt{-d})$ with $d > 2$ and the conductor $\mathfrak{f}_K$ of K (in the old sense – ignoring the infinite prime) is odd, then

$$h_K = \frac{1}{2 - \left(\frac{2}{d}\right)} \cdot \sum_{\substack{0<a<\mathfrak{f}_K/2 \\ (a,\mathfrak{f}_K)=1}} \left(\frac{a}{d}\right).$$

Here $\left(\dfrac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Recall that $\Delta_{K/\mathbb{Q}} = -15$, $\mathfrak{f}_K \mid \Delta_{K/\mathbb{Q}}$ and $\mathfrak{f}_K$ is divisible by every finite prime of $\mathbb{Q}$ which ramifies in K. Thus it is immediate that $\mathfrak{f}_K = 15$. It is now trivial to check that

$$h_K = \frac{1}{2 - (1)} \cdot \left[\left(\frac{1}{15}\right) + \left(\frac{2}{15}\right) + \left(\frac{4}{15}\right) + \left(\frac{7}{15}\right) \right] = 2.$$

Thus $K \subset L \subset \tilde{K}$ and $[\tilde{K} : K] = 2$ and hence $\tilde{K} = L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$, as claimed.

References

[1] D. Garbanati, Class Field Theory Summarized, *Rocky Mountain Journal of Mathematics*, **11** Number 2, (1981), 195–225.

[2] B. F. Wyman, What Is a Reciprocity Law?, *American Mathematical Monthly*, **79**, (1972), 571–586.

Department of Mathematics, Dartmouth College, Hanover, New Hampshire 03755
E-mail address: Thomas.Shemanske@dartmouth.edu