

Class field theory

Aaron Pollack

January 5, 2026

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA SAN DIEGO, LA JOLLA,
CA USA

Email address: `apollack@ucsd.edu`

Contents

Chapter 0. Overview	4
---------------------	---

CHAPTER 0

Overview

In this course, we will prove the main theorems of class field theory.

0.0.1. The Artin conjecture. To set the stage for these results, I begin by stating the Artin conjecture.

Suppose k is a number field, and K/k is a finite Galois extension with group $G = \text{Gal}(K/k)$. Suppose $\mathfrak{p}$ is a prime of k and P is a prime of K above $\mathfrak{p}$. Recall that the decomposition and inertia groups of P are determined by $\mathfrak{p}$ up to conjugacy in G .

Let $\rho : G \rightarrow \text{GL}(V)$ be a complex representation. We can define

$$L(\rho, s) = \prod_{\mathfrak{p}} \det(1 - \rho(\text{Frob}_{\mathfrak{p}}) N(\mathfrak{p})^{-s} |V^{I_{\mathfrak{p}}})^{-1}.$$

This is called the Artin L -function. It is easy to see:

LEMMA 0.0.1. *The Euler product $L(\rho, s)$ converges absolutely for $\text{Re}(s) > 1$ to define a holomorphic function in this region.*

The following conjecture is (believed to be) quite deep:

CONJECTURE 0.0.2 (Artin Conjecture). *Suppose ρ is irreducible and nontrivial. Then $L(\rho, s)$ extends to a holomorphic function of s on the entire complex plane.*

The Artin conjecture is known when $\dim(\rho) = 1$ for all k , but is already open when $k = \mathbf{Q}$ and $\dim(\rho) = 2$.

In this course, we will prove the following theorem.

THEOREM 0.0.3. *Notation as above.*

- (1) *If $\dim(\rho) = 1$, then the Artin conjecture holds.*
- (2) *In general, $L(\rho, s)$ has meromorphic continuation to the complex plane (although may have infinitely many poles.)*

In fact, the second part of the theorem follows from the first without so much difficulty, by writing an arbitrary $\rho \in \widehat{G}$ in terms of inductions of characters of subgroups. (Brauer's theorem).

0.0.2. Broad sketch. We will really focus on the first part, whose proof will be something as follows.

- (1) We will define a particularly nice class of L -functions, the **Hecke L -functions**, which come from characters of **generalized class groups** of k .
 - (a) More precisely, fix a nonzero integral ideal $\mathfrak{c}$ of k . Let $I(\mathfrak{c})$ denote the free abelian group generated by the prime ideal not dividing $\mathfrak{c}$. Let $P_{\mathfrak{c}}$ denote the subgroup of $I(\mathfrak{c})$ generated by $\alpha \in k^{\times}$ with $\alpha \equiv 1 \pmod{\mathfrak{c}}$ and $\sigma(\alpha) > 0$ for

every real embedding of k . The quotient $R(c) = I(c)/P_c$ is a generalized class group; it is finite abelian. For example, if $k = \mathbf{Q}$ and $c = m \in \mathbf{Z}_{\geq 1}$, then $R(m) = (\mathbf{Z}/m\mathbf{Z})^\times$.

- (b) Let $\chi : R(c) \rightarrow \mathbf{C}^\times$ be a character and define $L(\chi, s) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$.
- (c) Note that $L(\chi, s)$ is defined purely in terms of the arithmetic of k and *a priori* has nothing to do with Galois theory.
- (2) We will develop the basic analytic properties of the Hecke L -functions. E.g., $L(\chi, s)$ has analytic continuation to $s \in \mathbf{C}$ when $\chi \neq 1$.
- (3) Suppose now K/k is finite abelian, and c is sufficiently large (e.g., containing the ramified primes). Using the Frobenii, one defines a group homomorphism

$$I(c) \rightarrow \text{Gal}(K/k), \quad \mathfrak{p} \mapsto \text{Frob}_{\mathfrak{p}}.$$

Using that $\zeta_K(s)$ and $\zeta_k(s)$ have simple poles at $s = 1$ (which we will check), it is not so hard to show that this map is surjective.

- (4) We then prove something of a miracle: The map $I(c) \rightarrow \text{Gal}(K/k)$ factors through $R(c)$. This is called *Artin Reciprocity*. This step will *use* the properties of the Hecke L -functions that we developed above, along with lots of other results that we will develop. It follows that the Artin L -functions with $\dim(\rho) = 1$ are Hecke L -functions, completing the proof of the first part of the Theorem.
- (5) Going further, we will actually classify the abelian extensions of k in terms of generalized class groups of k .

The last three steps are called **Class field theory**. Along the way, we will develop a lot of technique that is useful for number theory.

0.0.3. Some context. One corollary of CFT is:

THEOREM 0.0.4 (Kronecker-Weber). *Suppose $K/\mathbf{Q}$ is finite abelian. Then $K \subseteq \mathbf{Q}(\zeta_m)$ for some positive integer m .*

To get a sense of the results of CFT, let us warm up with quadratic extensions of $\mathbf{Q}$ and quadratic reciprocity.

EXAMPLE 0.0.5. Suppose $a \in \mathbf{Z}$ is not a square, and let $K = \mathbf{Q}(\sqrt{a})$. If p is an odd prime, $p \nmid a$, then p is unramified in K . If $\left(\frac{a}{p}\right) = -1$, then p is inert in K , and if $\left(\frac{a}{p}\right) = 1$ then p splits in K . In particular, the map

$$I(2a) \rightarrow \text{Gal}(K/\mathbf{Q}), p \mapsto \text{Frob}_p$$

is exactly

$$p \mapsto \left(\frac{a}{p}\right) \in \mu_2 \simeq \text{Gal}(K/\mathbf{Q}).$$

The “miracle” eluded to above is that this map only depends on congruence conditions for p . Indeed, we know from quadratic reciprocity that $\left(\frac{a}{p}\right)$ only depends on the class of $p \in (\mathbf{Z}/4a\mathbf{Z})^\times$.

Let’s look at a similar example. A simple, general way to construct finite abelian extension K/k is by using Kummer theory: Assume $\mu_n \subseteq k$ and $K = k(a^{1/n})$ for some $a \in k^\times$.

Then $\text{Gal}(K/k)$ is cyclic, of order dividing n : The map $\text{Gal}(K/k) \rightarrow \mu_n$ given by

$$\sigma \mapsto \frac{\sigma(a^{1/n})}{a^{1/n}}$$

is a well-defined, injective group homomorphism.

EXAMPLE 0.0.6. Let's take $k = \mathbf{Q}(\mu_3)$ and $K = k(q^{1/3})$ for a rational prime q congruent to 2 modulo 3. Then $\text{Gal}(K/k)$ is a cyclic group of order 3.

Similar to the previous example, suppose π be a prime of k , relatively prime to $3q$, and suppose we'd like to determine whether q is a cube modulo π , as π varies. Note that $\mathbf{O}_k/\pi^\times$ has size $N(\pi) - 1$, which is divisible by 3, for example because it contains μ_3 . Because this group is cyclic, we can define a cubic Legendre symbol as $\left(\frac{q}{\pi}\right) = \zeta$, where ζ is the unique cube root of unity with $\zeta \equiv q^{(N(\pi)-1)/3}$.

On the other hand, q is a cube modulo π exactly when π splits in K/k , because in this case the polynomial $x^3 - q \in \mathbf{O}_k[x]$ has a root in $\mathbf{O}_k/\pi$. In other words:

$$\left(\frac{q}{\pi}\right) = 1 \iff \text{Frob}_\pi = 1 \in \text{Gal}(K/k).$$

More precisely, identifying $\text{Gal}(K/k)$ with μ_3 from Kummer theory, $\left(\frac{q}{\pi}\right) = \text{Frob}_\pi$. Indeed:

$$\zeta q^{1/3} = \text{Frob}_\pi(q^{1/3}) \equiv (q^{1/3})^{N(\pi)} \pmod{\pi}$$

so $\zeta \equiv q^{(N(\pi)-1)/3} \pmod{\pi}$. But now Artin reciprocity implies that $\left(\frac{q}{\pi}\right)$ only depends upon the class of $\pi \in (\mathbf{O}_k/3q)^\times$. This latter fact was proved by Eisenstein, and goes by the name of *cubic reciprocity*.

Another highlight theorem we will prove along the way is the Chebotarev density theorem. To define it, if T is a subset of the primes of k , define the Dirichlet density of T as

$$\delta(T) = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in T} N(\mathfrak{p})^{-s}}{\sum_{\text{all } \mathfrak{p}} N(\mathfrak{p})^{-s}} = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in T} N(\mathfrak{p})^{-s}}{\log((s-1)^{-1})}$$

if the limit exists.

THEOREM 0.0.7 (Chebotarev density theorem). *Suppose K/k is finite Galois with group G , not necessarily abelian. Let $C \subseteq G$ be a conjugacy class and $T(C)$ the unramified primes $\mathfrak{p}$ of k with $\text{Frob}_\mathfrak{p} \in C$. Then the Dirichlet density $\delta(T(C))$ exists and is equal to $\frac{\#C}{\#G}$.*

Note that when $k = \mathbf{Q}$, $K = \mathbf{Q}(\zeta_m)$, then $G = (\mathbf{Z}/m\mathbf{Z})^\times$ and Frob_p is the class $p + m\mathbf{Z}$ in G . Thus the Chebotarev density theorem is a generalization of Dirichlet's theorem that there are infinitely many primes p in any fixed residue class in $(\mathbf{Z}/m\mathbf{Z})^\times$.

0.0.4. Sources. There are different ways to prove the main theorems of CFT. I will roughly follow the argument in *Algebraic Number Theory*, second edition, by Serge Lang, but deviate from it in some non-trivial ways. For a different perspective on the proofs, see e.g., Kiran's notes on his website <https://kskedlaya.org/cft/root-1-2-2.html> and/or Milne's notes on Class field theory <https://www.jmilne.org/math/CourseNotes/cft.html>.