Class Field Theory Motivation

Caroline Nunn

Class field theory is the study of abelian extensions of number fields. We begin our study of abelian extensions with an observation linking the Galois group of an extension with local information at an unramified prime. Throughout this article, we use the notation $\mathcal{O}_K$ to denote the ring of integers of a number field K and $\kappa_\mathfrak{p}$ to denote the residue field at a prime $\mathfrak{p}$.

Let L/K be a finite Galois extension of number fields and let $\mathfrak{P}$ be a prime of L which is unramified over a prime $\mathfrak{p}$ of K. Recall the following definitions. The subgroup $Z_\mathfrak{P}$ of $\mathrm{Gal}(L/K)$ consisting of those elements which fix $\mathfrak{P}$ is called the decomposition group of $\mathfrak{P}$ over K. There is a surjective homomorphism $Z_\mathfrak{P} \to \mathrm{Gal}(\kappa_\mathfrak{P}/\kappa_\mathfrak{p})$ obtained by allowing elements of $Z_\mathfrak{P}$ act on the residue field $\kappa_\mathfrak{P}$. The kernel of this homomorphism is denoted $I_\mathfrak{P}$ and is called the inertia group of $\mathfrak{P}$ over K. The inertia group is trivial if and only if $\mathfrak{P}$ is unramified over $\mathfrak{p}$, so in our case the map $Z_\mathfrak{P} \to \mathrm{Gal}(\kappa_\mathfrak{P}/\kappa_\mathfrak{p})$ is an isomorphism.

Because $\kappa_\mathfrak{P}$ and $\kappa_\mathfrak{p}$ are both finite fields, the Galois group $\mathrm{Gal}(\kappa_\mathfrak{P}/\kappa_\mathfrak{p})$, is cyclic, generated by the Frobenius map $x \mapsto x^q$ where $q = |\kappa_\mathfrak{p}|$. Thus we have shown that $Z_\mathfrak{P}$ is cyclic, generated by the unique automorphism $\sigma_\mathfrak{P}$ determined by the relation

$$\sigma_\mathfrak{P}(x) \equiv x^q \pmod{\mathfrak{P}}.$$

In general, there will be many primes lying over a given prime $\mathfrak{p}$ of K, and the automorphism we obtain depends on which of these prime we choose. Specifically, let $\tau \in \mathrm{Gal}(L/K)$. Then by the definition of $\sigma_\mathfrak{P}$, we have for all $x \in L$ that $\sigma_\mathfrak{P}\tau^{-1}x \equiv (\tau^{-1}x)^q \pmod{\mathfrak{P}}$ and therefore $\tau\sigma_\mathfrak{P}\tau^{-1}x \equiv x^q \pmod{\tau\mathfrak{P}}$. Thus $\tau\sigma_P\tau^{-1}$ satisfies the relationship that uniquely determines $\sigma_{\tau\mathfrak{P}}$ and so

$$\sigma_{\tau\mathfrak{P}} = \tau\sigma_\mathfrak{P}\tau^{-1}.$$

Now suppose L/K is abelian. Then we may conclude that $\sigma_{\tau\mathfrak{P}} = \sigma_\mathfrak{P}$. Because $\mathrm{Gal}(L/K)$ acts transitively on the primes lying above $\mathfrak{p}$, this shows that the automorphism $\sigma_\mathfrak{P}$ depends only on the prime $\mathfrak{p}$ in K, not on the choice of prime lying above it. Thus we set $\sigma_\mathfrak{p} = \sigma_\mathfrak{P}$.

In summary, for a finite abelian extension L/K and an unramified prime $\mathfrak{p}$, we obtain an element of the Galois group $\mathrm{Gal}(L/K)$. Our hope is that if we do this for enough unramified primes, we will be able to piece together the entire Galois group.

More formally, let $\mathfrak{d}$ be the relative discriminant of L/K and let $I_\mathfrak{d}$ be the group of fractional ideals in K which are coprime to $\mathfrak{d}$. Since a prime divides the relative discriminant if and only if it is ramified, this is equivalent to taking the free abelian group generated by the unramified primes in K. Now we obtain a homomorphism $(\cdot, L/K) : I_\mathfrak{d} \to \mathrm{Gal}(L/K)$ given by

$$\prod \mathfrak{p}_i^{e_i} \mapsto \prod \sigma_{\mathfrak{p}_i}^{e_i}.$$

If this map, known as the Artin map, is surjective, and if we are able to determine its kernel, then we will be able to determine the Galois group of L/K by piecing together local information at the unramified primes. To get a feel for what to expect in the general situation, let's look at some examples.

Note that by the definition of the Artin map, an unramified prime $\mathfrak{p}$ satisfies $(\mathfrak{p}, L/K) = 1$ if and only if the residue class degree of $\mathfrak{p}$ in L/K is 1, which is true if and only if $\mathfrak{p}$ splits completely in L/K. Thus the primes in the kernel of the Artin map are exactly the primes which split completely in L/K. We will often make use of this simple observation.

Let $K = \mathbb{Q}$ and let L be the quadratic field with discriminant d. Then $\mathrm{Gal}(L/\mathbb{Q}) \simeq \{\pm 1\}$, so to determine if the Artin map is surjective, all we need to do is find a prime which does not map to the identity. By the above observation, this means we need find a prime which is inert, that is, any prime for which $\left(\frac{d}{p}\right) = -1$. Clearly such a prime exists, so the map is surjective. We'll ignore the kernel for now, since it isn't terribly interesting at this stage.

For a more involved example, we look at cyclotomic fields.

Theorem 1. *Let $K = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive mth root of unity. The Artin map induces an isomorphism*

$$I_m/P_m^+ \simeq \mathrm{Gal}(K/\mathbb{Q})$$

where

$$P_m^+ = \{(a/b) \in I_m : a \equiv b \pmod{m}, a/b > 0\}.$$

Proof. We recall a few basic facts about cyclotomic fields. The Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$; in particular, $[K : \mathbb{Q}] = \phi(m)$. The elements of $\mathrm{Gal}(K/\mathbb{Q})$ are the automorphisms τ_k determined by $\zeta \mapsto \zeta^k$ where $(k, m) = 1$. If m is a prime power, then the discriminant of $K/\mathbb{Q}$ is a power of the same prime. Therefore the prime factors of the discriminant of $K/\mathbb{Q}$ are exactly the prime factors of m (justifying the use of I_m for the domain of the Artin map.)

Let p be an unramified prime (equivalently, $p \nmid m$) and let $\mathfrak{p}$ be a prime of K lying above p. Then the automorphism $\tau_p \in \mathrm{Gal}(K/\mathbb{Q})$ satisfies

$$\tau(x) \equiv x^p \pmod{\mathfrak{p}}.$$

This relation uniquely determines the automorphism σ_p defined above, so we find $\sigma_p = \tau_p$.

To show that the Artin map is surjective, let k be an integer with $(k, m) = 1$. Assume without loss of generality that k is positive and factor k as $p_1^{e_1} \cdots p_r^{e_r}$. Then $\tau_k = (\sigma_{p_1})^{e_1} \cdots (\sigma_{p_r})^{e_r}$ is in the image of the Artin map.

Let $(a/b) \in P_m^+$, where we again assume that $a/b > 0$. Then by the above, $((a/b), K/\mathbb{Q}) = \tau_a \tau_b^{-1}$. Since, by definition, $a \equiv b \pmod{m}$, we conclude that $\tau_a \tau_b^{-1} = 1$ and so $P_m^+ \subseteq \ker(\cdot, K/\mathbb{Q})$.

We define a homomorphism $\phi : I_m \to (\mathbb{Z}/m\mathbb{Z})^\times$ by $\phi(a/b) = ab^{-1} \pmod{m}$, where we choose a/b to be the positive generator of this fractional ideal. This homomorphism is clearly surjective and has kernel P_m^+. So $I_m/P_m^+ \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. In particular, $[I_m : P_m^+] = \phi(m)$. Since $P_m^+ \leq \ker(\cdot, K/\mathbb{Q}) \leq I_m$ and $[I_m : \ker(\cdot, K/\mathbb{Q})] = \phi(m)$, we conclude that $\ker(\cdot, K/\mathbb{Q}) = P_m^+$. □

This result can easily be extended to extensions of $\mathbb{Q}$ which are subfields of cyclotomic fields.

Corollary 2. *Let $K = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive mth root of unity and let E be a subfield of K. There is a group H with $P_m^+ \leq H \leq I_m$ such that the Artin map induces an isomorphism*

$$I_m/H \simeq \mathrm{Gal}(E/\mathbb{Q}).$$

Proof. The Artin map factors as

$$\begin{array}{ccc} I_m & \xrightarrow{(\cdot\, K/\mathbb{Q})} & \mathrm{Gal}(K/\mathbb{Q}) \\ & \searrow^{(\cdot\, E/\mathbb{Q})} & \downarrow \pi \\ & & \mathrm{Gal}(E/\mathbb{Q}) \end{array}$$

where the vertical map is the quotient map. Thus the map $(\cdot, E/\mathbb{Q})$ surjects, and $\ker(\cdot, E/\mathbb{Q})$ contains $\ker(\cdot, K/\mathbb{Q}) = P_m^+$. □

Readers familiar with the Kronecker-Weber theorem will know that this completely determines the situation for general abelian extensions of $\mathbb{Q}$. In any case, we have now shown surjectivity and have a good description of the kernel of the Artin map for a large class of abelian extensions of $\mathbb{Q}$. In particular, we saw how in this class, the global Frobenius maps obtained from unramified primes generate the entire Galois group of the extension.

We now state the main results of class field theory. Let K be a number field $\mathfrak{m}$ be an integral ideal in K. We define $P_{\mathfrak{m}}^+$ to be the subgroup of $I_{\mathfrak{m}}$ generated by principal ideals with a generator α satisfying $\alpha \equiv 1 \pmod{m}$ and $\sigma(\alpha) > 0$ for ever real embedding $\sigma : K \to \mathbb{R}$. We observe that this agrees with the definition we gave earlier for P_m^+ when $\mathfrak{m} = (m)$ with $m \in \mathbb{Z}$.

Theorem 3 (Artin Reciprocity)**.** *Let L/K be a finite abelian extension of number fields. There exists an ideal $\mathfrak{f}$ of K such that*

1. *A prime $\mathfrak{p}$ in K ramifies if and only if $\mathfrak{p} \mid \mathfrak{f}$.*
2. *Let $\mathfrak{m}$ be an ideal with $\mathfrak{f} \mid \mathfrak{m}$. Then there is a group H with $P_{\mathfrak{m}}^+ \leq H \leq I_{\mathfrak{m}}$ such that the Artin map induces an isomorphism*

$$I_{\mathfrak{m}}/H \simeq \mathrm{Gal}(L/K).$$

In fact, there is a minimal ideal satisfying these conditions, which we call the conductor of the extension L/K. The conductor of a cyclotomic field $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$ is (m), and if $E/\mathbb{Q}$ is a subextension of a cyclotomic field, the conductor is the smallest m such that $E \subseteq \mathbb{Q}(\zeta_m)$.

Theorem 4 (Takagi existence theorem)**.** *Let K be a number field, let $\mathfrak{m}$ be an ideal of K, and let H be a group with $P_{\mathfrak{m}} \leq H \leq I_{\mathfrak{m}}$. Then there is a unique abelian extension L/K which is ramified only at primes dividing $\mathfrak{m}$ such that the Artin map induces an isomorphism*

$$I_{\mathfrak{m}}/H \simeq \mathrm{Gal}(L/K).$$

For the case $K = \mathbb{Q}$, the existence part of this theorem follows from Theorem 1 and Corollary 2. Uniqueness is not difficult – by the definition of the Artin map, a prime ideal in K splits completely in an extension L if and only if it is in the kernel of the Artin map. So two extensions satisfying the conclusion of this theorem must split completely at the same primes. Then the following analytic result (whose proof we omit) together with the following corollary show that these extensions are in fact the same.

Theorem 5. *Let K be a number field. Then the density of primes which split completely is $1/[K : \mathbb{Q}]$.*

Corollary 6. *Let K and L be finite Galois extensions of $\mathbb{Q}$. Let S be the set of primes which split completely in L but not in K. Then S has density zero if and only if $K \subseteq L$.*

Proof. If L is an extension of K, then every prime which splits completely L splits completely in K, so $S = \emptyset$. Conversely, suppose S has density zero. Let S_K, S_L, and S_{KL} be the sets of primes which split completely in K, L, and KL respectively. Then $S_{KL} = S_K \cap S_L$, so S_{KL} differs from S_L by a set of density zero. Then by the previous theorem, $[KL : \mathbb{Q}] = [L : \mathbb{Q}]$, whence $KL = L$. □

This result holds more generally for Galois extensions of arbitrary number fields, and, together with Artin reciprocity, is the basis for the next major result of class field theory.

Theorem 7 (Completeness)**.** *Let K be a number field and let L_1 and L_2 be finite abelian extensions with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$ respectively. Let $\mathfrak{m} = \mathfrak{f}_1\mathfrak{f}_2$ and let H_1 and H_2 be the subgroups of $I_\mathfrak{m}$ corresponding to L_1 and L_2. Then*

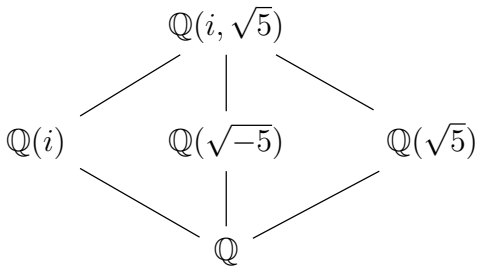
$$H_1 \subseteq H_2 \iff K_2 \subseteq K_1.$$

Together, Artin reciprocity, the Takagi existence theorem, and the completeness theorem show that there is a one-to-one correspondence between abelian extensions of a number field whose conductor divides a given ideal $\mathfrak{m}$ and subgroups of $I_\mathfrak{m}/P_\mathfrak{m}^+$. Furthermore, this correspondence can be identified in a natural way with the usual Galois correspondence of extensions. This is the main content of class field theory.

We give a brief application of class field theory. Recall that for a prime p, the equation $x^2 + y^2 = p$ has integer solutions according to whether or not the prime p is equivalent to 1 mod 4. In general, given an integer d, can we give a condition for which primes p there is an integer solution to $x^2 + dy^2 = p$ via a congruence modulo some integer? We do two examples illustrative of the general case.

Proposition 8. *Let p be a prime with $p \nmid 20$. The equation $x^2 + 5y^2 = p$ has solutions if and only if $p \equiv 1$ or $p \equiv 9$ (mod 20).*

Proof. Let $K = \mathbb{Q}(\sqrt{-5})$ and let L be the maximal unramified abelian extension of K, which by class field theory we know is a quadratic extension of K (because the class number is 2.) In fact, we can calculate K explicitly by looking at the following tower of fields.



By discriminant considerations, the extension $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}$ is ramified only at 2 and 5. These are also the primes at which $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ is ramified, both with ramification index 2. Now 2 is inert in $\mathbb{Q}(\sqrt{5})$ and therefore has residue class degree 2, so the ramification index and residue class degree of 2 for $\mathbb{Q}(i,\sqrt{5})$ are both at least 2, so they are both 2. Similarly, 5 splits completely in $\mathbb{Q}(i)$, so we find the ramification index of 5 for $\mathbb{Q}(i,\sqrt{5})$ is 2. So $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(\sqrt{-5})$ is unramified. Since it has the correct degree, we find $L=\mathbb{Q}(i,\sqrt{5})$.

For a prime $p \nmid 20$, the equation $x^2+5y^2=p$ has an integer solution if and only if (p) splits into two principal ideals (since a solution produces a principal ideal $(x+y\sqrt{-5})$ with norm p and vice versa.) The kernel of the Artin map $(\cdot, L/K)$ is the group of principal ideals in K, so a prime $\mathfrak{p}$ of K lying over p is principal if and only if $(\mathfrak{p}, L/K)=1$, which is true if and only if $\mathfrak{p}$ splits completely in L. Now since $L/\mathbb{Q}$ is Galois, the condition that p splits completely in K and the primes above p split completely in L is equivalent to the condition that p splits completely in L. Thus we have reduced the problem to finding which primes of $\mathbb{Q}$ split completely in L.

Note that i is a fourth root of unity, so $\mathbb{Q}(i)$ is a cyclotomic field. We also calculate $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$. (There are several ways to calculate this. We can do it explicitly, or by noting that the primes that split in $\mathbb{Q}(\zeta_5)$ also split in $\mathbb{Q}(\sqrt{5})$ and then using either Corollary 6 or the completeness theorem.) Taking composites, we see that $L \subseteq Q(\zeta_{20})$ and is in fact the unique biquadratic subfield thereof, corresponding to the subgroup $\{1,9\}$ of $(\mathbb{Z}/20\mathbb{Z})^\times$. The result then follows from Corollary 2. □

Proposition 9. *There is no integer such that a set of congruences modulo that integer characterizes which primes p have a solution to $x^2+23y^2=p$.*

Proof. As before, let $K=\mathbb{Q}(\sqrt{-23})$ and let L be the maximal unramified abelian extension of K, which this time should be a cubic extension. First we show that $L/\mathbb{Q}$ is Galois. Let τ denote complex conjugation. Then $\tau(L)=L$ since $\tau(L)$ is also an unramified abelian extension of K of the same degree as L. Then for any $\sigma \in \mathrm{Gal}(L/K)$, the map $\sigma\tau$ is an element of $\mathrm{Aut}_{\mathbb{Q}}(L)$ that does not fix K. Then $\#\,\mathrm{Aut}_{\mathbb{Q}}(L) = 2\#\,\mathrm{Gal}(L/K) = [L:\mathbb{Q}]$ as desired.

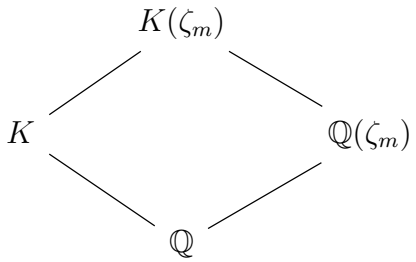
Therefore we have an exact sequence

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1.$$

Because $\mathrm{Gal}(L/K)$ is abelian, there is a well defined action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Gal}(L/K)$ given by conjugating an element of $\mathrm{Gal}(L/K)$ by a lift of an element of $\mathrm{Gal}(K/\mathbb{Q})$. Let τ denote complex conjugation, which we may take to be the lift of the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Then if $\mathfrak{p}$ is a prime of K and $\sigma_{\mathfrak{p}}$ is the corresponding global Frobenius element, we find

$\sigma_{\tau\mathfrak{p}} = \tau\sigma_{\mathfrak{p}}\tau^{-1}$. Now note that since in a quadratic field we have $\mathfrak{p}(\tau\mathfrak{p}) = (N\mathfrak{p})$ is principal, this implies that $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Gal}(L/K)$ by inversion, showing that $\mathrm{Gal}(L/\mathbb{Q})$ is the non-abelian group S_3.

On the other hand, suppose there is some integer m and some subset $H \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ such that for all but finitely many primes p, the equation $x^2 + 23y^2 = p$ has a solution if and only if $p \in H \pmod{m}$. By the same argument as before, p splits completely in L if and only if $p \in H \pmod{m}$. Consider the tower of fields



Let p be a prime that splits completely in $K(\zeta_m)$. Then p splits completely in $\mathbb{Q}$, so $p \equiv 1 \pmod{m}$. On the other hand, p also splits completely in K, so we find $p \in H \pmod{m}$. Therefore $1 \in H$ and so by Corollary 6, we find $K \subseteq \mathbb{Q}(\zeta_m)$. So $K/\mathbb{Q}$ is abelian, a contradiction. □

References

[1] Nancy Childress. *Class Field Theory*. Springer, 2009.

[2] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[3] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 2nd edition, 1997.