# Class Field Theory

Linus Setiabrata

Lecture 5. Mar 17, 2019
(Updated Nov 11, 2019)

The goal for today is to formulate the Artin reciprocity law. Jessie already did part of this section so I have the luxury of going slowly. I hope to shove fewer-than-usual many things under the rug, but that means I probably won't get to Chapter 6 today.

I've talked about this once before, but let's go over it again. Suppose $K/\mathbb{Q}$ is an abelian extension. By Kronecker-Weber, we have $K \subseteq \mathbb{Q}(\zeta_m)$ for some $m$. The minimal such $m$ for which this holds is called the conductor of $K$, and from now on $m$ will denote the conductor of $K/\mathbb{Q}$.

We get a surjective homomorphism

$$\begin{aligned} \varphi\colon \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) &\twoheadrightarrow \operatorname{Gal}(K/\mathbb{Q}) \\ \sigma &\mapsto \sigma|_K, \end{aligned}$$

also known as a surjective homomorphism

$$\begin{aligned} \varphi\colon (\mathbb{Z}/m\mathbb{Z})^\times &\twoheadrightarrow \operatorname{Gal}(K/\mathbb{Q}) \\ r &\mapsto \{\zeta_m \mapsto \zeta_m^r\}|_K. \end{aligned}$$

[$\star$The fact that $\sigma|_K$ is an automorphism of $K$ is guaranteed to us because $(\mathbb{Z}/m\mathbb{Z})^\times$ is abelian, hence all subgroups are normal.$\star$]

In fact, we can find this homomorphism in another way. Suppose $p \nmid m$; since $K$ is unramified above $p$ we have the automorphism $\{x \mapsto x^p \pmod{\mathfrak{p}}\} =: \operatorname{Frob}_p \in \operatorname{Gal}(K/\mathbb{Q})$. Now let $S_m$ denote the subgroup of $\mathbb{Q}$ generated by all primes not dividing $m$. We can extend the map $p \mapsto \operatorname{Frob}_p \in \operatorname{Gal}(K/\mathbb{Q})$ to a homomorphism $S_m \to \operatorname{Gal}(K/\mathbb{Q})$ by multiplicativity. So for example, with $m = 3$, the element $2/5 \mapsto \operatorname{Frob}_2 \operatorname{Frob}_5^{-1}$ (or $\operatorname{Frob}_5^{-1} \operatorname{Frob}_2$; it doesn't matter since $\operatorname{Gal}(K/\mathbb{Q})$ is abelian!). This is called the Artin map of $K/\mathbb{Q}$.

**Proposition 1.** *Let $\varphi$ be the projection defined above. As automorphisms of $K/\mathbb{Q}$, we have $\varphi(r) = \operatorname{Frob}_p$ if and only if $r \equiv p \pmod{m}$.*

*Proof.* If $r \equiv p \pmod{m}$ then $(\varphi(r))(1) = \operatorname{Frob}_p(1)$ and

$$(\varphi(r))(\zeta_m) = \zeta_m^r = \zeta_m^p \equiv \operatorname{Frob}_p(\zeta_m) \pmod{\mathfrak{p}},$$

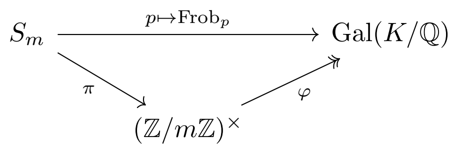
so $\varphi(r) = \operatorname{Frob}_p$.

Now suppose that $\varphi(r) = \operatorname{Frob}_p$. So in particular $\zeta_m^r \equiv \zeta_m^p \pmod{\mathfrak{p}}$ for some prime $\mathfrak{p}$ above $p$. This says that $\zeta_m^r(1 - \zeta_m^{p-r}) \in \mathfrak{p} \subseteq \mathcal{O}_K$; I want to claim that $r \equiv p \pmod{m}$. One way of seeing this is via machinery whack (I don't know how else to do it, but I bet this isn't necessary): go up to $\mathfrak{P} \subseteq \mathbb{Z}[\zeta_m]$ over $\mathfrak{p}$ to get rid of $\zeta_m^r$, and then if $p \not\equiv r \pmod{m}$ write $1 - \zeta_m^{p-r} = 1 - \zeta_d^k$ where $(d, k) = 1$, and use Proposition 2.8 in Washington's book. □

The punchline is that the Artin map of $K/\mathbb{Q}$, a priori from $S_m \subseteq \mathbb{Q}$ to $\mathrm{Gal}(K/\mathbb{Q})$, actually factors through $\varphi$. Namely, consider the projection

$$\pi\colon S_m \to (\mathbb{Z}/m\mathbb{Z})^\times$$
$$\prod_{i=1}^{n} p_i^{e_i} \mapsto \prod_{i=1}^{n} p_i^{e_i}$$

where the $e_i$ should be interpreted the way they're interpreted, e.g. if $m = 6$ we have $\pi(7/13) \mapsto 1$. Then we have the commutative diagram




This follows because we checked that the diagram commutes on the generators of $S_m$; this is Proposition 1. The homomorphism-ness of everything takes care of the rest.

Let me remark that not much math was done here. A lot of it was setup, we applied Kronecker-Weber to get this magical number $m$, and a relatively silly Proposition 1 gave us some result about how Frobs behave.

The Artin reciprocity law is a generalization of this to arbitrary abelian extensions $L/K$. But the relevant generalization of Kronecker-Weber is unknown so we don't instantly get the magical quantity $m$, and there are other complicating factors (e.g. the ring of integers of the base field is not always a PID). But for now none of these matter because I only need to state Artin reciprocity :)

Fix a number field $K$ (as a running example, the above considerations corresponded to $K = \mathbb{Q}$).

Let $\mathfrak{m}$ be a formal product of places of $K$ (as a running example, let $\mathfrak{m} = (m)\infty$, so an integer $m$ along with the real infinite place $\infty$ corresponding to the unique $\mathbb{Q} \hookrightarrow \mathbb{R}$).

Let $I_K^{\mathfrak{m}}$ be the group of fractional ideals of $K$ which are coprime to each finite place of $K$ occurring in $\mathfrak{m}$ (in our running example, $I_{\mathbb{Q}}^{m} = S_m$ defined earlier).

Let $P_K^{\mathfrak{m}} \subseteq I_K^{\mathfrak{m}}$ be the group of principal fractional ideals generated by $\alpha \in K$ such that for $\mathfrak{p}^e | \mathfrak{m}$ finite, $\alpha \equiv 1 \pmod{\mathfrak{p}^e}$, and for every real place $\tau$ in $\mathfrak{m}$, we have $\tau(\alpha) > 0$ (in our example, we are modding out by those $\langle\alpha\rangle$ with $\alpha \equiv 1 \pmod{m}$ and $\alpha > 0$).

**Definition 2.** The **ray class group**, denoted $\mathrm{Cl}^{\mathfrak{m}}(K)$ is the quotient $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. A quotient of a ray class group is called a **generalized ideal class group**.

The usual ideal class group is obtained when $\mathfrak{m}$ is the empty product of places, and in general for any $\mathfrak{m}$, the ideal class group is a quotient of $\mathrm{Cl}^{\mathfrak{m}}(K)$.

In our running example, $\mathrm{Cl}^{\mathfrak{m}}(K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Indeed, every $p^{-1} \in S_m$ is equivalent, in $\mathrm{Cl}^{\mathfrak{m}}(K)$, to the element $p^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Now let $L/K$ be an abelian extension, let $\mathfrak{p}$ be a prime of $K$ that doesn't ramify and $\mathfrak{q}$ a prime of $L$ above $\mathfrak{p}$; put $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ and $\mathbb{F}_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q}$. Since $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ is a finite extension of finite fields we can pull back the generator $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ which sends $x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}} \pmod{\mathfrak{q}}$.

Now if $\mathfrak{m}$ is divisible by all primes of $K$ which ramify in $L$ (e.g. let $K = \mathbb{Q}$ and $\mathfrak{m}$ be the conductor of $L$), we can define the Artin map that sends $\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}$ and extend multiplicatively to $I_K^{\mathfrak{m}}$.

**Theorem 3.** *(Artin reciprocity.) There exists a formal product* $\mathfrak{m}$ *of places of* $K$*, including all places over which* $L$ *ramifies, such that* $P_K^{\mathfrak{m}}$ *is contained in the kernel* $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$*.*

So we get a map, for some $\mathfrak{m}$, from $\mathrm{Cl}^{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$ that turns out to be surjective. So the Artin reciprocity theorem gives the magical $\mathfrak{m}$ that used to be supplied by Kronecker-Weber. It's also no longer clear to me why it's surjective (but Kedlaya punts it to an exercise).

The conductor $\mathfrak{m}$ of $L/K$ is the smallest formal product for which this Artin reciprocity holds. If $L/K$ has conductor dividing $\mathfrak{m}$, and $\mathrm{Cl}^{\mathfrak{m}}(K) \cong \mathrm{Gal}(L/K)$, then we say $L$ is the **ray class field** of $\mathfrak{m}$. For example, if $K = \mathbb{Q}$, then the ray class field of $\mathfrak{m} = (m)\infty$ is $\mathbb{Q}(\zeta_m)$ and if $\mathfrak{m} = m$ then it is $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, since $(\mathbb{Z}/m\mathbb{Z})^\times/\{1, -1\} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m + \zeta_m^{-1})/\mathbb{Q})$.

**Theorem 4.** *There exists a ray class field for any* $K$ *and* $\mathfrak{m}$*.*

On the other hand, we don't "know" what the ray class fields are, in the sense that when $K = \mathbb{Q}$, the ray class fields are simply "adjoin $\zeta_m$ or $\zeta_m + \zeta_m^{-1}$ depending on where there is $\infty$ or not". It turns out that for imaginary quadratic fields, the theory of elliptic curves with complex multiplication tells us which algebraic numbers to adjoin, and more generally Shimura extended this to CM fields (these are totally imaginary fields $L$ which have an index 2 totally real subfield $K$). In the function field case, there are these Drinfeld modules that "do something similar", whatever that means.