Class Field Theory Seminar
Week 1

Angus Chung

January 18th, 2017

1 What is Class Field Theory?

Class Field Theory is the study of abelian extensions of global fields. In our seminar, we will mainly focus on number fields, i.e. finite extensions of $\mathbb{Q}$. As a small digression, the other type of global fields is finite extensions of $\mathbb{F}_q(t)$. Indeed there is also class field theory on function fields, say elliptic curves. It is related to something called **complex multiplication**, though we will not study this in the seminar.
The name "Class Field Theory" comes as there are some correspondences between some ideal classes and abelian extensions of K. The motivation for this subject is the reciprocity laws, dated back to Gauss. One of Gauss' favorite results is his quadratic reciprocity law, stating that if p, q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

where $\left(\frac{=}{-}\right)$ is the Legendre symbol, i.e. the non-trivial quadratic character modulo q or p respectively.

2 Artin Map and Artin Symbol

Let L/K be a Galois extension of number fields, $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{q} \subset \mathcal{O}_L$ be primes with $\mathfrak{q}$ above $\mathfrak{p}$. Then we have an exact sequence relating the decomposition group, the inertia group, and the Galois group of residue fields.

$$1 \longrightarrow I(\mathfrak{q}|\mathfrak{p}) \longrightarrow D(\mathfrak{q}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \longrightarrow 1.$$

If $\mathfrak{q}$ is unramified, then the inertia group is trivial, so we have an isomorphism

$$D(\mathfrak{q}|\mathfrak{p}) \xrightarrow{\sim} \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})).$$

Since L, K are number fields, $k(\mathfrak{q})/k(\mathfrak{p})$ is an extension of finite fields. In particular, the Galois group of the residue field extension is generated by the Frobenius map $\mathrm{Frob}(x) = x^{N\mathfrak{p}}$. We can thus define the Frobenius element associated to $\mathfrak{q}/\mathfrak{p}$, $\mathrm{Frob}(\mathfrak{q}|\mathfrak{p})$ as the pull back of Frob along the isomorphism. Note that if $\mathfrak{q}$, $\mathfrak{q}'$ are distinct unramified primes above $\mathfrak{p}$, then their Frobenius are conjugates in $\mathrm{Gal}(L/K)$. Thus, if L/K is abelian and $\mathfrak{p} \subset \mathcal{O}_K$ is unramified, then $\mathrm{Frob}_\mathfrak{p}$ is well-defined in $\mathrm{Gal}(L/K)$.
We can now define the Artin symbol or the Artin map. Note that a prime $\mathfrak{p} \subset \mathcal{O}_K$ is unramified iff it is relatively prime to the discriminant $D_{L/K}$. Denote $I(D)$ to be the group of non-zero fractional ideals $\mathfrak{a}$ in K with $\nu_\mathfrak{p}(\mathfrak{a}) = 0$ for all $\mathfrak{p} \mid D_{L/K}$. This group is generated by all the prime ideals in $\mathcal{O}_K$ not dividing the discriminant, hence unramified.

Definition 2.1. Let L/K be an abelian extension. The **Artin map** is a group homomorphism

$$I(D) \longrightarrow \mathrm{Gal}(L/K)$$
$$\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}.$$

It is generally denoted by the **Artin symbol** $\left(\frac{L/K}{-}\right)$ or $\left(\frac{L}{-}\right)$ if K is understood.

3 Ray Class Group

However, mathematicians have found that it is important to take care of not only prime ideals, but also embeddings $K \hookrightarrow \mathbb{C}$. We call such embeddings **infinite primes** or **infinite places**, and prime ideals **finite primes** or **finite places**. We can talk about them uniformly, using the notion of **cycles** or **modulus**. For this section, I think Milne's [1, Chapter V] does a better job than Stevenhagen [2], so I will mainly follow Milne. (After all Stevenhagen's paper is just an overview, so he does not include proof. This makes the paper short, but we need another source for a proof.)

Definition 3.1. Let K be a number field. A **cycle** or a **modulus** $\mathfrak{m}$ of K is a formal product

$$\mathfrak{m} := \prod_{\mathfrak{p} \leq \infty} \mathfrak{p}^{m(\mathfrak{p})},$$

where

- $m(\mathfrak{p}) \in \mathbb{Z}_{\geq 0}$ for all $\mathfrak{p}$, and $m(\mathfrak{p}) = 0$ for all but finitely many primes $\mathfrak{p}$;
- $m(\mathfrak{p}) = 0$ or 1 if $\mathfrak{p}$ is a real place, i.e. an embedding $K \hookrightarrow \mathbb{R}$;
- $m(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is a complex place, i.e. not a real place.

We also write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is the finite part of $\mathfrak{m}$ (so it is an ideal in $\mathcal{O}_K$), and $\mathfrak{m}_\infty$ is the infinite part of $\mathfrak{m}$.

Given a cycle $\mathfrak{m}$, we can define an equivalence relation on $K^\times$, similar to how we define an equivalence relation modulo an ideal.

Definition 3.2. Let $\alpha, \beta \in K^\times$ and $\mathfrak{m}$ be a cycle. We define

$$\alpha \equiv \beta \pmod{{}^*\mathfrak{m}},$$

if all of the following hold.

(a) if $\mathfrak{p} \mid \mathfrak{m}_0$, i.e. $\mathfrak{p}$ is a finite place with $m(\mathfrak{p}) > 0$, then $\nu_\mathfrak{p}(\frac{\alpha}{\beta} - 1) \geq m(\mathfrak{p})$;

(b) if $\mathfrak{p} \mid \mathfrak{m}_\infty$ is an infinite place given by $\sigma : K \hookrightarrow \mathbb{C}$ (thus $\sigma : K \hookrightarrow \mathbb{R}$), then $\sigma(\frac{\alpha}{\beta}) > 0$.

Proposition 3.3. *This gives an equivalence relation on $K^\times$.*

Proof First, note that $\alpha \equiv \beta \pmod{{}^*\mathfrak{m}}$ iff $\alpha\beta^{-1} \equiv 1 \pmod{{}^*\mathfrak{m}}$. This will be used a couple of times here. Reflexivity is trivial. For symmetry, by the property above it suffices to show that $\alpha \equiv 1 \pmod{{}^*\mathfrak{m}}$ implies $1 \equiv \alpha \pmod{{}^*\mathfrak{m}}$. Suppose $\alpha \equiv 1 \pmod{{}^*\mathfrak{m}}$ and $\mathfrak{p}$ is a finite prime with $m(\mathfrak{p}) > 0$. Then $\nu_\mathfrak{p}(\alpha - 1) \geq m(\mathfrak{p}) > 0$. If $\nu_\mathfrak{p}(\alpha) > 0 = \nu_\mathfrak{p}(1)$, then $\nu_\mathfrak{p}(\alpha - 1) = \nu_\mathfrak{p}(1) = 0$, a contradiction. Thus $\nu_\mathfrak{p}(\alpha) = 0$. Now,

$$\nu_\mathfrak{p}(\alpha^{-1} - 1) = \nu_\mathfrak{p}((\alpha^{-1} - 1)(\alpha)) \geq m(\mathfrak{p}).$$

Finally for transitivity, it suffices to show that if $\alpha, \beta \equiv 1 \pmod{{}^*\mathfrak{m}}$, then $\alpha\beta \equiv 1 \pmod{{}^*\mathfrak{m}}$. To see that it suffices, note that $\alpha \equiv \beta \pmod{{}^*\mathfrak{m}}$ is equivalent to $\alpha\beta^{-1} \equiv 1 \pmod{{}^*\mathfrak{m}}$, and similarly for $\beta \equiv \gamma \pmod{{}^*\mathfrak{m}}$. We also have that $\alpha \equiv \gamma \pmod{{}^*\mathfrak{m}}$ is equivalent to $(\alpha\beta^{-1})(\beta\gamma^{-1}) = \alpha\gamma^{-1} \equiv 1 \pmod{{}^*\mathfrak{m}}$, showing that it is actually sufficient to prove our result.
Now, suppose $\alpha, \beta \equiv 1 \pmod{{}^*\mathfrak{m}}$. Then $\nu_\mathfrak{p}(\alpha - 1), \nu_\mathfrak{p}(\beta - 1) \geq m(\mathfrak{p})$. Note that

$$\nu_\mathfrak{p}(\alpha\beta - 1) = \nu_\mathfrak{p}((\alpha - 1)(\beta - 1) + (\alpha - 1) + (\beta - 1)) \geq \min\{\nu_\mathfrak{p}(\alpha - 1) \cdot \nu_\mathfrak{p}(\beta - 1), \nu_\mathfrak{p}(\alpha - 1), \nu_\mathfrak{p}(\beta - 1)\} \geq m(\mathfrak{p}),$$

since $m(\mathfrak{p}) \geq 1$ and hence all of the 3 quantities are at least $m(\mathfrak{p})$. This completes the proof. ∎
Our goal is to define the ray class group of $\mathfrak{m}$.

Definition 3.4. Define $P(\mathfrak{m}) \subset I(\mathfrak{m})$ to be the subgroup of principal fractional ideals in $I(\mathfrak{m})$.
Define $K(\mathfrak{m}) = \{\alpha \in K^\times \mid \nu_\mathfrak{p}(\alpha) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0\}$. Thus we have an obvious map $K(\mathfrak{m}) \to P(\mathfrak{m})$ sending α to (α), with kernel $\mathcal{O}_K^\times$.
Also define the **ray modulo $\mathfrak{m}$** to be

$$R(\mathfrak{m}) := \{\alpha\mathcal{O}_K \mid \alpha \equiv 1 \pmod{{}^*\mathfrak{m}}\}.$$

The **ray class group of $\mathfrak{m}$** is the quotient $Cl_\mathfrak{m} := I(\mathfrak{m})/R(\mathfrak{m})$.

We will have an exact sequence involving the ray class group of $\mathfrak{m}$, $Cl_\mathfrak{m}$, and the ideal class group Cl_K.

Proposition 3.5. *Let $S \subset \operatorname{Spec}\mathcal{O}_K$ be finite, i.e. it is a finite set of prime ideals in K. Then every ideal class in Cl_K contains an integral ideal not divisible by any prime in S.*

Proof It is done by Chinese Remainder Theorem. See [1, Ch. V Lemma 1.1].
As a corollary, fix a cycle $\mathfrak{m}$. Then $m(\mathfrak{p}) > 0$ for only finitely many primes. Thus we have a surjection

$$I(\mathfrak{m}) \longrightarrow Cl_K.$$

$I(\mathfrak{m})$ embeds into the group of all nonzero fractional ideals, which quotients out the subgroup of principal ideals to have the ideal class group. As a result, the kernel of the above map is $\mathfrak{P}(\mathfrak{m})$. Instead, we can write an exact sequence going from $K(\mathfrak{m})$ to $I(\mathfrak{m})$. Now we have proved the following proposition.

Proposition 3.6. *We have the following exact sequence:*

$$0 \longrightarrow \mathcal{O}_K^\times \longrightarrow K(\mathfrak{m}) \longrightarrow I(\mathfrak{m}) \longrightarrow Cl_K \to 0.$$

Now we quotient out the ray modulo $\mathfrak{m}$ equivalence to get $Cl_\mathfrak{m}$ from $I(\mathfrak{m})$. Look the composition of maps $K(\mathfrak{m}) \to I(\mathfrak{m}) \to Cl_\mathfrak{m}$. Pull back $R(\mathfrak{m}) \subset I(\mathfrak{m})$ to $K(\mathfrak{m})$, we get the subgroup $\{\alpha \in K^\times \mid \alpha\mathcal{O}_K \in R(\mathfrak{m})\}$. Call this $K_{\mathfrak{m},1}$ as in [1, Chapter V]. To summarize, we have the last proposition for this section.

Remark. Before we move on, in case you will be using [1, Chapter V] as a reference, his $K_\mathfrak{m}$ is our $K(\mathfrak{m})$. His $U = U_K$ is our $\mathcal{O}_K^\times$, and his $U_{\mathfrak{m},1} = U_K \cap K_\mathfrak{m}$ is our $\mathcal{O}_K^\times \cap K(\mathfrak{m})$.

Proposition 3.7. *We have the following exact sequence:*

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_{\mathfrak{m},1}) \longrightarrow K(\mathfrak{m})/K_{\mathfrak{m},1} \longrightarrow Cl_\mathfrak{m} \longrightarrow Cl_K \to 0.$$

We also have canonical isomorphisms

$$K(\mathfrak{m})/K_{\mathfrak{m},1} \xrightarrow{\simeq} \prod_{\mathfrak{p}\mid\mathfrak{m}_\infty} \{\pm 1\} \times \prod_{\mathfrak{p}\mid\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \xrightarrow{\simeq} \prod_{\mathfrak{p}\mid\mathfrak{m}_\infty} \{\pm 1\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times.$$

Thus $Cl_\mathfrak{m}$ is a finite group, with order

$$h_\mathfrak{m} = h_K \cdot [\mathcal{O}_K^\times : (\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})]^{-1} \cdot 2^r \cdot N_{K/\mathbb{Q}}(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}\mid\mathfrak{m}_0} \left(1 - \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})}\right),$$

where h_K is the class number of K and r is the number of real embeddings in $\mathfrak{m}_\infty$.

Proof We have shown the exact sequence already. For the isomorphisms, the second one is Chinese remainder theorem. So we just have to show the first one.
Define $K(\mathfrak{m}) \to \prod_{\mathfrak{p}\mid\mathfrak{m}_\infty}\{\pm 1\} \times \prod_{\mathfrak{p}\mid\mathfrak{m}_0}(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$ by sending α to $\sigma(\alpha)/|\sigma(\alpha)|$ for each $\mathfrak{p} \mid \mathfrak{m}_\infty$ given by $\sigma : K \to \mathbb{R}$, and to the quotient $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$ for each $\mathfrak{p} \mid \mathfrak{m}_0$. The latter part is well-defined (i.e. has image lying in $(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$, as $\alpha \in K(\mathfrak{m})$. This is clearly a group homomorphism. If α is mapped to 1, then $\alpha \equiv 1 \pmod{{}^*\mathfrak{m}}$ by definition. Thus the kernel of this map is $K_{\mathfrak{m},1}$, and we have the first isomorphism.
The formula for $h_\mathfrak{m}$ follows directly from the short exact sequence. ∎

4 Main Theorem of Global Class Field Theory

One last thing before the main theorem is the definition of a ramifying prime, when the prime is infinite.

Definition 4.1. Let L/K be an extension of number fields and $\mathfrak{p}$ be an infinite place on K represented by $\sigma : K \to \mathbb{C}$. We say that $\mathfrak{p}$ **ramifies** if σ is a real embedding, and there exists an extension $\tau : L \to \mathbb{C}$ that is not real.

Now we can state the main theorem.

Theorem 4.2. *Suppose L/K is an abelian extensions of number fields. Then:*

(a) There is a cycle $\mathfrak{m}$ divisible by all ramifying primes such that the Artin map factors through the ray class group $Cl_{\mathfrak{m}}$,

$$\begin{array}{ccc} I(D) & \xrightarrow{A} & \mathrm{Gal}(L/K) \\ \downarrow & \nearrow & \\ Cl_{\mathfrak{m}} & & \end{array}$$

and the map $Cl_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$, which is also called Artin map, is surjective.

(b) Among all such cycles $\mathfrak{m}$, there is a minimal such one $\mathfrak{f}(L/K)$ or simply $\mathfrak{f}$, called the **conductor** *of L/K. The conductor has the property that it acts like the discriminant. To be precise,*

(a) $\mathfrak{p} \mid \mathfrak{f}$ if and only if $\mathfrak{p}$ is ramified in L/K;

(b) $\mathfrak{p}^2 \mid \mathfrak{f}$ if and only if $\mathfrak{p}$ is wildly ramified in L/K.

(c) (Ray class field) Given a cycle $\mathfrak{m}$, there exists a **ray class field** *$H_{\mathfrak{m}} \subset K^{\mathrm{ab}}$ which is maximal in the sense $R(\mathfrak{m}) \subset \ker(A : I(D) \to \mathrm{Gal}(L/K))$, and*

$$Cl_{\mathfrak{m}} \xrightarrow{\simeq} \mathrm{Gal}(H_{\mathfrak{m}}/K).$$

Therefore, $K^{\mathrm{ab}} = \bigcup_{L/K \text{ finite abelian}} H_{\mathfrak{f}(L/K)} H_{\mathfrak{f}} \subset \overline{\mathbb{Q}}$.

5 More

We will also talk about idéles, and the main local theorem I believe. You can check the statements in [2].

References

[1] James S. Milne. Class field theory.

[2] Peter Stevenhagen. Class field theory.