Class field theory

Last time we learned that $\mathbb{Z}_p$ consists of limits of integers under the "p-adic" distance. Let us make this more precise.

Definition 1. Let $\mathbb{Q}_p$ be the fraction field of $\mathbb{Z}_p$. The elements of the field $\mathbb{Q}_p$ are called **p-adic numbers**. Every nonzero p-adic number is of the form $u \cdot p^k$, where $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$.

Definition 2. We define the **p-adic valuation**

$$\nu_p : \mathbb{Q}_p \to \mathbb{Z} \cup \infty$$

by $\nu_p(x) = k$ if $x = u \cdot p^k$ and $\nu_p(0) = \infty$, and the **p-adic metric** $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}$ by $|x|_p = p^{-\nu_p(x)}$.

One can easily show that $|\cdot|_p$ satisfies the axioms for a metric, thus the p-adic distance $d(x, y) := |x - y|_p$ makes sense. This distance matches our previous intuition: the higher the power of p dividing $x - y$, the "closer" x and y are.

Remark. $\mathbb{Q}_p$ is nothing but the completion of $\mathbb{Q}$ under the p-adic metric, as $\mathbb{R}$ is the completion of $\mathbb{Q}$ under the usual Euclidean metric. But unlike $\mathbb{R}$, the topology of $\mathbb{Q}_p$ is totally disconnected: its connected components are one-point sets.

This completion process works in general for any number field.

Definition 3. Let K be a number field and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above p. We denote by $\mathcal{O}_\mathfrak{p}$ the **$\mathfrak{p}$-adic completion** of $\mathcal{O}_K$ at $\mathfrak{p}$ and $K_\mathfrak{p} = \mathrm{Frac}(\mathcal{O}_\mathfrak{p})$ its fraction field. $K_\mathfrak{p}$ is then a p-adic field, i.e., a finite extension of $\mathbb{Q}_p$.

Analogous to $\mathbb{Q}_p$, each element of the field $K_\mathfrak{p}$ can be written as $x = u \cdot \pi^n$, where π is called a **uniformizer** and $u \in \mathcal{O}_\mathfrak{p}^\times$. The p-adic fields is surprisingly useful in modern number theory. It turns out that all inequivalent metrics on a number field K are divided into two classes: either a $\mathfrak{p}$-adic metric coming from $K \hookrightarrow K_\mathfrak{p}$, or a usual metric coming from an embedding $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$. So unsurprisingly we decide to give them a name.

Definition 4. Let K be a number field. An prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is called a **finite place** (or **non-archimedean place**) of K. An embedding $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$ is called an **infinite place** (or **archimedean place**) of K. An complex embedding $K \hookrightarrow \mathbb{C}$ and its complex conjugate are viewed as the same complex place.

By definition, the finite places of $\mathbb{Q}$ are the prime numbers $v = 2, 3, 5, \ldots$ and the only infinite place (usually denoted by $v = \infty$) of $\mathbb{Q}$ is the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$. Just as we study a space locally by studying the neighborhoods of its points, the fields $K_v = \mathbb{R}$, $\mathbb{C}$ or $K_\mathfrak{p}$ encode all the local information of the global object — the number field K. For this reason, the terminology **local fields** and **global fields** are commonly used.

Our next goal is to state the main results of class field theory and draw some important consequences out of it. We will proceed by two steps. The first step is local class field theory, which classifies all the abelian extensions of a p-adic field. Then binding the local information at all finite and infinite places appropriately gives the structure of all abelian extensions of a number field, which is the content of global class field theory.

Recall that $\mathrm{Spec}\,\mathbb{Z}_p$ is constructed as a tubular neighborhood of $\mathrm{Spec}\,\mathbb{F}_p$, so we would expect that they have the same etale fundamental groups.

Theorem 1. $\pi_1(\operatorname{Spec}\mathbb{Z}_p) \cong \pi_1(\operatorname{Spec}\mathbb{F}_p) = \hat{\mathbb{Z}}$.

In terms of field theory, this can be rephrased as $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, namely there is a bijection between unramified finite extensions of $\mathbb{Q}_p$ and finite extensions of the residue field $\mathbb{F}_p$. The same thing is true for any p-adic field K, thus at least we understand the structure of the subfield K^{ur} of the maximal abelian extension K^{ab} of K: $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \hat{\mathbb{Z}}$. Now we are in a position to state the main theorem of local class field theory.

Theorem 2 (Local class field theory)**.** Let K be a p-adic field.

- (Local reciprocity) There exists a unique homomorphism (called the **local reciprocity map**) $\rho_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying:
  1. The following diagram commutes:
  $$\begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow{\scriptstyle \nu} & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \hat{\mathbb{Z}}, \end{array}$$
  where ν is the valuation map.
  2. For any finite abelian extension L/K, ρ_K induces an isomorphism
  $$K^\times/\mathbb{N}_{L/K}L^\times \cong \mathrm{Gal}(L/K),$$
  where $\mathbb{N}_{L/K} : L^\times \to K^\times$ is the norm map.
- (Existence) There is a bijection
  $$\{\text{subgroups of finite index of } K^\times\} \Longleftrightarrow \{\text{finite abelian extensions of } K\}$$
  given by $\mathbb{N}_{L/K}L^\times \hookleftarrow L$.

Remark. Local class field theory tells us that the finite abelian extensions of K are essentially classified by the intrinsic group structure of $K^\times$! Using the local reciprocity law, we know that
$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \varprojlim_L \mathrm{Gal}(L/K) \cong \varprojlim_L K^\times/\mathbb{N}_{L/K}L^\times.$$
This is the same as the profinite completion of $K^\times$ by the existence theorem. Since
$$K^\times \cong \mathcal{O}^\times \times \pi^{\mathbb{Z}} \cong \mathcal{O}^\times \times \mathbb{Z},$$
we are able to conclude that

Corollary 1. $\mathrm{Gal}(K^{ab}/K) \cong \mathcal{O}^\times \times \hat{\mathbb{Z}}$.

Example 1. $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times \times \hat{\mathbb{Z}}$. Moreover, an extension $L/\mathbb{Q}_p$ is unramified if and only if $\rho_{\mathbb{Q}_p}(\mathbb{Z}_p^\times) = 1$ in $\mathrm{Gal}(L/\mathbb{Q}_p)$.

Example 2. Let p be an odd prime. We can further determine all the quadratic extensions of $\mathbb{Q}_p$. By local class field theory, a quadratic extension corresponds to a subgroup of $\mathbb{Q}_p^\times$ of index 2. Since such a subgroup must contain $(\mathbb{Q}_p^\times)^2$, it is equivalent to finding all subgroups of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ of index 2. Notice that

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p) \times \mathbb{Z} \cong \mathbb{Z}/(p-1) \times \mathbb{Z}_p \times \mathbb{Z},$$

where in the second equality the exponential map induces an isomorphism between $\mathbb{Z}_p$ and $(1+p\mathbb{Z}_p)$. We have $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which has exactly three subgroups of index 2. So there are exactly three quadratic extensions of $\mathbb{Q}_p$.

Exercise. Show that $\mathbb{Q}_p(\sqrt{c})$, $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{cp})$ are three non-isomorphic quadratic extensions, where c is any quadratic non-residue modulo p.

Now we intend to bind all local fields associated to a number field K. A natural option is to take the direct product $\prod_v K_v^\times$, where v runs over all places. But it turns out to be too huge to deal with arithmetic problems. For example, any element of K only has nonzero v-valuation at finitely many places v.

Definition 5. We define the **idele group** J_K to be the subgroup of $\prod_v K_v^\times$ consisting of elements (x_v) such that x_v has nonzero v-adic valuation for only finitely many finite places v (in other words, all but finitely many x_v lie in $\mathcal{O}_v^\times$). So $K^\times$ naturally sits inside J_K. We define the **idele class group** to be the quotient group $C_K := J_K/K^\times$.

Exercise. Show that $C_\mathbb{Q} \cong \mathbb{R}_{>0} \prod_p \mathbb{Z}_p^\times$.

The idele class group C_K is the group encoding both local and global information and turns out to be the right object characterizing the abelian extensions of K.

Theorem 3 (Global class field theory)**.** Let K be a number field.

- (Global reciprocity) There exists a unique continuous homomorphism (called the **global reciprocity map**) $\rho_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying:

  1. The following diagram commutes (compatibility with local reciprocity):

$$\begin{array}{ccc} K_v & \xrightarrow{\rho_{K_v}} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{\rho_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

  2. For any finite abelian extension L/K, ρ_K induces an isomorphism

$$C_K/\mathbb{N}_{L/K}(C_L) \cong \mathrm{Gal}(L/K),$$

  where $\mathbb{N}_{L/K}(x)_v = \prod_{w \text{ above } v} \mathbb{N}_{L_w/K_v}(x_w)$.

- (Existence) There is a bijection

$$\{\text{open subgroups of finite index of } C_K\} \Longleftrightarrow \{\text{finite abelian extensions of } K\}$$

  given by $\mathbb{N}_{L/K}C_L \hookleftarrow L$.

- ρ_K is surjective and the kernel is the connected component of 1 in C_K.

Example 3. The connected component of 1 in $C_{\mathbb{Q}}$ is $\mathbb{R}_{>0}$, therefore global class field theory gives $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times$. Moreover, an extension $L/\mathbb{Q}$ is unramified at p if and only $\rho_K(\mathbb{Z}_p^\times) = 1$ in $\mathrm{Gal}(L/\mathbb{Q})$. In particular, we know that the maximal unramified extension of $\mathbb{Q}$ unramified outside p has Galois group $\mathbb{Z}_p^\times$ (the prime group as promised last time).

The name of reciprocity maps hints at a possible relation with quadratic reciprocity. This is the case and quadratic reciprocity can be easily deduced from global class field theory. Indeed, generalizing quadratic reciprocity and other higher reciprocity laws is one of the major motivations for developing class field theory historically. The name of the idele class group hints at a possible relation with the ideal class group. This is also the case. We will justify this point and then introduce the basics of Iwasawa theory next time.