# Ideal class groups

Recall that class field theory classifies finite abelian extensions of a number field $K$ in terms of the idele class group $C_K$. There is a reciprocity map $\rho_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ inducing the isomorphism $C_K/\mathbb{N}_{L/K}C_L \cong \mathrm{Gal}(L/K)$. We found out that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times$ and now can easily recover the classical Kronecker-Weber theorem.

**Theorem 1** (Kronecker-Weber)**.** Each finite abelian extension of $\mathbb{Q}$ is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_N)$ for some $N$.

*Proof.* Notice that $\prod_p \mathbb{Z}_p^\times = \hat{\mathbb{Z}}^\times$ and $\varprojlim_N \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/N\mathbb{Z})^\times \cong \hat{\mathbb{Z}}^\times$. So $\mathbb{Q}^{\mathrm{ab}}$ is explictly the union of all cyclotomic fields $\mathbb{Q}(\zeta_N)$. □

*Remark.* This theorem marks the significance of cyclotomic fields for studying abelian number fields.

This global reciprocity map comprises local reciprocity maps $\rho_{K_v} : K_v^\times \to \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$ for each place $v$ of $K$. When $v$ is a finite place, $\rho_{K_v}$ is provided by local class field theory and gives a bijection between finite abelian extensions of $K_v$ and subgroups of $K_v^\times$ of finite index.

In view of class field theory, the infinite places should play an equal role as the finite places. It is also amusing to compare the picture at finite places with the two other local fields $\mathbb{C}$ and $\mathbb{R}$, though their extensions are rather simple. For $\mathbb{C}$, it has no nontrivial finite extension and $\mathbb{C}^\times$ also has no nontrivial subgroup of finite index. For $\mathbb{R}$, it has only one nontrivial finite extension $\mathbb{C}/\mathbb{R}$ of order 2 and $\mathbb{R}^\times$ has only one nontrivial subgroup $(\mathbb{R}^\times)^2 = \mathbb{R}_{>0}$ of index 2. Moreover, $\mathbb{R}_{>0}$ is exactly the image of the norm map $\mathbb{N}_{\mathbb{C}/\mathbb{R}}\mathbb{C}^\times$!

Now we can make sense of ramification of infinite places.

**Definition 1.** Let $L/K$ be an extension of number fields. Let $v$ be an infinite place. We say that an infinite place $w$ of $v$ **lies above** $v$ (denoted by $w \mid v$) if $w$ extends $v$. We say $v$ is **ramified in** $L$ if $v$ is real and $w$ is complex for some $w$ lying above $v$, and **unramified in** $L$ otherwise.

**Example 1.** The infinite place $v = \infty$ of $\mathbb{Q}$ is unramified in $\mathbb{Q}(\sqrt{2})$ but is ramified in $\mathbb{Q}(i)$.

By local class field theory, a finite place $v$ is unramified in $L$ if and only if $\rho_K(\mathcal{O}_v^\times) = 1$ in $\mathrm{Gal}(L/K)$. For the infinite place, the above definition gives an analogous result: let $v$ be an infinite place, then $v$ is unramified in $L$ if and only if $\rho_K(K_v^\times) = 1$, since $v$ being unramified simply means there is no appearance of the nontrivial element in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ at any infinite place.

We already know that the maximal unramified abelian extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself. What is the maximal unramified abelian extension of a general number field $K$? The question is a bit more subtle for fields other than $\mathbb{Q}$. We need to distinguish the following two definitions.

**Definition 2.** Let $K$ be a number field. The maximal abelian extension of $K$ unramified at all places (denoted by $H$) is called the **Hilbert class field** of $K$. The maximal abelian extension of $K$ unramified at all finite places (denoted by $H^+$) is called the **narrow Hilbert class field** of $K$. So $\pi_1^{\mathrm{ab}}(\mathrm{Spec}\,\mathcal{O}_K) \cong \mathrm{Gal}(H^+/K)$.

**Example 2.** For $K = \mathbb{Q}$, we have $H = H^+ = \mathbb{Q}$. But for general number fields, the inclusion $K \subseteq H \subseteq H^+$ may be strict.

In general, the Hilbert class field $H$ is closely related to an intrinsic invariant of the number field $K$ — its ideal class group. The **fractional ideals** of $\mathcal{O}_K$ are of the form $\prod_i \mathfrak{p}_i^{e_i}$, where $e_i \in \mathbb{Z}$. So the fractional ideals form a group under multiplication. The ideal class group measures how far these fractional ideals are away from principal ones.

**Definition 3.** Denote the **group of fractional ideals** of $K$ by $I(K)$. Denote $P(K)$ the subgroup of principal fractional ideals (i.e., those generated by an element in $K^\times$). We define the **(ideal) class group** of $K$ to be the quotient group $H(K) := I(K)/P(K)$. A fundamental theorem in algebraic number theory asserts that $H(K)$ is always a finite group. The order of $H(K)$ is called the **class number** of $K$.

*Remark.* By definition, $K$ has class number one if and only if $\mathcal{O}_K$ is a PID, if and only if $\mathcal{O}_K$ is a UFD.

Let $\phi : K^\times \to I(K)$ be the natural map $a \mapsto (a)$. Then $P(K) = \operatorname{Im}\phi$ and $H(K) = \operatorname{Coker}\phi$. On the other hand, as an abstract group, $I(K) \cong \bigoplus_{\mathfrak{p}} \mathbb{Z}$. So $\phi$ is nothing but the valuation map $K^\times \to \bigoplus_{\mathfrak{p}} \mathbb{Z}$. This valuation map natually extends to the idele group $J_K \to \bigoplus_{\mathfrak{p}} \mathbb{Z}$ and hence induces a map $C_K \to H(K)$. This is a surjection and the kernel is exactly $\prod_{v\nmid\infty} \mathcal{O}_v^\times \prod_{v|\infty} K_v^\times$. By class field theory, $C_K/\mathcal{O}_v^\times \prod_{v|\infty} K_v^\times \cong H(K)$ corresponds to the Hilbert class field $H$. So we have the following isomorphism between the class group and the Hilbert class field.

**Theorem 2.** The reciprocity map induces an isomorphism $H(K) \cong \operatorname{Gal}(H/K)$.

*Remark.* This important result justifies several terminologies: the "ideles" are a generalization of "ideals" and the Hilbert "class" field is the field with Galois group canonically isomorphic to the "class" group. So class field theory is a vast generalization of this correspondence between abelian number fields and idele class groups.

Similarly, the narrow Hilbert class field theory $H^+$ corresponds to $C_K/\prod_{v\nmid\infty} \mathcal{O}_v^\times \prod_{v|\infty} (K_v^\times)^2$. Instead of removing all elements in $K^\times$, we should remove those elements lying in $(K_v^\times)^2$ for all infinite places. This motivates the following definition.

**Definition 4.** An element $a \in K^\times$ is called **totally positive** if $\sigma(a) > 0$ for every real embedding $\sigma : K \hookrightarrow \mathbb{R}$. Let $P^+(K)$ be the subgroup of $P(K)$ generated by all totally positive elements. We define the **narrow class group** to be $H^+(K) := I(K)/P^+(K)$.

**Theorem 3.** The reciprocity map induces an isomorphism $H^+(K) \cong \operatorname{Gal}(H^+/K)$.

Notice that by definition $\operatorname{Gal}(H^+/K) = \pi_1^{\mathrm{ab}}(\operatorname{Spec} \mathcal{O}_K)$. So miraculously we can read off information about the etale fundamental group by computing the narrow class group!

**Example 3.** $K = \mathbb{Q}$. Each fractional ideal of $\mathbb{Q}$ can be generated by a positive rational number. So $H^+(\mathbb{Q}) = 1$, which corresponds to the familiar fact that the narrow class field $H^+ = \mathbb{Q}$ and $\pi_1^{\mathrm{ab}}(\operatorname{Spec} \mathbb{Z}) = 1$.

**Example 4.** $K = \mathbb{Q}(\sqrt{i})$ has class number 1 and has no real places. So $H(K) = H^+(K) = 1$ and $H = H^+ = K$.

When $K$ has class number greater than 1, the Hilbert class field may not that easy to find. The following proposition about ramification in general number fields is quite handy.

**Proposition 1.** Let $K$ be a number field and $L = K(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m})$. For a prime $\mathfrak{p}$ of $K$, if $a_i \notin \mathfrak{p}$ and $n_i \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in $L$.

**Example 5.** $K = \mathbb{Q}(\sqrt{-5})$ has class number 2 and has no real places. $H(K) = H^+(K)$ is represented by (1) and $(2, 1+\sqrt{-5})$. The Hilbert class field should be a quadratic extension of $K$. We claim that $H = H^+ = K(i)$. To prove it, it suffices to show that $K(i)/K$ is unramified at every prime. By the proposition, we know that only the primes of $K$ above (2) can be ramified in $K(i)$. Since $K(i) = K(\sqrt{5}) \hookrightarrow K(\zeta_5)$ ($\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$), the proposition also tells us that only the primes of $K$ over (5) can be ramified in $K(i)$. Therefore $K(i)/K$ is unramified everywhere.

**Exercise.** For $K = \mathbb{Q}(\sqrt{-6})$, show that $H = H^+ = K(\sqrt{-3})$ (hint: use the fact that $K$ has class number 2).

*Remark.* Here is a beautiful connection between the solution of the $p = x^2 + ny^2$ problem and the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$.

| | | |
|---|---|---|
| $p = x^2 + y^2$ | $p \equiv 1 \pmod 4$ | $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ |
| $p = x^2 + 5y^2$ | $p \equiv 1, 9 \pmod{20}$ | $\mathbb{Q}(\sqrt{-5}, i) \hookrightarrow \mathbb{Q}(\zeta_{20})$ |
| $p = x^2 + 6y^2$ | $p \equiv 1, 7 \pmod{24}$ | $\mathbb{Q}(\sqrt{-6}, \sqrt{-3}) \hookrightarrow \mathbb{Q}(\zeta_{24})$ |

In general, we have a criterion of the shape $p \equiv \cdots \pmod N$ if and only if the Hilbert class field $H$ of $\mathbb{Q}(\sqrt{-n})$ is an abelian extension of $\mathbb{Q}$ and in that case $N$ is the the smallest number such that $H \hookrightarrow \mathbb{Q}(\zeta_N)$ (ensured by the Kronecker-Weber theorem). Moreover, the correct residues modulo $N$ is exactly the subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ corresponding to the subfield $H \hookrightarrow \mathbb{Q}(\zeta_N)$ via Galois theory.

Here we also supply an example for which the narrow class group and the class group are different.

**Example 6.** For $K = \mathbb{Q}(\sqrt{3})$, $H = K$ and $H^+ = K(i)$.

Finally we summarize our analogy between the first homology group and class groups as follows. The class group is one of the most important arithmetic invariant of a number field. The analogy suggests that we can study $H(K)$ by studying an infinite tower of extension of $K$, in the way we obtained formulas for $\#H_1(M_n)$ via going to the infinite cyclic covering $X_\infty \to X_K$ for a knot $K$. We will talk more about this key idea in Iwasawa theory next time.

| homology group | ideal class group |
|---|---|
| $H_1(M) = \pi_1^{\mathrm{ab}}(M)$ | $H^+(K) = \pi_1^{\mathrm{ab}}(\operatorname{Spec}\mathcal{O}_K)$<br>$H(K) = \pi_1^{\mathrm{ab}}(\operatorname{Spec}\mathcal{O}_K \cup \{\infty\text{-places}\})$ |