Class Field Theory

Peter Stevenhagen

Class field theory is the study of extensions $\mathbb{Q} \subset K \subset L \subset K^{\mathrm{ab}} \subset \overline{K} = \overline{\mathbb{Q}}$, where L/K is a finite abelian extension with Galois group G.

1. Class Field Theory for $\mathbb{Q}$

First we discuss the situation where $K = \mathbb{Q}$. In this case, we have the cyclotomic extension $K = \mathbb{Q} \subset L = \mathbb{Q}(\zeta_m)$, and

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^* &\cong \mathrm{Gal}(L/\mathbb{Q}) \\ a \bmod n &\mapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a)\end{aligned}$$

It is the theorem of Kronecker-Weber that

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^* = \widehat{\mathbb{Z}}^* = \prod_p \mathbb{Z}_p^*.$$

In addition to an explicit description of the Galois group, we also can describe the splitting behavior of a prime p in $\mathbb{Q} \subset \mathbb{Q}(\zeta_m)$—it is determined by $p \bmod m$. For example, a prime $p = x^2 + y^2 = (x + iy)(x - iy) \in \mathbb{Z}[i] = \mathbb{Z}[\zeta_4]$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$. In particular:

(a) If p ramifies in $\mathbb{Q}(\zeta_m)$, then $p \mid m$; the ramification index e_p of the primes over p is $\phi(p^k) = (p-1)p^{k-1}$ if $p^k \parallel m$.
(b) The prime p is wildly ramified in $\mathbb{Q}(\zeta_m)$ if and only if $p^2 \mid m$.
(c) If $p \nmid m$, then p is unramified. In the ring of integers $\mathbb{Z}[\zeta_m]$ of $\mathbb{Q}(\zeta_m)$, we obtain $p\mathcal{O}_L = \prod_{i=1}^{g_p} \mathfrak{p}_i$. The primes $\mathfrak{p}_i$ have residue class degree $f_p = [\mathbb{F}_p(\zeta_m) : \mathbb{F}_p]$, which (by looking at the Frobenius $x \mapsto x^p$ acting on $\mathbb{F}_p(\zeta_m) = k_{\mathfrak{p}_i}$) is equal to the order of $p \bmod m$ in $(\mathbb{Z}/m\mathbb{Z})^*$. The number of such primes is

$$g_p = \#\{\mathfrak{p}_i | p\} = [(\mathbb{Z}/m\mathbb{Z})^* : \langle p \bmod m \rangle].$$

In particular, a prime splits competely if and only if $p \equiv 1 \pmod m$.

If $\mathbb{Q} \subset L^H \subset L = \mathbb{Q}(\zeta_m)$ is a subfield given by a subgroup $H \subset (\mathbb{Z}/m\mathbb{Z})^*$, then one has the Artin map

$$A : (\mathbb{Z}/m\mathbb{Z})^*/H \to \mathrm{Gal}(L/\mathbb{Q}).$$

If m is the minimal such number, it is called the *conductor* of L.

2. Weak Reciprocity

We would like to generalize this situation to a general number field K.

Let $K \subset L$ be an abelian extension of number fields. We first would like to make sense of the statement that the splitting behavior of primes $\mathfrak{p}$ of K in L is determined by $\mathfrak{p} \bmod \mathfrak{m}$.

Let $G = \mathrm{Gal}(L/K)$ be the Galois group of L over K, and let K and L have ring of integers $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Let $\mathfrak{p} \in \mathcal{O}_K$ be an unramified prime. We see that $\mathcal{O}_L/\mathfrak{p} = \prod_{i=1}^{g} \mathcal{O}_L/\mathfrak{q}_i$, where $\mathcal{O}_L/\mathfrak{q}_i$ over $\mathcal{O}_K/\mathfrak{p}$ is a finite extension of finite fields. This extension has a cyclic Galois group with a distinguished generator $\mathrm{Frob}_{\mathfrak{p}}$, which maps $x \mapsto x^{N\mathfrak{p}}$. We see that $f_{\mathfrak{p}} = \#\langle \mathrm{Frob}_{\mathfrak{p}} \rangle \subset G$, and $g_{\mathfrak{p}} = \#\{\mathfrak{q}_i | \mathfrak{p}\} = [G : \langle \mathrm{Frob}_{\mathfrak{p}} \rangle]$.

Lemma 2.1. *If L/K is an abelian extension of number fields and $\mathfrak{p}$ is unramified in L/K, then the Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ is locally induced by a unique element in $G = \mathrm{Gal}(L/K)$.*

We let I_K be the group of (fractional) $\mathcal{O}_K$-ideals, which is exactly

$$I_K = \bigoplus_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \text{prime}}} \mathbb{Z}.$$

Let D be the discriminant of L/K. We denote by $I_K(D)$ the subgroup of I_K generated by ideals which are coprime to D. We then define the Artin map

$$\begin{aligned} I_K(D) &\to G = \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \mathrm{Frob}_{\mathfrak{p}}\,. \end{aligned}$$

As for the case of $\mathbb{Q}$, we would like that the kernel of this map contains all primes which are 1 mod m. We must be careful: we have ideals, so we must restrict to the case of principal ideals, and we must take care of units of the field. From this, we have the following first weak form of reciprocity:

Theorem 2.1. *There exists an ideal $\mathfrak{m} \subset \mathcal{O}_K$ (divisible by all ramifying primes) such that*

$$\ker A \supset \{(\pi) : \pi \equiv 1 \in (\mathcal{O}_K/\mathfrak{m})^*,\ \pi \text{ totally positive}\}.$$

3. Cycles

We invent 'cycles' to allow us to talk about these congruences in a uniform way. A *cycle* in K is $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an ideal in $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a set of real primes of K. We also write

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

so that $m(\mathfrak{p}) \in \mathbb{Z}_{\geq 0}$ for all $\mathfrak{p}$, $m(\mathfrak{p})$ is zero for almost all $\mathfrak{p}$, and $m(\mathfrak{p})$ is 0 or 1 for a real prime, 0 for a complex prime.

If $\alpha \in K^*$, then we say $\alpha \equiv 1 \pmod{^* \mathfrak{m}}$ if and only if $\alpha \equiv 1 \in (\mathcal{O}/\mathfrak{m}_0\mathcal{O})^*$ and $\alpha >_\mathfrak{p} 0$ for all real primes $\mathfrak{p}$. This says that:

- For $\mathfrak{p} \mid \mathfrak{m}$ finite, $\operatorname{ord}_\mathfrak{p}(\alpha - 1) \geq m(\mathfrak{p})$;
- For $\mathfrak{p} \mid \infty$, given by $\sigma : K \hookrightarrow \mathbb{R}$, then $\sigma(\alpha) > 0$.

For example, $1/5 \equiv -1 \pmod{^* 6}$.

In this language, the theorem becomes: $\ker A \supset \{\alpha\mathcal{O}_K : \alpha \equiv 1 \pmod{^* \mathfrak{m}}\}$ for a suitable cycle $\mathfrak{m}$.

If $\mathfrak{m}$ is a cycle in K, we define

$$I(\mathfrak{m}) = \{\mathfrak{a} \in I_K : \operatorname{ord}_\mathfrak{p}(\mathfrak{a}) = 0 \text{ if } \mathfrak{p} \mid \mathfrak{m}_0\}.$$

The denote by $P(\mathfrak{m}) \subset I(\mathfrak{m})$ the subgroup of principal ideals with this property. We also have the *ray modulo* $\mathfrak{m}$,

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

with the containment $R(\mathfrak{m}) \subset P(\mathfrak{m})$.

Since any element of the ideal class group of K is generated by an ideal prime to the discriminant, we see that $I(\mathfrak{m}) \subset \mathrm{Cl}_K$. We define the *ray class group of* $\mathfrak{m}$, $I(\mathfrak{m})/R(\mathfrak{m}) = \mathrm{Cl}_\mathfrak{m}$. It admits a surjection $\mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl}_K$ with kernel

$$P(\mathfrak{m})/R(\mathfrak{m}) = (\mathcal{O}_K/\mathfrak{m})^* = (\mathcal{O}_K/\mathfrak{m}_0)^* \times \prod_{\mathfrak{p}\mid\mathfrak{m}_\infty} \langle -1 \rangle.$$

All together, we have the exact sequence

$$\mathcal{O}_K^* \to (\mathcal{O}_K/\mathfrak{m})^* \to \mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl}_K \to 0.$$

For an example, consider again $\mathbb{Q}$. Then any cycle is $\mathfrak{m} = (m)$ or $\mathfrak{m} = (m)\infty$. In the first case, we have the ray class group $(\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$, and in the other case simply $(\mathbb{Z}/m\mathbb{Z})^*$, which is what we would expect from the description above.

4. Class Field Theory

We now can state the main theorem of class field theory.

Theorem 4.1. *If $K \subset L$ is a finite abelian extension of number fields, then:*

(a) *There exists a cycle $\mathfrak{m}$ divisible by all ramifying primes (a real prime ramifies if it has a complex extension) such that the Artin map*

$$A : I(D) \to \mathrm{Gal}(L/K)$$
$$\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}$$

factors through $\mathrm{Cl}_\mathfrak{m}$ and the map

$$A : \mathrm{Cl}_\mathfrak{m} \to \mathrm{Gal}(L/K)$$
$$[\mathfrak{p}] \mapsto \mathrm{Frob}_\mathfrak{p}$$

is surjective.

(b) *There exists a minimal such cycle* $\mathfrak{f}$*, called the* conductor *of* L/K*, with the property that* $\mathfrak{p} \mid \mathfrak{f}$ *if and only if* $\mathfrak{p}$ *is ramified in* L/K*, and* $\mathfrak{p}^2 \mid \mathfrak{f}$ *if and only if* $\mathfrak{p}$ *is wildly ramified in* L/K*.*

(c) *(Existence) Given a cycle* $\mathfrak{m}$*, there exists a* ray class field $H_{\mathfrak{m}} \subset K^{\mathrm{ab}}$ *which is maximal in the sense that* $R(\mathfrak{m}) \subset \ker A$*, and*

$$\mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{m}}/K).$$

Therefore, $K^{\mathrm{ab}} = \bigcup_{\mathfrak{f}} H_{\mathfrak{f}} \subset \overline{\mathbb{Q}}$.

This construction is highly nontrivial. For example, for $\mathfrak{m} = (1)$, we see that from the exact sequence that $\mathrm{Cl}_{\mathfrak{m}} = \mathrm{Cl}_K$ gives us $H = H_1$, the ray class field mod 1, which is usually called the *Hilbert class field*. It has the property that

$$\mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}(H/K),$$

and H/K is unramified at *all* primes of K (including the infinite primes), which is often called *totally unramified*.

For example, the field $K = \mathbb{Q}(\sqrt{-5})$ has class group $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$. In this case, the Hilbert class field is $H = K(\sqrt{5})$. Also, for $K = \mathbb{Q}(\sqrt{-23})$, $\mathrm{Cl}_K \cong \mathbb{Z}/3\mathbb{Z}$, with $H = K(\alpha)$ where $\alpha^3 - \alpha - 1 = 0$. In each case, these extensions are in fact unramified everywhere.

5. Idèles

However, we would like to deal with the maximal abelian extension K^{ab}/K in one stroke. We have seen that $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim \mathrm{Cl}_{\mathfrak{f}}$, a projective limit of ray class groups. For example, for $K = \mathbb{Q}$ we get $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim (\mathbb{Z}/n\mathbb{Z})^* = \widehat{\mathbb{Z}}^*$. To realize this in general, we need to define the idèles.

Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$, so that if $\mathfrak{p}$ is real or complex, $K = \mathbb{R}$ or $\mathbb{C}$, respectively. We denote by $A_{\mathfrak{p}} \subset K_{\mathfrak{p}}$ the valuation ring

$$A_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}$$

with unit group

$$A_{\mathfrak{p}}^* = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} = 1\}.$$

Then we define the *idèle group* as the restricted direct product

$$\mathbf{J} = \prod_{\mathfrak{p} \leq \infty}{}' K_{\mathfrak{p}}^* = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \textstyle\prod_{\mathfrak{p} \leq \infty} K_{\mathfrak{p}}^* : x_{\mathfrak{p}} \in A_{\mathfrak{p}}^* \text{ for almost all } \mathfrak{p}\}.$$

Each of these factors has a topology, and we make $\mathbf{J}$ into a locally compact group by defining the open subgroups U to be, for S a finite set of primes,

$$U = \prod_{\mathfrak{p} \notin S} A_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \in S} O_{\mathfrak{p}},$$

where $O_{\mathfrak{p}} \subset K_{\mathfrak{p}}^*$ is an open subgroup.

We have a filtration

$$K_{\mathfrak{p}}^* \supset A_{\mathfrak{p}}^* = U_p^{(0)} \supset 1 + \mathfrak{p} \supset 1 + \mathfrak{p}^2 \supset \cdots \supset 1 + \mathfrak{p}^n = U_p^{(n)} \supset \ldots.$$

If $\mathfrak{p}$ is archimedean, we let $U_{\mathfrak{p}}^{(0)} = K_{\mathfrak{p}}^*$, and if $\mathfrak{p}$ is real, we let $U_{\mathfrak{p}}^{(1)} = \mathbb{R}_{>0}^*$. From this we see that $H \subset \mathbf{J}$ is an open subgroup if and only if

$$H \supset \prod_{\mathfrak{p} \leq \infty} U_{\mathfrak{p}}^{n(\mathfrak{p})}$$

with $n(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$, $n(\mathfrak{p}) \in \{0, 1\}$ for $\mathfrak{p}$ real, $n(\mathfrak{p}) = 0$ for $\mathfrak{p}$ complex. In particular, if $\mathfrak{f} = \prod \mathfrak{p}^{n(\mathfrak{p})}$ is a cycle, it corresponds to an open subgroup $W_{\mathfrak{f}} = \prod_{p \leq \infty} U_{\mathfrak{p}}^{n(\mathfrak{p})}$, and H is open in $\mathbf{J}$ if and only if $H \supset W_{\mathfrak{f}}$ for some cycle $\mathfrak{f}$.

We map $K^* \subset \mathbf{J}$ by $x \mapsto (x)_{\mathfrak{p}}$. We then obtain the *idèle class group* $C_K = \mathbf{J}/K^*$.

Lemma 5.1. *There exists an isomorphism*

$$\begin{aligned} A : \mathbf{J}/(K^* W_{\mathfrak{p}}) &\xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{f}} \\ \pi_{\mathfrak{p}} &\mapsto [\mathfrak{p}], \ (\mathfrak{p} \nmid \mathfrak{f}). \end{aligned}$$

Corollary 5.1 (Idèlic Main Theorem)**.** *If L/K is abelian, the Artin map gives a surjection*

$$\begin{aligned} C_K &\to \mathrm{Gal}(L/K) \to 0 \\ \pi_{\mathfrak{p}} &\mapsto \mathrm{Frob}_{\mathfrak{p}}, \ (\mathfrak{p} \nmid \mathfrak{f}). \end{aligned}$$

This yields a surjection $C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, and we obtain a bijection between open subgroups of C_K and finite abelian extensions L/K inside an algebraic closure $\overline{K}$, where L corresponds to $N_{L/K} C_L$.

6. Local Class Field Theory

If $\mathfrak{p}$ is a finite prime, given an abelian extension L/K of number fields, we obtain for a prime $\mathfrak{q}$ which lies over $\mathfrak{p}$ a corresponding local extension $L_{\mathfrak{q}}/K_{\mathfrak{p}}$, with

$$G_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\mathfrak{q} = \mathfrak{q}\} = \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \subset \mathrm{Gal}(L/K).$$

Then in the Artin surjection $\mathbf{J} \to \mathrm{Gal}(L/K)$, if we restrict to the factor $K_{\mathfrak{p}}^*$, this maps surjectively onto exactly the factor $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$. We have

$$1 \to I_{\mathfrak{p}} \to \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) = \langle \mathrm{Frob}_{\mathfrak{p}} \rangle \to 1,$$

where $I_{\mathfrak{p}}$ is the inertia group, a factor which is nontrivial only if $\mathfrak{p}$ ramifies at $\mathfrak{q}$. We then obtain maps:

$$\begin{array}{ccc} \mathbf{J} & \longrightarrow & \mathrm{Gal}(L/K) \\ \uparrow & & \uparrow \\ K_{\mathfrak{p}}^* & \longrightarrow & \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \\ \uparrow & & \uparrow \\ A_{\mathfrak{p}}^* & \longrightarrow & I_{\mathfrak{p}} \end{array}$$

Theorem 6.1. *Let $F = K_{\mathfrak{p}}$ be a local field. Given $E \supset F$ a finite abelian extension, there is an Artin map*

$$\begin{aligned} \langle \pi \rangle \times A_F^* = F^* &\to \mathrm{Gal}(E/F) \\ \pi &\mapsto \mathrm{Frob}_{\mathfrak{p}} \bmod I_{\mathfrak{p}} \\ A_F^* &\mapsto I_{\mathfrak{p}} \end{aligned}$$

In fact, $\ker A = N_{E/F}(E^*) \subset F^*$*, so*

$$F^*/NE^* \xrightarrow{\sim} \mathrm{Gal}(E/F).$$

One can show in fact that $F^* \hookrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$, with dense image. (The discrepancy occurs by replacing $\langle \pi \rangle \cong \mathbb{Z}$ mapping into the group $\widehat{\mathbb{Z}} \cong \mathrm{Gal}(F^{\mathrm{unr}}/F)$ consisting of powers of the Frobenius.)

Local class field theory allows us to compute conductors $\mathfrak{f}$ of L/K. We see that $\mathfrak{f} = \prod_{\mathfrak{p} \leq \infty} \mathfrak{p}^{n(\mathfrak{p})}$, $\mathfrak{p}$ is unramified if and only if $n(\mathfrak{p}) = 0$, $\mathfrak{p}$ is tamely ramified if and only if $n(\mathfrak{p}) = 1$, and $\mathfrak{p}$ is wildly ramified if and only if $n(\mathfrak{p}) \geq 2$. From the explicit description of the kernel of the Artin map in the local case, we see that the exponent $n(\mathfrak{p})$ is the smallest integer k such that $U_{\mathfrak{p}}^{(k)} \subset A_{\mathfrak{p}}^* \subset K_{\mathfrak{p}}^*$ is contained in $U_{\mathfrak{p}}^{(k)} \subset N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(L_{\mathfrak{q}}^*)$.

Example 6.2. *Let us find all quadratic extensions of $\mathbb{Q}_p$. If we use class field theory, we see that every such extension corresponds to subgroups $H = N_{E/\mathbb{Q}_p} E^* \subset \mathbb{Q}_p^*$ of index 2, with $\mathbb{Q}_p^*/H \cong \mathrm{Gal}(E/\mathbb{Q}_p)$. We have that $\mathbb{Q}_p^* = \langle p \rangle \times \mathbb{Z}_p^*$, and $(\mathbb{Q}_p^*)^2 = \langle p^2 \rangle \times (\mathbb{Z}_p^*)^2$, and for $p \neq 2$ in between there are exactly three subfields of index 2, giving the three quadratic extensions of $\mathbb{Q}_p$.*

It is in fact easy to find these fields directly: the extensions correspond to $\mathbb{Q}_p \subset_2 \mathbb{Q}_p(\sqrt{x})$ for $x \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, with $x = p$, $x = a$, $x = ap$, for $a \in \mathbb{Z}$ such that $\overline{a} \in \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$. More precisely:

$$\begin{aligned} N(\mathbb{Q}_p(\sqrt{-p})^* &= \langle p \rangle \times (\mathbb{Z}_p^*)^2 \ \textit{(ramified)} \\ N(\mathbb{Q}_p(\sqrt{-ap})^* &= \langle ap \rangle \times (\mathbb{Z}_p^*)^2 \ \textit{(ramified)} \\ N(\mathbb{Q}_p(\sqrt{a})^* &= \langle p^2 \rangle \times (\mathbb{Z}_p^*)^2 \ \textit{(unramified)} \end{aligned}$$

Exercises

In the first three exercises, we let K be an algebraic number field, Cl_K its ideal class group, and $h_K = \#\,\mathrm{Cl}_K$ its class number. Let $\overline{K}$ be an algebraic closure of K, and $H(K)$ the *Hilbert class field* of K, which is the maximal abelian totally unramified extension of K inside $\overline{K}$. It is a consequence of the main theorem of class field theory that $H(K)$ is a finite abelian extension of K of degree h_K, and that the Artin symbol induces a group isomorphism $\mathrm{Cl}_K \to \mathrm{Gal}(H(K)/K)$.

The three exercises below illustrate how properties of the Hilbert class field can be used to obtain information about the class number.

Exercise 2.1.

(a) Let E be a finite extension of K. Prove that $H(K) \subset H(E)$, and that h_K divides $h_E \cdot [E : K]$.
(b) Let E, F be two finite extensions of $\overline{\mathbb{Q}}$ inside $\overline{\mathbb{Q}}$. Prove: if $h_E = h_F = 1$, then $h_{E \cap F} = 1$.

Exercise 2.2.

(a) Let E be a finite extension of K, and denote by L the maximal abelian totally unramified extension of K inside E. Show that the cokernel of the norm map $N_{E/K} \colon \mathrm{Cl}_E \to \mathrm{Cl}_K$ is isomorphic to $\mathrm{Gal}(L/K)$.
(b) Let n be a positive integer, and denote by ζ_n a primitive n-th root of unity. Prove that the class number of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ divides the class number of $\mathbb{Q}(\zeta_n)$.

Exercise 2.3. The *Hilbert class field tower* of K is the sequence of fields

$$H^{(0)}(K) = K \subset H^{(1)}(K) = H(K) \subset H^{(2)}(K) = H(H(K)) \subset \ldots \subset H^{(i)}(K) \subset \ldots,$$

where each $H^{(i)}(K)$ is the Hilbert class field of $H^{(i-1)}(K)$. It is said to be *finite* if $H^{(i+1)}(K) = H^{(i)}(K)$ for some i. Prove that the Hilbert class field tower of K is finite if and only if there is a finite extension E of K with $h_E = 1$. [Golod and Shafarevich proved in 1964 that there exist number fields K for which the Hilbert class field tower is *infinite*.]

Exercise 2.4. Show that the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ equals $\mathbb{Q}(\sqrt{-5}, \sqrt{5})$.

Exercise 2.5. Let α be a zero of $X^3 - X - 1 \in \mathbb{Z}[X]$ in an algebraic closure of $\mathbb{Q}$, and write $K = \mathbb{Q}(\sqrt{-23})$, $L = K(\alpha)$.

(a) Prove that L is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, and that $K \subset L$ is an abelian extension of degree 3.
(b) Prove that exactly two primes of $\mathbb{Q}(\alpha)$ are ramified over $\mathbb{Q}$, and that they lie over 23 and ∞. Prove that in both cases the ramification index equals 2.
(c) Prove that $K \subset L$ is totally unramified.
(d) Prove that L is the Hilbert class field of K.

Exercise 2.6. For a prime number p, let m_p be the number of distinct zeros of $X^3 - X - 1$ in $\mathbb{F}_p$. Prove the following:

(a) $m_p = 0$ if and only if $\left(\frac{p}{23}\right) = 1$ and p cannot be written as $p = a^2 + 23b^2$ with a, $b \in \mathbb{Z}$.
(b) $m_p = 1$ if and only if $\left(\frac{p}{23}\right) = -1$.
(c) $m_p = 2$ if and only if $p = 23$.
(d) $m_p = 3$ if and only if p can be written as $p = a^2 + 23b^2$ with a, $b \in \mathbb{Z}$, $a \neq 0$.

Exercise 2.7.

(a) Prove that the field $\mathbb{Q}(\sqrt{5})$ has class number 1, and that the group of units of its ring of integers is generated by -1 and $(1+\sqrt{5})/2$.
(b) Let p be a prime number. Prove that there exists a field K satisfying

$$[K:\mathbb{Q}] = 4, \qquad \sqrt{5} \in K, \qquad |\Delta_{K/\mathbb{Q}}| = 25p$$

if and only if $p \not\equiv 2, 3 \bmod 5$. Prove also that if such a field exists, it is uniquely determined by p, up to isomorphism. We denote this field by $K_{(p)}$.
(c) Prove that among all fields $K_{(p)}$, the only one that is Galois over $\mathbb{Q}$ is the field $K_{(5)}$. Can you embed $K_{(5)}$ in a cyclotomic extension of $\mathbb{Q}$?

Exercise 2.8. A number field is called *totally real* if it has no complex primes, *totally complex* if it has no real primes, and *mixed* if it is neither totally real nor totally complex. The *Fibonacci sequence* $(F_n)_{n=0}^{\infty}$ is inductively defined by $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$. Let p be a prime number with $p \equiv 1$ or $4 \bmod 5$, and $K_{(p)}$ as in the previous exercise.

(a) Prove that $K_{(p)}$ is mixed if and only if $p \equiv 3 \bmod 4$.
(b) Suppose that $p \equiv 1 \bmod 8$. Prove that $K_{(p)}$ is totally real if p divides $F_{(p-1)/4}$, and totally complex otherwise.
(c) Suppose that $p \equiv 5 \bmod 8$. Prove that $K_{(p)}$ is totally complex if p divides $F_{(p-1)/4}$, and totally real otherwise.

Exercise 2.9. Let p be a prime number with $p \equiv 11$ or $19 \bmod 20$, and let $K_{(p)}$ be as above. Prove that $K_{(p)}$ has exactly one prime lying over 5 if $p \equiv 11 \bmod 20$, and exactly two primes lying over 5 if $p \equiv 19 \bmod 20$.

In the next two exercises, we let $K \subset L$ be a finite abelian extension of number fields, and $\mathbb{F}(L/K)$ the *conductor* of L over K; this is the greatest common divisor of all cycles $\mathfrak{m}$ of K for which L is contained in the ray class field modulo $\mathfrak{m}$ of K. Denote by $m_{\mathfrak{p}}$ the exponent to which a prime $\mathfrak{p}$ of K appears in $\mathbb{F}$. It is part of the main theorem of class field theory that $m_{\mathfrak{p}} \geq 1$ if and only if $\mathfrak{p}$ is ramified in L, and that $m_{\mathfrak{p}} \geq 2$ if and only if $\mathfrak{p}$ is finite and *wildly* ramified in L. We want to find an *upper* bound for m. We may and do assume that $\mathfrak{p}$ is *finite*. Denote by p be the prime of $\mathbb{Q}$ over which $\mathfrak{p}$ is lying, and let $e = e(\mathfrak{p}/p)$ be the ramification index of $\mathfrak{p}$ over p.

Exercise 2.10. For an integer $i > 0$, denote by U_i the open subgroup $1 + \mathfrak{p}^i$ of $K_{\mathfrak{p}}^*$. Prove the following assertions.

(a) If i, j are positive integers with $j \not\equiv 0 \bmod p$, then the map $U_i \to U_i$ sending every x to x^j is an isomorphism.
(b) If $i > e/(p-1)$, then there is an isomorphism $U_i \to U_{i+e}$ sending every x to x^p.
(c) If j is a positive integer, then $(K_{\mathfrak{p}}^*)^j$ is an *open* subgroup of $K_{\mathfrak{p}}^*$, and it contains $U_{e'+ke}$, where e' denotes the least integer $> e/(p-1)$ and k is the number of factors p in j.

(d) If $K_\mathfrak{p} \subset E$ is a finite extension, then $N_{E/K_\mathfrak{p}}[E^*]$ is an open subgroup of $K_\mathfrak{p}^*$, and it contains $U_{e'+ke}$, with e' as in (c) and k the number of factors p in $[E : K_\mathfrak{p}]$.

Exercise 2.11.

(a) Prove that $m \leq e' + ke$, where e' denotes the least integer $> e/(p-1)$ and k is the number of factors p in $[L : K]$.

(b) More precisely, prove that $m \leq e' + ke$, with e' as before, but with k now equal to the number of factors p in the exponent of the inertia group of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$.

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
E-mail address: psh@math.leidenuniv.nl