Chapter 2
Preliminaries—Fundamental Groups and Galois Groups

The purpose of this chapter is to recollect the preliminary materials from topology and number theory, for the sake of readers. In particular, we present a summary about fundamental groups and Galois theory for topological spaces and arithmetic rings in Sects. 2.1 and 2.2, since the analogies between topological and arithmetic fundamental/Galois groups are fundamental in this book. Sections 2.1 and 2.2 also contain basic concepts and examples in three dimensional topology and number fields which will be used in the subsequent chapters. In Sect. 2.3, we review class field theory as arithmetic duality theorems in Galois, étale cohomology groups.

The reader who wants to know more or see precise proofs may consult [Ms, Go1, Mr] for fundamental groups and Galois theory, [Go2, Go3, Go4, Hb, Mi1, Ne1, NSW, Tm] for Galois, étale cohomology and class field theory, and [BZ, Hl, Kw, Ro, Ln1, Ne2] for the basic materials in knot theory and algebraic number theory.

2.1 The Case of Topological Spaces

Throughout this book, any topological space is assumed to be a PL-manifold and any map between topological spaces is assumed to be a PL-map (with obvious exceptions). Note that a manifold is arcwise-connected if and only if it is connected.

Let X be a connected topological space and fix a base point $x \in X$. For paths $\gamma, \gamma' : [0,1] \to X$ with $\gamma(1) = \gamma'(0)$, we define a path $\gamma \vee \gamma' : [0,1] \to X$ by $(\gamma \vee \gamma')(t) := \gamma(2t)$ if $0 \leq t \leq 1/2$ and $(\gamma \vee \gamma')(t) := \gamma'(2t-1)$ if $1/2 \leq t \leq 1$. Let $\Omega(X,x)$ be the set of loops in X based at x. For $l, l' \in \Omega(X,x)$, we say that l and l' are homotopic fixing the base point x, denoted by $l \simeq_x l'$, if there is a homotopy l_t connecting l and l' so that $l_t \in \Omega(X,x)$ for any $t \in I$. Let $\pi_1(X,x)$ be the set of equivalence classes, $\Omega(X,x)/\simeq_x$. Then $\pi_1(X,x)$ forms a group by the well-defined multiplication $[l] \cdot [l'] = [l \vee l']$. This is called the *fundamental group* of X with base point x. For another base point x', the correspondence $[l] \mapsto$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_2, © Springer-Verlag London Limited 2012

$[\gamma^{-1} \vee l \vee \gamma]$ gives an isomorphism $\pi_1(X, x) \simeq \pi_1(X, x')$ where γ is a path from x to x'. Hence, we sometimes omit the base point and write simply $\pi_1(X)$. A continuous map $f : X \to Y$ induce a homomorphism $f_* : \pi_1(X, x) \to \pi_1(Y, f(x))$ by $f_*([l]) := [f \circ l]$, and we have $f_* = g_*$ if $f, g : X \to Y$ are homotopy and $f(x) = g(x)$. Thus, π_1 is a covariant functor from the homotopy category of based arcwise-connected topological spaces to the category of groups. We note that the Abelianization $\pi_1(X)/[\pi_1(X), \pi_1(X)]$ of $\pi_1(X)$ is isomorphic to the homology group $H_1(X)$ by sending $[l]$ to the homology class of l (Hurewicz theorem).

Example 2.1 (Circle) $S^1 := \{x \in \mathbb{R}^2 \mid \|x\| = 1\}$. Let l be the loop $x \in S^1$ which goes once around the circle counterclockwise. Then $\pi_1(S^1, x)$ is an infinite cyclic group generated by $[l]$ (Fig. 2.1).

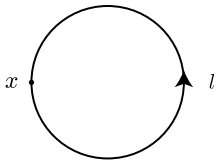


Fig. 2.1

Example 2.2 (Solid torus) $V := D^2 \times S^1$, where $D^2 := \{x \in \mathbb{R}^2 \mid \|x\| \leq 1\}$ is the unit 2-disk.

Since V is homotopy equivalent to S^1, one has $\pi_1(V) = \pi_1(S^1) = \langle[\beta]\rangle$, where $\beta = \{b\} \times S^1$, $b \in \partial D^2$. The boundary ∂V of V is a 2-dimensional torus $T^2 := S^1 \times S^1 = \partial V$. Define the projection $p_i : T^2 \to S^1$ for $i = 1, 2$ by $p_1(x, y) := x$, $p_2(x, y) := y$. Then $p_{1*} \times p_{2*}$ induces an isomorphism $\pi_1(T^2) \simeq \pi_1(S^1) \times \pi_1(S^1) = \langle[\alpha]\rangle \times \langle[\beta]\rangle$, where $\alpha = \partial D^2 \times \{a\}$, $a \in S^1$. Two loops α and β on T^2 are called a *meridian* and a *longitude*, respectively (Fig. 2.2).

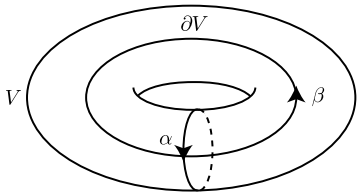


Fig. 2.2

Example 2.3 (n-sphere) $S^n := \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$ ($n \geq 2$). Since the space $S^n \setminus \{*\}$ obtained by removing a point $*$ from S^n is contractible, one has $\pi_1(S^n) = \{1\}$. A connected space X is called *simply-connected* if $\pi_1(X) = \{1\}$. The Poincaré conjecture, which was proved by G. Perelman (2003), asserts that a simply-connected closed 3-manifold is homeomorphic to S^3.

The *van Kampen theorem* provides a useful method to present a fundamental group in terms of generators and relations. Let $F(x_1, \ldots, x_r)$ denote the free group on letters (or words) $x_1, \ldots, x_r$. For $R_1, \ldots, R_s \in F(x_1, \ldots, x_r)$, let $\langle\langle R_1, \ldots, R_s \rangle\rangle$ denote the smallest normal subgroup of $F(x_1, \ldots, x_r)$ containing $R_1, \ldots, R_s$. When a group G is isomorphic to the quotient group $F(x_1, \ldots, x_r)/\langle\langle R_1, \ldots, R_s \rangle\rangle$, we write G by the following form

$$G = \langle x_1, \ldots, x_r \mid R_1 = \cdots = R_s = 1 \rangle$$

and call it a *presentation* of G in terms of generators and relations. Note that the choices of generators $x_1, \ldots, x_r$ and relators $R_1 = \cdots = R_s$ are not unique. If $r - s = k$, we say that G has a presentation of *deficiency* k. Now, let X be a topological space and suppose that there are two open subsets X_1 and X_2 of X such that $X = X_1 \cup X_2$ and $X_1 \cap X_2$ is nonempty. We assume that X, X_1, X_2 and $X_1 \cap X_2$ are arcwise-connected. Take a base point $x \in X_1 \cap X_2$ and suppose that we are given the following presentations:

$$\begin{aligned}
\pi_1(X_1, x) &= \langle x_1, \ldots, x_r \mid R_1 = \cdots = R_s = 1 \rangle, \\
\pi_1(X_2, x) &= \langle y_1, \ldots, y_t \mid Q_1 = \cdots = Q_u = 1 \rangle, \\
\pi_1(X_1 \cap X_2, x) &= \langle z_1, \ldots, z_v \mid P_1 = \cdots = P_w = 1 \rangle.
\end{aligned}$$

The inclusion maps $i_1 : X_1 \cap X_2 \hookrightarrow X_1$, $i_2 : X_1 \cap X_2 \hookrightarrow X_2$ induce the homomorphisms $i_{1*} : \pi_1(X_1 \cap X_2, x) \to \pi_1(X_1, x)$, $i_{2*} : \pi_1(X_1 \cap X_2, x) \to \pi_1(X_2, x)$. Then the van Kampen theorem asserts that $\pi_1(X, x)$ is given by amalgamating $\pi_1(X_1 \cap X_2, x)$ in $\pi_1(X_1, x)$ and $\pi_1(X_2, x)$, namely,

$$\pi_1(X, x) = \left\langle \begin{matrix} x_1, \ldots, x_r \\ y_1, \ldots, y_t \end{matrix} \middle| \begin{matrix} R_1 = \cdots = R_s = Q_1 = \cdots = Q_u = 1 \\ i_{1*}(z_1) i_{2*}(z_1)^{-1} = \cdots = i_{1*}(z_v) i_{2*}(z_v)^{-1} = 1 \end{matrix} \right\rangle.$$

Example 2.4 (Handlebody) Let us prepare g copies of a handle $D^2 \times D^1 = D^2 \times [0, 1]$ and a 3-ball D^3. For each handle, we fix a homeomorphism $D^2 \times \partial D^1 \to \partial D^3 = S^2$ and attach g handles to D^3 by identifying $x \in D^2 \times \partial D^2$ with $f(x)$. The resulting 3-manifold is called a *handlebody* of genus g and is denoted by H_g (Fig. 2.3).

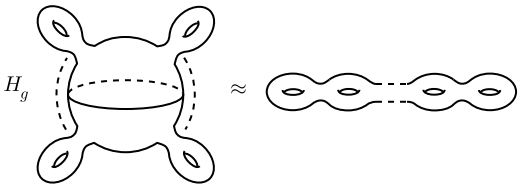


Fig. 2.3

H_g is homotopy equivalent to a bouquet B_g obtained by attaching g copies of S^1 at one point b (Fig. 2.4).

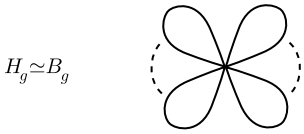


Fig. 2.4

Letting x_i be the loop starting from b and going once around the i-th S^1, the van Kampen theorem yields $\pi_1(H_g) = \pi_1(B_g) = F(x_1, \ldots, x_g)$.

Example 2.5 (Lens space) Let V_1, V_2 be oriented solid tori and let $f : \partial V_2 \xrightarrow{\approx} \partial V_1$ be a given orientation-reversing homeomorphism. We then make an oriented connected closed 3-manifold $M = V_1 \cup_f V_2$ by identifying $x \in \partial V_2$ with $f(x) \in \partial V_1$ in the disjoint union of V_1 and V_2. Let α_i and β_i denote a meridian and a longitude on V_i, respectively for each $i = 1, 2$. By Example 2.2, we may write

$$f_*\big([\alpha_2]\big) = p[\beta_1] + q[\alpha_1], \quad (p, q) = 1$$

in a unique way. The topological type of the space M is determined by the pair (p, q) of integers above and so M is called the *lens space* of type (p, q) and denoted by $L(p, q)$. Let us calculate the fundamental group of $L(p, q)$. Let $i_1 : \partial V_2 \to V_1$ be the composite of f with the inclusion map $\partial V_1 \hookrightarrow V_1$ and let $i_2 : \partial V_2 \hookrightarrow V_2$ be the inclusion map. Noting $\pi_1(V_i) = \langle \beta_i \rangle$ and $\pi_1(\partial V_2) = \langle \alpha_2 \rangle \times \langle \beta_2 \rangle$ and applying the van Kampen theorem, we have

$$\begin{aligned}
\pi_1\big(L(p, q)\big) &= \big\langle \beta_1, \beta_2 \mid i_{1*}(\alpha_2) = i_{2*}(\alpha_2), i_{1*}(\beta_2) = i_{2*}(\beta_2) \big\rangle \\
&= \big\langle \beta_1, \beta_2 \mid \beta_1^p \alpha_1^q = 1, i_{1*}(\beta_2) = \beta_2 \big\rangle \\
&= \big\langle \beta_1 \mid \beta_1^p = 1 \big\rangle \\
&\simeq \mathbb{Z}/p\mathbb{Z}.
\end{aligned}$$

So $\pi_1(L(p, q))$ is a finite cyclic group except the case $p = 0$ for which we have $L(0, \pm 1) \approx S^2 \times S^1$.

More generally, for oriented handlebodies V_1, V_2 of genus g and an orientation-reversing homeomorphism $f : \partial V_2 \xrightarrow{\approx} \partial V_1$, we can make an oriented connected closed 3-manifold $M := V_1 \cup_f V_2$ in a similar manner. One calls $M = V_1 \cup_f V_2$ a *Heegaard splitting* of M and g the genus of the splitting. Conversely, it is known that any orientable connected closed 3-manifold has such a Heegaard splitting. For a proof of this, we refer to [He, Chap. 2]. The fundamental group of a 3-manifold with a Heegaard splitting is computed in a similar way to the case of a lens space.

Example 2.6 (Knot group, link group) A *knot* is the image of an embedding of S^1 into S^3. So, by our assumption, a knot is always assumed to be a simple closed polygon in this book. We denote by V_K a *tubular neighborhood of* K. The complement

$X_K := S^3 \setminus \mathrm{int}(V_K)$ of an open tubular neighborhood $\mathrm{int}(V_K)$ in S^3 is called the *knot exterior*. It is a compact 3-manifold with a boundary being a 2-dimensional torus. A *meridian* of K is a closed (oriented) curve which is the boundary of a disk D^2 in V_K. A *longitude* of K is a closed curve on ∂X_K which intersects with a meridian at one point and is null-homologous in X_K (Fig. 2.5).

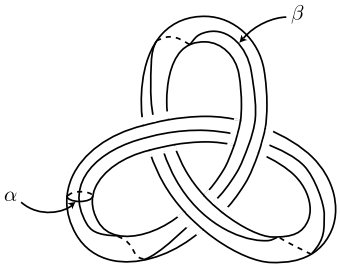


Fig. 2.5

The fundamental group $\pi_1(X_K) = \pi_1(S^3 \setminus K)$ is called the *knot group* of K and is denoted by G_K. Firstly, let us explain how we can obtain a presentation of G_K. We may assume $K \subset \mathbb{R}^3$. A projection of a knot K onto a plane in $\mathbb{R}^3$ is called *regular* if there are only finitely many multiple points which are all double points and no vertex of K is mapped onto a double point. There are sufficiently many regular projections of a knot. We can draw a picture of a regular projection of a knot in the way that at each double point the overcrossing line is marked. So a knot can be reconstructed from its regular projection. Now let us explain how we can get a presentation of G_K from a regular projection of K, by taking a trefoil for K as an illustration.

(0) First, give a regular projection of a knot K (Fig. 2.6).

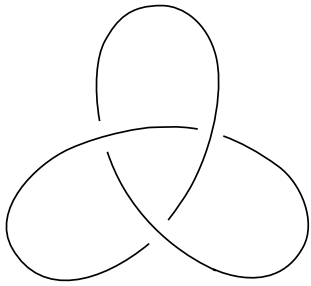


Fig. 2.6

(1) Give an orientation to K and divide K into arcs $c_1, \ldots, c_n$ so that c_i $(1 \leq i \leq n-1)$ is connected to c_{i+1} at a double point and c_n is connected to c_1 (Fig. 2.7).

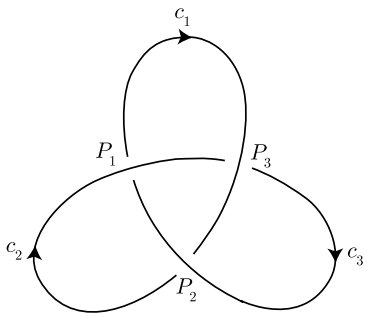


Fig. 2.7

(2) Take a base point b above K (for example $b = \infty$) and let x_i be a loop coming down from b, going once around under c_i from the right to the left, and returning to b (Fig. 2.8).

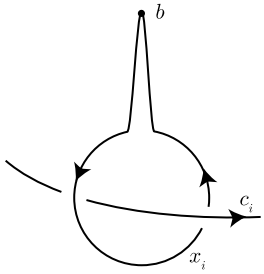


Fig. 2.8

(3) In general, one has the following two ways of crossing among c_i's at each double point. From the former case, one derives the relation $R_i = x_i x_k^{-1} x_{i+1}^{-1} x_k = 1$, and from the latter case one derives the relation $R_i = x_i x_k x_{i+1}^{-1} x_k^{-1} = 1$ (Fig. 2.9).

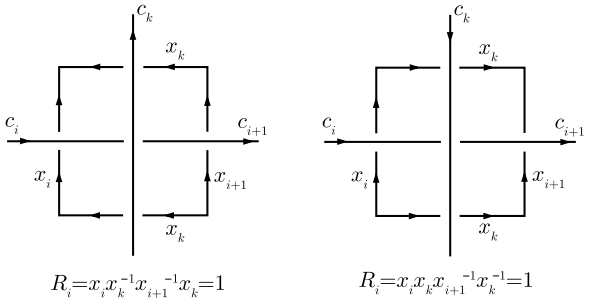


Fig. 2.9

Thus, we have n relations $R_1 = \cdots = R_n = 1$ for n double points $P_1, \ldots, P_n$, which give a presentation of G_K, $G_K = \langle x_1, \ldots, x_n \mid R_1 = \cdots = R_n = 1 \rangle$ (Fig. 2.10).

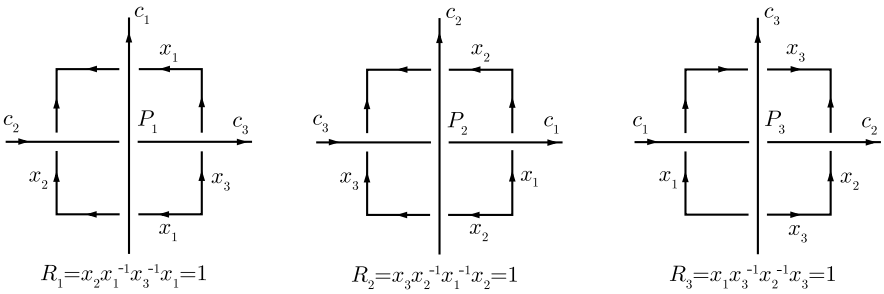


Fig. 2.10

Among these n relations we can derive any one from the other relations as follows. Let E be a plane, below K, on which we have a regular projection of K. Let C be an oriented circle such that a projection of K on E is lying inside C. Let γ be a path in X_K starting from the base point b to a fixed point Q on C and let $l := \gamma \vee C \vee \gamma^{-1}$. Note that $[l]$ is the identity in G_L. On the other hand, let l_i be a path in E starting from Q, going toward P_i and once around P_i with the same orientation as C, and returning Q. Then we see l is homotopic to $\prod_{i=1}^{n} \gamma \vee l_i \vee \gamma^{-1}$ (Fig. 2.11).

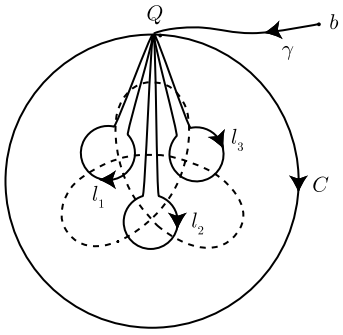


Fig. 2.11

Since a small circle around P_i corresponds to R_i or R_i^{-1}, there are $z_i \in F(x_1, \ldots, x_n)$ such that one has

$$\prod_{i=1}^{n} z_i R_i^{\pm 1} z_i^{-1} = 1. \tag{4}$$

Thus, G_K has a presentation of deficiency 1.

A presentation of G_K obtained in the way described above is called a *Wirtinger presentation*. As we can see from the form of each relation in (3), $x_1, \ldots, x_n$ are conjugate each other in G_K. Therefore, the Abelianization $G_K/[G_K, G_K] \simeq H_1(X_K)$ of G_K is an infinite cyclic group generated by the class of a meridian of K.

We can, of course, consider a knot in any orientable connected closed 3-manifold and define a tubular neighborhood, knot exterior etc similarly. The exterior $X_K = M \setminus \mathrm{int}(V_K)$ is an orientable compact connected 3-manifold with boundary being a 2-dimensional torus, and so X_K is collapsed to a 2-dimensional complex C with a single 0-cell. Since X_K has the Euler number 0, the knot group $G_K(M) := \pi_1(X_K) = \pi_1(C)$ has a presentation of deficiency 1. In general, $G_K(M)$ may not have a Wirtinger presentation (i.e., relations in (3) above).

An r-component *link* L is the image of an embedding of a disjoint union of r copies of S^1 into an oriented connected closed 3-manifold. So we can write $L = K_1 \cup \cdots \cup K_r$ where K_i's are mutually disjoint knots. A 1-component link is a knot. A *tubular neighborhood* V_L of $L = K_1 \cup \cdots \cup K_r$ is the union of tubular neighborhoods of K_i, $V_L = V_{K_1} \cup \cdots \cup V_{K_n}$ ($V_{K_i} \cap V_{K_j} = \emptyset$ for $i \neq j$). The *exterior* of L is $X_L := M \setminus \mathrm{int}(V_L)$ and the *link group* of L is defined by $G_L(M) := \pi_1(X_L) = \pi_1(M \setminus L)$. Like a knot group $G_K(M)$, $G_L(M)$ has a presentation of deficiency 1. When $M = S^3$ in particular, a regular projection of a link L is defined similarly to the case of a knot and G_L has a Wirtinger presentation. Here loops x_i and x_j are conjugate if and only if c_i and c_j are in the same component of a link and so the Abelianization $G_L/[G_L, G_L] \simeq H_1(X_L)$ of G_L is a free Abelian group of rank r generated by the classes of meridians of K_i, $1 \leq i \leq r$.

Finally, let us give the definition of equivalence among links. For links L, L' in an oriented connected closed 3-manifold M, we say that L and L' are *equivalent* if there is an isotopy $h_t : M \xrightarrow{\approx} M (0 \leq t \leq 1)$ such that $h_0 = \mathrm{id}_M$, $h_1(L) = L'$. For links in S^3, this condition is equivalent to the condition that there is an orientation-preserving homeomorphism $f : S^3 \xrightarrow{\approx} S^3$ such that $f(L) = L'$ [BZ, Proposition 1.10]. A quantity $\mathrm{inv}(L)$ defined on the set of all links is called a *link invariant* if $\mathrm{inv}(L) = \mathrm{inv}(L')$ for any two equivalent links L and L'. Likewise a *knot invariant* is a quantity defined on the set of all knots, which takes the same for any two equivalent knots. For example, a knot group is a knot invariant and a link group is a link invariant.

Next, let us recall basic materials concerning covering spaces. Let X be a connected space. A continuous map $h : Y \to X$ is called an (*unramified*) *covering* if for any $x \in X$, there is an open neighborhood U of x such that

$$\begin{cases} (1)\ h^{-1}(U) = \bigsqcup_{j \in J} V_j, \quad V_i \cap V_j = \emptyset \quad (i \neq j), \\ (2)\ h|_{V_j} : V_j \xrightarrow{\approx} U \quad \text{(homeomorphism)}, \end{cases}$$

where V_j is a connected component of $h^{-1}(U)$ and an open subset of Y (Fig. 2.12).

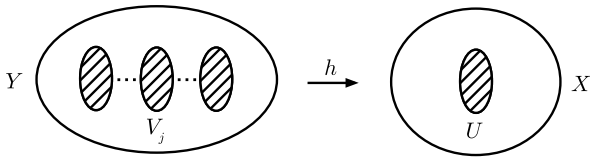


Fig. 2.12

A covering $h' : Y' \to X$ is called a *subcovering* of $h : Y \to X$ if there is a continuous map $\varphi : Y \to Y'$ such that $h' \circ \varphi = h$. Then φ is also a covering, and we denote by $C_X(Y, Y')$ the set of all such φ. If there is a homeomorphic $\varphi \in C_X(Y, Y')$, Y and Y' are said to be isomorphic over X. The set of isomorphisms $\varphi \in C_X(Y, Y)$ forms a group, called the group of *covering transformations* of $h : Y \to X$, and is denoted by $\mathrm{Aut}(Y/X)$.

The most basic fact in covering theory is the following lifting property of a path and its homotopy.

Proposition 2.7 *Let $h : Y \to X$ be a covering. For any path $\gamma : [0, 1] \to X$ and any $y \in h^{-1}(x)$ $(x = \gamma(0))$, there exists a unique lift $\hat{\gamma} : [0, 1] \to Y$ of γ (i.e., $h \circ \hat{\gamma} = \gamma$) with $\hat{\gamma}(0) = y$. Furthermore, for any homotopy γ_t $(t \in [0, 1])$ of γ with $\gamma_t(0) = \gamma(0)$ and $\gamma_t(1) = \gamma(1)$, there exists a unique lift of $\hat{\gamma}_t$ such that $\hat{\gamma}_t$ is the homotopy of $\hat{\gamma}$ with $\hat{\gamma}_t(0) = \hat{\gamma}(0)$ and $\hat{\gamma}_t(1) = \hat{\gamma}(1)$.*

In the following, we assume that any covering space is connected. By Proposition 2.7, the cardinality of the fiber $h^{-1}(x)$ is independent of $x \in X$. So we call $\#h^{-1}(x)$ the *degree* of $h : Y \to X$ which is denoted by $\deg(h)$ or $[Y : X]$. We define the right action of $\pi_1(X, x)$ on $h^{-1}(x)$ as follows. For $[l] \in \pi_1(X, x)$ and $y \in h^{-1}(x)$, we define $y.[l]$ to be the terminus $\hat{l}(1)$ where $\hat{l}$ is the lift of l with origin $\hat{l}(0) = y$. It is a transitive action such that the stabilizer of y is $h_*(\pi_1(Y, y))$ by Proposition 2.7 and hence one has a bijection $h^{-1}(x) \simeq h_*(\pi_1(Y, y))\backslash\pi_1(X, x)$. The induced representation $\rho_x : \pi_1(X, x) \to \mathrm{Aut}(h^{-1}(x))$ is called the *monodromy permutation representation* of $\pi_1(X, x)$, where $\mathrm{Aut}(h^{-1}(x))$ denotes the group of permutations on $h^{-1}(x)$ so that the multiplication $\sigma_1 \cdot \sigma_2$ is defined by the composite of maps $\sigma_2 \circ \sigma_1$ for $\sigma_1, \sigma_2 \in \mathrm{Aut}(h^{-1}(x))$. The representation ρ_x induces an isomorphism $\mathrm{Im}(\rho_x) \simeq \pi_1(X, x)/\bigcap_{y \in h^{-1}(x)} h_*(\pi_1(Y, y))$. It can be shown that the isomorphism class of a covering is determined by the equivalence class of the monodromy representation. On the other hand, the group $\mathrm{Aut}(Y/X)$ of covering transformations acts from the left on a fiber $h^{-1}(x)$. When this action is simply-transitive, namely, if the map $\mathrm{Aut}(Y/X) \ni \sigma \mapsto \sigma(y) \in h^{-1}(x)$ is bijective for $y \in h^{-1}(x)$, $h : Y \to X$ is called a *Galois covering*. This condition is independent of the choice of $x \in X$ and $y \in h^{-1}(x)$. For a Galois covering $h : Y \to X$, we call $\mathrm{Aut}(Y/X)$ the *Galois group* of Y over X and denote it by $\mathrm{Gal}(Y/X)$. The following is the main theorem of the Galois theory for coverings.

Theorem 2.8 (Galois correspondence) *The correspondence* $(h : Y \to X) \mapsto h_*(\pi_1(Y, y))(y \in h^{-1}(x))$ *gives rise to the following bijection*:

$$\{\textit{connected covering } h : Y \to X\}/\textit{isom. over } X$$
$$\xrightarrow{\sim} \{\textit{subgroup of } \pi_1(X, x)\}/\textit{conjugate}.$$

Furthermore, this bijection satisfies the following properties:

$h' : Y' \to X$ *is a subcovering of* $h : Y \to X \Leftrightarrow h'_*(\pi_1(Y', y'))$ $(y' \in h'^{-1}(x))$ *is a subgroup of* $h_*(\pi_1(Y, y))$ $(y \in h^{-1}(x))$ *up to conjugate.*
$h : Y \to X$ *is a Galois covering* $\Leftrightarrow h_*(\pi_1(Y, y))$ $(y \in h^{-1}(x))$ *is a normal subgroup of* $\pi_1(X, x)$. *Then one has* $\mathrm{Gal}(Y/X) \simeq \pi_1(X, x)/h_*(\pi_1(Y, y))$.

More generally, we can replace $\pi_1(X, x)$ *by* $\mathrm{Gal}(Z/X)$ *for a fixed Galois covering* $Z \to X$ *in the above bijection, and then we have a similar bijection*:

$$\{\textit{connected subcovering of } Z \to X\}/\textit{isom. over } X.$$
$$\xrightarrow{\sim} \{\textit{subgroup of } \mathrm{Gal}(Z/X)\}/\textit{conjugate}.$$

Thus, the fundamental group of a space X may be viewed as a group which controls the symmetry of the set of coverings of X. In particular, the covering $\tilde{h} : \tilde{X} \to X$ (unique up to isom. over X) which corresponds to the identity group of $\pi_1(X, x)$ is called the *universal covering* of X. The universal covering has the following properties (U):

$$\text{(U)} \quad \begin{cases} \text{(i) Fixing } \tilde{x} \in \tilde{X}, \text{ the map } C_X(\tilde{X}, Y) \ni \varphi \mapsto \varphi(\tilde{x}) \in h^{-1}(x) \\ \quad \text{is bijective for any covering } h : Y \to X \ (x = \tilde{h}(\tilde{x})). \\ \text{(ii) } \mathrm{Gal}(\tilde{X}/X) \simeq \pi_1(X, x) \ (x = \tilde{h}(\tilde{x})). \end{cases}$$

Example 2.9 The universal covering of S^1 is given by

$$\tilde{h} : \mathbb{R} \to S^1; \quad \tilde{h}(\theta) := \big(\cos(2\pi\theta), \sin(2\pi\theta)\big).$$

Let l be a loop starting from a base point x and going once around S^1 counterclockwise. Define the covering transformation $\sigma \in \mathrm{Gal}(\mathbb{R}/S^1)$ by $\sigma(\theta) := \theta + 1$. Then the correspondence $\sigma^n \mapsto [l^n]$ $(n \in \mathbb{Z})$ gives an isomorphism $\mathrm{Gal}(\mathbb{R}/S^1) \simeq \pi_1(S^1, x)$. Any subgroup $(\neq \{1\})$ of $\pi_1(X, x) = \langle [l] \rangle$ is given by $\langle [l^n] \rangle$ for some $n \in \mathbb{N}$ and the corresponding covering is given by

$$h_n : \mathbb{R}/n\mathbb{Z} \to S^1; \quad h_n(\theta \bmod n\mathbb{Z}) := \big(\cos(2\pi\theta), \sin(2\pi\theta)\big).$$

Example 2.10 The universal covering of a 2-dimensional torus $T^2 = S^1 \times S^1$ is the product of two copies of the universal covering S^1, namely,

$$\tilde{h} : \mathbb{R}^2 \to T^2;$$

$$\tilde{h}(\theta_1, \theta_2) := \big(\big(\cos(2\pi\theta_1), \sin(2\pi\theta_1)\big), \big(\cos(2\pi\theta_2), \sin(2\pi\theta_2)\big)\big).$$

Define the covering transformation $\sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{R}^2/T^2)$ by $\sigma_1(\theta_1, \theta_2) := (\theta_1 + 1, \theta_2), \sigma_2(\theta_1, \theta_2) := (\theta_1, \theta_2 + 1)$. Then the correspondence $\sigma_1 \mapsto [\alpha]$ (meridian), $\sigma_2 \mapsto [\beta]$ (longitude) gives an isomorphism $\mathrm{Gal}(\mathbb{R}^2/T^2) \simeq \pi_1(T^2)$.

Example 2.11 Let $L(p, q)$ be a lens space of type (p, q) (Example 2.5), where p and q are coprime integers. When $p = 0$, $L(0, \pm 1) = S^2 \times S^1$ and so the universal covering is given by $S^2 \times \mathbb{R}$. Assume $p \neq 0$ and let us construct the universal covering $L(p, q)$.[1] We identify S^1 with $\mathbb{R}/\mathbb{Z}$, D^2 with $(\mathbb{R}/\mathbb{Z} \times (0, 1]) \cup \{(0, 0)\}$, and regard a solid torus V as $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z} \times [0, 1]$, ∂V as $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. Let V_1, V_2, V_1', V_2' be copies of V. Let us consider the following map

$$f : \partial V_1 \to \partial V_2; \quad f(x, y) := \left(qx + \frac{y}{p}, px\right).$$

Since

$$\det \begin{pmatrix} q & p \\ \frac{1}{p} & 0 \end{pmatrix} = -1,$$

f is an orientation-reversing homeomorphism and $L(p, q)$ is obtained from the disjoint union of V_1 and V_2 by identifying ∂V_1 with ∂V_2 via f. Next, consider the following orientation-reversing homeomorphism

$$g : \partial V_1' \to \partial V_2'; \quad g(x, y) := (y, x).$$

The space obtained from the disjoint union of V_1' and V_2' by identifying $\partial V_1'$ with $\partial V_2'$ via g is S^3. Now define the map $h : S^3 = V_1' \cup_g V_2' \to L(p, q) = V_1 \cup_f V_2$ by

$$\begin{aligned} h|_{V_1'} : V_1' \to V_1; \quad & h|_{V_1'}(x, y, z) := \big(x, p(y - qx), z\big), \\ h|_{V_2'} : V_2' \to V_2; \quad & h|_{V_2'}(x, y, z) := (x, py, z). \end{aligned}$$

Then we see that h is well-defined and $h|_{V_i'}$ $(i = 1, 2)$ are both p-fold cyclic coverings, and hence h is a p-fold cyclic covering. Since S^3 is simply connected, $h : S^3 \to L(p, q)$ defined as above is the universal covering.

Example 2.12 Let $K \subset S^3$ be a knot, V_K a tubular neighborhood, $X_K := S^3 \setminus \mathrm{int}(V_K)$ the exterior of K, and $G_K := \pi_1(X_K)$ the knot group. Let α be a meridian of K. Since $G_K/[G_K, G_K]$ is the infinite cyclic group generated by the class of α, the map sending α to 1 defines a surjective homomorphism $\psi_\infty : G_K \to \mathbb{Z}$. Let $h_\infty : X_\infty \to X_K$ be the covering corresponding to $\mathrm{Ker}(\psi_\infty)$ in Theorem 2.8. The covering space X_∞ is independent of the choice of α and called the *infinite cyclic covering* of X_K. Let τ be the generator of $\mathrm{Gal}(X_\infty/X_K)$ corresponding to

[1] The following argument is due to S. Miyasaka, a graduate student at Kyoto University (2005).

$1 \in \mathbb{Z}$. For each $n \in \mathbb{N}$, $\psi_n : G_K \to \mathbb{Z}/n\mathbb{Z}$ be the composite of ψ_∞ with the natural homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, and let $h_n : X_n \to X_K$ be the covering corresponding to $\mathrm{Ker}(\psi_n)$. The space X_n is the unique subcovering of X_∞ such that $\mathrm{Gal}(X_n/X_K) \simeq \mathbb{Z}/n\mathbb{Z}$. We denote by the same τ for the generator of $\mathrm{Gal}(X_n/X_K)$ corresponding to 1 mod $n\mathbb{Z}$. The covering spaces X_n ($n \in \mathbb{N}$), X_∞ are constructed as follows. First, take a *Seifert surface* of K, an oriented connected surface Σ_K whose boundary is K. Let Y be the space obtained by cutting X_K along $X_K \cap \Sigma_K$. Let Σ^+, Σ^- be the surfaces, which are homeomorphic to $X_K \cap \Sigma_K$, as in the following picture (Fig. 2.13).

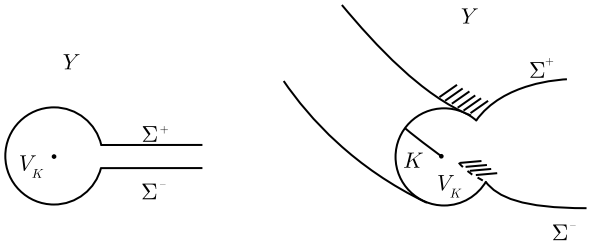


Fig. 2.13

Let $Y_0, \ldots, Y_{n-1}$ be copies of Y and let X_n be the space obtained from the disjoint union of all Y_i's by identifying Σ_0^+ with Σ_1^-, …, and Σ_{n-1}^+ with Σ_0^- (Fig. 2.14).

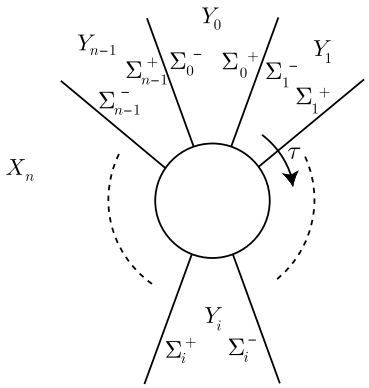


Fig. 2.14

Define $h_n : X_n \to X_K$ as follows: If $y \in Y_i \setminus (\Sigma_i^+ \cup \Sigma_i^-)$, define $h_n(y)$ to be the corresponding point of Y via $Y_i = Y$. If $y \in \Sigma_i^+ \cup \Sigma_i^-$, define $h_n(y)$ to be the corresponding point of Σ_K via $\Sigma_i^+, \Sigma_i^- \subset \Sigma_K$. By the construction, $h_n : X_n \to X_K$ is an n-fold cyclic covering. The generating covering transformation $\tau \in \mathrm{Gal}(X_n/X_K)$ is then given by the shift sending Y_i to Y_{i+1} ($i \in \mathbb{Z}/n\mathbb{Z}$). This construction is readily extended to the case $n = \infty$. Namely, taking copies Y_i ($i \in \mathbb{Z}$) of Y, let X_K^∞ be

the space obtained from the disjoint union of all Y_i's by identifying Σ_i^+ with Σ_{i+1}^- ($i \in \mathbb{Z}$) (Fig. 2.15).

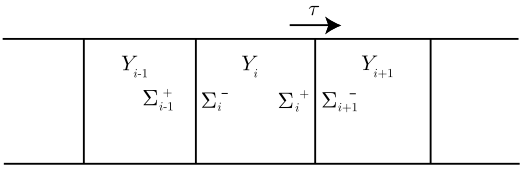


Fig. 2.15

The generating covering transformation $\tau \in \mathrm{Gal}(X_K^\infty / X_K)$ is given by the shift sending Y_i to Y_{i+1} ($i \in \mathbb{Z}$).

Example 2.13 The *Abelian fundamental group* of X is the Abelianization of $\pi_1(X)$, which we denote by $\pi_1^{\mathrm{ab}}(X)$. By the Hurewicz theorem, $H_1(X) \simeq \pi_1^{\mathrm{ab}}(X)$. The covering space corresponding to the commutator subgroup $[\pi_1(X), \pi_1(X)]$ in Theorem 2.8 is called the *maximal Abelian covering* of X which we denote by X^{ab}. Since $\pi_1^{\mathrm{ab}}(X) \simeq \mathrm{Gal}(X^{\mathrm{ab}}/X)$, we have a canonical isomorphism

$$H_1(X) \simeq \mathrm{Gal}\big(X^{\mathrm{ab}}/X\big).$$

Therefore, Abelian coverings of X are controlled by the homology group $H_1(X)$. This may be regarded as a topological analogue of unramified class field theory which will be presented in Example 2.44.

Finally, we shall consider ramified coverings. Let M, N be n-manifolds ($n \geq 2$) and let $f : N \to M$ be a continuous map. Set $S_N := \{y \in N \mid f$ is not a homeomorphism in a neighborhood of $y\}$ and $S_M := f(S_N)$. Let $D^k := \{x \in \mathbb{R}^k \mid \|x\| \leq 1\}$. Then $f : N \to M$ is called a *covering ramified over* S_M if the following conditions are satisfied:

$$\begin{cases} (1)\ f|_{N \setminus S_N} : N \setminus S_N \to M \setminus S_M \text{ is a covering.} \\ (2)\ \text{For any } y \in S_N, \text{ there are a neighborhood } V \text{ of } y, \text{ a neighborhood } U \\ \quad \text{of } f(y), \text{ a homeomorphism } \varphi : V \xrightarrow{\approx} D^2 \times D^{n-2}, \ \psi : U \xrightarrow{\approx} D^2 \times D^{n-2} \\ \quad \text{and an integer } e = e(y)(> 1) \text{ such that } (f_e \times \mathrm{id}_{D^{n-2}}) \circ \varphi = \psi \circ f. \end{cases}$$

Here, $g_e(z) := z^e$ for $z \in D^2 = \{z \in \mathbb{C} \mid |z| \leq 1\}$. The integer $e = e(y)$ is called the *ramification index* of y. We call $f|_{N \setminus S_N}$ the covering associated to f. If N is compact, $f|_{N \setminus S_N}$ is a finite covering. When $f|_{N \setminus S_N}$ is a Galois covering, f is called a *ramified Galois covering*.

Example 2.14 For a knot $K \subset S^3$, let V_K be a tubular neighborhood of K and $X_K = S^3 \setminus \mathrm{int}(V_K)$ the knot exterior. Let $h_n : X_n \to X_K$ be the n-fold cyclic covering defined in Example 2.12. Note that $h_n|_{\partial X_n} : \partial X_n \to \partial X_K$ is an n-fold cyclic covering of tori and a meridian of ∂X_n is given by $n\alpha$ where α is a meridian on

∂X_K. So we attach $V = D^2 \times S^1$ to X_n gluing ∂V with ∂X_n so that a meridian $\partial D^2 \times \{*\}$ coincides with $n\alpha$. Let M_n be the closed 3-manifold obtained in this way (Fig. 2.16).

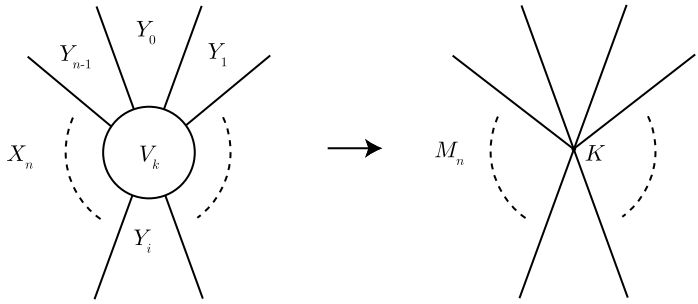


Fig. 2.16

Define $f_n : M_n \to S^3$ by $f_n|_{X_n} := h_n$ and $f_n|_V := f_n \times \mathrm{id}_{S^1}$. Then f_n is a covering ramified over K and the associated covering is h_n. $f_n : M_n \to S^3$ is called the completion of $h_n : X_n \to X_K$.

The completion given in Example 2.14 is called the *Fox completion* and such a completion can be constructed for any finite covering of a link exterior. In fact, the Fox completion can be defined for any covering (more generally, for a spread) of locally connected T_1-spaces [Fo2]. Here, let us explain an outline of the construction for a finite covering of a link exterior. Let M be an orientable connected closed 3-manifold and let L be a link in M. Let $X := M \setminus L$ and let $h : Y \to X$ be a given finite covering. Then there exists a unique covering $f : N \to M$ ramified over L such that the associated covering is $h : Y \to X$. Here, the uniqueness means that if there are such coverings N, N', then there is a homeomorphism $N \overset{\approx}{\to} N'$ so that the restriction to Y is the identity map. The construction of $f : N \to M$ is given as follows. Let g be the composite of h with the inclusion $X \hookrightarrow M$: $g : Y \to M$. To each open neighborhood U of $x \in M$, we associate a connected component $y(U)$ of $g^{-1}(U)$ in a way that $y(U_1) \subset y(U_2)$ if $U_1 \subset U_2$. Let N_x be the set of all such correspondences y. Let $N := \bigcup_{x \in M} N_x$ and define $f : N \to M$ by $f(y) = x$ if $y \in N_x$, namely, $N_x = f^{-1}(x)$. We give a topology on N so that the basis of open subsets of N are given by the subsets of the form $\{y \in N \mid y(U) = W\}$ where U ranges over all subsets of M and W ranges over all connected components of $f^{-1}(U)$. If $y \in Y$, we can associate to each open neighborhood U of $x = f(y)$ a unique connected component $y(U)$ of $g^{-1}(U)$ containing y and so we may regard $Y \subset N$. Intuitively, regarding $x \in L$ as the limit of its open neighborhood U as U smaller, $y \in N$ is defined as the limit of a connected component $y(U)$ of $g^{-1}(U)$. Let $V = D^2 \times D^1$ be a tubular neighborhood of L around $x = f(y) \in L$. Then it follows from the uniqueness of the Fox completion for the covering $h^{-1}(V \setminus L) \to V \setminus L$ that the condition (2) is satisfied in a neighborhood of $y \in f^{-1}(L)$.

Example 2.15 Let $L = K_1 \cup \cdots \cup K_r$ be a link in an orientable connected closed 3-manifold M, X_L the link exterior $G_L := \pi_1(X_L)$. Let α_i be a meridian of K_i $(1 \leq i \leq r)$. The map sending all α_i to 1 defines a surjective homomorphism $\psi_\infty : G_L \to \mathbb{Z}$. The infinite covering of X_L corresponding to $\mathrm{Ker}(\psi_\infty)$ is called the *total linking number covering* of X_L. For each $n \in \mathbb{N}$, let ψ_n be the composite of ψ_∞ with the natural homomorphism $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$: $\psi_n : G_L \to \mathbb{Z}/n\mathbb{Z}$. For an n-fold cyclic covering of X_L corresponding to $\mathrm{Ker}(\psi_n)$, we have the Fox completion M_n, which is an n-fold cyclic covering of M ramified over L.

Example 2.16 Let L be a 2-*bridge link* $B(a, b)$ $(0 < b < a, (a, b) = 1)$ presented by Schubert's normal form. If a is odd, L is a knot, and if a is even, L is a 2-component link (Fig. 2.17).

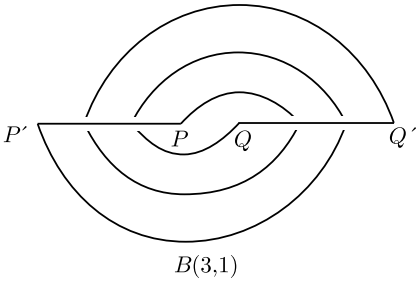


Fig. 2.17

The double covering of S^3 ramified over L is given by the lens space $L(a, b)$ (Example 2.5). To see this, divide $B(a, b)$ into two parts, say B_1 and B_2, where B_1 consists of 2 bridges (line segment $PP' \cup$ line segment QQ') and B_2 consists of 2 arcs passing under B_1 (arc $PQ' \cup$ arc $P'Q$ if a is odd and b is odd, arc $PQ \cup$ arc $P'Q'$ if a is odd and B is even, arc $PP' \cup$ arc QQ' if a is even). We see B_1 and B_2 as arcs inside 3-balls D_1^3 and D_2^3 respectively (Fig. 2.18).

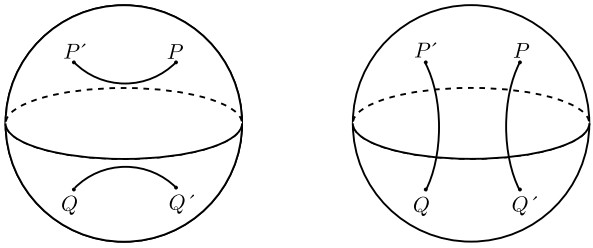


Fig. 2.18

According to the Heegaard decomposition $S^3 = D_1^3 \cup D_2^3$, L is decomposed as $L = B_1 \cup B_2$. Since the double covering of each D_i^3 ramified over B_i is a solid

torus V_i, the double covering M of S^3 ramified over L is a lens space. Further, we see that the image of a meridian α_1 on ∂V_1 (a lift of the bridge PP' to V_1) in ∂V_2 is given by $a[\beta_2] + b[\alpha_2]$ as a homology class (Fig. 2.19) and hence $M = L(a, b)$.

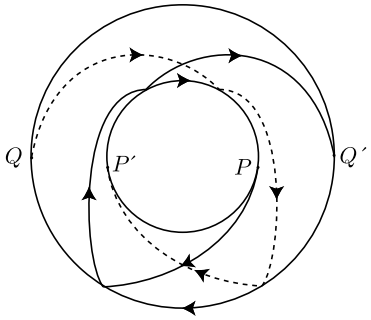


Fig. 2.19

2.2 The Case of Arithmetic Rings

Throughout this section, any ring is assumed to be a commutative ring with identity element and any homomorphism between rings is assumed to send the identity element to the identity element.

For a commutative ring R, let $\mathrm{Spec}(R)$ the set of prime ideals of R, called the *prime spectrum* of R. For $a \in R$, let $U_a := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid a \notin \mathfrak{p}\}$. The set $\mathrm{Spec}(R)$ is equipped with the topology, called the *Zariski topology*, whose open basis is given by $\mathcal{U} := \{U_a \mid a \in R\}$. On the topological space $\mathrm{Spec}(R)$, one has a sheaf of commutative rings $\mathcal{O}_{\mathrm{Spec}(R)}$ so that $\mathcal{O}_{\mathrm{Spec}(R)}(U_a) = R_a := \{\frac{r}{a^n} \mid a \in R, n \in \mathbb{Z} \geq 0\}$ $(a \neq 0)$. The pair $(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})$ is called an *affine scheme*. A *scheme* is defined to be a topological space X equipped with a sheaf $\mathcal{O}_X$ of commutative rings such that locally $(U, \mathcal{O}_X|_U)$, U being an open subset of X, is given as an affine scheme. Hereafter, we simply call $\mathrm{Spec}(R)$ an affine scheme, omitting the sheaf $\mathcal{O}_{\mathrm{Spec}(R)}$. A homomorphism $\psi : A \to B$ of commutative rings gives a continuous map $\varphi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ defined by $\varphi(\mathfrak{p}) := \psi^{-1}(\mathfrak{p})$ and a morphism $\psi^{\#} : \mathcal{O}_{\mathrm{Spec}(A)} \to \varphi_* \mathcal{O}_{\mathrm{Spec}(B)}$ of sheaves on $\mathrm{Spec}(A)$ defined by the natural homomorphism $A_a \to B_{\psi(a)}$ $(a \in A)$ induced by ψ. This correspondence gives rise to an anti-equivalence between the category of commutative rings and the category of affine schemes. Thus, algebraic properties concerning a ring R can be expressed in terms of geometric properties concerning an affine $\mathrm{Spec}(R)$. However, as is easily seen, the Zariski topology is too coarse to define topological notions such as loops on $\mathrm{Spec}(R)$ etc. As explained in the previous section, the fundamental group of X controls the symmetry of the set of all coverings of X. So considering the fundamental group which describes the homotopy type of a space is equivalent to considering

all coverings of the space. Similarly, we shall introduce the notion of an étale covering of $\mathrm{Spec}(R)$ which corresponds to a covering of a topological space and then define the étale fundamental group of $\mathrm{Spec}(R)$ following after the property (U) of the pointed universal covering in the previous section.

For a commutative ring R and $\mathfrak{p} \in \mathrm{Spec}(R)$, let $R_{\mathfrak{p}}$ denote the localization of R at $\mathfrak{p}$: $R_{\mathfrak{p}} := \{r/s \mid r \in R, s \in R \setminus \mathfrak{p}\}$. Let $\kappa(\mathfrak{p})$ denote the residue field of $R_{\mathfrak{p}}$: $\kappa(\mathfrak{p}) := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. A ring homomorphism $A \to B$ is said to be *finite étale* if

$$\begin{cases} (1)\ B \text{ is a finitely generated, flat } A\text{-module,} \\ (2)\ \text{For any } \mathfrak{p} \in \mathrm{Spec}(A), \\ \quad B \otimes_A \kappa(\mathfrak{p}) \simeq K_1 \times \cdots \times K_r \times (\kappa(\mathfrak{p})\text{-algebra isomorphism}), \end{cases}$$

where K_i is a finite separable extension of $\kappa(\mathfrak{p})$ $(1 \leq i \leq r)$.

In the rest of this section, a ring A shall denote an integrally closed domain and let F be the quotient field of A. An A-algebra B is called a *connected finite étale algebra* over A, if there is a finite separable extension K of F such that

$$\begin{cases} (1)\ B \text{ is the integral closure of } A \text{ in } K, \\ (2)\ \text{the inclusion map } A \hookrightarrow B \text{ is finite étale.} \end{cases}$$

An A-algebra B is called a *finite étale algebra* over A if B is isomorphic to the direct product $B_1 \times \cdots \times B_r$ of finite number of connected finite étale algebras $B_1, \ldots, B_r$ over A. An A-algebra B is called a *finite Galois algebra* over A if B is a connected finite étale algebra and if for any $\mathfrak{p} \in \mathrm{Spec}(A)$ and any algebraic closure Ω containing $\kappa(\mathfrak{p})$, the action of $\mathrm{Aut}(B/A) := \{\sigma \mid A\text{-algebra automorphism of } B\}$ on $\mathrm{Hom}_{A\text{-alg}}(B, \Omega) := \{\iota \mid A\text{-algebra homomorphism from } B \text{ to } \Omega\}$ defined by

$$\mathrm{Aut}(B/A) \times \mathrm{Hom}_{A\text{-alg}}(B, \Omega) \to \mathrm{Hom}_{A\text{-alg}}(B, \Omega);\ (\sigma, \iota) \mapsto \iota \circ \sigma$$

is simply transitive. This condition is independent of the choice of $\mathfrak{p}$ and Ω. If B is a finite Galois algebra over A, we write $\mathrm{Gal}(B/A)$ for $\mathrm{Aut}(B/A)$ and call it the *Galois group* of B over A. If K denotes the quotient field of B, B is a finite Galois algebra over A if and only if K/F is a finite Galois extension (see Example 2.17 below), and then $\mathrm{Gal}(B/A) = \mathrm{Gal}(K/F)$.

Example 2.17 (Field) Let F be a field. One has $\mathrm{Spec}(F) = \{(0)\}$. By definition, a connected finite étale algebra over F is nothing but a finite separable extension of F, and a étale algebra over F is an F-algebra which is isomorphic to the direct product of finite number of finite separable extensions of F. A finite Galois algebra over F is nothing but a finite Galois extension of F.

The most basic field in number theory is the *prime field* $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ for a prime number p. More generally, a *finite field* $\mathbb{F}_q$ consisting of q elements has the unique extension of degree n in a fixed separable closure $\overline{\mathbb{F}}_q$ for each $n \in \mathbb{N}$. On the other hand, over the field $\mathbb{Q}$ of rational numbers, there are infinitely many (non-isomorphic) quadratic extensions. Hence, $\mathbb{Q}$ is much more complicated than $\mathbb{F}_q$ from the viewpoint of field extensions.

Example 2.18 (Complete discrete valuation ring) A ring R is called a *discrete valuation ring* if the following conditions are satisfied:

$$\begin{cases} (1)\ R \text{ is a principal ideal domain,} \\ (2)\ R \text{ is a local ring with the maximal ideal } \mathfrak{p} \neq (0). \end{cases}$$

So $\mathrm{Spec}(R) = \{(0), \mathfrak{p}\}$. For $i \leq j$, let $f_{ij} : R/\mathfrak{p}^j \to R/\mathfrak{p}^i$ be the natural ring homomorphism. Then $\{R/\mathfrak{p}^i, f_{ij}\}$ is a projective system and the projective limit

$$\hat{R} := \varprojlim_{i \in \mathbb{N}} R/\mathfrak{p}^i := \left\{ (a_i) \in \prod_{i \in \mathbb{N}} R/\mathfrak{p}^i \mid f_{ij}(a_j) = a_i \ (i \leq j) \right\}$$

forms a subring of the direct product ring $\prod_i R/\mathfrak{p}^i$. Giving $R/\mathfrak{p}^i$ the discrete topology, we endow $\hat{R}$ with the induced topology of the direct product space $\prod_i R/\mathfrak{p}^i$. Then $\hat{R}$ becomes a topological ring and is called the $\mathfrak{p}$-*adic completion* of R. By the injective map $x \mapsto (x \bmod \mathfrak{p}^i)$, R is regarded as a subring of $\hat{R}$. If $R = \hat{R}$, we call R a *complete discrete valuation ring*. Let K be the quotient field of R. Let us fix a prime element π so that $\mathfrak{p} = (\pi)$. Any element $x \in K^\times$ is then written as $x = u\pi^n$ $(u \in R^\times, n \in \mathbb{Z})$ uniquely and so we set $v(x) := n$. Then v is a discrete valuation on K (v is independent of the choice of π). Namely, $v : K^\times \to \mathbb{Z}$ is a surjective homomorphism such that $v(x + y) \geq \min(v(x), v(y))$ $(\forall x, y \in K$; $v(0) := \infty)$. We call v the $\mathfrak{p}$-*adic* (*additive*) *valuation*. Take $c > 1$, define the $\mathfrak{p}$-adic multiplicative valuation by $|x| := c^{-v(x)}$. Then we have a metric d on K defined by $d(x, y) := |x - y|$. The topology on K defined in this way is independent of the choice of c. The completion $\hat{K}$ of the metric space (K, d) is called the $\mathfrak{p}$-*adic completion* of K. The metric d and the discrete valuation v are extended to those on $\hat{K}$ (written by the same d and v) so that $\hat{K}$ is a topological field. Now choose a system $S(\subset R)$ of complete representatives of $R/\mathfrak{p}$, where we choose 0 as a representative of the class 0 mod $\mathfrak{p}$). Then an element $x \in \hat{K}$ with $v(x) = n \in \mathbb{Z}$ is expanded uniquely as $x = a_n\pi^n + a_{n+1}\pi^{n+1} + \cdots$ $(a_i \in S)$, called the $\mathfrak{p}$-*adic expansion* of x. By the correspondence $x \mapsto (x \bmod \mathfrak{p}^i)$, the valuation ring $\{x \in \hat{K} \mid v(x) \geq 0\}$ of $\hat{K}$ is identified with $\hat{R}$. The quotient field $\hat{K}$ of $\hat{R}$ is called a *complete discrete valuation field*. The maximal ideal of $\hat{R}$ is the valuation ideal $\hat{\mathfrak{p}} := \{x \in \hat{K} \mid v(x) > 0\}$ and the residue field $\hat{R}/\hat{\mathfrak{p}}$ is identified with $R/\mathfrak{p}$. For example, $\mathbb{Z}_{(p)}$ for a prime number p is a discrete valuation ring. The completions of $\mathbb{Z}_{(p)}$ and $\mathbb{Q}$ with respect to the associated p-adic valuation are called the ring of *p-adic integers* and the *p-adic field*, respectively which are denoted by $\mathbb{Z}_p$ and $\mathbb{Q}_p$, respectively.

Let A be a complete discrete valuation ring and let F be the quotient field of A. Let K be a separable extension of F of degree n and let B be the integral closure of A in K. Then B is also a discrete valuation ring with the quotient field K. Furthermore, B is a free A-module of rank n. Let $\mathfrak{p}$ and $\mathfrak{P}$ be the maximal ideals of A and B, respectively. Then we can write $\mathfrak{p}B = \mathfrak{P}^e$ $(e \in \mathbb{N})$ uniquely. If $e = 1$, K/F is called an *unramified extension*, and if $e > 1$, K/F is called a *ramified extension*. The integer e is called the *ramification index* of K/F. If $e = n$, K/F is called a

totally ramified extension. Since $B \otimes_A \kappa(\mathfrak{p}) \simeq B/\mathfrak{P}^e$, one has

$$\begin{aligned} & B \text{ is a connected étale algebra over } A \\ \Leftrightarrow \quad & K/F \text{ is an unramified extension} \\ \Leftrightarrow \quad & \kappa(\mathfrak{P})/\kappa(\mathfrak{p}) \text{ is a separable extension of degree } n. \end{aligned}$$

Thus, the correspondences $K/F \mapsto B/A \mapsto \kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ gives rise to the following bijections:

$$\begin{aligned} & \{\text{finite unramified extension of } F\}/F\text{-isom.} \\ \xrightarrow{\sim} \ & \{\text{connected finite étale algebra over } A\}/A\text{-isom.} \\ \xrightarrow{\sim} \ & \{\text{finite separable extension of } \kappa(\mathfrak{p})\}/\kappa(\mathfrak{p})\text{-isom.} \end{aligned}$$

For the case that $A = \mathbb{Z}_p$ and $F = \mathbb{Q}_p$, B is called a *ring of* $\mathfrak{p}$*-adic integers* and K is called a $\mathfrak{p}$*-adic field* where $\mathfrak{p}$ stands for the maximal ideal of B.

Example 2.19 (Dedekind domain) A ring R is called a *Dedekind domain* if the following conditions are satisfied

$$\begin{cases} (1)\ R \text{ is a Noetherian integral domain (not a field),} \\ (2)\ R \text{ is integrally closed,} \\ (3) \text{ any non-zero prime ideal of } R \text{ is a maximal ideal.} \end{cases}$$

For example, a principal ideal domain is a Dedekind domain. In the rest of this book, we denote by $\mathrm{Max}(R)$ the set of maximal ideals of R. The condition (3) is equivalent to the condition that $\mathrm{Spec}(R) = \mathrm{Max}(R) \cup \{(0)\}$. In terms of ideal theory, a Dedekind domain R is characterized as follows: "Any non-zero ideal $\mathfrak{a}$ of R is expressed uniquely (up to order) as $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i$'s are distinct prime ideals of R and $e_i \in \mathbb{N}$". Let K be the quotient field of a Dedekind domain R. A finitely generated R-submodule$(\neq (0))$ of K is called a *fractional ideal* of R. For a fractional ideal $\mathfrak{a}$, we let $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subset R\}$. Then $\mathfrak{a}^{-1}$ is a fractional ideal of R and one has $\mathfrak{a}\mathfrak{a}^{-1} = R$. So any nonzero ideal $\mathfrak{a}$ of R is expressed uniquely (up to order) as $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i$'s are distinct prime ideals of R and $e_i \in \mathbb{Z}$. Hence, the set of all fractional ideals forms a group by multiplication, called the *fractional ideal group* of R, which is the free Abelian group generated by $\mathrm{Max}(R)$. The quotient group of the fractional ideal group by the subgroup consisting of principal ideals $(a) = aR$ $(a \in K^\times)$ is called the *ideal class group* of R.

Let R be a Dedekind domain. Since the localization $R_\mathfrak{p}$ of R at $\mathfrak{p} \in \mathrm{Max}(R)$ is a discrete valuation ring [Se2, Chap. I, Sect. 3], one has its completion $\hat{R}_\mathfrak{p}$ as in Example 2.18. The completed ring $\hat{R}_\mathfrak{p}$ is called the $\mathfrak{p}$*-adic completion* of R. The completion $K_\mathfrak{p}$ of the quotient field K of $R_\mathfrak{p}$ is defined similarly and is called the $\mathfrak{p}$*-adic completion* of K. We note that the localization $S^{-1}R$ of a Dedekind domain R with respect to any multiplicatively closed set $S(\neq R \setminus \{0\})$ is also a Dedekind domain.

Let A be a Dedekind domain and let F be the quotient field of A. Let K be a separable extension of F of degree n and let B be the integral closure of A in K. Then B is also a Dedekind domain with the quotient field K [ibid, Chap. I, Sect. 4]. Since $B \otimes_A A_{\mathfrak{p}}$ is a finitely generated flat $A_{\mathfrak{p}}$-module for any $\mathfrak{p} \in \mathrm{Spec}(A)$, B is a finitely generated flat A-module. For $\mathfrak{p} \in \mathrm{Max}(A)$, we can write in a unique manner $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where $\mathfrak{P}_i$'s are distinct prime ideals of B and $e_i \in \mathbb{N}$. We then say that $\mathfrak{P}_i$ *lies over* $\mathfrak{p}$. We say that $\mathfrak{P}_i$ is *unramified* in K/F if $e_i = 1$, and we say that $\mathfrak{P}_i$ is *ramified* in K/F if $e_i > 1$. The integer e_i is called the *ramification index* of $\mathfrak{P}_i$ in K/F. We say that $\mathfrak{p}$ is *unramified* in K/F if $e_1 = \cdots = e_r = 1$, and we say that $\mathfrak{p}$ is *ramified* in K/F if $e_i > 1$ for some i. We say that $\mathfrak{p}$ is *totally ramified* in K/F if $r = 1, e_1 = n$, and we say $\mathfrak{p}$ is *completely decomposed* in K/F if $r = n$, $e_1 = \cdots = e_r = 1$. We also say that $\mathfrak{p}$ is *inert* in K/F if $r = e_1 = \cdots = e_r = 1$. If any $\mathfrak{p} \in \mathrm{Max}(A)$ is unramified in K/F, K/F is called an *unramified extension*, and if there is a $\mathfrak{p} \in \mathrm{Max}(A)$ which is ramified K/F, K/F is called a *ramified extension*. Since $B \otimes_A \kappa(\mathfrak{p}) \simeq B/\mathfrak{P}_1^{e_1} \times \cdots \times B/\mathfrak{P}_r^{e_r}$, one has

$$B \text{ is a connected finite étale algebra over } A$$
$$\Leftrightarrow \quad K/F \text{ is an unramified extension.}$$

Since the étale fundamental group of a scheme is defined as a pro-finite group, we recall here some basic materials about pro-finite groups which will be used later on. Let (G_i, ψ_{ij}) $(i \in I)$ be a projective system consisting of finite groups G_i and homomorphisms $\psi_{ij} : G_j \to G_i$ $(i \leq j)$. Giving G_i the discrete topology, we endow the projective limit $\varprojlim_{i \in I} G_i$ with the induced topology as a subspace of the direct product space $\prod_{i \in I} G_i$. Then $\varprojlim_{i \in I} G_i$ becomes a topological group, called a *pro-finite group*. A pro-finite group is characterized as a topological group G which satisfies one of the following two properties: (1) G is a compact and totally disconnected, or (2) G has a fundamental system of neighborhoods of the identity consisting of compact and open subgroups of G. If each G_i is an l-group for a prime number l, the profinite $\varprojlim_i G_i$ is called a *pro-l group*.

Example 2.20 Let G be a group. Consider the set $\{N_i \mid i \in I\}$ of all normal subgroups of G with finite index and define $i \leq j$ if $N_j \subset N_i$. Let $\psi_{ij} : G/N_j \to G/N_i$ be the natural homomorphism for $i \leq j$. Then $(G/N_i, \psi_{ij})$ forms a projective system. The projective limit

$$\hat{G} := \varprojlim_i G/N_i$$

is called the *pro-finite completion* of G. If we consider only normal subgroups N_i of G such that each G/N_i is an l-group for a prime number l, the projective limit

$$\hat{G}(l) := \varprojlim_{G/N_i = l\text{-group}} G/N_i$$

is called the *pro-l completion* of G. If F is a free group on words $x_1, \ldots, x_r$, the pro-finite completion and pro-l completion of F (l being a prime number) is called

a *free pro-finite group* and a *free pro-l group* on $x_1, \ldots, x_r$ respectively. For example, the pro-l completion $\varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$ of the additive group $\mathbb{Z}$ is nothing but the additive group of the ring of l-adic integers $\mathbb{Z}_l$. The pro-finite completion $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$ is the direct product $\prod_l \mathbb{Z}_l$ (l running over all prime numbers) which is denoted by $\hat{\mathbb{Z}}$.

Let $\hat{F}$ be a free pro-finite group on words $x_1, \ldots, x_r$. For $R_1, \ldots, R_s \in \hat{F}$, we denote by $\langle\langle R_1, \ldots, R_s \rangle\rangle$ the smallest normal closed subgroup of F containing $R_1, \ldots, R_s$. If a pro-finite group $\mathfrak{G}$ is isomorphic to the quotient $\hat{F}/\langle\langle R_1, \ldots, R_s \rangle\rangle$, we write $\mathfrak{G}$ by the following form

$$\mathfrak{G} = \langle x_1, \ldots, x_r \mid R_1 = \cdots = R_s = 1 \rangle$$

and call it a presentation of $\mathfrak{G}$ in terms of generators and relations. We also define a presentation of a pro-l group similarly as a quotient of a free pro-l group $\hat{F}(l)$. For a pro-l group $\mathfrak{G}$, one has the following [NSW, Chap. III, Sect. 9] proposition.

Proposition 2.21 *A subset S of $\mathfrak{G}$ generates G topologically if and only if the set of residue classes S mod $\mathfrak{G}^l[\mathfrak{G}, \mathfrak{G}]$ generates $\mathfrak{G}/\mathfrak{G}^l[\mathfrak{G}, \mathfrak{G}]$ topologically. The cardinality of a minimal generator system of $\mathfrak{G}$ is given by the dimension of the 1st group cohomology group $H^1(\mathfrak{G}, \mathbb{F}_l)$ over $\mathbb{F}_l$. Further, the cardinality of minimal relations in a minimal generator system is given by the dimension of the 2nd group cohomology group $H^2(\mathfrak{G}, \mathbb{F}_l)$ over $\mathbb{F}_l$.*

Example 2.22 Let $\mathfrak{G}$ be a pro-finite group and let l be a prime number. By Zorn's lemma, one has a minimal element $\mathfrak{N}_l$ with respect to the inclusion relation among all normal subgroups $\mathfrak{N}$ of $\mathfrak{G}$ such that $\mathfrak{G}/\mathfrak{N}$ is a pro-l group. In fact, $\mathfrak{N}_l$ is characterized by the following two properties: (1) $\mathfrak{G}/\mathfrak{N}_l$ is a pro-l group, (2) if $\mathfrak{G}/\mathfrak{N}$ is a pro-l group, then $\mathfrak{N}_l \subset \mathfrak{N}$. We call $\mathfrak{G}/\mathfrak{N}_l$ the *maximal pro-l quotient* of $\mathfrak{G}$ and denote it by $\mathfrak{G}(l)$. The pro-l completion $\hat{G}(l)$ of a group G is the maximal pro-l quotient of the pro-finite completion $\hat{G}$ of G. For instance, $\mathbb{Z}_l$ is the maximal pro-l quotient of $\hat{\mathbb{Z}}$.

Now let A be an integrally closed domain again and let $X := \mathrm{Spec}(A)$. In order to define the étale fundamental group of X as a covariant functor, we need to consider all finite étale coverings of X including non-connected ones. We call a morphism $h : Y \to X$ of schemes a *finite étale covering* if there is a finite étale algebra $B = B_1 \times \cdots \times B_r$ (B_i being connected) over A such that $Y = \mathrm{Spec}(B) = \bigsqcup_{i=1}^r \mathrm{Spec}(B_i)$ (disjoint union of schemes) and h is the morphism associated to the inclusion $A \hookrightarrow B$. A finite étale covering $h' : Y' \to X$ is called a *subcovering* of $h : Y \to X$ if there is a morphism $\varphi : Y \to Y'$ such that $h' \circ \varphi = h$. We denote by $C_X(Y, Y')$ the set of such morphisms φ. If there is an isomorphism $\varphi \in C_X(Y, Y')$, we say that Y and Y' are isomorphic over X. The set of isomorphisms $\varphi \in C_X(Y, Y)$ forms a group, called the *group of covering transformations* of $h : Y \to X$, which denoted by $\mathrm{Aut}(Y/X)$.

Let $\mathfrak{p} \in X$ and fix an algebraically closed field Ω containing $\kappa(\mathfrak{p})$. It defines a morphism $\overline{x} : \mathrm{Spec}(\Omega) \to X$, called a *geometric base point* or simply a *base point* of X. For a finite étale covering $h : Y \to X$, we define the fiber of $\overline{x}$ by

$$\begin{aligned} F_{\overline{x}}(Y) &:= \mathrm{Hom}_X\big(\mathrm{Spec}(\Omega), Y\big) \\ &:= \big\{\overline{y} : \mathrm{Spec}(\Omega) \to Y \mid h \circ \overline{y} = \overline{x}\big\} \\ &\simeq \mathrm{Hom}_{A\text{-alg}}(B, \Omega), \end{aligned}$$

and, for $\varphi \in C_X(Y, Y')$, we define $F_{\overline{x}}(\varphi) : F_{\overline{x}}(Y) \to F_{\overline{x}}(Y')$ by $F_{\overline{x}}(\overline{y}) := \varphi \circ \overline{y}$ ($F_{\overline{x}}$ is called the *fiber functor* from the category of finite étale coverings of X to the category of sets). If Y is a connected (i.e., $Y = \mathrm{Spec}(B)$ for a connected finite étale algebra B over A), $\#F_{\overline{x}}(Y)$ is independent of the choice of $\overline{x}$. So we call $\#F_{\overline{x}}(Y)$ the *degree* of $h : Y \to X$ which is denoted by $\deg(h)$ or $[Y : X]$. A morphism $h : Y \to X$ is called a *finite Galois covering* if $Y = \mathrm{Spec}(B)$ for a finite Galois algebra B over A. In other words, Y is connected and the action of $\mathrm{Aut}(Y/X)$ on $F_{\overline{x}}(Y)$ defined by $(\sigma, \overline{y}) \mapsto \sigma \circ \overline{y}$ is simply transitive. This condition is independent of the choice of $\overline{x}$ (i.e., the choice of $\mathfrak{p}$ and Ω). For a finite Galois covering $h : Y \to X$, we call $\mathrm{Aut}(Y/X)$ the *Galois group* of Y over X and denote it by $\mathrm{Gal}(Y/X)$.

A pair of a finite étale covering $h : Y \to X$ and $\overline{y} \in F_{\overline{x}}(Y)$ is called a *pointed finite étale covering*. A morphism between pointed finite étale coverings (Y, y) and (Y', y') over X is given by a $\varphi \in C_X(Y, Y')$ satisfying $\varphi \circ \overline{y} = \overline{y}'$. Then we have the following theorem which is regarded as an analogue of the property (U)-(i) of the universal covering in Sect. 2.1.

Theorem 2.23 *There is a projective system $((Y_i \overset{h_i}{\to} X, \overline{y}_i), \varphi_{ij})$ of pointed finite Galois coverings such that for any finite étale covering $h : Y \to X$, the correspondence $C_X(Y_i, Y) \ni \varphi \mapsto \varphi \circ \overline{y}_i \in F_{\overline{x}}(Y)$ gives the following bijection*:

$$\varinjlim_i C_X(Y_i, Y) \simeq F_{\overline{x}}(Y).$$

Let $\tilde{X} = \varprojlim_i Y_i$ and $\tilde{x} = (\overline{y}_i)$. The pair $(\tilde{X}, \tilde{x})$ plays a role similar to the pointed universal covering of a manifold. Thus, as an analogue of (U)-(ii) in Sect. 2.1, we define the *étale fundamental group*[2] of X with base point $\overline{x}$ by

$$\pi_1(X, \overline{x}) := \mathrm{Gal}(\tilde{X}/X) := \varprojlim_i \mathrm{Gal}(Y_i/X),$$

where the projective limit is taken with respect to the composite

$$\mathrm{Gal}(Y_j/X) \simeq F_{\overline{x}}(Y_j) \overset{F_{\overline{x}}(\varphi_{ij})}{\to} F_{\overline{x}}(Y_i) \simeq \mathrm{Gal}(Y_i/X) \quad (i \le j).$$

[2] Although the étale fundamental group is often denoted by $\pi_1^{\text{ét}}(X, \overline{x})$, we write it by $\pi_1(X, \overline{x})$ or $\pi_1(X)$ for simplicity.

The group structure of $\overline{x}$ is independent of the choice of $\overline{x}$ (non-canonically isomorphic). Thus, we often write simply $\pi_1(X)$ omitting a base point and call it the étale fundamental group of X. By Theorem 2.23, for any finite étale covering Y over X, $\pi_1(X, \bar{x})$ acts on $F_{\overline{x}}(Y)$ continuously from the right. We write this action by $\overline{y}.\sigma$ $(\sigma \in \pi_1(X, \overline{x}), \overline{y} \in F_{\bar{x}}(Y))$.

Let A' be an integrally closed domain and let $A \to A'$ be a ring homomorphism. Let $f : X' := \mathrm{Spec}(A') \to X$ be the associated morphism of affine schemes. We fix an algebraic closure Ω' of $\kappa(\mathfrak{p}')$ and let $\overline{x}' : \mathrm{Spec}(\Omega') \to X'$ be the corresponding base point of X'. The composite $\overline{x} := f \circ \bar{x}' : \mathrm{Spec}(\Omega') \to X$ gives a base point of X. Then, for any finite étale covering $h : Y \to X$, one has the bijection

$$\begin{aligned} F_{\overline{x}'}(Y \times_X X') &= \mathrm{Hom}_{X'}\big(\mathrm{Spec}(\Omega'), Y \times_X X'\big) \\ &\simeq \mathrm{Hom}_X\big(\mathrm{Spec}(\Omega'), Y\big) = F_{\overline{x}}(Y). \end{aligned}$$

Here we note that $Y \times_X X'$ may not be connected, even though Y is connected. In the above bijection, let us take Y to be Y_i in Theorem 2.23 and let $\overline{y}'_i$ be the point in $F_{\overline{x}'}(Y_i \times_X X')$ corresponding to $\overline{y}_i \in F_{\bar{x}}(Y_i)$. Then for $\sigma' \in \pi_1(Y', \overline{y}')$, we have the unique $\sigma_i \in \mathrm{Gal}(Y_i/X)$ such that $\overline{y}'_i.\sigma' = \sigma_i \circ \overline{y}_i$. So letting $f_*(\sigma') := (\sigma_i)$, we have a continuous homomorphism $f_* : \pi_1(X', \overline{x}') \to \pi_1(X, \overline{x})$.

For a projective system $(Y_i \xrightarrow{h_i} X, \varphi_{ij})$ of (connected) finite étale coverings of X, the projective limit $Y = \varprojlim_i Y_i$ is called a (connected) *pro-finite étale covering*, and we let $F_{\overline{x}}(Y) := \{(\overline{y}_i) \mid \overline{y}_i \in F_{\overline{x}}(Y_i), \varphi_{ij} \circ \overline{y}_j = \overline{y}_i (1 \le j)\}$. For $\overline{y} \in F_{\overline{x}}(Y)$, we set $h_*(\pi_1(Y, \overline{y})) := \bigcap_i h_{i*}(\pi_1(Y_i, \overline{y}_i))$. If each Y_i is a Galois covering of X, we call Y a *pro-finite Galois covering* and define the *Galois group* of Y over X by $\mathrm{Gal}(Y/X) := \varprojlim_i \mathrm{Gal}(Y_i/X)$. The main theorem of the Galois theory (Galois correspondence) over X is stated as follows.

Theorem 2.24 (Galois correspondence) *The correspondence* $(h : Y \to X) \mapsto h_*(\pi_1(Y, \overline{y}))$ $(\bar{y} \in F_{\bar{x}}(Y))$ *gives rise to the following bijection*:

$$\begin{aligned} &\{\textit{connected pro-finite étale covering } h : Y \to X\}/\textit{isom. over } X \\ &\xrightarrow{\sim} \{\textit{closed subgroup of } \pi_1(X, \overline{x})\}/\textit{conjugate}. \end{aligned}$$

Furthermore, this bijection satisfies the followings:

$h : Y \to X$ is a connected finite étale covering $\Leftrightarrow$ $h_*(\pi_1(Y, \overline{y}))$ is an open subgroup.
$h' : Y' \to X$ is a subcovering of $h : Y \to X \Leftrightarrow h_*(\pi_1(Y, \overline{y}))(\bar{y} \in F_{\bar{x}}(Y))$ is a subgroup of $h'_*(\pi_1(Y', \overline{y}'))$ $(\bar{y}' \in F_{\bar{x}}(Y'))$ up to conjugate.
$h : Y \to X$ is a Galois covering $\Leftrightarrow$ $h_*(\pi_1(Y, \overline{y}))$ $(\overline{y} \in F_{\bar{x}}(Y))$ is a normal subgroup of $\pi_1(X, \overline{x})$. Then one has $\mathrm{Gal}(Y/X) \simeq \pi_1(X, \overline{x})/h_*(\pi_1(Y, \overline{y}))$.

More generally, we can replace $\pi_1(X, \overline{x})$ by $\mathrm{Gal}(Z/X)$ for a fixed pro-finite Galois covering $Z \to X$ in the above, and then we have a similar bijection:

$$\{\textit{connected subcovering of } Z \to X\}/\textit{isom. over } X.$$
$$\xrightarrow{\sim} \{\textit{closed subgroup of } \mathrm{Gal}(Z/X)\}/\textit{conjugate}.$$

Example 2.25 Let F be a field. Choose an algebraically closed field Ω containing F which defines a base point $\overline{x} : \mathrm{Spec}(\Omega) \to \mathrm{Spec}(F)$. Let $\overline{F}$ be the separable closure of F in Ω. The set of all finite Galois extensions of $K_i \subset \Omega$ of F is inductively ordered with respect to the inclusion relation and one has $\overline{F} = \varinjlim_i K_i$, the composite field of K_i's. Therefore, we can take $\mathrm{Spec}(K_i)$ for Y_i in Theorem 2.23 and hence

$$\pi_1\big(\mathrm{Spec}(F), \overline{x}\big) = \varprojlim_i \mathrm{Gal}(K_i/F) = \mathrm{Gal}(\overline{F}/F).$$

Let F be a finite field $\mathbb{F}_q$. For each $n \in \mathbb{N}$, there is the unique subfield $\mathbb{F}_{q^n} \subset \overline{\mathbb{F}}_q$ of degree n over $\mathbb{F}_q$ and so $\overline{\mathbb{F}}_q = \varinjlim_n \mathbb{F}_{q^n}$. Define the *Frobenius automorphism* $\sigma \in \mathrm{Gal}((\overline{\mathbb{F}}_q/\mathbb{F}_q)$ by

$$\sigma(x) = x^q \quad (x \in \overline{\mathbb{F}}_q).$$

For each $n \in \mathbb{N}$, the correspondence $\sigma|_{\mathbb{F}_{q^n}} \mapsto 1 \bmod n$ gives an isomorphism $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$. Hence, we have

$$\pi_1\big(\mathrm{Spec}(\mathbb{F}_q)\big) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Here, the Frobenius automorphism σ corresponds to $1 \in \hat{\mathbb{Z}}$.

Example 2.26 Let A be a complete discrete valuation ring with the quotient field F. Choose an algebraically closed field Ω containing F which defines a base point $\overline{x} : \mathrm{Spec}(\Omega) \to \mathrm{Spec}(A)$. Consider the set of all finite Galois algebras B_i over A in Ω, which is inductively ordered. Let K_i be the quotient field of B_i and let $\tilde{F} = \varinjlim_i K_i$, the composite field of K_i's. The field $\tilde{F}$ is called the *maximal unramified extension* of F in Ω. Then we can take $\mathrm{Spec}(B_i)$ for Y_i in Theorem 2.23 and hence

$$\pi_1\big(\mathrm{Spec}(A), \overline{x}\big) = \varprojlim_i \mathrm{Gal}(B_i/A) = \varprojlim_i \mathrm{Gal}(K_i/F) = \mathrm{Gal}(\tilde{F}/F).$$

Let $\mathfrak{p}$ be the maximal ideal of A. Let $f : \mathrm{Spec}(\kappa(\mathfrak{p})) \to \mathrm{Spec}(A)$ be the morphism associated to the natural homomorphism $A \to \kappa(\mathfrak{p})$. Choose an algebraically closed field Ω' containing $\kappa(\mathfrak{p})$. Let $\overline{x}' : \mathrm{Spec}(\Omega') \to \mathrm{Spec}(\kappa(\mathfrak{p}))$ be the associated base point and let $\overline{x} := f \circ \overline{x}'$. Since there is the bijection between the set of $\kappa(\mathfrak{p})$-isomorphism classes of finite separable extensions of $\kappa(\mathfrak{p})$ and the set of F-isomorphism classes of finite unramified extensions of F (Example 2.18), f induces the isomorphism $f_* : \pi_1(\mathrm{Spec}(\kappa(\mathfrak{p})), \overline{x}') \simeq \pi_1(\mathrm{Spec}(A), \overline{x})$.

Example 2.27 Let A a Dedekind domain with the quotient field F. Choose an algebraically closed field Ω containing F which defines a base point $\mathrm{Spec}(\Omega) \to$

$\mathrm{Spec}(A)$. Consider the set of all finite Galois algebras B_i over A in Ω, which is inductively ordered. Let K_i be the quotient field of B_i and let $\tilde{F} = \varinjlim_i K_i$, the composite of K_i's. The field $\tilde{F}$ is called the *maximal unramified extension* of F in Ω. Then we can take $\mathrm{Spec}(B_i)$ for Y_i in Theorem 2.23 and hence

$$\pi_1\big(\mathrm{Spec}(A), \overline{x}\big) = \varprojlim_i \mathrm{Gal}(B_i/A) = \varprojlim_i \mathrm{Gal}(K_i/F) = \mathrm{Gal}(\tilde{F}/F).$$

Example 2.28 Let A be an integrally closed domain and let $X = \mathrm{Spec}(A)$. Let Y_i's be finite Galois coverings of X in Theorem 2.23. Now let us consider only $Y_i \to X$ whose degree is a power of a fixed prime number l. We then define the *pro-l étale fundamental group* of X by

$$\pi_1(X, \overline{x})(l) := \varprojlim_{[Y:X]=\text{a power of } l} \mathrm{Gal}(Y_i/X).$$

In fact, $\pi_1(X, \overline{x})(l)$ is the maximal pro-l quotient of $\pi_1(X, \overline{x})$ (Example 2.22). Suppose A is a field F. Let $F(l)$ be the composite field of all finite l-extensions K_i of F (a finite l-extension means a finite Galois extension whose degree is a power of l) in Ω, called the *maximal l-extension* of F. Then one has $\pi_1(X, \overline{x})(l) = \mathrm{Gal}(F(l)/F)$. Suppose A is a Dedekind domain. Let $\tilde{F}(l)$ be the composite field of all finite unramified l-extensions of F in Ω, called the *maximal unramified l-extension* of F. Then one has $\pi_1(X, \overline{x})(l) = \mathrm{Gal}(\tilde{F}(l)/F)$.

A typical example of a Dedekind domain is the ring of integers of a number field and its localizations. Here we recall some basic material concerning number fields which shall be used later. A *number field* is an algebraic extension of the field of rational numbers $\mathbb{Q}$. The *ring of integers* of a number field k is the integral closure of $\mathbb{Z}$ in k and is denoted by $\mathcal{O}_k$. When the degree $[k : \mathbb{Q}]$ is finite, we often call k a *finite number field*. In the following, we assume k is a finite algebraic number field and set $n := [k : \mathbb{Q}]$ is finite. Since $\mathbb{Z}$ is a principal ideal domain, $\mathcal{O}_k$ is a Dedekind domain [Se2, Chap. I, Sect. 4]. Further, $\mathcal{O}_k$ is a free $\mathbb{Z}$-module of rank n. For $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$, $\mathfrak{p} \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ generated by a prime number p and the residue field $\kappa(\mathfrak{p}) = \mathcal{O}_k/\mathfrak{p}$ is a finite extension of $\mathbb{F}_p$. In this book, we shall often write $\mathbb{F}_\mathfrak{p}$ instead of $\kappa(\mathfrak{p})$ to indicate that it is a finite field. For an ideal $\mathfrak{a}(\neq (0))$, the quotient ring $\mathcal{O}_k/\mathfrak{a}$ is finite. The order $\#(\mathcal{O}_k/\mathfrak{a})$ is called the *norm* of $\mathfrak{a}$ and is denoted by $\mathrm{N}\mathfrak{a}$. For a fractional ideal $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$ ($e_\mathfrak{p} \in \mathbb{Z}$), the norm $\mathrm{N}\mathfrak{a}$ is defined by $\prod_\mathfrak{p} (\mathrm{N}\mathfrak{p})^{e_\mathfrak{p}}$. For a principal ideal (α) ($\alpha \in k^\times$), one has $\mathrm{N}(\alpha) = |\mathrm{N}_{k/\mathbb{Q}}(\alpha)|$ where $\mathrm{N}_{k/\mathbb{Q}}(\alpha) := \prod_{i=1}^n \alpha_i$ (α_i running over conjugates of α over $\mathbb{Q}$). The group of fractional ideals of $\mathcal{O}_k$ is called the *ideal group* of k which we denote by $I(k)$. It is a free Abelian group generated by $\mathrm{Max}(\mathcal{O}_k)$. The subgroup $P(k)$ consisting of principal fractional ideals is called the *principal ideal group* of k. The quotient group $I(k)/P(k)$ is called the *ideal class group* of k which we denote by $H(k)$.

For $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$, we denote by $\mathcal{O}_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of $\mathcal{O}_k$ and by $k_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of k, which are a ring of $\mathfrak{p}$-adic integers and a $\mathfrak{p}$-adic field in the sense of Example 2.18, respectively. So $k_\mathfrak{p}$ is equipped with the topology defined

by the $\mathfrak{p}$-adic valuation. Since the residue field $\mathbb{F}_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ is finite, $\mathcal{O}_\mathfrak{p}$ is a compact topological ring and $k_\mathfrak{p}$ is a locally compact topological field. An embedding of k into a locally compact topological field is given as one of the embeddings $k \hookrightarrow k_\mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$, $k \hookrightarrow \mathbb{R}$ or $k \hookrightarrow \mathbb{C}$. Among the conjugate fields of k (i.e., the images of embeddings $k \hookrightarrow \mathbb{C}$), let $\iota_i : k \simeq k^{(i)} \subset \mathbb{R}$ $(1 \le i \le r_1)$ be the real embeddings, and let $\iota_{r_1+j} : k \simeq k^{(r_1+j)} \subset \mathbb{C}$, $\overline{\iota}_{r_1+j} : k \simeq \overline{k}^{(r_1+j)} \subset \mathbb{C}$ $(1 \le j \le r_2)$ be the complex but not real embeddings where $\overline{\iota}_{r_1+j}$ and $\overline{k}^{(r_1+j)}$ mean the complex conjugate of ι_{r_1+j} and $k^{(r_1+j)}$, respectively and so $r_1 + 2r_2 = n$. For $a \in k$, we set $|a|_\mathfrak{p} := \mathrm{N}\mathfrak{p}^{-v_\mathfrak{p}(a)}$ ($\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$, $v_\mathfrak{p}$ is a $\mathfrak{p}$-adic additive valuation), $|a|_{\infty_i} := |\iota_j(a)|$ $(1 \le j \le r_1)$, $|a|_{\infty_{r_1+j}} := |\iota_{r_1+j}(a)|^2 = \iota_{r_1+j}(a)\overline{\iota}_{r_1+j}(a)$ $(1 \le j \le r_2)$. These give all nontrivial multiplicative valuations on k up to equivalence. We identify an embedding ι_j with the valuation $|\cdot|_{\infty_j}$ and call it an *infinite prime* of k and denote it by ∞_j or v_{∞_j} simply. The infinite primes $v_{\infty_1}, \ldots, v_{\infty_{r_1}}$ are called *real primes*, and $v_{\infty_{r_1+1}}, \ldots, v_{\infty_{r_1+r_2}}$ are called *complex primes*. We denote the set of infinite primes by $S_k^\infty := \{v_{\infty_1}, \ldots, v_{\infty_{r_1+r_2}}\}$ and often write v for an element of $S_k := \mathrm{Max}(\mathcal{O}_k) \cup S_k^\infty$. Then for $a \in k^\times$, the following product formula holds:

$$\prod_{v \in S_k} |a|_v = 1 \quad (a \in k^\times).$$

Intuitively, a scheme $\mathrm{Spec}(\mathcal{O}_k)$ is 'compactified' by adding S_k^∞. We thus write $\overline{\mathrm{Spec}(\mathcal{O}_k)} := \mathrm{Spec}(\mathcal{O}_k) \cup S_k^\infty$. An element $a \in k^\times$ is said to be *totally positive* if $\iota_j(a) > 0$ $(1 \le j \le r_1)$. We denote by $P^+(k)$ the group of principal fractional ideals generated by totally positive elements in k. The quotient group $I(k)/P^+(k)$ is called the *ideal class group in the narrow sense* or simply the *narrow ideal class group* of k, which we denote by $H^+(k)$. For a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_k$, we define the *discriminant* of k by $d_k := \det(\iota_i((\omega_j)))^2$. It is independent of the choice of basis $\omega_1, \ldots, \omega_n$.

Let K/k be a finite extension. For an infinite prime $v \in S_k^\infty$, we say that v is *ramified* in K/k if v is a real prime and is extended to a complex prime of K. Otherwise, namely, if v is a complex prime of k, or if v is a real prime and any extension of v to K is a real prime, then we say that v is *unramified* in K/k. According to the convention in algebraic number theory, we say that K/k is an *unramified extension*, if all $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$ and all $v \in S_k^\infty$ are unramified in K/k. When all $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$ are unramified and some infinite prime may be ramified in K/k, we say that K/k is an *unramified extension in the narrow sense* or simply a *narrow unramified extension*.

Since a number field k is embedded into $\mathbb{C}$ (or $\mathfrak{p}$-adic field) as we have seen above, the ring of integers $\mathcal{O}_k$ is not only a Dedekind domain but also enjoys some analytic properties. Here are most notable properties of a number field k of finite degree over $\mathbb{Q}$. Notations are as above:

Minkowski's theorem 2.29 *If $k \neq \mathbb{Q}$, then $|d_k| > 1$.*

The finiteness of ideal classes 2.30 The (narrow) ideal class group $H(k)$ (or $H^+(k)$) is a finite Abelian group.

Dirichlet's unit theorem 2.31 *The unit group $\mathcal{O}_k^\times$ is the direct product of the cyclic group of roots of unity in k and a free Abelian group of rank $r_1 + r_2 - 1$.*

Example 2.32 (Quadratic number field) Let m be a square-free integer ($\neq 1$) and let $k := \mathbb{Q}(\sqrt{m})$, a *quadratic number field*. Then one has

$$\mathcal{O}_k = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & m \equiv 1 \bmod 4, \\ \mathbb{Z}[\sqrt{m}] & m \equiv 2, 3 \bmod 4, \end{cases}$$

$$d_k = \begin{cases} m & m \equiv 1 \bmod 4, \\ 4m & m \equiv 2, 3 \bmod 4. \end{cases}$$

$$\mathcal{O}_k^\times \simeq \begin{cases} \{\pm 1\} \times \mathbb{Z} & m > 0, \\ \{\pm 1, \pm\sqrt{-1}\} & m = -1, \\ \{\pm 1, \pm\omega, \pm\omega^2\} \big(\omega := \frac{1+\sqrt{-3}}{2}\big) & m = -3, \\ \{\pm 1\} & m = -2,\ m < -3. \end{cases}$$

Example 2.33 (Cyclotomic field) Let n be an integer ≥ 3 and let $\zeta_n := \exp(\frac{2\pi\sqrt{-1}}{n})$. Let $k := \mathbb{Q}(\zeta_n)$, a *cyclotomic field*. Then k is a finite Abelian extension of $\mathbb{Q}$ whose Galois group $\mathrm{Gal}(k/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. This isomorphism is given as follows: For $g \in \mathrm{Gal}(k/\mathbb{Q})$, define $m(g)$ by $g(\zeta_n) = \zeta_n^{m(g)}$. Then the map $g \mapsto m(g)$ gives an isomorphism $\mathrm{Gal}(k/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Hence, $[k : \mathbb{Q}] = \phi(n)$(Euler function). One has $\mathcal{O}_k = \mathbb{Z}[\zeta_n]$ and $\mathcal{O}_k^\times \simeq \langle \pm\zeta_n \rangle \times \mathbb{Z}^{\phi(n)/2-1}$. The discriminant of k is given as follows: If $n = p^e$ for a prime number p,

$$d_k = \begin{cases} -p^{p^{e-1}(pe-e-1)} & p \equiv 3 \bmod 4 \text{ or } p = e = 2 \\ p^{p^{e-1}(pe-e-1)} & \text{otherwise.} \end{cases}$$

In general, for $n = p_1^{e_1} \cdots p_r^{e_r}$ the decomposition of prime factors of n, we have $d_k = d_{k_1}^{\frac{\phi(n)}{\phi(p_1^{e_1})}} \cdots d_{k_r}^{\frac{\phi(n)}{\phi(p_r^{e_r})}}$ where $k_i = \mathbb{Q}(\zeta_{p_i^{e_i}})$.

Example 2.34 Let $\mathcal{O}_\mathfrak{p}$ be a ring of $\mathfrak{p}$-adic integers and $k_\mathfrak{p}$ be its quotient field. By Example 2.26, one has

$$\pi_1\big(\mathrm{Spec}(\mathcal{O}_\mathfrak{p})\big) \simeq \pi_1\big(\mathrm{Spec}(\mathbb{F}_\mathfrak{p})\big) \simeq \hat{\mathbb{Z}}.$$

Since a separable closure of $\mathbb{F}_\mathfrak{p}$ is obtained by adjoining n-th roots of unity to $\mathbb{F}_\mathfrak{p}$ for all natural number n prime to $q := \mathrm{N}\mathfrak{p}$, the maximal unramified extension $\tilde{k}_\mathfrak{p}$ of $k_\mathfrak{p}$ is given by

$$\tilde{k}_\mathfrak{p} = k_\mathfrak{p}\big(\zeta_n \mid (n, q) = 1\big),$$

where ζ_n is a primitive n-th root of unity in $\overline{k}_\mathfrak{p}$. The element of $\pi_1(\mathrm{Spec}(\mathcal{O}_\mathfrak{p})) = \mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p})$ corresponding to the Frobenius automorphism $\sigma \in \pi_1(\mathrm{Spec}(\mathbb{F}_\mathfrak{p}) =$

$\mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$ under the above isomorphism is also called the *Frobenius automorphism*, denoted by the same σ, which is given by $\sigma(\zeta_n) = \zeta_n^q$.

Example 2.35 By Minkowski's theorem 2.29, there is no nontrivial connected finite étale algebra over $\mathbb{Z}$. Hence, we have

$$\pi_1\big(\mathrm{Spec}(\mathbb{Z})\big) = \{1\}.$$

Example 2.36 Let k be a number field of finite degree over $\mathbb{Q}$ and let $\mathcal{O}_k$ be the ring of integers of k. Let S be a finite set of maximal ideals of $\mathcal{O}_k$: $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By the finiteness of ideal classes (2.30), one finds $n_i \in \mathbb{N}$ for each i so that $\mathfrak{p}_i^{n_i} = (a_i)$, $a_i \in \mathcal{O}_k$. Set $A = \mathcal{O}_k[\frac{1}{a_1 \cdots a_n}]$. Since A is a localization of $\mathcal{O}_k$, A is a Dedekind domain and $\mathrm{Spec}(A) = \mathrm{Spec}(\mathcal{O}_k) \setminus S$. Choose an algebraically closed field Ω containing k which defines a base point $\overline{x} : \mathrm{Spec}(\Omega) \to \mathrm{Spec}(A)$. For a finite extension K/k in Ω, if any maximal ideal which is not contained in S is unramified in K/k, we say that K/k is *unramified outside* $S \cup S_k^\infty$ (S_k^∞ being the set of infinite primes of k). Let $k_S = \varinjlim_i k_i$ be the composite field of all finite Galois extensions k_i of k in Ω which are unramified outside $S \cup S_k^\infty$. The field k_S is called the *maximal Galois extension of k unramified outside* $S \cup S_k^\infty$. We can take $\mathrm{Spec}(k_i)$ for Y_i in Theorem 2.23 and hence

$$\pi_1\big(\mathrm{Spec}(\mathcal{O}_k) \setminus S, \overline{x}\big) = \mathrm{Gal}(k_S/k) = \varprojlim_i \mathrm{Gal}(k_i/k).$$

We denote this pro-finite group by $G_S(k)$. In the case $k = \mathbb{Q}$, we shall simply write G_S. For a prime number l, let $k_S(l)$ be *the maximal l-extension of k unramified outside* $S \cup S_k^\infty$. We then have $G_S(k)(l) = \mathrm{Gal}(k_S(l)/k)$.

Finally, we shall review some materials about ramified extensions over a Dedekind domain. Let A be a Dedekind domain with the quotient field F. Let K be a finite separable extension of F and let B be the integral closure of A in K. The morphism $f : N := \mathrm{Spec}(B) \to M := \mathrm{Spec}(A)$ induced from the inclusion $A \hookrightarrow B$ is called a *ramified covering* if K/F a ramified extension. The information on which $\mathfrak{P} \in \mathrm{Max}(B)$ or $\mathfrak{p} \in \mathrm{Max}(A)$ is ramified is detected by the different or the relative discriminant for B/A. Let $\iota_j : K \to \overline{F}$ $(1 \le j \le n)$ be all embeddings of K into a separable closure $\overline{F}$ of F. The trace $\mathrm{Tr}_{K/F}$ and the norm $\mathrm{N}_{K/F}$ are defined by $\mathrm{Tr}_{K/F}(a) := \iota_1(a) + \cdots + \iota_n(a)$ and $\mathrm{N}_{K/F}(a) := \iota_1(a) \cdots \iota_n(a)$, respectively. Let $\mathfrak{b} := \{b \in K \mid \mathrm{Tr}_{K/F}(ab) \in A \ \forall a \in B\}$. We easily see $\mathfrak{b}$ is a fractional ideal containing B. We then define the *different* of B/A by $\mathfrak{d}_{B/A} := \mathfrak{b}^{-1}$ and the *relative discriminant* of B/A by $d_{B/A} := \mathrm{N}_{K/F}(\mathfrak{d}_{B/A})$. If K/F is a finite extension of number fields of finite degree over $\mathbb{Q}$, we denote simply by $d_{K/F}$ the relative discriminant $d_{\mathcal{O}_K/\mathcal{O}_F}$ and call it the *relative discriminant* of K/F. In particular, $d_{k/\mathbb{Q}}$ coincides with the ideal of $\mathbb{Z}$ generated by the discriminant d_k. Now, as for the ramification, we have the following:

$$\begin{aligned} &\mathfrak{P} \text{ is ramified in } K/F \iff \mathfrak{P} | \mathfrak{d}_{B/A} \\ &\mathfrak{p} \text{ is ramified in } K/F \iff \mathfrak{p} | d_{B/A}. \end{aligned} \tag{2.1}$$

Therefore, only finitely many $\mathfrak{p} \in \mathrm{Max}(A)$ are ramified in K/F. Let S_F be the set of $\mathfrak{p} \in \mathrm{Max}(A)$ ramified in K/F and let $S_K := f^{-1}(S_F)$. We call $f|_{N\setminus S_K} : N \setminus S_K \to M \setminus S_F$ the *associated finite étale covering*. If $f|_{N\setminus S_K}$ is a Galois covering, f is called a *ramified Galois covering*. This condition amounts to K/F being a Galois extension. Finally, K/F is called a *tamely ramified extension*, if for any $\mathfrak{P} \in \mathrm{Max}(B)$ ramified in K/F, the ramification index of $\mathfrak{P}$ is prime to the characteristic of the residue field $\kappa(\mathfrak{P})$. Here if the characteristic of $\kappa(\mathfrak{P})$ is zero, no condition is meant. Unless a ramification is tame, i.e., the ramification index of $\mathfrak{P}$ is divisible by the positive characteristic of $\kappa(\mathfrak{P})$, then it is called a *wild ramification*. Let Ω be an algebraically closed field containing F which defines a base point $\overline{x} : \mathrm{Spec}(\Omega) \to X := \mathrm{Spec}(F)$, and let F^t be the composite field of all finite tamely ramified extensions K_i of F in Ω. The field F^t is called the *maximal tamely ramified extension* of F. Then we define the *tame fundamental group* of X by

$$\pi_1^t(X, \overline{x}) = \varprojlim_{K_i} \mathrm{Gal}(K_i/F) = \mathrm{Gal}\big(F^t/F\big),$$

where the projective limit is taken over all finite tamely ramified extensions K_i/F in Ω.

Example 2.37 Let k be a number field of finite degree over $\mathbb{Q}$ and let d_k be the discriminant of k. By (2.1), $\mathrm{Spec}(\mathcal{O}_k) \to \mathrm{Spec}(\mathbb{Z})$ is a finite covering which is ramified over primes (p), $p|d_k$, and $\mathrm{Spec}(\mathcal{O}_k[1/d_k]) \to \mathrm{Spec}(\mathbb{Z}[1/d_k])$ is the associated étale covering.

Example 2.38 Let p be a fixed prime number. For $n \in \mathbb{N}$, let $\zeta_{p^n} := \exp(\frac{2\pi\sqrt{-1}}{p^n})$ and $k_n := \mathbb{Q}(\zeta_{p^n})$. Set $\mathcal{O}_n := \mathcal{O}_{k_n}$, $M_n := \mathrm{Spec}(\mathcal{O}_n)$ and $X_n := \mathrm{Spec}(\mathcal{O}_n[\frac{1}{p}])$ for simplicity. By Example 2.33 and (2.1), the natural map $M_n \to M_0 = \mathrm{Spec}(\mathbb{Z})$ is a Galois covering ramified over (p), and $X_n \to X_0 = \mathrm{Spec}(\mathbb{Z}[\frac{1}{p}])$ is the associated étale covering. The Galois group is given by

$$\mathrm{Gal}(M_n/M_0) = \mathrm{Gal}(X_n/X_0) = \mathrm{Gal}(k_n/k_0) \simeq \big(\mathbb{Z}/p^n\mathbb{Z}\big)^\times.$$

By the natural maps $M_{n+1} \to M_n$ and $X_{n+1} \to X_n$, $M_\infty := \varprojlim_n M_n$ is a pro-finite ramified Galois covering over M_0 and $X_\infty := \varprojlim_n X_n$ is a pro-finite Galois covering over X_0. Let $k_\infty := \varinjlim_n k_n = \mathbb{Q}(\zeta_{p^n} \mid n \geq 1)$. Then the Galois group of M_∞ over M_0 is given by

$$\mathrm{Gal}(M_\infty/M_0) = \mathrm{Gal}(X_\infty/X_0) = \mathrm{Gal}(k_\infty/\mathbb{Q}) \simeq \varprojlim_n \big(\mathbb{Z}/p^n\mathbb{Z}\big)^\times = \mathbb{Z}_p^\times.$$

The ramification of (p) is as follows: Since the minimal polynomial of ζ_{p^n} over $\mathbb{Q}$ is $f(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$ and $f(1+X) \equiv X^{p^{n-1}(p-1)} \bmod p$, we have $p\mathcal{O}_n = \mathfrak{p}^{p^{n-1}(p-1)}$, where $\mathfrak{p} = (\zeta_{p^n} - 1)$. The ramification index $p^{n-1}(p-1)$ is same as the covering degree $[k_n : \mathbb{Q}] = \phi(p^n)$ and so (p) is totally ramified in $M_n \to M_0$.

Example 2.39 Let $k_\mathfrak{p}$ be a $\mathfrak{p}$-adic field with $q = \mathrm{N}\mathfrak{p}$ and let $X = \mathrm{Spec}(k_\mathfrak{p})$. Choose an algebraically closed field Ω containing $k_\mathfrak{p}$ and let $\overline{k}_\mathfrak{p}$ be the algebraic closure of $k_\mathfrak{p}$ in Ω. By Example 2.34, the maximal unramified extension $\tilde{k}_\mathfrak{p}$ of $k_\mathfrak{p}$ is given by $k_\mathfrak{p}(\zeta_n \mid (n,q) = 1)$, where ζ_n is a primitive n-th root of unity in $\overline{k}_\mathfrak{p}$ so that $\zeta_n^m = \zeta_{n/m}$ for $m|n$. The kernel of the natural homomorphism $\pi_1(X) = \mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p}) \to \pi_1(\mathrm{Spec}(\mathcal{O}_\mathfrak{p})) = \mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p})$ induced by the inclusion $\mathcal{O}_\mathfrak{p} \hookrightarrow k_\mathfrak{p}$ is called the *inertia group* of $k_\mathfrak{p}$ which we denote by $I_{k_\mathfrak{p}}$. The tame fundamental group $\pi_1^t(X)$ will be described as an extension of $\mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p})$ by the maximal tame quotient $I_{k_\mathfrak{p}}^t$ of $I_{k_\mathfrak{p}}$ as follows. Let π be a prime element of $k_\mathfrak{p}$. Then the maximal tamely ramified extension $k_\mathfrak{p}^t$ of $k_\mathfrak{p}$ is given by

$$k_\mathfrak{p}^t = \tilde{k}_\mathfrak{p}\big(\sqrt[n]{\pi} \mid (n,q) = 1\big).$$

We define the *monodromy* $\tau \in \mathrm{Gal}(k_\mathfrak{p}^t/k_\mathfrak{p})$ by

$$\tau(\zeta_n) = \zeta_n, \qquad \tau(\sqrt[n]{\pi}) = \zeta_n \sqrt[n]{\pi}.$$

Then τ is a topological generator of $I_{k_\mathfrak{p}}^t := \mathrm{Gal}(k_\mathfrak{p}^t/k_\mathfrak{p})$, the maximal tame quotient of $I_{k_\mathfrak{p}}$, and gives the following isomorphism

$$\mathrm{Gal}\big(k_\mathfrak{p}^t/\tilde{k}_\mathfrak{p}\big) \simeq \varprojlim_{(n,q)=1} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}^{(q')},$$

where τ corresponds to $1 \in \hat{\mathbb{Z}}^{(q')}$. Hence, we have the following short exact sequence:

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{Gal}(k_\mathfrak{p}^t/\tilde{k}_\mathfrak{p}) & \to & \mathrm{Gal}(k_\mathfrak{p}^t/k_\mathfrak{p}) & \to & \mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p}) & \to & 1. \\ & & \wr\downarrow & & & & \wr\downarrow & & \\ & & \hat{\mathbb{Z}}^{(q')} & & & & \hat{\mathbb{Z}} & & \end{array}$$

We define an extension of the Frobenius automorphism $\sigma \in \mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p})$ to $\mathrm{Gal}(k_\mathfrak{p}^t/k_\mathfrak{p})$, denoted by the same σ, by

$$\sigma(\zeta_n) = \zeta_n^q, \qquad \sigma(\sqrt[n]{\pi}) = \sqrt[n]{\pi}.$$

Then τ and σ are subject to the relation

$$\sigma\tau = \tau^q\sigma.$$

Thus, we have

$$\pi_1^t(X) = \mathrm{Gal}\big(k_\mathfrak{p}^t/k_\mathfrak{p}\big) = \big\langle \tau, \sigma \mid \tau^{q-1}[\tau,\sigma] = 1 \big\rangle.$$

We note that for a prime number l prime to q, the pro-l fundamental group $\pi_1(\mathrm{Spec}(k_\mathfrak{p}))(l)$ has a similar presentation.

Example 2.40 Let k be a number field of finite degree over $\mathbb{Q}$. Let S be a finite subset of $\mathrm{Max}(\mathcal{O}_k)$ and let $X := \mathrm{Spec}(\mathcal{O}_k) \setminus S$. Let k_S be the maximal Galois extension of k unramified outside $S \cup S_k^\infty$ (Example 2.36). Take a $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_k)$ and let $k_\mathfrak{p}$ be the $\mathfrak{p}$-adic field. Choose an algebraic closure $\overline{k}_\mathfrak{p}$ of $k_\mathfrak{p}$ and hence a base point $\overline{x} : \mathrm{Spec}(\overline{k}_\mathfrak{p}) \to \mathrm{Spec}(k_\mathfrak{p})$. Combining $\overline{x}$ with the natural morphism $\mathrm{Spec}(k_\mathfrak{p}) \to X$, we have a base point of X, $\overline{y} : \mathrm{Spec}(\overline{k}_\mathfrak{p}) \to X$. This defines an embedding $k_S \hookrightarrow \overline{k}_\mathfrak{p}$ over k and induces the homomorphism

$$\varphi_\mathfrak{p} : \pi_1\big(\mathrm{Spec}(k_\mathfrak{p}), \overline{x}\big) = \mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p}) \to \pi_1(X, \overline{y}) = G_S(k).$$

The embedding $k_S \hookrightarrow \overline{k}_\mathfrak{p}$ over k defines a prime $\overline{\mathfrak{p}}$ in k_S over $\mathfrak{p}$. Then the image of $\varphi_\mathfrak{p}$ coincides with the decomposition group of $\overline{\mathfrak{p}}$

$$D_{\overline{\mathfrak{p}}} := \big\{ g \in G_S(k) \mid g(\overline{\mathfrak{p}}) = \overline{\mathfrak{p}} \big\}.$$

Hereafter, we suppose an embedding $k_S \hookrightarrow \overline{k}_\mathfrak{p}$ and hence $\overline{\mathfrak{p}}$ is fixed, and we call $D_{\overline{\mathfrak{p}}}$ the *decomposition group over* $\mathfrak{p}$ in k_S/k and denote by $D_\mathfrak{p}$. Similarly, we call the image of the inertia group $I_{k_\mathfrak{p}}$ under $\varphi_\mathfrak{p}$ the *inertia group over* $\mathfrak{p}$ in k_S/k and denote by $I_\mathfrak{p}$. If we replace an embedding $k_S \hookrightarrow \overline{k}_\mathfrak{p}$ by another one, $D_\mathfrak{p}$ and $I_\mathfrak{p}$ are changed to some conjugate subgroups in $G_S(k)$.

Suppose $\mathfrak{p} \notin S$. Then $\mathfrak{p}$ is unramified in k_S/k, namely, $I_\mathfrak{p} = 1$. So $\varphi_\mathfrak{p}$ factors through $\mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p})$. We call the image $\sigma_\mathfrak{p} := \varphi_\mathfrak{p}(\sigma) \in G_S(k)$ of the Frobenius automorphism $\sigma \in \mathrm{Gal}(\tilde{k}_\mathfrak{p}/k_\mathfrak{p})$ the *Frobenius automorphism over* $\mathfrak{p}$. If we replace an embedding $k_S \hookrightarrow \overline{k}_\mathfrak{p}$ by another one, $\sigma_\mathfrak{p}$ is changed to a conjugate in $G_S(k)$. Therefore in an Abelian quotient of $G_S(k)$, the image of $\sigma_\mathfrak{p}$ is uniquely determined.

Although we have dealt with étale fundamental groups in this section, one has also the theories of étale (co)homology and higher homotopy groups for schemes which are defined by a simplicial method, similar to the method in topology (cf. [Go2, Go3, Go4, AM, Frl]). For example, $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ and $\mathrm{Spec}(\mathbb{F}_\mathfrak{p})$ are étale homotopy equivalent. For recent investigations on the subject, we refer to [Sc2] and references therein.

2.3 Class Field Theory

The *Abelian fundamental group* of $X = \mathrm{Spec}(A)$ is the Abelianization of the étale fundamental group $\pi_1(X)$ and is denoted by $\pi_1^{\mathrm{ab}}(X)$. The pro-finite covering of X corresponding to the closed commutator subgroup $[\pi_1(X), \pi_1(X)]$ is called the *maximal Abelian covering* of X which we denote by X^{ab}. So $\pi_1^{\mathrm{ab}}(X) = \mathrm{Gal}(X^{\mathrm{ab}}/X)$. If A is a field F, one has $\pi_1^{\mathrm{ab}}(\mathrm{Spec}(F)) = \mathrm{Gal}(F^{\mathrm{ab}}/F)$ where F^{ab} is the *maximal Abelian extension* of F, the composite field of all finite Abelian extensions of F. For a Dedekind domain A, let F be the quotient field of A.

Then one has $\pi_1^{\mathrm{ab}}(\mathrm{Spec}(A)) = \mathrm{Gal}(\tilde{F}^{\mathrm{ab}}/F)$ where $\tilde{F}^{\mathrm{ab}}$ is the *maximal unramified Abelian extension* of F, the composite field of all finite unramified Abelian extensions of F. *Class field theory* for a number field k describes the Abelian fundamental group $\pi_1^{\mathrm{ab}}(\mathrm{Spec}(k)) = \mathrm{Gal}(k^{\mathrm{ab}}/k)$ in terms of the base field k. Its local version for a $\mathfrak{p}$-adic field $k_{\mathfrak{p}}$, the theory describing $\pi_1^{\mathrm{ab}}(\mathrm{Spec}(k_{\mathfrak{p}})) = \mathrm{Gal}(k_{\mathfrak{p}}^{\mathrm{ab}}/k_{\mathfrak{p}})$ in terms of the base field $k_{\mathfrak{p}}$, is called *local class field theory*. Since for a number field k, $\pi_1^{\mathrm{ab}}(\mathrm{Spec}(k)) = \varprojlim_S \pi_1^{\mathrm{ab}}(\mathrm{Spec}(\mathcal{O}_k) \setminus S) = \varprojlim_S \mathrm{Gal}(k_S^{\mathrm{ab}}/k)$ (S running over finite subsets of $\mathrm{Max}(\mathcal{O}_k)$), class field theory amounts to describing $G_S(k)^{\mathrm{ab}} = \pi_1^{\mathrm{ab}}(\mathrm{Spec}(\mathcal{O}_k) \setminus S) = \mathrm{Gal}(k_S^{\mathrm{ab}}/k)$ in terms of k and S, where k_S^{ab} is the maximal Abelian extension of k unramified outside $S \cup S_k^{\infty}$ (Example 2.33). These descriptions are obtained as duality theorems in the étale cohomology of $\mathrm{Spec}(k_{\mathfrak{p}})$ and $\mathrm{Spec}(\mathcal{O}_k) \setminus S$.

In what follows, we shall consider some étale cohomology groups of $X = \mathrm{Spec}(A)$ with coefficients in locally constant étale sheaves on X defined by Abelian groups on which $\pi_1(X, \overline{x})$ acts continuously. Here an étale sheaf M on X is called *locally constant* if there is a connected finite étale covering $Y \to X$ such that $M|_Y$ is a constant sheaf of an Abelian group on Y. A finite $\pi_1(X, \overline{x})$-module M gives rise to a locally constant étale sheaf on X which is defined by associating to a connected finite étale covering $Y \to X$ the $\pi_1(Y, \overline{y})$-invariant subgroup $M^{\pi_1(Y,\overline{y})}$ ($\overline{y} \in F_{\overline{x}}(X)$) of M. Conversely, a locally constant, finite étale sheaf M gives rise to a finite $\pi_1(X, \overline{x})$-module $M_{\overline{x}}$, the stalk of M at $\overline{x}$. Thus, we identify a locally constant étale sheaf on X with the associated finite $\pi_1(X, \overline{x})$-module. For the case that A is a field F, an étale sheaf of finite Abelian group on $\mathrm{Spec}(F)$ is same as a finite Abelian group on which $\pi_1(\mathrm{Spec}(F)) = \mathrm{Gal}(\overline{F}/F)$ acts continuously. So the étale cohomology group $H^i(\mathrm{Spec}(F), M)$ is identified with the Galois cohomology group $H^i(\mathrm{Gal}(\overline{F}/F), M)$ which we denote by $H^i(F, M)$ for simplicity. The *étale cohomological dimension* of $X = \mathrm{Spec}(A)$ is defined by the smallest integer n (or ∞) such that $H^i(X, M) = 0$ for $i > n$ and any torsion étale sheaf M of Abelian groups on X. For a locally compact Abelian group G, we denote by G^* the Pontryagin dual of G, the locally compact Abelian group consisting of continuous homomorphisms $G \to \mathbb{R}/\mathbb{Z}$.

2.3.1 Finite Fields

Let F be a finite field $\mathbb{F}_q$. For a finite $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-module M, let $M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$. The action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on M^* is defined by $(g\varphi)(x) = \varphi(g^{-1}x)$ ($g \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, $\varphi \in M^*$, $x \in M$). Then the cup product

$$H^i(\mathbb{F}_q, M^*) \times H^{1-i}(\mathbb{F}_q, M) \to H^1(\mathbb{F}_q, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z} \quad (i = 0, 1)$$

gives a non-degenerate pairing of finite Abelian groups, and $\mathrm{Spec}(\mathbb{F}_q)$ has the étale cohomological dimension 1. In particular, if $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on M trivially, by using $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \hat{\mathbb{Z}}$, this pairing reduces to the duality $M \simeq M^{**}$.

2.3.2 $\mathfrak{p}$-*Adic Fields*

Let $k_\mathfrak{p}$ be a $\mathfrak{p}$-adic field. Let $\mathcal{O}_\mathfrak{p}$ be the ring of $\mathfrak{p}$-adic integers, π a prime element of $\mathcal{O}_\mathfrak{p}$ and $v_\mathfrak{p}$ the $\mathfrak{p}$-adic additive valuation with $v_\mathfrak{p}(\pi) = 1$. For a finite $\mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p})$-module M, let $M' := \mathrm{Hom}(M, \overline{k}_\mathfrak{p}^\times)$. The action of $\mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p})$ on M' is defined by $(g\varphi)(x) = g\varphi(g^{-1}x)$ $(g \in \mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p}), \varphi \in M', x \in M)$.

Tate local duality 2.41 *There is a canonical isomorphism* $H^2(k_\mathfrak{p}, \overline{k}_\mathfrak{p}^\times) \simeq \mathbb{Q}/\mathbb{Z}$ *and the cup product*

$$H^i(k_\mathfrak{p}, M') \times H^{2-i}(k_\mathfrak{p}, M) \to H^2(k_\mathfrak{p}, \overline{k}_\mathfrak{p}^\times) \simeq \mathbb{Q}/\mathbb{Z} \quad (0 \le i \le 2)$$

gives a non-degenerate pairing of finite Abelian groups. The étale cohomological dimension of $\mathrm{Spec}(k_\mathfrak{p})$ *is* 2.

Now consider the case $i = 1$ and $M = \mathbb{Z}/n\mathbb{Z}$. Then one has $M' = \mu_n$, the group of n-th roots of unity, $H^1(k_\mathfrak{p}, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(k_\mathfrak{p}^{\mathrm{ab}}/k_\mathfrak{p}), \mathbb{Z}/n\mathbb{Z})$, and $H^1(k_\mathfrak{p}, \mu_n) = k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^n$ (Kummer theory). Thus, Tate local duality induces an isomorphism

$$k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^n \simeq \mathrm{Gal}\big(k_\mathfrak{p}^{\mathrm{ab}}/k_\mathfrak{p}\big)/n\,\mathrm{Gal}\big(k_\mathfrak{p}^{\mathrm{ab}}/k_\mathfrak{p}\big).$$

By taking the projective limit $\varprojlim_n$, we obtain the *reciprocity homomorphism* of local class field theory

$$\rho_{k_\mathfrak{p}} : k_\mathfrak{p}^\times \longrightarrow \mathrm{Gal}\big(k_\mathfrak{p}^{\mathrm{ab}}/k_\mathfrak{p}\big),$$

which is injective and has the dense image. Further, by taking the pull-back by $\rho_{k_\mathfrak{p}}$, one has a bijection between the set of open subgroups of $\mathrm{Gal}(k_\mathfrak{p}^{\mathrm{ab}}/k)$ and the set of finite-index open subgroups of $k_\mathfrak{p}^\times$. Let $\tilde{k}_\mathfrak{p}$ be the maximal unramified extension of $k_\mathfrak{p}$. Then we have the following commutative exact diagram:

$$\begin{array}{ccccccccc}
0 \to & & \mathcal{O}_\mathfrak{p}^\times & \to & k_\mathfrak{p}^\times & \xrightarrow{v_\mathfrak{p}} & \mathbb{Z} & \to 0 \\
& & \wr\downarrow & & \downarrow\rho_{k_\mathfrak{p}} & & \cap\downarrow & \\
0 \to & \mathrm{Gal}(k_\mathfrak{p}^{\mathrm{ab}}/\tilde{k}_\mathfrak{p}) & \to & \mathrm{Gal}(k_\mathfrak{p}^{\mathrm{ab}}/k) & \to & \mathrm{Gal}(\tilde{k}_\mathfrak{p}/k) = \hat{\mathbb{Z}} & \to 0 &
\end{array}$$

Here the left vertical isomorphism is the restriction of $\rho_{k_\mathfrak{p}}$ to $\mathcal{O}_\mathfrak{p}^\times$ and the right vertical injection is the map sending 1 to the Frobenius automorphism $\sigma_\mathfrak{p}$. Therefore, $\rho_{k_\mathfrak{p}}(\pi) = \sigma_\mathfrak{p}$.

For a finite Abelian extension $K_\mathfrak{P}/k_\mathfrak{p}$, we define the *reciprocity homomorphism*

$$\rho_{K_\mathfrak{P}/k_\mathfrak{p}} : k_\mathfrak{p}^\times \longrightarrow \mathrm{Gal}(K_\mathfrak{P}/k_\mathfrak{p}) \tag{2.2}$$

by composing $\rho_{k_\mathfrak{p}}$ with the natural projection $\mathrm{Gal}(k_\mathfrak{p}^{\mathrm{ab}}/k_\mathfrak{p}) \to \mathrm{Gal}(K_\mathfrak{P}/k_\mathfrak{p})$. Then $\rho_{K_\mathfrak{P}/k_\mathfrak{p}}$ induces the isomorphism

$$k_\mathfrak{p}^\times/\mathrm{N}_{K_\mathfrak{P}/k_\mathfrak{p}}(K_\mathfrak{P}^\times) \simeq \mathrm{Gal}(K_\mathfrak{P}/k_\mathfrak{p}),$$

and it follows that any open subgroup of $k_{\mathfrak{p}}^{\times}$ with finite index is obtained as the norm group of the multiplicative group of a finite Abelian extension of $k_{\mathfrak{p}}$. Further, one has

$$\begin{aligned} K_{\mathfrak{P}}/k_{\mathfrak{p}} \text{ is unramified} &\iff \rho_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}}^{\times}) = \mathrm{id}_{K_{\mathfrak{P}}} \\ &\iff \mathrm{N}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{P}}^{\times}) = \mathcal{O}_{\mathfrak{p}}^{\times}, \end{aligned} \tag{2.3}$$

and, in this case, we have

$$\rho_{k_{\mathfrak{p}}}(x) = \sigma^{v_{\mathfrak{p}}(x)},$$

where $\sigma \in \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ is the Frobenius automorphism. On the other hand, if $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is totally ramified, the restriction of $\rho_{k_{\mathfrak{p}}}$ to $\mathcal{O}_{\mathfrak{p}}^{\times}$ induces the isomorphism

$$\mathcal{O}_{\mathfrak{p}}^{\times}/\mathrm{N}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{P}}^{\times}) \simeq \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

We now assume that $k_{\mathfrak{p}}$ contains a primitive n-th root of unity for some integer $n \geq 2$. Then the *Hilbert symbol*

$$\left(\frac{\ ,\ }{\mathfrak{p}}\right)_n : k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^n \times k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^n \longrightarrow \mu_n$$

is defined by

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n := \frac{\rho_{k_{\mathfrak{p}}}(b)(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

The Hilbert symbol is bi-multiplicative and skew symmetric and satisfies the following property:

$$\begin{aligned} \left(\frac{a,b}{\mathfrak{p}}\right)_n = 1 &\iff b \in \mathrm{N}_{k_{\mathfrak{p}}(\sqrt[n]{a})/k_{\mathfrak{p}}}\left(k_{\mathfrak{p}}(\sqrt[n]{a})^{\times}\right) \\ &\iff a \in \mathrm{N}_{k_{\mathfrak{p}}(\sqrt[n]{b})/k_{\mathfrak{p}}}\left(k_{\mathfrak{p}}(\sqrt[n]{b})^{\times}\right). \end{aligned} \tag{2.4}$$

When $k_{\mathfrak{p}}(\sqrt[n]{a})/k_{\mathfrak{p}}$ $(a \in k_{\mathfrak{p}}^{\times})$ is an unramified extension (this is the case if $a \in \mathcal{O}_{\mathfrak{p}}^{\times}$), the *$n$-th power residue symbol* is defined by

$$\left(\frac{a}{\mathfrak{p}}\right)_n := \left(\frac{a,\pi}{\mathfrak{p}}\right)_n = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}, \tag{2.5}$$

where $\sigma = \rho_{k_{\mathfrak{p}}(\sqrt[n]{a})/k_{\mathfrak{p}}}(\pi) \in \mathrm{Gal}(k_{\mathfrak{p}}(\sqrt[n]{a})/k_{\mathfrak{p}})$ is the Frobenius automorphism. Then one has

$$\begin{aligned} \left(\frac{a}{\mathfrak{p}}\right)_n = 1 &\iff a \in (k_{\mathfrak{p}}^{\times})^n \\ &\iff a \bmod \mathfrak{p} \in (\mathbb{F}_{\mathfrak{p}}^{\times})^n \quad (\text{if } a \in U_{\mathfrak{p}}). \end{aligned}$$

Let $k_{\mathfrak{p}} = \mathbb{Q}_p$ for an odd prime number p and let a be an integer prime to p. Then the power residue symbol $(\frac{a}{p})_2$ coincides with the Legendre symbol $(\frac{a}{p})$.

As for the field $\mathbb{R}$ of real numbers, we also have the duality theorem by using Tate's modified cohomology groups [Se2, Chap. VIII]. Let M be a finite $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module and let $M' = \mathrm{Hom}(M, \mathbb{C}^\times)$. The action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on M' is defined by $(g\varphi)(x) = g\varphi(g^{-1}x)$ $(g \in \mathrm{Gal}(\mathbb{C}/\mathbb{R}), \varphi \in M', x \in M)$. Then the cup product

$$\hat{H}^i(\mathbb{R}, M') \times \hat{H}^{2-i}(\mathbb{R}, M) \to H^2(\mathbb{R}, \mathbb{C}^\times) \simeq \mathbb{F}_2 \quad (i \in \mathbb{Z})$$

gives a non-degenerate pairing of finite Abelian groups. Letting $i = 1$ and $M = \mu_2$, we have the isomorphism

$$\rho_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^\times/(\mathbb{R}^\times)^2 = H^1(\mathbb{R}, \mu_2) \simeq H^1(\mathbb{R}, \mathbb{F}_2)^* = \mathrm{Gal}(\mathbb{C}/\mathbb{R}).$$

The *reciprocity homomorphism* $\rho_{\mathbb{R}} : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is then defined by composing the natural projection $\mathbb{R}^\times \to \mathbb{R}^\times/(\mathbb{R}^\times)^2$ with $\rho_{\mathbb{C}/\mathbb{R}}$. Hence, $\rho_{\mathbb{R}}$ is surjective and $\mathrm{Ker}(\rho_{\mathbb{R}}) = \mathbb{R}^\times$ (the connected component of 1).

2.3.3 Number Rings

Let k be a number field of finite degree over $\mathbb{Q}$. Let $\mathcal{O}_k$ be the ring of integers of k and set $X = \mathrm{Spec}(\mathcal{O}_k)$. An étale sheaf M of Abelian groups on X is said to be *constructible* if all stalks of M are finite and there is an open subset $U \subset X$ such that $M|_U$ is locally constant [Z]. For a constructible sheaf M on X, the modified étale cohomology groups $\hat{H}^i(X, M)$ $(i \in \mathbb{Z})$, which take the infinite primes into account, are defined. For the definition of modified cohomology, we refer to ([Z], [Kt1, Sect. 3], [Mi2]). We let $M' := \underline{\mathrm{Hom}}(M, \mathbb{G}_{m,X})$ where $\mathbb{G}_{m,X}$ is the étale sheaf on X defined by associating to a connected finite étale covering $\mathrm{Spec}(B) \to X$ the multiplicative group $\mathbb{G}_{m,X}(Y) = B^\times$.

Artin-Verdier duality 2.42 *Let M be a constructible sheaf on X. There is a canonical isomorphism $\hat{H}^3(X, \mathbb{G}_{m,X}) \simeq \mathbb{Q}/\mathbb{Z}$ and the natural pairing*

$$\hat{H}^i(X, M') \times \mathrm{Ext}_X^{3-i}(M, \mathbb{G}_{m,X}) \to \hat{H}^3(X, \mathbb{G}_{m,X}) \simeq \mathbb{Q}/\mathbb{Z}$$

gives a non-degenerate pairing of finite Abelian groups. The étale cohomological dimension of $X = \mathrm{Spec}(\mathcal{O}_k)$ is 3, up to 2-torsion in the case that k has a real prime.

Let U be an open subset of X. In the following, we shall use the notations $X_0 := \mathrm{Max}(\mathcal{O}_K)$, $U_0 := U \cap \mathrm{Max}(\mathcal{O}_k)$. Let S_k^∞ be the set of infinite primes of k, and set $S = X \setminus U$, $\overline{S} = S \cup S_k^\infty$ so that $\pi_1(U) = G_S(k) = \mathrm{Gal}(k_S/k)$ (Example 2.36). Let M be a finite $G_S(k)$-module and we use the same notation M to denote the corresponding locally constant, finite étale sheaf on U. Assume $\#M \in \mathcal{O}(U)^\times$ (S-unit). Let $j : U \hookrightarrow X$ be the inclusion map and define the constructible sheaf $j_!M$

on X as follows: For a finite étale covering $h : Y \to X$, $j_!M(Y) := M$ if $h(Y) \subset U$, and $j_!M(Y) = 0$ otherwise. Then we have $\mathrm{Ext}^i_X(j_!M, \mathbb{G}_{m,X}) = H^i(U, M')$ and the pairing of Artin-Verdier duality becomes the cup product

$$\hat{H}^i(X, j_!M) \times H^{3-i}(U, M') \to \hat{H}^3(X, \mathbb{G}_{m,X}) \simeq \mathbb{Q}/\mathbb{Z} \quad (i \in \mathbb{Z}).$$

Let V be an open subset of X so that $V \subset U$. Applying the excision

$$H^{i+1}_v(X, j_!M) = \begin{cases} \hat{H}^i(k_v, M) & (v \in S^\infty_k), \\ H^i(k_\mathfrak{p}, M) & (v = \mathfrak{p} \in S), \\ H^{i+1}_\mathfrak{p}(U, M) & (v = \mathfrak{p} \in U \setminus V) \end{cases}$$

to the relative étale cohomology sequence for the pair $V \subset X$ and taking the inductive limit $\varinjlim_{V:\,\text{smaller}}$, we obtain the following long exact sequence:

$$\begin{aligned} \cdots \to H^i_c(U, M) \to H^i(k, M) \to \bigoplus_{v \in \overline{S}} H^i(k_v, M) \oplus \bigoplus_{\mathfrak{p} \in U_0} H^{i+1}_\mathfrak{p}(U, M) \\ \to H^{i+1}_c(U, M) \to \cdots. \end{aligned}$$

Next, we take the inductive limit $\varinjlim_U$ making U smaller (i.e., S larger) in the above exact sequence. Noting $H^{i+1}_\mathfrak{p}(U, M) = \mathrm{Coker}(H^i(\mathbb{F}_\mathfrak{p}, M) \to H^i(k_\mathfrak{p}, M))$, we obtain the Tate–Poitou exact sequence:

Tate–Poitou exact sequence 2.43 *Let M be a finite* $\mathrm{Gal}(\overline{k}/k)$*-module and set* $M' = \mathrm{Hom}(M, \overline{k}^\times)$. *The action of* $\mathrm{Gal}(\overline{k}/k)$ *on M' is given by* $(g\varphi)(x) = g\varphi(g^{-1}x)$ $(g \in \mathrm{Gal}(\overline{k}/k), \varphi \in M', x \in M)$. *Then we have the following exact sequence of locally compact Abelian groups*:

$$\begin{aligned} 0 \to H^0(k, M) \to P^0(k, M) \to H^2(k, M')^* \to \ & H^1(k, M) \\ & \downarrow \\ & P^1(k, M) \\ & \downarrow \\ 0 \leftarrow H^0(k, M')^* \leftarrow P^2(k, M) \leftarrow H^2(k, M) \leftarrow & H^1(k, M')^* \end{aligned}$$

Here the cohomology groups $H^i(k, -)$, $H^i(k_v, -)$ are endowed with the discrete topology, and $P^i(k, M)$ is defined by

$$P^i(k, M) := \prod_{\mathfrak{p} \in X_0} H^i(k_\mathfrak{p}, M) \times \prod_{v \in S^\infty_k} \hat{H}^i(k_v, M),$$

where $\prod_{\mathfrak{p} \in X_0} H^i(k_\mathfrak{p}, M)$ means the restricted direct product of $H^i(k_\mathfrak{p}, M)$'s with respect to the subgroups

$$H^i_{\mathrm{ur}}(k_\mathfrak{p}, M) := \mathrm{Im}\big(H^i(\mathbb{F}_\mathfrak{p}, M) \to H^i(k_\mathfrak{p}, M)\big),$$

namely,

$$\prod_{\mathfrak{p}\in X_0} H^i(k_\mathfrak{p}, M) := \big\{(c_\mathfrak{p}) \mid c_\mathfrak{p} \in H^i_{\mathrm{ur}}(k_\mathfrak{p}, M) \text{ for all but finitely many of } \mathfrak{p}\text{'s}\big\}.$$

The topology of $P^i(k, M)$ is given as the restricted direct product topology, namely, the basis of neighborhoods of the identity is given by the compact groups

$$\prod_{v\in S_k^\infty} \hat{H}^i(k_v, M) \times \prod_{\mathfrak{p}\in S} H^i(k_\mathfrak{p}, M) \times \prod_{\mathfrak{p}\in U_0} H^i_{\mathrm{ur}}(k_\mathfrak{p}, M)$$

where U ranges over open subsets of X.

We define the *idèle group* J_k and the *idèle class group* C_k of k, respectively by

$$J_k := \prod_{\mathfrak{p}\in X_0} k_\mathfrak{p}^\times \times \prod_{v\in S_k^\infty} k_v^\times, \qquad C_k := J_k/k^\times, \tag{2.6}$$

where $\prod_{\mathfrak{p}\in X_0} k_\mathfrak{p}^\times$ means the restricted direct product of $k_\mathfrak{p}^\times$'s with respect to $\mathcal{O}_\mathfrak{p}^\times$'s and $k^\times$ is regarded as a closed subgroup of J_k embedded diagonally.

Now let us specialize M to be the group μ_n of n-th roots of unity in the Tate–Poitou exact sequence (2.43). Then we have

$$H^1(k, \mu_n) = k^\times/(k^\times)^n, \qquad P^1(k, \mu_n) = J_k/J_k^n,$$
$$H^2(k, \mu_n) = {}_n\mathrm{Br}(k), \qquad P^2(k, M) = \bigoplus_v {}_n\mathrm{Br}(k_v).$$

Here $\mathrm{Br}(R)$ stands for the Brauer group of R [NSW, Chap. VI, Sect. 3] and ${}_nA := \{x \in A \mid nx = 0\}$ for an Abelian (additive) group A. Since $H^1(k, \mathbb{Z}/n\mathbb{Z})^* = \mathrm{Gal}(k^{\mathrm{ab}}/k)/n\,\mathrm{Gal}(k^{\mathrm{ab}}/k)$ and the localization map $\mathrm{Br}(k) \to \bigoplus_{v\in X_0\cup S_k^\infty} \mathrm{Br}(k_v)$ is injective (Hasse principle for the Brauer group [ibid, Chap. VIII, Sect. 1]), the Tate–Poitou exact sequence yields the following isomorphism

$$C_k/C_k^n \simeq \mathrm{Gal}\big(k^{\mathrm{ab}}/k\big)/n\,\mathrm{Gal}\big(k^{\mathrm{ab}}/k\big).$$

Taking the projective limit $\varprojlim_n$, we obtain the *reciprocity homomorphism* of class field theory

$$\rho_k : C_k \longrightarrow \mathrm{Gal}(k^{\mathrm{ab}}/k). \tag{2.7}$$

The map ρ_k is surjective and $\mathrm{Ker}(\rho_k)$ coincides with the connected component of 1 in C_k. Further, taking the pull-back by ρ_k, one has a bijection between the set of open subgroups of $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ and the set of open subgroups of C_k. The relation with local class field theory is given as follows: Let $\iota_v : k_v^\times \to C_k$ be the map defined by $\iota_v(a_v) = [(1, \ldots, 1, a_v, 1, \ldots)]$. Then one has the following commutative diagram:

$$\begin{array}{ccc} k_v^\times & \xrightarrow{\rho_{k_v}} & \mathrm{Gal}(k_v^{\mathrm{ab}}/k_v) \\ {\scriptstyle \iota_v}\downarrow & & \downarrow \\ C_k & \xrightarrow{\rho_k} & \mathrm{Gal}(k^{\mathrm{ab}}/k) \end{array} \tag{2.8}$$

For a finite Abelian extension K/k, the *reciprocity homomorphism*

$$\rho_{K/k} : C_k \longrightarrow \mathrm{Gal}(K/k) \tag{2.9}$$

is defined by the composing ρ_k with the natural projection $\mathrm{Gal}(k^{\mathrm{ab}}/k) \to \mathrm{Gal}(K/k)$. Then $\rho_{K/k}$ induces the isomorphism

$$C_k/\mathrm{N}_{K/k}(C_K) \simeq \mathrm{Gal}(K/k)$$

and it follows that any open subgroup of C_k is obtained as the norm group of the idèle class group of a finite Abelian extension of k. Further, one has

$$\begin{aligned} \mathfrak{p} \text{ is completely decomposed in } K/k &\iff \rho_{K/k} \circ \iota_{\mathfrak{p}}(k_{\mathfrak{p}}^{\times}) = \mathrm{id}, \\ v \text{ is unramified in } K/k &\iff \rho_{K/k} \circ \iota_{\mathfrak{p}}(\mathcal{O}_v^{\times}) = \mathrm{id}, \end{aligned} \tag{2.10}$$

where we set $\mathcal{O}_v^{\times} := k_v^{\times}$ if $v \in S_k^{\infty}$.

Example 2.44 (Unramified class field theory) Let $\tilde{k}_+^{\mathrm{ab}}$ be the maximal Abelian extension of k such that any $\mathfrak{p} \in X_0$ is unramified. Then we have

$$\pi_1^{\mathrm{ab}}\big(\mathrm{Spec}(\mathcal{O}_k)\big) = \mathrm{Gal}\big(\tilde{k}_+^{\mathrm{ab}}/k\big).$$

By (2.10), the fundamental map ρ_k induces the isomorphism

$$J_k/k^{\times}\left(\prod_{v\in S_k^{\infty}} (k_v^{\times})^2 \times \prod_{\mathfrak{p}\in X_0} \mathcal{O}_{\mathfrak{p}}^{\times}\right) \simeq \mathrm{Gal}\big(\tilde{k}_+^{\mathrm{ab}}/k\big).$$

Note that the left-hand side is isomorphic to the narrow ideal class group $H^+(k)$ by the correspondence $J_k \ni (a_v) \mapsto \prod_{\mathfrak{p}\in X_0} \mathfrak{p}^{v_{\mathfrak{p}}(a_{\mathfrak{p}})} \in I_k$. Therefore, we have the following canonical isomorphism:

$$H^+(k) \simeq \mathrm{Gal}\big(\tilde{k}_+^{\mathrm{ab}}/k\big).$$

Let $\tilde{k}^{\mathrm{ab}}$ be the maximal Abelian extension such that any prime of k is unramified, called the *Hilbert class field of* k. Then the Galois group $\mathrm{Gal}(\tilde{k}^{\mathrm{ab}}/k)$ is canonically isomorphic to the ideal class group $H(k)$ of k:

$$H(k) \simeq \mathrm{Gal}\big(\tilde{k}^{\mathrm{ab}}/k\big).$$

The above two isomorphisms are regarded as arithmetic analogues of the isomorphism given by Hurewicz theorem in Example 2.13.

Example 2.45 Let S be a finite subset of $\mathrm{Max}(\mathcal{O}_k)$ and let k_S^{ab} be the maximal Abelian extension of k unramified outside $S \cup S_k^{\infty}$ so that $G_S(k)^{\mathrm{ab}} =$

$\pi_1^{\mathrm{ab}}(\mathrm{Spec}(\mathcal{O}_k) \setminus S) = \mathrm{Gal}(k_S^{\mathrm{ab}}/k)$ (Example 2.36). By (2.10), the reciprocity homomorphism ρ_k induces the isomorphism

$$J_k/\overline{k^\times\Big(\prod_{v\in S_k^\infty}(k_v^\times)^2 \times \prod_{\mathfrak{p}\in X\setminus S}\mathcal{O}_\mathfrak{p}^\times\Big)} \simeq \mathrm{Gal}\big(k_S^{\mathrm{ab}}/k\big),$$

where $\overline{k^\times(\cdots)}$ means the topological closure. By Example 2.44, $\mathrm{Gal}(\tilde{k}_+^{\mathrm{ab}}/k) \simeq H^+(k) = J_k/k^\times(\prod_{v\in S_k^\infty}(k_v^\times)^2 \times \prod_{\mathfrak{p}\in X_0}\mathcal{O}_\mathfrak{p}^\times)$ and

$$\begin{aligned} &k^\times\Big(\prod_{v\in S_k^\infty}(k_v^\times)^2 \times \prod_{\mathfrak{p}\in X_0}\mathcal{O}_\mathfrak{p}^\times\Big)\Big/\overline{k^\times\Big(\prod_{v\in S_k^\infty}(k_v^\times)^2 \times \prod_{\mathfrak{p}\in X\setminus S}\mathcal{O}_\mathfrak{p}^\times\Big)} \\ &\simeq \prod_{\mathfrak{p}\in S}\mathcal{O}_\mathfrak{p}^\times\Big/\Big(\prod_{\mathfrak{p}\in S}\mathcal{O}_\mathfrak{p}^\times \cap \overline{k^\times\Big(\prod_{v\in S_k^\infty}(k_v^\times)^2 \times \prod_{\mathfrak{p}\in X\setminus S}\mathcal{O}_\mathfrak{p}^\times\Big)}\Big) \\ &\simeq \prod_{\mathfrak{p}\in S}\mathcal{O}_\mathfrak{p}^\times/\overline{\mathcal{O}_k^+} \end{aligned}$$

where $\mathcal{O}_k^+ := \{a \in \mathcal{O}_k^\times \mid a \text{ is totally positive}\}$ and $\overline{\mathcal{O}_k^+}$ denotes the topological closure of the diagonal image of $\mathcal{O}_k^+$ in $\prod_{\mathfrak{p}\in S}\mathcal{O}_\mathfrak{p}^\times$. Hence, we have the following exact sequence:

$$0 \to \prod_{\mathfrak{p}\in S} U_\mathfrak{p}/\overline{\mathcal{O}_k^+} \to \mathrm{Gal}\big(k_S^{\mathrm{ab}}/k\big) \to H^+(k) \to 0.$$

As $\mathcal{O}_\mathfrak{p}^\times = \mathbb{F}_\mathfrak{p}^\times \times (1+\mathfrak{p})$, this exact sequence gives some restrictions on ramified primes in S. For example, if $\mathfrak{p}$ is ramified in a pro-l extension for some prime number l, one must have $\mathrm{N}\mathfrak{p} \equiv 1$ or $0 \bmod l$.

Example 2.46 Let $k = \mathbb{Q}$ and $S = \{(p_1), \ldots, (p_r)\}$ in Example 2.45. For this case, we have $H^+(\mathbb{Q}) = 1$ and $\mathbb{Z}^+ = \{1\}$ and hence

$$G_S^{\mathrm{ab}} \simeq \prod_{i=1}^r \mathbb{Z}_{p_i}^\times.$$

It follows $\mathbb{Q}_S^{\mathrm{ab}} = \mathbb{Q}(\mu_{p_i^\infty} \mid 1 \le i \le r)$ where $\mu_{p_i^\infty} := \bigcup_{d\ge 1}\mu_{p_i^d}$, $\mu_{p_i^d}$ being the group of p_i^d-th roots of unity.

Suppose that $p_i \equiv 1 \bmod n$ $(1 \le i \le r)$ for some integer $n(\ge 2)$. Fix a primitive root $\alpha_i \bmod p_i$, $\mathbb{F}_{p_i}^\times = \langle \alpha_i \rangle$. Let

$$\psi : \prod_{i=1}^r \mathbb{Z}_{p_i}^\times = \prod_{i=1}^r \mathbb{F}_{p_i}^\times \times (1 + p_i\mathbb{Z}_{p_i}) \to \mathbb{Z}/n\mathbb{Z}$$

be the homomorphism defined by $\psi(\alpha_i) = 1, \psi(1 + p_i\mathbb{Z}_{p_i}) = 0$. Let k be the subfield of $\mathbb{Q}_S^{\mathrm{ab}}$ corresponding to $\mathrm{Ker}(\psi)$ which is independent of the choice of α_i. The field k is the cyclic extension of $\mathbb{Q}$ of degree n such that any prime outside $S \cup \{\infty\}$ is unramified and each prime in S is totally ramified in $k/\mathbb{Q}$.

Next let $S = \{(p)\}$. Then one has

$$\mathbb{Q}_{\{p\}} = \mathbb{Q}(\mu_{p^\infty}), \qquad G_{\{p\}} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times.$$

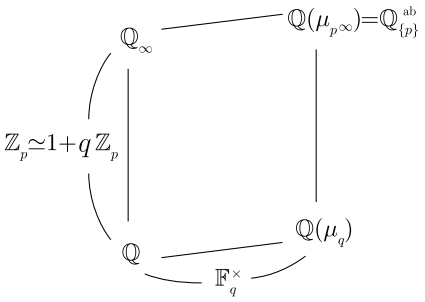
We set

$$q := \begin{cases} p & (p \text{ is a odd prime number}) \\ 4 & (p = 2), \end{cases}$$

and let

$$\psi : \mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \to 1 + q\mathbb{Z}_p \simeq \mathbb{Z}_p$$

be the projection on $1 + q\mathbb{Z}_p$. Let $\mathbb{Q}_\infty$ denote the subfield of $\mathbb{Q}_S^{\mathrm{ab}}$ corresponding to $\mathrm{Ker}(\psi)$. The field $\mathbb{Q}_\infty$ is then the unique Galois extension of $\mathbb{Q}$ whose Galois group $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p$. Note that only (p) is ramified in the extension $\mathbb{Q}_\infty/\mathbb{Q}$ and it is totally ramified.



In general, for a number field F of finite degree over $\mathbb{Q}$, $F_\infty := F\mathbb{Q}_\infty$ is a Galois extension with $\mathrm{Gal}(F_\infty/F)$ being isomorphic to $\mathbb{Z}_p$ such that only primes over p are ramified in F_∞/F. The extension F_∞ is called the *cyclotomic* $\mathbb{Z}_p$*-extension* of F.

As is seen above, the Artin–Verdier duality and the Tate–Poitou exact sequence, which contain the main content of class field theory, are arithmetic analogues of the 3-dimensional Poincaré duality and the relative cohomology sequence (+excision) in topology respectively. Readers may find similar features between Example 2.46 and Examples 2.12, 2.15, Example 2.44 and Example 2.13. We shall discuss these analogies more precisely in the subsequent chapters.

http://www.springer.com/978-1-4471-2157-2

Knots and Primes
An Introduction to Arithmetic Topology
Morishita, M.
2012, XI, 191 p. 42 illus., Softcover
ISBN: 978-1-4471-2157-2