Universitext

Masanori Morishita

Knots and Primes

An Introduction to Arithmetic Topology

Springer

Universitext

Universitext

Universitext is a series of textbooks that presents material from a wide variety of mathematical disciplines at master's level and beyond. The books, often well class-tested by their author, may have an informal, personal, even experimental approach to their subject matter. Some of the most successful and established books in the series have evolved through several editions, always following the evolution of teaching curricula, into very polished texts.

Thus as research topics trickle down into graduate-level teaching, first textbooks written for new, cutting-edge courses may make their way into *Universitext*.

For further volumes:
www.springer.com/series/223

Masanori Morishita

Knots and Primes

An Introduction to Arithmetic Topology

Springer

Masanori Morishita
Graduate School of Mathematics
Kyushu University
Fukuoka 819-0395
Japan
morisita@math.kyushu-u.ac.jp

The English language edition is based on the Japanese original edition:
Musubime to Sosu by Masanori Morishita

ISSN 0172-5939 e-ISSN 2191-6675
Universitext
ISBN 978-1-4471-2157-2 e-ISBN 978-1-4471-2158-9
DOI 10.1007/978-1-4471-2158-9
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2011940954

Mathematics Subject Classification: 11Rxx, 11Sxx, 57Mxx

Cover design: VTeX UAB, Lithuania

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To the memory of my mother,
Chieko Morishita

Preface

The theme of the present book is the analogy between knot theory and number theory, based on the homotopical analogies between knots and primes, 3-manifolds and number rings. Thus, the purpose of this book is to discuss and present, in a parallel and systematic manner, the analogies between the fundamental notions and theories of knot theory and number theory. For the sake of readers, basic materials from each field are recollected in Chap. 2.

If we look back over the history of knot theory and number theory, an origin of the modern development of both fields may be found in the work of C.F. Gauss (1777–1855). The aim of this book may be rephrased as bridging the two ways that branched out after Gauss and providing a foundation of *arithmetic topology*.

This volume is an English translation of my Japanese book [M12] with some things added. I thank Professor Y. Matsumoto for recommending that I should write a book on this subject. The contents of this book grew out of my intensive lectures at some universities in Japan (Kyushu, Kyoto, Tohoku and Tokyo) on various occasions during 2002–2007 and at the University of Heidelberg in the fall of 2008. I take this opportunity to acknowledge my gratitude to Y. Taguchi, K. Kato, A. Yukie, T. Yamazaki, T. Oda and D. Vogel for inviting me to give lectures on arithmetic topology, and I thank Y. Terashima for useful communication and joint work on Chap. 14. I am thankful to H. Hida, M. Kaneko, M. Kato, M. Kurihara, Y. Mizusawa and S. Ohtani for useful communication in the course of writing this book, and to F. Amano, H. Nibo and Y. Takakura for pointing out some misprints in the Japanese version. I also thank the referees for their useful comments and L. Stoney, D. Akmanavičius and M. Nakamura for their help with the production of this text. I would like to thank C. Deninger, M. Kapranov, T. Kohno, B. Mazur, J. Morava and T. Ono for their encouragements and interests in my work. Finally, I express my hearty thanks to J. Hillman and K. Murasugi for answering patiently my questions on knot/link theory over the years, especially to J. Hillman for his useful (both linguistic and mathematical) comments on the manuscript of this English version.

Fukuoka, Japan — Masanori Morishita

Contents

Notation and Convention

$\mathbb{N}$: the set of natural numbers (≥ 1).
$\mathbb{Z}$: the set of integers.
$\mathbb{Q}$: the set of rational numbers.
$\mathbb{R}$: the set of real numbers.
$\mathbb{C}$: the set of complex numbers.
$\#A$: the cardinality of a set A.
$R^\times$: the group of invertible elements in a ring R.

For $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, $\|x\| := \sqrt{x_1^2 + \cdots + x_n^2}$.

For an integer $n \geq 0$, an n-manifold means an n-dimensional manifold.

For topological spaces X and Y, $X \approx Y$ means that X and Y are homeomorphic, and $X \simeq Y$ means that X and Y are homotopy equivalent.

For a topological space X in an ambient space Y, $\mathrm{int}(X)$, ∂X and $\overline{X}$ denote the interior, the boundary and the closure of X, respectively.

For objects A and B with an algebraic structure, $A \simeq B$ means that A and B are isomorphic.

For a topological space X, $H_*(X)$ stands for the homology group of X with coefficients in $\mathbb{Z}$.

For a group G and $a_1, \ldots, a_n \in G$, $\langle\langle a_1, \ldots, a_n \rangle\rangle$ denotes the smallest normal subgroup of G containing $a_1, \ldots, a_n$.

For closed subgroups A, B of a topological group G, $[A, B]$ denotes the closed subgroup generated by commutators $[a, b] := aba^{-1}b^{-1}$ for $a \in A$, $b \in B$.

For a topological group G and $d \in \mathbb{N}$, $G^{(d)}$ denotes the d-th term of the lower central series of G defined by $G^{(1)} := G$, $G^{(d+1)} := [G^{(d)}, G]$.

Chapter 1
Introduction

1.1 Two Ways that Branched out from C.F. Gauss—Quadratic Residues and Linking Numbers

In his youth, C.F. Gauss proved the law of quadratic reciprocity and further created the theory of genera for binary quadratic forms ([Ga1], 1801).

For an odd prime number p and an integer a prime to p, consider the quadratic equation modulo p:

$$x^2 \equiv a \bmod p.$$

According as this equation has an integral solution or not, the integer a is called a quadratic residue or quadratic non-residue mod p, and the Legendre symbol is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & a \text{ is a quadratic residue mod } p \\ -1, & a \text{ is a quadratic non-residue mod } p. \end{cases}$$

For odd prime numbers p and q, Gauss proved the following relation between p being a quadratic residue mod q and q being a quadratic residue mod p:

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

In particular, the symmetric relation holds if p or $q \equiv 1 \bmod 4$:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

In terms of algebra today, Gauss' genus theory may be viewed as a classification theory of ideals of a quadratic field $k = \mathbb{Q}(\sqrt{m})$. Let $\mathcal{O}_k$ be the ring of integers of k. Nonzero fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_k$ (i.e., finitely generated $\mathcal{O}_k$-submodules of k) are said to be in the same class in the narrow sense if there is $\alpha \in k$ such that

$$\mathfrak{b} = \mathfrak{a}(\alpha), \quad \alpha, \bar{\alpha} > 0$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_1, © Springer-Verlag London Limited 2012

where $\bar{\alpha}$ denotes the conjugate of α. Let $H^+(k)$ denote the set of these classes. For the sake of simplicity, we assume for the moment that $m = p_1 \cdots p_r$ ($p_1, \ldots, p_r$ being different prime factors) and $p_i \equiv 1 \bmod 4$ ($1 \le i \le r$). Note that in each class we may choose an ideal in $\mathcal{O}_k$ prime to m. Such ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be in the same genus, written by $\mathfrak{a} \approx \mathfrak{b}$, if one has

$$\left(\frac{\mathrm{N}\mathfrak{a}}{p_i}\right) = \left(\frac{\mathrm{N}\mathfrak{b}}{p_i}\right) \quad (1 \le i \le r)$$

where $\mathrm{N}\mathfrak{a} := \#(\mathcal{O}_k/\mathfrak{a})$. This gives a well-defined equivalence relation on $H^+(k)$ and we can classify $H^+(k)$ by the relation $\approx$. Gauss proved that $H^+(k)$ forms a finite Abelian group by the multiplication of fractional ideals, which is called the ideal class group in the narrow sense, that the correspondence $[\mathfrak{a}] \mapsto ((\mathrm{N}\mathfrak{a}/p_1), \ldots, (\mathrm{N}\mathfrak{a}/p_r))$ gives rise to the following isomorphism

$$H^+(k)/\approx \simeq \left\{ (\xi_i) \in \{\pm 1\}^r \;\middle|\; \prod_{i=1}^{r} \xi_i = 1 \right\} \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}$$

and hence that the number of genera is 2^{r-1}. Gauss' investigation on quadratic residues may be seen as an origin of the modern development of algebraic number theory.

On the other hand, in [Ga2] 1833, Gauss discovered the notion of the linking number, together with its integral expression, in the course of his investigations of electrodynamics. Let K and L be disjoint, oriented simple closed curves in $\mathbb{R}^3$ (i.e., a 2-component link) with parametrizations given by smooth functions $a : [0, 1] \longrightarrow \mathbb{R}^3$ and $b : [0, 1] \longrightarrow \mathbb{R}^3$, respectively. Let us turn on an electric current with strength I in L so that the magnetic field $\mathbf{B}(x)$ ($x \in \mathbb{R}^3$) is generated. By the law of Biot–Savart, $\mathbf{B}(x)$ is given by

$$\mathbf{B}(x) = \frac{I\mu_0}{4\pi} \int_0^1 \frac{b'(t) \times (x - b(t))}{\|x - b(t)\|^3}\, dt,$$

where μ_0 stands for the magnetic permeability of a vacuum. Then Gauss showed the following integral formula:

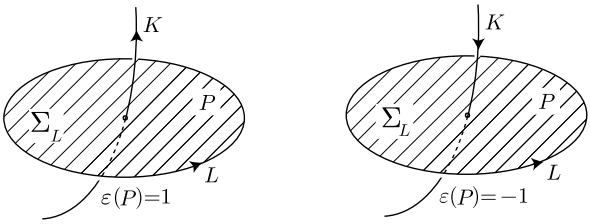
$$\frac{1}{I\mu_0} \int_0^1 \mathbf{B}\big(a(s)\big) \cdot a'(s)\, ds = \mathrm{lk}(L, K),$$

namely,

$$\frac{1}{4\pi} \int_0^1 \int_0^1 \frac{(b'(t) \times (a(s) - b(t))) \cdot a'(s)}{\|a(s) - b(t)\|^3}\, ds\, dt = \mathrm{lk}(L, K).$$

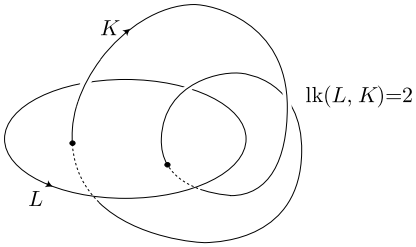
Here $\mathrm{lk}(L, K)$ is an integer, called the linking number of K and L, which is defined as follows. Let Σ_L be an oriented surface with $\partial \Sigma_L = L$. We may assume that K crosses Σ_L at right angles. Let P be an intersection point of K and Σ_L. According

as a tangent vector of K at P has the same or opposite direction to a normal vector of Σ_L at P, we assign a number $\varepsilon(P) := 1$ or -1 to each P:



Let $P_1, \ldots, P_m$ be the set of intersection points of K and Σ_L. Then the linking number $\mathrm{lk}(L, K)$ is defined by

$$\mathrm{lk}(L, K) := \sum_{i=1}^{m} \varepsilon(P_i).$$



By this definition or by Gauss' integral formula, we easily see that the symmetric relation holds:

$$\mathrm{lk}(L, K) = \mathrm{lk}(K, L).$$

Gauss already recognized that the linking number is a topological invariant, a quantity which is invariant under continuous moves of K and L. Furthermore, it is remarkable that Gauss' integral formula has been overlooked and its first generalization was studied only about 150 years later by E. Witten and M. Kontsevich etc., again in connection with physics [Kn].

Although there seems no connection between the Legendre symbol and the linking number at first glance, as we shall show in Chap. 4, there is indeed a close analogy between both notions and in fact they are defined in an exactly analogous manner. Since Gauss took an interest in knots in his youth [Du, XVII, p. 222], we may imagine that he already had a sense of the analogy between the Legendre symbol and the linking number. However, there was no mathematical language at his time to describe this analogy, and knot theory and number theory have grown up

in separate ways for a century and a half after Gauss. It was the "geometric viewpoint and language" brought into number theory during this long period of time that enabled us to bridge two ways that branched out after Gauss.

1.2 Geometrization of Number Theory

Gauss' Disquisitiones Arithmeticae has been developed by Kummer, Dedekind, Kronecker, Hilbert and others as arithmetic of number fields, which provided a foundation of algebraic number theory today. Gauss' quadratic reciprocity was also generalized along this line of development and culminated in class field theory by T. Takagi and E. Artin (1927). A guiding principle leading to this development was the viewpoint of the analogy between number fields and function fields. Behind this thought there might be an influence from the theory of complex functions (Riemann surfaces) which was a major field in the 19th century mathematics. The basic idea comes from the well known analogy between integers and polynomials and a prime ideal of a number ring is regarded as an analog of a point of an algebraic curve. In particular, there are close analogies between number fields and function fields with finite constant fields that were extensively investigated by E. Artin, A. Weil and others. On the other hand, I.M. Gelfand clarified the equivalence between rings and spaces by showing that any commutative C^*-algebra R is obtained as the algebra of functions on a compact space given by the set of maximal ideals of R. It was A. Grothendieck who pushed these thoughts further for arbitrary commutative rings and created the theory of schemes. For instance, the prime spectrum $\mathrm{Spec}(\mathcal{O}_k)$, namely, the set of prime ideals of the ring $\mathcal{O}_k$ of integers of a number field k is a 1-dimensional scheme, called an "arithmetic curve". Grothendieck's thought unified number theory and algebraic geometry and led to arithmetical algebraic geometry today.

On the other hand, although there was work by J.B. Listing (a student of Gauss) and the physicist P.G. Tait etc., there had not been remarkable progress in knot theory after Gauss, until the creation of topological notions such as fundamental groups, homology groups etc by H. Poincaré in the end of 19th century. However, after Poincaré, the homology theory has been rapidly developed by J.W. Alexander, S. Lefschetz and others, and subsequently knot theory was investigated by the homological and combinatorial group-theoretic methods (Alexander, M. Dehn, H. Seifert, K. Reidemeister et. al). Most notably, Alexander clarified the importance of knot theory in 3-dimensional topology by showing that any oriented connected closed 3-manifold is a finite covering of the 3-sphere ramified over a link, and also introduced the first polynomial invariant of a knot, called the Alexander polynomial (1928). It should also be noted that Reidemeister introduced the torsion of a CW complex and gave a homeomorphism classification of 3-dimensional lens spaces (1935).

The development of homology theory in topology had a favorable influence on algebraic number theory. Namely, T. Nakayama and J. Tate elaborated the theory of Galois cohomology and applied it to give a new proof of class field theory (1950s). On the other hand, motivated by Weil's conjecture asserting that there is a deep

connection between arithmetic properties of an algebraic variety over a finite field and topological properties of the associated complex manifold, Grothendieck initiated the theory of étale topology and introduced the étale fundamental group and étale (co)homology group for schemes which enjoy properties similar to those of the topological fundamental group and singular (co)homology group. For example, class field theory for a number field k is stated as a sort of 3-dimensional Poincaré duality in the étale cohomology of $\mathrm{Spec}(\mathcal{O}_k)$ (M. Artin, J.-L. Verdier [Mz1]). Furthermore, M. Artin and B. Mazur developed higher homotopy theory for schemes. Along this line of thoughts, B. Mazur pointed out the analogy between a knot and prime as follows [Mz5]. We first note that the prime spectrum of the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for a prime number p has the following étale homotopy groups

$$\pi_1^{\text{ét}}\big(\mathrm{Spec}(\mathbb{F}_p)\big) = \hat{\mathbb{Z}}, \qquad \pi_i^{\text{ét}}\big(\mathrm{Spec}(\mathbb{F}_p)\big) = 0 \quad (i \geq 2)$$

($\hat{\mathbb{Z}}$ being the pro-finite completion of $\mathbb{Z}$) and hence $\mathrm{Spec}(\mathbb{F}_p)$ is regarded as an arithmetic analogue of a circle S^1. Moreover, since $\mathrm{Spec}(\mathbb{Z})$ has the étale cohomological dimension 3 (up to 2-torsion) and $\pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{Z})) = 1$, the embedding

$$\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$$

is viewed as an analogue of an embedding, namely, a knot

$$S^1 \hookrightarrow \mathbb{R}^3.$$

The analogies between knots and primes, 3-manifolds and number rings were took up later by M. Kapranov and A. Reznikov and the study of those analogies was christened *arithmetic topology* [Kp2, Rz1, Rz2].

We note that in view of the analogy above, a knot group $G_K = \pi_1(\mathbb{R}^3 \setminus K)$ corresponds to a "prime group" $G_{\{(p)\}} = \pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{Z}) \setminus \{(p)\})$. More generally, a link L corresponds to a finite set S of primes, and the link group $G_L = \pi_1(\mathbb{R}^3 \setminus L)$ corresponds to $G_S := \pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{Z}) \setminus S)$, the Galois group of the maximal Galois extension of $\mathbb{Q}$ unramified outside S and the infinite prime.

1.3 The Outline of This Book

I started my own study of the analogy between knot theory and number theory, based on the analogy I noticed between the structures of a link group and a Galois group with restricted ramification (cf. Chap. 7). The purpose of this volume is to try to bridge two ways that branched out after Gauss from this viewpoint by discussing in a parallel manner the analogies between the fundamental notions and theories of knot theory and number theory. The outline of this book is as follows. In Chap. 3, we present basic analogies between 3-manifolds and number rings, knots and primes, which will be fundamental in later chapters. In Chaps. 4–6, we shall reexamine and unify Gauss' works on the quadratic residues, genus theory and the

linking number from the viewpoint of the analogies in Chap. 3. In Chap. 7, we present an analogy between J. Milnor's theorem on a link group and H. Koch's theorem on a pro-l Galois group with restricted ramification (l being a prime number). The analogy between linking numbers and power residue symbols is clearly explained by this group-theoretic point of view. Furthermore, in Chap. 8, we shall introduce arithmetic analogues of Milnor's higher linking numbers ($\overline{\mu}$-invariants). In particular, a triple symbol introduced by L. Rédei (1939) is interpreted as an arithmetic triple linking number. In Chap. 10, we shall describe, by using higher linking numbers, the Galois module structure of the l-part of the 1st homology of an l-fold cyclic ramified covering of S^3, and then we shall show, by using arithmetic higher linking numbers, an arithmetic analogue for the l-part of the ideal class group of a cyclic extension of $\mathbb{Q}$ of degree l, which may be regarded as a natural generalization of Gauss' genus theory. In Chaps. 9, 11 and 12, we discuss some analogies between Alexander–Fox theory and Iwasawa theory in a parallel manner, regarding the cyclotomic $\mathbb{Z}_p$-extension of a number field as an analog of the infinite cyclic covering of a knot complement. Further, in Chap. 13, we present analogies between Alexander–Fox theory and Iwasawa theory and their non-Abelian generalization from the viewpoint of moduli and deformation of representations of knot and prime groups. For the case of 2-dimensional representations, in the final Chap. 14, we shall show some intriguing analogies between deformations of hyperbolic structures and of p-adic ordinary modular forms.

As the history of mathematics tells us, pursuing analogies between different fields often raises new interesting problems and leads to development of both fields, and even open a new field of study. As we explained above, the geometrization of number theory enabled us to pursue the analogy between knot theory and number theory, and it is the theme of this book. In recent years, after the discovery of the Jones polynomial (1984), lots of knot invariants, called quantum invariants, have been constructed systematically in connection with mathematical physics. If one regards the classical electro-magnetic theory, from which Gauss' linking number originated, as Abelian gauge theory, this stream may be viewed as a development in the direction of non-Abelian gauge theory. On the other hand, Gauss' quadratic reciprocity is an origin of Abelian class field theory, and so non-Abelian class field theory may be seen as an arithmetic counter part of non-Abelian gauge theory. Here the relation (Langlands conjecture) between the motivic L-functions associated to representations of Galois groups of number fields and the automorphic L-functions (zeta integrals over adèle groups) may correspond to the relation between the geometric invariants associated to representations of knot, 3-manifold groups and the partition/correlation functions (path integral invariants):

Abelian gauge theory	$\longrightarrow$ Non-Abelian gauge theory
linking number	geometric invariant
= Gaussian integral	= path integral invariant
Abelian class field theory	$\longrightarrow$ Non-Abelian class field theory
Legendre symbol	motivic L-function
= Gaussian sum	= automorphic L-function

The aspect related to mathematical physics is an area of the future investigation for arithmetic topology (cf. [DGLZ, Kp1, MM]). I hope that pursuing further analogies between knot theory and number theory, in connection with mathematical physics, would raise new points of view and interesting problems, and lead to deeper understanding and progress of these fields.

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).

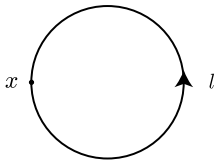


Fig. 2.1

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).

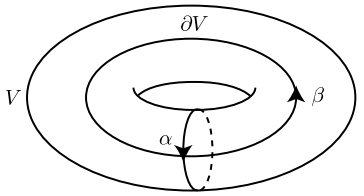


Fig. 2.2

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).

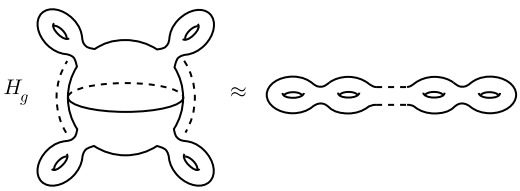


Fig. 2.3

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).

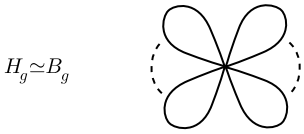


Fig. 2.4

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).

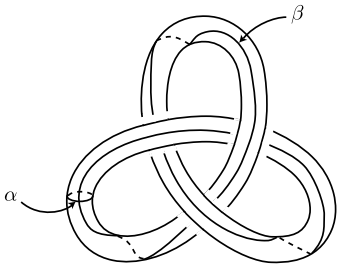


Fig. 2.5

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).

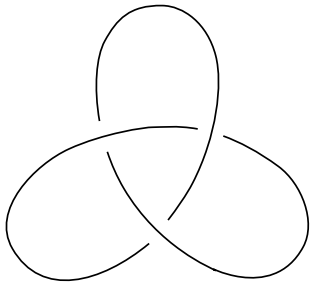


Fig. 2.6

(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).

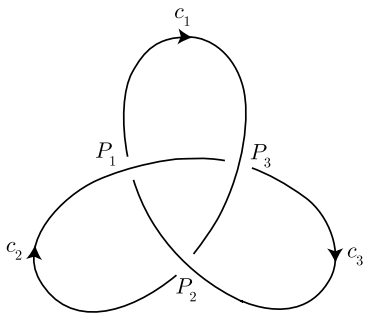


Fig. 2.7

(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).

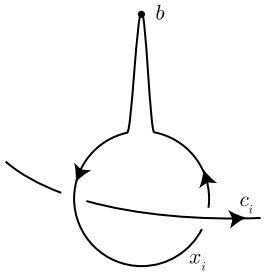


Fig. 2.8

(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).

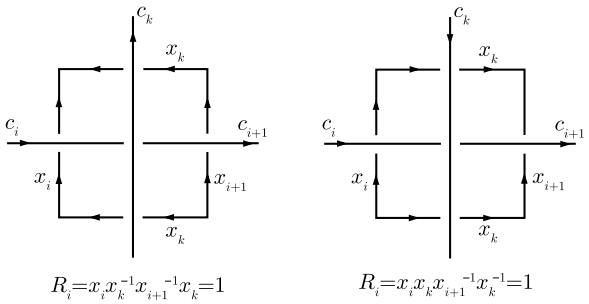


Fig. 2.9

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).

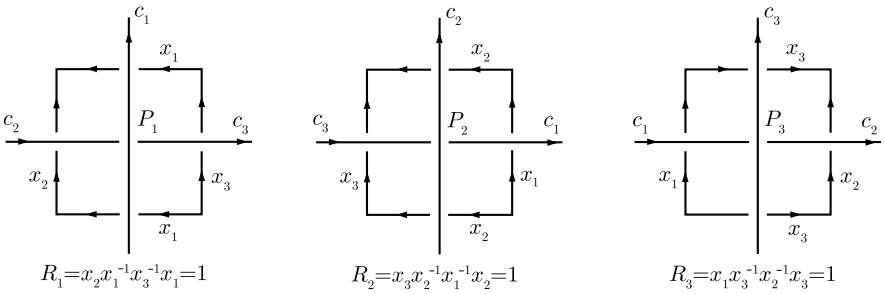


Fig. 2.10

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).

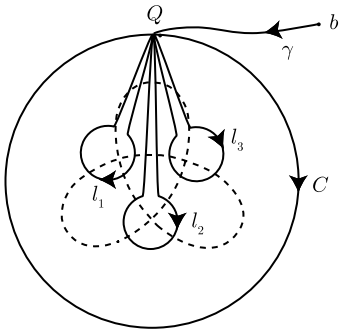


Fig. 2.11

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).

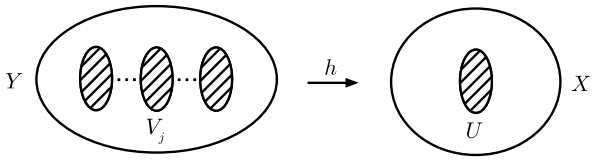


Fig. 2.12

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).

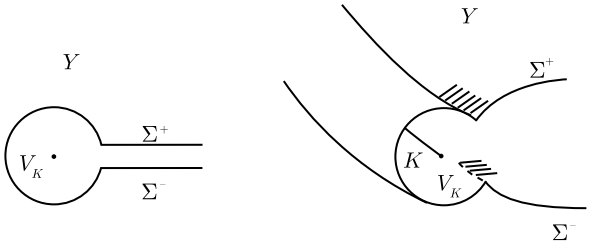


Fig. 2.13

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).

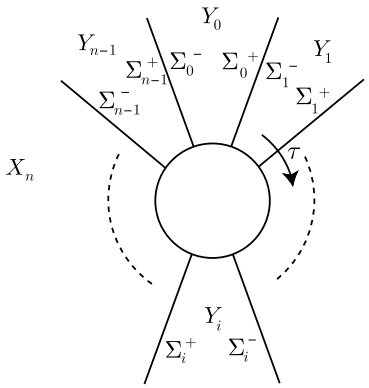


Fig. 2.14

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).

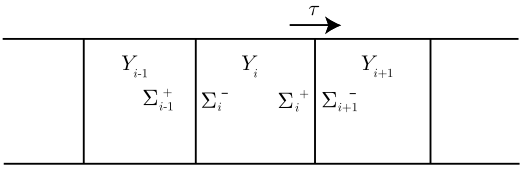


Fig. 2.15

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).

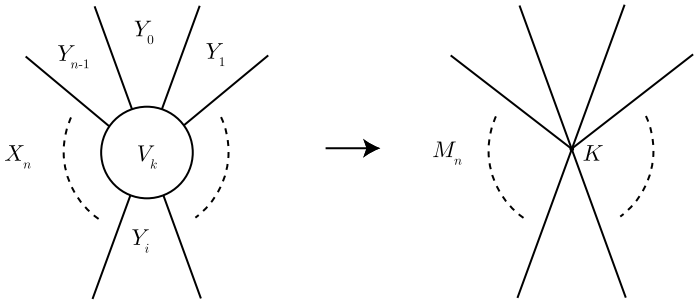


Fig. 2.16

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).

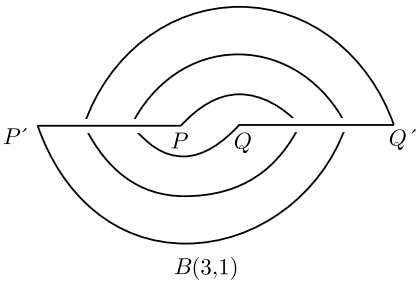


Fig. 2.17

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).

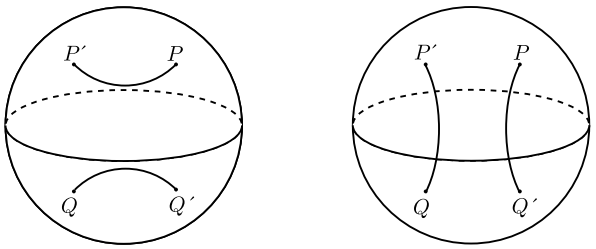


Fig. 2.18

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 $M = L(a, b)$.

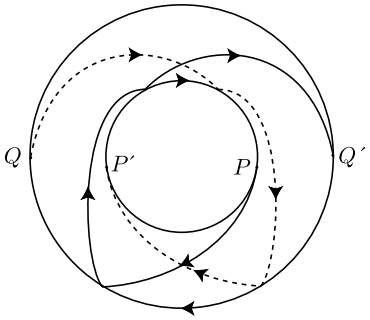


Fig. 2.19

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* $(h : Y \to X) \mapsto h_*(\pi_1(Y, \overline{y}))$ $(\bar{y} \in F_{\overline{x}}(Y))$ *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 $h : Y \to X \Leftrightarrow h_*(\pi_1(Y, \overline{y}))(\bar{y} \in F_{\overline{x}}(Y))$ is a subgroup of $h'_*(\pi_1(Y', \overline{y}'))$ $(\bar{y}' \in F_{\overline{x}}(Y'))$ up to conjugate.
$h : Y \to X$ is a Galois covering $\Leftrightarrow$ $h_*(\pi_1(Y, \overline{y}))$ $(\overline{y} \in F_{\overline{x}}(Y))$ 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*:

$$\begin{array}{l} 0 \to H^0(k, M) \to P^0(k, M) \to H^2(k, M')^* \to \quad H^1(k, M) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \downarrow \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad P^1(k, M) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \downarrow \\ 0 \leftarrow H^0(k, M')^* \leftarrow P^2(k, M) \leftarrow H^2(k, M) \leftarrow H^1(k, M')^* \end{array}$$

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

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

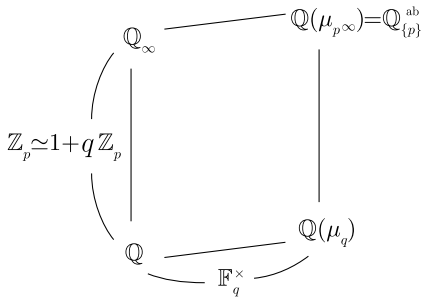
We set

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

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.

Chapter 3
Knots and Primes, 3-Manifolds and Number Rings

In this chapter, we explain the basic analogies between knots and primes, 3-manifolds and number rings, which will be fundamental in subsequent chapters.

By Examples 2.1 and Example 2.25, we find the following analogy between the fundamental groups of a circle S^1 and of a finite field $\mathbb{F}_q$.

$\pi_1(S^1) = \mathrm{Gal}(\mathbb{R}/S^1)$	$\pi_1(\mathrm{Spec}(\mathbb{F}_q)) = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$
$= \langle [l] \rangle$	$= \langle \sigma \rangle$
$\simeq \mathbb{Z}$	$\simeq \hat{\mathbb{Z}}$

(3.1)

Here, the loop l and the Frobenius automorphism σ, the universal covering $\mathbb{R}$ and the separable closure $\overline{\mathbb{F}}_q$, and the cyclic covering $\mathbb{R}/n\mathbb{Z} \to S^1$ and the cyclic extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ are corresponding, respectively. Since, in fact, $\pi_i(S^1)$ and $\pi_i(\mathrm{Spec}(\mathbb{F}_q))$ are trivial for $i \geq 2$, S^1 is the Eilenberg–MacLane space $K(\mathbb{Z}, 1)$ homotopically and $\mathrm{Spec}(\mathbb{F}_q)$ is regarded as an étale homotopical analogue $K(\hat{\mathbb{Z}}, 1)$.

Circle	Finite field
$S^1 = K(\mathbb{Z}, 1)$	$\mathrm{Spec}(\mathbb{F}_q) = K(\hat{\mathbb{Z}}, 1)$

(3.2)

A tubular neighborhood $V = S^1 \times D^2$ of a circle S^1 is homotopy-equivalent to the core S^1 and $V \setminus S^1$ is homotopy equivalent to the 2-dimensional torus ∂V. On the other hand, for a $\mathfrak{p}$-adic integer ring $\mathcal{O}_\mathfrak{p}$ whose residue field is $\mathbb{F}_q$ and quotient field is $k_\mathfrak{p}$ ($\mathfrak{p}$-adic field), $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ is étale homotopy equivalent to $\mathrm{Spec}(\mathbb{F}_q)$ and $\mathrm{Spec}(\mathcal{O}_\mathfrak{p}) \setminus \mathrm{Spec}(\mathbb{F}_q) = \mathrm{Spec}(k_\mathfrak{p})$. Hence $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ and $\mathfrak{p}$-adic field $\mathrm{Spec}(k_\mathfrak{p})$ are analogous to V and ∂V. In fact, we find the following analogy between $\pi_1(\partial V)$ and $\pi_1(\mathrm{Spec}(k_\mathfrak{p}))$. In the natural homomorphism $\pi_1(\partial V) \to \pi_1(V) = \pi_1(S^1)$, the image of a longitude $\beta = S^1 \times \{b\}$ ($b \in \partial D^2$) is a generator $l \in \pi_1(S^1)$ and the kernel is the infinite cyclic group generated by a meridian $\alpha = \{a\} \times \partial D^2$ ($a \in S^1$). Thus, $\pi_1(\partial V)$ is a free Abelian group generated by α and β which are subject to the relation $[\alpha, \beta] := \alpha\beta\alpha^{-1}\beta^{-1} = 1$ (Example 2.2). On the other hand, in the natural homomorphism $\pi_1(\mathrm{Spec}(k_\mathfrak{p})) \to \pi_1(\mathrm{Spec}(\mathcal{O}_\mathfrak{p})) = \pi_1(\mathrm{Spec}(\mathbb{F}_q))$, the image of an

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_3, © Springer-Verlag London Limited 2012

extension of the Frobenius automorphism (denoted by σ as well) in $\pi_1(\mathrm{Spec}(k_\mathfrak{p})) = \mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p})$ is $\sigma \in \pi_1(\mathrm{Spec}(\mathbb{F}_q)) = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and the kernel is the inertia group $I_{k_\mathfrak{p}}$. We call an element of $I_{k_\mathfrak{p}}$ *monodromy*. Although which monodromy we take as an analog of a meridian depends on the situation we are considering, there is a canonical generator τ, which corresponds to an meridian, in the maximal tame quotient $I^t_{k_\mathfrak{p}}$ of $I_{k_\mathfrak{p}}$. In fact, the tame fundamental group $\pi_1^t(\mathrm{Spec}(k_\mathfrak{p}))$ is a pro-finite group generated by τ and σ which are subject to the relation $\tau^{q-1}[\tau,\sigma] = 1$ (Example 2.39).

Tubular neighborhood V	$\mathfrak{p}$-adic integer ring $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$
Boundary ∂V	$\mathfrak{p}$-adic field $\mathrm{Spec}(k_\mathfrak{p})$
$1 \to \langle\alpha\rangle \to \pi_1(\partial V) \to \langle\beta\rangle \to 1$	$1 \to I_{k_\mathfrak{p}} \to \pi_1(\mathrm{Spec}(k_\mathfrak{p})) \to \langle\sigma\rangle \to 1$
β : longitude	σ : Frobenius automorphism
α : meridian	τ : monodromy ($\in I_{k_\mathfrak{p}}$)
$\pi_1(\partial V) = \langle\alpha,\beta \mid [\alpha,\beta] = 1\rangle$	$\pi_1^t(\mathrm{Spec}(k_\mathfrak{p})) = \langle\tau,\sigma \mid \tau^{q-1}[\tau,\sigma] = 1\rangle$

(3.3)

A knot is an embedding of S^1 into a 3-manifold M. On the other hand, as seen in Sect. 2.3, for the ring of integers $\mathcal{O}_k$ of a finite number field k, $\mathrm{Spec}(\mathcal{O}_k)$ is seen as an analog of a 3-dimensional manifold, since $\mathrm{Spec}(\mathcal{O}_k)$ has the étale cohomological dimension 3 (except for 2-torsion, when k has a real place) and satisfies the Artin–Verdier duality 2.42 which is an arithmetic analogue of 3-dimensional Poincaré duality.

3-manifold M	Number ring $\mathrm{Spec}(\mathcal{O}_k)$

(3.4)

For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$, by (3.2) and (3.4), the natural embedding $\mathrm{Spec}(\mathbb{F}_\mathfrak{p}) \hookrightarrow \mathrm{Spec}(\mathcal{O}_k)$ is regarded as an analogue of a knot.

Knot	Prime ideal
$S^1 \hookrightarrow M$	$\mathrm{Spec}(\mathbb{F}_\mathfrak{p}) \hookrightarrow \mathrm{Spec}(\mathcal{O}_k)$

(3.5)

In particular, since $\pi_1(\mathrm{Spec}(\mathbb{Z})) = 1$ (Example 2.35), $\mathrm{Spec}(\mathbb{Z})$ with the infinite prime ∞ is seen as an analogue of $S^3 = \mathbb{R} \cup \{\infty\}$, and the prime ideal (p) (p being a prime number) is seen as an analogue of a knot in $\mathbb{R}^3$.

Knot	Rational prime
$S^1 \hookrightarrow \mathbb{R}^3 \cup \{\infty\} = S^3$	$\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z}) \cup \{\infty\}$

(3.6)

Here we regard S^3 as the end-compactification of $\mathbb{R}^3$ and see the infinite prime as an analogue of the end. In general, the set of ends E_M of a non-compact 3-manifold M corresponds to the set of infinite primes S_k^∞ of a number field k [Dn2, Ra].

Ends E_M	Infinite primes S_k^∞

We should also note the analogy that any connected oriented 3-manifold is a finite covering of S^3 branched along a link (Alexander's theorem), just as any finite number field is a finite extension of $\mathbb{Q}$ ramified over a finite set of primes.

For a knot K in a 3-manifold M, let V_K be a tubular neighborhood of K, $X_K := M \setminus \mathrm{int}(V_K)$ the knot complement, $G_K = G_K(M) = \pi_1(X_K) = \pi_1(M \setminus K)$ the knot group (Example 2.6). The knot group G_K is the object which reflects how K is knotted in M. In fact, it is known that a prime knot K in S^3 is determined by the knot group G_K. Namely, for prime knots $K, L \subset S^3$, we have the following [GL, Wh]:

$$G_K \simeq G_L \iff K \simeq L. \tag{3.7}$$

Here $K \simeq L$ means that there is an auto-homeomorphism h of S^3 such that $h(K) = L$. Let α and β be a meridian and a longitude of K respectively. The image of the homomorphism $\pi_1(\partial X_K) = \langle \alpha, \beta \mid [\alpha, \beta] = 1 \rangle \to G_K$ induced by the inclusion $\partial X_K \hookrightarrow X_K$ is called the *peripheral group*, denoted by D_K. We also denote by I_K the image of the subgroup of generated by α in G_K. When $M = S^3$, we see by the Wirtinger presentation of G_K that G_K is generated by conjugates of I_K (Example 2.6).

On the other hand, by (3.3), for a prime ideal $\mathfrak{p}$ ($\neq (0)$) of $\mathcal{O}_k$, the $\mathfrak{p}$-adic field $\mathrm{Spec}(k_\mathfrak{p})$ plays a role of the "boundary" of $X_{\{\mathfrak{p}\}} := \mathrm{Spec}(\mathcal{O}_k) \setminus \{\mathfrak{p}\}$. How $\mathfrak{p}$ is knotted in $\mathrm{Spec}(\mathcal{O}_k)$ is reflected in the structure of the étale fundamental group $G_{\{\mathfrak{p}\}} := \pi_1(X_{\{\mathfrak{p}\}})$. Following the model of the knot group, we call $G_{\{\mathfrak{p}\}}$ the *prime group*. For prime numbers p, q, we have the following analogy of (3.7):

$$G_{\{(p)\}} \simeq G_{\{(q)\}} \iff p = q. \tag{3.8}$$

This is because the Abelianization $G_{\{p\}}^{\mathrm{ab}}$ of $G_{\{p\}}$ is isomorphic to $\mathbb{Z}_p^\times$ (Example 2.46). The arithmetic analogue of the peripheral group is the image of the natural homomorphism $\pi_1(\mathrm{Spec}(k_\mathfrak{p})) \to G_{\{\mathfrak{p}\}}$ induced by the inclusion $\mathrm{Spec}(k_\mathfrak{p}) \to X_{\{\mathfrak{p}\}}$, namely, the decomposition group $D_\mathfrak{p}$ over $\mathfrak{p}$, and the analogue of I_K is the inertia group $I_\mathfrak{p}$ over $\mathfrak{p}$ (Example 2.40).[1] When $k = \mathbb{Q}$, $G_{\{p\}}$ is generated by conjugates of $I_{\{p\}}$. In fact, if K denotes the extension of $\mathbb{Q}$ corresponding to the subgroup H of $G_{\{p\}}$ generated by conjugates of $I_{\{p\}}$, $K/\mathbb{Q}$ is an unramified extension in the narrow sense, and thus $K = \mathbb{Q}$ by $\pi_1(\mathrm{Spec}(\mathbb{Z})) = 1$. Hence, we have $H = G$. This may be regarded as a weak analogue of the Wirtinger presentation.

Boundary $\partial V_K \subset M \setminus \mathrm{int}(V_K)$	$\mathfrak{p}$-adic field $\mathrm{Spec}(k_\mathfrak{p}) \subset \mathrm{Spec}(\mathcal{O}_k) \setminus \{\mathfrak{p}\}$
Peripheral group D_K	Decomposition group $D_{\{\mathfrak{p}\}}$

(3.9)

In general, for a finite number field k and a finite subset S of $\mathrm{Max}(\mathcal{O}_k)$, the étale fundamental group $\pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$, namely, the Galois group $G_S(k) = \mathrm{Gal}(k_S/k)$ of

[1] Although we should write $G_{\{\mathfrak{p}\}}$, $D_{\{\mathfrak{p}\}}$ and $I_{\{\mathfrak{p}\}}$ as analogues of G_K, D_K and I_K respectively, we often write $G_\mathfrak{p}$, $D_\mathfrak{p}$ and $I_\mathfrak{p}$ for simplicity. For a prime number p, we also write $G_{\{p\}}$, $D_{\{p\}}$ and $I_{\{p\}}$ or simply G_p, D_p and I_p for $G_{\{(p)\}}$, $D_{\{(p)\}}$ and $I_{\{(p)\}}$, respectively.

the maximal Galois extension k_S over k unramified outside $S \cup S_k^\infty$ (Example 2.33) is regarded as an analogue of a link group G_L.

Link group	Galois group with restricted ramification
$G_L(M) = \pi_1(M \setminus L)$	$G_S(k) = \pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$

(3.10)

The pro-finite group $G_S(k)$ is huge in general, and it is unknown if even the prime group $G_{\{p\}}$ for a prime number p is finitely generated or not. It is a fundamental problem in algebraic number theory to understand the structure of $G_{\{p\}}$, in other words, to understand in the sense of étale homotopy theory

"how a prime number $\mathrm{Spec}(\mathbb{F}_p)$ is embedded in $\mathrm{Spec}(\mathbb{Z})$."

We note that this is the central problem in knot theory. The fact that the Galois group G_S is huge and complicated shows that the set S of primes is embedded in $\mathrm{Spec}(\mathcal{O}_k)$ in a very complicated, invisible manner. As we see in the subsequent chapters, however, it is possible to understand a glimpse of the "shape" of a prime number and how prime numbers are "linked", by taking the various quotients of G_S and comparing them with a link group G_L.

Remark 3.1 (1) We note that the analogies (3.4), (3.5) are conceptual, and it is not meant that there is a one to one correspondence between 3-manifolds and number rings, knots and primes. For instance, it is known that one has $\pi_1(\mathrm{Spec}(\mathcal{O}_k)) = 1$ for all imaginary quadratic fields of class number 1. Nevertheless, we have the following analogue of the Poincaré conjecture:

$$\hat{H}^i\big(\mathrm{Spec}(\mathcal{O}_k), \mathbb{Z}/n\mathbb{Z}\big) = \hat{H}^i\big(\mathrm{Spec}(\mathbb{Z}), \mathbb{Z}/n\mathbb{Z}\big) \quad (i \in \mathbb{Z}, n \geq 2)$$
$$\Longleftrightarrow \quad \mathcal{O}_k = \mathbb{Z}.$$

This follows from the Artin–Verdier duality 2.42 and Dirichlet's unit theorem 2.31. It should be noted that Dirichlet's unit theorem is analytic in nature.

(2) It has been commonly considered that a number ring $\mathrm{Spec}(\mathcal{O}_k)$ is an analogue of an algebraic curve C over a finite field $\mathbb{F}_q$ and so a prime ideal of a number ring corresponds to a point on a curve. Let $\overline{C} := C \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Since $\overline{C}$ is an algebraic curve over an algebraically closed field, $\overline{C}$ is of dimension 2 étale homotopically (Note that a curve over the field of complex numbers is a Riemann surface). In view of the fibration $\overline{C} \to C \to \mathrm{Spec}(\mathbb{F}_q)$, C may be regarded as a surface-bundle over S^1.

Algebraic curve over $\mathbb{F}_q$	Surface-bundle over S^1

Since a number ring has no constant field, the structure of $\pi_1(\mathrm{Spec}(\mathcal{O}_k))$ has no analogy with that of $\pi_1(C)$ and is quite random (it can be both finite and infinite). We may also note that the analogy of (3.7), (3.8) for 2 points on an affine line does not hold. Thus, it is appropriate to compare $\pi_1(\mathrm{Spec}(\mathcal{O}_k))$ with 3-manifold groups in general. One might regard the set of roots of unity in a number ring $\mathcal{O}_k$ as

like the constant field of $\mathcal{O}_k$. In fact, from this viewpoint, Iwasawa considered the extension k_∞/k obtained by adjoining all p-th power of roots of unity to k as an analog of the extension $\overline{\mathbb{F}}_q(\overline{C})/\mathbb{F}_q(C)$ of constant fields and showed some analogies between the number field k_∞ and the algebraic function field $\overline{\mathbb{F}}_q(\overline{C})$ [Iw1]; see also [NSW, Chap. XI]. However, it should be noted that the extension k_∞/k is ramified over p unlike the unramified extension $\overline{\mathbb{F}}_q(\overline{C})/\mathbb{F}_q(C)$. So, again, it is more natural to regard k_∞/k as an analogue of the tower of cyclic coverings of a 3-manifold ramified over a knot. It is our viewpoint throughout this book to regard a prime of a number field as an analogue of a knot in a 3-manifold rather than a point on an algebraic curve (Riemann surface classically), and the Galois group $G_S(k)$ as an analogue of a link group rather than the fundamental group of an algebraic curve (surface group). Although the idea of regarding a prime as an analogue of a circle has already been known in the study of closed geodesics in a Riemannian manifold or periodic orbits of a dynamical system [Sn], it is essential in our analogy to see a number ring as being 3-dimensional, together with the local analogies such as (3.3) and (3.9).

(3) C. Deninger [Dn1] proposed a conjecture that to any number field k one could associate a certain 3-dimensional space M_k with 2-dimensional foliation $\mathcal{F}$ and a dynamical system ϕ^t $(t \in \mathbb{R})$ on M_k so that the dynamical $\mathbb{R}$-action on the foliation cohomology $H^*_{\mathcal{F}}(M_k)$ would play a similar role to the $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-action on the geometric l-adic cohomology $H^*(\overline{C})$ of an algebraic curve C over $\mathbb{F}_q$. The conjecture also asserts that there would be a one to one correspondence between the set of maximal ideals $\mathfrak{p}$ of $\mathcal{O}_k$ and the set of closed $\mathbb{R}$-orbits (knots) γ in M_k under the equality $\mathrm{N}\mathfrak{p} =$ length of γ. B. Morin [Mn2] also studies arithmetic topology in connection with Deninger's conjecture using the notion of Weil-étale topos.

Chapter 4
Linking Numbers and Legendre Symbols

In this chapter, we shall discuss the analogy between the linking number and the Legendre symbol, based on the analogies between knots and primes in Chap. 3.

4.1 Linking Numbers

Let $K \cup L$ be a 2-component link in S^3. The *linking number* $\mathrm{lk}(L, K)$ is described in terms of the monodromy as follows. Let $X_L = S^3 \setminus \mathrm{int}(V_L)$ be the exterior of L and let $G_L = \pi_1(X_L)$ be the knot group of L. For a meridian α of L, let $\psi_\infty : G_L \to \mathbb{Z}$ be the surjective homomorphism sending α to 1. Let X_∞ be the infinite cyclic cover of X_L corresponding to $\mathrm{Ker}(\psi)$, and let τ denote the generator of $\mathrm{Gal}(X_\infty / X_L)$ corresponding to $1 \in \mathbb{Z}$ (Example 2.12). Let $\rho_\infty : G_L \to \mathrm{Gal}(X_\infty / X_L)$ be the natural homomorphism (monodromy permutation representation).

Proposition 4.1 $\rho_\infty([K]) = \tau^{\mathrm{lk}(L,K)}$.

Proof We construct X_∞ as in Example 2.12. Namely let Y be the space obtained by cutting X_L along the Seifert surface Σ_L of L, and we construct X_∞ by gluing the copies Y_i ($i \in \mathbb{Z}$) of Y as follows (Fig. 4.1).

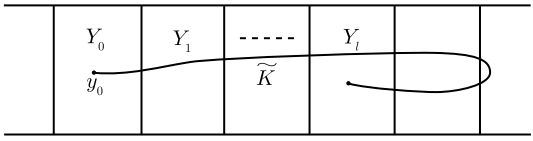


Fig. 4.1

Let $\tilde{K}$ be a lift of K in X_∞. According as K crosses Σ_L with intersection number $+1$ (resp. -1), $\tilde{K}$ crosses from Y_i to Y_{i+1} (resp. from Y_{i+1} to Y_i) for some i. Therefore, if the starting point y_0 of $\tilde{K}$ is in Y_0, the terminus of $\tilde{K}$ is in Y_l, $l = \mathrm{lk}(L, K)$.

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_4, © Springer-Verlag London Limited 2012

Hence, we have $\rho_\infty([K])(y_0) \in Y_l$. Since τ is the map sending Y_i to Y_{i+1}, this means $\rho_\infty([K]) = \tau^l$. □

Let $\psi_2 : G_L \to \mathbb{Z}/2\mathbb{Z}$ be the composite map of ψ_∞ with the natural homomorphism $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ and let $h_2 : X_2 \to X_L$ be the double covering of X_L corresponding to $\mathrm{Ker}(\psi_2)$. Let $\rho_2 : G_L \to \mathrm{Gal}(X_2/X_L)$ be the natural homomorphism. By Proposition 4.1, we have the following.

Corollary 4.2 *The image of* $[K]$ *under the composite map* $G_L \overset{\rho_2}{\to} \mathrm{Gal}(X_2/X_L) \simeq \mathbb{Z}/2\mathbb{Z}$ *is given by* $\mathrm{lk}(L, K) \bmod 2$:

$$\begin{aligned} G_L &\overset{\rho_2}{\to} \mathrm{Gal}(X_2/X_L) \simeq \mathbb{Z}/2\mathbb{Z} \\ [K] &\mapsto \mathrm{lk}(L, K) \bmod 2 \end{aligned}$$

For $y \in h_2^{-1}(x)$ $(x \in K)$, we see that

$$\begin{aligned} \rho_2\big([K]\big)(y) &= y.[K] \\ &= \text{the terminus of the lift of } K \text{ with starting point } y. \end{aligned}$$

This implies

$$\begin{aligned} &\rho_2\big([K]\big) = \mathrm{id}_{X_2} \iff h_2^{-1}(K) = K_1 \cup K_2 \quad \text{(2-component link in } X_2), \\ &\rho_2\big([K]\big) = \tau \iff h_2^{-1}(K) = \mathfrak{K} \quad \text{(knot in } X_2). \end{aligned}$$

Hence, by Corollary 4.2, we have the following:

$$h_2^{-1}(K) = \begin{cases} K_1 \cup K_2 & \mathrm{lk}(L, K) \equiv 0 \bmod 2, \\ \mathfrak{K} & \mathrm{lk}(L, K) \equiv 1 \bmod 2. \end{cases} \tag{4.1}$$

Example 4.3 Let $K \cup L$ be the following link (Fig. 4.2).

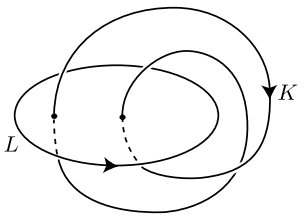


Fig. 4.2

Since $\mathrm{lk}(L, K) = 2$, K is decomposed in X_2 as $h_2^{-1}(K) = K_1 \cup K_2$. In fact, $h_2^{-1}(K)$ is drawn in X_2 as follows (Fig. 4.3).

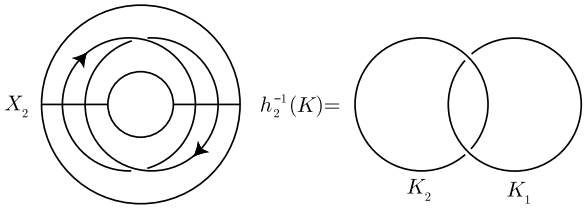


Fig. 4.3

Let $K \cup L$ be the following link (Fig. 4.4).

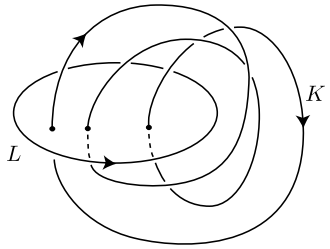


Fig. 4.4

Since $\mathrm{lk}(L, K) = 3$, K is lifted to a knot $h_2^{-1}(K) = \mathfrak{K}$ in X_2. In fact, $h_2^{-1}(K)$ is drawn in X_2 as follows (Fig. 4.5).

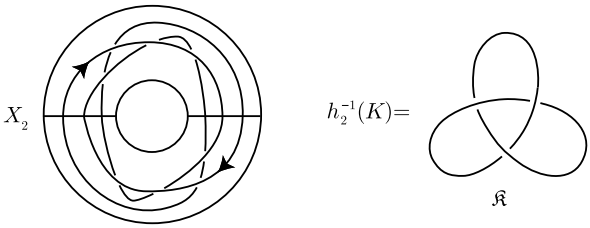


Fig. 4.5

4.2 Legendre Symbols

Let p and q be odd prime numbers. Let $X_{\{q\}} := \mathrm{Spec}(\mathbb{Z}) \setminus \{q\} = \mathrm{Spec}(\mathbb{Z}[1/q])$ and let $G_{\{q\}} = \pi_1(X_{\{q\}})$ be the prime group of q. Let α be a primitive root mod q and let $\psi_2 : G_{\{q\}} = \mathbb{Z}_q^\times = \mathbb{F}_q^\times \times (1 + q\mathbb{Z}_q) \to \mathbb{Z}/2\mathbb{Z}$ be the surjective homomorphism defined by $\psi_2(\alpha) = 1, \psi_2(1 + q\mathbb{Z}_q) = 0$. Let k be the quadratic extension of $\mathbb{Q}$

corresponding to $\mathrm{Ker}(\psi_2)$ (Example 2.46). Namely, $k = \mathbb{Q}(\sqrt{q^*})$, $q^* := (-1)^{\frac{q-1}{2}} q$. The field k is the unique quadratic extension of $\mathbb{Q}$ such that only q is ramified among all finite primes. Let $h_2 : X_2 \to X_{\{q\}}$ be the associated double étale covering where $X_2 := \mathrm{Spec}(\mathbb{Z}[(1+\sqrt{q^*})/2, 1/q])$. We note that $q \equiv 1 \bmod 4$ is a natural condition on q to get a situation closer to the knot case, since this is the condition that there is a (unique) quadratic extension of $\mathbb{Q}$ in which only q is ramified among all primes ((q) is homologous to 0). Let ρ_2 be the natural homomorphism $G_{\{q\}} \to \mathrm{Gal}(X_2/X_{\{q\}})$. According to (3.6) and Corollary 4.2, we define the $\bmod 2$ *linking number* $\mathrm{lk}_2(q, p)$ of p and q by the image of the Frobenius automorphism σ_p over p (Example 2.40) under the composite map $G_{\{q\}} \xrightarrow{\rho_2} \mathrm{Gal}(X_2/X_{\{q\}}) \simeq \mathbb{Z}/2\mathbb{Z}$:

$$\begin{aligned} G_{\{q\}} &\xrightarrow{\rho_2} \mathrm{Gal}(X_2/X_{\{q\}}) \simeq \mathbb{Z}/2\mathbb{Z} \\ \sigma_p &\longmapsto \mathrm{lk}_2(q, p). \end{aligned}$$

Then we have the following.

Proposition 4.4

$$(-1)^{\mathrm{lk}_2(q,p)} = \left(\frac{q^*}{p}\right).$$

Proof

$$\begin{aligned} \mathrm{lk}_2(q, p) = 0 &\iff \rho_2(\sigma_p) = \mathrm{id}_{X_2} \\ &\iff \sigma_p(\sqrt{q^*}) = \sqrt{q^*} \\ &\iff \sqrt{q^*} \in \mathbb{F}_p^\times \\ &\iff q^* \in (\mathbb{F}_p^\times)^2 \\ &\iff q^* \text{ is a quadratic residue } \bmod p \\ &\iff \left(\frac{q^*}{p}\right) = 1. \end{aligned}$$

□

By the ring isomorphism $\mathcal{O}_k/q\mathcal{O}_k \simeq \mathbb{F}_p[X]/(X^2 - q^*)$, the prime ideal decomposition of $p\mathcal{O}_k$ is given by the following:

$$p\mathcal{O}_k = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2, & q^* \text{ is a quadratic residue } \bmod p \\ \mathfrak{p}, & q^* \text{ is a quadratic non-residue } \bmod p. \end{cases}$$

By Proposition 4.4, we have

$$h_2^{-1}(\{p\}) = \begin{cases} \{\mathfrak{p}_1, \mathfrak{p}_2\}, & \mathrm{lk}_2(p, q) = 0 \\ \mathfrak{p}, & \mathrm{lk}_2(p, q) = 1. \end{cases} \tag{4.2}$$

This is the arithmetic analogue of (4.1). For example, the 5 primes $\{5, 13, 17, 29, 149\}$ are linked mod 2 as in the following Fig. 4.6.

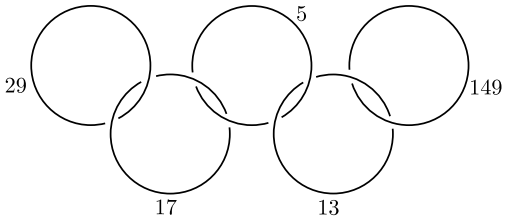


Fig. 4.6 Olympic primes

By Proposition 4.4, we see that the Legendre symbol is an arithmetic analogue of the mod2 linking number, and the symmetry of the linking number corresponds to the symmetry of the Legendre symbol for prime numbers $p, q \equiv 1 \bmod 4$.

Remark 4.5 The linking number is also given by the cup product. For a link $L = K_1 \cup K_2$ in S^3, let $\alpha_i^* \in H^1(X)$ (X being the exterior of L in S^3) be the dual of a meridian α_i of K_i. Under the isomorphism $H^2(X) \simeq \mathbb{Z}$ given by a generator of $H^2(X)$ which is the Lefschetz dual to a path from K_1 to K_2, the cup product $\alpha_1 \cup \alpha_2$ is sent to $\mathrm{lk}(K_1, K_2)$. Similarly, the Legendre symbol is also interpreted as a cup product in the étale (or Galois) cohomology group (cf. [Kc1, 8.11], [M9, 2], [Wl]).

Remark 4.6 What is an arithmetic analogue of Gauss' integral expression for the linking number in the Introduction? In order to answer this question, we first reformulate Gauss' formula as follows:

$$\int_{x \in K} \int_{y \in L} \omega(x - y) = \mathrm{lk}(K, L), \tag{4.3}$$

where ω is the differential 1-form on $\mathbb{R}^3$ given by

$$\omega = \frac{1}{4\pi \|x\|^3}(x_1\, dx_2 \wedge dx_3 + x_2\, dx_3 \wedge dx_1 + x_3\, dx_1 \wedge dx_2).$$

Furthermore, using the infinite dimensional integral, we rewrite the left-hand side of (4.3) in the following gauge-theoretic manner [Kh, 3.3]: For a framed link $K_1 \cup K_2$, one has

$$\begin{aligned}
&\int_{A(\mathbb{R}^3)} \exp\left(\frac{\sqrt{-1}}{4\pi} \int_{\mathbb{R}^3} a \wedge da + \sqrt{-1} \int_{K_1} a + \sqrt{-1} \int_{K_2} a\right) \mathcal{D}a \\
&\quad = \exp\left(\sum_{1 \le i, j \le 2} \int_{x \in K_i} \int_{y \in K_j} \omega(x - y)\right) \\
&\quad = \exp\left(\frac{\sqrt{-1}}{4} \sum_{1 \le i, j \le 2} \mathrm{lk}(K_i, K_j)\right).
\end{aligned} \tag{4.4}$$

Here $A(\mathbb{R}^3)$ stands for the space of differential 1-forms on $\mathbb{R}^3$ and the integral in the left-hand side means the path integral over $A(\mathbb{R}^3)$, and $\mathrm{lk}(K_i, K_i)$ denotes the self linking number. Since the integrals $\int_{\mathbb{R}^3} a \wedge da$ and $\int_{K_i} a$ are regarded as the quadratic and linear forms on $A(\mathbb{R}^3)$ respectively, by completing the square, the path integral in (4.4) is regarded as an infinite dimensional analogue of the Gaussian integral

$$\int_{\mathbb{R}} e^{-x^2} dx. \tag{4.5}$$

On the other hand, the arithmetic analogue of the Gaussian integral (4.5) on the finite field $\mathbb{F}_q$ is nothing but the Gaussian sum

$$\sum_{x \in \mathbb{F}_q} \zeta_q^{x^2},$$

where ζ_q is a q-th root of unity in an algebraic closure of $\mathbb{F}_p$. As Gauss showed, the Legendre symbol is expressed by the Gaussian sum as follows [Se1, 3.3, Lemma 2]:

$$\left(\sum_{x \in \mathbb{F}_q} \zeta_q^{x^2} \right)^{p-1} = \left(\frac{q^*}{p} \right) = (-1)^{\mathrm{lk}_2(q,p)}. \tag{4.6}$$

Comparing (4.4) and (4.6), one may find that the Gauss' integral formula for the linking number is analogous to the formula expressing the Legendre symbol by the Gaussian sum.

Summary

Linking number $\mathrm{lk}(L, K)$	Legendre symbol $(\frac{q^*}{p})$
$\mathrm{lk}(L, K) = \mathrm{lk}(K, L)$	$(\frac{q}{p}) = (\frac{p}{q})$ $(p, q \equiv 1 \bmod 4)$
Gauss' linking integral	Gaussian sum

Chapter 5
Decompositions of Knots and Primes

As we have seen in Sect. 4.2, the Legendre symbol describes how a prime number is decomposed in a quadratic extension. More generally, the Hilbert theory deals with, in a group-theoretic manner, the decomposition of a prime in a finite Galois extension of number fields, and further the Artin reciprocity of class field theory describes, in an arithmetic manner, the decomposition law of a prime in a finite Abelian extension. Based on the analogies in Chap. 3, we shall give a topological analogue of the Hilbert theory for coverings of 3-manifolds.

5.1 Decomposition of a Knot

Let $h : M \to S^3$ be a finite Galois covering of connected oriented closed 3-manifolds ramified over a link $L \subset S^3$, and let $X := S^3 \setminus L$, $Y := M \setminus h^{-1}(L)$, $G := \mathrm{Gal}(Y/X) = \mathrm{Gal}(M/S^3)$ and $n := \#G(\geq 1)$. Let K be a knot in S^3 which is a component of L or disjoint from L, and suppose $h^{-1}(K) = K_1 \cup \cdots \cup K_r$ ($r = r_K$-component link). For a tubular neighborhood V_K of K, let V_{K_i} be the connected component of $h^{-1}(V_K)$ containing K_i. Fix a base point $x \in \partial V_K$. Suppose $h^{-1}(x) = \{y_1, \ldots, y_n\}$. Let $\rho : G_L = \pi_1(X, x) \to \mathrm{Aut}(h^{-1}(x))$ be the monodromy permutation representation which induces an isomorphism $\pi_1(X, x)/h_*(\pi_1(Y, y_i)) \simeq \mathrm{Im}(\rho) \simeq G$. Note that $\pi_1(X, x)$ and hence G acts transitively on the set of knots $S_K := \{K_1, \ldots, K_r\}$ lying over K. We call the stabilizer D_{K_i} of K_i the *decomposition group* of K_i:

$$D_{K_i} := \{g \in G \mid g(K_i) = K_i\}.$$

Since we have the bijection $G/D_{K_i} \simeq S_K$ for each i, $\#D_{K_i} = n/r$ is independent of K_i. In fact, if $g(K_i) = K_j$ ($g \in G$), $D_{K_j} = gD_{K_i}g^{-1}$. Since each $g \in G$ induces a homeomorphism $g|_{\partial V_{K_i}} : \partial V_{K_i} \xrightarrow{\approx} \partial V_{g(K_i)}$, $g|_{\partial V_{K_i}}$ is a covering transformation of ∂V_{K_i} over ∂V_K for $g \in D_{K_i}$, and the correspondence $g \mapsto g|_{\partial V_{K_i}}$ gives an isomorphism

$$D_{K_i} \simeq \mathrm{Gal}(\partial V_{K_i}/\partial V_K).$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_5, © Springer-Verlag London Limited 2012

The Fox completion of the subcovering space of Y over X corresponding to D_{K_i} is called the *decomposition* (*covering*) *space* of K_i and is denoted by Z_{K_i}. The map $g \mapsto \overline{g} := g|_{K_i}$ induces the homomorphism

$$D_{K_i} \to \mathrm{Gal}(K_i/K)$$

whose kernel is called the *inertia group* of K_i and is denoted by I_{K_i}:

$$I_{K_i} := \{g \in D_{K_i} \mid \overline{g} = \mathrm{id}_{K_i}\}.$$

If $K_j = g(K_i)$ $(g \in G)$, one has $I_{K_j} = gI_{K_i}g^{-1}$ and hence $\#I_{K_i}$ is independent of K_i. Set $e = e_K := \#I_{K_i}$. The Fox completion of the subcovering space of Y over X corresponding to I_{K_i} is called the *inertia* (*covering*) *space* of K_i and is denoted by T_{K_i}:

$$M \longrightarrow T_{K_i} \longrightarrow Z_{K_i} \longrightarrow S^3.$$

Since the Galois group G acts on $h^{-1}(x)$ simply-transitively, we can understand D_{K_i} and I_{K_i} by looking at their actions on $h^{-1}(x)$. Let α be a meridian of K and β be a longitude of K, and take $y_{i_1} \in \partial V_i$. The orbits of y_{i_1} under the action of D_{K_i} and I_{K_i} coincide with the orbits of y_{i_1} under the action of $\rho(\langle\alpha, \beta\rangle)$ and $\rho(\langle\alpha\rangle)$, respectively. Let $\rho(\langle\alpha\rangle)(y_{i_1}) = \{y_{i_1}, \ldots, y_{i_e}\}$. If we write $\rho(\alpha)$ as the product of mutually disjoint cyclic permutations, the cyclic permutation $(y_{i_1} \cdots y_{i_e})$ is the factor containing y_{i_1} and e is the ramification index of K_i over K. On the other hand, $\rho(\langle\alpha, \beta\rangle)(y_{i_1})$ is nothing but the set of $y_j \in h^{-1}(x)$ so that $y_j \in \partial V_{K_i}$. Let $f = f_K$ be the minimum $m \in \mathbb{N}$ such that $y_{i_1}^m := \rho(\beta^m)(y_{i_1}) \in \{y_{i_1}, \ldots, y_{i_e}\}$. Then f is the covering degree of K_i over K and we have

$$\begin{aligned}\rho\big(\langle\alpha, \beta\rangle\big)(y_{i_1}) &= \big\{y_j \in h^{-1}(x) \mid y_j \in \partial V_i\big\} \\ &= \big\{y_{i_1}^m, \ldots, y_{i_e}^m \mid 0 \le m < f\big\} \quad \text{(Fig. 5.1)}.\end{aligned}$$

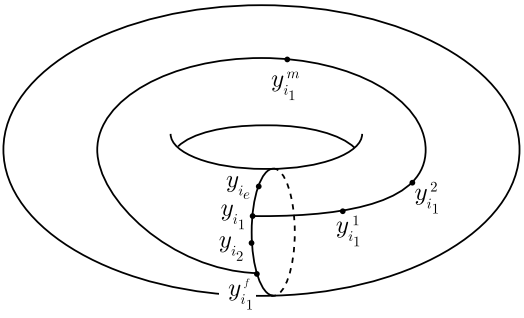


Fig. 5.1

Hence, we have the equalities

$$\begin{aligned}\#D_{K_i} &= \#\rho\big(\langle\alpha, \beta\rangle\big)(y_{i_1}) = ef, \\ \#I_{K_i} &= \#\rho\big(\langle\alpha\rangle\big)(y_{i_1}) = e, \qquad \#\mathrm{Gal}(K_i/K) = f.\end{aligned}$$

By comparing the orders, we see that the homomorphism $D_{K_i} \ni g \mapsto \overline{g} \in \mathrm{Gal}(K_i/K)$ is surjective:

$$1 \longrightarrow I_{K_i} \longrightarrow D_{K_i} \longrightarrow \mathrm{Gal}(K_i/K) \longrightarrow 1 \quad \text{(exact)}.$$

In particular, we have the equality $efr = n$, and therefore we have the following:

$$\begin{array}{lllll} D_{K_i} = 1 & \Longleftrightarrow & Z_{K_i} = M & \Longleftrightarrow & e = f = 1,\ r = n, \\ D_{K_i} = G & \Longleftrightarrow & Z_{K_i} = S^3 & \Longleftrightarrow & ef = n,\ r = 1, \\ I_{K_i} = 1 & \Longleftrightarrow & T_{K_i} = M & \Longleftrightarrow & e = 1,\ fr = n, \\ I_{K_i} = G & \Longleftrightarrow & T_{K_i} = S^3 & \Longleftrightarrow & e = n,\ f = r = 1. \end{array}$$

In general one has the following theorem. Let $K_{i,T}$ be the image of K_i under $M \to T_{K_i}$ and let $K_{i,Z}$ be the image of $K_{i,T}$ under $T_{K_i} \to Z_{K_i}$.

Theorem 5.1 *The map $M \to T_{K_i}$ is a ramified covering of degree e such that the ramification index of K_i over $K_{i,T}$ is e. The map $T_{K_i} \to Z_{K_i}$ is a cyclic covering of degree f such that the covering degree of $K_{i,T}$ over $K_{i,Z}$ is f. The map $Z_{K_i} \to S^3$ is a covering of degree r such that K is completely decomposed into an r-component link containing $K_{i,Z}$ as a component.*

Now assume that G is an Abelian group. Then D_{K_i}, I_{K_i} and Z_{K_i}, T_{K_i} are independent of K_i and so we write respectively, D_K, I_K and Z_K, T_K for them. In the covering $h : M \to S^3$, K is decomposed, covered and ramified as follows:

$$\begin{array}{ccc} \{1\} & M & \\ {\scriptstyle e}\big| & \big\downarrow & ramified \\ I_K & T_K & \\ {\scriptstyle f}\big| & \big\downarrow & covered \\ D_K & Z_K & \\ {\scriptstyle r}\big| & \big\downarrow & decomposed \\ G & S^3 & \end{array} \qquad \begin{array}{c} K_1, \ldots, K_r \\ \big\downarrow \\ K_{1,T}, \ldots, K_{r,T} \\ \big\downarrow \\ K_{1,Z}, \ldots, K_{r,Z} \\ \big\downarrow \\ K \end{array}$$

Assume further that K is unramified, namely, K is disjoint from L. Since $I_K = 1$, we have an isomorphism $D_K \simeq \mathrm{Gal}(K_i/K)$. Let σ_K be the generator of D_K which is defined by the inverse image under this isomorphism of the generator of $\mathrm{Gal}(K_i/K)$ corresponding the loop going once around K counterclockwise (Example 2.9). By the equality $fr = n$, the decomposition law of K in the covering $h : M \to S^3$ is determined by f, namely, the order of σ_K in G.

Remark 5.2 The above argument and results hold similarly for any finite Galois ramified covering $M \to N$ of 3-manifolds and a knot in N.

Finally, let us extend the relation between the mod 2 linking number and the decomposition law of a knot in a double covering in Sect. 4.1 to the case of any cyclic covering. Let $K \cup L \subset S^3$ be a 2-component link. For an integer $n \geq 2$, let $\psi : G_L \to \mathbb{Z}/n\mathbb{Z}$ be the homomorphism sending a meridian of L to 1 mod n. Let $X_n \to X_L$ be the cyclic covering of degree n corresponding to $\mathrm{Ker}(\psi)$ and let $h_n : M \to S^3$ be its Fox completion. Let τ be the generator of $\mathrm{Gal}(X_n/X_L)$ corresponding to 1 mod n (Example 2.12). Finally, let $\rho : G_L \to \mathrm{Gal}(X_n/X_L)$ be the natural homomorphism. Then we have, by the definition of σ_K above,

$$\sigma_K = \rho\big([K]\big).$$

Therefore, we have, by Proposition 4.1,

$$\sigma_K = \tau^{\mathrm{lk}(L,K)}. \tag{5.1}$$

Hence one has, for a positive divisor m of n,

$$\text{g.c.d.}\big(\mathrm{lk}(L,K), n\big) = m \iff h_n^{-1}(K) = K_1 \cup \cdots \cup K_m.$$

In particular, K is decomposed completely in X_n (i.e., decomposed into an n-component link) if and only if $\mathrm{lk}(L,K) \equiv 0 \bmod n$.

5.2 Decomposition of a Prime

Let $k/\mathbb{Q}$ be a finite Galois extension ramified over a finite set S of prime numbers. Let $h : \mathrm{Spec}(\mathcal{O}_k) \to \mathrm{Spec}(\mathbb{Z})$ be the associated ramified covering. We set $X := \mathrm{Spec}(\mathbb{Z}) \setminus S$, $Y := \mathrm{Spec}(\mathcal{O}_k) \setminus h^{-1}(S)$, $G := \mathrm{Gal}(Y/X) = \mathrm{Gal}(k/\mathbb{Q})$, $n := \#G (\geq 1)$. Let p be a prime number and let $S_p := h^{-1}(\{p\}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ $(r = r_p)$. One has $\mathcal{O}_k \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{i=1}^{r} \mathcal{O}_{\mathfrak{p}_i}$ where $\mathcal{O}_{\mathfrak{p}_i}$ is the $\mathfrak{p}_i$-adic completion of $\mathcal{O}_k$. Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and let $\overline{x} : \mathrm{Spec}(\overline{\mathbb{Q}}_p) \to X$ be the base point induced by the inclusion $\mathbb{Z}[1/S] \subset \overline{\mathbb{Q}}_p$. Let $F_{\overline{x}}(Y) = \mathrm{Hom}_X(\mathrm{Spec}(\overline{\mathbb{Q}}_p), Y) = \{y_1, \ldots, y_n\}$ and let $\rho : G_S := \pi_1(X, \overline{x}) \to \mathrm{Aut}(F_{\overline{x}}(Y))$ be the monodromy permutation representation which induces an isomorphism $\pi_1(X, \overline{x})/h_*(\pi_1(Y, y_i)) \simeq \mathrm{Im}(\rho) \simeq G$. Note that $\pi_1(X, \overline{x})$ and hence G acta on S_p transitively. We call the stabilizer $D_{\mathfrak{p}_i}$ of $\mathfrak{p}_i$ the *decomposition group* of $\mathfrak{p}_i$:

$$D_{\mathfrak{p}_i} := \big\{ g \in G \mid g(\mathfrak{p}_i) = \mathfrak{p}_i \big\}.$$

Since we have the bijection $G/D_{\mathfrak{p}_i} \simeq S_p$, $\#D_{\mathfrak{p}_i} = n/r$ is independent of $\mathfrak{p}_i$. In fact, if $\mathfrak{p}_j = g(\mathfrak{p}_i)$ $(g \in G)$, we have $D_{\mathfrak{p}_j} = g D_{\mathfrak{p}_i} g^{-1}$. Since $g \in G$ induces an isomorphism $\hat{g} : k_{\mathfrak{p}_i} \xrightarrow{\sim} k_{g(\mathfrak{p}_i)}$, $\hat{g}$ gives an isomorphism of $k_{\mathfrak{p}_i}$ over $\mathbb{Q}_p$ if $g \in D_{\mathfrak{p}_i}$, and the correspondence $g \mapsto \hat{g}$ gives the isomorphism

$$D_{\mathfrak{p}_i} \simeq \mathrm{Gal}(k_{\mathfrak{p}_i}/\mathbb{Q}_p).$$

The subfield of k corresponding to $D_{\mathfrak{p}_i}$ is called the *decomposition field* of $\mathfrak{p}_i$ and is denoted by $Z_{\mathfrak{p}_i}$. Furthermore, $g \in D_{\mathfrak{p}_i}$ induces the isomorphism $\overline{g}$ of $\mathbb{F}_{\mathfrak{p}_i} = \mathcal{O}_k/\mathfrak{p}_i$ over $\mathbb{F}_p$ defined by $\overline{g}(\alpha \bmod \mathfrak{p}_i) := g(\alpha) \bmod \mathfrak{p}_i$ $(\alpha \in \mathcal{O}_k)$. The map $g \mapsto \overline{g}$ gives the homomorphism

$$D_{\mathfrak{p}_i} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p).$$

whose kernel is called the *inertia group* of $\mathfrak{p}_i$ and is denoted by $I_{\mathfrak{p}_i}$ F

$$I_{\mathfrak{p}_i} := \{g \in D_{\mathfrak{p}_i} \mid \bar{g} = \mathrm{id}_{\mathbb{F}_{\mathfrak{p}_i}}\}.$$

If $g(\mathfrak{p}_i) = \mathfrak{p}_j$ $(g \in G)$, one has $I_{\mathfrak{p}_j} = g I_{\mathfrak{p}_i} g^{-1}$ and hence $\# I_{\mathfrak{p}_i}$ is independent of $\mathfrak{p}_i$. Set $e = e_p := \# I_{\mathfrak{p}_i}$. The subfield of k corresponding to $I_{\mathfrak{p}_i}$ is called the *inertia field* of $\mathfrak{p}_i$ and is denoted by $T_{\mathfrak{p}_i}$:

$$k \supset T_{\mathfrak{p}_i} \supset Z_{\mathfrak{p}_i} \supset \mathbb{Q}.$$

Lemma 5.3 *The homomorphism* $D_{\mathfrak{p}_i} \ni g \mapsto \overline{g} \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p)$ *is surjective*:

$$1 \longrightarrow I_{\mathfrak{p}_i} \longrightarrow D_{\mathfrak{p}_i} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p) \longrightarrow 1 \quad \text{(exact)}.$$

Proof Since $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p)$ is generated by the Frobenius automorphism σ, it suffices to show that there is $g \in D_{\mathfrak{p}_i}$ such that $\bar{g} = \sigma$. Take $\theta \in \mathcal{O}_k$ so that $\mathbb{F}_{\mathfrak{p}_i} = \mathbb{F}_p(\bar{\theta})$, $\bar{\theta} = \theta \bmod \mathfrak{p}_i$. By the Chinese remainder theorem, we have an $\alpha \in \mathcal{O}_k$ such that $\alpha \equiv \theta \bmod \mathfrak{p}_i$ and $\alpha \not\equiv 0 \bmod \mathfrak{p}_i^g$, $\forall g \notin D_{\mathfrak{p}_i}$. Using such an α, consider the polynomial

$$f(X) := \prod_{g \in G} \big(X - g(\alpha)\big).$$

Then we see easily $f(X) \in \mathbb{Z}[X]$, and $\bar{f}(X) := f(X) \bmod p \in \mathbb{F}_p[X]$ is decomposed as

$$\bar{f}(X) = X^m \bar{f}_1(X) \quad (m \geq 1), \qquad f_1(X) := \prod_{g \in D_{\mathfrak{p}_i}} \big(X - g(\alpha)\big).$$

Since $0 = \bar{f}(\bar{\alpha}) = \bar{f}(\bar{\theta}) = \bar{\theta}^m \bar{f}_1(\bar{\theta})$ $(\bar{\alpha} := \alpha \bmod \mathfrak{p}_i)$ and $\bar{\theta} \neq 0$, we have $\bar{f}_1(\bar{\theta}) = 0$. Let $h(X) \in \mathbb{F}_p[X]$ be the minimal polynomial of $\bar{\theta}$ over $\mathbb{F}_p$. Then we have $h(X) | \bar{f}_1(X)$. Since $\sigma(\bar{\theta})$ is a root of $h(X) = 0$, so is $\bar{f}_1(X) = 0$. Hence, there is $g \in D_{\mathfrak{p}_i}$ such that $\sigma(\bar{\theta}) = \bar{g}(\bar{\alpha}) = \bar{g}(\bar{\theta})$. □

Let $G = \bigsqcup_{i=1}^r g_i D_{\mathfrak{p}_i}$ be the coset decomposition such that $\mathfrak{p}_i = g_i(\mathfrak{p}_1)$ $(g_1 := 1)$. If we denote by e_i the ramification index of $\mathfrak{p}_i$, we have $p\mathcal{O}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = g_1(\mathfrak{p}_1)^{e_1} \cdots g_r(\mathfrak{p}_1)^{e_r}$. Letting $g \in G$ act on the both sides, we see $e_1 = \cdots = e_r = e$ by the uniqueness of the prime decomposition: $p\mathcal{O}_k = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$. Further, since $\mathbb{F}_{\mathfrak{p}_i} = \mathcal{O}_k/\mathfrak{p}_1^g \simeq \mathcal{O}_k/\mathfrak{p}_1 = \mathbb{F}_{\mathfrak{p}_1}$, $[\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p] = f_p = f$ is also independent of $\mathfrak{p}_i$: $N\mathfrak{p}_i = p^f$. Taking the norm of the both sides of $p\mathcal{O}_k = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$, we have

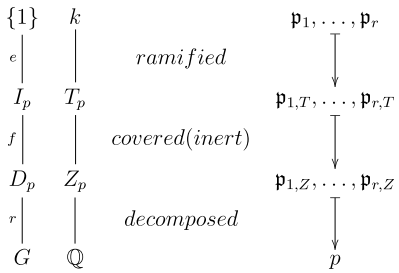
$p^n = p^{efr}$. Hence, we have $n = efr$ and $\#D_{\mathfrak{p}_i} = n/r = ef$. By Lemma 5.3, we have $\#I_{\mathfrak{p}_i} = e$. Therefore, we have the following:

$$\begin{array}{lllll} D_{\mathfrak{p}_i} = 1 & \Longleftrightarrow & Z_{\mathfrak{p}_i} = k & \Longleftrightarrow & e = f = 1,\ r = n, \\ D_{\mathfrak{p}_i} = G & \Longleftrightarrow & Z_{\mathfrak{p}_i} = \mathbb{Q} & \Longleftrightarrow & ef = n,\ r = 1, \\ I_{\mathfrak{p}_i} = 1 & \Longleftrightarrow & T_{\mathfrak{p}_i} = k & \Longleftrightarrow & e = 1,\ fr = n, \\ I_{\mathfrak{p}_i} = G & \Longleftrightarrow & T_{\mathfrak{p}_i} = \mathbb{Q} & \Longleftrightarrow & e = n,\ f = r = 1. \end{array}$$

In general, one has the following theorem. Let $\mathfrak{p}_{i,T} := \mathfrak{p}_i \cap \mathcal{O}_{T_{\mathfrak{p}_i}}$ and $\mathfrak{p}_{i,Z} := \mathfrak{p}_i \cap \mathcal{O}_{Z_{\mathfrak{p}_i}}$.

Theorem 5.4 *The extension $k/T_{\mathfrak{p}_i}$ is a ramified extension of degree e such that the ramification index of $\mathfrak{p}_i$ over $\mathfrak{p}_{i,T}$ is e. The extension $T_{\mathfrak{p}_i}/Z_{\mathfrak{p}_i}$ is a cyclic extension of degree f such that the covering (inert) degree of $\mathfrak{p}_{i,T}$ over $\mathfrak{p}_{i,Z}$ is f. The extension $Z_{\mathfrak{p}_i}/\mathbb{Q}$ is an extension of degree r such that p is completely decomposed into r prime ideals containing $\mathfrak{p}_{i,Z}$ as one prime factor.*

Now assume that G is an Abelian group. Then $D_{\mathfrak{p}_i}$, $I_{\mathfrak{p}_i}$ and $Z_{\mathfrak{p}_i}$, $T_{\mathfrak{p}_i}$ are independent of $\mathfrak{p}_i$ and so we write respectively D_p, I_p and Z_p, T_p for them. In the extension $k/\mathbb{Q}$, p is decomposed, covered and ramified as follows:



Assume further that $\mathfrak{p}$ is unramified. Since $I_{\mathfrak{p}} = 1$, we have the isomorphism $D_p \simeq \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p)$. Let σ_p be the generator of D_p which is defined by the inverse image under this isomorphism of the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p)$ (Example 2.25). By the equality $fr = n$, the decomposition law of p in the extension $k/\mathbb{Q}$ is determined by f, namely, the order of σ_p in G.

Remark 5.5 The above argument and results hold similarly for any finite Galois extension of number fields k/F and a prime ideal of F.

Finally, we extend the relation between the Legendre symbol and the decomposition law of a prime number in a quadratic extension in Sect. 4.2 to the case of any cyclic extension. Let $n \geq 2$ be an integer and let p and q be distinct prime numbers such that $p,\ q \equiv 1 \bmod n$. We fix a primitive root $\alpha \bmod q$ and let $\psi : G^{\mathrm{ab}}_{\{q\}} \simeq \mathbb{Z}_q^{\times} \to \mathbb{Z}/n\mathbb{Z}$ be the homomorphism defined by $\psi(\alpha) = 1$, $\psi(1 + q\mathbb{Z}_q) = 1$.

Let $k/\mathbb{Q}$ be the cyclic extension of degree n corresponding to $\mathrm{Ker}(\psi)$ and let $h_n : \mathrm{Spec}(\mathcal{O}_k) \to \mathrm{Spec}(\mathbb{Z})$ be the associated ramified covering. Let τ be the generator of $\mathrm{Gal}(k/\mathbb{Q})$ corresponding to $1 \in \mathbb{Z}/n\mathbb{Z}$ (Example 2.46). According to (5.1), we define the *mod n linking number* $\mathrm{lk}_n(q, p) \in \mathbb{Z}/n\mathbb{Z}$ of p and q by

$$\sigma_p = \tau^{\mathrm{lk}_n(q,p)}.$$

(This depends on the choice of α.) Let $\mathfrak{q}$ be the unique prime ideal of $\mathcal{O}_k$ lying over q. Then we have $k_\mathfrak{q} = \mathbb{Q}_q(\sqrt[n]{q})$. Note that the image of τ under the canonical isomorphism $\mathrm{Gal}(k/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(k_\mathfrak{q}/\mathbb{Q}_q)$ is given by $\rho_{k_\mathfrak{q}/\mathbb{Q}_q}(\alpha)$, where $\rho_{k_\mathfrak{q}/\mathbb{Q}_q}$ is the reciprocity homomorphism of local class field theory (2.2). Define the primitive n-th root of unity $\zeta \in \mathbb{Q}_q$ by

$$\zeta = \frac{\rho_{k_\mathfrak{q}/\mathbb{Q}_q}(\alpha)(\sqrt[n]{q})}{\sqrt[n]{q}}. \tag{5.2}$$

Proposition 5.6 *We have* $\zeta^{\mathrm{lk}_n(q,p)} = (\frac{p}{q})_n$ *where* $(\frac{*}{q})_n$ *stands for the n-th power residue symbol in* $\mathbb{Q}_q$.

Proof Let l be an integer (mod $q-1$) so that $p^{-1} \equiv \alpha^l \bmod q$. Then we shall show that

$$\mathrm{lk}_n(q, p) = l \bmod n.$$

Let $\mathbf{a}$ be the idèle of $\mathbb{Q}$ whose p-component is p and other components are all 1, $\mathbf{b}$ the idèle of $\mathbb{Q}$ whose q-component is p and other components are all 1 and $\mathbf{c}$ the idèle of $\mathbb{Q}$ whose p, q-components are 1 and other components are all p (2.6). Then we have $p = \mathbf{abc}$ in the idèle group $J_\mathbb{Q}$ of $\mathbb{Q}$. Let $\rho_{k/\mathbb{Q}} : C_\mathbb{Q} = J_\mathbb{Q}/\mathbb{Q}^\times \to \mathrm{Gal}(k/\mathbb{Q})$ be the reciprocity homomorphism in class field theory (2.9). We then have $\rho_{k/\mathbb{Q}}(q) = \mathrm{id}$ and $\rho_{k/\mathbb{Q}}(\mathbf{a}) = \sigma_p$. Since $k/\mathbb{Q}$ is unramified outside $\{q, \infty\}$, we have, by (2.10), $\rho_{k/\mathbb{Q}}(\mathbf{c}) = \mathrm{id}$. Therefore $\sigma_p = \rho_{k/\mathbb{Q}}(\mathbf{b}^{-1})$. By the following commutative diagram (cf. (2.8))

$$\begin{array}{ccc} \mathbb{Q}_q^\times & \xrightarrow{\rho_{k_\mathfrak{q}/\mathbb{Q}_q}} & \mathrm{Gal}(k_\mathfrak{q}/\mathbb{Q}_q) \\ \downarrow & & \wr \downarrow \iota_q \\ C_\mathbb{Q} & \xrightarrow{\rho_{k/\mathbb{Q}}} & \mathrm{Gal}(k/\mathbb{Q}), \end{array}$$

we have

$$\begin{aligned} \tau^l &= \iota_q\left(\rho_{k_\mathfrak{q}/\mathbb{Q}_q}(\alpha^l)\right) \\ &= \rho_{k/\mathbb{Q}}\left(\mathbf{b}^{-1}\right) \quad \left(p^{-1} = \alpha^l \bmod q\right) \\ &= \sigma_p. \end{aligned}$$

Hence, $\mathrm{lk}_n(q, p) = l \bmod n$. We also have

$$\left(\frac{p}{q}\right)_n = \left(\frac{p, q}{q}\right)_n \quad \text{by (2.5)}$$

$$
\begin{aligned}
&= \left(\frac{q, p^{-1}}{q}\right)_n \\
&= \frac{\rho_{k_\mathfrak{q}/\mathbb{Q}_q}(p^{-1})(\sqrt[n]{q})}{\sqrt[n]{q}} \\
&= \frac{\tau^l(\sqrt[n]{q})}{\sqrt[n]{q}} \\
&= \zeta^l \quad \text{by (5.2)}.
\end{aligned}
$$

This yields the assertion. □

By the definition of $\mathrm{lk}_n(q, p)$, one has, for a positive divisor m of n,

$$\mathrm{g.c.d.}\big(\mathrm{lk}(q, p), n\big) = m \iff h_n^{-1}\big(\{p\}\big) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\},$$

where $\mathrm{lk}(q, p) \in \mathbb{Z}$, $\mathrm{lk}(q, p) \bmod n = \mathrm{lk}_n(q, p)$. In particular, p is decomposed completely in k if and only if $\mathrm{lk}_n(q, p) = 0 \bmod n$.

Remark 5.7 (1) When $n = 2$, we have $(p/q)_2 = (q^*/p)_2$ and hence Proposition 5.6 is regarded as an extension of Proposition 4.4.

(2) When $n > 2$, one does not have the reciprocity law for $(q/p)_n$ since $\mathbb{Q}$ has no primitive n-th root of unity. In order to obtain the reciprocity law, one should consider the n-th power residue symbol for two principal prime ideal of a number field containing a primitive n-th root of unity [Hib, Sect. 154], as an analogue of the linking number of two null-homologous knots in a 3-manifold.

Summary

Galois covering of degree n $M \xrightarrow{h} S^3$ $K_i \mapsto K$	Galois covering of degree n $\mathrm{Spec}(\mathcal{O}_k) \xrightarrow{h} \mathrm{Spec}(\mathbb{Z})$ $\mathfrak{p}_i \mapsto (p)$
I_{K_i}: inertia group of K_i T_{K_i}: inertia space of K_i $\#I_{K_i} = [M : I_{K_i}] = e$	$I_{\mathfrak{p}_i}$: inertia group of $\mathfrak{p}_i$ $T_{\mathfrak{p}_i}$ inertia field of $\mathfrak{p}_i$ $\#I_{\mathfrak{p}_i} = [k : T_{\mathfrak{p}_i}] = e$
D_{K_i}: decomposition group of K_i Z_{K_i}: decomposition space of K_i $\#D_{K_i} = [M : Z_{K_i}] = ef$	$D_{\mathfrak{p}_i}$: decomposition group of $\mathfrak{p}_i$ $Z_{\mathfrak{p}_i}$: decomposition field of $\mathfrak{p}_i$ $\#D_{\mathfrak{p}_i} = [k : Z_{\mathfrak{p}_i}] = ef$
$efr = n$ $(h^{-1}(K) = K_1 \cup \cdots \cup K_r)$	$efr = n$ $(h^{-1}(\{p\}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\})$

Chapter 6
Homology Groups and Ideal Class Groups I—Genus Theory

In this chapter, we review Gauss' genus theory from the link-theoretic point of view. We shall see that the notion of genera is defined by using the idea analogous to the linking number. We also present, vice versa, a topological analogue of genus theory.

6.1 Homology Groups and Ideal Class Groups

Firstly, let us see the analogy between the 1st homology group of a 3-manifold and the ideal class group of a number field [Kp2, Rz2]. Let M be a connected oriented 3-manifold. Recall that knots in M generate the group $Z_1(M)$ of 1-cycles of M. The boundaries ∂D of 2-chains $D \in C_2(M)$ generate the subgroup $B_1(M)$ of $Z_1(M)$, and the 1st homology group $H_1(M)$ is defined by the quotient group:

$$H_1(M) = Z_1(M)/B_1(M).$$

On the other hand, let k be a number field of finite degree over $\mathbb{Q}$. Recall that prime ideals ($\neq 0$) of the ring $\mathcal{O}_k$ of integers of k generate the ideal group $I(k)$ of k. The principal ideals (a) generated by numbers $a \in k^\times$ (resp. totally positive $a \in k^\times$) form the subgroup $P(k)$ (resp. $P^+(k)$) of $I(k)$, and the ideal class group (resp. the narrow ideal class group) is defined by the quotient group:

$$H(k) = I(k)/P(k) \quad (\text{resp. } H^+(k) = I(k)/P^+(k)).$$

Note that 2-chains D with $\partial D = 0$ form the 2nd homology group of M, while numbers $a \in k^\times$ with $(a) = \mathcal{O}_k$ form the unit group $\mathcal{O}_k^\times$.

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_6,

Summing up, we have the following analogies:

$C_2(M) \to Z_1(M)$ $D \mapsto \partial D$	$k^\times \to I(k)$ $a \mapsto (a)$
$B_1(M)$	$P(k)(P^+(k))$
1st Homology group $H_1(M) = Z_1(M)/B_1(M)$	(narrow) Ideal class group $H(k) = I(k)/P(k)$ $(H^+(k) = I(k)/P^+(k))$
2nd Homology group $H_2(M)$	Unit group $\mathcal{O}_k^\times$

Finally, we summarize the analogy between the Hurewicz theorem (for 3-manifolds) and the Artin reciprocity.

Hurewicz Theorem Let $f : M \to S^3$ be a finite Abelian covering ramified over a link L. Set $X := S^3 \setminus L$, $Y := f^{-1}(X)$, $G := \mathrm{Gal}(Y/X)$. For a knot $K \subset X$, let σ_K be the generator of the decomposition group D_K defined in Sect. 5.1. Defining $\sigma_c := \prod_K \sigma_K^{n_K}$ for a 1-cycle $c = \sum_K n_K K \in Z_1(X)$, we get the homomorphism $\sigma_{M/S^3} : Z_1(X) \to G$; $c \mapsto \sigma_c$. Then σ_{M/S^3} is surjective and $\mathrm{Ker}(\sigma_{M/S^3}) = f_*(Z_1(Y)) + B_1(X)$. Hence, one has the isomorphism $\sigma_{M/S^3} : H_1(X)/f_*(H_1(Y)) \simeq G$.

Artin Reciprocity Let $k/\mathbb{Q}$ be a finite Abelian extension ramified over a finite set S of primes, and let $f : \mathrm{Spec}(\mathcal{O}_k) \to \mathrm{Spec}(\mathbb{Z})$ be the associated covering of the rings of integers. Set $X := \mathrm{Spec}(\mathbb{Z}) \setminus S$, $X_0 := \mathrm{Max}(\mathbb{Z}) \setminus S$, $S_k := f^{-1}(S)$, $Y := \mathrm{Spec}(\mathcal{O}_k) \setminus S_k$, $Y_0 := \mathrm{Max}(\mathcal{O}_k) \setminus S_k$, $G = \mathrm{Gal}(k/\mathbb{Q})$. Further, we set

$$
\begin{aligned}
&I(X) := \bigoplus_{p \in X_0} \mathbb{Z}, \qquad P(X) := \left\{(a) \in P^+(\mathbb{Q}) \mid a \equiv 1 \bmod q \ (\forall q \in S)\right\},\\
&H(X) := I(X)/P(X),\\
&I(Y) := \bigoplus_{\mathfrak{p} \in Y_0} \mathbb{Z}, \qquad P(Y) := \left\{(\alpha) \in P^+(k) \mid \alpha \equiv 1 \bmod \mathfrak{q} \ (\forall \mathfrak{q} \in S_k)\right\},\\
&H(Y) := I(Y)/P(Y).
\end{aligned}
$$

For a prime number $p \in X_0$, we have $\sigma_p \in G$ defined as in Sect. 5.2. Defining $\sigma_{\mathfrak{a}} := \prod_{p \in X_0} \sigma_p^{n_p}$ for $\mathfrak{a} = \prod_{p \in X_0} p^{n_p} \in I(X)$, we get the homomorphism $\sigma_{k/\mathbb{Q}} : I(X) \to G$; $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$. Then $\sigma_{k/\mathbb{Q}}$ is surjective and $\mathrm{Ker}(\sigma_{k/\mathbb{Q}}) = \mathrm{N}_{k/\mathbb{Q}}(I(Y))P(X)$. Hence, we have the isomorphism $\sigma_{k/\mathbb{Q}} : H(X)/\mathrm{N}_{k/\mathbb{Q}}(H(Y)) \simeq G$.

6.2 Genus Theory for a Link

Let $L = K_1 \cup \cdots \cup K_r \subset S^3$ be an r-component link and let $X_L := S^3 \setminus \mathrm{int}(V_L)$ the link exterior and $G_L := \pi_1(X_L)$. For an integer $n \geq 2$, let $\psi : G_L \to \mathbb{Z}/n\mathbb{Z}$ be

the surjective homomorphism sending each meridian α_i of K_i to $1 \in \mathbb{Z}/n\mathbb{Z}$. Let $h : Y \to X_L$ be the cyclic covering of degree n corresponding to $\mathrm{Ker}(\psi)$. The Fox completion $f : M \to S^3$ (Example 2.15) is a cyclic covering of degree n over S^3 ramified along L. Let τ be the generator of $\mathrm{Gal}(M/S^3)$ corresponding to $1 \in \mathbb{Z}/n\mathbb{Z}$. In the following, a 1-cycle representing a homology class of $H_1(M)$ will be taken to be disjoint from $f^{-1}(L)$. Now we say that $[a], [b] \in H_1(M)$ belong to the same *genus*, written as $[a] \approx [b]$, if the following holds:

$$\mathrm{lk}\big(f_*(a), K_i\big) \equiv \mathrm{lk}\big(f_*(b), K_i\big) \bmod n \quad (1 \le i \le r).$$

This definition is shown to be independent of the choice of 1-cycles representing homology classes as follows. Suppose that $[a] = 0 \in H_1(M)$. It suffices to show $\mathrm{lk}(f_*(a), K_i) \equiv 0 \mod n$. The relative homology exact sequence $H_2(M, Y) \xrightarrow{\partial} H_1(Y) \to H_1(M)$ yields $[a] \in \mathrm{Im}(\partial)$. By the excision, $H_2(M, Y)$ is generated by 2-cycles whose boundaries are meridians $\tilde{\alpha}_i$ of components of $f^{-1}(L)$, and so $\mathrm{Im}(\partial)$ is generated by $[\tilde{\alpha}_i]$ $(1 \le i \le r)$. Since $f_*([\tilde{\alpha}_i]) = n[\alpha_i] \in H_1(X_L)$, $\mathrm{lk}(f_*(a), K_i) \equiv 0 \bmod n$.

Theorem 6.1 ([M4]) *Let $\chi : H_1(M) \to (\mathbb{Z}/n\mathbb{Z})^r$ be the homomorphism defined by $\chi([a]) := (\mathrm{lk}(f_*(a), K_i) \bmod n)$. Then one has the following*:

$$\mathrm{Im}(\chi) = \left\{ (\varepsilon_i) \in (\mathbb{Z}/n\mathbb{Z})^r \;\middle|\; \sum_{i=1}^{r} \varepsilon_i = 0 \right\}, \qquad \mathrm{Ker}(\chi) = (\tau - 1)H_1(M)$$

and hence

$$H_1(M)/\approx \simeq H_1(M)/(\tau - 1)H_1(M) \simeq (\mathbb{Z}/n\mathbb{Z})^{r-1}.$$

Proof Let j denote the inclusion $Y \hookrightarrow M$. Then $j_* : H_1(Y) \to H_1(M)$ is surjective and, as explained before the theorem, we have $B := \mathrm{Ker}(j_*) = \mathbb{Z}([\tilde{\alpha}_1]) \oplus \cdots \oplus \mathbb{Z}([\tilde{\alpha}_r])$, where $\tilde{\alpha}_i$ is a meridian of a component of $f^{-1}(L)$ lying over K_i. Hence, we have $f_*(B) = h_*(B) = \mathbb{Z}(n[\alpha_1]) \oplus \cdots \oplus \mathbb{Z}(n[\alpha_r]) \subset H_1(X_L) = \mathbb{Z}[\alpha_1] \oplus \cdots \oplus \mathbb{Z}[\alpha_r]$. From the short exact sequence of chain complexes

$$0 \to C_*(Y) \xrightarrow{\tau - 1} C_*(Y) \xrightarrow{h_*} C_*(X_L) \to 0,$$

we have the long exact sequence (Wang exact sequence)

$$\cdots \to H_1(Y) \xrightarrow{\tau - 1} H_1(Y) \xrightarrow{h_*} H_1(X_L) \to \cdots.$$

Therefore, we have the following commutative exact diagram:

$$\begin{array}{ccccccc}
 & & & & 0 & & 0 \\
 & & & & \downarrow & & \downarrow \\
 & & & & B & \xrightarrow{f_*} & f_*(B) \quad \to 0 \\
 & & & & \downarrow & & \downarrow \\
0 \to & (\tau-1)H_1(Y) & \to & H_1(Y) & \xrightarrow{f_*} & f_*(H_1(Y)) & \to 0 \\
 & \downarrow j_* & & \downarrow j_* & & & \\
0 \to & (\tau-1)H_1(M) & \to & H_1(M) & & & \\
 & \downarrow & & \downarrow & & & \\
 & 0 & & 0 & & &
\end{array}$$

This yields the exact sequence

$$0 \to (\tau-1)H_1(M) \to H_1(M) \to f_*(H_1(Y))/f_*(B) \to 0. \tag{6.1}$$

Define $\varphi : H_1(X_L) \to (\mathbb{Z}/n\mathbb{Z})^r$ by $\varphi(c) := (\mathrm{lk}(c, K_i) \bmod n)$. It is easy to see that φ is surjective and $\mathrm{Ker}(\varphi) = \mathbb{Z}(n[\alpha_1]) \oplus \cdots \oplus \mathbb{Z}(n[\alpha_r]) = f_*(B)$. So we have the following commutative exact diagram for a covering $Y \to X_L$:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & f_*(B) & = & f_*(B) & & \\
 & & \downarrow & & \downarrow & & \\
0 \to & f_*(H_1(Y)) & \to & H_1(X_L) & \to & \mathrm{Gal}(Y/X_L) & \to 0 \\
 & \downarrow & & \downarrow \varphi & & \wr\downarrow & \\
 & f_*(H_1(Y))/f_*(B) & & (\mathbb{Z}/n\mathbb{Z})^r & \xrightarrow{\Sigma} & \mathbb{Z}/n\mathbb{Z} & \\
 & \downarrow & & \downarrow & & & \\
 & 0 & & 0 & & &
\end{array}$$

Here $\Sigma : (\mathbb{Z}/n\mathbb{Z})^r \to \mathbb{Z}/n\mathbb{Z}$ is the homomorphism defined by $\Sigma((\varepsilon_i)) := \sum_{i=1}^r \varepsilon_i$, and $\mathrm{Gal}(Y/X) \simeq \mathbb{Z}/n\mathbb{Z}$ is the isomorphism sending τ to 1 mod n. Hence, we have

$$f_*\big(H_1(Y)\big)/f_*(B) \overset{\varphi}{\simeq} \mathrm{Ker}(\Sigma) \simeq (\mathbb{Z}/n\mathbb{Z})^{r-1}. \tag{6.2}$$

By (6.1), (6.2) and $\chi = \varphi \circ f_*$, we have the exact sequence

$$0 \to (\tau-1)H_1(M) \to H_1(M) \xrightarrow{\chi} (\mathbb{Z}/n\mathbb{Z})^{r-1} \to 0$$

which yields our assertion. □

For the case of $n = 2$, we have the following topological analogue of Gauss' theorem:

Corollary 6.2 *Let $f : M \to S^3$ be a double covering of connected oriented closed 3-manifolds ramified over an r-component link $L = K_1 \cup \cdots \cup K_r$. Then the homomorphism $\chi : H_1(M) \to (\mathbb{Z}/2\mathbb{Z})^r$ defined by $\chi([a]) := (\mathrm{lk}(f_*(a), K_i) \bmod 2)$*

induces the following isomorphism:

$$H_1(M)/2H_1(M) \simeq \left\{ (\varepsilon_i) \in (\mathbb{Z}/2\mathbb{Z})^r \;\middle|\; \sum_{i=1}^{r} \varepsilon_i = 0 \right\} \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

Proof By Theorem 6.1, it suffices to show $(\tau - 1)H_1(M) = 2H_1(M)$. Let $\mathrm{tr} : H_1(S^3) \to H_1(M)$ denote the transfer map. Since $\mathrm{tr} \circ f_* : H_1(M) \to H_1(M)$ is $1 + \tau$, one has $\tau = -1$ as $H_1(S^3) = 0$. Hence $(\tau - 1)H_1(M) = 2H_1(M)$. □

Example 6.3 Let $L = B(a, b)$ be a 2-bridge link where a is an even integer (≥ 2) and $0 < b < a$, $(a, b) = 1$. The double covering M of S^3 ramified over L is the lens space $L(a, b)$ (Example 2.16). Then one has $H_1(M) \simeq \mathbb{Z}/a\mathbb{Z}$, and $H_1(M)/\approx = H_1(M)/2H_1(M) \simeq \mathbb{Z}/2\mathbb{Z}$.

6.3 Genus Theory for Prime Numbers

Let $n \geq 2$ be an integer and let $S = \{p_1, \ldots, p_r\}$ be the set of r distinct prime numbers such that $p_i \equiv 1 \bmod n$ $(1 \leq i \leq r)$. Let $G_S := \pi_1(\mathrm{Spec}(\mathbb{Z}[1/(p_1 \cdots p_r)])) = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, where $\mathbb{Q}_S$ is the maximal Galois extension of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$ (Example 2.36). For each p_i, we fix a primitive root $\alpha_i \bmod p_i$. Let $\psi : G_S^{\mathrm{ab}} = \prod_{i=1}^r \mathbb{Z}_{p_i}^\times = \prod_{i=1}^r \mathbb{F}_{p_i}^\times \times (1 + p_i\mathbb{Z}_{p_i}) \to \mathbb{Z}/n\mathbb{Z}$ be the homomorphism defined by $\psi(\alpha_i) = 1$, $\psi(1 + p_i\mathbb{Z}_{p_i}) = 0$ $(1 \leq i \leq r)$. Let k be the cyclic extension of $\mathbb{Q}$ of degree n corresponding to $\mathrm{Ker}(\psi)$. Let τ be the generator of $\mathrm{Gal}(k/\mathbb{Q})$ corresponding to $1 \in \mathbb{Z}/n\mathbb{Z}$ (Example 2.46). Let $\mu_n \subset \overline{\mathbb{Q}}$ denote the group of n-th roots of unity and we fix an embedding $\mathbb{Q}(\mu_n) \subset \mathbb{Q}_{p_i}$ $(1 \leq i \leq r)$. In the following, an ideal representing an ideal class of the narrow ideal class group $H^+(k)$ will be taken to an ideal of $\mathcal{O}_k$ disjoint from S. Now we say that $[\mathfrak{a}], [\mathfrak{b}] \in H^+(k)$ belong to the same *genus*—written as $[\mathfrak{a}] \approx [\mathfrak{b}]$—, if the following holds:

$$\left(\frac{\mathrm{N}\mathfrak{a}}{p_i}\right)_n = \left(\frac{\mathrm{N}\mathfrak{b}}{p_i}\right)_n \quad (1 \leq i \leq r),$$

where $(\frac{*}{p_i})_n$ denotes the n-th power residue symbol in $\mathbb{Q}_{p_i}$ taking the value in μ_n. This definition is shown to be independent of the choice of ideals representing ideal classes as follows. Suppose $[\mathfrak{a}] = 0 \in H^+(k)$. It suffices to show $(\frac{\mathrm{N}\mathfrak{a}}{p_i})_n = 1$. There is a totally positive $\alpha \in k^\times$ such that $\mathfrak{a} = (\alpha)$. So $\mathrm{N}\mathfrak{a} = \mathrm{N}_{k/\mathbb{Q}}(\alpha) = \mathrm{N}_{k_{\mathfrak{p}_i}/\mathbb{Q}_{p_i}}(\alpha)$. (Here $\mathfrak{p}_i$ is a prime ideal of k lying over p_i and $k_{\mathfrak{p}_i} = \mathbb{Q}_{p_i}(\sqrt[n]{p_i})$.) By (2.4), (2.5), we have $(\frac{\mathrm{N}\mathfrak{a}}{p_i})_n = 1$.

Theorem 6.4 ([IT]) *Let* $\chi : H^+(k) \to \mu_n^r$ *be the homomorphism defined by* $\chi([\mathfrak{a}]) := ((\frac{\mathrm{N}\mathfrak{a}}{p_i})_n)$. *Then one has the following*

$$\mathrm{Im}(\chi) = \left\{ (\zeta_i) \in \mu_n^r \;\middle|\; \prod_{i=1}^{r} \zeta_i = 1 \right\}, \qquad \mathrm{Ker}(\chi) = H^+(k)^{\tau - 1}$$

and hence

$$H^+(k)/\approx \simeq H^+(k)/H^+(k)^{\tau-1} \simeq (\mathbb{Z}/n\mathbb{Z})^{r-1}.$$

Proof Let $J_{\mathbb{Q}}$ and J_k be the idèle group of $\mathbb{Q}$ and k respectively. We set $U_k := \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_k)} \mathcal{O}_{\mathfrak{p}}^{\times} \times \prod_{v\in S_k^{\infty}} (k_v^{\times})^2$ and we then have the isomorphism $J_k/U_k k^{\times} \simeq H^+(k)$ (Example 2.44). Next, we shall show that the kernel of the norm map $\mathrm{N}_{k/\mathbb{Q}} : J_k/k^{\times} \to \mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^{\times}/\mathbb{Q}^{\times}$ induced on the idèle class groups is given by $(J_k/k^{\times})^{\tau-1}$. First, it is obvious that $(J_k/k^{\times})^{\tau-1} \subset \mathrm{Ker}(\mathrm{N}_{k/\mathbb{Q}})$. For $\mathbf{a} \in J_k$, assume $\mathrm{N}_{k/\mathbb{Q}}(\mathbf{a}) \in \mathbb{Q}^{\times}$. By the Hasse norm theorem one has

$$\mathrm{N}_{k/\mathbb{Q}}(J_k) \cap \mathbb{Q}^{\times} = \mathrm{N}_{k/\mathbb{Q}}(k^{\times})$$

and hence there is $\alpha \in k^{\times}$ such that $\mathrm{N}_{k/\mathbb{Q}}(\mathbf{a}) = \mathrm{N}_{k/\mathbb{Q}}(\alpha)$. The Hilbert theorem 90 which asserts that for $\mathbf{b} \in J_k$,

$$\mathrm{N}_{k/\mathbb{Q}}(\mathbf{b}) = 1 \quad \Rightarrow \quad \exists \mathbf{c} \in J_k, \quad \mathbf{b} = \mathbf{c}^{\tau-1}$$

and so there is $\mathbf{c} \in J_k$ such that $\mathbf{a} = \alpha \mathbf{c}^{\tau-1}$. Therefore, we have $\mathbf{a}k^{\times} = \mathbf{c}^{\tau-1}k^{\times} \in (J_k/k^{\times})^{\tau-1}$. Hence, we have the following commutative exact diagram:

$$\begin{array}{ccccccc}
 & & & & 0 & & 0 \\
 & & & & \downarrow & & \downarrow \\
 & & & & U_k k^{\times}/k^{\times} & \xrightarrow{\mathrm{N}_{k/\mathbb{Q}}} & \mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^{\times}/\mathbb{Q}^{\times} \to 0 \\
 & & & & \downarrow & & \downarrow \\
0 \to & (J_k/k^{\times})^{\tau-1} & \to & J_k/k^{\times} & \xrightarrow{\mathrm{N}_{k/\mathbb{Q}}} & \mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^{\times}/\mathbb{Q}^{\times} \to 0 & \\
 & \downarrow & & \downarrow & & & \\
0 \to & H^+(k)^{\tau-1} & \to & H^+(k) & & & \\
 & \downarrow & & \downarrow & & & \\
 & 0 & & 0 & & &
\end{array}$$

This yields the exact sequence

$$0 \to H^+(k)^{\tau-1} \to H^+(k) \to \mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^{\times}/\mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^{\times} \to 0. \tag{6.3}$$

Since $H_{\mathbb{Q}}^+ = 1$, we have $J_{\mathbb{Q}} = \mathbb{Q}^{\times}((\mathbb{R}^{\times})^2 \times \prod_p \mathbb{Z}_p^{\times})$. Therefore, we can choose uniquely an idèle of the form $\mathbf{a} = ((a_p), a_{\infty})$ with $a_p \in \mathbb{Z}_p^{\times}$ $(\forall p \in \mathrm{Max}(\mathbb{Z}))$ and $a_{\infty} > 0$ as a representative of each idèle class in $J_{\mathbb{Q}}/\mathbb{Q}^{\times}$. We then define the homomorphism $\varphi : J_{\mathbb{Q}}/\mathbb{Q}^{\times} \to \mu_n^r$ by

$$\varphi(\mathbf{a}\mathbb{Q}^{\times}) := \left(\left(\frac{a_{p_i}}{p_i} \right)_n \right).$$

We first note that φ is surjective, since the map $\mathbb{Z}_{p_i}^{\times} \ni u \mapsto (\frac{u}{p_i})_n \in \mu_n$ is surjective $(1 \le i \le r)$ as $(\frac{\alpha_i}{p_i})_n$ is a primitive n-th root of unity. Next we will show that

$\mathrm{Ker}(\varphi) = \mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^\times/\mathbb{Q}^\times$. By (2.4), we have $(\frac{a_{p_i}}{p_i})_n = 1 \Leftrightarrow a_{p_i} \in \mathrm{N}_{k_{\mathfrak{p}_i}/\mathbb{Q}_{p_i}}(\mathcal{O}_{\mathfrak{p}_i}^\times)$ for any prime ideal $\mathfrak{p}_i$ of k over p_i. If $p \notin S$, we have $\mathrm{N}_{k_\mathfrak{p}/\mathbb{Q}_p}(\mathcal{O}_\mathfrak{p}^\times) = \mathbb{Z}_p^\times$ for any prime ideal $\mathfrak{p}$ of k, since p is unramified in $k/\mathbb{Q}$ (cf. (2.3)), and we have $\mathrm{N}_{k_v/\mathbb{R}}((k_v^\times)^2) = (\mathbb{R}^\times)^2$ for $v \in S_k^\infty$. Therefore, we have $\mathrm{Ker}(\varphi) = \mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^\times/\mathbb{Q}^\times$. Finally, noting the isomorphism $\rho_{k/\mathbb{Q}} : J_\mathbb{Q}/\mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^\times \simeq G$ in class field theory (2.9), we have the following commutative exact diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & \mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^\times/\mathbb{Q}^\times & = & \mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^\times/\mathbb{Q}^\times & & \\
 & & \downarrow & & \downarrow & & \\
0 \to & \mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^\times/\mathbb{Q}^\times & \to & J_\mathbb{Q}/\mathbb{Q}^\times & \xrightarrow{\rho_{k/\mathbb{Q}}} & \mathrm{Gal}(k/\mathbb{Q}) \to 0 \\
 & \downarrow & & \downarrow \varphi & & \wr \downarrow & \\
 & \mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^\times/N(U_k)\mathbb{Q}^\times & & \mu_n^r & \xrightarrow{\Sigma} & \mathbb{Z}/n\mathbb{Z} \\
 & \downarrow & & \downarrow & & & \\
 & 0 & & 0 & & &
\end{array}$$

Here $\Sigma : \mu_n^r \to \mathbb{Z}/n\mathbb{Z}$ is defined as follows: Let $\xi_i : \mu_n \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ be the isomorphism defined by sending $(\frac{\alpha_i}{p_i})_n$ to 1 mod n. Then we set $\Sigma((\zeta_i)) := \sum_{i=1}^r \xi_i(\zeta_i)$. The isomorphism $\mathrm{Gal}(k/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ is defined by sending τ to 1 mod n. From the diagram above, we have

$$\mathrm{N}_{k/\mathbb{Q}}(J_k)\mathbb{Q}^\times/\mathrm{N}_{k/\mathbb{Q}}(U_k)\mathbb{Q}^\times \overset{\varphi}{\simeq} \mathrm{Ker}(\Sigma) \simeq \mu_n^{r-1}. \tag{6.4}$$

Noting (6.3), (6.4) and $\chi = \varphi \circ \mathrm{N}_{k/\mathbb{Q}}$, we have the exact sequence

$$0 \to H^+(k)^{\tau-1} \to H^+(k) \xrightarrow{\chi} (\mathbb{Z}/2\mathbb{Z})^{r-1} \to 0$$

which yields our assertion. □

For the case that $n = 2$, we have the following Gauss' theorem,

Corollary 6.5 *Let $k/\mathbb{Q}$ be a quadratic extension ramified over r odd primes $p_1, \ldots, p_r$ (the infinite prime of $\mathbb{Q}$ is possibly ramified). Then the homomorphism $\chi : H^+(k) \to \{\pm 1\}^r$ defined by $\chi([\mathfrak{a}]) := ((\frac{\mathrm{N}\mathfrak{a}}{p_i}))$ induces the following isomorphism*:

$$H^+(k)/H^+(k)^2 \simeq \left\{ (\zeta_i) \in \{\pm 1\}^r \;\middle|\; \prod_{i=1}^r \zeta_i = 1 \right\} \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}.$$

Proof By Theorem 6.4, it suffices to show that $H^+(k)^{\tau-1} = H^+(k)^2$. Since $H^+(\mathbb{Q}) = 1$, we have $\mathrm{N}_{k/\mathbb{Q}}([\mathfrak{a}]) = [\mathfrak{a}][\mathfrak{a}]^\tau = 1$ for $[\mathfrak{a}] \in H^+(k)$ and so $\tau = -1$. Hence, one has $H^+(k)^{\tau-1} = H^+(k)^2$. □

Example 6.6 Let $k = \mathbb{Q}(\sqrt{145})$, which is a quadratic extension of $\mathbb{Q}$ ramified over $\{5, 29\}$. Let $\mathfrak{p} := (2, (1+\sqrt{145})/2)$. Then one has $H^+(k)(= H(k)) = \langle[\mathfrak{p}]\rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $H^+(k)/\approx = H^+(k)/H^+(k)^2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Remark 6.7 (1) In [Si], A. Sikora studied the analogies between a group action on a 3-manifold M and a number field k and showed some analogous formulas relating the number of ramified knots in a cyclic covering $M \to M/G$ (resp. ramified primes in a cyclic covering k/k^G) to the cyclic group G-action on $H_1(M)$ (resp. $H(k)$). In [Mn1], B. Morin gave a unified proof of Sikora's results in the arithmetic and topological cases introducing the equivariant étale cohomology.

(2) Besides the Hilbert theory and genus theory, some analogies for 3-manifolds of the capitulation problem and class tower problem etc have also been investigated (See [Fl, M6, Rz1, RM, U]).

Summary

1st Homology group $H_1(M)$	(narrow) Ideal class group $H^+(k)$
Classification of homology classes by the linking numbers	Classification of ideal classes by the Legendre symbols
$H_1(M)/2H_1(M) \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}$ ($M \to S^3$: double covering)	$H^+(k)/H^+(k)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}$ ($k/\mathbb{Q}$: quadratic extension)

In Chaps. 4–6, we reexamined Gauss' theory on linking numbers, quadratic residues and genus theory from the viewpoint of the analogy between knots and primes in Chap. 3. In the rest of this book, we shall try to bridge knot theory and algebraic number theory, that branched out after the works of Gauss and have grown up in their separate ways, from the viewpoint of this analogy.

Chapter 7
Link Groups and Galois Groups with Restricted Ramification

As explained in Chap. 3, our basic idea is to regard a Galois group with restricted ramification $G_S = \pi_1(\mathrm{Spec}(\mathbb{Z}) \setminus S)$, $S = \{p_1, \ldots, p_r\}$, as an analogue of a link group $G_L = \pi_1(S^3 \setminus L)$, $L = K_1 \cup \cdots \cup K_r$ (cf. (3.10)). Since the profinite group G_S is too big in general, we consider a maximal pro-l quotient $G_S(l)$ for some prime number l to derive the information how S is "linked". As for pro-l extensions of number fields, there are classical and extensive works due to I. Šafarevič and H. Koch etc., and a theorem by Koch on the structure of $G_S(l)$ turns out to be an analogue of J. Milnor's theorem on the structure of the link group G_L.

7.1 Link Groups

Let $L = K_1 \cup \cdots \cup K_r$ be an r-component link in S^3 and let $G_L = \pi_1(S^3 \setminus L)$ be the link group of L. Let F be the free group on the words $x_1, \ldots, x_r$ where x_i corresponds to a meridian of K_i.

Theorem 7.1 ([Ml1]) *For each $d \in \mathbb{N}$, there is $y_i^{(d)} \in F$ such that*

$$G_L/G_L^{(d)} = \langle x_1, \ldots, x_r \mid [x_1, y_1^{(d)}] = \cdots = [x_r, y_r^{(d)}] = 1,\ F^{(d)} = 1 \rangle,$$
$$y_i^{(d)} \equiv y_i^{(d+1)} \bmod F^{(d)},$$

where $y_i^{(d)}$ is a word representing a longitude β_i of K_i in $G_L/G_L^{(d)}$. We also have

$$\beta_j \equiv \prod_{i \neq j} \alpha_i^{\mathrm{lk}(K_i, K_j)} \bmod G_L^{(2)}.$$

Proof As in Example 2.6, we choose a regular projection of L into a hyperplane and divide K_i into arcs $\alpha_{i1}, \ldots, \alpha_{i\lambda_i}$. Fix a base point b above the hyperplane and let x_{ij}

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_7, © Springer-Verlag London Limited 2012

be a loop coming down from b, passing below α_{ij} from right to left, and returning b. Then we have the following presentation for G_L:

$$G_L = \left\langle x_{ij}(1 \le i \le r, 1 \le j \le \lambda_i) \;\middle|\; \begin{array}{c} R_{ij} := x_{ij}u_{ij}x_{ij+1}^{-1}u_{ij}^{-1} = 1 \\ (1 \le i \le r, 1 \le j < \lambda_i) \\ R_{i\lambda_i} := x_{i\lambda_i}u_{i\lambda_i}x_{i1}^{-1}u_{i\lambda_i}^{-1} = 1 \ (1 \le i \le r) \end{array} \right\rangle, \tag{7.1}$$

where u_{ij} is a word of x_{kl}'s (Fig. 7.1).

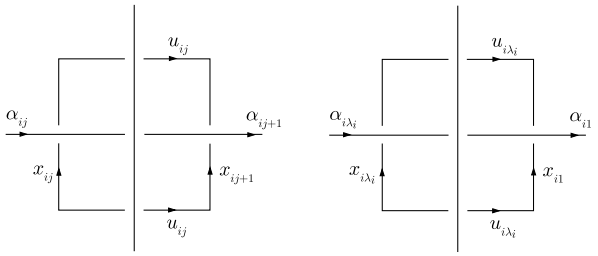


Fig. 7.1

Let $v_{ij} := u_{i1} \cdots u_{ij}$. Then $v_{i\lambda_i}$ represents a parallel of K_i [Ml1] and a longitude of K_i is represented by $v_{i\lambda_i}x_{i1}^{k_i} = u_{i1} \cdots u_{i\lambda_i}x_{i1}^{k_i}$ where the integer k_i is defined so that the sum of powers of x_{ij} in the word $v_{i\lambda_i}x_{i1}^{k_i}$ is 0. Set

$$\begin{cases} s_{ij} := x_{i1}v_{ij}x_{ij+1}^{-1}v_{ij}^{-1} & (1 \le j < \lambda_i,\ 1 \le i \le r) \\ s_{i\lambda_i} := x_{i1}v_{i\lambda_i}x_{i1}^{-1}v_{i\lambda_i}^{-1} & (1 \le i \le r). \end{cases}$$

Then one has

$$\begin{cases} R_{i1} = s_{i1} & (1 \le i \le r), \\ R_{ij} = v_{ij-1}^{-1}s_{ij-1}^{-1}s_{ij}v_{ij-1} & (1 < j \le \lambda_i,\ 1 \le i \le r). \end{cases} \tag{7.2}$$

By (7.1) and (7.2), we have

$$G_L = \langle x_{ij}\ (1 \le i \le r, 1 \le j \le \lambda_i) \mid s_{ij} = 1\ (1 \le i \le r, 1 \le j \le \lambda_i) \rangle. \tag{7.3}$$

Let $\overline{F}$ be the free group on the words x_{ij} $(1 \le i \le r, 1 \le j \le \lambda_i)$ and F the free group on the words x_{i1} $(1 \le i \le r)$. We regard F as a subgroup of $\overline{F}$ in the obvious way. For each $d \in \mathbb{N}$, we define the homomorphism $\eta_d : \overline{F} \to F$ inductively by

$$\begin{cases} \eta_1(x_{ij}) := x_{i1}, \\ \eta_{d+1}(x_{i1}) := x_{i1}, \\ \eta_{d+1}(x_{ij+1}) := \eta_d\left(v_{ij}^{-1}x_{i1}v_{ij}\right) & (1 \le j < \lambda_i). \end{cases}$$

Let $N := \langle\langle R_{ij}\ (1 \le i \le r, 1 \le j \le \lambda_i)\ (1 \le i \le r, 1 \le j \le \lambda_i)\rangle\rangle = \langle\langle s_{ij}\ (1 \le i \le r, 1 \le j \le \lambda_i)\rangle\rangle$. Then one has

(1_d) $\eta_d(x_{ij}) \equiv x_{ij} \bmod \overline{F}^{(d)} N$ $(1 \le i \le r, 1 \le j \le \lambda_i)$,
(2_d) $\eta_d(x_{ij}) \equiv \eta_{d+1}(x_{ij}) \bmod F^{(d)}$ $(1 \le i \le r, 1 \le j \le \lambda_i)$. □

Proof of (1_d) Since $\overline{F}^{(1)} = \overline{F}$, (1_d) is obviously true for $d = 1$. Assume that (1_d) holds for $d \ge 1$. We then have $\eta_d(v_{ij}) \equiv v_{ij} \bmod \overline{F}^{(d)} N$. Since $\eta_d(x_{i1}) = x_{i1}$, one has $\eta_d(v_{ij}^{-1} x_{i1} v_{ij}) \equiv v_{ij}^{-1} x_{i1} v_{ij} \bmod \overline{F}^{(d+1)} N$. Here, we used the following (7.4):

$$x \in F, \quad a \equiv b \bmod \overline{F}^{(d)} N \quad \Rightarrow \quad a^{-1} x a \equiv b^{-1} x b \bmod \overline{F}^{(d+1)} N. \tag{7.4}$$

Therefore, one has $\eta_{d+1}(x_{ij+1}) = \eta_d(v_{ij}^{-1} x_{i1} v_{ij}) \equiv v_{ij}^{-1} x_{i1} v_{ij} \bmod \overline{F}^{(d+1)} N$. Since $s_{ij} = x_{i1} v_{ij} x_{ij+1}^{-1} v_{ij}^{-1} \in N$, $v_{ij}^{-1} x_{i1} v_{ij} \equiv x_{ij+1} \bmod N$. Hence, $\eta_{d+1}(x_{ij+1}) \equiv x_{ij+1} \bmod \overline{F}^{(d+1)} N$, and $\eta_{d+1}(x_{i1}) = x_{i1}$ by definition. So (1_{d+1}) holds.

Proof of (2_d) Since $F^{(1)} = F$, (2_d) is obvious for the cases of $d = 1$. Assume that (2_d) holds for $d \ge 1$. $\eta_d(v_{ij}) \equiv \eta_{d+1}(v_{ij}) \bmod F^{(d)}$. Since $\eta_d(x_{i1}) = \eta_{d+1}(x_{i1}) = x_{i1}$, we have $\eta_{d+1}(x_{ij+1}) = \eta_d(v_{ij}^{-1} x_{i1} v_{ij}) \equiv \eta_{d+1}(v_{ij}^{-1} x_{i1} v_{ij}) = \eta_{d+2}(x_{ij+1}) \bmod F^{(d+1)}$. (Here, we used the assertion obtained by replacing $\overline{F}^{(d)} N$ by $F^{(d)}$ in (7.4), and $\eta_d(x_{i1}) = \eta_{d+1}(x_{i1}) = x_{i1}$). We also have $\eta_{d+1}(x_{i1}) = \eta_{d+2}(x_{i1}) = x_{i1}$ by definition. So (2_{d+1}) holds.

Therefore, we have, by (7.3),

$$\begin{aligned} G_L / G_L^{(d)} &= \langle x_{ij} \mid s_{ij} = 1,\ \overline{F}^{(d)} = 1 \rangle \\ &= \langle x_{ij} \mid s_{ij} = 1,\ x_{ij} = \eta_d(x_{ij}),\ \overline{F}^{(d)} = 1 \rangle \quad \text{(by } (1_d)\text{)} \\ &\simeq \langle x_{i1} \mid \eta_d(s_{ij}) = 1,\ F^{(d)} = 1 \rangle \left(\eta_d\left(\overline{F}^{(d)}\right) = F^{(d)} \right). \end{aligned}$$

Here we have, for $1 \le j < \lambda_i$,

$$\begin{aligned} \eta_d(s_{ij}) &= \eta_d(x_{i1}) \eta_d(v_{ij}) \eta_d(x_{ij+1})^{-1} \eta_d(v_{ij})^{-1} \\ &\equiv x_{i1} \eta_d(v_{ij}) \eta_{d+1}(x_{ij+1})^{-1} \eta_d(v_{ij})^{-1} \bmod F^{(d)} \quad \text{(by } (2_d)\text{)} \\ &= x_{i1} \eta_d(v_{ij}) \eta_d(v_{ij}^{-1} x_{i1} v_{ij})^{-1} \eta_d(v_{ij})^{-1} \\ &= 1, \end{aligned}$$

and hence

$$G_L / G_L^{(d)} = \langle x_{i1}\ (1 \le i \le r) | \eta_d(s_{i\lambda_i}) = 1,\ F^{(d)} = 1 \rangle.$$

Letting $x_i := x_{i1}$, $y_i^{(d)} := \eta_d(v_{i\lambda_i} x_{i1}^{k_i})$, we have $\eta_d(s_{i\lambda_i}) = \eta_d(x_{i1} v_{i\lambda_i} x_{i1}^{-1} v_{i\lambda_i}^{-1}) = \eta_d(x_{i1} v_{i\lambda_i} x_{i1}^{k_i} x_{i1}^{-1} x_{i1}^{-k_i} v_{i\lambda_i}^{-1}) = [x_i, y_i^{(d)}]$. Thus, we obtain

$$G_L / G_L^{(d)} = \langle x_1, \ldots, x_r \mid [x_1, y_1^{(d)}] = \cdots = [x_r, y_r^{(d)}] = 1,\ F^{(d)} = 1 \rangle,$$

and $y_i^{(d)} \equiv y_i^{(d+1)} \bmod F^{(d)}$ by (2_d). It follows from Proposition 4.1 that $\beta_j \equiv \prod_{i \neq j} \alpha_i^{\mathrm{lk}(K_i, K_j)} \bmod G_L^{(2)}$. □

Remark 7.2 (1) Two r-component links $L = K_1 \cup \cdots \cup K_r$ and $L' = K_1' \cup \cdots \cup K_r'$ are called *isotopic* if there is a continuous family $h_t : rS^1 \to S^3$ such that $h_t : rS^1 \overset{\approx}{\to} h_t(rS^1)$ is a homeomorphism for all $t \in [0, 1]$, $L = h_0(rS^1)$ and $L' = h_1(rS^1)$, where rS^1 means the disjoint union of r copies of S^1. If L, L' are equivalent, then L, L' are isotopic. It is shown [Ml1] that if L and L' are isotopic, then $G_L/G_L^{(d)}$ and $G_{L'}/G_{L'}^{(d)}$ are isomorphic so that for given pairs of a meridian and a longitude (α_i, β_i), (α_i', β_i') of K_i, K_i' respectively, (α_i, β_i) is sent to a simultaneous conjugate $(\gamma\alpha_i'\gamma^{-1}, \gamma\beta_i'\gamma^{-1})$ under this isomorphism.

(2) Theorem 7.1 can be extended for a link in any homology 3-sphere [Tu].

(3) When L is a *pure braid link* (a link obtained by closing a pure braid), it is known that $y_i^{(d)}$ is independent of d and G_L itself has the following presentation (E. Artin's theorem [Bi, Theorem 2.2]):

$$G_L = \langle x_1, \ldots, x_r \mid [x_1, y_1] = \cdots = [x_r, y_r] = 1 \rangle.$$

Let l be a prime number. For a group G, $G^{(d,l)}$ denotes the d-th term of the l-lower central series of G defined by $G^{(1,l)} := G$, $G^{(d+1,l)} := (G^{(d,l)})^l [G^{(d,l)}, G]$. Now we note that for any normal subgroup N of G_L whose index $[G_L : N]$ is a power of l, there is a (sufficiently large) d such that $G_L^{(d,l)} \subset N$. Hence, the pro-l completion $\hat{G}_L(l)$ of the link group G_L is given as the projective limit $\hat{G}_L(l) := \varprojlim_d G_L/G_L^{(d,l)}$. Similarly, we have $\hat{F}(l) = \varprojlim_d F/F^{(d,l)}$. Since $y_i^{(d)} \equiv y_i^{(d+1)} \bmod F^{(d,l)}$, $y_i := (y_i^{(d)} \bmod F^{(d,l)})$ defines an element of $\hat{F}(l)$ whose image under the natural map $\hat{F}(l) \to \hat{G}_L(l)$ represents a longitude of K_i. The following theorem asserts that any link looks like a pure braid link after the pro-l completion.

Theorem 7.3 ([HMM]) *The pro-l group $\hat{G}_L(l)$ has the following presentation*:

$$\hat{G}_L(l) = \langle x_1, \ldots, x_r \mid [x_1, y_1] = \cdots = [x_r, y_r] = 1 \rangle.$$

Proof Let $N_d := \langle\langle [x_i, y_i^{(d)}] (1 \leq i \leq r) \rangle\rangle$. Then we have, by Theorem 7.1,

$$G_L/G_L^{(d,l)} \simeq F/N_d F^{(d,l)}.$$

Taking the projective limit, we get our assertion. □

7.2 Pro-*l* Galois Groups with Restricted Ramification

Let l be a fixed prime number and let $S = \{p_1, \ldots, p_r\}$ be a set of r distinct prime numbers such that $p_i \equiv 1 \bmod l$ $(1 \leq i \leq r)$. We let $e_S := \max\{e \mid p_i \equiv$

$1 \bmod l^e (1 \le i \le r)\}$ and fix $m = l^e$ $(1 \le e \le e_S)$. Choose an algebraic closure of $\mathbb{Q}$ (a base point $\overline{x}$) and let $G_S(l)$ be the maximal pro-l quotient of $\pi_1(\mathrm{Spec}(\mathbb{Z}) \setminus S, \overline{x})$, namely, the Galois group $\mathrm{Gal}(\mathbb{Q}_S(l)/\mathbb{Q})$ of the maximal pro-l extension $\mathbb{Q}_S(l)(\subset \overline{\mathbb{Q}})$ of $\mathbb{Q}$, unramified outside $S \cup \{\infty\}$ (Example 2.36). We fix an algebraic closure $\overline{\mathbb{Q}}_{p_i}$ of each $\mathbb{Q}_{p_i}$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{p_i}$. Let $\mathbb{Q}_{p_i}(l)$ be the maximal pro-l extension of $\mathbb{Q}_{p_i}(\subset \overline{\mathbb{Q}}_{p_i})$ (Example 2.39). Then we have

$$\mathbb{Q}_{p_i}(l) = \mathbb{Q}_{p_i}\big(\zeta_{l^n},\ \sqrt[l^n]{p_i} \mid n \ge 1\big),$$

where $\zeta_{l^n} \in \overline{\mathbb{Q}}$ is a primitive l^n-th root of unity such that $\zeta_{l^t}^{l^s} = \zeta_{l^{t-s}}$ $(t \ge s)$. Note that $\zeta_m \in \mathbb{Q}_{p_i}$ $(1 \le i \le r)$ by our choice of m. Set $G_{\mathbb{Q}_{p_i}}(l) := \mathrm{Gal}(\mathbb{Q}_{p_i}(l)/\mathbb{Q}_{p_i})$. The local pro-$l$ group $G_{\mathbb{Q}_{p_i}}(l)$ is then generated by the monodromy τ_i and the extension of the Frobenius automorphism σ_i defined by

$$\begin{aligned} \tau_i(\zeta_{l^n}) &= \zeta_{l^n}, & \tau_i\big(\sqrt[l^n]{p_i}\big) &= \zeta_{l^n}\sqrt[l^n]{p_i}, \\ \sigma_i(\zeta_{l^n}) &= \zeta_{l^n}^{p_i}, & \sigma_i\big(\sqrt[l^n]{p_i}\big) &= \sqrt[l^n]{p_i} \end{aligned} \tag{7.5}$$

and τ_i, σ_i are subject to the relations $\tau_i^{p_i-1}[\tau_i, \sigma_i] = 1$ (Example 2.39). Note that a choice of an extension of the Frobenius automorphism is determined modulo the inertia group and (7.5) gives a normalization such a choice. The embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{p_i}$ induces the embedding $\mathbb{Q}_S(l) \hookrightarrow \mathbb{Q}_{p_i}(l)$ (hence a prime of $\mathbb{Q}_S(l)$ over p_i). From this we have the homomorphism $\eta_i : \mathrm{Gal}(\mathbb{Q}_{p_i}(l)/\mathbb{Q}_{p_i}) \to G_S(l)$. We denote by the same τ_i, σ_i the image of τ_i, σ_i under η_i. Let $\hat{F}(l)$ denote the free pro-l group on the words $x_1, \ldots, x_r$ where x_i represents τ_i.

Theorem 7.4 ([Kc2, 6]) *The pro-l group $G_S(l)$ has the following presentation*:

$$G_S(l) = \big\langle x_1, \ldots, x_r \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 \big\rangle,$$

where $y_i \in \hat{F}(l)$ is the pro-l word representing σ_i. Define $\mathrm{lk}(p_i, p_j) \in \mathbb{Z}_l$ and $\mathrm{lk}_m(p_i, p_j) \in \mathbb{Z}/m\mathbb{Z}$ by

$$\sigma_j \equiv \prod_{i \ne j} \tau_i^{\mathrm{lk}(p_i, p_j)} \bmod G_S(l)^{(2)}, \qquad \mathrm{lk}_m(p_i, p_j) := \mathrm{lk}(p_i, p_j) \bmod m.$$

Then one has

$$\zeta_m^{\mathrm{lk}_m(p_i, p_j)} = \left(\frac{p_j}{p_i}\right)_m.$$

Here $(\frac{*}{p_i})_m$ stands for the m-th power residue symbol in $\mathbb{Q}_{p_i}$ (2.5).

Proof Since an analogue of the Wirtinger presentation for the Galois group $G_S(l)$ is not known, we shall use the Tate–Poitou theorem 2.43 instead in order to obtain an arithmetic analogue of Theorem 7.1 or 7.3. Let τ_i' denote the image of τ_i under

the Abelianization $G_S(l) \to G_S(l)/G_S(l)^{(2)}$. Then one has, by Example 2.46,

$$G_S(l)/G_S(l)^{(2)} = \langle \tau_1' \rangle \times \cdots \times \langle \tau_r' \rangle \simeq \mathbb{Z}/l^{f_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/l^{f_r}\mathbb{Z},$$

where f_i is defined by $p_i - 1 = l^{f_i} q_i$, $(l, q_i) = 1$. Therefore, by Proposition 2.21, the pro-l group $G_S(l)$ is generated topologically by τ_i $(1 \le i \le r)$. In the following, we denote simply by $H^i(\mathfrak{G})$ the cohomology group $H^i(\mathfrak{G}, \mathbb{F}_l)$ for a pro-finite group $\mathfrak{G}$. Recall that the minimal number of relations among the generators $\tau_1, \ldots, \tau_r$ is given by $\dim_{\mathbb{F}_l} H^2(G_S(l))$ (Proposition 2.21). These relations all come from the relations $\tau_i^{p_i - 1}[\tau_i, \sigma_i] = 1$ of the local Galois groups $G_{\mathbb{Q}_{p_i}}(l)$ if the homomorphism on the Galois cohomology groups

$$\varphi : H^2\big(G_S(l)\big) \to \prod_{i=1}^{r} H^2\big(G_{\mathbb{Q}_{p_i}}(l)\big)$$

induced by $\eta_i : G_{\mathbb{Q}_{p_i}}(l) \to G_S(l)$ is injective [Kc2, Proposition 1.14]. We shall show this next. Let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let I_S be the kernel of the natural homomorphism $G_{\mathbb{Q}} \to G_S(l)$:

$$1 \longrightarrow I_S \longrightarrow G_{\mathbb{Q}} \longrightarrow G_S(l) \longrightarrow 1 \quad \text{(exact)}.$$

We then have the following Hochschild–Serre exact sequence:

$$H^1(G_{\mathbb{Q}}) \xrightarrow{\text{res}} H^1(I_S)^{G_S(l)} \xrightarrow{\text{tra}} H^2\big(G_S(l)\big) \xrightarrow{\text{inf}} H^2(G_{\mathbb{Q}}). \tag{7.6}$$

For each prime number p, let $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and $I_{\mathbb{Q}_p}$ be the inertia group. Let $G_{\mathbb{Q}_p}(l)$ be the maximal pro-l quotient of $G_{\mathbb{Q}_p}$. Then we note that the natural homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p}(l)$ induces the isomorphism $H^i(G_{\mathbb{Q}_p}(l)) \xrightarrow{\sim} H^i(G_{\mathbb{Q}_p})$ $(i \ge 1)$, since $H^i(T) = 0$ $(i \ge 1)$ for $T := \mathrm{Ker}(G_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p}(l))$. Then we consider the following diagram:

$$\begin{array}{ccc} H^2\big(G_S(l)\big) & \longrightarrow & H^2(G_{\mathbb{Q}}) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle j} \\ \displaystyle\bigoplus_{i=1}^{r} H^2\big(G_{\mathbb{Q}_{p_i}}(l)\big) & \xrightarrow{\iota} & \displaystyle\bigoplus_{p} H^2(G_{\mathbb{Q}_p}), \end{array} \tag{7.7}$$

where ι is the natural injection and θ is the localization map. Since the composite $H^2(G_S(l)) \to H^2(G_{\mathbb{Q}}) \to H^2(G_{\mathbb{Q}_p})$ is 0-map if $p \notin S$, one sees that the above diagram is commutative. By the Tate–Poitou exact sequence 2.43, one has

$$\begin{aligned} \mathrm{Ker}(j) &\simeq \mathrm{Ker}\left(H^1(\mathbb{Q}, \mu_l) \longrightarrow \prod_p H^1(\mathbb{Q}_p, \mu_l) \right)^* \\ &\simeq \mathrm{Ker}\left(\mathbb{Q}^\times/(\mathbb{Q}^\times)^l \longrightarrow \prod_p \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^l \right)^* \\ &= 0 \end{aligned}$$

where μ_l denotes the group of l-th roots of unity. Hence, j is injective. Therefore, by (7.6), (7.7), we have the exact sequence

$$H^1(G) \longrightarrow H^1(I_S)^{G_S(l)} \longrightarrow \mathrm{Ker}(\varphi) \longrightarrow 0.$$

Consider the following commutative exact diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & H^1(G_{\mathbb{Q}}) & \to & H^1(I_S)^{G_S(l)} & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & \prod_{v\in\overline{S}} H^1(G_{\mathbb{Q}_v}) \times \prod_{p\notin\overline{S}} H^1_{\mathrm{ur}}(G_{\mathbb{Q}_p}) & \to & \prod_{v\in S_{\mathbb{Q}}} H^1(G_{\mathbb{Q}_v}) & \to & \bigoplus_{p\notin\overline{S}} H^1(I_{\mathbb{Q}_p})^{G_{\mathbb{Q}_p}} & \to & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & H^1(\mathbb{Q},\mu_l)^* & & H^1(\mathbb{Q},\mu_l)^* & & & & \\
 & & & & \downarrow & & & & \\
 & & & & 0, & & & &
\end{array}$$

where we set $S_{\mathbb{Q}} := \mathrm{Max}(\mathbb{Z}) \cup \{\infty\}$, $\overline{S} := S \cup \{\infty\}$ and $G_{\mathbb{Q}_\infty} = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. The exact sequence in the middle row follows from the short exact sequence $1 \to I_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p} \to \hat{\mathbb{Z}} \to 1$, and the exact sequences in the middle and right columns follow from the Tate–Poitou exact sequence and the definition of I_S respectively. Hence, one has

$$\begin{aligned}
\mathrm{Ker}(\varphi) &\hookrightarrow \mathrm{Coker}\left(\prod_{v\in\overline{S}} H^1(G_{\mathbb{Q}_v}) \times \prod_{p\notin\overline{S}} H^1_{\mathrm{ur}}(G_{\mathbb{Q}_p}) \to H^1(\mathbb{Q},\mu_l)^*\right) \\
&\simeq \mathrm{Ker}\left(\mathbb{Q}^\times/(\mathbb{Q}^\times)^l \to \prod_{v\in\overline{S}} \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^l \times \prod_{p\notin\overline{S}} \mathbb{Q}_p^\times/\mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^l\right)^* \\
&= 0.
\end{aligned}$$

Our assertion about the mod m linking number $\mathrm{lk}_m(p_i, p_j)$ of p_j, p_i is shown in the same manner as in Proposition 5.6. □

The analogy between Theorem 7.1 (or 7.3) and Theorem 7.4 is clear, and we can see the group-theoretic analogy clearly between the linking number and the power residue symbol. We also note that the relations $[x_i, y_i] = 1$ for G_L and $x_i^{p_i-1}[x_i, y_i] = 1$ for $G_S(l)$ come from the relations (3.3) for the local fundamental groups $\pi_1(\partial V_{K_i})$ and $\pi_1^t(\mathrm{Spec}(\mathbb{Q}_{p_i}))$, respectively.

Remark 7.5 (1) Theorem 7.4 can be extended for a finite set of primes in a number field as follows. Let k be a number field of finite degree over $\mathbb{Q}$ which contains a primitive l-th root ζ of unity, and let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be a set of r distinct primes of k such that $\mathrm{N}\mathfrak{p}_i \equiv 1 \bmod l$ $(1 \le i \le r)$. We assume that (1) the class number of k is prime to l and (2) $B_S := \{\alpha \in k^\times | (\alpha) = \mathfrak{a}^l$ ($\mathfrak{a}$ being an ideal), $\alpha \in (k_{\mathfrak{p}_i}^\times)^l (1 \le i \le r)\}/(k^\times)^l = 1$. Then the maximal pro-$l$ quotient $G_S(k)(l)$ of

$\pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$ has the following presentation:

$$G_S(k)(l) = \left\langle x_1, \ldots, x_r \mid x_1^{\mathrm{N}\mathfrak{p}_1 - 1}[x_1, y_1] = \cdots = x_r^{\mathrm{N}\mathfrak{p}_r - 1}[x_r, y_r] = 1 \right\rangle, \tag{7.8}$$

where x_i represents a monodromy over $\mathfrak{p}_i$ and y_i represents an extension of the Frobenius automorphism over $\mathfrak{p}_i$. The assumption $B_S = 1$ is a sufficient condition for the localization map $H^2(G_S(k)(l)) \to \prod_{i=1}^r H^2(D_{\mathfrak{p}_i}(l))$ to be injective [Kc2, Theorem 4.2].

(2) Turaev [Tu] gave a homological proof of Theorem 7.1 using Stallings' result [St], which may be close to the proof of Theorem 7.4.

(3) Some properties (mildness, cohomological l-dimension etc.) of the Galois group $G_S(l)$, more generally of pro-l groups of Koch type, were investigated using the arithmetic linking numbers in [Lb1, LM] and [Sc1].

Summary

J. Milnor's theorem	H. Koch's theorem
$G_L/G_L^{(d)} = \langle x_1, \ldots, x_r \mid [x_1, y_1^{(d)}] = \cdots = [x_r, y_r^{(d)}] = 1, F^{(d)} = 1 \rangle$	$G_S(l) = \langle x_1, \ldots, x_r \mid x_1^{p_1 - 1}[x_1, y_1] = \cdots = x_r^{p_r - 1}[x_r, y_r] = 1 \rangle$
x_i : meridian of K_i	x_i : monodromy over p_i
$y_i^{(d)}$: longitude of K_i	y_i : Frobenius auto. over p_i

Chapter 8
Milnor Invariants and Multiple Residue Symbols

The notion of higher linking numbers (Milnor $\overline{\mu}$-invariants) was introduced by J. Milnor [Ml1]. By the analogy between link groups and Galois groups with restricted ramification in Chap. 7, we can introduce arithmetic analogues of the Milnor invariants for prime numbers. They may be regarded as multiple generalization of the power residue symbol and the Rédei triple symbol.

8.1 Fox Free Differential Calculus

For a group G and a commutative ring R, we set

$$R[G] := \left\{ \sum_{g \in G} a_g g \;\middle|\; a_g \in R, a_g = 0 \text{ except for a finite number of } g \right\}.$$

For $\alpha = \sum a_g g$, $\beta = \sum b_g g \in R[G]$ and $c \in R$, we define the sum, the action of R and the multiplication on $R[G]$ by

$$\begin{cases} \alpha + \beta := \sum (a_g + b_g) g \\ c\alpha := \sum (c a_g) g \\ \alpha \cdot \beta := \sum_g (\sum_h a_h b_{h^{-1}g}) g. \end{cases}$$

Then $R[G]$ forms an R-algebra, called the *group algebra* of G over R. Note that if we identify an element $\alpha = \sum a_g g$ with an R-valued function $\alpha : g \mapsto a_g$ with finite support, the sum, R-action and multiplication in the above correspond to the usual sum, R-action and convolution for R-valued functions, respectively.

A homomorphism $\psi : G \to H$ of groups is naturally extended to an R-algebra homomorphism which we also denote by the same ψ:

$$\psi : R[G] \to R[H]; \qquad \psi\left(\sum a_g g\right) := \sum a_g \psi(g).$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_8, © Springer-Verlag London Limited 2012

In particular, when H is the unit group $\{e\}$, we have, by identifying $a \in R$ with ae, the R-algebra homomorphism

$$\epsilon_{R[G]} : R[G] \to R; \qquad \epsilon_{R[G]}\left(\sum a_g g\right) := \sum a_g$$

which is called the *augmentation map*. The kernel $\mathrm{Ker}(\epsilon_{R[G]})$ is called the *augmentation ideal* of $R[G]$ and is denoted by $I_{R[G]}$.

Let $\mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle$ be the algebra of non-commutative formal power series of variables $X_1, \ldots, X_r$ over $\mathbb{Z}$:

$$\mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle := \left\{ \sum_{1 \le i_1, \ldots, i_n \le r} a_{i_1 \cdots i_n} X_{i_1} \cdots X_{i_n} \,\middle|\, n \ge 0, a_{i_1 \cdots i_n} \in \mathbb{Z} \right\}.$$

The *degree* of $f = f(X_1, \ldots, X_r) = \sum a_{i_1 \cdots i_n} X_{i_1} \cdots X_{i_n}$ is the smallest integer n such that $a_{i_1 \cdots i_n} \neq 0$ and is denoted by $\deg(f)$.

Let F be the free group on the letters $x_1, \ldots, x_r$. Define the homomorphism

$$M : F \longrightarrow \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle^{\times}$$

by

$$M(x_i) := 1 + X_i, \qquad M\left(x_i^{-1}\right) := 1 - X_i + X_i^2 - \cdots \quad (1 \le i \le r).$$

We extend, in the $\mathbb{Z}$-linear manner, M to a $\mathbb{Z}$-algebra homomorphism

$$M : \mathbb{Z}[F] \longrightarrow \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle$$

which is also denoted by M.

Lemma 8.1 *The map M is injective.* (*M is called the Magnus embedding.*)

Proof Assume $f \in F$ is not the identity and let $f = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ $(1 \le i_1, \ldots, i_n \le r, i_j \neq i_{j+1}, e_j (\neq 0) \in \mathbb{Z})$ be a reduced word. Then we can write

$$M\left(x_{i_j}^{e_j}\right) = 1 + e_j X_{i_j} + X_{i_j}^2 g_j(X_{i_j}), \quad g_j(X_{i_j}) \in \mathbb{Z}\langle\langle X_{i_j}\rangle\rangle$$

and hence we have

$$M(f) = \left(1 + e_1 X_{i_1} + X_{i_1}^2 g_1(X_{i_1})\right) \cdots \left(1 + e_n X_{i_n} + X_{i_n}^2 g_n(X_{i_n})\right).$$

Here the coefficient $X_{i_1} \cdots X_{i_n}$ is $e_1 \cdots e_n \neq 0$ and so $M(f) \neq 1$. Therefore, $M : F \to \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle^{\times}$ is injective and hence the extended M is also injective. □

For $\alpha \in \mathbb{Z}[F]$,

$$M(\alpha) = \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{\substack{I = (i_1 \cdots i_n) \\ 1 \le i_1, \ldots, i_n \le r}} \mu(I; \alpha) X_I, \quad X_I := X_{i_1} \cdots X_{i_n}$$

is called the *Magnus expansion* of α and the coefficients $\mu(I;\alpha)\,(\in\mathbb{Z})$ are called the *Magnus coefficients*. As we shall show in the following, the Fox free differential calculus gives an interpretation of the Magnus expansion as the "Taylor expansion" with respect to the non-commutative variables $x_1,\dots,x_r$.

Theorem 8.2 ([Fo1]) *For any $\alpha\in\mathbb{Z}[F]$, there exists α_j uniquely for each j $(1\le j\le r)$ such that one has*

$$\alpha=\epsilon_{\mathbb{Z}[F]}(\alpha)+\sum_{j=1}^{r}\alpha_j(x_j-1).$$

We call α_j the *Fox free derivative* of α with respect to x_j and write $\alpha_j=\partial\alpha/\partial x_j$.

Proof For $f=x_{i_1}^{e_1}\cdots x_{i_n}^{e_n}$ $(e_j=\pm1)$, we set

$$\begin{cases}\dfrac{\partial f}{\partial x_j}:=\dfrac{\partial x_{i_1}^{e_1}}{\partial x_j}+x_{i_1}^{e_1}\dfrac{\partial x_{i_2}^{e_2}}{\partial x_j}+\cdots+x_{i_1}^{e_1}\cdots x_{i_{n-1}}^{e_{n-1}}\dfrac{\partial x_{i_n}^{e_n}}{\partial x_j}\\ \dfrac{\partial x_i}{\partial x_j}:=\delta_{ij},\qquad \dfrac{\partial x_i^{-1}}{\partial x_j}:=-x_i^{-1}\delta_{ij}\quad\text{where }\delta_{ij}=\begin{cases}1 & (i=j),\\ 0 & (i\ne j)\end{cases}\end{cases}$$

and for $\alpha=\sum a_f f\in\mathbb{Z}[F]$, we set

$$\frac{\partial\alpha}{\partial x_j}=\sum a_f\frac{\partial f}{\partial x_j}.$$

Noting $(\partial x_i^{e_i}/\partial x_j)(x_i-1)=(x_i^{e_i}-1)\delta_{ij}$, one has

$$\begin{aligned}&1+\sum_{j=1}^{r}\frac{\partial f}{\partial x_j}(x_j-1)\\ &=1+\sum_{j=1}^{r}\frac{\partial x_{i_1}^{e_1}}{\partial x_j}(x_j-1)+\sum_{j=1}^{r}x_{i_1}^{e_1}\frac{\partial x_{i_2}^{e_2}}{\partial x_j}(x_j-1)\\ &\quad+\cdots+\sum_{j=1}^{r}x_{i_1}^{e_1}\cdots x_{i_{n-1}}^{e_{n-1}}\frac{\partial x_{i_n}^{e_n}}{\partial x_j}(x_j-1)\\ &=1+\left(x_{i_1}^{e_1}-1\right)+x_{i_1}^{e_1}\left(x_{i_2}^{e_2}-1\right)+\cdots+x_{i_1}^{e_1}\cdots x_{i_{n-1}}^{e_{n-1}}\left(x_{i_n}^{e_n}-1\right)\\ &=x_{i_1}^{e_1}\cdots x_{i_n}^{e_n}\\ &=f\end{aligned}$$

and hence one has, for $\alpha\in\mathbb{Z}[F]$,

$$\alpha=\epsilon_{\mathbb{Z}[F]}(\alpha)+\sum_{j=1}^{r}\frac{\partial\alpha}{\partial x_j}(x_j-1).$$

Next, suppose

$$\alpha = \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \alpha_j (x_j - 1) = \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \alpha'_j (x_j - 1) \quad (\alpha_j, \alpha'_j \in \mathbb{Z}[F]).$$

Applying the Magnus embedding, one has

$$\sum_{j=1}^{r} \big(M(\alpha_j) - M(\alpha'_j)\big) X_j = 0$$

and therefore

$$M(\alpha_j) = M(\alpha'_j) \quad (1 \le j \le n).$$

By Lemma 8.1, we have $\alpha_j = \alpha'_j$ $(1 \le j \le n)$. □

Proposition 8.3 *The Fox derivative* $\partial/\partial x_j : \mathbb{Z}[F] \to \mathbb{Z}[F]$ *satisfies the following properties*:

(1) $\dfrac{\partial x_i}{\partial x_j} = \delta_{ij}$.

(2) $\dfrac{\partial(\alpha+\beta)}{\partial x_j} = \dfrac{\partial \alpha}{\partial x_j} + \dfrac{\partial \beta}{\partial x_j}$, $\dfrac{\partial(c\alpha)}{\partial x_j} = c\dfrac{\partial \alpha}{\partial x_j}$ $(\alpha, \beta \in \mathbb{Z}[F], c \in \mathbb{Z})$.

(3) $\dfrac{\partial(\alpha\beta)}{\partial x_j} = \dfrac{\partial \alpha}{\partial x_j}\epsilon_{\mathbb{Z}[F]}(\beta) + \alpha\dfrac{\partial \beta}{\partial x_j}$ $(\alpha, \beta \in \mathbb{Z}[F])$.

(4) $\dfrac{\partial f^{-1}}{\partial x_j} = -f^{-1}\dfrac{\partial f}{\partial x_j}$ $(f \in F)$.

Proof (1) follows from the definition. We leave the proof of (2) to readers. Let us prove (3) and (4).

(3) By Theorem 8.2, we have

$$\begin{aligned}\alpha\beta &= \left(\epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1)\right) \cdot \left(\epsilon_{\mathbb{Z}[F]}(\beta) + \sum_{k=1}^{r} \frac{\partial \beta}{\partial x_k}(x_k - 1)\right) \\ &= \epsilon_{\mathbb{Z}[F]}(\alpha\beta) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}\epsilon_{\mathbb{Z}[F]}(\beta)(x_j - 1) + \sum_{k=1}^{r} \epsilon_{\mathbb{Z}[F]}(\alpha)\frac{\partial \beta}{\partial x_k}(x_k - 1) \\ &\quad + \sum_{j,k=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1)\frac{\partial \beta}{\partial x_k}(x_k - 1)\end{aligned}$$

$$
\begin{aligned}
&= \epsilon_{\mathbb{Z}[F]}(\alpha\beta) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j} \epsilon_{\mathbb{Z}[F]}(\beta)(x_j - 1) \\
&\quad + \sum_{k=1}^{r} \left(\epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1) \right) \frac{\partial \beta}{\partial x_k}(x_k - 1) \\
&= \epsilon_{\mathbb{Z}[F]}(\alpha\beta) + \sum_{j=1}^{r} \left(\frac{\partial \alpha}{\partial x_j} \epsilon_{\mathbb{Z}[F]}(\beta) + \alpha \frac{\partial \beta}{\partial x_j} \right)(x_j - 1),
\end{aligned}
$$

which yields the assertion by the uniqueness of the Fox derivative.

(4) Taking the Fox derivative of the both sides of $f \cdot f^{-1} = 1$ using (3), we have

$$
\frac{\partial f}{\partial x_j} + f \frac{\partial f^{-1}}{\partial x_j} = 0
$$

which yields the assertion. □

We define the higher derivatives inductively by

$$
\frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}} := \frac{\partial}{\partial x_{i_1}} \left(\frac{\partial^{n-1} \alpha}{\partial x_{i_2} \cdots \partial x_{i_n}} \right) (\alpha \in \mathbb{Z}[F]).
$$

For simplicity, we also denote this by $D_I(\alpha)$ ($I = (i_1 \cdots i_n)$). The relation with the Magnus coefficients is given as follows.

Proposition 8.4 *For $\alpha, \beta \in \mathbb{Z}[F]$ and $I = (i_1 \cdots i_n)$, we have the following*:

(1) $\mu(I; \alpha) = \epsilon_{\mathbb{Z}[F]}(D_I(\alpha))$.
(2) $\mu(I; \alpha\beta) = \sum_{I=JK} \mu(J; \alpha)\mu(K; \beta)$ *where the sum ranges over the pairs* (J, K) *such that* $I = JK$.

Proof (1) By Theorem 8.2, we have

$$
\begin{aligned}
\alpha &= \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1) \\
&= \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \left(\epsilon_{\mathbb{Z}[F]}\left(\frac{\partial \alpha}{\partial x_j} \right) + \sum_{i=1}^{r} \frac{\partial^2 \alpha}{\partial x_i \partial x_j}(x_i - 1) \right)(x_j - 1) \\
&= \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{j=1}^{r} \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial \alpha}{\partial x_j} \right)(x_j - 1) \\
&\quad + \sum_{1 \le i, j \le r} \frac{\partial^2 \alpha}{\partial x_i \partial x_j}(x_i - 1)(x_j - 1) \\
&\quad \vdots
\end{aligned}
$$

$$= \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{i_1=1}^{r} \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial \alpha}{\partial x_{i_1}}\right)(x_{i_1} - 1) + \cdots$$
$$+ \sum_{1 \le i_1, \ldots, i_n \le r} \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}}\right)(x_{i_1} - 1) \cdots (x_{i_n} - 1)$$
$$+ \sum_{1 \le i_1, \ldots, i_{n+1} \le r} \frac{\partial^{n+1} \alpha}{\partial x_{i_1} \cdots \partial x_{i_{n+1}}}(x_{i_1} - 1) \cdots (x_{i_{n+1}} - 1).$$

Hence, we have

$$M(\alpha) = \epsilon_{\mathbb{Z}[F]}(\alpha) + \sum_{i_1=1}^{r} \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial \alpha}{\partial x_{i_1}}\right) X_{i_1} + \cdots$$
$$+ \sum_{1 \le i_1, \ldots, i_n \le r} \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}}\right) X_{i_1} \cdots X_{i_n}$$
$$+ \sum_{1 \le i_1, \ldots, i_{n+1} \le r} M\left(\frac{\partial^{n+1} \alpha}{\partial x_{i_1} \cdots \partial x_{i_{n+1}}}\right) X_{i_1} \cdots X_{i_{n+1}}.$$

Comparing the coefficients of $X_{i_1} \cdots X_{i_n}$, we obtain the assertion.

(2) By Proposition 8.3(2), (3), we have

$$\frac{\partial^n (\alpha\beta)}{\partial x_{i_1} \cdots \partial x_{i_n}} = \frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}} \epsilon_{\mathbb{Z}[F]}(\beta)$$
$$+ \sum_{m=1}^{n-1} \frac{\partial^m \alpha}{\partial x_{i_1} \cdots \partial x_{i_m}} \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial^{n-m} \beta}{\partial x_{i_{m+1}} \cdots \partial x_{i_{n-m}}}\right)$$
$$+ \alpha \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial^n \beta}{\partial x_{i_1} \cdots \partial x_{i_n}}\right).$$

Applying $\epsilon_{\mathbb{Z}[F]}$ to both sides, we get the assertion by (1). □

The relation between the Magnus coefficients and the lower central series of a free group is given as follows. For a multiple index $I = (i_1 \cdots i_n)$, let $|I| := n$.

Proposition 8.5 *For $d \ge 2$, the following conditions are equivalent.*

(1) $f \in F^{(d)}$

(2) *For any I with $\le |I| < d$, $\mu(I; f) = \epsilon_{\mathbb{Z}[F]}(D_I(f)) = 0$.*
Namely, we have

$$F^{(d)} = \left\{ f \in F \mid \deg(M(f) - 1) \ge d \right\}.$$

Proof Set $F_{(d)} := \{f \in F \mid \deg(M(f) - 1) \geq d\}$. Then $\{F_{(d)}\}_{d\geq 1}$ forms a descending series of normal subgroups of F. First, we show $F^{(d)} \subset F_{(d)}$ by induction on d. By definition, $F^{(1)} = F_{(1)}$. Assume $F^{(d-1)} \subset F_{(d-1)}$. Let $f \in F$, $g \in F^{(d-1)}$. Writing $M(f) = 1 + P$, $M(g) = 1 + Q$ ($\deg(P) \geq 1$, $\deg(Q) \geq d - 1$), we have

$$\begin{aligned} M\big([f,g]\big) &= M(f)M(g)M(f)^{-1}M(g)^{-1} \\ &= (1+P)(1+Q)\big(1 - P + P^2 - \cdots\big)\big(1 - Q + Q^2 - \cdots\big) \\ &= 1 + (PQ - QP) + (\text{the terms of higher degree}). \end{aligned}$$

Since $\deg(PQ - QP) \geq d$, we have $[f,g] \in F_{(d)}$. Hence, $F^{(d)} \subset F_{(d)}$. From this, we have the natural homomorphism for $d \geq 1$

$$\varphi_d : F^{(d)}/F^{(d+1)} \to F_{(d)}/F_{(d+1)}.$$

It suffices to show that φ_d is injective for any $d \geq 1$, because $0 = \mathrm{Ker}(\varphi_d) = F_{(d+1)}/F^{(d+1)}$ implies $F^{(d+1)} = F_{(d+1)}$. The injectivity of φ_d is shown as follows. First, we define $\pi : F \to \bigoplus_{d\geq 1} F^{(d)}/F^{(d+1)}$ as follows: if $f \in F^{(m)}$ and $f \notin F^{(m+1)}$, set $\pi(f)_m := f \bmod F^{(m+1)}$, $\pi(f)_n := 0$, $n \neq m$. We then define $\pi(f)$ by $(\pi(f)_d)$. Next, define $\lambda : \bigoplus_{d\geq 1} F_{(d)}/F_{(d+1)} \to \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle$ as follows: For $f_d \in F_{(d)}$, letting $M(f_d) = 1 + P_d + P_{d+1} + \cdots$ (P_j = the sum of monomials of degree j), set $\lambda(f_d \bmod F_{(d+1)}) := P_d$. For $f = (f_d) \in \bigoplus_{d\geq 1} F_{(d)}/F_{(d+1)}$, we set $\lambda(f) := \sum_{d\geq 1} \lambda(f_d)$. Let $\varphi := \bigoplus_{d\geq 1} \varphi_d$. The composite

$$F \xrightarrow{\pi} \bigoplus_{d\geq 1} F^{(d)}/F^{(d+1)} \xrightarrow{\varphi} \bigoplus_{d\geq 1} F_{(d)}/F_{(d+1)} \xrightarrow{\lambda} \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle$$

satisfies $(\lambda \circ \varphi \circ \pi)(f) = M(f) - 1$ ($f \in F$). Since M is injective, $\lambda \circ \varphi \circ \pi$ is so. Hence, φ is injective. □

Finally, we shall show the shuffle relation among Magnus coefficients. For multiple indices $I = (i_1 \cdots i_m)$, $J = (j_1 \cdots j_n)$, a pair (a, b) of sequences of integers $a = (a(1), \ldots, a(m))$, $b = (b(1), \ldots, b(n))$ is called the *shuffle* of I and J, if one has

$$\begin{aligned} &1 \leq a(1) < \cdots < a\big(|I|\big) \leq |I| + |J|, \\ &1 \leq b(1) < \cdots < b\big(|J|\big) \leq |I| + |J| \end{aligned}$$

and there is a multiple index $H = (h_1 \cdots h_l)$ such that the following conditions hold:

$$\begin{cases} (1)\ h_{a(s)} = i_s\ (s = 1, \ldots, m),\ h_{b(t)} = j_t\ (t = 1, \ldots, n), \\ (2)\ \text{for any } u = 1, \ldots, l,\ \text{there is } s \text{ or } t \text{ such that } u = a(s) \text{ or } u = b(t) \\ \quad (\text{possibly } u = a(s) = b(t)) \end{cases}$$

A multiple index $H = (h_1 \cdots h_l)$ ($l \leq m + n$) determined from a shuffle of I and J as above is called a *result of a shuffle*. For example, when $I = (12)$ and $J = (123)$,

both ($a = (12), b = (134)$) and ($a = (13), b = (124)$) are shuffles of I and J whose result is the same $H = (1223)$. Let $\mathrm{Sh}(I, J)$ denote the set of results of shuffles of I and J allowing overlapping (it corresponds bijectively to the set of shuffles of I and J). A shuffle (a, b) is called a *proper shuffle* if $a(s) \neq b(t)$ $(1 \leq s \leq m, 1 \leq t \leq n)$. The result H of a proper shuffle (a, b) has length $m + n$. We denote by $\mathrm{PSh}(I, J)$ the set of results of proper shuffles of I and J. The Magnus coefficients satisfy the following shuffle relation.

Proposition 8.6 ([CFL]) *For multiple indices I, J $(|I|, |J| \geq 1)$ and $f \in F$, we have the following formula*:

$$\mu(I; f)\mu(J; f) = \sum_{H \in \mathrm{Sh}(I,J)} \mu(H; f).$$

Proof We shall prove the above equality by induction on the length of a word f.

When $f = x_i$: The both sides of the equality are 0 unless $I = J = (i)$. If $I = J = (i)$, $\mathrm{Sh}((i), (i)) = \{(i), (ii), (ii)\}$, $\mu((i); x_i) = 1$, $\mu((ii), x_i) = 0$. Hence, the both sides are 1.

When $f = x_i^{-1}$: The both sides of the equality is 0 unless I and J are of the form $(i \cdots i)$. If $I = (i \cdots i)$ with $|I| = s$ and $J = (i \cdots i)$ with $|J| = t$, then the left-hand side $= \mu(I; x_i^{-1})\mu(J; x_i^{-1}) = (-1)^s(-1)^t = (-1)^{s+t}$. Letting $(s, t)_u$ denote the number of $H = (i \cdots i) \in \mathrm{Sh}(I, J)$ with $|H| = u$, the right-hand side $= \sum_{u=\max\{s,t\}}^{s+t}(-1)^u(s, t)_u$. Therefore, it suffices to show

$$(*)_{r,s} \qquad \sum_{u=\max\{s,t\}}^{s+t} (-1)^u(s, t)_u = (-1)^{s+t}. \tag{8.1}$$

Proof of (8.1): Induction on t. First, noting $(s, 1)_s = s$ and $(s, 1)_{s+1} = s + 1$, we have $(-1)^s s + (-1)^{s+1}(s + 1) = (-1)^{s+1}$ and so $(*)_{s,1}$ holds for any s. Let $t \geq 1$ and assume that $(*)_{s,t}$ holds for any s. Then we have

$$\begin{aligned}
&t(-1)^{s+t} + (t + 1) \sum_{u=\max\{s,t+1\}}^{s+t+1} (-1)^u(s, t + 1)_u \\
&= \sum_{v=t}^{t+1} \sum_{u=\max\{s,v\}}^{s+v} (-1)^u(s, v)_u(1, t)_v \quad \text{(by the inductive hypothesis)} \\
&= \sum_{w=s}^{s+1} \sum_{u=\max\{w,t\}}^{w+t} (-1)^u(s, 1)_w(w, t)_u \\
&\qquad\qquad (\mathrm{Sh}(I, \mathrm{Sh}((i), J)) = \mathrm{Sh}(\mathrm{Sh}(I, (i)), J)) \\
&= \sum_{w=s}^{s+1} (-1)^{w+t}(s, 1)_w \quad \text{(by the inductive hypothesis)} \\
&= (-1)^{s+t+1}.
\end{aligned}$$

Therefore, we have

$$\sum_{u=\max\{s,t+1\}}^{s+t+1} (-1)^u (s, t+1)_u$$
$$= \frac{1}{t+1}\big((-1)^{s+t+1} - t(-1)^{s+t}\big) = (-1)^{s+t+1}$$

and hence (8.1) holds.

When f has length > 1, we can write $f = f_1 f_2$ $(f_1, f_2 \in F)$. Then we have

$$\begin{aligned}
&\mu(I; f)\mu(J; f) \\
&= \Big(\sum_{I=I_1I_2} \mu(I_1; f_1)\mu(I_2; f_2)\Big)\Big(\sum_{J=J_1J_2} \mu(J_1; f_1)\mu(J_2; f_2)\Big) \\
&\qquad \text{(Proposition 8.4(2))} \\
&= \sum_{I=I_1I_2, J=J_1J_2} \mu(I_1; f_1)\mu(J_1; f_1)\mu(I_2; f_2)\mu(J_2; f_2) \\
&= \sum_{I=I_1I_2, J=J_1J_2} \sum_{H_1\in \mathrm{Sh}(I_1,J_1), H_2\in \mathrm{Sh}(I_2,J_2)} \mu(H_1; f_1)\mu(H_2; f_2) \\
&= \sum_{H\in \mathrm{Sh}(I,J)} \sum_{H=H_1H_2} \mu(H_1; f_1)\mu(H_2; f_2) \\
&= \sum_{H\in \mathrm{Sh}(I,J)} \mu(H; f) \quad \text{(Proposition 8.4(2))}.
\end{aligned}$$

Hence, the induction works and the assertion follows. □

8.2 Milnor Invariants

Let $L = K_1 \cup \cdots \cup K_r$ be a link in S^3 and let $G_L = \pi_1(S^3 \setminus L)$ be the link group of L. In this section, we shall use the same notation as in Sect. 7.1. Let α_i be a meridian of K_i and let F be the free group on the words $x_1, \ldots, x_r$ where x_i represents α_i. By Theorem 7.1, for each $d \geq 1$, there is $y_i^{(d)} \in F$ such that

$$G_L/G_L^{(d)} = \langle x_1, \ldots, x_r \mid [x_1, y_1^{(d)}] = \cdots = [x_r, y_r^{(d)}] = 1, F^{(d)} = 1\rangle,$$
$$y_i^{(d)} \equiv y_i^{(d+1)} \bmod F^{(d)} \quad (1 \leq i \leq r).$$

Here $y_i^{(d)}$ is the word which represents a longitude β_i of K_i in $G_L/G_L^{(d)}$. Let

$$M\big(y_i^{(d)}\big) = 1 + \sum_{\substack{I=(i_1\cdots i_n)\\ 1\leq i_1,\ldots,i_n\leq r}} \mu^{(d)}(Ii) X_I$$

be the Magnus expansion of $y_i^{(d)}$. By Proposition 8.4(1), we have

$$\mu^{(d)}(Ii) = \epsilon_{\mathbb{Z}[F]}\big(D_I\big(y_i^{(d)}\big)\big).$$

By Proposition 8.5, $\mu^{(d)}(I)$ is independent of d if $d \geq |I|$ and so we define the *Milnor number* $\mu(I)$ to be $\mu^{(d)}(I)$ by taking a sufficiently large d. For a multi-index I with $|I| \geq 2$, we define $\Delta(I)$ to be the ideal of $\mathbb{Z}$ generated by $\mu(J)$ where J runs over cyclic permutations of proper subsequences of I. If $|I| = 1$, we set $\mu(I) := 0$. So $\Delta(I) = 0$ if $|I| = 1, 2$. We then define the *Milnor $\overline{\mu}$-invariant* by

$$\overline{\mu}(I) := \mu(I) \bmod \Delta(I).$$

Theorem 8.7 ([Ml1]) (1) $\overline{\mu}(ij) = \mathrm{lk}(K_i, K_j)$ $(i \neq j)$.

(2) *If* $2 \leq |I| \leq d$, $\overline{\mu}(I)$ *is a link invariant* L (*In fact, it is an isotopy invariant*).

(3) (*Shuffle relation*) *For any* I, J $(|I|, |J| \geq 1)$ *and* i $(1 \leq i \leq r)$, *we have*

$$\sum_{H \in \mathrm{PSh}(I,J)} \overline{\mu}(Hi) \equiv 0 \bmod \text{ g.c.d.}\{\Delta(Hi) \mid H \in \mathrm{PSh}(I, J)\}.$$

(4) (*Cyclic symmetry*) $\overline{\mu}(i_1 \cdots i_n) = \overline{\mu}(i_2 \cdots i_n i_1) = \cdots = \overline{\mu}(i_n i_1 \cdots i_{n-1})$.

Proof (1) By Theorem 7.1, $\beta_j \equiv \prod_{i \neq j} \alpha_i^{\mathrm{lk}(K_i, K_j)} \bmod G_L^{(2)}$. Hence, we have

$$M(y_j^{(d)}) = 1 + \sum_{i \neq j} \mathrm{lk}(K_i, K_j) X_i + (\text{higher terms})$$

which yields $\overline{\mu}(ij) = \mu(ij) = \mathrm{lk}(K_i, K_j)$.

(2) We need to show that $\overline{\mu}(I)$ is determined by the link group G_L, namely, independent of the choice of a meridian and a longitude. Let $I = (i_1 \cdots i_n)$, $2 \leq n \leq d$. It then suffices to show the following:

(i) $\overline{\mu}(I)$ is not changed if $y_{i_n}^{(d)}$ is replaced by a conjugate.
(ii) $\overline{\mu}(I)$ is not changed if x_i is replaced by a conjugate.
(iii) $\overline{\mu}(I)$ is not changed if $y_{i_n}^{(d)}$ is multiplied by a conjugate of $[x_i, y_i^{(d)}]$.
(iv) $\overline{\mu}(I)$ is not changed if $y_{i_n}^{(d)}$ is multiplied by an element of $F^{(d)}$.

Let $I' := (i_1 \cdots i_{n-1})$.

Proof of (i) For $f \in F$, $M(x_i f x_i^{-1}) = (1 + X_i)M(f)(1 - X_i + X_i^2 + \cdots)$. Comparing the coefficients of $X_{I'}$ in both sides, we have $\mu(I'; x_i f x_i^{-1}) \equiv \mu(I'; f) \bmod \mathfrak{a}(I')$ where $\mathfrak{a}(I')$ is the ideal of $\mathbb{Z}$ generated by $\mu(J; f)$ where J ranges over all proper subsequences of I'. Similarly, we have $\mu(I'; x_i^{-1} f x_i) \equiv \mu(I'; f) \bmod \mathfrak{a}(I')$. Letting $f = y_{i_n}^{(d)}$ and noting $\mathfrak{a}(I') \subset \Delta(I)$, we obtain the assertion (i).

Proof of (ii) Suppose that x_i is replaced by $\bar{x}_i = x_j x_i x_j^{-1}$. As $x_i = x_j^{-1} \bar{x}_i x_j$, we have $1 + X_i = (1 - X_j + X_j^2 - \cdots)(1 + \bar{X}_i)(1 + X_j)$. Therefore, $X_i =$

$\bar{X}_i$ + (terms containing $X_j\bar{X}_i$ or $\bar{X}_iX_j$). Each time X_i occurs in the Magnus expansion $M(y_j^{(d)})$, it is to be replaced by this last expansion. Then the coefficient of $\bar{X}_{i_1}\cdots\bar{X}_{i_{n-1}}$ in the new Magnus expansion of $y_{i_n}^{(d)}$ with respect to $\bar{X}_i$'s is given by

$$\mu(I)+\sum_J \mu(Ji_n) \quad (J \text{ is a proper subsequence of } I')$$

and so it equals $\mu(I)$ mod $\Delta(I)$. Similarly, $\overline{\mu}(I)$ is not changed when x_i is replaced by $\bar{x}_i = x_j^{-1}x_ix_j$.

Proof of (iii) Let $J=(i_1\cdots i_s)$ $(1\le s<n)$ be an initial segment of I' and let $J'=(j_1\cdots j_t)$ be a subsequence of J. Comparing the coefficients of $X_{J'}$ in the both sides of the equality

$$M\big([x_i, y_i^{(d)}]\big) = 1+\big(M\big(x_iy_i^{(d)}\big)-M\big(y_i^{(d)}x_i\big)\big)M\big(x_i^{-1}\big)M\big(y_i^{(d)^{-1}}\big),$$

we have

$$\mu\big(J';[x_i,y_i^{(d)}]\big)\equiv\mu\big(J';x_iy_i^{(d)}\big)-\mu\big(J';y_i^{(d)}x_i\big) \bmod \Delta(I), \tag{8.2}$$

where

$$\mu\big(J';x_iy_i^{(d)}\big)=\begin{cases}\mu(J'i) & (\text{if } i\ne j_1),\\ \mu(J'j_1)+\mu(j_2\cdots j_tj_1) & (\text{if } i=j_1),\end{cases}$$

$$\mu\big(J';y_i^{(d)}x_i\big)=\begin{cases}\mu(J'i) & (i\ne j_t),\\ \mu(J'j_t)+\mu(J') & (i=j_t)\end{cases}$$

and hence we have

$$\begin{aligned}&\mu\big(J';x_iy_i^{(d)}\big)-\mu\big(J';y_i^{(d)}x_i\big)\\ &=\begin{cases}\mu(j_2\cdots j_tj_1)-\delta_{j_1j_t}\mu(J') & (i=j_1),\\ \mu(j_2\cdots j_tj_1)\delta_{j_1j_t}-\mu(J') & (i=j_t),\\ 0 & (\text{otherwise})\end{cases}\\ &\equiv 0 \bmod \Delta(I).\end{aligned}$$

Therefore, we have, by (8.2),

$$\mu\big(J';[x_i,y_i^{(d)}]\big)\equiv 0 \bmod \Delta(I).$$

As in the proof of (i), one obtains

$$\mu\big(J;x_j^{\varepsilon}[x_i,y_i^{(d)}]x_j^{-\varepsilon}\big)\equiv\mu\big(J;[x_i,y_i^{(d)}]\big)\equiv 0 \bmod \Delta(I) \quad (\varepsilon=\pm1). \tag{8.3}$$

By Proposition 8.4(2),

$$\mu\big(I';x_j^{\varepsilon}[x_i,y_i^{(d)}]x_j^{-\varepsilon}y_{i_n}^{(d)}\big)=\sum_{I'=JK}\mu\big(J;x_j^{\varepsilon}[x_i,y_i^{(d)}]x_j^{-\varepsilon}\big)\mu(Ki_n). \tag{8.4}$$

By (8.3) and (8.4),

$$\mu\big(I'; x_j^{\varepsilon}\big[x_i, y_i^{(d)}\big]x_j^{-\varepsilon} y_{i_n}^{(d)}\big) \equiv \mu\big(I'; y_{i_n}^{(d)}\big) = \mu(I) \bmod \Delta(I).$$

By the same argument as above applied for a tail segment J of I' and a subsequence J' of J, we have $\mu(I'; y_{i_n}^{(d)} x_j^{\varepsilon}[x_i, y_i^{(d)}]x_j^{-\varepsilon}) \equiv \mu(I'; y_{i_n}^{(d)}) = \mu(I) \bmod \Delta(I)$.

Proof of (iv) If $n \le d$, $|I'| < d$ and hence, we have $\mu(I'; y_{i_n}^{(d)} f) = \mu(I'; y_{i_n}^{(d)})$ for $f \in F^{(d)}$ by Proposition 8.5. Similarly, we have $\mu(I'; f y_{i_n}^{(d)}) = \mu(I'; y_{i_n}^{(d)})$ for $f \in F^{(d)}$.

It follows from Remark 7.2(2) that $\overline{\mu}(I)$ is an isotopy invariant.

(3) Shuffle relation: By Proposition 8.6, we have

$$\mu(Ii)\mu(Ji) = \sum_{H \in \mathrm{Sh}(I,J)} \mu(Hi).$$

Here the left-hand side is congruent to 0 mod $\mathrm{g.c.d.}\{\Delta(Hi) \mid H \in \mathrm{PSh}(I, J)\}$, while $\mu(Hi)$ in the right-hand side is congruent to 0 if $H \notin \mathrm{PSh}(I, J)$. Hence, the assertion follows.

(4) Cyclic symmetry: We use the same notations as in the proof of Theorem 7.1. Fix d such that $d > n$. By Example 2.6(4), there are $z_{ij} \in \overline{F}$ such that

$$\prod_{i=1}^{r} \prod_{j=1}^{\lambda_i} z_{ij} r_{ij} z_{ij}^{-1} = 1. \tag{8.5}$$

Set $z_i = \eta_d(z_{i\lambda_i})$. Since $\eta_d(r_{ij}) \equiv 1 \bmod F^{(d)}$ $(1 \le j < \lambda_i)$ and $\eta_d(r_{i\lambda_i}) \equiv [x_i, y_i^{(d)}] \bmod F^{(d)}$, (8.5) implies

$$\prod_{i=1}^{r} z_i\big[x_i, y_i^{(d)}\big]z_i^{-1} \in F^{(d)}. \tag{8.6}$$

Let $D := \{\sum_I c_I X_I \in \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle \mid c_I \equiv 0 \bmod \Delta(I),\ |I| \le d\}$. Note that D is a two-sided ideal of $\mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle$. Let $M(y_i^{(d)}) = 1 + w_i$ $(1 \le i \le r)$. Since Ii is a cyclic permutation of a proper subsequence of any of jiI, jIi, iIj and Iij, $X_j X_i w_i$, $X_j w_i X_i$, $X_i w_i X_j$, $w_i X_i X_j \in D$. Therefore, we have

$$\begin{aligned} M\big(z_i\big[x_i, y_i^{(d)}\big]z_i^{-1}\big) &= 1 + M(z_i)\big(M(x_i)M\big(y_i^{(d)}\big) - M\big(y_i^{(d)}\big)M(x_i)\big) \\ &\quad \times M\big(x_i^{-1}\big)M\big(y_i^{(d)^{-1}}\big)M\big(z_i^{-1}\big) \\ &= 1 + M(z_i)(X_i w_i - w_i X_i)M\big(x_i^{-1}\big)M\big(y_i^{(d)^{-1}}\big)M\big(z_i^{-1}\big) \\ &\equiv 1 + X_i w_i - w_i X_i \bmod D. \end{aligned}$$

Hence, by (8.6), $\sum_{i=1}^{r}(X_i w_i - w_i X_i) \in D$. Since the coefficient of X_{iJ} in this sum is $\mu(Ji) - \mu(iJ)$, we have $\mu(Ji) \equiv \mu(iJ) \bmod \Delta(iJ)$, $|iJ| \leq d$. This yields the cyclic symmetry. □

As the linking number is an invariant associated to an Abelian covering of X_L (i.e., Abelian quotient of G_L), Milnor invariants are regarded as invariants associated to nilpotent coverings of X_L (i.e., nilpotent quotients of G_L). For a commutative ring R, let $N_n(R)$ be the group consisting of n by n unipotent upper-triangular matrices. For a multi-index $I = (i_1 \cdots i_n)$ $(n \geq 2)$, we define the map $\rho_I : F \to N_n(\mathbb{Z}/\Delta(I))$ by

$$\rho_I(f) := \begin{pmatrix} 1 & \epsilon(\frac{\partial f}{\partial x_{i_1}}) & \epsilon(\frac{\partial^2 f}{\partial x_{i_1}\partial x_{i_2}}) & \cdots & \epsilon(\frac{\partial^{n-1} f}{\partial x_{i_1}\cdots\partial x_{i_{n-1}}}) \\ 0 & 1 & \epsilon(\frac{\partial f}{\partial x_{i_2}}) & \cdots & \epsilon(\frac{\partial^{r-2} f}{\partial x_{i_2}\cdots\partial x_{i_{n-1}}}) \\ \vdots & & \ddots & \ddots & \vdots \\ & & & 1 & \epsilon(\frac{\partial f}{\partial x_{i_{n-1}}}) \\ 0 & & \cdots & 0 & 1 \end{pmatrix} \bmod \Delta(I)$$

where we set $\epsilon = \epsilon_{\mathbb{Z}[F]}$ for simplicity. By Proposition 8.4, we see that ρ_I is a homomorphism of groups.

Theorem 8.8 (Cf. [Mu2]) (1) *The homomorphism ρ_I factors through the link group G_L. Further it is surjective if $i_1, \ldots, i_{n-1}$ are all distinct.*

(2) *Suppose that $i_1, \ldots, i_{n-1}$ are all distinct. Let $X_I \to X_L$ be the Galois covering corresponding to* $\mathrm{Ker}(\rho_I)$ *whose Galois group* $\mathrm{Gal}(M_I/S^3) = N_n(\mathbb{Z}/\Delta(I))$. *When $\Delta(I) \neq 0$, let $M_I \to S^3$ be the Fox completion of $X_I \to X_L$. Then $M_I \to S^3$ is a Galois covering ramified over the link $K_{i_1} \cup \cdots \cup K_{i_{n-1}}$. For a longitude β_{i_n} of K_{i_n}, one has*

$$\rho_I(\beta_{i_n}) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \overline{\mu}(I) \\ 0 & 1 & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ & & & 1 & 0 \\ 0 & & \cdots & 0 & 1 \end{pmatrix}$$

and hence the following holds:

$$\overline{\mu}(I) = 0 \iff K_{i_n} \text{ is completely decomposed in } M_I \to S^3.$$

Proof (1) First, let us show that ρ_I factors through G_L. Take d such that $d > n$. By Theorem 7.1, it suffices to show that $\rho_I([x_i, y_i^{(d)}]) = I$ $(1 \leq i \leq r)$ and $\rho_I(f) = I$ $(f \in F^{(d)})$. The former can be shown in the manner similar to the proof of (iii) in the proof of Theorem 8.7(1). The latter follows from Proposition 8.5. Next, suppose

that $i_1, \dots, i_{n-1}$ are all distinct. Since

$$\rho_I(x_{i_t}) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & 1 & \cdots & \cdots & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{pmatrix} (t$$

and so $\rho_I(x_{i_1}), \dots, \rho_I(x_{i_{n-1}})$ generate $N_n(\mathbb{Z}/\Delta(I))$, ρ_I is surjective.

(2) By (1), we have $\mathrm{Gal}(M_I/S^3) = N_n(\mathbb{Z}/\Delta(I))$. Since $\rho_I(x_j) = I$ $(j \neq i_1, \dots, i_{n-1})$, $M_I \to S^3$ is a covering ramified over $K_{i_1} \cup \cdots \cup K_{i_{n-1}}$ when $\Delta(I) \neq 0$. For $J = (i_p \cdots i_q)$ $(|J| < n-1)$, $\mu(J; y_{i_n}) \equiv 0 \bmod \Delta(I)$ by definition of $\Delta(I)$. Hence, the latter assertion follows. □

Example 8.9 (1) Let $L = K_1 \cup K_2 \cup K_3$ be the *Borromean rings* (Fig. 8.1).

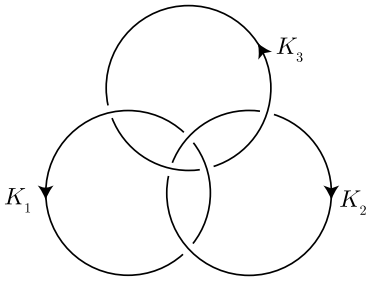


Fig. 8.1

We easily see that $\mu(ij) = \mathrm{lk}(K_i, K_j) = 0$ for any i, j. We also see that $\beta_1 = \alpha_2\alpha_3\alpha_2^{-1}\alpha_3^{-1}$, $\beta_2 = \alpha_3\alpha_1\alpha_3^{-1}\alpha_1^{-1}$ and $\beta_3 = \alpha_1\alpha_2\alpha_1^{-1}\alpha_2^{-1}$. Hence, for instance, we have

$$\begin{aligned} M(y_3) &= (1+X_1)(1+X_2)\big(1 - X_1 + X_1^2 - \cdots\big)\big(1 - X_2 + X_2^2 - \cdots\big) \\ &= 1 + X_1X_2 - X_2X_1 + (\text{terms of degree } \geq 3) \end{aligned}$$

and so $\mu(123) = 1$, $\mu(213) = -1$ and other $\mu(ij3)$'s are all 0. Likewise, we see that $\mu(ijk) = \pm 1$ if ijk is a permutation of 123 and $\mu(ijk) = 0$ otherwise.

Remark 8.10 Milnor invariants can be described in terms of the Massey products in the cohomology of X_L [Tu, P]. This may be seen as a higher order generalization of the cup product interpretation of the linking number (Remark 4.5). It follows immediately from this interpretation that Milnor invariants depends only on the space X_L.

8.3 Pro-l Fox Free Differential Calculus

Let $\mathfrak{R}$ be a compact complete local ring and let $\mathfrak{m}$ be its maximal ideal: $\mathfrak{R} = \varprojlim_i \mathfrak{R}/\mathfrak{m}^i$. Let $\mathfrak{G}$ be a pro-finite group and let $\{\mathfrak{N}_j \mid j \in J\}$ be the set of open normal subgroups of $\mathfrak{G}$. For $i' \geq i$ and $\mathfrak{N}_{j'} \subset \mathfrak{N}_j$, let $\varphi_{(i,j)}^{(i',j')}$ denote the natural ring homomorphism $\mathfrak{R}/\mathfrak{m}^{i'}[\mathfrak{G}/\mathfrak{N}_{j'}] \to \mathfrak{R}/\mathfrak{m}^i[\mathfrak{G}/\mathfrak{N}_j]$. Then $\{\mathfrak{R}/\mathfrak{m}^i[\mathfrak{G}/\mathfrak{N}_j], \varphi_{(i,j)}^{(i',j')}\}$ forms a projective system of finite rings. The projective limit $\varprojlim_{i,j} \mathfrak{R}/\mathfrak{m}^i[\mathfrak{G}/\mathfrak{N}_j]$ is called the *complete group algebra* of $\mathfrak{G}$ over $\mathfrak{R}$ and is denoted by $\mathfrak{R}[[\mathfrak{G}]]$. So $\mathfrak{R}[[\mathfrak{G}]]$ is a pro-finite algebra, in particular, a compact topological algebra. A continuous homomorphism $f : \mathfrak{G} \to \mathfrak{H}$ of pro-finite groups induces a continuous homomorphism $f : \mathfrak{R}[[\mathfrak{G}]] \to \mathfrak{R}[[\mathfrak{H}]]$ of completed group algebras. When $\mathfrak{H}$ is the unit group $\{e\}$, the induced map, denoted by $\epsilon_{\mathfrak{R}[[\mathfrak{G}]]} : \mathfrak{R}[[\mathfrak{G}]] \to \mathfrak{R}$, is called the *augmentation map*, and its kernel $I_{\mathfrak{R}[[\mathfrak{G}]]} := \mathrm{Ker}(\epsilon_{\mathfrak{R}[[\mathfrak{G}]]})$ is called the *augmentation ideal* of $\mathfrak{R}[[\mathfrak{G}]]$.

Let l be a prime number and let $\hat{F}(l)$ be the free pro-l group on the letters $x_1, \ldots, x_r$. Let $\mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle$ be the algebra of non-commutative formal power series of variables $X_1, \ldots, X_r$ over $\mathbb{Z}_l$. Let $\mathfrak{I}$ denote the kernel of the ring homomorphism

$$\mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle \to \mathbb{Z}_l; \quad f(X_1, \ldots, X_r) \mapsto f(0, \ldots, 0).$$

So $\mathfrak{I} = (X_1, \ldots, X_r)$. We give a topology on $\mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle$ so that the two-sided ideals $(l^j, \mathfrak{I}^d)_{j,d\geq 1}$ form a fundamental system of neighborhood of 0, and regard $\mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle$ as a compact $\mathbb{Z}_l$-algebra. Let $M' : F \to \mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle$ be the composite of the Magnus embedding $M : F \hookrightarrow \mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle$ with the inclusion $\mathbb{Z}\langle\langle X_1, \ldots, X_r\rangle\rangle \subset \mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle$. By Proposition 8.5, M' induces a $\mathbb{Z}_l$-algebra homomorphism

$$\mathbb{Z}/l^j\mathbb{Z}\big[F/F^{(d,l)}\big] \longrightarrow \mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle/\big(l^j, \mathfrak{I}^d\big).$$

Taking the projective limit $\varprojlim_{j,d}$ and noting $\hat{F}(l) = \varprojlim_d F/F^{(l,d)}$, we obtain a continuous $\mathbb{Z}_l$-algebra homomorphism

$$\hat{M} : \mathbb{Z}_l[[\hat{F}(l)]] \longrightarrow \mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle.$$

Note that the restriction of $\hat{M}$ to $\mathbb{Z}[F]$ is the Magnus embedding M.

Lemma 8.11 *The map $\hat{M}$ gives an isomorphism of topological $\mathbb{Z}_l$-algebras*

$$\mathbb{Z}_l[[\hat{F}(l)]] \simeq \mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle.$$

$\hat{M}$ is called the pro-l Magnus isomorphism.

Proof Since $(x_i - 1)^d$ converges to 0 in $\mathbb{Z}_l[[\hat{F}(l)]]$ as $d \to \infty$, the map $X_i \to x_i - 1$ gives a continuous homomorphism $\hat{N} : \mathbb{Z}_l\langle\langle X_1, \ldots, X_r\rangle\rangle \to \mathbb{Z}_l[[\hat{F}(l)]]$. Since

$\hat{M}$ and $\hat{N}$ are inverse maps each other, $\hat{M}$ is an isomorphism of topological $\mathbb{Z}_l$-algebras. □

For $\alpha \in \mathbb{Z}_l[[\hat{F}(l)]]$,

$$\hat{M}(\alpha) = \epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(\alpha) + \sum_{\substack{I=(i_1\cdots i_n) \\ 1\le i_1,\ldots,i_n\le r}} \hat{\mu}(I;\alpha)X_I, \quad X_I := X_{i_1}\cdots X_{i_n}$$

is called the *pro-l Magnus expansion* of α and the coefficients $\hat{\mu}(I;\alpha)(\in \mathbb{Z}_l)$ the *pro-l Magnus coefficients*. For the case of pro-l groups, the analogue of Theorem 8.2 follows easily from Lemma 8.11.

Theorem 8.12 ([Ih1, Od]) *For any $\alpha \in \mathbb{Z}_l[[\hat{F}(l)]]$, there exists uniquely $\alpha_j \in \mathbb{Z}_l[[\hat{F}(l)]]$ for each j $(1 \le j \le r)$ such that*

$$\alpha = \epsilon_{\mathbb{Z}_l[[\mathfrak{F}]]}(\alpha) + \sum_{j=1}^{r} \alpha_j(x_j - 1).$$

We call α_j the *pro-l Fox free derivative* of α with respect to x_j and write $\alpha_j = \partial\alpha/\partial x_j$.

Proof Since $\hat{M}(\alpha) = f(X_1,\ldots,X_r) \in \mathbb{Z}_l\langle\langle X_1,\ldots,X_r\rangle\rangle$ is written in a unique manner as

$$f(X_1,\ldots,X_r) = f(0,\ldots,0) + \sum_{j=1}^{n} f_j X_j, \quad f_j \in \mathbb{Z}_l\langle\langle X_1,\ldots,X_r\rangle\rangle,$$

the assertion follows from Lemma 8.11. □

Note that the pro-l Fox derivative $\partial/\partial x_j : \mathbb{Z}_l[[\hat{F}(l)]] \to \mathbb{Z}_l[[\hat{F}(l)]]$ is a continuous map whose restriction to $\mathbb{Z}[F]$ is the Fox derivative. The basic properties of pro-l Fox free derivatives are similar to those of Fox free derivatives given in Proposition 8.3 (we omit the proof):

Proposition 8.13 *The pro-l Fox derivative $\partial/\partial x_j : \mathbb{Z}_l[[\hat{F}(l)]] \to \mathbb{Z}_l[[\hat{F}(l)]]$ satisfies the following properties*:

(1) $\dfrac{\partial x_i}{\partial x_j} = \delta_{ij}$.

(2) $\dfrac{\partial(\alpha+\beta)}{\partial x_j} = \dfrac{\partial\alpha}{\partial x_j} + \dfrac{\partial\beta}{\partial x_j}, \qquad \dfrac{\partial(c\alpha)}{\partial x_j} = c\dfrac{\partial\alpha}{\partial x_j} \quad (\alpha,\beta \in \mathbb{Z}_l[[\hat{F}(l)]], c \in \mathbb{Z}_l)$.

(3) $\dfrac{\partial(\alpha\beta)}{\partial x_j} = \dfrac{\partial\alpha}{\partial x_j}\epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(\beta) + \alpha\dfrac{\partial\beta}{\partial x_j} \quad (\alpha,\beta \in \mathbb{Z}_l[[\hat{F}(l)]])$.

(4) $\dfrac{\partial f^{-1}}{\partial x_j} = -f^{-1}\dfrac{\partial f}{\partial x_j} \quad (f \in \hat{F}(l))$.

We define the higher pro-l Fox derivatives inductively by

$$\frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}} := \frac{\partial}{\partial x_{i_1}} \left(\frac{\partial^{n-1} \alpha}{\partial x_{i_2} \cdots \partial x_{i_n}} \right) \quad (\alpha \in \mathbb{Z}_l[[\hat{F}(l)]])$$

which is also denoted by $D_I(\alpha)$ ($I = (i_1 \cdots i_n)$). The relations of the pro-l Fox derivatives with the pro-l Magnus coefficients and the lower central series are similar to those given in Propositions 8.4 and 8.5 (The proofs are omitted).

Proposition 8.14 *For $\alpha, \beta \in \mathbb{Z}_l[[\hat{F}(l)]]$ and a multi-index I, we have the following*:

(1) $\hat{\mu}(I; \alpha) = \epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(D_I(\alpha))$.

(2) $\hat{\mu}(I; \alpha\beta) = \sum_{I=JK} \hat{\mu}(J; \alpha)\hat{\mu}(K; \beta)$, *where the sum ranges over all pairs of multi-indices (J, K) such that $I = JK$.*

Proposition 8.15 *For $d \geq 2$, the following conditions are equivalent*:

(1) $f \in \hat{F}(l)^{(d)}$

(2) *For any I such that $1 \leq |I| < d$, $\hat{\mu}(I; f) = \epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(D_I(f)) = 0$.*

Namely, we have

$$\hat{F}(l)^{(d)} = \left\{ f \in \hat{F}(l) \mid \deg(\hat{M}(f) - 1) \geq d \right\}.$$

Proposition 8.16 *For multi-indices I, J ($|I|, |J| \geq 1$) and $f \in F$, we have*

$$\hat{\mu}(I; f)\hat{\mu}(J; f) = \sum_{H \in \mathrm{Sh}(I,J)} \hat{\mu}(H; f).$$

Proof Since F is a dense subgroup of $\hat{F}(l)$ and $\hat{\mu}(I; *)$ coincides with $\mu(I; *)$ on F, the assertion follows from Proposition 8.6. □

Remark 8.17 In [Ih2, Appendix], the Fox free derivative is defined for a free profinite group and similar properties are shown.

We fix $m = l^e$ ($e \geq 1$). Taking mod m in the pro-l Magnus isomorphism, we have the *mod m Magnus isomorphism*

$$M_m : \mathbb{Z}/m\mathbb{Z}[[\hat{F}(l)]] \simeq \mathbb{Z}/m\mathbb{Z}\langle\langle X_1, \ldots, X_r \rangle\rangle.$$

For $\alpha \in \mathbb{Z}/m\mathbb{Z}[[\hat{F}(l)]]$, we have the *mod m Magnus expansion*

$$M_m(\alpha) = \epsilon_{\mathbb{Z}/m\mathbb{Z}[[\hat{F}(l)]]}(\alpha) + \sum_I \mu_m(I; \alpha) X_I.$$

The coefficients $\mu_m(I; \alpha)$ are called the *mod m Magnus coefficients*. For a pro-l group $\mathfrak{G}$ and $d \geq 1$, we define a normal subgroup of $\mathfrak{G}$ by

$$\mathfrak{G}_{(m,d)} := \left\{ g \in \mathfrak{G} \mid g - 1 \in (I_{\mathbb{Z}/m\mathbb{Z}[[\mathfrak{G}]]})^d \right\}.$$

Then $\{\mathfrak{G}_{(m,d)}\}_{d\geq 1}$ forms a lower central series of $\mathfrak{G}$, called the *Zassenhaus filtration* of $\mathfrak{G}$. By definition, one sees, for $f \in \hat{F}(l)$ and $d \geq 2$,

$$f \in \hat{F}(l)_{(m,d)} \quad \Leftrightarrow \quad \mu_m(I; f) = 0 \quad \text{for any } I \text{ with } 1 \leq |I| < d. \tag{8.7}$$

8.4 Multiple Residue Symbols

Let l be a given prime number. Let $S = \{p_1, \ldots, p_r\}$ be a set of r distinct prime numbers such that $p_i \equiv 1 \bmod l$ $(1 \leq i \leq r)$. Let $G_S(l) = \pi_1(\mathrm{Spec}(\mathbb{Z}) \setminus S)(l) = \mathrm{Gal}(\mathbb{Q}_S(l)/\mathbb{Q})$, where $\mathbb{Q}_S(l)$ is the maximal pro-l extension of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$. Set $e_S := \max\{e \mid p_i \equiv 1 \bmod l^e (1 \leq i \leq r)\}$ and fix $m = l^e$ $(1 \leq e \leq e_S)$. In the following, we keep the same notation as in Sect. 7.2. Let x_i be the word representing a monodromy τ_i over p_i, $1 \leq i \leq r$, and let $\hat{F}(l)$ be the free pro-l group on $x_1, \ldots, x_r$. By Theorem 7.4, there is a pro-l word $y_i \in \hat{F}(l)$ representing an extension of the Frobenius automorphism over p_i for each i such that

$$G_S(l) = \langle x_1, \ldots, x_r \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 \rangle.$$

Let

$$\hat{M}(y_i) = 1 + \sum \hat{\mu}(Ii) X_I$$

be the pro-l Magnus expansion of y_i. By Proposition 8.14(1), we have

$$\hat{\mu}(Ii) = \epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(D_I(y_i)).$$

We call the coefficient $\hat{\mu}(I)$ the *l-adic Milnor number*. Similarly, let

$$M_m(y_i) = 1 + \sum \mu_m(Ii) X_I$$

be the mod m Magnus expansion of y_i and we call the coefficient

$$\mu_m(I) = \hat{\mu}(I) \bmod m$$

the *mod m Milnor number*. For a multi-index I with $1 \leq |I| \leq l^{e_S}$, let $\Delta_m(I)$ be the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by $\binom{l^{e_S}}{t}$ $(1 \leq t < |I|)$ and $\mu_m(J)$ (J running over cyclic permutations of proper subsequences of I). Then we define the *Milnor $\overline{\mu}_m$-invariant* by

$$\overline{\mu}_m(I) := \mu_m(I) \bmod \Delta_m(I).$$

Theorem 8.18 ([M1, M2, M7]) (1) $\zeta_m^{\mu_m(ij)} = (\frac{p_j}{p_i})_m$ *where ζ_m is the primitive m-th root of unity given in* (7.5).

(2) *If $2 \leq |I| \leq l^{e_S}$, $\overline{\mu}_m(I)$ is an invariant depending only on S and l.*

(3) *Let r be an integer such that $2 \le r \le l^{e_S}$. For multi-indices I, J $(|I| + |J| = r - 1)$ and i $(1 \le i \le r)$, we have*

$$\sum_{H \in \mathrm{PSh}(I,J)} \overline{\mu}_m(Hi) \equiv 0 \bmod \text{g.c.d.}\{\Delta(Hi) | H \in \mathrm{PSh}(I,J)\}.$$

Proof (1) By Theorem 7.4, $\sigma_j \equiv \prod_{i \ne j} \tau_i^{\mathrm{lk}(p_i,p_j)} \bmod G_S(l)^{(2)}$. Therefore, we have

$$\hat{M}(y_j) = 1 + \sum_{i \ne j} \mathrm{lk}(p_i, p_j) X_i + (\text{terms of degree} \ge 2).$$

Hence, $\mu_m(ij) = \mathrm{lk}_m(p_i, p_j)$ and the assertion follows from Theorem 7.4.

(2) We must show that $\overline{\mu}_m(I)$ is independent of the choices of a monodromy over p_i and an extension of the Frobenius automorphism over p_i, namely, independent of the choice of a prime of $\mathbb{Q}_S(l)$ over p_i. Let $I = (i_1 \cdots i_n)$, $2 \le n \le l^{e_S}$. It suffices to show the following:

(i) $\overline{\mu}_m(I)$ is not changed if y_{i_n} is replaced by a conjugate.
(ii) $\overline{\mu}_m(I)$ is not changed if x_i i.e. replaced by a conjugate.
(iii) $\overline{\mu}_m(I)$ is not changed if y_{i_n} is multiplied by a conjugate of $x_i^{p_i-1}[x_i, y_i]$.

Let $I' := (i_1 \cdots i_{n-1})$.

The proofs of (i) and (ii) are similar to those of (i) and (ii) in Proof of Theorem 8.7(2), respectively.

Proof of (iii) Let J be an initial segment of I' and let J' be a subsequence of J. Then as in the proof of (iii) in Proof of Theorem 8.7(2), we have

$$\mu_m\big(J'; [x_i, y_i]\big) \equiv 0 \bmod \Delta_m(I).$$

By definition of $\Delta_m(I)$, we have

$$\begin{aligned}\hat{M}\big(x_i^{p_i-1}\big) &= (1 + X_i)^{p_i-1} \\ &\equiv 1 + (\text{terms of deg} \ge |I|) \bmod \Delta_m(I).\end{aligned}$$

Therefore, $\mu_m(J'; x_i^{p_i-1}[x_i, y_i]) \equiv 0 \bmod \Delta_m(I)$. It follows from this that

$$\mu_m\big(J; x_j^{\varepsilon} x_i^{p_i-1}[x_i, y_i] x_j^{-\varepsilon}\big) \equiv \mu_m \upsilon\big(J; x_i^{p_i-1}[x_i, y_i]\big) \equiv 0 \bmod \Delta_m(I) \ (\varepsilon = \pm 1).$$

Hence we have, by Proposition 8.14(2),

$$\mu_m\big(I'; x_j^{\varepsilon} x_i^{p_i-1}[x_i, y_i] x_j^{-\varepsilon} y_{i_n}\big) \equiv \mu_m(I) \bmod \Delta_m(I).$$

By the same argument as above applied for a tail segment J of I' and a subsequence J' of J, we can show $\mu_m(I'; y_{i_n} x_j^{\varepsilon} x_i^{p_i-1}[x_i, y_i] x_j^{-\varepsilon}) \equiv \mu_m(I'; y_{i_n}) = \mu_m(I) \bmod \Delta_m(I)$.

(3) By Proposition 8.16, this is shown in the same manner as in the proof of Theorem 8.7(3). □

Remark 8.19 Our arithmetic Milnor invariants $\overline{\mu}_m(I)$ do not satisfy the cyclic symmetry in general, since $\mathbb{Q}$ do not contain a primitive l-th root of unity if $l > 2$. When $l = 2$, the cyclic symmetry holds if $|I| = 2$ (quadratic reciprocity law), or if $I = (ijk)$ and ijk are all distinct. (This is Rédei's reciprocity law. See Theorem 8.26).

As in the case of links, Milnor $\overline{\mu}_m$-invariants describe the decomposition law of a prime number in certain nilpotent extensions of $\mathbb{Q}$. Let $I = (i_1 \cdots i_n)$, $2 \leq n \leq l^{es}$ and assume $\Delta_m(I) \neq \mathbb{Z}/m\mathbb{Z}$. Define a group homomorphism $\rho_{(m,I)} : \hat{F}(l) \longrightarrow N_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m(I))$ by

$$\rho_{(m,I)}(f) := \begin{pmatrix} 1 & \epsilon(\frac{\partial f}{\partial x_{i_1}})_m & \epsilon(\frac{\partial^2 f}{\partial x_{i_1}\partial x_{i_2}})_m & \cdots & \epsilon(\frac{\partial^{n-1} f}{\partial x_{i_1}\cdots\partial x_{i_{n-1}}})_m \\ 0 & 1 & \epsilon(\frac{\partial f}{\partial x_{i_2}})_m & \cdots & \epsilon(\frac{\partial^{n-1} f}{\partial x_{i_2}\cdots\partial x_{i_{n-1}}})_m \\ \vdots & & \ddots & \ddots & \vdots \\ & & & 1 & \epsilon(\frac{\partial f}{\partial x_{i_{n-1}}})_m \\ 0 & & \cdots & 0 & 1 \end{pmatrix} \mod \Delta_m(I),$$

where we set for simplicity $\epsilon(\alpha)_m = \epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(\alpha) \bmod m$ for $\alpha \in \mathbb{Z}_p[[\hat{F}(l)]]$.

Theorem 8.20 ([M8]) (1) *The homomorphism $\rho_{(m,I)}$ factors through the Galois group $G_S(l)$. Further it is surjective if $i_1, \ldots, i_{n-1}$ are all distinct.*

(2) *Suppose that $i_1, \ldots, i_{n-1}$ are all distinct. Let $k_{(m,I)}$ be the extension over $\mathbb{Q}$ corresponding to* $\mathrm{Ker}(\rho_{(m,I)})$. *Then $k_{(m,I)}$ is a Galois extension of $\mathbb{Q}$ ramified over $p_{i_1}, \ldots, p_{i_{n-1}}$ with Galois group* $\mathrm{Gal}(k_{(m,I)}/\mathbb{Q}) = N_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m(I))$. *For a Frobenius automorphism σ_{i_n} over p_{i_n}, one has*

$$\rho_{(m,I)}(\sigma_{i_n}) = \begin{pmatrix} 1 & 0 & \ldots & 0 & \overline{\mu}_m(I) \\ 0 & 1 & \ldots & & 0 \\ \vdots & & \ddots & & \vdots \\ & & & 1 & 0 \\ 0 & & \ldots & 0 & 1 \end{pmatrix}$$

and hence the following holds:

$$\overline{\mu}_m(I) = 0 \iff p_{i_n} \text{ is completely decomposed in } k_{(m,I)}/\mathbb{Q}.$$

Proof (1) It suffices to show by Theorem 7.4 that $\rho_{(m,I)}(x_i^{p_i-1}[x_i, y_i]) = I$ $(1 \leq i \leq r)$. This is proved as in the proof of (iii) in Proof of Theorem 8.18(1). The latter is shown in the same manner as in the proof of Theorem 8.8(1). The proof of (2) is also similar to that of Theorem 8.8(2). □

Example 8.21 (The Rédei symbol) Let $l = 2$ and let $S := \{p_1, p_2, p_3\}$ be a triple of distinct prime numbers such that

$$p_i \equiv 1 \bmod 4, \qquad \left(\frac{p_j}{p_i}\right) = 1 \ (1 \le i \ne j \le 3). \tag{8.8}$$

Set $k_i = \mathbb{Q}(\sqrt{p_i})$ $(i = 1, 2)$.

Lemma 8.22 ([Rd2]) (1) *There is* $\alpha_2 \in \mathcal{O}_{k_1}$ *such that the following conditions hold*:

(i) $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha_2) = p_2 z^2$ (z *is a non-zero integer*),
(ii) $\mathrm{N}(d_{k_1(\sqrt{\alpha_2})/k_1}) = p_2$ ($d_{k_1(\sqrt{\alpha_2})/k_1}$ *is the relative discriminant*).

(2) *Let* $\mathfrak{p}_3$ *be a prime ideal of* $\mathcal{O}_{k_1}$ *over* p_3. *For such an* α_2 *as above, one has the Frobenius automorphism* $\sigma_{\mathfrak{p}_3} = (\frac{k_1(\sqrt{\alpha_2})/k_1}{\mathfrak{p}_3}) \in \mathrm{Gal}(k_1(\sqrt{\alpha_2})/k_1)$, *since* $\mathfrak{p}_3$ *is unramified in* $k_1(\sqrt{\alpha_2})/k_1$.

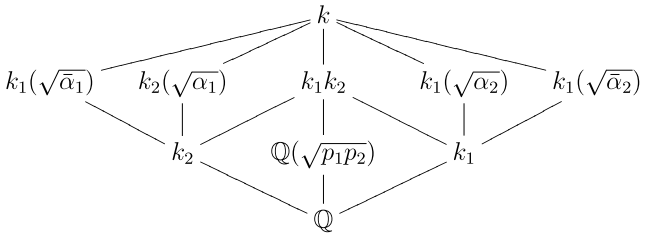
Then $\sigma_{\mathfrak{p}_3}$ *is independent of the choices of* α_2 *and* $\mathfrak{p}_3$.

Remark 8.23 One can find α_2 in Lemma 8.22(1) as follows: By the assumption (8.8) and the computation of the Hilbert symbols, we can find a nontrivial integral solution (x, y, z) of $x^2 - p_1 y^2 - p_2 z^2 = 0$ [Se1, Chap. 3]. Set $\alpha_2 = x + y\sqrt{p_1}$. Then (1) is satisfied. Furthermore, by an elementary argument, we may assume $\mathrm{g.c.d.}(x, y, z) = 1$, $y \equiv 0 \bmod 2$, $x - y \equiv 1 \bmod 4$. We then see that (2) is satisfied.

Definition 8.24 Notation being as in Lemma 8.22, we define the *Rédei symbol* by

$$[p_1, p_2, p_3] = \begin{cases} 1 & \text{if } \sigma_{\mathfrak{p}_3} = \mathrm{id}_{k_1(\sqrt{\alpha_2})}, \\ -1 & \text{otherwise.} \end{cases}$$

We set $\alpha_1 := \alpha_2 + \bar{\alpha}_2 + 2\sqrt{p_2}z = (\sqrt{\alpha_2} + \sqrt{\bar{\alpha}_2})^2 \in k_2$ and $k := k_1 k_2(\sqrt{\alpha_2}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_2})$. Then the extension $k/\mathbb{Q}$ is a Galois extension with Galois group being the dihedral group of order 8 and it is unramified outside p_1, p_2, ∞ by Lemma 8.22(1).[1] The intermediate fields of $k/\mathbb{Q}$ are given as follows:



[1] Recently, F. Amano [Am] characterized Rédei's extension $k/\mathbb{Q}$ as the Galois extension over $\mathbb{Q}$ whose Galois group is the dihedral group of order 8 and which is unramified outside p_1, p_2 and ∞.

Define $s, t \in \mathrm{Gal}(k/\mathbb{Q})$ by

$$\begin{aligned} &s(\sqrt{p_1}) = \sqrt{p_1}, \qquad s(\sqrt{p_2}) = -\sqrt{p_2}, \qquad s(\sqrt{\alpha_2}) = \sqrt{\alpha_2} \\ &t(\sqrt{p_1}) = -\sqrt{p_1}, \qquad t(\sqrt{p_2}) = -\sqrt{p_2}, \qquad t(\sqrt{\alpha_2}) = -\sqrt{\bar{\alpha}_2}. \end{aligned}$$

The Galois group $\mathrm{Gal}(k/\mathbb{Q})$ is then generated by s, t and the relations are given by

$$s^2 = t^4 = 1, \qquad sts^{-1} = t^{-1}.$$

The subfields $k_1(\sqrt{\alpha_2})$ and $\mathbb{Q}(\sqrt{p_1 p_2})$ correspond to the subgroups generated by s and t respectively, and the subfields $k_1 k_2 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ and $k_2(\sqrt{\alpha_1})$ correspond to the subgroups generated by t^2 and st, respectively. By the assumption (8.8), p_3 is completely decomposed in the extension $k_1 k_2/\mathbb{Q}$. Let $\mathfrak{P}_3$ be a prime ideal in $k_1 k_2$ over p_3. Since $\mathfrak{P}_3$ is decomposed in $k/k_1 k_2$ if and only if $\mathfrak{p}_3$ is decomposed in $k_1(\sqrt{\alpha_2})/k_1$, we have, by Definition 8.24,

$$[p_1, p_2, p_3] = \begin{cases} 1 & \sigma_{\mathfrak{P}_3} = \mathrm{id}_k \\ -1 & \text{otherwise.} \end{cases} \tag{8.9}$$

By Theorem 7.4,

$$\begin{aligned} G_S(2) &= \mathrm{Gal}\big(\mathbb{Q}_S(2)/\mathbb{Q}\big) \\ &= \big\langle x_1, x_2, x_3 \mid x_1^{p_1-1}[x_1, y_1] = x_2^{p_2-1}[x_2, y_2] = x_3^{p_3-1}[x_3, y_3] = 1 \big\rangle. \end{aligned}$$

Let $\hat{F}(2)$ be the free pro-2 group on x_1, x_2, x_2 and let $\pi : \hat{F}(2) \to G_S(2)$ be the natural homomorphism. Since $k \subset \mathbb{Q}_S(2)$, we have the natural homomorphism $\psi : G_S(2) \to \mathrm{Gal}(k/\mathbb{Q})$. Let $\varphi := \psi \circ \pi : \hat{F}(2) \to \mathrm{Gal}(k/\mathbb{Q})$. We then see that

$$\varphi(x_1) = st, \qquad \varphi(x_2) = s, \qquad \varphi(x_3) = 1.$$

Therefore, the relations among s, t are equivalent to the following relations:

$$\varphi(x_1)^2 = \varphi(x_2)^2 = 1, \qquad \varphi(x_1 x_2)^4 = 1, \qquad \varphi(x_3) = 1. \tag{8.10}$$

On the other hand, since $\mu_2(ij) = 0$ $(1 \le i, j \le 3)$ by the assumption (8.8), $\overline{\mu}_2(123) = \mu_2(123) \in \mathbb{F}_2$.

Theorem 8.25 ([M1, M2, M7]) *The following equality holds*:

$$(-1)^{\mu_2(123)} = [p_1, p_2, p_3].$$

Proof By (8.9), we have

$$\varphi(y_3) = \begin{cases} 1 & ([p_1, p_2, p_3] = 1), \\ t^2 = \varphi((x_1 x_2)^2) & ([p_1, p_2, p_3] = -1). \end{cases}$$

By (8.10), $\mathrm{Ker}(\varphi)$ is generated as a normal subgroup of $\hat{F}(2)$ by x_1^2, x_2^2, $(x_1x_2)^4$, x_3 and one has

$$\begin{aligned}
&M_2\big(x_1^2\big) = (1+X_1)^2 = 1+X_1^2,\\
&M_2\big(x_2^2\big) = (1+X_2)^2 = 1+X_2^2,\\
&M_2\big((x_1x_2)^4\big) = \big((1+X_1)(1+X_2)\big)^4 \equiv 1 \bmod \deg \geq 4,\\
&M_2(x_3) = 1+X_3.
\end{aligned}$$

Therefore, $\mu_2((1);*)$, $\mu_2((2);*)$ and $\mu_2((12);*)$ take their values 0 on $\mathrm{Ker}(\varphi)$.

If $\varphi(y_3)=1$, $\mu_2(123)=\mu_2((12);y_3)=0$ by $y_3\in\mathrm{Ker}(\varphi)$.

If $\varphi(y_3)=t^2=\varphi((x_1x_2)^2)$, we can write $y_3=(x_1x_2)^2R$, $R\in\mathrm{Ker}(\varphi)$. Then comparing the coefficients of X_1X_2 in $M_2(y_3)=M_2((x_1x_2)^2)M_2(R)$, we have

$$\begin{aligned}
\mu_2(123) &= \mu_2\big((12);y_3\big)\\
&= \mu_2\big((12);(x_1x_2)^2\big)+\mu_2\big((12);R\big)+\mu_2\big((1);(x_1x_2)^2\big)\mu_2\big((2);R\big)\\
&= 1.
\end{aligned}$$

This yields our assertion. □

We may note that Theorem 8.25 implies Lemma 8.22(2). Namely, the mod 2 Milnor invariants are regarded as "universal" invariants determining the Rédei symbol as a special case. We also note that the correspondence

$$s\mapsto\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix},\qquad t\mapsto\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

gives the isomorphism $\mathrm{Gal}(k_{(2,(123))}/\mathbb{Q})\simeq N_3(\mathbb{F}_2)$ and that $\rho_{(2,(123))}$ in Theorem 8.20 is nothing but the composite map $\hat{F}(2)\xrightarrow{\varphi}\mathrm{Gal}(k_{(2,(123))}/\mathbb{Q})\simeq N_3(\mathbb{F}_2)$:

$$\begin{array}{ccccc}
\rho_{(2,(123))}:\hat{F}(2) & \to & \mathrm{Gal}(k_{(2,(123))}/\mathbb{Q}) & \simeq & N_3(\mathbb{F}_2)\\
y_3 & \mapsto & \sigma_{\mathfrak{P}_3} & \mapsto & \begin{pmatrix}1&0&\overline{\mu}_2(123)\\0&1&0\\0&0&1\end{pmatrix}.
\end{array}$$

The following theorem is due to Rédei.

Theorem 8.26 ([Rd2]) *For any permutation ijk of* 123, *one has*

$$[p_i,p_j,p_k]=[p_1,p_2,p_3].$$

By Theorem 8.25 and Theorem 8.26, $\mu_2(ijk)$ is invariant under permutations of ijk.

Example 8.27 D. Vogel [V1, V2] showed that for $S = \{13, 61, 937\}$,

$$\mu_2(ij) = 0 \quad (1 \le i, j \le 3),$$
$$\mu_2(ijk) = 1 \quad (ijk \text{ is a permutation of } 123), \qquad \mu_2(ijk) = 0 \text{ (otherwise)}.$$

In view of Example 8.9, this triple of prime numbers may be called the *Borromean primes* (Fig. 8.2).

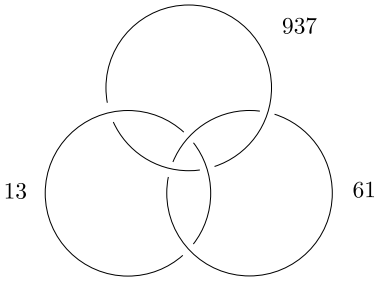


Fig. 8.2

He also computes $\mu_2(ijk)$ for the case that ijk may not be pairwise distinct [ibid].

Remark 8.28 (1) As in the case of links, arithmetic Milnor invariants are described in terms of the Massey products in the étale cohomology of $X_S = \mathrm{Spec}(\mathbb{Z}) \setminus S$ [M7]. This may be seen as a higher order generalization of the relation between the power residue symbol and the cup product [Kc1, 8.11], [M9, 2], [Wl]. In particular, we have an interpretation of the Rédei symbol as a triple Massey product. It follows from this interpretation that arithmetic Milnor invariants depend only on X_S. For an application of Massey products in Galois cohomology to arithmetic, we may also refer to [Sr].

(2) We may define arithmetic Milnor invariants for more general number fields. Let k and S be a pair satisfying the assumption (1), (2) in Remark 7.5. Then by (7.8) we can define the Milnor invariants $\overline{\mu}_m(I)$ in the same manner as above. Suppose $\mu_m(I) = 0$ for any I with $|I| < n$. We then have the arithmetic Milnor invariant $\mu_m(i_1 \cdots i_n) \in \mathbb{Z}/m\mathbb{Z}$ which depends only on S and l, and we may define the *multiple residue symbol* for prime ideals $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_n}$ by

$$[\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_n}] := \zeta_l^{\mu_m(i_1 \cdots i_n)}.$$

This symbol can be regarded as a multiple generalization of the Legendre and the Rédei symbols for a number field.

(3) Recently, F. Amano [Am] constructed a Galois extension $k/\mathbb{Q}$ whose Galois group is $N_4(\mathbb{F}_2)$ of order 64 and which is unramified outside p_1, p_2, p_3, ∞ (under a certain condition), and introduced the 4-th multiple symbol $[p_1, p_2, p_3, p_4] \in \{\pm 1\}$,

where p_1, p_2, p_3, p_4 are distinct prime numbers such that $p_i \equiv 1 \bmod 4$ $(1 \leq i \leq 4)$, $(\frac{p_i}{p_j}) = 1 (1 \leq i \neq j \leq 4)$ and $[p_i, p_j, p_k] = 1 (i, j, k$ are distinct each other). The symbol $[p_1, p_2, p_3, p_4]$ describes the decomposition law of p_4 in $k/\mathbb{Q}$, just like the Rédei symbol. He then showed the equality

$$(-1)^{\mu_2(1234)} = [p_1, p_2, p_3, p_4]$$

which extends Theorem 8.25.

Summary

Fox free derivative	pro-l (pro-finite) Fox free derivative
Milnor numbers $\mu(i_1 \cdots i_n) = \epsilon_{\mathbb{Z}[F]}\left(\frac{\partial y_{i_n}^{(d)}}{\partial x_1 \cdots \partial x_{i_{n-1}}}\right)$	l-adic Milnor numbers $\hat{\mu}(i_1 \cdots i_n) = \epsilon_{\mathbb{Z}_l[[\hat{F}]]}\left(\frac{\partial y_{i_n}}{\partial x_1 \cdots \partial x_{i_{n-1}}}\right)$
Milnor invariants $\overline{\mu}(i_1 \cdots i_n)$	mod m Milnor invariants $\overline{\mu}_m(i_1 \cdots i_n)$

Chapter 9
Alexander Modules and Iwasawa Modules

In this chapter, we shall introduce the differential module for a group homomorphism and show the Crowell exact sequence associated to a short exact sequence of groups. Applying these constructions to the Abelianization map of a link group, we obtain the Alexander module of a link and the exact sequence relating the Alexander module with the link module. The argument is purely group-theoretical and can be applied to pro-finite (pro-l) groups in a parallel manner to obtain the complete differential module and the complete Crowell exact sequence. Applying these constructions to a homomorphism from a Galois group with restricted ramification, we obtain the complete Alexander module for a set of primes and the exact sequence relating the complete Alexander module with a Galois (Iwasawa) module.

9.1 Differential Modules

Let G and H be groups and let $\psi : G \to H$ be a homomorphism. We also denote by the same ψ for the algebra homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ of group algebras induced by ψ.

Definition 9.1 The *ψ-differential module* A_ψ is defined to be the quotient module of the left free $\mathbb{Z}[H]$-module $\bigoplus_{g\in G} \mathbb{Z}[H]\,dg$ on the symbols dg $(g \in G)$ by the left $\mathbb{Z}[H]$-submodule generated by elements of the form $d(g_1g_2) - dg_1 - \psi(g_1)\,dg_2$ $(g_1, g_2 \in G)$:

$$A_\psi := \left(\bigoplus_{g\in G} \mathbb{Z}[H]\,dg\right) \Big/ \left\langle d(g_1g_2) - dg_1 - \psi(g_1)\,dg_2 \ (g_1, g_2 \in G)\right\rangle_{\mathbb{Z}[H]}.$$

By definition, the map $d : G \to A_\psi$ defined by the correspondence $g \mapsto dg$ is a ψ-differential, namely, for $g_1, g_2 \in G$, one has

$$d(g_1g_2) = d(g_1) + \psi(g_1)\,d(g_2)$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_9,

and the following universal property holds:

For any left $\mathbb{Z}[H]$-module A and any ψ-differential $\partial : G \to A$, there exists a unique $\mathbb{Z}[H]$-homomorphism $\varphi : A_\psi \to A$ such that $\varphi \circ d = \partial$. (9.1)

Example 9.2 Let $H = G$ and $\psi = \mathrm{id}_G$. The map $\delta : G \to I_{\mathbb{Z}[G]}$ defined by $\delta(g) := g - 1$ is an id_G-differential as $g_1 g_2 - 1 = g_1 - 1 + g_1(g_2 - 1)$ $(g_1, g_2 \in G)$. Further, δ satisfies the universal property (9.1). (Take φ to be $\varphi(dg) := g - 1$.) Hence, $A_{\mathrm{id}_G} = I_{\mathbb{Z}[G]}$.

We set $N := \mathrm{Ker}(\psi : G \to H)$.

Lemma 9.3 *One has*

$$\mathrm{Ker}\big(\psi : \mathbb{Z}[G] \to \mathbb{Z}[H]\big) = I_{\mathbb{Z}[N]}\mathbb{Z}[G].$$

If ψ is surjective, we have an isomorphism of right $\mathbb{Z}[G]$-modules

$$\mathbb{Z}[G]/I_{\mathbb{Z}[N]}\mathbb{Z}[G] \simeq \mathbb{Z}[H].$$

Here $\mathbb{Z}[G]$ acts on $\mathbb{Z}[H]$ by the right multiplication via ψ.

Proof Since $\psi(I_{\mathbb{Z}[N]}) = 0$, we have $I_{\mathbb{Z}[N]}\mathbb{Z}[G] \subset \mathrm{Ker}(\psi)$. Let $\alpha = \sum_{g\in G} a_g g \in \mathrm{Ker}(\psi)$. Then we have

$$0 = \psi(\alpha) = \sum_{g\in G} a_g \psi(g) = \sum_{h\in\psi(G)} \Big(\sum_{\psi(g)=h} a_g \Big) h$$

and so $\sum_{\psi(g)=h} a_g = 0$ for any $h \in \psi(G)$. Let Ng_h denote the element of $N\backslash G$ corresponding to $h \in \psi(G)$ under the isomorphism $N\backslash G \simeq \psi(G)$. Then we have

$$\begin{aligned}
\sum_{\psi(g)=h} a_g g &= \sum_{g\in Ng_h} a_g (g-1) \\
&= \sum_{n\in N} a_{ng_h} (ng_h - 1) \\
&= \sum_{n\in N} a_{ng_h} \big\{ (n-1)g_h + (g_h - 1) \big\} \\
&= \sum_{n\in N} a_{ng_h} (n-1) g_h \in I_{\mathbb{Z}[N]}\mathbb{Z}[G].
\end{aligned}$$

Hence, $\alpha = \sum_{g\in G} a_g g = \sum_{h\in\psi(G)} (\sum_{\psi(g)=h} a_g g) \in I_{\mathbb{Z}[N]}\mathbb{Z}[G]$. The assertion of the latter half is easily verified. □

In the rest of this section, we assume that ψ is surjective:

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\psi} H \longrightarrow 1 \quad \text{(exact)}.$$

Proposition 9.4 *The correspondence $dg \mapsto g - 1$ gives rise to the following isomorphism of left $\mathbb{Z}[H]$-modules*:

$$A_\psi \simeq I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}.$$

Here $\beta \in \mathbb{Z}[H]$ acts on the right hand side by multiplication by any $\alpha \in \psi^{-1}(\beta)$.

Proof Via ψ, we regard $\mathbb{Z}[H]$ as a right $\mathbb{Z}[G]$-module. By Definition 9.1, we then have

$$A_\psi = \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G}.$$

Hence, by Example 9.2 and Lemma 9.3, we have the following isomorphism of left $\mathbb{Z}[H]$-modules:

$$A_\psi \simeq \left(\mathbb{Z}[G]/I_{\mathbb{Z}[N]}\mathbb{Z}[G]\right) \otimes_{\mathbb{Z}[G]} I_{\mathbb{Z}[G]} \simeq I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}. \qquad \square$$

Next, we suppose that G is a finitely presented group and choose a presentation

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

Then we shall describe the ψ-differential module A_ψ using the Fox free differential calculus. Let F be the free group on $x_1, \ldots, x_r$ and let $\pi : F \to G$ be the natural homomorphism. Consider the $\mathbb{Z}[H]$-homomorphism

$$d_2 : \mathbb{Z}[H]^s \to \mathbb{Z}[H]^r; \qquad (\beta_i) \mapsto \left(\sum_{j=1}^{r} \beta_i (\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right).$$

Theorem 9.5 *The correspondence $dg \mapsto ((\psi \circ \pi)(\partial f/\partial x_j))$ gives rise to an isomorphism of left $\mathbb{Z}[H]$-modules*:

$$A_\psi \simeq \mathrm{Coker}(d_2),$$

where $f \in F$ is any element such that $\pi(f) = g$.

Proof Define the $\mathbb{Z}[H]$-homomorphism $\xi : \bigoplus_{g \in G} \mathbb{Z}[H]\, dg \to \mathrm{Coker}(d_2)$ by

$$\xi(dg) := \left((\psi \circ \pi)\left(\frac{\partial f}{\partial x_j}\right)\right) \bmod \mathrm{Im}(d_2) \quad (\pi(f) = g).$$

Since we have, for $k \in \ker(\pi)$,

$$\psi\left(\pi\left(\frac{\partial (fk)}{\partial x_j}\right)\right) = \psi\left(\pi\left(\frac{\partial f}{\partial x_j} + f\frac{\partial k}{\partial x_j}\right)\right) \equiv \psi\left(\pi\left(\frac{\partial f}{\partial x_j}\right)\right) \bmod \mathrm{Im}(d_2),$$

ξ is independent of the choice of f such that $\pi(f) = g$. For $g_1 = \pi(f_1)$, $g_2 = \pi(f_2) \in G$, by Proposition 8.3(3), we have

$$\begin{aligned}
&\xi\big(d(g_1g_2) - dg_1 - \psi(g_1)\,dg_2\big)\\
&\quad= \psi\left(\pi\left(\frac{\partial(f_1f_2)}{\partial x_j}\right)\right) - \psi\left(\pi\left(\frac{\partial f_1}{\partial x_j}\right)\right) - \psi(g_1)\psi\left(\pi\left(\frac{\partial f_2}{\partial x_j}\right)\right)\\
&\quad= 0
\end{aligned}$$

and so ξ induces the $\mathbb{Z}[H]$-homomorphism

$$\xi : A_\psi \longrightarrow \mathrm{Coker}(d_2).$$

On the other hand, we define $\eta : \mathbb{Z}[H]^r \to A_\psi$ by

$$\eta\big((\alpha_j)\big) := \left[\sum_{j=1}^{r} \alpha_j\, d\pi(x_j)\right].$$

Then we have

$$\eta\left(\psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right)\right) = \left[\sum_{j=1}^{r} \psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right) d\pi(x_j)\right].$$

Let μ be the $\mathbb{Z}[H]$-homomorphism $I_{\mathbb{Z}[G]} \to A_\psi$ induced by the isomorphism in Proposition 9.4. Noting $d\pi(x_j) = \mu(\pi(x_j) - 1)$, we have

$$\begin{aligned}
\sum_{j=1}^{r} \psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right) d\pi(x_j) &= \sum_{j=1}^{r} \psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right)\big(\mu\big(\pi(x_j) - 1\big)\big)\\
&= \mu\left(\sum_{j=1}^{r} \pi\left(\frac{\partial R_i}{\partial x_j}\right)\big(\pi(x_j) - 1\big)\right)\\
&= \mu\left(\pi\left(\sum_{j=1}^{r} \frac{\partial R_i}{\partial x_j}(x_j - 1)\right)\right)\\
&= \mu\big(\pi(R_i - 1)\big)\\
&= 0.
\end{aligned}$$

Hence, η induces the $\mathbb{Z}[H]$-homomorphism

$$\eta : \mathrm{Coker}(d_2) \longrightarrow A_\psi$$

and we have

$$\begin{aligned}
(\eta \circ \xi)(dg) &= \eta\left(\left(\psi\left(\pi\left(\frac{\partial f}{\partial x_j}\right)\right)\right)\right) \quad (\pi(f) = g)\\
&= \psi\left(\sum_{j=1}^{r} \pi\left(\frac{\partial f}{\partial x_j}\right) d\pi(x_j)\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{r} \psi\left(\pi\left(\frac{\partial f}{\partial x_j}\right)\right)\mu\big(\pi(x_j)-1\big) \\
&= \mu\big(\pi(f-1)\big) \\
&= \mu(g-1) \\
&= dg.
\end{aligned}
$$

Hence, $\eta \circ \xi = \mathrm{id}_{A_\psi}$. $\xi \circ \eta = \mathrm{id}_{\mathrm{Coker}(d_2)}$ is also proved easily. □

Corollary 9.6 *The ψ-differential module A_ψ has a free resolution over $\mathbb{Z}[H]$:*

$$\mathbb{Z}[H]^s \xrightarrow{Q_\psi} \mathbb{Z}[H]^r \longrightarrow A_\psi \longrightarrow 0$$

whose presentation matrix Q_ψ is given by

$$Q_\psi := \left((\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right).$$

When G is a free group, we have $A_\psi \simeq \mathbb{Z}[H]^r$.

For a commutative ring Z and a finitely generated Z-module M, let

$$Z^s \xrightarrow{Q} Z^r \longrightarrow M \longrightarrow 0$$

be a free resolution of M over Z with presentation matrix Q. For an $d \geq 0$, we define $E_d(M)$ by the ideal of Z generated by $(r-d)$-minors of Q if $0 < r-d \leq s$, and set $E_d(M) := Z$ if $r-d \leq 0$ and $E_d(M) := 0$ if $r-d > s$. It is known [CF] that $E_d(M)$ is independent of the choice of a free resolution of M and is called the *d-th elementary ideal* (*Fitting ideal*). For the above case that $Z = \mathbb{Z}[H]$ and $M = A_\psi$, $E_d(A_\psi)$ can be defined if H is an Abelian group. Furthermore, if Z is a Noetherian unique factorization domain, a generator of the minimal principal ideal containing $E_d(M)$ (the intersection of all principal ideal containing $E_d(M)$) is defined up to the multiplication by an element of $Z^\times$. We denote such a generator by $\Delta_d(M)$.

Example 9.7 Let $L = K_1 \cup \cdots \cup K_r \subset S^3$ be an r-component link. The link group $G_L = \pi(S^3 \setminus L)$ has a Wirtinger presentation

$$G_L = \langle x_1, \ldots, x_n \mid R_1 = \cdots = R_{n-1} = 1 \rangle$$

with deficiency 1 (Example 2.6). Take a quotient group H of G_L and let $\psi : G_L \to H$ be the natural homomorphism. We call the ψ-differential module A_ψ the *ψ-Alexander module* of L. In particular, consider the Abelianization map $\psi : G_L \to H = G_L^{\mathrm{ab}} = G_L/G_L^{(2)}$. Since H is the free Abelian group generated by the homology classes of meridians α_i of K_i $(1 \leq i \leq r)$, $\mathbb{Z}[H]$ is identified with the Laurent polynomial ring $\Lambda_r := \mathbb{Z}[t_1^{\pm 1}, \ldots, t_r^{\pm 1}]$ where t_i is a variable corresponding

to α_i. The Λ_r-module A_ψ is called the *Alexander module* of L and is denoted by A_L. The presentation matrix Q_L of A_L defined in Corollary 9.6 is then an $(n-1)\times n$ matrix over Λ_r and is called the *Alexander matrix* of L. (It depends on the choice of a Wirtinger presentation). Since Λ_r is a Noetherian unique factorization domain, $E_d(A_L)$ and $\Delta_d(A_L)$ are defined for $d \geq 1$ and are called the *d-th Alexander ideal* and the *d-th Alexander polynomial* of L respectively. Next, consider the homomorphism $\psi : G_L \to H = \mathbb{Z}$ defined by $\psi(\alpha_i) = 1$ $(1 \leq i \leq r)$. Then $\mathbb{Z}[H]$ is identified with the Laurent polynomial ring $\Lambda := \Lambda_1 = \mathbb{Z}[t^{\pm 1}]$ $(t \leftrightarrow 1 \in \mathbb{Z})$ and hence A_ψ becomes a Λ-module. This Λ-module A_ψ is called the *reduced Alexander module* of L and is denoted by A_L^{red}. The presentation matrix Q_L^{red} of A_L^{red} is then an $(n-1)\times n$ matrix over Λ and is called the *reduced Alexander matrix*. When L is a knot K, we have $A_K = A_K^{\mathrm{red}}$. We can regard Λ as a Λ_r-module via the ring homomorphism $\eta : \Lambda_r \to \Lambda$ defined by $\eta(t_i) := t$. We then have $A_L^{\mathrm{red}} = A_L \otimes_{\Lambda_r} \Lambda$. $\eta(E_d(A_L)) = E_d(A_L^{\mathrm{red}})$ and $\eta(\Delta_d(A_L))$ $(d \geq 0)$ are called the *d-th reduced Alexander ideal* and the *d-th reduced Alexander polynomial* of L, respectively.

9.2 The Crowell Exact Sequence

As in Sect. 9.1, suppose that we are given a short exact sequence of groups:

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\psi} H \longrightarrow 1. \tag{9.2}$$

Theorem 9.8 *We have the exact sequence of left $\mathbb{Z}[H]$-modules*

$$0 \longrightarrow N^{\mathrm{ab}} \xrightarrow{\theta_1} A_\psi \xrightarrow{\theta_2} \mathbb{Z}[H] \xrightarrow{\epsilon_{\mathbb{Z}[H]}} \mathbb{Z} \longrightarrow 0.$$

Here N^{ab} is the Abelianization $N/N^{(2)}$ of N, θ_1 is the homomorphism induced by $n \mapsto dn$ $(n \in N)$ and θ_2 is the homomorphism induced by $dg \mapsto \psi(g) - 1$ $(g \in G)$.

This exact sequence is called the *Crowell exact sequence* attached to (9.2) [Cr].

Proof Taking the N-homology sequence of the short exact sequence of left $\mathbb{Z}[N]$-modules

$$0 \longrightarrow I_{\mathbb{Z}[G]} \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon_{\mathbb{Z}[G]}} \mathbb{Z} \longrightarrow 0,$$

we obtain the exact sequence

$$H_1\big(N, \mathbb{Z}[G]\big) \to H_1(N, \mathbb{Z}) \to H_0(N, I_{\mathbb{Z}[G]}) \to H_0\big(N, \mathbb{Z}[G]\big) \to H_0(N, \mathbb{Z}).$$

Here we have

$$\begin{aligned}
&H_0(N, \mathbb{Z}) = \mathbb{Z},\\
&H_0\big(N, \mathbb{Z}[G]\big) = \mathbb{Z}[G]/I_{\mathbb{Z}[N]}\mathbb{Z}[G] \simeq \mathbb{Z}[H] \quad \text{by Lemma 9.3},\\
&H_0(N, I_{\mathbb{Z}[G]}) = I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}\mathbb{Z}[G] \simeq A_\psi \quad \text{by Proposition 9.4},
\end{aligned}$$

$$H_1(N,\mathbb{Z}) = N^{\mathrm{ab}},$$
$$H_1\big(N,\mathbb{Z}[G]\big) = 0.$$

Since

$$H_1\big(N,\mathbb{Z}[G]\big) = H_1\big(G,\mathbb{Z}[G/N]\otimes_{\mathbb{Z}}\mathbb{Z}[G]\big)$$

by Shapiro's lemma and $\mathbb{Z}[G/N]\otimes_{\mathbb{Z}}\mathbb{Z}[G]$ is a free $\mathbb{Z}[G]$-module.

Therefore, we have the exact sequence

$$0 \longrightarrow N^{\mathrm{ab}} \to A_\psi \longrightarrow \mathbb{Z}[H] \xrightarrow{\epsilon_{\mathbb{Z}[H]}} \mathbb{Z} \longrightarrow 0.$$

It is easy to see that each map θ_i is the $\mathbb{Z}[H]$-homomorphism given in the statement. □

Next, suppose that G is a finitely presented group with presentation

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

Let us describe the Crowell exact sequence in terms of the Fox derivatives. Consider the $\mathbb{Z}[H]$-homomorphism

$$d_1 : \mathbb{Z}[H]^r \to \mathbb{Z}[H]; \qquad (\alpha_j) \mapsto \sum_{j=1}^{r} \alpha_j\big(\psi\circ\pi(x_j) - 1\big).$$

First, we see easily $\mathrm{Im}(d_1) = I_{\mathbb{Z}[H]}$. Since we have

$$\begin{aligned}
(d_1\circ d_2)\big((\beta_i)\big) &= d_1\left(\sum_{i=1}^{s}\beta_i\psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right)\right)\\
&= \sum_{j=1}^{r}\left(\sum_{i=1}^{s}\beta_i\psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right)\right)\big(\psi\pi(x_j) - 1\big)\\
&= \sum_{i=1}^{s}\beta_i\psi\left(\pi\left(\sum_{j=1}^{r}\frac{\partial R_i}{\partial x_j}(x_j - 1)\right)\right)\\
&= \sum_{i=1}^{r}\beta_i\psi\big(\pi(R_i - 1)\big)\\
&= 0,
\end{aligned}$$

we have a complex

$$\mathbb{Z}[H]^s \xrightarrow{d_2} \mathbb{Z}[H]^r \xrightarrow{d_1} \mathbb{Z}[H]$$

from which we obtain the exact sequence of left $\mathbb{Z}[H]$-modules

$$0 \to \mathrm{Ker}(d_1)/\mathrm{Im}(d_2) \to \mathrm{Coker}(d_2) \xrightarrow{\overline{d}_1} \mathbb{Z}[H] \xrightarrow{\epsilon_{\mathbb{Z}[H]}} \mathbb{Z} \to 0.$$

We identify $\mathrm{Coker}(d_2)$ with A_ψ by the isomorphism in Theorem 9.5. Since we have

$$d_1\left(\psi\left(\pi\left(\frac{\partial f}{\partial x_i}\right)\right)\right) = \sum_{j=1}^{r} \psi\left(\pi\left(\frac{\partial f}{\partial x_j}\right)\right) d\pi(x_j) = \psi\big(\pi(f) - 1\big),$$

$\overline{d}_1$ coincides with θ_2. Hence, we have

$$N^{\mathrm{ab}} \simeq \mathrm{Ker}(\theta_2) \simeq \mathrm{Ker}(\overline{d}_1) \simeq \mathrm{Ker}(d_1)/\mathrm{Im}(d_2),$$

where $n \bmod N^{(2)}$ is mapped to $(\psi(\pi(\partial f/\partial x_j))) \bmod \mathrm{Im}(d_2)$ $(\pi(f) = g)$.

When G is a free group, the Crowell exact sequence boils down to the following *Blanchfield–Lyndon exact sequence*:

$$0 \longrightarrow N^{\mathrm{ab}} \longrightarrow \mathbb{Z}[H]^r \xrightarrow{d_1} \mathbb{Z}[H] \xrightarrow{\epsilon_{\mathbb{Z}[H]}} \mathbb{Z} \longrightarrow 0.$$

Let $L = K_1 \cup \cdots \cup K_r \subset S^3$ be an r-component link, X_L the link exterior and $G_L = \pi_1(X_L)$ the link group. For the case that $G = G_L$, the Crowell exact sequence has the following topological interpretation as follows. Let $h : X_H \to X_L$ be the covering corresponding to N: $\mathrm{Gal}(X_H/X_L) = H$. We fix a base point $x_0 \in X_L$ such that $G_L = \pi_1(X_L, x_0)$. Fix $y_0 \in h^{-1}(x_0)$ so that $N = \pi_1(X_H, y_0)$. Then we have the exact sequence

$$1 \longrightarrow N \xrightarrow{h_*} G_L \xrightarrow{\psi} H \longrightarrow 1$$

and the attached Crowell exact sequence is given by

$$0 \longrightarrow N^{\mathrm{ab}} \xrightarrow{\theta_1} A_\psi \xrightarrow{\theta_2} \mathbb{Z}[H] \xrightarrow{\epsilon_{\mathbb{Z}[H]}} \mathbb{Z} \longrightarrow 0. \tag{9.3}$$

On the other hand, one has the relative homology sequence for the pair $(X_H, h^{-1}(x_0))$:

$$0 \to H_1(X_H) \xrightarrow{j} H_1\big(X_H, h^{-1}(x_0)\big) \xrightarrow{\delta} H_0\big(h^{-1}(x_0)\big) \xrightarrow{i} H_0(X_H) \to 0. \tag{9.4}$$

The sequences (9.3) and (9.4) are identified as follows.

- The correspondence $1 \mapsto [y_0]$ gives a $\mathbb{Z}$-isomorphism

$$\varphi_0 : \mathbb{Z} \simeq H_0(X_H).$$

Since X_H is arcwise-connected, $[\sigma(y_0)] = [y_0]$ for $\sigma \in H$. Hence, φ_0 is a $\mathbb{Z}[H]$-isomorphism.

- Since $H_0(h^{-1}(x_0)) = \bigoplus_{y\in h^{-1}(x_0)} H_0(\{y\}) = \bigoplus_{y\in h^{-1}(x_0)} \mathbb{Z}$ and the correspondence $\sigma \mapsto \sigma(y_0)$ induces the bijection $H \to h^{-1}(x_0)$, we have a $\mathbb{Z}$-isomorphism

$$\varphi_1 : \mathbb{Z}[H] \simeq H_0\big(h^{-1}(x_0)\big); \qquad \sigma \mapsto \big[\sigma(y_0)\big].$$

  Since we have, for $\sigma_1, \sigma_2 \in H$,

$$\varphi_1(\sigma_1\sigma_2) = \big[\sigma_1\sigma_2(y_0)\big] = \sigma_1\big(\big[\sigma_2(y_0)\big]\big) = \sigma_1\varphi_1(\sigma_2),$$

  φ_1 is a $\mathbb{Z}[H]$-isomorphism.
- For $g = [l] \in G_L$, let $\tilde{l}$ denote a lift of l with starting point y_0. Then $\tilde{l} \in C_1(X_H, h^{-1}(x_0))$ and we have the map

$$\partial : G_L \to H_1\big(X_H, h^{-1}(x_0)\big); \qquad \partial(g) := [\tilde{l}].$$

  We claim that this ∂ is a ψ-differential. In fact, for $g_1 = [l_1]$, $g_2 = [l_2] \in G_L$, let $\tilde{l}_1$, $\tilde{l}_2$ and $\widetilde{l_1 \vee l_2}$ be the lifts of l_1, l_2 and $l_1 \vee l_2$ with starting point y_0 respectively, and let $\tilde{l}_2'$ be the lift of l_2 with starting point $\tilde{l}_1(1)$. Then we have $\partial(g_1g_2) = [\widetilde{l_1 \vee l_2}] = [\tilde{l}_1] + [\tilde{l}_2']$ and $\partial(g_1) + \psi(g_1)\partial(g_2) = [\tilde{l}_1] + \psi(g_1)[\tilde{l}_2] = [\tilde{l}_1] + [\tilde{l}_2']$. Hence $\partial(g_1g_2) = \partial(g_1) + \psi(g_1)\partial(g_2)$. By the universal property of the ψ-differential module, we have a $\mathbb{Z}[H]$-homomorphism

$$\varphi_2 : A_\psi \to H_1\big(X_H, h^{-1}(x_0)\big); \qquad dg \mapsto [\tilde{l}].$$

- By Hurewicz's theorem, one has the $\mathbb{Z}[H]$-isomorphism:

$$\varphi_3 : N^{\mathrm{ab}} \simeq H_1(X_H).$$

  Putting all these together, we have the following diagram:

$$\begin{array}{ccccccccc}
0 \to & N^{\mathrm{ab}} & \xrightarrow{\theta_1} & A_\psi & \xrightarrow{\theta_2} & \mathbb{Z}[H] & \xrightarrow{\epsilon_{\mathbb{Z}[H]}} & \mathbb{Z} & \to 0 \\
& \downarrow \varphi_3 & & \downarrow \varphi_2 & & \downarrow \varphi_1 & & \downarrow \varphi_0 & \\
0 \to & H_1(X_H) & \xrightarrow{j} & H_1(X_H, h^{-1}(x_0)) & \xrightarrow{\delta} & H_0(h^{-1}(x_0)) & \xrightarrow{i} & H_0(X_H) & \to 0
\end{array}$$

  This diagram is commutative.
- The right square: For $\sigma \in H$, $(i \circ \varphi_1)(\sigma) = i([\sigma(y_0)]) = [y_0]$ and $(\varphi_0 \circ \epsilon_{\mathbb{Z}[H]})(\sigma) = \varphi_0(1) = [y_0]$. Hence $i \circ \varphi_1 = \varphi_0 \circ \epsilon_{\mathbb{Z}[H]}$.
- The middle square: Since all maps are $\mathbb{Z}[H]$-homomorphism, it suffices to look at the images of $[dg] \in A_\psi$. One has $(\delta \circ \varphi_2)([dg]) = \delta([\tilde{l}]) = [\tilde{l}(1)] - [\tilde{l}(0)] = [\tilde{l}(1)] - [y_0]$ and $(\varphi_1 \circ \theta_2)([dg]) = \varphi_1(\psi(g) - 1) = [(\psi(g) - 1)(y_0)] = [\tilde{l}(1)] - [y_0]$. Hence $\delta \circ \varphi_2 = \varphi_1 \circ \theta_2$.
- The left square: Let $n = [\tilde{l}] \in N$. Then we have $(\varphi_2 \circ \theta_1)(n) = \varphi_2[dn] = [\tilde{l}]$ and $(j \circ \varphi_3)(n) = j([\tilde{l}]) = [\tilde{l}]$. Hence, $\varphi_2 \circ \theta_1 = j \circ \varphi_3$.

Since φ_0, φ_1 and φ_3 are isomorphisms, φ_2 is isomorphic. Thus, we see that the Crowell exact sequence (9.3) is nothing but the relative homology sequence (9.4).

Example 9.9 Let $\psi : G_L \to H = G_L^{\mathrm{ab}}$ be the Abelianization map. Then X_H is the maximal Abelian covering of X_L (Example 2.13) and the Λ_r-module $N^{\mathrm{ab}} = H_1(X_L^{\mathrm{ab}})$ is called the *link module* of L. If $\psi : G_L \to H = \langle t \rangle = \mathbb{Z}$ is defined by sending each meridian of K_i to t, then X_H is the total linking number covering X_∞ of X_L (Example 2.15) and the Λ-module $N^{\mathrm{ab}} = H_1(X_\infty)$ is called the *reduced link module* of L. When L is a knot K, the link module coincides with the reduced link module and is called the *knot module*. By Theorem 9.8 and $I_\Lambda \simeq \Lambda$, we have a Λ-isomorphism $A_L^{\mathrm{red}} \simeq H_1(X_\infty) \oplus \Lambda$. Hence, we have $E_d(H_1(X_\infty)) = E_{d+1}(A_L^{\mathrm{red}})$ and $\Delta_d(H_1(X_\infty)) = \Delta_{d+1}(A_L^{\mathrm{red}})$ $(d \geq 0)$.

9.3 Complete Differential Modules

Let $\mathfrak{G}$ and $\mathfrak{H}$ be pro-finite groups and let $\psi : \mathfrak{G} \to \mathfrak{H}$ be a continuous homomorphism. Let l a prime number fixed throughout this section. We also denote by the same ψ for the algebra homomorphism $\mathbb{Z}_l[[\mathfrak{G}]] \to \mathbb{Z}_l[[\mathfrak{H}]]$ of complete group algebras over $\mathbb{Z}_l$ induced by ψ.

Definition 9.10 The *complete ψ-differential module* $\mathfrak{A}_\psi$ is defined to be the quotient module of the left free $\mathbb{Z}_l[[\mathfrak{H}]]$-module $\bigoplus_{g \in \mathfrak{G}} \mathbb{Z}_l[[\mathfrak{H}]] dg$ on the symbols dg $(g \in \mathfrak{G})$ by the left $\mathbb{Z}_l[[\mathfrak{H}]]$-submodule generated by elements of the form $d(g_1 g_2) - dg_1 - \psi(g_1)\, dg_2$ $(g_1, g_2 \in \mathfrak{G})$:

$$\mathfrak{A}_\psi := \left(\bigoplus_{g \in \mathfrak{G}} \mathbb{Z}_l[[\mathfrak{H}]]\, dg \right) \Big/ \left\langle d(g_1 g_2) - dg_1 - \psi(g_1)\, dg_2 \ (g_1, g_2 \in \mathfrak{G}) \right\rangle_{\mathbb{Z}_l[[\mathfrak{H}]]}.$$

By definition, the map $d : \mathfrak{G} \to \mathfrak{A}_\psi$ defined by the correspondence $g \mapsto dg$ is a ψ-differential, namely, one has

$$d(g_1 g_2) = d(g_1) + \psi(g_1)\, d(g_2) \quad (g_1, g_2 \in \mathfrak{G})$$

and the following universal property holds.

For any left $\mathbb{Z}_l[[\mathfrak{H}]]$-module $\mathfrak{A}$ and any ψ-differential $\partial : \mathfrak{G} \to \mathfrak{A}$, there exists a unique $\mathbb{Z}_l[[\mathfrak{H}]]$-homomorphism $\varphi : \mathfrak{A}_\psi \to \mathfrak{A}$ such that $\varphi \circ d = \partial$. (9.5)

Example 9.11 Let $\mathfrak{H} = \mathfrak{G}$ and $\psi = \mathrm{id}_{\mathfrak{G}}$. Let $\mathfrak{G} = \varprojlim_i G_i$ (each G_i being a finite group). The map $\delta_i : G_i \to I_{\mathbb{Z}_l[G_1]}$ defined by $\delta_i(g) = g - 1$ is an id_{G_i}-differential (Example 9.2). Taking the projective limit $\varprojlim_i$, we obtain an $\mathrm{id}_{\mathfrak{G}}$-differential $\delta : \mathfrak{G} \to I_{\mathbb{Z}_l[[\mathfrak{G}]]}$ and we easily see that δ satisfies the universal property (9.5) $(\varphi(dg) = g - 1)$.

We set $\mathfrak{N} := \mathrm{Ker}(\psi : \mathfrak{G} \to \mathfrak{H})$.

Lemma 9.12 *One has*

$$\mathrm{Ker}\big(\psi : \mathbb{Z}_l[[\mathfrak{G}]] \to \mathbb{Z}_l[[\mathfrak{H}]]\big) = I_{\mathbb{Z}_l[[\mathfrak{N}]]}\mathbb{Z}_l[[\mathfrak{G}]].$$

If ψ is surjective, we have an isomorphism of right $\mathbb{Z}_l[[\mathfrak{G}]]$-modules:

$$\mathbb{Z}_l[[\mathfrak{G}]]/I_{\mathbb{Z}_l[[\mathfrak{N}]]}\mathbb{Z}_l[[\mathfrak{G}]] \simeq \mathbb{Z}_l[[\mathfrak{H}]].$$

Here $\mathbb{Z}_l[[\mathfrak{G}]]$ acts on $\mathbb{Z}_l[[\mathfrak{H}]]$ by the right multiplication via ψ.

Proof Let $\mathfrak{G} = \varprojlim_i G_i$ and $\mathfrak{H} = \varprojlim_j H_j$ (G_i, H_j being finite groups). Let ψ_{ij} be the composite $G_i \to \mathfrak{G} \xrightarrow{\psi} \mathfrak{H} \to H_j$ and set $N_{ij} := \mathrm{Ker}(\psi_{ij})$. By Lemma 7.1.4, we have $\mathrm{Ker}(\psi_{ij} : \mathbb{Z}_l[G_i] \to \mathbb{Z}_l[H_j]) = I_{\mathbb{Z}_l[N_{ij}]}\mathbb{Z}_l[G_i]$. Taking the projective limit $\varprojlim_{i,j}$, we get our assertion. The assertion of the latter half is easily verified. □

In the rest of this section, we assume that ψ is surjective:

$$1 \longrightarrow \mathfrak{N} \longrightarrow \mathfrak{G} \xrightarrow{\psi} \mathfrak{H} \longrightarrow 1 \quad \text{(exact)}.$$

The following proposition can be proved in the same manner as in Proposition 9.4.

Proposition 9.13 *The correspondence $dg \mapsto g - 1$ induces an isomorphism of left $\mathbb{Z}_l[[\mathfrak{H}]]$-modules*:

$$\mathfrak{A}_\psi \simeq I_{\mathbb{Z}_l[[\mathfrak{G}]]}/I_{\mathbb{Z}_l[[\mathfrak{N}]]}I_{\mathbb{Z}_l[[\mathfrak{G}]]}.$$

Here $\beta \in \mathbb{Z}_l[[\mathfrak{H}]]$ acts on the right hand side by the multiplication by any $\alpha \in \psi^{-1}(\beta)$.

Next, suppose that $\mathfrak{G}$ is a finitely presented pro-l group and choose a presentation

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

Then we shall describe the complete ψ-differential module $\mathfrak{A}_\psi$ using the pro-l Fox free differential calculus. (We would also have a similar description for a pro-finite group with finite presentation using the pro-finite Fox free differential calculus. cf. Remark 8.17). Let $\hat{F}(l)$ be the free pro-l group on $x_1, \ldots, x_r$ and let $\pi : \hat{F}(l) \to \mathfrak{G}$ be the natural homomorphism. Consider the $\mathbb{Z}_l[[\mathfrak{H}]]$-homomorphism

$$d_2 : \mathbb{Z}_l[[\mathfrak{H}]]^s \to \mathbb{Z}_l[[\mathfrak{H}]]^r; \qquad (\beta_i) \mapsto \left(\sum_{i=1}^{s} \beta_i \left(\psi\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)\right)\right)\right).$$

As in Theorem 9.5, we have the following theorem.

Theorem 9.14 ([M2]) *The correspondence* $dg \mapsto ((\psi \circ \pi)(\partial f/\partial x_j))$ *gives rise to an isomorphism of left* $\mathbb{Z}_l[[\mathfrak{H}]]$*-modules*:

$$\mathfrak{A}_\psi \simeq \mathrm{Coker}(d_2),$$

where $f \in \hat{F}(l)$ *is any element such that* $\pi(f) = g$.

Corollary 9.15 *The complete* ψ*-differential module* $\mathfrak{A}_\psi$ *has a free resolution over* $\mathbb{Z}_l[[\mathfrak{H}]]$:

$$\mathbb{Z}_l[[\mathfrak{H}]]^s \xrightarrow{\mathfrak{Q}_\psi} \mathbb{Z}_l[[\mathfrak{H}]]^r \longrightarrow \mathfrak{A}_\psi \longrightarrow 0$$

whose presentation matrix $\mathfrak{Q}_\psi$ *is given by*

$$\mathfrak{Q}_\psi := \left((\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right).$$

When $\mathfrak{G}$ *a free pro-l group, we have* $\mathfrak{A}_\psi \simeq \mathbb{Z}_l[[\mathfrak{H}]]^r$.

When $\mathfrak{H}$ is an Abelian group, the *d-th elementary ideal* (*Fitting ideal*) $E_d(\mathfrak{A}_\psi)$ of $\mathfrak{A}_\psi$ is defined for an integer $d \geq 0$ as in the discrete case.

Example 9.16 Let k be a finite algebraic number field and let S be the finite set of maximal ideals of $\mathcal{O}_k$. Let us take $\mathfrak{G}$ to be a (standard) quotient group of $G_S(k) = \pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$. Choose a quotient $\mathfrak{H}$ of $\mathfrak{G}$ and consider the natural homomorphism $\psi : \mathfrak{G} \to \mathfrak{H}$. The we call the completed ψ-differential module $\mathfrak{A}_\psi$ the *complete* ψ*-Alexander module* of S. When $\mathfrak{H}$ is an Abelian group, we call $E_d(\mathfrak{A}_\psi)$ the *d-th complete* ψ*-Alexander ideal* of S. What $\mathfrak{H}$ we take depends on the situation we are considering. For example, if $\mathfrak{G}$ is the Galois group $G_S(l)$ ($k = \mathbb{Q}$, $S = \{p_1, \ldots, p_r\}$, $p_i \equiv 1 \bmod l$), dealt in Chaps. 7 and 8, we can take $\mathfrak{H}$ to be $\mathbb{Z}/m\mathbb{Z}$ ($m = l^e$, $p_i \equiv 1 \bmod m$) and ψ defined by $\psi(\tau_i) = 1 \bmod m$. For this case, $\mathfrak{A}_\psi$ is a module over $\mathbb{Z}_l[[\mathbb{Z}/m\mathbb{Z}]] = \mathbb{Z}_l[[X]]/((1+X)^m - 1)$. (This will be dealt in Chap. 10). When S contains the set of primes of k over l, we can take $\mathfrak{H}$ to be any $\mathbb{Z}_p$-extension $\mathrm{Gal}(k_\infty/k) = \mathbb{Z}_l$. For this case, $\mathfrak{A}_\psi$ becomes a module over $\hat{\Lambda} := \mathbb{Z}_l[[T]] \simeq \mathbb{Z}_l[[\mathrm{Gal}(k_\infty/k)]]$ by the pro-l Magnus isomorphism. (This case will be dealt in Chaps. 11–13). The algebra $\hat{\Lambda}$ is called the *Iwasawa algebra*. Since $\hat{\Lambda}$ is a Noetherian unique factorization domain, $\Delta_d(\mathfrak{A}_\psi)$ ($d \geq 0$) is defined and in fact we can take $\Delta_d(\mathfrak{A}_\psi)$ to be a polynomial over $\mathbb{Z}_l$ as we will see in Lemma 11.8.

9.4 The Complete Crowell Exact Sequence

In this section, we present a complete version of the Crowell exact sequence in Sect. 9.2 ([Ng, 1], [NSW, Sect. 6]). Suppose that we are given a short exact sequence of profinite groups

$$1 \longrightarrow \mathfrak{N} \longrightarrow \mathfrak{G} \xrightarrow{\psi} \mathfrak{H} \longrightarrow 1. \tag{9.6}$$

Theorem 9.17 *We have the exact sequence of left $\mathbb{Z}_l[[\mathfrak{H}]]$-modules*

$$0 \longrightarrow \mathfrak{N}^{\mathrm{ab}}(l) \xrightarrow{\theta_1} \mathfrak{A}_\psi \xrightarrow{\theta_2} \mathbb{Z}_l[[\mathfrak{H}]] \xrightarrow{\epsilon_{\mathbb{Z}_l[[\mathfrak{H}]]}} \mathbb{Z}_l \longrightarrow 0.$$

Here $\mathfrak{N}^{\mathrm{ab}}(l)$ is the maximal pro-l quotient of the Abelianization $\mathfrak{N}/\mathfrak{N}^{(2)}$ of $\mathfrak{N}$, θ_1 is the homomorphism induced by $n \mapsto dn$ $(n \in \mathfrak{N})$ and θ_2 is the homomorphism induced by $dg \mapsto \psi(g) - 1$ $(g \in \mathfrak{G})$. This exact sequence is called the *complete Crowell exact sequence* attached to (9.6).

Proof Taking the $\mathfrak{N}$-homology sequence of the short exact sequence of left $\mathbb{Z}_l[[\mathfrak{N}]]$-modules

$$0 \longrightarrow I_{\mathbb{Z}_l[[\mathfrak{G}]]} \longrightarrow \mathbb{Z}_l[[\mathfrak{G}]] \xrightarrow{\epsilon_{\mathbb{Z}_l[[\mathfrak{G}]]}} \mathbb{Z}_l \longrightarrow 0,$$

we have the exact sequence

$$\begin{aligned} H_1\big(\mathfrak{N}, \mathbb{Z}_l[[\mathfrak{G}]]\big) \to H_1(\mathfrak{N}, \mathbb{Z}_l) \to H_0(\mathfrak{N}, I_{\mathbb{Z}_l[[\mathfrak{G}]]}) \\ \to H_0\big(\mathfrak{N}, \mathbb{Z}_l[[\mathfrak{G}]]\big) \to H_0(\mathfrak{N}, \mathbb{Z}_l). \end{aligned}$$

Here, we have $H_1(\mathfrak{N}, \mathbb{Z}_l) = \mathfrak{N}^{\mathrm{ab}}(l)$. Since the other terms are described as in the proof of Theorem 9.8 by using Lemma 9.12 and Proposition 9.13, we obtain the desired exact sequence. □

When $\mathfrak{G}$ is a finitely presented pro-l-group, as in the discrete case, we can give a description of the complete Crowell exact sequence in terms of the pro-l Fox derivatives by using Theorem 9.14.

Example 9.18 Let k be a finite algebraic number field and let S be a finite set of maximal ideals of $\mathcal{O}_k$. Let $\mathfrak{G}$ be a quotient of $G_S(k) = \pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$, and we take $\mathfrak{H}$ to be a quotient of $\mathfrak{G}$ and consider the natural homomorphism $\psi : \mathfrak{G} \to \mathfrak{H}$. Then $\mathfrak{N}^{\mathrm{ab}}(l)$ is called the *ψ-Galois module*. When S contains of the set of primes over l and $\mathfrak{H} = \mathbb{Z}_l$, we call the ψ-Galois module $\mathfrak{N}^{\mathrm{ab}}(l)$ the *Iwasawa module*. By Theorem 9.17 and $I_{\hat{\Lambda}} \simeq \hat{\Lambda}$, we have a $\hat{\Lambda}$-isomorphism $\mathfrak{A}_\psi \simeq \mathfrak{N}^{\mathrm{ab}}(l) \oplus \hat{\Lambda}$. Therefore, we have $E_d(\mathfrak{N}^{\mathrm{ab}}(l)) = E_{d+1}(\mathfrak{A}_\psi)$, $\Delta_d(\mathfrak{N}^{\mathrm{ab}}(l)) = \Delta_{d+1}(\mathfrak{A}_\psi)$ $(d \geq 0)$. $\Delta_0(\mathfrak{N}^{\mathrm{ab}}(l))$ may be regarded as an analogue of the Alexander polynomial in the context of Iwasawa theory. Note, however, that we use the term *Iwasawa polynomial* of the $\hat{\Lambda}$-module $\mathfrak{N}^{\mathrm{ab}}(l)$ in a different sense, according to the convention in Iwasawa theory (See Sect. 11.2). If $\mathfrak{N}^{\mathrm{ab}}(l)$ is a finitely generated and torsion $\hat{\Lambda}$-module and has no non-trivial finite $\hat{\Lambda}$-submodule, it is known that $\Delta_0(\mathfrak{N}^{\mathrm{ab}}(l))$ coincides with the Iwasawa polynomial of $\mathfrak{N}^{\mathrm{ab}}(l)$ [Ws, p. 299, Ex. (3)], [MW1, Appendix]. For example, this condition on $\mathfrak{N}^{\mathrm{ab}}(l)$ is known to be satisfied if k is totally real (i.e., any infinite prime of k is a real prime) and $\mathfrak{H}$ is the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of k [Iw2, Theorem 18], [Ws, Theorem 13.31], [NSW, 11.3.2].

Summary

Alexander module A_ψ $\psi : G \to H$	Complete Alexander module $\mathfrak{A}_\psi$ $\psi : \mathfrak{G} \to \mathfrak{H}$
Crowell exact sequence $0 \to N^{\mathrm{ab}} \to A_\psi \to I_{\mathbb{Z}[H]} \to 0$ $(N = \mathrm{Ker}(\psi : G \twoheadrightarrow H))$	Complete Crowell exact sequence $0 \to \mathfrak{N}^{\mathrm{ab}} \to \mathfrak{A}_\psi \to I_{\mathbb{Z}_l[[\mathfrak{H}]]} \to 0$ $(\mathfrak{N} = \mathrm{Ker}(\mathfrak{G} \twoheadrightarrow \mathfrak{H}))$
Link module N^{ab} $(G = G_L, H = \mathbb{Z})$	Iwasawa module $\mathfrak{N}^{\mathrm{ab}}$ $(\mathfrak{G} = G_S(k), \mathfrak{H} = \mathbb{Z}_l)$

Chapter 10
Homology Groups and Ideal Class Groups II—Higher Order Genus Theory

Let M be a rational homology 3-sphere which is a double covering of S^3 ramified over a r-component link and let k be a quadratic extension of $\mathbb{Q}$ ramified over r odd prime numbers. By the genus theory in Chap. 6, the 2-part of the homology group $H_1(M)$ or the 2-part of the narrow ideal class group $H^+(k)$ has the form

$$\bigoplus_{i=1}^{r-1} \mathbb{Z}/2^{a_i}\mathbb{Z} \quad (a_i \geq 1).$$

Since Gauss' time, it has been a problem to determine the 2^d-rank of $H^+(k)$ for $d > 1$ in terms of some quantities related to ramified prime numbers [Y]. Among many works on this problem, L. Rédei ([Rd1], [Rd2, Sect. 4]) expressed the 4-rank in terms of a matrix whose entries are given by the Legendre symbols involving p_i's. According to the analogy between the linking number and the Legendre symbol in Chap. 4, we find that Rédei's matrix is nothing but an arithmetic analogue of the mod 2 linking matrix. Therefore, it would be a natural generalization to express the 2^d-rank in terms of a "higher linking matrix" whose entries are defined by using the Milnor numbers in Chap. 8 (M. Kapranov's question [Kp2]). In this chapter, we shall show such a formula for a link, and then, imitating the method for a link, we shall show a higher order generalization of Gauss' genus theory.

Throughout this chapter, let l be a fixed prime number.

10.1 The Universal Linking Matrix for a Link

Let $L = K_1 \cup \cdots \cup K_r$ be a r-component link in S^3, $X_L := S^3 \setminus \mathrm{int}(V_L)$ the link exterior and $G_L = \pi_1(X_L)$ the link group. By Theorem 7.3, the pro-l completion of G_L has the following presentation:

$$\hat{G}_L(l) = \langle x_1, \ldots, x_r \mid [x_1, y_1] = \cdots = [x_r, y_r] = 1 \rangle,$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_10, © Springer-Verlag London Limited 2012

where x_i is the word representing a meridian of K_i and y_i is the pro-l word representing a longitude of K_i. Let $\hat{\psi} : \hat{G}_L(l) \to \hat{G}_L(l)^{\mathrm{ab}} = \mathbb{Z}_l^r$ be the Abelianization map and let $\hat{A}_L$ be the complete $\hat{\psi}$-differential module. Letting $\tau_i := \hat{\psi}(x_i)$, we have $\mathbb{Z}_l^r = \overline{\langle \tau_1 \rangle} \times \cdots \times \overline{\langle \tau_r \rangle}$, $\overline{\langle \tau_i \rangle} = \mathbb{Z}_l$. By the correspondence $\tau_i \mapsto 1 + T_i$, we identify the complete group algebra $\mathbb{Z}_l[[\hat{G}_L(l)^{\mathrm{ab}}]] = \mathbb{Z}_l[[\mathbb{Z}_l^r]]$ with the commutative formal power series ring $\hat{\Lambda}_r := \mathbb{Z}_l[[T_1, \ldots, T_r]]$, and so $\hat{A}_L$ becomes a $\hat{\Lambda}_r$-module. Let A_L be the Alexander module of L. Then we have $\hat{A}_L = A_L \otimes_{\Lambda_r} \hat{\Lambda}_r$ where we regard Λ_r as a subring of $\hat{\Lambda}_r$ by the correspondence $t_i \mapsto 1 + T_i$. We call $\hat{A}_L$ the *complete Alexander module* of L. Similarly, let $\hat{\psi}^{\mathrm{red}} : \hat{G}_L(l) \to \mathbb{Z}_l$ be the homomorphism defined by $\hat{\psi}^{\mathrm{red}}(x_i) = 1$ $(1 \le i \le r)$ and let $\hat{A}_L^{\mathrm{red}}$ be the complete $\hat{\psi}^{\mathrm{red}}$-differential module. Then $\hat{A}_L^{\mathrm{red}}$ is a module over the Iwasawa algebra $\hat{\Lambda} = \mathbb{Z}_l[[T]]$ and one has $\hat{A}_L^{\mathrm{red}} = A_L^{\mathrm{red}} \otimes_{\Lambda} \hat{\Lambda}$ where A_L^{red} is the reduced Alexander module of L. We call $\hat{A}_L^{\mathrm{red}}$ the *reduced completed Alexander module*. Regarding $\hat{\Lambda}$ as a $\hat{\Lambda}_r$-module by the ring homomorphism $\eta : \hat{\Lambda}_r \to \hat{\Lambda}$ defined by $\eta(T_i) = T$ $(1 \le i \le r)$, one has $\hat{A}_L^{\mathrm{red}} = \hat{A}_L \otimes_{\hat{\Lambda}_r} \hat{\Lambda}$.

Now let

$$\hat{M}(y_i) = 1 + \sum_{\substack{I=(i_1 \cdots i_n) \\ 1 \le i_1, \ldots, i_n \le r}} \hat{\mu}(Ii) X_I, \quad X_I := X_{i_1} \cdots X_{i_n}$$

be the pro-l Magnus expansion of y_i. Here $\hat{\mu}(I)$ is the image of the Milnor number $\mu(I) = \mu^{(d)}(I)$ $(d \ge |I|)$ under the natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_l$.

Definition 10.1 We define the *universal linking matrix* $\hat{Q}_L = (\hat{Q}_L(ij))_{1 \le i,j \le r}$ of L over $\hat{\Lambda}_r$ by

$$\hat{Q}_L(ij) := \begin{cases} -\sum_{n \ge 1} \sum_{\substack{1 \le i_1, \ldots, i_n \le r \\ i_n \ne i}} \hat{\mu}(i_1 \cdots i_n i) T_{i_1} \cdots T_{i_n} & (i = j), \\ \hat{\mu}(ji) T_i + \sum_{n \ge 1} \sum_{1 \le i_1, \ldots, i_n \le r} \hat{\mu}(i_1 \cdots i_n ji) T_i T_{i_1} \cdots T_{i_n} & (i \ne j). \end{cases}$$

We also define the *reduced universal linking matrix* $\hat{Q}_L^{\mathrm{red}}$ of L over $\hat{\Lambda}$ by $\eta(\hat{Q}_L)$.

Theorem 10.2 ([HMM]) *The universal linking matrix $\hat{Q}_L$ gives a presentation matrix for $\hat{A}_L$ over $\hat{\Lambda}_r$:*

$$(\hat{\Lambda}_r)^r \xrightarrow{\hat{Q}_L} (\hat{\Lambda}_r)^r \longrightarrow \hat{A}_L \longrightarrow 0 \quad \text{(exact)}.$$

The reduced universal linking matrix $\hat{Q}_L^{\mathrm{red}}$ gives a presentation matrix for $\hat{A}_L^{\mathrm{red}}$ over $\hat{\Lambda}$.

Proof Since $\hat{A}_L^{\mathrm{red}} = \hat{A}_L \otimes_{\hat{\Lambda}_r} \hat{\Lambda}$, it suffices to show the assertion for $\hat{A}_L$. Let $\hat{F}(l)$ be the free pro-l group on $x_1, \ldots, x_r$ and let $\pi : \hat{F}(l) \to \hat{G}_L(l)$ be the natural homo-

morphism. By Corollary 9.15, we must show

$$(\hat{\psi}\circ\pi)\left(\frac{\partial[x_i,y_i]}{\partial x_j}\right)=\hat{Q}_L(ij),\quad 1\le i,j\le r.$$

Firstly, by Proposition 8.13, we have

$$\frac{\partial[x_i,y_i]}{\partial x_j}=\left(1-x_iy_ix_i^{-1}\right)\delta_{ij}+\left(x_i-[x_i,y_i]\right)\frac{\partial y_i}{\partial x_j}.$$

Next, note that the following diagram is commutative:

$$\begin{array}{ccc}\mathbb{Z}_l[[\hat{F}(l)]] & \xrightarrow{\pi} & \mathbb{Z}_l[[\hat{G}_L(l)]]\\ \hat{M}\downarrow & & \downarrow\hat{\psi}\\ \mathbb{Z}_l\langle\langle X_1,\dots,X_r\rangle\rangle & \xrightarrow{\varphi} & \hat{\Lambda}_r=\mathbb{Z}_l[[T_1,\dots,T_r]]\end{array}$$

where $\varphi:\mathbb{Z}_l\langle\langle X_1,\dots,X_r\rangle\rangle\to\hat{\Lambda}_r=\mathbb{Z}_l[[T_1,\dots,T_r]]$; $X_i\mapsto T_i$, is the Abelianization map and $\hat{M}$ is the pro-l Magnus isomorphism (Lemma 8.11). Since

$$\hat{M}(y_i)=1+\sum_{n\ge1}\sum_{1\le i_1,\dots,i_n\le r}\hat{\mu}(i_1\cdots i_ni)X_{i_1}\cdots X_{i_n},$$

$$\hat{M}\left(\frac{\partial y_i}{\partial x_j}\right)=\hat{\mu}(ji)+\sum_{n\ge1}\sum_{1\le i_1,\dots,i_n\le r}\hat{\mu}(i_1\cdots i_nji)X_{i_1}\cdots X_{i_n},$$

we have

$$\begin{aligned}&(\hat{\psi}\circ\pi)\left(\frac{\partial[x_i,y_i]}{\partial x_j}\right)\\&=(\hat{\psi}\circ\pi)\left(\left(1-x_iy_ix_i^{-1}\right)\delta_{ij}+\left(x_i-[x_i,y_i]\right)\frac{\partial y_i}{\partial x_j}\right)\\&=(\varphi\circ\hat{M})\left(\left(1-x_iy_ix_i^{-1}\right)\delta_{ij}+\left(x_i-[x_i,y_i]\right)\frac{\partial y_i}{\partial x_j}\right)\\&=-\delta_{ij}\sum_{n\ge1}\sum_{1\le i_1,\dots,i_n\le r}\hat{\mu}(i_1\cdots i_ni)T_{i_1}\cdots T_{i_n}\\&\quad+\hat{\mu}(ji)T_i+\sum_{n\ge1}\sum_{1\le i_1,\dots,i_n\le r}\hat{\mu}(i_1\cdots i_nji)T_iT_{i_1}\cdots T_{i_n}\\&=\begin{cases}-\sum_{n\ge1}\sum_{\substack{1\le i_1,\dots,i_n\le r\\ i_n\ne i}}\hat{\mu}(i_1\cdots i_ni)T_{i_1}\cdots T_{i_n} & (i=j),\\ \hat{\mu}(ji)T_i+\sum_{r\ge1}\sum_{1\le i_1,\dots,i_n\le r}\hat{\mu}(i_1\cdots i_nji)T_iT_{i_1}\cdots T_{i_n} & (i\ne j)\end{cases}\end{aligned}$$

which yields the assertion. □

Definition 10.3 For an integer $d \geq 2$, we define the *d-th truncated universal linking matrix* $\hat{Q}_L^{(d)} = (\hat{Q}_L^{(d)}(ij))$ of L by

$$\hat{Q}_L^{(d)}(ij) = \begin{cases} -\sum_{n=1}^{d-1} \sum_{1 \leq i_1, \ldots, i_n \leq r} \hat{\mu}(i_1 \cdots i_n i) T_{i_1} \cdots T_{i_n} & (i = j), \\ \hat{\mu}(ji) T_i + \sum_{n=1}^{d-2} \sum_{\substack{1 \leq i_1, \ldots, i_n \leq r \\ i_n \neq i}} \hat{\mu}(i_1 \cdots i_n j i) T_i T_{i_1} \cdots T_{i_n} & (i \neq j). \end{cases}$$

We also define the *d-th truncated reduced universal linking matrix* $\hat{Q}_L^{\mathrm{red},(d)}$ by $\eta(\hat{Q}_L^{(d)})$.

Example 10.4 For $d = 2$, one has $\hat{Q}_L^{\mathrm{red},(2)} = T \cdot C_L$ where $C_L = (C_L(ij))$ is the *linking matrix* of L defined by

$$C_L(ij) = \begin{cases} -\sum_{j \neq i} \mathrm{lk}(K_j, K_i) & \text{if } i = j, \\ \mathrm{lk}(K_j, K_i) & \text{if } i \neq j. \end{cases}$$

10.2 Higher Order Genus Theory for a Link

Let $\psi_\infty : G_L \to \mathbb{Z}$ be the homomorphism sending all meridians of each component of L to 1 and let X_∞ be the total linking number covering of X_L corresponding to $\mathrm{Ker}(\psi_\infty)$. Let τ be the generator of $\mathrm{Gal}(X_\infty / X_L)$ corresponding to 1 and identify $\mathbb{Z}[\mathrm{Gal}(X_\infty / X_L)]$ with $\Lambda = \mathbb{Z}[t^{\pm 1}]$ by the correspondence $\tau \leftrightarrow t$. For $n \in \mathbb{N}$, let $\psi_n : G_L \to \mathbb{Z}/n\mathbb{Z}$ be the composite of ψ_∞ with the natural map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Let X_n be the n-fold cyclic covering of X_L corresponding to $\mathrm{Ker}(\psi_n)$ and let M_n be the Fox completion of X_n (Example 2.15). We also denote by τ the generator of $\mathrm{Gal}(X_n / X_L)$ corresponding to 1 mod $n \in \mathbb{Z}/n\mathbb{Z}$. We set $\nu_n(t) := t^{n-1} + \cdots + t + 1$. Let $f : M_n \to S^3$ be the ramified covering map. Since the composite of $f_* : H_1(M_n) \to H_1(S^3)$ and the transfer $H_1(S^3) \to H_1(M_n)$ is $\nu_n(\tau)_*$ and $H_1(S^3) = 0$, we can regard $H_1(M_n)$ a module over $\mathcal{O}_n := \Lambda/(\nu_n(t))$. Fix a primitive n-th root of unity $\zeta (\in \overline{\mathbb{Q}})$ so that we identify $\mathcal{O}_n$ with the Dedekind ring $\mathbb{Z}[\zeta]$ by the correspondence t mod $(\nu_n(t)) \mapsto \zeta$.

Theorem 10.5 *We have the following isomorphisms of $\mathcal{O}_n$-modules*:

$$H_1(X_\infty)/\nu_n(t) H_1(X_\infty) \simeq H_1(M_n),$$
$$A_L^{\mathrm{red}}/\nu_n(t) A_L^{\mathrm{red}} \simeq H_1(M_n) \oplus \Lambda/\big(\nu_n(t)\big).$$

Proof Noting the Λ-isomorphism $I_\Lambda \simeq \Lambda$, the Crowell exact sequence (Theorem 9.8) splits and gives the Λ-isomorphism

$$A_L^{\mathrm{red}} \simeq H_1(X_\infty) \oplus \Lambda.$$

By tensoring $\Lambda/(\nu_n(t))$ with the both sides over Λ, the second assertion follows from the first one. Therefore it suffices to show the first isomorphism. The exact sequence of coefficient modules over X_L

$$0 \to \mathbb{Z} \overset{\times \nu_n(t)}{\longrightarrow} \Lambda/\big(t^n - 1\big) \to \Lambda/\big(\nu_n(t)\big) \to 0$$

gives rise to the long exact sequence

$$\cdots \to H_1(X_L) \overset{\mathrm{tr}_1}{\to} H_1(X_n) \to H_1\big(X_L, \Lambda/\big(\nu_n(t)\big)\big) \to H_0(X_L) \overset{\mathrm{tr}_0}{\to} H_0(X_n).$$

Here tr_i $(i = 0, 1)$ denotes the transfer. Since the image of tr_1 is generated by the classes of meridians of components of $f^{-1}(L)$, $\mathrm{Coker}(\mathrm{tr}_1) \simeq H_1(M_n)$. And clearly $\mathrm{tr}_0 : H_0(X_L) = \mathbb{Z} \to H_0(X_n) = \mathbb{Z}$ is the multiplication by n and so injective. Therefore,

$$H_1(M_n) \simeq H_1\big(X_L, \Lambda/\big(\nu_n(t)\big)\big). \tag{10.1}$$

On the other hand, the short exact sequence of chain complexes

$$0 \to C_*(X_\infty) \overset{\nu_n(t)}{\to} C_*(X_\infty) \to C_*(X_\infty) \otimes_\Lambda \Lambda/\big(\nu_n(t)\big) \to 0$$

gives rise to the long exact sequence

$$\cdots \to H_1(X_\infty) \overset{\nu_n(t)}{\to} H_1(X_\infty) \to H_1\big(X_\infty, \Lambda/\big(\nu_n(t)\big)\big) \to H_0(X_\infty) \overset{\nu_n(t)}{\to} H_0(X_\infty).$$

Since $\nu_n(t)$ acts on $H_0(X_\infty) = \mathbb{Z}$ as the multiplication by n, we have

$$H_1\big(X_\infty, \Lambda/\big(\nu_n(t)\big)\big) \simeq H_1(X_\infty)/\nu_n(t)H_1(X_\infty). \tag{10.2}$$

By (10.1) and (10.2), we obtain the first isomorphism. □

In the following, let $n = l$ and set $M := M_l$, $\mathcal{O} := \mathcal{O}_l$ for simplicity. We assume that M is a rational homology 3-sphere. We let $H_1(M)(l)$ denote the l-Sylow subgroup of $H_1(M)$: $H_1(M)(l) = H_1(M) \otimes_{\mathbb{Z}} \mathbb{Z}_l = H_1(M, \mathbb{Z}_l)$. $H_1(M)(l)$ is regarded as a module over $\hat{\mathcal{O}} := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l = \mathbb{Z}_l[\zeta]$. Here $\hat{\mathcal{O}}$ is a complete discrete valuation ring with the maximal ideal $\mathfrak{p} = (\varpi)$, $\varpi := \zeta - 1$, and the residue field $\hat{\mathcal{O}}/\mathfrak{p} = \mathbb{F}_l$. By the genus theory in Sect. 6.2, we have the following.

Lemma 10.6 $\dim_{\mathbb{F}_l} H_1(M)(l) \otimes_{\hat{\mathcal{O}}} \mathbb{F}_l = r - 1$.

Proof By Theorem 6.1, we have

$$H_1(M)/(\tau - 1)H_1(M) \simeq \mathbb{F}_l^{r-1}.$$

Since the left-hand side $= H_1(M) \otimes_{\mathcal{O}} \mathcal{O}/(\zeta - 1) \simeq H_1(M)(l) \otimes_{\hat{\mathcal{O}}} \mathbb{F}_l$, the assertion follows. □

By Lemma 10.6, $H_1(M)(l)$ has the following form as an $\hat{\mathcal{O}}$-module

$$H_1(M)(l) = \bigoplus_{i=1}^{r-1} \hat{\mathcal{O}}/\mathfrak{p}^{a_i} \quad (a_i \geq 1).$$

Hence, the determination of the $\hat{\mathcal{O}}$-module structure of $H_1(M)(l)$ amounts to describing the $\mathfrak{p}^d$-rank

$$e_d := \#\{i \mid a_i \geq d\}$$

for each $d \geq 2$. In the following, we shall describe e_d in terms of the d-th truncated reduced universal linking matrix introduced in Sect. 10.1. We define the *reduced universal linking matrix* $\hat{Q}_L^{\mathrm{red}}(\varpi)$ of L over $\hat{\mathcal{O}}$ by $\hat{Q}_L^{\mathrm{red}}|_{T=\varpi}$ and define the *d-th truncated reduced universal linking matrix* $\hat{Q}_L^{\mathrm{red},(d)}(\varpi)$ of L over $\hat{\mathcal{O}}$ by $\hat{Q}_L^{\mathrm{red},(d)}|_{T=\varpi}$.

Theorem 10.7 ([HMM]) *The matrix $\hat{Q}_L^{\mathrm{red}}(\varpi)$ gives a representation matrix for $H_1(M)(l) \oplus \hat{\mathcal{O}}$ over $\hat{\mathcal{O}}$. For each $d \geq 2$, the matrix $\hat{Q}_L^{\mathrm{red},(d)}(\varpi)$ gives a presentation matrix for $H_1(M)(l)/\mathfrak{p}^d \oplus \hat{\mathcal{O}}/\mathfrak{p}^d$ over $\hat{\mathcal{O}}/\mathfrak{p}^d$.*

Proof By Theorem 10.5, we have the following $\hat{\mathcal{O}}$-isomorphisms:

$$\begin{aligned} H_1(M)(l) &\simeq \big(H_1(X_\infty)/\nu_l(t)H_1(X_\infty)\big) \otimes_{\mathbb{Z}} \mathbb{Z}_l \\ &\simeq H_1(X_\infty) \otimes_{\Lambda} \big((\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_l)/\big(\nu_l(t)\big)\big) \\ &\simeq H_1(X_\infty) \otimes_{\Lambda} \hat{\Lambda}/\big(\nu_l(1+T)\big) \\ &\simeq H_1(X_\infty) \otimes_{\Lambda} \hat{\mathcal{O}}. \end{aligned}$$

Here the last isomorphism is given by the map sending T to ϖ. By tensoring $\hat{\mathcal{O}}$ with $A_L^{\mathrm{red}} \simeq H_1(X_\infty) \oplus \Lambda$ over Λ, we have an $\hat{\mathcal{O}}$-isomorphism $A_L^{\mathrm{red}} \otimes_{\Lambda} \hat{\mathcal{O}} \simeq H_1(M)(l) \oplus \hat{\mathcal{O}}$. Then, by Theorem 10.2, $\mathfrak{Q}_L^{\mathrm{red}}(\varpi)$ gives a representation matrix of $A_L^{\mathrm{red}} \otimes_{\Lambda} \hat{\mathcal{O}}$ over $\hat{\mathcal{O}}$ and hence the first assertion. The second assertion is obtained by taking $\mathrm{mod}\,\mathfrak{p}^d$. □

From Theorem 10.7, we have the following.

Theorem 10.8 ([HMM]) *For each $d \geq 2$, let $\varepsilon_1^{(d)}, \ldots, \varepsilon_{r-1}^{(d)}, \varepsilon_r^{(d)} = 0$, $\varepsilon_i^{(d)} | \varepsilon_{i+1}^{(d)}$, be the elementary divisors of $\hat{Q}_L^{\mathrm{red},(d)}(\varpi)$. Then we have*

$$e_d = \#\big\{i \mid 1 \leq i \leq r, \varepsilon_i^{(d)} \equiv 0 \bmod \mathfrak{p}^d\big\} - 1.$$

Corollary 10.9 *For $d = 2$, we have the following equality*:

$$e_2 = r - 1 - \mathrm{rank}_{\mathbb{F}_l}(C_L \bmod l),$$

where C_L is the linking matrix of L (Example 10.4).

Proof Since $\hat{Q}_L^{\mathrm{red},(2)}(\varpi) = \varpi C_L$, this follows from Theorem 10.8. □

For the case that $r = 2$, we have

$$H_1(M) = \hat{O}/\mathfrak{p}^a \quad (a \geq 1)$$

and so $e_d = 0$ or 1.

Corollary 10.10 *Let $r = 2$. Assume $e_d = 1$ for $d \geq 1$. Then we have the following*:

$$e_{d+1} = 1 \iff \begin{cases} \displaystyle\sum_{n=1}^{d} \sum_{i_1,\ldots,i_{n-1}=1,2} \hat{\mu}(i_1 \cdots i_{n-1} 21)\varpi^n \equiv 0 \bmod \mathfrak{p}^{d+1}, \\ \displaystyle\sum_{n=1}^{d} \sum_{i_1,\ldots,i_{n-1}=1,2} \hat{\mu}(i_1 \cdots i_{n-1} 12)\varpi^n \equiv 0 \bmod \mathfrak{p}^{d+1}. \end{cases}$$

Proof Noting $\hat{Q}_L^{\mathrm{red},(d)}(12)(\varpi) = -\hat{Q}_L^{\mathrm{red},(d)}(11)(\varpi)$ and $\hat{Q}_L^{\mathrm{red},(d)}(21)(\varpi) = -\hat{Q}_L^{\mathrm{red},(d)}(22)(\varpi)$ for $d \geq 1$, we have

$$\begin{aligned} e_{d+1} = 1 &\Leftrightarrow \hat{Q}_L^{\mathrm{red},(d+1)}(\varpi) \equiv O_2 \bmod \mathfrak{p}^{d+1} \\ &\Leftrightarrow \begin{cases} \hat{Q}^{\mathrm{red},(d+1)}(12)(\varpi) \equiv 0 \bmod \mathfrak{p}^{d+1}, \\ \hat{Q}^{\mathrm{red},(d+1)}(21)(\varpi) \equiv 0 \bmod \mathfrak{p}^{d+1}. \end{cases} \end{aligned}$$

From Definition 10.3, the assertion follows. □

Example 10.11 Let $L = K_1 \cup K_2$ be the Whitehead link (Fig. 10.1):

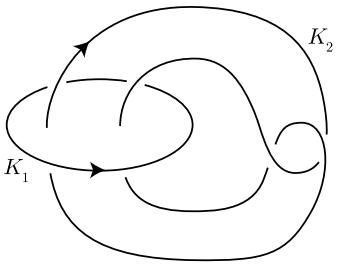


Fig. 10.1

Since $\mu(12) = \mu(21) = 0$, we have $e_2 = 1$ by Corollary 10.10. We note the following formula for a 2-component link ([Mu1, Remark, p. 100], [Fo1, (3.9), p. 555]): For $(i, j) = (1, 2)$ or $(2, 1)$, one has

$$\bar{\mu}(\underbrace{i \cdots i}_{n \text{ times}}\, j) \equiv \binom{\mathrm{lk}(K_1, K_2)}{n} \bmod \Delta(\underbrace{i \cdots i}_{n \text{ times}}\, j), \tag{10.3}$$

Since $\mu(12) = \mu(21) = 0$, we have $\Delta(112) = \Delta(221) = 0$. So, by (10.3), $\mu(112) = \mu(221) = 0$. By the cyclic symmetry (Theorem 8.7(4)), we have $\mu(121) = \mu(212) = 0$. Therefore, by Corollary 10.10, $e_3 = 1$. Since $\Delta(1112) = \Delta(2221) = 0$, we have, by (10.3), $\mu(1112) = \mu(2221) = 0$. The cyclic symmetry yields $\mu(1121) = \mu(2212) = 0$. By the shuffle relation (Theorem 8.7(3)), we have $\mu(1221) + \mu(2121) + \mu(2211) = 0$, $\mu(1212) + \mu(2112) + \mu(1122) = 0$. On the other hand, by [Mu2, Example 2, p. 131] or [Mu1, Theorem 4.1], $\mu(1122) = \mu(2211) = 1$. Therefore, by Corollary 10.10, $e_4 = 0$. Hence we have, as an $\hat{\mathcal{O}}$-module,

$$H_1(M)(l) = \hat{\mathcal{O}}/\mathfrak{p}^3.$$

10.3 The Universal Linking Matrix for Primes

Let $S = \{p_1, \ldots, p_r\}$ be a set of r distinct prime numbers such that $p_i \equiv 1 \bmod l$ $(1 \leq i \leq r)$. In the following, we shall use the same notation as in Sect. 7.2. Let $G_S(l) := \pi_1(\mathrm{Spec}(\mathbb{Z}) \setminus S)(l) = \mathrm{Gal}(\mathbb{Q}_S(l)/\mathbb{Q})$ where $\mathbb{Q}_S(l)$ is the maximal pro-l extension of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$. By Theorem 7.4, the pro-l group $G_S(l)$ has the following presentation

$$G_S(l) = \left\langle x_1, \ldots, x_r \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 \right\rangle,$$

where x_i and y_i represent respectively a monodromy and a Frobenius automorphism over p_i given in (7.5). Let $\psi : G_S(l) \to G_S(l)^{\mathrm{ab}}$ be the Abelianization map and let $\mathfrak{A}_S$ be the complete ψ-differential module. Write $p_i - 1 = m_i q_i$, $(m_i = l^{e_i}, (l, q_i) = 1)$. Then $G_S(l)^{\mathrm{ab}}$ is isomorphic to $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ by class field theory (Example 2.46). By the correspondence $1 \bmod m_i \in \mathbb{Z}/m_i\mathbb{Z} \mapsto 1 + T_i$, the complete group algebra $\mathbb{Z}_l[[G_S(l)^{\mathrm{ab}}]]$ is identified with $\Lambda_S := \hat{\Lambda}_r/((1 + T_1)^{m_1} - 1, \ldots, (1 + T_r)^{m_r} - 1)$ (Lemma 9.12). This also follows from $\mathbb{Z}_p[[G_S(l)^{\mathrm{ab}}]] = \mathbb{Z}_p[G_S(l)^{\mathrm{ab}}] = \mathbb{Z}_p[t_1, \ldots, t_r]/(t_1^{m_1} - 1, \ldots, t^{m_r} - 1)$ and the isomorphism $\mathbb{Z}_p[t_1, \ldots, t_r]/(t_1^{m_1} - 1, \ldots, t^{m_r} - 1) \simeq \hat{\Lambda}_r/((1 + T_1)^{m_1} - 1, \ldots, (1 + T_r)^{m_r} - 1)$ $(t \leftrightarrow 1 + T)$ which is shown by using Lemma 11.8(1). Hence, $\mathfrak{A}_S$ is regarded as a module over Λ_S. We call $\mathfrak{A}_S$ the *complete Alexander module* of S.

Let fix a power m of l such that $p_i \equiv 1 \bmod m$ $(1 \leq i \leq r)$. So m is a divisor of each m_i. Let $\psi^{\mathrm{red}} : G_S(l) \to \mathbb{Z}/m\mathbb{Z}$ be the homomorphism defined by $\psi^{\mathrm{red}}(x_i) = 1 \bmod m$ $(1 \leq i \leq r)$ and let $\mathfrak{A}_S^{\mathrm{red}}$ be the complete ψ^{red}-differential module. By the correspondence $1 \bmod m \mapsto 1 + T$, the complete group algebra $\mathbb{Z}_l[[\mathbb{Z}/m\mathbb{Z}]]$ is identified with $\Lambda_S^{\mathrm{red}} := \hat{\Lambda}/((1 + T)^m - 1)$. Therefore, $\mathfrak{A}_S^{\mathrm{red}}$ is regarded as a module over Λ_S^{red}. We call $\mathfrak{A}_S^{\mathrm{red}}$ the *reduced complete Alexander module* of S. Let $\eta : \Lambda_S \to \Lambda_S^{\mathrm{red}}$ be the homomorphism defined by $\eta(T_i) = T$ and we regard Λ_S^{red} as a Λ_S-module via η. Then one has we have $\mathfrak{A}_S^{\mathrm{red}} = \mathfrak{A}_S \otimes_{\Lambda_S} \Lambda_S^{\mathrm{red}}$.

Let $\hat{\mu}(I)$ denote an l-adic Milnor number of S in Sect. 8.4.

Definition 10.12 We define the *universal linking matrix* $\mathfrak{Q}_S = (\mathfrak{Q}_S(ij))_{1\le i,j\le r}$ of S over Λ_S by

$$\mathfrak{Q}_S(ij) := \begin{cases} T_i^{-1}\big((1+T_i)^{p_i-1}-1\big) \\ \quad -\sum_{n\ge 1}\sum_{\substack{1\le i_1,\dots,i_n\le r \\ i_n\ne i}} \hat{\mu}(i_1\cdots i_n i)T_{i_1}\cdots T_{i_n} \quad (i=j), \\ \hat{\mu}(ji)T_i + \sum_{n\ge 1}\sum_{1\le i_1,\dots,i_n\le r} \hat{\mu}(i_1\cdots i_n ji)T_iT_{i_1}\cdots T_{i_n} \quad (i\ne j), \end{cases}$$

where the power series in the right hand side are regarded as elements in Λ_S (namely, as the images under the natural map $\hat{\Lambda}_r \to \Lambda_S$). We also define the *reduced universal linking matrix* $\mathfrak{Q}_S^{\mathrm{red}}$ of S over Λ_S^{red} by $\eta(\mathfrak{Q}_S)$.

Theorem 10.13 ([M11]) *The universal linking matrix $\mathfrak{Q}_S$ gives a presentation matrix for $\mathfrak{A}_S$ over Λ_S*:

$$(\Lambda_S)^r \xrightarrow{\mathfrak{Q}_S} (\Lambda_S)^r \longrightarrow \mathfrak{A}_S \longrightarrow 0 \quad \text{(exact)}.$$

The reduced universal linking matrix $\mathfrak{Q}_S^{\mathrm{red}}$ gives a presentation matrix for $\mathfrak{A}_S^{\mathrm{red}}$ over Λ_S^{red}.

Proof Since $\mathfrak{A}_S^{\mathrm{red}} = \mathfrak{A}_S \otimes_{\Lambda_S} \Lambda_S^{\mathrm{red}}$, it suffices to show the assertion for $\mathfrak{A}_S$. Let $\hat{F}(l)$ be the free pro-l group on $x_1,\dots,x_r$ and let $\pi : \hat{F}(l) \to G_S(l)$ be the natural homomorphism. By Corollary 9.15, we must show

$$(\psi\circ\pi)\left(\frac{\partial x_i^{p_i-1}[x_i,y_i]}{\partial x_j}\right) = \mathfrak{Q}_S(ij).$$

By Proposition 8.13(3) and $(\psi\circ\pi)(x_i^{p_i-1}) = (1+T_i)^{p_i-1} = 1 \in \Lambda_S$, we have

$$\begin{aligned}&(\psi\circ\pi)\left(\frac{\partial x_i^{p_i-1}[x_i,y_i]}{\partial x_j}\right) \\ &\quad = (\psi\circ\pi)\left(\frac{\partial x_i^{p_i-1}}{\partial x_j}\right) + (\psi\circ\pi)\left(\frac{\partial [x_i,y_i]}{\partial x_j}\right). \end{aligned} \tag{10.4}$$

As for the first term in the right-hand side, using

$$\frac{\partial x_i^{p_i-1}}{\partial x_j} = \frac{x_i^{p_i-1}-1}{x_i-1}\frac{\partial x_i}{\partial x_j},$$

we have

$$(\psi\circ\pi)\left(\frac{\partial x_i^{p_i-1}}{\partial x_j}\right) = T_i^{-1}\big((1+T_i)^{p_i-1}-1\big)\delta_{ij}. \tag{10.5}$$

As for the second term, as in the proof of Theorem 10.2, we have

$$\begin{aligned}(\psi\circ\pi)\left(\frac{\partial[x_i,y_i]}{\partial x_j}\right)&\\ =-\delta_{ij}\sum_{n\geq 1}\sum_{1\leq i_1,\dots,i_n\leq r}\hat{\mu}(i_1\cdots i_n i)T_{i_1}\cdots T_{i_n}&\\ +\hat{\mu}(ji)T_i+\sum_{n\geq 1}\sum_{1\leq i_1,\dots,i_n\leq r}\hat{\mu}(i_1\cdots i_n ji)T_iT_{i_1}\cdots T_{i_n}.&\qquad(10.6)\end{aligned}$$

From (10.4)–(10.6), the assertion follows. □

Definition 10.14 For an integer $d\geq 2$, we define the *d-th truncated universal linking matrix* $\mathfrak{Q}_S^{(d)}=(\mathfrak{Q}_S^{(d)}(ij))$ of S over Λ_S by the following:

$$\mathfrak{Q}_S^{(d)}(ij)=\begin{cases}-\sum_{n=1}^{d-1}\sum_{\substack{1\leq i_1,\dots,i_n\leq r\\ i_n\neq i}}\hat{\mu}(i_1\cdots i_n i)T_{i_1}\cdots T_{i_n} & (i=j),\\ \hat{\mu}(ji)T_i+\sum_{n=1}^{d-2}\sum_{1\leq i_1,\dots,i_n\leq r}\hat{\mu}(i_1\cdots i_n ji)T_iT_{i_1}\cdots T_{i_n} & (i\neq j).\end{cases}$$

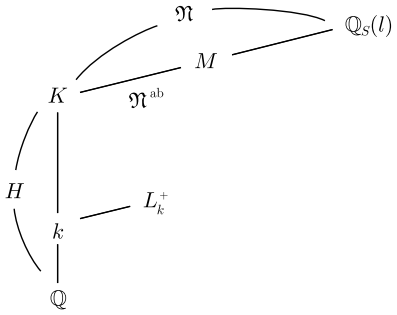
We also define the *d-th truncated reduced universal linking matrix* $\mathfrak{Q}_S^{\mathrm{red},(d)}$ of S over Λ_S^{red} by $\eta(\mathfrak{Q}_S^{(d)})$.

Example 10.15 For $d=2$, one has $\mathfrak{Q}_S^{\mathrm{red},(2)}=T\cdot C_S$ where $C_S=(C_L(ij))$ is the l-adic *linking matrix* of S defined by

$$C_S(ij)=\begin{cases}-\sum_{j\neq i}\hat{\mu}(ji) & \text{if } i=j,\\ \hat{\mu}(ji) & \text{if } i\neq j.\end{cases}$$

10.4 Higher Order Genus Theory for Primes

Let $\mathfrak{N}$ be the kernel of $\psi^{\mathrm{red}}: G_S(l)\to\mathbb{Z}/m\mathbb{Z}$ and let K be the subfield of $\mathbb{Q}_S(l)$ corresponding to $\mathfrak{N}$. Let τ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to 1 mod m. By sending τ to $1+T$, we identify $\mathbb{Z}_l[\mathrm{Gal}(K/\mathbb{Q})]$ with Λ_S^{red}. Let k be the subfield of K of degree l over $\mathbb{Q}$, and we shall also write the same τ for the generator $\tau|_k$ of $\mathrm{Gal}(k/\mathbb{Q})$. Let M be the maximal Abelian subextension of $\mathbb{Q}_S/K$ so that $\mathfrak{N}^{\mathrm{ab}}=\mathrm{Gal}(M/K)$. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathfrak{N}^{\mathrm{ab}}$ by $x^g:=\tilde{g}x\tilde{g}^{-1}$ ($g\in\mathrm{Gal}(K/\mathbb{Q})$, $x\in\mathfrak{N}^{\mathrm{ab}}$) where $\tilde{g}$ denotes a lift of g to $\mathrm{Gal}(M/\mathbb{Q})$. Let L_k^+ be the narrow Hilbert l-class field of k (i.e., the maximal Abelian l-extension of k such that all finite primes of k are unramified) and let $H^+(k)(l)$ be the l-Sylow subgroup of the narrow ideal class group of k. By Artin's reciprocity, $\mathrm{Gal}(L_k^+/k)\simeq H^+(k)(l)$ (Example 2.44 and Sect. 6.1).



As in Sect. 7.2, we choose a prime $\mathfrak{p}_j$ in $\mathbb{Q}_S(l)$ over p_j. Let $I_j = I_j(M/k)$ be the inertia group of $\mathfrak{p}_j|_M$ in M/k $(1 \le j \le r)$. Let $s_j := \tau_j|_M$ so that I_j is generated by s_j^l. Since L_k^+ is the maximal Abelian subextension of M/k unramified over S, we have

$$\begin{aligned} H^+(k)(l) &\simeq \mathrm{Gal}(L_k^+/k) \\ &\simeq \mathrm{Gal}(M/k)/\overline{\langle \mathrm{Gal}(M/k)^{(2)}, I_j \ (1 \le j \le r)\rangle}. \end{aligned} \tag{10.7}$$

Since $s_j|_K = s_1|_K = \tau$, we may write $s_j = u_j s_1, u_j \in \mathfrak{N}^{\mathrm{ab}}$ $(1 \le j \le r)$ where we put $u_1 = 1$. Let $\nu_l(t) := 1 + t + \cdots + t^{l-1}$.

Lemma 10.16 $\mathrm{Gal}(M/k) = \mathfrak{N}^{\mathrm{ab}} I_j, s_j^l = u_j^{\nu_l(\tau)} s_1^l$ $(1 \le j \le r)$.

Proof Since $s_j|_K = \tau$ and $I_j = \langle s_j^l \rangle$, the composite map $I_j \hookrightarrow \mathrm{Gal}(M/k) \to \mathrm{Gal}(M/k)/\mathfrak{N}^{\mathrm{ab}} = \mathrm{Gal}(K/k) = \langle \tau^l \rangle$ is surjective. From this, the first assertion follows. The latter half is verified as follows:

$$\begin{aligned} s_j^l &= (u_j s_1)^l \\ &= u_j s_1 u_j s_1^{-1} s_1^2 \cdots s_1^{l-1} u_j s_1^{-(l-1)} s_1^l \\ &= u_j u_j^{s_1} \cdots u_j^{s_1^{l-1}} s_1^l \\ &= u_j^{\nu_l(\tau)} s_1^l. \end{aligned}$$

□

Lemma 10.17 $\mathrm{Gal}(M/k)^{(2)} = (\tau^l - 1)\mathfrak{N}^{\mathrm{ab}}$.

Proof Let $a, b \in \mathrm{Gal}(M/k)$ and write $a = \alpha x, b = \beta y$ with $x, y \in \mathfrak{N}^{\mathrm{ab}}$ and $\alpha = \tilde{\tau}^{li}$, $\beta = \tilde{\tau}^{lj}$ where $\tilde{\tau}^l$ denotes an extension of τ^l to $\mathrm{Gal}(M/k)$. Then we have

$$\begin{aligned} [a, b] &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^{\alpha} \left(y x^{-1}\right)^{\alpha\beta} \alpha\beta\alpha^{-1} y^{-1} \beta^{-1} \\ &= \left(x^{\alpha}\right)^{1-\beta} \left(y^{\beta}\right)^{\alpha-1}. \end{aligned}$$

Set $\beta = 1$, $\alpha = \tilde{\tau}^l$. Then $y^{\tilde{\tau}^l - 1} = [a, b]$ for any $y \in \mathfrak{N}^{\mathrm{ab}}$. Hence $(\tau^l - 1)\mathfrak{N}^{\mathrm{ab}} \subset \mathrm{Gal}(M/k)^{(2)}$. On the other hand, since $1 - \beta = 1 - \tilde{\tau}^{lj} = (1 - \tilde{\tau}^l)\nu_j(\tilde{\tau}^l)$, $(x^\alpha)^{1-\beta} \in (\tau^l - 1)\mathfrak{N}^{\mathrm{ab}}$. Similarly, we have $(y^\beta)^{\alpha-1} \in (\tau^l - 1)\mathfrak{N}^{\mathrm{ab}}$. Therefore, $[a, b] \in (\tau^l - 1)\mathfrak{N}^{\mathrm{ab}}$. Hence, $\mathrm{Gal}(M/k)^{(2)} \subset (\tau^l - 1)\mathfrak{N}^{\mathrm{ab}}$. □

Let $\mathrm{tr} : H^+(\mathbb{Q}) \to H^+(k)$ denote the homomorphism induced by the extension of ideals of $\mathbb{Q}$ to k. Since $tr \circ \mathrm{N}_{k/\mathbb{Q}} = \nu_l(\tau)$ and $H^+(\mathbb{Q}) = 1$, $H^+(k)(l)$ is regarded as a module over $\hat{\mathcal{O}} := \mathbb{Z}_l[\mathrm{Gal}(k/\mathbb{Q})]/(\nu_l(\tau)) = \Lambda_S^{\mathrm{red}}/(\nu_l(1 + T))$. Fix a primitive l-th root ζ of unity ($\in \overline{\mathbb{Q}}$). Then, by the correspondence $\tau \mapsto \zeta$, $\hat{\mathcal{O}}$ is identified with the complete discrete valuation ring $\mathbb{Z}_l[\zeta]$ whose maximal ideal $\mathfrak{p}$ is generated by $\varpi = \zeta - 1$ and the residue field is $\hat{\mathcal{O}}/\mathfrak{p} = \mathbb{F}_l$.

Theorem 10.18 ([M11]) *We have the following isomorphism of $\hat{\mathcal{O}}$-modules*:

$$\mathfrak{N}^{\mathrm{ab}}/\nu_l(\tau)\mathfrak{N}^{\mathrm{ab}} \simeq H^+(k)(l).$$

Proof By (10.7), Lemma 10.16 and Lemma 10.17, we have the following $\hat{\mathcal{O}}$-isomorphism:

$$\begin{aligned} \mathrm{Gal}(L_k^+/k) &\simeq \mathfrak{N}^{\mathrm{ab}} I_1(M/k)/\overline{\left\langle (\tau^l - 1)\mathfrak{N}^{\mathrm{ab}}, u_j^{\nu_l(\tau)} s_1^l \ (1 \le j \le r) \right\rangle} \\ &\simeq \mathfrak{N}^{\mathrm{ab}}/\nu_l(\tau)\overline{\left\langle (\tau - 1)\mathfrak{N}^{\mathrm{ab}}, u_j \ (2 \le j \le r) \right\rangle}. \end{aligned} \tag{10.8}$$

Replacing k by $\mathbb{Q}$, we have similarly

$$1 = H^+(\mathbb{Q})(l) = \mathfrak{N}^{\mathrm{ab}}/\left\langle (\tau - 1)\mathfrak{N}^{\mathrm{ab}}, u_j \ (2 \le j \le r) \right\rangle. \tag{10.9}$$

By (10.8), (10.9), we obtain the assertion. □

Theorem 10.19 *We have the following $\hat{\mathcal{O}}$-isomorphism*:

$$\mathfrak{A}_S^{\mathrm{red}}/\nu_l(\tau)\mathfrak{A}_S^{\mathrm{red}} = \mathfrak{A}_S^{\mathrm{red}} \otimes_{\Lambda_S^{\mathrm{red}}} \hat{\mathcal{O}} \simeq H^+(k)(l) \oplus \hat{\mathcal{O}}.$$

Proof The complete Crowell exact sequence (Theorem 9.17) yields the exact sequence of Λ_S^{red}-modules:

$$0 \longrightarrow \mathfrak{N}^{\mathrm{ab}} \xrightarrow{\theta_2} \mathfrak{A}_S^{\mathrm{red}} \xrightarrow{\theta_1} I_{\Lambda_S^{\mathrm{red}}} \longrightarrow 0.$$

Tensoring $\hat{\mathcal{O}}$ with the above sequence over Λ_S^{red}, we have, by Theorem 10.18, the following exact sequence of $\hat{\mathcal{O}}$-modules

$$\to \mathrm{Tor}_1(I_{\Lambda_S^{\mathrm{red}}}, \hat{\mathcal{O}}) \xrightarrow{\delta} H^+(k)(l) \to \mathfrak{A}_S^{\mathrm{red}} \otimes_{\Lambda_S^{\mathrm{red}}} \hat{\mathcal{O}} \to I_{\Lambda_S^{\mathrm{red}}} \otimes_{\Lambda_S^{\mathrm{red}}} \hat{\mathcal{O}} \to 0.$$

Let $\xi := (\tau^m - 1)/\nu_l(\tau) = ((1+T)^m - 1)/\nu_l(1+T)$ and consider a cyclic Λ_S^{red}-free resolution of $\hat{\mathcal{O}} = \Lambda_S^{\mathrm{red}}/(\nu_l(\tau))$:

$$\cdots \xrightarrow{\xi} \Lambda_S^{\mathrm{red}} \xrightarrow{\nu_l(\tau)} \Lambda_S^{\mathrm{red}} \xrightarrow{\xi} \Lambda_S^{\mathrm{red}} \xrightarrow{\nu_l(\tau)} \Lambda_S^{\mathrm{red}} \longrightarrow \hat{\mathcal{O}} \longrightarrow 0.$$

From this, we get

$$\begin{aligned} &I_{\Lambda_S^{\mathrm{red}}} \otimes_{\Lambda_S^{\mathrm{red}}} \hat{\mathcal{O}} = \hat{\mathcal{O}}, \\ &\mathrm{Tor}_1(I_{\Lambda_S^{\mathrm{red}}}, \hat{\mathcal{O}}) = \xi \Lambda_S^{\mathrm{red}}/\xi I_{\Lambda_S^{\mathrm{red}}} \simeq \Lambda_S^{\mathrm{red}}/\big(\tau - 1, \nu_l(\tau)\big) \simeq \mathbb{F}_l. \end{aligned}$$

Here we note that $\xi \bmod \xi I_{\Lambda_S^{\mathrm{red}}}$ corresponds to $1 \bmod l$ in the second isomorphism. Since $\theta_1(\tau_1^m - 1) = \nu_l(\tau)\xi, \theta_2(s_1^m) = \tau_1^m - 1$ (where we identify $\mathfrak{A}_S^{\mathrm{red}}$ with $I_{\mathbb{Z}_l[[G_S(l)]]}/I_{\mathbb{Z}_l[[\mathfrak{N}]]}I_{\mathbb{Z}_l[[G_S(l)]]}$), the image of $1 \bmod l$ under the map

$$\delta : \mathbb{F}_l \simeq \mathrm{Tor}_1(I_{\Lambda_S^{\mathrm{red}}}, \hat{\mathcal{O}}) \to \mathfrak{N}^{\mathrm{ab}}/\nu_l(\tau)\mathfrak{N}^{\mathrm{ab}} \simeq H^+(k)(l)$$

is $s_1^m \bmod \nu_l(\tau)\mathfrak{N}^{\mathrm{ab}}$. On the other hand, since the image of $s_1^m \bmod \nu_l(\tau)\mathfrak{N}^{\mathrm{ab}}$ under the isomorphism

$$\mathfrak{N}^{\mathrm{ab}}/\nu_l(\tau)\mathfrak{N}^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{Gal}(M/k)/\big\langle \big(\tau^l - 1\big)\mathfrak{N}^{\mathrm{ab}}, u_j^{\nu_l(\tau)} s_1^l \ (1 \le j \le r) \big\rangle$$

in the proof of Theorem 10.18 is 0, we see that δ is the 0-map. Hence, we have the exact sequence of $\hat{\mathcal{O}}$-modules

$$0 \longrightarrow H^+(k)(l) \longrightarrow \mathfrak{A}_S^{\mathrm{red}}/\nu_l(\tau)\mathfrak{A}_S^{\mathrm{red}} \longrightarrow \hat{\mathcal{O}} \longrightarrow 0$$

which yields the assertion. □

Now by genus theory in Sect. 6.3, we have the following.

Lemma 10.20 $\dim_{\mathbb{F}_l} H^+(k)(l) \otimes_{\hat{\mathcal{O}}} \mathbb{F}_l = r - 1$.

Proof By Theorem 6.4, we have

$$H^+(k)/(\tau - 1)H^+(k) \simeq \mathbb{F}_l^{r-1}.$$

Since the left-hand side $= H^+(k)(l) \otimes_{\hat{\mathcal{O}}} \hat{\mathcal{O}}/(\zeta - 1) \simeq H^+(k)(l) \otimes_{\hat{\mathcal{O}}} \mathbb{F}_l$, the assertion follows. □

By Lemma 10.20, $H^+(k)(l)$ has the following form as an $\hat{\mathcal{O}}$-module:

$$H^+(k)(l) = \bigoplus_{i=1}^{r-1} \hat{\mathcal{O}}/\mathfrak{p}^{a_i} \quad (a_i \ge 1).$$

Hence, the determination of the $\hat{\mathcal{O}}$-module structure of $H^+(k)(l)$ amounts to describing the $\mathfrak{p}^d$-rank

$$e_d := \#\{i \mid a_i \geq d\}$$

for each $d \geq 2$. We define the *reduced universal linking matrix* $\mathfrak{Q}_S^{\mathrm{red}}(\varpi)$ of S over $\hat{\mathcal{O}}$ by $\mathfrak{Q}_S^{\mathrm{red}}|_{T=\varpi}$ and define the *d-th truncated reduced universal linking matrix* $\mathfrak{Q}_S^{\mathrm{red},(d)}(\varpi)$ of S over $\hat{\mathcal{O}}$ by $\mathfrak{Q}_S^{\mathrm{red},(d)}|_{T=\varpi}$. Here, we remark that the term $T^{-1}((1+T)^{p_i-1}-1)$ in the definition of $\mathfrak{Q}_S^{\mathrm{red}}(ii)$ becomes 0 if we set $T=\varpi$. Hence, $\mathfrak{Q}_S^{\mathrm{red}}(\varpi) = \lim_{d\to\infty} \mathfrak{Q}_S^{\mathrm{red},(d)}(\varpi)$.

By Theorem 10.13 and Theorem 10.19, we can show the following Theorem 10.21, Theorem 10.22 and Corollary 10.23 as in proofs of Theorem 10.7, Theorem 10.8 and Corollary 10.9.

Theorem 10.21 ([M11]) *The matrix $\mathfrak{Q}_S^{\mathrm{red}}(\varpi)$ gives a presentation matrix for $H^+(k)(l) \oplus \hat{\mathcal{O}}$ over $\hat{\mathcal{O}}$. For $d \geq 2$, the matrix $\mathfrak{Q}_S^{\mathrm{red},(d)}(\varpi)$ gives a presentation matrix for $H^+(k)(l)/\mathfrak{p}^d \oplus \hat{\mathcal{O}}/\mathfrak{p}^d$ over $\hat{\mathcal{O}}/\mathfrak{p}^d$.*

Theorem 10.22 ([M11]) *For $d \geq 2$, let $\varepsilon_1^{(d)}, \ldots, \varepsilon_{r-1}^{(d)}, \varepsilon_r^{(d)} = 0$ $(\varepsilon_i^{(d)} | \varepsilon_{i+1}^{(d)})$ be the elementary divisors of $\mathfrak{Q}_S^{\mathrm{red},(d)}(\varpi)$. Then we have*

$$e_d = \#\left\{i \mid 1 \leq i \leq r,\ \varepsilon_i^{(d)} \equiv 0 \bmod \mathfrak{p}^d\right\} - 1.$$

For $d=2$, Theorem 10.22 yields the following theorem by Rédei ([Rd1], [Rd2, Sect. 4] deals with the case $l=2$).

Corollary 10.23 *For $d=2$, we have the following equality*:

$$e_2 = r - 1 - \mathrm{rank}_{\mathbb{F}_l}(C_S \bmod l),$$

where C_S is the linking matrix of S (*Example* 10.15).

For the case $r=2$, we have

$$H^+(k)(l) = \hat{\mathcal{O}}/\mathfrak{p}^a \quad (a \geq 1)$$

and so $e_d = 0$ or 1.

Corollary 10.24 *Let $r=2$. Assume $e_d = 1$ for $d \geq 1$. Then we have the following*:

$$e_{d+1} = 1 \iff \begin{cases} \displaystyle\sum_{n=1}^{d} \sum_{i_1,\ldots,i_{n-1}=1,2} \hat{\mu}(i_1 \cdots i_{n-1} 21)\varpi^n \equiv 0 \bmod \mathfrak{p}^{d+1}, \\ \displaystyle\sum_{n=1}^{d} \sum_{i_1,\ldots,i_{n-1}=1,2} \hat{\mu}(i_1 \cdots i_{n-1} 12)\varpi^n \equiv 0 \bmod \mathfrak{p}^{d+1}. \end{cases}$$

Proof Noting $\mathfrak{Q}_S^{\mathrm{red},(d)}(12)(\varpi) = -\mathfrak{Q}_S^{\mathrm{red},(d)}(11)(\varpi), \mathfrak{Q}_L^{\mathrm{red},(d)}(21)(\varpi) = -\mathfrak{Q}_L^{\mathrm{red},(d)}(22)(\varpi)$ for $d \geq 1$, the assertion is shown in the same way as in the proof of Corollary 10.10. □

Example 10.25 Let $l = 2$, $r = 3$, $(p_1, p_2, p_3) = (13, 41, 937)$, and $k = \mathbb{Q}(\sqrt{13 \cdot 41 \cdot 937})$. We then have by Example 8.21

$$\begin{cases} \mu_2(ij) = 0 & (1 \leq i, j \leq 3), \\ \mu_2(ijk) = 1 & (ijk \text{ is a permutation of } 123), \\ \mu_2(ijk) = 0 & (\text{otherwise}). \end{cases}$$

Furthermore, we see that $\mu_4(ij) = 0$ if $i \neq j$, since $p_j^{(p_i-1)/4} \equiv 1 \bmod p_i$. Therefore, we have $\mathfrak{Q}_S^{\mathrm{red},(2)}(-2) \equiv O_3 \bmod 4$ $(\varpi = -2)$ and

$$\mathfrak{Q}_S^{\mathrm{red},(3)}(-2) \equiv \begin{pmatrix} 0 & 4 & 4 \\ 4 & 0 & 4 \\ 4 & 4 & 0 \end{pmatrix} \sim \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix} \bmod 8$$

and so $e_2 = 2, e_3 = 0$. Hence, $H^+(k)(2) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Sections 10.1 and 10.2 are an application of number theoretic method to link theory, while Sects. 10.3 and 10.4 may be regarded as an application of the knot theoretic idea to number theory.

Summary

Higher order genus theory for a link	Higher order genus theory for primes
$H_1(M)(l) = \bigoplus_{i=1}^{r-1} \hat{\mathcal{O}}/\mathfrak{p}^{a_i}$	$H^+(k)(l) = \bigoplus_{i=1}^{r-1} \hat{\mathcal{O}}/\mathfrak{p}^{a_i}$
Description of $\mathfrak{p}^d$-rank by the Milnor numbers	Description of $\mathfrak{p}^d$-rank by the l-adic Milnor numbers

Chapter 11
Homology Groups and Ideal Class Groups III—Asymptotic Formulas

As we discussed in Chap. 9, there is a group-theoretic analogy between the knot module associated to the infinite cyclic covering of a knot exterior and the Iwasawa module associated to the cyclotomic $\mathbb{Z}_p$-extension of number fields. Base on this analogy, there are found close parallels between the Alexander–Fox theory and Iwasawa theory. In this chapter, as a consequence of this analogy, we shall show asymptotic formulas on the orders of the homology groups (p-ideal class groups) of cyclic ramified coverings (extensions). Up to till Chap. 10, we have dealt mainly with tame quotients of the Galois group $G_S(k) = \pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$. In the rest of this book, we shall deal with quotient groups of $G_S(k)$ with wild ramification and investigate analogies with knot groups.

As for the basic materials on Iwasawa theory, we refer to [Ws, Ln2].

11.1 The Alexander Polynomial and Homology Groups

Let K be a knot in a rational homology 3-sphere M. Let α a meridian of K, $X_K := M \setminus \mathrm{int}(V_K)$ the knot exterior and $G_K = \pi_1(X_K)$. In the following, we assume that K is null-homologous in M, namely, there is an oriented surface $\Sigma \subset M$ such that $\partial \Sigma = K$. Then we have

$$H_1(X_K) \simeq \langle [\alpha] \rangle \oplus H_1(M), \quad \langle [\alpha] \rangle \simeq \mathbb{Z}.$$

In fact, if we denote by $\varphi(c)$ the intersection number (with signature) of 1-cycle $c \in Z_1(X_K)$ with Σ, φ defines a surjective homomorphism $H_1(X_K) \to \mathbb{Z}$ with $\varphi(\alpha) = 1$. Therefore, we have $H_1(X_K) = \langle [\alpha] \rangle \oplus \mathrm{Ker}(\varphi)$, $\langle [\alpha] \rangle \simeq \mathbb{Z}$. By the relative homology exact sequence and the excision, we have $H_1(X_K) \simeq \langle [\alpha] \rangle \oplus H_1(X_K, \partial V_K) \simeq \langle [\alpha] \rangle \oplus H_1(M, V_K) \simeq \langle [\alpha] \rangle \oplus H_1(M)$. Hence, we have $\mathrm{Ker}(\varphi) \simeq H_1(M)$.

Let X_∞ be the infinite cyclic covering of X_K corresponding to the kernel of the natural projection $\psi : G_K \to H_1(X_K) \to \langle [\alpha] \rangle = \mathbb{Z}$, and let τ be a genera-

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_11, © Springer-Verlag London Limited 2012

tor of $\mathrm{Gal}(X_\infty/X_K)$ corresponding to $1 \in \mathbb{Z}$. Let $\Lambda := \mathbb{Z}[t^{\pm 1}] = \mathbb{Z}[\mathrm{Gal}(X_\infty/X_K)]$ $(t \leftrightarrow \tau)$. For $n \in \mathbb{N}$, let X_n be the cyclic subcovering of $X_\infty \to X_K$ of degree n, and let M_n be the Fox completion of X_n.

$$\begin{array}{ccc} & & X_\infty \\ & & \downarrow \\ \mathbb{Z}/n\mathbb{Z} & \left\{ \begin{array}{cc} X_n & \subset M_n \\ \downarrow & \downarrow \end{array} \right. \\ & X_K & \subset M \end{array}$$

Proposition 11.1 *We have the following isomorphism*:

$$H_1(M_n) \simeq H_1(X_\infty)/\big(t^n - 1\big)H_1(X_\infty) \quad (n \geq 1).$$

Proof By the Wang exact sequence $H_1(X_\infty) \overset{t^n-1}{\to} H_1(X_\infty) \to H_1(X_n) \to \mathbb{Z} \to 0$, we have

$$H_1(X_n) \simeq H_1(X_\infty)/\big(t^n - 1\big)H_1(X_\infty) \oplus \mathbb{Z}.$$

Here $1 \in \mathbb{Z}$ corresponds to a lift $[\tilde{\alpha}^n]$ of $[\alpha^n]$ to X_n (Since the image of α^n in $\mathrm{Gal}(X_n/X_K) \simeq \mathbb{Z}/n\mathbb{Z}$ is 0, α^n can be lifted to X_n). Since $H_1(M_n) = H_1(X_n)/\langle[\tilde{\alpha}^n]\rangle$, we obtain our assertion. □

Let $G_K = \langle x_1, \ldots, x_m \mid R_1 = \cdots = R_{m-1} = 1\rangle$ be a presentation of G_K (Example 2.6) and let $\pi : F(x_1, \ldots, x_m) \to G_K$ be the natural homomorphism. The *Alexander module* of K is defined by the ψ-differential module and is denoted by A_K. Then $Q_K := ((\psi \circ \pi)(\partial R_i/\partial x_j))$ gives a presentation matrix of the Λ-module A_K (Corollary 9.6). Since $A_K \simeq H_1(X_\infty) \oplus \Lambda$ (Λ-isomorphism) by the Crowell exact sequence (Theorem 9.8), we may assume $Q_K = (Q_1|0)$ by some elementary operations if necessary. Here Q_1 gives a presentation square matrix of the Λ-module $H_1(X_\infty)$.

Proposition 11.2 *$H_1(X_\infty)$ is a finitely generated, torsion Λ-module, and we have* $E_0(H_1(X_\infty)) = (\det(Q_1))$, $\Delta_0(H_1(X_\infty)) = \det(Q_1)(\neq 0)$.

Proof Since $H_1(X_\infty) = \Lambda^{m-1}/Q_1(\Lambda^{m-1})$, $H_1(X_\infty)$ is finitely generated over Λ. If $\mathrm{rank}_\Lambda H_1(X_\infty) \geq 1$, Proposition 11.1 and $\Lambda/(t-1)\Lambda \simeq \mathbb{Z}$ imply $\mathrm{rank}_\mathbb{Z} H_1(M) \geq 1$. This is a contradiction. The latter part is obvious. □

We let $\Delta_K(t) := \Delta_0(H_1(X_\infty)) = \det(Q_1)$ and call it the *Alexander polynomial* of K. $\Delta_K(t)$ is determined up to multiplication by an element of $\Lambda^\times$. Since $\Lambda_\mathbb{Q} := \Lambda \otimes_\mathbb{Z} \mathbb{Q} = \mathbb{Q}[t^{\pm 1}]$ is a principal ideal domain, we have a $\Lambda_\mathbb{Q}$-isomorphism

$$H_1(X_\infty) \otimes_\mathbb{Z} \mathbb{Q} \simeq \bigoplus_{i=1}^{s} \Lambda_\mathbb{Q}/(f_i), \quad f_i \in \Lambda_\mathbb{Q}.$$

Here noting that τ acts on the right hand side as the multiplication by t, one has[1]

$$\Delta_K(t) = f_1 \cdots f_s = \det(t \cdot \mathrm{id} - \tau \mid H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}) \bmod \Lambda_{\mathbb{Q}}^{\times}. \tag{11.1}$$

Now, suppose that M is a homology 3-sphere. Then Proposition 11.1 and the following Lemma 11.3 implies $\Delta_K(1) = \pm 1$, and hence $\Delta_K(t)$ coincides with the characteristic polynomial $\det(t\mathrm{id} - \tau \mid H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q})$ up to multiplication of an element $\Lambda^{\times} = \{\pm t^n \mid n \in \mathbb{Z}\}$.

Next, we prepare an algebraic lemma. For the proof, we refer to [Hl, Theorem 3.13].

Lemma 11.3 *Let N be a finitely generated, torsion Λ-module and suppose that $E_0(N) = (\Delta)$. Then, for a non-constant $f(t) \in \mathbb{Z}[t]$, $N/f(t)N$ is a torion Abelian group if and only if $\Delta(\xi) \neq 0$ for any root $\xi \in \overline{\mathbb{Q}}$ of $f(t) = 0$. Further, if $f(t)$ is decomposed into the form $\pm \prod_{j=1}^{n}(t - \xi_j)$, one has*

$$\#(N/f(t)N) = \prod_{j=1}^{n} \left|\Delta(\xi_j)\right|.$$

For $g(t) = c_0 t^d + \cdots + c_d \in \mathbb{Z}[t]$ ($c_0 \neq 0$, $d \geq 1$), we define the *Mahler measure* $m(g)$ of $g(t)$ by

$$m(g) := \exp\left(\int_0^1 \log\left|g\left(e^{2\pi\sqrt{-1}x}\right)\right| dx\right).$$

If $g(t) = c_0 \prod_{i=1}^{d}(t - \theta_i)$, by Jensen's formula [Ah, Chap. 5, 3.1], we have $m(g) = c_0 \prod_{i=1}^{d} \max(|\theta_i|, 1)$.

Theorem 11.4 *Assume that there is no root of $\Delta_K(t) = 0$ which is an n-th root of unity for some n. Then all M_n's are rational homology 3-spheres and we have*

$$\lim_{n\to\infty} \frac{1}{n} \log \#H_1(M_n) = \log m(\Delta_K).$$

Proof By Proposition 11.1, Lemma 11.3 and the assumption, any $H_1(M_n)$ is finite and we have

$$\#H_1(M_n) = \prod_{j=0}^{n-1} \left|\Delta_K\left(e^{2\pi\sqrt{-1}j/n}\right)\right|.$$

[1] $a = b \bmod R^{\times}$ means that $b = au$ for some $u \in R^{\times}$.

Hence, we have

$$\lim_{n\to\infty}\frac{1}{n}\log\#H_1(M_n)=\lim_{n\to\infty}\frac{1}{n}\sum_{j=0}^{n-1}\log\left|\Delta_K\left(e^{2\pi\sqrt{-1}j/n}\right)\right|$$
$$=\int_0^1\log\left|\Delta_K\left(e^{2\pi\sqrt{-1}x}\right)\right|dx$$
$$=\log m(\Delta_K).\qquad\square$$

Remark 11.5 (1) The asymptotic formula in Theorem 11.4 was shown in [GS, No2] when M is a homology 3-sphere. For some extensions to the case of cyclic covering ramified along a link or an Iwasawa-theoretic type formulas (cf. Sect. 11.2), we refer to [HMM, KaM, SW].

(2) The homology growth rate in Theorem 11.4 is also interpreted as the entropy of the natural $\mathbb{Z}=\{\tau^n|n\in\mathbb{Z}\}$-action on the compact Protryagin dual $H_1(X_\infty,\mathbb{Z})^*$ [SW, Sh].

Example 11.6 Let $K\subset S^3$ be the figure eight knot $B(5,3)$ (Fig. 11.1).

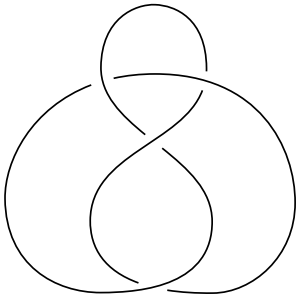


Fig. 11.1

Using the presentation $G_K=\langle x_1,x_2|x_2x_1^{-1}x_2x_1x_2^{-1}=x_1^{-1}x_2x_1x_2^{-1}x_1\rangle$, we obtain $\Delta_K=t^2-3t+1$. Hence, we have

$$\lim_{n\to\infty}\frac{1}{n}\log\#H_1(M_n)=\log m(\Delta_K)=\log\frac{3+\sqrt{5}}{2}.$$

11.2 The Iwasawa Polynomial and p-Ideal Class Groups

Let k be a finite algebraic number field and let p be a prime number. Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension of k (Example 2.46). In the following, we assume that only one prime ideal $\mathfrak{p}$ of k is ramified in k_∞/k and it is totally ramified. (This is an

assumption analogous to the knot case). We note that $\mathfrak{p}$ must be a prime ideal over p by class field theory. We denote by μ_{p^d} the group of p^d-th roots of unity. The fields $k = \mathbb{Q}(\mu_{p^d})$ or their subfields satisfy the assumption.

For an integer $n \geq 0$, let k_n be the cyclic subfield of k_∞/k of degree p^n, and let H_n be the p-Sylow subgroup of the ideal class group of k_n: $H_n := H(k_n)(p)$. Let L_n be the maximal unramified Abelian p-extension of k_n (Hilbert p-class field). By unramified class field theory (Example 2.44, Sect. 6.1), we have the following isomorphism for each n:

$$\varphi_n : H_n \simeq \mathrm{Gal}(L_n/k_n); \qquad \varphi_n([\mathfrak{a}]) = \sigma_{\mathfrak{a}}.$$

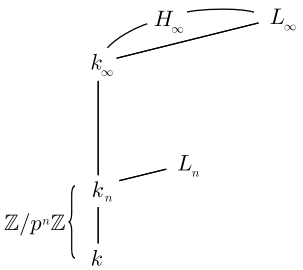
For $n \geq m$, let $\mathrm{N}_{n/m} : H_n \to H_m$ be the norm map. Then we have the commutative diagram:

$$\begin{array}{ccc} H_n & \xrightarrow{\varphi_n} & \mathrm{Gal}(L_n/k_n) \\ {\scriptstyle \mathrm{N}_{n/m}}\downarrow & & \downarrow \\ H_m & \xrightarrow{\varphi_m} & \mathrm{Gal}(L_m/k_m) \end{array} \tag{11.2}$$

where the right vertical map is the restriction map. Note that $\{H_n\}_{n\geq 0}$ forms a projective system with respect to the norm maps, and let $H_\infty := \varprojlim_n H_n$. Let $L_\infty := \bigcup_{n\geq 0} L_n$. By (11.2), we have an isomorphism of pro-p Abelian groups:

$$\varphi_\infty : H_\infty \simeq \mathrm{Gal}(L_\infty/k_\infty).$$

Since L_n is the maximal unramified Abelian p-extension of k_n, we see that L_n is a Galois extension of k, and hence L_∞/k is a pro-p Galois extension.



Let $\tilde{\mathfrak{p}}$ be a prime of L_∞ lying over $\mathfrak{p}$ and let $I_{\mathfrak{p}}$ be the inertia group of $\tilde{\mathfrak{p}}$. By the assumption, we have $I_{\mathfrak{p}} \simeq \mathrm{Gal}(L_\infty/k)/\mathrm{Gal}(L_\infty/k_\infty) \simeq \mathrm{Gal}(k_\infty/k)$. We fix a topological genetator γ of $\mathrm{Gal}(k_\infty/k)$. By sending γ to $1+T$, we identify $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$ with $\hat{\Lambda} := \mathbb{Z}_p[[T]]$ (pro-p Magnus isomorphism). Note that the Galois group $\mathrm{Gal}(L_\infty/k_\infty)$ is an *Iwasawa module* (ψ-Galois module) in the sense of Example 9.18 for the natural homomorphism $\psi : \mathrm{Gal}(L_\infty/k) \to \mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_p$. We note that $g \in \mathrm{Gal}(k_\infty/k)$ acts on $\mathrm{Gal}(L_\infty/k_\infty)$ by the inner-automorphism $g(x) = \tilde{g} \circ x \circ \tilde{g}^{-1}$ ($\tilde{g}$ being an extension of g to $\mathrm{Gal}(L_\infty/k)$) and that $\hat{\Lambda}$ acts on H_∞ in the natural manner, and we see that the isomorphism φ_∞ commutes with these actions. The following proposition is an analogue of Proposition 11.1.

Proposition 11.7 *We have the following isomorphism*:

$$H_n \simeq H_\infty/\big((1+T)^{p^n}-1\big)H_\infty \quad (n \geq 0).$$

Proof Note that $H_n \simeq \mathrm{Gal}(L_n/k_n) \simeq \mathrm{Gal}(L_\infty/k_n)/\mathrm{Gal}(L_\infty/L_n)$. Since $I_{\mathfrak{p}}^{p^n} \simeq \mathrm{Gal}(k_\infty/k_n)$, we have

$$\mathrm{Gal}(L_\infty/k_n) = \mathrm{Gal}(L_\infty/k_\infty)\cdot I_{\mathfrak{p}}^{p^n}, \qquad \mathrm{Gal}(L_\infty/L_n) = \big\langle \mathrm{Gal}(L_\infty/k_n)^{(2)}, I_{\mathfrak{p}}^{p^n}\big\rangle.$$

By an argument similar to the proof of Lemma 10.17, we can show

$$\mathrm{Gal}(L_\infty/k_n)^{(2)} = \big(\gamma^{p^n}-1\big)\,\mathrm{Gal}(L_\infty/k_\infty).$$

Hence, we have

$$\begin{aligned} H_n &\simeq \mathrm{Gal}(L_\infty/k_\infty) I_{\mathfrak{p}}^{p^n} / \big\langle \big(\gamma^{p^n}-1\big)\,\mathrm{Gal}(L_\infty/k_\infty), I_{\mathfrak{p}}^{p^n}\big\rangle \\ &\simeq \mathrm{Gal}(L_\infty/k_\infty)/\big(\gamma^{p^n}-1\big)\,\mathrm{Gal}(L_\infty/k_\infty) \\ &\simeq H_\infty/\big((1+T)^{p^n}-1\big)H_\infty. \end{aligned}$$

□

Next, we prepare algebraic lemmas concerning the structures of the Iwasawa algebra $\hat{\Lambda}$ and $\hat{\Lambda}$-modules. A polynomial $g(T) \in \mathbb{Z}_p[T]$ is called a *Weierstrass polynomial* if it is of the form $g(T) = T^\lambda + c_1 T^{\lambda-1} + \cdots + c_\lambda$, $c_1, \ldots, c_\lambda \equiv 0 \bmod p$. (The Weierstrass polynomial of degree $\lambda = 0$ is defined to be 1). For example, $(1+T)^{p^n} - 1$ $(n \geq 0)$ is a Weierstrass polynomial.

Lemma 11.8 (1) *Let g be a Weierstrass polynomial of degree $\lambda(\geq 1)$. Then any element $f \in \hat{\Lambda}$ can be written uniquely in the form*

$$f = qg + r, \quad q \in \hat{\Lambda},\ r \in \mathbb{Z}_p[T], \quad \deg(r) \leq \lambda - 1.$$

(2) (*p-adic Weierstrass preparation theorem*) *Any $f(T)(\neq 0) \in \hat{\Lambda}$ can be written uniquely in the form*

$$\begin{cases} f(T) = p^\mu g(T) u(T), \\ \mu \in \mathbb{Z}_{\geq 0}, \quad g(T) \text{ is a Weierstrass polynomial, } u(T) \in \hat{\Lambda}^\times. \end{cases}$$

The quantities $\mu = \mu(f)$, $\lambda = \lambda(f) := \deg(g)$ are called the μ-invariant *and the* λ-invariant *of f, respectively.*

For the proof of Lemma 11.8, we refer to [NSW, 5.3.1, 5.3.4].

Two $\hat{\Lambda}$-modules $\mathfrak{N}$, $\mathfrak{N}'$ are said to be *pseudo-isomorphic*, written as $\mathfrak{N} \sim \mathfrak{N}'$, if there is a $\hat{\Lambda}$-homomorphism $\varphi : \mathfrak{N} \to \mathfrak{N}'$ such that $\mathrm{Ker}(\varphi)$ and $\mathrm{Coker}(\varphi)$ are finite.

Lemma 11.9 *Let $\mathfrak{N}$ be a compact $\hat{\Lambda}$-module.*

(1) (*Nakayama's lemma*) $\mathfrak{N}$ *is a finitely generated* $\hat{\Lambda}$*-module if and only if* $\mathfrak{N}/(p, T)\mathfrak{N}$ *is finite.*
(2) *Suppose that* $\mathfrak{N}$ *is a finitely generated* $\hat{\Lambda}$*-module. Then we have*

$$\mathfrak{N} \sim \hat{\Lambda}^r \oplus \bigoplus_{i=1}^{s} \hat{\Lambda}/\big(p^{m_i}\big) \oplus \bigoplus_{i=1}^{t} \hat{\Lambda}/\big(f_i^{e_i}\big),$$

where r *is an integer* (≥ 0), m_i, $e_i \in \mathbb{N}$ *and* f_i *is an irreducible Weierstrass polynomial.*

For the proof of Lemma 11.9, we refer to [NSW, 5.2.8, 5.3.8].

Let $\mathfrak{N}$ be a finitely generated, torsion $\hat{\Lambda}$-module. By Lemma 11.9(2), we have

$$\mathfrak{N} \sim \bigoplus_{i=1}^{s} \hat{\Lambda}/\big(p^{m_i}\big) \oplus \bigoplus_{i=1}^{t} \hat{\Lambda}/\big(f_i^{e_i}\big).$$

The ideal generated by $f := \prod_{i=1}^{s} p^{m_i} \prod_{i=1}^{t} f_i^{e_i}$, which is determined by the $\hat{\Lambda}$-module $\mathfrak{N}$, is called the *characteristic ideal* of $\mathfrak{N}$. f is determined up to multiplication of an element of $\hat{\Lambda}^\times$ and is called the *Iwasawa polynomial* of $\mathfrak{N}$. When $\mathfrak{N}$ has no nontrivial finite $\hat{\Lambda}$-submodule, it can be shown that the characteristic ideal of $\mathfrak{N}$ coincides with the 0-th elementary ideal $E_0(\mathfrak{N})$ and $f = \Delta_0(\mathfrak{N})$ [Ws, p. 299, Ex. (3)], [MW1, Appendix]. Since $\hat{\Lambda}_{\mathbb{Q}_p} := \hat{\Lambda} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathbb{Q}_p[[T]]$ is a principal ideal domain, we have a $\hat{\Lambda}_{\mathbb{Q}_p}$-isomorphism

$$\mathfrak{N} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \bigoplus_{i=1}^{t} \hat{\Lambda}_{\mathbb{Q}_p}/\big(f_i^{e_i}\big).$$

Note that $\gamma - 1$ acts on the right-hand side by the multiplication by T, we have

$$f(T) = \det\big(T \cdot \mathrm{id} - (\gamma - 1) \mid \mathfrak{N} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\big) \bmod (\hat{\Lambda}_{\mathbb{Q}_p})^\times. \tag{11.3}$$

The quantities $\mu(f) := \sum_{i=1}^{t} m_i$, $\lambda(f) := \sum_{i=1}^{s} \deg(f_i^{e_i})$, which are determined uniquely by $\mathfrak{N}$, are called the μ*-invariant*, λ*-invariant* of $\mathfrak{N}$, written as $\mu(\mathfrak{N})$, $\lambda(\mathfrak{N})$, respectively. If $\mu(\mathfrak{N}) = 0$, f equals to the characteristic polynomial $\det(T\,\mathrm{id} - (\gamma - 1) \mid \mathfrak{N} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \bmod \hat{\Lambda}^\times$.

Proposition 11.10 H_∞ *is a finitely generated, torsion* $\hat{\Lambda}$*-module.*

Proof Since H_n is finite (The finitess of ideal classes 2.30), by Proposition 11.7 and Lemma 11.9 (1), H_∞ is a finitely generated $\hat{\Lambda}$-module. If H_∞ is not torsion over $\hat{\Lambda}$, $H_\infty \approx \hat{\Lambda}^r \oplus \cdots$, $r \geq 1$. Since $\hat{\Lambda}/T\hat{\Lambda} \simeq \mathbb{Z}_p$ is infinite, this contradicts to Proposition 11.7. □

We have the following asymptotic formula for $\#H_n$ which may be regarded as an arithmetic analogue of Theorem 11.4 for a knot.

Theorem 11.11 (Iwasawa's class number formula) *Let* $\mu = \mu(H_\infty)$, $\lambda = \lambda(H_\infty)$. *For sufficiently large* n, *we have*

$$\log_p \#H_n = \mu p^n + \lambda n + \nu,$$

where ν *is a constant independent of* n.

Proof By Lemma 11.9(2) and Proposition 11.10, we have

$$H_\infty \sim E := \bigoplus_{i=1}^{s} \hat{\Lambda}/(p^{m_i}) \oplus \bigoplus_{i=1}^{t} \hat{\Lambda}/(f_i^{e_i}),$$

where $m_i, e_i \in \mathbb{N}$, f_i is an irreducible Weierstrass polynomial. From this, it can be shown [Ws, p. 284] that there is a constant c independent of n such that

$$\#\big(H_\infty/\big((1+T)^{p^n}-1\big)H_\infty\big) = p^c \#\big(E/\big((1+T)^{p^n}-1\big)E\big). \tag{11.4}$$

When $E = \hat{\Lambda}/(p^m)$:

$$\begin{aligned}\#\big(E/\big((1+T)^{p^n}-1\big)E\big) &= \#\big(\mathbb{Z}/p^m\mathbb{Z}[T]/\big((1+T)^{p^n}-1\big)\big)\\ &= \big(p^m\big)^{\deg\left((1+T)^{p^n}-1\right)}\\ &= p^{mp^n}. \end{aligned}\tag{11.5}$$

When $E = \hat{\Lambda}/(g)$ (g being a Weierstrass polynomial of $\deg(g) \geq 1$):

$$\begin{aligned}\#\big(E/\big((1+T)^{p^n}-1\big)E\big) &= \#\big(\mathbb{Z}_p[T]/\big(g,(1+T)^{p^n}-1\big)\big)\\ &= \prod_{\zeta^{p^n}=1} \big|g(\zeta-1)\big|_p^{-1}.\end{aligned}$$

Here $|\cdot|_p$ stands for the p-adic multiplicative valuation with $|p|_p^{-1} = p$ (Note that $g(\zeta-1) \neq 0$ for any p^n-th root ζ of unity, as $E/((1+T)^{p^n}-1)E$ is finite). Let v_p be the p-adic additive valuation ($|x|_p = p^{-v_p(x)}$) and suppose $g(T) = T^d + a_1T^{d-1} + \cdots + a_d$, $a_i \equiv 0 \bmod p$. If n is sufficiently large, we have $v_p((\zeta-1)^d) < v_p(p)$ for a primitive p^n-th root ζ of unity and hence $v_p(g(\zeta-1)) = v_p((\zeta-1)^d)$. Therefore, when n is sufficiently large,

$$\begin{aligned}v_p\Big(\prod_{\zeta^{p^n}=1} g(\zeta-1)\Big) &= v_p\Big(\prod_{\substack{\zeta^{p^n}=1\\ \zeta\neq 1}} (\zeta-1)^d\Big) + C\\ &= v_p(p^{nd}) + C\\ &= nd + C,\end{aligned}$$

where C is a constant independent of n. Hence, we have

$$\#\big(E/\big((1+T)^{p^n}-1\big)E\big) = p^{nd+C}. \tag{11.6}$$

By (11.4)–(11.6) and $\mu = \sum_{i=1}^{s} m_i$, $\lambda = \sum_{i=1}^{t} \deg(f_i^{e_i})$, we obtain the desired formula. □

Remark 11.12 (1) Note that the $\hat{\Lambda}$-module H_∞ and hence the Iwasawa invariants $\mu(H_\infty), \lambda(H_\infty)$ depend only on k and p. It is known that $\mu(H_\infty) = 0$ if $k/\mathbb{Q}$ is an Abelian extension [Ws, 7.5], and conjectured that this is always the case.

(2) As in the case for knots (Remark 11.5(2)), it would be interesting to study some arithmetic meaning of the entropy of the $\mathbb{Z} = \{\gamma^n | n \in \mathbb{Z}\}$-action on the Iwasawa module H_∞.

Example 11.13 Let $k = \mathbb{Q}(\mu_p)$. Then we have $k_\infty = \mathbb{Q}(\mu_{p^\infty})$, $\mu_{p^\infty} = \bigcup_{d\geq 1} \mu_{p^d}$, and our assumption is satisfied. By Remark 11.12, we have

$$\log_p \#H_n = \lambda n + \nu \quad (n \gg 0).$$

If we assume the Vandiver conjecture which asserts that the class number of $\mathbb{Q}(\zeta + \zeta^{-1})$ is not divisible by p, it is known that the following formula

$$\#H_n = \prod_{\zeta^{p^n}=1} |f(\zeta - 1)|_p^{-1}$$

holds for any $n \geq 1$ [Ws, Theorem 10.16]. Here $f(T)$ stands for the Iwasawa polynomial of H_∞.

Summary

Infinite cyclic covering $X_\infty \to X_K$ $\mathrm{Gal}(X_\infty/X_K) = \langle\tau\rangle \simeq \mathbb{Z}$	Cyclotomic $\mathbb{Z}_p$-extension k_∞/k $\mathrm{Gal}(k_\infty/k) = \langle\gamma\rangle \simeq \mathbb{Z}_p$
Knot module $H_1(X_\infty)$	Iwasawa module H_∞
Alexander polynomial $\det(t\cdot\mathrm{id} - \tau \mid H_1(X_\infty)\otimes_{\mathbb{Z}}\mathbb{Q})$	Iwasawa polynomial $\det(T\cdot\mathrm{id} - (\gamma-1) \mid H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$
Asymptotic formula for $\#H_1(M_n)$	Asymptotic formula for $\#H(k_n)(p)$

Chapter 12
Torsions and the Iwasawa Main Conjecture

The Iwasawa main conjecture asserts that the Iwasawa polynomial coincides essentially with the Kubota–Leopoldt p-adic analytic zeta function. This can also be regarded as a determinant expression of the p-adic zeta function, which was originally conjectured by Iwasawa as an analogue of the determinant expression, due to Weil and Grothendieck, of the congruence zeta function. According to the analogy between the Iwasawa polynomial and the Alexander polynomial discussed in Chaps. 9 and 11, an analogue of the Iwasawa main conjecture in knot theory may be a connection between the Alexander polynomial and a certain analytically defined zeta function. As Milnor [Ml2] already pointed out, such a connection is given as the relation between the Reidemeister–Milnor torsion and the Lefschetz zeta function associated to the infinite cyclic covering of a knot exterior. If one takes the Ray–Singer spectral zeta function as an analytic zeta function, such a connection is also given as the relation between the Reidemeister torsion and the analytic torsion (J. Cheeger, W. Müller and W. Lück).

12.1 Torsions and Zeta Functions

Let V be an n-dimensional vector space over a field F. For two (ordered) bases $\boldsymbol{b} = (b_1, \ldots, b_n)$ and $\boldsymbol{c} = (c_1, \ldots, c_n)$, we let $[\boldsymbol{b}/\boldsymbol{c}] := \det(a_{ij}) \in F^\times$ where $b_i = \sum_{j=1}^n a_{ij} c_j$. Let

$$C: \ 0 \longrightarrow C_m \xrightarrow{\partial_m} C_{m-1} \xrightarrow{\partial_{m-1}} \cdots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \longrightarrow 0$$

be an acyclic complex (i.e., exact sequence) of finite dimensional based vector spaces C_i over F and let $\boldsymbol{c}_i$ be a given basis of C_i (a based vector space means a vector space with a distinguished basis). Choose a basis $\boldsymbol{b}_i$ of $B_i := \mathrm{Im}(\partial_{i+1}) = \mathrm{Ker}(\partial_i)$. Consider the short exact sequence

$$0 \longrightarrow B_i \longrightarrow C_i \xrightarrow{\partial_i} B_{i-1} \longrightarrow 0.$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_12, © Springer-Verlag London Limited 2012

Choosing a lift $\tilde{\boldsymbol{b}}_{i-1}$ of $\boldsymbol{b}_{i-1}$ in C_i, the pair $(\boldsymbol{b}_i, \tilde{\boldsymbol{b}}_{i-1})$ forms a basis of C_i ($\boldsymbol{b}_{-1}$ is defined to be empty). We then define the *torsion* of C by

$$\tau(C) := \prod_{i=0}^{m} \left[(\boldsymbol{b}_i, \tilde{\boldsymbol{b}}_{i-1})/\boldsymbol{c}_i\right]^{(-1)^{i+1}}.$$

One easily see that $\tau(C)$ depends on $C_i, \boldsymbol{c}_i$, but not on the choices of $\boldsymbol{b}_i, \tilde{\boldsymbol{b}}_i$. Next, let R be a Noetherian unique factorization domain and let

$$D: \ 0 \longrightarrow D_m \xrightarrow{\partial_m} D_{m-1} \xrightarrow{\partial_{m-1}} \cdots \xrightarrow{\partial_2} D_1 \xrightarrow{\partial_1} D_0 \longrightarrow 0$$

be a complex of free R-modules with finite rank such that the homology group $H_i(D)$ is a torsion R-module for any i. Let $\Delta_i := \Delta_0(H_i(D))$, and let F be the quotient field of R. We then define the *homology torsion* of D by

$$\tau^h(D) := \prod_{i=0}^{m} \Delta_i^{(-1)^{i+1}} (\in F),$$

which is determined up to multiplication of a unit in $R^\times$. Let us choose a R-basis $\boldsymbol{d}_i$ of each D_i and let $C := D \otimes_R F$. Since C is then an acyclic complex of finite dimensional based vector spaces over F, the torsion $\tau(C)$ is defined. Then we have the following lemma.

Lemma 12.1 $\tau(C) = \tau^h(D) \bmod R^\times$.

Proof We follow [Hl, Theorem 3.15]. We shall prove the assertion by induction on the length m of D. The assertion is clearly true for $m = 1$ and so we assume that $m > 1$ and that the assertion holds for all such complexes over R of length less than m.

Let $Z_{m-2} = \mathrm{Ker}(\partial_{m-2})$ have rank r, and choose $d'_1, \ldots, d'_r \in D_{m-1}$ whose images under ∂_{m-1} generate a rank r free submodule D'_{m-1} of D_{m-1}. Let $j : D'_{m-1} \hookrightarrow D_{m-1}$ be the inclusion. Let D' be the subcomplex of D such that $(D')_i = D_i$ if $i < m-1$, $(D')_{m-1} = D'_{m-1}$ and $(D')_i = 0$ if $i \geq m$. Let E be the complex $\cdots D'_{m-1} \xrightarrow{\mathrm{id}} D'_{m-1} \cdots$ concentrated in degrees m and $m-1$, and let $D'' := D \oplus E$. Define a chain homomorphism $\alpha : D' \to D''$ by $\alpha_i := \mathrm{id}_{D_i}$ if $i < m-1$ and $\alpha_{m-1} := j \oplus \mathrm{id}_{D'_{m-1}}$. Then α is injective, and the cokernel A of α is the complex $\cdots D_m \oplus D'_{m-1} \xrightarrow{\partial_m + j} D_{m-1} \cdots$ concentrated in degrees m and $m-1$. Let $C' := D' \otimes_R F$, $C'' := D'' \otimes_R F$ and $B := A \otimes_R F$. Note that the complexes D', D'' and A are all free over R and that C', C'' and B are acyclic.

Equip each of D', D'' and A with obvious bases. Since torsions are multiplicative with respect to an exact sequence of complexes, we have $\tau(C) = \tau(C'') = \tau(C')\tau(B)$. The inclusion of D into D'' is a chain homotopy equivalence, and so $H_i(D) \simeq H_i(D'')$ for all i. The long exact sequence $0 \to D' \xrightarrow{\alpha} D'' \to A \to 0$

breaks up into isomorphisms $H_i(D') = H_i(D)$ if $i < m-2$ and an exact sequence $0 \to H_{m-1}(D) \to H_{m-1}(A) \to H_{m-2}(D') \to H_{m-2}(D) \to 0$. These modules are all R-torsion and so $\Delta_0(H_{m-1}(A))\Delta_0(H_{m-2}(D'))^{-1} = \Delta_0(H_{m-1}(D))\Delta_0(H_{m-2}(D))^{-1}$. As D' and A are each of length $\leq m-1$, the result follows from the induction hypothesis. □

Now let $K \subset S^3$ be a knot, $X_K = S^3 \setminus \mathrm{int}(V_K)$ the link exterior and $G_K = \pi_1(X_K)$ the knot group. Let $\psi : G_K \to G_K^{\mathrm{ab}} = \langle \alpha \rangle \simeq \mathbb{Z}$ be the Abelianization map and let X_∞ be the infinite cyclic covering of X_K corresponding to $\mathrm{Ker}(\psi)$. Set $\Lambda := \mathbb{Z}[t^{\pm 1}] = \mathbb{Z}[\langle \alpha \rangle]$ $(t \leftrightarrow \alpha)$. Let $G_K = \langle x_1, \ldots, x_n \mid R_1 = \cdots = R_{n-1} = 1 \rangle$ be a Wirtinger presentation (Example 2.6) and let $\pi : F = \langle x_1, \ldots, x_n \rangle \to G_K$ be the natural homomorphism. We associate to the presentation of G_K a complex of Λ-modules

$$D: \ 0 \longrightarrow D_2 = \Lambda^{n-1} \xrightarrow{\partial_2} D_1 = \Lambda^n \xrightarrow{\partial_1} D_0 = \Lambda \longrightarrow 0, \tag{12.1}$$

where $\partial_2 = ((\psi \circ \pi)(\partial R_i / \partial x_j))$ is the Alexander matrix and $\partial_1 = ((\psi \circ \pi)(x_i - 1))$. Since X_K collapses to a 2-dimensional complex obtained from the presentation of G_K, we may regard the complex D of (12.1) as $C_*(X_\infty) = C_*(X_K, \Lambda)$ and so the homology group $H_i(X_\infty) = H_i(X_K, \Lambda)$ is given by $H_i(D)$.

Proposition 12.2 *For any $i \geq 0$, $H_i(X_\infty)$ is a finitely generated, torsion Λ-module. Furthermore, we have $H_i(X_\infty) = 0$ $(i \geq 2)$, $E_0(H_1(X_\infty)) = (\Delta_K(t))$, $E_0(H_0(X_\infty)) = (t-1)$, where $\Delta_K(t)$ is the Alexander polynomial of K.*

Proof It is obvious that $H_i(X_\infty) = 0$ $(i \geq 3)$ and $E_0(H_0(X_\infty)) = (t-1)$. The assertion about $H_1(X_\infty)$ follows from Proposition 11.2. Thus, it suffices to show $H_2(X_\infty) = 0$. We associate to (12.1) an exact sequence of Λ-modules

$$0 \longrightarrow H_2(X_\infty) \longrightarrow \Lambda^{n-1} \xrightarrow{\partial_2} \Lambda^n \longrightarrow A_K \longrightarrow 0,$$

where A_K is the Alexander module of K. Since $H_2(X_\infty)$ is a Λ-submodule of the free Λ-module Λ^{n-1}, it has no torsion. On the other hand, as A_K has Λ-rank 1, the Λ-rank of $H_2(X_\infty)$ is 0. Hence, $H_2(X_\infty) = 0$. □

Let k be an extension of $\mathbb{Q}$ and let $F = k(t)$. Choose the standard basis of D_i in (12.1). Then, by Proposition 12.2, the complex $C_*(X_K, F) = C_*(X_K, \Lambda) \otimes_\Lambda F = C_*(X_\infty) \otimes_\Lambda F$ becomes an acyclic complex of finite dimensional based vector spaces over F. Therefore we have, by Lemma 12.1 and Proposition 12.2, the following.

Proposition 12.3 $\tau(C_*(X_K, F)) = \tau^h(C_*(X_\infty)) = \frac{\Delta_K(t)}{t-1} \bmod \Lambda^\times$.

$\tau(C_*(X_K, F)) = \tau^h(C_*(X_\infty))$ is called the *Reidemeister–Milnor torsion* of X_K which we denote by $\tau(X_K, \Lambda)$.

Remark 12.4 (1) The torsion $\tau(X_K, \Lambda)$ can be described in terms of the determinant module [KnM, Mz5] as follows: Tensoring Λ over $\mathbb{Z}$ with the exact sequence

$$0 \longrightarrow C_*(X_\infty) \xrightarrow{\alpha-1} C_*(X_\infty) \longrightarrow C_*(X_K) \longrightarrow 0,$$

we have the exact sequence of Λ-modules

$$0 \longrightarrow C_*(X_\infty, \Lambda) \xrightarrow{\alpha-1} C_*(X_\infty, \Lambda) \longrightarrow C_*(X_K, \Lambda) \longrightarrow 0.$$

From this, we have the following Λ-isomorphisms

$$\begin{aligned}\Lambda &\simeq \det_{\Lambda} C_*(X_\infty, \Lambda) \otimes_\Lambda \det_{\Lambda} C_*(X_\infty, \Lambda)^{-1} \\ &\simeq \det_{\Lambda} C_*(X_K, \Lambda) \\ &\simeq \det_{\Lambda} H_*(X_K, \Lambda) \quad \text{(Euler isomorphism)}.\end{aligned}$$

Now let $\zeta(X_K, \Lambda)$ be the image of $1 \in \Lambda$ in $\det_\Lambda H_*(X_K, \Lambda)$ under the above isomorphism. The torsion $\tau(X_K, \Lambda)$ is then nothing but the image of $\zeta(X_K, \Lambda)$ in F under the isomorphism $\det_\Lambda H_*(X_K, \Lambda) \otimes_\Lambda F \simeq \det_F H_*(X_K, F) = \det_F(0) = F$. $\zeta(X_K, \Lambda)$ is an analogue in knot theory of K. Kato's *zeta element* [Kt2].

(2) More generally, we may consider the Reidemeister–Milnor torsion associated to a representation of a knot group $\rho : G_K \to GL(V)$ (V being a finite dimensional vector space over k) (cf. [KiL, KGM]). Let $\Lambda_k := \Lambda \otimes_{\mathbb{Z}} k$, $V[t^{\pm 1}] := V \otimes_k \Lambda_k$ and $V(t) := V \otimes_k F$. We regard $V[t^{\pm 1}]$ as a left $k[G_K]$-module via the representation $\rho \otimes \psi : G_K \to GL(V[t^{\pm 1}])$ and consider the complex $C_*(X_K, V[t^{\pm 1}]) = C_*(\tilde{X}_K, k) \otimes_{k[G_K]} V[t^{\pm 1}]$. Since $C_*(X_K, V[t^{\pm 1}]) = C_*(X_K, \Lambda_k) \otimes_k V$, by Proposition 12.2, $H_i(X_K, V[t^{\pm 1}]) = H_i(X_K, \Lambda_k) \otimes_k V$ is a finitely generated, torsion Λ_k-module for any i. So, choosing a basis of V over k, $C_*(X_K, V(t)) := C_*(X_K, \Lambda_k) \otimes_{\Lambda_k} F$ becomes an acyclic complex of finite dimensional based vector spaces over F. Letting $\Delta_{i,\rho}(t) := \Delta_0(H_i(X_K, V[t^{\pm 1}]))$, we have by Lemma 12.1,

$$\tau\big(C_*\big(X_K, V(t)\big)\big) = \tau^h\big(C_*\big(X_K, V\big[t^{\pm 1}\big]\big)\big) = \frac{\Delta_{1,\rho}(t)}{\Delta_{0,\rho}(t)} \bmod (\Lambda_k)^\times.$$

Here $\Delta_{1,\rho}$ is called the *twisted Alexander polynomial* of K associated to the representation ρ.

The torsion $\tau(X_K, \Lambda_k)$ has the following dynamical interpretation [Ml2]. The monodromy (meridian) action $\alpha : X_\infty \to X_\infty$ defines a discrete dynamical system on X_∞. The torsion $\tau(X_K, \Lambda_k)$ is then expressed by the Lefschetz zeta function of this dynamical system. For $n \in \mathbb{N}$, let $L(\alpha^n)$ be the Lefschetz number of α^n defined by

$$L\big(\alpha^n\big) := \sum_{i=0}^{1} (-1)^i \operatorname{Tr}\big((\alpha_*)^n \mid H_i(X_\infty, k)\big).$$

The *Lefschetz zeta function* is then defined by

$$\zeta_K(t) := \exp\left(\sum_{n=1}^{\infty} L\big(\alpha^n\big)\frac{t^n}{n}\right)(\in k[[t]]).$$

Theorem 12.5 (See [Ml2, No1]) $\zeta_K(t) = \tau(X_K, \Lambda_k) \bmod (\Lambda_k)^{\times}$.

Proof Note that for a matrix $A \in M_N(k)$, the following equality holds in $k[[t]]$:

$$\det(I - tA)^{-1} = \exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}\big(A^n\big)\frac{t^n}{n}\right).$$

Therefore, we have

$$\begin{aligned}\zeta_K(t) &= \prod_{i=1}^{1} \det\big(I - t\alpha_* \mid H_i(X_\infty, k)\big)^{(-1)^{i+1}} \\ &= \tau(X_K, \Lambda_k) \bmod (\Lambda_k)^{\times}.\end{aligned}$$

□

The Reidemeister torsion is also expressed by the spectral zeta function (Hodge theoretic interpretation). Let $\rho : G_K \to O(V)$ be an orthogonal representation where V is a finite dimensional vector space over $\mathbb{R}$ equipped with an inner product. We consider the relative chain complex $C_*(X_K, \partial X_K, V) := C_*(X_K, \partial X_K) \otimes_{\mathbb{Z}[G_K]} V$. Choosing a cell decomposition of X_K and an orthonormal basis of V, the Reidemeister torsion $\tau(X_K, \partial X_K, V)$ is defined up to ± 1 [KGM, Lemmas 5.2.5–5.2.7]. On the other hand, we give a Riemannian metric on X_K. The metric is assumed to be a product near ∂X_K. Then the space of V-valued i-forms $\Omega^i(X_K, V)$ is equipped with an inner product, and the Hodge star operator $* : \Omega^i(X_K, V) \to \Omega^{3-i}(X_K, V)$ and the adjoint of the differential operator $\delta := - * d^{3-i} * : \Omega^i(X_K, V) \to \Omega^{i-1}(X_K, V)$ are defined. We set

$$\Omega^i(X_K, \partial X_K, V) := \big\{\omega \in \Omega^i(X_K, V) \mid \omega|_{\partial X_K} = \delta\omega|_{\partial X_K} = 0\big\}$$

on which the Laplace operator $\Delta^i := d^{i-1} \circ \delta^i + \delta^{i+1} \circ d^i$ acts as a self-adjoint operator. The *Ray–Singer spectral zeta function* is then defined by

$$\zeta_{\Delta^i}(s) := \sum_{\lambda > 0} \lambda^{-s}, \qquad \zeta_{\Delta}(s) := \sum_{i=0}^{3} (-1)^i i \zeta_{\Delta^i}(s),$$

where λ ranges over positive eigenvalues of Δ^i. It is shown that $\zeta_\Delta(s)$ is continued analytically to the whole complex plane and is analytic at $s = 0$. The connection with the Reidemeister torsion is given as follows.

Theorem 12.6 ([Lü]) $\exp(\zeta'_\Delta(0)) = \pm\tau(X_K, \partial X_K, V)$.

Here $\exp(\zeta'_\Delta(0))$ is called the *analytic torsion* of $(X_K, \partial X_K, V)$. By Theorem 12.6, this is independent of the choice of Riemannian metric.

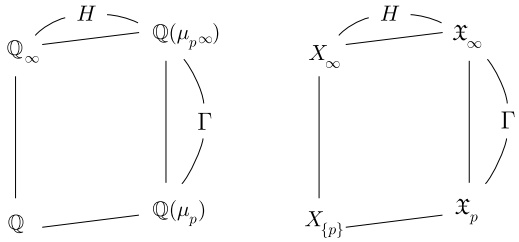
Remark 12.7 When M is a complete hyperbolic 3-manifold which is closed or of finite volume, one has a closer analogy with number theory. For an orthonormal representation $\rho : \pi_1(M) \to O(V)$, consider the following zeta function of M

$$Z(s) := \prod_{\mathfrak{p}} \det\bigl(I - \rho(\mathfrak{p})e^{-sl(\mathfrak{p})}\bigr)^{-1}$$

where $\mathfrak{p}$ runs over prime closed geodesics of M and $l(\mathfrak{p})$ stands for the length of $\mathfrak{p}$. $Z(s)$ is a geometric analogue of the zeta function of a number field (Artin motive). The analytic torsion $\exp(\zeta'_\Delta(0))$ is then shown to coincide with the coefficient $Z_M(0)^*$ of the main part of $Z_M(s)$ at $s = 0$ up to an elementary factor ($\in \mathbb{Q}^\times$). From this, $Z_M(0)^*$ is expressed essentially by the Reidemeister torsion $\tau(M, V)$ [Fr, Sg1, Sg2, Sg3]. This formula may be seen as an analogue of the analytic class number formula of a number field. Furthermore, if M admits an infinite cyclic covering, the relation between the order of the Milnor torsion at $t = 1$ and the order of $Z(s)$ at $s = 0$ is also shown [Sg1, Sg2, Sg3].

12.2 The Iwasawa Main Conjecture

Let p be an odd prime number, $X_{\{p\}} := \mathrm{Spec}(\mathbb{Z}[1/p])$ and $G_{\{p\}} := \pi_1(X_{\{p\}})$ the prime group. Let $\psi : G_{\{p\}} \to G^{\mathrm{ab}}_{\{p\}}$ be the Abelianization map and let $\mathfrak{X}_\infty$ be the pro-étale covering of $X_{\{p\}}$ corresponding to $\mathrm{Ker}(\psi)$. By class field theory, we have $G^{\mathrm{ab}}_{\{p\}} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$, where $\mu_{p^\infty} := \bigcup_{n\geq 1} \mu_{p^n}$, μ_{p^n} being the group of p^n-th roots of unity. According to the decomposition $\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$, one has the decomposition of $G^{\mathrm{ab}}_{\{p\}}$: $G^{\mathrm{ab}}_{\{p\}} = H \times \Gamma$, $H = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}_\infty) = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = \mathbb{F}_p^\times$, $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = 1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$. Here $\mathbb{Q}_\infty$ stands for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ (Example 2.46). $\mathfrak{X}_\infty$ is the integral closure of $X_{\{p\}}$ in $\mathbb{Q}(\mu_{p^\infty})$. Let $\mathfrak{X}_p := \mathrm{Spec}(\mathbb{Z}[\mu_p, 1/p])$ and let X_∞ be the integral closure of $X_{\{p\}}$ in $\mathbb{Q}_\infty$.



For $g \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, we define $\kappa(g) \in \mathbb{Z}_p^\times$ by $g(\zeta) = \zeta^{\kappa(g)}$ ($\zeta \in \mu_{p^\infty}$). κ gives the isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ and is called the *cyclotomic character*. We

set $\omega := \kappa|_H : H \hookrightarrow \mathbb{Z}_p^\times$. Fix a generator δ of H and a topological generator γ of Γ and let $\hat{\Lambda} := \mathbb{Z}_p[[T]] = \mathbb{Z}_p[[\Gamma]]$ $(1+T \leftrightarrow \gamma)$ and $\tilde{\Lambda} := \mathbb{Z}_p[[G^{\mathrm{ab}}_{\{p\}}]] = \mathbb{Z}_p[H][[\Gamma]]$.

For each $j \bmod p-1$, we define the H-module $\mathbb{Z}/p^n\mathbb{Z}[j]$ $(n \geq 1)$ by $\mathbb{Z}/p^n\mathbb{Z}$ as an Abelian group on which $\delta \in H$ acts as multiplication by $\omega(\delta)^j$, and let $\mathbb{Z}_p[j] := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}[j]$. Then we have $\mathbb{Z}_p[H] = \bigoplus_j \mathbb{Z}_p[j]$. Let $\tilde{\Lambda}^{(j)} := \mathbb{Z}_p[j][[\Gamma]]$ so that $\tilde{\Lambda} = \bigoplus_j \tilde{\Lambda}^{(j)}$. For a $\tilde{\Lambda}$-module M, we let $M^{(j)} := M \otimes_{\tilde{\Lambda}} \tilde{\Lambda}^{(j)}$. $M^{(j)}$ is the maximal quotient of M on which $\delta \in H$ acts as multiplication by $\omega(\delta)^j$. For $n \in \mathbb{Z}$, we define the $\hat{\Lambda}$-module $\mathbb{Z}_p(n)$ by $\mathbb{Z}_p$ as an Abelian group on which $\gamma \in \Gamma$ acts as multiplication by $\kappa(\gamma)^n$, and let $A(n) := A \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(n)$ (Tate twist) for a $\hat{\Lambda}$-module A.

We identify an H-module with a finite étale sheaf on $X_{\{p\}}$ which becomes a constanf seaf on $\mathfrak{X}_p$. We define $H_i(X_\infty, \mathbb{Z}_p[j])$ (which is also denoted by $H_i(X_{\{p\}}, \tilde{\Lambda}^{(j)})$) by

$$H_i\big(X_\infty, \mathbb{Z}_p[j]\big) := \Big(\varinjlim_n H^i\big(X_\infty, \mathbb{Z}/p^n\mathbb{Z}[j]\big)\Big)^*,$$

where $*$ means the Pontryagin dual. (Although the étale sheaf $\mathbb{Z}/p^n\mathbb{Z}[j]$ in the right hand side should be $\mathbb{Z}/p^n\mathbb{Z}[-j]$, we adopt the above definition to simplify the notations below) Finally, we let $\mathfrak{M} := \pi_1^{\mathrm{ab}}(\mathfrak{X}_\infty)(p) = \mathrm{Gal}(M/\mathbb{Q}(\mu_{p^\infty}))$ where M denotes the maximal Abelian extension of $\mathbb{Q}(\mu_{p^\infty})$ unramified outside p. The Galois group $G^{\mathrm{ab}}_{\{p\}}$ acts on $\mathfrak{M}$ by the inner automorphism and $\mathfrak{M}$ is then regarded as a compact $\tilde{\Lambda}$-module.

Proposition 12.8 *For any i and even j, $H_i(X_\infty, \mathbb{Z}_p[j])$ is a finitely generated, torsion $\hat{\Lambda}$-module. More precisely, we have*

$$H_i\big(X_\infty, \mathbb{Z}_p[j]\big) = 0 \quad (i \geq 2,\ j : \textit{even}),$$

$$H_1\big(X_\infty, \mathbb{Z}_p[j]\big) = \mathfrak{M}^{(j)} \quad (j : \textit{even}),$$

$$H_0\big(X_\infty, \mathbb{Z}_p[j]\big) = \begin{cases} \mathbb{Z}_p & (j=0), \\ 0 & (j \neq 0), \end{cases} \qquad E_0\big(H_0\big(X_\infty, \mathbb{Z}_p[j]\big)\big) = \begin{cases} (T) & (j=0), \\ (1) & (j \neq 0). \end{cases}$$

If j is even, $E_0(H_1(X_\infty, \mathbb{Z}_p[j]))$ coincides with the characteristic ideal of $H_1(X_\infty, \mathbb{Z}_p[j])$ and is generated by $\Delta_p^{(j)} := \Delta_0(H_1(X_\infty, \mathbb{Z}_p[j]))$. Furthermore, $\Delta_p^{(j)}$ satisfies

$$\Delta_p^{(j)} = \det\big(T \cdot \mathrm{id} - (\gamma - 1) \mid H_1\big(X_\infty, \mathbb{Z}_p[j]\big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\big) \bmod \hat{\Lambda}^\times.$$

Proof We follow [BN, Proposition 5.5] for the computation of $H^i(X_\infty, \mathbb{Z}/p^n\mathbb{Z}[j])$. Since $\#H$ is prime to p, the Hochschild–Serre spectral sequence

$$H^k\big(H, H^i\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}[j]\big)\big) \quad \Rightarrow \quad H^{k+i}\big(X_\infty, \mathbb{Z}/p^n\mathbb{Z}[j]\big)$$

degenerates and yields

$$\begin{aligned} H^i\big(X_\infty, \mathbb{Z}/p^n\mathbb{Z}[j]\big) &= H^0\big(H, H^i\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}[j]\big)\big) \\ &= H^0\big(H, H^i\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}\big)^{(j)}\big) \\ &= H^i\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}\big)^{(-j)}. \end{aligned}$$

Since $\mathbb{Z}[\mu_{p^\infty}, 1/p]$ is the Dedekind domain containing μ_{p^∞}, the cohomological p-dimension of $\mathfrak{X}_\infty = \mathrm{Spec}(\mathbb{Z}[\mu_{p^\infty}, 1/p])$ is 2. Therefore $H^i(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}[j]) = 0$ $(i \geq 3)$ and so $H_i(X_\infty, \mathbb{Z}_p[j]) = 0$ $(i \geq 3)$.

To see $H_2(X_\infty, \mathbb{Z}_p[j]) = 0$, we note first that

$$\begin{aligned} H^2\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}\big)^{(-j)} &= \big(H^2(\mathfrak{X}_\infty, \mu_{p^n})(-1)\big)^{(-j)} \\ &= \big(\big(\mathrm{Cl}(\mathfrak{X}_\infty) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}\big)(-1)\big)^{(-j)} \\ &= \big(\mathrm{Cl}(\mathfrak{X}_\infty) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}\big)^{(1-j)}(-1), \end{aligned}$$

where $\mathrm{Cl}(\mathfrak{X}_\infty)$ denotes the ideal class group of $\mathbb{Z}[\mu_{p^\infty}, 1/p]$. Let $\mathfrak{X}_k := \mathrm{Spec}(\mathbb{Z}[\mu_{p^k}, 1/p])$. Since $\mathrm{Cl}(\mathfrak{X}_k)$ is a finite Abelian group, $\mathrm{Cl}(\mathfrak{X}_\infty) = \varinjlim_k \mathrm{Cl}(\mathfrak{X}_k)$ is a torsion Abelian group. Therefore, $\varinjlim_n H^2(\mathfrak{X}_\infty, \mathbb{Z}/p^n)^{(-j)} = (\mathrm{Cl}(\mathfrak{X}_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{(1-j)}(-1) = 0$. Hence, $H_2(X_\infty, \mathbb{Z}_p[j]) = 0$.

Next we have

$$\begin{aligned} H^1\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}\big)^{(-j)} &= \mathrm{Hom}_c\big(\mathfrak{M}, \mathbb{Z}/p^n\mathbb{Z}\big)^{(-j)} \\ &= \mathrm{Hom}_c\big(\mathfrak{M}^{(j)}, \mathbb{Z}/p^n\mathbb{Z}\big) \end{aligned}$$

where Hom_c stands for the group of continuous homomorphisms. Therefore, $H_1(X_\infty, \mathbb{Z}_p[j]) = \mathrm{Hom}_c(\mathfrak{M}^{(j)}, \mathbb{Q}_p/\mathbb{Z}_p)^* = \mathfrak{M}^{(j)}$. If j is even, it is known ([BN, Lemma 5.3], [Ws, Proposition 15.36]) that $\mathfrak{M}^{(j)}$ is a finitely generated, torsion $\hat{\Lambda}$-module and has no nontrivial finite $\hat{\Lambda}$-submodule and $\mu(\mathfrak{M}^{(j)}) = 0$. So $E_0(H_1(X_\infty, \mathbb{Z}_p[j]))$ coincides with the characteristic ideal of $H_1(X_\infty, \mathbb{Z}_p[j])$ and $\Delta_p^{(j)}$ equals, $\mathrm{mod}\hat{\Lambda}^\times$, the characteristic polynomial in the statement. Finally, we see obviously

$$H^0\big(\mathfrak{X}_\infty, \mathbb{Z}/p^n\mathbb{Z}\big)^{(-j)} = \big(\mathbb{Z}/p^n\mathbb{Z}\big)^{(-j)} = \begin{cases} \mathbb{Z}/p^n\mathbb{Z} & (j = 0) \\ 0 & (j \neq 0) \end{cases}$$

and so $H_0(X_\infty, \mathbb{Z}_p[j]) = \mathbb{Z}_p$ $(j = 0)$, $= 0$ $(j \neq 0)$. The assertion for $E_0(H_0(X_\infty, \mathbb{Z}_p[j]))$ is also obvious. □

By Proposition 12.8, for an even integer j mod $p-1$, we define the *homology torsion* of $H_*(X_\infty, \mathbb{Z}_p[j])$ by

$$\tau\big(X_{\{p\}}, \tilde{\Lambda}^{(j)}\big) := \begin{cases} \Delta_p^{(j)}/T & (j = 0), \\ \Delta_p^{(j)} & (j \neq 0). \end{cases}$$

This is determined up to multiplication by an element in $\hat{\Lambda}^\times$.

The torsion $\tau(X_{\{p\}}, \tilde{\Lambda}^{(j)})$ is expressed by the Kubota–Leopoldt p-adic analytic zeta function. Let $\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} n^{-s}$ be the Riemann zeta function. It is known that $\zeta_{\mathbb{Q}}(s)$ is continued analytically to the whole complex plane and $\zeta_{\mathbb{Q}}(-n) \in \mathbb{Q}$ for $n \in \mathbb{N}$. Further, one has $\zeta_{\mathbb{Q}}(-n) \neq 0$ if and only if n is odd. T. Kubota and H. Leopoldt constructed a p-adic analytic function which interpolates the values $\zeta_{\mathbb{Q}}(-n)$ for odd n, called the *p-adic zeta function*.

Theorem 12.9 (Kubota and Leopoldt [KuL]) *For each even j mod $p-1$, there is a p-adic analytic function*

$$\zeta_p(\omega^j,) : \mathbb{Z}_p \setminus \{1\} \to \mathbb{Q}_p$$

such that for any $n \equiv j-1 \bmod p-1$, one has the equality

$$\zeta_p(\omega^j, -n) = (1-p^n)\zeta_{\mathbb{Q}}(-n).$$

For the proof of Theorem 12.9, we refer to ([KuL], [Ws, Chaps. 5 and 7], [CaS]).

The following theorem, due to B. Mazur and A. Wiles, gives the relation between the torsion $\tau(X_{\{p\}}, \tilde{\Lambda}^{(j)})$ and the p-adic zeta function $\zeta_p(\omega^j, s)$.

Theorem 12.10 (The Iwasawa main conjecture [MW1]) *For even j, there is a generator $\Delta_p^{(j)}$ of the ideal $E_0(H_1(X_\infty, \mathbb{Z}_p^{(j)}))$ such that one has*

$$\zeta_p(\omega^j, s) = \tau(X_{\{p\}}, \tilde{\Lambda}^{(j)})\big|_{T=q^{1-s}-1},$$

where $q := \kappa(\gamma)$.

For the proof of Theorem 12.10, we refer to ([MW1], [Ws, Chap. 15], [Ln2, Appendix], [CaS]).

Remark 12.11 As in the case of knots, we can introduce a generalization of the Iwasawa module associated to a certain p-adic representation $\rho : G_{\{p\}} \to \mathrm{Aut}(L)$ (L being a free $\mathbb{Z}_p$-module of finite rank). It is in fact defined as the Pontryagin dual of a certain subgroup $\mathrm{Sel}(X_\infty, \rho)$, called the *Selmer group*, of $H^1(X_\infty, V/L)$ ($V = L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$) [Ge]. A generator of the characteristic ideal of $\mathrm{Sel}(X_\infty, \rho)^*$, called the *twisted Iwasawa polynomial*, is an analogue of the twisted Alexander polynomial. When ρ is coming from a motive $H^m(Y)(n)$ (Y being a smooth projective variety over $\mathbb{Q}$), it is conjectured that an associated p-adic analytic L-function is defined and coincides essentially with the twisted Iwasawa polynomial (*generalized Iwasawa main conjecture* [CaP, Kt2]).

Summary

Relation between Alexander polynomial and Lefschetz (spectral) zeta function	Relation between Iwasawa polynomial and p-adic analytic zeta function

Chapter 13
Moduli Spaces of Representations of Knot and Prime Groups

In view of the analogy between a knot group $G_K = \pi_1(S^3 \setminus K)$ and a prime group $G_{\{p\}} = \pi_1(\mathrm{Spec}(\mathbb{Z}) \setminus \{p\})$, we expect some analogies between the moduli spaces of representations of knot and prime groups [Mz4]. In particular, the Alexander–Fox theory and Iwasawa theory are regarded as the theories on the moduli spaces of 1-dimensional representations of a knot and prime groups and associated topological and arithmetic invariants, respectively.

13.1 Character Varieties of Complex Representations of a Knot Group

For a knot $K \subset S^3$ and $N \in \mathbb{N}$, let $\mathcal{R}_{K,N}$ be the set of N-dimensional complex representations of the knot group G_K:

$$\begin{aligned}\mathcal{R}_{K,N} &:= \mathrm{Hom}\big(G_K, GL_N(\mathbb{C})\big) \\ &:= \big\{\rho : G_K \to GL_N(\mathbb{C}) \mid \rho \text{ is a homomorphism}\big\}.\end{aligned}$$

Let $G_K = \langle x_1, \ldots, x_n \mid r_1 = \cdots = r_{n-1} = 1\rangle$ be a Wirtinger presentation for the knot group, as in Example 2.6. Then by the correspondence $\rho \mapsto (\rho(x_1), \ldots, \rho(x_n))$, $\mathcal{R}_{K,N}$ is identified with the affine algebraic set in $GL_N(\mathbb{C})^n$ defined by $r_1(X_1, \ldots, X_n) = \cdots = r_{n-1}(X_1, \ldots, X_n) = I$:

$$\begin{aligned}\mathcal{R}_{K,N} = \big\{&(X_1, \ldots, X_n) \in GL_N(\mathbb{C})^n \mid \\ &r_1(X_1, \ldots, X_n) = \cdots = r_{n-1}(X_1, \ldots, X_n) = I\big\}.\end{aligned}$$

Let $R_{K,N}$ be the coordinate ring of $\mathcal{R}_{K,N}$ and consider the tautological representation

$$\rho_{K,N} : G_K \longrightarrow GL_N(R_{K,N}); \qquad x_k \mapsto X_k \quad (1 \le k \le n)$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_13, © Springer-Verlag London Limited 2012

which has the following universal property: For any representation $\rho : G_K \to GL_N(A)$ with a $\mathbb{C}$-algebra A, there exists uniquely a $\mathbb{C}$-algebra homomorphism $\varphi : R_{K,N} \to A$ such that $\varphi \circ \rho_{K,N} = \rho$.

The group $GL_N(\mathbb{C})$ acts on the ring $R_{K,N}$ by $(g, X_k) \mapsto gX_kg^{-1}$ $(1 \le k \le n)$. Let $R_{K,N}^{GL_N(\mathbb{C})}$ be the invariant ring of this conjugate action. Then we define the *character variety* $\mathcal{X}_{K,N} = \mathcal{R}_{K,N}/\!/GL_N(\mathbb{C})$ of N-dimensional complex representations of G_K by the affine algebraic set whose coordinate ring is $R_{K,N}^{GL_N(\mathbb{C})}$:

$$\mathcal{X}_{K,N} := \big(\mathrm{Spec}\big(R_{K,N}^{GL_N(\mathbb{C})}\big)\big)(\mathbb{C}) = \mathrm{Hom}_{\mathbb{C}\text{-alg}}\big(R_{K,N}^{GL_N(\mathbb{C})}, \mathbb{C}\big). \tag{13.1}$$

The inclusion $R_{K,N}^{GL_N(\mathbb{C})} \hookrightarrow R_{K,N}$ induces the morphism $\mathcal{R}_{K,N} \to \mathcal{X}_{K,N}$. We write $[\rho] \in \mathcal{X}_{K,N}$ for the image of $\rho \in \mathcal{R}_{K,N}$ under this morphism. Then, for $\rho, \rho' \in \mathcal{R}_{K,N}$, one has $[\rho] = [\rho'] \Leftrightarrow \mathrm{Tr}(\rho) = \mathrm{Tr}(\rho')$ [CuS].

13.2 The Character Variety of Complex 1-Dimensional Representations of a Knot Group and Alexander Ideals

We fix a meridian α of K. Note that a 1-dimensional representation of G_K factors through the Abelianization G_K^{ab}. Since G_K^{ab} is an infinite cyclic group generated by the class of α, we have the following theorem on $\mathcal{X}_{K,1}$ and $\rho_{K,1}$. We set $\Lambda := \mathbb{Z}[t^{\pm 1}] = \mathbb{Z}[G_K^{\mathrm{ab}}]$ $([\alpha] \leftrightarrow t)$.

Theorem 13.1 *The correspondence $\rho \mapsto \rho(\alpha)$ gives an isomorphism*

$$\mathcal{X}_{K,1} \simeq \mathbb{C}^{\times}.$$

Hence, the coordinate ring $R_{K,1}$ of $\mathcal{X}_{K,1}$ is the Laurent polynomial ring $\Lambda_{\mathbb{C}} := \Lambda \otimes_{\mathbb{Z}} \mathbb{C} = \mathbb{C}[t^{\pm 1}]$ over $\mathbb{C}$ and the tautological representation $\rho_{K,1} : G_K \to \Lambda_{\mathbb{C}}^{\times}$ is given by the composite of the Abelianization map $G_K \to G_K^{\mathrm{ab}}$ with the inclusion $G_K^{\mathrm{ab}} \subset \Lambda_{\mathbb{C}}^{\times}$.

Let A_K be the Alexander module of K and let $E_d(A_K)$ be the d-th Alexander ideal for each $d \in \mathbb{N}$. The ideal $E_d(A_K)$ coincides with $E_{d-1}(H_1(X_\infty))$ where X_∞ is the infinite cyclic covering of the knot exterior $X_K = S^3 \setminus \mathrm{int}(V_K)$ (Example 9.9), and $E_0(H_1(X_\infty))$ is generated by the Alexander polynomial $\Delta_K(t)$ (Proposition 11.2). We then define the *d-th Alexander set* in $\mathcal{X}_{K,1}$ by

$$\mathcal{A}_K(d) := \big\{\rho \in \mathcal{X}_{K,1} \mid f\big(\rho(\alpha)\big) = 0 \text{ for any } f \in E_d(A_K)\big\}.$$

Thus, we have a descending series $\mathcal{X}_{K,1} \supset \mathcal{A}_K(1) \supset \cdots \supset \mathcal{A}_K(d) \supset \cdots$. On the other hand, for $\rho \in \mathfrak{X}_{K,1}$, we define the G_K-module $\mathbb{C}(\rho)$ by the additive group $\mathbb{C}$ equipped with G_K-action given by $g.z = \rho(g)z$ $(g \in G_K, z \in \mathbb{C})$. We then define the *$d$-th cohomology jumping set* in $\mathcal{X}_{K,1}$ by

$$\mathcal{C}_K(d) := \big\{\rho \in \mathcal{X}_{K,1} \mid \dim_{\mathbb{C}} H^1\big(G_K, \mathbb{C}(\rho)\big) \ge d\big\}.$$

Thus, we have another descending series $\mathcal{X}_{K,1} \supset \mathcal{C}_K(1) \supset \cdots \supset \mathcal{C}_K(d) \supset \cdots$.

Theorem 13.2 ([Hr, Le]) *One has*

$$\mathcal{A}_K(d) = \mathcal{C}_K(d) \quad (d > 1), \qquad \mathcal{A}_K(1) \cup \{\mathbf{1}\} = \mathcal{C}_K(1),$$

where $\mathbf{1}$ *stands for the trivial representation of* G_K.

For the proof of Theorem 13.2, we prepare one lemma. We regard $\mathbb{C}(\rho)$ as a Λ-module by $t.z = \rho(\alpha)z$ ($t \in \Lambda, z \in \mathbb{C}(\rho)$) and set $A_K(\rho) := A_K \otimes_\Lambda \mathbb{C}(\rho)$.

Lemma 13.3 (1) *We have the following isomorphism*:

$$\mathrm{Hom}_{\mathbb{C}}\big(A_K(\rho), \mathbb{C}\big) \simeq Z^1\big(G_K, \mathbb{C}(\rho)\big),$$

where $Z^1(G_K, \mathbb{C}(\rho))$ *stands for the group of* 1*-cocycles*.

(2) *We have the following*:

$$\dim H^1\big(G_K, \mathbb{C}(\rho)\big) = \begin{cases} \dim A_K(\rho) - 1, & \rho \neq \mathbf{1}, \\ 1, & \rho = \mathbf{1}. \end{cases}$$

Proof (1) By Definition 9.1 and Example 9.7,

$$A_K(\rho) = \left(\bigoplus_{g \in G_K} \mathbb{C}(\rho)\, dg \right) \Big/ \big\langle d(g_1 g_2) - dg_1 - \rho(g_1)\, dg_2 \big\rangle_{\mathbb{C}}.$$

Hence, we have

$$\begin{aligned} \mathrm{Hom}_{\mathbb{C}}\big(A_K(\rho), \mathbb{C}\big) &\simeq \big\{ c : G_K \to \mathbb{C} \mid c(g_1 g_2) - c(g_1) - \rho(g_1) c(g_2) = 0 \big\} \\ &= Z^1\big(G_K, \mathbb{C}(\rho)\big). \end{aligned}$$

(2) Noting that $\rho(g)z = z \Leftrightarrow \rho(g) = 1$ or $z = 0$, the group of 1-coboundaries $B^1(G_K, \mathbb{C}(\rho))$ is given by

$$B^1\big(G_K, \mathbb{C}(\rho)\big) = \begin{cases} \mathbb{C}, & \rho \neq \mathbf{1}, \\ \{0\}, & \rho = \mathbf{1}. \end{cases}$$

Together with (1), we get the assertion. □

Proof of Theorem 13.2 Let Q_K be a representation matrix for the Λ-module A_K:

$$\Lambda^{n-1} \xrightarrow{Q_K} \Lambda^n \longrightarrow A_K \longrightarrow 0 \quad \text{(exact)}. \tag{13.2}$$

The ideal $E_d(A_K)$ is generated by $(n-d)$-minors of Q_K if $d < n$, and is Λ if $d \geq n$. Tensoring $\mathbb{C}(\rho)$ with (13.2) over Λ, we have

$$\mathbb{C}(\rho)^{n-1} \xrightarrow{\rho(Q_K)} \mathbb{C}(\rho)^n \longrightarrow A_K(\rho) \longrightarrow 0 \quad \text{(exact)},$$

where $\rho(Q_K)$ is the matrix over $\mathbb{C}$ obtained by the evaluation $\Lambda \ni t \mapsto \rho(\alpha) \in \mathbb{C}$. Therefore, $\dim A_K(\rho) = n - (\text{rank of } \rho(Q_K))$. Hence we have, for $d > 1$,

$$\begin{aligned}
&\dim H^1\big(G_K, \mathbb{C}(\rho)\big) \geq d \\
&\quad \Leftrightarrow \quad \dim A_K(\rho) \geq d+1 \quad \text{(Lemma 13.3(2))} \\
&\quad \Leftrightarrow \quad \text{rank of } \rho(Q_K) \leq n-(d+1) \\
&\quad \Leftrightarrow \quad \text{any } (n-d)\text{-minor of } \rho(Q_K) = 0 \\
&\quad \Leftrightarrow \quad f\big(\rho(\alpha)\big) = 0 \text{ for any } f \in E_d(A_K),
\end{aligned}$$

and we have, for $d = 1$,

$$\begin{aligned}
&\dim H^1\big(G_K, \mathbb{C}(\rho)\big) \geq 1 \\
&\quad \Leftrightarrow \quad \rho \neq \mathbf{1} \quad \text{and} \quad \dim_{\mathbb{C}} A_K(\rho) \geq 2, \text{ or } \rho = \mathbf{1} \text{ (Lemma 13.3(2))} \\
&\quad \Leftrightarrow \quad \rho \neq \mathbf{1} \quad \text{and} \quad f\big(\rho(\alpha)\big) = 0 \text{ for any } f \in E_1(A_K), \text{ or } \rho = \mathbf{1}.
\end{aligned}$$

The proof is done. □

Corollary 13.4 *Assume that $\rho \neq \mathbf{1}$. Then we have*

$$\Delta_K\big(\rho(\alpha)\big) = 0 \iff H^1\big(G_K, \mathbb{C}(\rho)\big) \neq 0.$$

Proof By $E_1(A_K) = (\Delta_K(t))$ and $\Delta_K(1) = \pm 1$, our assertion follows from Theorem 13.2. □

13.3 Universal Deformation Spaces of p-Adic Representations of a Prime Group

Let p be a prime number and let $G_{\{p\}} = \pi_1(\mathrm{Spec}(\mathbb{Z}[1/p])) = \mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q})$ be the prime group. Here $\mathbb{Q}_{\{p\}}$ is the maximal Galois extension of $\mathbb{Q}$ unramified outside $\{p, \infty\}$. In the following, we assume $p > 2$ and consider representations of $G_{\{p\}}$. Since $G_{\{p\}}$ is a huge pro-finite group (it is not known if $G_{\{p\}}$ is finitely generated or not), we do not have a good moduli space by considering naively all N-dimensional representations of $G_{\{p\}}$ over a ring. So, following B. Mazur [Mz2], we consider the set of p-adic deformations of a given residual representation. Let

$$\overline{\rho} : G_{\{p\}} \longrightarrow GL_N(\mathbb{F}_p)$$

be a given N-dimensional continuous residual (mod p) representation of $G_{\{p\}}$. A pair (A, ρ) is called a *deformation* of $\overline{\rho}$ if

$$\begin{cases}
(1)\ A \text{ is a complete Noetherian local } \mathbb{Z}_p\text{-algebra with redidue field} \\
\quad A/\mathfrak{m}_A = \mathbb{F}_p, \\
(2)\ \rho : G_p \to GL_N(A) \text{ is a continuous representation such that} \\
\quad \rho \bmod \mathfrak{m}_A = \overline{\rho}.
\end{cases}$$

If the composite of $\overline{\rho}$ with the inclusion $GL_N(\mathbb{F}_p) \subset GL_N(\overline{\mathbb{F}}_p)$ for an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ is an irreducible representation over $\overline{\mathbb{F}}_p$, $\overline{\rho}$ is said to be absolutely irreducible. (This is independent of the choice of $\overline{\mathbb{F}}_p$). We say that two deformations (A, ρ) and (A, ρ') are strictly equivalent—written as $\rho \approx \rho'$–, if there is a $P \in I + M_N(\mathfrak{m}_A)$ such that one has $\rho'(g) = P\rho(g)P^{-1}$ for all $g \in G_{\{p\}}$. The following theorem due to Mazur is fundamental.

Theorem 13.5 ([Mz2, 1.2]) *Assume that $\overline{\rho}$ is absolutely irreducible. There is a deformation of $\overline{\rho}$*

$$\rho_{p,N} : G_{\{p\}} \longrightarrow GL_N(R_{p,N})$$

having the following universal property: For any deformation $\rho : G_{\{(p)\}} \to GL_N(A)$ of $\overline{\rho}$, there exists uniquely a $\mathbb{Z}_p$-algebra homomorphism $\varphi : R_{p,N} \to A$ such that $\varphi \circ \rho_{p,N} \approx \rho$. (Although it is more precise to write $R_{p,N}(\bar{\rho})$ since $R_{p,N}$ depends on $\bar{\rho}$, we abbreviate it to $R_{p,N}$ for simplicity.)

If two deformations (A, ρ) and (A', ρ') of $\overline{\rho}$ satisfy the above universal property, we have a $\mathbb{Z}_p$-algebra isomorphism $\varphi : A \xrightarrow{\sim} A'$ such that $\varphi \circ \rho \approx \rho'$. Therefore, the pair $(R_{p,N}, \rho_{p,N})$ is unique in this sense (up to equivalence) and is called the *universal deformation* of $\overline{\rho}$. We define the *universal deformation space* of $\overline{\rho}$ by

$$\mathcal{X}_{p,N}(\overline{\rho}) := \big(\mathrm{Spec}(R_{p,N})\big)(\overline{\mathbb{Q}}_p) = \mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}(R_{p,N}, \overline{\mathbb{Q}}_p), \tag{13.3}$$

where $\overline{\mathbb{Q}}_p$ is an algebraic closure of $\mathbb{Q}_p$ and $\mathcal{X}_{p,N}(\overline{\rho})$ is regarded as a p-adic analytic space. For $\varphi \in \mathcal{X}_{p,N}(\overline{\rho})$, we denote $\varphi \circ \rho_{p,N}$ by ρ_φ.

13.4 The Universal Deformation Space of p-Adic 1-Dimensional Representations of a Prime Group and Iwasawa Ideals

Assume that $p > 2$ for simplicity. Note that a 1-dimensional representation of $G_{\{p\}}$ factors through the Abelianization $G_{\{p\}}^{\mathrm{ab}}$ of $G_{\{p\}}$. By class field theory, we have $G_{\{p\}}^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = H \times \Gamma$, $H := \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = \mathbb{F}_p^\times$, $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = 1 + p\mathbb{Z}_p$. (We keep the same notations as in Sect. 12.2.) We denote by $[g] = (g^{(p)}, g_p)$ the image of $g \in G_{\{p\}}$ under the Abelianization $G_{\{p\}} \to G_{\{p\}}^{\mathrm{ab}} = \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$. Fixing a topological generator γ of $\Gamma = 1 + p\mathbb{Z}_p$, we identify $\mathbb{Z}_p[[\Gamma]]$ with $\hat{\Lambda} := \mathbb{Z}_p[[T]]$ by the correspondence $\gamma \leftrightarrow 1 + T$.

Let $\bar{\rho} : G_{\{p\}} \to \mathbb{F}_p^\times$ be a 1-dimensional continuous residual representation. We identify $\mathbb{F}_p^\times$ with the group of $(p-1)$-th roots of 1 in $\mathbb{Z}_p^\times$. Then the *Teichmüller lift* $\tilde{\rho}$ of $\bar{\rho}$ is defined by the composite of $\bar{\rho}$ with the inclusion $\mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$. The following theorem may be regarded as an arithmetic analogue of Theorem 13.1.

Theorem 13.6 ([Mz2, 1.4]) *Define $\rho_{p,1} : G_{\{p\}} \to \hat{\Lambda}^\times$ by*

$$\rho_{p,1}(g) := \tilde{\rho}(g)g_p.$$

Then the pair $(\hat{\Lambda}, \rho_{p,1})$ *is the universal deformation of* $\bar{\rho}$. *Hence,* $\mathcal{X}_{p,1}(\bar{\rho})$ *is identified with the p-adic unit disk* $\mathcal{D}_p := \{x \in \overline{\mathbb{Q}}_p \mid |x|_p < 1\}$:

$$\mathcal{X}_{p,1}(\bar{\rho}) \xrightarrow{\sim} \mathcal{D}_p; \qquad \varphi \mapsto \varphi(T).$$

Proof Since $\rho_{p,1}(g) \bmod \mathfrak{m}_{\hat{\Lambda}} = \tilde{\rho}(g) \bmod p = \bar{\rho}(g)$, $\rho_{p,1}$ is a deformation of $\bar{\rho}$. Let (A, ρ) be any deformation of $\bar{\rho}$: $A/\mathfrak{m}_A = \mathbb{F}_p$, $\rho(g) \bmod \mathfrak{m}_A = \bar{\rho}(g)$. Define the $\mathbb{Z}_p$-algebra homomorphism $\varphi : \hat{\Lambda} \to A$ by $\varphi(g_p) := \rho((1, g_p))$, $g_p \in \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. For any $g \in G_{\{p\}}$, we have

$$\begin{aligned}(\varphi \circ \rho_{p,1})(g) &= \varphi\big(\tilde{\rho}(g) g_p\big) \\ &= \tilde{\rho}(g)\rho\big((1, g_p)\big) \\ &= \rho(g) \quad \big(\tilde{\rho}(g) = \rho\big(\big(g^{(p)}, 1\big)\big)\big).\end{aligned}$$

The uniqueness of φ is clear and hence $(\hat{\Lambda}, \rho_{p,1})$ is the universal deformation of $\bar{\rho}$. The assertion about $\mathcal{X}_{p,1}(\bar{\rho})$ is obvious. □

As in the case of the Alexander polynomial, the zeros of the Iwasawa polynomial are described by the variation of Galois cohomology of $G_{\{p\}}$ on the universal deformation space $\mathfrak{X}_p(\bar{\rho})$. In the following, we show it for the Iwasawa polynomial $\Delta_p^{(j)}(T)$ in Sect. 12.2. We keep the same notations as in Sect. 12.2.

Let $\bar{\omega} : G_{\{p\}} \to H = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \simeq \mathbb{F}_p^\times$ be the natural homomorphism. We denote the composite of the natural map $G_{\{p\}} \to H$ with $\omega : H \hookrightarrow \mathbb{Z}_p^\times$ in Sect. 12.2 by the same ω. This ω is the Teichmüller lift of $\bar{\omega}$. For each $j \bmod p-1$, let $\rho^{(j)} : G_{\{p\}} \to \hat{\Lambda}^\times$ be the universal deformation of $\bar{\omega}^j$ and let $\mathcal{X}_p^{(j)} := \mathcal{X}_{p,1}(\bar{\omega}^j)$ be the universal deformation space of $\bar{\omega}^j$. For $\varphi \in \mathcal{X}_p^{(j)}$, we set $\rho_\varphi^{(j)} := \varphi \circ \rho^{(j)}$.

Let $\psi : G_{\{p\}} \to \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = H \times \Gamma$ be the Abelianization map and let $\mathfrak{A}_p$ be the complete ψ-differential module. Set $\tilde{\Lambda} := \mathbb{Z}_p[[H \times \Gamma]] = \mathbb{Z}_p[H][[\Gamma]]$. Then $\mathfrak{A}_p$ is a $\tilde{\Lambda}$-module. Let $\mathfrak{A}_p^{(j)} := \mathfrak{A}_p \otimes_{\tilde{\Lambda}} \tilde{\Lambda}^{(j)}$. By tensoring $\tilde{\Lambda}^{(j)}$ with the complete Crowell exact sequence (Theorem 9.17)

$$0 \longrightarrow \mathfrak{M} \longrightarrow \mathfrak{A}_p \longrightarrow I_{\tilde{\Lambda}} \longrightarrow 0$$

over $\tilde{\Lambda}$, we have the exact sequence of $\tilde{\Lambda}^{(j)}$-modules

$$0 \longrightarrow \mathfrak{M}^{(j)} \longrightarrow \mathfrak{A}_p^{(j)} \longrightarrow I_{\tilde{\Lambda}^{(j)}} \longrightarrow 0$$

for each $j \bmod p-1$. From this, we have $E_{d-1}(\mathfrak{M}^{(j)}) = E_d(\mathfrak{A}_p^{(j)})$ for $d \geq 1$. When j is even, $E_0(\mathfrak{M}^{(j)}) = E_1(\mathfrak{A}_p^{(j)})$ is generated by the Iwasawa polynomial $\Delta_p^{(j)}(T)$ (Proposition 12.8). We then define the *d-th Iwasawa set* in $\mathcal{X}_p^{(j)}$ by

$$\mathcal{A}_p^{(j)}(d) := \big\{\varphi \in \mathcal{X}_p^{(j)} \mid f\big(\varphi(\gamma) - 1\big) = 0 \text{ for all } f \in E_d\big(\mathfrak{A}_p^{(j)}\big)\big\}.$$

Thus, we have a descending series $\mathcal{X}_p^{(j)} \supset \mathcal{A}_p^{(j)}(1) \supset \cdots \supset \mathcal{A}_p^{(j)}(d) \supset \cdots$. On the other hand, for $\varphi \in \mathcal{X}_p^{(j)}$, we define the $G_{\{p\}}$-module $\overline{\mathbb{Q}}_p(\rho_\varphi^{(j)})$ by the additive group $\overline{\mathbb{Q}}_p$ equipped with $G_{\{p\}}$-action given by $g.z = \rho_\varphi^{(j)}(g)z$, $(g \in G_{\{p\}}, z \in \overline{\mathbb{Q}}_p)$. We then define the *$d$-th cohomology jumping set* in $\mathcal{X}_p^{(j)}$ by

$$\mathcal{C}_p^{(j)}(d) := \left\{\rho \in \mathcal{X}_p^{(j)} \mid \dim_{\overline{\mathbb{Q}}_p} H^1\left(G_K, \overline{\mathbb{Q}}_p\left(\rho_\varphi^{(j)}\right)\right) \geq d\right\}.$$

Thus, we have another descending series $\mathcal{X}_p^{(j)} \supset \mathcal{C}_p^{(j)}(1) \supset \cdots \supset \mathcal{C}_p^{(j)}(d) \supset \cdots$.

Theorem 13.7 ([M10]) *For each even $j \pmod{p-1}$, one has*

$$\mathcal{A}_p^{(j)}(d) = \mathcal{C}_p^{(j)}(d) \quad (d > 1),$$
$$\mathcal{A}_p^{(j)}(1) = \mathcal{C}_p^{(j)}(1) \quad (j \neq 0), \qquad \mathcal{A}_p^{(0)}(1) \cup \{\mathbf{1}\} = \mathcal{C}_p^{(0)}(1),$$

where $\mathbf{1}$ stands for the trivial representation of $G_{\{p\}}$.

We regard $\overline{\mathbb{Q}}_p(\rho_\varphi^{(j)})$ as a $\tilde{\Lambda}$-module and set $\mathfrak{A}_p(\rho_\varphi^{(j)}) := \mathfrak{A}_p \otimes_{\tilde{\Lambda}} \overline{\mathbb{Q}}_p(\rho_\varphi^{(j)})$. If we denote by $\overline{\mathbb{Q}}_p(\varphi)$ the additive group $\overline{\mathbb{Q}}_p$ with Γ-action defined by $\gamma.z := \varphi(\gamma)z$, we have $\mathfrak{A}_p(\rho_\varphi^{(j)}) = \mathfrak{A}_p^{(j)} \otimes_{\hat{\Lambda}} \overline{\mathbb{Q}}_p(\varphi)$.

Lemma 13.8 (1) *We have the following isomorphism*:

$$\mathrm{Hom}_{\overline{\mathbb{Q}}_p}\left(\mathfrak{A}_p\left(\rho_\varphi^{(j)}\right), \overline{\mathbb{Q}}_p\right) \simeq Z^1\left(G_{\{p\}}, \overline{\mathbb{Q}}_p\left(\rho_\varphi^{(j)}\right)\right),$$

where $Z^1(G_{\{p\}}, \overline{\mathbb{Q}}_p(\rho_\varphi^{(j)}))$ stands for the group of continuous 1-cocycles.

(2) *We have the following*:

$$\dim H^1\left(G_{\{p\}}, \overline{\mathbb{Q}}_p\left(\rho_\varphi^{(j)}\right)\right) = \begin{cases} \dim \mathfrak{A}_p(\rho_\varphi^{(j)}) - 1, & (j, \varphi) \neq (0, \mathbf{1}), \\ 1, & (j, \varphi) = (0, \mathbf{1}). \end{cases}$$

Proof (1) By Definition 9.10,

$$\mathfrak{A}_p\left(\rho_\varphi^{(j)}\right) = \left(\bigoplus_{g \in G_{\{p\}}} \overline{\mathbb{Q}}_p\left(\rho_\varphi^{(j)}\right) dg\right) \Big/ \left\langle d(g_1 g_2) - dg_1 - \rho_\varphi^{(j)}(g_1)\, dg_2 \right\rangle_{\overline{\mathbb{Q}}_p}.$$

Hence, we have

$$\begin{aligned} \mathrm{Hom}_{\overline{\mathbb{Q}}_p}\left(\mathfrak{A}_p\left(\rho_\varphi^{(j)}\right), \overline{\mathbb{Q}}_p\right) &\simeq \left\{c : G_{\{p\}} \to \overline{\mathbb{Q}}_p \mid c(g_1 g_2) - c(g_1) - \rho_\varphi^{(j)}(g_1) c(g_2) = 0\right\} \\ &= Z^1\left(G_{\{p\}}, \overline{\mathbb{Q}}_p\left(\rho_\varphi^{(j)}\right)\right). \end{aligned}$$

(2) By definition of $\rho^{(j)}$, we have $\rho_\varphi^{(j)} = \mathbf{1} \Leftrightarrow (i, \varphi) = (0, \mathbf{1})$. Therefore, the group of coboundaries $B^1(G_{\{p\}}, \overline{\mathbb{Q}}_p(\rho_\varphi^{(j)}))$ is given by

$$B^1\big(G_{\{p\}}, \overline{\mathbb{Q}}_p\big(\rho_\varphi^{(j)}\big)\big) = \begin{cases} \overline{\mathbb{Q}}_p, & (j, \varphi) \neq (0, \mathbf{1}), \\ \{0\}, & (j, \varphi) = (0, \mathbf{1}). \end{cases}$$

Together with (1), we get the assertion. □

Proof of Theorem 13.7 Let j be an even integer. Then $\mathfrak{M}^{(j)}$ is a finitely generated, torsion $\hat{\Lambda}$-module (Proposition 12.8). Let $\mathfrak{Q}_p^{(j)}$ be a representation matrix of the $\hat{\Lambda}$-module $\mathfrak{A}_p^{(j)}$:

$$\hat{\Lambda}^m \xrightarrow{\mathfrak{Q}_p^{(j)}} \hat{\Lambda}^n \longrightarrow \mathfrak{A}_p^{(j)} \longrightarrow 0 \quad \text{(exact)}. \tag{13.4}$$

The ideal $E_d(\mathfrak{A}_p^{(j)})$ is generated by $(n-d)$-minors of $\mathfrak{Q}_p^{(j)}$ if $d < n$, and is $\hat{\Lambda}$ if $d \geq n$. By tensoring $\overline{\mathbb{Q}}_p(\varphi)$ with (13.4) over $\hat{\Lambda}$, we have the exact sequence

$$\overline{\mathbb{Q}}_p(\varphi)^m \xrightarrow{\varphi(\mathfrak{Q}_p^{(j)})} \overline{\mathbb{Q}}_p(\varphi)^n \longrightarrow \mathfrak{A}_p(\rho_\varphi^{(j)}) \longrightarrow 0 \quad \text{(exact)},$$

where $\varphi(\mathfrak{Q}_p^{(j)})$ is the matrix over $\overline{\mathbb{Q}}_p$ obtained by the evaluation $\hat{\Lambda} \ni T \mapsto \varphi(T) \in \overline{\mathbb{Q}}_p$. Therefore, we have $\dim \mathfrak{A}_p(\rho_\varphi^{(j)}) = n - (\text{rank of } \varphi(\mathfrak{Q}^{(j)}))$. Hence we have, for $d > 1$,

$$\begin{aligned} &\dim H^1\big(G_{\{p\}}, \overline{\mathbb{Q}}_p\big(\rho_\varphi^{(j)}\big)\big) \geq d \\ &\quad \Leftrightarrow \quad \dim \mathfrak{A}_p\big(\rho_\varphi^{(j)}\big) \geq d+1 \quad \text{(Lemma 13.8(2))} \\ &\quad \Leftrightarrow \quad \text{rank of } \varphi\big(\mathfrak{Q}_p^{(j)}\big) \leq n-(d+1) \\ &\quad \Leftrightarrow \quad \text{any } (n-d)\text{-minor of } \varphi\big(\mathfrak{Q}_p^{(j)}\big) = 0 \\ &\quad \Leftrightarrow \quad \text{for all } f \in E_d\big(\mathfrak{A}_p\big(\rho_\varphi^{(j)}\big)\big), \\ &\qquad\quad f\big(\varphi(\gamma) - 1\big) = 0, \end{aligned}$$

and we have, for $d = 1$,

$$\begin{aligned} &\dim H^1\big(G_{\{p\}}, \overline{\mathbb{Q}}_p\big(\rho_\varphi^{(j)}\big)\big) \geq 1 \\ &\quad \Leftrightarrow \quad \rho_\varphi^{(j)} \neq \mathbf{1} \quad \text{and} \quad \dim \mathfrak{A}_p\big(\rho_\varphi^{(i)}\big) \geq 2, \quad \text{or} \quad \rho_\varphi^{(j)} = \mathbf{1} \quad \text{(Lemma 13.8(2))} \\ &\quad \Leftrightarrow \quad (j, \varphi) \neq (0, \mathbf{1}) \quad \text{and} \quad f\big(\varphi(\gamma) - 1\big) = 0 \quad \text{for all } f \in E_1\big(\mathfrak{A}_p(\rho_\varphi^{(j)})\big), \\ &\qquad\quad \text{or } (j, \varphi) = (0, \mathbf{1}). \end{aligned}$$

The proof is done. □

Corollary 13.9 *For each even* $j \pmod{p-1}$, *we have*

$$\Delta_p^{(j)}\big(\varphi(\gamma)-1\big)=0 \iff H^1\big(G_{\{p\}},\overline{\mathbb{Q}}_p\big(\rho_\varphi^{(j)}\big)\big)\neq 0.$$

Proof This follows from $E_1(\mathfrak{A}_p^{(j)})=(\Delta_p^{(j)})$ and Theorem 13.7. □

Remark 13.10 (1) It is known that the Alexander module A_K (or the knot module $H_1(X_\infty)$) has a standard resolution by the Seifert matrix [Kw, 5.4]. As for the Iwasawa module $H_\infty^{(i)}$, M. Kurihara gave a resolution using a certain Euler–Kolyvagin system and showed a refined form of the main conjecture of Iwasawa [Kr1, Kr2].

(2) It would be interesting to extend Theorem 13.2 and Theorem 13.7 for higher dimensional representations of the knot and prime groups (cf. [Mz4])

Summary

Character variety of N-dim. complex representations of G_K $\mathcal{X}_{K,N}$	Deformation space of N-dim. p-adic representations of $G_{\{p\}}$ $\mathcal{X}_{p,N}(\overline{\rho})$
$\mathcal{X}_{K,1}=\mathrm{Hom}_{\mathbb{C}\text{-alg}}(\Lambda,\mathbb{C})=\mathbb{C}^\times$ $(\Lambda=\mathbb{Z}[t^{\pm 1}])$	$\mathcal{X}_{p,1}(\overline{\rho})=\mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}(\hat{\Lambda},\overline{\mathbb{Q}}_p)=\mathcal{D}_p$ $(\hat{\Lambda}=\mathbb{Z}_p[[T]])$
d-th Alexander set (Zeros of Alexander polynomial) and cohomology jump set	d-th Iwasawa set (Zeros of Iwasawa polynomial) and cohomology jump set

Chapter 14
Deformations of Hyperbolic Structures and p-Adic Ordinary Modular Forms

As we have seen in Chap. 13, the Alexander–Fox theory and Iwasawa theory may be regarded as theories on the moduli spaces of 1-dimensional representations. H. Hida [Hd1, Hd2] and B. Mazur [Mz2] generalized the Iwasawa theory to a non-Abelian theory from the viewpoint of the deformation theory of higher dimensional representations. A similar theory on the moduli of higher dimensional representations of a knot group would provide a natural non-Abelian generalization of the Alexander–Fox theory. In particular, for 2-dimensional representations, we find intriguing analogies between the family of holonomy representations associated to deformations of hyperbolic structures and the family of Galois representations associated to deformations of p-adic ordinary modular forms.

We refer to [Th] and [Hd3] for 3-dimensional hyperbolic geometry and modular forms, respectively.

14.1 Deformation of Hyperbolic Structures

Let K be a hyperbolic knot in S^3. Namely, $S^3 \setminus K$ is a complete hyperbolic 3-manifold of finite volume with a cusp. Thus, the knot group G_K is a discrete subgroup of $PSL_2(\mathbb{C}) = \mathrm{Aut}(\mathbb{H}^3)$, where $\mathbb{H}^3$ denotes the hyperbolic 3-space, and $S^3 \setminus K$ is written as the quotient space $\mathbb{H}^3/G_K$. Let V_K be a tubular neighborhood of K and $X_K := S^3 \setminus \mathrm{int}(V_K)$, and fix a meridian α and a longitude β of K $(\alpha, \beta \subset \partial X_K)$.

Let $\bar{\rho}_h : G_K \to PSL_2(\mathbb{C})$ be the holonomy representation associated to the complete hyperbolic structure on $S^3 \setminus K$. Since $H^2(G_K, \mathbb{F}_2) = H^2(X_K, \mathbb{F}_2) = 0$, we note that $\bar{\rho}_h \in H^1(G_K, PSL_2(\mathbb{C}))$ can be lifted to $\rho_h \in H^1(G_K, SL_2(\mathbb{C}))$ by considering the exact sequence of group cohomology with non-commutative coefficients [Se2, Chap. VII, Appendix] attached to the exact sequence $1 \to \{\pm I\} \to SL_2(\mathbb{C}) \to PSL_2(\mathbb{C}) \to 1$. In this chapter, we shall be concerned with representations of G_K associated to (incomplete) hyperbolic structures and therefore we shall consider $SL_2(\mathbb{C})$-representations of G_K in the following, and thus set

$$\mathcal{R}_K := \mathrm{Hom}\big(G_K, SL_2(\mathbb{C})\big), \qquad \mathcal{X}_K := \mathcal{R}_K /\!\!/ GL_2(\mathbb{C}).$$

M. Morishita, *Knots and Primes*, Universitext,
DOI 10.1007/978-1-4471-2158-9_14, © Springer-Verlag London Limited 2012

Since $D_K = \pi_1(\partial X_K)$ is Abelian, the restriction of $\rho \in \mathrm{Hom}(G_K, SL_2(\mathbb{C}))$ to D_K is equivalent to an upper triangular representation:

$$\rho|_{D_K} \simeq \begin{pmatrix} \chi_\rho & * \\ 0 & \chi_\rho^{-1} \end{pmatrix}, \tag{14.1}$$

where $\chi_\rho : G_K \to \mathbb{C}^\times$ is a 1-dimensional representation. Let $\mathcal{X}_K^\circ(\rho_h)$ be the connected component of $\mathcal{X}_K$ containing ρ_h. Then we have the following theorem due to W. Thurston. (For the proof, we refer to [Th], [BP, Appendix B].)

Theorem 14.1 *The mapping*

$$\Psi_K : \mathcal{X}_K^\circ(\rho_h) \longrightarrow \mathbb{C}; \qquad \Psi_K([\rho]) := \mathrm{Tr}\big(\rho(\alpha)\big)$$

is biholomorphic in a neighborhood W of $[\rho_h]$. In particular, $\mathcal{X}_K^\circ(\rho_h)$ is a complex algebraic curve.

The character curve $\mathcal{X}_K^\circ(\rho_h)$ is related to the deformation space of hyperbolic structures on $S^3 \setminus K$ as follows. Let $S(z)$ denote the ideal tetrahedron in $\mathbb{H}^3$ with vertices $0, 1, z$ and ∞ ($z \in \mathbb{C} \setminus \{0, 1\}$) (Fig. 14.1).

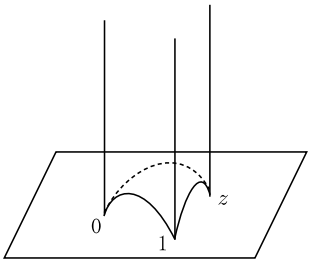


Fig. 14.1

Fix an ideal triangulation of $S^3 \setminus K$

$$S^3 \setminus K = S(z_1^\circ) \cup \cdots \cup S(z_n^\circ).$$

At each edge, the sum of dihedral angles of the tetrahedron around the edge is equal 2π. The parameters $z_1^\circ, \ldots, z_n^\circ$ satisfy a system of equation of the form

$$\prod_{i=1}^{n} z_i^{r'_{ij}} (1 - z_i)^{r'_{ij}} = \pm 1 \quad (j = 1, \ldots, n). \tag{14.2}$$

Let $\mathcal{Y}$ be the affine algebraic set in $(\mathbb{C} \setminus \{0, 1\})^n$ defined by (14.2). W. Neumann and D. Zagier [NZ] showed that the irreducible component $\mathcal{X}_K^{\mathrm{H}}(z^\circ)$ of $\mathcal{Y}$ containing $z^\circ := (z_1^\circ, \ldots, z_n^\circ)$ is a complex algebraic curve, called the *deformation curve of hyperbolic structures*. Then $\mathcal{X}_K^{\mathrm{H}}(z^\circ)$ is a double covering over $W \subset \mathcal{X}_K^\circ(\rho_h)$.

Namely, there are a neighborhood U of z° in $\mathcal{X}_K^{\mathrm{H}}(z^\circ)$ and a holomorphic local coordinate x_K on U with $x_K(z^\circ) = 0$ such that we have the following commutative diagram:

$$\begin{array}{ccc} U & \overset{x_K}{\hookrightarrow} & \mathbb{C} \\ \pi \downarrow & & \downarrow h \\ W & \overset{\Psi_K}{\hookrightarrow} & \mathbb{C} \end{array}$$

where $h(x) := e^{x/2} + e^{-x/2}$ and π is a double covering ramified over z°. In fact, for each $z \in U$, we can construct the developing mapping $\widetilde{S^3 \setminus K} \to \mathbb{H}^3$ with holonomy representation $\bar{\rho}_z$, and express a lift ρ_z, $SL_2(\mathbb{C})$-representation, of $\bar{\rho}_z$ as $\rho_z = t(\pi(z))$ by a local section $t : W \to \mathcal{R}_K$. Then we have the following:

$$\rho_z(\alpha) \simeq \begin{pmatrix} e^{x_K(z)/2} & * \\ 0 & e^{-x_K(z)/2} \end{pmatrix},$$

$$\rho_z(\beta) \simeq \begin{pmatrix} e^{y_K(z)/2} & * \\ 0 & e^{-y_K(z)/2} \end{pmatrix}.$$

Here, using χ_ρ of (14.1), we have

$$x_K(z) = 2\log \chi_{\rho_z}(\alpha), \qquad y_K(z) = 2\log \chi_{\rho_z}(\beta) \quad (z \in U).$$

For each $z \in U$, we define $(q, p) \in \mathbb{R}^2 \cup \{\infty\} = S^2$ by $(q, p) := \infty$ if $z = z^\circ$ and by $qx_K(z) + py_K(z) = 2\pi\sqrt{-1}$ if $z \neq z^\circ$. Then the correspondence $z \mapsto (q, p)$ gives an homeomorphism from U to a neighborhood of ∞ in S^2. When p, q are coprime integers, we obtain a closed hyperbolic 3-manifold $M(q, p)$ by the *Dehn surgery* along K with surgery coefficient q/p. (For a solid torus V and a meridian $m \subset \partial V$, $M(q, p)$ is obtained by gluing X_K and V by a homeomorphism $f : \partial V \overset{\approx}{\to} \partial V_K = \partial X_K$ such that $[f_*(m)] = q[\alpha] + p[\beta]$.) A point $z \in U$ corresponding to such a (q, p) or z° is called a *Dehn surgery point with integral coefficient*.

Since x_K is a local coordinate on U, y_K can be regarded as a function of x_K. Then it was shown by Neumann–Zagier [NZ] that there is a holomorphic function $\tau(x_K)$ such that $y_K = x_K\tau(x_K)$ and $\tau(0)$ is a modulus of the 2-dimensional torus ∂X_K whose complex structure is induced by the complete hyperbolic structure on $S^3 \setminus K$.

Theorem 14.2 ([NZ, Lemma 4.1]) *Let* $q_K := \exp(2\pi\sqrt{-1}\tau(0))$. *Then* q_K *gives a multiplicative period of* ∂X_K: $\partial X_K = \mathbb{C}^\times/(q_K)^{\mathbb{Z}}$, *and we have*

$$\left.\frac{dy_K}{dx_K}\right|_{x_K=0} = \frac{1}{2\pi\sqrt{-1}}\log q_K.$$

The integral of y_K with respect to x_K is related with the $SL_2(\mathbb{C})$-Chern–Simons functional as follows. For an $sl_2(\mathbb{C})$-valued 1-form A on X_K, the $SL_2(\mathbb{C})$-*Chern–Simons functional* is defined by

$$CS(A) := \frac{1}{8\pi^2}\int_{X_K} \mathrm{Tr}\left(dA \wedge A + \frac{2}{3}A \wedge A \wedge A\right).$$

For $z \in \mathcal{X}_K^{\mathrm{H}}(z^\circ)$, we define $CS(\rho_z)$ by $CS(A_{\rho_z})$ where A_{ρ_z} is the connection 1-form of the flat connection corresponding to the representation ρ_z.

Theorem 14.3 ([MT2]) *Notation being as above, we have*

$$\int_0^{x_K(z)} y_K\, dx_K - \frac{1}{2}x_K y_K = 8\pi^2 CS(\rho_z) \quad (z \in U).$$

14.2 Deformation of p-Adic Ordinary Modular Galois Representations

Let p be an odd prime number, $G_{\{p\}}$ the prime group, and $D_{\{p\}}$, $I_{\{p\}}$ the decomposition, inertia groups over p respectively (Example 2.40). We shall be concerned with 2-dimensional p-adic representations of $G_{\{p\}}$. Firstly, in order to obtain an arithmetic analogue of the boundary condition (14.1), which is automatically satisfied for the knot case, we consider the 'boundary' condition, called p-ordinariness, on representations $G_{\{p\}}$, following after the analogy (3.9). Namely, a representation $\rho : G_{\{p\}} \to GL_2(A)$ is said to be *p-ordinary*, if $\rho|_{D_{\{p\}}}$ is equivalent to an upper triangular representation of the following type:

$$\rho|_{D_{\{p\}}} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}, \qquad \chi_2|_{I_{\{p\}}} = \mathbf{1},$$

where $\chi_i : D_{\{p\}} \to A^\times$ is a 1-dimensional representation ($i = 1, 2$).

Now we fix an absolutely irreducible and p-ordinary continuous residual representation $\bar{\rho} : G_{\{p\}} \to GL_2(\mathbb{F}_p)$. Then we have the following theorem for *p-ordinary deformation* of $\bar{\rho}$:

Theorem 14.4 ([Mz2, 1.7]) *There is a p-ordinary deformation of $\overline{\rho}$*

$$\rho_p^\circ : G_{\{p\}} \longrightarrow GL_2(R_p^\circ)$$

such that for any p-ordinary deformation $\rho : G_{\{p\}} \to GL_N(A)$ of $\overline{\rho}$, there exists uniquely a $\mathbb{Z}_p$-algebra homomorphism $\varphi : R_p^\circ \to A$ with $\varphi \circ \rho_p^\circ \approx \rho$.

The pair $(R_p^\circ, \rho_p^\circ)$ is unique up to equivalence and called the *universal p-ordinary deformation* of $\overline{\rho}$. We define the *universal p-ordinary deformation space* of $\overline{\rho}$ by

$$\mathcal{X}_p^\circ(\overline{\rho}) := \big(\mathrm{Spec}(R_p^\circ)\big)(\overline{\mathbb{Q}}_p) = \mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}(R_p^\circ, \overline{\mathbb{Q}}_p).$$

We regard $\mathcal{X}_p^\circ(\bar{\rho})$ as an arithmetic analogue of $\mathcal{X}_K^\circ$.

Since $\det \boldsymbol{\rho}_p^\circ : G_{\{p\}} \to (R_p^\circ)^\times$ is a deformation of $\det \bar{\rho} : G_{\{p\}} \to \mathbb{F}_p^\times$, by Theorem 13.6, there exists a unique $\mathbb{Z}_p$-algebra homomorphism $\iota^\circ : \hat{\Lambda} \to R_p^\circ$ such that $\iota^\circ \circ \rho_{p,1} = \det \boldsymbol{\rho}_p^\circ$. We regard R_p° as a $\hat{\Lambda}$-algebra via ι°.

The deformation space $\mathcal{X}_p^\circ(\bar{\rho})$ is related with the family of Galois representations in Hida's theory on the universal ordinary p-adic Hecke algebra. Firstly, we recall some facts on Galois representations associated to modular forms. Let f be a cuspidal eigenform of level p-power on $\Gamma_0(p^m)$ $(m \geq 1)$ of weight $w_f \geq 2$ and character ε_f. Here we mean by f being an eigenform that f is an eigenfunction of the Hecke operator T_l for each prime number $l \neq p$ and an eigenfunction of the Atkin operator U_p. For the Fourier expansion $f = \sum_{n\geq 1} a_n(f) e^{2\pi\sqrt{-1}nz}$ at ∞, the Fourier coefficients $a_l(f)$ $(l \neq p)$ and $a_p(f)$ are eigenvalues of T_l and U_p respectively. Let $\mathcal{O}_f$ be the integral closure of the ring $\mathbb{Z}[a_n(f) | n \geq 1]$ in $\mathbb{C}$. Then $\mathcal{O}_f$ is the ring of integers in a finite algebraic number field k_f. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_f$ over p, let $k_{f,\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of k_f and $\mathcal{O}_{f,\mathfrak{p}}$ the ring of integers of $k_{f,\mathfrak{p}}$.

Theorem 14.5 (1) ([Dl]) *There is an absolutely irreducible representation*

$$\rho_{f,\mathfrak{p}} : G_{\{p\}} \longrightarrow GL_2(\mathcal{O}_{f,\mathfrak{p}})$$

such that for any prime number $l \neq p$, one has

$$\mathrm{Tr}\big(\rho_{f,\mathfrak{p}}(\sigma_l)\big) = a_l(f), \qquad \det\big(\rho_{f,\mathfrak{p}}(\sigma_l)\big) = \varepsilon_f(l) l^{w_f - 1},$$

and such a representation is unique up to equivalence over $k_{f,\mathfrak{p}}$. Here $\sigma_l \in G_{\{p\}}$ stands for the Frobenius automorphism over l.

(2) ([MW2]) *Assume that f is p-ordinary, namely, $a_p(f) \in \mathcal{O}_{f,\mathfrak{p}}^\times$ (This condition is independent of the choice of $\mathfrak{p}$). Then $\rho_{f,\mathfrak{p}}$ is also p-ordinary*:

$$\rho_{f,\mathfrak{p}}|_{D_{\{p\}}} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}, \qquad \chi_2|_{I_{\{p\}}} = \mathbf{1}.$$

In the rest of this chapter, we fix an absolutely irreducible representation

$$\bar{\rho} = \rho_{f^\circ,\mathfrak{p}} \bmod \mathfrak{p} : G_{\{p\}} \longrightarrow GL_2(\mathbb{F}_p)$$

associated to a p-ordinary cuspidal eigenform f° with $\mathcal{O}_{f^\circ}/\mathfrak{p} = \mathbb{F}_p$. Hida [Hd1, Hd2] constructed a big Galois representation from a certain completion of the Hecke algebra which has the following universal property.

Theorem 14.6 ([Hd1, Hd2]) *There is a p-ordinary deformation of $\bar{\rho}$*

$$\rho_p^{\mathrm{H}} : G_{\{p\}} \longrightarrow GL_2\big(R_p^{\mathrm{H}}\big)$$

which has the following property: *If $\rho_{f,\mathfrak{p}} : G_{\{p\}} \to GL_2(\mathcal{O}_{f,\mathfrak{p}})$ is a deformation of $\bar{\rho}$ associated to a p-ordinary cuspidal eigenform f of level p-power, there exists a unique $\mathbb{Z}_p$-algebra homomorphism $\varphi : R_p^{\mathrm{H}} \to \mathcal{O}_{f,\mathfrak{p}}$ such that $\varphi \circ \rho_2^{\mathrm{H}} \approx \rho_{f,\mathfrak{p}}$.*

Such a pair $(R_p^{\mathrm{H}}, \rho_p^{\mathrm{H}})$ is unique up to equivalence and is called the *universal p-ordinary modular deformation* of $\bar{\rho}$. We define the *universal p-ordinary modular deformation space* by

$$\mathcal{X}_p^{\mathrm{H}}(\bar{\rho}) := \mathrm{Spec}\big(R_p^{\mathrm{H}}\big)(\overline{\mathbb{Q}}_p) = \mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}\big(R_p^{\mathrm{H}}, \overline{\mathbb{Q}}_p\big).$$

For $\varphi \in \mathcal{X}_p^{\mathrm{H}}(\bar{\rho})$, we write $\rho_\varphi^{\mathrm{H}}$ for $\varphi \circ \rho_p^{\mathrm{H}}$.

Let $(R_{p,1} = \hat{\Lambda}, \rho_{p,1})$ be the universal deformation of $\det \bar{\rho}$. Then there exists uniquely a $\mathbb{Z}_p$-algebra homomorphism $\iota^{\mathrm{H}} : \hat{\Lambda} \to R_p^{\mathrm{H}}$ such that $\iota^{\mathrm{H}} \circ \rho_{p,1} = \det \rho_p^{\mathrm{H}}$. Via ι^{H}, we regard R_p^{H} as a $\hat{\Lambda}$-algebra. ι^{H} induces a p-adic analytic mapping

$$x_p : \mathcal{X}_p^{\mathrm{H}}(\bar{\rho}) \longrightarrow \mathcal{D}_p; \qquad \varphi \mapsto \big(\varphi \circ \iota^{\mathrm{H}}\big)(T).$$

A prime ideal $\mathfrak{P} \in \mathrm{Spec}(R_p^{\mathrm{H}})$ of height 1 is called an *arithmetic point*, if there are integers $w \geq 0$ and a Dirichlet character ε mod p-power such that the image of $1+T$ under the natural homomorphism $R_{p,2}^{\mathrm{H}} \to R_{p,2}^{\mathrm{H}}/\mathfrak{P}$ equals $\varepsilon(1+p)(1+p)^{w-2}$. Then the point $\mathfrak{P}$ corresponds to a cuspidal eigenform of weight w and character ε. A point $\varphi \in \mathcal{X}_p^H(\bar{\rho})$ is called an *arithmetic point*, if $\mathfrak{P} = \mathrm{Ker}(\varphi)$ is an arithmetic point. Arithmetic points in $\mathcal{X}_p^H(\bar{\rho})$ may be viewed as analogues of Dehn surgery points of integral coefficients in the deformation space $\mathcal{X}_K^{\mathrm{H}}(z^\circ)$ of hyperbolic structures. As for the $\hat{\Lambda}$-algebra structure of R_p^{H}, the following theorem, due to Hida, is fundamental for us.

Theorem 14.7 ([Hd1, Corollary 1.4], [Hd2]) *R_p^{H} is a finite and flat algebra over $\hat{\Lambda}$. Furthermore, $(R_p^{\mathrm{H}})_{\mathfrak{P}}$ is an étale algebra over $\hat{\Lambda}_{\mathfrak{p}}$ for any arithmetic point $\mathfrak{P} \in \mathrm{Spec}(R_p^{\mathrm{H}})$ where $\mathfrak{p} := (\iota^H)^{-1}(\mathfrak{P})$. In particular x_p gives a p-adic analytic local coordinate around φ.*

Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ (Example 2.46). We fix a topological generator γ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = 1 + p\mathbb{Z}_p$ and identify $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$ with $\hat{\Lambda}$ by the correspondence $\gamma \leftrightarrow 1+T$. We choose $\tau \in G_{\{p\}}$ which is sent to γ under the natural homomorphism $G_{\{p\}} \to \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. The following theorem may be regarded as an arithmetic analogue for $\mathcal{X}_p^{\mathrm{H}}(\bar{\rho})$ of Theorem 14.1.[1]

Theorem 14.8 ([MT1]) *The map*

$$\Psi_p : \mathcal{X}_p^{\mathrm{H}}(\bar{\rho}) \longrightarrow \overline{\mathbb{Q}}_p; \qquad \Psi_p(\varphi) := \mathrm{Tr}\big(\rho_\varphi^{\mathrm{H}}(\tau)\big)$$

is p-adically bianalytic in a neighborhood of φ°. Here φ° is defined by $\rho_{\varphi^\circ}^{\mathrm{H}} = \varphi^\circ \circ \rho_p^{\mathrm{H}} \approx \rho_{f^\circ,\mathfrak{p}}$.

[1] The analogy between two deformation spaces $\mathcal{X}_K^\circ(\rho_h)$ and $\mathcal{X}_p^{\mathrm{H}}(\bar{\rho})$ was firstly pointed out by K. Fujiwara [Fw]. See also [Oh].

Proof Since $\rho_\varphi^{\mathrm{H}}$ is p-ordinary for $\varphi \in \mathcal{X}_p^{\mathrm{H}}(\bar{\rho})$, we have

$$\rho_\varphi^{\mathrm{H}} \simeq \begin{pmatrix} \chi_{1,\varphi} & * \\ 0 & \chi_{2,\varphi} \end{pmatrix}, \qquad \chi_{2,\varphi}|_{I_{\{p\}}} = \mathbf{1}.$$

Therefore, we have

$$\begin{aligned} \chi_{1,\varphi}(\tau) &= \det\bigl(\rho_\varphi^{\mathrm{H}}(\tau)\bigr) \\ &= \varphi\bigl(\det\bigl(\rho_p^{\mathrm{H}}(\tau)\bigr)\bigr) \\ &= \varphi\bigl(\iota^{\mathrm{H}} \circ \rho_{p,1}(\tau)\bigr) \\ &= \varphi\bigl(\omega(\tau)\iota^{\mathrm{H}}(\gamma)\bigr) \\ &= \omega(\tau)\varphi\bigl(\iota^{\mathrm{H}}(\gamma)\bigr) \\ &= \omega(\tau)\bigl(1 + x_p(\varphi)\bigr) \quad (\gamma = 1 + T), \end{aligned}$$

where ω denotes the Teichmüller lift of $\det \bar{\rho}$. Hence, we have

$$\begin{aligned} \Psi_p^{\mathrm{H}}\bigl(\rho_\varphi^{\mathrm{H}}(\tau)\bigr) &= \mathrm{Tr}\bigl(\rho_\varphi^{\mathrm{H}}(\tau)\bigr) \\ &= \chi_{1,\varphi}(\tau) + 1 \\ &= \omega(\tau)\bigl(1 + x_p(\varphi)\bigr) + 1. \end{aligned}$$

Since x_p is a p-adically bianalytic function on φ° by Theorem 14.7, so is Ψ_p^{H}. □

By the universality of $(R_p^\circ, \rho_p^\circ)$, there exists a unique $\mathbb{Z}_p$-algebra homomorphism $\psi : R_p^\circ \to R_p^{\mathrm{H}}$ such that $\psi \circ \rho_p^\circ \approx \rho_p^{\mathrm{H}}$. Since $\iota^{\mathrm{H}} \circ \psi = \iota^\circ$, we see that ψ is a $\hat{\Lambda}$-algebra homomorphism. Then Mazur [Mz3] conjectured that ψ is an isomorphism, which was proved by A. Wiles.

Theorem 14.9 (See [Wi, TW]) *Let $k = \mathbb{Q}(\sqrt{p^*})$, $p^* = (-1)^{(p-1)/2}p$, and assume that the level of f° is p and that $\bar{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/k)}$ is absolutely irreducible. Then, ψ is an isomorphism. Hence, $\mathcal{X}_p^{\mathrm{H}}(\bar{\rho}) = \mathcal{X}_p^\circ(\bar{\rho})$.*

Remark 14.10 Theorem 14.9 may be regarded as a non-Abelian generalization of class field theory in Sect. 2.3.3. Let $\mathbb{A}_\mathbb{Q} = \prod_p' \mathbb{Q}_p \times \mathbb{R}$ be the adèle ring of $\mathbb{Q}$, where $\prod_p'$ means the restricted product of $\mathbb{Q}_p$'s with respect to $\mathbb{Z}_p$'s. Note that the idèle group $J_\mathbb{Q}$ and the idèle class group $C_\mathbb{Q} = J_\mathbb{Q}/\mathbb{Q}^\times$ (2.6) are written as

$$J_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\times = GL_1(\mathbb{A}_\mathbb{Q})$$

and

$$C_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times = GL_1(\mathbb{A}_\mathbb{Q})/GL_1(\mathbb{Q})$$

respectively. Then, via the reciprocity homomorphism $\rho_k : C_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ of class field theory (2.7), one has a bijection between the sets of certain 1-dimensional representations of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ and $GL_1(\mathbb{A}_{\mathbb{Q}})/GL_1(\mathbb{Q})$. On the other hand, noting that an cuspidal eigenform may be regarded as a function on $GL_2(\mathbb{A}_{\mathbb{Q}})/GL_2(\mathbb{Q})$, Theorem 14.9 tells us that there is a bijection, called the *Langlands correspondence*, between the set of certain 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the set of certain functions on $GL_2(\mathbb{A}_{\mathbb{Q}})/GL_2(\mathbb{Q})$. Therefore, Theorem 14.9 may be viewed as a GL_2-version of class field theory. For more precise account of this issue, we refer to [Hd3, **1**].

Now we consider the case that $\rho_{f^\circ,\mathfrak{p}}$ is coming from an elliptic curve E defined over $\mathbb{Q}$: $\rho_{f^\circ,\mathfrak{p}} = \rho_E$. Her ρ_E is the representation arising from the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Tate module $\varprojlim_n E[p^n] = \mathbb{Z}_p^{\oplus 2}$ of E and is assumed to be unramified outside $\{p, \infty\}$. In particular, the weight w_{f° of f° must be 2 and $\mathcal{O}_{f^\circ,\mathfrak{p}} = \mathbb{Z}_p$. Furthermore, we assume that E is split-multiplicative at p, namely, E is extended to a smooth group scheme $\mathcal{E}$ over $\mathbb{Z}_p$ whose special fiber $\mathcal{E} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ is isomorphic to $\mathbb{G}_m$ over $\mathbb{F}_p$, where $\mathbb{G}_m = \mathrm{Spec}(\mathbb{F}_p[X, Y]/(XY - 1))$ is the multiplicative group over $\mathbb{F}_p$.

We let

$$\rho_p^{\mathrm{H}} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}, \qquad \chi_2|_{I_{\{p\}}} = \mathbf{1}$$

and set $y_p := \chi_2(\sigma_p)$. Here σ_p stands for the Frobenius automorphism over p. Let $\varphi^\circ \in \mathcal{X}^H_{p,2}(\bar{\rho})$ be the arithmetic point corresponding to $\rho_E = \rho_{f^\circ,\mathfrak{p}}$. Since x_p is p-adically bianalytic in a neighborhood of φ° and $\varphi^\circ \circ \iota^H(T) = 0$, y_p is regarded as a p-adic analytic function of x_p around $0 \in \mathcal{D}_p$. Then we have the following theorem due to R. Greenberg and G. Stevens.

Theorem 14.11 (See [GeS], [Hd4, 1.5]) *Let q_E be the Tate period of E: $E(\overline{\mathbb{Q}}_p) = \overline{\mathbb{Q}}_p^\times/(q_E)^{\mathbb{Z}}$. Then we have the following formula*:

$$\left.\frac{dy_p}{dx_p}\right|_{x_p=0} = -\frac{1}{2\log_p(\gamma)}\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)},$$

where $\log_p$ *stands for the p-adic logarithm*. The quantity $\log_p(q_E)/\mathrm{ord}_p(q_E)$ is called the $\mathfrak{L}$-*invariant* of the elliptic curve E.

Remark 14.12 In view of Theorem 14.3 and our analogy, it would be an interesting problem to study an arithmetic meaning of the p-adic integral of y_p with respect to x_p, $\int_0^{x_p} y_p\, dx_p$. A result by R. Coleman [Cl] on the relation between p-adic Dirichlet L-values and p-adic polylogarithms may suggest that there would be some relation between this integral and the p-adic modular L-value when x_p is an arithmetic point corresponding to a modular form.

Summary

Hyperbolic structures and associated holonomy representations	p-Adic ordinary modular forms and associated Galois representations
Deformation space $\mathcal{X}_K^{\mathrm{H}}(z^\circ)$	Deformation space $\mathcal{X}_p^{\mathrm{H}}(\bar{\rho})$
Dehn surgery points with integral coefficient	Arithmetic points (modular forms of integral weight)
Meridian function x_K Longitude function y_K	Monodromy function x_p Frobenius function y_p
Modulus of ∂X_K	$\mathfrak{L}$-invariant

References

[Ah] Ahlfors, L.: Complex Analysis: An Introduction of the Theory of Analytic Functions of One Complex Variable, 3rd edn. McGraw-Hill Book, New York (1979)

[Am] Amano, F.: Master thesis. Kyushu University, in preparation (2011)

[AM] Artin, M., Mazur, B.: Etale Homotopy. Lecture Notes in Mathematics, vol. 100. Springer, Berlin (1969)

[BN] Bayer, P., Neukirch, J.: On values of zeta functions and l-adic Euler characteristics. Invent. Math. **50**(1), 35–64 (1978)

[Bi] Birman, J.: Braids, Links, and Mapping Class Groups. Annals of Mathematics Studies, vol. 82. Princeton Univ. Press/Univ. of Tokyo Press, Princeton/Tokyo (1974)

[BP] Boileau, M., Porti, J.: Geometrization of 3-Orbifolds of Cyclic Type. Astérisque, vol. 272 (2001)

[Bo] Boston, N.: Galois p-groups unramified at p—a survey. In: Primes and Knots. Contemporary Mathematics, vol. 416, pp. 31–40. Am. Math. Soc., Providence (2006)

[BZ] Burde, G., Zieschang, H.: Knots, 2nd edn. de Gruyter Studies in Mathematics, vol. 5 (2003)

[CFL] Chen, K.-T., Fox, R., Lyndon, R.: Free differential calculus. IV. The quotient groups of the lower central series. Ann. Math. (2) **68**, 81–95 (1958)

[CaP] Coates, J., Perrin-Riou, B.: On p-adic L-functions attached to motives over $\mathbb{Q}$. In: Algebraic Number Theory. Advanced Studies in Pure Mathematics, vol. 17, pp. 23–54. Academic Press, Boston (1989)

[CaS] Coates, J., Sujatha, R.: Cyclotomic Fields and Zeta Values. Springer Monographs in Mathematics. Springer, Berlin (2006)

[Cl] Coleman, R.: Dilogarithms regulators and p-adic L-functions. Invent. Math. **69**(2), 171–208 (1982)

[Cr] Crowell, R.: The derived module of a homomorphism. Adv. Math. **6**, 210–238 (1971)

[CF] Crowell, R., Fox, R.: Introduction to Knot Theory. Graduate Texts in Mathematics, vol. 57. Springer, New York (1977). Reprint of the 1963 original

[CuS] Culler, M., Shalen, P.: Varieties of group representations and splittings of 3-manifolds. Ann. Math. **117**, 109–146 (1983)

[Dl] Deligne, P.: Formes modulaires et représentations l-adiques. In: Lecture Notes in Mathematics, vol. 179, pp. 136–172. Springer, Berlin (1971)

[Dn1] Deninger, C.: Some analogies between number theory and dynamical systems on foliated spaces. Doc. Math. J. DMV. Extra Volume ICM I, 23–46 (1998)

[Dn2] Deninger, C.: A note on arithmetic topology and dynamical systems. In: Algebraic Number Theory and Algebraic Geometry. Contemporary Mathematics, vol. 300, pp. 99–114. Am. Math. Soc., Providence (2002)

DOI 10.1007/978-1-4471-2158-9,

[DGLZ] Dimofte, T., Gukov, S., Lenells, J., Zagier, D.: Exact results for perturbative Chern–Simons theory with complex gauge group. Commun. Number Theory Phys. **3**(2), 363–443 (2009)

[Du] Dunnington, G.W.: Carl Friedrich Gauss, Titan of Science. The Mathematical Association of America, Washington (2004)

[Fo1] Fox, R.H.: Free differential calculus. I: Derivation in the free group ring. Ann. Math. **57**, 547–560 (1953)

[Fo2] Fox, R.H.: Covering spaces with singularities. In: A Symposium in Honor of S. Lefschetz, pp. 243–257. Princeton Univ. Press, Princeton (1957)

[Fr] Fried, D.: Analytic torsion and closed geodesics on hyperbolic manifolds. Invent. Math. **84**(3), 523–540 (1986)

[Frl] Friedlander, E.: Étale Homotopy of Simplicial Schemes. Annals of Mathematics Studies, vol. 104. Princeton Univ. Press/Univ. of Tokyo Press, Princeton/Tokyo (1982)

[Fw] Fujiwara, K.: Algebraic number theory and low dimensional topology. Report of the 47-th Algebra Symposium at Muroran Inst. Univ., pp. 172–185 (2002)

[Fl] Fuluta, K.: On capitulation theorems for infinite groups. In: Primes and Knots. Contemporary Mathematics, vol. 416, pp. 41–47. Am. Math. Soc., Providence (2006). Preprint (2003)

[Ga2] Gauss, C.F.: Zur mathematischen Theorie der electrodynamischen Wirkungen, Werke V (1833)

[Ga1] Gauss, C.F.: Disquisitiones Arithmeticae. Yale Univ., New Haven (1966)

[GS] González-Acuña, F., Short, H.: Cyclic branched coverings of knots and homology spheres. Rev. Mat. Univ. Complut. Madr. **4**(1), 97–120 (1991)

[GL] Gordon, C., Luecke, J.: Knots are determined by their complements. J. Am. Math. Soc. **2**, 371–415 (1989)

[Ge] Greenberg, R.: Iwasawa theory for p-adic representations. In: Algebraic Number Theory. Advanced Studies in Pure Mathematics, vol. 17, pp. 97–137. Academic Press, Boston (1989)

[GeS] Greenberg, R., Stevens, G.: p-adic L-functions and p-adic periods of modular forms. Invent. Math. **111**(2), 407–447 (1993)

[Go1] Grothendieck, A.: Revêtements étales et groupe fondamental, Séminaire de Géometrie Algébrique du Bois Marie 1960–1961 (SGA 1). Lecture Notes in Mathematics, vol. 224. Springer, Berlin (1971)

[Go2] Grothendieck, A.: Théorie des topos et cohomologie étale des schémas, Tome 1. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4). Lecture Notes in Mathematics, vol. 269. Springer, Berlin (1972). With M. Artin and J. L. Verdier (in French)

[Go3] Grothendieck, A.: Théorie des topos et cohomologie étale des schémas, Tome 2. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4). Lecture Notes in Mathematics, vol. 270. Springer, Berlin (1972). With M. Artin and J. L. Verdier (in French)

[Go4] Grothendieck, A.: Théorie des topos et cohomologie étale des schémas, Tome 3. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4). Lecture Notes in Mathematics, vol. 305. Springer, Berlin (1973). With M. Artin and J. L. Verdier (in French)

[Hb] Haberland, K.: Galois Cohomology of Algebraic Number Fields. VEB Deutscher Verlag der Wissenschaften, Berlin (1978) (145 pp.)

[Har] Harada, S.: Hasse–Weil zeta function of absolutely irreducible SL_2 representations of the figure 8 knot group. Proc. Am. Math. Soc. **139**, 3115–3125 (2011)

[He] Hempel, J.: 3-Manifolds. Annals of Mathematics Studies, vol. 86. Princeton Univ. Press/Univ. of Tokyo Press, Princeton/Tokyo (1976)

[Hd1] Hida, H.: Iwasawa modules attached to congruences of cusp forms. Ann. Sci. Éc. Norm. Super. (4) **19**, 231–273 (1986)

[Hd2] Hida, H.: Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms. Invent. Math. **85**, 545–613 (1986)

[Hd3] Hida, H.: Modular Forms and Galois Cohomology. Cambridge Studies in Advanced Mathematics, vol. 69. Cambridge Univ. Press, Cambridge (2000)
[Hd4] Hida, H.: Hilbert Modular Forms and Iwasawa Theory. Oxford Mathematical Monographs. Oxford Univ. Press, Oxford (2006)
[Hib] Hilbert, D.: Die Theorie der algebraischen Zahlkörper. Jahresber. Dtsch. Math.-Ver. **4**, 175–546 (1897). In: Gesammelte Abhandlungen. Band I: Zahlentheorie, 2nd edn. Springer, Berlin (1970) (in German)
[Hl] Hillman, J.: Algebraic Invariants of Links. Series on Knots and Everything, vol. 32. World Scientific, Singapore (2002)
[HMM] Hillman, J., Matei, D., Morishita, M.: Pro-p link groups and p-homology groups. In: Primes and Knots. Contemporary Mathematics, vol. 416, pp. 121–136. Am. Math. Soc., Providence (2006)
[Hr] Hironaka, E.: Alexander stratifications of character varieties. Ann. Inst. Fourier **47**, 555–583 (1997)
[Ih1] Ihara, Y.: On Galois representations arising from towers of coverings of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. Invent. Math. **86**, 427–459 (1986)
[Ih2] Ihara, Y.: On beta and gamma functions associated with the Grothendieck–Teichmüller groups. In: Aspects of Galois Theory, Gainesville, FL, 1996. London Mathematical Society Lecture Note Series, vol. 256, pp. 144–179. Cambridge Univ. Press, Cambridge (1999)
[Iw1] Iwasawa, K.: On a certain analogy between algebraic number fields and function fields. Sūgaku **15**, 65–67 (1963) (in Japanese)
[Iw2] Iwasawa, K.: On $\mathbb{Z}_l$-extensions of algebraic number fields. Ann. Math. (2) **98**, 246–326 (1973)
[IT] Iyanaga, S., Tamagawa, T.: Sur la theorie du corps de classes sur le corps des nombres rationnels. J. Math. Soc. Jpn. **3**, 220–227 (1951)
[KaM] Kadokami, T., Mizusawa, Y.: Iwasawa type formulas for covers of a link in a rational homology sphere. J. Knot Theory Ramif. **17**(10), 1199–1221 (2008)
[Kp1] Kapranov, M.: Analogies between the Langlands correspondence and topological quantum field theory. In: Progress in Math., vol. 131, pp. 119–151. Birkhäuser, Basel (1995)
[Kp2] Kapranov, M.: Analogies between number fields and 3-manifolds. Unpublished Note (1996)
[Kt1] Kato, K.: A Hasse principle for two-dimensional global fields. J. Reine Angew. Math. **366**, 142–183 (1986)
[Kt2] Kato, K.: Lectures on the approach to Iwasawa theory for Hasse–Weil L-functions via B_{dR}. In: Arithmetic Algebraic Geometry. Lecture Note in Mathematics, vol. 1553, pp. 50–163. Springer, Berlin (1993)
[Kw] Kawauchi, A.: A Survey of Knot Theory. Birkhäuser, Basel (1996). Translated and revised from the 1990 Japanese original by the author
[KiL] Kirk, P., Livingston, C.: Twisted Alexander invariants, Reidemeister torsion, and Casson–Gordon invariants. Topology **38**(3), 635–661 (1999)
[KGM] Kitanao, T., Goda, H., Morifuji, T.: Twisted Alexander Invariants. MSJ Memoir, vol. 5. Math. Soc. Jpn., Tokyo (2006) (in Japanese)
[KnM] Knudsen, F., Mumford, D.: The projectivity of the moduli space of stable curves. I. Preliminaries on "det" and "Div". Math. Scand. **39**(1), 19–55 (1976)
[Kc1] Koch, H.: Galoissche Theorie der p-Erweiterungen. Springer/VEB Deutscher Verlag der Wissenschaften, Berlin (1970)
[Kc2] Koch, H.: On p-extensions with given ramification, Appendix 1. In: [Hb], pp. 89–126
[Kh] Kohno, T.: Conformal Field Theory and Topology. Iwanami Series in Modern Mathematics, Translations of Mathematical Monographs, vol. 210. Am. Math. Soc., Providence (2002)
[Kn] Kontsevich, M.: Vassiliev's knot invariants. In: I.M. Gelfand Seminar. Advances in Soviet Mathematics, Part 2, vol. 16, pp. 137–150. Am. Math. Soc., Providence (1993)
[KuL] Kubota, T., Leopoldt, H.: Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. J. Reine Angew. Math. **214/215**, 328–339 (1964)

[Kr1] Kurihara, M.: Iwasawa theory and Fitting ideals. J. Reine Angew. Math. **561**, 39–86 (2003)

[Kr2] Kurihara, M.: Refined Iwasawa theory and Kolyvagin systems of Gauss sum type. Preprint (2008)

[Lb1] Labute, J.: Mild pro-p-groups and Galois groups of p-extensions of $\mathbf{Q}$. J. Reine Angew. Math. **596**, 155–182 (2006)

[LM] Labute, J., Mináč, J.: Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification. J. Algebra **332**, 136–158 (2011)

[Ln1] Lang, S.: Algebraic Number Theory, 2nd edn. Graduate Texts in Mathematics, vol. 110. Springer, New York (1994)

[Ln2] Lang, S.: Cyclotomic Fields I and II, Combined 2nd edn. Graduate Texts in Mathematics, vol. 121. Springer, New York (1990). With an appendix by Karl Rubin

[Le] Le, T.: Varieties of representations and their subvarieties of homology jumps for certain knot groups. Russ. Math. Surv. **46**, 250–251 (1991)

[Lü] Lück, W.: Analytic and topological torsion for manifolds with boundary and symmetry. J. Differ. Geom. **37**, 263–322 (1993)

[MM] Manin, Y., Marcolli, M.: Holography principle and arithmetic of algebraic curves. Adv. Theor. Math. Phys. **5**(3), 617–650 (2001)

[Ms] Massey, W.: Algebraic Topology: An Introduction. Graduate Texts in Mathematics, vol. 56. Springer, New York (1977). Reprint of the 1967 edition

[Mz1] Mazur, B.: Notes on étale cohomology of number fields,. Ann. Sci. Éc. Norm. Super. (4) **6**, 521–552 (1973)

[Mz2] Mazur, B.: Deforming Galois representations. In: Galois Groups over $\mathbb{Q}$. Mathematical Sciences Research Institute Publications, vol. 16, pp. 385–437. Springer, Berlin (1989)

[Mz3] Mazur, B.: Two-dimensional p-adic Galois representations unramified away from p. Compos. Math. **74**, 115–133 (1990)

[Mz4] Mazur, B.: The theme of p-adic variation. In: Mathematics: Frontiers and Perspectives, pp. 433–459. Am. Math. Soc., Providence (2000)

[Mz5] Mazur, B.: Remarks on the Alexander polynomial. Unpublished Note (1963 or 1964)

[MW1] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$. Invent. Math. **76**(2), 179–330 (1984)

[MW2] Mazur, B., Wiles, A.: On p-adic analytic families of Galois representations. Compos. Math. **59**(2), 231–264 (1986)

[Mc] McMullen, C.: From dynamics on surfaces to rational points on curves. Bull., New Ser., Am. Math. Soc. **37**(2), 119–140 (2000)

[Mi1] Milne, J.: Étale Cohomology. Princeton Mathematical Series, vol. 33. Princeton Univ. Press, Princeton (1980)

[Mi2] Milne, J.: Arithmetic Duality Theorems. Perspectives in Mathematics, vol. 1. Academic Press, Boston (1986)

[Ml1] Milnor, J.: Isotopy of links. In: Fox, R.H., Spencer, D.S., Tucker, W. (eds.) Algebraic Geometry and Topology, pp. 280–306. Princeton Univ. Press, Princeton (1957). A Symposium in Honour of S. Lefschetz

[Ml2] Milnor, J.: Infinite cyclic coverings. In: Conference on the Topology of Manifolds, Michigan State Univ., E. Lansing, Mich., 1967, pp. 115–133. Prindle, Weber & Schmidt, Boston (1968)

[Mn1] Morin, B.: Utilisation d'une cohomologie étale equivariante en topologie arithmétique. Compos. Math. **144**(1), 32–60 (2008)

[Mn2] Morin, B.: Sur le topos Weil-étale d'un corps de nombres. Thèse, Université Bordeaux I (2008)

[M1] Morishita, M.: Milnor's link invariants attached to certain Galois groups over $\mathbb{Q}$. Proc. Jpn. Acad. **76**(2), 18–21 (2000)

[M2] Morishita, M.: On certain analogies between knots and primes. J. Reine Angew. Math. **550**, 141–167 (2002)

[M3] Morishita, M.: Knots and prime numbers, 3-dimensional manifolds and algebraic number fields. Sūrikaisekikenkyūsho Kōkyūroku **1200**, 103–115 (2001). Algebraic Number Theory and Related Topics (Kyoto, 2000) (in Japanese)

[M4] Morishita, M.: A theory of genera for cyclic coverings of links. Proc. Jpn. Acad. **77**(7), 115–118 (2001)

[M5] Morishita, M.: Primes and knots—on analogies between algebraic number theory and 3-dimensional topology. Report of the 47-th Algebra Symposium at Muroran Inst. Univ., pp. 157–171 (2002) (in Japanese)

[M6] Morishita, M.: On capitulation problem for 3-manifolds. In: Galois Theory and Modular Forms. Developments in Mathematics, vol. 11, pp. 305–313. Kluwer Academic, Dordrecht (2003)

[M7] Morishita, M.: Milnor invariants and Massey products for prime numbers. Compos. Math. **140**, 69–83 (2004)

[M8] Morishita, M.: Analogies between prime numbers and knots. Sūgaku **58**(1), 40–63 (2006) (in Japanese)

[M9] Morishita, M.: Analogies between knots and primes, 3-manifolds and number rings. Sūgaku Expo. **23**(1), 1–30 (2010)

[M10] Morishita, M.: On the Alexander stratification in the deformation space of Galois characters. Kyushu J. Math. **60**, 405–414 (2006)

[M11] Morishita, M.: Milnor invariants and l-class groups. In: Geometry and Dynamics of Groups and Spaces. In Memory of Alexander Reznikov. Progress in Mathematics, vol. 265, pp. 589–603. Birkäuser, Basel (2007)

[M12] Morishita, M.: Knots and Primes. Springer-Japan, Tokyo (2009) (in Japanese, xiii + 201 pp.)

[MT1] Morishita, M., Terashima, Y.: Arithmetic topology after Hida theory. In: Intelligence of Low Dimensional Topology. Knots and Everything Book Series, vol. 40, pp. 213–222. World Scientific, Singapore (2006)

[MT2] Morishita, M., Terashima, Y.: Chern–Simons variation and Deligne cohomology. In: Spectral Analysis in Geometry and Number Theory on Professor Toshikazu Sunada's 60th Birthday. Contemporary Math., vol. 484, pp. 127–134. Am. Math. Soc., Providence (2009)

[Mu1] Murasugi, K.: On Milnor's invariant for links. Trans. Am. Math. Soc. **124**, 94–110 (1996)

[Mu2] Murasugi, K.: Nilpotent coverings of links and Milnor's invariant. In: Low-Dimensional Topology. London Mathematical Society Lecture Note Series, vol. 95, pp. 106–142. Cambridge Univ. Press, Cambridge (1985)

[Mu3] Murasugi, K.: Classical knot invariants and elementary number theory. In: Primes and Knots. Contemporary Mathematics, vol. 416, pp. 167–196. Am. Math. Soc., Providence (2006)

[Mr] Murre, J.P.: Lectures on an Introduction to Grothendieck's Theory of the Fundamental Group, Notes by S. Anantharaman. Tata Institute of Fundamental Research Lectures on Mathematics, vol. 40. Tata Institute of Fundamental Research, Bombay (1967)

[Ne1] Neukirch, J.: Class Field Theory. Grundlehren der Mathematischen Wissenschaften, vol. 280. Springer, Berlin (1986)

[Ne2] Neukirch, J.: Algebraic Number Theory. Grundlehren der Mathematischen Wissenschaften, vol. 322. Springer, Berlin (1999). Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder

[NSW] Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, 2nd edn. Grundlehren der Mathematischen Wissenschaften, vol. 323. Springer, Berlin (2008)

[NZ] Neumann, W., Zagier, D.: Volumes of hyperbolic three-manifolds. Topology **24**(3), 307–332 (1985)

[Ng] Nguyen Quang Do, T.: Formations de classes et modules d'Iwasawa. In: Number Theory, Noordwijkerhout, 1983. Lecture Notes in Mathematics, vol. 1068, pp. 167–185. Springer, Berlin (1984)

[No1] Noguchi, A.: A functional equation for the Lefschetz zeta functions of infinite cyclic coverings with an application to knot theory. Topol. Proc. **29**(1), 277–291 (2005). Spring Topology and Dynamical Systems Conference

[No2] Noguchi, A.: Zeros of the Alexander polynomial of knot. Osaka J. Math. **44**(3), 567–577 (2007)

[Od] Oda, T.: Note on meta-abelian quotients of pro-l free groups. Preprint (1985)

[Oh] Ohtani, S.: An analogy between representations of knot groups and Galois groups. Osaka J. Math. (to appear)

[P] Porter, R.: Milnor's $\bar{\mu}$-invariants and Massey products. Trans. Am. Math. Soc. **275**, 39–71 (1980)

[Ra] Ramachandran, N.: A note on arithmetic topology. C. R. Math. Acad. Sci. Soc. R. Can. **23**(4), 130–135 (2001)

[Rd1] Rédei, L.: Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. J. Reine Angew. Math. **171**, 55–60 (1934)

[Rd2] Rédei, L.: Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, I. J. Reine Angew. Math. **180**, 1–43 (1939)

[Rz1] Reznikov, A.: Three-manifolds class field theory (Homology of coverings for a nonvirtually b_1-positive manifold). Sel. Math. New Ser. **3**, 361–399 (1997)

[Rz2] Reznikov, A.: Embedded incompressible surfaces and homology of ramified coverings of three-manifolds. Sel. Math. New Ser. **6**, 1–39 (2000)

[RM] Reznikov, A., Moree, P.: Three-manifold subgroup growth, homology of coverings and simplicial volume. Asian J. Math. **1**(4), 764–768 (1997)

[Ro] Rolfsen, D.: Knots and Links. Mathematics Lecture Series, vol. 7. Publish or Perish, Berkeley (1976)

[Sa] Sakuma, M.: The homology groups of abelian coverings of links. Math. Semin. Notes Kobe Univ. **7**(3), 515–530 (1979)

[Sh] Schmidt, K.: Dynamical Systems of Algebraic Origin. Progress in Mathematics, vol. 128. Birkhäuser, Basel (1995) (xviii+310 pp.)

[Sc1] Schmidt, A.: Circular sets of prime numbers and p-extensions of the rationals. J. Reine Angew. Math. **596**, 115–130 (2006)

[Sc2] Schmidt, A.: Singular homology of arithmetic schemes. Algebra Number Theory **1**(2), 183–222 (2007)

[Se1] Serre, J.-P.: A Course in Arithmetic. Graduate Texts in Mathematics, vol. 7. Springer, New York (1973). Translated from the French

[Se2] Serre, J.-P.: Local Fields. Graduate Texts in Mathematics, vol. 67. Springer, New York (1979). Translated from the French by Marvin Jay Greenberg

[Sr] Sharifi, R.: Massey products and ideal class groups. J. Reine Angew. Math. **603**, 1–33 (2007)

[Si] Sikora, A.: Analogies between group actions on 3-manifolds and number fields. Comment. Math. Helv. **78**, 832–844 (2003)

[SW] Silver, D., Williams, S.: Mahler measure, links and homology growth. Topology **41**, 979–991 (2002)

[St] Stallings, J.: Homology and central series of groups. J. Algebra **2**, 170–181 (1965)

[Sg1] Sugiyama, K.: An analog of the Iwasawa conjecture for a compact hyperbolic threefold. J. Reine Angew. Math. **613**, 35–50 (2007)

[Sg2] Sugiyama, K.: The geometric Iwasawa conjecture from a viewpoint of the arithmetic topology. In: Proceedings of the Symposium on Algebraic Number Theory and Related Topics. RIMS Kôkyûroku Bessatsu, vol. 4, pp. 235–247. Res. Inst. Math. Sci. (RIMS), Kyoto (2007)

[Sg3] Sugiyama, K.: On geometric analogues of Iwasawa main conjecture for a hyperbolic threefold. In: Noncommutativity and Singularities. Advanced Studies in Pure Mathematics, vol. 55, pp. 117–135. Math. Soc. Jpn., Tokyo (2009)

[Sn] Sunada, T.: Fundamental Groups and Laplacians. Kinokuniya, Tokyo (1988) (in Japanese)

[Tk] Takakura, Y.: Gauss' theory from the viewpoint of arithmetic topology. Master thesis, Kyushu University (2007) (in Japanese)
[Tm] Tamme, G.: Introduction to Étale Cohomology. Universitext. Springer, Berlin (1994). Translated from the German by Manfred Kolster
[TW] Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. Ann. Math. (2) **141**(3), 553–572 (1995)
[Th] Thurston, W.: The Geometry and Topology of 3-Manifolds. Lecture Note, Princeton (1977)
[Tr] Traldi, L.: Milnor's invariants and the completions of link modules. Trans. Amer. Math. Soc. **284**, 401–424
[Tu] Turaev, V.G.: Milnor's invariants and Massey products. J. Sov. Math. **12**, 128–137 (1979) (English transl.)
[U] Ueki, J.: On the homology of branched coverings of 3-manifolds. Preprint (2011)
[V1] Vogel, D.: Massey products in the Galois cohomology of number fields. Dissertation, Universität Heidelberg (2004)
[V2] Vogel, D.: On the Galois group of 2-extensions with restricted ramification. J. Reine Angew. Math. **581**, 117–150 (2005)
[Wl] Waldspurger, J.-L.: Entrelacements sur Spec($\mathbb{Z}$). Bull. Sci. Math. **100**, 113–139 (1976)
[Ws] Washington, L.: Introduction to Cyclotomic Fields, 2nd edn. Graduate Texts in Mathematics, vol. 83. Springer, Berlin (1997)
[Wh] Whitten, W.: Knots complements and groups. Topology **26**, 41–44 (1987)
[Wi] Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. Math. (2) **141**(3), 443–551 (1995)
[Y] Yamamoto, Y.: Class number problems for quadratic fields (concentrating on the 2-part). Sūgaku **40**(2), 167–174 (1988) (in Japanese)
[Z] Zink, T.: Etale cohomology and duality in number fields, Appendix 2. In: [Hb], pp. 127–145

Index

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