T.D. van Mulligen

Knots in Number Theory

Master thesis, September 2017

Thesis supervisor: Dr. R.I. van der Veen
Second supervisor: Dr. G.S. Zalamansky

Mathematisch Instituut, Universiteit Leiden

Contents

1. *Introduction* 1

2. *Topological preliminaries* 5
   - 2.1 Knots 5
   - 2.2 Covering spaces 7

3. *Algebraic preliminaries* 13
   - 3.1 Profinite groups 13
   - 3.2 Affine schemes 15
   - 3.3 Finite étale coverings 17
   - Interlude on Galois categories 19
   - 3.4 Étale fundamental groups 20

4. *The linking number and the Legendre symbol* 23
   - 4.1 The linking number 23
   - 4.2 The mod 2 linking number for primes 26

5. *Decomposition of knots and primes* 31
   - 5.1 Decomposition of knots 31
   - 5.2 Decomposition of primes 37

6. *Homology groups and ideal class groups* 43
   - 6.1 Homology groups and the Hurewicz theorem 43
   - 6.2 Ideal class groups and Artin reciprocity 44

7. *The Alexander and Iwasawa polynomials* 47
7.1 Differential modules 47
7.2 The Alexander polynomial 55
7.3 The Alexander polynomial as a characteristic polynomial 61
7.4 Complete differential modules 63
7.5 The Iwasawa polynomial 66
7.6 The Iwasawa polynomial as a characteristic polynomial 69

Bibliography 71

CHAPTER 1

Introduction

It had long been the consensus that arithmetic topology sprung from the mind of Barry Mazur in the 1960s. However, in 2011 a set of unpublished notes by Mazur, titled "Remarks on the Alexander Polynomial", was discovered, which was dated 1963/1964. In its introduction, Mazur states:

> "Mumford has suggested a most elegant model as a geometric interpretation of the above situation: Spec $\mathbb{Z}/p\mathbb{Z}$ is like a one-dimensional knot in Spec $\mathbb{Z}$ which is like a simply connected three-manifold."

The dimension they talk of is the *étale cohomological dimension*, and indeed, as a result of Artin-Verdier duality the étale cohomological dimension of Spec $\mathcal{O}_k$ is 3, where $\mathcal{O}_k$ is a ring of integers, while it is 1 for a finite field Spec $\mathbb{F}_q$ [Mor12, p. 40 and 2.42]. This suggests a connection between knots, which are embeddings

$$S^1 \hookrightarrow M$$

of a 1-dimensional object into a 3-manifold M, and primes, which can be viewed as embeddings

$$\operatorname{Spec} \mathcal{O}_k/\mathfrak{p} \hookrightarrow \operatorname{Spec} \mathcal{O}_k,$$

where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_k$ and $\mathcal{O}_k/\mathfrak{p}$ a finite field.

The suggestion by Mumford has inspired a fruitful analogy between knots and primes and this field is now known as *arithmetic topology*. Some of the analogous concepts are listed in table 1.1. In this thesis we intend to explore the merits of this analogy. In chapters 2 and 3 we will give some background information on the topological and the algebraic side of things, including the analogy between the topological fundamental group π_1 and the étale fundamental group $\pi_1^{\text{ét}}$. This will further motivate the analogy between knots and primes, since we will show that

Knots	Primes
S^1	$\operatorname{Spec} \mathbb{F}_p$
$\mathbb{R}^3$	$\operatorname{Spec} \mathbb{Z}$
Knot $S^1 \hookrightarrow \mathbb{R}^3$	Prime $\operatorname{Spec} \mathbb{F}_p \hookrightarrow \operatorname{Spec} \mathbb{Z}$
Tubular neighborhood V_K	Field of p-adic numbers $\mathbb{Q}_p$
Mod 2 linking number $\mathrm{lk}_2(L, K)$	Legendre symbol $(\frac{q^*}{p})$ $(q^* = (-1)^{(q-1)/2}q)$
$\mathrm{lk}(K, L) = \mathrm{lk}(L, K)$	Quadratic reciprocity: $(\frac{q^*}{p}) = (\frac{p}{q^*})$
First homology group $H_1(X)$	Ideal class group $H(k)$
Hurewicz theorem	Artin reciprocity
Alexander module A_K	Complete Alexander module A_ψ
Knot module $H_1(X_\infty)$	Iwasawa module H_∞
Alexander polynomial $\Delta_K(t)$	Iwasawa polynomial $f(T)$

Tab. 1.1: Some analogous concepts in the theory of knots and primes.

$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_p) \cong \hat{\mathbb{Z}} \qquad \text{and} \qquad \pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Z}) = 1,$$

where $\hat{\mathbb{Z}}$ indicates the *profinite completion* of $\mathbb{Z}$. This is analogous to the case of knots where we have

$$\pi_1(S^1) \cong \mathbb{Z} \qquad \text{and} \qquad \pi_1(R^3) = 1.$$

In chapter 4 we will start our exploration of arithmetic topology by studying the linking number (for knots) and the Legendre symbol (for primes). Although these two concepts don't seem connected at first, we will see that they are actually defined very similarly and that they imply similar results on the decomposition of knots and primes in coverings. Chapter 5 will expand on this and discusses decomposition in more generality while considering subcovers and ramification of knots and primes.

In chapter 6 we will give an argument for the analogy between the first homology group and the ideal class group. This chapter serves as a stepping stone for chapter 7, where the Alexander polynomial for knots is compared to the Iwasawa polynomial for primes. We build the theory to compute the Alexander polynomial from the ground up, after which we will show that the same construction very much applies to the Iwasawa polynomial.

Although chapters 2 and 3 serve to review some background knowledge, not everything can be covered. Some knowledge of algebraic topology (particularly homology), knot theory (particularly the knot group and the Wirtinger presentation), geometry (particularly affine schemes), algebraic number theory (particularly ramification of primes in number fields and possibly some class field theory) and profinite groups will be useful.

Every chapter is written so that the first half deals with knots and the second half deals with primes. Furthermore, the results in every chapter are as much as possible laid out in such a way

that putting the halves of a chapter side by side would instantly show the similarities between knot theory and number theory. Ideally, the reader will experience multiple instances of déjà vu over the course of reading this text.

CHAPTER 2

Topological preliminaries

In order to define and recognize analogous concepts in the theory of knots and primes, we will need some basic familiarity with knots and covering spaces.

2.1 *Knots*

We know knots from everyday life. Mathematical knots, however, need to be closed. The way to model this is to define a knot as an embedding of a circle in 3-space.

Definition 2.1.1. *Let* M *be a 3-manifold. A* knot *is an embedding* $S^1 \hookrightarrow M$. *The manifold* M *is called the* ambient space *and we call* $X_{S^1} := M \setminus S^1$ *the* knot complement. *We denote a* tubular neighborhood *of* K *by* V_K *and define the* knot exterior *as* $X_K := M \setminus V_K$.

Usually, we will take $M = S^3$. See figure 2.1 for some basic knots. To streamline notation, when we talk of a knot K, we mean the image $f(S^1) \subseteq M$ of the embedding $f : S^1 \hookrightarrow M$. Of course, topologically, any two knots will always be homeomorphic. However, we obviously don't want every embedding $S^1 \hookrightarrow \mathbb{R}^3$ to be considered the same. Therefore, we need a different notion of equivalence between knots.

Unknot | Trefoil knot | Figure-eight knot | Cinquefoil knot | Three-twist knot

Fig. 2.1: Some basic knots.

Definition 2.1.2. *Let* $K, L \subseteq M$ *be two knots. We say that* K *and* L *are* equivalent *if there exists an* ambient isotopy *taking* K *to* L, *i.e., there exists a continuous map* $F : M \times [0,1] \to M$ *such that* F_0 *is the identity on* M, F_t *is a homeomorphism for every* $0 \leq t \leq 1$ *and* $F_1(K) = L$.

See figure 2.2 for an ambient isotopy between two representations of the trefoil knot.

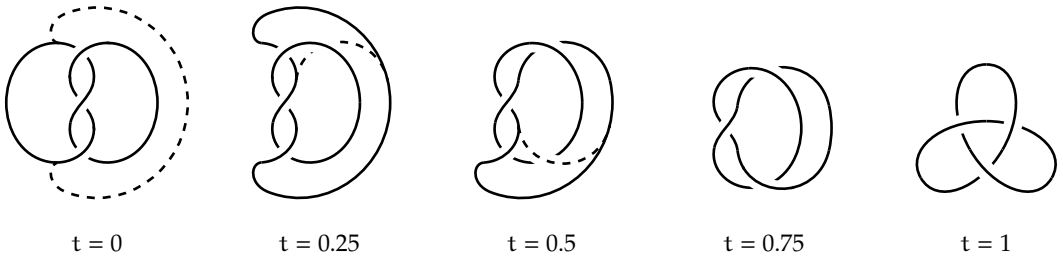


Fig. 2.2: Ambient isotopy on the trefoil knot. The dashed lines indicate the deformation of the knot.

Since we are going to take a closer look at the way different knots interact with each other, we need to define the notion of a link.

Definition 2.1.3. *Let* M *be a 3-manifold and* $n \geq 1$*. We call an embedding* $\bigsqcup_{i=1}^{n} S^1 \hookrightarrow M$ *an* n-component link*. Here* $\bigsqcup_{i=1}^{n} S^1$ *is the disjoint union of* n *circles.*

A knot is a link with 1 component and two links L_1 and L_2 are equivalent if there exists an ambient isotopy taking L_1 to L_2.

One of our goals is to construct covering spaces using knots. We are going to do this by cutting open multiple copies of the ambient space and gluing them together in a certain way. For this we need the following definitions.

Definition 2.1.4. *A knot is* polygonal *if it consists of a finite set of straight line segments. We call a knot* tame *if it is equivalent to a polygonal knot.*

All knots in this text are assumed to be tame. Figure 2.3 illustrates why the trefoil knot is a tame knot.

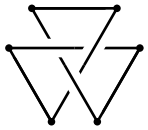


Fig. 2.3: A polygonal representation of the trefoil knot.

We move on to the definition of a Seifert surface.

Definition 2.1.5. *Let* K *be a knot. A* Seifert surface *is a compact, connected, oriented surface* S *such that* $\partial S = K$*, where* ∂S *is the boundary of* S*.*

It's a known fact that every tame knot has a Seifert surface [Rol03, Chap. 5, Sect. A, Theorem 4]. See figure 2.4 for a Seifert surface of the trefoil knot.

We end this section with a definition of the knot group.

Definition 2.1.6. *Let* K *be a knot in* S^3*. The* knot group G_K *is defined as the fundamental group of the knot complement in* S^3*, i.e.,* $G_K := \pi_1(S^3 \setminus K)$*.*

In the next section we're going to take a look at covering spaces. Using covering spaces, we will be able to obtain information about the knot group.

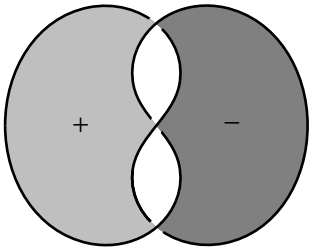


Fig. 2.4: Seifert surface of the trefoil knot, with + and − indicating the orientation.

2.2 *Covering spaces*

The theory of covering spaces is important for the study of the fundamental group. Let us first define what a covering space is.

Definition 2.2.1. *Let X be a topological space. A* covering map *is a continuous surjective map $p : Y \to X$ such that for every $x \in X$ there is an open neighborhood U_x of x such that $p^{-1}(U_x) = \bigsqcup_{i\in I} V_i$ for some index set I and $p|_{V_i} : V_i \to U_x$ is a homeomorphism for every $i \in I$. The space Y is called the* covering space. *An open subset $U \subseteq X$ such that $p^{-1}(U) = \bigsqcup_{i\in I} V_i$ is called* evenly covered by p. *The cardinality $\#p^{-1}(x)$ is called the* degree *of the covering. If $\#p^{-1}(x) = n < \infty$, then we speak of a* finite cover *and in particular of an n-fold cover.*

Let's take a look at some examples of covering spaces.

Example 2.2.2 (Coverings of the circle)**.** We view $S^1 \subseteq \mathbb{C}$ as the unit circle in the complex plane. Define $p_n : S^1 \to S^1, z \mapsto z^n$ for $n \geq 1$ and $p_\infty : \mathbb{R} \to S^1, x \mapsto e^{2\pi x i}$. These are coverings of the circle. ▶

One thing coverings allow us to do, is lift a homotopy in X to its covering space Y.

Theorem 2.2.3. *Let $p : Y \to X$ be a covering map and let $H : Z \times [0,1] \to X$ be a homotopy and $\tilde{H}_0 : Z \times \{0\} \to Y$ a lift of H_0 in Y, i.e., $H_0 = p \circ \tilde{H}_0$. Then there exists a unique homotopy $\tilde{H} : Z \times [0,1] \to Y$ extending $\tilde{H}_0$ and lifting H, i.e., $H = p \circ \tilde{H}$.*

In particular, taking Z to be a singleton, theorem 2.2.3 tells us that a path in X can be lifted to its covering space.

Corollary 2.2.4. *Let $p : Y \to X$ be a covering map and let $\gamma : [0,1] \to X$ be a path in X. Let $x := \gamma(0)$ and choose a point $y \in p^{-1}(x)$. Then there exists a unique path $\tilde{\gamma} : [0,1] \to Y$ such that $\gamma = p \circ \tilde{\gamma}$ and $\tilde{\gamma}(0) = y$.*

Using the path-lifting property, we can define an action of $\pi_1(X)$ on a fiber $p^{-1}(x)$.

Definition 2.2.5. *Let $p : Y \to X$ be a covering and let $\gamma : [0,1] \to X$ be a loop in X with endpoints $x \in X$. Denote with $[\gamma]$ the class of γ in $\pi_1(X)$. For every $y \in p^{-1}(x)$, there exists a unique lift $\tilde{\gamma}_y : [0,1] \to Y$ of γ such that $\tilde{\gamma}_y(0) = y$. Then we define $[\gamma] \cdot y := \tilde{\gamma}_y(1) \in h^{-1}(x)$. This is called the* monodromy action *of $\pi_1(X)$ on $h^{-1}(x)$. The induced map $\rho_x : \pi_1(X) \to \mathrm{Aut}(p^{-1}(x))$ is called the* monodromy permutation representation.

Proposition 2.2.6. *The monodromy action is well-defined.*

Proof. Firstly, note that a constant path in X can only be lifted to a constant path in Y, since the elements of a fiber can be separated by disjoint open sets and a path has to be continuous. Secondly, for two loops $\gamma, \gamma' : [0,1] \to X$ with $[\gamma] = [\gamma'] \in \pi_1(X)$ a path homotopy $H : [0,1] \times [0,1] \to X$ between γ and γ' can be lifted to a homotopy $\tilde{H} : [0,1] \times [0,1] \to Y$ between $\tilde{\gamma}$ and $\tilde{\gamma}'$ by theorem 2.2.3. Since $\tilde{H}_1$ is a lift of the constant map to $\gamma(1) = \gamma'(1)$, we have $\tilde{\gamma}(1) = \tilde{\gamma}'(1)$.

Also note that every element $[\gamma]$ of $\pi_1(X)$ actually defines an automorphism on the fiber $p^{-1}(x)$: denote with γ^{-1} the reverse path of γ, i.e., we define $\gamma^{-1} : [0,1] \to X, t \mapsto \gamma(1-t)$. If $[\gamma] \cdot y = [\gamma] \cdot y'$ for some $y, y' \in p^{-1}(x)$, then let $\tilde{\gamma}_y \odot \tilde{\gamma}_{y'}^{-1}$ be the concatenation of $\tilde{\gamma}_y$ and $\tilde{\gamma}_{y'}^{-1}$. Note that $(\tilde{\gamma}_y \odot \tilde{\gamma}_{y'}^{-1})(1) = y'$. Then $[p(\tilde{\gamma}_y \odot \tilde{\gamma}_{y'}^{-1})] = [\gamma \odot \gamma^{-1}] = [\mathrm{const}_x]$, where const_x is the constant map on x. Then we find $y = [\mathrm{const}_x] \cdot y = [p(\tilde{\gamma}_y \odot \tilde{\gamma}_{y'}^{-1})] \cdot y = y'$. This proves injectivity. For any $y \in p^{-1}(x)$ let $\widetilde{\gamma^{-1}}_y$ be the lift of γ^{-1} with $\widetilde{\gamma^{-1}}_y(0) = y$. Denote $y' := \widetilde{\gamma^{-1}}_y(1)$. Then $\widetilde{\gamma^{-1}}_y^{-1}$ is the lift of γ with $\widetilde{\gamma^{-1}}_y^{-1}(0) = y'$ and $\widetilde{\gamma^{-1}}_y^{-1}(1) = y$. Therefore, $[\gamma] \cdot y' = y$. This proves surjectivity. □

There is a correspondence between covering spaces and subgroups of the fundamental group. Before we state this correspondence, we're going to expand our vocabulary of covering spaces a little.

Definition 2.2.7. *Let $p : Y \to X$ be a covering.*

(1) A covering $p' : Y' \to X$ is called a subcovering *of p if there exists a continuous $f : Y \to Y'$ such that $p = p' \circ f$. Then f is called a* morphism of coverings.

(2) A deck transformation *or* covering transformation *is a homeomorphism $h : Y \to Y$ such that $p = p \circ h$. The group of deck transformations is denoted by* $\mathrm{Aut}(Y/X)$.

(3) The covering p is called Galois *or* Normal *if for every x and every pair $y, y' \in p^{-1}(x)$, there exists a deck transformation $h \in \mathrm{Aut}(Y/X)$ such that $h(y) = y'$. We then denote the group of deck transformations by* $\mathrm{Gal}(Y/X)$.

(4) The space Y is called a universal covering space *if it is simply connected, i.e., if $\pi_1(Y) = 1$.*

It is known that a morphism $Y \to Y'$ of coverings over X is itself a covering if Y, Y' and X are connected and X is locally connected [Ful95, Exercise 11.12]. Furthermore, if Y is connected and $p : Y \to X$ is a covering, then P is Galois if and only if for every x and every pair $y, y' \in p^{-1}(x)$ there is a unique $h \in \mathrm{Aut}(Y/X)$ such that $h(y) = y'$ [Die10, p. 65]. Since these conditions certainly hold for connected covers of 3-manifolds (e.g. connected covers of the knot complement X_K in S^3), we will make regular use of these facts.

Example 2.2.8. We continue our example of the circle. Let p_n and p_∞ be defined as in example 2.2.2. Since $\mathbb{R}$ is simply connected, p_∞ is a universal cover. Define $h_n : \mathbb{R} \to S^1, x \mapsto e^{2\pi x i/n}$ for $n \geq 1$ and note that $p_\infty = p_n \circ h_n$. This shows that every p_n is a subcover of p_∞. ▶

We now state the Galois correspondence for coverings.

Theorem 2.2.9. *By a* connected covering *we mean a covering $p : Y \to X$ such that Y is connected. The map $p_* : \pi_1(Y) \to \pi_1(X)$ induced by such coverings is injective and gives rise to a bijection*

$$\{\text{conn. cov. } p : Y \to X\}/\text{isom.} \longrightarrow \{\text{subgroups of } \pi_1(X)\}/\text{conjugacy}$$
$$(p : Y \to X) \longmapsto p_*(\pi_1(Y)).$$

This correspondence has the following properties:

(1) *A covering* $p' : Y' \to X$ *is a subcover of* $p : Y \to X$ *if and only if* $p_*(\pi_1(Y))$ *is a subgroup of* $p'_*(\pi_1(Y'))$ *up to conjugacy.*

(2) *A covering* $p : Y \to X$ *is Galois if and only if* $p_*(\pi_1(Y))$ *is a normal subgroup of* $\pi_1(X)$. *We then have* $\mathrm{Gal}(Y/X) \cong \pi_1(X)/p_*(\pi_1(Y))$.

Furthermore, if $p : Y \to X$ *is a Galois cover we have a bijection*

$$\{\text{conn. subcov. of } p : Y \to X\}/\mathrm{Gal}(Y/X) \longrightarrow \{\text{subgroups of } \mathrm{Gal}(Y/X)\}/\text{conjugacy}$$

between connected subcovers of p *and subgroups of* $\mathrm{Gal}(Y/X)$.

Example 2.2.10. Let X be a topological space and suppose it has a universal covering $\tilde{X} \to X$. Since $\pi_1(\tilde{X}) = 1$, theorem 2.2.9(2) tells us that p is a Galois cover with $\mathrm{Gal}(\tilde{X}/X) \cong \pi_1(X)/p_*(\pi_1(\tilde{X})) = \pi_1(X)$. Since $p_*(\pi_1(\tilde{X}))$ is a subgroup of any subgroup of $\pi_1(X)$, by theorem 2.2.9(1) any connected cover of X is a subcover of the universal cover.

A connected and locally path-connected space X has a universal covering if and only if X is semilocally simply connected, i.e., every point $x \in X$ has a neighborhood U such that the homomorphism $\pi_1(U, x) \to \pi_1(X, x)$ is trivial [Kos80, Theorem 22.1]. In particular, this holds for link complements, so every connected cover of a link complement is a subcover of its universal cover. ▶

Example 2.2.11. We continue our example of the circle. Define p_n and p_∞ as in example 2.2.2. Since p_∞ is a Galois cover, theorem 2.2.9 tells us

$$\pi_1(S^1) = \pi_1(S^1)/(p_\infty)_*(\pi_1(\mathbb{R})) \cong \mathrm{Gal}(\mathbb{R}/S^1) \cong \mathbb{Z}.$$

Note that the only subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for $n \geq 0$. Since every covering $p_n : S^1 \to S^1$ is Galois with

$$\mathrm{Gal}(S^1/S^1) = \langle z \mapsto \zeta_n z \rangle \cong \mathbb{Z}/n\mathbb{Z} \cong \pi_1(S^1)/n\mathbb{Z},$$

by theorem 2.2.9(2) we get $(p_n)_*(\pi_1(S^1)) \cong n\mathbb{Z}$ for every $n \in \mathbb{N}$. Therefore, p_∞ and p_n give all possible connected coverings of the circle. ▶

As seen in the last two examples, we can get information on the structure of the fundamental group by looking at the universal cover. Next, we want to define the so-called infinite cyclic cover of a knot complement. For this we will need some information about the knot group. Here is a key fact that we will use.

Lemma 2.2.12. *Let* $K \subseteq S^3$ *be a knot. We have* $G_K^{ab} \cong \mathbb{Z}$, *where* G_K^{ab} *is the abelianization of the knot group.*

Proof. This proof will make use of some homology theory. Let $V := V_K$ be a tubular neighboorhood of K. Set $U := S^3 \setminus K$, the knot complement of K. Since $U \cup V = S^3$, we can apply the Mayer-Vietoris sequence

$$\ldots \longrightarrow H_2(S^3;\mathbb{Z}) \longrightarrow H_1(U \cap V;\mathbb{Z}) \longrightarrow H_1(U;\mathbb{Z}) \oplus H_1(V;\mathbb{Z}) \longrightarrow H_1(S^3;\mathbb{Z}) \longrightarrow \ldots \tag{2.1}$$

The first homology group of the torus T is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$ (this can be calculated using the homology of CW-complexes, which we will not go into here). Since $U \cap V$ is homotopy equivalent to the torus, we have $H_1(U \cap V;\mathbb{Z}) \cong H_1(T;\mathbb{Z})$. Likewise, we get $H_1(V;\mathbb{Z}) \cong H_1(S^1;\mathbb{Z}) \cong \mathbb{Z}$, so (2.1) reduces to the exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \longrightarrow H_1(U;\mathbb{Z}) \oplus \mathbb{Z} \longrightarrow 0.$$

From the isomorphism $\mathbb{Z} \oplus \mathbb{Z} \cong H_1(U;\mathbb{Z}) \oplus \mathbb{Z}$ it follows that $H_1(U;\mathbb{Z})$ is a finitely generated projective $\mathbb{Z}$-module [Eis04, Appendix 3, Proposition A3.1], so it is free[Corollary 8.5]Rot-Adv. This gives us $H_1(U;\mathbb{Z}) \cong \mathbb{Z}$. By the Hurewicz theorem we have $H_1(U;\mathbb{Z}) \cong \pi_1^{ab}(U)$, from which $G_K^{ab} \cong \mathbb{Z}$ follows. □

We can now define the infinite cyclic cover.

Definition 2.2.13. *Let $K \subseteq S^3$ be a knot and $X_K := S^3 \setminus K$ the knot complement. By theorem 2.2.9 there exists a connected cover $p : X_\infty \to X_K$ such that $p_*(\pi_1(X_\infty)) = [G_K, G_K]$ which is uniquely defined up to isomorphism over X_K. We then have*

$$\mathrm{Gal}(X_\infty/X) \cong \pi_1(X)/p_*(\pi_1(X_\infty)) = G_K^{ab} \cong \mathbb{Z}.$$

We call X_∞ the infinite cyclic cover *of X. By theorem 2.2.9, there exists a subcover $X_n \to X_K$ such that $\mathrm{Gal}(X_n/X_K) \cong \mathbb{Z}/n\mathbb{Z}$. We call this cover X_n the* n-fold cyclic cover *of X_K.*

Using Seifert surfaces, we can give an explicit construction of the infinite cyclic cover.

Example 2.2.14. Let $K \subseteq S^3$ be a knot. Let S_K be a Seifert surface of K. Let Y be the space obtained by cutting the knot complement $X_K := S^3 \setminus K$ along $S_K \cap X_K$. Figure 2.5 illustrates this cut. We can also see how Y contains two surfaces homeomorphic to $S_K \cap X_K$, indicated in figure 2.5 by S^+ and S^-.

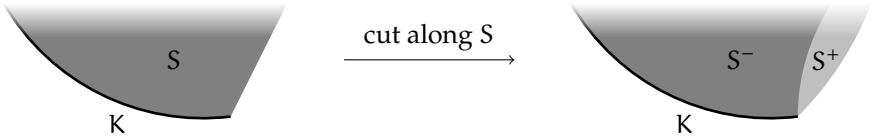


Fig. 2.5: Cutting along a Seifert surface S.

Now let Y_i be a copy of Y for every $i \in \mathbb{Z}$, where we denote $S_i^+ := S^+ \subseteq Y_i$ and $S_i^- := S^- \subseteq Y_i$. Then we get X_∞ by taking the disjoint union $\bigsqcup_{i\in\mathbb{Z}} Y_i$ and identifying S_i^+ with S_{i+1}^- for every $i \in \mathbb{Z}$. The canonical projection $p : X_\infty \to X_K$ now gives an infinite cyclic cover.

We can construct an n-fold cyclic cover X_n of X_K likewise. We simply let Y_i be a copy of Y for every $i \in \mathbb{Z}/n\mathbb{Z}$ and define S_i^+ and S_i^- as above. We then obtain X_n by taking the disjoint union $\bigsqcup_{i\in\mathbb{Z}/n\mathbb{Z}} Y_i$ and identifying S_i^+ with S_{i+1}^- for every $i \in \mathbb{Z}/n\mathbb{Z}$. ▶

Finally, we give the definition of a ramified covering.

Definition 2.2.15. *Let M and N be n-manifolds, where $n \geq 2$, and let $f : N \to M$ be continuous. Define $S_N := \{y \in N \mid f \text{ is not a homeomorphism in a neighborhood of } y\}$ and $S_M := f(S_N)$. Let $D^k \subseteq \mathbb{R}^k$ be the k-dimensional unit disk. We say that $f : N \to M$ is a* covering ramified over S_M *if the following conditions are satisfied:*

1) *The map $f|_{N\setminus S_N} : N \setminus S_N \to M \setminus S_M$ is a covering map.*

2) *For every $y \in S_N$, there are a neighborhood V of y, a neighborhood U of $f(y)$, homeomorphisms $\phi : V \to D^2 \times D^{n-2}$ and $\psi : U \to D^2 \times D^{n-2}$ and an integer $e = e(y) > 1$ such that $(f_e \times \mathrm{id}_{D^{n-2}}) \circ \phi = \psi \circ f$, where $f_e(z) := z^e$ (considering D^2 in the complex plane). The integer e is called the* ramification index *of y.*

We call $f|_{N\setminus S_N}$ *the* covering associated to f. *When* $f|_{N\setminus S_N}$ *is a Galois covering, we call* f *a* ramified Galois covering.

The concept of ramified coverings serves a very useful purpose in the context of knots and links.

Example 2.2.16. Let K be a knot in S^3 and let S_K be a Seifert surface of K. Let Y be S^3 cut along S_K. Then we obtain two surfaces S^+ and S^- homeomorphic to S_K (cf. example 2.2.14). If we take $n > 0$ copies of Y, we can construct a space M_n by identifying $S_i^+ := S^+ \subseteq Y_i$ with $S_{i+1}^- := S^- \subseteq Y_{i+1}$ for all $i \in \mathbb{Z}/n\mathbb{Z}$. The canonical projection $p : M_n \to S^3$ is almost a covering map. To be exact, $p|_{M_n \setminus p^{-1}(K)} : M_n \setminus p^{-1}(K) \to X_K$ is the n-fold cyclic cover. We will show that the map p is actually a covering ramified over K.

Let $y \in p^{-1}(K)$ and set $x := p(y) \in K$. Let V_K be a tubular neighborhood of K. Take U to be a neighborhood of x homeomorphic to $D^2 \times D^1 \subseteq V_K$ through ψ. Set $V := p^{-1}(U)$ and $V_i = p^{-1}(U) \cap Y_i$ for all i. We have $V \cong D^2 \times D^1$ through a homeomorphism ϕ, where the solid torus segment V has to wrap around $p^{-1}(K)$ in n copies of Y. Therefore, if we set $f_n : D^2 \to D^2, z \mapsto z^n$, then

$$\begin{array}{ccc} V & \xrightarrow{\phi} & D^2 \times D^1 \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle f_n \times \mathrm{id}_{D^1}} \\ U & \xrightarrow{\psi} & D^2 \times D^1 \end{array}$$

commutes, so p is a ramified (Galois!) covering over K with ramification index n. See figure 2.6 for an illustration where $n = 3$. This construction is called the *Fox completion* of the covering $p|_{M_n \setminus p^{-1}(K)} : M_n \setminus p^{-1}(K) \to X_K$. ▶

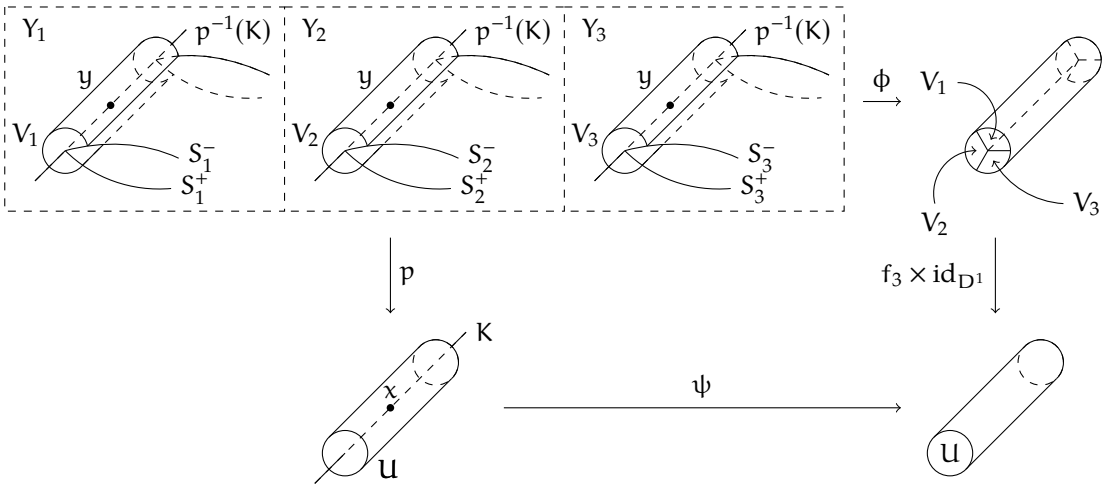


Fig. 2.6: A covering $Y_1 \cup Y_2 \cup Y_3 \to S^3$ ramified over K with ramification index $e = 3$.

CHAPTER 3

Algebraic preliminaries

In this chapter we'll gain some familiarity with concepts and constructions such as p-adic numbers, étale morphisms and affine schemes.

3.1 *Profinite groups*

To define the étale fundamental group, we'll need to know what a profinite group is. We start with the definition of a topological group.

Definition 3.1.1. *A* topological group *is a group* G *with a topology such that the group operation is continuous.*

A profinite group is constructed using inverse systems of finite groups. We'll need the following definitions.

Definition 3.1.2. *Let* $(I, \leq)$ *be a partially ordered set. Let* $(C_i)_{i\in I}$ *be a collection of objects in a category* C *and for every* $i \leq j$ *let* $f_{ij} : C_j \to C_i$ *be a morphism. Then* $((C_i)_{i\in I}, (f_{ij})_{i\leq j})$ *is an* inverse system *if it satisfies the following properties:*

1) For every $i \in I$ *we have* $f_{ii} = \mathrm{id}_{C_i}$.

2) For every $i \leq j \leq k$ *we have* $f_{ik} = f_{ij} \circ f_{jk}$.

Inverse systems give rise to inverse limits.

Definition 3.1.3. *Let* $((G_i)_{i\in I}, (f_{ij})_{i\leq j})$ *be an inverse system of groups. We define the inverse limit of this inverse system as follows:*

$$\varprojlim_i G_i := \{(x_i)_{i\in I} \in \prod_{i\in I} G_i \mid \text{for all } i \leq j \text{ we have } f_{ij}(x_j) = x_i\}.$$

We will most commonly deal with inverse systems of groups or rings, specifically profinite groups and rings.

Definition 3.1.4. *We call a group* G *a* profinite group *if we have*

$$G \cong \varprojlim_i G_i$$

for some inverse system $((G_i)_{i\in I}, (f_{ij})_{i\leq j})$ *of finite groups. Similarly, a ring* R *is called a* profinite ring *if we have*

$$R \cong \varprojlim_j R_j$$

for some inverse system $((R_j)_{j\in J}, (g_{ij})_{i\leq j})$ *of finite rings.*

Profinite groups $G = \varprojlim_i G_i$ and profinite rings $R = \varprojlim_j R_j$ are often endowed with the topology induced by the product topology on $\prod_{i\in I} G_i$ or $\prod_{j\in J} R_j$, which turns them into topological groups and topological rings, respectively.

The canonical example of a profinite group or ring are the p-adic integers. These arise as the inverse limit of an inverse system obtained by modular arithmetic. Firstly, note that $\mathbb{N}$ has an obvious partial order. Secondly, for every $m \leq n$ we have canonical quotient maps $q_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$. Since for every $l \leq m \leq n$ we have $q_{ln} = q_{lm} \circ q_{mn}$, we find that the quotient groups $\mathbb{Z}/p^n\mathbb{Z}$ form an inverse system. We can now define the p-adic integers.

Definition 3.1.5. *Let* $p \in \mathbb{Z}$ *be a prime. The* ring of p-adic integers $\mathbb{Z}_p$ *is the inverse limit of the inverse system* $((\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}, (q_{mn})_{m\leq n})$*:*

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Let's see what the p-adic integers look like explicitly.

Example 3.1.6. Elements of $\mathbb{Z}_p$ are sequences $(a_1, a_2, a_3, \ldots)$ of integers where $a_n \equiv a_m \bmod p^m$ for all $m \leq n$. The ring homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ sends an integer n to the element $(n, n, n, \ldots) \in \mathbb{Z}_p$. This homomorphism is not surjective, however. For example,

$$\Big(\sum_{i=0}^{n-1} p^i\Big)_{n\in\mathbb{Z}} = (1, 1+p, 1+p+p^2, 1+p+p^2+p^3, \ldots)$$

is well-defined in $\mathbb{Z}_p$, but is not in the image of $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. Now let's observe some more facts of $\mathbb{Z}_p$. Addition and multiplication in $\mathbb{Z}_p$ is done pointwise, i.e., we have

$$(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) := (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$$

and

$$(a_1, a_2, a_3, \ldots) \cdot (b_1, b_2, b_3, \ldots) := (a_1b_1, a_2b_2, a_3b_3, \ldots).$$

This is well-defined because addition and multiplication of integers respects the congruence relation in modular arithmetic. This means that $(1, 1, 1, \ldots)$ is the multiplicative identity in $\mathbb{Z}_p$. Then what does $\mathbb{Z}_p^\times$ look like? It turns out that the units of $\mathbb{Z}_p$ are easy to characterize.

Let $(x_1, x_2, x_3, \ldots) \in \mathbb{Z}_p$. To find out if $(x_1, x_2, x_3, \ldots)$ is a unit, we have to find out if any multiple of x_i is congruent to 1 for all i. The answer is neatly given by the following equivalences:

$$nx_i \equiv 1 \bmod p^i \text{ for some } n \in \mathbb{N} \iff \gcd(x_i, p^i) = 1 \iff p \nmid x_i \iff x_1 \neq 0.$$

Therefore, $(x_1, x_2, x_3, \ldots) \in \mathbb{Z}_p^\times$ if and only if $x_1 \neq 0$. ▶

Lastly, we mention the profinite completion of a group. Let G be a group and consider the set $\mathcal{N}$ of normal subgroups $N \lhd G$ such that G/N is finite. Then the quotient groups, together with the canonical quotient maps $q_{MN} : G/M \to g/N$ for $M \subseteq N$, form an inverse system of finite groups. We define the profinite completion as its inverse limit.

Definition 3.1.7. *Let G be a group and define the set*

$$\mathcal{N} := \{N \lhd G \mid G/N \text{ is finite}\},$$

which is naturally partially ordered by inclusion. Then the profinite group

$$\hat{G} := \varprojlim_{N \in \mathcal{N}} G/N$$

is called the profinite completion *of* G.

Example 3.1.8. Consider the group $\mathbb{Z}$. Every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, so $\mathcal{N}$ is the set of all sugroups of $\mathbb{Z}$. We get

$$\hat{\mathbb{Z}} = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z}$$

and elements of $\hat{\mathbb{Z}}$ are sequences $(a_1, a_2, a_3, \ldots)$ where $a_n \in \mathbb{Z}/n\mathbb{Z}$ and where $a_n \equiv a_m \bmod m$ if $m|n$, e.g., $(0, 1, 2, 3, \ldots) \in \hat{\mathbb{Z}}$. ▶

3.2 *Affine schemes*

In this section we'll briefly explore affine schemes. Since an affine scheme is defined as the spectrum of some commutative ring with a certain topology defined on it, they are integral to the study of primes. We start with the definition of the Zariski topology on the spectrum of a ring.

Proposition 3.2.1. *Let R be a commutative ring with an ideal $I \subseteq R$. Define $V_I := \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}$. The collection of closed sets $\bigcup_{I \subseteq R \text{ ideal}} \{V_I\}$ defines a topology on* $\operatorname{Spec} R$. *We call this the* Zariski topology.

Proposition 3.2.1, as well as the following lemma, is easy to prove, but can be found in [Mum99, Chap. II, Sect. 1].

Lemma 3.2.2. *Let R be a commutative ring and $f \in R$. Define $D_f := \{\mathfrak{p} \in \operatorname{Spec} R \mid f \notin \mathfrak{p}\}$. Then $(D_f)_{f \in R}$ forms a basis for the Zariski topology on* $\operatorname{Spec} R$.

In the following, let R_f indicate the localization of the ring R at the multiplicatively closed set $\{f, f^2, f^3, \ldots, \}$, i.e., R_f consists of fractions r/f^n, where $r \in R$ and $n \in \mathbb{N}$. For a more rigorous treatment, see [Eis04, Chap. 2, Sect. 1].

Lemma 3.2.3. *Let R be a commutative ring and endow* $\operatorname{Spec} R$ *with the Zariski topology. Define the partial order $f \leq g \Leftrightarrow D_f \subseteq D_g$. Let $f, g \in R$ and suppose $D_f \subseteq D_g$. Then $f^n = gh$ for some $n \in \mathbb{N}$ and $h \in R$ and we can define a map $\phi_{fg} : R_g \to R_f, \frac{a}{g^m} \mapsto \frac{ah^m}{f^{nm}}$. Then $((R_f)_{f \in R}, (\phi_{fg})_{f \leq g})$ is an inverse system of rings.*

Proof. First, suppose $D_f \subseteq D_g$. Then for every $\mathfrak{p}$ with $g \in \mathfrak{p}$ we have $f \in \mathfrak{p}$. It is a basic fact in commutative algebra that the radical of an ideal I is the intersection of all prime ideals containing I, so $f \in \sqrt{(g)}$. This gives us $f^n = gh$ for some $n \in \mathbb{N}$ and $h \in R$. To check that $((R_f)_{f\in R}, (\phi_{fg})_{f\leq g})$ is an inverse system, let $f_1 \leq f_2 \leq f_3$, with $f_1^{n_1} = f_2 h_1$ and $f_2^{n_2} = f_3 h_2$ (so $f_1^{n_1 n_2} = f_3 h_1^{n_2} h_2$). Then

$$(\phi_{f_2 f_3} \circ \phi_{f_1 f_2})(a/(f_1^i)) = \phi_{f_2 f_3}(a h_2^i / f_2^{n_2 i}) = a h_2^i h_1^{n_2 i} / f_1^{n_1 n_2 i} = \phi_{f_1 f_3}(a/f_3^i).$$

Also, we clearly have $\phi_{ff} = \mathrm{id}_{R_f}$, so $((R_f)_{f\in R}, (\phi_{fg})_{f\leq g})$ is an inverse system of rings. □

Now we are ready to define the structure sheaf on a spectrum. To this end, note that a topological space X can be viewed as a category with the open sets as its objects and inclusion maps between open sets as its arrows. This way, we can view $\operatorname{Spec} R$ as a category.

Definition 3.2.4. *Let* R *be a commutative ring and endow* $\operatorname{Spec} R$ *with the Zariski topology. The* structure sheaf *on* $\operatorname{Spec} R$ *is the functor*

$$\begin{aligned} \mathcal{O}_{\operatorname{Spec} R} : \quad \operatorname{Spec} R &\longrightarrow \mathbf{CRing} \\ U &\longmapsto \varprojlim_{\substack{f\in R \\ D_f \subseteq U}} R_f \\ (i : U_1 \hookrightarrow U_2) &\longmapsto \left(\varprojlim_{\substack{f\in R \\ D_f \subseteq U_2}} R_f \to \varprojlim_{\substack{f\in R \\ D_f \subseteq U_1}} R_f, (x_f)_{D_f \subseteq U_2} \mapsto (x_f)_{D_f \subseteq U_1} \right), \end{aligned}$$

where **CRing** *is the category of commutative rings.*

The idea behind this definition is that the structure sheaf on $\operatorname{Spec} R$ is the unique sheaf that sends open sets D_f to R_f.

Definition 3.2.5. *An* affine scheme $(\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$ *is a spectrum* $\operatorname{Spec} R$ *of some commutative ring* R *equipped with the Zariski topology together with its structure sheaf.*

We will rarely make explicit use of the Zariski topology and the structure sheaf. Instead, we will make extensive use of the following duality between the category of affine schemes and the category of commutative rings.

Theorem 3.2.6. *The functor*

$$\begin{aligned} \operatorname{Spec} : \quad \mathbf{CRing} &\longrightarrow \mathbf{Aff} \\ R &\longmapsto \operatorname{Spec} R \\ (f : R \to S) &\longmapsto (\operatorname{Spec} S \to \operatorname{Spec} R, \mathfrak{p} \mapsto f^{-1}(\mathfrak{p})) \end{aligned}$$

defines a duality between the category **CRing** *of commutative rings and the category* **Aff** *of affine schemes.*

There are some very useful consequences of this duality. For one, for all $R, S \in \mathbf{CRing}$ there is a one-to-one correspondence between ring homomorphisms $R \to S$ and morphisms of schemes $\operatorname{Spec} S \to \operatorname{Spec} R$. Also, since $\mathbb{Z}$ is an initial object in **CRing**, i.e., for every commutative ring R there is exactly one ring homomorphism $\mathbb{Z} \to R$, by the above duality $\operatorname{Spec} \mathbb{Z}$ is a terminal object in **Aff**, i.e., for every affine scheme $\operatorname{Spec} R$ there is exactly one morphism of schemes $\operatorname{Spec} R \to \operatorname{Spec} \mathbb{Z}$.

Example 3.2.7. Let's take a look at $\operatorname{Spec}\mathbb{Z}$ and how it interacts with $\operatorname{Spec}\mathbb{F}_p$. For every prime $p \in \mathbb{Z}$ there is a unique ring homomorphism $q : \mathbb{Z} \to \mathbb{F}_p$. Therefore, there is also a unique morphism of schemes $i : \operatorname{Spec}\mathbb{F}_p \to \operatorname{Spec}\mathbb{Z}$. Since every field has only one prime ideal, namely the zero ideal 0, we have $i(0) = q^{-1}(0) = (p)$. Figure 3.1 illustrates the way $\operatorname{Spec}\mathbb{F}_p$ injects into $\operatorname{Spec}\mathbb{Z}$. ▶

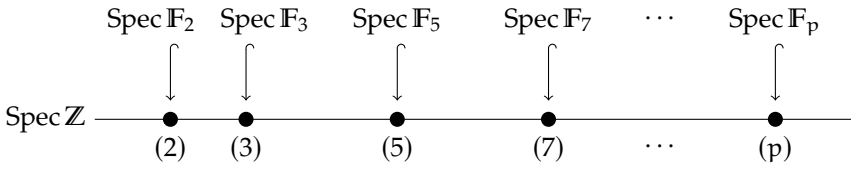


Fig. 3.1: Primes in $\operatorname{Spec}\mathbb{Z}$.

3.3 *Finite étale coverings*

In order to define the étale fundamental group, we need to know what a finite étale algebra is.

Definition 3.3.1. *Let* K *be a field and let* A *be a* K*-algebra. We call* A finite étale *if* A *is a finite product of finite separable extensions, i.e.,* $A = \prod_{i=1}^{n} L_i$ *for some* n*, where every* L_i/K *is a finite separable field extension.*

Next we have the notion of a finite étale morphism.

Definition 3.3.2. *Let* $f : \operatorname{Spec} B \to \operatorname{Spec} A$ *be a morphism of affine schemes. We call* f *(or the corresponding ring homomorphism* $A \to B$*) a* finite étale morphism *or a* finite étale covering *if* B *is a finitely generated, flat* A*-module and for any prime* $\mathfrak{p} \in \operatorname{Spec} A$*, the* fiber $B \otimes_A \kappa(\mathfrak{p})$ *is a finite étale* $\kappa(\mathfrak{p})$*-algebra. Here* $\kappa(\mathfrak{p}) := \operatorname{Frac}(A/\mathfrak{p})$ *is the* residue field *of* $\mathfrak{p}$*. We call* B *a* finite étale A-algebra *if there exists a finite étale morphism* $A \to B$*.*

As the terminology implies, finite étale covers are the algebraic analogue of finite topological coverings. To see this, let $p : Y \to X$ be an n-fold covering and $U \subseteq X$ an evenly covered open set, i.e., $p^{-1}(U) = \bigsqcup_{i=1}^{n} V_i$. Then the inverse $p^{-1}(U)$ and its maps $p^{-1}(U) \to U$ and $p^{-1}(U) \to Y$ give the pullback of $U \hookrightarrow X \hookleftarrow Y$:

$$\begin{array}{ccc} \bigsqcup_{i=1}^{n} V_i & \longrightarrow & Y \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ U & \hookrightarrow & X \end{array}.$$

Now suppose we have a finite étale covering $f : \operatorname{Spec} B \to \operatorname{Spec} A$ and let $\mathfrak{p} \in \operatorname{Spec} A$. The canonical map $A \to \kappa(\mathfrak{p})$ induces an embedding $\operatorname{Spec}\kappa(\mathfrak{p}) \hookrightarrow \operatorname{Spec} A$ that sends the only prime 0 of $\kappa(\mathfrak{p})$ to $\mathfrak{p} \in \operatorname{Spec} A$. It turns out that the pullback of $\operatorname{Spec}\kappa(\mathfrak{p}) \hookrightarrow \operatorname{Spec} A \hookleftarrow \operatorname{Spec} B$ is given by $\operatorname{Spec} B \otimes_A \kappa(\mathfrak{p})$ with maps $\operatorname{Spec} B \otimes_A \kappa(\mathfrak{p}) \to \operatorname{Spec}\kappa(\mathfrak{p})$ and $\operatorname{Spec} B \otimes_A \kappa(\mathfrak{p}) \to \operatorname{Spec} B$. Since $\operatorname{Spec} B \to \operatorname{Spec} A$ is finite étale, we have $B \otimes_A \kappa(\mathfrak{p}) = \prod_{i=1}^{n} L_i$, where $L_i/\kappa(\mathfrak{p})$ is a finite separable

extension for every i. Since $\operatorname{Spec} \prod_{i=1}^{n} L_i = \bigsqcup_{i=1}^{n} \operatorname{Spec} L_i$, we get the following pullback diagram:

$$\begin{array}{ccc} \bigsqcup_{i=1}^{n} \operatorname{Spec} L_i & \longrightarrow & \operatorname{Spec} B \\ \downarrow & & \downarrow f \\ \operatorname{Spec} \kappa(\mathfrak{p}) & \hookrightarrow & \operatorname{Spec} A \end{array}.$$

We can see that, analogous to the topological case, $\operatorname{Spec} \kappa(\mathfrak{p})$ is covered by the n primes of $\prod_{i=1}^{n} L_i$.

Example 3.3.3. Let $A \to B$ be a ring homomorphism. If A is a field, then its only prime is (0) and we have $B \otimes_A \kappa(\mathfrak{p}) \cong B \otimes_A A \cong B$. Therefore, a $A \to B$ is finite étale if and only if B is a finite étale A-algebra, i.e., if and only if $B = \prod_{i=1}^{n} L_i$ for some n, where every L_i/A is a finite separable field extension. In particular, a field extension B/A is finite étale if and only if it is finite separable. ▶

Example 3.3.4. Let d be a squarefree integer. Let's take a look at the map $\mathbb{Z} \to \mathbb{Z}[\sqrt{d}]$ and why it is not finite étale. Let p be a prime number. We have

$$\mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} \mathbb{Z}/(p) \cong \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}],$$

so if $p\mathbb{Z}[\sqrt{d}]$ is a prime ideal, the fiber $\mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$ is the finite separable field extension $\mathbb{F}_p[\sqrt{d}]$. If we have a decomposition $p\mathbb{Z}[\sqrt{d}] = \prod_{i=1}^{r} \mathfrak{p}_i$ of $p\mathbb{Z}[\sqrt{d}]$ into pairwise distinct prime ideals, by the Chinese remainder theorem we get

$$\mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} \mathbb{Z}/(p) \cong \prod_{i=1}^{r} \mathbb{Z}[\sqrt{d}]/\mathfrak{p}_i,$$

which is a finite product of finite separable extensions of $\mathbb{F}_p$.

Now suppose p ramifies in $\mathbb{Z}[\sqrt{d}]$, i.e., we have a decomposition $p\mathbb{Z}[\sqrt{d}] = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ of $p\mathbb{Z}[\sqrt{d}]$ into prime ideals where $e_j > 1$ for some $1 \le j \le r$. Choose a non-zero element $x_i \in \mathfrak{p}_i$ for every $1 \le i \le r$. Then $\prod_{i=1}^{r} x_i \in \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$ is a non-trivial nilpotent element, which means $\mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$ can't be a finite product of finite separable field extensions. To summarize: if p ramifies in $\mathbb{Z}[\sqrt{d}]$, then $\mathbb{Z} \to \mathbb{Z}[\sqrt{d}]$ is not finite étale. Since a prime p ramifies in $\mathbb{Z}[\sqrt{d}]$ if and only if p divides the discriminant of $\mathbb{Z}[\sqrt{d}]$ [Mar77, Theorem 24 and Theorem 34] and since the discriminant $\Delta(\mathbb{Z}[\sqrt{d}])$ equals $4d$, we find that there exists some p such that $\mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$ is not a finite étale $\kappa(p)$-algebra. Therefore, $\mathbb{Z} \to \mathbb{Z}[\sqrt{d}]$ is not a finite étale algebra.

More generally, it is known that if $\mathbb{Z} \to B$ is a finite étale cover, then $\operatorname{Frac}(B)/\operatorname{Frac}(\mathbb{Q})$ is an unramified extension. However, by Minkowski's bound, for any non-trivial finite extension $K/\mathbb{Q}$ there is a prime that ramifies in K. Therefore, there are no finite étale covers of $\mathbb{Z}$. ▶

We close this section by defining a finite étale Galois cover.

Definition 3.3.5. *Let A be an integral domain. A finite étale cover $\operatorname{Spec} B \to \operatorname{Spec} A$ is called a* finite étale Galois cover *of $\operatorname{Spec} A$ if $\operatorname{Frac}(B)/\operatorname{Frac}(A)$ is a finite Galois extension and if there exists a finite separable extension $K/\operatorname{Frac}(B)$ such that B is the integral closure of A in K. We then call B a* finite Galois algebra *over A and denote the automorphism group of B over A by $\operatorname{Gal}(B/A)$. Likewise, we write $\operatorname{Gal}(\operatorname{Spec} B/\operatorname{Spec} A) := \operatorname{Aut}(\operatorname{Spec} B/\operatorname{Spec} A)$.*

For a finite étale Galois cover $\operatorname{Spec} B \to \operatorname{Spec} A$ we have

$$\operatorname{Gal}(\operatorname{Spec} B/\operatorname{Spec} A) \cong \operatorname{Gal}(B/A) \cong \operatorname{Gal}(\operatorname{Frac}(B)/\operatorname{Frac}(A)).$$

Interlude on Galois categories

Before we define the étale fundamental group, let's take a look at how the topological fundamental group arises in the context of category theory. We need some rudimentary concepts for this.

Definition 3.3.6. *Let G be a topological group. A* G-set *is a set X with a group action of G on X which is continuous when X is equipped with the discrete topology.*

Next we need to know what the automorphism group of a functor is.

Definition 3.3.7. *Let $\mathcal{C}$ and $\mathcal{D}$ be categories and let $F : \mathcal{C} \to \mathcal{D}$ be a functor. An* automorphism of F *is a collection of isomorphisms $(\mu_C : F(C) \to F(C))_{C \in \mathcal{C}}$ such that for every morphism $f : C \to D$ in $\mathcal{C}$ the diagram*

$$\begin{array}{ccc} F(C) & \xrightarrow{F(f)} & F(D) \\ {\scriptstyle \mu_C}\downarrow & & \downarrow{\scriptstyle \mu_D} \\ F(C) & \xrightarrow{F(f)} & F(D) \end{array}$$

commutes. The automorphisms on F form a group, the automorphism group *of F, usually denoted* $\operatorname{Aut}(F)$.

Now we can move on to Galois categories.

Definition 3.3.8. *A* Galois category *is a category $\mathcal{C}$ together with a functor $F : \mathcal{C} \to \mathbf{Set}$ such that $\mathcal{C}$ is equivalent to the category* $\operatorname{Aut}(F)$-**set** *of finite* $\operatorname{Aut}(F)$*-sets. The functor F is called the* fundamental functor.

To illustrate where this is going, let's compute the automorphism group of a functor explicitly.

Example 3.3.9. Let $\mathbf{Cov}_X$ be the category of connected coverings of a topological space X with basepoint $x \in X$ and let $F : \mathbf{Cov}_X \to \mathbf{Set}$ be the functor that sends a covering $p : Y \to X$ to the fiber $p^{-1}(x)$ and that sends a morphism $f : Y \to Y'$ of coverings to its restriction $f|_{p^{-1}(x)}$. Now let $\mu \in \operatorname{Aut}(F)$ be an automorphism of F and let $f : Y \to Y'$ be a morphism of coverings $p : Y \to X$ and $p' : Y' \to X$. Note that f is a covering map (definition 2.2.7) and therefore surjective. The following diagram commutes:

$$\begin{array}{ccc} p^{-1}(x) & \xrightarrow{f} & (p')^{-1}(x) \\ {\scriptstyle \mu_Y}\downarrow & & \downarrow{\scriptstyle \mu_{Y'}} \\ p^{-1}(x) & \xrightarrow{f} & (p')^{-1}(x) \end{array}.$$

The important thing to realize here is that since Y' is a subcover of Y, the bijection $\mu_{Y'}$ is determined by μ_Y: for every element $y \in (p')^{-1}(x)$ we have $\mu_{Y'}(y) = (f \circ \mu_Y \circ f^{-1})(y)$. By theorem 2.2.9, we know that the universal cover $\tilde{X}$ of X covers all coverings, so the entire automorphism μ is determined by the bijection $\mu_{\tilde{X}}$, which is in turn determined by a deck transformation $g \in \operatorname{Gal}(\tilde{X}/X)$. Therefore, the automorphism group of F is isomorphic to $\operatorname{Gal}(\tilde{X}/X)$, which is isomorphic to $\pi_1(X)$ by theorem 2.2.9. ▶

Looking at the chosen terminology, one could expect that the automorphism group of the fundamental functor is the fundamental group. Alas, since the category $\mathbf{Cov}_X$ does not only contain finite covers, it is not a Galois category. The category $\mathbf{FCov}_X$ of finite connected covers of X, however, is Galois, and it turns out that it is equivalent to the category of finite $\hat{\pi}_1(X)$-sets, where $\hat{\pi}_1(X)$ is the profinite completion of $\pi_1(X)$.

Similarly to $\mathbf{FCov}_X$, the category $\mathbf{FEt}_X$ of finite étale covers of an affine scheme X together with the fiber functor $F : \mathbf{FEt}_X \to \mathbf{Set}$ which we will define in the next section, is also a Galois category. Therefore, it is equivalent to the category of finite $\mathrm{Aut}(F)$-sets. This automorphism group of F will be the étale fundamental group.

3.4 *Étale fundamental groups*

We now want to define the étale fundamental group. In the case of topological spaces, there is an isomorphism $\pi_1(X) \cong \mathrm{Gal}(\tilde{X}/X)$ between the fundamental group of a space X and the galois group of its universal cover $\tilde{X}$ over X. This leads us to define the étale fundamental group of an affine scheme $X := \operatorname{Spec} A$ as the Galois group of its "universal étale covering" over X. Naturally, we need to find the appropriate notion of a universal cover for finite étale maps. For this we need the following results.

Proposition 3.4.1. *Let X be a topological space and $\tilde{p} : \tilde{X} \to X$ a universal covering. Let $x \in X$. Then the fiber functor*

$$\begin{aligned} F_x : \quad \mathbf{Cov}_X &\longrightarrow \mathbf{Set} \\ (Y \to X) &\longmapsto \mathrm{Hom}_X(x, Y) \\ (Y \to Y') &\longmapsto (\mathrm{Hom}_X(x, Y) \to \mathrm{Hom}_X(x, Y')) \end{aligned}$$

is represented by the universal covering, i.e., for any connected covering $p : Y \to X$ there is a bijection

$$\mathrm{Hom}_X(\tilde{X}, Y) \cong p^{-1}(x) = \mathrm{Hom}_X(x, Y).$$

This characterizes a universal property of the universal covering of X. We can now translate this into algebraic terms.

Theorem 3.4.2. *Let A be a commutative ring and $X := \operatorname{Spec} A$. Let $x = \operatorname{Spec} \Omega \hookrightarrow \operatorname{Spec} A$ be a* geometric point, *i.e., Ω is an algebraically closed field. Then the fiber functor*

$$\begin{aligned} F_x : \quad \mathbf{FEt}_X &\longrightarrow \mathbf{Set} \\ (Y \to X) &\longmapsto \mathrm{Hom}_X(x, Y) \\ (Y \to Y') &\longmapsto (\mathrm{Hom}_X(x, Y) \to \mathrm{Hom}_X(x, Y') \end{aligned}$$

is prorepresentable, i.e., there exists an inverse system $((X_i)_{i\in I}, \phi_{ij})$ of finite étale Galois coverings of X such that

$$\varinjlim_{i\in I} \mathrm{Hom}_X(X_i, Y) \cong \mathrm{Hom}_X(x, Y).$$

Although the algebraic analogue of the universal covering is the affine scheme $\tilde{X} := \varprojlim_i X_i$, the fiber functor in theorem 3.4.2 is not actually representable because $\tilde{X}$ is not generally a finite étale cover of X. However, now that we have an analogue of the universal covering space $\tilde{X}_T$ of a topological space X_T, we can use the identity $\mathrm{Gal}(\tilde{X}_T/X_T) \cong \pi_1(X_T)$ (see example 2.2.10) to define the étale fundamental group of an affine scheme.

Definition 3.4.3. *Let* X, x *and* $((X_i)_{i\in I}, \phi_{ij})$ *be as in theorem 3.4.2. Define* $\tilde{X} := \varprojlim_{i\in I} X_i$. *The* étale fundamental group *of* X *is*

$$\pi_1^{\text{ét}}(X, x) := \mathrm{Gal}(\tilde{X}/X) := \varprojlim_{i\in I} \mathrm{Gal}(X_i/X).$$

Example 3.4.4. Let F be a field. Then a finite étale Galois cover of $\operatorname{Spec} F$ corresponds to a finite Galois extension E/F (see also example 3.3.3). Every finite Galois extension is contained in the *separable closure* F^{sep} of F, i.e., the maximal separable extension of F contained in an algebraic closure $\bar{F}$. The extension F^{sep}/F is Galois and we have

$$\pi_1^{\text{ét}}(\operatorname{Spec} F) := \varprojlim_{E/F \text{ finite Galois}} \mathrm{Gal}(E/F) = \mathrm{Gal}\left(\left(\varinjlim_{E/F \text{ finite Galois}} E\right)/F\right) = \mathrm{Gal}(F^{\text{sep}}/F)$$

[Ser79, p. 54, Corollary 1].

Let's see what this means for finite fields. Let p be a prime. The finite extensions of $\mathbb{F}_p$ are $\mathbb{F}_{p^n}$ with $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$. These extensions are naturally ordered by inclusion and can all be embedded in the separable closure $\bar{\mathbb{F}}_p$. We find

$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_p) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Recall that this is the analogue of $\pi_1(S^1) \cong \mathbb{Z}$. ▶

Example 3.4.5. We can further generalize the argument in example 3.3.4 to any Dedekind domain A. Let F be the field of fractions of A and let $A \to B$ be a finite étale Galois cover. Then B is the integral closure of some field K over A and as such, B is itself a Dedekind domain with $\mathrm{Frac}(B) = K$ [Ser79, Chap. 1, Sect. 4]. Let $\mathfrak{p}$ be a non-zero prime in A. Since B is a Dedekind domain, we have a prime decomposition $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ and by the Chinese remainder theorem we have

$$B \otimes_A \kappa(\mathfrak{p}) \cong \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}.$$

From this we find that B is unramified. Therefore, we find that the finite étale Galois covers of A are exactly the unramified ring extensions $A \to B$. Let $\{B_i \mid i \in I\}$ be the collection of unramified ring extensions of A and let $K_i := \mathrm{Frac}(B_i)$ for every $i \in I$. Define $\tilde{F} := \varinjlim_i K_i$. We have

$$\pi_1^{\text{ét}}(\operatorname{Spec} A) = \varprojlim_i \mathrm{Gal}(B_i/A) = \mathrm{Gal}(\tilde{F}/F)$$

and we call $\tilde{F}$ the *maximal unramified extension* of F. ▶

Example 3.4.6. We combine example 3.3.4 and example 3.4.5. Since there are no finite étale covers of $\mathbb{Z}$, the maximal unramified extension of $\mathbb{Q}$ is $\tilde{\mathbb{Q}} = \mathbb{Q}$ and we find

$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Z}) = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) = 1.$$

Recall that this is the analogue of $\pi_1(\mathbb{R}^3) = 1$. ▶

CHAPTER 4

The linking number and the Legendre symbol

For a 2-component link $K \cup L \subset S^3$, the linking number $\mathrm{lk}(L, K)$ measures how the two components are tangled up. Taking the linking number mod 2, we have a function that assigns to a 2-component link the value 0 or 1. On this basic level, we can note that for primes p and q the Legendre symbol $(\frac{p}{q}) \in \{-1, 1\}$ does a similar thing. In this chapter we will see that the mod 2 linking number and the Legendre symbol are actually defined analogously.

4.1 *The linking number*

Let K and L form a 2-component link and let $p_\infty : X_\infty \to X_L$ be the infinite cyclic cover of the knot complement X_L. Consider K as a loop in X_L with endpoints $x \in K$. Then the monodromy permutation representation of G_L induces a homomorphism $\rho_\infty : G_L \to \mathrm{Gal}(X_\infty/X_L)$.

Definition 4.1.1. *Let τ be a generator of the Galois group $\mathrm{Gal}(X_\infty/X_L)$. Then $\rho_\infty([K]) = \tau^n$ for some $n \in \mathbb{Z}$. We define $\mathrm{lk}(L, K) := n$ and we call this the* linking number *of K and L. We define the* mod 2 linking number $\mathrm{lk}_2(L, K) \in \mathbb{F}_2$ *by $\mathrm{lk}(L, K) \equiv \mathrm{lk}_2(L, K) \bmod 2$. The sign of $\mathrm{lk}(L, K)$ depends on the choice of τ and the orientation of K as a loop in X_L.*

There are many ways to define the linking number [Rol03, Chap. 5, Sect. D]. The linking number is known to be symmetric, i.e., we have $\mathrm{lk}(L, K) = \mathrm{lk}(K, L)$ [Rol03, Chap. 5, Sect. D, Theorem 6]. For a particularly intuitive definition of the linking number that showcases its symmetry, see [Ada05, p. 18]. We now turn to the following characterization of the mod 2 linking number.

Proposition 4.1.2. *Let $\bar{\tau}$ be a generator of the Galois group $\mathrm{Gal}(X_2/X_L)$ and let $\rho_2 : G_L \to \mathrm{Gal}(X_2/X_L)$ be the map induced by the monodromy permutation representation. We have*

$$\rho_2([K]) = \bar{\tau}^{\mathrm{lk}_2(L,K)}.$$

Proof. Note that $p_2 : X_2 \to X_L$ is a subcover of $p_\infty : X_\infty \to X_L$, so by theorem 2.2.9, we know that $(p_\infty)_*(\pi_1(X_\infty)) \subseteq (p_2)_*(\pi_1(X_2))$. Also note that ρ_2 is the composite

$$G_L \xrightarrow{q_2} G_L/(p_2)_*(\pi_1(X_2)) \xrightarrow{\sim} \mathrm{Gal}(X_2/X_L),$$

where the second map is the isomorphism from theorem 2.2.9 and where q_2 is the natural quotient map. Likewise, we have

$$G_L \xrightarrow{q_\infty} G_L/(p_\infty)_*(\pi_1(X_\infty)) \xrightarrow{\sim} \mathrm{Gal}(X_\infty/X_L).$$

Then the quotient map $G_L/(p_\infty)_*(\pi_1(X_\infty)) \to G_L/(p_2)_*(\pi_1(X_2))$ induces a commutative diagram

$$\begin{array}{ccc} G_L & \xrightarrow{\rho_2} & \mathrm{Gal}(X_2/X_L) \\ {\scriptstyle \rho_\infty}\downarrow & \nearrow_{r} & \\ \mathrm{Gal}(X_\infty/X_L) & & \end{array},$$

where r sends a generator $\tau \in \mathrm{Gal}(X_\infty/X_L)$ to the generator $\bar{\tau} \in \mathrm{Gal}(X_2/X_L)$. We now have

$$\rho_2([K]) = r(\rho_\infty([K])) = r(\tau^{\mathrm{lk}(L,K)}) = \bar{\tau}^{\mathrm{lk}(L,K)} = \bar{\tau}^{\mathrm{lk}_2(L,K)}.$$

□

Example 4.1.3. We are going to compute the linking number of the Hopf link to prove that it is, in fact, linked. Let $K \cup L$ be the Hopf link in S^3 comprised of two unknots K and L and let S be the Seifert surface of K. In other words, S is a disk with boundary K. We consider L as a loop in the knot complement X_K with endpoints x. This is pictured in figure 4.1.

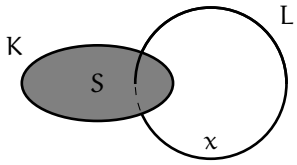


Fig. 4.1: Hopf link $K \cup L$, with Seifert surface S of K.

We construct the infinite cyclic cover of X_K as we did in example 2.2.14. For every $i \in \mathbb{Z}$, let Y_i be a copy of X_K and cut it open along S. In every Y_i we obtain two disks S_i^+ and S_i^- homeomorphic to S. For every i, we identify S_i^+ with S_{i+1}^-. Then $X_\infty := \bigcup_{i\in\mathbb{Z}} Y_i$ is the infinite cyclic cover of X_K with covering map $p_\infty : X_\infty \to X_K$. Its Galois group $\mathrm{Gal}(X_\infty/X_K)$ is generated by the deck transformation $\tau : X_\infty \to X_\infty$ defined by $\tau(Y_i) = Y_{i+1}$. Let $p^{-1}(x) = \bigcup_{i\in\mathbb{Z}}\{y_i\}$, where $y_i \in Y_i$. Figure 4.2 shows X_∞ with the lift $\tilde{L}$ of L in X_∞ with starting point y_0. Here $Y_i \overset{S}{\leftrightarrow} Y_{i+1}$ indicates that S_i^+ is identified with S_{i+1}^-.

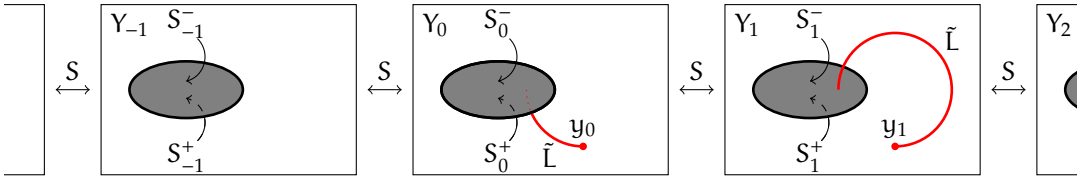


Fig. 4.2: The infinite cyclic cover X_∞ of X_K with the lift $\tilde{L}$ of L.

Since the endpoint of $\tilde{L}$ is y_1, we see that $\rho_\infty([L]) = \tau$ and we get $\mathrm{lk}(K, L) = 1$. Note how the linking number depends on our choice of τ and the orientation (clockwise or counterclockwise) on L. ▶

Example 4.1.4. Although unlinked knots have linking number zero, the converse is not necessarily true. This example serves to illustrate that. Let K and L be two unknots that are linked together as in figure 4.3. This link is called the *Whitehead link*.

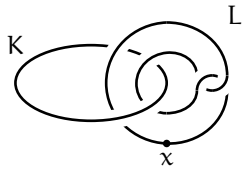


Fig. 4.3: Whitehead link.

We construct the infinite cyclic cover X_∞ of X_K as in the previous example, using a Seifert surface S of K to cut open copies of S^3. Let $\tau \in \mathrm{Gal}(X_\infty/X_K)$ again be the element that sends every Y_i to Y_{i+1} and let $\tilde{L}$ once again be the lift of the loop L. The result is pictured in figure 4.4.

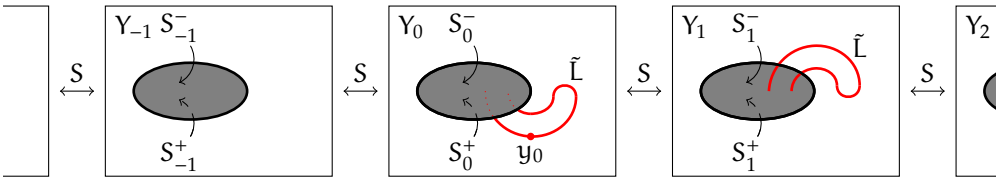


Fig. 4.4: The infinite cyclic cover X_∞ of X_K with the lift $\tilde{L}$ of L.

We see that the endpoint of $\tilde{K}$ is the same as its starting point y_0, so $\rho_\infty([K]) = \mathrm{id}_{X_\infty}$ and we find $\mathrm{lk}(K, L) = 0$, even though the Whitehead link can't be untangled. ▶

The following corollary describes the connection between the mod 2 linking number and the decomposition of a knot in X_2.

Corollary 4.1.5. *Let* K *and* L *form a 2-component link with double cover* $p_2 : X_2 \to X_L$. *If* $\mathrm{lk}_2(L, K) = 0$, *there exist knots* $K_1, K_2 \subseteq X_2$ *such that* $p_2^{-1}(K) = K_1 \cup K_2$ *and if* $\mathrm{lk}_2(L, K) = 1$ *there exists a knot* $\mathfrak{K} \subseteq X_2$ *such that* $p_2^{-1}(K) = \mathfrak{K}$. *In other words, we have:*

$$p_2^{-1}(K) = \begin{cases} K_1 \cup K_2 & \text{if } \mathrm{lk}_2(L, K) = 0 \\ \mathfrak{K} & \text{if } \mathrm{lk}_2(L, K) = 1. \end{cases}$$

Proof. Let $x \in K$ and let $p_2^{-1}(x) = \{y_1, y_2\}$. For a loop γ in X_L, let $\tilde{\gamma}_{y_i} : [0, 1] \to X_2$ be the lift of γ in X_2 with starting point $\tilde{\gamma}_{y_i}(0) = y_i$. Since $\rho_2 : G_L \to \mathrm{Gal}(X_2/X_L)$ is induced by the monodromy permutation representation, we have $\rho_2([\gamma])(y_i) := \tilde{\gamma}_{y_i}(1)$.

Note that if $\tilde{K}_{y_1}(1) = y_1$, then $\tilde{K}_{y_1}(0) = \tilde{K}_{y_1}(1)$ and $\tilde{K}_{y_1}$ is actually a knot in X_2. Then the same holds for $\tilde{K}_{y_2}$ and we have $p_2^{-1}(K) = K_1 \cup K_2$, where $K_i := \tilde{K}_{y_i}$ and K decomposes into a 2-component link in X_2. Conversely, if K decomposes into two knots $K_1 \ni y_1$ and $K_2 \ni y_2$ in X_2, then $K_1 = \tilde{K}_{y_1}$ and $K_2 = \tilde{K}_{y_2}$ by definition and we have $\tilde{K}_{y_1}(1) = y_1$.

If, however, we have $\tilde{K}_{y_1}(1) = y_2$, then $\tilde{K}_{y_2}(1) = y_1$ and $\tilde{K}_{y_1}$ and $\tilde{K}_{y_2}$ together actually form a knot in X_2, which we denote by $\mathfrak{K}$. Then we have $p_2^{-1}(K) = \mathfrak{K}$. Conversely, suppose $p_2^{-1}(K)$ is a knot in X_2. Note that by the previous paragraph, we have $\tilde{K}_{y_1}(1) = y_1 \Rightarrow p_2^{-1}(K) = K_1 \cup K_2$ for

some knots K_1 and K_2 in X_2. Since $p_2^{-1}(K) \neq K_1 \cup K_2$ for any two disjoint knots K_1 and K_2 in X_2, we find $\tilde{K}_{y_1}(1) \neq y_1$, i.e., $\tilde{K}_{y_1}(1) = \tilde{K}_{y_1}(1) = y_2$.

Using proposition 4.1.2, we get the following equivalences:

$$\begin{aligned}
lk_2(L,K) = 0 &\iff \rho_2([K]) = id_{X_2} \iff \rho_2([K])(y_1) = y_1 \iff \tilde{K}_{y_1}(1) = y_1 \\
&\iff p_2^{-1}(K) = K_1 \cup K_2, \\
lk_2(L,K) = 1 &\iff \rho_2([K]) = \bar{\tau} \iff \rho_2([K])(y_1) = y_2 \iff \tilde{K}_{y_1}(1) = y_2 \\
&\iff p_2^{-1}(K) = \mathfrak{K},
\end{aligned}$$

which is what we wanted to prove. □

Example 4.1.6. We continue the example of the Hopf link and the Whitehead link. Let's start with the Hopf link $K \cup L$. According to corollary 4.1.5, since the mod 2 linking number of the Hopf link is 1, we should have $p^{-1}(L) = \mathfrak{L}$ for some knot $\mathfrak{L} \subseteq X_2$. In figure 4.5 we can see the double cover X_2 of X_K consisting of two copies Y_0 and Y_1 of S^3 cut open along S where we identify S_0^+ with S_1^- and where we identify S_1^+ with S_0^-.

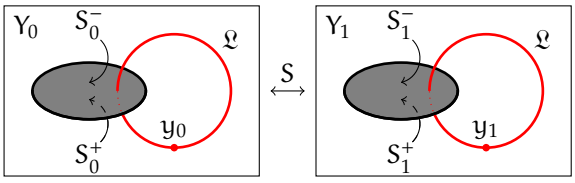


Fig. 4.5: The double cover X_2 of X_K with the knot $\mathfrak{L}$ over L.

Now let K and L denote the components of the Whitehead link. Since $lk_2(K,L) = 0$, we have $p^{-1}(L) = L_1 \cup L_2$ for two knots L_1 and L_2 in X_2. This is shown in figure 4.6. ▶

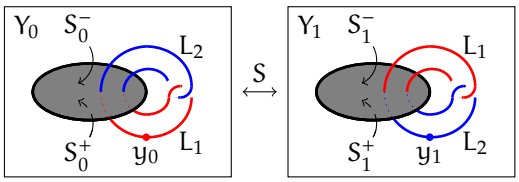


Fig. 4.6: The double cover X_2 of X_K with the knots L_1 and L_2 over L.

4.2 *The mod 2 linking number for primes*

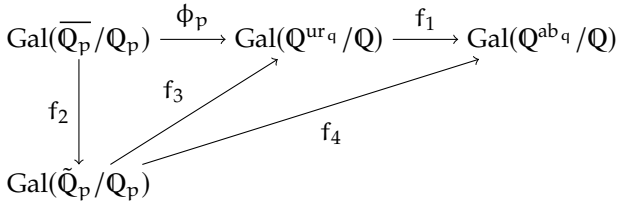
For knots we just saw how the linking number $lk(K,L)$ gave us information about the decomposition of the knot K in the double cover $X_2 \to X_L$. We will now do the same thing for primes. In order to define the mod 2 linking number for primes, we need to define the double cover X_2 of $X_{\{q\}}$, then associate p to an element $\sigma_p \in G_{\{q\}}$ and finally we have to define a map $\rho_2 : G_{\{q\}} \to \mathrm{Gal}(X_2/X_{\{q\}})$.

Let p and q be odd primes and define $X_{\{q\}} := \operatorname{Spec}\mathbb{Z} \setminus \{q\} = \operatorname{Spec}\mathbb{Z}[\frac{1}{q}]$ as an analogue of the knot complement. To find a double étale cover of $X_{\{q\}}$ we need an extension of $\mathbb{Z}$ that's only ramified over q. Since q is ramified in the ring of integers O_k of a field extension $k/\mathbb{Q}$ if and only if q divides the discriminant of k [Neu99, Chap. III, Corollary 2.12], we want a field extension of $\mathbb{Q}$ with discriminant a power of q. Such a field extension is given by $\mathbb{Q}(\sqrt{q^*})$, where $q^* := (-1)^{(q-1)/2}q$. We define q^* this way to ensure $q^* \equiv 1 \bmod 4$, since the discriminant of $\mathbb{Q}(\sqrt{q})$ is equal to $4q$ if $q \equiv 3 \bmod 4$, which would mean that 2 also ramifies in $O_{\mathbb{Q}(\sqrt{q})}$. However, the discriminant of $\mathbb{Q}(\sqrt{q^*})$ is q. Now, for extensions of the form $\mathbb{Q}(\sqrt{d})$ with d squarefree and $d \equiv 1 \bmod 4$ we have $O_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[(1+\sqrt{d})/2]$, so we have $O_{\mathbb{Q}(\sqrt{q^*})} = \mathbb{Z}[(1+\sqrt{q^*})/2]$. Set $X_2 := \operatorname{Spec}\mathbb{Z}[\frac{1}{q}, (1+\sqrt{q})/2]$. The double étale cover of $X_{\{q\}}$ is therefore the map

$$h_2 : \qquad X_2 \longrightarrow X_{\{q\}}$$

induced by the embedding $\mathbb{Z}[\frac{1}{q}] \longrightarrow \mathbb{Z}[\frac{1}{q}, (1+\sqrt{q})/2]$.

In the knot case, we viewed a knot K as an element of $\pi_1(X_L)$. We now want to perform the arithmetic analogue, i.e., we want p to induce an element $\sigma_p \in G_{\{q\}}$. We have $G_{\{q\}} = \operatorname{Gal}(\mathbb{Q}^{\mathrm{ur}_q}/\mathbb{Q})$, where $\mathbb{Q}^{\mathrm{ur}_q}$ is the maximal Galois extension of $\mathbb{Q}$ unramified outside q. The problem is that we have next to no insight into the structure of $\mathbb{Q}^{\mathrm{ur}_q}$. We are going to solve this problem by embedding $\mathbb{Q}^{\mathrm{ur}_q}$ into a field we know a little more of. Namely, we take an embedding $\mathbb{Q}^{\mathrm{ur}_q} \subseteq \overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}_p}$ of $\mathbb{Q}^{\mathrm{ur}_q}$ into the algebraic closure of $\mathbb{Q}_p$, where $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ is induced by the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. This induces a homomorphism $\phi_p : \operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \operatorname{Gal}(\mathbb{Q}^{\mathrm{ur}_q}/\mathbb{Q})$. Define $\tilde{\mathbb{Q}}_p := \mathbb{Q}_p(\zeta_n \mid \gcd(n,p) = 1)$, which is the maximal unramified extension of $\mathbb{Q}_p$. Since p is unramified in $\mathbb{Q}^{\mathrm{ur}_q}$, the homomorphism ϕ_p factors through $\operatorname{Gal}(\tilde{\mathbb{Q}}_p/\mathbb{Q}_p)$ [Mor12, Example 2.40]. Note that $\mathbb{Q}^{\mathrm{ab}_q} \subseteq \tilde{\mathbb{Q}}_p$, where $\mathbb{Q}^{\mathrm{ab}_q} := \mathbb{Q}(\zeta_{q^\infty})$ is the maximal Abelian extension of $\mathbb{Q}$ unramified outside of q. Also note that since every $g \in \operatorname{Gal}(\tilde{\mathbb{Q}}_p/\mathbb{Q}_p)$ can be extended to an automorphism $g \in \operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, the map $\operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \operatorname{Gal}(\tilde{\mathbb{Q}}_p/\mathbb{Q}_p)$ is surjective. Therefore, the diagram



commutes. Let $\tilde{\sigma} \in \operatorname{Gal}(\tilde{\mathbb{Q}}_p/\mathbb{Q}_p)$ be the Frobenius element that is defined by $\zeta_n \mapsto \zeta_n^p$ for all n coprime with p. Let $\bar{\sigma} \in \operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ be the extension of $\tilde{\sigma}$ to $\overline{\mathbb{Q}_p}$, i.e., we have $f_2(\bar{\sigma}) = \tilde{\sigma}$. A logical choice for the element $\sigma_p \in \operatorname{Gal}(\mathbb{Q}^{\mathrm{ur}_q}/\mathbb{Q}) = G_{\{q\}}$ is the image $\phi_p(\bar{\sigma})$. We call σ_p the *Frobenius automorphism over* p. Since we have field extensions $\mathbb{Q}^{\mathrm{ab}_q} = \mathbb{Q}(\zeta_{q^n} \mid n \in \mathbb{N}) \subseteq \mathbb{Q}_p(\zeta_n \mid \gcd(n,p) = 1) = \tilde{\mathbb{Q}}_p$, we find that

$$f_1(\sigma_p) = (f_1 \circ \phi_p)(\bar{\sigma}) = (f_4 \circ f_2)(\sigma) = f_4(\tilde{\sigma})$$

is the Frobenius automorphism on $\mathbb{Q}^{\mathrm{ab}_q}$ which sends ζ_{q^n} to $\zeta_{q^n}^p$ for all n. We set $\sigma_p^{\mathrm{ab}} := f_1(\sigma_p)$.

Now that we have defined σ_p, it's time to define our map $\rho_2 : G_{\{q\}} \to \operatorname{Gal}(X_2/X_{\{q\}})$. Note that $\operatorname{Gal}(X_2/X_{\{q\}}) = \operatorname{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$. It is known that $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q)$ [Wei06, Theorem 4.5.1], so we get field extensions $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(\zeta_{q^\infty}) \subseteq \mathbb{Q}^{\mathrm{ur}_q}$ which means that the natural map

$$\rho_2 : \qquad G_{\{q\}} \longrightarrow \operatorname{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$$

sends σ_p to the restriction of $\sigma_p^{ab} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q^\infty})/\mathbb{Q})$ to $\mathbb{Q}(\sqrt{q^*})$.

Definition 4.2.1. *Let τ be the generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{q^*})$. Then $\rho_2(\sigma_p) = \tau^n$ for some $n \in \mathbb{Z}/2\mathbb{Z}$. We define $\mathrm{lk}_2(q,p) := n$ and we call this the* mod 2 linking number *of p and q.*

Let's refresh our memory a bit regarding the Legendre symbol.

Definition 4.2.2. *Let n be an odd prime and let k be an integer such that n and k are coprime. The* Legendre symbol *or* quadratic residue symbol $(\frac{k}{n})$ *is defined*

$$\left(\frac{k}{n}\right) := \begin{cases} 1 & \text{if } k \equiv x^2 \bmod n \text{ for some } x \\ -1 & \text{if } k \not\equiv x^2 \bmod n \text{ for all } x. \end{cases}$$

Proposition 4.2.3. *The Legendre symbol has the following properties.*

(1) (quadratic reciprocity) Let m and n be two distinct odd primes. Then

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

(2) Let n be an odd prime and let k and l be integers such that $\gcd(k,n) = 1 = \gcd(l,n)$. The Legendre symbol is multiplicative, i.e., we have

$$\left(\frac{k}{n}\right)\left(\frac{l}{n}\right) = \left(\frac{kl}{n}\right).$$

(3) Let n be an odd prime. Then we have

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

From these properties it follows that we have

$$\left(\frac{q^*}{p}\right)\left(\frac{p}{q^*}\right) = 1 \qquad \text{and} \qquad \left(\frac{q^*}{p}\right)\left(\frac{p}{q}\right) = 1.$$

We are now ready to prove the connection between the mod 2 linking number and the Legendre symbol.

Proposition 4.2.4. *We have*

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

Proof. Define

$$S_q := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \zeta_q^k.$$

We have $S_q = \sqrt{q^*}$ [Wei06, Remark 4.5.6]. Since $\sigma_p^{ab}(\zeta_q) = \zeta_q^p$, we have

$$\begin{aligned}\rho_2(\sigma_p)(\sqrt{q^*}) = \sigma_p^{ab}|_{\mathbb{Q}(\sqrt{q^*})}(\sqrt{q^*}) = \sigma_p^{ab}(S_q) &= \sum_{k=1}^{q-1}\left(\frac{k}{q}\right)\zeta_q^{kp} \\ &= \left(\frac{q^*}{p}\right)\left(\frac{p}{q}\right)\sum_{k=1}^{q-1}\left(\frac{k}{q}\right)\zeta_q^{kp} = \left(\frac{q^*}{p}\right)\sum_{k=1}^{q-1}\left(\frac{kp}{q}\right)\zeta_q^{kp} = \left(\frac{q^*}{p}\right)S_p \\ &= \left(\frac{q^*}{p}\right)\sqrt{q^*},\end{aligned}$$

from which we get

$$\left(\frac{q^*}{p}\right) = -1 \iff \rho_2(\sigma_p) = \tau^1 \iff \mathrm{lk}_2(q,p) = 1.$$

It follows that $(\frac{q^*}{p}) = (-1)^{\mathrm{lk}_2(q,p)}$. □

From proposition 4.2.4, we can deduce that $\mathrm{lk}_2(q,p) = \mathrm{lk}_2(p,q)$. The following corollary describes the connection between the mod 2 linking number and the decomposition of a prime in X_2.

Corollary 4.2.5. *Let p and q be odd primes and define $h_2 : X_2 \to X_{\{q\}}$ as above. We have:*

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

Proof. We have an isomorphism of quotient rings $\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}/p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} \cong \mathbb{F}_p[X]/(X^2 - X - q^*) \cong \mathbb{F}_p[X]/(X^2 - q^*)$. Since p is not ramified in $\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}$, we have either $p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} = \mathfrak{p}$ if $p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}$ is prime or $p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} = \mathfrak{p}_1\mathfrak{p}_2$ if $p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}$ splits, where $\mathfrak{p}, \mathfrak{p}_1\mathfrak{p}_2$ are primes in $\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}$. Using proposition 4.2.4, we get the following equivalences:

$$\begin{aligned}\mathrm{lk}_2(q,p) = 0 &\iff \left(\frac{q^*}{p}\right) = 1 &&\iff q^* \equiv x^2 \bmod p \text{ for some } x \\ &\iff \mathbb{F}_p[X]/(X^2 - q^*) \text{ is not a domain} &&\iff \mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}/p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} \text{ is not a domain} \\ &\iff p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} \text{ is not prime} \\ \mathrm{lk}_2(q,p) = 1 &\iff \left(\frac{q^*}{p}\right) = -1 &&\iff q^* \not\equiv x^2 \bmod p \text{ for all } x \\ &\iff \mathbb{F}_p[X]/(X^2 - q^*) \text{ is a domain} &&\iff \mathcal{O}_{\mathbb{Q}(\sqrt{q^*})}/p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} \text{ is a domain} \\ &\iff p\mathcal{O}_{\mathbb{Q}(\sqrt{q^*})} \text{ is prime,}\end{aligned}$$

from which the claim follows. □

CHAPTER 5

Decomposition of knots and primes

In the preliminaries we defined topological covers $M \to S^3$ ramified over a knot and finite covers $\operatorname{Spec} B \to \operatorname{Spec} A$ ramified over a prime. In this chapter we will examine the decomposition of knots and primes through coverings.

5.1 *Decomposition of knots*

Let $p : M \to S^3$ be a finite Galois covering ramified over a link $L \subseteq S^3$, where M is a connected oriented closed 3-manifold. Defining $X := S^3 \setminus L$ and $Y := M \setminus p^{-1}(L)$ gives us the unramified finite cover $p|_Y : Y \to X$ with Galois group $G := \operatorname{Gal}(M/S^3)$ of maps $g : M \to S^3$ that restrict to deck transformations $g|_Y : Y \to X$. Set $n := \#G$. Let $K \subseteq S^3$ be a knot that is either a component of L or disjoint from L. Suppose $p^{-1}(K)$ is an r-component link (if K is disjoint from L, this holds automatically as a consequence of theorem 2.2.4), so take $p^{-1}(K) = K_1 \sqcup \ldots \sqcup K_r$ and let $S_K := \{K_1, \ldots, K_r\}$ be the set of knots lying over K. We have the following lemma.

Lemma 5.1.1. *The elements of* G*, when restricted to* $p^{-1}(K)$*, define a transitive* G*-action on* S_K*.*

Proof. Denote with V_K a tubular neighborhood of K and let V_{K_i} be the connected component of $p^{-1}(V_K)$ containing K_i. Let $x \in \partial V_K$ and let $p^{-1}(x) = \{y_1, \ldots, y_n\}$. Let $\rho : \pi_1(X) \to \operatorname{Aut}(p^{-1}(x))$ be the monodromy permutation representation. We have $\pi_1(X)/p_*(\pi_1(Y)) \cong G$, so since $\pi_1(X)$ acts transitively on $p^{-1}(x)$, we know that G acts transitively on $p^{-1}(x)$ and therefore on S_K as well. □

Definition 5.1.2. *Let* G*,* S_K*,* $p : Y \to X$ *and* $K_1, \ldots, K_r$ *be as above.*

1) *The* decomposition group of K_i*, denoted with* D_{K_i}*, is the stabilizer of* $K_i \in S_K$ *under the action of* G*:*
$$D_{K_i} := \{g \in G \mid g(K_i) = K_i\}.$$

2) *The* inertia group of K_i*, denoted with* I_{K_i}*, is the subgroup of* D_{K_i} *consisting of all elements that are the identity on* K_i*:*
$$I_{K_i} := \{g \in D_{K_i} \mid g|_{K_i} = \mathrm{id}_{K_i}\}.$$

3) *Let* $Z \to X$ *be the subcovering of* $Y \to X$ *such that* $\mathrm{Gal}(Y/Z) \cong D_{K_i}$. *Then the* decomposition (covering) space of K_i, *denoted with* Z_{K_i}, *is the Fox completion (cf. example 2.2.16) of* Z.

4) *Let* $Z \to X$ *be the subcovering of* $Y \to X$ *such that* $\mathrm{Gal}(Y/Z) \cong I_{K_i}$. *Then the* inertia (covering) space of K_i, *denoted with* T_{K_i}, *is the Fox completion (cf. example 2.2.16) of* Z.

Since G acts transitively on S_K, the orbit of any K_i is equal to S_K. Therefore, by the orbit-stabilizer theorem we have $\#(G/D_{K_i}) = \#S_K$, so $\#D_{K_i} = n/r$ is independent of i.

Let V_K be a tubular neighborhood of K and let V_{K_i} be the connected component of $p^{-1}(V_{K_i})$ that contains K_i. Let $x \in \partial V_K$ and let $p^{-1}(x) = \{y_1, \ldots, y_n\}$, with $y_i \in \partial V_{K_i}$ for every i. Every element of g induces a homeomorphism $g|_{\partial V_{K_i}} : \partial V_{K_i} \to \partial V_{g(K_i)}$, so if $g \in D_{K_i}$ we have a deck transformation $g|_{\partial V_{K_i}}$ of ∂V_{K_i} over ∂V_K. This gives a map

$$\phi : \qquad D_{K_i} \longrightarrow \mathrm{Gal}(\partial V_{K_i}/\partial V_K), \qquad g \longmapsto g|_{\partial V_{K_i}}.$$

Proposition 5.1.3. *The map* ϕ *is a group isomorphism.*

Proof. To show that ϕ is injective, let $g \in D_{K_i}$ such that $g|_{\partial V_{K_i}} = \mathrm{id}_{V_{K_i}}$. Then $g(x) = x$. Since $p : Y \to X$ is a Galois covering, the action of G on $p^{-1}(x)$ is regular. Therefore, g can only be the identity, so the kernel of ϕ is trivial. To show that ϕ is surjective, let $g \in \mathrm{Gal}(\partial V_{K_i}/\partial V_K)$ and suppose $g(x) = y$. Let $g' \in G$ such that $g'(x) = y$. Then $g'(\partial V_{K_i}) = \partial V_{K_i}$, so $g' \in D_{K_i}$. Since ∂V_{K_i} is connected, the action of $\mathrm{Gal}(\partial V_{K_i}/\partial V_K)$ on $p^{-1}(x)$ is free. This means that $g'|_{\partial V_{K_i}} = g$, so ϕ is surjective. □

If we restrict a map $g \in D_{K_i}$ to K_i, we get a deck transformation of K_i over K. This gives us a group homomorphism

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

with kernel I_{K_i}. We have the following result.

Lemma 5.1.4. *The homomorphism* $D_{K_i} \to \mathrm{Gal}(K_i/K)$, $g \mapsto g|_{K_i}$ *is surjective, i.e., the sequence*

$$1 \longrightarrow I_{K_i} \longrightarrow D_{K_i} \longrightarrow \mathrm{Gal}(K_i/K) \longrightarrow 1$$

is exact.

Proof. Let $\rho : G_L = \pi_1(X, x) \to \mathrm{Aut}(p^{-1}(x))$ be the monodromy permutation representation. Let α be a meridian of K and β a longitude of K. Set $e := \#I_{K_i}$. For $g \in G$ with $g(K_i) = K_j$, we have $I_{K_j} = gI_{K_i}g^{-1}$, so e is independent of i. Note that e agrees with the ramification index e' of K_i over K: by definition of a ramified covering, $\rho(\alpha^{e'})$ is the identity on $p^{-1}(x)$. Let $\{z_{i_1}, \ldots, z_{i_{e'}}\}$ be the orbit of $z_{i_1} \in p^{-1}(x)$ under $\langle\rho(\alpha)\rangle$. Since every $g \in G$ that fixes the orbit of z_{i_1} is the identity on K_i, we have $I_{K_i} \cong \langle\rho(\alpha)\rangle$, so $e = e'$.

Let $y_i \in \partial V_{K_i}$. Note that every element in $\mathrm{Gal}(\partial V_{K_i}/\partial V_K) \cong D_{K_i}$ is induced by an element of $\pi_1(\partial V_K)$ and that we have $\pi_1(\partial V_K) = \langle[\alpha], [\beta]\rangle$. Since $\rho(\alpha)(y_i) \in \partial V_{K_i}$ and $\rho(\beta)(y_i) \in \partial V_{K_i}$, we find $D_{K_i} \cong \rho(\langle\alpha, \beta\rangle)$. Let $f \in \mathbb{N}$ be minimal such that $\rho(\beta^f)(y_1) = y_1$. Since $\rho(\alpha)$ is the identity on K_i, we find that f is the covering degree of K_i over K. We have $D_{K_i} \cong \rho(\langle\alpha, \beta\rangle) = \{\rho(\alpha^j\beta^k) \mid 0 \le j \le e-1, 0 \le k \le f-1\}$, which gives us $\#D_{K_i} = ef$ and also $\#\mathrm{Gal}(K_i/K) = f$. Then we have

$$\#\mathrm{im}(D_{K_i} \to \mathrm{Gal}(K_i/K)) = \#(D_{K_i}/I_{K_i}) = ef/e = f = \#\mathrm{Gal}(K_i/K),$$

so the map $D_{K_i} \to \mathrm{Gal}(K_i/K)$ is surjective. □

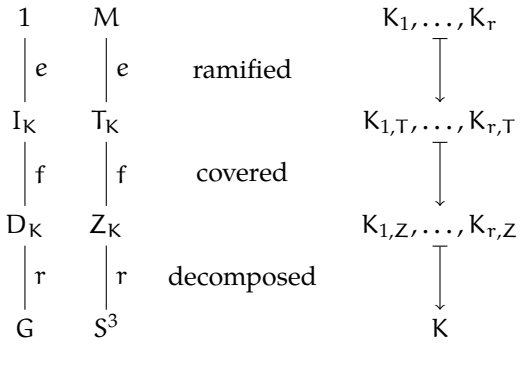
From $n/r = \#D_{K_1} = ef$ we get $efr = n$. Keeping in mind that $D_{K_1} \cong \mathrm{Gal}(M/Z_{K_i})$ and $I_{K_i} \cong \mathrm{Gal}(M/T_{K_i})$, we find

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

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 $T_{K_i} \to Z_{K_i}$. We have the following theorem.

Theorem 5.1.5. *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.*

Suppose the Galois group G of the covering $M \to S^3$ is Abelian. Then, since the decomposition groups D_{K_i} are conjugate, they are independent of K_i. Therefore, we can write D_K. Likewise, we can write I_K for the inertia group and we write Z_K and T_K for the decomposition and inertia spaces, as well. Theorem 5.1.5 then shows how K is decomposed, covered and then ramified through the coverings $M \to T_K$, $T_K \to Z_K$ and $Z_K \to S^3$:



In the covering $p_1 : Z_p \to S^3$, K is completely decomposed, i.e., we have $p_1^{-1}(K) = \bigsqcup_{i=1}^{r} K_{i,Z}$. In the covering $p_2 : T_K \to Z_K$, every $K_{i,Z}$ is covered with degree f, i.e., we have $p_2^{-1}(K_{i,Z}) = K_{i,T}$, but $\#p_2^{-1}(x) = \#\mathrm{Gal}(K_{i,T}/K_{i,Z}) = 2$ for every $x \in K_{i,Z}$. Lastly, in the covering $p_3 : M \to T_K$ we have $p_3^{-1}(K_{i,T}) = K_i$ with ramification index e for all i.

Let's illustrate all this with some examples.

Example 5.1.6. Let's take a look at the Hopf link. We call the components of the Hopf link K and L and we let S be the disk with boundary K. In other words, S is the Seifert surface of K (see also example 4.1.3).

Let $m \in \mathbb{N}$. By cutting S^3 along the surface S, as in example 2.2.14, we can construct the m-fold cover M of S^3 ramified over K. Let $Y_1, \ldots, Y_m$ be m copies of S^3. Note that in each Y_i we obtain surfaces S_i^+ and S_i^-, both homeomorphic to S, by cutting Y_i along S. We get the m-fold cyclic cover M of S^3 ramified over K by taking the union $\sqcup_{i=1}^{m} Y_i$ and identifying S_i^+ with S_{i+1}^- for

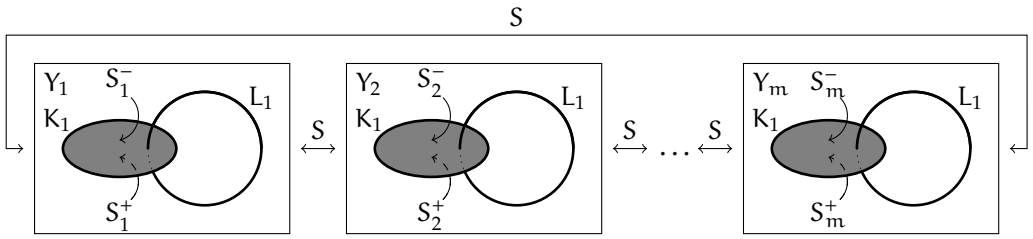


Fig. 5.1: The covering space M of S^3 ramified over K.

every $i \in \mathbb{Z}/m\mathbb{Z}$. The space M is displayed in figure 5.1, where $Y_i \overset{S}{\leftrightarrow} Y_{i+1}$ indicates that S_i^+ is identified with S_{i+1}^-.

Let $p : M \to S^3$ be the covering map. We have $G := \mathrm{Gal}(Y/S^3) = \langle \sigma : Y_i \mapsto Y_{i+1} \rangle \cong \mathbb{Z}/m\mathbb{Z}$. Since L is unramified, its ramification index is $e(L) = 1$ the inertia group I_L is trivial and the inertia space is $T_K = M$. This is clear upon inspection, since σ^i is clearly only the identity on L when $Y_i \mapsto Y_i$, i.e., when $i = 0$. As for the decomposition group, since L decomposes into the single knot L_1, we have $r = 1$ and every element of G fixes L_1. Therefore, we have $D_L = G$ and $Z_L = S^3$. By contrast, the component K is ramified with ramification index $e(K) = n$, so the inertia group is $I_K = G$ and the inertia field is $T_K = S^3$. Furthermore, we have $D_K = G$ and $Z_K = S^3$. It is easy to see this simply by observing figure 5.1. ▶

Example 5.1.7. In all constructions we've seen so far, we either had $I_{K_i} = 1$ or $I_{K_i} = G$. In this example we're going to construct a covering such that $1 \subsetneq I_{K_i} \subsetneq D_{K_i} \subsetneq G$. We're going to add another unknot to the Hopf link. Let S, T and U be their Seifert surfaces, i.e., discs with boundary K, L and M, respectively. See figure 5.2.

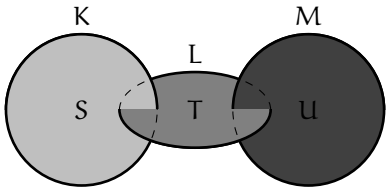


Fig. 5.2: The 3-component link consisting of knots K, L and M, with Seifert surfaces S, T and U.

We're now going to construct a covering space Y ramified over K, L and M by cutting S^3 along all three of their Seifert surfaces S, T and U. As in the previous example, we let Y_1 and Y_2 be copies of S^3, cut open along the Seifert surface S. We obtain surfaces S_1^+ and S_1^- in Y_1 and surfaces S_2^+ and S_2^- in Y_2. By identifying S_1^+ with S_2^- and identifying S_2^+ with S_1^-, we obtain a double cover $(Y_1 \cup Y_2)/\sim$ of S^3 ramified over K.

We can now repeat this process by taking a copy $(Y_3 \cup Y_4)/\sim$ of $(Y_1 \cup Y_2)/\sim$, where $Y_3 \cong Y_1$ and $Y_4 \cong Y_2$. Now we can cut open $(Y_1 \cup Y_2)/\sim$ and $(Y_3 \cup Y_4)/\sim$ along T to obtain surfaces $T_i^+, T_i^- \subseteq Y_i$ for every $1 \le i \le 4$. We identify $T^+_{i \bmod 4}$ with $T^-_{i+2 \bmod 4}$ for $1 \le i \le 4$. We now obtain a cover $(Y_1 \cup Y_2 \cup Y_3 \cup Y_4)/\sim'$ of S^3 ramified over K and L.

We can now do this a third time by taking a copy $(Y_5 \cup Y_6 \cup Y_7 \cup Y_8)/\sim'$, where $Y_i \cong Y_{i-4}$ for $5 \le i \le 8$. Cutting along U will give us surfaces $U_i^+, U_i^- \subseteq Y_i$ for every $1 \le i \le 8$. This time we identify $U^+_{i \bmod 8}$ with $U^-_{i+4 \bmod 8}$ for $1 \le i \le 8$ to obtain a cover $Y := (\bigcup_{1 \le i \le 8} Y_i)/\sim''$ of S^3

ramified over K, L and M. Figure 5.3 shows what Y_1 looks like after it has been cut along S, T and U.

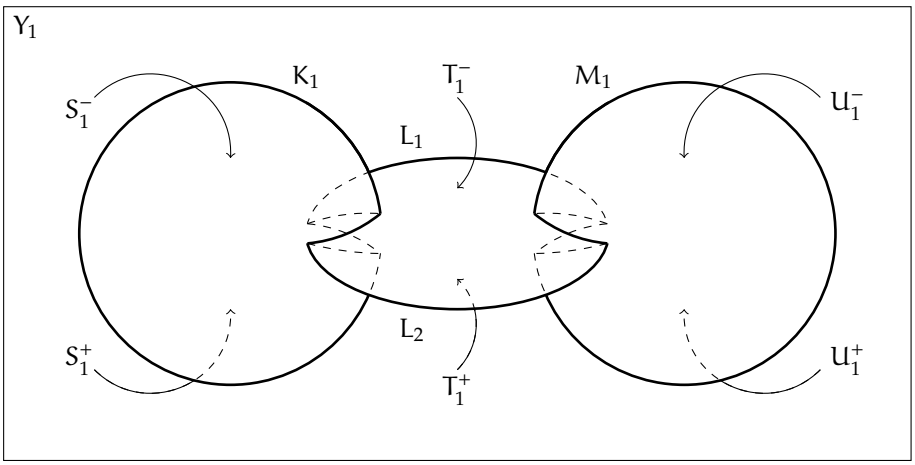


Fig. 5.3: The 3-sphere cut along S, T and U.

Lastly, $p : Y \to S^3$ be the natural covering map. Figure 5.4 shows the space Y with the identifications between the spaces Y_i. Here $Y_i \overset{S}{\longleftrightarrow} Y_j$ indicates that S_i^+ is identified with S_j^- and S_j^+ is identified with S_i^- (likewise for T and U).

One can check that $p : Y \to S^3$ is Galois by the way the Seifert surfaces are identified. It is clear that every element of $G := \mathrm{Gal}(Y/S^3)$ permutes the spaces Y_i. Furthermore, because Y is connected, for every pair $1 \le i, j \le 8$ there is a unique $g \in G$ such that $g(Y_i) = Y_j$. Therefore, we have $\#G = 8$ (in fact, $G \cong (\mathbb{Z}/2\mathbb{Z})^3$).

For $1 \le i \le 8$, let $g_i \in G$ be such that $g_i(Y_1) = Y_i$. We'll be focussing on K_1. Note that since S_1^+ is identified with S_2^- and S_2^+ with S_1^-, we have $p^{-1}(K) \cap Y_1 = p^{-1}(K) \cap Y_2$. Also note that K_1 passes through T_1^+ and T_1^- in Y_1 and through T_2^+ and T_2^- in Y_2. Hence, we have $p^{-1}(K) = \{K_1, K_2\}$ with $K_1 = p^{-1}(K) \cap (Y_1 \cup Y_2 \cup Y_3 \cup Y_4)$ and likewise $K_2 = p^{-1}(K) \cap (Y_5 \cup Y_6 \cup Y_7 \cup Y_8)$. Therefore, the elements of G that map K_1 onto itself are g_1, g_2, g_3 and g_4, so $D_K = \{g_1, g_2, g_3, g_4\}$. We have $Z_K = Y_1 \cup Y_5 \subseteq M$ with the natural covering map $Y' \to Z_K$ that sends Y_1, Y_2, Y_3 and Y_4 to Y_1 and that sends Y_5, Y_6, Y_7 and Y_8 to Y_5. Note that g_2 transposes Y_1 and Y_2 as well as Y_3 and Y_4. Since S_1^+ is identified with S_2^- and S_2^+ is identified with S_1^- (likewise for S_3^+, S_4^-, S_4^+ and S_3^-), we can see that g_2 is actually the identity on K_1. Therefore, we have $I_K = \{g_1, g_2\}$ and therefore $1 \subsetneq I_{K_1} \subsetneq D_{K_1} \subsetneq G$, as was our goal. The inertia space is $T_K = Y_1 \cup Y_3 \cup Y_5 \cup Y_7$ with the covering map $Y' \to T_K$ that sends Y_i to $Y_{\lceil i/2 \rceil}$ for every i. The knot K is decomposed, covered and ramified as follows:

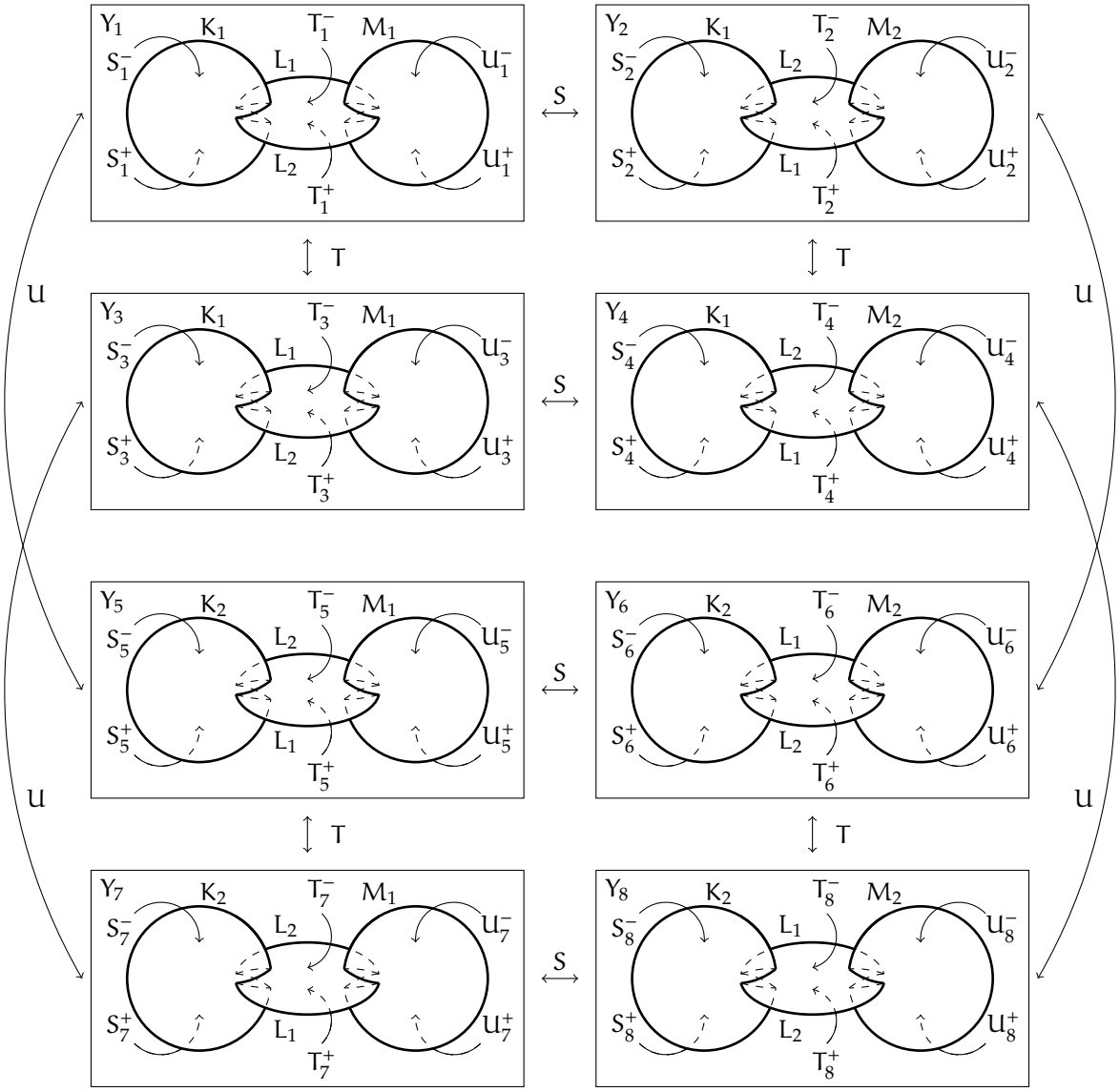


Fig. 5.4: The covering space Y of S^3 ramified over K, L and M.

$$Y = \bigcup_{i=1}^{8} Y_i \quad \overset{2}{\supseteq} \quad T_K = Y_1 \cup Y_3 \cup Y_5 \cup Y_7 \quad \overset{2}{\supseteq} \quad Z_K = Y_1 \cup Y_5 \quad \overset{2}{\supseteq} \quad S^3,$$

$$K_1 = p^{-1}(K) \cap \bigcup_{i=1}^{4} Y_i \quad \supseteq \quad K_{1,T} = K_1 \cap (Y_1 \cup Y_3) \quad \supseteq \quad K_{1,Z} = K_1 \cap Y_1 \quad \supseteq \quad K,$$

$$K_2 = p^{-1}(K) \cap \bigcup_{i=5}^{8} Y_i \quad \supseteq \quad K_{2,T} = K_2 \cap (Y_5 \cup Y_7) \quad \supseteq \quad K_{2,Z} = K_1 \cap Y_5 \quad \supseteq \quad K.$$

Here $\overset{2}{\subseteq}$ indicates that the covering degree is 2. As per theorem 5.1.5, we see that the preimage of K in Z_K is $K_{1,Z} \cup K_{2,Z}$, the preimage of $K_{i,Z}$ in T_K is $K_{i,T}$ with $\mathrm{Gal}(K_{i,T}/K_{i,Z}) \cong \mathbb{Z}/2\mathbb{Z}$ and the preimage of $K_{i,T}$ in Y is K_i with ramification index 2. ▶

5.2 *Decomposition of primes*

Let $k/\mathbb{Q}$ be a finite Galois extension such that the extension $\mathbb{Z} \subseteq \mathcal{O}_k$ is ramified over a set of primes $S \subseteq \operatorname{Spec}\mathbb{Z}$. Then let $h : \operatorname{Spec}\mathcal{O}_k \to \operatorname{Spec}\mathbb{Z}$ be the ramified covering induced by the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_k$. If we take $X := \operatorname{Spec}\mathbb{Z} \setminus S$ and $Y := \operatorname{Spec}\mathcal{O}_k \setminus h^{-1}(S)$, we get a finite étale covering $p : Y \to X$. Let $G := \mathrm{Gal}(Y/X) := \mathrm{Gal}(k/\mathbb{Q})$ and set $n := \#G$. Let $p \in \operatorname{Spec}\mathbb{Z}$ and let $S_p := h^{-1}(p) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ be the set of primes lying over p. We have the following lemma.

Lemma 5.2.1. *The elements of* G*, when restricted to* $h^{-1}(p)$*, define a transitive* G*-action on* S_p*.*

Proof. Suppose there is $i \neq j$ such that for every $\sigma \in G$ we have $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$. Since $\mathfrak{p}_j$ is not contained in $\sigma(\mathfrak{p}_i)$ for any $\sigma \in G$, there exists $x \in \mathfrak{p}_j$ such that $x \notin \sigma(\mathfrak{p}_i)$ for any $\sigma \in G$ (this is a result of the *prime avoidance lemma* [Eis04, Lemma 3.3]). Using the field norm of x, defined as $N_{k/\mathbb{Q}}(x) := \prod_{\sigma\in G} \sigma(x)$, we notice that $\mathrm{id}_k(x) = x$, so $N_{k/\mathbb{Q}}(x) \in \mathfrak{p}_j$. We also have $\sigma(x) \notin \mathfrak{p}_i$ for any $\sigma \in G$, so $N_{k/\mathbb{Q}}(x) \notin \mathfrak{p}_i$. However, we have $N_{k/\mathbb{Q}} \in \mathbb{Z}$, so

$$N_{k/\mathbb{Q}}(x) \in \mathfrak{p}_j \cap \mathbb{Z} = p = \mathfrak{p}_i \cap \mathbb{Z},$$

which gives a contradiction. □

We now define the arithmetic analogues to definition 5.1.2.

Definition 5.2.2. *Let* G*,* S_p*,* $h : Y \to X$ *and* $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ *be as above.*

1) *The* decomposition group of $\mathfrak{p}_i$*, denoted with* $D_{\mathfrak{p}_i}$*, is the stabilizer of* $\mathfrak{p}_i \in S_p$ *under the action of* G*:*

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

2) *Any map* $g \in D_{\mathfrak{p}_i}$ *induces an isomorphism* $\bar{g} : \mathbb{F}_{\mathfrak{p}_i} \to \mathbb{F}_{\mathfrak{p}_i}$ *that is the identity on* $\mathbb{F}_p$*, where* $\mathbb{F}_{\mathfrak{p}_i} := \mathcal{O}_k/\mathfrak{p}_i$*. This gives a map* $D_{\mathfrak{p}_i} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p)$*,* $g \mapsto \bar{g}$*. The* inertia group of $\mathfrak{p}_i$*, denoted with* $I_{\mathfrak{p}_i}$*, is the kernel of this map:*

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

3) *Let* $Z_{\mathfrak{p}_i}$ *be the subfield of* k *such that* $\mathrm{Gal}(k/Z_{\mathfrak{p}_i}) \cong D_{\mathfrak{p}_i}$*. We call* $Z_{\mathfrak{p}_i}$ *the* decomposition field of $\mathfrak{p}_i$*.*

4) *Let* $T_{\mathfrak{p}_i}$ *be the subfield of* k *such that* $\mathrm{Gal}(k/T_{\mathfrak{p}_i}) \cong I_{\mathfrak{p}_i}$*. We call* $T_{\mathfrak{p}_i}$ *the* inertia field of $\mathfrak{p}_i$*.*

Since G acts transitively on S_p, the orbit of any $\mathfrak{p}_i$ is equal to S_p. Therefore, we have an equivalence $G/D_{\mathfrak{p}_i} \cong G \cdot \mathfrak{p}_i = S_p$, so $\#D_{\mathfrak{p}_i} = n/r$ is independent of i. Also, for $g \in G$ with $g(\mathfrak{p}_i) = \mathfrak{p}_j$, we have $I_{\mathfrak{p}_j} = gI_{\mathfrak{p}_i}g^{-1}$, so $\#I_{\mathfrak{p}_i}$ is independent of i. We set $e := \#I_{\mathfrak{p}_i}$.

Recall that $I_{\mathfrak{p}_i}$ is defined as the kernel of the map $D_{\mathfrak{p}_i} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p)$ that sends an element $g \in D_{\mathfrak{p}_i}$ to $\bar{g}$, defined by $\bar{g}(x \bmod \mathfrak{p}_i) = g(x) \bmod \mathfrak{p}_i$. Analogous to lemma 5.1.4 for the knot case, we have the following result.

Lemma 5.2.3. *The homomorphism* $D_{\mathfrak{p}_i} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_\mathfrak{p})$, $g \mapsto \bar{g}$ *is surjective, i.e., the sequence*

$$1 \longrightarrow I_{\mathfrak{p}_i} \longrightarrow D_{\mathfrak{p}_i} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_\mathfrak{p}) \longrightarrow 1$$

is exact.

Proof. The ring of integers $\mathcal{O}_k$ is a number ring, so all non-zero primes in $\mathcal{O}_k$ are maximal. So $\mathbb{F}_{\mathfrak{p}_i} = \mathcal{O}_k/\mathfrak{p}_i$ is a finite field. Therefore, $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_\mathfrak{p})$ is generated by the Frobenius automorphism σ. Therefore, all we have to prove is that there is some $g \in D_{\mathfrak{p}_i}$ such that $\bar{g} = \sigma$.

Since $\mathbb{F}_{\mathfrak{p}_i}$ is a finite field, it is a simple extension of the field $\mathbb{F}_\mathfrak{p}$. Let $\theta \in \mathcal{O}_k$ be such that $\mathbb{F}_{\mathfrak{p}_i} = \mathbb{F}_\mathfrak{p}(\bar{\theta})$, where $\theta \equiv \bar{\theta} \bmod \mathfrak{p}_i$. We know that all $\mathfrak{p}_i$ are distinct maximal ideals, so they are pairwise coprime. Since $\bigcap_{i=1}^r \mathfrak{p}_i = (p)$, we can apply the Chinese remainder theorem to get an isomorphism

$$\mathcal{O}_k/(p) \cong \mathcal{O}_k/\mathfrak{p}_1 \times \ldots \times \mathcal{O}_k/\mathfrak{p}_r = \mathbb{F}_{\mathfrak{p}_1} \times \ldots \times \mathbb{F}_{\mathfrak{p}_r}.$$

Now let $\alpha \in \mathcal{O}_k$ be such that $\alpha \equiv \bar{\theta} \bmod \mathfrak{p}_i$ and $\alpha \equiv 0 \bmod \mathfrak{p}_j$ for $j \neq i$, i.e., $\alpha \in \mathfrak{p}_j$ for all $j \neq i$. Now consider the characteristic polynomial

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

of α. Note that G acts transitively on $S_\mathfrak{p}$. Then, for any element $g \in G \setminus D_{\mathfrak{p}_i}$, there exists some $j \neq i$ such that $g(\mathfrak{p}_j) = \mathfrak{p}_i$. Since $\alpha \in \mathfrak{p}_j$, this gives $g(\alpha) \in \mathfrak{p}_i$ for all $g \notin D_{\mathfrak{p}_i}$. If we take $f(X) \equiv \bar{f}(X) \bmod \mathfrak{p}_i$, then we get

$$\mathbb{F}_{\mathfrak{p}_i} \ni \bar{f}(X) = X^{\#G \setminus D_{\mathfrak{p}_i}} \cdot \bar{h}(X), \qquad h(X) := \prod_{g \in D_{\mathfrak{p}_i}} (X - g(\alpha)).$$

Let $\alpha \equiv \bar{\alpha} \bmod \mathfrak{p}_i$ and note that we have $\bar{\alpha} = \bar{\theta}$. This gives $0 = \bar{f}(\bar{\alpha}) = \bar{f}(\bar{\theta}) = \bar{\theta}^{\#G \setminus D_{\mathfrak{p}_i}} \cdot \bar{h}(\bar{\theta})$ and since $\bar{\theta} \neq 0$, we find $\bar{h}(\bar{\theta}) = 0$.

Let $f^{\bar{\theta}}_{\mathbb{F}_\mathfrak{p}} = \prod_{g \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_\mathfrak{p})}(X - g(\bar{\theta}))$ be the minimal polynomial of $\bar{\theta}$ over $\mathbb{F}_\mathfrak{p}$. Note that $f(X) \in \mathbb{Z}[X]$, so $\bar{f}(X) \in \mathbb{F}_\mathfrak{p}[X]$, so $\bar{h}(X) \in \mathbb{F}_\mathfrak{p}[X]$. Then this gives $f^{\bar{\theta}}_{\mathbb{F}_\mathfrak{p}} \mid \bar{h}(X)$. Since $f^{\bar{\theta}}_{\mathbb{F}_\mathfrak{p}}(\sigma(\bar{\theta})) = 0$, we have $\bar{h}(\bar{\theta}) = 0$. Therefore, there exists $g \in D_{\mathfrak{p}_i}$ such that $\sigma(\sigma(\bar{\theta})) = \bar{g}(\bar{\alpha}) = \bar{g}(\bar{\theta})$. Since $\mathbb{F}_{\mathfrak{p}_i} = \mathbb{F}_\mathfrak{p}(\bar{\theta})$, this means that for such $g \in D_{\mathfrak{p}_i}$ and any $x \in \mathbb{F}_{\mathfrak{p}_i}$, we have $\sigma(x) = \bar{g}(x)$, so $\bar{g} = \sigma$ and the homomorphism $D_{\mathfrak{p}_i} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_\mathfrak{p})$ is surjective. □

Remark 5.2.4. Recall that in the case of knots, we had $I_{K_i} = \{g \in D_{K_i} \mid g|_{K_i} = \mathrm{id}_{K_i}\}$. One might expect the equality $I_{\mathfrak{p}_i} = \{g \in D_{\mathfrak{p}_i} \mid g|_{\mathfrak{p}_i} = \mathrm{id}_{\mathfrak{p}_i}\}$ to hold in the case of primes, as well. However, take $k = \mathbb{Q}(i)$ with prime $\mathfrak{p} = (1+i)$ over $(2) \subseteq \mathbb{Z}$ and $g \in G$ the map $i \mapsto -i$. Since $1+i = i \cdot (1-i)$, we find $g(\mathfrak{p}) = \mathfrak{p}$, so $g \in D_\mathfrak{p}$. We now find $g \notin \{g \in D_\mathfrak{p} \mid g|_\mathfrak{p} = \mathrm{id}_\mathfrak{p}\}$. However, the induced map $\bar{g} : \mathbb{F}_{(1+i)} \to \mathbb{F}_{(1+i)}$ is the identity on $\mathbb{F}_{(1+i)}$, so $g \in I_\mathfrak{p}$.

This is because the analogy between knots and primes does not refer to primes as ideals of rings, but rather as elements of a spectrum. In this case, $\mathfrak{p}_i$ denotes the embedding $\mathrm{Spec}\,\mathbb{F}_{\mathfrak{p}_i} \hookrightarrow \mathrm{Spec}\,\mathcal{O}_k$ induced by the quotient map $\mathcal{O}_k \to \mathbb{F}_{\mathfrak{p}_i}$. This is why the proper analogue of $\mathrm{Gal}(K_i/K)$ is $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_\mathfrak{p})$. ►

Set f to be the degree of $\mathbb{F}_{\mathfrak{p}_i}$ over $\mathbb{F}_p$. As in the case of knots, we can relate e, r, f and n. For every $1 \leq i \leq r$, let $g_i \in G$ be such that $\mathfrak{p}_i = g_i(\mathfrak{p}_1)$ and let e_i be the ramification index of $\mathfrak{p}_i$ over p, i.e., $pO_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Applying g_i gives

$$\mathfrak{p}_i^{e_1} \cdot g_i(\mathfrak{p}_2)^{e_2} \cdot \ldots \cdot g_i(\mathfrak{p}_r)^{e_r} = g_i(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = g_i(pO_k) = pO_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Being the ring of integers of k, we know that O_k has unique prime decomposition, so $e_1 = e_i$. By choosing different values of i, we get $e_1 = \ldots = e_r$, so we have $pO_k = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{e_1}$. Also, since every g_i induces an isomorphism $\mathbb{F}_{\mathfrak{p}_1} \to \mathbb{F}_{\mathfrak{p}_i}$, we find that $f = [\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p]$ is independent of i.

Since O_k has an integral basis $\omega_1, \ldots, \omega_n \in O_k$, we find $O_k \cong \omega_1\mathbb{Z} \oplus \ldots \oplus \omega_n\mathbb{Z}$ as abelian groups. Therefore, $O_k/(p) \cong \omega_1\mathbb{F}_p \oplus \ldots \oplus \omega_n\mathbb{F}_p$ as abelian groups and we find $\#O_k/(p) = p^n$. By multiplicativity of the ideal norm, we have

$$\#O_k/(\mathfrak{p}_1^{e_1}) = [O_k : \mathfrak{p}^{e_i}] = [O_k : \mathfrak{p}]^{e_i} = p^{e_1 f}.$$

Since all $\mathfrak{p}_i$ are coprime, the powers $\mathfrak{p}_i^{e_1}$ are also coprime, so we can apply the Chinese remainder theorem to obtain

$$p^n = \#O_k/(p) = \#(O_k/(\mathfrak{p}_1^{e_1}) \times \ldots \times O_k/(\mathfrak{p}_r^{e_1})) = p^{e_1 f r}$$

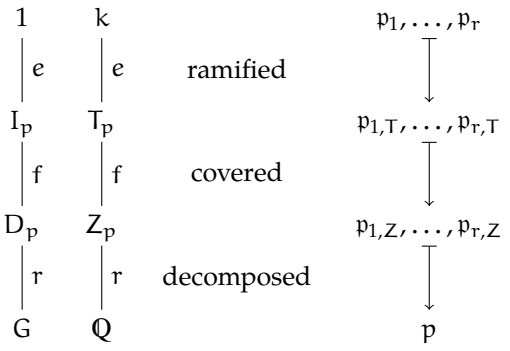
(see also [Mar77, Theorem 22]). This gives us $n = e_1 f r$. By lemma 5.2.3 we know $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_i}/\mathbb{F}_p) \cong D_{\mathfrak{p}_i}/I_{\mathfrak{p}_i}$, so $f = (n/r)/e$, which gives us $e = n/(fr) = e_1$. We now conclude the following:

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

Let $\mathfrak{p}_{i,T} := \mathfrak{p}_i \cap O_{T_{\mathfrak{p}_i}}$ and let $\mathfrak{p}_{i,Z} = \mathfrak{p}_i \cap O_{Z_{\mathfrak{p}_i}}$. We have the following theorem.

Theorem 5.2.5. *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 degree of $\mathfrak{p}_{i,T}$ over $\mathfrak{p}_{i,Z}$ is f and $\mathfrak{p}_{i,Z}$ is inert in $T_{\mathfrak{p}_i}$. The extension $Z_{\mathfrak{p}_i}/\mathbb{Q}$ is an extension of degree r such that p is completely decomposed into r ideals containing $\mathfrak{p}_{i,Z}$ as a prime factor.*

Suppose the Galois group G of the field extension $k/\mathbb{Q}$ is Abelian. Then, since the decomposition groups $D_{\mathfrak{p}_i}$ are conjugate, they are independent of $\mathfrak{p}_i$ lying over p. Therefore, we can write D_p. Likewise, we can write I_p for the inertia group and we write Z_p and T_p for the decomposition and inertia fields, as well. Theorem 5.2.5 then shows how p is decomposed, covered and then ramified through the field extensions k/T_p, T_p/Z_p and $Z_p/\mathbb{Q}$:



In the extension $Z_p/\mathbb{Q}$, p is completely decomposed, i.e., we have $pO_{Z_p} = \prod_{i=1}^{r} \mathfrak{p}_{i,Z}$. In the extension T_p/Z_p, every $\mathfrak{p}_{i,Z}$ is covered in the finite étale sense. Recall the pullback diagram in section 3.3. Here the tensor product of the fraction field $\kappa(\mathfrak{p}_{i,Z}) = O_{Z_p}/\mathfrak{p}_{i,Z}$ with O_{T_p} is given by

$$\kappa(\mathfrak{p}_{i,Z}) \otimes_{O_{Z_p}} O_{T_p} = O_{Z_p}/\mathfrak{p}_{i,Z} \otimes_{O_{Z_p}} O_{T_p} \cong O_{T_p}/\mathfrak{p}_{i,Z}O_{T_p} \cong \prod_{j=1}^{f} O_{Z_p}/\mathfrak{p}_{i,Z}.$$

Therefore, we have a commutative diagram

$$\begin{array}{ccc} \bigsqcup_{i=1}^{f} \operatorname{Spec} O_{Z_p}/\mathfrak{p}_{i,Z} & \longrightarrow & \operatorname{Spec} O_{T_p} \\ \downarrow & & \downarrow \eta \\ \operatorname{Spec} \kappa(\mathfrak{p}_{i,Z}) & \hookrightarrow & \operatorname{Spec} O_{Z_p} \end{array}$$

where η is induced by the embedding $O_{Z_p} \to O_{T_p}$ and where $\operatorname{Spec} \kappa(\mathfrak{p}_{i,Z}) \to \operatorname{Spec} O_{Z_p}$ sends the only prime ideal of $\kappa(\mathfrak{p}_{i,Z})$ to $\mathfrak{p}_{i,Z}$. We can see that $\mathfrak{p}_{i,Z}$ is covered f times through η. Lastly, in the extension k/T_p we have $\mathfrak{p}_{i,T}O_k = \mathfrak{p}_i^e$ for every i, so all $\mathfrak{p}_{i,T}$ ramify.

Let's look at an example.

Example 5.2.6. Let $k := \mathbb{Q}(\zeta_n)$ be a cyclotomic extension of $\mathbb{Q}$. We have $O_k = \mathbb{Z}[\zeta_n]$ and $G := \operatorname{Gal}(k/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. A prime number p is ramified in k if and only if $p|n$. Let p be a prime of $\mathbb{Q}$ and $\mathfrak{p}$ a prime in k lying over p. If $p \nmid n$, then $e = 1$, so the inertia group $I_\mathfrak{p}$ of a prime $\mathfrak{p}$ over p is trivial and the inertia field is $T_\mathfrak{p} = k$. Since $I_\mathfrak{p}$ is trivial, we know that the decomposition group $D_\mathfrak{p}$ is isomorphic to $\operatorname{Gal}(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p)$, which is generated by the Frobenius automorphism

$$\bar{\sigma}: \qquad \mathbb{F}_p(\zeta_n) \longrightarrow \mathbb{F}_p(\zeta_n), \qquad x \longmapsto x^p.$$

Therefore, $f := \#D_\mathfrak{p} = \#\operatorname{Gal}(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p) = \#\langle\sigma\rangle$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ and we have $D_\mathfrak{p} = \langle\sigma\rangle$, where σ is defined

$$\sigma: \qquad \mathbb{Q}(\zeta_n) \longrightarrow \mathbb{Q}(\zeta_n), \qquad x \longmapsto x^p.$$

In particular, $D_\mathfrak{p}$ is trivial if and only if $p \equiv 1 \bmod n$, in which case we have $r = n$. In other words, p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \bmod n$.

As an example, take $p = 7$ and $n = 6$. The primes over (7) are $(7, \zeta_6 - 3)$ and $(7, \zeta_6 - 5)$ (see also [Neu99, Chap. 1, Proposition 8.3] and [Lan94, Chap. 1, Proposition 25]), so $r = 2 = n$, since $\operatorname{Gal}(\mathbb{Q}(\zeta_6)/\mathbb{Q}) \cong (\mathbb{Z}/6\mathbb{Z})^\times = \{1 \bmod 6, 5 \bmod 6\}$.

Now suppose $p|n$ and let m be such that $p^m|n$ but $p^m \nmid n$. Set $G := \operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q})$. The ramification index of p in $\mathbb{Q}(\zeta_n)$ is $e = (p-1)p^{m-1}$ and our inertia field is $T_{\mathfrak{p}_i} = \mathbb{Q}(\zeta_{n/p^m})$. Note that we have

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/p^m})] = [\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = (\mathbb{Z}/p^m\mathbb{Z})^\times = (p-1)p^{m-1} = e,$$

as claimed in theorem 5.2.5.

As an example, let $p = 3$ and $n = 24$. We have

$$(3) = (3, \zeta_{24}^2 + \zeta_{24} + 2)^2(3, \zeta_{24}^2 + 2\zeta_{24} + 2)^2$$

in $\mathbb{Z}(\zeta_{24})$, so $r = 2$. We have $m = 1$ and $e = 2$, so the inertia field of p is $T_{\mathfrak{p}_i} = \mathbb{Q}(\zeta_8)$. Note that the minimal polynomial of ζ_{24} over $\mathbb{Q}(\zeta_8)$ is $f_{\mathbb{Q}(\zeta_8)}^{\zeta_{24}} = x^2 + \zeta_8^3 x - \zeta_8^2$, so $[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}(\zeta_8)] = 2$.

Since $[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = \phi(24) = 8$, where ϕ is the Euler totient function, we have $f = 8/(er) = 2$, so according to theorem 5.2.5 we have $1 \subsetneq I_{\mathfrak{p}_1} \subsetneq D_{\mathfrak{p}_1} \subsetneq G$. Explicitly, we have

$$\begin{array}{lcllcll}
k = \mathbb{Q}(\zeta_{24}) & \overset{2}{\supseteq} & T_p = \mathbb{Q}(\zeta_8) & \overset{2}{\supseteq} & Z_p = \mathbb{Q}(i\sqrt{2}) & \overset{2}{\supseteq} & \mathbb{Q}, \\
\mathfrak{p}_1 = (3, \zeta_{24}^2 + \zeta_{24} + 2) & \supseteq & \mathfrak{p}_{1,T} = (\zeta_8^2 + \zeta - 1) & \supseteq & \mathfrak{p}_{1,Z} = (1 + i\sqrt{2}) & \supseteq & p = (3), \\
\mathfrak{p}_2 = (3, \zeta_{24}^2 + 2\zeta_{24} + 2) & \supseteq & \mathfrak{p}_{2,T} = (\zeta_8^7 + \zeta^6 - 1) & \supseteq & \mathfrak{p}_{2,Z} = (1 - i\sqrt{2}) & \supseteq & p = (3),
\end{array}$$

and we have $p\mathcal{O}_{Z_p} = \mathfrak{p}_{1,Z}\mathfrak{p}_{2,Z}$, $\mathfrak{p}_{i,Z}\mathcal{O}_{T_p} = \mathfrak{p}_{i,T}$ and $\mathfrak{p}_{i,T}\mathcal{O}_k = \mathfrak{p}_i^2$.

For more details on the various results above regarding cyclotomic fields, see [Mar77, Chap. 2]. ►

CHAPTER 6

Homology groups and ideal class groups

We are now going to make the switch from fundamental groups to homology. In this section we're going to take a quick look at a homologically motivated analogy between knots and primes.

6.1 *Homology groups and the Hurewicz theorem*

Recall the construction of the first homology group of a space X: we use part of the singular chain complex

$$\dots \xrightarrow{\partial_3} C_2(X) \xrightarrow{\partial_2} C_1(X) \xrightarrow{\partial_1} C_0(X)$$

and define the group of 1-cycles $Z_1(X) := \ker \partial_1$ and the group of 1-boundaries $B_1(X) := \operatorname{im} \partial_2$. Then the first homology group of X is $H_1(X) := Z_1(X)/B_1(X)$. The important thing to realize here is that knots can be seen as loops, and therefore as 1-cycles, i.e., for a knot $\gamma : S^1 \to S^3$ with endpoints $\gamma(0) = \gamma(1) = x$ we have $\partial_1(K) = x - x = 0$, so $\gamma \in \ker \partial_1$ and we can speak of $\gamma \in H_1(X)$.

Let $p : M \to S^3$ be a finite abelian covering covering ramified over a link L. Define $X := S^3 \setminus L$ and $Y := M \setminus p^{-1}(L)$, so $G := \mathrm{Gal}(M/S^3) := \mathrm{Gal}(Y/X)$. As a consequence of the Hurewicz theorem, we have the following theorem.

Theorem 6.1.1. *We have an isomorphism*

$$H_1(X)/p_*(H_1(Y)) \cong G.$$

Proof. We start by noting that we have $\pi_1(X)/p_*(\pi_1(Y)) \cong G$ by construction. We can now apply the Hurewicz theorem, along with fact that for a group H with normal subgroup N we have $H^{ab}/N^{ab} \cong (H/N)^{ab}$. We get

$$\begin{aligned} H_1(X)/p_*(H_1(Y)) &\cong \pi_1(X)^{ab}/p_*(\pi_1(Y)^{ab}) = \pi_1(X)^{ab}/p_*(\pi_1(Y))^{ab} \\ &\cong (\pi_1(X)/p_*(\pi_1(Y)))^{ab} \cong G^{ab} = G, \end{aligned}$$

which is what we needed to prove. □

6.2 *Ideal class groups and Artin reciprocity*

Let's consider the case of primes. Let k be a finite Abelian extension of $\mathbb{Q}$. Just as knots can be considered 1-cycles, primes in $\mathcal{O}_k$ can be considered invertible ideals.

Definition 6.2.1. *A* fractional $\mathcal{O}_k$-ideal I *is an* $\mathcal{O}_k$*-submodule of* k *such that* $xI \subseteq \mathcal{O}_k$ *for some* $x \in k^*$. *A fractional ideal* $I \subseteq k$ *is called an* invertible ideal *if there exists a fractional ideal* $J \subseteq k$ *such that* $IJ = \mathcal{O}_k$. *A fractional ideal* $I \subseteq k$ *is called* integral *if* $I \subseteq \mathcal{O}_k$.

In particular, an integral ideal I is invertible if and only if IJ is a non-zero principal ideal for some integral ideal $J \subseteq \mathcal{O}_k$. It is a basic number theoretic result that all prime ideals in a ring of integers $\mathcal{O}_k$ are invertible, so the primes in $\mathcal{O}_k$ can indeed be considered invertible fractional ideals. For two fractional $\mathcal{O}_k$-ideals I and J, we define the *ideal quotient* $I : J$ as follows:

$$I : J := \{x \in k \mid xJ \subseteq I\}.$$

The set $I(k)$ of invertible $\mathcal{O}_k$-ideals becomes a group under the operations of ideal multiplication and ideal quotients. Let $P(k)$ be the subgroup of $I(k)$ consisting of all principal fractional $\mathcal{O}_k$-ideals. The analogue of the first homology group is now the *ideal class group* $H(k)$ of k:

$$H(k) := I(k)/P(k).$$

Suppose k is ramified over a set of primes $S = \{p_1, \ldots, p_r\}$ of $\mathbb{Q}$. Let $f : \operatorname{Spec}\mathcal{O}_k \to \operatorname{Spec}\mathbb{Z}$ and $S_k := f^{-1}(S)$. Let $X := \operatorname{Spec}\mathbb{Z} \setminus S$ and $Y := \operatorname{Spec}\mathcal{O}_k \setminus S_k$. Define $G := \operatorname{Gal}(Y/X) := \operatorname{Gal}(k/\mathbb{Q})$. It is known that for a number field K, any fractional ideal $\mathfrak{a} \in I(\mathcal{O}_K)$ has a unique prime ideal decomposition $\mathfrak{a} = \prod_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} \mathfrak{p}^{n_\mathfrak{p}}$, i.e., we have $I(\mathcal{O}_K) \cong \bigoplus_{\mathfrak{p}\in\mathcal{O}_K} \mathbb{Z}$. As the group $I(X)$ of invertible fractional $\mathbb{Z}[1/p_1, \ldots, 1/p_r]$-ideals, then, we define

$$I(X) := \bigoplus_{0\neq\mathfrak{p}\in X} \mathbb{Z},$$

and likewise,

$$I(Y) := \bigoplus_{0\neq\mathfrak{p}\in Y} \mathbb{Z}.$$

Let $p \in X$ be a non-zero prime and let $\mathfrak{p} \in Y$ be a prime lying over p, i.e., $p = \mathfrak{p} \cap \mathbb{Z}$. Recall from section 5.2 that the decomposition group of $\mathfrak{p}$ is defined $D_\mathfrak{p} := \{g \in G \mid g(\mathfrak{p}) = \mathfrak{p}\}$. As we saw in section 5.2, for another prime $\mathfrak{q}$ lying over p, the decomposition groups $D_\mathfrak{p}$ and $D_\mathfrak{q}$ are conjugate. Since k is an Abelian extension of $\mathbb{Q}$, this means that $D_\mathfrak{p} = D_\mathfrak{q}$, so the decomposition group is uniquely determined by p and we write D_p. Also, since p is unramified we know $D_p \cong \operatorname{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$, so D_p is cyclic and we denote with $\sigma_\mathfrak{p}$ a generator of D_p. For a fractional ideal $\mathfrak{a} = \prod_{0\neq\mathfrak{p}\in X} \mathfrak{p}^{n_\mathfrak{p}}$ we can generalize this by defining $\sigma_\mathfrak{a} := \prod_{0\neq\mathfrak{p}\in X} \sigma_\mathfrak{p}^{n_\mathfrak{p}}$. We can now define the following map on $I(X)$:

$$\phi : \quad I(X) \longrightarrow G, \qquad \mathfrak{a} \longmapsto \sigma_\mathfrak{a}.$$

The kernel of ϕ can be given in terms of principal fractional ideals. Specifically, we define the following subgroups of $I(X)$ and $I(Y)$:

$$P(X) := \{(a) \in P(\mathbb{Q}) \mid a \equiv 1 \bmod q \text{ for all } q \in S\}$$

and

$$P(Y) := \{(a) \in P(k) \mid a \equiv 1 \bmod q \text{ for all } q \in S_k \text{ and } \sigma(a) > 0 \text{ for all embeddings } \sigma : k \hookrightarrow \mathbb{R}\}$$

(note that the requirement that $\sigma(\mathfrak{a}) > 0$ for all embeddings $\sigma : \mathbb{Q} \hookrightarrow \mathbb{R}$ puts no further restrictions on $P(\mathbb{Q})$, since every principal fractional ideal in $P(\mathbb{Q})$ has a positive generator). The map ϕ is surjective and the kernel is given by $\ker \phi = N_{k/\mathbb{Q}}(I(Y))P(X)$, where

$$N_{k/\mathbb{Q}} : \qquad I(Y) \longrightarrow I(X), \qquad \prod_{0 \neq \mathfrak{p} \in Y} \mathfrak{p}^{n_\mathfrak{p}} \longmapsto \prod_{0 \neq \mathfrak{p} \in Y} (\#(\mathcal{O}_k/\mathfrak{p}))^{n_\mathfrak{p}}$$

is the ideal norm map [Mor12, Ch. 6, Sect. 2]. Define $H(X) := I(X)/P(X)$ and $H(Y) := I(Y)/P(Y)$. We get the following result.

Theorem 6.2.2 (Artin reciprocity law)**.** *The map*

$$\sigma_{k/\mathbb{Q}} : \qquad H(X)/N_{k/\mathbb{Q}}(H(Y)) \longrightarrow G, \qquad [\mathfrak{a}] \longmapsto \sigma_\mathfrak{a}$$

induced by ϕ is an isomorphism.

This result can be generalized. For example, if K is a number field and L is the maximal unramified Abelian extension of K (known as the *Hilbert class field* of k_n), the map

$$\sigma_{L/K} : \qquad H(K) \longrightarrow \mathrm{Gal}(L/K), \qquad \mathfrak{a} \longmapsto \sigma_\mathfrak{a},$$

commonly referred to as the *Artin map*, is actually an isomorphism [Cox13, Theorem 5.23].

We have now established ideal class groups and Artin reciprocity as the arithmetic analogues of homology and the Hurewicz theorem, respectively. We will apply the analogy between homology and ideal class groups further in the next section.

CHAPTER 7

The Alexander and Iwasawa polynomials

In this chapter we're going to take a look at the analogy between the Alexander polynomial for knots and the Iwasawa polynomial for primes. We'll start by laying the groundwork to later compute the Alexander polynomial.

7.1 *Differential modules*

In previous chapters, we've looked at the fundamental group as a source of information about the structure of knots. The Alexander polynomial is a knot invariant that stems from the desire to understand the homology of knots. Specifically, we will be looking at the first homology group of the infinite cyclic cover $H_1(X_\infty)$ and give a presentation of it as a module over the group ring $\mathbb{Z}[G_K^{ab}]$. In the next section we will give the definition of the Alexander polynomial, but in order to effectively calculate it, we will need some results regarding group rings and differential modules.

Definition 7.1.1. *Let* G *be a group and* R *be a ring. The* group ring *or* group algebra $R[G]$ *is the set of formal sums* $\sum_{g\in G} r_g g$ *with finite support, i.e.,*

$$R[G] := \Big\{ \sum_{g\in G} r_g g \,|\, r_g = 0 \text{ for almost all } g \in G \Big\}.$$

The ring operations are defined by $\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G}(r_g + s_g)g$ *and* $(\sum_{g\in G} r_g g)\cdot(\sum_{g\in G} s_g g) = \sum_{g\in G}(\sum_{h\in G} r_g s_h gh)$. *The action of* R *on* $R[G]$ *is defined by* $r(\sum_{g\in G} r_g g) = \sum_{g\in G} rr_g g$.

Example 7.1.2. Let K be a knot and G_K the knot group. Since $G_K^{ab} \cong \mathbb{Z}$, the group ring $\mathbb{Z}[G_K^{ab}]$ is isomorphic to the group ring of Laurent polynomials $\mathbb{Z}[t, t^{-1}]$. As we shall see soon, the Alexander polynomial is defined to be an element of $\mathbb{Z}[t, t^{-1}]$. ▶

In order to construct some very useful exact sequences later, we now define the augmentation map and its kernel, the augmentation ideal.

Definition 7.1.3. *Let G be a group and R be a ring. Then the R-algebra homomorphism $\epsilon_{R[G]} : R[G] \to R, \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g$ is called the* augmentation map. *The ideal $I_{R[G]} := \ker \epsilon_{R[G]}$ of $R[G]$ is called the* augmentation ideal.

The augmentation ideal will be instrumental in connecting the homology of the infinite cyclic cover with the Alexander module later on. The next proposition reveals more about the nature of this ideal.

Proposition 7.1.4. *Let G be a group and R be a ring. The augmentation ideal $I_{R[G]}$ is generated by $\{g - 1 \mid g \in G\}$.*

Proof. The inclusion $(g-1) \subseteq I_{R[G]}$ is clear. Let $\sum_{g\in G} r_g g \in I_{R[G]}$. Then $\sum_{g\in G} r_g = 0$, so $r_1 = -\sum_{g\neq 1} r_g$. Then we have

$$\sum_{g\in G} r_g g = \sum_{g\neq 1} r_g g + r_1 = \sum_{g\neq 1} r_g g - \sum_{g\neq 1} r_g = \sum_{g\neq 1} r_g (g-1),$$

so the other inclusion holds, as well. □

Any group homomorphism $\psi : G \to H$ can be extended to a ring homomorphism $\psi : R[G] \to R[H], \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g \psi(g)$. We continue with the definition of a ψ-differential.

Definition 7.1.5. *Let $\psi : G \to H$ be a group homomorphism and let M be an H-module. Then a map $d : G \to M$ is a ψ-differential if, for all $g_1, g_2 \in G$, it satisfies the relation*

$$d(g_1 g_2) = d(g_1) + \psi(g_1) d(g_2).$$

We put this definition into practice immediately with the ψ-differential module.

Definition 7.1.6. *Let $\psi : G \to H$ be a group homomorphism. Let $\bigoplus_{g\in G} \mathbb{Z}[H]dg$ be the free $\mathbb{Z}[H]$-module on the generating set $\{dg \mid g \in G\}$. Then we define the* ψ-differential module A_ψ *as follows:*

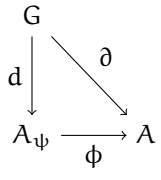
$$A_\psi := \left(\bigoplus_{g\in G} \mathbb{Z}[H]dg \right) / \langle \{ d(g_1 g_2) - dg_1 - \psi(g_1) dg_2 \mid g_1, g_2 \in G \} \rangle_{\mathbb{Z}[H]}.$$

Here $\langle \{ d(g_1 g_2) - dg_1 - \psi(g_1) dg_2 \mid g_1, g_2 \in G \} \rangle_{\mathbb{Z}[H]}$ is the $\mathbb{Z}[H]$-module generated by the elements of the form $d(g_1 g_2) - dg_1 - \psi(g_1) dg_2$.

By definition, we have $d(g_1 g_2) = dg_1 + \psi(g_1) dg_2$ in A_ψ, so the map $G \to A_\psi, g \mapsto dg$ is by definition a ψ-differential. Also useful to note, is that we have $d1 = 0$.

This unwieldy construction occurs naturally as the result of a universal property concerning ψ-differentials.

Proposition 7.1.7. *Let $\psi : G \to H$ be a group homomorphism and let A_ψ be the ψ-differential module with canonical ψ-differential $d : G \to A_\psi$. For any $\mathbb{Z}[H]$-module A with ψ-differential $\partial : G \to A$, there exists a unique $\phi : A_\psi \to A$ such that $\phi \circ d = \partial$, i.e., the following diagram commutes:*



This property determines A_ψ uniquely up to isormorphism.

Proof. Since the dg generate A_ψ as a $\mathbb{Z}[H]$-module, we only have to define ϕ for elements dg. We have $\phi(dg) = \partial(g)$, so ϕ is uniquely determined. Also, since

$$\phi(d(g_1g_2)) = \partial(g_1g_2) = \partial(g_1) + \psi(g_1)\partial(g_2) = \phi(dg_1 + \psi(g_1)dg_2)$$

this map is well-defined.

Suppose that for any $\mathbb{Z}[H]$-module B with ψ-differential $\delta : G \to B$, there exists a unique $\mathbb{Z}[H]$-homomorphism $\xi : A \to B$ such that $\xi \circ \partial = \delta$. Then the unique morphism $\xi : A \to A$ such that $\xi \circ \partial = \partial$ is id_A. Since there also exists a $\xi' : A \to A_\psi$ such that $\xi' \circ \partial = d$, we have $\phi \circ \xi' \circ \partial = \phi \circ d = \partial$, so $\phi \circ \xi' = \mathrm{id}_A$. Likewise, we find $\xi' \circ \phi = \mathrm{id}_{A_\psi}$, so the universal property indeed determines A_ψ uniquely up to isomorphism. □

The Alexander polynomial is obtained by finding a presentation matrix of a differential module and looking at its minors. Therefore, our goal now is to find a free presentation of a differential module. For this we need a few auxiliary results.

Lemma 7.1.8. *Let G be a group. We have an isomorphism $A_{\mathrm{id}_G} \cong I_{\mathbb{Z}[G]}$ induced by $dg \mapsto g - 1$.*

Proof. We're going to use the universal property of the ψ-differential module. The map $\delta : G \to I_{\mathbb{Z}[G]}, g \mapsto g - 1$ is an id_G-differential, since

$$\delta(g_1g_2) = g_1g_2 - 1 = g_1 - 1 + g_1(g_2 - 1) = \delta(g_1) + \mathrm{id}_G(g_1)\delta(g_2)$$

for all $g_1, g_2 \in G$. For a $\mathbb{Z}[G]$-module A with ψ-differential $\partial : G \to A$, a map $\phi : I_{\mathbb{Z}[G]} \to A$ with $\phi \circ \delta = \partial$ has to satisfy $\phi(g - 1) = (\phi \circ \delta)(g) = \partial(g)$, which uniquely determines ϕ. Therefore, $I_{\mathbb{Z}[G]}$ satisfies the universal property of ψ-diffential modules and we have $A_{\mathrm{id}_G} \cong I_{\mathbb{Z}[G]}$. □

Lemma 7.1.9. *Let $\psi : G \to H$ be a surjective group homomorphism and $\tilde{\psi} : \mathbb{Z}[G] \to \mathbb{Z}[H]$ the induced ring homomorphism. Let $N := \ker \psi$. We have an isomorphism*

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

of $\mathbb{Z}[G]$-modules, where we view $\mathbb{Z}[H]$ as a $\mathbb{Z}[G]$-modules through $\tilde{\psi}$.

Proof. We are first going to show $\ker \tilde{\psi} = I_{\mathbb{Z}[N]}\mathbb{Z}[G]$. The augmentation ideal $I_{\mathbb{Z}[N]}$ is the kernel of the augmentation map $\epsilon_{\mathbb{Z}[N]} : \mathbb{Z}[N] \to \mathbb{Z}$. Therefore, for $\sum_{g\in N} n_g g \in I_{\mathbb{Z}[N]}$, we have

$$\tilde{\psi}\left(\sum_{g\in N} n_g g\right) = \sum_{g\in N}(n_g\psi(g)) = \left(\sum_{g\in N} n_g\right)\cdot 1 = \epsilon_{\mathbb{Z}[N]}\left(\sum_{g\in N} n_g g\right)\cdot 1 = 0 \cdot 1,$$

so $I_{\mathbb{Z}[N]}\mathbb{Z}[G] \subseteq \ker \psi$. Now let $\alpha = \sum_{g\in G} r_g g \in \ker \psi$. We have

$$0 = \tilde{\psi}(\alpha) = \sum_{g\in G} r_g\psi(g) = \sum_{h\in\psi(G)}\left(\sum_{\psi(g)=h} r_g\right)h,$$

so $\sum_{\psi(g)=h} r_g = 0$ for all $h \in \psi(G)$. Let $h \in \psi(G)$ and $g_h \in G$ such that $\psi(g_h) = h$. Since $N\backslash G \cong \psi(G)$, we know $Ng_h = \phi^{-1}(h)$. Then

$$\begin{aligned}\sum_{\psi(g)=h} r_g g &= \sum_{\psi(g)=h} r_g g - \sum_{\psi(g)=h} r_g g_h = \sum_{n\in N} r_{ng_h} n g_h - \sum_{n\in N} r_{ng_h} g_h \\ &= \left(\sum_{n\in N} r_{ng_h} n - \sum_{n\in N} r_{ng_h}\right) g_h \in I_{\mathbb{Z}[N]}\mathbb{Z}[G].\end{aligned}$$

Therefore, we have

$$\alpha = \sum_{g\in G} r_g g = \sum_{h\in\psi(G)} \left(\sum_{\psi(g)=h} r_g g \right) \in I_{\mathbb{Z}[N]}\mathbb{Z}[G],$$

which gives us $\ker \tilde{\psi} \subseteq I_{\mathbb{Z}[N]}\mathbb{Z}[G]$ as was claimed. Since $\tilde{\psi}$ is surjective, this gives us the isomorphism

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

of $\mathbb{Z}[G]$-modules. □

Proposition 7.1.10. *Let $\psi : G \to H$ be a surjective group homomorphism. Let A_ψ be the ψ-differential module. Let $N := \ker \psi$. Then there is an isomorphism*

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

of $\mathbb{Z}[H]$-modules defined by $dg \mapsto g - 1$.

Proof. We will first show $A_\psi \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G}$ using the universal property for ψ-differential modules. Note that we can view $\mathbb{Z}[H]$ as a $\mathbb{Z}[G]$-module through $\tilde{\psi} : \mathbb{Z}[G] \to \mathbb{Z}[H]$, the map induced by ψ. By extension of scalars, $\mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G}$ is then a $\mathbb{Z}[H]$-module. Define the map

$$\delta : \quad G \longrightarrow \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G}, \qquad g \longmapsto 1 \otimes dg.$$

This map is a ψ-differential, since we have

$$\delta(g_1g_2) = 1 \otimes d(g_1g_2) = 1 \otimes dg_1 + 1 \otimes g_1dg_2 = 1 \otimes dg_1 + \psi(g_1) \otimes dg_2 = \delta(g_1) + \psi(g_1)\delta(g_2).$$

Now let A be a $\mathbb{Z}[H]$-module with ψ-differential $\partial : G \to A$. We want to define a $\mathbb{Z}[H]$-module homomorphism $\phi : \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G} \to A$ such that $\phi \circ \delta = \partial$. This map is uniquely determined, since we have

$$\phi(1 \otimes dg) = (\phi \circ \delta)(g) = \partial(g).$$

Therefore, $\mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G}$ satisfies the universal property of ψ-differential modules. We have $A_\psi \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G}$ and this $\mathbb{Z}[H]$-isomorphism is defined by $dg \mapsto 1 \otimes dg$. Using lemma 7.1.8 and lemma 7.1.9 we now find the isomorphism

$$A_\psi \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} A_{\mathrm{id}_G} \cong (\mathbb{Z}[G]/I_{\mathbb{Z}[N]}\mathbb{Z}[G]) \otimes_{\mathbb{Z}[G]} I_{\mathbb{Z}[G]} \cong I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}$$

of $\mathbb{Z}[G]$-modules defined by $dg \mapsto g - 1$.

Let $\beta \in \mathbb{Z}[H]$ and $\alpha_1, \alpha_2 \in \psi^{-1}(\beta)$. Since $\psi(\alpha_1 - \alpha_2) = 0$ we have $\alpha_1 - \alpha_2 \in \ker \psi = I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}$. Therefore, we have an action of $\mathbb{Z}[H]$ on $I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}$, where the action of $\beta \in \mathbb{Z}[H]$ is multiplication by any $\alpha \in \psi^{-1}(\beta)$. This turns $I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}$ into a $\mathbb{Z}[H]$-module. Therefore, we have an isomorphism $A_\psi \cong I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}$ of $\mathbb{Z}[H]$-modules. □

Before we introduce the main theorem that will allow us to compute the Alexander polynomial, we need to define the Fox free derivative.

Definition 7.1.11. *Let F be the free group on generators $x_1, \ldots, x_m$ with identity element e. The* Fox free derivative with respect to x_i *is a map $\frac{\partial}{\partial x_i} : \mathbb{Z}[F] \to \mathbb{Z}[F]$, where $1 \le i \le m$, which is determined by the following properties:*

(1) $\dfrac{\partial(\alpha+\beta)}{\partial x_i} = \dfrac{\partial\alpha}{\partial x_i} + \dfrac{\partial\beta}{\partial x_i}$ *for any $\alpha, \beta \in \mathbb{Z}[F]$,*

(2) $\dfrac{\partial x_j}{\partial x_i} = \delta_{ij}$,

(3) $\dfrac{\partial(uv)}{\partial x_i} = \dfrac{\partial u}{\partial x_i} + u\dfrac{\partial v}{\partial x_i}$ *for any* $u, v \in F$.

These properties uniquely determine $\frac{\partial}{\partial x_i}$ [CF63, Chap. VII, 2.9]. Following this definition, we can check that for inverses we have the following rule:

$$\frac{\partial(u^{-1})}{\partial x_i} = -u^{-1}\frac{\partial u}{\partial x_i} \text{ for any } u \in F.$$

The following computational result is going to be important in a later proof.

Lemma 7.1.12. *Let* F *be the free group on the generators* $x_1, \dots, x_r$ *and consider the Fox free derivative* $\partial/\partial x_j : \mathbb{Z}[F] \to \mathbb{Z}[F]$. *Let* $\alpha \in F$. *We have*

$$\sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1) = \alpha - 1.$$

Proof. First note that we can recursively work out

$$\frac{\partial x_i^n}{\partial x_j} = \frac{\partial x_i}{\partial x_j} + x_i\frac{\partial x_i^{n-1}}{\partial x_j} = \frac{\partial x_i}{\partial x_j} + x_i\left(\frac{\partial x_i}{\partial x_j} + x_i\frac{\partial x_i^{n-2}}{\partial x_j}\right) = \dots = (1 + x_i + \dots + x_i^{n-1})\delta_{ij},$$

where δ_{ij} is the Kronecker delta. Multiplying by $(x_i - 1)$ gives $\frac{\partial x_i^n}{\partial x_j}(x_i - 1) = (x_i^n - 1)\delta_{ij}$. We use this fact to get

$$\sum_{j=1}^{r} \frac{\partial(x_i^n)}{\partial x_j}(x_j - 1) = \sum_{j=1}^{r}(1 + x_i + \dots + x_i^{n-1})\delta_{ij}(x_j - 1) = x_i^n - 1.$$

Now let $\alpha = x_{i_1}^{e_{i_1}} \cdots x_{i_n}^{e_{i_n}} \in F$. This gives us

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

which concludes the proof. □

Let G be a finitely presented group with presentation $G = \langle x_1, \dots, x_r \mid R_1, \dots, R_s \rangle$. Let F be the free group on generators $x_1, \dots, x_r$ with the canonical quotient map $\pi : F \to G$. Let $\psi : G \to H$ be a surjective group homomorphism. Consider the $\mathbb{Z}[H]$-module homomorphism

$$d_2 : \quad \mathbb{Z}[H]^s \longrightarrow \mathbb{Z}[H]^r, \qquad (\beta_i)_{1\le i\le s} \longmapsto \left(\sum_{i=1}^{s} \beta_i (\psi\circ\pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right)_{1\le j\le r},$$

i.e., d_2 is given by multiplication of $(\beta_1, \dots, \beta_s)$ with the matrix

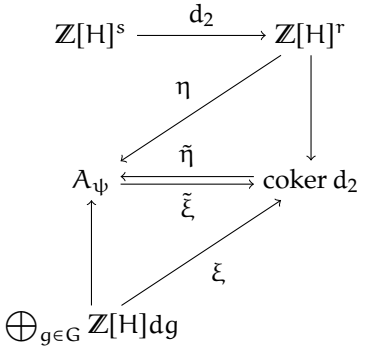
$$\begin{pmatrix} (\psi\circ\pi)\left(\frac{\partial R_1}{\partial x_1}\right) & \cdots & (\psi\circ\pi)\left(\frac{\partial R_1}{\partial x_r}\right) \\ \vdots & \ddots & \vdots \\ (\psi\circ\pi)\left(\frac{\partial R_s}{\partial x_1}\right) & \cdots & (\psi\circ\pi)\left(\frac{\partial R_s}{\partial x_r}\right) \end{pmatrix}.$$

We now give the main theorem of this section.

Theorem 7.1.13. *We have an isomorphism of $\mathbb{Z}[H]$-modules*

$$A_\psi \cong \operatorname{coker} d_2.$$

Proof. We are going to define the $\mathbb{Z}[H]$-module homomorphisms $\eta : \mathbb{Z}[H]^r \to A_\psi$ and $\xi : \bigoplus_{g\in G} \mathbb{Z}[H]dg \to \operatorname{coker} d_2$ that induce maps $\tilde\eta : \operatorname{coker} d_2 \to A_\psi$ and $\tilde\xi : A_\psi \to \operatorname{coker} d_2$. Our goal is to get the following commutative diagram:



Define the $\mathbb{Z}[H]$-module homomorphism $\xi : \bigoplus_{g\in G} \mathbb{Z}[H]dg \to \operatorname{coker} d_2$ by

$$\xi(dg) := \left((\psi\circ\pi)\left(\frac{\partial f}{\partial x_j}\right)\right)_{1\le j\le r},$$

where $f \in \pi^{-1}(g)$. To show that this is independent of the choice of f, let $f \in \pi^{-1}(g)$ and $k \in \ker \pi$. We have

$$\xi(fk) = \left((\psi\circ\pi)\left(\frac{\partial (fk)}{\partial x_j}\right)\right)_{1\le j\le r} = \left((\psi\circ\pi)\left(\frac{\partial f}{\partial x_j}\right)\right)_{1\le j\le r} + \left((\psi\circ\pi)\left(f\frac{\partial k}{\partial x_j}\right)\right)_{1\le j\le r},$$

so it suffices to show $((\psi \circ \pi)(f\partial k/\partial x_j))_{1\leq j\leq r} \in \operatorname{im} d_2$. Note that G is the quotient group of F by the normal closure of $\{R_1, \ldots, R_s\}$, i.e., the normal subgroup generated by elements $\tilde{f}R_i\tilde{f}^{-1} \in F$, where $\tilde{f} \in F$ and $1 \leq i \leq s$. Therefore, k can be written as

$$k = (f_{i_1} R_{i_1} f_{i_1}^{-1}) \cdots (f_{i_n} R_{i_n} f_{i_n}^{-1}).$$

For $\tilde{f}$ and $1 \leq i \leq s$ we have

$$\begin{aligned}
\pi\left(\frac{\partial(\tilde{f}R_i\tilde{f}^{-1})}{\partial x_j}\right) &= \pi\left(\frac{\partial \tilde{f}}{\partial x_j} + \tilde{f}\frac{\partial R_i}{\partial x_j} + \tilde{f}R_i\frac{\partial \tilde{f}^{-1}}{\partial x_j}\right) \\
&= \pi\left(\frac{\partial \tilde{f}}{\partial x_j} + \tilde{f}\frac{\partial R_i}{\partial x_j} - \tilde{f}R_i\tilde{f}^{-1}\frac{\partial \tilde{f}}{\partial x_j}\right) \\
&= \tilde{f}\pi\left(\frac{\partial R_i}{x_j}\right),
\end{aligned}$$

since $\partial f^{-1}/\partial x_j = f^{-1}\partial f/\partial x_j$ and $\pi(R_i) = 1$. We now find

$$\begin{aligned}
\pi\left(\frac{\partial k}{\partial x_j}\right) &= \pi\left(\frac{\partial((f_{i_1} R_{i_1} f_{i_1}^{-1}) \cdots (f_{i_n} R_{i_n} f_{i_n}^{-1}))}{\partial x_j}\right) \\
&= \pi\left(\frac{\partial(f_{i_1} R_{i_1} f_{i_1}^{-1})}{\partial x_j} + f_{i_1} R_{i_1} f_{i_1}^{-1}\frac{\partial(f_{i_2} R_{i_2} f_{i_2}^{-1})}{\partial x_j} + \ldots \right. \\
&\quad \left. + (f_{i_1} R_{i_1} f_{i_1}^{-1}) \cdots (f_{i_{n-1}} R_{i_{n-1}} f_{i_{n-1}}^{-1})\frac{\partial(f_{i_n} R_{i_n} f_{i_n}^{-1})}{\partial x_j}\right) \\
&= \pi\left(\frac{\partial(f_{i_1} R_{i_1} f_{i_1}^{-1})}{\partial x_j}\right) + \ldots + \pi\left(\frac{\partial(f_{i_n} R_{i_n} f_{i_n}^{-1})}{\partial x_j}\right) \\
&= f_{i_1}\pi\left(\frac{\partial R_{i_1}}{\partial x_j}\right) + \ldots + f_{i_n}\pi\left(\frac{\partial R_{i_n}}{\partial x_j}\right),
\end{aligned}$$

which we can rewrite as

$$\pi\left(\frac{\partial k}{\partial x_j}\right) = \alpha_1\pi\left(\frac{\partial R_1}{\partial x_j}\right) + \ldots + \alpha_n\pi\left(\frac{\partial R_n}{\partial x_j}\right) = \sum_{i=1}^{s} \alpha_1\pi\left(\frac{\partial R_i}{\partial x_j}\right)$$

for some $\alpha_1, \ldots, \alpha_n \in G$. Denote $\beta_i = \psi(\alpha_i)$ and $h = (\psi \circ \pi)(f)$. We now find

$$\left((\psi \circ \pi)\left(f\frac{\partial k}{\partial x_j}\right)\right)_{1\leq j\leq r} = \left(\sum_{i=1}^{s} h\beta_i(\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right)_{1\leq j\leq r} = \xi((h\beta_i)_{1\leq i\leq s}) \in \operatorname{im} d_2.$$

We conclude that the image of ξ is independent of choice of f.

To show that ξ induces a map $\tilde{\xi} : A_\psi \to \operatorname{coker} d_2$, we have to show that for all $g_1, g_2 \in G$ we have $\xi(d(g_1g_2) - dg_1 - \psi(g_1)dg_2) = 0$. Let $g_1, g_2 \in G$ and $f_1, f_2 \in F$ such that $\pi(f_1) = g_1$ and $\pi(f_2) = g_2$. Now we clearly have

$$\xi(d(g_1g_2) - dg_1 - \psi(g_1)dg_2) = \left((\psi \circ \pi)\left(\frac{\partial(f_1f_2)}{\partial x_j}\right) - (\psi \circ \pi)\left(\frac{\partial f_1}{\partial x_j}\right) - \psi(g_1)(\psi \circ \pi)\left(\frac{\partial f_2}{\partial x_j}\right)\right)_{1\leq j\leq r} = 0,$$

since

$$(\psi\circ\pi)\left(\frac{\partial(f_1f_2)}{\partial x_j}\right)=(\psi\circ\pi)\left(\frac{\partial f_1}{\partial x_j}+f_1\frac{\partial f_2}{\partial x_j}\right)=(\psi\circ\pi)\left(\frac{\partial f_1}{\partial x_j}\right)+\psi(g_1)(\psi\circ\pi)\left(\frac{\partial f_2}{\partial x_j}\right),$$

so ξ indeed induces a map $\tilde{\xi}:A_\psi\longrightarrow\operatorname{coker}d_2$.

Now we define

$$\eta:\qquad\mathbb{Z}[H]^r\longrightarrow A_\psi,\qquad(\beta_j)_{1\leq j\leq r}\longmapsto\sum_{j=1}^{r}\beta_j\,d\pi(x_j)$$

and prove that it induces $\tilde{\eta}:\operatorname{coker}d_2\longrightarrow A_\psi$. To this end, we have to show $\eta\circ d_2=0$. Let $(\alpha_i)_{1\leq i\leq s}\in\mathbb{Z}[H]^s$. Let $\mu:I_{\mathbb{Z}[G]}/I_{\mathbb{Z}[N]}I_{\mathbb{Z}[G]}\longrightarrow A_\psi$ be the isomorphism defined by $g-1\mapsto dg$ as in proposition 7.1.10. Using lemma 7.1.12 we get

$$\begin{aligned}
(\eta\circ d_2)((\alpha_i)_{1\leq i\leq s})&=\sum_{j=1}^{r}\sum_{i=1}^{s}\alpha_i(\psi\circ\pi)\left(\frac{\partial R_i}{\partial x_j}\right)d\pi(x_j)\\
&=\sum_{i=1}^{s}\alpha_i\sum_{j=1}^{r}(\psi\circ\pi)\left(\frac{\partial R_i}{\partial x_j}\right)\mu(\pi(x_j)-1)\\
&=\sum_{i=1}^{s}\alpha_i\sum_{j=1}^{r}\mu\left(\pi\left(\frac{\partial R_i}{\partial x_j}\right)(\pi(x_j)-1)\right)\\
&=\sum_{i=1}^{s}\alpha_i\mu\left(\pi\left(\sum_{j=1}^{r}\left(\frac{\partial R_i}{\partial x_j}\right)(x_j-1)\right)\right)\\
&=\sum_{i=1}^{s}\alpha_i\mu(\pi(R_i-1))\\
&=\sum_{i=1}^{s}\alpha_i\mu(0)\\
&=0,
\end{aligned}$$

so $\eta\circ d_2=0$, so η induces a map $\tilde{\eta}:\operatorname{coker}d_2\longrightarrow A_\psi$. To conclude the proof we need to show $\tilde{\eta}\circ\tilde{\xi}=\mathrm{id}_{A_\psi}$ and $\tilde{\xi}\circ\tilde{\eta}=\mathrm{id}_{\operatorname{coker}d_2}$. It suffices to show this for all generators $dg\in A_\psi$ and $(\delta_{kj})_{1\leq j\leq r}\in\operatorname{coker}d_2$, where $g\in G$ and $1\leq k\leq r$. Let $g\in G$ and $1\leq k\leq r$, with $f\in F$ such that $\pi(f)=g$. Then we have

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

and

$$\begin{aligned}
(\tilde{\xi} \circ \tilde{\eta})((\delta_{kj})_{1\leq j\leq r}) &= \tilde{\xi}\left(\sum_{j=1}^{r} \delta_{kj}\, d\pi(x_j)\right) \\
&= \tilde{\xi}(d\pi(x_k)) \\
&= \left((\psi \circ \pi)\left(\frac{\partial x_k}{\partial x_j}\right)\right)_{1\leq j\leq r} \\
&= (\delta_{kj})_{1\leq j\leq r},
\end{aligned}$$

which concludes the proof. □

Theorem 7.1.13 has the following immediate consequence.

Corollary 7.1.14. *The ψ-differential module A_ψ has a free presentation over $\mathbb{Z}[H]$:*

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

Its presentation matrix Q_ψ is given by

$$Q_\psi = \left((\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right)_{\substack{1\leq i\leq s \\ 1\leq j\leq r}} = \begin{pmatrix} (\psi \circ \pi)\left(\frac{\partial R_1}{\partial x_1}\right) & \cdots & (\psi \circ \pi)\left(\frac{\partial R_1}{\partial x_r}\right) \\ \vdots & \ddots & \vdots \\ (\psi \circ \pi)\left(\frac{\partial R_s}{\partial x_1}\right) & \cdots & (\psi \circ \pi)\left(\frac{\partial R_s}{\partial x_r}\right) \end{pmatrix}.$$

7.2 *The Alexander polynomial*

We've already seen in lemma 2.2.12 that the first homology group $H_1(S^3 \setminus K)$ of a knot complement is always isomorphic to $\mathbb{Z}$. However, for an infinite cyclic cover the first homology group is more

interesting. Let K be a knot in S^3 and let X_K be the knot exterior. Let $p : X_\infty \to X_K$ be an infinite cyclic cover of the knot complement X_K, so we have $\pi_1(X_\infty) \cong p_*(\pi_1(X_\infty)) = [G_K, G_K]$ (recall that p_* is injective by theorem 2.2.9). In order to make the jump from the fundamental group to homology, we will now introduce the Crowell exact sequence.

Theorem 7.2.1. *Let*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\psi} H \longrightarrow 1$$

be a short exact sequence of groups. Then we have an exact sequence of $\mathbb{Z}[H]$-modules

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

where θ_1 is the homomorphism induced by $n \mapsto dn$ and θ_2 is the homomorphism induced by $dg \mapsto \psi(g) - 1$. This sequence is called the Crowell exact sequence.

Proof. The action of $\mathbb{Z}[H]$ on A_ψ and $\mathbb{Z}[H]$ is clear. The action of $\mathbb{Z}[H]$ on $\mathbb{Z}$ is defined by $(\sum_{h\in H} n_h h)m := \epsilon_{\mathbb{Z}[H]}(\sum_{h\in H} n_h h)m = \sum_{h\in H} n_h m$, where $n_h, m \in \mathbb{Z}$. As for the action of $\mathbb{Z}[H]$ on N^{ab}, it is induced by the action $h(n) := g_h n g_h^{-1}$ of H on N^{ab}, where $g_h \in G$ such that $\psi(g_h) = h$. This action is independent of the choice of g_h: suppose $g, g' \in G$ with $\psi(g) = \psi(g')$. Then $\psi(g(g')^{-1}) = 1$, so $g(g')^{-1} \in N$, so also $gn(g')^{-1} = (gng^{-1})(g(g')^{-1}) \in N$. Then we have

$$gng^{-1}g'n^{-1}(g')^{-1} = (gn(g')^{-1})(g'g^{-1})(gn(g')^{-1})^{-1}(g'g^{-1})^{-1} = 1 \in N^{ab},$$

so $gng^{-1} = g'n(g')^{-1}$. Therefore N^{ab} is well-defined as a $\mathbb{Z}[H]$-module.

Let $m, n \in N$. Since

$$dm^{-1} = d(m^{-1}m) - \psi(m^{-1})dm = d1 - dm = -dm,$$

we have

$$\begin{aligned} d(m^{-1}n^{-1}mn) &= dm^{-1} + \psi(m^{-1})dn^{-1} + \psi(m^{-1}n^{-1})dm + \psi(m^{-1}n^{-1}m)dn \\ &= -dm - dn + dm + dn = 0, \end{aligned}$$

so θ_1 is well-defined. Now let $g_1, g_2 \in G$. We have

$$d(g_1g_2) - dg_1 - \psi(g_1)dg_2 \longmapsto (\psi(g_1g_2) - 1) - (\psi(g_1) - 1) - \psi(g_1)(\psi(g_2) - 1) = 0,$$

so θ_2 is well-defined.

To show that θ_1 is injective, we are going to construct a left inverse $\eta : A_\psi \to N^{ab}$ such that $\eta \circ \theta_1 = \mathrm{id}_{N^{ab}}$. Let $r : H \to G$ be a map such that $\psi \circ r = \mathrm{id}_H$ with $r(1) = 1$. Note that r is not necessarily a homomorphism. We define a group homomorphism $\tau : \bigoplus_{g\in G} \mathbb{Z}[H]dg \to N^{ab}$ that will induce the group homomorphism η. Since $\bigoplus_{g\in G} \mathbb{Z}[H]dg$ is free as a group on the set $\{hdg \mid g \in G, h \in H\}$ of generators, we will define τ on the elements hdg. Define

$$\tau(hdg) := r(h)gr(h\psi(g))^{-1}.$$

Note that this is well-defined, since

$$\psi(r(h)gr(h\psi(g))^{-1}) = h\psi(g)(h\psi(g))^{-1} = 1.$$

Since we have Now let $g_1, g_2 \in G$. We have

$$\begin{aligned}&\tau(h\mathrm{d}(g_1g_2) - h\mathrm{d}g_1 - h\psi(g_1)\mathrm{d}g_2)\\ &\quad = r(h)g_1g_2r(h\psi(g_1g_2))^{-1} \cdot (r(h)g_1r(h\psi(g_1))^{-1})^{-1} \cdot (r(h\psi(g_1))g_2r(h\psi(g_1)\psi(g_2))^{-1})^{-1} = 0,\end{aligned}$$

so τ indeed induces a map $\eta : A_\psi \to N^{ab}$. Since we have

$$(\eta \circ \theta_1)(n) = \eta(1\mathrm{d}n) = r(1)nr(1\psi(n))^{-1} = n,$$

we find that $\eta \circ \theta_1 = \mathrm{id}_{N^{ab}}$, so θ_1 is injective.

The sequence is exact at A_ψ by the series of equivalences

$$\mathrm{d}g \in \ker\, \theta_2 \Leftrightarrow \psi(g) - 1 = 0 \Leftrightarrow \psi(g) = 1 \Leftrightarrow \mathrm{d}g \in \mathrm{im}\, \theta_1.$$

Exactness at $\mathbb{Z}[H]$ can be seen by noting that $\ker\, \epsilon_{\mathbb{Z}[H]} =: I_{\mathbb{Z}[H]}$ is generated as a $\mathbb{Z}[H]$-module by elements $g - 1$, and since $g - 1 = \theta_2(\mathrm{d}g) \in \mathrm{im}\, \theta_2$ for all $g \in G$, we have $\ker\, \epsilon_{\mathbb{Z}[H]} = \mathrm{im}\, \theta_2$. Lastly, since $\epsilon_{\mathbb{Z}[H]}$ is obviously surjective, we can conclude that the sequence is exact. □

The Crowell exact sequence helps us bridge the gap between the knot module and the Alexander module.

Definition 7.2.2. *Let K be a knot in S^3. Let G_K be the knot group and G_K^{ab} its abelianization, with the canonical projection map $\psi : G_K \to G_K^{ab}$. We call $A_K := A_\psi$ the* Alexander module. *By the Crowell exact sequence, we can consider $H_1(X_\infty)$ as a $\mathbb{Z}[G_K^{ab}]$-module. We then call $H_1(X_\infty)$ the* knot module.

Since $H_1(X_\infty) = [G_K, G_K]^{ab}$ by the Hurewicz theorem, we can apply the Crowell exact sequence to the short exact sequence

$$1 \longrightarrow [G_K, G_K] \longrightarrow G_K \xrightarrow{\psi} G_K^{ab} \longrightarrow 1.$$

This gives us

$$0 \longrightarrow H_1(X_\infty) \longrightarrow A_K \longrightarrow \mathbb{Z}[G_K^{ab}] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

This sequence actually occurs naturally when we look at the long exact sequence of homology groups for the space pair $(X_\infty, p^{-1}(x_0))$, where $x_0 \in X_K$. This sequence ends as follows

$$\begin{aligned}\ldots \longrightarrow H_1(p^{-1}(x_0)) \longrightarrow H_1(X_\infty) \longrightarrow H_1(X_\infty, p^{-1}(x_0))\\ \longrightarrow H_0(p^{-1}(x_0)) \longrightarrow H_0(X_\infty) \longrightarrow H_0(X_\infty, p^{-1}(x_0)) \longrightarrow 0.\end{aligned}$$

Since $p^{-1}(x_0)$ is discrete, $H_1(p^{-1}(x_0)) = 0$. Furthermore, since X_∞ is path connected and $p^{-1}(x_0)$ is non-empty, we have $H_0(X_\infty, p^{-1}(x_0)) = 0$ [Rot88, Theorem 5.12], so the sequence reduces to

$$0 \longrightarrow H_1(X_\infty) \longrightarrow H_1(X_\infty, p^{-1}(x_0)) \longrightarrow H_0(p^{-1}(x_0)) \longrightarrow H_0(X_\infty) \longrightarrow 0.$$

It is a theorem that there exists a diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & [G_K, G_K]^{ab} & \longrightarrow & A_K & \longrightarrow & \mathbb{Z}[G_K^{ab}] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\
0 & \longrightarrow & H_1(X_\infty) & \longrightarrow & H_1(X_\infty, p^{-1}(x_0)) & \longrightarrow & H_0(p^{-1}(x_0)) & \longrightarrow & H_0(X_\infty) & \longrightarrow & 0
\end{array}$$

where every square commutes [Cro71, p. 233]. In other words, when we apply the Crowell exact sequence to the knot group, we get the long exact sequence of homology groups.

Note that $G_K^{ab} \cong \langle t \rangle \cong \mathbb{Z}$ and let α be a meridian of K such that $\psi : G_K \to G_K^{ab}$ sends α to t. From now on, we will denote with $\Lambda := \mathbb{Z}[t, t^{-1}] \cong \mathbb{Z}[G_K^{ab}]$ the ring of Laurent polynomials. Since $I_\Lambda = (t-1) \cong \Lambda$ as Λ-modules through $t - 1 \mapsto 1$, we can write the Crowell exact sequence in the form

$$0 \longrightarrow H_1(X_\infty) \longrightarrow A_K \longrightarrow \Lambda \longrightarrow 0.$$

Since Λ is a free Λ-module, this sequence splits [Eis04, Appendix 3, Proposition A3.1], so we have $A_K \cong H_1(X_\infty) \oplus \Lambda$ as Λ-modules. We can now reformulate theorem 7.1.14.

Theorem 7.2.3. *Let $G_K = \langle x_1, \dots, x_r \mid R_1, \dots, R_s \rangle$ be a finite presentation of the knot group. Define $F := \langle x_1, \dots, x_r \rangle$ with $\pi : F \to G_K$ and $\psi : G_K \to G_K^{ab}$ the canonical quotient maps. Then the Alexander module A_K has a free resolution over Λ:*

$$\Lambda^s \xrightarrow{Q} \Lambda^r \longrightarrow A_K \longrightarrow 0.$$

The presentation matrix Q is given by

$$Q := \left((\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j} \right) \right)_{\substack{1 \le i \le s \\ 1 \le j \le r}}$$

and is called the Alexander matrix *of K. It depends on the choice of presentation of G_K.*

We are now ready to define Fitting ideals and more Alexander terminology.

Definition 7.2.4. *Let R be a commutative ring and M a finitely generated R-module with presentation*

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

and $s \times r$ presentation matrix Q. For $d \ge 0$ we define the d-th Fitting ideal $F_d(M)$ *(or the* d-th elementary ideal*) of M as follows:*

(1) If $0 < s - d \le r$, then $F_d(M)$ is the ideal generated by the $r - d$-minors of Q.

(2) If $s - d > r$, then $F_d(M) = 0$.

(3) If $s - d \le 0$, then $F_d(M) = R$.

A special case of the Fitting ideal, is the Alexander ideal.

Definition 7.2.5. *Let K be a knot and let Q be the $s \times r$ Alexander matrix of K with $s \le r$. The* Alexander ideal *of A_K is the 0-th Fitting ideal $F_0(A_K) \subseteq \Lambda$ generated by the s-minors of Q. We define the* Alexander polynomial *$\Delta_K(t) \in \Lambda$ of K to be a generator of $F(A_K)$.*

The Alexander ideal exists for any knot, since the Wirtinger presentation gives us an Alexander matrix with $s = n - 1 \le n = r$ for some n. It is known that the Fitting ideal is independent of the choice of presentation [Lan02, Chap. XIX, Lemma 2.3]. Also, as we shall see soon, the Fitting ideal of A_K is principal, so $\Delta_K(t)$ is defined up to multiplication by an element of $\Lambda^\times = \{\pm t^n \mid n \in \mathbb{Z}\}$.

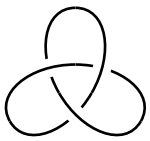


Fig. 7.1: The trefoil knot

Example 7.2.6. We're going to compute the Alexander polynomial of the trefoil knot K, displayed in figure 7.1.

The knot group has a Wirtinger presentation

$$G_K = \langle x, y \mid xyx = yxy \rangle.$$

Let $F = \langle x, y \rangle$, with $\pi : F \to G_K$ and $\psi : G_K \to G_K^{ab} = \langle t \rangle$ the canonical quotient maps. We denote with π and ψ also the induced maps $\mathbb{Z} \to \mathbb{Z}[G_K]$ and $\mathbb{Z}[G_K] \to \Lambda$, respectively. In the Wirtinger presentation above, x and y are meridians of K and we have $(\psi \circ \pi)(x) = t = (\psi \circ \pi)(y)$. Using

$$\frac{\partial(xyx - yxy)}{\partial x} = \frac{\partial x}{\partial x} + x\frac{\partial y}{\partial x} + xy\frac{\partial x}{\partial x} - \frac{\partial y}{\partial x} - y\frac{\partial x}{\partial x} - yx\frac{\partial y}{\partial x} = 1 - y + xy$$

(and, likewise, $\partial(xyx - yxy)/\partial y = -1 + x - yx$), we find the following Alexander matrix:

$$\begin{aligned} Q &= \begin{pmatrix} (\psi \circ \pi)\left(\dfrac{\partial(xyx - yxy)}{\partial x}\right) & (\psi \circ \pi)\left(\dfrac{\partial(xyx - yxy)}{\partial y}\right) \end{pmatrix} \\ &= \begin{pmatrix} (\psi \circ \pi)(1 - y + xy) & (\psi \circ \pi)(-1 + x - yx) \end{pmatrix} \\ &= \begin{pmatrix} 1 - t + t^2 & -1 + t - t^2 \end{pmatrix}. \end{aligned}$$

We find $F_0(A_K) = (1 - t + t^2, -1 + t - t^2) = (1 - t + t^2)$, so the Alexander polynomial of K is $\Delta_K(t) = 1 - t + t^2$.

Let's choose a different presentation of G_K:

$$G_K = \langle u, v \mid u^2 = v^3 \rangle.$$

Since the Alexander polynomial is a knot invariant, we should end up with $1 - t + t^2$ again, up to multiplication by $\Lambda^\times$.

Previously, while using the Wirtinger presentation, we knew that x and y corresponded to meridians of K. In that case, we knew $(\psi \circ \pi)(x) = t = (\psi \circ \pi)(y)$. Since we now use a different presentation, this is no longer necessarily the case. There is no obvious way in general to find out what $(\psi \circ \pi)(u)$ and $(\psi \circ \pi)(v)$ are, but with the knowledge of the Wirtinger presentation, all we need to do is find an isomorphism

$$\langle u, v \mid u^2 = v^3 \rangle \longrightarrow \langle x, y \mid xyx = yxy \rangle.$$

One such isomorphism is given by $u \mapsto xy$ and $v \mapsto yxy$, which gives $(\psi \circ \pi)(u) = t^3$ and $(\psi \circ \pi)(v) = t^2$. In general, for an (a, b)-torus knot K' with knot group presentation $G_{K'} = \langle g_1, g_2 \mid g_1^a = g_2^b \rangle$, the element $g_2^d g_1^{-c}$ describes the meridian of K', where $ad - bc = 1$ [BZH13, Proposition 3.38(b)]. We then have

$$g_1 = g_1^{ad-bc} = (g_1^a)^d g_1^{-bc} = g_2^{bd} g_1^{-bc} = (g_2^d g_1^{-c})^b$$

and likewise, $g_2 = (g_2^d g_1^{-c})^a$, so $(\psi\circ\pi)(g_1) = t^b$ and $(\psi\circ\pi)(g_2) = t^a$, which agrees with our case (recall that the trefoil knot is a $(2,3)$-torus knot). The presentation matrix for this presentation is therefore

$$\begin{aligned} Q &= \begin{pmatrix} (\psi\circ\pi)\left(\frac{\partial(u^2-v^3)}{\partial u}\right) & (\psi\circ\pi)\left(\frac{\partial(u^2-v^3)}{\partial v}\right)\end{pmatrix} \\ &= \begin{pmatrix} (\psi\circ\pi)(1+u) & (\psi\circ\pi)(-1-v-v^2)\end{pmatrix} \\ &= \begin{pmatrix} 1+t^3 & -1-t^2-t^4\end{pmatrix}. \end{aligned}$$

The 1-minors of Q are $1+t^3$ and $-1-t^2-t^4$. Using the Euclidean algorithm, we find

$$\gcd(1+t^2+t^4, 1+t^3) = \gcd(1+t^3, 1-t+t^2) = \gcd(1-t+t^2, 1-t+t^2) = 1-t+t^2,$$

so $F_0(A_K) = (1-t+t^2)$ and $\Delta_K(t) = 1-t+t^2$, as expected. ▶

Example 7.2.7. We're going to compute the Alexander polynomial of the figure-eight knot K, displayed in figure 7.2.

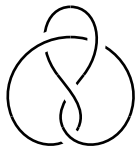


Fig. 7.2: The figure-eight knot

The knot group of K has the following Wirtinger presentation:

$$G_K = \langle w, x, y, z \,|\, wy^{-1}x^{-1}y = xzy^{-1}z^{-1} = yw^{-1}z^{-1}w = 1\rangle$$

(i.e., $R_1 = wy^{-1}x^{-1}y$, $R_2 = xzy^{-1}z^{-1}$ and $R_3 = yw^{-1}z^{-1}w$). For brevity's sake, we define $f := \psi\circ\pi : \mathbb{Z}[F] \to \mathbb{Z}[G_K^{ab}]$. This gives us the following Alexander matrix:

$$\begin{aligned} Q &= \begin{pmatrix} (\psi\circ\pi)\left(\frac{\partial R_1}{\partial w}\right) & (\psi\circ\pi)\left(\frac{\partial R_1}{\partial x}\right) & (\psi\circ\pi)\left(\frac{\partial R_1}{\partial y}\right) & (\psi\circ\pi)\left(\frac{\partial R_1}{\partial z}\right) \\ (\psi\circ\pi)\left(\frac{\partial R_2}{\partial w}\right) & (\psi\circ\pi)\left(\frac{\partial R_2}{\partial x}\right) & (\psi\circ\pi)\left(\frac{\partial R_2}{\partial y}\right) & (\psi\circ\pi)\left(\frac{\partial R_2}{\partial z}\right) \\ (\psi\circ\pi)\left(\frac{\partial R_3}{\partial w}\right) & (\psi\circ\pi)\left(\frac{\partial R_3}{\partial x}\right) & (\psi\circ\pi)\left(\frac{\partial R_3}{\partial y}\right) & (\psi\circ\pi)\left(\frac{\partial R_3}{\partial z}\right)\end{pmatrix} \\ &= \begin{pmatrix} f(1) & f(-wy^{-1}x^{-1}) & f(-wy^{-1}+wy^{-1}x^{-1}) & f(0) \\ f(0) & f(1) & f(-xzy^{-1}) & f(x+xzy^{-1}z^{-1}) \\ f(-yw^{-1}+yw^{-1}z^{-1}) & f(0) & f(1) & f(-yw^{-1}z^{-1})\end{pmatrix} \\ &= \begin{pmatrix} 1 & -t^{-1} & -1+t^{-1} & 0 \\ 0 & 1 & -t & -1+t \\ -1+t^{-1} & 0 & 1 & -t^{-1}\end{pmatrix}. \end{aligned}$$

The 3-minors of Q are all $\pm(t^{-2}-3t^{-1}+1)$, so $F_0(A_K) = (t^{-2}-3t^{-1}+1)$ and the Alexander polynomial of K is $\Delta_K(t) = t^{-2}-3t^{-1}+1$. ▶

7.3 *The Alexander polynomial as a characteristic polynomial*

In the last section, we used the structure of A_K to compute the Alexander polynomial $\Delta_K(t)$. Using the Λ-module identity $A_K \cong H_1(X_\infty) \oplus \Lambda$, we shall now see how the Alexander polynomial is actually determined by $H_1(X_\infty)$ and how it is related to a $\mathbb{Q}$-endomorphism on $H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Let K be a knot in S^3. Let $G_K = \langle x_1, \ldots, x_m \mid R_1 = \ldots = R_{m-1} = 1 \rangle$ be a presentation of the knot group of K. Let $\pi : \langle x_1, \ldots, x_m \rangle \to G_K$ and $\psi : G_K \to G_K^{ab}$ be the canonical quotient maps. We identify $\Lambda := \mathbb{Z}[t, t^{-1}] \cong \mathbb{Z}[\mathrm{Gal}(X_\infty/X_K)]$, where X_∞ is the infinite cyclic cover of the knot complement X_K. Take τ to be a generator of the Galois group of X_∞ over X_K such that τ corresponds to t, i.e., $\mathrm{Gal}(X_\infty/X_K) = \langle \tau \rangle$. Let

$$\Lambda^{m-1} \xrightarrow{Q_K} \Lambda^m \longrightarrow A_K \longrightarrow 0$$

be a free presentation of A_K with $m-1 \times m$ presentation matrix Q_K. By applying elementary column operations if necessary, we can assume $Q_K = (Q_1 \mid 0)$, where Q_1 is a $m-1 \times m-1$ matrix. Since $A_K \cong H_1(X_\infty) \oplus \Lambda$ as Λ-modules, we get a free presentation

$$\Lambda^{m-1} \xrightarrow{Q_1} \Lambda^{m-1} \longrightarrow H_1(X_\infty) \longrightarrow 0$$

of $H_1(X_\infty)$ with presentation matrix Q_1. Since $Q_K = (Q_1 \mid 0)$, the $m-1$-minors of Q_K are $\det(Q_1)$ and 0, so the Alexander ideal (the 0-th Fitting ideal) is $F_0(H_1(X_\infty)) = (\det(Q_1))$ with Alexander polynomial $\Delta_K(t) = \det(Q_1)$. Define $\Lambda_{\mathbb{Q}} := \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ and note that $H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}$ is finitely generated as a $\Lambda_{\mathbb{Q}}$-module. Since $\Lambda_{\mathbb{Q}} \cong \mathbb{Q}[t, t^{-1}]$ is a principal ideal domain, the structure theorem for finitely generated modules over a principal ideal domain tells us that there are $f_i \in \Lambda_{\mathbb{Q}}$, with $1 \leq i \leq s$ for some s, such that

$$H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i).$$

Note that τ acts on Λ (and thus also on $\bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i)$) through multiplication by t.

Theorem 7.3.1. *Let $\Delta_K(t) \in \Lambda \subset \Lambda_{\mathbb{Q}}$ be the Alexander polynomial of K. We have*

$$\Delta_K(t) = f_1 \cdots f_s = \det(t \cdot \mathrm{id} - \tau \mid H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}) \bmod \Lambda_{\mathbb{Q}}^{\times},$$

where $\tau : H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q} \to H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-linear map.

Proof. Tensoring with $\mathbb{Q}$ we find a free presentation

$$\Lambda_{\mathbb{Q}}^s \xrightarrow{Q_1} \Lambda_{\mathbb{Q}}^s \longrightarrow \bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i) \longrightarrow 0$$

for $H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}$, with Fitting ideal $F_0(H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}) = (\det(Q_1))$. Since the Fitting ideal is independent of the choice of presentation, the fitting ideal of $\bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i)$ is $(f_1 \cdots f_s)$ [Lan02, Chap. XIX, Corollary 2.9]. This can be seen if we let Q_1' be the $s \times s$ matrix with the elements f_i along the diagonal. We get a presentation

$$\Lambda_{\mathbb{Q}}^s \xrightarrow{Q_1'} \Lambda_{\mathbb{Q}}^s \longrightarrow \bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i) \longrightarrow 0$$

and $F_0(H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}) = \det(Q_1') = f_1 \cdots f_s$. Considering the Alexander polynomial in the ring $\Lambda_{\mathbb{Q}}$, we now find

$$\Delta_K(t) = \det(Q_1') = f_1 \cdots f_s.$$

Now for the second equality we have to prove. By tensoring $H_1(X_\infty)$ with $\mathbb{Q}$, we have acquired a vector space over $\mathbb{Q}$. Since τ acts on $\bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i)$ through multiplication by t, we know that τ is a linear map on $\bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i)$. For every i, define $\tau_i := \tau|_{\Lambda_{\mathbb{Q}}/(f_i)} : \Lambda_{\mathbb{Q}}/(f_i) \to \Lambda_{\mathbb{Q}}/(f_i)$. Choose $\lambda t^{a_i} \in \Lambda_{\mathbb{Q}}^{\times}$ such that $g_i := f_i \cdot \lambda t^{a_i}$ is of the form $a_{i0} + a_{i1}t + \ldots + a_{i,n_i-1}t^{n_i-1} + t^{n_i}$, where $a_{i0} \neq 0$ and $n_i := \deg(g_i)$. We then have $\Lambda_{\mathbb{Q}}/(f_i) = \Lambda_{\mathbb{Q}}/(g_i)$ and $\Lambda_{\mathbb{Q}}/(g_i)$ is a n_i-dimensional vector space with basis $(1, t, \ldots, t^{n_i-1})$. The linear map τ_i that sends an element $p \in \Lambda_{\mathbb{Q}}/(g_i)$ to pt has the following matrix representation:

$$\tau_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & -a_{i0} \\ 0 & 1 & \cdots & 0 & -a_{i1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{i,n_i-1} \end{pmatrix}.$$

The characteristic polynomial of τ_i is

$$\det(t \cdot \mathrm{id} - \tau_i) = \det \begin{pmatrix} t & 0 & \cdots & \cdots & 0 & 0 \\ -1 & t & \cdots & \cdots & 0 & a_{i0} \\ 0 & -1 & \ddots & & 0 & a_{i1} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t & a_{i,n_i-2} \\ 0 & 0 & \cdots & 0 & -1 & t + a_{i,n_i-1} \end{pmatrix} = (-1)^{n_i+1} t g_i \equiv f_i \bmod \Lambda_{\mathbb{Q}}^{\times}.$$

Since τ is a linear endomorphism on $\bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i)$, its matrix representation is the following block matrix:

$$\tau = \left(\begin{array}{c|c|c|c} \tau_1 & 0 & \cdots & 0 \\ \hline 0 & \tau_2 & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & \tau_s \end{array}\right).$$

Therefore, the characteristic polynomial of τ as a $\mathbb{Q}$-linear map on $\bigoplus_{i=1}^{s} \Lambda_{\mathbb{Q}}/(f_i) \cong H_1(X_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}$ is

$$\begin{aligned} \det(t \cdot \mathrm{id} - \tau) &= \det \left(\begin{array}{c|c|c|c} t \cdot \mathrm{id} - \tau_1 & 0 & \cdots & 0 \\ \hline 0 & t \cdot \mathrm{id} - \tau_2 & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & t \cdot \mathrm{id} - \tau_s \end{array}\right) \\ &= \prod_{i=1}^{s} \det(t \cdot \mathrm{id} - \tau_i) \equiv f_1 \cdots f_s \bmod \Lambda_{\mathbb{Q}}^{\times}, \end{aligned}$$

which concludes the proof. □

7.4 *Complete differential modules*

In order to define the analogue of the Alexander polynomial, we need analogues of differential modules that we can apply to étale fundamental groups. These groups are profinite, so we need some profinite analogues. From here on, let R be a compact complete local ring with maximal ideal $\mathfrak{m}$, i.e., $R = \hat{R} := \varprojlim_i R/\mathfrak{m}^i$. We endow R with the *Krull topology* or the $\mathfrak{m}$-*adic topology*, i.e., the topology that has as its basis the sets $r + \mathfrak{m}_n$, where $\mathfrak{m}_n$ is the kernel of the quotient map $R \to R/\mathfrak{m}^n$. This implies that for every quotient ring $R/\mathfrak{m}^i$ is discrete and has an open cover $\{r + \mathfrak{m}^i \mid r \in R\}$. Since $R/\mathfrak{m}^i$ is compact, every $R/\mathfrak{m}^i$ is in fact finite. Therefore, R is a profinite ring.

Let G be a profinite group and let $\{N_j \mid j \in J\}$ be the set of open normal subgroups of G. Since the N_j are open and normal, the quotient groups G/N_j are finite [RZ10, Theorem 2.1.3]. If we let $i' \geq i$ and $N_{j'} \subseteq N_j$, we can define the natural ring homomorphism $\phi_{(i,j)}^{(i',j')} : R/\mathfrak{m}^{i'}[G/N_{j'}] \to R/\mathfrak{m}^i[G/N_j]$. Then $\{R/\mathfrak{m}^i[G/N_j], \phi_{(i,j)}^{(i',j')}\}$ forms a projective system of finite rings.

Definition 7.4.1. *Let G be a profinite group and let $\{N_j \mid j \in J\}$ be the set of open normal subgroups of G. The projective limit $\varprojlim_{i,j} R/\mathfrak{m}^i[G/N_j]$ is called the* complete group ring *or* complete group algebra *of G over R and is denoted by $R[[G]]$.*

In other words, $R[[G]]$ is the completion of $R[G]$ [RZ10, Lemma 5.3.5] and $R[[G]]$ is a profinite ring. Since we have

$$\begin{aligned} R[[G]] :&= \varprojlim_{i,j} R/\mathfrak{m}^i[G/N_j] \cong \varprojlim_j \left(\varprojlim_i (R/\mathfrak{m}^i[G/N_j]) \right) \cong \varprojlim_j \left(\varprojlim_i R/\mathfrak{m}^i \right)[G/N_j] \\ &= \varprojlim_j R[G/N_j], \end{aligned}$$

we can write elements of $R[[G]]$ in the form $\left(\sum_{g_j \in G/N_j} r_{g_j}(g_j + N_j) \right)_{j \in J}$.

Example 7.4.2. The arithmetic analogue of the infinite cyclic covering is called the cyclotomic $\mathbb{Z}_p$-extension and has Galois group G isomorphic to $\mathbb{Z}_p$. Analogous to the group ring $\mathbb{Z}[G_K^{ab}]$ for knots, the complete group ring $\mathbb{Z}_p[[G]]$ will be important in defining the Iwasawa polynomial later. ▶

Let G and H be profinite groups with $f : G \to H$ a continuous homomorphism. Let $\{N_j \mid j \in J\}$ be the set of open normal subgroups of G and $\{M_k \mid k \in K\}$ the set of open normal subgroups of H. Note that $f^{-1}(M_k) \in \{N_j \mid j \in J\}$ for all k. Then we get an induced continuous homomorphism

$$f : \quad R[[G]] \longrightarrow R[[H]], \quad \left(\sum_{g_j \in G/N_j} r_{g_j}(g_j + N_j) \right)_{j \in J} \longmapsto \left(\sum_{g_k \in G/f^{-1}(M_k)} r_{g_k}(f(g_k) + M_k) \right).$$

When $H = 1$ we get the augmentation map.

Definition 7.4.3. *Let G be a profinite group. Let $\{N_j \mid j \in J\}$ be the set of open normal subgroups of G and set $N_0 := G$. Then the R-algebra homomorphism*

$$\epsilon_{R[[G]]} : \quad R[[G]] \longrightarrow R, \quad \left(\sum_{g_j \in G/N_j} r_{g_j}(g_j + N_j) \right)_{j \in J} \longmapsto r_{g_0}$$

(here $g_0 \in G/N_0 = 1$ *is the unique element of the trivial group) is called the* augmentation map. *The ideal* $I_{\epsilon_{R[[G]]}} := \ker \epsilon_{R[[G]]}$ *of* $R[[G]]$ *is called the* augmentation ideal.

The group ring $R[G]$ is embedded in $R[[G]]$ through

$$R[G] \longrightarrow R[[G]], \qquad \sum_{g\in G} r_g g \longmapsto \left(\sum_{g\in G} r_g (g + N_j) \right)_{j\in J}$$

(in fact, $R[G]$ is dense in $R[[G]]$ [RZ10, Lemma 5.3.5(c)]) and this embedding is implicitly invoked when we talk of an element $\sum_{g\in G} r_g g \in R[[G]]$.

The following proposition is a complete analogue of proposition 7.1.4. For a proof, see [RZ10, Lemma 6.3.2(c)].

Proposition 7.4.4. *Let* G *be a profinite group. The augmentation ideal* $I_{R[[G]]}$ *is generated by* $\{g-1 \mid g \in G\} \subseteq R[[G]]$.

We are now ready to introduce the complete analogue of the ψ-differential module.

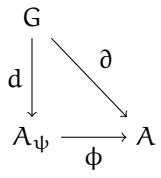
Definition 7.4.5. *Let* $\psi : G \to H$ *be a continuous homomorphism of profinite groups. Let* l *be a prime number. Let* $\bigoplus_{g\in G} \mathbb{Z}_l[[H]]dg$ *be the free* $\mathbb{Z}_l[[H]]$*-module on the generating set* $\{dg \mid g \in G\}$. *Then we define the* complete ψ-differential module *as follows:*

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

Here $\langle \{d(g_1g_2) - dg_1 - \psi(g_1)dg_2 \mid g_1, g_2 \in G\} \rangle_{\mathbb{Z}_l[[H]]}$ *is the* $\mathbb{Z}_l[[H]]$*-module generated by the elements of the form* $d(g_1g_2) - dg_1 - \psi(g_1)dg_2$.

As in definition 7.1.6, $G \to A_\psi, g \mapsto dg$ is by definition a ψ-differential, and as in definition 7.1.6, this construction arises from the following universal property of complete ψ-differentials.

Proposition 7.4.6. *Let* $\psi : G \to H$ *be a continuous group homomorphism of profinite groups and let* A_ψ *be the complete* ψ*-differential module with canonical* ψ*-differential* $d : G \to A_\psi$. *For any* $\mathbb{Z}_l[[H]]$*-module* A *with* ψ*-differential* $\partial : G \to A$, *there exists a unique* $\phi : A_\psi \to A$ *such that* $\phi \circ d = \partial$, *i.e., the following diagram commutes:*



This property determines A_ψ *uniquely up to isomorphism.*

We can apply this to prove the following analogue to lemma 7.1.8.

Lemma 7.4.7. *Let* G *be a profinite group. We have an isomorphism* $A_{\mathrm{id}_G} \cong I_{\mathbb{Z}_l[[G]]}$ *induced by* $dg \mapsto g - 1$.

Proof. Suppose $G = \varprojlim_i G_i$ and define $\delta_i : G_i \to I_{\mathbb{Z}_l[G_i]}, g \mapsto g - 1$. As in the proof of lemma 7.1.8, every δ_i is an id_{G_i}-differential. Taking the projective limit, we obtain an id_G-differential $\delta : G \to I_{\mathbb{Z}_l[[G]]}$. For a $\mathbb{Z}_l[[G]]$-module A with ψ-differential $\partial : G \to A$, a map $\phi : I_{\mathbb{Z}_l[[G]]} \to A$ with $\phi \circ \delta = \partial$ has to satisfy $\phi(g-1) = (\phi \circ \delta)(g) = \partial(g)$, which uniquely determines ϕ. Therefore, $I_{\mathbb{Z}_l[[G]]}$ satisfies the universal property of complete ψ-differential modules and we have $A_{\mathrm{id}_G} \cong I_{\mathbb{Z}_l[[G]]}$. □

Lemma 7.4.8. *Let $\psi : G \to H$ be a continuous homomorphism between profinite groups and $\tilde{\psi} : \mathbb{Z}_l[[G]] \to \mathbb{Z}_l[[H]]$ the induced ring homomorphism. Let $N := \ker \psi$. We have an isomorphism*

$$\mathbb{Z}_l[[G]]/I_{\mathbb{Z}_l[[N]]}\mathbb{Z}_l[[G]] \cong \mathbb{Z}_l[[H]]$$

of $\mathbb{Z}_l[[G]]$-modules, where we view $\mathbb{Z}_l[[H]]$ as a $\mathbb{Z}_l[[G]]$-module through $\tilde{\psi}$.

Proof. As in the proof of lemma 7.1.9, we are first going to show $\ker \tilde{\psi} = I_{\mathbb{Z}_l[[N]]}\mathbb{Z}_l[[G]]$. Suppose $G = \varprojlim_i G_i$ and $H = \varprojlim_j H_j$. For every i, j we have a homomorphism $\psi_{ij} : G_i \to H_j$ defined by the composite $G_i \to G \xrightarrow{\psi} H \to H_i$. Set $N_{ij} := \ker \psi_{ij}$ and let $\tilde{\psi}_{ij} : \mathbb{Z}_l[G_i] \to \mathbb{Z}_l[H_j]$ be the map induced by ψ_{ij}. Lemma 7.1.9 tells us that $\ker \tilde{\psi}_{ij} = I_{\mathbb{Z}_l[N_{ij}]}\mathbb{Z}_l[G_i]$. Taking the projective limit, we get $\ker \tilde{\psi} = I_{\mathbb{Z}_l[[N]]}\mathbb{Z}_l[[G]]$. Since $\tilde{\psi}$ is surjective, this gives us the isomorphism

$$\mathbb{Z}_l[[G]]/I_{\mathbb{Z}_l[[N]]}\mathbb{Z}_l[[G]] \cong \mathbb{Z}_l[[H]]$$

of $\mathbb{Z}_l[[G]]$-modules. □

The following proposition can be proven entirely analogously to proposition 7.1.10.

Proposition 7.4.9. *Let $\psi : G \to H$ be a surjective continuous homomorphism between profinite groups. Let A_ψ be the complete ψ-differential module. Let $N := \ker \psi$. Then there is an isomorphism*

$$A_\psi \cong I_{\mathbb{Z}_l[[G]]}/I_{\mathbb{Z}_l[[N]]}I_{\mathbb{Z}_l[[G]]}$$

of $\mathbb{Z}_l[[H]]$-modules defined by $dg \mapsto g - 1$.

We will now introduce the appropriate analogue to the Fox free derivative.

Definition 7.4.10. *Let $\hat{F}(l)$ be the free pro-l group on the generators $x_1, \dots, x_r$. The* pro-l Fox derivative *is a map $\partial/\partial x_i : \mathbb{Z}_l[[\hat{F}(l)]] \to \mathbb{Z}_l[[\hat{F}(l)]]$, where $1 \le i \le m$, which is determined by the following properties:*

(1) $\dfrac{\partial(\alpha+\beta)}{\partial x_i} = \dfrac{\partial\alpha}{\partial x_i} + \dfrac{\partial\beta}{\partial x_i}$ *for any $\alpha, \beta \in \mathbb{Z}_l[[\hat{F}(l)]]$,*

(2) $\dfrac{\partial x_j}{\partial x_i} = \delta_{ij}$,

(3) $\dfrac{\partial(uv)}{\partial x_i} = \dfrac{\partial u}{\partial x_i} + u\dfrac{\partial v}{\partial x_i}$ *for any $u, v \in \hat{F}(l)$.*

Since $\mathbb{Z}_l[\hat{F}(l)]$ is dense in $\mathbb{Z}_l[[\hat{F}(l)]]$ and since the profinite ring $\mathbb{Z}_l[[\hat{F}(l)]]$ is Hausdorff, the fact that these properties uniquely determine the Fox free derivative $\frac{\partial}{\partial x_i} : \mathbb{Z}_l[\hat{F}(l)] \to \mathbb{Z}_l[\hat{F}(l)]$ implies that they also uniquely determine the pro-l Fox free derivative $\frac{\partial}{\partial x_i} : \mathbb{Z}_l[[\hat{F}(l)]] \to \mathbb{Z}_l[[\hat{F}(l)]]$.

Let G be a finitely presented pro-l group with presentation $G = \langle x_1, \dots, x_r \mid R_1 = \dots = R_s \rangle$. Let $\hat{F}(l)$ be the free pro-l group on generators $x_1, \dots, x_r$ with the canonical quotient map $\pi : \hat{F}(l) \to G$. Let $\psi : G \to H$ be a surjective continuous homomorphism of profinite groups. Consider the $\mathbb{Z}_l[[H]]$-module homomorphism

$$d_2 : \quad \mathbb{Z}_l[[H]]^s \longrightarrow \mathbb{Z}_l[[H]]^r, \qquad (\beta_i)_{1\le i\le s} \longmapsto \left(\sum_{i=1}^{s} \beta_i (\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right)_{1\le j\le r}.$$

Analogous to theorem 7.1.13 and its corollary, we have the following theorems.

Theorem 7.4.11. *We have an isomorphism of $\mathbb{Z}_l[[H]]$-modules*

$$A_\psi \cong \operatorname{coker} d_2.$$

Corollary 7.4.12. *The complete ψ-differential A_ψ has a free presentation over $\mathbb{Z}_l[[H]]$:*

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

Its presentation matrix Q_ψ is given by

$$Q_\psi = \left((\psi \circ \pi)\left(\frac{\partial R_i}{\partial x_j}\right)\right)_{\substack{1\le i\le s \\ 1\le j\le r}} = \begin{pmatrix} (\psi \circ \pi)\left(\frac{\partial R_1}{\partial x_1}\right) & \cdots & (\psi \circ \pi)\left(\frac{\partial R_s}{\partial x_1}\right) \\ \vdots & \ddots & \vdots \\ (\psi \circ \pi)\left(\frac{\partial R_1}{\partial x_r}\right) & \cdots & (\psi \circ \pi)\left(\frac{\partial R_s}{\partial x_r}\right) \end{pmatrix}.$$

7.5 *The Iwasawa polynomial*

Now that we've laid the groundwork for the presentation of complete ψ-differential modules, let us start the construction of the Iwasawa polynomial. Let p be a prime number and define $\mathbb{Q}_\infty := \mathbb{Q}(\zeta_{p^\infty}) := \mathbb{Q}(\zeta_{p^n} \mid n \in \mathbb{N})$. Then $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times \cong \mathbb{F}_p \times (1 + p\mathbb{Z}_p)$, so there is a quotient k_∞ of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(k_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. We call k_∞ the *cyclotomic $\mathbb{Z}_p$-extension* of $\mathbb{Q}$. Let k_n be the cyclic subextension of $k_\infty/\mathbb{Q}$ of degree p^n and let H_n be the Sylow p-subgroup of its ideal class group, i.e., $H_n := H(k_n)(p)$. Suppose the order of the class group of k_n has prime factorization $\#H(k_n) = p_1^{e_1} \cdots p_r^{e_r}$. Assume without loss of generality $p = p_1$. Since $H(k_n)$ is Abelian we know that $H(k_n) \cong H(k_n)(p_1) \times \dots \times H(k_n)(p_r)$ [Rot10, Proposition 4.42]. Therefore, H_n is isomorphic to the maximal p-quotient $H(k_n)_p := H(k_n)/(H(k_n)(p_2) \times \dots \times H(k_n)(p_r))$ of $H(k_n)$. Lastly, let L_n' be the maximal unramified Abelian extension of k_n (the Hilbert class field of k_n) and let L_n be the maximal unramified Abelian p-extension of k_n. It's a well-known fact the Artin map defined in section 6.2 induces an isomorphism

$$\phi_n' : \quad H(k_n) \longrightarrow \mathrm{Gal}(L_n'/k_n), \qquad \mathfrak{a} \longmapsto \sigma_\mathfrak{a},$$

where $\sigma_\mathfrak{a}$ is defined as in section 6.2 [Cox13, Theorem 5.23]. On the Sylow p-subgroup of $H(k_n)$ this is an isomorphism on the maximal unramified Abelian p-extension of k_n, i.e., for each n, we have $H_n := H(k_n)(p) \cong H(k_n)_p \cong \mathrm{Gal}(L_n'/k_n)_p \cong \mathrm{Gal}(L_n/k_n)$ through

$$\phi_n : \quad H_n \longrightarrow \mathrm{Gal}(L_n/k_n), \qquad \mathfrak{a} \longmapsto \sigma_\mathfrak{a},$$

where $H(k_n)_p$ and $\mathrm{Gal}(L'_n/k_n)_p$ denote the maximal p-quotients of $H(k_n)$ and $\mathrm{Gal}(L'_n/k_n)$, respectively. We want to define an arithmetic analogue H_∞ of $H_1(X_\infty)$. This has to be a profinite group and a natural choice is the inverse limit of the projective system $((H_n)_{n\geq 0}, (N_{n/m})_{n\geq m})$, where $N_{n/m} : H_n \to H_m$ is the norm map uniquely determined by $\mathfrak{q} \mapsto \mathfrak{p}^{[\mathcal{O}_{k_n}/\mathfrak{q}:\mathcal{O}_{k_m}/\mathfrak{p}]}$ on prime ideals $\mathfrak{q} \in \mathcal{O}_{k_n}$, where $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_{k_m}$. Hence we define $H_\infty := \varprojlim_n H_n$. Define $L_\infty := \bigcup_{n\geq 0} L_n$. The diagram

$$\begin{array}{ccc} H_n & \xrightarrow{\phi_n} & \mathrm{Gal}(L_n/k_n) \\ {\scriptstyle N_{n/m}}\downarrow & & \downarrow \\ H_m & \xrightarrow{\phi_m} & \mathrm{Gal}(L_m/k_m) \end{array}$$

commutes, so we have an isomorphism

$$\phi_\infty : \quad H_\infty \longrightarrow \mathrm{Gal}(L_\infty/k_\infty), \qquad (\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \ldots) \longmapsto \varinjlim_n \sigma_{\mathfrak{p}_n}$$

Since L'_n is the maximal unramified Abelian extension of k_n, we know that L'_n is a Galois extension of $\mathbb{Q}$ [Was97, p. 399], so $L_n/\mathbb{Q}$ is a Galois extension. We have $\#\mathrm{Gal}(L_n/k) = [L_n : \mathbb{Q}] = [L_n : k_n] \cdot [k_n : \mathbb{Q}]$, so $L_n/\mathbb{Q}$ is actually a p-extension. Therefore, $L_\infty/\mathbb{Q}$ is a pro-p Galois extension. We will now state the complete analogue of theorem 7.2.1. For a proof see [Mor12, Theorem 9.17].

Theorem 7.5.1. *Let l be a prime number and let*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\psi} H \longrightarrow 1$$

be a short exact sequence of profinite groups. Then we have an exact sequence of $\mathbb{Z}_l[[H]]$-modules

$$0 \longrightarrow N^{ab}(l) \xrightarrow{\theta_1} A_\psi \xrightarrow{\theta_2} \mathbb{Z}_l[[H]] \xrightarrow{\epsilon_{\mathbb{Z}_l[[H]]}} \mathbb{Z}_l \longrightarrow 0,$$

where $N^{ab}(l)$ is the maximal pro-l quotient of the abelianization N^{ab} of N. The homomorphism θ_1 is induced by $n \mapsto dn$ and θ_2 is the homomorphism induced by $dg \mapsto \psi(g) - 1$. This sequence is called the complete Crowell exact sequence.

We now introduce some more terminology.

Definition 7.5.2. *Let k be a finite algebraic number field and let S be a finite set of prime ideals of $\mathcal{O}_k$. Let $G := G_S(k) = \pi_1^{\text{ét}}(\mathrm{Spec}\,\mathcal{O}_k \setminus S)$ and let $H := (G_S(k))^{ab}$ be its abelianization with the canonical projection map $\psi : G \to H$. Define $N := \ker \psi$. We call A_ψ the* complete ψ-Alexander module *of S. When $H \cong \mathbb{Z}_l$ for some prime number l, we call the $\mathbb{Z}_l[[H]]$-module $N^{ab}(l)$ the* Iwasawa module.

We now apply the complete Crowell exact sequence to the short exact sequence

$$1 \longrightarrow N \longrightarrow \mathrm{Gal}(L_\infty/\mathbb{Q}) \xrightarrow{\psi} \mathrm{Gal}(k_\infty/\mathbb{Q}) \longrightarrow 1$$

to get

$$0 \longrightarrow N^{ab}(p) \longrightarrow A_\psi \longrightarrow \mathbb{Z}_p[[\mathrm{Gal}(k_\infty/\mathbb{Q})]] \longrightarrow \mathbb{Z}_p \longrightarrow 0.$$

Note that $N = \mathrm{Gal}(L_\infty/k_\infty) \cong H_\infty$ is an Abelian pro-p group, so we have $N^{ab}(p) \cong N(p) \cong N \cong \mathrm{Gal}(L_\infty/k_\infty) \cong H_\infty$. From now on, we will denote $\hat{\Lambda} := \mathbb{Z}_p[[T]]$ and we call $\hat{\Lambda}$ the *Iwasawa algebra*. By theorem 7.5.1, we have $A_\psi \cong N^{ab}(p) \oplus \hat{\Lambda}$ as $\hat{\Lambda}$-modules.

Much like the Alexander polonomial was an element of $\Lambda := \mathbb{Z}[t, t^{-1}]$ defined up to multiplication by $\Lambda^\times$, the Iwasawa polynomial will be defined as an element of $\hat{\Lambda}$ up to multiplication by $\hat{\Lambda}^\times$. The Iwasawa polynomial will be defined analogously to the characterization of the Alexander polynomial in section 7.3. For this, we will need a few algebraic lemmas concerning Weierstrass polynomials.

Definition 7.5.3. *Let l be a prime number. A polynomial $g(T) \in \mathbb{Z}_l[T]$ is called a* Weierstrass polynomial *if it is of the form*

$$g(T) = T^\lambda + c_1 T^{\lambda-1} + \ldots + c_\lambda, \qquad c_i \cong 0 \bmod p.$$

Lemma 7.5.4. *We have the following facts about Weierstrass polynomials.*

(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

$$f = qg + r, \qquad q \in \hat{\Lambda}, \quad r \in \mathbb{Z}_l[T], \quad \deg(r) \leq \lambda - 1.$$

(2) (p-adic Weierstrass Preparation Theorem) Any $f(T) \in \hat{\Lambda}$ with $f(T) \neq 0$ can be written uniquely in the form

$$f(T) = p^\mu g(T) u(T),$$

where $\mu \in \mathbb{Z}_{\geq 0}$, $g(T)$ is a Weierstrass polynomial and $u(T) \in \hat{\Lambda}^\times$. The integers μ and $\lambda = \deg(g)$ are called the μ-invariant *and the* λ-invariant *of f, respectively.*

For a proof of lemma 7.5.4(1), see [Was97, Proposition 7.2]. For a proof of lemma 7.5.4(2), see [Was97, Theorem 7.3].

Definition 7.5.5. *We call two $\hat{\Lambda}$-modules N and N'* pseudo-isomorphic, *notation $N \sim N'$, if there is a $\hat{\Lambda}$-homomorphism $\phi : N \to N'$ such that $\ker \phi$ and $\operatorname{coker} \phi$ are finite.*

Lemma 7.5.6. *Let N be a compact $\hat{\Lambda}-$module.*

(1) (Nakayama's lemma) The module N is a finitely generated $\hat{\Lambda}$-module if and only if $N/(p, T)N$ is finite.

(2) (Structure theorem for Iwasawa modules) Suppose N is a finitely generated $\hat{\Lambda}$-module. Then we have

$$N \sim \hat{\Lambda}^r \oplus \bigoplus_{i=1}^{s} \hat{\Lambda}/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \hat{\Lambda}(f_j^{e_j}),$$

where r is a non-negative integer, $m_i, e_j \in \mathbb{N}$ and f_j is an irreducible Weierstrass polynomial. The numbers r, m_i, e_j and the prime ideals (f_j) are uniquely determined by N.

For a proof of lemma 7.5.6(1), see [Was97, Lemma 13.16]. For a proof of lemma 7.5.6(2), see [NSW08, Theorem 5.3.8].

Now we can finally define the Iwasawa polynomial.

Definition 7.5.7. *Let N be a finitely generated, torsion $\hat{\Lambda}$-module. We have*

$$N \sim \bigoplus_{i=1}^{s} \hat{\Lambda}/(p^{m_i}) \oplus \bigoplus_{i=1}^{t} \hat{\Lambda}/(f_i^{e_i}).$$

The ideal generated by $f := \prod_{i=1}^{s} p^{m_i} \prod_{i=1}^{t} f_i^{e_i}$ is called the characteristic ideal *of N. The polynomial f is defined up to multiplication by $\hat{\Lambda}^\times$ and is called the* Iwasawa polynomial*.*

Before we can apply this to our $\hat{\Lambda}$-module H_∞, though, we need to know the following. For a proof, see [Mor12, proposition 11.10].

Proposition 7.5.8. *The $\hat{\Lambda}$-module H_∞ is finitely generated and torsion.*

It is known that if a $\hat{\Lambda}$-module N has no non-trivial finite $\hat{\Lambda}$-submodule, the characteristic ideal of N equals the 0-th fitting ideal $F_0(N)$ [Mor12, Example 9.18]. Hence its Iwasawa polynomial then equals $\Delta_0(N)$. In particular, the Iwasawa module for the short exact sequence $1 \to N \to \mathrm{Gal}(L_\infty/\mathbb{Q}) \to \mathrm{Gal}(k_\infty/\mathbb{Q}) \to 1$ is known to satisfy this condition since $\mathbb{Q}$ is totally real [Mor12, Example 9.18]. Furthermore, since the extension $L_\infty/\mathbb{Q}$ is a subextension of $\mathbb{Q}^{\mathrm{ur}_p}/\mathbb{Q}$ (where $\mathbb{Q}^{\mathrm{ur}_p}$ is the maximal Galois extension of $\mathbb{Q}$ unramified outside p), by the Galois correspondence for finite étale coverings we know that $\mathrm{Gal}(L_\infty/\mathbb{Q})$ is a quotient of the prime group $G_{\{p\}}$. This brings the analogy with knots full circle. If we could find a presentation of the group $\mathrm{Gal}(L_\infty/\mathbb{Q})$, then we could apply corollary 7.4.12 to compute the Iwasawa polynomial explicitly. Alas, much of the structure of $G_{\{p\}}$ and its quotients is still unknown.

7.6 *The Iwasawa polynomial as a characteristic polynomial*

Let k be a finite algebraic number field and let p be a prime. Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension of k and define $\hat{\Lambda} := \mathbb{Z}_p[[T]]$. Let γ be a topological generator of the Galois group of k_∞ over k. We have $\langle\gamma\rangle = \mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p$. It is known that $\gamma \mapsto 1 + T$ induces an isomorphism $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]] \cong \mathbb{Z}_p[[T]]$ [NSW08, Proposition 5.3.5]. Define $\hat{\Lambda}_{\mathbb{Q}_p} := \hat{\Lambda} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and note that $\hat{\Lambda}_{\mathbb{Q}_p} \cong \mathbb{Q}_p[[T]]$. By lemma 7.5.6 we have

$$H_\infty \sim \bigoplus_{i=1}^{s} \hat{\Lambda}/(p^{m_i}) \oplus \bigoplus_{i=1}^{t} \hat{\Lambda}/(f_i^{e_i}).$$

Let $f(T) = \prod_{i=1}^{s} p^{m_i} \prod_{i=1}^{t} f_i^{e_i} \in \hat{\Lambda}$ be the Iwasawa polynomial of H_∞. Analogous to theorem 7.3.1, we now have the following result.

Theorem 7.6.1. *Let $f(T) \in \hat{\Lambda}$ be the Iwasawa polynomial of H_∞. We have*

$$f(T) = \det(T \cdot \mathrm{id} - (\gamma - 1) \mid H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \bmod (\hat{\Lambda}_{\mathbb{Q}_p})^\times.$$

Proof. Note that $p^{m_i} \in \hat{\Lambda}_{\mathbb{Q}_p}^\times$, so tensoring with $\mathbb{Q}_p$ gives us

$$H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \sim \bigoplus_{i=1}^{t} \hat{\Lambda}_{\mathbb{Q}_p}/(f_i^{e_i}).$$

Since $\hat{\Lambda}_{\mathbb{Q}_p}$ is a principal ideal domain, the structure theorem for finitely generated modules over a principal ideal domain tells us that we have

$$H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{i=1}^{r} \hat{\Lambda}_{\mathbb{Q}_p}/(g_i),$$

where the (g_i) are primary ideals. In a PID this means that $(g_i) = ((g_i')^{e_i'})$ for some irreducible g_i'. By lemma 7.5.4(2) we can write $g_i' = p^{\mu_i} \cdot h_i \cdot u_i$, where h_i is a Weierstrass polynomial and $u \in \hat{\Lambda}_{\mathbb{Q}_p}^\times$. Therefore, we have $(g_i) = ((g_i')^{e_i'}) = (h_i^{e_i'})$ for every $1 \leq i \leq r$. Note that h_i' is irreducible as well. Therefore, we have

$$H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \sim \bigoplus_{i=1}^{r} \hat{\Lambda}/(h_i^{e_i'}).$$

Since the f_i and e_i are uniquely determined by $H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, we find $t = r$ and for every $1 \leq i \leq r$ we have $h_i = f_i$ and $e_i' = e_i$, so

$$H_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{i=1}^{t} \hat{\Lambda}_{\mathbb{Q}_p}/(f_i^{e_i}).$$

Since we have an isomorphism $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]] \cong \mathbb{Z}_p[[T]]$ induced by $\gamma \mapsto 1 + T$, we know that $\gamma - 1$ acts on $\bigoplus_{i=1}^{t} \hat{\Lambda}_{\mathbb{Q}_p}/(f_i^{e_i})$ through multiplication by T. Since we have $\hat{\Lambda}_{\mathbb{Q}_p}/(f_i^{e_i}) = \mathbb{Q}_p[[T]]/(f_i^{e_i}) \cong \mathbb{Q}_p[T]/(f_i^{e_i})$ [NSW08, Corollary 5.3.3], the rest of the proof is analogous to the proof of theorem 7.3.1. □

Bibliography

[Ada05] C.C. Adams. *The Knot Book. An Elementary Introduction to the Mathematical Theory of Knots*. Reprint of the 1994 original. Providence: American Mathematical Society, 2005.

[BZH13] G. Burde, H. Zieschang, and M. Heusener. *Knots*. 3rd ed. Vol. 5. De Gruyter Studies in Mathematics. Berlin: De Gruyter, 2013.

[CF63] R.H. Crowell and R.H. Fox. *Introduction to Knot Theory*. 1st ed. Vol. 57. Graduate Texts in Mathematics. New York: Springer, 1963.

[Cox13] D.A. Cox. *Primes of the form x^2+ny^2. Fermat, class field theory, and complex multiplication*. 2nd ed. Pure and Applied Mathematics. Hoboken: Wiley, 2013.

[Cro71] R.H. Crowell. "The Derived Module of a Homomorphism". In: *Advances in Mathematics* 6.2 (1971), pp. 210–238. URL: http://www.sciencedirect.com/science/article/pii/0001870871900168 (visited on 08/04/2017).

[Die10] T. tom Dieck. *Algebraic Topology*. Vol. 7. Textbooks in Mathematics. Corrected 2nd printing. Zürich: European Mathematical Society, 2010.

[Eis04] D. Eisenbud. *Commutative Algebra. with a View Toward Algebraic Geometry*. 1st ed. Vol. 150. Graduate Texts in Mathematics. New York: Springer, 2004.

[Ful95] W. Fulton. *Algebraic Topology. A First Course*. 1st ed. Vol. 153. Graduate Texts in Mathematics. New York: Springer, 1995.

[Kos80] C. Kosniowski. *A First Course in Algebraic Topology*. 1st ed. Cambridge: Cambridge University Press, 1980.

[Lan02] S. Lang. *Algebra*. 3rd ed. Vol. 211. Graduate Texts in Mathematics. New York: Springer, 2002.

[Lan94] S. Lang. *Algebraic Number Theory*. 2nd ed. Vol. 110. Graduate Texts in Mathematics. New York: Springer, 1994.

[Mar77] D.A. Marcus. *Number Fields*. 1st ed. Universitext. New York: Springer, 1977.

[Mor12] M. Morishita. *Knots and Primes. An Introduction to Arithmetic Topology*. 1st ed. Universitext. London: Springer, 2012.

[Mum99] D. Mumford. *The Red Book of Varieties and Schemes. Includes the Michigan Lectures (1974) on Curves and their Jacobians*. Vol. 1358. Lecture Notes in Mathematics. 2nd, expanded edition. Berlin: Springer, 1999.

[Neu99] J. Neukirch. *Algebraic Number Theory*. 1st ed. Vol. 322. Grundlehren der mathematischen Wissenschaften. Berlin: Springer, 1999.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. 2nd ed. Vol. 323. Grundlehren der mathematischen Wissenschaften. Berlin: Springer, 2008.

[Rol03] D. Rolfsen. *Knots and Links*. Reprint of the 1990 edition. Providence: American Mathematical Society, 2003.

[Rot10] J.J. Rotman. *Advanced Modern Algebra*. 2nd ed. Vol. 114. Graduate Studies in Mathematics. Providence: American Mathematical Society, 2010.

[Rot88] J.J. Rotman. *An Introduction to Algebraic Topology*. 1st ed. Vol. 119. Graduate Texts in Mathematics. New York: Springer, 1988.

[RZ10] L. Ribes and P. Zalesskii. *Profinite Groups*. 2nd ed. Vol. 40. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Berlin: Springer, 2010.

[Ser79] J.-P. Serre. *Local Fields*. 1st ed. Vol. 67. Graduate Texts in Mathematics. New York: Springer, 1979.

[Was97] L.C. Washington. *Introduction to Cyclotomic Fields*. 2nd ed. Vol. 83. Graduate Texts in Mathematics. New York: Springer, 1997.

[Wei06] S.H. Weintraub. *Galois Theory*. 1st ed. Universitext. New York: Springer, 2006.