Outer automorphisms of the absolute Galois group of local fields of mixed characteristic

Dissertation

zur Erlangung des Doktorgrades
der Naturwissenschaften

vorgelegt beim Fachbereich für Informatik und Mathematik
der Johann Wolfgang Goethe-Universität
in Frankfurt am Main

von

Theresa Kumpitsch
aus Bad Nauheim

Frankfurt (2022)

(D 30)

vom Fachbereich für Informatik und Mathematik der

Johann Wolfgang Goethe-Universität als Dissertation angenommen

Dekan:	Prof. Dr. Martin Möller
Gutachter:	Prof. Dr. Jakob Stix Prof. Dr. Annette Werner
Datum der Disputation:	17.10.2022

Contents

1 Introduction

1.1 Motivation

The ideas behind Galois theory were first introduced by Évarist Galois before his early death in a duel in 1832. The motivation was the study of roots of polynomial equation - an open question during that time being the existence of formulas for polynomials in degree 5 or higher merely involving algebraic operations and taking radicals. This question was settled by Abel in 1824. What Galois ultimately provided was a connection between the theory of field extensions and group theory. This is expressed in what we now refer to as the *fundamental theorem of Galois theory.*

In the past 200 years this has been generalized significantly. Galois theory is still a relevant area of of research in mathematics, regarding questions e.g. in algebra, geometry or number theory. Given a field K with some separable closure K^{sep}, one difficult problem is to describe the *absolute Galois group* $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ of K, which is the group of automorphisms of K^{sep} fixing K. This is a profinite group which can be expressed as the projective limit of Galois groups of finite Galois subextensions. It is a large and complicated group that one often studies by considering certain subgroups or quotients. One question is how much information about the base field this group contains. This is related to questions in geometry where one wants to extract information about a variety from its fundamental group.

In this thesis, we work in a number theoretic setting, while the problems being discussed are not really motivated by number theory. We assume that K is a p-adic local field, i.e. a finite extension of the p-adic numbers $\mathbb{Q}_p$ for some prime p. In what follows, we will mostly assume p to be odd.

The p-adic numbers are a very natural object to study. The famous theorem of Ostrowski states that up to equivalence, all absolute values on $\mathbb{Q}$ are either trivial, the usual absolute value, or the p-adic absolute value corresponding to some prime p. The p-adic numbers may be defined as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value, the same way the real numbers can be defined as the completion of $\mathbb{Q}$ with respect to the usual absolute value. But this is clearly not the main motivation of studying them. They are a powerful tool in number theory, algebraic geometry (and beyond). An important principle, or more of a philosophy, in number theory is the so-called *local-global* or *Hasse principle,* which states that when studying a problem over $\mathbb{Q}$, one should study it in $\mathbb{R}$ and $\mathbb{Q}_p$ – just like in geometry one studies global properties of certain geometric objects by studying local properties around a point.

In this thesis we set out to gain a better understanding of the *outer automorphism group* of the absolute Galois group Gal_K of K, which we denote by $\mathrm{Out}(\mathrm{Gal}_K)$. This is defined to be the group of equivalence classes of automorphisms of Gal_K as a profinite group up to inner automorphisms. So we are interested in those automorphisms not induced by conjugation by a group element. It is natural to study $\mathrm{Out}(\mathrm{Gal}_K)$ instead of the group of automorphisms $\mathrm{Aut}(\mathrm{Gal}_K)$. We can embed the group of field automorphisms of K, which we shall denote by $\mathrm{Aut}(K)$ and will often refer to as *geometric automorphisms*, into $\mathrm{Out}(\mathrm{Gal}_K)$. The induced automorphism on Gal_K of a geometric automorphism will only be well-defined up to inner automorphism of Gal_K, as it involves a choice of extension to a separable closure of K. This is as in topology, where a homeomorphism of a surface S defines an isomorphism of its fundamental group $\pi_1(S)$ up to inner automorphism. However, as we will explain later, this embedding is in general not surjective. In contrast, this holds for the case of number fields, which was proved by Neukirch and Uchida.

For us this is good news: Not only does $\mathrm{Out}(\mathrm{Gal}_K)$ appear to be a sufficiently interesting object, there are still plenty of things to understand about its structure. The subgroup of geometric automorphism $\mathrm{Aut}(K) \subseteq \mathrm{Out}(\mathrm{Gal}_K)$ has been studied by Mochizuki, Hoshi and others (see e.g. [Moc97], [HN20]) in the context of *anabelian geometry.* This field roughly aims to recover arithmetic and geometric information from the associated fundamental groups. Another automorphism, not induced by a geometric one, appears in the work of Jannsen and Wingberg [JW82]. It arises from the group presentation of Gal_K that is determined in this work. However, this is only a special case, and we will provide a way of studying many more automorphisms arising from the combinatorics of a given group presentation, and call this class of automorphisms *combinatorial automorphisms* of Gal_K.

The previous results are at the core of the present thesis. We provide more detail in the subsequent sections.

Anabelian results for p-adic local fields

Let K be a p-adic number field. It is well-known that the map

$$\mathrm{Aut}(K) \hookrightarrow \mathrm{Out}(\mathrm{Gal}_K), \qquad \alpha \mapsto \overline{\alpha} \circ \sigma \circ \overline{\alpha}^{-1}, \tag{$*$}$$

where $\overline{\alpha}$ is an extension of $\alpha \in \mathrm{Aut}(K)$ to an algebraic closure $\overline{K}$, is injective; see Section 3.2.

Definition. The *group of geometric automorphisms* of Gal_K is the image of $\mathrm{Aut}(K)$ in $\mathrm{Out}(\mathrm{Gal}_K)$ under the emdedding $(*)$. We denote this by $\mathrm{Aut}(K)$ as well.

There is an equivalent description of the group of geometric automorphisms. Let

$$\mathrm{Out}_{\mathrm{filt}}(\mathrm{Gal}_K)$$

denote the set of outer automorphisms of Gal_K compatible with the filtration given by the higher (i.e. with index > 0) ramification groups in the upper numbering. A special case of Mochizuki's anabelian result on p-adic local fields, see [Moc97], can be stated as follows.

Theorem (Mochizuki)**.** *The map $(*)$ induces an isomorphism*

$$\mathrm{Aut}(K) \xrightarrow{\sim} \mathrm{Out}_{\mathrm{filt}}(\mathrm{Gal}_K).$$

The study of $\mathrm{Aut}(K)$ in $\mathrm{Out}(\mathrm{Gal}_K)$ is of great interest from an "anabelian perspective". An important result in this direction due to [HN20] states that under certain conditions of K, the set of conjugates of the image of $(*)$ in the group of outer automorphisms $\mathrm{Out}(\mathrm{Gal}_K)$ is infinite, implying it is not a normal subgroup. Hoshi and Nishio then claim that one may conclude it is impossible to establish a functorial group-theoretic reconstruction of Gal_K from the image of $\mathrm{Aut}(K)$ under $(*)$. In the proof of the main result, the authors use that there exist outer automorphisms of Gal_K coming from the combinatorics of the group presentation provided in the works of Jannsen and Wingberg. In fact, they use the same simple combinatorial isomorphism as in [JW82]. We shall recall this crucial result, as it plays a large role in this thesis as well.

The Jannsen–Wingberg presentation and combinatorial automorphisms

In a series of papers ([Jan82], [Win82], [JW82]) Jannsen and Wingberg show that Gal_K is topologically finitely generated, and give a description in terms of generators and relations, but not a finite presentation of Gal_K as a profinite group. Important previous work is done by Koch in [Koc65], who gives a description of the maximal extension of K without tame ramification. Furthermore, in [Koc78] Koch provides a cohomological characterization of the absolute Galois group that plays a central role in the work of Jannsen and Wingberg. Previously, Gal_K had also been expressed in terms of generators and relations in [Jak68] by Jakovlev. However, that work includes errors which are only partly corrected in [Jak78]. The case $p = 2$ was settled by Diekert in [Die84] for K containing the fourth roots of unity. In this thesis we will mostly assume $p \neq 2$ and comment on whenever the statements for $p = 2$ also hold. Furthermore, we make an additional restriction which greatly simplifies the "wild" relation given in the Jannsen–Wingberg presentation. Namely, we assume that K contains the pth roots of unity μ_p.

Their description depends on some invariants of K. Let $N = [K : \mathbb{Q}_p]$ denote the degree of $K/\mathbb{Q}_p$, and let q denote the cardinality of the residue field of K. By K^{tr} we denote the maximal tame extension of K. It is a well-known result due to Iwasawa that the Galois group $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ is generated by two elements σ and τ satisfying $\sigma\tau\sigma^{-1} = \tau^q$, where σ is a lift of Frobenius and τ denotes a generator of its inertia subgroup. Let p^s be the order of the group $\mu_{\mathrm{tr}} = \mu_{p^\infty}(K^{\mathrm{tr}})$ of all p-power roots of unity in K^{tr}/K. Let $\alpha\colon \mathrm{Gal}(K^{\mathrm{tr}}/K) \to (\mathbb{Z}/p^s\mathbb{Z})^\times$ be the cyclotomic character given by $\rho(\zeta) = \zeta^{\alpha(\rho)}$ for $\rho \in \mathrm{Gal}(K^{\mathrm{tr}}/K)$ and $\zeta \in \mu_{\mathrm{tr}}$. We choose $g, h \in \mathbb{Z}_p$ such that

$$g \equiv \alpha(\sigma), \quad h \equiv \alpha(\tau) \bmod p^s.$$

Note that if $\mu_p \subseteq K$, we may choose $h = 1$.

In the following we denote the commutator $xyx^{-1}y^{-1}$ by $[x, y]$.

Theorem (Jannsen–Wingberg–Diekert). *If $p \neq 2$, we assume that $\mu_p \subseteq K$. If $p = 2$, we assume $\mu_4 \subseteq K$. The group Gal_K is isomorphic to the profinite group generated by $N + 3$ generators $\sigma, \tau, x_0, \ldots, x_N$, subject to the following conditions.*

(i) The closed normal subgroup topologically generated by $x_0, \ldots, x_N$ is a pro-p group.

(ii) The elements σ, τ satisfy the "tame" relation

$$\sigma\tau\sigma^{-1} = \tau^q.$$

(iii) The generators satisfy a further "wild" relation

$$\sigma x_0 \sigma^{-1} = ((x_0\tau)^\pi)^g x_1^{p^s} [x_1, x_2] [x_3, x_4] \cdots [x_{N-1}, x_N],$$

where $\pi = \pi_p$ is the unique idempotent element of $\widehat{\mathbb{Z}}$ with $\pi\hat{\mathbb{Z}} = \mathbb{Z}_p$.

Note that this result implies that Gal_K is finitely generated but not that it is finitely presentable as this is not a finite presentation of Gal_K. The way it is stated, it is not a presentation at all. However, one can express condition (i) as infinitely many profinite words. While we do not know a way of turning the above result into a finite presentation of Gal_K, in Theorem 3.2.16 we show that Gal_K is in fact finitely presentable. This is based on work by Lubotzky [Lub01].

In the last chapter of this thesis we try to use the combinatorial structure of the above description to generate automorphisms of Gal_K in the case $N = [K : \mathbb{Q}_p] > 1$.

The automorphism that has so far been used to show that $\mathrm{Out}(\mathrm{Gal}_K)$ is non-trivial is constructed as follows. We will refer to it as the *Jannsen–Wingberg automorphism* of Gal_K and denote it by ψ^{JW}. We consider the generators $\sigma, \tau, x_0, \dots, x_N$ on Gal_K satisfying the relations given in the above theorem. Let $F = \widehat{F}_{\{\sigma,\tau,x_0,\dots,x_N\}}$ denote the free profinite group in these generators. We define an automorphism $\psi\colon F \to F$ as

$$\psi(y) = \begin{cases} y, & \text{for } y = \sigma, \tau, x_0, \dots, x_{N-1}, \\ x_N \cdot x_{N-1}, & \text{for } y = x_N. \end{cases}$$

Since

$$[x_{N-1}, x_N] = x_{N-1}x_N x_{N-1}^{-1} x_N^{-1} = x_{N-1}x_N x_{N-1} x_{N-1}^{-1}(x_N x_{N-1})^{-1} = [x_{N-1}, x_N x_{N-1}],$$

the generators $\sigma, \tau, x_0, \dots, x_{N-1}, x_N \cdot x_{N-1}$ also satisfy the relations given in above theorem. Hence, this induces an automorphism of Gal_K

$$\begin{tikzcd} F \arrow[r, "\psi", "\cong"'] \arrow[d, two heads, "p"] & F \arrow[d, two heads, "p"] \\ \mathrm{Gal}_K \arrow[r, dashed, "\psi^{\mathrm{JW}}", "\cong"'] & \mathrm{Gal}_K . \end{tikzcd}$$

The map ψ^{JW} is not an inner automorphism, as it is not trivial on the abelianization of Gal_K, and one can also show that it does not come from a geometric automorphism, as its image on the abelianization has infinite order (see Section 3.2.2).

This result leads us to further exploration of what we call *combinatorial automorphisms.* The idea behind this is essentially the following: Any choice of generators for a presentation of a group induces an automorphism of that group. Assuming that K contains pth roots of unity the maximal pro-p quotient $\mathrm{Gal}_K(p)$ of Gal_K is a *Demuškin group*, i.e. a one-relator pro-p group admitting a particular nice presentation. A large part of this thesis is dedicated to providing further insight into the structure of automorphisms of these groups, following ideas used in the well-known classification result due to Demuškin, Serre, and Labute. Essentially, the automorphisms on the abelian level up to torsion that lift a step along a suitable filtration are controlled by the cup product and Bockstein homomorphism. The properties of Demuškin groups ensure that we can modify such an automorphism to lift it further along the filtration in a compatible way. We give an explicit description of the obstructions to such lifts and show that for such a group G the group of $\mathrm{Aut}(G)$ is an extension of an explicitly given subgroup of a maximal parabolic group of the general symplectic group with values in a specific finite quotient Λ of $\mathbb{Z}_p$ by a pro-p group, see Theorem 6.3.2. This result may be viewed as an analogue to the *symplectic representation* of the mapping class group of a closed surface $S = S_g$.

We then use results on the mapping class group to produce a large subgroup of the group of outer automorphisms $\operatorname{Out}(G)$. We even give some explicit formulas in terms of generators. Finally, in the arithmetic case, we can adapt the previous results to generate a large subgroup of $\operatorname{Out}(\operatorname{Gal}_K)$, and give a new interpretation of the Jannsen–Wingberg automorphism.

In some more detail, this thesis is structured as described below.

1.2 Outline and statements of the main results

In Chapter 2 we provide some preliminaries, recall some facts on profinite, in particular pro-p groups, group cohomology, and presentations of profinite groups. We also briefly discuss automorphisms of group extensions, and show that for finitely generated profinite groups, the group of automorphisms is a profinite group.

In Chapter 3 we recall some structure results on the arithmetic of a p-adic local field as well as some well-known reconstruction algorithms for its invariants. We also state some results on the group of geometric automorphisms $\operatorname{Aut}(K)$ in $\operatorname{Out}(\operatorname{Gal}_K)$. Furthermore, we state the theorem of Jannsen and Wingberg in full generality, as well as the theorem of Diekert for the case $p = 2$. As sketched above, we use the Jannsen–Wingberg automorphism in the case $N = [K : \mathbb{Q}_p] > 1$ to prove the following result.

Proposition (Jannsen–Wingberg, cf. Proposition 3.2.2)**.** *Let $p \neq 2$ be a prime and let $K/\mathbb{Q}_p$ be a finite extension. Then $\operatorname{Out}(\operatorname{Gal}_K)$ is non-trivial. Moreover, there exists a non-inner automorphism of Gal_K which does not arise from any automorphism of the field K.*

We show that Gal_K is finitely presentable. We are not aware of this statement in the literature and it does not follow from the previously mentioned results by Jannsen–Wingberg.

Theorem (Cf. Theorem 3.2.16)**.** *The absolute Galois group of a p-adic local field K is finitely presentable. If $p \neq 2$ and $\mu_p \subseteq K$, there exists a profinite presentation with $N + 2$ generators and $N + 1$ relations. This is the minimal number of generators and relations, respectively.*

In Chapter 4 we study the induced automorphisms of geometric automorphisms on certain characteristic quotients of Gal_K. Recall that Gal_K has a filtration

$$V_K \subseteq I_K \subseteq \operatorname{Gal}_K,$$

where I_K denotes the inertia group and V_K denotes the wild inertia group of K. The quotient

$$\operatorname{Gal}_K / I_K = \operatorname{Gal}(K^{\mathrm{nr}}/K) \cong \operatorname{Gal}_{\mathbb{F}_q} \cong \widehat{\mathbb{Z}}$$

is the maximal unramified quotient of Gal_K. We show that all automorphisms of Gal_K induce the identity on $\operatorname{Gal}(K^{\mathrm{nr}}/K)$, see Lemma 4.1.1. We can identify the Iwasawa group $\mathrm{Iw}_q = \widehat{\mathbb{Z}}'(1) \rtimes_q \widehat{\mathbb{Z}}$ with the maximal tamely ramified quotient $\operatorname{Gal}(K^{\mathrm{tr}}/K)$. Setting $\mathrm{Iw}_q^{\mathrm{nr}} = \mathrm{Iw}_q^{\mathrm{ab}}/\mathrm{tors}$ and $\mathrm{Iw}_q^{\mathrm{tr}} = \ker(\mathrm{Iw}_q \to \mathrm{Iw}_q^{\mathrm{nr}})$, we show (by essentially the same argument as before), that any automorphism φ of Iw_q induces the identity on $\mathrm{Iw}_q^{\mathrm{nr}}$ and some automorphism φ^{tr} on $\mathrm{Iw}_q^{\mathrm{tr}}$. By a result of Wells [Wel71] (see also Section 2.5.2), the kernel $\operatorname{Out}_0(\mathrm{Iw}_q)$ of

$$\operatorname{Out}(\mathrm{Iw}_q) \to \operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{tr}})/\operatorname{Inn}(\mathrm{Iw}_q) \cong (\widehat{\mathbb{Z}}')^{\times}/q^{\widehat{\mathbb{Z}}}$$

is given by

$$\mathrm{Out}_0(\mathrm{Iw}_q) = H^1(\mathrm{Iw}_q^{\mathrm{nr}}, \mathrm{Iw}_q^{\mathrm{tr}}) \cong \mathbb{F}_q^{\times}.$$

Now let K_0 denote the maximal unramified subextension of $K/\mathbb{Q}_p$, and let K_1 denote the maximal tamely ramified subextension of $K/\mathbb{Q}_p$. The two main results of Chapter 4 are the following.

Theorem (Cf. Theorem 4.2.8)**.** *The subgroup of* $\mathrm{Aut}(K)$ *mapping to* $\mathrm{Out}_0(\mathrm{Iw}_q)$ *under*

$$\mathrm{Aut}(K) \hookrightarrow \mathrm{Out}(\mathrm{Gal}_K) \to \mathrm{Out}(\mathrm{Gal}(K^{\mathrm{tr}}/K)) = \mathrm{Out}(\mathrm{Iw}_q)$$

is $\mathrm{Aut}(K/K_0)$*.*

Theorem 1.2.1 (Cf. Theorem 4.2.9)**.** *We have*

$$\ker(\mathrm{Aut}(K/K_0) \to \mathrm{Out}_0(\mathrm{Iw}_q)) = \mathrm{Aut}(K/K_1).$$

Hence, the subgroup of $\mathrm{Aut}(K)$ *inducing the identity in* $\mathrm{Out}(\mathrm{Iw}_q)$ *is* $\mathrm{Aut}(K/K_1)$*.*

In Chapter 5 we turn our attention to finitely generated pro-p groups. For a finitely generated pro p-group G, we define the invariant $n = n(G)$ as

$$n = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p),$$

which is the minimal number of generators of G. We define the invariant $\Lambda = \Lambda(G)$ as the maximal quotient $\mathbb{Z}_p \twoheadrightarrow \Lambda$ such that $G^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} \Lambda$ is a free Λ-module of rank n. In particular, if G^{ab} has a nontrivial torsion subgroup, then $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$ for some power $q = q(G)$ of p, otherwise $\Lambda = \mathbb{Z}_p$. In this case, we set $q(G) = 0$.

There are a few natural filtrations to consider when studying finitely generated pro-p groups. For q a power of p, the *descending q-central series* of G is the filtration $C_q^{\bullet}G$ defined by

$$C_q^1 G = G, \quad C_q^{i+1} G = \left(C_q^i G\right)^q \left[C_q^i G, G\right],$$

where $\left[C_q^i G, G\right]$ denotes the closed subgroup topologically generated by commutators $[x, y]$ for $x \in C_q^i G, y \in G$. When $q = q(G)$, we also call this the *the descending Λ-central series*, or just *Λ-filtration*, where for $q(G) = 0$ we consider the usual descending central series. We denote this by $C^{\bullet}G = C_{\Lambda}^{\bullet}G$.

We recall a central result in the study of finitely generated pro-p groups, which states that $\rho \in C^2F$ up to C^3F is determined by the cup product, and the Bockstein homomorphism if $q \neq 0$, see Proposition 5.1.12. Eventually, we turn our attention to a special class of pro-p groups defined as follows.

Definition. A pro-p group G is called a *Demuškin group* if its cohomology has the following properties:

(i) $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,

(ii) $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$,

(iii) the cup-product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is non-degenerate.

Thus, if such a group G is a finitely generated topological group with minimal number of generators $n = n(G) = \dim H^1(G, \mathbb{F}_p)$, (ii) implies the existence of a presentation $G = F/\langle\langle \rho \rangle\rangle$. Here, F is a free pro-p group of rank n and $\langle\langle \rho \rangle\rangle$ denotes the normal subgroup of F generated by some $\rho \in F^p[F,F]$. We also refer to $n = n(G)$ as the rank of G. Recall the following structure result about Demuškin groups.

Theorem (Demuškin)**.** *Let G be a one-relator pro-p group. Suppose that the invariant q of G is different from 2. Then G is a Demuškin group if and only if it is isomorphic to the pro-p group defined by n generators $x_1, \dots, x_n$ subject to the one relation*

$$x_1^q [x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n] = 1.$$

In particular, G is determined by the two invariants n and q up to isomorphism.

The full classification of Demuškin groups, including the case $q = 2$, was settled by Labute in [Lab67]. In this section we recall the proof of the above result, as we will use some of the central ideas in Chapter 6. However, we will mostly assume $p \neq 2$.

The most important example of this thesis is stated in the following result:

Theorem (Structure of the maximal pro-p quotient of Gal_K)**.** *Let p be a prime and let K be a p-adic local field of degree $N = [K : \mathbb{Q}_p]$.*

(i) If $\mu_p \nsubseteq K$, then $\mathrm{Gal}_K(p)$ is a free pro-p group of rank $N + 1$.

(ii) If $\mu_p \subseteq K$, then $\mathrm{Gal}_K(p)$ is a Demuškin group of rank $N + 2$. Furthermore,

$$q(\mathrm{Gal}_K(p)) = p^t := \#\mu_{p^\infty}(K).$$

Hence, in this case, if $p^t > 2$, then $\mathrm{Gal}_K(p)$ is isomorphic to the pro-p group defined by $N + 2$ generators $y_1, \dots, y_{N+2}$, subject to the relation

$$y_1^{p^t} [y_1, y_2][y_3, y_4] \cdots [y_{N+1}, y_{N+2}] = 1.$$

Another important example arising from algebraic geometry, which will play a big role in the last chapter, is the following.

Example. Let $G = \pi_1(S)$ be the fundamental group of a compact orientable surface S of genus g with $g \geq 1$. Then the pro-p completion $G^{\wedge p}$ is a Demuškin group of rank $2g$ with $q(G) = 0$.

In Chapter 6 we gain better understanding of the automorphism group of Demuškin groups, and finitely generated pro-p groups in general. Given such a group G with minimal presentation

$$1 \to R \to F \to G \to 1$$

with the previous choice of Λ, the Λ-modules $G/C^2G = G^{\mathrm{ab}} \otimes \Lambda$ and $F/C^2F = F^{\mathrm{ab}} \otimes \Lambda$ are isomorphic. On this level we have an easy description of the automorphisms group, since after choosing a basis, this is just $\mathrm{GL}_n(\Lambda)$. We ask which of these automorphisms lift to an automorphism of G. We introduce the following notation.

Definition. Let G, H be finitely generated pro-p groups. Let $\Lambda = \Lambda(G)$ and let $C^\bullet(-)$ denote the Λ-filtration. For every $m \geq 2$ we call a morphism $\varphi_m \colon G \to H/C^m H$ *k-liftable*, if there exists a morphism $\varphi_{m+k} \colon G \to H/C^{m+k}H$ such that $\varphi_{m+k} \equiv \varphi_m \bmod C^m H$. In this case, we call φ_{m+k} a k-lift of φ_m.

We denote the subset of k-liftable morphisms as

$$\mathrm{Hom}^{(+k)}(G, H/C^m H) \subseteq \mathrm{Hom}(G, H/C^m H).$$

If we only consider surjective morphisms $G \to H/C^m H$, we denote the subset of surjective k-liftable morphisms as

$$\mathrm{Hom}^{(+k)}(G, H/C^m H)_{\mathrm{surj}} \subseteq \mathrm{Hom}(G, H/C^m H)_{\mathrm{surj}}.$$

In the case $G = H$ we set

$$\mathrm{Aut}^{(+k)}(G/C^m G) := \mathrm{Hom}^{(+k)}(G, G/C^m G)_{\mathrm{surj}}.$$

We answer the question under what conditions a morphism $\varphi_m \colon G \to H/C^m H$ is liftable to a morphism $\varphi \colon G \to H$ step by step, as $H = \varprojlim_m H/C^m H$, with index set $(\mathbb{N}, \leq)$, starting with $m = 2$. In this case, we can give an answer for finitely generated pro-p groups G. The following result gives a cohomological condition in terms of compatibility with cup products and Bockstein homomorphisms. For simplicity, we state the result when $G = H$ is a Demuškin group here, a more general result can be found in Section 6.1.

Theorem (Cf. Theorem 6.1.2)**.** *Let G be a Demuškin group, and let $\varphi_2 \colon G \to G/C^2 G = G^{\mathrm{ab}} \otimes \Lambda$ be a morphism of pro-p groups. Then the following are equivalent.*

(a) The morphism φ_2 is 1-liftable.

(b) There exists a homomorphism $H^2(G, \Lambda) \to H^2(G, \Lambda)$ compatible with cup products and, if $q \neq 0$, Bockstein homomorphisms.

This allows us to give a dual description of $\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda)$. We may identify $H^2(G, \Lambda) \cong \Lambda$. The cup product induces a symplectic pairing

$$- \cup - \colon H^1(G, \Lambda) \times H^1(G, \Lambda) \to \Lambda$$

and, if $q \neq 0$, the Bockstein homomorphism induces a Λ-linear form

$$\beta \colon H^1(G, \Lambda) \to \Lambda.$$

If $q \neq 0$ we define

$$\mathrm{Aut}^{(-\cup-,\beta)}(H^1(G, \Lambda)) := \{(A, \lambda) \mid A^*(- \cup -) = \lambda(- \cup -), A^*\beta = \lambda\beta\}$$

to be the group of automorphisms of the free Λ-module $H^1(G, \Lambda)$ respecting the symplectic structure on $H^1(G, \Lambda)$, and the Bockstein homomorphism β up to a factor λ. Hence, after choosing a symplectic basis, we may view this as a subgroup of (the Λ-valued points of) the general symplectic group

$$\underline{\mathrm{GSp}}(H^1(G, \Lambda))(\Lambda) = \mathrm{GSp}_n(\Lambda).$$

If $q \neq 0$, this yields an isomorphism

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda))$$

and for $q = 0$ it holds that

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \mathbb{Z}_p) \cong \mathrm{GSp}_n(\mathbb{Z}_p).$$

The choice of generators $x_1, \dots, x_n$ in the Theorem of Demuškin yields a basis $\overline{x_1}, \dots, \overline{x_n}$ of the free Λ-module $G^{\mathrm{ab}} \otimes \Lambda$, dual to a Λ-basis $\chi_1, \dots, \chi_n$ of $H^1(G,\Lambda)$ with $\beta(\chi_i) = \delta_{i1}$, which is symplectic with respect to the cup-product. In particular, we have a filtration of $H^1(G,\Lambda)$ given by the isotropic subspace $\ker\beta^{\perp}$, i.e.

$$(0) \subset \ker\beta^{\perp} \subset \ker\beta \subset H^1(G,\Lambda),$$

where we choose our basis elements $\chi_1, \dots, \chi_n$ such that

$$\ker(\beta)^{\perp} = \langle \chi_2 \rangle \quad \text{and} \quad \ker(\beta) = \langle \chi_2, \dots, \chi_n \rangle\,.$$

In particular, $M' = \ker(\beta)/\ker(\beta)^{\perp}$ has a Λ-basis given by the images of $\chi_3, \dots, \chi_n$, and the image of χ_1 spans $\beta(M) = M/\ker(\beta)$. One immediately sees that $\mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda))$ is a subgroup of the maximal parabolic subgroup $P_{\ker\beta^{\perp}}(M)(\Lambda)$ corresponding to $\ker\beta^{\perp}$.

Proposition (Cf. Proposition 6.1.5)**.** *Rearranging the previous basis as* $(\chi_2, \chi_3, \dots, \chi_n, \chi_1)$ *we may identify* $\mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda))$ *with the subgroup of* $\mathrm{GSp}_n(\Lambda)$ *of the form*

$$\left\{ \left(\begin{array}{c|c|c} 1 & * \quad \cdots \quad * & * \\ \hline & & * \\ & \underline{\mathrm{GSp}}^{(\lambda)}(M')(\Lambda) & \vdots \\ & & * \\ \hline & & \lambda \end{array} \right) \;\middle|\; \lambda \in \Lambda^{\times} \right\}$$

where $\underline{\mathrm{GSp}}^{(\lambda)}(M')(\Lambda)$ *denotes the subset of* $\underline{\mathrm{GSp}}(M')(\Lambda)$ *with factor of similitude equal to* λ*.*

For $m \geq 3$ we then show that a surjective morphism $\varphi_m \colon G \to H/C^mH$ always admits a (special kind of) lift. We note that now assuming that G is a Demuškin group is crucial in our proof.

Theorem (Cf. Theorem 6.2.5)**.** *Let G be a Demuškin group. Let $m \geq 3$, and let H be a finitely generated pro-p group. Let $\varphi_m \colon G \to H/C^mH$ be a surjective morphism. There exists a lift $\varphi_{m+1} \colon G \to H/C^{m+1}H$ of φ_m such that $\varphi_{m+1} \equiv \varphi_m \bmod C^{m-1}H$.*

By a standard limit argument there exists a morphism $\varphi \colon G \twoheadrightarrow H$ such that $\varphi \equiv \varphi_m \bmod C^mH$. In particular, for $H = G$ we see that $(\mathrm{Aut}^{(+1)}(G/C^mG))_{m\geq 2}$ is a surjective system for $\mathrm{Aut}(G)$, i.e.

$$\mathrm{Aut}(G) \cong \varprojlim_m \mathrm{Aut}^{(+1)}(G/C^mG).$$

Finally, we conclude the chapter with the following result on the structure of $\mathrm{Out}(G)$.

Theorem (Cf. Theorem 6.3.2)**.** *There is a continuous surjective group homomorphism*

$$\mathrm{Out}(G) \twoheadrightarrow \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda)),$$

whose kernel is a pro-p group.

We view this as an analogue to the symplectic representation of the mapping class group of a surface S.

In Chapter 7 we provide a general framework to study automorphisms of a group arising from a given presentation, inspired by the Jannsen–Wingberg automorphism of Gal_K.

For a discrete free group F in $x_1, \ldots, x_n$ and $S \subseteq F$, we denote by

$$\mathrm{Aut}^{(S)}(F) = \{\varphi \colon F \to F \text{ automorphism} \mid \varphi(\rho) = \rho \text{ for all } \rho \in S\}$$

the subgroup of $\mathrm{Aut}(F)$ fixing all $\rho \in S$.

Let $X = \{x_i\}_{i \in I}$ and $Y = \{y_j\}_{j \in J}$ denote disjoint sets of letters. Let $R \subseteq F_{X \cup Y}$ denote a system of relations. We shall assume that for all relations $\rho \in R$ we have

$$\rho = \rho_X \cdot \rho_Y$$

where $\rho_X \in F_X$ and $\rho_Y \in F_Y$, as this is the case in the examples that we are interested in. Assume we are given a group G_{discr} in the presentation

$$G_{\mathrm{discr}} = \langle X \cup Y | R \rangle$$

and set $S = \{\rho_Y | \rho \in R\}$.

Any automorphism of the free group F_Y in Y fixing the relations S can be extended to an automorphism of $F_{X \cup Y}$ as the identity on the generators in X, which will then also fix all relations in R. Such an automorphism induces an automorphism of G_{discr} by the universal property of the cokernel. Previous construction allows us to define a map

$$\mathcal{K}^{(S)}_{\mathrm{discr}} \colon \mathrm{Aut}^{(S)}(F_Y) \to \mathrm{Aut}(G_{\mathrm{discr}}),$$

which we call the *discrete combinatorial automorphism map* for a set of relations S.

We then want to use this construction to find large subgroups of automorphisms of the outer automorphism group of Demuškin groups, and the absolute Galois group Gal_K. We use the fact that a Demuškin group G, in a sense, is very similar to a surface group, i.e. the fundamental group of a surface. This is reflected in its standard presentation, where the product of commutators appearing in the single defining relation comes from the symplectic structure of $H^1(G, \Lambda)$. A lot of things are known about the outer automorphism group of surface groups through the study of the mapping class group.

Let $S = S_g$ be a closed orientable surface of genus g. We choose the standard presentation of its fundamental group, i.e.

$$\pi_1(S) = \langle a_1, b_1, \ldots, a_g, b_g | \delta = 1 \rangle$$

with $\delta = [a_1, b_1] \ldots [a_g, b_g]$. In Section 7.2 we recall results on the mapping class group $\mathrm{Mod}(S)$ of S, which is defined as the group of isotopy classes of orientation-preserving diffeomorphisms $S \to S$. In particular, it is known to be finitely generated, see Theorem 7.2.8. We consider the set of *Lickorish generators* of $\mathrm{Mod}(S)$, which are Dehn twists at finitely many simple closed curves on S. We show that we can lift these Dehn twists T_c to automorphisms of the free group in the generators $a_1, b_1, \ldots, a_g, b_g$, which turn out to fix δ.

Definition. We call the subgroup of $\mathrm{Aut}^{(\delta)}(F)$ generated by the lifts of Lickorish generators of $\mathrm{Mod}(S)$ the *group of combinatorial Dehn twists on F*, and denote this group by $\mathrm{Dehn}(S)$.

In particular, we have a surjective group homomorphism

$$\mathrm{Dehn}(S) \twoheadrightarrow \mathrm{Sp}(H^1(S,\mathbb{Z})) \cong \mathrm{Sp}_{2g}(\mathbb{Z}),$$

which is an isomorphism for $g = 1$.

In Section 7.4 we assume $p \neq 2$ and consider a p-Demuškin group G. Let $q = q(G)$ as before. By Theorem of Demuškin, we know that G is isomorphic to the pro-p group defined by n generators $y_1, \dots, y_n$ subject to the one relation

$$y_1^q[y_1,y_2][y_3,y_4]\cdots[y_{n-1},y_n] = 1.$$

We denote by G_{discr} the discrete group given by this presentation. In particular, G is isomorphic to the pro-p completion of G_{discr}. Furthermore, we assume $n \geq 4$ and set $m = n-2$ if $q \neq 0$ and we assume $n \geq 2$ and set $m = n$ if $q = 0$. We choose a surface $S = S_g$ such that $2g = m$. Now in the previous discussion, the choice of presentation of $\pi_1(S)$ with generators $a_1, b_1, \dots, a_g, b_g$ corresponds to the choice of a symplectic $\mathbb{Z}$-basis of $H^1(S,\mathbb{Z})$. Considering the (discrete) free group F in the generators $a_1, b_1, \dots, a_g, b_g$, we get a map $F \to G_{\mathrm{discr}}$ by mapping

$$a_1 \mapsto x_3, \quad b_1 \mapsto x_4, \quad \dots \quad a_g \mapsto x_{n-1}, \quad b_g \mapsto x_n.$$

Furthermore, we may define a *pro-p combinatorial automorphism map* for the relation δ as the composition

$$\mathcal{K}^{(\delta)}_{\text{pro-}p}\colon \mathrm{Aut}^{(\delta)}(F) \xrightarrow{\mathcal{K}^{(\delta)}_{\mathrm{discr}}} \mathrm{Aut}(G_{\mathrm{discr}}) \xrightarrow{(-)^{\wedge p}} \mathrm{Aut}(G).$$

This allows us to write down a lot of concrete examples of automorphisms of a Demuškin groups that not only come from the combinatorics of the group presentation, but also have a geometric interpretation. We can even argue that we have found a large subgroup of $\mathrm{Out}(G)$, as we can show the following.

Theorem (Cf. Theorem 7.4.2)**.** *The subgroup $\mathcal{K}^{(\delta)}_{\text{pro-}p}(\mathrm{Dehn}(S))$ in $\mathrm{Out}(G)$ has dense image in $\mathrm{Sp}_m(\mathbb{Z}_p)$.*

In Section 7.5 we want to generate a large subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$ using these ideas. We assume the field K to be a finite extension of $\mathbb{Q}_p$ of degree N containing the pth roots of unity when $p \neq 2$ and assuming $\sqrt{-1} \in K$ (i.e. $\mu_4 \subseteq K$) when $p = 2$. As before let $p^s = \#\mu_{\mathrm{tr}}$.

In order to work with combinatorial Dehn twists, we need to write down a suitable discrete group G and a suitable completion with respect to some property $\mathcal{P}$ on open normal subgroups of G. This needs to be chosen such that $G^{\wedge\mathcal{P}} \cong \mathrm{Gal}_K$, and such that the combinatorial automorphism map respects the condition $\mathcal{P}$.

Rewriting conditions (i) and (iii) from the Theorem of Jannsen–Wingberg–Diekert yields the following choice of discrete group.

Definition. The *discrete Jannsen–Wingberg group* JW is the group given by the presentation

$$\left\langle \sigma, \tau, x_0, \dots, x_N, y, z \;\middle|\; \begin{array}{c} \sigma\tau\sigma^{-1} = \tau^q \\ (x_0\tau)^g = yz \\ [y,z] = 1 \\ \sigma x_0 \sigma^{-1} = z x_1^{p^s}[x_1,x_2]\dots[x_{N-1},x_N] \end{array} \right\rangle.$$

We define a property $\mathcal{P}$ of finite index normal subgroups N of JW as follows.

($\mathcal{P}$) N satisfies $\mathcal{P}$ if the quotient map $\pi_N\colon \mathrm{JW} \to \mathrm{JW}/N$ satisfies the following properties.

(a) The image of $\langle\langle x_0, \ldots, x_N \rangle\rangle$ under π_N is a p-group.

(b) The image of y under π_N has order prime to p.

The class of open normal subgroups described by $\mathcal{P}$ is a cofiltered saturated index system and we have a well-defined notion of pro-$\mathcal{P}$ completion

$$\mathrm{JW}^{\wedge\mathcal{P}} = \lim_{N \text{ satisfies } \mathcal{P}} \mathrm{JW}/N.$$

Furthermore, we have a diagram

$$\begin{tikzcd} & \mathrm{JW}^{\wedge\mathcal{P}} \arrow[dd] \\ \mathrm{JW} \arrow[ur] \arrow[dr] & \\ & \mathrm{Gal}_K \end{tikzcd}$$

where the vertical arrow is an isomorphism by the result of Jannsen–Wingberg–Diekert and the universality of the above construction. We believe this is a natural way of understanding their result.

Now we assume that $N \geq 4$. Choosing F to be the discrete free group in the generators $x_3, \ldots, x_N$ and setting $\delta = [x_3, x_4] \cdot \ldots \cdot [x_{N-1}, x_N]$, there exists a discrete combinatorial automorphism map for δ

$$\mathcal{K}^{(\delta)}_{\mathrm{discr}}\colon \mathrm{Aut}^{(\delta)}(F) \to \mathrm{Aut}(\mathrm{JW}).$$

By the choice of $\mathcal{P}$ this factors through

$$\mathrm{Aut}^{(\mathcal{P})}(\mathrm{JW}) = \{\varphi \in \mathrm{Aut}(\mathrm{JW}) \mid \text{ for all } N \text{ open normal: } N \text{ has } \mathcal{P} \Leftrightarrow \varphi(N) \text{ has } \mathcal{P}\}\,.$$

The $\mathcal{P}$-completion functor allows us to define a combinatorial automorphism map for δ that maps to $\mathrm{Aut}(\mathrm{Gal}_K)$, namely as

$$\mathcal{K}^{(\delta)}_{\mathcal{P}} : \qquad \mathrm{Aut}^{(\delta)}(F) \xrightarrow{\mathcal{K}^{(\delta)}_{\mathrm{discr}}} \mathrm{Aut}^{(\mathcal{P})}(\mathrm{JW}) \xrightarrow{(-)^{\mathcal{P}}} \mathrm{Aut}(\mathrm{Gal}_K).$$

Now let $S = S_g$ be a closed oriented surface with $2g = N - 2$. We again consider $\pi_1(S)$ in the usual presentation. For some $P \in S$ we have $\pi_1(S \setminus P) \cong F$, as this is a free discrete group of rank $2g$. This allows us to give a nice geometric interpretation of the Jannsen–Wingberg automorphism.

Proposition (Cf. Proposition 7.5.6)**.** *The Jannsen–Wingberg automorphisms* ψ^{JW} *is contained in the image of* $\mathrm{Dehn}(S)$ *under* $\mathcal{K}^{(\delta)}_{\mathcal{P}}$.

In fact, we can describe the specific Lickorish generator of $\mathrm{Mod}(S)$ such that the respective lift to $\mathrm{Aut}^{(\delta)}(F)$ maps to ψ^{JW}. Furthermore, all images of combinatorial Dehn twists coming from the set of Lickorish generators have non-trivial image in $\mathrm{Out}(\mathrm{Gal}_K)$. Considering the induced map on the abelianization, one furthermore sees that they are not geometric automorphisms. We conjecture that

$$\mathcal{K}_{\mathcal{P}}^{(\delta)}(\mathrm{Dehn}(S)) \cap \mathrm{Aut}(K) = \{1\}.$$

Assuming $p \neq 2$, a slight modification of the argument used in the case of Demuškin groups enables us to conclude $\mathcal{K}_{\mathcal{P}}^{(\delta)}(\mathrm{Dehn}(S))$ is in fact a large subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$, in the following sense.

Theorem (Cf. Theorem 7.5.5)**.** *The subgroup* $\mathcal{K}_{\mathcal{P}}^{(\delta)}(\mathrm{Dehn}(S))$ *in* $\mathrm{Out}(\mathrm{Gal}_K)$ *has dense image in* $\mathrm{Sp}_{N-2}(\mathbb{Z}_p)$*.*

This result provides a rather large lower bound for the image of $\mathrm{Out}(\mathrm{Gal}_K)$ under

$$\mathrm{Out}(\mathrm{Gal}_K) \to \mathrm{Out}(\mathrm{Gal}_K(p)) \twoheadrightarrow \mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda)).$$

We conjecture this composition to be surjective.

1.3 Notation

For a profinite group G, we shall use the following notation.

$\mathrm{Aut}(G)$	group of (continuous) automorphisms of G
$\mathrm{Inn}(G)$	group of automorphisms given by conjugation
$\mathrm{Out}(G) = \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$	group of outer automorphisms
$Z(G)$	center of G
$N_G(H)$	normalizer of a subgroup H in G
G^{ab}	abelianization of G
$\widehat{G}$	profinite completion of G
$G^{\wedge p}, G(p)$	pro-p completion of G
$d(G)$	generator rank, i.e. minimal numbers of generators of G
$r(G)$	relations rank, i.e. minimal numbers of relations of G

For an abelian group G, we shall use the following notation.

G_{tor}	group of torsion elements in G
$G[p]$	group of p-torsion elements in G
$G[p^\infty]$	group of p-primary elements in G

For a pro-p group G, we shall use the following notation.

$H^n(G) = H^n(G, \mathbb{F}_p)$	group cohomology with $\mathbb{F}_p$-coefficients
$n(G) = \dim_{\mathbb{F}_p} H^1(G)$	minimal numbers of generators of G
$\Lambda(G)$	maximal quotient of $\mathbb{Z}_p$ such that $G^{\mathrm{ab}} \otimes \Lambda$ is free Λ-modules of rank $n(G)$
$q(G)$	group invariant defined as $q(G) = \#\Lambda(G)$ if finite and $q(G) = 0$ otherwise

For p-adic number fields, we shall always use the following notation.

K	finite extension of $\mathbb{Q}_p$ (where p is fixed prime)
$\overline{K}$	a (fixed) algebraic closure of K
$K(p)$	the maximal pro-p extension of K
K^{nr}	maximal unramified extension of K
K^{tr}	maximal tamely ramified extension of K
$\mathrm{Gal}_K = \mathrm{Gal}(\overline{K}/K)$	absolute Galois group of K
$I_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$	the inertia subgroup of Gal_K
$V_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{tr}})$	the (wild) ramification subgroup of Gal_K
$\Gamma_K = \mathrm{Gal}(K^{\mathrm{nr}}/K) = \mathrm{Gal}_K/I_K$	maximal unramified quotient of Gal_K
$\mathrm{Gal}(K^{\mathrm{tr}}/K) = \mathrm{Gal}_k/V_K$	maximal tamely ramified quotient of Gal_K
$\mathrm{Iw}_q = \widehat{\mathbb{Z}}'(1) \rtimes_q \widehat{\mathbb{Z}}$	Iwasawa group for the parameter q
$\mathrm{Gal}_K(p) = \mathrm{Gal}(K(p)/K)$	maximal pro-p quotient of Gal_K
$q = q_K = p^f_K$	cardinality of residue field
$e = e_K$	absolute ramification index of K
$f = f_K$	residue degree of K
$\mathcal{O}_K$	ring of integers of K
$\mathfrak{p} = \mathfrak{p}_K$	maximal ideal of $\mathcal{O}_K$
$\mathbb{F} = \mathbb{F}_K = \mathcal{O}_K/\mathfrak{p}_K$	residue field of K
$U_K^{(n)} = 1 + \mathfrak{p}_K^n$	group of n-units of K

Acknowledgements

First of all, I would like to thank my dissertation supervisor Jakob Stix not only for being a great advisor who would always take time to answer my questions and provide mathematical guidance, but also never failed to be kind and encouraging when I was struggling to make progress with the thesis (or just struggling in general). I also want to thank Annette Werner for agreeing to be the second assessor and being a great mentor.

I want to thank all my current and former colleagues. In particular, I want to thank Martin Lüdtke for always spotting the typos in my exercise sheets, being a great collaborator, and conference-travel buddy. Sara Lamboglia for being the best first office buddy one could ask for. Markus Rennig for being a friend that I could always count on (and Artilleriefeuer). Riccardo Zuffetti for always making sure inert groups of mathematicians get up from the lunch table, and Jaro Eichler for reminding me that not putting on so much effort all the time is also an option (and being good friends as well, of course). I also want to thank Max Bieri, Matteo Costantini, Felix Göbler, Johannes Horn, Şevda Kurul, Rosemarie Martienssen, Matthias Nickel, Stefan Rettenmayr, Felix Röhrle, Nithi Rungtanapirom, Jeonghoon So, Johannes Schwab, David Torres-Teigell, and Jonathan Zachhuber. It was a pleasure to share many terrible Mensa lunches, in-person and virtual coffee breaks and the occasional apple wine with you. Special thanks to Yanik Kleibrink for allowing me use some pictures for this thesis!

I want to thank the rollergrrrlgang for introducing me to fabulous world of roller derby, being just an overall amazing group of people, and providing the best distraction from writing this thesis (which is smashing into other people on roller skates, obviously). Next in the category of things that distracted me from this thesis: the Hessische Schülerakademie. Thanks to everyone involved for providing the ideal setting to teach, learn and grow. In particular, thanks to Cynthia Hog-Angeloni and Wolfgang Metzler for founding this program and entrusting me with the math class for the past five years. Clearly, I cannot omit the amazing distractions that I call my friends. I will omit naming most of them, as they will never see this. However, I want to thank Isa for playing an invaluable role in (somewhat) keeping me sane in the past months and always being up for fun nonsense, and Tanasgol for nearly 15 years of friendship.

And of course, I want to thank my family who has supported me unconditionally, even though they still have no idea what I'm doing.

2 Preliminaries

In this chapter, we introduce some notation, classical results and concepts that will be relevant for this thesis.

2.1 Profinite groups

2.1.1 Basic definitions and properties

We recall some facts about profinite groups. A comprehensive introduction to profinite groups can be found in [RZ00]. A good overview on pro-p groups is given in [Dix+03] and [Koc13a]. Most proofs to standard results will be omitted and can be found in most of these references.

There are essentially two ways of viewing profinite groups. The first characterization is of topological nature.

Definition 2.1.1 (Profinite Group)**.** A *profinite group* is a compact Hausdorff topological group whose open subgroups form neighbourhood basis of the identity.

In order to give the second definition, we recall the following constructions. A *directed set* is a partially ordered set $I = (I, \preceq)$ such that for all $i, j \in I$ there exists $k \in I$ such that $k \succeq i$ and $k \succeq j$. An *inverse system* $(G_i; \varphi_{ij})$ of groups (or sets, rings, topological spaces, etc.) over I consists of a family of groups (or sets, rings, topological spaces, etc.) $G_i, i \in I$, and morphisms $\varphi_{ij} : G_i \to G_j$ for $i \preceq j$, satisfying the compatibility conditions

$$\varphi_{ii} = \mathrm{id}_{G_i} \quad \text{and} \quad \varphi_{ij} \circ \varphi_{jk} = \varphi_{ik} \quad \text{for all } i, j, k \in I \text{ with } i \preceq j \preceq k.$$

Example 2.1.2. Let G be a profinite group, and let $\mathcal{N}$ denote the family of all open normal subgroups. We may order $\mathcal{N}$ by reverse inclusion to obtain an inverse system $(G/N)_{N\in\mathcal{N}}$, where the transition maps are given by the natural epimorphisms $G/N \to G/M$, where N is a subgroup of M.

The *inverse limit* of the inverse system $(G_i; \varphi_{ij})$ is the group

$$G \coloneqq \varprojlim G_i \coloneqq \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \mid \varphi_{ij}(g_i) = g_j \text{ if } i \succeq j \right\}$$

with the natural projections $\pi_i : G \to G_i$. As usual, this construction can (and should) be understood via a universal property. We say that a group G together with compatible homomorphisms $\pi_i \colon G \to G_i$ $(i \in I)$ is an inverse limit for the inverse system $(G_i; \varphi_{ij})$ if for any group H and compatible homomorphisms $\psi_i \colon H \to G_i$, there exists a unique homomorphism $\psi \colon H \to G$ such that $\pi_i \circ \psi = \psi_i$ for all $i \in I$.

Remark 2.1.3. In the case $I = \mathbb{N}$ and where $\succeq$ is just the ordinary order relation $\leq$, one can think of the inverse limit as the limit object of a chain of homomorphisms, as depicted below.

$$\begin{tikzcd}
& G = \varprojlim G_i \arrow[d, dashed, "\pi_i"] \arrow[rrd, dashed, "\pi_3"] \arrow[rrrd, dashed, "\pi_2"] \arrow[rrrrd, dashed, "\pi_1"] & & & & \\
\cdots \arrow[r, "\varphi_{i+1,i}"] & G_i \arrow[r, "\varphi_{i,i-1}"] & \cdots \arrow[r, "\varphi_{4,3}"] & G_3 \arrow[r, "\varphi_{3,2}"] & G_2 \arrow[r, "\varphi_{2,1}"] & G_1.
\end{tikzcd}$$

If the groups G_i in the inverse system are finite groups, we can give each of them the discrete topology, and $\prod_{i\in I} G_i$ the product topology. The inverse limit $\varprojlim G_i$ endowed with the induced topology is a topological group and one can easily verify that it is totally-disconnected, compact, and Hausdorff, hence a profinite group.

The crucial observation for our second definition is that all profinite groups are of this form.

Proposition 2.1.4. *If G is a profinite group, then G is topologically isomorphic to*

$$\varprojlim_{N\in\mathcal{N}} G/N.$$

Let X be a subset of G. We say that a profinite group G is *topologically generated by* X if the abstract subgroup $\langle X\rangle$ of G generated by X is dense in G. We write $G = \overline{\langle X\rangle}$. We say that G is *finitely generated* if G is topologically generated by some finite set X. We call X *minimal* if no proper subset of X generates G. The smallest cardinality of a set of generators is known as the *generator rank* of G, which we will denote by $d(G)$.

Example 2.1.5. (i) The additive group of p-adic integers $\mathbb{Z}_p$ is profinite. We have

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z},$$

where n ranges over $\mathbb{N}$ and the transition maps are given by $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for $m \leq n$. Note that the topology on this profinite group is precisely the topology arising from the p-adic valuation. The group of profinite integers $\widehat{\mathbb{Z}}$ is the inverse limit

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z},$$

where n ranges over $\mathbb{N}$ and the transition maps are given by the natural maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$. Note that $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

(ii) Profinite groups arise as the Galois groups of algebraic field extensions: Let K be a field, and L/K a Galois extension. Then the Galois group $\mathrm{Gal}(L/K)$, consisting of the field automorphisms of L fixing K, is a profinite group. It is obtained as the inverse limit

$$\mathrm{Gal}(L/K) = \varprojlim_M \mathrm{Gal}(M/K),$$

where the inverse system ranges over all intermediate fields $L/M/K$ such that M/K is a finite Galois extension, and the transition maps are given by the restriction maps

$\mathrm{Gal}(M_2/K) \to \mathrm{Gal}(M_1/K)$ where $M_1 \subseteq M_2$. The topology on $\mathrm{Gal}(L/K)$ is called the *Krull-Topology.*

If $K = K^{\mathrm{sep}}$ denotes a separable closure of the field K, we call the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ the *absolute Galois group* of K, and denote this by Gal_K, omitting the choice of separable closure.

In even greater generality, this can be phrased in the following way. Let $\mathcal{C}$ be a Galois category and let $F\colon \mathcal{C} \to (\mathrm{FinSets})$ denote a fibre functor of $\mathcal{C}$. Then the automorphism group $\mathrm{Aut}(F)$ of F is a profinite group. See [Sta21, Tag 0BMQ].

(iii) Let G be an arbitrary group. Then there exists a profinite group $\widehat{G}$ of G and a homomorphism $\eta\colon G \to \widehat{G}$, such that $\eta(G)$ is dense in $\widehat{G}$, and for all profinite groups H and group homomorphisms $f\colon G \to H$, there exists a unique continuous group homomorphism $h\colon \widehat{G} \to H$ such that $f = h \circ \eta$. Namely, this group can be constructed as the inverse limit of the inverse system $(G/N)_{N \in \mathcal{N}}$.

(iv) Let X be a set, F a profinite group, and $\iota\colon X \to F$ a map. We say (F, ι) is a *free profinite group* on X, if the following property is satisfied: For all profinite groups G and mappings $\varphi\colon X \to G$ convergent to $1 \in G$ there exists a (unique) continuous homomorphism $\widetilde{\varphi}\colon F \to G$ such that the following diagram commutes

$$\begin{tikzcd}
F \arrow[r, dotted, "\widetilde{\varphi}"] & G. \\
X \arrow[u, "\iota"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Such a group exists and is unique. The construction works as follows. Let X be a set and let F_X denote the free discrete group on X. Then profinite completion $\widehat{F_X}$ of F_X is the free profinite group on X in the above sense.

If $X = \{x_1, \ldots, x_n\}$ is of finite cardinality n, we write $\widehat{F_n}$ and call this the *free profinite group of rank n.*

Definition 2.1.6 (Frattini Subgroup)**.** Let G be a profinite group. The *Frattini subgroup* of G is

$$\Phi(G) = \bigcap_M M,$$

where the intersection is taken over all maximal proper open subgroups of G.

As any continuous automorphism maps maximal subgroups to maximal subgroups, the Frattini subgroup is a characteristic and hence normal subgroup of G, i.e. there exists a homomorphism

$$\mathrm{Aut}(G) \to \mathrm{Aut}(G/\Phi(G)).$$

One can think of $\Phi(G)$ as the "subgroup of non-generators". To make this more precise, we recall the following fact.

Proposition 2.1.7 (Frattini argument)**.** *Let G be a profinite group, and X a subset of G. Then X generates G topologically if and only if the image of X under $G \to G/\Phi(G)$ generates $G/\Phi(G)$.*

Finitely generated profinite groups are *Hopfian groups*, i.e. they have the following property.

Proposition 2.1.8. *Let G be a finitely generated profinite group and let*

$$\varphi : G \longrightarrow G$$

be a continuous epimorphism. Then φ is an isomorphism of profinite groups.

Proof. See [RZ00, Prop. 2.5.2]. □

When trying to deduce properties of profinite groups from properties of its finite quotients, the following result is very useful.

Proposition 2.1.9. *Let $(X_i)_{i \in I}$ be an inverse system of non-empty compact spaces over a directed set I. Then $\varprojlim_I X_i$ is non-empty.*

2.1.2 Pro-p groups

In this section we review some definitions and properties about an important class of profinite groups, pro-p groups.

Definition 2.1.10 (Pro-p group)**.** A pro-p group is a profinite group such that all open normal subgroup have index equal to some power of p.

In the spirit of the second characterization of profinite groups seen in Proposition 2.1.4: a pro-p group is a profinite group that is an inverse limit of finite p-groups.

Example 2.1.11. (i) The p-adic integers $\mathbb{Z}_p$ form a pro-p group with respect to addition.

(ii) Let K be a field, and let $K(p)/K$ denote the maximal p-extension, i.e. the compositum of all extensions of K with a p-power degree in a fixed separable closure of K. Then $\mathrm{Gal}(K(p)/K)$ is a pro-p group.

(iii) Let G be an arbitrary group. Similar to the profinite completion of G, one may define the *pro-p completion* of G. This group can be constructed as the inverse limit of the inverse system $(G/N)_{N \in \mathcal{N}_p}$, where $\mathcal{N}_p$ denote the family of all normal subgroups N of G such that G/N is a finite p-group. We denote this by $G^{\wedge p} = \varprojlim_{N \in \mathcal{N}_p} G/N$.

(iv) Let X be a set and let F_X denote the free discrete group on X. We call the pro-p completion of F_X the *free pro-p group on X* and denote this by $\widehat{F}_X(p)$. Just like in Ex. 2.1.5 (iv), there is a categorical description of free pro-p group via a universal property.

For a group G let $[G, G]$ denote the subgroup of G generated by the commutators

$$[x, y] = xyx^{-1}y^{-1} \quad x, y \in G.$$

The Frattini subgroup of a finitely generated pro-p group can be described rather explicitly.

Proposition 2.1.12. *Let G be a pro-p group. The following holds.*

(i) $\Phi(G) = \overline{G^p[G, G]}$,

(ii) The group G is finitely generated if and only if $\Phi(G)$ is open in G. In that case, we have $\Phi(G) = G^p[G,G]$.

(iii) Let n be the generator rank of G. The group $G/\Phi(G)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. In particular, we have $(G : \Phi(G)) = p^n$.

Proof. See [RZ00, Lemma 2.8.7]. □

An important feature of finitely generated pro-p groups is expressed in the following theorem. We refer to [Dix+03, Thm. 1.17] for the proof, which is originally due to Serre, using Proposition 2.1.12 (iii).

Theorem 2.1.13 (Serre)**.** *Let G be a finitely generated pro-p group. Every subgroup of finite index is open in G.*

This result actually generalizes to profinite groups, i.e. in every finitely generated profinite group, every subgroup of finite index is open. This is due to Nikolov and Segal.

We state two important consequences of this:

Corollary 2.1.14. *Let G be a finitely generated pro-p group. Then the following holds.*

(i) Every homomorphism of G to a profinite group is continuous.

(ii) The topology of G is determined by its group structure.

(iii) Every automorphism of G (as an abstract group) is a topological automorphism.

2.2 Group cohomology

In this section we give a quick recap of cohomology of profinite group. There are various good sources on the subject, e.g. [RZ00]. A great introduction on Galois cohomology is given in [NSW13], and of course [Ser13a].

2.2.1 Basic definitions

Definition 2.2.1 (topological (left) G-module)**.** A *topological (left) G-module A* is an abelian Hausdorff topological group which is an abstract G-module such that the action $G \times A \to A$, where $G \times A$ us equipped with the product topology, is a continuous map.

From now on, we shall assume all G-modules to be discrete. For every $n \geq 0$, we denote by $G^{\times n}$ the direct product of n copies of G, which we equip with the product topology. The abelian group

$$C^n(G, A) := \{f : G^{\times n} \to A \mid f \text{ continuous}\}$$

is called the group of *(inhomogeneous) n-cochains* of G with values in A. We identify $C^0(G, A) = A$ for $n = 0$. For $n \geq 2$, we define a map

$$\partial_n : C^{n-1}(G, A) \to C^n(G, A)$$

as

$$\begin{aligned}(\partial_n f)(g_1,\dots,g_n) \coloneqq{}& g_1 f(g_2,\dots,g_n) \\ &+ \sum_{i=1}^{n-1}(-1)^i f(g_1,\dots g_{i-1}, g_i g_{i+1}, g_{i+2},\dots,g_n) \\ &+ (-1)^n f(g_1,\dots,g_{n-1}).\end{aligned}$$

In the special cases $n = 1, 2$, we have

$$\begin{aligned}(\partial_1 a)(g) &= g.a - a \quad \text{for } a \in A, \\ (\partial_2 f)(g) &= g_1.f(g_2) - f(g_1, g_2) + f(g_1) \quad \text{for } f \in C^1(G, A).\end{aligned}$$

We set

$$Z^n(G, A) = \ker(\partial_{n+1}),$$

called the group of (inhomogeneous) n-cocycles, and

$$B^n(G, A) = \operatorname{im}(\partial^n),$$

called the group of (inhomogeneous) n-coboundaries. Finally, we define

Definition 2.2.2 (Cohomology group)**.** For $n \geq 0$ the quotient

$$H^n(G, A) = Z^n(G, A)/B^n(G, A)$$

is called the *n-th cohomology group of G* with coefficients in A.

Note that the 0-th cohomology group of a profinite group G with coefficients in A is the subgroup of G-invariant elements, i.e.

$$H^0(G, A) = A^G.$$

In particular, if G acts trivially on A, one has $H^0(G, A) = A$.

2.2.2 Functoriality

The group $H^1(G, A)$ gives information about the deviation from exactness when passing from an exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

to the left exact sequence of G-invariant subgroups

$$0 \to A^G \to B^G \to C^G.$$

There is a canonical homomorphism $\delta\colon C^G \to H^1(G, A)$ extending above sequence to the exact sequence

$$0 \to A^G \to B^G \to C^G \to H^1(G, A).$$

This leads us to the following fundamental property of group cohomology.

Proposition 2.2.3. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of discrete G-modules. Then for all $n \geq 0$ we have connecting homomorphisms*

$$\delta^n \colon H^n(G,C) \to H^{n+1}(G,A),$$

such that

$$\ldots \to H^n(G,A) \to H^n(G,B) \to H^n(G,C) \xrightarrow{\delta^n} H^{n+1}(G,A) \to \ldots$$

is a long exact sequence.

Remark 2.2.4. We may phrase this in the language of category theory by saying $H^n(G,-)$ is a covariant cohomological δ-functor.

Let Γ, Δ be profinite groups, let $\varphi : \Gamma \to \Delta$ be a continuous group homomorphism, and let M, M' be a topological Γ- and Δ-module, respectively. Let $f \colon M' \to M$ be a continuous group homomorphism. Recall that we call a pair (φ, f) *compatible* if $xf(m) = f(\varphi(x)m)$ for all $x \in \Delta$ and $m \in M'$. In particular, if $\Gamma = \Delta$ and φ is the identity map, then the pair is compatible if and only if f is a homomorphism of G-modules.

Proposition 2.2.5. *Let (φ, f) be a compatible pair of maps. There is a homomorphism*

$$\begin{gathered}(\varphi^*, f_*) \colon C^n\left(\Delta, M'\right) \to C^n\left(\Gamma, M\right), \\ (\varphi^*, f_*)(\alpha))\left(x_1, \ldots, x_n\right) = f\left(\alpha\left(\varphi\left(x_1\right), \ldots, \varphi\left(x_n\right)\right)\right),\end{gathered}$$

for all $n \geq 0$, inducing a homomorphism on cohomology groups

$$H^n\left(\Delta, M'\right) \to H^n\left(\Gamma, M\right).$$

In particular, the cohomology groups $H^n(\Gamma, M)$ are functorial in Γ and M simultaneously.

We conclude this section with special cases of maps $H^n\left(\Delta, N\right) \to H^n\left(\Gamma, M\right)$.

Inflation

Let G be a profinite group, let N be a normal closed subgroup of G, and let A be a G-module. The group of H-invariants A^N is a G/N-module. The projection $G \to G/N$, and the injection $A^N \to A$ are compatible. The induced homomorphism

$$\mathrm{infl}_G^{G/N} : H^n\left(G/N, A^N\right) \longrightarrow H^n(G,A)$$

is called *inflation.*

Restriction

For a closed subgroup H of G and a G-module A, the inclusion $H \hookrightarrow G$ and identity on A form a compatible pair, inducing a homomorphism

$$\begin{aligned}\mathrm{res}_H^G \colon H^n(G,A) &\to H^n(H,A), \\ f + B^n(G,A) &\mapsto f|_{H^n} + B^n(H,A).\end{aligned}$$

Note that both restriction and inflation are functorial in the G-module, and commute with the δ-homomorphism.

Inner automorphisms on cohomology

Let G be a group and let A be a G-module. Let $G \to G, h \mapsto ghg^{-1}$ be an inner automorphism and let $A \to A, a \mapsto g^{-1}a$ be an automorphism of A. We note that is a compatible pair. Hence, for any $g \in G$, this defines an automorphism σ_g on cohomology $H^i(G, A)$.

Proposition 2.2.6. *The automorphisms $\sigma_g \colon H^i(G, A) \to H^i(G, A)$ are trivial.*

This may be generalized as follows. Let N be a closed normal subgroup of G and let A be a G-module. Then the cohomology group $H^i(N, A)$ is a discrete G-module, too. Indeed, every element $g \in G$ acts by conjugation σ_g.

Proposition 2.2.7. *The closed normal subgroup acts trivially on the cohomology group $H^i(N, A)$, i.e. $H^i(N, A)$ is a G/N-module.*

Proof. See [NSW13, Prop. 1.6.3]. □

Transgression map

Proposition 2.2.8. *Let N be a normal subgroup of G and A a G-module. There is a canonical homomorphism*

$$\mathrm{tg} : H^1(N, A)^{G/N} \longrightarrow H^2\left(G/N, A^N\right)$$

called transgression*, which is given as follows. If $x : N \to A$ is an inhomogeneous 1-cocycle in a class $[x] \in H^1(N, A)^{G/N}$, there exists a 1-cochain $y \colon G \to A$ such that $y|_N = x$ and that $(\partial y)(\sigma_1, \sigma_2)$ is contained in A^N and depends only on the cosets $\sigma_1 N, \sigma_2 N$, i.e. may be regarded as a cocycle of G/N. For each such cochain y we have*

$$\mathrm{tg}[x] = [\partial y].$$

Proof. See e.g. [NSW13, Prop. 1.6.6]. □

Theorem 2.2.9 (Hochschild–Serre spectral sequence)**.** *Let G be a profinite group, let A be a G-module, and let N a closed normal subgroup. There exists a first quadrant spectral sequence*

$$E_2^{pq} = H^p(G/N, H^q(N, A)) \Rightarrow H^{p+q}(G, A),$$

called Hochschild-Serre spectral sequence*.*

As a consequence of a standard result on spectral sequences, we get the following 5-term sequence.

Proposition 2.2.10 (5-term sequence)**.** *Let N be a normal closed subgroup of G. Then there exists an exact sequence*

$$0 \to H^1\left(G/N, A^N\right) \xrightarrow{\text{infl}} H^1(G, A) \xrightarrow{\text{res}} H^1(N, A)^G \xrightarrow{\text{tg}} H^2\left(G/N, A^N\right) \to H^2(G, A),$$

called the five term exact sequence*.*

Proof. See e.g. [NSW13, Prop. 1.6.7]. □

Note that it requires some work to check that the respective differential in the spectral sequence is in fact the transgression map.

2.2.3 Cup product and Bockstein homomorphism

Recall that for G-modules A, B the tensor product $A \otimes_{\mathbb{Z}} B$ is a G-module via $g.(a \otimes b) = g.a \otimes g.b$. Let A, B, C be G-modules with bilinear pairings

$$A \times B \longrightarrow A \otimes_{\mathbb{Z}} B \longrightarrow C. \tag{2.1}$$

This induces a well-defined bilinear map

$$H^n(G, A) \times H^m(G, B) \xrightarrow{\cup} H^{n+m}(G, C),$$

called the *cup product.*

Proposition 2.2.11. *The cup product is associative and skew-commutative, i.e.*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \quad \text{ and } \quad \alpha \cup \beta = (-1)^{nm} \beta \cup \alpha,$$

for every $\alpha \in H^n(G, A)$, $\beta \in H^m(G, B)$ and $\gamma \in H^k(G, C)$ with the identifications

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \quad \text{ and } \quad A \otimes B = B \otimes A.$$

There is a connecting homomorphism that will play a central role throughout this thesis, the so-called *Bockstein homomorphism.*

Definition 2.2.12. Let $m, n > 1$ be positive integers. For a profinite group G the (m, n)-*Bockstein homomorphism*

$$\beta = \beta_{m,n}(G) \colon H^1(G, \mathbb{Z}/m\mathbb{Z}) \to H^2(G, \mathbb{Z}/n\mathbb{Z})$$

is the connecting homomorphism in the long exact cohomology sequence associated to the short exact sequence of (trivial) G-modules

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{m} \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0. \tag{2.2}$$

2.2.4 Some cohomological invariants

We define an invariant for the cohomological complexity of a profinite group G.

Definition 2.2.13 (Cohomological dimension)**.** The *cohomological dimension* of G (resp. *strict cohomological dimension* of G), denoted by $\operatorname{cd} G$ (and resp. $\operatorname{scd} G$), is the smallest integer $n > 0$ such that $H^k(G, A) = 0$ for all $k > n$ and for all torsion (resp. all) G-modules A. If no such n exists, we set $\operatorname{cd} G = \infty$ and say that G has (strict) infinite cohomological dimension.

If $G = \mathrm{Gal}_K$ is the absolute Galois group of a field K, we set $\operatorname{cd} K \coloneqq \operatorname{cd} \mathrm{Gal}_K$.

For a prime p, the *(strict) cohomological p-dimension* of G, denoted by $\operatorname{cd}_p G$ (resp. $\operatorname{scd}_p G$), is the smallest integer n, such that $H^k(G, A)[p] = 0$ for all $k > n$ and for all torsion (resp. all) G-modules A. Again, if no such n exists, then we say that G has infinite (strict) cohomological p-dimension and we write $\operatorname{cd}_p G = \infty$.

In particular, we have $\operatorname{cd} G = \sup \operatorname{cd}_p G$. If G is a p-group, we have $\operatorname{cd} G = \operatorname{cd}_p G$.

We can define another invariant of a pro-p (resp. profinite) group G, the *Euler-Poincaré characteristic* of G (at p).

Definition 2.2.14. Let G be a pro-p group such that $\operatorname{cd}(G)$ is finite and $H^i(G, \mathbb{Z}/p\mathbb{Z})$ is finite for all i. Let A be a finite $\mathbb{F}_p[\![G]\!]$-module. The *Euler–Poincaré characteristic* of G for A is given by

$$\chi(G, A) = \sum_{i=0}^{\infty}(-1)^i \dim H^i(G, A).$$

If $A = \mathbb{Z}/p\mathbb{Z}$, we set $\chi(G) = \chi(G, \mathbb{Z}/p\mathbb{Z})$.

For a profinite group G the *Euler–Poincaré characteristic of* G *at* p for a finite $\mathbb{F}_p[\![G]\!]$-module$A$ is given by

$$\chi_p(G, A) = \sum_i (-1)^i \dim_{\mathbb{F}_p} H^i(G, A).$$

Proposition 2.2.15. *Let G be a pro-p group such that $\operatorname{cd}(G)$ is finite and $H^i(G, \mathbb{Z}/p\mathbb{Z})$ is finite for all i. Let A be a finite $\mathbb{F}_p[\![G]\!]$-module. If U is an open subgroup of G, then*

$$\chi(U, A) = (G : U) \cdot \chi(G, A).$$

Proof. See [NSW13, Prop. 3.3.13]. □

Free pro-p groups may be characterized via their cohomological dimension. Namely, the following holds.

Proposition 2.2.16. *For a pro-p-group G the following are equivalent.*

(i) The cohomological dimension of G is 1.

(ii) Every group extension of G by a pro-p-group G' splits.

(iii) The group G is free.

Proof. This follows from [NSW13, Thm. 3.5.6]. □

Example 2.2.17. Proposition 2.2.16 implies that $\operatorname{cd}(\widehat{\mathbb{Z}}) = 1$ as $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

If F is a free pro- p group and H is a closed subgroup of F then H is also a free pro-p group since $\operatorname{cd}(H) \leq \operatorname{cd}(F) \leq 1$. If F is of finite rank and H is open in F, then the rank of H is also finite and we have Schreier's formula

$$d(H) - 1 = (F : H)(d(F) - 1). \tag{2.3}$$

Note that this is not true for profinite groups.

2.2.5 Poincaré groups

Essentially all examples of groups we consider in later chapters are Poincaré groups, i.e. groups for which a duality theorem of Poincaré type holds. We give a definition for pro-p groups following [Ser13a, §4.3].

Definition 2.2.18. Let G be an infinite pro-p group. The group G is a Poincaré group of dimension n if G satisfies the following conditions.

(i) The cohomology group $H^i(G,\mathbb{F}_p)$ is finite for all i.

(ii) $\dim H^n(G,\mathbb{F}_p) = 1$.

(iii) For any $i \geq 0$ the cup-product

$$H^i(G,\mathbb{F}_p) \times H^{n-i}(G,\mathbb{F}_p) \to H^n(G,\mathbb{F}_p)$$

is a nondegenerate bilinear form.

Notice that (iii) implies that $H^i(G,\mathbb{F}_p) = 0$ if $i > n$, i.e. $\mathrm{cd}(G) = n$. Up to isomorphism $\mathbb{Z}_p$ is the only Poincaré group of dimension 1. We will study Poincaré groups of dimension 2, which are called *Demuškin groups*, in more detail later.

For an (abstract) abelian group A, we use the notation

$$A^\vee = \mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z}).$$

We note that for a n-dimensional Poincaré group, the cohomology groups $H^i(G,A)$ are finite for all finite A, (cf. [Ser13a, Prop. 17]) and with condition (i), we may define a dualizing module as

$$I = \varinjlim_k \varinjlim_U H^n(U,\mathbb{Z}/p^k\mathbb{Z})^\vee,$$

where in the second limit U runs through the open normal subgroups of G, and the limit is taken over the duals of the corestriction. Note that we have a functorial isomorphism

$$H^n(G,A)^\vee \to \mathrm{Hom}_G(A,I).$$

This enables us to write down the sense in which such a group G satisfies a duality of Poincaré-type.

Proposition 2.2.19. *Let G be an n-dimensional Poincaré pro p-group, and let I be its dualizing module. Then the following holds:*

(i) $I \cong \mathbb{Q}_p/\mathbb{Z}_p$ as abelian groups.

(ii) The canonical homomorphism $H^n(G,I) \to \mathbb{Q}/\mathbb{Z}$ is an isomorphism of $H^n(G,I)$ and $\mathbb{Q}_p/\mathbb{Z}_p$ viewed as a subgroup of $\mathbb{Q}/\mathbb{Z}$.

(iii) For all finite G-modules A and integers i, the cup product

$$H^i(G,A) \times H^{n-i}(G,\mathrm{Hom}(A,I)) \longrightarrow H^n(G,I) = \mathbb{Q}_p/\mathbb{Z}_p$$

gives a duality between the two finite groups $H^i(G,A)$ and $H^{n-i}(G,\mathrm{Hom}(A,I))$.

Proof. See [Ser13a, I.4.5, Prop. 30]. □

Under the assumption of Proposition 2.2.19, we have $\mathrm{Aut}(I) = \mathbb{Z}_p^\times$, i.e. G acts on I via a continuous character

$$\chi\colon G \to \mathbb{Z}_p^\times,$$

and I is determined by χ (up to isomorphism). Since G is a pro-p group, $\mathrm{im}(\chi)$ is contained in the 1-units, i.e. such units which are $\equiv 1 \bmod p$. By the Serre criterion (see [NSW13, Cor. 3.4.5]) the following holds.

Proposition 2.2.20. *Let G be a n-dimensional Poincaré group, and $\chi\colon G \to \mathbb{Z}_p^\times$ the associated character described above. Then*

$$\operatorname{scd}(G) = n + 1 \quad \textit{if and only if} \quad \operatorname{im}\chi \textit{ is finite.}$$

For $p \neq 2$ this is the case if and only if χ is trivial. If $p = 2$, the condition is equivalent to $\chi(G) = \{1\}$ or $\{\pm 1\}$.

We remark that if $\operatorname{im}\chi$ is infinite, then $\operatorname{scd}(G) = n$.

2.3 Cohomology of p-adic local fields

In the cohomology theory of p-adic local fields we have a few crucial tools, namely class field theory, Kummer theory and Tate duality. We shall discuss them briefly and recall the main results. First off, we introduce Galois cohomology as a special case of group cohomology.

2.3.1 Galois cohomology

Let K be a field and let L/K be a Galois extension with $G = \operatorname{Gal}(L/K)$. If A is a discrete G-module, we set

$$H^n(L/K, A) := H^n(G, A).$$

If $L = K^{\text{sep}}$ is a separable closure of K, then we write $H^i(K, A)$ for $H^n(K^{\text{sep}}/K, A)$. This is well-defined as for any other choice of separable closure will induce a canonical isomorphism on cohomology. Furthermore, we set

$$\begin{aligned} H^i(L/K) &:= H^i(L/K, L^\times) = H^i(L/K, \mathbb{G}_m), \\ H^i(K) &:= H^i(K, (K^{\text{sep}})^\times) = H^i(K, \mathbb{G}_m). \end{aligned}$$

We recall the famous Hilbert 90, stating that the first cohomology group of $\operatorname{Gal}(L/K)$ with coefficients in the multiplicative group $L^\times$ is trivial.

Proposition 2.3.1 (Hilbert 90)**.** *Let L/K be a Galois extension. Then*

$$H^1(L/K, \mathbb{G}_m) = 0.$$

2.3.2 Cohomology of the multiplicative group and Local Duality

From now on let K always denote a p-adic local field (even though some results are true for local fields in general), and let q denote the cardinality of its residue field $\mathbb{F} = \mathbb{F}_K$. Recall the structure of the multiplicative group of K.

Proposition 2.3.2 (Units in K)**.** *Let π be a uniformizer of K. For the multiplicative group of K the following holds:*

$$K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U_K^{(1)} \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus U_K^{(1)}.$$

The p-adic logarithm induces a homomorphism

$$U_K^{(n)} \to \mathfrak{p}^n = \pi^n \mathcal{O}_K \cong \mathcal{O}_K \quad \textit{for } n \gg 0.$$

The torsion subgroup of $U_K^{(1)}$ is the group of p-power roots of unity. Hence, there is a free finitely generated $\mathbb{Z}_p$-submodule V of $U_K^{(1)}$ of rank $N = ef = [K:\mathbb{Q}_p]$ such that

$$U_K^{(1)} = \mu_{p^s} \times V \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}_p^N.$$

Proof. See [Neu06, II, Satz 5.7]. □

Invariant map

As any finite unramified extension of K corresponds to a finite extension of its residue field, the Galois group $\Gamma_K = \mathrm{Gal}(K^{\mathrm{nr}}/K)$ is a pro-cyclic group topologically generated by the Frobenius automorphism, and canonically isomorphic to $\widehat{\mathbb{Z}}$.

The valuation v on K^{nr} induces a short exact sequence

$$0 \to \mathcal{O}_{K^{\mathrm{nr}}}^{\times} \to (K^{\mathrm{nr}})^{\times} \xrightarrow{v} \mathbb{Z} \to 0.$$

The first crucial observation is that the group of units $\mathcal{O}_{K^{\mathrm{nr}}}^{\times}$ is in fact a cohomologically trivial Γ_K-module, see [NSW13, Prop. 7.1.2]. Furthermore, we have the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where $\mathbb{Q}$ is a cohomologically trivial Γ_K-module. We get the following isomorphism, which we denote by $\mathrm{inv}_{K^{\mathrm{nr}}/K}$:

$$\begin{aligned} H^2(K^{\mathrm{nr}}/K) &\xrightarrow[\sim]{v} H^2(\Gamma_K, \mathbb{Z}) \\ &\xrightarrow[\sim]{\delta^{-1}} H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\sim]{\mathrm{ev}_{\mathrm{Frob}}} \mathbb{Q}/\mathbb{Z}. \end{aligned} \tag{2.4}$$

Note that this map is compatible with finite extensions L/K. More precisely, the following diagram commutes:

$$\begin{tikzcd} H^2(L^{\mathrm{nr}}/L) \arrow[r, "\mathrm{inv}"] & \mathbb{Q}/\mathbb{Z} \\ H^2(K^{\mathrm{nr}}/K) \arrow[r, "\mathrm{inv}"] \arrow[u, "\mathrm{res}"] & \mathbb{Q}/\mathbb{Z}. \arrow[u, "{[L:K]}"'] \end{tikzcd}$$

Theorem 2.3.3. *We have $H^2(K) = H^2(K^{\mathrm{nr}}/K)$. Hence, there is a canonical isomorphism*

$$\mathrm{inv}_K \colon H^2(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z},$$

called the invariant map*, compatible with finite extensions in above sense.*

Proof. See [NSW13, (7.1.3-4)]. □

Corollary 2.3.4. *Let K be a p-adic local field. Then*

$$\mathrm{cd}(K) = \mathrm{cd}_p(K) = 2.$$

Kummer theory

Given a field K and positive integer m invertible in K, let $\mu_m(K)$ denote the roots of unity of order m that are contained in K. We have a short exact sequence

$$1 \longrightarrow \mu_m(K^{\mathrm{sep}}) \longrightarrow (K^{\mathrm{sep}})^\times \xrightarrow{m} (K^{\mathrm{sep}})^\times \longrightarrow 1,$$

inducing a long exact sequence on cohomology, namely

$$K^\times \xrightarrow{m} K^\times \longrightarrow H^1(K, \mu_m(K^{\mathrm{sep}})) \longrightarrow H^1(K, \mathbb{G}_m) = 0.$$

This gives us the following result.

Proposition 2.3.5 (Kummer theory)**.** *For a p-adic local field we have*

$$H^i(K, \mu_m) = \begin{cases} K^\times/(K^\times)^m & \textit{for } i = 1, \\ \frac{1}{m}\mathbb{Z}/\mathbb{Z} & \textit{for } i = 2, \\ 0 & \textit{for } i \geq 3. \end{cases}$$

Furthermore, we have $H^2(K, \mu) \cong \mathbb{Q}/\mathbb{Z}$*.*

2.3.3 Tate duality

In order to state a duality theorem, one wants an explicit description of the dualizing module of the category of Gal_K-modules in question, namely discrete Gal_K-modules which are torsion as abelian groups. One can show that this is canonically isomorphic to the Gal_K-module μ of all roots of unity in $\overline{K}$. For a finite Gal_K-module A we set $A' = \mathrm{Hom}(A, \mu)$.

Theorem 2.3.6 (Tate duality)**.** *Let K be a p-adic local field. If A be a finite* Gal_K*-module, then for* $0 \leq i \leq 2$ *the cup-product*

$$H^i(K, A') \times H^{2-i}(K, A) \xrightarrow{\cup} H^2(K, \mu) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

induces an isomorphism of finite abelian groups

$$H^i(K, A') \xrightarrow{\sim} H^{2-i}(K, A)^\vee.$$

Note that for most of our applications considering finite Gal_K-modules is sufficient. However, there is a more general duality statement where A can be replaced by a Gal_K-module which is finitely generated as a $\mathbb{Z}$-module, see [NSW13, Thm. 7.2.9].

Main statement of Local Class Field Theory

The main theorem of local class field theory is the local reciprocity law, which can be phrased as follows.

Theorem 2.3.7 (Main theorem of local class field theory)**.** *Let K be a p-adic local field and let L/K be a finite Galois extension. Then there is a unique continuous map, the so called* local reciprocity map *or* Artin map*,*

$$\theta_K = (-, K)\colon K^\times \to \mathrm{Gal}_K^{\mathrm{ab}}$$

with the property that for each finite abelian extension L/K the homomorphism

$$\theta_{L/K} = (-, L/K)\colon K^\times \to \mathrm{Gal}(L/K)$$

obtained via composition of θ_K with the quotient map $\mathrm{Gal}_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$ satisfies the following properties:

(i) If L/K is unramified, then for any uniformizer π, we have $\theta_{L/K}(\pi) = \mathrm{Frob}_{L/K}$.

(ii) The homomorphism $\theta_{L/K}$ is surjective with kernel $N_{L/K}(L^\times)$, inducing $K^\times/N_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$.

Furthermore, the local reciprocity map induces a canonical isomorphism

$$\widehat{\theta}_K\colon \widehat{K^\times} \to \mathrm{Gal}_K^{\mathrm{ab}}$$

of profinite groups.

Corollary 2.3.8. *The local reciprocity map induces an isomorphism*

$$K^\times/K^{\times m} \to \mathrm{Gal}_K^{\mathrm{ab}}/m.$$

Note that by the structure theorem for units of K, we know that $\widehat{K^\times} \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$. While this isomorphism is not canonical as it requires a choice of uniformizer, taking profinite completion gives a canonical commutative diagram of exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\cong"] & K^\times \arrow[r, "v"] \arrow[d, hook, "\theta_K"] & \mathbb{Z} \arrow[r] \arrow[d, hook, "i"] & 0 \\
1 \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}}) \arrow[r] & \mathrm{Gal}_K^{\mathrm{ab}} \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(K^{\mathrm{nr}}/K) \arrow[r] & 1.
\end{tikzcd}$$

There is a connection between the local reciprocity map and the previously defined invariant map, which looks as follows.

Proposition 2.3.9. *For every $\chi \in H^1(K, \mathbb{Q}/\mathbb{Z})$ we have*

$$\chi((a, K)) = \mathrm{inv}_K(a \cup \delta\chi),$$

where δ is the connecting homomorphism $\delta\colon H^1(K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(K, \mathbb{Z})$.

2.4 Group presentations of profinite groups

To simplify the discussion, we now denote by $\mathcal{C}$ any class of finite groups that is closed under the formation of subgroups, homomorphic images and extensions. A *pro-$\mathcal{C}$ group* is an inverse limit of an inverse system of groups in the class $\mathcal{C}$. So if we take $\mathcal{C}$ to be the collection of all finite groups, this leads us to the notion of profinite groups. If we take $\mathcal{C}$ to be all groups of p-power order, where p is some prime, this corresponds to our previous notion of pro-p groups. One defines the notion of *pro-$\mathcal{C}$* completion, and *free pro-$\mathcal{C}$* analogously to these special cases.

Definition 2.4.1 (Presentation of profinite groups)**.** Let G be a finitely generated pro-$\mathcal{C}$ group, and suppose that X is a system of generators the G with $|X| = n$. Let F be the free pro-$\mathcal{C}$ group on X. The exact sequence

$$1 \to R \to F \to G \to 1$$

is called a *presentation of* G *as a pro-$\mathcal{C}$-group.*

Let S be a set convergent to 1 of topological generators of R as a normal subgroup of F. Then G is completely determined by X and S, and we often write $G = \langle X \mid S\rangle$. We call S a *system of relations.* A system of relations is said to be *minimal* if no proper subset of S generates R. In that case we denote the cardinality by $d_F(G)$. If $d_F(R) < \infty$, we say that above presentation is a finite presentation of G and that G is *finitely presentable.* If $n = d(G)$, we call it a *minimal presentation* of G as a profinite group. We define the *relation rank* of a group G to be the smallest $d_F(R)$ for any presentation of G and denote it by $r(G) = r_{\mathcal{C}}(G)$.

Presentations of pro-$\mathcal{C}$ groups are essentially unique in a strong sense. In fact, this makes the theory much easier than in the case of discrete groups.

Proposition 2.4.2. *Let G be a finitely generated pro-$\mathcal{C}$ group and let $d(G) = d \leq m \leq n < \infty$. Let F be the free pro-$\mathcal{C}$ group of rank n.*

(i) (Gaschütz Lemma) Let $\varphi : F \longrightarrow G$ be a continuous epimorphism. Then there exists a basis

$$\{x_1, \dots, x_m, x_{m+1}, \dots, x_n\}$$

of F such that $\varphi(x_{m+1}) = \dots = \varphi(x_n) = 1$. Consequently, if we put $F' = \overline{\langle x_1, \dots, x_m\rangle}$, the restriction $\varphi|_{F'} \colon F' \to G$ is an epimorphism from the free pro-$\mathcal{C}$ group F' onto G. If $m = d$, this defines a minimal pro-$\mathcal{C}$ presentation for G.

(ii) Let

$$1 \to R_i \to F \overset{\varphi_i}{\to} G \to 1, \quad \textit{for } i = 1, 2,$$

be two presentations of G as pro-$\mathcal{C}$ group. Then there exists an automorphism $\tau : F \longrightarrow F$ of F such that $\tau(R_1) = R_2$. In particular the generator ranks of R_1 and R_2 as subgroups of F agree, i.e. $d_F(R_1) = d_F(R_2)$.

(iii) Given two presentations

$$1 \to R_1 \to F_1 \to G, \quad 1 \to R_2 \to F_2 \to G,$$

of G as a pro-$\mathcal{C}$ group such that $\operatorname{rank}(F_1) \leq \operatorname{rank}(F_2) < \infty$, *then $d_{F_1}(R_1) \leq d_{F_2}(R_2)$. In particular, given a minimal presentation $1 \to R \to F \to G$ of G as a pro-$\mathcal{C}$ group, we have $r(G) = d_F(G)$.*

Proof. See [RZ00, Prop. C.1.1]. □

Note that, as a consequence, a pro-$\mathcal{C}$ group G is finitely presentable as a profinite group if and only if it is finitely presentable as a pro-$\mathcal{C}$ group. See [Lub01, Cor. 1.2].

We take a closer look at the example of pro-p groups which will be of particular interest for us. First, we recall that for a pro-p group G the cohomology group $H^1(G, \mathbb{F}_p)$ is Pontryagin dual to $G/\Phi(G)$, namely

$$H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p) = \mathrm{Hom}(G/\Phi(G), \mathbb{F}_p).$$

If G is finitely generated and $\mathcal{X} = \{x_1, \ldots, x_d\}$ is a minimal set of generators of G, then $H^1(G, \mathbb{F}_p)$ has a basis of generators $\mathcal{X}^* = \{\chi_1, \ldots, \chi_d\}$ dual to $\mathcal{X}$, i.e. we have $\chi_i(x_j) = \delta_{ij}$. A short exact sequence of pro-p groups

$$1 \to R \to F \to G \to 1$$

is a *minimal presentation* of F if F is a free pro-p group and $R \subseteq \Phi(F)$. This is equivalent to saying that the induced inflation map by the epimorphism $F \to G$ induces an isomorphism

$$\mathrm{infl}\colon H^1(G, \mathbb{F}_p) \xrightarrow{\sim} H^1(F, \mathbb{F}_p).$$

Using the fact that free pro-p groups have cohomological dimension 1, the five-term sequence from Proposition 2.2.10 for a topological G-module is of the form

$$0 \to H^1(G, \mathbb{F}_p) \xrightarrow{\mathrm{infl}} H^1(F, \mathbb{F}_p) \xrightarrow{\mathrm{res}} H^1(R, \mathbb{F}_p)^F \xrightarrow{\mathrm{tg}} H^2(G, \mathbb{F}_p) \to 0.$$

Hence, the map tg is also an isomorphism. By duality one has

$$(R/R^p[R, F])^\vee \cong H^1(R, \mathbb{F}_p)^F \xrightarrow{\mathrm{tg}} H^2(G, \mathbb{F}_p),$$

meaning that the defining relations of G grive rise to a $\mathbb{F}_p$-basis of $R/R^p[R, F]$, yielding a basis of $H^2(G, \mathbb{F}_p)$ via tg.

In particular, this means that generator and relation rank have a nice cohomological interpretation for pro-p group, see [Ser13a, §4.2-3] for a more detailed proof of these results.

Proposition 2.4.3 (Cohomological Interpretation of Generators and Relations)**.** *Let G be a pro-p group.*

(i) $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$.

(ii) $r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$.

Note that for a profinite group G, there exists a cohomological description of the relation rank of G depending on the generator rank $d = d(G)$ due to Lubotzky [Lub01].

2.5 Automorphisms of group extensions

2.5.1 Outer automorphisms

For a (profinite) group G let $\mathrm{Aut}(G)$ denote the group of all (continuous) automorphisms of G. We consider $\mathrm{Aut}(G)$ acting on G on the left. The subgroup of *inner automorphisms* of G is denoted by $\mathrm{Inn}(G)$. We denote by $Z(G)$ the *center* of G. If G has trivial center, we also say that it is *center-free*. For a subgroup $H \subseteq G$ we denote by $C_G(H)$ the centralizer and $N_G(H)$ the normalizer of H in G.

Proposition 2.5.1. *The continuous homomorphism $G/Z(G) \to \operatorname{Inn}(G)$ is a bijection.*

Lemma 2.5.2. *If G is center-free, we may identify $G \xrightarrow{\sim} \operatorname{Inn}(G)$.*

As an important example we note the following.

Proposition 2.5.3. *Let $K/\mathbb{Q}_p$ be a p-adic local field. The absolute Galois group Gal_K is center-free.*

Proof. Let $\sigma \in Z(\operatorname{Gal}_K)$ then $\sigma \operatorname{Gal}_L \sigma^{-1} = \operatorname{Gal}_L$ for all L/K finite, and hence $\sigma(L) = L$ by Galois theory. We have a diagram

$$\begin{tikzcd}
L^\times \arrow[r, "\sigma|_L"] \arrow[d, "\theta_L"] & L^\times \arrow[d, "\theta_L"] \\
\operatorname{Gal}_L^{\mathrm{ab}} \arrow[r, "\mathrm{Ver}"] & \operatorname{Gal}_L^{\mathrm{ab}},
\end{tikzcd}$$

where the local reciprocity map θ_L is injective. The map on the bottom is given by conjugation with σ. This is just a special case of the functoriality of the reciprocity map. Since $\sigma \in Z(\operatorname{Gal}_K)$, this must be the identity. It follows that $\sigma|_L$ must be the identity. Varying L, it follows that σ must be trivial. □

The group of *outer automorphisms* is defined as the quotient $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$.

2.5.2 Well's sequence

Let

$$\mathcal{E}\colon 1 \to N \xrightarrow{\iota} \Pi \xrightarrow{\pi} \Gamma \to 1 \tag{2.5}$$

be a an extension of profinite groups. We get an induced outer action

$$\rho = \rho_{\mathcal{E}}\colon \Gamma \to \operatorname{Out}(N)$$

given by $g \mapsto s(g)(-)s(g)^{-1}$. We refer to (Γ, ρ) as the *abstract kernel* of $\mathcal{E}$. One can easily check that this is well-defined. Indeed, given two lifts $\tilde{g}, g'$ we have $\tilde{g}g'^{-1} = x$ for some $x \in N$ and hence $g'^{-1}(-)g' = \tilde{g}^{-1}x(-)x^{-1}\tilde{g}$. So the corresponding automorphisms differ only by an inner automorphism and this map does not depend on the choice of section s. Note that however, this induces an ordinary action on the center $Z = Z(N)$ of N which we will denote by

$$\rho_0\colon Q \to \operatorname{Aut}(Z).$$

Let $\operatorname{Aut}^*(\Pi)$ denote the subgroup of $\operatorname{Aut}(\Pi)$ of automorphisms respecting the short exact sequence above, i.e. those $\beta \in \operatorname{Aut}(\Pi)$ restricting to automorphisms $\beta|_N := A(\beta) = \alpha$ of N, and inducing automorphisms $\overline{\beta} := C(\beta) = \gamma$ on the quotient Γ. We are interested in studying the following map:

$$\begin{aligned} \Theta\colon\ \operatorname{Aut}^*(\Pi) &\to \operatorname{Aut}(N) \times \operatorname{Aut}(\Gamma), \\ \beta &\mapsto (A(\beta), C(\beta)). \end{aligned}$$

Let $Z^1_\rho(\Gamma, Z)$ be the set of 1-cocycles, i.e. continuous 1-cochains $a\colon \Gamma \to Z$ such that

$$a(gh) = a(g)s(g)a(h)s(g)^{-1} \quad \text{for } g, h \in \Gamma.$$

Proposition 2.5.4. *There is a natural exact sequence*

$$1 \to Z^1_\rho(\Gamma, Z) \to \mathrm{Aut}^*(\Pi) \to \mathrm{Aut}(N) \times \mathrm{Aut}(\Gamma). \tag{2.6}$$

Proof. Let

$$\mathrm{Aut}_0(\Pi) := \ker(\Theta) = \ker(A) \cap \ker(C)$$

To prove (2.6) we have to give an isomorphism $Z^1_\rho(\Gamma, Z) \cong \mathrm{Aut}_0(\Pi)$. Let $\varphi \in \mathrm{Aut}_0(\Pi)$. Every element of Π is mapped to the same N-coset, i.e. $\varphi(g) = a(g)g$ with $a(g) \in N$. As the restriction of φ to N is the identity, this is indeed independent of the choice of representative. Hence a factors through Γ, i.e. we get a map $a\colon \Gamma \to N$. The image lies in the center of N. Indeed, for $n \in N, g \in \Pi$ we have

$$\begin{aligned} \varphi(ng) &= a(ng)ng = a(g)ng, \\ \varphi(ng) &= \varphi(n)\varphi(g) = n\varphi(g) = na(g)g, \end{aligned}$$

implying $a(g)n = na(g)$. Let $g, h \in \Pi$. Using the fact that φ is a homomorphism, we have

$$a(gh)gh = \varphi(gh) = \varphi(g)\varphi(h) = a(g)ga(h)h = a(g)(C[g]a(h))gh,$$

and it follows that $a(gh) = a(g)(C[g]a(h))$. Hence, $a\colon \Gamma \to Z$ is a 1-cocycle.

Conversely, for every 1-cocycle $a : \Gamma \to Z$ we get a group homomorphism $\varphi \in \mathrm{Aut}_0(\Pi)$ via

$$\varphi(g) = a(gN)g.$$

One can easily check that these maps are inverse group homomorphisms. □

Now let $\mathrm{Inn}(\Pi, Z)$ denote the subgroup of conjugations by elements of Z.

Proposition 2.5.5. *The isomorphism* $Z^1(\Gamma, Z) \cong \mathrm{Aut}_0(\Pi)$ *maps 1-coboundaries isomorphically to* $\mathrm{Inn}(\Pi, Z)$*, inducing*

$$H^1_\rho(\Gamma, Z) \cong \mathrm{Aut}_0(\Pi)/\operatorname{Inn}(\Pi, Z) =: \mathrm{Out}_0(\Pi).$$

Proof. As before, let $\rho_0\colon \Gamma \to \mathrm{Aut}(Z)$. The coboundary $a\colon \Gamma \to Z$ given by

$$a(x) = h[\rho_0(x)h]^{-1}$$

induces the automorphism of Π

$$g \mapsto a(g)g = h[\rho_0(\pi(g))h]^{-1}g = h(ghg^{-1})^{-1}g = hgh^{-1} = C[h](g),$$

hence the inner automorphism $C[h]$ induced by h. And every inner automorphism by elements of Z is induced in this way by a 1-coboundary. □

2.6 Profinite structure of $\mathrm{Aut}(G)$ and $\mathrm{Out}(G)$

There are several natural ways of expressing a topologically finitely generated profinite group G as a projective limit of characteristic quotients. The following notation is due to Stix. Assume that G is of finite corank, i.e. there are only finitely many continuous quotients of order n for all n. We set

$$Q_n(G) = G/\bigcap_{\varphi} \ker \varphi$$

where φ ranges over all continuous homomorphisms $G \to H$ with $\#H \leq n$ (up to isomorphism). Note that

$$Q_n(G) \hookrightarrow \prod_{\varphi} H.$$

So in particular, $Q_n(G)$ is finite and the map

$$G \to \varprojlim_n Q_n(G)$$

is an isomorphism. Furthermore, the subgroup $\ker(G \to Q_n(G))$ is characteristic in G. In particular, we have

$$\mathrm{Aut}(G) = \varprojlim_n \mathrm{Aut}(Q_n(G)) \quad \text{and} \quad \mathrm{Out}(G) = \varprojlim_n \mathrm{Out}(Q_n(G)).$$

Proposition 2.6.1. *Let G be a profinite group of finite corank. Then* Aut(G) *and* Out(G) *are profinite.*

Lemma 2.6.2. *Let G be a finitely generated topological group. Then G has finite corank.*

Corollary 2.6.3. *Let G be a finitely generated profinite group. Then* Aut(G) *and* Out(G) *are profinite.*

The following result is a consequence of Proposition 2.1.7 in the case of finitely generated pro-p groups.

Lemma 2.6.4 (Λ-Frattini argument)**.** *Let P be a finitely generated pro-p group. Let $\Lambda = \mathbb{Z}/q\mathbb{Z}$ for some $q = p^s$. Then $x_1, \dots, x_n \in P$ are generators of P if and only if $\overline{x}_1, \dots, \overline{x}_n$ are generators of the Λ-module $P^{\mathrm{ab}} \otimes \Lambda$.*

Any automorphism $\sigma\colon G \to G$ induces an automorphism on the abelianization G^{ab}, which we denote by σ^{ab}, and hence an automorphism of $G^{\mathrm{ab}} \otimes \Lambda$. We may conclude the following.

Proposition 2.6.5. *Let G be a finitely generated pro-p group and $\Lambda = \mathbb{Z}/q\mathbb{Z}$ for some $q = p^s$. Then*

$$\ker\Big(\mathrm{Aut}(G) \to \mathrm{Aut}(G^{\mathrm{ab}} \otimes \Lambda)\Big)$$

is a pro-p group.

Proof. We first assume that G is a finite p-group, and let n be minimal number of generators of G. Let K denote the group of automorphisms of G such that the induced map on $G^{\mathrm{ab}} \otimes \Lambda$ is the identity. We fix a set $x_1, \dots, x_n$ of generators of $G^{\mathrm{ab}} \otimes \Lambda$. The group K acts freely on the group

$$\left\{ (y_1, \dots, y_n) \middle| \text{ min. system of generators of } G \text{ such that } y_i \equiv x_i \text{ in } G^{\mathrm{ab}} \otimes \Lambda \right\},$$

which we shall denote by T_G. Let $N = \ker(G \to G^{\mathrm{ab}} \otimes \Lambda)$. Note that this is a p-group, and $\#T_G = (\#N)^n$ by Lemma 2.6.4. Since K acts freely on T_G, it follows that $\#K \mid \#T_G$, and is hence a p-group. Passing to pro-p groups is now a standard argument. □

Note that in the same way we can conclude that

$$\ker\Big(\mathrm{Out}(G) \to \mathrm{Aut}(G^{\mathrm{ab}} \otimes \Lambda)\Big)$$

is a pro-p group as inner automorphisms induce the identity on the abelianization.

3 Anabelian Geometry of Gal_K

Anabelian geometry is an area of arithmetic geometry studying what information about the geometry and arithmetic of (geometric) objects is encoded in the arithmetic fundamental groups. Classically, one asks whether an object can be classified by its fundamental group up to isomorphism. So taking two geometric objects, one would for example study the relationship between their set of isomorphisms and the set of isomorphisms of the respective fundamental groups. In contrast, one may also study a single object, and ask what information, e.g. invariants can be recovered purely from the topological group structure of the respective fundamental group. Mochizuki refers to these two different points of view as *bi-anabelian geometry* and *mono-anabelian geometry*, respectively.

In this chapter we discuss some known results in this direction for the case of p-adic local fields.

3.1 Reconstruction algorithms

Let p be a prime, and let $K/\mathbb{Q}_p$ be a finite extension. In this section we shall give a quick recap of how to reconstruct invariants of K from the absolute Galois group Gal_K.

3.1.1 The induced map between Galois groups

Let $L/\mathbb{Q}_p$ be a finite extension, and assume there exists a field isomorphism $\alpha\colon K \to L$. Let $\overline{K}$ and $\overline{L}$ denote some (fixed) algebraic closure of K and L, respectively and let $i_K\colon K \to \overline{K}$ and $i_L\colon L \to \overline{L}$ denote the respective embeddings of K, L. By the universal property of the algebraic closure, there exists a field homomorphism $\overline{\alpha}\colon \overline{K} \to \overline{L}$ such that the following diagram commutes

$$\begin{tikzcd}
\overline{K} \arrow[r, "\overline{\alpha}"] & \overline{L} \\
K \arrow[u, "i_K"] \arrow[r, "\sim", "\alpha"'] & L. \arrow[u, "i_L"']
\end{tikzcd}$$

We denote the set of such pairs $(\alpha, \overline{\alpha})$ by $\mathrm{Isom}((\overline{K}/K), (\overline{L}/L))$. Furthermore, we denote by $\mathcal{A}$ the category consisting of objects $\overline{K}/K$, denoting the tripel $(K, \overline{K}, i_K)$, and morphisms being elements of $\mathrm{Isom}((\overline{K}/K), (\overline{L}/L))$.

Given a field extension L/K, and an isomorphism $\alpha\colon K \to L$, we get an isomorphism on absolute Galois groups

$$\begin{aligned}\Phi(\overline{\alpha}) = \Phi_{K,L}(\overline{\alpha})\colon\ \mathrm{Gal}_K &\xrightarrow{\sim} \mathrm{Gal}_L, \\ \sigma &\mapsto \overline{\alpha} \circ \sigma \circ \overline{\alpha}^{-1}. \end{aligned} \tag{3.1}$$

Note that for a different choice of extension $\overline{\alpha}'$ of α the image $\Phi(\overline{\alpha}')$ varies from $\Phi(\overline{\alpha})$ only by an inner automorphism of Gal_L. Namely, we have

$$(\overline{\alpha}' \circ \overline{\alpha}^{-1}) \circ \Phi(\overline{\alpha})(\sigma) \circ (\overline{\alpha}' \circ \overline{\alpha}^{-1})^{-1} = \Phi(\overline{\alpha}')(\sigma), \quad \text{for } \sigma \in \mathrm{Gal}_K .$$

Choosing an inner automorphism of Gal_L, i.e. the conjugation by some $\overline{\beta} \in \mathrm{Gal}_L$, we have

$$\overline{\beta} \circ \Phi(\overline{\alpha})(\sigma) \circ \overline{\beta}^{-1} = \Phi(\overline{\beta} \circ \overline{\alpha})(\sigma).$$

Setting

$$\mathrm{OutIsom}(\mathrm{Gal}_K, \mathrm{Gal}_L) = \mathrm{Isom}(\mathrm{Gal}_K, \mathrm{Gal}_L)/\operatorname{Inn}(\mathrm{Gal}_L)$$

we get a well-defined map

$$\Phi = \Phi_{K,L} \colon \mathrm{Isom}(K, L) \to \mathrm{OutIsom}(\mathrm{Gal}_K, \mathrm{Gal}_L) \tag{3.2}$$

by mapping any isomorphism $\alpha \colon K \to L$ to the equivalence class of $\Phi(\overline{\alpha})$ for any extension $\overline{\alpha}$ of α. Alternatively, one can also write down this map, avoiding the use of equivalence classes, as follows:

$$\begin{aligned} \Phi \colon \mathrm{Isom}((\overline{K}/K), (\overline{L}/L)) &\to \mathrm{Isom}(\mathrm{Gal}_K, \mathrm{Gal}_L), \\ (\alpha, \overline{\alpha}) &\mapsto \Phi(\overline{\alpha}). \end{aligned}$$

In fact, this induces a functor from $\mathcal{A}$ to the category of profinite groups.

Theorem 3.1.1. *Let L, K be p-adic local fields. Then the map*

$$\begin{aligned} \Phi \colon \mathrm{Isom}((\overline{K}/K), (\overline{L}/L)) &\to \mathrm{Isom}(\mathrm{Gal}_K, \mathrm{Gal}_L), \\ (\alpha, \overline{\alpha}) &\mapsto \Phi(\overline{\alpha}) \end{aligned}$$

is injective but (in general) not surjective. Furthermore, the isomorphism class of a p-adic local field is not determined by the isomorphism class of its absolute Galois group.

Proof. Let $\overline{\alpha}, \overline{\beta} \in \mathrm{Isom}(\overline{K}, \overline{L})$ with $\overline{\alpha}|_K = \alpha$ and $\overline{\beta}|_L = \beta$ such that $\Phi(\overline{\alpha}) = \Phi(\overline{\beta})$, which we shall denote by φ. Consider the induced automorphism on the abelianization

$$\begin{aligned} \varphi^{\mathrm{ab}} \colon \mathrm{Gal}_K^{\mathrm{ab}} &\to \mathrm{Gal}_L^{\mathrm{ab}} \\ \sigma &\mapsto \overline{\alpha} \circ \sigma \circ \overline{\alpha}^{-1}|_{L^{\mathrm{ab}}} = \overline{\beta} \circ \sigma \circ \overline{\beta}^{-1}|_{L^{\mathrm{ab}}}. \end{aligned}$$

The reciprocity maps are compatible with $\overline{\alpha}$ and $\overline{\beta}$ respectively. Hence, we get commutative diagrams

$$\begin{tikzcd} \mathrm{Gal}_K^{\mathrm{ab}} \arrow[r, "\varphi^{\mathrm{ab}}"] & \mathrm{Gal}_L^{\mathrm{ab}} \\ K^\times \arrow[u, hook, "\theta_K"] \arrow[r, "\alpha"] & L^\times, \arrow[u, hook, "\theta_L"'] \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Gal}_K^{\mathrm{ab}} \arrow[r, "\varphi^{\mathrm{ab}}"] & \mathrm{Gal}_L^{\mathrm{ab}} \\ K^\times \arrow[u, hook, "\theta_K"] \arrow[r, "\beta"] & L^\times. \arrow[u, hook, "\theta_L"'] \end{tikzcd}$$

As θ_L is injective, it follows that $\alpha = \beta$.

In order to show that $\overline{\alpha} = \overline{\beta}$, we consider a finite extension M/K, we denote by N/L the finite extension such that $\mathrm{Gal}_N = \varphi(\mathrm{Gal}_M)$. As per assumption $\Phi(\overline{\alpha}) = \Phi(\overline{\beta})$, we have $N = \overline{\alpha}(M) = \overline{\beta}(M)$. Note that

$$\varphi_M = \overline{\alpha} \circ (-) \circ \overline{\alpha}^{-1}|_{\mathrm{Gal}_M} = \overline{\beta} \circ (-) \circ \overline{\beta}^{-1}|_{\mathrm{Gal}_M}$$

defines

$$\varphi_M = \varphi|_{\mathrm{Gal}_M} \colon \mathrm{Gal}_M \to \mathrm{Gal}_N\,.$$

Applying the previous argument to $(\overline{\alpha}, \overline{\alpha}|_M)$ and $(\overline{\beta}, \overline{\beta}|_M)$, it follows that $\overline{\alpha}|_M = \overline{\beta}|_M$. Taking the limit over all finite extensions M/K we can conclude $\overline{\alpha} = \overline{\beta}$.

For the failure of surjectivity, one has to show that there exists non-isomorphic finite extension of $\mathbb{Q}_p$ that have isomorphic absolute Galois groups. Such an example can be found using the result by Jarden–Ritter below. □

Theorem 3.1.2 (Jarden–Ritter, [JR79]). *Let K, L be finite extensions of $\mathbb{Q}_p$. Assume $\mu_p \subseteq K$. Then the following are equivalent:*

(i) The absolute Galois groups Gal_K and Gal_L are isomorphic.

(ii) $[K : \mathbb{Q}_p] = [L : \mathbb{Q}_p]$, and the maximal abelian subfield $K_0 = K \cap \mathbb{Q}_p(\mu_\infty)$ is isomorphic to the maximal abelian subfield $L_0 = L \cap \mathbb{Q}_p(\mu_\infty)$.

In [JR79] Jarden and Ritter provide explicit examples of non-isomorphic finite extensions of $\mathbb{Q}_p$ that have isomorphic absolute Galois groups. We discuss another way of showing that (3.2) is not surjective in the case $L = K$ in Section 3.2.

A central result in anabelian geometry of p-adic local fields is the characterization of the image of this map due to Mochizuki. For this, let $\mathrm{Isom}_{\mathrm{filt}}(\mathrm{Gal}_K, \mathrm{Gal}_L)$ denote the subset of isomorphisms of profinite groups respecting the filtration on Gal_K and Gal_L, respectively, given by the higher, i.e. index > 0, ramification groups in the upper numbering. For a definition, see e.g. [Ser13b, Ch. IV].

Theorem 3.1.3 (Mochizuki). *Let L, K be finite extensions of $\mathbb{Q}_p$. Then the map*

$$\begin{aligned}\Phi \colon \mathrm{Isom}((\overline{K}/K), (\overline{L}/L)) &\to \mathrm{Isom}_{\mathrm{filt}}(\mathrm{Gal}_K, \mathrm{Gal}_L),\\ (\alpha, \overline{\alpha}) &\mapsto \Phi(\overline{\alpha}),\end{aligned}$$

is bijective.

For a proof of this result, see [Moc97]. Injectivity follows from the injectivity proved in Theorem 3.1.1. The difficult part is the surjectivity, which requires taking a different point of view. Roughly speaking, for any finite extension $E/\mathbb{Q}_p$, an isomorphism $f \colon \mathrm{Gal}_K \to \mathrm{Gal}_L$ induces an equivalence

$$f^* \colon \mathrm{Rep}_{\mathrm{Gal}_K}(E) \to \mathrm{Rep}_{\mathrm{Gal}_L}(E)$$

between continuous Gal_K-, and Gal_L-representations in finite dimensional E-vector spaces, respectively. We call f *Hodge-Tate*, if f^* maps Hodge-Tate representations to Hodge-Tate representations. It turns out that this property is equivalent to the condition that f is compatible with the ramification filtration, and Mochizuki shows that this in fact implies that f comes from a field isomorphism.

We will not use this point of view in the rest of this thesis. However, we will take a brief look at the related question what invariants of a p-adic local field can be recovered purely from its absolute Galois group.

3.1.2 Reconstructions from Gal_K

We first ought to explain what it means to reconstruct invariants of K group theoretically from Gal_K. Namely, for any finite extension $L/\mathbb{Q}_p$ and any isomorphism of absolute Galois groups $\varphi\colon \mathrm{Gal}_K \xrightarrow{\sim} \mathrm{Gal}_L$ the invariant of K must correspond to the respective invariant of L under φ. Less vaguely, one can define this as follows.

Definition 3.1.4. For some suitable category $\mathcal{D}$, let $F\colon \mathcal{A} \to \mathcal{D}$ be a functor. A *method of reconstruction* of an object $F(\overline{K}/K)$ from Gal_K consists of a map

$$r_{\overline{K}/K,\overline{L}/L}\colon \mathrm{Isom}(\mathrm{Gal}_K, \mathrm{Gal}_L) \to \mathrm{Isom}(F(\overline{K}/K), F(\overline{L}/L))$$

for any pair $(\overline{K}/K), (\overline{L}/L)$ such that r is functorial and

$$r_{\overline{K}/K,\overline{L}/L}(\Phi(\overline{\alpha})) = F((\alpha, \overline{\alpha}))$$

for all $(\alpha, \overline{\alpha}) \in \mathrm{Hom}_{\mathcal{A}}((\overline{K}/K), (\overline{L}/L))$. If a method of reconstruction exists, we say that $F(\overline{K}/K)$ can be *reconstructed (group theoretically) from* Gal_K.

Now we shall reconstruct some invariants.

Proposition 3.1.5. *The* Gal_K*-module* $\mu(\overline{K})$ *can be reconstructed from* Gal_K*.*

Proof. Consider the short exact sequence of Gal_K-modules induced by the reciprocity map from Theorem 2.3.7

$$1 \to \mathcal{O}_K^\times \xrightarrow{\theta_K} \mathrm{Gal}_K^{\mathrm{ab}} \to \widehat{\mathbb{Z}} \to 1.$$

We have the same short exact sequence for any finite Galois extension L/K

$$1 \to \mathcal{O}_L^\times \xrightarrow{\theta_L} \mathrm{Gal}_L^{\mathrm{ab}} \to \widehat{\mathbb{Z}} \to 1,$$

where θ_L is a homomorphism of $\mathrm{Gal}(L/K)$-modules or rather of Gal_K-modules. Here Gal_K acts on Gal_L (and hence on $\mathrm{Gal}_L^{\mathrm{ab}}$) by conjugation. Passing to the torsion subgroup, we get an isomorphism

$$\theta_L\colon \mu(L) \xrightarrow{\sim} (\mathrm{Gal}_L^{\mathrm{ab}})_{\mathrm{tors}},$$

which is a Gal_K-module isomorphism. Furthermore, for $K \subseteq L \subseteq L'$ we have the following commutative diagram

$$\begin{tikzcd}
\mu(L) \arrow[r, "\theta_L"] \arrow[d, "i"] & (\mathrm{Gal}_L^{\mathrm{ab}})_{\mathrm{tors}} \arrow[d, "\mathrm{Ver}"] \\
\mu(L') \arrow[r, "\theta_{L'}"] & (\mathrm{Gal}_{L'}^{\mathrm{ab}})_{\mathrm{tors}}.
\end{tikzcd}$$

Hence, we can reconstruct the Gal_K-module $\mu(L)$ as well as the inclusion $\mu(L) \subseteq \mu(L')$ group theoretically. Finally, we can reconstruct the Gal_K-module

$$\mu(\overline{K}) = \varinjlim_{L/K} \mu(L).$$

□

Corollary 3.1.6. *The cyclotomic character* $\chi\colon \mathrm{Gal}_K \to \widehat{\mathbb{Z}}^\times$ *can be reconstructed from* Gal_K.

Proof. As the cyclotomic character is given by the Gal_K-action on $\mu(\overline{K})$, this follows from Proposition 3.1.5. □

As always, let $q = q(K)$ denote the residue degree of K. In order to reconstruct q we need the following result.

Lemma 3.1.7. *The roots of unity in* K *of order coprime to* p *are precisely the* $(q-1)$*th roots of unity* $\mu_{q-1}(\overline{K})$.

Corollary 3.1.8. *The residue degree* $q = q(K)$ *of* K*, the characteristic of the residue field* $\mathbb{F}_K$ *and multiplicative group* $\mathbb{F}_K^\times$ *can be reconstructed from* Gal_K.

Proof. In fact, the multiplicative group $\mathbb{F}_K$ corresponds to the prime-to-p roots of unity $\mu'(K)$ and $\mu(K)$ are the Gal_K-invariants of $\mu(\overline{K})$, which is reconstructed in Proposition 3.1.5. Thus, we have $q = 1 + \#\mu'(K)$. □

Proposition 3.1.9. *The degree* $[K : \mathbb{Q}_p]$ *of the field extension* $K/\mathbb{Q}_p$ *can be reconstructed from* Gal_K*. Furthermore, the absolute ramification index* $e_K = e(K/\mathbb{Q}_p)$ *as well as the absolute inertia degree* $f_K = f(K/\mathbb{Q}_p)$ *can be reconstructed.*

Proof. It holds that

$$\begin{aligned}
[K : \mathbb{Q}_p] &= \dim_{\mathbb{F}_p} H^1(K, \mu_p) - 1 - \dim_{\mathbb{F}_p} \mu_p(K) \\
&= \dim_{\mathbb{F}_p} H^1(K, \mu_p) - \dim_{\mathbb{F}_p} H^2(K, \mu_p) - \dim_{\mathbb{F}_p} H^0(K, \mu_p) \\
&= -\sum_{i=0}^{2} (-1)^i \dim_{\mathbb{F}_p} H^i(K, \mu_p) \\
&= -\chi_p(K, \mu_p) = -\chi_p(K, \mathbb{Z}/p\mathbb{Z}).
\end{aligned}$$

As

$$[K : \mathbb{Q}_p] = e_K \cdot f_K,$$

and we can reconstruct the cardinality of the residue field $q = p^{f_K}$ by Corollary 3.1.8, we can reconstruct e_K and f_K. □

Corollary 3.1.10. *The inertia subgroup* I_K *can be reconstructed from* Gal_K.

Proof. Recall that we have

$$I_K = \lim_{L/K \text{ Galois}} \mathrm{Gal}(L/L^{\mathrm{nr}}).$$

Now for any open subgroup H corresponding to a Galois extension L/K we may reconstruct the respective (absolute) ramification index e_L and inertia degree f_L and by multiplicativity of these invariants, we may reconstruct the relative ramification index and inertia index $e(L/K)$ and $f(L/K)$. Now L/K is unramified if and only if $e(L/K) = 1$. Thus, it is possible to determine the open subgroups H of Gal_K corresponding to unramified extensions, and in particular the subgroup corresponding to the maximal unramified subextension $L/L^{\mathrm{nr}}/K$. Hence, we can determine $\mathrm{Gal}(L/L^{\mathrm{nr}})$ from Gal_K and $\mathrm{Gal}_L \subseteq \mathrm{Gal}_K$, which shows the claim. □

Corollary 3.1.11. *The wild inertia V_K can be reconstructed from* Gal_K*.*

Proof. This follows from the previous result as V_K is the p-Sylow subgroup of I_K. □

Corollary 3.1.12. *The unit group $\mathcal{O}_K^\times$, the group of principal units $U_K^{(1)}$, and the class of Frobenius in $\Gamma_K = \mathrm{Gal}_K / I_K$ can be reconstructed from* Gal_K*.*

Proof. The first two claims follow using local reciprocity as $\mathcal{O}_K^\times = \ker(\mathrm{Gal}_K^{\mathrm{ab}} \to \mathrm{Gal}_K / I_K)$ and $U_K^{(1)} = \ker(\mathrm{Gal}_K^{\mathrm{ab}} \to (\mathrm{Gal}_K / V_K)^{\mathrm{ab}})$. The Frobenius in Gal_K / I_K can be completely determined by its action on the Gal_K-module $\mu(\overline{K})$ as the maximal unramified extension K^{nr} is contained in the maximal cyclotomic extension of K. □

As it is a central argument in Chapter 4, we furthermore note the following.

Lemma 3.1.13. *The cyclotomic character $\overline{\chi}$ on the residue field $\mathbb{F}_K$ of K*

$$\begin{tikzcd}
\mathrm{Gal}_K \arrow[r, "\chi"] \arrow[d, two heads] & \widehat{\mathbb{Z}}^\times \arrow[d, two heads] \\
\Gamma_K = \mathrm{Gal}_{\mathbb{F}_K} \arrow[r, "\overline{\chi}"] & (\widehat{\mathbb{Z}}')^\times \\
\mathrm{Frob}_K \arrow[r, mapsto] & q
\end{tikzcd}$$

is injective.

Proof. The algebraic closure of $\mathbb{F}_K$ is generated by the prime-to-p roots of unity μ'. □

3.2 Geometric automorphisms

Recall that by construction (3.1) we have a map

$$\mathrm{Aut}(K) \to \mathrm{Out}(\mathrm{Gal}_K), \quad \alpha \mapsto \Phi(\alpha) = [\Phi(\overline{\alpha})] \tag{3.3}$$

given in the following way. Choose an algebraic closure $i_K : K \to \overline{K}$ and extend $\alpha \in \mathrm{Aut}(K)$ to $\overline{\alpha} \in \mathrm{Aut}(\overline{K})$ such that $\overline{\alpha} \circ i_K = i_K \circ \alpha$. This induces a continuous automorphism

$$\Phi(\overline{\alpha})\colon \ \mathrm{Gal}_K \to \mathrm{Gal}_K, \quad \sigma \mapsto \overline{\alpha} \circ \sigma \circ \overline{\alpha}^{-1}.$$

This is well-defined up to an inner automorphism of Gal_K. Choosing $\Phi(\alpha)$ to be the equivalence class of $\Phi(\overline{\alpha})$ yields the desired map. Furthermore, this map is injective, which is a special case of Theorem 3.1.1.

Definition 3.2.1. We call the image of $\mathrm{Aut}(K)$ in $\mathrm{Out}(\mathrm{Gal}_K)$ under the above emdedding the *group of geometric automorphisms* of Gal_K and also denote this by $\mathrm{Aut}(K)$.

Theorem 3.1.3 yields a description of the image of (3.3). Namely, for any automorphism $\sigma\colon \mathrm{Gal}_K \to \mathrm{Gal}_K$ the outer automorphism determined by σ is contained in the image of Φ if and only if it is compatible with the ramification filtration on Gal_K, i.e. we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Aut}(K) \arrow[r, hook] \arrow[dr, "\cong"] & \mathrm{Out}(\mathrm{Gal}_K) \\
& \mathrm{Out}_{\mathrm{filt}}(\mathrm{Gal}_K), \arrow[u, hook]
\end{tikzcd}$$

where $\mathrm{Out}_{\mathrm{filt}}(\mathrm{Gal}_K)$ denotes the group of outer automorphisms compatible with the ramification filtration on Gal_K.

A natural question to ask is whether $\mathrm{Out}(\mathrm{Gal}_K)$ is non-trivial for any p-adic number field K, i.e. whether there exists a non-inner automorphism. This is indeed true.

Proposition 3.2.2 (Jannsen–Wingberg)**.** *Let $p \neq 2$ be a prime and let $K/\mathbb{Q}_p$ be a finite extension. The group $\mathrm{Out}(\mathrm{Gal}_K)$ is non-trivial.*

Remark 3.2.3. This is also true for $p = 2$ when $\sqrt{-1} \in K$ (see Remark 3.2.17).

Whenever $\mathrm{Aut}(K)$ is non-trivial, this may not be so surprising (at least up to discussing whether the induced automorphism on Gal_K is inner). However, this is not always the case, as e.g. the only automorphism of $K = \mathbb{Q}_p$ is the identity. However, the previous statement holds true regardless and for any p-adic number field K we can even prove the following.

Proposition 3.2.4. *There exists a non-inner automorphism of Gal_K which does not arise from any automorphism of the field K.*

This may be deduced from results on the structure of Gal_K due to Jannsen and Wingberg, which we shall recall in the next section.

3.2.1 The work of Jannsen and Wingberg and finite presentation of Gal_K

First, we recall some basic facts about the Galois theory of local fields. The maximal unramified quotient $\Gamma_K = \mathrm{Gal}(K^{\mathrm{nr}}/K)$ is a pro-cyclic group topologically generated by the Frobenius automorphism, and canonically isomorphic to $\widehat{\mathbb{Z}}$. We have a short exact sequence

$$1 \to \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) \to \mathrm{Gal}(K^{\mathrm{tr}}/K) \to \Gamma_K \to 1,$$

which splits after choosing a preimage of the Frobenius. Hence, $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ is a semi-direct product. In fact, the following holds.

Theorem 3.2.5 (Iwasawa)**.** *The Galois group $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ of the maximal tamely ramified extension of a local field K is isomorphic to the profinite group generated by two elements σ, τ with the only relation*

$$\sigma\tau\sigma^{-1} = \tau^q,$$

which we call the Iwasawa group to the parameter q, and so

$$\mathrm{Gal}(K^{\mathrm{tr}}/K) \simeq \mathrm{Iw}_q := \langle \sigma, \tau \mid \sigma\tau\sigma^{-1} = \tau^q \rangle \simeq \hat{\mathbb{Z}}'(1) \rtimes_q \hat{\mathbb{Z}}.$$

Proposition 3.2.6. *The ramification group V_K of the absolute Galois group of K is a free pro-p group of countably infinite rank. In particular, it is the maximal normal pro-p subgroup of* Gal_K .

Proof. See [NSW13, Prop. 7.5.1, Cor. 7.5.7]. □

Corollary 3.2.7. *The exact sequence*

$$1 \longrightarrow V_K \longrightarrow \mathrm{Gal}_K \longrightarrow \mathrm{Gal}(K^{\mathrm{tr}}/K) \longrightarrow 1$$

splits.

Sketch of proof. By [Ser13a, Prop. 16] a group extension

$$1 \longrightarrow H \longrightarrow G \longrightarrow \mathcal{G} \longrightarrow 1$$

of a profinite group $\mathcal{G}$ by a pro-p group H is split if if $\mathrm{cd}_p(\mathcal{G}) \leq 1$. Note that every p-Sylow subgroup of $\mathrm{Gal}(K^{\mathrm{tr}}/K) \cong \mathrm{Iw}_q$ is isomorphic to $\mathbb{Z}_p$. It follows that $\mathrm{cd}_p(\mathrm{Gal}(K^{\mathrm{tr}}/K)) = 1$, and hence the claim. □

Before quoting the famous result by Jannsen and Wingberg, we shall prove a small lemma.

Lemma 3.2.8. *Let $K/\mathbb{Q}_p$ be a p-adic local field. The order of p-power roots of unity in the maximal tamely ramified extension K^{tr} of K is finite., i.e. $\#\mu_{p^\infty}(K^{\mathrm{tr}}) = p^s$ for some non-negative integer s.*

Proof. Let L/K be a finite tamely ramified extension. We first note that the p-part of the total ramification indices of L and K agree, i.e.

$$v_p(e(L/\mathbb{Q}_p)) = v_p(e(K/\mathbb{Q}_p)).$$

Assume that L contains the totally ramified field $\mathbb{Q}_p(\mu_{p^n})$. Then we have

$$v_p(e(L/\mathbb{Q}_p)) \geq v_p(e(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)) = [\mathbb{Q}_p(\mu_{p^n}) : \mathbb{Q}_p] = p^{n-1}.$$

Hence, $n \leq 1 + \log_p(v_p(e(K/\mathbb{Q}_p))$, and the claim follows. □

Assume $p \neq 2$. Let $K/\mathbb{Q}_p$ be a finite extension of degree N and let p^s be the order of the group $\mu_{\mathrm{tr}} = \mu_{p^\infty}(K^{\mathrm{tr}})$ of all p-power roots of unity in K^{tr}/K. Let $g, h \in \mathbb{Z}_p$ be chosen such that

$$\sigma(\zeta) = \zeta^g \quad \text{and} \quad \tau(\zeta) = \zeta^h \quad \text{for } \zeta \in \mu_{\mathrm{tr}},$$

where σ, τ denote the chosen generators of $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ with defining relation $\sigma\tau\sigma^{-1} = \tau^q$. We recall the main result of Jannsen and Wingberg as stated in [NSW13].

Theorem 3.2.9 (Jannsen–Wingberg)**.** *The group Gal_K is isomorphic to the profinite group generated by $N+3$ generators $\sigma, \tau, x_0, \ldots, x_N$, subject to the following conditions.*

(i) The closed normal subgroup topologically generated by $x_0, \ldots, x_N$ is a pro-p group.

(ii) The elements σ, τ satisfy the "tame" relation

$$\sigma\tau\sigma^{-1} = \tau^q.$$

(iii) The generators satisfy a further "wild" relation, namely

a) for even N

$$x_0^\sigma = \langle x_0, \tau\rangle^g \, x_1^{p^s} \, [x_1, x_2] \, [x_3, x_4] \cdots [x_{N-1}, x_N]$$

b) and for odd N

$$x_0^\sigma = \langle x_0, \tau\rangle^g \, x_1^{p^s} \, [x_1, y_1] \, [x_2, x_3] \, [x_4, x_5] \cdots [x_{N-1}, x_N] \, ,$$

where

$$\langle x_0, \tau\rangle = \left(x_0^{h^{p-1}} \tau x_0^{h^{p-2}} \tau \cdots x_0^h \tau \right)^{\frac{\pi}{p-1}} ,$$

where π is the unique idempotent element of $\widehat{\mathbb{Z}}$ with $\pi\hat{\mathbb{Z}} = \mathbb{Z}_p$, and where y_1 is a certain element in the subgroup generated by x_1, σ, τ, described below.

Let $\alpha\colon \operatorname{Gal}(K^{\mathrm{tr}}/K) \to (\mathbb{Z}/p^s\mathbb{Z})^\times$ be the character describing the action of $\operatorname{Gal}(K^{\mathrm{tr}}/K)$ on μ_{tr}, and let $\beta\colon \operatorname{Gal}(K^{\mathrm{tr}}/K) \to \mathbb{Z}_p^\times$ be a lift of α as a map of sets. For $\rho \in \langle \sigma, \tau\rangle \subseteq \operatorname{Gal}_K$ and $x \in \operatorname{Gal}_K$ set

$$\{x, \rho\} := \left(x^{\beta(1)} \rho^2 x^{\beta(\rho)} \rho^2 \cdots x^{\beta\left(\rho^{p-2}\right)} \rho^2 \right)^{\frac{\pi}{p-1}} .$$

Writing $\tau_2 = \tau^{\pi_2}$ and $\sigma_2 = \sigma^{\pi_2}$, where π_2 is the element of $\hat{\mathbb{Z}}$ with $\pi_2\hat{\mathbb{Z}} = \mathbb{Z}_2$ the generator y_1 is given by

$$y_1 = x_1^{\tau_2^{p+1}} \left\{ x_1, \tau_2^{p+1} \right\}^{\sigma_2 \tau_2^a} \left\{ \left\{ x_1, \tau_2^{p+1} \right\}, \sigma_2 \tau_2^a \right\}^{\sigma_2 \tau_2^b + \tau_2^{\frac{p+1}{2}}} .$$

Here $a, b \in \mathbb{Z}$ are chosen such that

$$-\alpha\left(\sigma\tau^a\right) \bmod p \in \left(\mathbb{F}_p^\times\right)^2 \text{ and } -\alpha\left(\sigma\tau^b\right) \bmod p \notin \left(\mathbb{F}_p^\times\right)^2 .$$

Proof. A complete proof of Theorem 3.2.9 is given in a series of papers ([Win82], [Jan82], [JW82]). □

Corollary 3.2.10. *The isomorphism type of* Gal_K *is determined as a profinite group by the following invariants:*

(i) the residue characteristic p,

(ii) the size of the residue field q,

(iii) the degree $N = [K : \mathbb{Q}_p]$,

(iv) the tame Galois action on μ_{tr}.

Example 3.2.11. (i) Let $K = \mathbb{Q}_p$. Then $\operatorname{Gal}_{\mathbb{Q}_p}$ is generated by σ, τ, x_0, x_1 which satisfy the relations

$$\sigma\tau\sigma^{-1} = \tau^p,$$

$$\sigma x_0 \sigma^{-1} = \langle x_0, \tau\rangle x_1^p [x_1, x_1^{\tau_2^{p+1}} \{x_1, \tau_2^{p+1}\}^{\sigma_2 \tau_2^{\frac{p-1}{2}}} \{\{x_1, \tau_2^{p+1}\}, \sigma_2 \tau_2^{\frac{p-1}{2}}\}^{\sigma_2 \tau_2^{\frac{p+1}{2}} + \tau_2^{\frac{p+1}{2}}}].$$

(ii) Let $K = \mathbb{Q}_p(\zeta_p)$. Then $N = p - 1$ and Gal_K is generated by elements $\sigma, \tau, x_0, \dots, x_{p-1}$ satisfying

$$\begin{aligned} \sigma\tau\sigma^{-1} &= \tau^p, \\ \sigma x_0 \sigma^{-1} &= (x_0\tau)^{\pi}\, x_1^p\, [x_1, x_2] \cdots [x_{p-2}, x_{p-1}]\,. \end{aligned}$$

(iii) If N is even and $\alpha(\tau) = 1$, i.e. $h = 1$, the second relation becomes much easier. Namely, given generators $\sigma, \tau, x_0, x_1, \dots, x_N$ the "wild relation" is of the form

$$\sigma x_0 \sigma^{-1} = (x_0\tau)^{\pi g} x_1^{p^s} [x_1, x_2] \dots [x_{N-1}, x_N].$$

Note that this is the case e.g. when $\mu_p \subseteq K$.

The case $p = 2$ has been treated by Diekert in [Die84, Thm. 3.1] for the case where K is a 2-adic number field with $\sqrt{-1} \in K$.

Theorem 3.2.12 (Diekert)**.** *Let $K/\mathbb{Q}_2$ be a 2-adic number field of degree $N = [K : \mathbb{Q}_2]$ and assume $\mu_4 \subseteq K$. Then the absolute Galois group Gal_K is isomorphic to the profinite group generated by $N + 3$ generators $\sigma, \tau, x_0, \dots, x_N$, subject to the following defining conditions.*

(i) The closed normal subgroup topologically generated by $x_0, \dots, x_N$ is a pro-p group.

(ii) The elements σ, τ satisfy the "tame" relation

$$\sigma\tau\sigma^{-1} = \tau^q.$$

(iii) In addition, the generators satisfy a further relation:

$$\sigma x_0 \sigma^{-1} = (x_0\tau)^{\pi g} x_1^{p^s} [x_1, x_2] \dots [x_{N-1}, x_N],$$

where π denotes the idempotent element of $\widehat{\mathbb{Z}}$ such that $\pi\widehat{\mathbb{Z}} = \mathbb{Z}_2$ and $g \in \mathbb{Z}_2$ as before denotes the action of Frobenius σ on μ_{tr}.

The descriptions in Theorem 3.2.9 and Theorem 3.2.12 are not group presentations. However, condition (i) could be expressed in profinite words. Let $\pi' = 1 - \pi$ denote the idempotent element of $\widehat{\mathbb{Z}}$ such that $\pi'\widehat{\mathbb{Z}} = \prod_{\ell \neq p} \mathbb{Z}_\ell$.

(i') For all $w \in \langle\langle x_0, \dots, x_N \rangle\rangle$ we have $w^{\pi'} = 0$.

We must note that this yields infinitely many relations. So the result of Jannsen and Wingberg does not yield a finite presentation.

We use the following result by Lubotzky to show that Gal_K is in fact finitely presentable. We call a profinite group G *d-abelian-indexed* if for every finite index subgroup H, the abelianization H^{ab} is isomorphic to $\widehat{\mathbb{Z}}^r$ for $r = 1 + (d-1)(G : H)$. In particular, d is the rank of G^{ab}, which is free.

Theorem 3.2.13 (Lubotzky)**.** *Let G be a finitely generated profinite group G with $d(G) = d$. Then for the relation rank the following holds*

$$r(G) = \begin{cases} 0, & \text{if } G = \hat{F}_d \text{ free,} \\ 1, & \text{if } G \text{ is } d\text{-abelian-indexed but not free,} \\ \sup\limits_{\ell} \sup\limits_{A} \left\{ \left\lceil \frac{h^2(G,A) - h^1(G,A)}{\dim A} \right\rceil + d - \mathbb{1}_{\{\mathbb{F}_\ell \neq A\}} \right\}, & \text{otherwise.} \end{cases}$$

In the last case A runs over all finite simple $\mathbb{F}_\ell[\![G]\!]$-modules and ℓ runs over all prime numbers and $h^i(G, A) = \dim_{\mathbb{F}_\ell} H^i(G, A)$ for all i.

Proof. See [Lub01, Thm. 0.2]. □

Lubotzky then concludes that a finitely generated profinite group is finitely presented if and only if there exists a constant C such that for every prime ℓ and every finite simple $\mathbb{F}_p[\![G]\!]$-module A we have $\dim H^2(G, A) \leq C \dim A$. See [Lub01, Thm. 0.3]. For our purposes the following observation is more useful.

Corollary 3.2.14. *Let G be a finitely generated profinite group G. Assume that G is of cohomological dimension 2 and we have $\sup_\ell \chi_\ell(G, \mathbb{F}_\ell) < \infty$ where ℓ runs over all primes. Then G is finitely presentable. In particular, if G is not d-abelian-indexed, we have*

$$r(G) = d - 1 + \sup_{\ell} \chi_\ell(G, \mathbb{F}_\ell).$$

Proof. If G is a free abelian group or d-abelian-indexed, we are done. We fix a prime ℓ and a finite $\mathbb{F}_\ell[\![G]\!]$-module A and note that

$$h^2(G, A) - h^1(G, A) = \chi_\ell(G, A) - h^0(G, A).$$

It follows that

$$\begin{aligned} \left\lceil \frac{h^2(G, A) - h^1(G, A)}{\dim A} \right\rceil + d - \mathbb{1}_{\{\mathbb{F}_\ell \neq A\}} &= \left\lceil \frac{\chi_\ell(G, A) - h^0(G, A)}{\dim A} \right\rceil + d - \mathbb{1}_{\{\mathbb{F}_\ell \neq A\}} \\ &= \left\lceil \frac{\chi_\ell(G, A)}{\dim A} \right\rceil + d - 1. \end{aligned}$$

Hence, we have

$$\sup_A \left\{ \left\lceil \frac{h^2(G, A) - h^1(G, A)}{\dim A} \right\rceil + d - \mathbb{1}_{\{\mathbb{F}_\ell \neq A\}} \right\} = d - 1 + \sup_A \left\lceil \frac{\chi_\ell(G, A)}{\dim A} \right\rceil.$$

By Proposition 2.2.15 for any subgroup H of G such that $A|_H$ is trivial we have

$$\begin{aligned} \chi_\ell(G, A) &= (G : H)\chi_\ell(H, A|_H) = (G : H) \dim_{\mathbb{F}_\ell}(A)\chi_\ell(H, \mathbb{F}_\ell) \\ &= \dim_{\mathbb{F}_\ell}(A)\chi_\ell(G, \mathbb{F}_\ell). \end{aligned}$$

Thus, we have

$$r(G) = d - 1 + \sup_{\ell} \chi_\ell(G, \mathbb{F}_\ell) < \infty.$$ □

For a p-adic local field K and a finite $\mathbb{F}_\ell[\![\mathrm{Gal}_K]\!]$-module A, the Euler characteristic is

$$\chi_\ell(K,A) := \chi_\ell(\mathrm{Gal}_K, A) = h^0(\mathrm{Gal}_K, A) - h^1(\mathrm{Gal}_K, A) + h^2(\mathrm{Gal}_K, A).$$

The following holds.

Theorem 3.2.15 (Serre)**.** *Let A be a finite $\mathbb{F}_\ell[\![\mathrm{Gal}_K]\!]$-module. If $\ell \neq p$, we have $\chi_\ell(K,A) = 0$. If $\ell = p$, we have*

$$\chi_p(K,A) = -\dim_{\mathbb{F}_p}(A)[K:\mathbb{Q}_p].$$

Proof. See [NSW13, Thm. 7.3.2]. □

Theorem 3.2.16. *The absolute Galois group of a p-adic local field K is finitely presentable. If $p \neq 2$ and $\mu_p \subseteq K$, then $d(\mathrm{Gal}_K) = N+2$ and $r(\mathrm{Gal}_K) = N+1$. In particular, there exists a profinite presentation with $N+2$ generators and $N+1$ relations.*

Proof. This is now an immediate consequence of Corollary 3.2.14, Theorem 3.2.15, and the fact that Gal_K is of cohomological dimension 2, see Corollary 2.3.4.

Now in the case $\mu_p \subseteq K$ Jannsen and Wingberg show that Gal_K can be generated by $N+2$ generators. See [NSW13, Bsp. 1.4 (c)]. Hence $d \leq N+2$. On the other hand, as $\mathrm{Gal}_K^{\mathrm{ab}} \cong \widehat{K^\times}$, by Proposition 2.3.2, $\mathrm{Gal}_K^{\mathrm{ab}}$ has at least $N+2$ generators. Hence, $d \geq N+2$. It follows that $d = N+2$. Finally, Gal_K is neither free nor d-abelian indexed as e.g. $\mathrm{Gal}_K^{\mathrm{ab}}$ is not free. So it follows that

$$r(\mathrm{Gal}_K) = d - 1 + \sup_\ell \chi_\ell(K, \mathbb{F}_\ell) = d - 1 = N+1.$$

The last claim follows by a result of Lubotzky, see [Lub01, Cor. 2.5], which is a consequence of the Gaschütz lemma stated in Proposition 2.4.2. □

3.2.2 Jannsen–Wingberg automorphism

The description above enables us to prove Proposition 3.2.4. In particular, in [JW82, §5] Jannsen and Wingberg produce one explicit non-inner automorphism of Gal_K that doesn't come from a geometric automorphism. In the case $N > 1$ this is essentially based on the following identity of commutators

$$[x, yx] = xyxx^{-1}(yx)^{-1} = xyx^{-1}y^{-1} = [x,y]. \tag{3.4}$$

For the case $K = \mathbb{Q}_p$ we refer to [JW82, §5].

Proof of Proposition 3.2.4. Assume $N > 1$. We consider the generators

$$\sigma, \tau, x_0, \dots, x_N$$

on Gal_K satisfying the relations given in Theorem 3.2.9. Let $F = F_{\{\sigma,\tau,x_0,\dots,x_N\}}$ denote the free profinite group in these generators. We define a map $\psi\colon F \to F$ by setting

$$\psi(y) = \begin{cases} y & \text{for } y = \sigma, \tau, x_0, \dots, x_{N-1} \\ x_N \cdot x_{N-1} & \text{for } y = x_N. \end{cases}$$

Clearly, this is an automorphism of F. Because of (3.4) the generators

$$\sigma, \tau, x_0, \ldots, x_{N-1}, x_N \cdot x_{N-1}$$

also satisfy the relations given in the above theorem. By the universal property of the cokernel,

$$\begin{tikzcd}
F \arrow[r, "\psi", "\cong"'] \arrow[d, two heads, "p"] & F \arrow[d, two heads, "p"] \\
\mathrm{Gal}_K \arrow[r, dashed, "\psi^{\mathrm{JW}}", "\cong"'] & \mathrm{Gal}_K
\end{tikzcd}$$

this induces an automorphism $\psi^{\mathrm{JW}} = \psi_N^{\mathrm{JW}}$ of Gal_K. Of course, it remains to show two things, (1) this is not an inner automorphism, (2) this does not come from a geometric automorphism. Both of these facts can essentially be seen when passing to the abelianization. Consider the image of $\mathrm{Out}(\mathrm{Gal}_K)$ in $\mathrm{GL}_N(\mathbb{Z}_p)$ via the following maps

$$\begin{aligned}\mathrm{Out}(\mathrm{Gal}_K) \to \mathrm{Aut}_{\mathrm{Fil}}(\mathrm{Gal}_K^{\mathrm{ab}}) &\xrightarrow[\theta_K]{\sim} \mathrm{Aut}_{\mathrm{Fil}}(\widehat{K}^\times) \\ &\to \mathrm{Aut}(\mathcal{O}_K^\times) \to \mathrm{Aut}(U_K^{(1)}/\mathrm{tors}) \cong \mathrm{GL}_N(\mathbb{Z}_p),\end{aligned}$$

where $\mathrm{Aut}_{\mathrm{Fil}}(\mathrm{Gal}_K^{\mathrm{ab}})$ denotes the automorphisms of $\mathrm{Gal}_K^{\mathrm{ab}}$ compatible with the filtration given by the maximal unramified quotient. Then, after suitable choice of basis, the details of which will be discussed in Section 7.5, the image of ψ^{JW} in $\mathrm{GL}_N(\mathbb{Z}_p)$ can be described as

$$\psi \mapsto \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}.$$

Hence, ψ^{JW} cannot be an inner automorphism. As an element $\alpha \in \mathrm{Aut}(K)$ fixes $\mathbb{Q}_p$ and $K/\mathbb{Q}_p$ is finite, the image of α in $\mathrm{GL}_N(\mathbb{Z}_p)$ must be finite. Since the image of ψ^{JW} has infinite order, it follows that ψ^{JW} cannot come from a geometric automorphism. This proves the claim. □

Remark 3.2.17. Using Theorem 3.2.12, the proof of Proposition 3.2.2 works for $p = 2$ and $\mu_4 \subseteq K$ as well.

Clearly, for any even $j \geq 2$ we can define an automorphism of the free group F via $x_j \mapsto x_j \cdot x_{j-1}$ inducing an automorphism of Gal_K for the same reason. This gives us an entire class of what we refer to as *combinatorial automorphisms* of Gal_K. Specifically, we shall call this particular class of automorphisms as *Jannsen–Wingberg automorphism* and denote them by ψ_j^{JW}. We will give a new interpretation of these in Chapter 7, and give the approach above a more general framework.

3.2.3 Further results on $\mathrm{Aut}(K) \subseteq \mathrm{Out}(\mathrm{Gal}_K)$

There are further questions one can ask about the characterization of $\mathrm{Aut}(K)$ in $\mathrm{Out}(\mathrm{Gal}_K)$, some of which are stated in the introduction of [Hos19].

(fin) Is $\mathrm{Aut}(K) \subseteq \mathrm{Out}(\mathrm{Gal}_K)$ the uniquely determined maximal finite subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$?

(char) Is $\mathrm{Aut}(K) \subseteq \mathrm{Out}(\mathrm{Gal}_K)$ characteristic?

(norm) Is $\mathrm{Aut}(K) \subseteq \mathrm{Out}(\mathrm{Gal}_K)$ normal?

An affirmative answer to (fin) implies an affirmative answer to (char) and hence to (norm). A result by Hoshi [Hos19, Thm. G] states conditions under which we get a negative answer to all these questions. This is further explored by Hoshi and Nishio in [HN20], where the authors show the following.

Theorem 3.2.18 (Hoshi–Nishio, Thm.B)**.** *Assume $p \neq 2$. Let $K/\mathbb{Q}_p$ be a finite abelian Galois extension of even degree. Then the set of $\mathrm{Out}(\mathrm{Gal}_K)$-conjugates of $\mathrm{Aut}(K) \subsetneq \mathrm{Out}(\mathrm{Gal}_K)$ is infinite.*

Theorem 3.2.19 (Hoshi–Nishio, Thm.C)**.** *Under the same assumptions above the following hold.*

(i) The subgroup $\mathrm{Aut}(K) \subseteq \mathrm{Out}(\mathrm{Gal}_K)$ is not normal.

(ii) There exist infinitely many distinct subgroups of $\mathrm{Out}(\mathrm{Gal}_K)$ isomorphic to $\mathrm{Aut}(K)$.

Hoshi and Nishio claim that this means that it is not possible to establish a functorial group-theoretic reconstruction of $\mathrm{Aut}(K)$.

4 Automorphisms on the maximal tame quotient

Again for any prime p let $K/\mathbb{Q}_p$ denote a p-adic local field. The first two steps in the ramification filtration of Gal_K (in any numbering) are given by the inertia group I_K and the wild inertia group V_K, i.e. we have a filtration $V_K \subseteq I_K \subseteq \mathrm{Gal}_K$ with quotients

$$\Gamma_K = \mathrm{Gal}_K / I_K = \mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \widehat{\mathbb{Z}},$$

and $\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) \cong \widehat{\mathbb{Z}}'(1)$.

Recall that by Theorem 3.1.1 there exists an injective map

$$\Phi\colon \mathrm{Aut}(K) \hookrightarrow \mathrm{Out}(\mathrm{Gal}_K).$$

We want to study the image of $\mathrm{Aut}(K)$ on the maximal unramified, and maximal tamely ramified quotient, respectively. In this chapter we essentially prove the following four results:

(i) All automorphisms of Gal_K are trivial on the maximal unramified quotient $\Gamma_K = \mathrm{Gal}_K / I_K$ of Gal_K, see Lemma 4.1.1.

(ii) Any automorphism of the maximal tame quotient of Gal_K induces the identity on its respective unramified quotient, see Proposition 4.2.2.

(iii) The geometric automorphisms that are trivial on the inertia group of the maximal tamely ramified quotient Gal_K / V_K come from field automorphisms fixing the maximal unramified subextension $K/K_0/\mathbb{Q}_p$, see Theorem 4.2.8.

(iv) The geometric automorphisms trivial on all of Gal_K / V_K come from field automorphisms fixing the maximal tamely ramified subextension $K/K_1/\mathbb{Q}_p$, see Theorem 4.2.9.

4.1 Automorphisms on the maximal unramified quotient

Lemma 4.1.1. *Any automorphism $\varphi\colon \mathrm{Gal}_K \to \mathrm{Gal}_K$ induces the identity on the quotient Γ_K.*

Proof. Recall that the cyclotomic character

$$\chi\colon \mathrm{Gal}_K \to \mathrm{Aut}(\mu(\overline{K})) = \widehat{\mathbb{Z}}^\times$$

can be reconstructed from Gal_K (Corollary 3.1.6), i.e. $\chi = \chi \circ \varphi$. Now consider the following diagram

$$\begin{tikzcd}
\mathrm{Gal}_K \arrow[r, "\chi"] \arrow[d, two heads] & \widehat{\mathbb{Z}}^\times \arrow[d, two heads] \\
\Gamma_K = \mathrm{Gal}_{\mathbb{F}_K} \arrow[r, "\overline{\chi}"] & (\widehat{\mathbb{Z}}')^\times .
\end{tikzcd}$$

By Corollary 3.1.10, φ induces φ^{nr} as

$$\begin{tikzcd}
\mathrm{Gal}_K \arrow[r, "\varphi"] \arrow[d, two heads] & \mathrm{Gal}_K \arrow[d, two heads] \\
\Gamma_K = \mathrm{Gal}_K / I_K \arrow[r, "\varphi^{\mathrm{nr}}"] & \Gamma_K .
\end{tikzcd}$$

Hence, $\overline{\chi} \circ \varphi^{\mathrm{nr}} = \overline{\chi}$. As the the map $\overline{\chi}$ is injective by Lemma 3.1.13, it follows that $\varphi^{\mathrm{nr}} = \mathrm{id}$. □

4.2 Automorphisms on the maximal tame quotient

Note that an automorphism $\varphi\colon \mathrm{Gal}_K \to \mathrm{Gal}_K$ induces an automorphism on the maximal tamely ramified quotient of Gal_K, as the wild inertia group V_K is a characteristic subgroup by Corollary 3.1.11. By Theorem 3.2.5, the quotient is isomorphic to the *Iwasawa group* Iw_q associated to the parameter q, i.e.

$$\mathrm{Iw}_q \coloneqq \widehat{\mathbb{Z}}'(1) \rtimes_q \widehat{\mathbb{Z}} = \left\langle \sigma, \tau \mid \sigma\tau\sigma^{-1} = \tau^q \right\rangle .$$

In additive notation we have

$$(x, a) + (y, b) \coloneqq (x + q^a y, a + b)$$

for the addition of $x, y \in \widehat{\mathbb{Z}}'(1)$ and $a, b \in \widehat{\mathbb{Z}}$.

We note the following.

Proposition 4.2.1. *The maximal tame quotient* Iw_q *is center-free.*

Proof. The short exact sequence

$$1 \to \widehat{\mathbb{Z}}'(1) \to \mathrm{Iw}_q \to \widehat{\mathbb{Z}} \to 1 \tag{4.1}$$

induces a faithful action

$$\begin{aligned} \widehat{\mathbb{Z}} &\hookrightarrow \mathrm{Aut}(\widehat{\mathbb{Z}}'(1)) = (\widehat{\mathbb{Z}}')^\times \\ 1 &\mapsto q. \end{aligned}$$

by Lemma 3.1.13. It follows that $Z(\mathrm{Iw}_q) \subseteq \widehat{\mathbb{Z}}'(1)$. But since conjugation by σ acts as multiplication by q on $\widehat{\mathbb{Z}}'(1)$, and this group is torsion free, the center must be trivial. □

The sequence (4.1) is group theoretically characteristic. We shall describe it as follows. Let

$$\mathrm{Iw}_q^{\mathrm{nr}} \coloneqq \mathrm{Iw}_q^{\mathrm{ab}} / \mathrm{tors}$$

denote the maximal unramified quotient of Iw_q and let

$$\mathrm{Iw}_q^{\mathrm{tr}} \coloneqq \ker(\mathrm{Iw}_q \to \mathrm{Iw}_q^{\mathrm{nr}})$$

denote the inertia group of Iw_q. The sequence

$$1 \to \mathrm{Iw}_q^{\mathrm{tr}} \to \mathrm{Iw}_q \to \mathrm{Iw}_q^{\mathrm{nr}} \to 1$$

is isomorphic to (4.1). We want to study the (outer) automorphisms of Iw_q via this sequence. We have the following result:

Proposition 4.2.2. *Let $\varphi \in \operatorname{Aut}(\mathrm{Iw}_q)$. This induces the identity on $\mathrm{Iw}_q^{\mathrm{nr}}$ and an automorphism φ^{tr} on $\mathrm{Iw}_q^{\mathrm{tr}}$.*

Proof. This is a similar argument as in Lemma 4.1.1, but this time we start with an automorphism of the quotient $\operatorname{Gal}(K^{\mathrm{tr}}/K)$ as opposed to an automorphism of Gal_K. Clearly, the quotient $\mathrm{Iw}_q \to \mathrm{Iw}_q^{\mathrm{nr}}$ is characteristic, inducing a map $\operatorname{Aut}(\mathrm{Iw}_q) \to \operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{nr}})$. Consider the action

$$\begin{aligned} \rho: \quad \mathrm{Iw}_q^{\mathrm{nr}} &\to \operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{tr}}) \\ \sigma &\mapsto (x \mapsto \sigma.x := \widetilde{\sigma} x \widetilde{\sigma}^{-1}), \end{aligned} \tag{4.2}$$

where $\widetilde{\sigma} \in \mathrm{Iw}_q$ denotes a lift of σ. Then for all $x \in \mathrm{Iw}_q^{\mathrm{tr}}$ it holds that

$$\varphi^{\mathrm{tr}}(\sigma.x) = \varphi(\widetilde{\sigma})\varphi^{\mathrm{tr}}(x)\varphi(\widetilde{\sigma})^{-1} = \varphi^{\mathrm{nr}}(\sigma).\varphi^{\mathrm{tr}}(x).$$

There is a unique Frobenius element $\mathrm{Frob}_q \in \mathrm{Iw}_q^{\mathrm{nr}}$ such that $\mathrm{Frob}_q .x = x^q$. As

$$\mathrm{Frob}_q .\varphi^{\mathrm{tr}}(x) = \varphi^{\mathrm{tr}}(x)^q = \varphi^{\mathrm{tr}}(\mathrm{Frob}_q .x) = \varphi^{\mathrm{nr}}(\mathrm{Frob}_q).\varphi^{\mathrm{tr}}(x),$$

we have $\varphi^{\mathrm{nr}}(\mathrm{Frob}_q) = \mathrm{Frob}_q$ as (4.2) is fully faithful. Thus, $\varphi^{\mathrm{nr}} = \mathrm{id}$. □

As $\mathrm{Iw}_q^{\mathrm{tr}} \cong \widehat{\mathbb{Z}}'(1)$, we have canonically $\operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{tr}}) = (\widehat{\mathbb{Z}}')^\times$.

Corollary 4.2.3. *The map $\varphi \mapsto \varphi^{\mathrm{tr}}$ induces a group homomorphism*

$$\operatorname{Aut}(\mathrm{Iw}_q) \to \operatorname{Aut}(\mathrm{Iw}^{\mathrm{tr}}) = (\widehat{\mathbb{Z}}')^\times.$$

We denote the kernel by $\operatorname{Aut}_0(\mathrm{Iw}_q)$. For $\varepsilon \in (\widehat{\mathbb{Z}}')^\times$ we can define an an automorphism of Iw_q by

$$\varphi_\varepsilon(x, a) = (\varepsilon x, a)$$

for all $(x, a) \in \mathrm{Iw}_q$. The map $\varepsilon \mapsto \varphi_\varepsilon$ constructs a homomorphism

$$(\widehat{\mathbb{Z}}')^\times \to \operatorname{Aut}(\mathrm{Iw}_q).$$

Proposition 4.2.4. *The sequence*

$$1 \to \operatorname{Aut}_0(\mathrm{Iw}_q) \to \operatorname{Aut}(\mathrm{Iw}_q) \to \operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{tr}}) \to 1$$

is short exact and splits by $\varepsilon \mapsto \varphi_\varepsilon$.

Note that inner automorphisms of Iw_q map onto the subgroup generated by q in $\widehat{\mathbb{Z}}$, i.e. onto $q^{\widehat{\mathbb{Z}}} = \langle q \rangle$. We obtain an induced surjective homomorphism

$$\operatorname{Out}(\mathrm{Iw}_q) \to \operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{tr}})/\operatorname{Inn}(\mathrm{Iw}_q) = (\widehat{\mathbb{Z}}')^\times/\left\langle q^{\widehat{\mathbb{Z}}}\right\rangle$$

and we denote the kernel of this map by $\operatorname{Out}_0(\mathrm{Iw}_q)$. By a result by Wells (cf. Proposition 2.5.4) and Kummer theory, we have

$$\begin{aligned} \operatorname{Aut}_0(\mathrm{Iw}_q) &\cong Z^1(\mathrm{Iw}_q^{\mathrm{nr}}, \mathrm{Iw}_q^{\mathrm{tr}}) \quad \text{and} \quad & \operatorname{Out}_0(\mathrm{Iw}_q) &\cong H^1(\mathrm{Iw}_q^{\mathrm{nr}}, \mathrm{Iw}_q^{\mathrm{tr}}) \\ &= Z^1(\mathbb{F}_q, \widehat{\mathbb{Z}}'(1)), & &= H^1(\mathbb{F}_q, \widehat{\mathbb{Z}}'(1)) \\ & & &= \varprojlim_{p \nmid n} (\mathbb{F}_q^\times/n) = \mathbb{F}_q^\times. \end{aligned}$$

With above notation, we have

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Out}_0(\mathrm{Iw}_q) \arrow[r] \arrow[d, equal] & \mathrm{Out}(\mathrm{Iw}_q) \arrow[r] & \mathrm{Aut}(\widehat{\mathbb{Z}}'(1))/\,\mathrm{Iw}_q^{\mathrm{tr}} \arrow[r] \arrow[d, equal] & 1. \\
 & \mathbb{F}_q^\times & & (\widehat{\mathbb{Z}}')^\times/q^{\widehat{\mathbb{Z}}} &
\end{tikzcd}$$

In the rest of this chapter we are interested in the following question:

Question 4.2.5. We fix an isomorphism

$$\mathrm{Iw}_q \xrightarrow{\cong} \mathrm{Gal}(K^{\mathrm{tr}}/K), \quad (1,0) \mapsto \tau,\ (0,1) \mapsto \sigma$$

as in Theorem 3.2.5, where σ is a lift of Frobenius, and τ generates the tame inertia group. Can we describe the image of $\mathrm{Aut}(K)$ in $\mathrm{Out}(\mathrm{Gal}(K^{\mathrm{tr}}/K)) = \mathrm{Out}(\mathrm{Iw}_q)$?

We need the following results.

Lemma 4.2.6. *Let $K/\mathbb{Q}_p$ be a finite extension. There exists a maximal unramified intermediate field K_0 of $K/\mathbb{Q}_p$.*

Proof. This follows from [Ser13b, III.6, Cor. 3]. □

Proposition 4.2.7. *Let $K/\mathbb{Q}_p$ be a finite extension. Then there is a subextension $K/K_1/\mathbb{Q}_p$ such that $K_1/\mathbb{Q}_p$ is tamely ramified and K/K_1 is purely wildly ramified.*

Proof. The compositum of two tamely ramified subextensions of $\mathbb{Q}_p$ in K is again tamely ramified. Hence, we can choose K_1 to be the compositum of all such tamely ramified subextensions. Then $K_1/\mathbb{Q}_p$ is a tamely ramified, see e.g. [Neu06, III, Kor. 7.9]. It remains to show that K/K_1 is purely wildly ramified. Let $L = \widetilde{K}$ denote the Galois closure of K with respect to K_1, and let $G = \mathrm{Gal}(L/K_1)$ and $H = \mathrm{Gal}(L/K)$. Then G admits a quotient to a group Γ such that the respective field extension L^Γ/K_1 is maximally tame in L. Denoting the kernel of this quotient by P, which the wild inertia group of G, i.e. a p-group, we have a short exact sequence

$$1 \to P \to G \to \Gamma \to 1.$$

By definition of K_1 the extension L/K_1 has no intermediate extension M with M/K_1 tame, hence it follows that the image of the subgroup H under this quotient is Γ. Thus, we have a short exact sequence

$$1 \to P \cap H \to H \to \Gamma \to 1.$$

It follows that

$$[K : K_1] = (G : H) = \frac{\#G}{\#H} = \frac{\#P}{\#P \cap H},$$

which is a power of p. This shows the claim. □

The first main result of this section now states the following.

Theorem 4.2.8. *The subgroup of* $\operatorname{Aut}(K)$ *mapping to* $\operatorname{Out}_0(\mathrm{Iw}_q)$ *under*

$$\operatorname{Aut}(K) \hookrightarrow \operatorname{Out}(\mathrm{Gal}_K) \to \operatorname{Out}(\mathrm{Gal}(K^{\mathrm{tr}}/K)) = \operatorname{Out}(\mathrm{Iw}_q)$$

is $\operatorname{Aut}(K/K_0)$.

Proof. Let $\alpha \in \operatorname{Aut}(K)$ and let $\overline{\alpha}\colon \overline{K} \to \overline{K}$ denote some extension to an algebraic closure $\overline{K}$ of K. Then $\overline{\alpha}(-)\overline{\alpha}^{-1}$ is an automorphism of Gal_K (see Theorem 3.1.1). We want to compute the image of α in

$$\operatorname{Aut}(K) \hookrightarrow \operatorname{Out}(\mathrm{Gal}_K) \longrightarrow \operatorname{Out}(\mathrm{Gal}(K^{\mathrm{tr}}/K)) \longrightarrow \operatorname{Aut}(\mathrm{Iw}_q^{\mathrm{tr}})/\operatorname{Inn}(\mathrm{Iw}_q) = (\widehat{\mathbb{Z}}')^{\times}/q^{\widehat{\mathbb{Z}}}, \qquad (4.3)$$

which we denote by $\varepsilon = \varepsilon(\overline{\alpha})$.

We denote the tame character by

$$t\colon \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) \xrightarrow{\sim} \widehat{\mathbb{Z}}'(1) = \varprojlim_{p\nmid n} \mu_n,$$

which is an isomorphism. Now let n be a positive integer coprime to p. Let t_n denote the induced map on the quotient $\widehat{\mathbb{Z}}'(1) \twoheadrightarrow \mu_n$. Recall that this map is given by

$$g \mapsto \frac{g(\sqrt[n]{\pi})}{\sqrt[n]{\pi}},$$

for a uniformizer π of K. We denote the induced isomorphism of ε on the quotient μ_n by $(-)^{\varepsilon_n}$. Now we consider the following commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) \arrow[r, "t", "\cong"'] \arrow[d, "\overline{\alpha}(-)\overline{\alpha}^{-1}", "\cong"'] & \widehat{\mathbb{Z}}'(1) \arrow[r, "t_n"] \arrow[d, "\varepsilon", "\cong"'] & \mu_n \arrow[d, "(-)^{\varepsilon_n}", "\cong"'] \\
\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) \arrow[r, "t"'] & \widehat{\mathbb{Z}}'(1) \arrow[r, "t_n"'] & \mu_n.
\end{tikzcd}$$

Let π denote a uniformizer of K. Then $\alpha(\pi)$ is also a uniformizer of K, i.e. there exists an element $u \in \mathcal{O}_K^{\times}$ such that $\alpha(\pi) = u\pi$. We make a choice of nth root of π, which we denote by $\sqrt[n]{\pi}$. Then

$$\overline{\alpha}(\sqrt[n]{\pi}) = u_n \sqrt[n]{\pi},$$

for some unit u_n such that $(u_n)^n = u$. But this must be an element of K^{nr} as $T^n - u_n$ is separable over the residue field $\mathbb{F}_K$. Furthermore, let χ_n denote the nth cyclotomic character.

Let $g \in \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}})$. The following computation now yields a specific description of ε_n:

$$\begin{aligned}
t_n(\overline{\alpha}g\overline{\alpha}^{-1}) &= \frac{\overline{\alpha}g\overline{\alpha}^{-1}(\sqrt[n]{\pi})}{\sqrt[n]{\pi}} = \frac{\overline{\alpha}g\overline{\alpha}^{-1}(u_n^{-1}\overline{\alpha}(\sqrt[n]{\pi})}{\sqrt[n]{\pi}} \\
&= \frac{\overline{\alpha}g\overline{\alpha}^{-1}(u_n^{-1})\overline{\alpha}g(\sqrt[n]{\pi})}{\sqrt[n]{\pi}} = u_n^{-1}\frac{\overline{\alpha}g(\sqrt[n]{\pi})}{\sqrt[n]{\pi}} \\
&= \frac{\overline{\alpha}(t_n(g)\sqrt[n]{\pi})}{u_n\sqrt[n]{\pi}} = \frac{t_n(g)^{\chi_n(\overline{\alpha})}\cdot u_n\sqrt[n]{\pi}}{u_n\sqrt[n]{\pi}} \\
&= t_n(g)^{\chi_n(\overline{\alpha})}.
\end{aligned}$$

It follows that $\varepsilon_n = \chi_n(\overline{\alpha})$. Thus, we have $\varepsilon = \chi_{\mathrm{cyc}}(\overline{\alpha})$, where χ_{cyc} denotes the cyclotomic character.

So far, the description of ε depends on the choice of $\overline{\alpha}$. Let $N_{\mathrm{Gal}_{\mathbb{Q}_p}}(\mathrm{Gal}_K)$ denote the normalizer of Gal_K in $\mathrm{Gal}_{\mathbb{Q}_p}$. For any $\alpha \in \mathrm{Aut}(K) = \mathrm{Aut}_{\mathbb{Q}_p}(K)$ choosing a lift $\overline{\alpha}$ yields an element in $N_{\mathrm{Gal}_{\mathbb{Q}_p}}(\mathrm{Gal}_K)$ which is well-defined up to Gal_K. In fact, any element of $N_{\mathrm{Gal}_{\mathbb{Q}_p}}(\mathrm{Gal}_K)/\,\mathrm{Gal}_K$ yields a $\mathbb{Q}_p$-linear automorphism of K, and we have a natural identification

$$\mathrm{Aut}(K) = N_{\mathrm{Gal}_{\mathbb{Q}_p}}(\mathrm{Gal}_K)/\,\mathrm{Gal}_K\,.$$

Note that we have a morphism

$$N_{\mathrm{Gal}_{\mathbb{Q}_p}}(\mathrm{Gal}_K)/\,\mathrm{Gal}_K \to \mathrm{Gal}_{\mathbb{Q}_p}/\,\langle\!\langle \mathrm{Gal}_K \rangle\!\rangle\,.$$

As the image of Gal_K under the cyclotomic character is the subgroup of $(\widehat{\mathbb{Z}}')^\times$ generated by q, we have a map

$$\mathrm{Gal}_{\mathbb{Q}_p}/\,\langle\!\langle \mathrm{Gal}_K \rangle\!\rangle \xrightarrow{\chi_{\mathrm{cyc}}} (\widehat{\mathbb{Z}}')^\times/\,\langle q \rangle\,,$$

which in fact has image in the subgroup generated by p, i.e. in $\langle p \rangle\,/\,\langle q \rangle$. We now consider the following diagram

$$\begin{tikzcd}
\mathrm{Aut}(K) \arrow[r] \arrow[d, "="', "\mathrm{lift}"] & \mathrm{Out}(\mathrm{Gal}_K) \arrow[r] & \mathrm{Out}(\mathrm{Gal}(K^{\mathrm{tr}}/K)) \arrow[d, two heads, "\mathrm{mod}\,\mathrm{Out}_0(\mathrm{Gal}(K^{\mathrm{tr}}/K))"] & \\
N_{\mathrm{Gal}_{\mathbb{Q}_p}}(\mathrm{Gal}_K)/\,\mathrm{Gal}_K \arrow[r] & \mathrm{Gal}_{\mathbb{Q}_p}/\,\langle\!\langle \mathrm{Gal}_K \rangle\!\rangle \arrow[r, "\chi_{\mathrm{cyc}}"] \arrow[dr, dashed] & (\widehat{\mathbb{Z}}')^\times/\,\langle q \rangle \arrow[r, "\mathrm{mod}\,q-1"] & \mathrm{Aut}(\mathbb{F}_q^\times) \\
 & & \langle p \rangle\,/\,\langle q \rangle \arrow[r, "\cong"] \arrow[u, hook] & \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p). \arrow[u, hook]
\end{tikzcd}$$

This commutes by our previous calculations. In particular, we see that $\varepsilon = \chi_{\mathrm{cyc}}(\overline{\alpha})$ as an element of $(\widehat{\mathbb{Z}}')^\times/\,\langle q \rangle$ does not depend on the choice of $\overline{\alpha}$.

Now the theorem deals with the subgroup of $\mathrm{Aut}(K)$ that maps trivially to $(\widehat{\mathbb{Z}}')^\times/\,\langle q \rangle$. Recall that we can identify $\mathbb{F}_q^\times$ with μ_{q-1} and

$$\mu_{q-1} \subseteq K_0 = \mathbb{Q}_p(\mu_{q-1}) \subseteq K.$$

We need to describe the automorphisms $\alpha \in \mathrm{Aut}(K)$ such that for a lift $\overline{\alpha}\colon \overline{K} \to \overline{K}$ it holds that $\chi_{q-1}(\overline{\alpha}) = 1$. But

$$\chi_{q-1}(\overline{\alpha}) = \overline{\alpha}|_{\mathbb{Q}_p(\mu_{q-1})} = \overline{\alpha}|_{K_0} = \alpha|_{K_0}.$$

Thus, $\chi_{q-1}(\overline{\alpha}) = 1$, if and only if $\alpha \in \mathrm{Aut}(K/K_0)$.

□

Back to Question 4.2.5. We try to give a similar description for the geometric automorphisms that are trivial (as outer automorphisms) on the maximal tamely ramified quotient of Gal_K. Note that the geometric automorphisms that are the identity on Iw_q are precisely those in the kernel of

$$T\colon \ker(\varepsilon) = \mathrm{Aut}(K/K_0) \to \mathrm{Out}_0(\mathrm{Iw}_q) = H^1(\mathbb{F}_q, \widehat{\mathbb{Z}}'(1)) = \mathbb{F}_q^\times.$$

The second main result of this section is the following.

Theorem 4.2.9. *We have*

$$\ker(T) = \mathrm{Aut}(K/K_1).$$

Hence, the subgroup of $\mathrm{Aut}(K)$ *inducing the identity in* $\mathrm{Out}(\mathrm{Iw}_q)$ *is* $\mathrm{Aut}(K/K_1)$.

Proof. We want to compute the kernel of

$$\mathrm{Aut}(K/K_0) \to \mathrm{Out}_0(\mathrm{Gal}(K^{\mathrm{tr}}/K)) = H^1(K^{\mathrm{nr}}/K, \widehat{\mathbb{Z}}'(1)) = \mathbb{F}_q^\times. \tag{4.4}$$

First, we give a more explicit description of the right-hand side in terms of Galois cohomology. In particular, any element of $H^1(K^{\mathrm{nr}}/K, \widehat{\mathbb{Z}}'(1))$ is represented by a 1-cocycle

$$c\colon \mathrm{Gal}(K^{\mathrm{nr}}/K) \to \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) = \widehat{\mathbb{Z}}'(1), \quad \gamma \mapsto c_\gamma.$$

We evaluate c in Frob_K. This yields an element c_{Frob_K} in $\widehat{\mathbb{Z}}'(1)$ but only up to coboundaries, i.e. $\mathrm{mod}(\mathrm{Frob}_K - 1)\widehat{\mathbb{Z}}'(1)$. This means we get the identification of $H^1(K^{\mathrm{nr}}/K, \widehat{\mathbb{Z}}'(1))$ with $\mathbb{F}_q^\times$ by evaluating cocycles in Frob_K and then applying the tame character mod $(q-1)$

$$t_{q-1}\colon \widehat{\mathbb{Z}}'(1) \to \mathbb{F}_q^\times = \mu_{q-1}.$$

Now let $\alpha \in \mathrm{Aut}(K)$. We choose any lift $\overline{\alpha}\colon K^{\mathrm{tr}} \to K^{\mathrm{tr}}$, yielding an automorphism $\overline{\alpha}(-)\overline{\alpha}^{-1}$ of $\mathrm{Gal}(K^{\mathrm{tr}}/K)$. By the theory of Section 2.5.2 the map (4.4) sends α to the class of the cocycle

$$\gamma \mapsto \overline{\alpha}\widetilde{\gamma}\overline{\alpha}^{-1}\widetilde{\gamma}^{-1},$$

where $\widetilde{\gamma}$ denote lifts of γ to K^{tr}. As we have just established: To compute $T(\alpha)$ we must now evaluate in Frob_K and then apply t_{q-1}.

But as everything is independent of the choice of extension $\overline{\alpha} \in \mathrm{Aut}(K^{\mathrm{tr}})$ of α, we may make a special choice. Recall that K/K_0 is purely ramified, hence we have $K^{\mathrm{nr}} = K \otimes_{K_0} K^{\mathrm{nr}}$, and $\mathrm{Frob}_K = \mathrm{id} \otimes \mathrm{Frob}_{K_0}$. We choose $\overline{\alpha}$ such that the restriction to K^{nr} is given by $\alpha \otimes \mathrm{id}$. Then we have

$$\overline{\alpha}|_{K^{\mathrm{nr}}} \circ \mathrm{Frob}_K = (\alpha \otimes \mathrm{id})(\mathrm{id} \otimes \mathrm{Frob}_{K_0}) = (\mathrm{id} \otimes \mathrm{Frob}_{K_0})(\alpha \otimes \mathrm{id}) = \mathrm{Frob}_K \circ \overline{\alpha}|_{K^{\mathrm{nr}}},$$

i.e. Frob_K and $\overline{\alpha}$ commute as automorphisms of K^{nr}/K_0.

Set $n = q-1$. Before we compute $T(\alpha)$, we note that $\mathrm{Frob}_K(\pi) = \pi$. Let $\widetilde{\mathrm{Frob}_K}$ be a lift of Frob_K to K^{tr}. Hence, there exists a $\zeta \in \mu_n \subseteq K_0$ such that

$$\widetilde{\mathrm{Frob}_K}(\sqrt[n]{\pi}) = \zeta \sqrt[n]{\pi} \quad \text{and} \quad \widetilde{\mathrm{Frob}_K}^{-1}(\sqrt[n]{\pi}) = \zeta^{-1} \sqrt[n]{\pi}.$$

Again $\overline{\alpha}$ maps uniformizers to uniformizers, i.e. $\overline{\alpha}(\pi) = u\pi$ for some $u \in \mathcal{O}_K^\times$. It follows that $\overline{\alpha}(\sqrt[n]{\pi}) = u_n \sqrt[n]{\pi}$ with $(u_n)^n = u$, which implies $u_n \in K^{\mathrm{nr}}$ as in the proof of Theorem 4.2.8. Together with the fact that Frob_K and $\overline{\alpha}$ commute on K^{nr}, we may compute.

$$\begin{aligned}
T(\alpha) = t_n(\overline{\alpha}\widetilde{\mathrm{Frob}_K}\overline{\alpha}^{-1}\widetilde{\mathrm{Frob}_K}^{-1}) &= \frac{\overline{\alpha}\widetilde{\mathrm{Frob}_K}\overline{\alpha}^{-1}\widetilde{\mathrm{Frob}_K}^{-1}(\sqrt[n]{\pi})}{\sqrt[n]{\pi})} \\
&= \frac{\overline{\alpha}\widetilde{\mathrm{Frob}_K}\overline{\alpha}^{-1}(\sqrt[n]{\pi})}{\zeta\sqrt[n]{\pi})} = \frac{\overline{\alpha}\widetilde{\mathrm{Frob}_K}\overline{\alpha}^{-1}(u_n^{-1}\overline{\alpha}(\sqrt[n]{\pi}))}{\zeta\sqrt[n]{\pi})} \\
&= \left(\overline{\alpha}\widetilde{\mathrm{Frob}_K}\overline{\alpha}^{-1}\right)\Big|_{K^{\mathrm{nr}}}(u_n^{-1}) \cdot \frac{\overline{\alpha}\widetilde{\mathrm{Frob}_K}(\sqrt[n]{\pi})}{\zeta\sqrt[n]{\pi}} = \mathrm{Frob}_K(u_n^{-1})\frac{\overline{\alpha}(\zeta\sqrt[n]{\pi})}{\zeta\sqrt[n]{\pi}} \\
&= \frac{u_n}{\mathrm{Frob}_K(u_n)}.
\end{aligned}$$

It follows that

$$T(\alpha) = 1 \quad \Longleftrightarrow \quad \mathrm{Frob}_K(u_n) = u_n \quad \Longleftrightarrow \quad u_n \in K \quad \Longleftrightarrow \quad \frac{\alpha(\pi)}{\pi} \in (\mathcal{O}_K^\times)^n.$$

As $n = q - 1$ is prime to p we have

$$\mathcal{O}_K^\times / (\mathcal{O}_K^\times)^n = \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^n = \mathbb{F}_q^\times.$$

This implies

$$T(\alpha) = 1 \quad \Longleftrightarrow \quad \frac{\alpha(\pi)}{\pi} \equiv 1 \bmod (\pi).$$

By [Neu06, §9], this is equivalent to the extension $K/K^{\langle\alpha\rangle}$ being purely wildly ramified, i.e.$K_1 \subseteq K^{\langle\alpha\rangle} \subseteq K$. Hence, we have $T(\alpha) = 1$ if and only if $\alpha \in \mathrm{Aut}(K/K_1)$, which was the claim. □

5 Finitely generated pro-p groups

5.1 Basics on finitely generated pro-p groups

First, we need to recall some more general facts about finitely generated pro-p groups. Let G be a finitely generated pro-p group of rank $n = n(G) = \dim_{\mathbb{F}_p} H^1(G) < \infty$. Recall that n is the minimal number of generators of G. Let $\mathcal{R} = \{\rho_i\}_{i\in I}$ denote a minimal system of defining relations of G. Thus we have an exact sequence

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1,$$

where F is the free pro-p-group of rank n and R is generated by $\mathcal{R}$ as normal subgroup of F. Recall that $H^1(G, \mathbb{F}_p) = \operatorname{Hom}\left(G^{\mathrm{ab}}, \mathbb{F}_p\right) = (\mathbb{Z}/p\mathbb{Z})^n$. Passing to the abelianization we obtain G^{ab} as a quotient of $F^{\mathrm{ab}} \cong \mathbb{Z}_p^n$ by the image of $N = R/[F, R]$. In the following, we will choose a maximal quotient $\mathbb{Z}_p \twoheadrightarrow \Lambda = \Lambda(G)$ such that

$$G^{\mathrm{ab}} \otimes \Lambda \cong F^{\mathrm{ab}} \otimes \Lambda$$

as free Λ-modules of rank n, where $-\otimes\Lambda$ means $-\otimes_{\mathbb{Z}_p}\Lambda$. In particular, if G^{ab} has a nontrivial torsion subgroup, we set $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$ for some power $q = q(G)$ of p, namely the smallest elementary divisor of G^{ab} as $\mathbb{Z}_p$-module. If N is trivial, i.e. $G^{\mathrm{ab}} \cong \mathbb{Z}_p^n$, we set $\Lambda = \mathbb{Z}_p$, work with continuous cochain cohomology, and set $q = q(G) = 0$.

A natural way of studying pro-p groups is via suitable filtrations, and the associated graded Lie algebras. Throughout this chapter, we will consider the following filtration.

5.1.1 Λ-filtration on pro-p groups

We use the left notation for the conjugation of group elements, i.e. for $x, y \in G$ we write ${}^{x}y = xyx^{-1}$, and define the commutator as $[x, y] = ({}^{x}y)y^{-1} = xyx^{-1}y^{-1}$. First we state some basic commutator identities.

Lemma 5.1.1 (Basic Commutator Identities)**.** *Let G be a finitely generated pro-p group. For all $x, y, z \in G$ the following identities hold.*

(i) $[x, y]^{-1} = [y, x]$.

(ii) $[xy, z] = ({}^{x}[y, z])[x, z]$, *and* $[x, yz] = [x, y]({}^{y}[x, z])$.

(iii) $[x, y^{-1}] = \left({}^{y^{-1}}[x, y]\right)^{-1}$ *and* $[x^{-1}, y] = {}^{x^{-1}}\left([x, y]\right)^{-1}$.

Definition 5.1.2. Let G be a finitely generated pro-p-group, and let q be a power of p. Then the *descending q-central series* of G is the filtration $C^{\bullet}G = C_q^{\bullet}G$ defined by

$$C^1G = G, \quad C^{i+1}G = \left(C^iG\right)^q \left[C^iG, G\right],$$

where $\big(C^iG\big)^q$ denotes the closed subgroup generated by qth powers of C^iG, and $\big[C^iG, G\big]$ denotes the closed subgroup topologically generated by commutators $[x, y]$ for $x \in C^iG, y \in G$. We call i the *weight* of this commutator. We set $q = 0$ to refer to the usual *descending central series* of G.

Let $\Lambda = \Lambda(G)$ and $q = q(G)$ be defined as above. For this specific choice of q, we refer to this filtration as the *descending* Λ*-central series* or just Λ*-filtration* and denote it by $C^\bullet_\Lambda G$.

Note that for all i the group $C^{i+1}G$ is normal in C^iG and also normal in G. We denote the quotient $C^iG/C^{i+1}G$ by $\mathrm{gr}^i(G) = \mathrm{gr}^i_C(G)$, which we now write additively. Note that we have $[C^iG, C^jG] \subseteq C^{i+j}G$ for all i, j. So in particular, calling this a central filtration is justified.

Lemma 5.1.3. *Let G be a finitely generated pro-p group and $i \geq 1$, and let $C^\bullet G$ denote the q-central series.*

(i) The group $\mathrm{gr}^i(G)$ is abelian and central in $G/C^{i+1}G$, i.e. we have a central short exact sequence

$$0 \to \mathrm{gr}^i(G) \to G/C^{i+1}G \to G/C^iG \to 1. \tag{5.1}$$

(ii) Let $\varphi\colon G \to H$ be a morphism of pro-p groups. Then $\varphi(C^iG) \subseteq C^iH$. If φ is surjective, this is an equality. In particular, it follows that the subgroup C^iG is a characteristic subgroup of G.

(iii) It holds that

$$\bigcap_{i\geq 1} C^iG = 1.$$

If $q \neq 0$, then the subgroups C^iG form a fundamental system of open neighbourhoods of 1.

Proof. Straight forward. □

Corollary 5.1.4. *Let G be a finitely generated pro-p group, let $\varphi\colon G \to G$ be an automorphism. For any $m \geq 2$ this induces an automorphism $\varphi_m\colon G/C^mG \to G/C^mG$ such that $\varphi \equiv \varphi_m \mod C^mG$. In particular, for $m \geq 1$ the groups $\mathrm{Aut}(G/C^mG)$ form a projective system of finite groups and we have an isomorphism*

$$\mathrm{Aut}(G) \to \varprojlim_m \mathrm{Aut}(G/C^mG).$$

The direct sum

$$\mathrm{gr}(G) := \bigoplus_{i=1}^{\infty} \mathrm{gr}^i(G)$$

is a Lie algebra over Λ. The Lie bracket for homogeneous elements of $\mathrm{gr}(G)$ is induced by the commutator, i.e. for $\xi = \overline{x} \in \mathrm{gr}^i(G)$, and $\eta = \overline{y} \in \mathrm{gr}^j(G)$ we define $[\xi, \eta]$ to be the image of $[x, y]$ in $\mathrm{gr}^{i+j}(G)$.

Note that the map $C^iG \to C^{i+1}G$ given by $x \mapsto x^q$ induces a map $\pi_i\colon \mathrm{gr}^i(G) \to \mathrm{gr}^{i+1}(G)$. See e.g. [Lab67, Prop. 1] for a proof. The family (π_i) then induces a map

$$\pi_*\colon \mathrm{gr}(G) \to \mathrm{gr}(G).$$

If $q \neq 0$, let π denote an indeterminate over $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$ and if $q = 0$, let π denote the zero element of $\Lambda = \mathbb{Z}_p$. There exists a unique mapping

$$\Phi \colon \Lambda[\pi] \times \mathrm{gr}(G) \to \mathrm{gr}(G),$$

which is Λ-linear in the first component and such that $\Phi(\pi^i, \xi) = \pi_*^i(\xi)$. Set $\alpha \cdot \xi = \Phi(\alpha, \xi)$.

From standard commutator computations, one can deduce the following formulas that hold in $\mathrm{gr}(G)$, as stated in [Lab67, Prop. 2].

Proposition 5.1.5. *Let G be a finitely generated pro-p group. Let $\xi \in \mathrm{gr}^i(G)$, $\eta \in \mathrm{gr}^j(G)$. Then*

$$\begin{array}{lll}
\text{(i)} & \pi\cdot(\xi+\eta) = \pi\cdot\xi + \pi\cdot\eta, & \textit{if} \quad i = j > 1,\\
\text{(ii)} & \pi\cdot(\xi+\eta) = \pi\cdot\xi + \pi\cdot\eta + \binom{q}{2}[\xi,\eta], & \textit{if} \quad i = j = 1,\\
\text{(iii)} & \pi\cdot[\xi,\eta] = [\pi\cdot\xi,\eta], & \textit{if} \quad i \neq 1,\\
 & \pi\cdot[\xi,\eta] = [\xi,\pi\cdot\eta], & \textit{if} \quad j \neq 1,\\
\text{(iv)} & [\pi\cdot\xi,\eta] = \pi\cdot[\xi,\eta] + \binom{q}{2}[[\xi,\eta],\xi], & \textit{if} \quad i = j = 1,\\
\text{(v)} & [\xi,\pi\cdot\eta] = \pi\cdot[\xi,\eta] + \binom{q}{2}[[\xi,\eta],\eta], & \textit{if} \quad i = j = 1.
\end{array}$$

Remark 5.1.6. If q is not a power of 2, then $\mathrm{gr}(G)$ is a Lie algebra in graded $\Lambda[\pi]$-modules.

For $x_1, \dots, x_r \in \mathrm{gr}^1(G)$, we shall denote λ by the iterated commutator

$$\lambda(x_1, \dots, x_r) \coloneqq [x_1, [x_2, [x_3, \dots [x_{r-1}, x_r] \dots],$$

which is of weight r. This is a so-called *basic commutator* of weight r. We have the following result, which follows by completion from a result by Hall for discrete free groups. See [Hal59, Thm. 11.2.4].

Proposition 5.1.7. *Let F be a free pro-p group with generators $x_1, \dots, x_n$. Let $m \geq 1$. There exists a Λ-linear surjective map*

$$\bigoplus_{r \leq m} \left(\mathrm{gr}^1(F)\right)^{\otimes r} \to \mathrm{gr}^m(F), \quad x_1 \otimes \ldots \otimes x_r \mapsto \pi^{m-r}\lambda(x_1, \dots, x_r).$$

Now we assume that $G = F$ is a free pro-p group of rank n, and let q be some power of p or zero. Note that if q is not a power of 2, the factor $\binom{q}{2} \equiv 0 \bmod q$ vanishes in Λ, simplifying above expressions. We introduce some further notation to give a more detailed description of $\mathrm{gr}(F)$ in this case. From now on, we assume $p \neq 2$.

We denote by $A = \Lambda \langle\langle X_1, \dots, X_r \rangle\rangle$ the algebra of associative, non-commutative formal power series of variables $X_1, \dots, X_r$ over Λ, i.e.

$$A = \Lambda \langle\langle X_1, \dots, X_r \rangle\rangle \coloneqq \left\{ \sum_{1 \leq i_1, \dots, i_n \leq r} a_{i_1 \cdots i_n} X_{i_1} \cdots X_{i_n} \mid n \geq 0, a_{i_1 \cdots i_n} \in \Lambda \right\}.$$

The degree $\deg(f)$ of $f = f(X_1, \dots, X_r) = \sum a_{i_1 \cdots i_n} X_{i_1} \cdots X_{i_n}$ is the smallest integer n such that $a_{i_1 \cdots i_n} \neq 0$. Let $I(\underline{X})$ denote the kernel of the ring homomorphism evaluating formal power series in 0, i.e. $I(\underline{X}) = (X_1, \dots, X_n)$. Note that the two sided ideals $(p^j, I(\underline{X})^d)_{j,d}$ induce a profinite topology on $\Lambda \langle\langle X_1, \dots, X_n \rangle\rangle$, which we now regard as a compact Λ-algebra. The multiplicative group of 1-units U_A^1 consisting of elements with constant term 1, contains the elements $1 + X_i$. Note that U_A^1 is a pro-p group. The universal property of the free pro-p group induces a group homomorphism

$$\varepsilon \colon F \to U_A^1, \quad x_i \mapsto 1 + X_i.$$

Proposition 5.1.8. *The group homomorphism $\varepsilon\colon F \to U_A^1$ is injective.*

In the pro-p setting, the well-known *Magnus embedding* becomes a homeomorphism. For any p-adically complete, Noetherian, local ring R with finite residue field, and G a profinite group we denote the usual abstract group algebra by RG consisting of all formal sums $\sum_{g\in G} a_g g$, where $a_g \in R$ and $a_g = 0$ for all but finitely many $g \in G$. We define the *complete group algebra* $R[[G]]$ as the inverse limit

$$R[[G]] = \varprojlim_{I,U} (R/I)[G/U],$$

where I and U range over the open ideals of R and the open normal subgroups of G, respectively. So $R[[G]]$ is a profinite algebra. We now have the following result on the complete group ring of a free pro-p group in the generators $x_1, \dots, x_n$.

Theorem 5.1.9. *Let $\Lambda = \mathbb{Z}_p$ or $\mathbb{Z}/q\mathbb{Z}$. There is a continuous isomorphism of Λ-algebras*

$$M_\Lambda\colon \Lambda[[F]] \to \Lambda\langle\langle X_1, \dots, X_n\rangle\rangle\,, \quad x_i \mapsto 1 + X_i.$$

The composition with the embedding $F \hookrightarrow \Lambda[[F]]$ is called the pro-p or mod q, resp. Magnus embedding.

Proof. See [Mor11, Lemma 8.11] for details. □

In fact, one may show that the descending Λ-central series is induced by the $I(\underline{X})$-adic filtration on A. In particular, we have

$$C^i F = \varepsilon^{-1}(1 + I(\underline{X})^i).$$

We have the following result.

Proposition 5.1.10. *Assume $p \neq 2$, and let $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$ or $\mathbb{Z}_p$ as above. Then $\operatorname{gr}(F)$ is a free Lie algebra over $\Lambda[\pi]$.*

In fact, it is a free Lie sub-algebra of $\operatorname{gr}\Lambda\langle\langle X_1, \dots, X_n\rangle\rangle$ in the letters $x_1, \dots, x_n$ with coefficients in $\Lambda[\pi]$. The elements $\pi, x_1, \dots, x_n$ are of degree 1. Furthermore, we note that on $\operatorname{gr}(F)$, the quotient $\operatorname{gr}^2 F$ contains a Λ-basis given by expressions of the form πx_i and $[x_j, x_k]$ with $j < k$, as the next result will yield.

Proposition 5.1.11. *Let F be a free pro-p group in the generators $x_1, \dots, x_n$. Then every element $\rho \in C^2 F$ has a representation*

$$\rho = \prod_{j=1}^{n} x_j^{qa_j} \cdot \prod_{1\le k<\ell\le n} [x_k, x_\ell]^{a_{k\ell}} \bmod C^3 F, \quad a_j, a_{k\ell} \in \Lambda.$$

The $a_{k\ell}$ are uniquely determined, and if $q \neq 0$, so are the a_j.

Proof. Let $\rho \in C^2 F$. Then ρ has a unique expression $\prod_{j=1}^n x_j^{qa_j} \bmod [F,F]$ with $a_j \in \mathbb{Z}_p$, i.e. it is of the form $\rho = \prod_{j=1}^n x_j^{qa_j} \cdot c$ where $c \in [F,F]$. Commutators of the form $[x_k, x_\ell]$ for $1 \le k < \ell \le n$ provide a $\mathbb{Z}_p$-basis of $[F,F]/[[F,F],F]$. This is due to Hall [Hal59, Thm.

11.2.4] in the discrete case, but the commutator identities used still hold for topological groups noting that the discrete free group in $x_1, \dots, x_n$ is dense in F. It follows that

$$\rho \equiv \prod_{j=1}^{n} x_j^{qa_j} \prod_{1 \le k < \ell \le n} [x_k, x_\ell]^{a_{k\ell}} \bmod [[F,F],F], \quad a_j, a_{k\ell} \in \mathbb{Z}_p.$$

As $[[F,F],F] \subseteq C^2F$, reducing the above expression mod C^2F will yield the same where in the case $q \neq 0$ the exponents $a_j, a_{k,\ell}$ are reduced mod q. The image of ρ in $F/F^{q^2}[F,F] = (\mathbb{Z}/q^2\mathbb{Z})^n$ is $(qa_1, \dots, qa_n)$, showing that the exponents a_j are uniquely determined in $\Lambda = \mathbb{Z}/q\mathbb{Z}$. The uniqueness of $a_{k\ell}$ follows from Proposition 5.1.12 (i). □

5.1.2 Finitely generated pro-p groups are determined by cup product and Bockstein homomorphism up to third filtration step

Let G be a finitely generated pro-p group with $n = \dim_{\mathbb{F}_p} H^1(G) < \infty$. Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

denote a minimal presentation of G as before. We choose $\Lambda = \Lambda(G)$ as stated in the beginning of the chapter, and throughout the section we consider the Λ-filtration $C^\bullet G = C^\bullet_\Lambda G$ on G. Note that with this choice of Λ we have $R \subseteq C^2F$.

The basis $x_1, \dots, x_n$ defines an isomorphism $F/F^q[F,F] \cong \Lambda^n$ yielding a Λ-basis $\chi_1, \dots, \chi_n$ of

$$H^1(F,\Lambda) = \mathrm{Hom}(F,\Lambda) = \mathrm{Hom}(G,\Lambda) = H^1(G,\Lambda)$$

such that $\chi_i(x_j) = \delta_{ij}$. We define a trace map on $H^2(G,\Lambda)$ in the following way. First recall the 5-term exact sequence from Proposition 2.2.10

$$0 \longrightarrow H^1(G,\Lambda) \xrightarrow{\text{inf}} H^1(F,\Lambda) \xrightarrow{\text{res}} H^1(R,\Lambda)^G \xrightarrow{\text{tg}} H^2(G,\Lambda) \xrightarrow{\text{inf}} H^2(F,\Lambda),$$

where tg denotes the transgression map introduced in Proposition 2.2.8. The choice of Λ yields that $H^1(G,\Lambda) \xrightarrow{\text{inf}} H^1(F,\Lambda)$ is an isomorphism. Furthermore, we have $H^2(F,\Lambda) = 0$ as free pro-p groups have cohomological dimension 1. Furthermore,

$$\mathrm{Hom}(R/R^q[R,F],\Lambda) = \mathrm{Hom}_G(R^{\text{ab}},\Lambda) = H^1(R,\Lambda)^G \xrightarrow{\text{tg}} H^2(G,\Lambda)$$

is an isomorphism. Therefore, any element $\rho \in R$ gives rise to a trace map

$$\mathrm{tr} = \mathrm{tr}_\rho \colon H^2(G,\Lambda) \to \Lambda, \quad \varphi \mapsto (\mathrm{tg}^{-1}\varphi)(\rho).$$

We get a bilinear form

$$H^1(G,\Lambda) \times H^1(G,\Lambda) \xrightarrow{\cup} H^2(G,\Lambda) \xrightarrow{\mathrm{tr}_\rho} \Lambda.$$

Note that this bilinear form induced by the cup-product is non-degenerate if and only if it is non-degenerate mod p. In this case the map tr_ρ is surjective.

If G is only subject to one relation ρ, the homomorphism $\mathrm{tr}_\rho \colon H^2(G,\Lambda) \to \Lambda$ is injective, as the image of ρ is a generator of $R/R^q[R,F]$. Hence, if G is a one-relator group $G = F/(\rho)$ with non-degenerated cup-product, tr_ρ is a bijection.

The following classical result on finitely generated pro-p groups states that the group structure up to the third filtration step in the Λ-filtration is determined by the cup product and the Bockstein homomorphism.

Proposition 5.1.12. *Let G be a finitely generated pro-p group, and let*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G. Choose Λ as described above. Let $x_1, \dots, x_n$ be a basis of F and $\chi_1, \dots, \chi_n$ the corresponding dual basis of $H^1(F, \Lambda) = H^1(G, \Lambda)$. The following holds.

(i) Assume that ρ is a defining relation of G, i.e. $\rho \in \mathcal{R}$. The bilinear form given by $\operatorname{tr}_\rho(- \cup -)$ is given by the matrix $B = (b_{k\ell})$ with respect to the basis $\chi_1, \dots, \chi_n$ with

$$b_{k\ell} = \operatorname{tr}_\rho(\chi_k \cup \chi_\ell) = \begin{cases} -a_{k\ell} & \text{if} \quad k < \ell, \\ a_{\ell k} & \text{if} \quad k > \ell, \\ -\binom{q}{2} a_k & \text{if} \quad k = \ell, \end{cases}$$

where $a_{k\ell}, a_k \in \Lambda$ as in Proposition 5.1.11.

(ii) Assume $\rho \in \mathcal{R}$, and $q \neq 0$, i.e. $\Lambda = \mathbb{Z}/q\mathbb{Z}$. Then we have $\operatorname{tr}_\rho(\beta(\chi_j)) = -a_j$, where β denotes the Bockstein homomorphism and $a_j \in \Lambda$ as in Proposition 5.1.11.

Proof. (i) Let $\chi_k \cup \chi_\ell \in H^2(G, \Lambda)$. This class is represented by a 2-cocycle

$$c_0 = c_0^{(k,\ell)} \colon G \times G \to \Lambda$$

given by $c_0(\sigma, \tau) = \chi_k(\sigma)\chi_\ell(\tau)$. Let $c = \operatorname{infl}(c_0) \in Z^2(F, \Lambda)$ denote the inflation of c_0 to F. As F is a free group, $H^2(F, \Lambda) = 0$. Hence, there exists a cochain

$$u = u^{(k,\ell)} \colon F \to \Lambda$$

such that $c = \partial u$. We may assume that $u(x_i) = 0$ for all i by substracting a suitable 1-cocycle, i.e. homomorphism. Then for $x, y \in F$ we have

$$u(xy) = u(x) + u(y) - \chi_k(x)\chi_l(y), \tag{5.2}$$

and $u(xy) = u(x) + u(y)$ if x or $y \in C^2F$. Note that C^3F is topologically generated by $x^q[x, y]$ where $x \in C^2F, y \in F$. It follows that the restriction of u to C^2F induces a homomorphism $u_2 \in \operatorname{Hom}(\operatorname{gr}^2 F, \Lambda)$. If $y \in R \subseteq C^2F$ and $x \in F$, then

$$u(xyx^{-1}) = u([x, y]y) \underset{y \in C^2F}{=} \underbrace{u([x, y])}_{=0 \text{ as } [x,y] \in C^3F} + u(y) = u(y).$$

Therefore $v := u_2|_R$ is an element of $\operatorname{Hom}_G(R, \Lambda) = H^1(R, \Lambda)^G$. Consider the isomorphism given by the transgression map $\operatorname{tg} \colon H^1(R, \Lambda)^G \xrightarrow{\cong} H^2(G, \Lambda)$. By definition we have

$$\operatorname{tg}(v) = [\partial u] = \chi_k \cup \chi_\ell.$$

It follows that

$$b_{k\ell} = \mathrm{tr}_\rho(\chi_k \cup \chi_\ell) = v(\rho) = u^{(k,\ell)}(\rho).$$

Recall that by Proposition 5.1.11 we can write ρ as

$$\rho = \prod_{j=1}^{n} x_j^{qa_j} \cdot \prod_{1 \leq \nu < \mu \leq n} [x_\nu, x_\mu]^{a_{\nu\mu}} \bmod C^3F.$$

Notice that u is a homomorphism on C^2F that vanishes on C^3F. Hence, we have a map $u\colon \mathrm{gr}^2 F \to \Lambda$. We deduce that

$$u(\rho) = \sum_{j=1}^{n} a_j \cdot u\left(x_j^q\right) + \sum_{1 \leq \nu < \mu \leq n} a_{\nu\mu} \cdot u\left([x_\nu, x_\mu]\right)$$

and in order to prove the uniqueness in Proposition 5.1.11 and prove (i), it suffices to compute the values of $u(x_j^q)$ and $u([x_\nu, x_\mu])$.

Since $u(x) + u\left(x^{-1}\right) + \chi_k(x)\chi_l(x) = 0$ for $x \in F$ by (5.2), we have

$$u(x_\nu x_\mu) = u(x_\nu) + u(x_\mu) - \chi_k(x_\nu)\chi_\ell(x_\mu) \qquad \text{for } \nu < \mu$$

and hence

$$\begin{aligned} u\left([x_\nu, x_\mu]\right) &= u(x_\nu x_\mu (x_\mu x_\nu)^{-1}) = u(x_\nu x_\mu) + u((x_\mu x_\nu)^{-1}) + \chi_k(x_\nu x_\mu)\chi_\ell(x_\mu x_\nu) \\ &= -\chi_k(x_\nu)\chi_\ell(x_\mu) - (u(x_\nu x_\mu) + \chi_k(x_\mu x_\nu)\chi_\ell(x_\mu x_\nu)) + \chi_k(x_\nu x_\mu)\chi_\ell(x_\mu x_\nu) \\ &= \delta_{k\mu}\delta_{\ell\nu} - \delta_{k\nu}\delta_{\ell\mu}. \end{aligned}$$

It follows that

$$u\left([x_\nu, x_\mu]\right) = \begin{cases} -1 & \text{if } k = \nu, \ell = \mu, \\ 1 & \text{if } k = \mu, \ell = \nu, \\ 0 & \text{otherwise.} \end{cases}$$

If $k \neq \ell$, we have $u(x_i^m) = u(x_i^{m+1})$ and $u(x_i^{-1}) = 0$, implying $u(x_i^m) = 0$ for all $m \in \mathbb{Z}$. Now if $k = \ell$, we have

$$u(x_i^{m+1}) = u(x_i^m) - \chi_k(x_i)\chi_\ell(x_i) = u(x_i^m) - m\delta_{ki},$$

implying

$$u(x_i^m) = -\binom{m}{2}\delta_{ki}.$$

for all $m \geq 1$. It follows that

$$b_{k\ell} = \mathrm{tr}_\rho\left(\chi_k \cup \chi_\ell\right) = u(\rho) = \left\{ \begin{array}{rll} -a_{k\ell} & \text{if} & k < \ell, \\ a_{\ell k} & \text{if} & k > \ell, \\ -\binom{q}{2}a_k & \text{if} & k = \ell. \end{array} \right.$$

(ii) We assume that $q \neq 0$, i.e. $\Lambda = \mathbb{Z}/q\mathbb{Z}$. Let $\chi = \chi_i \in Z^1(G, \Lambda)$ and let $s\colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q^2\mathbb{Z}$ be a map of sets that selects representatives modulo q^2, and furthermore we ask for $s(0) = 0$. Then $\widetilde{\chi} = s \circ \chi$ is a lift of χ to a map

$$\widetilde{\chi}\colon G \to \mathbb{Z}/q^2\mathbb{Z} \in C^1(G, \mathbb{Z}/q^2\mathbb{Z}).$$

As the Bockstein homomorphism is a connecting homomorphism in the long sequence in cohomology coming from the short exact sequence

$$0 \longrightarrow \mathbb{Z}/q\mathbb{Z} \xrightarrow{q} \mathbb{Z}/q^2\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow 0,$$

see also (2.2), we can determine a cocycle representation of $\beta(\chi)$ in the following way:

$$(d\widetilde{\chi})_{\sigma,\tau} = \sigma.\widetilde{\chi}_\tau - \widetilde{\chi}_{\sigma\tau} + \widetilde{\chi}_\sigma = \widetilde{\chi}(\sigma) + \widetilde{\chi}(\tau) - \widetilde{\chi}(\sigma\tau) \in q\mathbb{Z}/q^2\mathbb{Z}.$$

Hence, we can define the cocycle $b_0 = (b_0)_\chi \in Z^2(G, \Lambda)$ corresponding to $\beta(\chi) \in H^2(G, \Lambda)$ as

$$(b_0)_{\sigma,\tau} = \frac{1}{q}(d\widetilde{\chi})_{\sigma,\tau} = \frac{1}{q}\left(\widetilde{\chi}(\sigma) + \widetilde{\chi}(\tau) - \widetilde{\chi}(\sigma\tau)\right).$$

Let $b = \operatorname{infl}(b_0) \in Z^2(F, \Lambda)$. Again, as $H^2(F, \Lambda) = 0$, there exists a cochain

$$u = u_\chi\colon F \to \Lambda$$

such that $b = \partial u$. Here we may assume that $u(x_i) = 0$ for all i by subtracting a suitable homomorphism, i.e. 1-cocycle. As in (2), the restriction $u|_{C^2F}$ is a group homomorphism. Indeed, for x or $y \in C^2F$ we have

$$\big(u(x) + u(y)\big) - u(xy) = (\partial u)_{x,y} = b_{x,y} = \frac{1}{q}\left(\widetilde{\chi}(x) + \widetilde{\chi}(y) - \widetilde{\chi}(xy)\right) = 0,$$

since $\widetilde{\chi}$ is constant on C^2F-cosets and $\widetilde{\chi}(1) = 0$. Furthermore, $u|_{C^2F}$ vanishes on C^3F, i.e. for every $y \in C^2F$ and $x \in F$ we have

$$u(xyx^{-1}) = u(y).$$

Let $v = u|_R \in H^1(R, \Lambda)^G$. It follows that

$$\operatorname{tr}_\rho(\beta(\chi)) = v(\rho) = u(\rho)$$

and just as before to show the claim it suffices to compute the values $u(x_j^q)$ and $u\left([x_\nu, x_\mu]\right)$. Let $\chi = \chi_\ell$ for some fixed ℓ. Straight forward computations yield that $u(x_j^q) = -\delta_{j\ell}$ and $u\left([x_\nu, x_\mu]\right) = 0$. Thus, the claim follows.

□

We want to state two further observations that will be useful in the next chapter.

Lemma 5.1.13. *The sequence*

$$0 \to \operatorname{Hom}(\operatorname{gr}^2 G, \Lambda) \to \operatorname{Hom}(\operatorname{gr}^2 F, \Lambda) \to H^1(R, \Lambda)^G$$

is exact.

Proof. As $R/R^q[R,F]$ surjects on the kernel of $\mathrm{gr}^2 F \twoheadrightarrow \mathrm{gr}^2 G$, the claim follows after applying $\mathrm{Hom}(-,\Lambda)$. □

In the next result we essentially determine the kernel of the cup product and Bockstein homomorphism. The kernel of the cup product was e.g. given by Sullivan in [Sul75], where he omitted the proof saying it requires "a certain amount of soul searching classical algebraic topology". Explicit computations for the kernel of the cup product (with coefficients in a field) can be found in [Hil85]. For us there will be no need for more soul searching, as we show that computing this kernel essentially can be reduced to the computations we already did in Proposition 5.1.12.

Lemma 5.1.14. *In the case $q = 0$ the following sequence is exact:*

$$0 \longrightarrow \mathrm{Hom}(\mathrm{gr}^2 G, \Lambda) \xrightarrow{[\,,\,]^*} \bigwedge^2 H^1(G,\Lambda) \xrightarrow{(-\cup-)} H^2(G,\Lambda).$$

Assuming $q \neq 0$, the sequence

$$0 \longrightarrow \mathrm{Hom}(\mathrm{gr}^2 G, \Lambda) \xrightarrow{[\,,\,]^*, Q^*} \bigwedge^2 H^1(G,\Lambda) \bigoplus H^1(G,\Lambda) \xrightarrow{(-\cup-)\oplus\beta_G} H^2(G,\Lambda)$$

is exact.

Proof. We will discuss the case $q \neq 0$ here, i.e. $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$. Let $\beta\colon H^1(G,\Lambda) \to H^2(G,\Lambda)$ denote the Bockstein homomorphism. The case $q = 0$ follows by the same argument. Now consider the following diagram for any $\rho \in R$

$$\begin{tikzcd}
 & 0 \arrow[d] & & \\
0 \arrow[r, dotted] & \mathrm{Hom}(\mathrm{gr}^2 G, \Lambda) \arrow[r, "{[\,,\,]^*, Q^*}"] \arrow[d, hook] & \bigwedge^2 H^1(G,\Lambda) \bigoplus H^1(G,\Lambda) \arrow[r, "(-\cup-)\oplus\beta_G"] \arrow[d, "\cong"] & H^2(G,\Lambda) \arrow[dd, "\mathrm{tr}_\rho"] \\
 & \mathrm{Hom}(\mathrm{gr}^2 F, \Lambda) \arrow[r, "\cong", "{[\,,\,]^*, Q^*}"'] \arrow[d, "i^*"] & \bigwedge^2 H^1(F,\Lambda) \bigoplus H^1(F,\Lambda) & \\
 & \mathrm{Hom}(R/R^q[R,F], \Lambda) \arrow[rr, "\mathrm{ev}_\rho"'] \arrow[uurr, bend right=15, "\mathrm{tg}", "\cong"'] & & \Lambda.
\end{tikzcd}$$

The exactness on the left-hand column was shown in the previous lemma. The vertical middle arrow is an isomorphism by assumption on Λ, as we have $F^{\mathrm{ab}} \otimes \Lambda \cong G^{\mathrm{ab}} \otimes \Lambda$. Recall that by a theorem of Hall [Hal59, Thm. 11.2.4], the Λ-module $\mathrm{gr}^2 F$ is free abelian with basis of the form $[x_\ell, x_k]$ and x_j^q. This explains the isomorphism in the middle row.

We want to show exactness of the top row. Essentially, this follows from the exactness of the left-hand column, and the commutativity of the diagram up to sign. For injectivity, we require the top-left square to commute, which is clear. For the commutativity of the rest of the diagram, we rearrange the data as follows

$$\begin{tikzcd}
 & & \operatorname{Hom}(\bigwedge^2(F^{\mathrm{ab}}\otimes\Lambda)\oplus(F^{\mathrm{ab}}\otimes\Lambda),\Lambda) \arrow[d, equal] \\
\operatorname{Hom}(\operatorname{gr}^2 F,\Lambda) \arrow[r, "\cong", "{[\,,\,]^*,Q^*}"'] \arrow[ddr, "i^*"] & \bigwedge^2 H^1(F,\Lambda)\bigoplus H^1(F,\Lambda) & \bigwedge^2 H^1(G,\Lambda)\bigoplus H^1(G,\Lambda) \arrow[l, "\cong"'] \arrow[d, "{(-\cup-,\,\beta)}"] \\
 & H^1(R,\Lambda)^G \arrow[r, "\cong", "\mathrm{tg}"'] \arrow[d, equal] & H^2(G,\Lambda) \arrow[d, "\mathrm{tr}_\rho"] \\
 & \operatorname{Hom}(R/R^q[F,R],\Lambda) \arrow[r, "\mathrm{ev}_\rho"] & \Lambda.
\end{tikzcd}$$

Let $\xi_1,\dots,\xi_n$ denote the image of $x_1,\dots,x_n$ in $\operatorname{gr}^1 F$. Furthermore, let $\chi_1,\dots,\chi_n$ denote a basis of $H^1(F,\Lambda)\cong H^1(G,\Lambda)$ dual to $\xi_1,\dots,\xi_n$, i.e. $\chi_i(x_j)=\delta_{ij}$. Recall that by Proposition 5.1.12 (i) the element ρ, which is contained in C^2F by assumption, is of the form

$$\rho=\prod_{j=1}^n x_j^{a_j}\prod_{k<\ell}[x_k,x_\ell]^{a_{k,\ell}} \operatorname{mod} C^3F,$$

where the exponents are uniquely determined elements of Λ. In particular, they are determined by the cup product and Bockstein homomorphism, as stated in the same proposition. Thus, commutativity comes down to a retelling of the arguments in the respective proofs of Proposition 5.1.12, and hence will be omitted. □

5.2 Demuškin groups

Demuškin groups are a special class of finitely generated pro-p groups. They satisfy the condition

$$\dim H^2(G,\mathbb{F}_p)=1,$$

and the cup product

$$-\cup-\colon H^1(G,\mathbb{F}_p)\times H^1(G,\mathbb{F}_p)\to H^2(G,\mathbb{F}_p)$$

is a nondegenerate bilinear form. In number theory, they arise as the Galois group $\operatorname{Gal}(K(p)/K)$ of the maximal pro-p extension of a p-adic number field K containing the pth roots of unity, and in algebraic geometry as maximal pro-p quotients of fundamental groups of projective curves. The former example is the main motivation for studying this class of pro-p groups in this thesis and the latter example will provide substantial insight in the last chapter of the thesis.

Demuškin groups are of great interest on their own, as they display many nice properties. There is a complete classification of Demuškin groups: This is based on work by Demuškin [Dem61], [Dem63], and Serre [Ser62], and was completed by Labute in [Lab67]. In particular, a Demuškin group G is determined, up to isomorphism, by two invariants $n=\dim H^1(G,\mathbb{F}_p)$, which we call the rank of G, and q, which is the cardinality of the torsion part of the abelianization[1] of G. One obtains an explicit form for the relations of Demuškin groups. However, this

[1] When $q=2$ a finer invariant is needed

does not exhaust the interest in these groups. They are still studied in group theory, including, but not limited to works like [Son74], [DL83], [KZ05], [Koc13b], [SZ16], [SZ20]. Our motivating examples also provide plenty of further questions of arithmetic or field theoretic nature to explore. One big open question arising is of "anabelian" nature, asking if the property of having a Demuškin group as the Galois group of the maximal pro-p extension implies some sort of arithmetic structure on the field, resembling the structure of p-adic number fields containing pth roots of unity. Questions of this sort are discussed in e.g. [Win89], [Koe98], [Efr03], or [Lab+06].

In this section, we recall the proof of the structure theorem for Demuškin groups for $p \neq 2$, as some of the arguments provide central ideas for the next chapter. First, we shall discuss some preliminaries on symplectic forms on free modules over local rings.

5.2.1 Symplectic forms and isotropic subspaces

Let $(\Lambda, \mathfrak{m})$ be a local ring with residue field $\kappa = \Lambda/\mathfrak{m}$. Let M be a free Λ-module of rank n. We assume that $\operatorname{char} \kappa \neq 2$.

Definition 5.2.1 (Symplectic form)**.** A bilinear form $\omega \colon M \times M \to \Lambda$ is called a *symplectic form* if

(i) it is skew-symmetric, i.e. $\omega(a, b) = -\omega(b, a)$ for all $a, b \in M$,

(ii) it is non-degenerate, i.e. for some (or equivalently any) basis $a_1, \ldots, a_n$ of M as a Λ-module, we have $\det(\omega(a_i, a_j)_{i,j}) \in \Lambda^\times$.

Notice that (ii) in the above definition, given (i), is equivalent to ω inducing a symplectic bilinear form on the κ-vector space $M \otimes_\Lambda \kappa$.

Assuming char$\kappa \neq 2$ implies that n is even. We set $t = n/2$. A tuple $(e_1, f_1, \ldots, e_t, f_t)$ is a *symplectic basis* over Λ if

(i) $\omega(e_i, f_i) = 1$ for all $1 \leq i \leq t$,

(ii) $\omega(e_i, f_j) = \omega(e_i, e_j) = \omega(f_i, f_j) = 0$ otherwise.

We call a submodule N of M *isotropic* if $\omega(a, b) = 0$ for all $a, b \in N$. Note that the rank of any free isotropic subspace is at most t by non-degeneracy of ω. Furthermore, for any isotropic subspace we have $N \subseteq N^\perp$, and ω induces a symplectic form on the quotient $N^\perp/N$.

Proposition 5.2.2. *Let $(\Lambda, \mathfrak{m})$ be a local ring, let $M \cong \Lambda^n$ be a free Λ-module, let ω be a symplectic form, and let N be a pure isotropic submodule of rank $s < t$. Then there exists a symplectic basis $e_1, f_1, \ldots, e_t, f_t$ of M over Λ such that $e_1, \ldots, e_s$ is a basis for N. Furthermore, one of the basis elements e_i of N can be prescribed.*

Proof. See [Son74, Prop. 3]. □

For $N = 0$, this yields the following result.

Lemma 5.2.3. *Let $(\Lambda, \mathfrak{m})$ be a local ring, let $M \cong \Lambda^n$ be a free Λ-module, and let ω be a symplectic form. Then there exists a symplectic basis of M.*

More specifically, we will be interested in the following situation. We consider a surjective Λ-linear map $\beta\colon M \to \Lambda$. For any choice of section $s\colon \Lambda \to M$ we have $M = \ker\beta \oplus s\Lambda$. In particular, as a projective submodule that is a direct summand, $\ker\beta$ is a free Λ-module. Furthermore, we note that $\ker\beta^{\perp}$ is an isotropic subspace as it is of rank 1. We claim that it is also free. Indeed, the above mentioned isomorphism $M \xrightarrow{\sim} \operatorname{Hom}(M,\Lambda)$ restricts to

$$M \cong \operatorname{Hom}(M,\Lambda) \to \operatorname{Hom}(\ker\beta,\Lambda),$$

which must be surjective as $\ker\beta$ is a direct summand. Note that $\operatorname{Hom}(\ker\beta,\Lambda)$ is a free Λ-module as $\ker\beta$ is a free Λ-module. Thus, we have a short exact sequence of Λ-modules

$$0 \to \ker\beta^{\perp} \to M \to \operatorname{Hom}(\ker\beta,\Lambda) \to 0,$$

which implies that $\ker\beta^{\perp}$ is free, as claimed. Furthermore, it follows that $(\ker\beta^{\perp})^{\perp} = \ker\beta$.

Corollary 5.2.4. *Let $(\Lambda,\mathfrak{m})$ be a local ring, let $M \cong \Lambda^n$ be a free Λ-module, let ω be a symplectic form, and let $\beta\colon M \to \Lambda$ be a surjective Λ-linear map. There exists a symplectic basis $x_1,\dots,x_n$ of M such that $\beta(x_i) = \delta_{i1}$.*

5.2.2 Basics about Demuškin groups

Let G be a finitely generated pro-p group. For this section, we set $H^i(G) = H^i(G,\mathbb{Z}/p\mathbb{Z})$ and consider these groups as $\mathbb{F}_p$-vector spaces. Recall that $H^1(G)$ is the Pontryagin dual of the group $G/\Phi(G)$. Here $\Phi(G) = G^p[G,G]$ is the Frattini subgroup of G, see Proposition 2.1.12.

First, we give a purely cohomological description of Demuškin groups.

Definition 5.2.5 (Demuškin group)**.** A pro-p group G is called a *Demuškin group* if its cohomology has the following properties:

(i) $\dim_{\mathbb{F}_p} H^1(G) < \infty$,

(ii) $\dim_{\mathbb{F}_p} H^2(G) = 1$,

(iii) the cup-product $H^1(G) \times H^1(G) \to H^2(G)$ is non-degenerate.

The only finite Demuškin group occurs for $p = 2$ and $\dim_{\mathbb{F}_p} H^1(G) = 1$, i.e. $G \cong \mathbb{Z}/2\mathbb{Z}$. See [NSW13, Prop. 3.9.10] for a proof. From now on we shall always assume that G is infinite.

If G is a Demuškin group, G is a finitely generated topological group with minimal number of generators $n = n(G) = \dim H^1(G)$. Condition (ii) implies the existence of one relation such that G is the quotient $F/\langle\!\langle\rho\rangle\!\rangle$. In this notation F is a free pro-p group of rank n and $\langle\!\langle\rho\rangle\!\rangle$ denotes the normal subgroup of F generated by some $\rho \in \Phi(F) = F^p[F,F]$. Passing to the maximal abelian quotient G^{ab}, we obtain G^{ab} as a quotient of $\mathbb{Z}_p^n$ by either a subgroup isomorphic to $\mathbb{Z}_p$ or zero. This leads us to the previously defined invariant $q = q(G)$ as the cardinality of the torsion part of G^{ab}.

The main example of Demuškin groups in number theory is the following.

Theorem 5.2.6. *Let p be a prime and let K be a p-adic local field of degree $N = [K:\mathbb{Q}_p]$.*

(i) If $\mu_p \not\subseteq K$, then $\operatorname{Gal}_K(p)$ is a free pro-p group of rank $N+1$.

(ii) If $\mu_p \subseteq K$, then $\mathrm{Gal}_K(p)$ *is a Demuškin group of rank $N+2$. Furthermore,*

$$q(\mathrm{Gal}_K(p)) = \#\mu_{p^\infty}(K).$$

Proof. See [NSW13, Thm. 7.5.11]. A detailed discussion of this special case can be found in [Koc13a, §8]. □

Another example arising from algebraic geometry is the following.

Example 5.2.7. Let $G = \pi_1(S)$ be the fundamental group of a compact orientable surface S of genus g with $g \geq 1$. Then the pro-p completion $G^{\wedge p}$ is a Demuškin group of rank $2g$ with $q(G) = 0$. This example will play a key role in the last chapter of this thesis.

In the following we will always assume that $p \neq 2$. In particular, we have $q \neq 2$ and n is even, because the cup-product is a symplectic pairing.

The structure of Demuškin groups has been studied in the 60's by Demuškin when q is not a power of 2, by Serre for $q \neq 2$, and finally by Labute, who completed the case $p = 2$, thus giving a full classification. We will only consider the result for $q \neq 2$, and only prove the case $p \neq 2$, in this thesis.

Theorem 5.2.8 (Demuškin)**.** *Let G be a one-relator pro-p group. Suppose that the invariant q of G is different from* 2*. Then G is a Demuškin group if and only if it is isomorphic to the pro-p group defined by n generators $x_1, \dots, x_n$, for some even number $n \geq 2$, subject to the one relation*

$$x_1^q[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n] = 1.$$

In particular, G is then determined by the two invariants n and q up to isomorphism.

So in the example of Theorem 5.2.6, we have the following result.

Theorem 5.2.9 (Demuškin)**.** *Let K be a p-adic local field of degree N and let $p^t = \#\mu_{p^\infty}(K)$. If $p^t > 2$, then* $\mathrm{Gal}_K(p)$ *is isomorphic to the pro-p group defined by $N+2$ generators $y_1, \dots, y_{N+2}$, subject to the one relation*

$$y_1^{p^t}[y_1, y_2][y_3, y_4] \cdots [y_{N+1}, x_{N+2}] = 1.$$

We will discuss the proof of this result in the next section, as it will provide key insights towards studying the automorphisms of Demuškin groups. Furthermore, we want to note that by Proposition 2.2.19 we get the following result.

Proposition 5.2.10. *Let G be a Demuškin group. Then G is a Poincaré group of dimension 2 and its dualizing module is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as an abelian group.*

For a Demuškin group G, and a continuous homomorphism $\chi\colon G \to \mathbb{Z}_p^\times$, we set $I = \mathbb{Q}_p/\mathbb{Z}_p(\chi)$ for the G-module structure on $\mathbb{Q}_p/\mathbb{Z}_p$ where G acts via the character χ. Note that $I[p^n] = \mathrm{Hom}(\mathbb{Z}/p^n\mathbb{Z}, I)$ for all $n \geq 1$. Furthermore, we have a short exact sequence

$$0 \to I[p^{n-1}] \to I[p^n] \xrightarrow{\cdot p^{n-1}} I[p] \to 0 \tag{5.3}$$

where we understand the right-hand map as the multiplication with p^{n-1} after identifying $I[p]$ with its image in $I[p^n]$. We can now state the following result characterizing the dualizing module of a Demuškin group.

Proposition 5.2.11. *Let G be a Demuškin group, and let $\chi\colon G \to \mathbb{Z}_p^\times$ denote a continuous homomorphism. Let $I = \mathbb{Q}_p/\mathbb{Z}_p(\chi)$. Then the following are equivalent:*

(i) I is dualizing (in the sense of Proposition 2.2.19),

(ii) For all $n \geq 1$ the map $H^1(G, I[p^n]) \to H^1(G, I[p])$ is surjective.

Proof. Let I be a dualizing module of G. Considering (5.3), and using $\operatorname{cd}(G) = 2$, we get a long exact sequence

$$H^1(G, I[p^n]) \to H^1(G, I[p]) \xrightarrow{\partial} H^2(G, I[p^{n-1}]) \to H^2(G, I[p^n]) \to H^2(G, I[p]) \to 0.$$

We show $\partial = 0$. By duality this is equivalent to the surjectivity of

$$H^0(G, \operatorname{Hom}(I[p^n], I)) \to H^0(G, \operatorname{Hom}(I[p^{n-1}], I))$$

induced by restriction. But $\operatorname{Hom}(I[p^n], I) \cong \mathbb{Z}/p^n\mathbb{Z}$ as G-modules, and restriction induces the canonical map

$$\mathbb{Z}/p^n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

Now we prove the converse direction and assume (ii), i.e. we have a short exact sequence

$$0 \to H^2(G, I[p^{n-1}]) \to H^2(G, I[p^n]) \xrightarrow{\pi} H^2(G, I[p]) \to 0. \tag{5.4}$$

By induction we get injective maps $H^2(G, I[p]) \hookrightarrow H^2(G, I[p^n])$ induced by the inclusion. Thus the map π comes from multiplication by p^{n-1}, i.e. we have

$$\begin{tikzcd}
H^2(G, I[p^n]) \arrow[r, "\pi"] \arrow[dr, "p^{n-1}\cdot"] & H^2(G, I[p]) \arrow[d, hook] \\
 & H^2(G, I[p^n]).
\end{tikzcd}$$

As G is a Demuškin group, we have $H^2(G, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$. Since $I[p] \cong \mathbb{Z}/p\mathbb{Z}$ as G-modules, there is no non-trivial action of a p-group G on $\mathbb{Z}/p\mathbb{Z}$. We have $\#H^2(G, I[p]) = p$. By induction on n, we get $\#H^2(G, I[p^n]) = p^n$ by (5.4). Thus, $H^2(G, I[p^{n-1}])$ is the p^{n-1}-torsion part of $H^2(G, I[p^n])$. By induction, the p-torsion of $H^2(G, I[p^n])$ is $H^2(G, I[p])$, which is of order p. As $H^2(G, I[p^n])$ has order p^n, we conclude by the structure theory of abelian groups that $H^2(G, I[p^n])$ is cyclic of order p^n. Thus we get an isomorphism $\operatorname{tr}_n\colon H^2(G, I[p^n]) \xrightarrow{\cong} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$, which can be chosen compatibly as $H^2(G, I[p^{n-1}])$ is the p^{n-1}-torsion part of $H^2(G, I[p^n])$. Taking the colimit over all n, we get the trace map

$$\begin{tikzcd}
H^2(G, I) \arrow[r, "\operatorname{tr}", "\cong"'] \arrow[d, equal] & \mathbb{Q}_p/\mathbb{Z}_p. \\
\operatorname{colim}_n H^2(G, I[p^n]) \arrow[ur, "\operatorname{colim}_n \operatorname{tr}_n"'] &
\end{tikzcd}$$

We want to show that for any finite G-module A there exists an isomorphism

$$\operatorname{Hom}_G(A, I) = H^0(G, \operatorname{Hom}(A, I)) \cong H^2(G, A)^\vee.$$

We do this by induction on the order of A. As $\mathbb{Z}/p\mathbb{Z}$ is the only simple G-module and the category of finite G-modules is noetherian, for any such A there exists a sequence of G-modules

$$0 \to A_1 \to A \to A_2 \to 0$$

where $\#A_2 = p$, i.e. $A_2 \cong \mathbb{Z}/p\mathbb{Z}$. The claim holds for A_2 by the properties of Demuškin groups. Consider the dual sequence

$$0 \to \operatorname{Hom}(A_2, I) \to \operatorname{Hom}(A, I) \to \operatorname{Hom}(A_1, I) \to 0.$$

For the induction step we consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_G(A_2, I) \arrow[r] \arrow[d, "\cong"] & \operatorname{Hom}_G(A, I) \arrow[r] \arrow[d, "f \mapsto \operatorname{tr} \circ f_*"] & \operatorname{Hom}_G(A_1, I) \arrow[r, "\delta"] \arrow[d] & H^1(G, \operatorname{Hom}(A_2, I)) \arrow[d, "a \mapsto (b \mapsto \operatorname{tr}(a \cup b))", "\cong"'] \\
0 \arrow[r] & H^2(G, A_2)^\vee \arrow[r] & H^2(G, A)^\vee \arrow[r] & H^2(G, A_1)^\vee \arrow[r, "\delta^\vee"] & H^1(G, A_2)^\vee.
\end{tikzcd} \tag{5.5}$$

The right-hand square commutes by a cocycle computation using the formal properties of the cup product. We note that as a G-module $\operatorname{Hom}(A_2, I) \cong \mathbb{Z}/p\mathbb{Z}$. Hence, the right-hand vertical arrow is an isomorphism induced by the cup-product by the properties of G. As $\#A_1 < \#A$, the claim now follows by induction. □

This enables us to explicitly describe the action of G on the dualizing module I in terms of the generators from Theorem 5.2.8.

Theorem 5.2.12 (Labute). *Let G be a Demuškin group. If $x_1, \dots, x_n$ are generators of G, and $q = q(G)$, and $\rho = x_1^q[x_1, x_2][x_3, x_4] \cdot \ldots \cdot [x_{n-1}, x_n]$ is the defining relation of G as in Theorem 5.2.8, then the action of G on the dualizing module I, or equivalently the associated character $\chi\colon G \to \operatorname{Aut}(I) = \mathbb{Z}_p^\times$, is given by*

$$\chi(x_i) = \begin{cases} (1-q)^{-1}, & \textit{if } i = 2, \\ 1, & \textit{otherwise.} \end{cases}$$

In particular, $\operatorname{im}(\chi)$ *is an invariant of G, and we have* $\operatorname{im}(\chi) = 1 + q\mathbb{Z}_p$ *and $q = \#I^G$.*

Proof. Let F be a free pro-p group in the generators $x_1, \dots, x_n$. We define a group homomorphism as follows

$$\begin{aligned} \chi\colon F &\to \mathbb{Z}_p^\times \\ x_i &\mapsto \begin{cases} (1-q)^{-1}, & \text{if } i = 2, \\ 1, & \text{otherwise.} \end{cases} \end{aligned}$$

This factors over G as

$$\chi(\rho) = \chi(x_1^q) = 1.$$

We verify that the G-module $I = \mathbb{Q}_p/\mathbb{Z}_p(\chi)$ is indeed the dualizing module of G. Let

$$T_p(I) = \lim_n I[p^n] \cong \mathbb{Z}_p,$$

and let R denote the normal subgroup of F generated by ρ. Consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & H^1(G,T_p(I)) \arrow[r] \arrow[d] & H^1(F,T_p(I)) \arrow[r, "\mathrm{res}"] \arrow[d, two heads] & H^1(R,T_p(I))^G \\
0 \arrow[r] & H^1(G,I[p]) \arrow[r] & H^1(F,I[p]) \arrow[r] & H^1(R,I[p]).
\end{tikzcd}$$

The second vertical arrow is surjective as F has cohomological dimension 1. The restriction map

$$H^1(F,T_p(I)) \to H^1(R,T_p(I))^G$$

is zero by a computation of Labute, which is contained in the proof of [Lab67, Thm. 4]. It follows that

$$H^1(G,T_p(I)) \to H^1(G,I[p])$$

is surjective and hence

$$H^1(G,I[p^n]) \to H^1(G,I[p])$$

is surjective for all n. Thus, the claim follows by the characterization of the dualizing module of G given in Proposition 5.2.11.

It remains to show the claim about q. Consider the sequence

$$0 \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Q}_p/\mathbb{Z}_p \to 0 \tag{5.6}$$

and note that

$$\begin{aligned}
H^1(G,\mathbb{Q}_p/\mathbb{Z}_p) &= (G^{\mathrm{ab}})^\vee, \\
H^2(G,\mathbb{Z}/p^n\mathbb{Z})^\vee &= H^0(G,I[p^n]) = I^G[p^n], \\
H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)^\vee &= (\operatorname{colim}_n H^2(G,\mathbb{Z}/p^n\mathbb{Z}))^\vee = \lim_n H^0(G,I[p^n]) = T_p(I)^G = 0.
\end{aligned}$$

Hence the Pontryagin dual of the cohomology sequence of (5.6) is

$$0 \to I^G[p^n] \to G^{\mathrm{ab}} \xrightarrow{p^n\cdot} G^{\mathrm{ab}}.$$

Taking the colimit over all n yields an isomorphism

$$I^G \xrightarrow{\cong} (G^{\mathrm{ab}})_{\mathrm{tors}}.$$

The torsion subgroup of of G^{ab} is of order $q = q(G)$, thus proving the second claim. □

The classification result by Labute shows that Demuškin groups are classified up to isomorphism by the invariants n and $\mathrm{im}(\chi)$. We express this in the following structure theorem.

Theorem 5.2.13 (Labute)**.** *Let F be a free pro-p group, let $\rho, \rho' \in F^p[F,F]$ and let $G = F/\langle\langle\rho\rangle\rangle$ and $G' = F/\langle\langle\rho'\rangle\rangle$ be Demuškin groups with characters $\chi\colon G \to \mathbb{Z}_p^\times$ resp. $\chi'\colon G' \to \mathbb{Z}_p^\times$ characterizing the dualizing module. If $\operatorname{im}\chi = \operatorname{im}\chi'$, then there exists an automorphism of F mapping ρ to ρ'. In particular, G and G' are isomorphic.*

5.2.3 Proof of Theorem 5.2.8

We present a proof of Theorem 5.2.8 following [NSW13] which in turn follows John Labute [Lab67]. We shall always assume that $p \neq 2$, but note that this case is treated by Labute.

Let $G = F/\langle\langle \rho \rangle\rangle$ be a Demuškin group. In the case $q = q(G) \neq 0$ there is a uniquely determined class $\sigma \operatorname{mod} [F, F]$ in F^{ab} (which is a free abelian pro-p group) such that

$$\rho \equiv \sigma^q \bmod [F, F].$$

As $- \cup -$ induces a symplectic form on $H^1(G, \Lambda) = H^1(F, \Lambda)$ there exists a $\chi_\sigma \in H^1(G, \Lambda)$ such that for all $\eta \in H^1(G, \Lambda)$ we have $\eta \cup \chi_\sigma = \eta(\sigma)$.

Proposition 5.1.12 and Proposition 5.2.2 prove the following first key insight towards Theorem 5.2.8.

Proposition 5.2.14. *Let $G = F/\langle\langle \rho \rangle\rangle$ be a Demuškin group. There exists a basis $\chi_1, \ldots, \chi_n$ of $H^1(G, \Lambda)$ such that*

$$\chi_1 \cup \chi_2 = \chi_3 \cup \chi_4 = \ldots = \chi_{n-1} \cup \chi_n = 1$$

with $\chi_i \cup \chi_j = 0$ for all other $i < j$. If $q \neq 0$ we may choose this basis such that $\chi_i(\sigma) = \delta_{1i}$, or equivalently $\chi_\sigma = \chi_2$.

Remark 5.2.15. As linear forms

$$\eta \mapsto \eta \cup \chi_2 \quad \text{and} \quad \eta \mapsto \eta \cup \chi_\sigma$$

agree on above basis, by non-degeneracy of the cup-product it follows that $\chi_2 = \chi_\sigma$. Hence, we have

$$\chi_\sigma(\sigma) = \chi_\sigma \cup \chi_\sigma = \chi_2 \cup \chi_\sigma = 0.$$

The next step towards proving Theorem 5.2.8 is the observation that, in a sense, it suffices to consider relations up to the third step of the Λ-filtration.

Proposition 5.2.16. *Let $G = F/\langle\langle \rho \rangle\rangle$ be a finitely generated one relator pro-p group with invariants (n, q). Then G is a Demuškin group if and only if there exists a basis $x_1, \ldots, x_n$ of F such that*

$$\rho \equiv x_1^q \, [x_1, x_2] \, [x_3, x_4] \cdots [x_{n-1}, x_n] \bmod C^3F.$$

Proof. Assume $G = F/\langle\langle \rho \rangle\rangle$ is a Demuškin group. Then the cup product is non-degenerate by definition and we can choose a basis $\chi_1, \ldots, \chi_n$ of $H^1(G, \Lambda)$ of the previously described form. Recall that $H^1(G, \Lambda)^\vee \cong F/F^q[F, F]$. Let $\xi_1, \ldots, \xi_n \in F/F^q[F, F]$ denote the dual basis and $x_1, \ldots, x_n$ a lift to F. This gives a minimal generator system of F with corresponding basis $\chi_1, \ldots, \chi_n$. By Proposition 5.1.12 we know that

$$\rho = \prod_{j=1}^{n} x_j^{q a_j} \cdot \prod_{1 \leq k < \ell \leq n} [x_k, x_\ell]^{a_{k\ell}} \bmod C^3F, \quad a_j, a_{k\ell} \in \Lambda$$

where $a_{k\ell}$ are uniquely determined. If $q \neq 0$, so are the a_j. Furthermore, as $a_{k\ell} = \chi_k \cup \chi_\ell$, we have

$$\rho = \prod_{j=1}^{n} x_j^{q a_j} \cdot [x_1, x_2] \, [x_3, x_4] \cdots [x_{n-1}, x_n] \bmod C^3F, \quad a_j \in \Lambda.$$

For $q = 0$ we are done. Assume $q \neq 0$. As

$$\sigma \equiv \prod_{j=1}^{n} x_j^{\widehat{a}_j} \bmod [F,F], \quad \widehat{a}_j \in \mathbb{Z}_p$$

with

$$a_j \equiv \widehat{a}_j \bmod q\mathbb{Z}_p = \chi_j(\sigma) = \delta_{1j}$$

the claim follows because of the uniqueness of the exponents a_j.

Now assuming

$$\rho \equiv x_1^q \, [x_1, x_2] \, [x_3, x_4] \cdots [x_{n-1}, x_n] \bmod C^3F$$

we have

$$B = \begin{pmatrix} -\binom{q}{2} & 1 & & & \\ -1 & -\binom{q}{2} & & 0 & \\ & & \ddots & & \\ & 0 & & -\binom{q}{2} & 1 \\ & & & -1 & -\binom{q}{2} \end{pmatrix}$$

with $B = (\mathrm{tr}_\rho(\chi_i \cup \chi_j))$ as in Proposition 5.1.12. Then $\det(B)$ is invertible in Λ. Hence, the cup-product is non-degenerate and G is a Demuškin group. □

We need to find an equation from the above congruence. For every n -tuple $y = (y_1, \dots, y_n)$ with $y_i \in F$ we set

$$r(y) = y_1^q \, [y_1, y_2] \, [y_3, y_4] \cdots [y_{n-1}, y_n] \, .$$

Let $x_1, \dots, x_n$ be a basis of F and let $\xi_1, \dots, \xi_n$ denote the image in $\mathrm{gr}^1(F)$. Let $j \geq 2$. Let $t_1, \dots, t_n \in C^{j-1}F$, and set $y_i = x_i t_i^{-1}$. Then $y_1, \dots, y_n$ is a basis of F, as $x_i \equiv y_i \bmod C^2F$, satisfying

$$r(x) = r(y) d_{j-1}(t_1, \dots, t_n),$$

where $d_{j-1}(t_1, \dots, t_n)$ is a uniquely determined element of C^jF. Let τ_i denote the image of t_i in $\mathrm{gr}^{j-1}(F)$. Then it follows from well-known formulas in $\mathrm{gr}(F)$ stated in [NSW13, Prop. 3.8.5] that the image of $d_{j-1}(t_1, \dots, t_n)$ in $\mathrm{gr}^j(F)$ is given by

$$\delta_{j-1}(\tau_1, \dots, \tau_n) \coloneqq \pi \cdot \tau_1 + [\tau_1, \xi_2] + [\xi_1, \tau_2] + \ldots + [\tau_{n-1}, \xi_n] + [\xi_{n-1}, \tau_n] \, . \tag{5.7}$$

Hence, we have a map of $\Lambda[\pi]$-modules $\delta_{j-1} \colon \mathrm{gr}^{j-1}(F)^n \to \mathrm{gr}^j(F)$. This induces a morphism of graded $\Lambda[\pi]$-modules

$$\delta \colon (\mathrm{gr}(F))^n \to \mathrm{gr}(F)[1],$$

where $\mathrm{gr}(F)[1]$ denotes the graded $\Lambda[\pi]$-module with the grading shifted by 1.

One of the most important insights towards understanding the structure of Demuškin groups lies in the fact that this map is surjective. This was proven in [Lab67, Prop. 5 (1)], but we give a slightly modified argument. Note that this statement does not hold when $p = 2$.

Proposition 5.2.17. *The map $\delta \colon \mathrm{gr}(F)^n \to \mathrm{gr}(F)[1]$ is surjective. In particular, for all $j \geq 2$ the map $\delta_{j-1} \colon \mathrm{gr}^{j-1}(F)^n \to \mathrm{gr}^j(F)$ is surjective, i.e. $\mathrm{gr}^j(F) = \mathrm{im}(\delta_{j-1})$.*

Proof. Set $L = \operatorname{gr}(F)$, and let $\overline{L} = L \otimes_{\Lambda[\pi]} \Lambda = L/\pi L$. The image of δ is a graded $\Lambda[\pi]$-submodule of $L[1]$. Consider

$$\overline{\delta} = \delta \otimes_{\Lambda[\pi]} \Lambda \colon (\overline{L})^n \to \overline{L[1]}.$$

Looking at (5.7), the surjectivity of $\overline{\delta}$ is immediate. Using the Nakayama lemma for graded $\Lambda[\pi]$-modules the claim follows. Indeed, given surjectivity of $\overline{\delta}$, it holds that

$$\begin{aligned} L[1] &= \operatorname{im}\delta + \pi L[1] = \operatorname{im}\delta + \pi \operatorname{im}\delta + \pi^2 L[1] \\ &= \operatorname{im}\delta + \pi \operatorname{im}\delta + \pi^2 \operatorname{im}\delta + \dots \pi^k \operatorname{im}\delta + \pi^{k-1} L[1] \\ &= \operatorname{im}\delta + \pi^{k-1} L[1], \end{aligned}$$

and in degree m for $k \geq m$ we have $(\pi^{k-1}L[1])_m = \pi^{k-1}L[1]_{m-k-1} = 0$. □

This results implies the following statement, which is the crucial idea in proving Theorem 5.2.8.

Lemma 5.2.18. *Let $\rho \in C^2F$. For every $j \geq 3$ there exists a basis $x = (x_1, \dots, x_n)$ of F such that*

$$\rho \equiv r(x) \bmod C^jF$$

provided this is true for $j = 3$.

Proof. Let $j \geq 3$. The claim essentially follows from the previous discussion. Assume there exists a minimal generator system $x = (x_1, \dots, x_n)$ of F such that $\rho = r(x)e_j$ for some $e_j \in C^jF$. Let ε_i denote the image of e_j in $\operatorname{gr}^j(F)$. There exist $t_1, \dots, t_n \in C^{j-1}F$ with image τ_i of t_i in $\operatorname{gr}^{j-1} F$, such that

$$\delta_{j-1}(\tau_1, \dots, \tau_n) = -\varepsilon_j.$$

Then $y_i = x_i t_i^{-1}$ for $i = 1, \dots, n$ is a minimal generator system of F such that

$$\rho = r(x)e_j = r(y)d_{j-1}(t_1, \dots, t_n)e_j \equiv r(y) \bmod C^{j+1}F.$$ □

We can now prove the classification result on Demuškin groups.

Proof of Theorem 5.2.8. Let $G = F/\langle\langle \rho \rangle\rangle$ be a Demuškin group. Then by Lemma 5.2.18 and Proposition 5.2.16 we find a minimal system of generators $x^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$ of F such that

$$\rho \equiv r(x^{(j)}) \bmod C^jF.$$

Let $X^{(j)}$ denote the set of all minimal systems of generators $x^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$ with $\rho \equiv r(x^{(j)}) \bmod C^jF$. This is non-empty and compact, and hence the projective limit $X = \varprojlim X^{(j)}$ is non-empty by Proposition 2.1.9. Choosing any $x = (x_1, \dots, x_n)$ in X yields a basis of F such that $\rho = r(x)$.

Let $G = F/\langle\langle \rho \rangle\rangle$ be a one relator pro-p-group such that there exists a basis $x = (x_1, \dots, x_n)$ of F with $\rho = r(x)$. Then $\rho \equiv r(x) \bmod C^3F$. It follows that G is a Demuškin group by Proposition 5.2.16. □

Remark 5.2.19. One of the key ingredients of the proof was the surjectivity of

$$\delta =: \delta_r\colon \operatorname{gr}(F)^n \to \operatorname{gr}(F)[1].$$

Let $G = F/\langle\langle\rho\rangle\rangle$ be a 1-relator group, where F is a free pro-p group in $x_1, \ldots, x_n$ and $\rho = r(x) \in C^2F$. An interesting follow-up question could be to study under what condition on ρ the "deformation map" $\delta = \delta_r$, defined as above, is surjective. As via the Magnus embedding $\operatorname{gr}(F)$ can be viewed as a free sub-Lie algebra of $\operatorname{gr}\Lambda\langle\langle X_1, \ldots, X_n\rangle\rangle$ in the letters $x_1, \ldots, x_n$ with coefficients in $\Lambda[\pi]$, pro-p Fox calculus might be a helpful tool to answer this question.

5.2.4 Further properties of Demuškin groups

Lemma 5.2.20. *Let G be a Demuškin group.*

(i) (Schreier formula) Every subgroup H of finite index is a Demuškin group with

$$n(H) = 2 + (G : H)(n(G) - 2).$$

(ii) Every subgroup H of infinite index is free pro-p.

Remark 5.2.21. In fact the property in Lemma 5.2.20 (i) gives an equivalent definition of Demuškin groups. See [DL83].

Lemma 5.2.22. *Let $F = \widehat{F}_X$ be a free pro-p group of rank at least two. Then F has trivial center.*

Proof. By assumption $F \neq Z(F)$. Further assume that $Z(F) \neq \{1\}$. Then there exist elements $1 \neq z \in Z(F), g \in F \setminus Z(F)$. Let A denote the normal subgroup generated by z, g. This is an abelian torsion-free subgroup of F. Hence, it is of cohomological dimension at most 1. It follows that $A \cong \mathbb{Z}_p = \langle g\rangle$. Thus, there exists an integer $n \geq 1$ such that $g^n \in \langle z\rangle$. It follows that for all $g \in F \setminus Z(F)$ there exists an integer $n \geq 1$ such that $g^n \in Z(F)$. But this cannot be true for the generators of F. If $x, y \in X$, then for any $n, m \geq 1$ the image of the commutator $[x^n, y^m]$ in $\operatorname{gr}^2 F$ is congruent to $nm[x, y]$, thus not trivial. □

Lemma 5.2.23. *Let G be a Demuškin group. Then for any short exact sequence*

$$1 \to F_\varphi \to G \xrightarrow{\varphi} \mathbb{Z}_p \to 1$$

the kernel $F_\varphi = \ker\varphi$ is a free pro-p group.

Proof. This is clear as F_φ must have cohomological dimension 1 by Lemma 5.2.20 (ii). □

Note that an infinite Demuškin group G can only be abelian if $n = \dim_{\mathbb{F}_p} H^1(G) = 2$. In that case $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proposition 5.2.24. *Let G be a Demuškin group of rank $n \geq 4$. Then G has trivial center.*

Proof. Assume there exists an element $1 \neq z \in Z(G)$. Let $\overline{z}$ denote the image of z in G^{ab}. Then the quotient

$$G^{\mathrm{ab}} \to G^{\mathrm{ab}} / \langle z \rangle$$

is finitely generated of rank $n-2$ as a $\mathbb{Z}_p$-module. Hence, there exists a surjective homomorphism

$$G^{\mathrm{ab}} / \langle z \rangle \twoheadrightarrow \mathbb{Z}_p.$$

So we have found a surjective homomorphism

$$\varphi \colon G^{\mathrm{ab}} \twoheadrightarrow \mathbb{Z}_p$$

such that $\varphi(\overline{z}) = 0$. As φ is determined on generators of G, we have a short exact sequence

$$1 \to F_\varphi \to G \xrightarrow{\varphi} \mathbb{Z}_p \to 0$$

where F_φ is free by Lemma 5.2.23. As by construction we have $\varphi(z) = 0$, it follows that $z \in F_\varphi$. Per assumption $z \in Z(G)$, hence $z \in Z(F)$. By Lemma 5.2.22 this is a contradiction. □

Remark 5.2.25. For any $K/\mathbb{Q}_p$ of degree N we have

$$\mathrm{Gal}_K(p) \ncong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Indeed, $\mathbb{Z}_p \times \mathbb{Z}_p$ has cohomological dimension 2. By Theorem 5.2.6 this could only be possible if $\mu_p \subseteq K$. But in this case the rank of the Demuškin group $\mathrm{Gal}_K(p)$ is $N+2$, i.e. larger than 2.

6 Automorphisms of Demuškin groups

In this section we again always assume that $p \neq 2$. We want to give lifting conditions for morphisms of finitely generated pro-p groups. First, we introduce some new notation.

Definition 6.0.1 (k-liftability)**.** Let G, H be finitely generated pro-p groups. Let $\Lambda = \Lambda(G)$ and let $C^{\bullet}(-)$ denote the Λ-filtration. For every $m \geq 2$ we call a morphism $\varphi_m \colon G \to H/C^m H$ *k-liftable*, if there exists a morphism $\varphi_{m+k} \colon G \to H/C^{m+k}H$ such that $\varphi_{m+k} \equiv \varphi_m \bmod C^m H$. In this case, we call φ_{m+k} a k-lift of φ_m.

We denote the subset of k-liftable morphisms as

$$\mathrm{Hom}^{(+k)}(G, H/C^m H) \subseteq \mathrm{Hom}(G, H/C^m H).$$

If we only consider surjective morphisms $G \to H/C^m H$, we denote the subset of surjective k-liftable morphisms as

$$\mathrm{Hom}^{(+k)}(G, H/C^m H)_{\mathrm{surj}} \subseteq \mathrm{Hom}(G, H/C^m H)_{\mathrm{surj}},$$

where we note that the respective lifts are automatically surjective. In the case $G = H$ we set

$$\mathrm{Aut}^{(+k)}(G/C^m G) \coloneqq \mathrm{Hom}^{(+k)}(G, G/C^m G)_{\mathrm{surj}}.$$

Note that, while

$$\mathrm{Hom}(G, H/C^m H) = \mathrm{Hom}(G/C^m G, H/C^m H),$$

we do not use this notation for the set of k-liftable morphisms to avoid suggesting that the induced morphisms $G/C^m G \to H/C^m H$ lift. Furthermore, note that, in fact $\mathrm{Aut}^{(+k)}(G/C^m G) \subseteq \mathrm{Aut}(G/C^m G)$, as any (surjective) morphism $G \to G/C^m G$ factors through a (surjective) morphism $G/C^m G \to G/C^m G$, and as finitely generated profinite groups are Hopfian, see Proposition 2.1.8, any epimorphism is an isomorphism.

In this chapter, we deal with the question when a morphism $\varphi_m \colon G \to H/C^m H$ is liftable to a morphism $\varphi \colon G \to H$. We can do this step by step as $H = \varprojlim_m H/C^m H$, with index set $(\mathbb{N}, \leq)$, starting with $m = 2$. In this case, we can give an answer for finitely generated pro-p groups G. This is what we do in the first section. Theorem 6.1.2 gives a cohomological condition in terms of compatibility with cup product and Bockstein homorphism.

In the next section we specialize to the case where G is a Demuškin group. Assuming $m \geq 3$ we show that any surjective morphism φ_m admits a lift $\varphi_{m+1} \colon G \to H/C^{m+1}H$ such that

$$\varphi_{m+1} \equiv \varphi_m \bmod C^{m-1}H.$$

This is shown in Theorem 6.2.5. In particular for $H = G$, we see that $(\mathrm{Aut}^{(+1)}(G/C^m G))_{m \geq 2}$ is a surjective system for $\mathrm{Aut}(G)$, i.e.

$$\mathrm{Aut}(G) \cong \varprojlim_m \mathrm{Aut}^{(+1)}(G/C^m G).$$

In the case where G is a Demuškin group, the result of Section 6.1 will yield an isomorphism

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup -,\beta)}(H^1(G,\Lambda)),$$

where the right-hand group denotes all automorphisms of the free Λ-module $H^1(G,\Lambda)$ that are compatible with the cup product and, if $q \neq 0$, the Bockstein homomorphism, up to a factor. In the right choice of basis we provide a rather explicit description of $\mathrm{Aut}^{(-\cup -,\beta)}(H^1(G,\Lambda))$, see Proposition 6.1.5. Finally, we conclude that we have a surjective group homomorphism

$$\overline{\pi_2}\colon \mathrm{Out}(G) \twoheadrightarrow \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup -,\beta)}(H^1(G,\Lambda)),$$

which we view as an analogue to the symplectic representation of the mapping class group of a surface S.

6.1 Lifting conditions for level $m = 2$

6.1.1 Cup product and Bockstein

The goal of this section is to apply the ideas of Proposition 5.1.12 to the following question. Let G, H be finitely generated pro-p groups. Assume we are given a morphism

$$\varphi_2\colon G \to H/C^2H.$$

Under what conditions does φ_2 lift to a morphism $\varphi_3\colon G \to H/C^3H$?

If $\Lambda := \Lambda(G)$ is torsion, we denote the image of cup-product and Bockstein homomorphism

$$-\cup - \oplus \beta\colon \bigwedge^2 H^1(G,\Lambda) \bigoplus H^1(G,\Lambda) \to H^2(G,\Lambda)$$

by $H^2_{(-\cup -,\beta)}(G,\Lambda)$ (and similarly $H^2_{(-\cup -,\beta)}(H,\Lambda)$ for H). If $\Lambda = \mathbb{Z}_p$, we only consider the image of the cup-product, and denote this by $H^2_{(-\cup -)}(G,\Lambda)$, and $H^2_{(-\cup -)}(H,\Lambda)$, respectively.

Before we can state the main result, we want to recall that a Λ-module M is *reflexive* if the natural map

$$M \to \mathrm{Hom}_\Lambda(\mathrm{Hom}_\Lambda(M,\Lambda),\Lambda)$$

is an isomorphism. We also note the following.

Lemma 6.1.1. *Let Λ be a ring and M a finitely generated Λ-module.*

(i) If $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$, then M is reflexive.

(ii) If $\Lambda = \mathbb{Z}_p$ and M is free, then M is reflexive.

The main result now goes as follows.

Theorem 6.1.2. *Let G, H be finitely generated pro-p groups. Assume that $\mathrm{gr}^2 G, \mathrm{gr}^2 H$ are reflexive Λ-modules. Let $\varphi_2\colon G \to H/C^2H$ be a morphism of pro-p groups. Then the following are equivalent.*

(a) The morphism φ_2 is 1-liftable.

(b) *(i) If $q = 0$, there exists a map $H^2_{(-\cup-)}(H,\Lambda) \to H^2_{(-\cup-)}(G,\Lambda)$ compatible with cup product, i.e. the following diagram commutes*

$$\begin{tikzcd}
\bigwedge^2 H^1(H,\Lambda) \arrow[r, "\wedge^2\varphi_2^*"] \arrow[d, "-\cup-"] & \bigwedge^2 H^1(G,\Lambda) \arrow[d, "-\cup-"] \\
H^2_{(-\cup-)}(H,\Lambda) \arrow[r] & H^2_{(-\cup-)}(G,\Lambda).
\end{tikzcd}$$

(ii) If $q \neq 0$, there exists a map $H^2_{(-\cup-,\beta)}(H,\Lambda) \to H^2_{(-\cup-,\beta)}(G,\Lambda)$ compatible with cup product, and Bockstein homomorphism, i.e. the following diagram commutes

$$\begin{tikzcd}
\bigwedge^2 H^1(H,\Lambda) \bigoplus H^1(H,\Lambda) \arrow[r] \arrow[d, "-\cup-\oplus\beta"] & \bigwedge^2 H^1(G,\Lambda) \bigoplus H^1(G,\Lambda) \arrow[d, "-\cup-\oplus\beta"] \\
H^2_{(-\cup-,\beta)}(H,\Lambda) \arrow[r] & H^2_{(-\cup-,\beta)}(G,\Lambda).
\end{tikzcd}$$

Let

$$1 \to R \to F \to G \to 1$$

denote a group presentation of G, where F is the free pro-p group on generators $x_1,\dots,x_n$ such that $F^{\mathrm{ab}} \otimes \Lambda = G^{\mathrm{ab}} \otimes \Lambda$, i.e. R is generated by elements $\rho_1,\dots,\rho_r \in C^2F$.

Recall from Section 5.1.1 that we have a commutator map

$$\begin{tikzcd}
\mathrm{gr}^1 G \times \mathrm{gr}^1 G \arrow[r, "{[\,,\,]}"] \arrow[d] & \mathrm{gr}^2 G \\
\bigwedge^2 \mathrm{gr}^1 G \arrow[ur] &
\end{tikzcd}$$

given by $(x \bmod C^2G, y \bmod C^2G) \mapsto [x,y] \bmod C^3G$ for all $x,y \in G$.

Furthermore, assuming $q \neq 0$, we have a map

$$Q\colon\ \mathrm{gr}^1 G \to \mathrm{gr}^2 G,\quad y \mapsto \widetilde{y}^q.$$

We first give a reformulation of (a).

Lemma 6.1.3. *Let $\psi\colon F \to H/C^3H$ be a lift of $\varphi_2\colon G \to H/C^2H$, i.e.*

$$\begin{tikzcd}
F \arrow[r, "\psi"] \arrow[d, two heads] & H/C^3H \arrow[d, two heads] \\
G \arrow[r, "\varphi_2"] & H/C^2H.
\end{tikzcd}$$

Then the following are equivalent.

(a) ψ factors through G.

(a') The induced morphism of Λ*-modules* $\mathrm{gr}^2\,\psi\colon\ \mathrm{gr}^2 F \to \mathrm{gr}^2 H$ *factors through* $\mathrm{gr}^2 G$*.*

(a') The induced morphism of* Λ*-modules* $(\mathrm{gr}^2\,\psi)^*\colon\ \mathrm{Hom}(\mathrm{gr}^2 H, \Lambda) \to \mathrm{Hom}(\mathrm{gr}^2 F, \Lambda)$ *factors through* $\mathrm{Hom}(\mathrm{gr}^2 G, \Lambda)$*.*

Proof. The implication (a') to (a'*) is always true. The reverse implication follows as $\mathrm{gr}^2 G$ and $\mathrm{gr}^2 H$ are reflexive Λ-modules by assumption. Consider the following diagram where the vertical arrows are central exact sequences:

$$\begin{tikzcd}
1 \arrow[d] & & \\
\mathrm{gr}^2 F \arrow[d] \arrow[rd, two heads] \arrow[rrd, dashed] & 1 \arrow[d, "\mathrm{gr}^2\,\psi"] & 1 \arrow[d] \\
F/C^3F \arrow[d] \arrow[rd, two heads] \arrow[rrd, dashed] & \mathrm{gr}^2 G \arrow[r, dotted] \arrow[d, "\psi \bmod C^3H"] & \mathrm{gr}^2 H \arrow[d] \\
F/C^2F \arrow[d] \arrow[rd, "\cong"] & G/C^3G \arrow[r, dotted] \arrow[d] & H/C^3H \arrow[d] \\
1 & G/C^2G \arrow[r] \arrow[d] & H/C^2H \arrow[d] \\
 & 1 & 1.
\end{tikzcd}$$

We see that ψ factors through G if and only if $\psi \bmod C^3H$ factors through G/C^3G. By assumption we have $F/C^2F \cong G/C^2G$. It follows that

$$\ker(\mathrm{gr}^2 F \to \mathrm{gr}^2 G) \xrightarrow{\cong} \ker(F/C^3F \to G/C^3G).$$

Now finally, we note that

$$\psi(\ker(\mathrm{gr}^2 F \to \mathrm{gr}^2 G)) = 0 \quad \Leftrightarrow \quad \mathrm{gr}^2\,\psi(\ker(\mathrm{gr}^2 F \to \mathrm{gr}^2 G)) = 0,$$

which shows the equivalence of (a) and (a'). □

Remark 6.1.4. We want to note that in the proof above, we choose a lift $\psi\colon F \to H/C^3H$. However, we see that it does not matter which lift we choose as $\mathrm{gr}^2\,\psi$ only depends on $\psi \bmod C^2H$, which is determined by φ_2. If there exists such a lift to F that factors through G, so do all. In other words, if there exists a lift of φ_2, there exist many lifts of φ_2.

Proof of Theorem 6.1.2. First, we note that (a) in Theorem 6.1.2 is equivalent to (a) in Lemma 6.1.3. So let $\psi\colon F \to H/C^3H$ be a lift of

$$F \to F/C^2F = G/C^2G \xrightarrow{\varphi_2} H/C^2H.$$

By Lemma 6.1.3 it now suffices to show the equivalence of (b) and (a'*). This follows from a diagram chase in the following diagram (which needs to be adjusted when $q = 0$), where the vertical sequences are exact by Lemma 5.1.14 and the definition of $H^2_{-\cup-,\beta}$. The bottom 0 in the right column comes from the fact that free groups have cohomological dimension 1.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
\mathrm{Hom}(\mathrm{gr}^2 H, \Lambda) \arrow[r, dashed] \arrow[d, "{[\,,\,]^*, Q^*}"'] \arrow[rr, bend left, "(\mathrm{gr}^2 \psi)^*"] & \mathrm{Hom}(\mathrm{gr}^2 G, \Lambda) \arrow[r, hook] \arrow[d, "{[\,,\,]^*, Q*}"'] & \mathrm{Hom}(\mathrm{gr}^2 F, \Lambda) \arrow[d, "{[\,,\,]^*, Q^*}"', "\cong"] \\
\begin{array}{c}\bigwedge^2 H^1(H,\Lambda) \\ \bigoplus H^1(H,\Lambda)\end{array} \arrow[r] \arrow[d, "-\cup-\oplus\beta"] & \begin{array}{c}\bigwedge^2 H^1(G,\Lambda) \\ \bigoplus H^1(G,\Lambda)\end{array} \arrow[r, "\cong"] \arrow[d, "-\cup-\oplus\beta"] & \begin{array}{c}\bigwedge^2 H^1(F,\Lambda) \\ \bigoplus H^1(F,\Lambda)\end{array} \arrow[d, "-\cup-\oplus\beta"] \\
H^2_{(-\cup-,\beta)}(H, \Lambda) \arrow[r, dashed] \arrow[d] & H^2_{(-\cup-,\beta)}(G, \Lambda) \arrow[r] \arrow[d] & 0. \\
0 & 0 &
\end{tikzcd}$$

□

6.1.2 The group of 1-liftable automorphisms of $G^{\mathrm{ab}} \otimes \Lambda$

Let Λ be a local ring, and let M be a free Λ-module of rank n. Let $\omega \colon M \times M \to \Lambda$ be a symplectic form, and let $\beta \colon M \to \Lambda$ be a surjective Λ-linear map. We define

$$\mathrm{Aut}^{(\omega,\beta)}(M) := \{(A, \lambda) \in \mathrm{GL}(M) \times \Lambda^\times \mid A^*\omega = \lambda\omega, A^*\beta = \lambda\beta\}$$

to be the group of automorphisms of the free Λ-module M respecting both the symplectic structure on M as well as the linear condition imposed by β up to a factor λ. The group $\mathrm{Aut}^{(\omega,\beta)}(M)$ is a subgroup of the Λ-valued points of the general symplectic group after choosing a symplectic basis

$$\mathrm{Aut}^{(\omega,\beta)}(M) \hookrightarrow \mathrm{GSp}(M, \omega) = \mathrm{GSp}_n(\Lambda).$$

We will from now on consider $\mathrm{GSp}(M, \omega)$ as an algebraic group over Λ, so that

$$\mathrm{Aut}^{(\omega,\beta)}(M) \subseteq \underline{\mathrm{GSp}}(M, \omega)(\Lambda).$$

Recall that there exists a symplectic basis $\chi_1, \dots, \chi_n$ of M such that $\beta(\chi_i) = \delta_{i1}$ by Corollary 5.2.4. Using this particular choice of basis, we can give a very explicit description of $\mathrm{Aut}^{(\omega,\beta)}(M)$. Recall that a *parabolic subgroup* of $\underline{\mathrm{GSp}}(M, \omega)(\Lambda)$ is the stabilizer of some flag on $\Lambda^n = M$, where a flag is just a sequence of isotropic subspaces $(N_1, \dots, N_r)$ of M, i.e.

$$(0) \subset N_1 \subset \ldots \subset N_r \subset N_r^\perp \subset N_{r-1}^\perp \subset \ldots \subset N_1^\perp \subset M.$$

For an isotropic subspace N the flag

$$(0) \subset N \subset N^\perp \subset M$$

determines a corresponding *maximal parabolic subgroup* $P_N(M) \hookrightarrow \underline{\mathrm{GSp}}(M, \omega)$.

Now consider the filtration on M given by $\ker\beta^{\perp}$, i.e.

$$(0) \subset \ker\beta^{\perp} \subset \ker\beta \subset M,$$

where we choose our basis elements $\chi_1, \ldots, \chi_n$ such that

$$\ker(\beta)^{\perp} = \langle \chi_2 \rangle \quad \text{and} \quad \ker(\beta) = \langle \chi_2, \ldots, \chi_n \rangle .$$

In particular, $M' = \ker(\beta)/\ker(\beta)^{\perp}$ has a Λ-basis given by the images of $\chi_3, \ldots, \chi_n$, and the image of χ_1 spans $\beta(M) = M/\ker(\beta)$.

One immediately sees that $\mathrm{Aut}^{(\omega,\beta)}(M)$ is a subgroup of the Λ-valued points $P_{\ker\beta^{\perp}}(M)(\Lambda)$ of the maximal parabolic subgroup $P_{\ker\beta^{\perp}}(M)$. Considering the maps

$$\begin{aligned} P_{\ker\beta^{\perp}}(M)(\Lambda) &\to \mathbb{G}_m(\Lambda), \quad (A,\lambda) \mapsto \lambda, \\ P_{\ker\beta^{\perp}}(M)(\Lambda) &\to \mathbb{G}_m(\Lambda), \quad (A,\lambda) \mapsto a_{11} =: \mu \end{aligned}$$

where $(a_{ij}) = A$ is represented with respect to the basis $\chi_1, \ldots, \chi_n$, the following holds.

Proposition 6.1.5. *There is a short exact sequence*

$$1 \to \mathrm{Aut}^{(\omega,\beta)}(M) \to P_{\ker\beta^{\perp}}(M)(\Lambda) \xrightarrow{\lambda\mu^{-1}} \mathbb{G}_m(\Lambda) \to 1.$$

Rearranging the previous choice of basis as $(\chi_2, \chi_3, \ldots, \chi_n, \chi_1)$ we may identify $\mathrm{Aut}^{(\omega,\beta)}(M)$ with the subgroup of $\mathrm{GSp}_n(\Lambda)$ of the form

$$\left\{ \left(\begin{array}{c|ccc|c} 1 & * & \cdots & * & * \\ \hline & & & & * \\ & & \underline{\mathrm{GSp}}^{(\lambda)}(M')(\Lambda) & & \vdots \\ & & & & * \\ \hline & & & & \lambda \end{array} \right) \;\middle|\; \lambda \in \Lambda^{\times} \right\}$$

where $\underline{\mathrm{GSp}}^{(\lambda)}(M')(\Lambda)$ denotes the subset of $\underline{\mathrm{GSp}}(M')(\Lambda)$ with factor of similitude equal to λ.

Proof. Set $P := P_{\ker\beta^{\perp}}(M)(\Lambda)$. Note that $\beta \circ A = \lambda \cdot \beta$ means that β and $\beta \circ A$ have the same kernel. For $n = 2$ we consider the basis χ_2, χ_1 with $\beta(\chi_1) = 1$ and $\chi_2 \in \ker\beta^{\perp}$. Noting that $\mathrm{GSp}_2(\Lambda) = \mathrm{GL}_2(\Lambda)$, the symplectic form ω is just the determinant. Hence, elements of P are of the form

$$\begin{pmatrix} \mu & * \\ & \lambda\mu^{-1} \end{pmatrix}.$$

Now an element of P belongs to $\mathrm{Aut}^{(\omega,\beta)}(M)$ if and only if $\lambda = \mu$. The claim follows. Now let $n > 2$. Let H denote the subgroup of P of the form

$$\begin{pmatrix} 1 & * & & & & & \cdots & * \\ & \lambda & & & & & & \vdots \\ & & 1 & & & & & \\ & & & \ddots & & & & \vdots \\ & & & & \ddots & & & \\ & & & & & \lambda & & \\ & & & & & & 1 & * \\ & & & & & & & \lambda \end{pmatrix}.$$

Then surjectivity of the right-hand map is already clear from restricting to H. □

As the parabolic group is a subgroup of upper block diagonal matrices, we can state the following corollary.

Corollary 6.1.6. *There is a natural inclusion*

$$\underline{\mathrm{GSp}}(\ker\beta/\ker\beta^{\perp})(\Lambda) \hookrightarrow \mathrm{Aut}^{(\omega,\beta)}(M), \quad (B,\lambda) \mapsto \begin{pmatrix} 1 & 0 & \dots & 0 \\ & & B & \vdots \\ & & & 0 \\ & & & \lambda \end{pmatrix}$$

and projection

$$\mathrm{Aut}^{(\omega,\beta)}(M) \twoheadrightarrow \underline{\mathrm{GSp}}(\ker\beta/\ker\beta^{\perp}), \quad \begin{pmatrix} 1 & * & \dots & * \\ & & B & \vdots \\ & & & * \\ & & & \lambda \end{pmatrix} \mapsto (B,\lambda)$$

which are group homomorphisms.

In particular, the results of the previous section yield the following.

Proposition 6.1.7. *Let G be a Demuškin group. Assume that $q \neq 0$, and let β denote the Bockstein homomorphism $H^1(G,\Lambda) \to \Lambda$. Then*

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda)).$$

Choosing $x_1, \dots, x_n$ to be generators of G as in Theorem 5.2.8, then for the corresponding dual basis $\chi_2, \chi_3, \dots, \chi_n, \chi_1$ this group is of the form described in Proposition 6.1.5. If $q = 0$, we have

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \mathbb{Z}_p) \cong \mathrm{GSp}_n(\mathbb{Z}_p).$$

6.2 Lifting conditions for level $m \geq 3$

Again assume G, H are finitely generated pro-p groups. We have established conditions for morphisms $\varphi_2 \colon G \to H^{\mathrm{ab}} \otimes \Lambda = H/C^2H$ to lift to morphisms $\varphi_3 \colon G \to H/C^3H$. The obvious follow-up questions are the following.

(i) Let $m \geq 3$. What is the condition for a morphism $G \to H/C^mH$ of pro-p groups to lift to a morphism of pro-p groups $G \to H/C^{m+1}H$?

(ii) What are the obstructions to lifting? How many possibilities are there?

We are able to give a partial answer to (i) whenever G is a Demuškin group, using similar ideas that appear in the proof of Theorem 5.2.8. First, we need to establish some basic results required for the main result of this section. We recall the following.

Lemma 6.2.1. *Let*

$$(\alpha)\colon \quad 1 \to A \to H \to Q \to 1 \tag{6.1}$$

denote the extension of a pro-p group by an abelian group A, and let $\varphi\colon G \to Q$ be a map such that we can regard A as a G-module. The embedding problem

$$\begin{tikzcd} & & & G \arrow[dl, dashed] \arrow[d, "\varphi"] & \\ 1 \arrow[r] & A \arrow[r] & H \arrow[r] & Q \arrow[r] & 1. \end{tikzcd}$$

is solvable if and only if the class $[\alpha]$ of the 2-cocycle α corresponding to the bottom row lies in the kernel of the inflation map induced by φ

$$H^2(Q, A) \to H^2(G, A).$$

Let $m \geq 2$. Recall that we always assume n is even and $q = q(G) \neq 2$. Let F be a free group of rank n, and let $x_1, \ldots, x_n$ denote a basis. For any $y = (y_1, \ldots, y_n) \in F^n$ we set

$$r(y) = y_1^q \, [y_1, y_2] \, [y_3, y_4] \cdots [y_{n-1}, y_n] \, .$$

Previously, we defined a map

$$d_m \colon (C^m F)^n \to C^{m+1} F, \quad t = (t_1, \ldots, t_n) \mapsto r(x) r(xt^{-1})^{-1},$$

which induced a surjective Λ-linear map

$$\delta_m \colon (\operatorname{gr}^m F)^n \to \operatorname{gr}^{m+1} F,$$

see Proposition 5.2.17. Let $\xi_1, \ldots, \xi_n$ denote the images of $x_1, \ldots, x_n$ in $\operatorname{gr}^1(F)$, and let $\tau = (\tau_1, \ldots, \tau_n)$ denote the image of an element $t = (t_1, \ldots, t_n) \in (C^m F)^n$ in $(\operatorname{gr}^m F)^n$. We note that $\operatorname{gr}^{m+1} F$ is generated by elements of the form $\pi \cdot \tau, [\tau, \xi]$ for all $i = 1, \ldots, n$. The proof of surjectivity of δ_m now provides the following result.

Corollary 6.2.2. *Let $m \geq 2$, and let F be a free pro-p group on the generators $x_1, \ldots, x_n$. Then the Λ-module $\operatorname{gr}^m F$ is generated by elements of the form*

$$\pi\tau + [\tau, \xi_2] \quad \text{and} \quad [\tau, \xi_i], \quad i \neq 2, \quad \text{for } \tau \in \operatorname{gr}^{m-1} F.$$

Lemma 6.2.3. *Let G be a Demuškin group of rank n, and let H be a finitely generated pro-p group such that there exists a surjective morphism $\varphi_m \colon G \to H/C^m H$ for some $m \geq 2$. Then there exists a minimal set of generators $x_1, \ldots, x_n$ of G such that $\operatorname{gr}^m H$ is generated by elements of the form*

$$\pi\tau + [\tau, \varphi_2(x_2)] \quad \text{and} \quad [\tau, \varphi_2(x_i)], \quad i \neq 2, \quad \text{for } \tau \in \operatorname{gr}^{m-1} F,$$

where $\varphi_2 = \varphi_m \bmod C^2 H$.

Proof. Let $x_1, \ldots, x_n$ be a minimal system of generators of G as in Theorem 5.2.8. Note that the surjection $G \twoheadrightarrow H/C^m H$ factors through a surjection $G/C^m G \twoheadrightarrow H/C^m H$. Let $\xi_j \in H$ denote the lifts $\varphi_2(x_j)$. The group $H/C^m H$ is generated by $\xi_j \bmod C^m H$. The claim follows from Corollary 6.2.2. □

Note that for $m \geq 2$ that the group $C^m H/C^{m+2}H$ is abelian, as $[C^m H, C^m H] \subseteq C^{m+2}H$.

Lemma 6.2.4. *Let G be a Demuškin group of rank n with invariant q, and let H be a finitely generated pro-p group. Let $m \geq 2$ and let $\varphi_{m+1}\colon G \twoheadrightarrow H/C^{m+1}H$ be a surjective morphism. There is an isomorphism*

$$H^2(G, C^m H/C^{m+2}H) \xrightarrow{\cong} H^2(G, \operatorname{gr}^m H).$$

Proof. Consider the exact sequence of G-modules

$$0 \to \operatorname{gr}^{m+1} H \to C^m H/C^{m+2}H \to \operatorname{gr}^m H \to 0. \tag{6.2}$$

Let I denote the dualizing module of G. This induces an exact sequence

$$0 \to \operatorname{Hom}_G(\operatorname{gr}^m H, I) \to \operatorname{Hom}_G(C^m H/C^{m+2}H, I) \to \operatorname{Hom}_G(\operatorname{gr}^{m+1} H, I).$$

We claim that the right-hand map is zero. Let $f \in \operatorname{Hom}_G(C^m H/C^{m+2}H, I)$. We need to show that f vanishes when restricted to $\operatorname{gr}^{m+1} H$.

Let $x_1, \ldots, x_n$ be a minimal system of generators as above. By Lemma 6.2.3, $\operatorname{gr}^{m+1} H$ is generated by elements of the form

$$\pi\tau + [\tau, \xi_2], \quad [\tau, \xi_j], \quad j \neq 2, \quad \text{for } \tau \in \operatorname{gr}^i H,$$

where $\xi_i = \varphi_2(x_i)$ for all $i = 1, \ldots, n$. We compute the images of these generators. First for any $\tau \in \operatorname{gr}^m H$, let $\widetilde{\tau} \in C^m H/C^{m+2}H$ such that $\widetilde{\tau} \bmod C^{m+1}H = \tau$. The action of G, in terms of the generators $x_1, \ldots, x_n$ of G, is given by conjugation. Written additively as an expression in $\operatorname{gr} H$, we have

$$x_j.\widetilde{\tau} = [\xi_j, \tau] + \widetilde{\tau}.$$

Let $\chi\colon G \to \operatorname{Aut}(I) = \mathbb{Z}_p^\times$ denote the character associated to G. It follows that

$$f([\xi_j, \tau] + \widetilde{\tau}) = f(x_j.\widetilde{\tau}) = \chi(x_j) \cdot f(\widetilde{\tau}).$$

By Theorem 5.2.12 the action of G in terms of this choice of basis is known. Namely, the character $\chi\colon G \to \operatorname{Aut}(I)$ is given by $\chi(x_2) = (1-q)^{-1}$ and $\chi(x_j) = 1$ otherwise by Theorem 5.2.12. Hence, for $j \neq 2$ we get

$$f([\tau, \xi_j]) = -f([\chi_j, \tau]) = f(\widetilde{\tau}) - f([\xi_j, \tau] + \widetilde{\tau}) = f(\widetilde{\tau}) - \chi(x_j) f(\widetilde{\tau}) = 0.$$

For $j = 2$ we note that

$$\begin{aligned} f(\pi\tau + [\tau, \xi_2]) &= f((\pi\tau)^{1+q+\cdots}) - f([\xi_2, \tau]) \\ &= f((\pi\tau)^{1+q+\cdots}) + f(\widetilde{\tau}) - f([\xi_2, \widetilde{\tau}] + \widetilde{\tau}) \\ &= f(\widetilde{\tau}^{(1-q)^{-1}}) - f(x_2.\widetilde{\tau}) \\ &= (1-q)^{-1} f(\widetilde{\tau}) - \chi(x_2) f(\widetilde{\tau}) = 0. \end{aligned}$$

This shows the claim, i.e. the map

$$\operatorname{Hom}_G(C^m H/C^{m+1}H, I) \to \operatorname{Hom}_G(C^m H/C^{m+2}H, I)$$

is an isomorphism. By duality it follows that we have an isomorphism

$$H^2(G, C^m H/C^{m+2}H) \xrightarrow{\cong} H^2(G, C^m H/C^{m+1}H). \qquad \square$$

Now we can state our main result. A similar proof can be found in [Win01, Prop. 1.3].

Theorem 6.2.5 (+1-liftability). *Let $m \geq 2$, let H be a finitely generated pro-p group, and let $\varphi_{m+1}\colon G \twoheadrightarrow H/C^{m+1}H$ be a surjective morphism. There exists a surjective morphism*

$$\varphi_{m+2}\colon G \twoheadrightarrow H \quad \textit{such that} \quad \varphi_{m+2} \equiv \varphi_{m+1} \bmod C^m H.$$

Proof. Let

$$\varphi_m\colon G \xrightarrow{\varphi_{m+1}} H/C^{m+1}H \twoheadrightarrow H/C^m H$$

denote the composition with the canonical projection. Consider the following diagram

$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi_m"] & \\
1 \arrow[r] & C^m H/C^{m+2}H \arrow[r] & H/C^{m+2}H \arrow[r] & H/C^m H \arrow[r] & 1.
\end{tikzcd} \tag{6.3}$$

To prove the claim, we need to show that the embedding problem (6.3) is solvable. The group extension in the bottom corresponds to a 2-cocycle β_m in $Z^2(H/C^m H, C^m H/C^{m+2}H)$. As stated in Lemma 6.2.1 the embedding problem translates to showing that the class β_m in $H^2(H/C^m H, C^m H/C^{m+2}H)$ maps to zero under this inflation map

$$H^2(H/C^m H, C^m H/C^{m+2}H) \to H^2(G, C^m H/C^{m+2}H).$$

Consider the following commutative diagram with exact rows

$$\begin{tikzcd}
 & & & & G \arrow[d, two heads, "\varphi_m"] \arrow[ddl, two heads, "\varphi_{m+1}"'] & \\
(\beta_m) & 1 \arrow[r] & C^m H/C^{m+2}H \arrow[r] \arrow[d, two heads, "\mathrm{can}"'] & H/C^{m+2}H \arrow[r] \arrow[d, two heads] & H/C^m H \arrow[r] \arrow[d, equal] & 1 \\
(\alpha_m) & 1 \arrow[r] & \operatorname{gr}^m H \arrow[r] & H/C^{m+1}H \arrow[r] & H/C^m H \arrow[r] & 1.
\end{tikzcd}$$

Note that there is a solution to the bottom embedding problem that we have denoted by α_m, meaning that the class of the corresponding 2-cocycle vanishes under the inflation map, i.e. $\varphi_m^*([\alpha_m]) = 0$. We now consider the induced diagram

$$\begin{tikzcd}
H^2(H/C^m H, C^m H/C^{m+2}H) \arrow[r, "\varphi_{m+1}^*"] \arrow[d, "\mathrm{can}_*"] & H^2(G, C^m H/C^{m+2}H) \arrow[d, "\mathrm{can}_*"', "\cong"] \\
H^2(H/C^m H, \operatorname{gr}^m H) \arrow[r, "\varphi_m^*"] & H^2(G, \operatorname{gr}^m H).
\end{tikzcd}$$

The injectivity of the vertical right arrow was proved in Lemma 6.2.4. As this diagram commutes, we have

$$\mathrm{can}_* \circ \varphi_m^*([\beta_m]) = \varphi_m^* \circ \mathrm{can}_*([\beta_m]) = \varphi_m^*([\alpha_m]) = 0.$$

As the vertical map on the right-hand side is injective, it follows that $\varphi_m^*([\beta_m]) = 0$. Hence, there exists a solution $\varphi_{m+2}\colon G \to H/C^{m+2}H$ to the embedding problem (β_m). The fact that φ_{m+2} is surjective follows from the surjectivity of φ_m using [NSW13, Prop. 3.9.1]. By construction this map induces φ_m, thus proving the claim. □

Proposition 6.2.6. *Let $m \geq 3$, let H be a finitely generated pro-p group. If there exists a surjective morphism $\varphi_m \colon G \twoheadrightarrow H/C^m H$, then there exists a surjective morphism $\varphi \colon G \twoheadrightarrow H$ such that $\varphi \equiv \varphi_j \bmod C^j H$ for all $j \geq m-1$.*

Proof. Note that

$$\operatorname{Hom}(G, H) = \varprojlim_m \operatorname{Hom}(G, H/C^m H).$$

As the inverse limit of any inverse system of non-empty finite sets is non-empty, this claim follows from the previous proposition. □

We want to provide an alternative proof of the previous result in a special case. We will assume that $H = G$. Let

$$1 \to \langle\langle \rho \rangle\rangle \to F \to G \to 1,$$

denote a presentation of G where F denotes the free pro-p group on the generators $x_1, \ldots, x_n$ such that $\chi(x_2) = (1-q)^{-1}$ and $\chi(x_i) = 1$ for all $i \neq 2$ (i.e. we are once again considering the standard Demuškin presentation). Again, we assume that for some $m \geq 2$ there exists a surjection

$$\varphi_{m+1} \colon G \twoheadrightarrow G/C^{m+1}G.$$

Clearly, there exists a lift $\psi_{m+2} \colon F \to G/C^{m+2}G$ of

$$\psi_{m+1} = \varphi_{m+1} \circ \mathrm{pr} \colon F \twoheadrightarrow G/C^{m+1}G.$$

Hence, we have the following diagram

$$\begin{tikzcd}
F \arrow[d, two heads, "\mathrm{pr}"] \arrow[dr, "\psi_{m+2}"] & \\
G \arrow[r, dotted, "\varphi_{m+2}"] \arrow[dr, "\varphi_{m+1}"] \arrow[ddr, "\varphi_m"'] & G/C^{m+2}G \arrow[d, two heads] \\
& G/C^{m+1}G \arrow[d, two heads] \\
& G/C^m G
\end{tikzcd}$$

and we claim that there exists a $\varphi_{m+2} \colon G \to G/C^{m+2}G$ such that $\varphi_{m+2} \equiv \varphi_{m+1} \bmod C^m H$.

Note that for $\underline{\tau} = (\tau_1, \ldots, \tau_n) \in \left(C^m G/C^{m+2}G\right)^n$ the map

$$\psi_{m+2} + \underline{\tau} \colon F \to G/C^{m+2}G$$

is a lift of $\varphi_m \circ \mathrm{pr}$.

Lemma 6.2.7. *Let F denote the free pro-p group in the generators $x_1, \ldots, x_n$. Let $m \geq 2$, and let $d_m \colon (C^m F)^n \to C^{m+1}F$ given by mapping $t = (t_1, \ldots, t_n)$ to $r(x)r(xt^{-1})^{-1}$, where $r(x) = x_1^q[x_1, x_2] \ldots [x_{n-1}, x_n]$. Then the induced map*

$$\delta_{m,m+2} \colon (C^m F/C^{m+2}F)^n \to \operatorname{gr}^{m+1} F$$

is surjective.

Proof. This is clear, as the induced map on graded Lie algebras is the same as in Proposition 5.2.17. □

The previous proposition may now be rephrased as follows.

Proposition 6.2.8. *With assumptions as above there exists a* $\underline{\tau} = (\tau_1, \dots, \tau_n) \in \left(C^m G/C^{m+2}G\right)^n$ *such that*

$$(\psi_{m+2} + \underline{\tau})(\rho) = 0.$$

In particular, there exists a surjective morphism

$$\varphi_{m+2} \colon G \to G/C^{m+2} \quad \textit{such that} \quad \varphi_{m+2} \equiv \varphi_{m+1} \bmod C^m G.$$

Proof. Note that $\psi_{m+2}(\rho) \in \mathrm{gr}_C^{m+1}(G)$ and we have

$$\psi_{m+2}(\rho) = (\psi_{m+2} + \underline{\tau})(\rho) + \delta_{m,m+2}(\underline{\tau}).$$

The claim now follows from the surjectivity of $\delta_{m,m+2}$. □

Remark 6.2.9. Both proofs of (+1)-liftability have Proposition 5.2.17 as a key input. The first proof uses the fact that Demuškin groups are Poincaré duality groups of dimension 2. The key input is used together with the fact that we can write out the action of the dualizing module for our standard set of generators of a Demuškin group. We choose to include this proof because it could be extended to another question raised in the beginning, namely how many possibilities of lifts there are, as this has a cohomological description in terms of first cohomology groups. However, this is computationally harder because we cannot use Poincaré duality in the same way.

6.3 Structure of the automorphism group of Demuškin groups

Now let G be a Demuškin group with invariants n and q, where q is not a power of 2. By Proposition 6.2.6 we get the following result:

Proposition 6.3.1. $(\mathrm{Aut}^{(+1)}(G/C^m G))_{m\geq 2}$ *is a surjective inverse system of the profinite group* $\mathrm{Aut}(G)$. *In particular, we have*

$$\mathrm{Aut}(G) \xrightarrow{\cong} \varprojlim_m \mathrm{Aut}^{(+1)}(G/C^m G).$$

This result in particular implies the following.

Theorem 6.3.2 (Symplectic representation for Demuškin groups)**.** *There is a continuous surjective group homomorphism*

$$\pi_2 \colon \mathrm{Aut}(G) \twoheadrightarrow \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup -,\beta)}(H^1(G, \Lambda)). \tag{6.4}$$

Furthermore, the kernel of π_2 *is a pro-p group.*

Proof. The surjectivity is a direct consequence of Proposition 6.3.1. The second claim follows from Proposition 2.6.5, as the kernel of $\mathrm{Aut}(G) \to \mathrm{Aut}(G^{\mathrm{ab}} \otimes \Lambda)$ being pro-p implies that $\ker \psi$ is pro-p. □

Corollary 6.3.3 (Symplectic representation for Demuškin groups)**.** *The above map induces a surjective group homomorphism*

$$\overline{\pi_2}\colon\ \mathrm{Out}(G) \twoheadrightarrow \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup -,\beta)}(H^1(G,\Lambda)). \tag{6.5}$$

Furthermore, the kernel of $\overline{\pi_2}$ *is a pro-p group.*

7 Combinatorial Automorphisms

The first goal of this section is to provide a general framework to study automorphisms of a group arising from a given presentation. We have seen an example of this for Gal_K, which we referred to as *Jannsen–Wingberg automorphism* in Section 3.2.2. Given a discrete group and some finite presentation of it, any automorphism of the free discrete group in the respective generators which fixes all relations induces an action on the group presentation. But as finding such automorphisms of the free group that fix all relations can be challenging, we use the fact that the group presentations that we are interested in are of a special kind. Namely, we can write the set of generators as a disjoint union $X \cup Y$ with $X = \{x_i\}_{i\in I}$ and $Y = \{y_j\}_{j\in J}$, such that all relations ρ are of the form $\rho = \rho_X \cdot \rho_Y$, where $\rho_X \in F_X$ and $\rho_Y \in F_Y$.

Any automorphism of the free group F_Y fixing all ρ_Y can be trivially extended to an automorphism on $F_{X\cup Y}$ (as the identity on F_X) and will automatically fix all relations ρ. We will refer to the map inducing such automorphisms on a group (presentation) as the *(discrete) combinatorial automorphism map* for a given set of relations. We note that these also induce an automorphism of any group isomorphic to a suitable completion of given presentation.

The second goal of this chapter is to use this approach to find large subgroups of automorphisms of the (outer) automorphism group of Demuškin groups, and the absolute Galois group Gal_K. We use the fact that a Demuškin group G, in a sense, is very similar to surface groups. This is reflected in its standard presentation, where the product of commutators appearing in the single defining relation comes from the symplectic structure of $H^1(G, \Lambda)$, as explained in Section 5.2.

Now let $S = S_g$ be a closed orientable surface of genus g. We choose the standard presentation of its fundamental group, i.e.

$$\pi_1(S_g) = \langle a_1, b_1, \dots, a_g, b_g | \delta = 1\rangle$$

with $\delta = [a_1, b_1] \dots [a_g, b_g]$. The outer automorphism group $\mathrm{Out}(\pi_1(S))$ can be identified with the extended mapping class group of S. The mapping class group $\mathrm{Mod}(S)$ is known to be finitely generated (even finitely presented). We consider the set of *Lickorish generators* of $\mathrm{Mod}(S)$, which are Dehn twists at finitely many simple closed curves on S. We show that we can lift these Dehn twists T_c to automorphisms of the free group in the generators $a_1, b_1, \dots, a_g, b_g$, which turn out to fix δ. Through the previously defined combinatorial automorphism map, with the correct choice of $S = S_g$, we are able to argue that these Dehn twists induce automorphism of Demuškin groups, and Gal_K. For the generators of this group, we can also argue that the induced maps are not inner automorphisms, and, in the case of Gal_K, do not come from geometric automorphisms. Using the "symplectic representation" for the (outer) automorphism groups of Demuškin groups established in Corollary 6.3.3, we then give another conceptual proof why the subgroup induced by these Dehn twists is large.

7.1 The combinatorial automorphism map

7.1.1 The discrete case

For a discrete free group F in $x_1, \dots, x_n$ and $S \subseteq F$ we define

$$\mathrm{Aut}^{(S)}(F) = \{\varphi\colon F \to F \text{ automorphism} \mid \varphi(\rho) = \rho \text{ for all } \rho \in S\}$$

to be the subgroup of $\mathrm{Aut}(F)$ fixing all $\rho \in S$. If $S = \{\rho\}$, we set $\mathrm{Aut}^{(\rho)}(F) = \mathrm{Aut}^{(\{\rho\})}(F)$.

Let $X = \{x_i\}_{i \in I}$ and $Y = \{y_j\}_{j \in J}$ denote disjoint sets of letters. Let $R \subseteq F_{X \cup Y}$ denote a system of relations. We shall assume that for all relations $\rho \in R$ we have $\rho = \rho_X \cdot \rho_Y$, where $\rho_X \in F_X$ and $\rho_Y \in F_Y$. Then $F_X *_{F_R} F_Y$ is defined as the pushout

$$\begin{tikzcd}
F_R \arrow[r, "\rho\mapsto\rho_X^{-1}"] \arrow[d, "\rho\mapsto\rho_Y"] & F_X \arrow[d] \\
F_Y \arrow[r] & F_X *_{F_R} F_Y.
\end{tikzcd}$$

Now assume we are given a group G_{discr} in the presentation

$$G_{\mathrm{discr}} = \langle X \cup Y | R \rangle = F_X *_{F_R} F_Y,$$

and set $S = \{\rho_Y | \rho \in R\}$.

We define a map as the following composition

$$\begin{aligned}
&\mathrm{Aut}^{(S)}(F_Y) \longrightarrow \mathrm{Aut}^{(S \cup X)}(F_X * F_Y) \longrightarrow \mathrm{Aut}^{(R)}(F_{X\cup Y}) \longrightarrow \mathrm{Aut}(G_{\mathrm{discr}}). \\
&\quad \varphi \longmapsto \mathrm{id}_X * \varphi
\end{aligned} \tag{7.1}$$

In other words, any automorphism of the free group F_Y in Y fixing the relations S can be extended to an automorphism of $F_{X \cup Y}$ as the identity on the generators in X, which will then by construction also fix all relations in R. Such an automorphism induces an automorphism of G_{discr} by the universal property of the cokernel.

Definition 7.1.1 (Discrete combinatorial automorphism map)**.** We denote the map defined in (7.1) by

$$\mathcal{K}^{(S)}_{\mathrm{discr}}\colon \mathrm{Aut}^{(S)}(F_Y) \to \mathrm{Aut}(G_{\mathrm{discr}})$$

and call it the *discrete combinatorial automorphism map* for a set of relations S.

7.1.2 The pro-$\mathcal{P}$ case

We want to discuss some conditions that we can impose on open normal subgroups of a (discrete) group G such that there is a well-defined notion of completion with respect to this property.

Given a group G, we say that a property $\mathcal{P}$ on the set of all open normal subgroups $N \subseteq G$ is a *cofiltered index system* if

(i) there exists at least one open normal subgroup N satisfying $\mathcal{P}$,

(ii) for all N_1, N_2 satisfying $\mathcal{P}$, there exists an open normal subgroup N_3 satisfying $\mathcal{P}$ such that

$$\begin{tikzcd}
& G/N_1 \\
G \arrow[ru] \arrow[r] \arrow[rd] & G/N_3 \arrow[u, dotted] \arrow[d, dotted] \\
& G/N_2.
\end{tikzcd}$$

We call $\mathcal{P}$ *saturated* if for any open normal subgroup N satisfying $\mathcal{P}$ it holds that any open normal subgroup M of G containing N also satisfies $\mathcal{P}$.

If $\mathcal{P}$ is a saturated cofiltered index system for G, we say that G is *$\mathcal{P}$-completable.* Indeed, in this case we have a well-defined notion of completion with respect to $\mathcal{P}$, which we shall denote by

$$G^{\wedge\mathcal{P}} := \lim_{N \text{ has } \mathcal{P}} G/N,$$

and call the *pro-$\mathcal{P}$-completion* of G. In particular, this is a profinite group.

Note that when $\mathcal{P}$ describes the set of open normal subgroups (such that G/N is a p-group), the notion of $\mathcal{P}$-completion agrees with the notion of profinite (resp. pro-p) completion.

We now define a subgroup of the groups of automorphisms of G that will allow us to give a definition of a pro-$\mathcal{P}$ combinatorial automorphism map. Namely, we set

$$\mathrm{Aut}^{(\mathcal{P})}(G) := \{\varphi \in \mathrm{Aut}(G) \,|\, \text{for all open normal subgroups } N \subseteq G : N \text{ has } \mathcal{P} \Leftrightarrow \varphi(N) \text{ has } \mathcal{P}\}\,.$$

Of course, any such automorphism of G will induce an automorphism of $G^{\wedge\mathcal{P}}$. Hence, there exists a map

$$\mathrm{Aut}^{(\mathcal{P})}(G) \to \mathrm{Aut}(G^{\wedge\mathcal{P}}),$$

which we will denote by $(-)^{\wedge\mathcal{P}}$ as it is induced by the pro-$\mathcal{P}$ completion.

Now we assume that $G = G_{\mathrm{discr}}$ is given via a discrete group presentation, using the same notation as in the previous section (which is the setting we will work with in the next sections). We furthermore assume there exists a map

$$\begin{tikzcd}
& \mathrm{Aut}^{(\mathcal{P})}(G) \arrow[d, hook] \\
\mathrm{Aut}^{(S)}(F_Y) \arrow[ru, dashed] \arrow[r, "\mathcal{K}^{(S)}_{\mathrm{discr}}"] & \mathrm{Aut}(G).
\end{tikzcd}$$

Then precomposing of the discrete combinatorial automorphism map yields

$$\mathrm{Aut}^{(S)}(F_Y) \xrightarrow{\mathcal{K}^{(S)}_{\mathrm{discr}}} \mathrm{Aut}^{(\mathcal{P})}(G) \xrightarrow{(-)^{\wedge\mathcal{P}}} \mathrm{Aut}(G^{\wedge\mathcal{P}}). \tag{7.2}$$

Definition 7.1.2 (Pro-$\mathcal{P}$ combinatorial automorphism map)**.** We denote the map defined in (7.2) by

$$\mathcal{K}^{(S)}_{\mathcal{P}} \colon \mathrm{Aut}^{(S)}(F_Y) \to \mathrm{Aut}(G^{\wedge\mathcal{P}})$$

and call it the *pro-$\mathcal{P}$ combinatorial automorphism map* for a set of relations S.

Let $\mathcal{P}$ describe the class of open normal subgroups (with p-power index in G). Then the map $\mathcal{K}^{(S)}_{\text{discr}}$ always factors through $\text{Aut}^{(\mathcal{P})}(G)$, i.e. the pro-$\mathcal{P}$ combinatorial automorphism map

$$\text{Aut}^{(S)}(F_Y) \to \text{Aut}^{(\mathcal{P})}(G) \to \text{Aut}(G^{\wedge\mathcal{P}})$$

is well-defined. In this case, we write $\mathcal{K}^{(S)}_{\mathcal{P}} = \mathcal{K}^{(S)}_{\text{profinite}}$ (and $\mathcal{K}^{(S)}_{\mathcal{P}} = \mathcal{K}^{(S)}_{\text{pro-}p}$, resp.) and simply refer to it as the profinite (resp. pro-p) combinatorial automorphism map.

The defining relation of the standard presentation of Demuškin groups, as well as the "wild relation" appearing in the work of Jannsen and Wingberg, contain a product of commutators of a subset of generators. In the next section we want to study automorphisms of the free group fixing this product of commutators, as these will induce automorphisms of the groups we are interested in. It turns out we know a large subgroup of this group of automorphisms through the geometry of surfaces, as it is related to the *mapping class group.* The next section is dedicated to reviewing some results on the mapping class group.

7.2 The mapping class group

The *mapping class group* $\text{Mod}(S) = \text{Mod}^+(S)$ of an oriented surface S is defined as the group of isotopy classes of orientation-preserving diffeomorphisms $S \to S$, and the *extended mapping class group* $\text{Mod}^{\pm}(S)$ is defined as the group of isotopy classes of all diffeomorphisms $S \to S$. These are central objects in the topology of surfaces, but also play a large role in the theory of Teichmüller spaces. Let $\pi_1(S)$ denote the fundamental group of S. Under the right assumption one may identify the extended mapping class group $\text{Mod}^{\pm}(S)$ with the group of outer automorphisms $\text{Out}(\pi_1(S))$.

The study of the mapping class group started with Dehn [Deh38] in the 1920s and Nielsen [Nie27], [Nie29], [Nie32], though they had rather different approaches. The work of Dehn adressed, for example, the question whether the mapping class group was finitely generated, while Nielsen studied the finer structure of certain elements of this group. In this chapter we state some fundamental results on the structure of the mapping class group in order to apply these results in the next chapter of this thesis. All material discussed is fairly classical, and we will mostly follow the standard references [FM11].

7.2.1 Basic results on surfaces

First, we recall some notions and results that are at the foundation of the theory of the mapping class group.

Theorem 7.2.1 (Classification of surfaces)**.** *Every connected, orientable surface which can be obtained from a compact surface after removing finitely many points is diffeomorphic to some $S_{g,n,b}$, the surface obtained by gluing $g \geq 0$ copies of the torus with the 2-sphere, and removing b open discs and n points.*

The compact surfaces $S_{g,0,b}$ are the ones without punctures and the closed surfaces $S_g = S_{g,0,0}$ are the ones with neither punctures nor boundary components. When we talk about surfaces throughout this chapter we will always assume them to be oriented, connected, and compact, unless stated otherwise. Recall that the genus may be defined as the maximal number of disjoint circles on the surfaces S which do not separate S. The genus and the number of boundary components is related by the Euler characteristic. Namely there is the well-known formula

$$\chi(S_{g,n,b}) = 2 - 2g - (b + n).$$

The standard proof of the above classification result is based on triangulations and cutting and pasting arguments. This provides a canonical model of S_g (and $S_{g,0,b}$): we can obtain it from a $4g$-gon after identifying sides (and removing b discs from the interior). This identification can be described by the word

$$\delta = [a_1, b_1] \dots [a_g, b_g]$$

and leads to the following group presentation in the case of punctured surfaces.

$$\pi_1(S_{g,0,n}) = \langle a_1, b_1, \dots, a_g, b_g, c_1, \dots, c_n | [a_1, b_1] \dots [a_g, b_g] c_1 \dots c_n = 1 \rangle \,. \tag{7.3}$$

When $n > 0$ one can eliminate one c_i and it follows that $\pi_1(S_{g,0,n})$ is a free group. These generators can be represented as embedded circles, and the (image of) the obvious loops representing $a_1, \dots, a_g, b_1, \dots, b_g$ are non-separating (i.e. the complement of S by the respective circle is connected).

By a *closed curve* in a surface S we mean a continuous map $S^1 \to S$, which we will usually identify with its image. Given an oriented closed curve $c \subseteq S$ we may identify it with an element of $\pi_1(S)$ by choosing a path from the base point to any point on c. We get an element of $\pi_1(S)$ which is well-defined up to conjugacy. In fact there is a bijective correspondence between nontrivial conjugacy classes in $\pi_1(S)$ and nontrivial free homotopy classes of oriented closed curves in S. Recall that an element g of a group G is called *primitive* if, whenever $g = h^k$ for some $h \in G$ and $k > 0$, it follows that $k = 1$ and $g = h$. We call a closed curve in S *primitive* if the corresponding class in $\pi_1(S)$ is primitive. A closed curve is *simple* if it is embedded, i.e. $S^1 \to S$ is injective. These curves are of interest as we may cut and twist along them. Furthermore, they represent primitive elements via the above correspondence. More precisely, given a non-nullhomotopic simple closed curve c in S, each element of the conjugacy class in $\pi_1(S)$ is primitive.

Furthermore, we recall that two simple closed curves α, β are *isotopic* if there is a homotopy $H \colon S^1 \times [0, 1] \to S$ from α to β such that the closed curve $H^1(S^1 \times \{t\})$ is simple for all $t \in [0, 1]$. A result due to Baer (see [FM11, Prop. 1.10] for a proof) states that two essential simple closed curves in S are isotopic if and only if they are homotopic. Furthermore, there are some useful facts on surface topology to pass between different description of the mapping class group, which we shall cite below. See [FM11, §1.4] for details.

Theorem 7.2.2. *Let S be a compact surface.*

(i) Two orientation-preserving homeomorphisms of S are homotopic if and only if they are isotopic.

(ii) Every homeomorphism of S is isotopic to a diffeomorphism of S.

(iii) If S is not homeomorphic to $S^2, \mathbb{R}^2, D^2, T^2$, or the closed annulus, then $\mathrm{Homeo}_0(S)$ *is contractible. In particular, it is simply connected.*

7.2.2 Generators of the mapping class group

Definition of the mapping class group and symplectic representation

Let $\mathrm{Homeo}^+(S, \partial S)$ denote the group of orientation-preserving homeomorphisms that fix the boundary componentwise and let $\mathrm{Homeo}_0(S, \partial S)$ denote the connected component of the identity in this group. We furthermore denote by $\mathrm{Diff}^+(S, \partial S)$ the group of orientation-preserving diffeomorphisms that are the identity on the boundary, on which we may define an equivalence relation as smooth isotopy (or homotopy) relative to the boundary. The above results enable us to give the following equivalent definitions of the mapping class group

$$\begin{aligned}\mathrm{Mod}(S) &= \pi_0(\mathrm{Homeo}^+(S, \partial S))\\ &= \mathrm{Homeo}^+(S, \partial S)/\mathrm{Homeo}_0(S, \partial S)\\ &\cong \mathrm{Homeo}^+(S, \partial S)/\text{homotopy}\\ &\cong \pi_0(\mathrm{Diff}^+(S, \partial S))\\ &\cong \mathrm{Diff}^+(S, \partial S)/\sim .\end{aligned}$$

Now assume $S = S_g$. The action of a diffeomorphism f on the homology of S is well-defined on the level of isotopy, giving rise to the *symplectic representation*

$$\Psi\colon\ \mathrm{Mod}(S) \to \mathrm{Aut}(H_1(S, \mathbb{Z})) \cong \mathrm{Aut}(H^1(S, \mathbb{Z}))$$

of S, which can be understood as a sort of linear approximation to $\mathrm{Mod}(S_g)$. Intersection product (resp. cup product) make $H_1(S, \mathbb{Z})$ (resp. $H^1(S, \mathbb{Z})$) into a symplectic space, and the symplectic structure is preserved by maps induced from orientation-preserving diffeomorphisms (even homeomorphisms). Therefore the image of Ψ lies in $\mathrm{Sp}_{2g}(\mathbb{Z})$. We shall briefly recall how this symplectic structure is definded.

Let α, β be a pair of transverse, oriented, simple closed curves in S. The *algebraic intersection number* $\hat{i}(\alpha, \beta)$ is defined as the sum of the indices of intersection points of the curves α and β, where we give an intersection point the index $+1$ whenever the orientation of α and β agrees, and -1 otherwise. Note that orientation-preserving homeomorphisms preserve algebraic intersection numbers. In fact, the algebraic intersection number only depends on the homology classes a and b of α and β. We get a bilinear form of $\mathbb{Z}$-modules

$$H_1(S, \mathbb{Z}) \times H_1(S, \mathbb{Z}) \to \mathbb{Z},$$

which is symplectic. Furthermore, we note that via the duality of cohomology and homology, this corresponds to the cup-product

$$- \cup -\colon H^1(S, \mathbb{Z}) \times H^1(S, \mathbb{Z}) \to H^2(S, \mathbb{Z}) = \mathbb{Z}.$$

As the discussion in the previous chapters might suggest, this point of view will be preferred for most parts of later discussion.

Recall that we can choose a collection of oriented simple closed curves $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ such that the corresponding cohomology classes $a_1, b_1, \ldots, a_g, b_g$ form a symplectic basis for $H^1(S, \mathbb{Z})$ and the symplectic form given by $- \cup -$. There is a choice of basis yielding generators of $\pi_1(S)$, which we shall also denote by $a_1, b_1, \ldots, a_g, b_g$, such that

$$\pi_1(S) = \langle a_1, \ldots, a_g, b_1, \ldots, b_g | [a_1, b_1] \ldots [a_g, b_g] = 1 \rangle .$$

Example 7.2.3. We consider the torus T^2. Nontrivial free homotopy classes of oriented simple closed curves in T^2 correspond to primitive elements of $\mathbb{Z}^2$. We denote such an object as (p,q). Now $H_1(T^2,\mathbb{Z})$ is a free $\mathbb{Z}$-module in the basis e_1,e_2. As the intersection number is bilinear, we have

$$\hat{i}(pe_1+qe_2,p'e_1+q'e_2)=(pq'-p'q)\hat{i}(e_1,e_2)=(pq'-p'q).$$

We now give the easiest examples of the mapping class group (that is relevant to us): the mapping class group of the torus, and the once-punctured torus. In particular, studying this group is instructive for the higher genus cases. This was proven by Nielsen in his PhD thesis in 1913.

Proposition 7.2.4. *Let T^2 denote the torus and let $S_{1,1}$ denote the once-punctured torus.*

(i) The homomorphism $\Psi\colon \mathrm{Mod}(T^2)\to \mathrm{SL}_2(\mathbb{Z})$ given by the action on $H_1(T^2,\mathbb{Z})\cong\mathbb{Z}^2$ is an isomorphism.

(ii) The homomorphism $\Psi\colon \mathrm{Mod}(S_{1,1})\to \mathrm{SL}_2(\mathbb{Z})$ given by the action on $H_1(S_{1,1},\mathbb{Z})\cong\mathbb{Z}^2$ is an isomorphism.

Proof. (i): Any homeomorphism ϕ of the torus T^2 induces an automorphism ϕ_* of $H_1(T^2,\mathbb{Z})$. We may identify $H_1(T^2,\mathbb{Z})$ with $\mathbb{Z}^2$. As homotopic maps induce the same map on homology, $\phi\mapsto\phi_*$ induces a map $\psi\colon \mathrm{Mod}(T^2)\to\mathrm{Aut}(\mathbb{Z}^2)\cong\mathrm{GL}_2(\mathbb{Z})$. Now the image of ψ lies in$\mathrm{SL}_2(\mathbb{Z})$, since the algebraic intersection number is given as a determinant (as seen in the previous example). For surjectivity, let M be an element of $\mathrm{SL}_2(\mathbb{Z})$. Then M induces an orientation-preserving linear homeomorphism of $\mathbb{R}^2$ leaving $\mathbb{Z}^2$ invariant, inducing a linear homeomorphism ϕ_M of the torus $T^2=\mathbb{R}^2/\mathbb{Z}^2$ such that the respective homotopy class $[\phi_M]$ is mapped to M by σ. For injectivity, note that homotopy classes of based maps $T^2\to T^2$ correspond to homomorphisms $\mathbb{Z}^2\to\mathbb{Z}^2$ (as T^2 is a $K(G,1)$-space). In particular, any mapping class f of T^2 admits a representative ϕ fixing the base point of T^2. The condition to lie in the kernel of σ means that ϕ as a based map must be homotopic to the identity. The rest follows by Theorem 7.2.2 (i).

(ii): We note that $H_1(S_{1,1},\mathbb{Z})=H_1(T^2,\mathbb{Z})\cong\mathbb{Z}^2$. In the same way as before we get a map $\psi\colon\mathrm{Mod}(S_{1,1})\to\mathrm{SL}_2(\mathbb{Z})$. The surjectivity follows as any $M\in\mathrm{SL}_2(\mathbb{Z})$ can be realized as a map of $\mathbb{R}^2$ equivariant with respect to $\mathbb{Z}^2$ fixing the origin, and such a map descends to a homeomorphism of $S_{1,1}$. For injectivity we take two closed simple curves α,β intersecting in one point. We consider a mapping class in $S_{1,1}$ in the kernel of ψ which shall be represented by an element ϕ. Then $\phi(\alpha)$ and $\phi(\beta)$ are isotopic to α and β respectively, and we can modify ϕ such that it fixes α and β pointwise. Cutting $S_{1,1}$ along $\alpha\cup\beta$ yields a once-punctured disk, and ϕ induces a homeomorphism of this disk fixing the boundary, which is homotopic to the identity (Alexander trick). □

Now any orientation-preserving homeomorphism f induces an automorphism $f_*\colon H^1(S,\mathbb{Z})\to H^1(S,\mathbb{Z})$, and any two homotopic homeomorphism induce the same map. Hence, we get a representation

$$\psi_0\colon \mathrm{Mod}(S)\to\mathrm{Aut}(H^1(S,\mathbb{Z}))\cong\mathrm{GL}_{2g}(\mathbb{Z}),$$

where the isomorphism on the right requires a choice of basis. The image lies $\mathrm{Sp}_{2g}(\mathbb{Z})$, and hence we regard this as a representation

$$\psi\colon \mathrm{Mod}(S)\to\mathrm{Sp}_{2g}(\mathbb{Z}),$$

which we call the *symplectic representation* of $\mathrm{Mod}(S)$. We have the following result:

Theorem 7.2.5. *Let $S = S_g$ or $S_{g,1}$ for $g \geq 1$. The symplectic representation*

$$\psi\colon \mathrm{Mod}(S) \to \mathrm{Sp}_{2g}(\mathbb{Z})$$

is surjective.

Proof. See [FM11, §6.3] for three different proofs. □

Let $S = S_g$ or $S_{g,1}$ for $g \geq 1$. We call the kernel of the symplectic representation, i.e. the subgroup of elements of $\mathrm{Mod}(S)$ that act trivially on $H^1(S, \mathbb{Z})$, *Torelli subgroup* of $\mathrm{Mod}(S)$ and shall denote it by $\mathcal{I}(S)$. It is known that $\mathcal{I}(S)$ is torsion free, see [FM11, Thm. 6.12]. Dehn twists about separating simple closed curves yield examples of elements of $\mathcal{I}(S)$.

Dehn twists

There are special kinds of elements of the mapping class group, introduced by Max Dehn (originally as "Schraubungen"), called *Dehn twists*, which we shall introduce here.

Let $A = S^1 \times [0,1]$ denote the annulus, which we give an orientation by embedding it in the (θ, r)-plane (with standard orientation) via the map $(\theta, t) \mapsto (\theta, t+1)$. We define the (left) twist map $T\colon A \to A$ via the formula $T(\theta, t) = (\theta + 2\pi t, t)$, which is orientation-preserving fixing the boundary of A point-wise.

Now let S be an oriented surface and α a simple closed curve in S. Let N be a regular neighbourhood of α. Choosing an orientation-preserving homeomorphism $\varphi\colon A \to N$, we define the *Dehn twist about* α as

$$T_\alpha\colon S \to S, \quad x \mapsto \begin{cases} \varphi \circ T \circ \varphi^{-1}(x) & \text{if } x \in N, \\ x & \text{otherwise.} \end{cases}$$

This involves a choice of N and φ, but only depends on it up to isotopy. Furthermore, T_α only depends on α up to isotopy. Hence if a denotes the isotopy class of α, we get a well-defined element of $\mathrm{Mod}(S)$, which we shall denote by T_a, called the *Dehn twist about a*. Furthermore, the following holds.

Proposition 7.2.6. *Let S be a an oriented surface, and let a denote the isotopy class of a simple closed curve α in S. If α is not homotopic to a point or a puncture in S, then T_a is a non-trivial element of* $\mathrm{Mod}(S)$ *of infinite order.*

Proof. See [FM11, Prop. 3.1-2] □

Example 7.2.7 (Dehn twists on T^2)**.** In Theorem 6.3.2 we gave an isomorphism

$$\psi\colon \mathrm{Mod}(T^2) \to \mathrm{SL}_2(\mathbb{Z}).$$

The elements of $\mathrm{Mod}(T^2)$ given by Dehn twists around the $(1,0)$-curve and the $(0,1)$-curve are mapped to the matrices

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

which are generators of $\mathrm{SL}_2(\mathbb{Z})$. Hence, $\mathrm{Mod}(T^2)$ is generated by these Dehn twists.

In fact, the previous observation generalizes to $\mathrm{Mod}(S_g)$, which we shall state in Theorem 7.2.8.

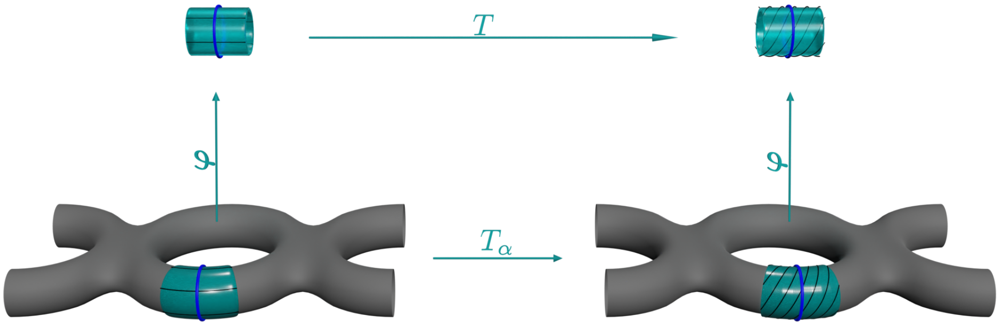

Figure 7.1: Dehn twist along a closed simple curve. Image by Yanik Kleibrink.

Finite generation of $\mathrm{Mod}(S)$

In this section, we state another crucial structure theorem about the mapping class group. Namely, it is generated by a finite number of Dehn twists. This goes back to Dehn [Deh38] in the 1920's, and was independently proved by Lickorish [Lic64] for a set of $3g-1$ curves as depicted below. In 1979 Humphries [Hum79] showed for $g \geq 2$ that $2g+1$ curves suffice, which is in fact a minimal set of generators.

Theorem 7.2.8 (Dehn–Lickorisch–Humphries)**.** *Let $S = S_g$ with $g \geq 0$. The group* $\mathrm{Mod}^+(S)$ *is generated by Dehn twists along nonseparating curves.*

Assuming $g \geq 1$, a finite set of generators is given by the Dehn twists along the curves $a_1, \dots, a_g$, $m_1, \dots, m_g$ and $c_1, \dots, c_{g-1}$ as pictured in Figure 7.2. In fact, we can choose a minimal set of generators from these elements. Namely, for $g \geq 2$ it suffices to consider the Dehn twists along $a_1, \dots, a_g, c_1, \dots, c_{g-1}$ and m_1, m_2.

Proof. For proofs of these claims, we refer to [FM11, §4.4]. □

Note that for $g = 1$, i.e. when $S = T$ is the 2-dimensional torus, a set of generators of $\mathrm{Mod}(T)$ is given by Dehn twists along the curves a_1 and m_1.

Also note that for the once-punctured surface $S_{g,1}$ the above result on the finite set of Dehn twist generators still holds. However for a surface $S_{g,n}$ with $n \geq 2$ punctures the statement is no longer true, but can be replaced by a statement on the so-called *pure mapping class group* $\mathrm{PMod}(S_{g,n})$, which is the subgroup of $\mathrm{Mod}(S_{g,n})$ of elements fixing each puncture.

In fact, the mapping class group of a compact closed surface $S = S_g$ is even finitely presented. The standard presentation in terms of Humphries generators is given by Wajnryb [Waj83]. See also [FM11, §5.2].

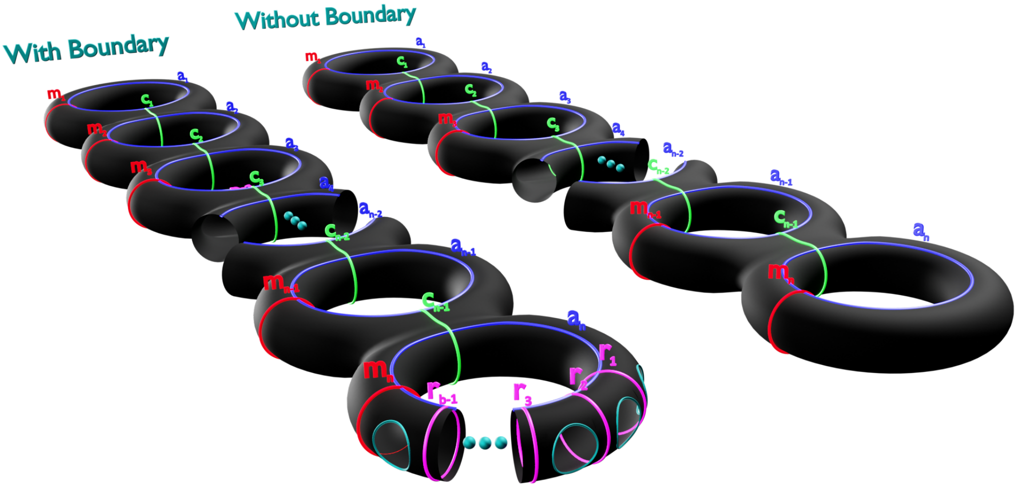

Figure 7.2: Simple closed curves corresponding to Lickorish generators of $\mathrm{Mod}(S)$. We will only consider the case where S has no boundary. Image by Yanik Kleibrink.

7.2.3 Birman exact sequence

Now let S be any surface. For us it suffices to consider $S = S_g$ with $g \geq 2$, or more generally S with $\chi(S) < 0$. Let $P \in S$ be a point of S and let $S^* = S \setminus P$ denote the once-punctured surface. So we have an inclusion $S^* \to S$. This induces the forgetful map on the mapping class groups

$$\mathrm{Mod}(S^*) \xrightarrow{\text{forget}} \mathrm{Mod}(S),$$

which is surjective. One may explicitly describe the kernel of this map, which is the content of the following theorem.

Theorem 7.2.9 (Birman exact sequence)**.** *In the above setting the following sequence is exact*

$$1 \to \pi_1(S, P) \to \mathrm{Mod}(S^*) \to \mathrm{Mod}(S) \to 1. \tag{7.4}$$

Furthermore, this sequence does not split.

Proof. See [FM11, Thm. 4.6, Cor. 5.11]. □

Furthermore, we note that when $g = 1$, i.e. $S = T$ is the torus, the Birman exact sequence becomes an isomorphism

$$\mathrm{Mod}(T^*) \xrightarrow{\cong} \mathrm{Mod}(T).$$

See [Bir69, Cor. 1.3].

7.2.4 The extended mapping class group

The *extended mapping class group* $\operatorname{Mod}^{\pm}(S)$ is the group of isotopy classes of homeomorphisms of S and contains the mapping class group $\operatorname{Mod}(S)$ as a subgroup of index 2. We have a short exact sequence

$$1 \to \operatorname{Mod}(S) \to \operatorname{Mod}^{\pm}(S) \to \mathbb{Z}/2\mathbb{Z} \to 1$$

where the right-hand map records the whether an element of $\operatorname{Mod}^{\pm}(S)$ is orientation-preserving. This sequence splits as there always exists an element of order 2 that reverses orientation.

We now want to give a purely algebraic description of the mapping class group. We will use this description to apply results on the mapping class group to questions on the outer automorphism groups of other groups.

Let f be a homeomorphism of S. This defines an isomorphism $f_*\colon \pi_1(S) \to \pi_1(S)$, which only depends on the homotopy type of f and is well-defined only up to inner automorphisms as we do not assume f_* to preserve the base point. Hence, we have a well-defined map

$$\operatorname{Mod}^{\pm}(S) \to \operatorname{Out}(\pi_1(S)).$$

Theorem 7.2.10 (Dehn–Nielsen–Baer Theorem). *Let S be a closed surface of genus $g \geq 1$. Then the extended mapping class group $\operatorname{Mod}^{\pm}(S)$ is isomorphic to the outer automorphism group $\operatorname{Out}(\pi_1(S))$ of the fundamental group $\pi_1(S)$.*

Proof. Several proofs can be found in [FM11, §8]. □

We may complement this theorem by stating what subgroup of $\operatorname{Out}(\pi_1(S))$ corresponds to the mapping class group $\operatorname{Mod}(S)$. In the above setting we have

$$H^2(\pi_1(S), \mathbb{Z}) = H^2(S, \mathbb{Z}) = \mathbb{Z},$$

on which $\operatorname{Out}(\pi_1(S))$ acts naturally as inner automorphisms act trivially on cohomology groups. An element of $\operatorname{Mod}^{\pm}(S)$ is orientation-perserving, i.e. an element of $\operatorname{Mod}(S)$, if and only if the induced action on $H^2(S, \mathbb{Z})$ is trivial. Let $\operatorname{Out}^{+}(\pi_1(S))$ denote the subgroup of $\operatorname{Out}(\pi_1(S))$ consisting of elements acting trivially on $H^2(S, \mathbb{Z})$. Clearly, $\operatorname{Mod}(S)$ maps into $\operatorname{Out}^{+}(\pi_1(S))$. In fact, the following holds.

Theorem 7.2.11. *Let $S = S_g$ be a closed surface of of genus $g \geq 1$. The natural homomorphism $\operatorname{Mod}(S) \to \operatorname{Out}^{+}(\pi_1(S))$ is an isomorphism.*

Example 7.2.12. We can reprove the result on the mapping class group of the torus T^2. As $\pi_1(T^2) \cong \mathbb{Z}^2$ is abelian, we have

$$\operatorname{Mod}^{\pm}(T^2) \cong \operatorname{Out}(\pi_1(T^2)) = \operatorname{Aut}(\pi_1(T^2)) \cong \operatorname{Aut}(\mathbb{Z}^2) = \operatorname{GL}_2(\mathbb{Z}).$$

In particular, the subgroup $\operatorname{Mod}(T^2)$ is isomorphic to $\operatorname{SL}_2(\mathbb{Z})$.

7.3 Combinatorial Dehn twists

We consider a closed surface $S = S_g$ with $g \geq 1$. Then for a point $P \in S$, we denote by S^* the punctured surface. For $g = 1$ we have an isomorphism

$$\mathrm{Mod}(S^*) \xrightarrow{\cong} \mathrm{Mod}(S)$$

and for $g \geq 2$ we have the Birman exact sequence

$$1 \to \pi_1(S, P) \to \mathrm{Mod}(S^*) \to \mathrm{Mod}(S) \to 1,$$

see (7.4). We may identify $\mathrm{Mod}(S^*)$ with a subgroup of $\mathrm{Out}(\pi_1(S \setminus P))$, namely

$$\mathrm{Out}^*(\pi_1(S \setminus P)) \coloneqq \mathrm{Aut}^*(\pi_1(S \setminus P))/\pi_1(S \setminus P),$$

where by $\mathrm{Aut}^*(\pi_1(S \setminus P))$ we denote the automorphism of $\pi_1(S \setminus P)$ fixing the inertia group of P. In fact, we shall give a more explicit description of this group. We choose the standard presentations of $\pi_1(S)$ and $\pi_1(S \setminus P)$ as in (7.3), i.e. we have

$$\pi_1(S) = \langle a_1, b_1, \ldots, a_g, b_g, |[a_1, b_1] \ldots [a_g, b_g] = 1\rangle$$

and

$$\pi_1(S \setminus P) = \langle a_1, b_1, \ldots, a_g, b_g, c|[a_1, b_1] \ldots [a_g, b_g]c = 1\rangle .$$

Setting $\delta = [a_1, b_1] \ldots [a_g, b_g]$, we have $c = \delta^{-1}$, hence $\pi_1(S \setminus P)$ is a free group in the generators $a_1, b_1, \ldots, a_g, b_g$, which we shall denote by F from now on. An element f of $\mathrm{Aut}^*(F)$ is therefore an automorphism of F such that $f(\delta)$ is conjugate to δ. Using the notation introduced in Section 7.1, we can view $\mathrm{Aut}^{(\delta)}(F)$ as a subgroup of $\mathrm{Aut}^*(F)$.

Proposition 7.3.1. *There is a central short exact sequence*

$$1 \to \langle\delta\rangle \to \mathrm{Aut}^{(\delta)}(F) \to \mathrm{Mod}(S^*) \to 1.$$

Proof. The surjectivity of $\mathrm{Aut}^{(\delta)}(F) \to \mathrm{Mod}(S^*)$ follows from the fact that $\mathrm{Aut}^*(F) \to \mathrm{Mod}(S^*)$ is surjective and any automorphism such that the image of δ is a conjugate of δ can be modified to be an automorphism fixing δ by composition with an inner automorphism. The kernel of the map are precisely the elements of the centralizer of δ in F. The following two lemmas finish the proof. □

Lemma 7.3.2. *The element δ is primitive in F.*

Proof. Assume δ is not primitive, i.e. $\delta = (\delta')^k$ for some $\delta' \in F$ and $k > 1$. The claim follows after comparison on the descending central series of F, because δ is primitive in $\mathrm{gr}^2 F$. □

Lemma 7.3.3. *Let F be a discrete free group, and $0 \neq \gamma \in F$. Then the centralizer of γ in F is a cyclic group containing the subgroup generated by γ. In particular, if γ is primitive, we have $Z_F(\gamma) = \langle\gamma\rangle$.*

Proof. Assume $Z_F(\gamma)$ is not cyclic. Then it must contain a non-cyclic abelian subgroup A. As F has cohomological dimension 1, it follows that F is torsion-free. But then $A \cong \mathbb{Z}^2$ and hence of cohomological dimension 2, which is a contradiction. □

Hence, the kernel of the composition map

$$\mathrm{Aut}^{(\delta)}(F) \to \mathrm{Mod}(S^*) \to \mathrm{Mod}(S)$$

is the maximal quotient of F in which δ is central. Furthermore, there exists a surjective group homomorphism, the symplectic representation of $\mathrm{Mod}(S)$,

$$\psi\colon\ \mathrm{Mod}(S) \to \mathrm{Sp}(H^1(S,\mathbb{Z})) \cong \mathrm{Sp}_{2g}(\mathbb{Z}).$$

We now consider the action of Dehn twists

$$T_{a_1}, \dots, T_{a_g}, T_{m_1}, \dots, T_{m_g}, T_{c_1}, \dots, T_{c_{g-1}}$$

in $\mathrm{Mod}(S)$ described in Theorem 7.2.8, where for $g = 1$ we just consider the Dehn twists T_{a_1}, T_{m_1}, and write down an explicit formula for the action on the generators $a_1, \dots, a_g, b_1, \dots, b_g$ as done in [Mor93]. Given a Dehn twist T_c, we denote this action by τ_c.

Lemma 7.3.4. *The Dehn twists $T_{a_1}, \dots, T_{a_g}, T_{m_1}, \dots, T_{m_g}, T_{n_1}, \dots, T_{n_{g-1}}$ from Theorem 7.2.8 and their inverses act on $a_1, b_1, \dots, a_g, b_g$ as follows. The effect on the other generators not explicitly mentioned is the identity.*

(i) For all $i = 1, \dots, g$ we have

$$\tau_{a_i}\colon F \to F, \quad b_i \mapsto b_i a_i$$

and

$$\tau_{a_i}^{-1}\colon F \to F, \quad b_i \mapsto b_i a_i^{-1}.$$

(ii) For all $i = 1, \dots, g$ we have

$$\tau_{m_i}\colon F \to F, \quad a_i \mapsto a_i b_i^{-1}$$

and

$$\tau_{m_i}^{-1}\colon F \to F, \quad a_i \mapsto a_i b_i.$$

(iii) In the case $g \geq 2$, for all $i = 1, \dots, g-1$ we have

$$\begin{aligned} \tau_{c_i}\colon F &\to F \\ a_i &\mapsto a_i b_i^{-1} a_{i+1} b_{i+1} a_{i+1}^{-1} \\ b_i &\mapsto a_{i+1} b_{i+1}^{-1} a_{i+1}^{-1} b_i a_{i+1} b_{i+1} a_{i+1}^{-1} \\ a_{i+1} &\mapsto a_{i+1} b_{i+1}^{-1} a_{i+1}^{-1} b_i a_{i+1} \end{aligned}$$

and

$$\begin{aligned} \tau_{c_i}^{-1}\colon F &\to F \\ a_i &\mapsto a_i a_{i+1} b_{i+1}^{-1} a_{i+1}^{-1} b_i \\ b_i &\mapsto b_i^{-1} a_{i+1} b_{i+1} a_{i+1}^{-1} b_i a_{i+1} b_{i+1}^{-1} a_{i+1}^{-1} b_i \\ a_{i+1} &\mapsto b_i^{-1} a_{i+1} b_{i+1}. \end{aligned}$$

Furthermore, we note the following.

Lemma 7.3.5. *The maps given in Lemma 7.3.4 generate a subgroup of* $\mathrm{Aut}^{(\delta)}(F)$*.*

Definition 7.3.6. We call the subgroup of $\mathrm{Aut}^{(\delta)}(F)$ given in Lemma 7.3.5 *group of combinatorial Dehn twists on* F, and denote this group by $\mathrm{Dehn}(S)$.

We note that the set of generators of $\mathrm{Dehn}(S)$ are lifts of Lickorish generators of $\mathrm{Mod}(S)$. Hence, we have a surjective map

$$\mathrm{Dehn}(S) \twoheadrightarrow \mathrm{Sp}(H^1(S,\mathbb{Z})) \cong \mathrm{Sp}_{2g}(\mathbb{Z}),$$

which is an isomorphism for $g = 1$.

7.4 Combinatorial automorphisms of Demuškin groups

Now let $p \neq 2$ be a prime and let G be a (p-)Demuškin group of rank n with invariant q. For this discussion we shall first assume that $q \neq 0$. Set $\Lambda = \Lambda(G) = \mathbb{Z}_p/q\mathbb{Z}_p$. We assume $n \geq 4$, and choose a surface $S = S_g$ such that $2g = n-2$. Note that by assumption on n we have $g \geq 1$. In Section 6.3 we showed that there is a surjective map

$$\mathrm{Out}(G) \to \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda)).$$

After choosing generators $y_1, y_2, \ldots, y_n$ of G as in Theorem 5.2.8, Proposition 6.1.5 gave an explicit description of $\mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda))$ as a subgroup Λ-valued points of the maximal parabolic subgroup of $\underline{\mathrm{GSp}}(H^1(G,\Lambda))$ corresponding to the isotropic subspace $\ker\beta^{\perp}$. In particular, denoting the dual basis of $y_1, y_2, \ldots, y_n$ by $\chi_1, \ldots, \chi_n$, the images of the elements $\chi_3, \ldots, \chi_n$ generate the symplectic space $\ker\beta/\ker\beta^{\perp}$. We have the following diagram

$$\begin{tikzcd}
\mathrm{Out}(G) \arrow[rr, two heads] \arrow[d, two heads, "\pi_2"] & & \underline{\mathrm{GSp}}(\ker\beta/\ker\beta^{\perp})(\Lambda) \arrow[r, equal, "\sim"] & \mathrm{GSp}_{n-2}(\Lambda) \\
\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \arrow[r, equal] & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda)) \arrow[r, hook] \arrow[ur, two heads] & P_{\ker\beta^{\perp}}(H^1(G,\Lambda))(\Lambda), \arrow[u, two heads] &
\end{tikzcd}$$

where the surjections come from Corollary 6.1.6 and the top vertical arrow is defined as a composition. Let G_{discr} denote the corresponding discrete group given by generators $y_1, \ldots, y_n$ satisfying the relation $y_1^q[y_1,y_2]\ldots[y_{n-1},y_n]$. Now in the previous discussion, the choice of presentation of $\pi_1(S)$ with generators $a_1, b_1, \ldots, a_g, b_g$ corresponds to the choice of a symplectic $\mathbb{Z}$-basis of $H^1(S,\mathbb{Z})$, which we shall denote by $a_1, b_1, \ldots, a_g, b_g$. Considering the (discrete) free group F in the generators $a_1, b_1, \ldots, a_g, b_g$, we get a map $F \to G_{\mathrm{discr}}$ by mapping

$$a_1 \mapsto y_3, b_1 \mapsto y_4, \ldots, a_g \mapsto y_{n-1}, b_g \mapsto y_n.$$

This induces a group homomorphism on the abelianizations $\pi_1(S)^{\mathrm{ab}} \to G^{\mathrm{ab}}$. Furthermore, $H^1(S,\mathbb{Z}) \otimes \Lambda = H^1(S,\Lambda)$ and $H^1(G,\Lambda)$ are dual to $\pi_1(S)^{\mathrm{ab}} \otimes \Lambda$ and $G^{\mathrm{ab}} \otimes \Lambda$, respectively.

In particular, this induces a map

$$\begin{tikzcd}
\mathrm{Sp}(H^1(S,\mathbb{Z})) \arrow[r] \arrow[d, equal] & \underline{\mathrm{Sp}}(\ker\beta/\ker\beta^{\perp})(\Lambda) \arrow[d, equal] \\
\mathrm{Sp}_{2g}(\mathbb{Z}) \arrow[r, "-\otimes\Lambda"] & \mathrm{Sp}_{n-2}(\Lambda).
\end{tikzcd}$$

Finally, we consider the pro-p combinatorial automorphism map for the relation δ given by

$$\widehat{\mathcal{K}} := \mathcal{K}^{(\delta)}_{\text{pro-}p}\colon\ \mathrm{Aut}^{(\delta)}(F) \to \mathrm{Out}(G).$$

Note that this map is not trivial. First of all, we note that the images of combinatorial Dehn twists $\mathrm{Dehn}(S)$ induce automorphisms of G which can be explicitly written down in terms of the choice of generators $y_1, \dots, y_n$. It suffices to find such an element, which is non-trivial on $G^{\mathrm{ab}} \otimes \Lambda$. Take, e.g. the element τ_{a_g} in $\mathrm{Mod}(S)$. This induces the automorphism

$$G \to G, \quad y_n \mapsto y_n \cdot y_{n-1}.$$

Note that this is essentially a pro-p analogue of the Jannsen–Wingberg automorphism that we have previously discussed. Taking the dual of this yields an element of $\mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda))$ of the form

$$\begin{pmatrix} 1 &&&&& \\ & 1 &&&& \\ && \ddots &&& \\ &&& 1 & 1 & \\ &&& 0 & 1 & \\ &&&&& 1 \end{pmatrix}.$$

Hence, the above automorphism is not an inner automorphism. So in particular, $\widehat{\mathcal{K}}$ is not trivial.

We may now sum up the previous discussion as follows:

Theorem 7.4.1. *The following diagram*

$$\begin{tikzcd}
\mathrm{Out}(G) \arrow[rr, two heads, "\overline{\pi_2}"] & & \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \arrow[r, equal] & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{GSp}_n(\Lambda) \\
 & & & \underline{\mathrm{GSp}}(\ker\beta/\ker\beta^{\perp})(\Lambda) \arrow[r, equal] & \mathrm{GSp}_{n-2}(\Lambda) \\
 & & & \underline{\mathrm{Sp}}(\ker\beta/\ker\beta^{\perp})(\Lambda) \arrow[r, equal] \arrow[u, hook] & \mathrm{Sp}_{n-2}(\Lambda) \arrow[u, hook] \\
\mathrm{Aut}^{(\delta)}(F) \arrow[r, two heads] \arrow[uuu, "\widehat{\mathcal{K}}"] & \mathrm{Mod}(S^*) \arrow[r, two heads] & \mathrm{Mod}(S) \arrow[r, two heads] & \mathrm{Sp}(H^1(S,\mathbb{Z})) \arrow[r, equal] \arrow[u, two heads] & \mathrm{Sp}_{n-2}(\mathbb{Z}) \arrow[u, two heads, "-\otimes\Lambda"]
\end{tikzcd}$$

commutes.

In particular, we have now found a “large” subgroup of $\mathrm{Out}(G)$.

Theorem 7.4.2. *The subgroup* $\widehat{\mathcal{K}}(\mathrm{Dehn}(S))$ *in* $\mathrm{Out}(G)$ *has dense image in* $\mathrm{Sp}_{n-2}(\mathbb{Z}_p)$.

Proof. Consider the previous diagram

$$\begin{tikzcd}
\mathrm{Out}(G) \arrow[rrr, two heads, "\overline{\pi_2}"] & & & \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \arrow[r, equal] & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(G,\Lambda))(\Lambda) \arrow[d, two heads] \\
& & & & \mathrm{GSp}_{n-2}(\Lambda) \\
& \widehat{\mathcal{K}}(\mathrm{Dehn}(S)) \arrow[ul, hook] \arrow[r, dashed] & \mathrm{Sp}_{n-2}(\mathbb{Z}_p) \arrow[rr, two heads] & & \mathrm{Sp}_{n-2}(\Lambda) \arrow[u, hook] \\
\mathrm{Dehn}(S) \arrow[uuu, "\widehat{\mathcal{K}}"] \arrow[ur, two heads] \arrow[r, two heads] & \mathrm{Mod}(S^*) \arrow[r, two heads] & \mathrm{Mod}(S) \arrow[rr, two heads] & & \mathrm{Sp}_{n-2}(\mathbb{Z}). \arrow[u, two heads, "-\otimes\Lambda"] \arrow[ull, hook]
\end{tikzcd}$$

First, we note that $\mathrm{Dehn}(S)$ maps surjectively onto $\mathrm{Sp}(H^1(S,\mathbb{Z})) \cong \mathrm{Sp}_{n-2}(\mathbb{Z})$ and this is a dense subgroup of $\mathrm{Sp}_{n-2}(\mathbb{Z}_p)$, since for all n the reduction maps $\mathrm{Sp}_{n-2}(\mathbb{Z}) \to \mathrm{Sp}_{n-2}(\mathbb{Z}/n\mathbb{Z})$ are surjective, see [NS64]. Then the claim follows from the previous theorem after arguing that here is a well-defined map

$$\widehat{\mathcal{K}}(\mathrm{Dehn}(S)) \to \mathrm{Sp}_{n-2}(\mathbb{Z}_p).$$

Note that we have

$$\mathrm{Sp}(H^1(S,\mathbb{Z}_p)) \subseteq \mathrm{GL}(H^1(G,\mathbb{Z}_p))$$

under the inclusion of the “symplectic block”, i.e.

$$B \mapsto \begin{pmatrix} 1 & & \\ & B & \\ & & 1 \end{pmatrix}.$$

Now after noting that $\mathrm{Dehn}(S)$ has dense image in $\mathrm{Sp}_{n-2}(\mathbb{Z}_p)$ the bottom square in following diagram obviously commutes

$$\begin{tikzcd}
\mathrm{Out}(G) \arrow[rr] & & \mathrm{GL}(H^1(G,\mathbb{Z}_p)) \\
& \widehat{\mathcal{K}}(\mathrm{Dehn}(S) \arrow[ul, hook] \arrow[r, dashed] & \mathrm{Sp}(H^1(S,\mathbb{Z}_p)) \arrow[u, hook] \\
\mathrm{Dehn}(S) \arrow[uu, "\widehat{\mathcal{K}}"] \arrow[ur, two heads] \arrow[rr] & & \mathrm{Mod}(S) \arrow[u, "\text{dense image}"]
\end{tikzcd}$$

yielding the desired map. □

Now assume that G is a Demuškin group of rank n with $q = q(G) = 0$. It suffices to assume $n \geq 2$. Then G is isomorphic to the pro-p completion of the fundamental group of a closed surface $S = S_g$ with $2g = n$. In this case we have

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \mathbb{Z}_p) \cong \mathrm{GSp}_n(\mathbb{Z}_p)$$

and repeating the same discussion as above it follows that the subgroup $\widehat{\mathcal{K}}(\mathrm{Dehn}(S))$ in $\mathrm{Out}(G)$ has dense image in $\mathrm{Sp}_n(\mathbb{Z}_p)$.

7.5 Combinatorial automorphisms of Gal_K

In this section K shall always denote a finite extension of $\mathbb{Q}_p$ of degree N containing the pth roots of unity when $p \neq 2$ and assuming $\sqrt{-1} \in K$, i.e. $\mu_4 \subseteq K$ when $p = 2$. Hence, the maximal pro-p quotient is a Demuškin group of rank $N+2$ with $q = p^t$. As this is a characteristic quotient, any outer automorphism of Gal_K induces an outer automorphism of the maximal pro-p quotient $\mathrm{Gal}_K(p)$.

For $p \neq 2$ we have shown that there exists a surjective map of $\mathrm{Out}(\mathrm{Gal}_K(p))$ to the group of automorphisms of $H^1(K, \Lambda)$ respecting the symplectic structure and Bockstein homomorphism, where $\Lambda = \mathbb{Z}_p/p^t\mathbb{Z}_p$ for $p^t = \#\mu_{p^\infty}(K)$. To be precise, Corollary 6.3.3 yields a map

$$\mathrm{Out}(\mathrm{Gal}_K) \to \mathrm{Out}(\mathrm{Gal}_K(p)) \twoheadrightarrow \mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda)).$$

In Section 7.5.3 we provide a pretty large lower bound for the image of $\mathrm{Out}(\mathrm{Gal}_K)$ in the group $\mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda))$ and write down a few explicit examples of (outer) automorphisms that are induced by combinatorial Dehn twists. In fact, we conjecture that this map is surjective. In order to talk about combinatorial Dehn twists, we need to write down a suitable discrete group and a suitable $\mathcal{P}$-completion allowing us to define a pro-$\mathcal{P}$ combinatorial automorphism map to $\mathrm{Aut}(\mathrm{Gal}_K)$.

7.5.1 The combinatorial automorphisms map for the Jannsen–Wingberg presentation

We once more recall the main result of [JW82] and [Die84], as discussed in Section 3.2.1.

Theorem (Jannsen–Wingberg–Diekert)**.** *If $p \neq 2$, we assume that $\mu_p \subseteq K$. If $p = 2$, we assume $\mu_4 \subseteq K$. The group Gal_K is isomorphic to the profinite group generated by $N+3$ generators $\sigma, \tau, x_0, \ldots, x_N$, subject to the following conditions.*

(i) The closed normal subgroup topologically generated by $x_0, \ldots, x_N$ is a pro-p group.

(ii) The elements σ, τ satisfy the "tame" relation

$$\sigma\tau\sigma^{-1} = \tau^q.$$

(iii) The generators satisfy a further "wild" relation

$$x_0^\sigma = ((x_0\tau)^\pi)^g x_1^{p^s} [x_1, x_2] [x_3, x_4] \cdots [x_{N-1}, x_N],$$

where $\pi = \pi_p$ is the unique idempotent element of $\widehat{\mathbb{Z}}$ with $\pi\hat{\mathbb{Z}} = \mathbb{Z}_p$.

We have previously discussed why one should not refer to this as a presentation of Gal_K. In this section will define a discrete group JW (or rather group presentation) and a suitable condition $\mathcal{P}$ on finite index normal subgroups such that the respective completion yields Gal_K. In a sense, we want to argue that this is in fact the correct way one should understand the result of Jannsen and Wingberg.

Let $\pi' = 1 - \pi$ denote the idempotent element of $\widehat{\mathbb{Z}}$ such that $\pi'\widehat{\mathbb{Z}} = \prod_{\ell \neq p} \mathbb{Z}_\ell$. Then condition (i) can be expressed as follows:

(i') For all $w \in \langle\langle x_0, \dots, x_N \rangle\rangle$ we have $w^{\pi'} = 0$.

We trivially rewrite the third relation as

(iii') $((x_0\tau)^g)^\pi = \sigma x_0 \sigma^{-1} \left(x_1^{p^s} [x_1, x_2] \dots [x_{N-1}, x_N] \right)^{-1}$.

We note that the right-hand side is contained in the pro-p normal subgroup generated by $x_0, \dots, x_N$. The cyclic subgroup generated by $w = (x_0\tau)^g$ is of the form

$$\langle w \rangle = \left\langle w^{\pi'} \right\rangle \times \langle w^\pi \rangle .$$

Hence, we choose y, z such that $(x_0\tau)^g = y \cdot z$ such that

(a) $[y, z] = 1$,

(b) $z^\pi = z$, i.e. $z = \sigma x_0 \sigma^{-1} \left(x_1^{p^s} [x_1, x_2] \dots [x_{N-1}, x_N] \right)^{-1}$,

(c) $y^\pi = 0$.

Definition 7.5.1. We call the group JW given by the presentation

$$\left\langle \sigma, \tau, x_0, \dots, x_N, y, z \;\middle|\; \begin{array}{c} \sigma\tau\sigma^{-1} = \tau^q \\ (x_0\tau)^g = yz \\ [y, z] = 1 \\ \sigma x_0 \sigma^{-1} = z x_1^{p^s} [x_1, x_2] \dots [x_{N-1}, x_N] \end{array} \right\rangle$$

discrete Jannsen–Wingberg group.

We now define a property $\mathcal{P}$ of finite index normal subgroups N of JW as follows

($\mathcal{P}$) N satisfies $\mathcal{P}$ if for the quotient map $\pi_N \colon \mathrm{JW} \to \mathrm{JW}/N$ the following holds:

(a) the image of $\langle\langle x_0, \dots, x_N \rangle\rangle$ under π_N is a p-group,

(b) the image of y under π_N has order prime to p.

We claim that $\mathcal{P}$ is a cofiltered index system. Indeed, given N_1, N_2 satisfying $\mathcal{P}$, we choose $N_3 = N_1 \cap N_2$. As $G/(N_1 \cap N_2) = \mathrm{im}(G \to G/N_1 \times N_2)$, we can directly see that if y has order prime to p under G/N_1 and G/N_2, it must have order prime to p in their product, and the property of a normal subgroup to be pro-p is also preserved by products. Furthermore, $\mathcal{P}$ is complete as these properties are preserved after passing to quotients by larger normal subgroups.

Hence, as discussed in Section 7.1.2, we have a well-defined notion of pro-$\mathcal{P}$ completion

$$\mathrm{JW}^{\wedge\mathcal{P}} = \lim_{N \text{ satisfies } \mathcal{P}} \mathrm{JW}/N.$$

Furthermore, we have a diagram

$$\begin{tikzcd} & \mathrm{JW}^{\wedge\mathcal{P}} \arrow[dd] \\ \mathrm{JW} \arrow[ur] \arrow[dr] & \\ & \mathrm{Gal}_K \end{tikzcd}$$

where the vertical arrow must be an isomorphism by the result of Jannsen–Wingberg and the universality of the above construction.

Now we assume that $N \geq 6$. Choosing F to be the discrete free group in the generators $x_3, \ldots, x_N$ and setting $\delta = [x_3, x_4] \ldots [x_{N-1}, x_N]$, there exists a discrete combinatorial automorphism map for δ

$$\mathcal{K}^{(\delta)}_{\mathrm{discr}} \colon \mathrm{Aut}^{(\delta)}(F) \to \mathrm{Aut}(\mathrm{JW}). \tag{7.5}$$

In fact, by the choice of $\mathcal{P}$ this factors through $\mathrm{Aut}^{(\mathcal{P})}(\mathrm{JW})$. Indeed, let $\varphi \in \mathrm{Aut}^{(\delta)}(F)$, let N be an open normal subgroup, and consider the group homomorphisms

$$h \colon \mathrm{JW} \xrightarrow{\varphi} \mathrm{JW} \twoheadrightarrow \mathrm{JW}/N \quad \text{and} \quad \pi_{\varphi(N)} \colon \mathrm{JW} \twoheadrightarrow \mathrm{JW}/\varphi(N).$$

As by construction φ maps the subgroup $\langle x_0, \ldots, x_N \rangle$ isomorphically to itself, the same is true for the normal subgroup $P \coloneqq \langle\langle x_0, \ldots, x_N \rangle\rangle$ generated by these elements. Hence, the image of P under h is isomorphic to the image under $\pi_{\varphi(N)}$. The latter is isomorphic to the quotient

$$h \circ \varphi^{-1} \colon \mathrm{JW} \to \mathrm{JW} \twoheadrightarrow \mathrm{JW}/N,$$

and it holds that $h \circ \varphi^{-1}(P) = h(P)$. Furthermore, by construction we have $\varphi(y) = y$. As $h(y)$ is isomorphic to $\pi_{\varphi(N)}(y)$ and thus they have the same order.

The $\mathcal{P}$-completion functor allows us to define a combinatorial automorphism map for δ that maps to $\mathrm{Aut}(\mathrm{Gal}_K)$, namely as

$$\widehat{\mathcal{K}} = \mathcal{K}^{(\delta)}_{\mathcal{P}} : \qquad \mathrm{Aut}^{(\delta)}(F) \xrightarrow{\mathcal{K}^{(\delta)}_{\mathrm{discr}}} \mathrm{Aut}^{(\mathcal{P})}(\mathrm{JW}) \xrightarrow{(-)^{\mathcal{P}}} \mathrm{Aut}(\mathrm{Gal}_K). \tag{7.6}$$

We want to restate Theorem 7.4.1 for the absolute Galois group Gal_K. So next we discuss how to identify the pro-p completion of the Jannsen–Wingberg presentation and the standard Demuškin presentation of $\mathrm{Gal}_K(p)$. From now on we will assume that $p \neq 2$ as we use previous results requiring this assumption.

7.5.2 Pro-p completion of the Jannsen–Wingberg presentation

In this section, we want to express the Demuškin group $\mathrm{Gal}_K(p)$ in terms of the image of the generators $\sigma, \tau, x_0, \ldots, x_N$, and then give an explicit isomorphism of this presentation and the standard Demuškin presentation.

To simplify the notation, we shall call the images of these generators in the quotient $\mathrm{Gal}_K(p)$ by the same letters. Note that the image of τ acts trivial on $\mathrm{Gal}_K(p)$. Hence for the pro-p completion of the Jannsen-Wingberg presentation one has

$$\left\langle \sigma, x_0, \ldots, x_N \middle| x_0^{\sigma} = x_0^{g} x_1^{p^s} [x_1, x_2] [x_3, x_4] \cdots [x_{N-1}, x_N] \right\rangle.$$

We denote this group by G. In order to simplify the comparison, we do a base change and set $\widetilde{x_0} = x_0^{-1}$ as a new generator. Let F' denote the free pro-p group in the generators $\sigma, \widetilde{x_0}, \ldots, x_N$. To simplify some notation, we set $x_{-1} = \sigma$. Writing $g = 1 - u \cdot p^t$ for some unit u, the defining relation of above group is given as

$$\rho' = \widetilde{x_0}^{up^t} x_1^{p^s} [x_1, x_2] [x_3, x_4] \cdots [x_{N-1}, x_N] [x_{-1}, \widetilde{x_0}].$$

Now let F be a free pro-p group in generators $y_{-1}, y_0, \dots, y_N$ and let

$$\rho = y_{-1}^{p^t}[y_{-1}, y_0] \dots [y_{N-1}, y_N].$$

Then $D = F/\langle\langle\rho\rangle\rangle$ is a Demškin group "in standard form" of rank $N+2$ with invariant q^t. By the structure theorem for Demuškin groups (Theorem 5.2.13), there exists an automorphism $F' \to F$ mapping ρ' to ρ. We want to make this (more) explicit.

Using Proposition 6.2.6, it suffices to find an isomorphism

$$f_2 \colon G^{\mathrm{ab}} \otimes \Lambda \to D^{\mathrm{ab}} \otimes \Lambda$$

that lifts to an isomorphism

$$f_3 \colon G/C^3G \to D/C^3D,$$

where $C^\bullet G$, and $C^\bullet D$ denote the respective Λ-filtration. While this result guarantees the existence of a lift $\varphi = \varphi_\infty \colon G \to D$, it will not provide an explicit expression for it in terms of generators. However, this will not be needed in the later discussion.

Let $\chi_{-1}, \dots, \chi_N$ and $\eta_{-1}, \eta_0, \dots, \eta_N$ denote the basis of $H^1(D, \Lambda)$ and $H^1(G, \Lambda) = H^1(K, \Lambda)$, respectively, dual to the images $\overline{y_{-1}}, \dots, \overline{y_N}$ in $D^{\mathrm{ab}} \otimes \Lambda$ and $\overline{x_{-1}}, \overline{\widetilde{x_0}} \dots, \overline{x_N}$ in G^{ab}. In this choice of basis, we are looking for a Λ-linear map A

$$\begin{tikzcd}
G^{\mathrm{ab}} \otimes \Lambda \arrow[r, "\varphi_2"] \arrow[d, equal] & D^{\mathrm{ab}} \otimes \Lambda \arrow[d, equal] \\
\Lambda^{N+2} \arrow[r, "A"] & \Lambda^{N+2}
\end{tikzcd}$$

and hence, we may instead determine the dual map

$$\begin{tikzcd}
H^1(D, \Lambda) \arrow[r, "\varphi_2^*"] \arrow[d, equal] & H^1(G, \Lambda) \arrow[d, equal] \\
\Lambda^{N+2} \arrow[r, "A^*"] & \Lambda^{N+2}
\end{tikzcd}$$

in the respective dual bases given above. Using Theorem 6.1.2, the lifting condition for f_2 can be translated into a compatibility of f_2^* of the induced maps on cohomology with cup-product and Bockstein. So we will determine the dual map A^* with respect to this basis.

By Proposition 5.1.12 the bilinear forms induced by the respective cup products on $H^1(D, \Lambda)$ and $H^1(G, \Lambda)$ composed with the trace maps corresponding to ρ and ρ', are given by the matrix

$$J = \begin{pmatrix} 0 & -1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & -1 \\ & & & 1 & 0 \end{pmatrix}.$$

Compatibility with cup-product for $A^* \in \mathrm{Isom}(H^1(D, \Lambda), \mathrm{H}^1(G, \Lambda)) \cong \mathrm{GL}_{N+2}(\Lambda)$ thus means that $(A^*)^t J A^* = J$. Let $\beta_D \colon H^1(D, \Lambda) \to H^2(D, \Lambda) \cong \Lambda$, and $\beta_G \colon H^1(G, \Lambda) \to H^2(G, \Lambda) \cong \Lambda$

denote the Bockstein homomorphism for D and G, where the identification with Λ is again done via the respective trace maps. By definition we have

$$\begin{aligned} \beta_D(\chi) &= \chi \cup \chi_0, && \text{for all } \chi \in H^1(D,\Lambda) \\ \beta_G(\eta) &= \eta \cup (-u\eta_{-1} + p^{s-t}\eta_2), && \text{for all } \eta \in H^1(G,\Lambda). \end{aligned}$$

So this determines the column of A^* corresponding to χ_0 as

$$\begin{pmatrix} -u \\ 0 \\ 0 \\ p^{s-t} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We may assume that the map we are looking for maps $\chi_i \mapsto \eta_i$ for all $i \geq 3$. Hence, for the remaining discussion we will assume $N = 2$. We note that the orthogonal space of χ_0 is spanned by χ_0, χ_1, χ_2, and the orthogonal space of $A^*\chi_0 = -u\eta_{-1} + p^{s-t}\eta_2$ is spanned by η_{-1}, η_2, and $p^{s-t}\eta_0 - u\eta_1$. We will assume that $A^*\chi_2 = \eta_2$. As $A^*\chi_1$ is orthogonal to $A^*\chi_0$, we may write it as

$$A^*\chi_1 = a\eta_{-1} + b\eta_2 + c(p^{s-t}\eta_0 - u\eta_1), \quad a, b, c \in \Lambda.$$

The condition $\chi_2 \cup \chi_1 = 1 = \eta_2 \cup A^*\chi_1$ implies $c = u^{-1}$. Choosing $a = b = 0$, we get $A^*\chi_1 = \eta_1 - u^{-1}p^{s-t}\eta_0$. Note that these choices in fact make sure that A^* is an isomorphism on the orthogonal spaces of χ_0 and $A^*\chi_0$. Now it remains to determine

$$A^*\chi_{-1} = a\eta_{-1} + b\eta_0 + c\eta_1 + d\eta_2, \quad a, b, c, d \in \Lambda.$$

Using the conditions on the cup-product, we get $b = u^{-1}, c = 0$, and $d = -au^{-1}p^{s-t}$. We may now choose $a = 0$, hence getting $d = 0$, which yields an invertible matrix

$$A^* = \begin{pmatrix} 0 & -u & 0 & 0 \\ u^{-1} & 0 & -p^{s-t}u^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & p^{s-t} & 0 & 1 \end{pmatrix}, \tag{7.7}$$

satisfying the conditions described above by construction. So in particular, we have determined the Λ-linear map A as its dual. After another base change we get the following result.

Proposition 7.5.2. *With respect to the basis $\overline{y_{-1}}, \overline{y_0}, \ldots, \overline{y_N}$, and $\overline{\sigma} = \overline{x_{-1}}, \overline{x_0}, \ldots, \overline{x_N}$ of $D^{\mathrm{ab}} \otimes \Lambda$ and $G^{\mathrm{ab}} \otimes \Lambda$, respectively, there exists a 1-liftable Λ-linear map $f_2 \colon G^{\mathrm{ab}} \otimes \Lambda \to D^{\mathrm{ab}} \otimes \Lambda$ given by the matrix*

$$A = \begin{pmatrix} 0 & u^{-1} & 0 & 0 & \\ u & 0 & 0 & -p^{s-t} & \\ 0 & -u^{-1}p^{s-t} & 1 & 0 & \\ 0 & 0 & 0 & 1 & \\ & & & & I \end{pmatrix}$$

where I denotes the $(N-2) \times (N-2)$ identity matrix.

Note that in the above choice of basis for $H^1(K,\Lambda)$ and $H^1(D,\Lambda)$, the images of generators $\eta_3,\dots,\eta_N$ and $\chi_3,\dots,\chi_N$ generate a proper subspace of $\ker\beta_G/\ker\beta_G^\perp$, and $\ker\beta_D/\ker\beta_D^\perp$, respectively, which we shall call W'_G and W'_D.

In particular, we may conclude the following.

Corollary 7.5.3. *Any 1-liftable map $\varphi_2\colon \mathrm{Gal}_K(p)^{\mathrm{ab}}\otimes\Lambda \to \mathrm{Gal}_K(p)^{\mathrm{ab}}$ induces a 1-liftable map $f_2\circ\varphi_2\circ f_2^{-1}\colon D^{\mathrm{ab}}\otimes\Lambda\to D^{\mathrm{ab}}\otimes\Lambda$. In particular, we have the following commutative diagram*

$$\begin{tikzcd}
\mathrm{Aut}^{(+1)}(\mathrm{Gal}_K(p)^{\mathrm{ab}}\otimes\Lambda) \arrow[r, equal, "\sim"] \arrow[d, "\cong"] & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda)) & \underline{\mathrm{GSp}}(W'_G)(\Lambda) \arrow[l, hook'] \\
\mathrm{Aut}^{(+1)}(D^{\mathrm{ab}}\otimes\Lambda) \arrow[r, equal, "\sim"] & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(D,\Lambda)) \arrow[u, "\cong"] & \underline{\mathrm{GSp}}(W'_D)(\Lambda). \arrow[l, hook'] \arrow[u, "\cong"]
\end{tikzcd}$$

7.5.3 Generating a large subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$

We choose a similar set up as in the previous section. We will from now on assume $N\geq 4$. Note that this is not a very strong assumption. This would be satisfied when assuming $p\geq 5$. The only field K we are omitting here is $K=\mathbb{Q}_3(\zeta_3)$.

We consider the map

$$\mathrm{Out}(\mathrm{Gal}_K)\to\mathrm{Out}(\mathrm{Gal}_K(p))\twoheadrightarrow\mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda))\cong\mathrm{Aut}^{(-\cup-,\beta)}(H^1(D,\Lambda)),$$

where we choose the right-hand identification via the explicit base change map used in Corollary 7.5.3, i.e. we choose generators $y_0,\dots,y_N,y_{-1}$, of D as in Theorem 5.2.8. Hence, the group $\mathrm{Aut}^{(-\cup-,\beta)}(H^1(D,\Lambda))$ is a subgroup of the maximal parabolic subgroup of the Λ-valued points of $\underline{\mathrm{GSp}}(H^1(D,\Lambda))$ corresponding to the isotropic subspace $\ker\beta_D^\perp$.

In particular, using the same notation as above, the images of $\chi_3,\dots,\chi_N$ generate a $(N-2)$-dimensional subspace W' of the N-dimensional symplectic space

$$W=\ker\beta_D/\ker\beta_D^\perp.$$

Let $S=S_g$ be a closed surface with $2g=N-2$. By assumption on N, we have $g\geq 2$. Denoting F to be the free discrete group in generators $x_3,\dots,x_N$, where we identify $x_3,\dots,x_N$ with the usual generators of the fundamental group of S^*. In Section 7.3 we have defined the map

$$\mathrm{Aut}^{(\delta)}(F)\to\mathrm{Sp}(H^1(S,\mathbb{Z}))\cong\mathrm{Sp}_{N-2}(\mathbb{Z}).$$

By Section 7.5.1 we have a well-defined notion of combinatorial automorphism map for $\mathrm{Gal}_K\cong\mathrm{JW}^{\wedge\mathcal{P}}$,

$$\widehat{\mathcal{K}}=\mathcal{K}_{\mathcal{P}}^{(\delta)}\colon\ \mathrm{Aut}^{(\delta)}(F)\to\mathrm{Out}(\mathrm{Gal}_K).$$

Hence, we have the following result:

Theorem 7.5.4. *There is a commutative diagram*

$$\begin{tikzcd}
\mathrm{Out}(\mathrm{Gal}_K) \arrow[r] & \mathrm{Out}(\mathrm{Gal}_K(p)) \arrow[r, two heads, "\overline{\pi_2}"] & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda)) \arrow[r, hook] \arrow[d, equal] & \mathrm{GSp}_{N+2}(\Lambda) \\
 & & \mathrm{Aut}^{(-\cup-,\beta)}(H^1(D,\Lambda)) & \\
 & & \underline{\mathrm{Sp}}(W')(\Lambda) \arrow[u, hook] \arrow[r, equal] & \mathrm{Sp}_{N-2}(\Lambda) \\
\mathrm{Aut}^{(\delta)}(F) \arrow[uuu, "\widehat{\mathcal{K}}"] \arrow[rr, two heads] & & \mathrm{Sp}(H^1(S,\mathbb{Z})) \arrow[u, two heads] \arrow[r, equal] & \mathrm{Sp}_{N-2}(\mathbb{Z}). \arrow[u, two heads, "-\otimes\Lambda"']
\end{tikzcd}$$

In particular, we have now found also found a "large" subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$.

Theorem 7.5.5. *The subgroup* $\widehat{\mathcal{K}}(\mathrm{Dehn}(S))$ *in* $\mathrm{Out}(\mathrm{Gal}_K)$ *has dense image in* $\mathrm{Sp}_{N-2}(\mathbb{Z}_p)$.

Proof. This is the same argument as in Theorem 7.4.2. □

7.5.4 Revisiting the Jannsen–Wingberg automorphism

In this section, we may again include the case $p = 2$. We first do not require any other assumptions on K except $N = [K : \mathbb{Q}_p] > 1$ and when $p = 2$ we assume $\mu_4 \subseteq K$. In the proof Proposition 3.2.4 we described an automorphism, which we called *Jannsen–Wingberg automorphism* as follows: We choose generators $\sigma, \tau, x_0, \ldots, x_N$ of Gal_K as in Theorem 3.2.9 for $p \neq 2$ and Theorem 3.2.12 for $p = 2$. Let F denote the free profinite group in these generators. In the proof we defined an automorphism on F as

$$(\psi_0)_N^{\mathrm{JW}} \colon F \to F, \quad x_N \mapsto x_N \cdot x_{N-1},$$

and as the identity on all other generators. This induces an automorphism on Gal_K, which we shall denote by

$$\psi_N^{\mathrm{JW}} \colon \mathrm{Gal}_K \to \mathrm{Gal}_K.$$

Now the same argument works for all x_j with $j = 3, \ldots, N$ even. Namely, we may define automorphism on the free group

$$(\psi_0)_j^{\mathrm{JW}} \colon F \to F, \quad x_j \mapsto x_j \cdot x_{j-1},$$

and as the identity on all other generators, which induce automorphisms $\psi_j^{\mathrm{JW}} \colon \mathrm{Gal}_K \to \mathrm{Gal}_K$. Now considering the image of these maps under

$$\mathrm{Aut}(\mathrm{Gal}_K) \to \mathrm{Aut}(\mathrm{Gal}_K(p)) \to \mathrm{Aut}(\mathrm{Gal}_K(p)^{\mathrm{ab}})$$

is of the form

$$\psi_j^{\mathrm{JW}} \mapsto \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 1 & 1 & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

This shows that these maps can neither be inner automorphism nor geometric automorphism: Inner automorphisms would be trivial on the abelianization of $\mathrm{Gal}_K(p)$, and geometric automorphism have finite order in $\mathrm{Out}(\mathrm{Gal}_K)$ and thus finite order in abelianization of $\mathrm{Gal}_K(p)$.

The framework we have provided in Section 7.3 now allows us to give a new interpretation of this class of Jannsen–Wingerg automorphism. Now we again assume $\mu_p \subseteq K$ in the case $p \neq 2$, as we only defined the the discrete Jannsen–Wingberg group in this case.

Proposition 7.5.6. *The set of Jannsen–Wingberg automorphisms ψ_j^{JW} is contained in the image of* $\mathrm{Dehn}(S)$ *under $\widehat{\mathcal{K}}$. More precisely, they are images of Dehn twists of the type the elements τ_{a_i} described in Lemma 7.3.4.*

Proof. After suitable identification of generators, the elements τ_{a_i} described in Lemma 7.3.4, which are a subset of the set of generators of $\mathrm{Dehn}(S)$, induce the same automorphisms on Gal_K as described above. □

Hence, the (class of) Jannsen–Wingberg automorphism(s), that has previously been known and used, is in fact part of a large subgroup of what we call combinatorial automorphisms, and more specifically such automorphisms induced by combinatorial Dehn twists. So not only do these maps come from the combinatorics of a given group presentation of Gal_K, they actually have a geometric interpretation.

7.5.5 Further observations about $\mathrm{Out}(\mathrm{Gal}_K)$

We want to conclude this thesis with the following conjecture:

Conjecture 7.5.7. The images of combinatorial Dehn twists under the combinatorial automorphism map of Gal_K for δ are not geometric automorphism, i.e.

$$\overline{\widehat{\mathcal{K}}(\mathrm{Dehn}(S))} \cap \mathrm{Aut}(K) = \{1\},$$

where we view $\mathrm{Aut}(K)$ as a subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$ under the embedding from Theorem 3.1.1.

A reason to conjecture this is that $\mathrm{Aut}(K)$ is a finite subgroup of $\mathrm{Out}(\mathrm{Gal}_K)$ while $\overline{\widehat{\mathcal{K}}(\mathrm{Dehn}(S))}$ is not. Furthermore, similar to the argument above, one can directly show that the induced automorphism of Gal_K for any of the generators of $\mathrm{Dehn}(S)$ described in Lemma 7.3.4, is not a geometric automorphism.

There is another observation supporting this conjecture.

Lemma 7.5.8. *Any induced automorphisms of combinatorial Dehn twists coming from a geometric automorphism of K must be the identity on the p-power roots of unity of K.*

Proof. By local reciprocity (see Theorem 2.3.7) and the multiplicative structure of K, it holds that

$$\mathrm{Gal}_K(p)^{\mathrm{ab}} \cong (K^\times)^p \cong U_K^{(1)} \times \mathbb{Z}_p.$$

Now let $\varphi\colon K \to K$ denote a geometric automorphism. We shall denote its image in $\mathrm{Out}(\mathrm{Gal}_K)$ by the same name. Assuming this comes from a combinatorial Dehn twist, this fixes the generators $\sigma, \tau, x_0, x_1, x_2$ of Gal_K. So in particular, after passing to the standard Demuškin presentation of Gal_K, it fixes the generators y_1, y_2. But by the choice of these generators, this means that it acts trivially on the torsion part of $\mathrm{Gal}_K(p)^{\mathrm{ab}}$. □

Now if K is a Galois extension of $\mathbb{Q}_p$, and $\mathbb{Q}_p(\mu_p)$ is a subextension, then there exist $\mathbb{Q}_p$-linear automorphisms of K, which do not leave the p-th roots of unity invariant. Hence, under certain conditions, we can immediately see that there are geometric automorphisms that cannot come from the group of combinatorial Dehn twists.

Bibliography

[Bir69] J. S. Birman. “Mapping class groups and their relationship to braid groups”. In: *Communications on Pure and Applied Mathematics* 22.2 (1969), pp. 213–238.

[Deh38] M. Dehn. “Die Gruppe der Abbildungsklassen”. In: *Acta mathematica* 69.1 (1938), pp. 135–206.

[Dem61] S.P. Demuškin. “The group of a maximal p-extension of a local field”. In: *Izv. Akad. Nauk SSSR Ser. Mat* 25 (1961), pp. 329–346.

[Dem63] S.P. Demuškin. “On 2-extensions of a local field”. In: *Sibirskii Matematicheskii Zhurnal* 4.4 (1963), pp. 951–955.

[Die84] V. Diekert. “Über die absolute Galoisgruppe dyadischer Zahlkörper”. In: *Journal für die reine und angewandte Mathematik* 350 (1984), pp. 152–172.

[Dix+03] J.D. Dixon et al. *Analytic pro-p groups*. 61. Cambridge University Press, 2003.

[DL83] D. Dummit and J.P. Labute. “On a new characterization of Demuskin groups”. In: *Inventiones mathematicae* 73.3 (1983), pp. 413–418.

[Efr03] I. Efrat. “Demuškin fields with valuations”. In: *Mathematische Zeitschrift* 243 (2003), pp. 333–353.

[FM11] B. Farb and D. Margalit. *A Primer on Mapping Class Groups*. Princeton University Press, 2011.

[Hal59] M. Hall. *The Theory of Groups*. Macmillan, 1959.

[Hil85] J. A. Hillman. “The kernel of the cup product”. In: *Bulletin of the Australian Mathematical Society* 32.2 (1985), pp. 261–274.

[HN20] Y. Hoshi and Y. Nishio. “On the Outer Automorphism Groups of the Absolute Galois Groups of Mixed-characteristic Local Fields”. In: (2020).

[Hos19] Y. Hoshi. “Topics in the anabelian geometry of mixed-characteristic local fields”. In: *Hiroshima Mathematical Journal* 49.3 (2019), pp. 323–398.

[Hum79] S. P. Humphries. “Generators for the mapping class group”. In: *Topology of low-dimensional manifolds*. Springer, 1979, pp. 44–47.

[Jak68] A.V. Jakovlev. “The Galois group of the algebraic closure of a local field”. In: *Mathematics of the USSR-Izvestiya* 2.6 (1968), p. 1231.

[Jak78] A.V. Jakovlev. “Remarks on my paper “The Galois group of the algebraic closure of a local field””. In: *Mathematics of the USSR-Izvestiya* 12.1 (1978), p. 205.

[Jan82] U. Jannsen. “Über Galoisgruppen lokaler Körper”. In: *Inventiones mathematicae* 70.1 (1982), pp. 53–69.

[JR79] M. Jarden and J. Ritter. “On the characterization of local fields by their absolute Galois groups”. In: *Journal of Number Theory* 11.1 (1979), pp. 1–13.

[JW82] U. Jannsen and K. Wingberg. “Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper [The structure of the absolute Galois group of p-adic number fields]”. In: *Inventiones Mathematicae* 70.1 (1982), pp. 71–98.

[Koc13a] H. Koch. *Galois Theory of p-Extensions*. Springer Science & Business Media, 2013.

[Koc13b] D. Kochloukova. “Subdirect products of free pro-p and Demushkin groups”. In: *International Journal of Algebra and Computation* 23.05 (2013), pp. 1079–1098.

[Koc65] H. Koch. “Über Galoissche Gruppen von p-adischen Zahlkörpern”. In: *Mathematische Nachrichten* 29.1-2 (1965), pp. 77–111.

[Koc78] H. Koch. “The Galois group of a p-closed extension of a local field”. In: *Doklady Akademii Nauk*. Vol. 238. 1. Russian Academy of Sciences. 1978, pp. 19–22.

[Koe98] J. Koenigsmann. “Pro- p galois groups of rank ≤ 4”. In: *Manuscripta Mathematica* 95 (Dec. 1998), pp. 251–271.

[KZ05] D. H Kochloukova and P. Zalesskii. “Free-by-Demushkin pro-p groups”. In: *Mathematische Zeitschrift* 249.4 (2005), pp. 731–739.

[Lab+06] J. Labute et al. “Demuškin groups, Galois modules, and the Elementary Type Conjecture”. In: *Journal of Algebra* 304.2 (2006), pp. 1130–1146.

[Lab67] J.P. Labute. “Classification of Demushkin groups”. In: *Canadian Journal of Mathematics* 19 (1967), pp. 106–132.

[Lic64] W. B. R. Lickorish. “A finite set of generators for the homeotopy group of a 2-manifold”. In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 60. 4. Cambridge University Press. 1964, pp. 769–778.

[Lub01] A. Lubotzky. “Pro-finite presentations”. In: *Journal of algebra* 242.2 (2001), pp. 672–690.

[Moc97] S. Mochizuki. “A version of the Grothendieck conjecture for p-adic local fields”. In: *International Journal of Mathematics* 8.4 (1997), pp. 499–506.

[Mor11] M. Morishita. *Knots and primes: an introduction to arithmetic topology*. Springer Science & Business Media, 2011.

[Mor93] S. Morita. “The extension of Johnson’s homomorphism form the Torelli group to the mapping class group.” In: *Inventiones mathematicae* 111.1 (1993), pp. 197–224.

[Neu06] J. Neukirch. *Algebraische zahlentheorie*. Springer-Verlag, 2006.

[Nie27] J. Nielsen. “Untersuchungen zur Topologie der geschlossenen zweiseitigen Flächen”. In: *Acta Mathematica* 50.1 (1927), pp. 189–358.

[Nie29] J. Nielsen. “Untersuchungen zur Topologie der geschlossenen zweiseitigen Flächen. II”. In: *Acta Mathematica* 53 (1929), pp. 1–76.

[Nie32] J. Nielsen. “Untersuchungen zur Topologie der geschlossenen zweiseitigen Flächen. III”. In: *Acta Mathematica* 58 (1932), pp. 87–167.

[NS64] M. Newman and J. Smart. “Symplectic modulary groups”. In: *Acta Arithmetica* 9.1 (1964), pp. 83–89.

[NSW13] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields.* Vol. 323. Springer Science & Business Media, 2013.

[RZ00] L. Ribes and P. Zalesskii. “Profinite groups”. In: *Profinite Groups.* Springer, 2000, pp. 19–77.

[Ser13a] J.-P. Serre. *Galois cohomology.* Springer Science & Business Media, 2013.

[Ser13b] J.-P. Serre. *Local fields.* Vol. 67. Springer Science & Business Media, 2013.

[Ser62] J.-P. Serre. “Structure de certains pro-p-groupes”. In: *Séminaire Bourbaki* 63 (1962), pp. 357–364.

[Son74] J. Sonn. “Epimorphisms of Demushkin groups”. In: *Israel Journal of Mathematics* 17.2 (1974), pp. 176–190.

[Sta21] The Stacks project authors. *The Stacks project.* `https://stacks.math.columbia.edu`. 2021.

[Sul75] D. Sullivan. “On the intersection ring of compact three manifolds”. In: *Topology* 14.3 (1975), pp. 275–277.

[SZ16] I. Snopce and P. Zalesskii. “Subgroup properties of Demushkin groups”. In: *Mathematical Proceedings of the Cambridge Philosophical Society.* Vol. 160. 1. Cambridge University Press. 2016, pp. 1–9.

[SZ20] M. Shusterman and P. Zalesskii. “Virtual retraction and Howson’s theorem in pro-p groups”. In: *Transactions of the American Mathematical Society* 373.3 (2020), pp. 1501–1527.

[Waj83] B. Wajnryb. “A simple presentation for the mapping class group of an orientable surface”. In: *Israel Journal of Mathematics* 45.2 (1983), pp. 157–174.

[Wel71] C. Wells. “Automorphisms of group extensions”. In: *Transactions of the American Mathematical Society* 155.1 (1971), pp. 189–194.

[Win01] K. Wingberg. *Demuskin groups with operators.* 2001. arXiv: `math/0111333 [math.NT]`.

[Win82] K. Wingberg. “Der Eindeutigkeitssatz für Demuškinformationen”. In: *Inventiones mathematicae* 70.1 (1982), pp. 99–113.

[Win89] K. Wingberg. “On Demuškin groups with involution”. In: *Annales scientifiques de l’École Normale Supérieure* Ser. 4, 22.4 (1989), pp. 555–567.

Zusammenfassung

Sei K ein Körper und bezeichne K^{sep} einen separablen Abschluss von K. Die *absolute Galoisgruppe* von K ist definiert als $\text{Gal}_K := \text{Gal}(K^{\text{sep}}/K)$. Speziell sei K immer ein lokaler Körper gemischter Charakteristik, d.h. eine endliche Erweiterung des Körpers der p-adischen Zahlen $\mathbb{Q}_p$. Das Hauptziel dieser Arbeit ist es, einen Teil der Struktur der äußeren Automorphismengruppe

$$\text{Out}(\text{Gal}_K) = \text{Aut}(\text{Gal}_K)/\,\text{Inn}(\text{Gal}_K)$$

besser zu verstehen.

Diese Gruppe wurde beispielsweise im Kontext *anabelscher Geometrie* studiert, die sich u.a. mit der Frage beschäftigt, ob die absolute Galoisgruppe eines Körpers (oder allgemeiner die arithmetische Fundamentalgruppe eines Schemas) diesen bis auf Isomorphie festlegt. Während dies für Zahlkörper nach dem bekannten Resultat von Neukirch–Uchida richtig ist, muss diese Frage im Fall lokaler Körper von gemischter Charakteristik verneint werden (siehe hierzu [Moc97], [JR79]).

Seien $\text{Aut}(K)$ die Körperautomorphismen von K. Dann existiert eine injektive Abbildung

$$\Phi\colon\ \text{Aut}(K) \to \text{Out}(\text{Gal}_K).$$

Wir bezeichnen die Elemente im Bild dieser Abbildung auch als *geometrische Automorphismen* von Gal_K. Für diese existiert eine äquivalente Beschreibung. Nach einem Ergebnis von Mochizuki, siehe [Moc97], entsprechen diese genau den Automorphismen, die die Verzweigungsgruppenfiltrierung auf Gal_K respektieren.

Darüber hinaus ist viel über die Struktur der Gruppe Gal_K bekannt. In einer Reihe von Inventiones-Artikeln ([Jan82], [Win82],[JW82]) haben Jannsen und Wingberg im Fall $p \neq 2$ angeben, durch welche Invarianten Gal_K festgelegt ist und haben eine konkrete Beschreibung von Gal_K durch Erzeuger, die gewisse Bedingungen erfüllen, angegeben. Der Fall $p = 2$ wurde unter der Annahme, dass K die vierten Einheitswurzeln enthält, von Diekert in [Die84] behandelt. Diese Beschreibungen von Gal_K spielen im letzten Kapitel dieser Arbeit eine größere Rolle.

Es ist natürlich, Automorphismen einer Gruppe zu studieren, indem man zu charakteristischen Quotienten übergeht. Es gibt eine Filtrierung

$$V_K \subseteq I_K \subseteq \text{Gal}_K$$

auf Gal_K, wobei I_K die Trägheitsgruppe und V_K die wilde Trägheitsgruppe bezeichne. Jeder Automorphismus von Gal_K induziert die Identität auf dem maximal unverzweigten Quotienten $\text{Gal}(K^{\text{nr}}/K) = \text{Gal}_K/I_K$. Der maximal zahm-verzweigte Quotient $\text{Gal}(K^{\text{tr}}/K) = \text{Gal}_K/V_K$ ist isomorph zur Iwasawa-Gruppe

$$\text{Iw}_q = \widehat{\mathbb{Z}}'(1) \rtimes_q \widehat{\mathbb{Z}}$$

Setze $\text{Iw}_q^{\text{nr}} = \text{Iw}_q^{\text{ab}}/\text{tors}$ und $\text{Iw}_q^{\text{tr}} = \ker(\text{Iw}_q \to \text{Iw}_q^{\text{nr}})$. Wir zeigen, dass die Automorphismen φ von Iw_q trivial auf Iw_q^{nr} operieren und auf Iw_q^{tr} einen Automorphismus φ^{tr} induzieren. Nach

einem Resultat von Wells [Wel71] ist der Kern von

$$\mathrm{Out}(\mathrm{Iw}_q) \to \mathrm{Aut}(\mathrm{Iw}_q^{\mathrm{tr}})/\operatorname{Inn}(\mathrm{Iw}_q) \cong (\widehat{\mathbb{Z}}')^\times/q^{\widehat{\mathbb{Z}}},$$

welchen wir als $\mathrm{Out}_0(\mathrm{Iw}_q)$ bezeichnen, gegeben durch

$$H^1(\mathrm{Iw}_q^{\mathrm{nr}}, \mathrm{Iw}_q^{\mathrm{tr}}) \cong \mathbb{F}_q^\times.$$

Bezeichne nun K_0 die maximale unverzweigte Teilerweiterung von $K/\mathbb{Q}_p$ und K_1 die maximal zahm-verzweigte Teilerweiterung von $K/\mathbb{Q}_p$. Die beiden Hauptresultate von Kapitel 4 lauten wie folgt.

Theorem (Cf. Theorem 4.2.8)**.** *Die Untergruppe von* $\mathrm{Aut}(K)$*, die auf* $\mathrm{Out}_0(\mathrm{Iw}_q)$ *unter*

$$\mathrm{Aut}(K) \hookrightarrow \mathrm{Out}(\mathrm{Gal}_K) \to \mathrm{Out}(\mathrm{Gal}(K^{\mathrm{tr}}/K)) = \mathrm{Out}(\mathrm{Iw}_q)$$

abbildet, ist $\mathrm{Aut}(K/K_0)$*.*

Theorem (Cf. Theorem 4.2.9)**.** *Es gilt*

$$\ker(\mathrm{Aut}(K/K_0) \to \mathrm{Out}_0(\mathrm{Iw}_q)) = \mathrm{Aut}(K/K_1).$$

Das heißt die Untergruppe von $\mathrm{Aut}(K)$*, die die Identität auf* $\mathrm{Out}(\mathrm{Iw}_q)$ *induziert, ist* $\mathrm{Aut}(K/K_1)$*.*

Andererseits studieren wir in dieser Arbeit Automorphismen auf dem maximalen pro-p Quotient $\mathrm{Gal}_K(p)$ von Gal_K. Dabei handelt es sich um eine pro-p-Gruppe. Enthält K die p-ten Einheitswurzeln enthält, so handelt es sich bei $\mathrm{Gal}_K(p)$ um eine Demuškin-Gruppe von Rang $[K : \mathbb{Q}_p] + 2$. Kapitel 6 beschäftigt sich deshalb mit den Automorphismen von Demuškin-Gruppen. Einige Resultate gelten dabei allgemeiner für Morphismen endlich erzeugterpro-p-Gruppen, die wir hier nicht in voller Allgemeinheit darstellen wollen. Zunächst sind sind Demuškin-Gruppen wie folgt definiert:

Definition (Demuškin-Gruppe)**.** Eine pro-p Gruppe G heißt *Demuškin-Gruppe* wenn folgende Bedingungen erfüllt sind

(i) $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,

(ii) $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$,

(iii) das Cup-Produkt $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ ist nicht-ausgeartet.

Insbesondere sind Demuškin-Gruppen also endlich erzeugte pro-p-Gruppen, wobei die Invariante

$$n = n(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$$

die minimale Anzahl von Erzeugern in einer Präsentation als pro-p Gruppe angibt. Ferner bedeutet (ii), dass es sich um eine 1-Relator-Gruppe handelt. Wir definieren die Invariante $q = q(G)$ als die Mächtigkeit des Torsionsanteils in G^{ab}. Es gilt das folgende Klassifikationsresultat.

Theorem (Demuškin). *Sei G eine 1-Relator pro-p-Gruppe mit $q = q(G) \neq 2$. Dann ist G genau dann eine Demuškin-Gruppe, wenn G isomorph ist zu der pro-p Gruppe in n Erzeugern $x_1, \ldots, x_n$, welche folgende Relation erfüllen*

$$x_1^q[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n] = 1.$$

Insbesondere ist G durch die Invarianten n und q bis auf Isomorphie bestimmt.

Dieses Resultat geht auf Demuškin [Dem61] für $p \neq 2$ und Serre [Ser62] für $p = 2$ und $q \neq 2$ zurück. Der Fall $q = 2$, und damit die vollständige Klassifizierung von Demuškin-Gruppen, liefert Labute in [Lab67]. In allen unseren Resultaten über Demuškin-Gruppen setzen wir $p \neq 2$ voraus.

Wir definieren eine Invariante $\Lambda = \Lambda(G)$ als $\Lambda = \mathbb{Z}_p/q\mathbb{Z}_p$, wenn $q = q(G) \neq 0$ und als $\Lambda = \mathbb{Z}_p$ sonst. Dabei handelt es sich um den maximalen Quotienten von $\mathbb{Z}_p$, sodass $G^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} \Lambda$ ein freier Λ-Modul von Rang $n = n(G)$ ist. Ferner betrachten wir für $q \neq 0$ die absteigende q-Zentralreihe $C^\bullet G$, welche definiert ist als

$$C^1G = G, \quad C^{i+1}G = \left(C^iG\right)^q \left[C^iG, G\right],$$

wobei $\left[C^iG, G\right]$ die abgeschlossene Untergruppe bezeichne, die topologisch von Kommutatoren $[x, y] = xyx^{-1}y^{-1}$ für $x \in C^iG, y \in G$ erzeugt wird. Für $q = 0$ betrachten wir die herkömmliche absteigende Zentralreihe.

Sei nun $m \geq 2$. Angenommen, es existiert ein Morphismus

$$\varphi_m \colon G \to G/C^mG.$$

Gibt es einen Morphismus

$$\varphi_{m+1} \colon G \to G/C^{m+1}G,$$

sodass $\varphi_{m+1} \equiv \varphi_m \bmod C^mG$, so sagen wir φ_m ist 1-*liftbar*. Wir bezeichnen die Teilmenge der (surjektiven) 1-liftbaren Morphismen $G \to G/C^mG$ als

$$\mathrm{Hom}^{(+1)}(G, G/C^mG) \subseteq \mathrm{Hom}(G, G/C^mG)$$

(bzw. $\mathrm{Hom}^{(+1)}(G, G/C^mG)_{\mathrm{surj}}$). Wir bemerken, dass ein Morphismus $G \to G/C^mG$ über G/C^mG faktorisiert und surjektive Endomorphismen endlich erzeugter proendlicher Gruppen Isomorphismen sind. Das rechtfertigt folgende Definition:

$$\mathrm{Aut}^{(+1)}(G/C^mG) \coloneqq \mathrm{Hom}^{(+1)}(G, G/C^mG)_{\mathrm{surj}}.$$

Wir können die folgenden Ergebnisse über die Liftbarkeit von Morphismen entlang der q-Zentralreihe zeigen:

Theorem (Cf. Theorem 6.1.2). *Sei G eine Demuškin-Gruppe und $\varphi_2 \colon G \to G/C^2G$ ein Morphismus. Dann sind äquivalent.*

(a) φ_2 ist 1-liftbar.

(b) Es gibt einen Λ-Modulhomomorphismus $H^2(G, \Lambda) \to H^2(G, \Lambda)$, der kompatibel ist mit Cup-Produkt sowie, wenn $q \neq 0$, Bocksteinhomomorphismus.

Wenn $q \neq 0$, definieren wir

$$\mathrm{Aut}^{(-\cup -,\beta)}(H^1(G,\Lambda)) := \{(A,\lambda) \mid A^*(-\cup -) = \lambda(-\cup -), A^*\beta = \lambda\beta\},$$

als Gruppe von Automorphismen des freien Λ-Moduls $H^1(G,\Lambda)$, welche das cup-Produkt

$$-\cup -\colon H^1(G,\Lambda) \times H^1(G,\Lambda) \to \Lambda$$

und den Bocksteinhomomorphismus $\beta\colon H^1(G,\Lambda) \to \Lambda$ respektieren. Damit können wir diese Gruppe nach Wahl einer symplektischen Basis als Untergruppe der (Λ-wertigen Punkte) der allgemeinen symplektischen Gruppe

$$\underline{\mathrm{GSp}}(H^1(G,\Lambda))(\Lambda) = \mathrm{GSp}_n(\Lambda)$$

auffassen. Ist $q \neq 0$, so liefert obiges Resultat einen Isomorphismus

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda) \cong \mathrm{Aut}^{(-\cup -,\beta)}(H^1(G,\Lambda)).$$

Für $q = 0$ gilt

$$\mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \mathbb{Z}_p) \cong \mathrm{GSp}_n(\mathbb{Z}_p).$$

Theorem (Cf. Theorem 6.2.5). *Sei G eine Demuškingruppe, $m \geq 2$. Angenommen es gibt einen surjektiven Morphismus*

$$\varphi_{m+1}\colon G \to H/C^{m+1}H.$$

Dann existiert ein surjektiver Morphismus $\varphi_{m+2}\colon G \to H/C^{m+2}H$ mit $\varphi_{m+2} \equiv \varphi_{m+1} \bmod C^mG$.

Das Resultat impliziert, dass $\{\mathrm{Aut}^{(+1)}(G/C^mG)\}_{m\geq 1}$ ein surjektives projektives System von $\mathrm{Aut}(G)$ liefern. Insbesondere können wir also Folgendes zeigen:

Theorem (Cf. Theorem 6.3.2). *Es existiert ein surjektiver Gruppenhomomorphismus*

$$\mathrm{Out}(G) \twoheadrightarrow \mathrm{Aut}^{(+1)}(G^{\mathrm{ab}} \otimes \Lambda),$$

dessen Kern eine pro-p Gruppe ist.

Wir verstehen dieses Resultat als Analogie zur symplektischen Darstellung der Abbildungsklassengruppe einer topologischen Fläche.

In Kapitel 7 wird ein Rahmen definiert, in dem wir Automorphismen einer Gruppe untersuchen, die sich aus der Kombinatorik ihrer Gruppenpräsentation ergeben. Das geht so: Sei $G_{\mathrm{discr}} = \langle X \cup Y | R\rangle$ eine diskrete Gruppenpräsentation. Angenommen für alle $\rho \in R$ gilt $\rho = \rho_X \cdot \rho_Y$, wobei $\rho_X \in F_X$ und $\rho_Y \in F_Y$. Setze $S = \{\rho_Y \mid \rho \in R\}$ und

$$\mathrm{Aut}^{(S)}(F_Y) := \{\varphi\colon F \to F \mid \varphi(\rho) = \rho \text{ for all } \rho \in S\}.$$

Jeder Automorphismus in $\mathrm{Aut}^{(S)}(F_Y)$ lässt sich trivial zu einem Automorphismus von $F_{X\cup Y}$ fortsetzen, der alle Relationen in R fixiert. Wir erhalten eine Abbildung

$$\mathcal{K}^{(S)}_{\mathrm{discr}}\colon \mathrm{Aut}^{(S)}(F_Y) \to \mathrm{Aut}(G_{\mathrm{discr}}),$$

die wir *diskrete kombinatorische Automorphismenabbildung* für eine gegebene Menge von Relationen S nennen.

Wir definieren einen Begriff von Vervollständigung bezüglich eines Prädikats $\mathcal{P}$ für normale Untergruppen von endlichem Index in G_{discr}, welcher es möglich macht, eine pro-$\mathcal{P}$-Version dieser Abbildung zu definieren, d.h. eine Abbildung

$$\mathcal{K}_{\mathcal{P}}^{(S)}\colon \operatorname{Aut}^{(S)}(F_Y) \to \operatorname{Aut}(G_{\mathrm{discr}}^{\wedge\mathcal{P}}),$$

die wir *pro-$\mathcal{P}$ kombinatorische Automorphismenabbildung* für eine gegebene Menge von Relationen S nennen.

Wir betrachten nun eine geschlossene orientierbare Fläche $S = S_g$ vom Geschlecht $g \geq 1$. Wir betrachten die Standardpräsentation der Fundamentalgruppe

$$\pi_1(S) = \langle a_1, b_1, \ldots, a_g, b_g | \delta = 1\rangle$$

mit $\delta = [a_1, b_1] \ldots [a_g, b_g]$. Sei F die Fundamentalgruppe der einfach punktierten Fläche S^*. Dies ist eine freie Gruppe in den Erzeugern $a_1, b_1, \ldots, a_g, b_g$. Wir betrachten nun die Gruppe $\operatorname{Aut}^{(\delta)}(F)$. Diese hängt zusammen mit der Abbildungsklassengruppe $\operatorname{Mod}(S)$ von S, welche als Isotopieklassen von orientierungserhaltenden Homöomorphismen $S \to S$ definiert ist. Nach Arbeiten von Dehn (siehe [Deh38]) ist diese endlich erzeugt durch Dehntwists entlang geschlossener einfacher Kurven. Lickorish hat in [Lic64] gezeigt, dass eine bestimmte Menge von $3g - 1$ solcher Erzeuger ausreicht. Wir bezeichnen diese als *Lickorish-Erzeuger* von $\operatorname{Mod}(S)$. Wir können zeigen, dass die Wirkung dieser Lickorish-Erzeuger auf der Fundamentalgruppe zu Automorphismen von F geliftet werden können, die δ fixieren. Wir bezeichnen die von diesen Elementen erzeugte Untergruppe als

$$\operatorname{Dehn}(S) \subseteq \operatorname{Aut}^{(\delta)}(F)$$

und nennen sie *kombinatorische Dehntwists.* Insbesondere existiert ein surjektiver Gruppenhomomorphismus

$$\operatorname{Dehn}(S) \twoheadrightarrow \operatorname{Sp}(H^1(S,\mathbb{Z})) \cong \operatorname{Sp}_{2g}(\mathbb{Z}).$$

Mit Blick auf die Standardpräsentation von Demuškin-Gruppen aus dem Theorem von Demuškin sehen wir, dass kombinatorische Dehntwists Automorphismen auf Demuškin-Gruppen induzieren. Sei G eine (p-)Demuškin-Gruppe, $p \neq 2$ und angenommen $n = n(G) \geq 4$. Mit einer Wahl von $S = S_g$ mit $2g = m$ mit $m = n$ für $q(G) = 0$ und $m = n - 2$ sonst, zeigen wir schließlich, dass die so gefundene Untergruppe der äußeren Automorphismengruppe von G groß sein muss. Genauer zeigen wir Folgendes.

Theorem (Cf. Theorem 7.4.2)**.** *Die Untergruppe $\mathcal{K}_{\text{pro-}p}^{(\delta)}(\operatorname{Dehn}(S))$ in $\operatorname{Out}(G)$ hat dichtes Bild in $\operatorname{Sp}_m(\mathbb{Z}_p)$.*

Ein ähnliches Ergebnis kann für die absolute Galoisgruppe eines p-adischen Zahlkörpers gezeigt werden. Dazu benötigen wir die konkrete Aussage des oben erwähnten Resultats von Jannsen–Wingberg und Diekert. Wir führen zunächst die Invarianten ein, die in der Beschreibung benötigt werden.

Sei $K/\mathbb{Q}_p$ eine endliche Erweiterung vom Grad $N = [K : \mathbb{Q}_p]$ und sei q die Mächtigkeit des Restklassenkörpers von K. Nach einem Resultat von Iwasawa ist der maximal zahme Quotient $\operatorname{Gal}(K^{\mathrm{tr}}/K)$ erzeugt von zwei Elementen σ und τ, für welche die Relation $\sigma\tau\sigma^{-1} = \tau^q$ gilt, wobei σ ein Lift des Frobenius und τ ein Erzeuger der Trägheitsgruppe ist. Sei nun p^s die Ordnung der Gruppe $\mu_{\mathrm{tr}} = \mu_{p^\infty}(K^{\mathrm{tr}})$ von p-Potenz Einheitswurzeln von K^{tr}/K, und sei $\alpha\colon \operatorname{Gal}(K^{\mathrm{tr}}/K) \to (\mathbb{Z}/p^s\mathbb{Z})^\times$ der zyklotomische Charakter $\rho(\zeta) = \zeta^{\alpha(\rho)}$, wobei $\rho \in \operatorname{Gal}(K^{\mathrm{tr}}/K)$ und $\zeta \in \mu_{\mathrm{tr}}$. Wir wählen $g, h \in \mathbb{Z}_p$ so dass

$$g \equiv \alpha(\sigma), \quad h \equiv \alpha(\tau) \bmod p^s.$$

Im Spezialfall $\mu_p \subseteq K$ wählen wir $h = 1$ und die Aussage lautet wie folgt.

Theorem (Jannsen–Wingberg–Diekert)**.** *Angenommen $\mu_p \subseteq K$ und, wenn $p = 2$, angenommen $\mu_4 \subseteq K$. Dann ist die Gruppe Gal_K isomorph zur proendlichen Gruppe in $N + 3$ Erzeugern $\sigma, \tau, x_0, \ldots, x_N$, welche die folgenden Relationen bzw. Bedingungen erfüllen.*

(i) Die abgeschlossene normale Untergruppe, die von $x_0, \ldots, x_N$ erzeugt wird, ist eine pro-p-Gruppe.

(ii) Die Elemente σ, τ erfüllen die "zahme" Relation

$$\sigma\tau\sigma^{-1} = \tau^q.$$

(iii) Ferner erfüllen die Erzeuger die folgende "wilde" Relation

$$\sigma x_0 \sigma^{-1} = ((x_0\tau)^\pi)^g x_1^{p^s} [x_1, x_2] [x_3, x_4] \cdots [x_{N-1}, x_N],$$

wobei $\pi = \pi_p$ das eindeutige idempotente Element von $\widehat{\mathbb{Z}}$ mit $\pi\hat{\mathbb{Z}} = \mathbb{Z}_p$ bezeichne.

Dieses Resultat impliziert, dass die absolute Galoisgruppe Gal_K topologisch endlich erzeugt ist. Man bemerke, dass es sich um keine endliche Präsentation handelt, denn (i) lässt sich nicht durch endlich viele Relationen beschreiben. Ferner kommen in der Beschreibung durch Relationen echte proendliche Wörter vor. Wir möchten das Resultat anders interpretieren. Wir betrachten dazu zunächst eine passende diskrete Gruppe.

Definition. Die *diskrete Jannsen–Wingberg-Gruppe* JW sei definiert durch die Präsentation

$$\left\langle \sigma, \tau, x_0, \ldots, x_N, y, z \;\middle|\; \begin{array}{c} \sigma\tau\sigma^{-1} = \tau^q \\ (x_0\tau)^g = yz \\ [y, z] = 1 \\ \sigma x_0 \sigma^{-1} = z x_1^{p^s} [x_1, x_2] \ldots [x_{N-1}, x_N] \end{array} \right\rangle.$$

Wir definieren ein Prädikat $\mathcal{P}$ normaler Untergruppen N von endlichem Index in JW wie folgt.

($\mathcal{P}$) N erfüllt $\mathcal{P}$, wenn für den Quotienten $\pi_N\colon \mathrm{JW} \to \mathrm{JW}/N$ folgendes gilt.

  (a) Das Bild von $\langle\!\langle x_0, \ldots, x_N \rangle\!\rangle$ unter π_N ist eine p-Gruppe.

  (b) Das Bild von y unter π_N hat Ordnung prim zu p.

Dies beschreibt ein kofiltriertes saturiertes Indexsystem und es gibt einen wohldefinierten Begriff von pro-$\mathcal{P}$-Vervollständigung

$$\mathrm{JW}^{\wedge\mathcal{P}} = \lim_{N \text{ erfüllt } \mathcal{P}} \mathrm{JW}/N.$$

Wir haben folgendes Diagramm

$$\begin{tikzcd}
 & \mathrm{JW}^{\wedge\mathcal{P}} \arrow[dd] \\
\mathrm{JW} \arrow[ur] \arrow[dr] & \\
 & \mathrm{Gal}_K,
\end{tikzcd}$$

in dem der vertikale Pfeil ein Isomorphismus nach den Resultaten von Jannsen–Wingberg–Diekert und der Universalität obiger Konstruktion ist. Wir halten dies für eine natürliche Art, die Darstellung von Jannsen–Wingberg–Diekert zu verstehen.

Sei nun $N \geq 4$. Wir wählen eine Fläche $S = S_g$ mit $2g = N - 2$. Es gibt eine wohldefinierte Abbildung

$$\mathcal{K}_{\mathcal{P}}^{(\delta)} : \qquad \mathrm{Aut}^{(\delta)}(F) \longrightarrow \mathrm{Aut}(\mathrm{Gal}_K).$$

Dies macht es uns möglich, den Automorphismus aus [JW82, §5] als Bild eines kombinatorischen Dehn-Twists zu interpretieren.

Wenn $p \neq 2$ und $\mu_p \subseteq K$, können wir wie im Demuškin-Fall argumentieren, dass $\mathcal{K}_{\mathcal{P}}^{(\delta)}(\mathrm{Dehn}(S))$ eine große Untergruppe von $\mathrm{Out}(\mathrm{Gal}_K)$ ist. Wieder ist dies in folgendem Sinne zu verstehen.

Theorem (Cf. Theorem 7.5.5)**.** *Die Untergruppe* $\mathcal{K}_{\mathcal{P}}^{(\delta)}(\mathrm{Dehn}(S))$ *in* $\mathrm{Out}(\mathrm{Gal}_K)$ *hat dichtes Bild in* $\mathrm{Sp}_{N-2}(\mathbb{Z}_p)$.

Insbesondere liefert dieses Ergebnis eine große untere Schranke für das Bild von $\mathrm{Out}(\mathrm{Gal}_K)$ unter

$$\mathrm{Out}(\mathrm{Gal}_K) \to \mathrm{Out}(\mathrm{Gal}_K(p)) \twoheadrightarrow \mathrm{Aut}^{(-\cup-,\beta)}(H^1(K,\Lambda)).$$

Wir vermuten, dass diese Abbildung surjektiv ist.