View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Scholarship@Western

Western Graduate&PostdoctoralStudies

Western University

Scholarship@Western

Electronic Thesis and Dissertation Repository

5-25-2015 12:00 AM

Combinatorial Techniques in the Galois Theory of p-Extensions

Michael Rogelstad
The University of Western Ontario

Supervisor
Professor Jan Minac
The University of Western Ontario

Graduate Program in Mathematics
A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy
© Michael Rogelstad 2015

Follow this and additional works at: https://ir.lib.uwo.ca/etd

Part of the Algebra Commons

Recommended Citation

Rogelstad, Michael, "Combinatorial Techniques in the Galois Theory of p-Extensions" (2015). *Electronic Thesis and Dissertation Repository*. 2905.
https://ir.lib.uwo.ca/etd/2905

This Dissertation/Thesis is brought to you for free and open access by Scholarship@Western. It has been accepted for inclusion in Electronic Thesis and Dissertation Repository by an authorized administrator of Scholarship@Western. For more information, please contact wlswadmin@uwo.ca.

COMBINATORIAL TECHNIQUES IN THE GALOIS THEORY OF P-EXTENSIONS

(Thesis format: Monograph)

by

Michael L. Rogelstad

Graduate Program in Mathematics

A thesis submitted in partial fulfilment
of the requirements for the degree of
Doctor of Philosophy

The School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

© Michael L. Rogelstad 2015

Abstract

A major open problem in current Galois theory is to characterize those profinite groups which appear as absolute Galois groups of various fields. Obtaining detailed knowledge of the structure of quotients and subgroup filtrations of Galois groups of p-extensions is an important step toward a solution. We illustrate several techniques for counting Galois p-extensions of various fields, including pythagorean fields and local fields. An expression for the number of extensions of a formally real pythagorean field having Galois group the dihedral group of order 8 is developed. We derive a formula for computing the $\mathbb{F}_p$-dimension of an n-th graded piece of the Zassenhaus filtration for various finitely generated pro-p groups, including free pro-p groups, Demushkin groups and their free pro-p products. Several examples are provided to illustrate the importance of these dimensions in characterizing pro-p Galois groups. We also show that knowledge of small quotients of pro-p Galois groups can provide information regarding the form of relations among the group generators.

Keywords: Galois theory, p-extension, pro-p group, absolute Galois group, local field, formally real pythagorean field, Zassenhaus filtration, Demushkin group.

Co-Authorship Statement

Chapters 3, 4 and 5 of this thesis incorporate material that is the result of joint research with Professor Ján Mináč and Dr. Nguyễn Duy Tân. Chapter 4 is based on the paper [MRT15]:

> Dimensions of Zassenhaus Filtration Subquotients of Some Pro-p Groups, *arXiv:1405.6980v2*, Mar 2015,

which is to appear in the Israel Journal of Mathematics.

Acknowledgements

I would like to extend a most sincere thank you to my supervisor, Professor Ján Mináč, for the opportunity to pursue this research, for many interesting and valuable discussions and for his constant encouragement, enthusiastic assistance and unending patience in seeing this work to completion. My friend and colleague Dr. Nguyễn Duy Tân provided a tremendous amount of help along the way and for all of his efforts I am also exceedingly grateful. This thesis would not have been possible without the kind and generous assistance of these two extraordinary mathematicians.

I very much appreciate the helpful suggestions and guidance provided by supervisory committee members, Professors Dan Christensen and Nicole Lemire, and examiners, Professors Tatyana Barron, Sunil Chebolu, Masoud Khalkhali and Marc Moreno Maza. A special thank you to Professor Chebolu for making the trip to London, Ontario for my thesis examination and for subsequent discussions regarding the thesis material which I found very useful and encouraging. I would like to thank Janet Williams for her kind help with various administrative tasks over the past few years.

My thanks are also extended to the faculty of the Department of Mathematics for many excellent courses and seminars. I owe a particular debt of gratitude to Professor Stuart Rankin and the late Professors Richard Kane and André Boivin. Dedicated and outstanding teachers, they were an early source of inspiration leading to my pursuit of graduate studies in mathematics.

And last but not least, to my family, for the many sacrifices and unwavering support that made this fascinating journey possible, I will be forever grateful.

Contents

Abstract **ii**

Co-Authorship Statement **iii**

Acknowledgements **iv**

1 Introduction **1**

2 Background **6**
2.1 Profinite Groups 6
2.1.1 Pro-p groups 8
2.1.2 Completed group algebras 11
2.1.3 Filtrations 12
2.2 Galois Cohomology 16
2.2.1 Cohomology of profinite groups 16
2.2.2 The lower dimensional cohomology groups 21
2.3 Central Simple Algebras and the Brauer Group 26
2.4 Quadratic Forms and Quaternion Algebras 29
2.5 The Incidence Algebra and Möbius Functions 36

3 Counting Galois p-Extensions **43**
3.1 The Inverse Galois Problem 44
3.2 Dihedral Extensions and W-Groups 46
3.3 Local Fields 48
3.3.1 Constructing extensions 48
3.3.2 A group-theoretic approach 50
3.3.3 Quaternion algebras 51
3.3.4 Complex characters and Möbius functions 53
3.3.5 Cup products in cohomology 59
3.4 Formally Real Pythagorean Fields 68
3.4.1 Extensions of SAP fields 71
3.4.2 The group $G_F(2)$ 75

4 Dimensions of Zassenhaus Filtration Subquotients **79**
4.1 The Hilbert-Poincaré Series 80
4.2 Free Pro-p Groups 88

4.3 Free Products of Cyclic Groups 95
4.3.1 Free products of cyclic groups of order 2 96
4.3.2 Free products of cyclic groups of order 2 as semidirect products . 96
4.4 Another Semidirect Product 100
4.5 Demushkin Groups 103
4.6 Some Other Groups 105
4.6.1 Free products of a finite number of Demushkin groups and free pro-p-groups 105
4.6.2 A free product of a cyclic group of order 2 and a free pro-2-group 106
4.6.3 A free product of a cyclic group of order p and a free pro-p-group 106

5 Relations in Pro-p Galois Groups **108**
5.1 The Case $\zeta_{p^2} \in F$ 109
5.2 The Case $\zeta_p \in F,\ \zeta_{p^2} \notin F$ 110

6 Conclusion **113**

Bibliography **115**

Curriculum Vitae **120**

Chapter 1

Introduction

Nearly 200 years after his untimely death in a duel at the age of 20, the legacy of Évariste Galois lives on in the theory that bears his name. While remarkable progress has certainly been made, a number of open questions remain. One major problem is, given a field F with separable closure F_s, to characterize, among other profinite groups, the absolute Galois group $G_F := \mathrm{Gal}(F_s/F)$ of F. One means of approaching this question is to study the structure of subgroups and quotients of certain profinite groups. Such fundamental problems in current Galois theory also have important implications in other areas of mathematics. For example, knowing how much information Galois groups carry about base fields is closely related to the problem in algebraic geometry of determining how much information about algebraic varieties is contained in the knowledge of fundamental groups.

Given a prime p, one can consider the Galois group $G_F(p)$ of the maximal p-extension of F. This is a pro-p group which is the maximal pro-p quotient of G_F. To shed some light on the structure of this group, one can then ask whether, for a given pro-p group G, there exists a normal extension K/F with Galois group isomorphic to G. This is the inverse Galois problem and the solution is closely related to properties of the base field F. The next question which naturally arises is to determine the number of such extensions.

Similarly, the structure of subgroups, particularly certain central subgroup filtrations, of profinite groups has a close connection with Galois theory. For example, in 1947, I. R. Shafarevich [Sha47] showed that $G_F(p)$, for local fields F not containing a primitive p-th

root of unity, was a free pro-p group simply by determining the cardinality of some of its filtration quotients. Zassenhaus filtrations of groups were introduced in [Zas40] and, in the case of absolute Galois groups, these filtrations and their subquotients have recently been investigated in [CEM12, Efr14b, Efr14a, EM11a, MT13, MT15]. Other filtrations of absolute Galois groups, such as the descending p-central series, are also of interest (see, for example, [Lab70, EM11b]).

Our focus is on the Galois theory of p-extensions, which are Galois extensions K/F of a base field F whose Galois group is a pro-p group, and our goal here is twofold. First, we endeavour to illustrate several methods for counting finite p-extensions. We compare these methods to show that, by employing various algebraic tools, one can develop relatively efficient counting techniques. Our second goal, and main result, is to develop a method for determining the $\mathbb{F}_p$-dimension of subquotients of the Zassenhaus filtration of finitely generated pro-p groups. We derive an explicit formula for these dimensions in a number of specific cases and point out several examples of their importance in the Galois theory of p-extensions.

These various techniques are dependent upon results from a broad range of subjects, including Galois cohomology, the theory of quadratic forms and quaternion algebras, and the general theory of Möbius functions. The necessary background is presented in the next chapter. We begin that chapter with an overview of the theory of profinite groups and discuss several results that will be needed in the study of filtration quotients in chapter 4. For example, in section 2.1.3 the descending q-central series and the Zassenhaus p-filtrations are defined and the connections between filtrations of a finitely generated pro-p group G and the structure of both the completed group algebra $\mathbb{F}_p[[G]]$ of G and the Magnus algebra with coefficients in $\mathbb{F}_p$ are described. These connections are important in developing the technique for counting $\mathbb{F}_p$-dimensions of Zassenhaus filtration subquotients in section 4.1.

In chapter 3 we turn to the problem of counting Galois p-extensions of a field F. Beginning with the case $p = 2$, we point out the connection between a small quotient of the group $G_F(2)$, called the W-group of F, and the number of Galois extensions of F having Galois group isomorphic to the dihedral group D_4 of order 8, which are referred to as

D_4-extensions. The W-group is the quotient $G_F^{[3]} = G_F/G_F^{(3)}$ in the descending 2-central series $(G_F^{(i)})_{i\geq 1}$ of G_F, and is considered a Galois-theoretic analog of the cohomology ring $H^*(G_F, \mathbb{F}_2)$ [CEM12, MS96]. This further suggests that enumerating p-extensions and filtration quotient dimensions can play an important role in elucidating the structure of absolute Galois groups.

We first consider the case of p-extensions of local fields. Section 3.3.1 describes the method of directly constructing D_4-extensions of the field of p-adic numbers, $\mathbb{Q}_p$, for both p odd and $p = 2$, due to H. Naito [Nai95]. In the proof of Proposition 3.3.1, we illustrate an alternative, group-theoretic approach based on knowledge of the W-group of $\mathbb{Q}_p$ and in section 3.3.3 we outline an approach based on the theory of quaternion algebras over $\mathbb{Q}_p$.

Turning, in section 3.3.4, to the more general case of a local field K which is a finite extension of $\mathbb{Q}_p$, we describe an interesting method of counting p-extensions of K using Möbius functions and complex characters, due to M. Yamagishi [Yam95] which relies on lemma 2.5.6 from the general theory of Möbius functions. In example 3.3.3, we show that if K does not contain a primitive p-th root of unity, this method can be used to obtain an earlier result of Shafarevich [Sha47]. The case in which K is a finite extension of $\mathbb{Q}_2$ of odd degree not containing a primitive 4-th root of unity is shown in detail in example 3.3.6. This example illustrates that the method produces a simple expression for the number of D_4-extensions of K which depends only on n, but requires detailed knowledge of the classification of Demushkin groups as well as the complex character theory of D_4 and all of its subgroups.

In section 3.3.5, we assume that K is a finite extension of $\mathbb{Q}_p$ containing a primitive p-th root of unity and develop a method based on Galois cohomology and the solution of embedding problems to count the number of $\mathbb{U}_3(\mathbb{F}_p)$-extensions of K, where $\mathbb{U}_3(\mathbb{F}_p)$ is the group of unipotent three by three matrices over $\mathbb{F}_p$. This is the 'cup product analogue' of a technique using Massey products to compute the number of $\mathbb{U}_4(\mathbb{F}_p)$-extensions of K developed by J. Mináč and N. D. Tân [MT14]. Since $D_4 \cong \mathbb{U}_3(\mathbb{F}_2)$, this provides another method of enumerating the D_4-extensions of certain local fields.

We introduce the theory of formally real pythagorean fields in section 3.4 and use

properties of the set of orderings, cup products and quaternion algebras to derive an expression for the number of D_4-extensions of a formally real pythagorean SAP field F with finite square class group $F^\times/(F^\times)^2$. We also characterize the group $G_F(2)$ for both pythagorean SAP fields and superpythagorean fields. The structure of these groups is then studied further in chapter 4.

The main results appear in chapter 4. We introduce the Hilbert-Poincaré series and define $c_n(G)$ to be the $\mathbb{F}_p$ dimension of the n-th graded piece $G_{(n)}/G_{(n+1)}$ of the Zassenhaus filtration of a finitely generated pro-p group G. Using a beautiful theorem of Jennings and Lazard, we develop an explicit formula for $c_n(G)$ for various families groups G, including finitely generated free pro-p-groups, Demushkin groups, and free pro-2 products of finitely many copies of the cyclic group C_2 of order 2. In Proposition 4.1.14, we point out a relationship between $c_n(G)$ and the $\mathbb{Z}_p$-rank of the n-th graded piece of the descending central series of G.

Section 4.2 deals with free pro-p groups. The Magnus homomorphism introduced in Theorem 2.1.25 allows us, in Lemma 4.2.1, to characterize a finitely generated free pro-p group by its Hilbert-Poincaré series and in Remark 4.2.4, we show that determining finitely generated free pro-p groups within the family of all Galois groups of the maximal p-extensions of fields containing a primitive p-th root of unity actually requires only the two numbers, $c_1(G)$ and $c_2(G)$. We observe also that, for a free pro-p group S, the numbers $c_n(S)$ determine the minimal number of generators of the Zassenhaus subgroups of S and we give an explicit $\mathbb{F}_p$-basis for $S_{(n)}/S_{(n+1)}$, for each n in terms of Hall commutators. In Lemma 4.2.12 and Corollary 4.2.13, we again meet the group $\mathbb{U}_n(\mathbb{F}_p)$ and provide an interesting, purely group theoretical result based on the formula for $c_n(S)$.

Following up on the characterization of the Galois groups of maximal p-extensions of pythagorean fields given in section 3.4.2, we study, in section 4.3, groups G which are free products of a finite number of cyclic groups of order 2. We show that each such group G contains a free pro-2 subgroup H of index 2 and in Corollary 4.3.5 we obtain, for each $n \geq 2$, the interesting relation $H_{(n)} = H \cap G_{(n)}$ using knowledge of the numbers $c_n(G)$ and $c_n(H)$. In Remarks 4.4.4 we observe that $c_1(G_F(2))$ and $c_2(G_F(2))$ are sufficient to determine the group $G_F(2)$ if F is either a pythagorean SAP field or a superpythagorean

field. These examples illustrate the fact that the numbers $c_n(G)$ can be very useful in group theory and Galois theory.

We conclude chapter 4 by looking at Demushkin groups as well as some other groups. We observe again that, for a Demushkin group G, the numbers $c_n(G)$ determine the minimal number of generators of the Zassenhaus subgroups of G.

Finally in chapter 5, we consider relations among the generators of finitely generated pro-p Galois groups and show that knowledge of small quotients of these groups can be useful in determining the form of these relations.

The following is a list of the theorems/propositions/lemmas/corollaries which constitute the main results of this thesis: 3.4.10, 3.4.12, 3.4.15, 4.1.13, 4.1.14, 4.2.1, 4.2.9, 4.2.13, 4.3.3, 4.3.4, 4.3.5, 4.4.1, 5.1.2, 5.2.1.

Chapter 2

Background

In this chapter we review some of the basic theory of profinite groups and introduce the tools that will be needed in subsequent chapters. We outline a connection between central filtrations of profinite groups and filtrations of completed group algebras which will be important in developing a technique for computing filtration subquotient dimensions in chapter 4. Galois cohomology as well as the theories of quaternion algebras and quadratic forms lead to interesting methods for counting Galois p-extensions. We review the pertinent background and relevant connections as a prelude to illustrating several combinatorial techniques in chapter 3. Many problems of enumeration, including those that we study in chapters 3 and 4, are closely related to the theory of Möbius functions. The final section of this chapter outlines that general theory.

2.1 Profinite Groups

Definition 2.1.1. A *profinite group* is a compact Hausdorff topological group whose open subgroups form a neighbourhood basis at the identity.

There are several other equivalent definitions, the most important of which is based on the concept of an *inverse* (or *projective*) *limit*. We briefly outline this construction. A *directed set* is a non-empty partially ordered set $(\Lambda, \leq)$ such that for every $\lambda, \mu \in \Lambda$ there exists $\nu \in \Lambda$ with $\nu \geq \lambda$ and $\nu \geq \mu$. An *inverse system* of groups over Λ is a family of groups $(G_\lambda)_{\lambda \in \Lambda}$ together with homomorphisms $\pi_{\lambda\mu} \colon G_\lambda \to G_\mu$ whenever $\lambda \geq \mu$,

satisfying the conditions

$$\pi_{\lambda\lambda} = \mathrm{Id}_{G_\lambda} \quad \text{and} \quad \pi_{\lambda\nu} = \pi_{\mu\nu}\pi_{\lambda\mu} \text{ whenever } \lambda \geq \mu \geq \nu.$$

The *inverse limit*

$$\varprojlim G_\lambda = \varprojlim (G_\lambda)_{\lambda\in\Lambda}$$

is the subgroup of the direct product $\prod_{\lambda\in\Lambda} G_\lambda$ consisting of all elements $(g_\lambda)_{\lambda\in\Lambda}$ such that $\pi_{\lambda\mu}(g_\lambda) = g_\mu$ whenever $\lambda \geq \mu$. An analogous construction can also be applied to other structures such as sets, rings or topological spaces.

A profinite group can then be defined as a topological group that can be realized as an inverse limit of finite groups endowed with the discrete topology. It can be shown (see, for example [DSMS99, Proposition 1.3]) that these two definitions are equivalent.

Example 2.1.2.

1. Given a group G, let Λ be the set of all normal subgroups of finite index in G, directed by reverse inclusion. Then the family of quotients $(G/N)_{N\in\Lambda}$ forms an inverse system of finite groups. The inverse limit

$$\hat{G} = \varprojlim (G/N)_{N\in\Lambda}$$

is a profinite group, called the *profinite completion* of G.

2. Profinite groups arise in this way as the Galois groups of algebraic field extensions. If K/F is a Galois extension, its Galois group

$$\mathrm{Gal}(K/F) \cong \varprojlim \mathrm{Gal}(M/F)_{M\in\Gamma},$$

where Γ is the set of all finite Galois sub-extensions M/F of K/F. In the case that $K = F_s$ is the separable closure of F, then $G_F := \mathrm{Gal}(F_s/F)$ is the *absolute Galois group* of F.

3. If F is a finite field with algebraic closure $\bar{F}$, then $\mathrm{Gal}(\bar{F}/F) \cong \hat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$.

2.1.1 Pro-p groups

Definition 2.1.3. Let p be a prime number. A *pro-p group* is a profinite group in which every open normal subgroup has index equal to some power of p.

In an analogous way to the case of profinite groups, it can be shown that a topological group G is a pro-p group if and only if G is topologically isomorphic to an inverse limit of finite p-groups.

Example 2.1.4.

1. Given a group G, let Λ be the set of all normal subgroups of G whose index is a power of p, directed by reverse inclusion. Then

$$\hat{G}_p = \varprojlim (G/N)_{N\in\Lambda}$$

is a pro-p group, called the *pro-p completion* of G.

2. Historically, the subject began with what is regarded as the prototype of all pro-p groups, the additive group of p-adic integers,

$$\mathbb{Z}_p = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}} = \{(x_n)_{n\in\mathbb{N}} \mid x_i \equiv x_j (\mathrm{mod} p^j) \text{ if } i \geq j\}$$

3. The *maximal p-extension* $F(p)$ of a field F is the compositum of all finite Galois sub-extensions K/F of F_s/F with $[K : F]$ a power of p. The group $G_F(p) = \mathrm{Gal}(F(p)/F)$ is the maximal pro-p quotient of the absolute Galois group G_F of F.

Definition 2.1.5. Let G be a pro-p group. A *system of generators* of G is a subset X of G with the following properties:

1. G is the smallest (closed) subgroup containing X;
2. every neighbourhood of the identity in G contains almost all (i.e. all but finitely many) elements of X.

Definition 2.1.6. A system X of generators of the pro-p group G is called *minimal* if no proper subset of X is a system of generators of G. The cardinality of a minimal system

of generators of G will be denoted $d(G)$ and is often referred to as the *rank* of G. G is said to be *finitely generated* if $d(G) < \infty$.

Definition 2.1.7. Let G be a profinite group. The *Frattini subgroup* of G is

$$\Phi(G) = \cap\{M \mid M \text{ is a maximal proper open subgroup of } G\}.$$

The Frattini subgroup plays an important role in the study of pro-p groups. In particular, we have

Theorem 2.1.8 (Burnside's Basis Theorem)**.** *Let G be a pro-p group and $X = \{x_i \mid i \in I\}$ a subset of G such that every neighbourhood of $1 \in G$ contains almost all elements of X. Then X is a system of generators of G if and only if $\{x_i\Phi(G) \mid i \in I\}$ generates $G/\Phi(G)$.*

Proof. See [Koc02, Theorem 4.10]. □

We will be primarily interested in finitely generated pro-p groups and in this case we have the following useful results.

Proposition 2.1.9. *If G is a pro-p group then G is finitely generated if and only if $\Phi(G)$ is open in G.*

Proof. See [DSMS99, Proposition 1.14]. □

Theorem 2.1.10 (Serre)**.** *If G is a finitely generated pro-p group then every subgroup of finite index in G is open.*

Proof. See [DSMS99, Theorem 1.17]. □

Corollary 2.1.11. *If G is a finitely generated pro-p group then $\Phi(G) = G^p[G, G]$, where $[G, G]$ is the subgroup generated by commutators $g^{-1}h^{-1}gh$ with $g, h \in G$, and $G^p =< g^p \mid g \in G >$.*

Proof. See [DSMS99, Corollary 1.20]. □

Note that $G/G^p[G,G]$ is an $\mathbb{F}_p$-vector space, so if G is a finitely generated pro-p group, then $d(G) = \dim_{\mathbb{F}_p}(G/\Phi(G))$.

Corollary 2.1.12. *The topology of a finitely generated pro-p group is determined by its group structure.*

Proof. See [DSMS99, Corollary 1.21]. □

An important method of describing a pro-p group is via a presentation by generators and relations.

Definition 2.1.13. Let I be an index set and let S_I be the free discrete group on the generators $\{s_i \mid i \in I\}$. Let $\mathfrak{N}$ be the set of normal subgroups N of S_I such that:

1. S_I/N is a finite p-group;

2. N contains almost all elements of $\{s_i \mid i \in I\}$.

Then $\{S_I/N \mid N \in \mathfrak{N}\}$ is an inverse system and $S(I) = \varprojlim(S_I/N)_{N\in\mathfrak{N}}$ is a pro-p group called the *free pro-p group with system of generators* $\{s_i \mid i \in I\}$.

When $I = \{1, \ldots, n\}$ one often writes $S(n)$ instead of $S(I)$ and refers to $S(n)$ as the *free pro-p group of rank n.*

Definition 2.1.14. Let G be a pro-p group. An exact sequence

$$1 \longrightarrow R \longrightarrow S \xrightarrow{\varphi} G \longrightarrow 1,$$

where S is a free pro-p group with system of generators $\{s_i \mid i \in I\}$ is called a *presentation* of G by S.

If $\{\varphi(s_i) \mid i \in I\}$ is a minimal system of generators of G, then the presentation is called *minimal.*

A subset $E \subseteq R$ is called a *system of relations* of G if

1. R is the smallest closed normal subgroup of S containing E;

2. every open normal subgroup of R contains almost all elements of E.

We say E is *minimal* if no subset of E is a system of relations for G.

Example 2.1.15. Demushkin groups (see Definition 3.3.4) are an interesting example of finitely generated pro-p groups having only a single relation among a minimal system of generators. These groups play an important role in the Galois theory of local fields and we will have much more to say about them in subsequent chapters.

2.1.2 Completed group algebras

In order to study the structure of pro-p groups in greater detail, we introduce two related objects; the completed group algebra of a pro-p group and the Magnus algebra.

Let Λ be a compact commutative ring with identity, let G be a profinite group and let $\mathfrak{N}_G$ be the set of all open normal subgroups of G. For $N, N' \in \mathfrak{N}_G$ with $N \supseteq N'$ the natural map

$$G/N' \longrightarrow G/N$$

induces an epimorphism

$$\Lambda[G/N'] \longrightarrow \Lambda[G/N]$$

of group algebras. These maps define an inverse system $\{\Lambda[G/N] \mid N \in \mathfrak{N}_G\}$ of compact rings.

Definition 2.1.16. The *completed group algebra* $\Lambda[[G]]$ of the profinite group G over the compact ring Λ is the inverse limit of the system $\{\Lambda[G/N] \mid N \in \mathfrak{N}_G\}$.

By the map

$$g \longmapsto \prod_{N \in \mathfrak{N}_G} gN,$$

G embeds into $\Lambda[[G]]$ and the subring $\Lambda[G]$, which is given the subspace topology, is dense in $\Lambda[[G]]$.

Theorem 2.1.17. *(i) Let A be a compact Λ-algebra. Every morphism $\phi\colon G \to A^\times$ from G into the group of units $A^\times$ of A can be extended uniquely to a morphism $\Lambda[[G]] \to A$.*

(ii) Let $\phi\colon G \to G'$ be a morphism of profinite groups with kernel N. The kernel of the induced morphism $\Lambda[[G]] \to \Lambda[[G']]$ is the closed ideal I(N) generated by $\{h - 1 \mid h \in N\}$.

Proof. See [Koc02, Theorem 7.2]. □

Theorem 2.1.18. *Let Λ be a finite ring and G a profinite group. The system $\{I(N) \mid N \in \mathfrak{N}_G\}$ is a neighbourhood basis at $0 \in \Lambda[[G]]$.*

Proof. See [Koc02, Theorem 7.3]. □

Definition 2.1.19. Let K be a commutative ring with identity, let I be an index set and let $U = \{u_i \mid i \in I\}$. The *Magnus algebra* $K\langle\langle U\rangle\rangle$ is the associative algebra of formal power series in the non-commuting indeterminates u_i, $i \in I$, with coefficients in K.

Let $\mathcal{I}$ be the ideal of $K\langle\langle U\rangle\rangle$ consisting of all formal power series having constant term 0. If $u \in \mathcal{I}$, then $1 + u$ is invertible and

$$(1+u)^{-1} = 1 - u + u^2 - u^3 + \ldots + (-1)^n u^n + \ldots$$

The invertible elements $1 + u_i$ generate a subgroup of the group of units of $K\langle\langle U\rangle\rangle$. This group is the image of the free group S_I under the homomorphism $\psi\colon S_I \to K\langle\langle U\rangle\rangle^\times$ given by $s_i \mapsto 1 + u_i$ and is referred to as the *Magnus group*.

Lemma 2.1.20. *The map ψ is injective.*

Proof. See [Koc02, Lemma 4.4]. □

Identifying S_I with its image in $K\langle\langle U\rangle\rangle$, we have $s_i = 1 + u_i$ and if $s \in S_I, s \neq 1$, we have $s = 1 + u$ with $u \in \mathcal{I}^n, u \notin \mathcal{I}^{n+1}$, for some $n \geq 1$. Magnus called n the *dimension* of s.

2.1.3 Filtrations

In attempting to elucidate the structure of Galois groups, the study of certain filtrations can be very useful. We are particularly interested in filtrations of pro-p groups and the corresponding filtrations on the completed group algebra and the Magnus algebra.

Let G be a group. A *central filtration* (or *central series* or *central sequence*) of G is a sequence $(G_n)_{n\geq 1}$ of subgroups of G such that

$$G_1 = G, \qquad G_{i+1} \leq G_i, \qquad [G_i, G_j] \leq G_{i+j},$$

where $[H, K]$ denotes the subgroup of G generated by the commutators $[h, k] = h^{-1}k^{-1}hk$ with $h \in H$, $k \in K$. The name arises from the fact that for any such filtration and any $i \geq 1$, $G_i \trianglelefteq G$ and G_i/G_{i+1} lies in the centre of G/G_{i+1}.

Let G be a profinite group and let q be either a p-power or 0. The *descending* (or *lower*) *q-central series* $(G^{(n,q)})_{n\geq 1}$ of G is defined inductively by

$$G^{(1,q)} = G, \qquad G^{(i+1,q)} = (G^{(i,q)})^q[G^{(i,q)}, G], \quad i = 1, 2, \ldots,$$

where, given closed subgroups H and K of G, $[H, K]$ (respectively H^q, HK) denotes the closed subgroup topologically generated by all commutators $[h, k]$ (respectively q-th powers, products hk) with $h \in H$, $k \in K$. Note that $G^{(i,q)}$ is normal in G. For $i \geq 1$, let $G^{[i,q]} = G/G^{(i,q)}$. If q is understood, we generally abbreviate

$$G^{(i)} = G^{(i,q)}, \qquad G^{[i]} = G^{[i,q]}.$$

When $q = 0$ the series $G^{(i,0)}$ is called the *descending* (or *lower*) *central series* of G. In this case we will adopt the commonly used notation

$$G_i = G^{(i,0)}.$$

We can define another central filtration $(G_{(n)})_{n\geq 1}$ on the profinite group G by

$$G_{(1)} = G, \qquad G_{(n)} = G^p_{(\lceil n/p \rceil)} \prod_{i+j=n} [G_{(i)}, G_{(j)}], \quad n = 2, 3, \ldots,$$

where p is a fixed prime and $\lceil n/p \rceil$ is the least integer r such that $pr \geq n$. Then $[G_{(i)}, G_{(j)}] \leq G_{(i+j)}$ and $G^p_{(i)} \leq G_{(pi)}$ for all $i, j \geq 1$ and $(G_{(n)})_{n=1,2,\ldots}$ is the fastest

descending sequence of closed subgroups of G having these properties. This sequence is the *Zassenhaus p-filtration* of G. For quotients we again adopt the notation $G_{[i]} = G/G_{(i)}$. We will usually be considering the Zassenhaus p-filtration of a pro-p group G and will often refer to this simply as the *Zassenhaus filtration* of G.

We now turn our attention to the special case in which G is a finitely generated pro-p group and look at the connections between the filtrations of G and the structure of both the completed group algebra $\mathbb{F}_p[[G]]$ of G and the Magnus algebra with coefficients in $\mathbb{F}_p$.

Definition 2.1.21. The *augmentation ideal* $I(G)$ of $\mathbb{F}_p[[G]]$ is the closed two-sided ideal generated by the elements $g - 1$, $g \in G$ and $I^n(G)$ is the closure of the n-th power of $I(G)$ in $\mathbb{F}_p[[G]]$.

Theorem 2.1.22. *Let G be a finitely generated pro-p group. Then $\{I^n(G) \mid n = 1, 2, \ldots\}$ is a neighbourhood basis at $0 \in \mathbb{F}_p[[G]]$.*

Proof. See [Koc02, Theorem 7.8]. □

There is a close relationship between the filtration $I^n(G)$ of $\mathbb{F}_p[[G]]$ and the Zassenhaus p-filtration $G_{(n)}$ of G.

Theorem 2.1.23. *Let G be a finitely generated pro-p group and $I(G)$ the augmentation ideal of $\mathbb{F}_p[[G]]$. Then*

$$G_{(n)} = (1 + I^n(G)) \cap G, \qquad n \geq 1$$

Proof. Since the topology of a finitely generated pro-p group is determined by its group structure, the result follows from [DSMS99, Theorem 12.9]. □

So for each $n \geq 1$, $G_{(n)}$ is the kernel of the natural homomorphism of G into the group of units of $\mathbb{F}_p[[G]]/I^n(G)$; that is,

$$G_{(n)} = \{g \mid g - 1 \in I^n(G)\}.$$

Remark 2.1.24. In view of this theorem, the Zassenhaus filtration has also been referred to as the dimension series, with the subgroups $G_{(n)}$ being called the dimension subgroups in characteristic p.

Now let $U = \{u_1, \ldots, u_d\}$ and consider the Magnus algebra $\mathbb{F}_p\langle\langle U\rangle\rangle$. Let $\mathcal{I}^n$ denote the ideal of all power series in $\mathbb{F}_p\langle\langle U\rangle\rangle$ whose homogeneous components have degree at least n. Then $\mathcal{I}^n/\mathcal{I}^{n+1}$ is the submodule of $\mathbb{F}_p\langle\langle U\rangle\rangle$ generated by the monomials of degree n. Also, $\{\mathcal{I}^n \mid n = 1, 2, \ldots\}$ is a basis of open neighbourhoods of $0 \in \mathbb{F}_p\langle\langle U\rangle\rangle$ and with this topology, $\mathbb{F}_p\langle\langle U\rangle\rangle$ is the direct product of its homogeneous components, $\mathcal{I}^n/\mathcal{I}^{n+1}$, hence compact.

Let $S = S(d)$ be the free pro-p group with system of generators $\{s_1, \ldots, s_d\}$. We have the Magnus embedding $S \hookrightarrow \mathbb{F}_p\langle\langle U\rangle\rangle^\times$ given by $s_i \mapsto 1 + u_i$, $i = 1, \ldots, d$. Furthermore, we have

Theorem 2.1.25. *The map*

$$s_i \longmapsto 1 + u_i, \qquad i = 1, \ldots, d,$$

can be extended to an isomorphism $\mathbb{F}_p[[S]] \cong \mathbb{F}_p\langle\langle U\rangle\rangle$.

Proof. See [Koc02, Theorem 7.16]. □

Identifying $\mathbb{F}_p\langle\langle U\rangle\rangle$ and $\mathbb{F}_p[[S]]$, we then have

Theorem 2.1.26. *Let G be a finitely generated pro-p group with presentation*

$$1 \longrightarrow R \longrightarrow S \longrightarrow G \longrightarrow 1.$$

Let $\{r_i \mid i \in I\}$ be a system of relations with respect to this presentation. Then the kernel of the induced map $\mathbb{F}_p[[S]] \to \mathbb{F}_p[[G]]$ is generated as an ideal of $\mathbb{F}_p[[S]]$ by $\{r_i - 1 \mid i \in I\}$.

Proof. See [Koc02, Theorem 7.17]. □

Hence we have the following commutative diagram:

$$\begin{tikzcd}
S \arrow[r] \arrow[d] & \mathbb{F}_p\langle\langle U\rangle\rangle \arrow[dd] \\
G \arrow[d] & \\
\mathbb{F}_p[[G]] \arrow[r] & \mathbb{F}_p\langle\langle U\rangle\rangle/J
\end{tikzcd}$$

where J is the ideal of $\mathbb{F}_p\langle\langle U\rangle\rangle$ generated by the set $\{r_i \mid i \in I\}$ and all other maps are defined in the obvious way.

2.2 Galois Cohomology

Given a field F and a Galois extension K/F with Galois group $G = \mathrm{Gal}(K/F)$, the cohomology groups $H^n(G, A)$, where A is a G-module, often contain important arithmetic information. The study of these groups is referred to as Galois cohomology. Since Galois groups are profinite groups, we begin by looking at the more general case of the cohomology of profinite groups. Subsequently, we look in more detail at the groups $H^n(G, A)$ for $n = 0, 1, 2$ and consider some specific choices of G and A which will be of interest in the chapters that follow.

2.2.1 Cohomology of profinite groups

Let G be a profinite group and A a discrete G-module. An (inhomogeneous) *n-cochain* of G with coefficients in A is a continuous function $y : G^n \to A$. The set of all such functions is an abelian group denoted $C^n(G, A)$ and these groups form a complex

$$C^0(G, A) \xrightarrow{d^1} C^1(G, A) \xrightarrow{d^2} C^2(G, A) \longrightarrow \cdots,$$

where the coboundary operator $d^{n+1} : C^n(G, A) \to C^{n+1}(G, A)$ is given by

$$\begin{aligned}(d^{n+1}y)(g_1, \ldots, g_{n+1}) = {} & g_1 y(g_2, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i y(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\ & + (-1)^{n+1} y(g_1, \ldots, g_n)\end{aligned}$$

for $y \in C^n(G, A)$ and $n \geq 0$. The group of *n-cocycles* is

$$Z^n(G, A) := \ker(C^n(G, A) \xrightarrow{d^{n+1}} C^{n+1}(G, A)).$$

The group of *n-coboundaries* is the subgroup of $Z^n(G, A)$ defined by

$$B^n(G, A) := \mathrm{im}(C^{n-1}(G, A) \xrightarrow{d^n} C^n(G, A))$$

with $B^0(G, A) := 0$. Then, for $n \geq 0$, the quotient group $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ is the *n-dimensional cohomology group* of G with coefficients in A.

If $f : A \to B$ is a G-module homomorphism, then we have the induced homomorphism

$$f : C^n(G, A) \to C^n(G, B), \quad x(g_1, \ldots, g_n) \mapsto fx(g_1, \ldots, g_n)$$

and the commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r] & C^n(G, A) \arrow[r, "d^{n+1}"] \arrow[d, "f"] & C^{n+1}(G, A) \arrow[r] \arrow[d, "f"] & \cdots \\
\cdots \arrow[r] & C^n(G, B) \arrow[r, "d^{n+1}"] & C^{n+1}(G, B) \arrow[r] & \cdots .
\end{tikzcd}$$

So $f : A \to B$ induces a homomorphism $f : C^\bullet(G, A) \to C^\bullet(G, B)$ of complexes and hence we obtain homomorphisms $f : H^n(G, A) \to H^n(G, B)$.

In addition, using the Snake lemma of homological algebra, one can show (see for example [NSW08, §1.3]) that every exact sequence $0 \to A \to B \to C \to 0$ of G-modules gives rise to a canonical *connecting homomorphism*

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

and we obtain the *long exact cohomology sequence*

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^n(G, A) \longrightarrow H^n(G, B) \longrightarrow H^n(G, C) \xrightarrow{\delta} H^{n+1}(G, A) \longrightarrow \cdots .$$

There are also several important maps between cohomology groups involving a "change of groups" rather than a "change of modules". Given two profinite groups G and G', a

G-module A, a G'-module A', we say that two homomorphisms

$$f : A \to A', \quad \varphi : G' \to G$$

are a *compatible pair* if $f(\varphi(g')a) = g'f(a)$ for $g' \in G'$, $a \in A$. From such a pair of homomorphisms we obtain a homomorphism

$$C^n(G, A) \to C^n(G', A'), \quad a \mapsto f \circ a \circ \varphi.$$

This commutes with d and hence induces a homomorphism of cohomology groups

$$H^n(G, A) \to H^n(G', A').$$

Example 2.2.1. Let H be a closed normal subgroup of G and A a G-module. Then A^H is a G/H-module. The projection and injection

$$G \twoheadrightarrow G/H, \quad A^H \hookrightarrow A$$

form a compatible pair of homomorphisms, which induce the *inflation* homomorphism

$$inf : H^n(G/H, A^H) \to H^n(G, A),$$

given by

$$(inf\ x)(g_1, \ldots, g_n) = x(\bar{g_1}, \ldots, \bar{g_n}), \quad g_i \in G,$$

where the image of $g \in G$ in G/H is denoted $\bar{g}$.

Example 2.2.2. For an arbitrary closed subgroup H of G, the G-module A is also an H-module. The compatible homomorphisms

$$H \hookrightarrow G, \quad id : A \to A$$

induce the *restriction* homomorphism

$$res : H^n(G, A) \to H^n(H, A),$$

given by

$$(res\ x)(h_1, \ldots, h_n) = x(h_1, \ldots, h_n), \quad h_i \in H.$$

If H is an open subgroup of G, then in addition to the restriction, we have a map in the opposite direction called the *corestriction*

$$cor : H^n(H, A) \to H^n(G, A).$$

This is a kind of norm map and for $n = 0$, is the usual norm map

$$N_{G/H} : A^H \to A^G, \quad a \mapsto \sum_{\sigma \in G/H} \sigma a.$$

One of the main properties of the corestriction map is that $cor \circ res = [G : H]$.

We also have a bilinear map defined on the cohomology groups of G which plays an important role in Galois cohomology. It arises as follows. Let $A,\ B,\ C$ be G-modules and suppose there exists a continuous bilinear map $A \times B \to C$, $(a, b) \mapsto a \cdot b$, such that $g(a \cdot b) = (ga) \cdot (gb)$ for $g \in G,\ a \in A,\ b \in B$. For any pair $p,\ q \geq 0$, we can define a bilinear map, called the *(cochain) cup product*

$$\cup : C^p(G, A) \times C^q(G, B) \to C^{p+q}(G, C)$$

by

$$(x \cup y)(g_1, \ldots, g_p, h_1, \ldots, h_q) = x(g_1, \ldots, g_p) \cdot g_1 g_2 \ldots g_p y(h_1, \ldots, h_q).$$

For this map, we have the formula

$$d(x \cup y) = dx \cup y + (-1)^p x \cup dy.$$

It follows that if x and y are cocycles then $x \cup y$ is a cocycle, and if one of the cochains

x and y is a coboundary and the other a cocycle, then $x \cup y$ is a coboundary. Hence we obtain a cup product on cohomology

$$\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, C).$$

The cohomology groups of a profinite group G can be built up from those of the finite quotient groups of G. Let U, V run through the open normal subgroups of G. If $V \subseteq U$, the projections

$$G^n \longrightarrow (G/V)^n \longrightarrow (G/U)^n$$

induce homomorphisms

$$C^n(G/U, A^U) \longrightarrow C^n(G/V, A^V) \longrightarrow C^n(G, A),$$

which commute with the operators d^n. Hence, we obtain homomorphisms

$$H^n(G/U, A^U) \longrightarrow H^n(G/V, A^V) \longrightarrow H^n(G, A).$$

The groups $H^n(G/U, A^U)$ form a direct system giving a canonical homomorphism

$$\varinjlim_U H^n(G/U, A^U) \to H^n(G, A).$$

Proposition 2.2.3. *The above homomorphism is an isomorphism:*

$$H^n(G, A) \cong \varinjlim_U H^n(G/U, A^U).$$

Proof. See [NSW08, Proposition 1.2.5]. □

Hence, in what follows, we may assume that G is finite. We will be interested primarily in the cases $n = 0, 1, 2$.

2.2.2 The lower dimensional cohomology groups

The group $H^0(G, A)$: We identify $C^0(G, A)$ with A via the natural isomorphism $y \mapsto y(1)$. Then, for $a \in A$, $(d^1 a)(g) = ga - a$, so $H^0(G, A) = A^G$, the set of elements of A left invariant by G.

The group $H^1(G, A)$: A 1-cocycle is a continuous function $y : G \to A$ such that

$$y(gh) = y(g) + gy(h) \quad \text{for all } g, h \in G.$$

Such a function is also called a *crossed homomorphism*. It is a coboundary if there exists an element $a \in A$ such that $y(g) = ga - a$ for all $g \in G$. A crossed homomorphism of this type is called *principal*.

Let F be a field and K/F a Galois extension with $G = \mathrm{Gal}(K/F)$. Both the additive group K^+ and the multiplicative group $K^\times$ are G-modules. We have

Theorem 2.2.4 (Hilbert's Satz 90)**.** $H^1(G, K^\times) = 1$

Proof. By Proposition 2.2.3, we may assume that K/F is finite. Let $a : G \to K^\times$ be a 1-cocycle. Since the automorphisms $\sigma \in G$ are linearly independent over K, there exists $c \in K^\times$ such that

$$b = \sum_{\sigma \in G} a(\sigma)\sigma c \neq 0.$$

Then, for $\tau \in G$, we have

$$\tau b = \sum_{\sigma \in G} \tau(a(\sigma))\tau\sigma c = \sum_{\sigma \in G} a(\tau)^{-1} a(\tau\sigma)\tau\sigma c = a(\tau)^{-1} b.$$

Thus $a(\tau) = b\tau(b)^{-1}$, so a is a 1-coboundary. □

This in turn leads to the following important result, called *Kummer theory*. Choose $n \in \mathbb{N}$ prime to the characteristic of F. Denote the group of n-th roots of unity in the separable closure F_s of F by μ_n and the absolute Galois group $\mathrm{Gal}(F_s/F)$ of F by G_F.

From the exact sequence of G_F-modules

$$1 \longrightarrow \mu_n \longrightarrow F_s^\times \xrightarrow{a \mapsto a^n} F_s^\times \longrightarrow 1.$$

we obtain, by Hilbert's Satz 90, the exact sequence

$$H^0(G_F, F_s^\times) = F^\times \xrightarrow{a \mapsto a^n} F^\times \xrightarrow{\delta} H^1(G_F, \mu_n) \longrightarrow H^1(G_F, F_s^\times) = 1,$$

and hence

$$H^1(G_F, \mu_n) \cong F^\times/(F^\times)^n.$$

Note that if p is a prime such that F contains a primitive p-th root of unity ζ_p, then μ_p is a trivial G_F-module and we have

$$F^\times/(F^\times)^p \cong H^1(G_F, \mathbb{F}_p) = \mathrm{Hom}(G_F, \mathbb{F}_p),$$

where we consider $\mathbb{F}_p$ to be a G_F-module with trivial action. For each $a \in F^\times$, we have an element $\chi_a \in H^1(G_F, \mathbb{F}_p)$ defined by $\sigma(\sqrt[p]{a}) = \zeta_p^{\chi_a(\sigma)} \sqrt[p]{a}$, for all $\sigma \in G_F$.

We obtain another important result by considering the case in which G is a pro-p group and $\mathbb{F}_p$ is a G-module with trivial G action. $H^1(G, \mathbb{F}_p)$ is then the $\mathbb{F}_p$-vector space of all continuous homomorphisms of G into the discrete group $\mathbb{F}_p$. Since each such homomorphism vanishes on $G^p[G, G]$, $H^1(G, \mathbb{F}_p) \cong H^1(G/G^p[G, G], \mathbb{F}_p) = \mathrm{Hom}(G/G^p[G, G], \mathbb{F}_p)$. This implies that $H^1(G, \mathbb{F}_p)$ and $G/G^p[G, G]$ are dual to each other. By Burnside's Basis Theorem, if $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n < \infty$, G is a finitely generated pro-p group with n as the minimal number of generators.

The group $H^2(G, A)$: A 2-cocycle is a continuous function $x : G \times G \to A$ such that $d^3x = 0$, that is

$$x(gh, k) + x(g, h) = x(g, hk) + gx(h, k) \quad \text{for all } g, h, k \in G.$$

Such a function is a 2-coboundary if

$$x(g,h) = y(g) - y(gh) + gy(h)$$

for a 1-cochain $y : G \to A$.

The 2-cocycles occur in connection with group extensions. Let

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1.$$

be a group extension with abelian kernel A such that $\iota(\sigma a) = \hat{\sigma}\iota(a)\hat{\sigma}^{-1}$ for $\sigma \in G$ and $a \in A$, where $\hat{\sigma} \in E$ is a pre-image of σ. We refer to this as an extension of G by the G-module A. An extension of G by a trivial G-module is called *central*. Two extensions

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1.$$

and

$$1 \longrightarrow A \longrightarrow F \longrightarrow G \longrightarrow 1.$$

are said to be *equivalent* if there exists a homomorphism $\varphi : E \to F$ making the diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & A \arrow[r] & F \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

commute. In this case φ is an isomorphism and both extensions induce the same G-module structure on A.

If $s : G \to E$ is a section, we obtain a map $c : G \times G \to A$ by

$$s_\sigma s_\tau = \iota(c_{\sigma,\tau}) s_{\sigma\tau}$$

for $\sigma, \tau \in G$, where, for convenience of notation, we write s_σ for $s(\sigma)$ and similarly for c.

Then, by associativity in E, we have

$$c_{\rho\sigma,\tau} + c_{\rho,\sigma} = c_{\rho,\sigma\tau} + \rho c_{\sigma,\tau} \quad \text{for all } \rho, \sigma, \tau \in G.$$

Such a map c is called a *factor system*. The set of factor systems forms an abelian group $\mathcal{Z}^2(G, A)$ under point-wise addition.

Let $a : G \to A$ be an arbitrary function. The map $(\sigma, \tau) \mapsto a_\sigma + \sigma a_\tau - a_{\sigma\tau}$ is a factor system, referred to as *split*, and the map a is called a set of *splitting factors* for the factor system. The split factor systems form a subgroup $\mathcal{B}^2(G, A)$ of $\mathcal{Z}^2(G, A)$ and

$$H^2(G, A) \cong \mathcal{Z}^2(G, A)/\mathcal{B}^2(G, A).$$

Given another section $t : G \to E$, we must have $t_\sigma = \iota(a_\sigma)s_\sigma$ for some map $a : G \to A$, and the factor system given by t is

$$(\sigma, \tau) \mapsto c_{\sigma,\tau} + (a_\sigma + \sigma a_\tau - a_{\sigma\tau}).$$

Hence, the cohomology class of c is well defined and is referred to as the cohomology class of the extension

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1.$$

We then have

Theorem 2.2.5. *Two extensions of G by the G-module A are equivalent if and only if they have the same cohomology class. Furthermore, for $\gamma \in H^2(G, A)$ there exists an extension with cohomology class γ.*

Proof. See [Led05, Theorem 2.3.1]. □

Example 2.2.6. The extension with cohomology class $0 \in H^2(G, A)$ is

$$1 \longrightarrow A \xrightarrow{a \mapsto (a,1)} A \rtimes G \xrightarrow{(a,\sigma) \mapsto \sigma} G \longrightarrow 1,$$

where $A \rtimes G$ is the *semi-direct product*, i.e. the set $A \times G$ equipped with the composition $(a, \sigma)(b, \tau) = (a + \sigma b, \sigma\tau)$.

Example 2.2.7. In the case where $G = C_n$ is a cyclic group of order n generated by σ, we can choose the section $G \to E$ as $\sigma^i \mapsto s^i,\ i = 0, 1, \ldots, n-1$, where $s \in E$ is a pre-image of σ. Then $s^n = \iota(a)$ for some $a \in A$ and since $\iota(\sigma a) = s\iota(a)s^{-1}$, we have $a \in A^{C_n}$. So every cohomology class in $H^2(C_n, A)$ is represented by a factor system of the form

$$c_{\sigma^i,\sigma^j} = \begin{cases} 0, & i + j < n \\ a, & i + j \geq n \end{cases}$$

for $i, j \in \{0, 1, \ldots, n-1\}$, where $a \in A^{C_n}$. Conversely, for any such a this is a factor system. A set of splitting factors for c is given by $a_1 = 0,\ a_\sigma = b,\ a_{\sigma^2} = b + \sigma b, \ldots, a_{\sigma^{n-1}} = b + \sigma b + \cdots + \sigma^{n-2} b$, where $b \in A$ with $\mathrm{Tr}_{C_n}(b) = a$. Hence

$$H^2(C_n, A) \cong A^{C_n}/\mathrm{Tr}_{C_n} A.$$

We obtain another important result when we consider the case in which G is a finitely generated pro-p group. Suppose $\{x_1, \ldots, x_n\}$ is a minimal system of generators of G. Then G has a minimal presentation

$$1 \longrightarrow R \longrightarrow S(n) \longrightarrow G \longrightarrow 1,$$

where $S(n)$ is the free pro-p group of rank n. The *rank* of the (closed normal) subgroup R is the number of relations between the x_i's.

Proposition 2.2.8. *The following two conditions are equivalent:*

(i) The subgroup R is of finite rank (as a closed normal subgroup of $S(n)$

(ii) $H^2(G, \mathbb{F}_p)$ is of finite dimension

If these conditions are satisfied, one has the equality

$$r = n - h_1 + h_2,$$

where r is the rank of the normal subgroup R and $h_i = \dim_{\mathbb{F}_p} H^i(G, \mathbb{F}_p)$.

Proof. See [Ser02, Proposition 27] □

Since $\{x_1, \ldots, x_n\}$ is a minimal system of generators of G, $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n$. Hence $r = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$ is the minimal number of relations between the generators of G.

2.3 Central Simple Algebras and the Brauer Group

Definition 2.3.1. A *central simple algebra* (CSA) A/F over a field F is a finite dimensional F-algebra having center F and no proper nontrivial two-sided ideals. We say that an extension field K/F is a *splitting field* for A/F, or that A/F *splits* over K, if $A/F \otimes_F K \cong M_n(K)$ for some n. Two CSA's A/F and B/F are called *similar* if $A/F \otimes_F M_r(F) \cong B/F \otimes_F M_s(F)$ for some r, s and we write $A/F \sim B/F$. If F is understood, we will abbreviate A/F to A.

We have the following characterization and properties of central simple algebras.

Proposition 2.3.2. *For a finite dimensional F-algebra A the following are equivalent:*

(i) A is a CSA.

(ii) If F_s is the separable closure of F, then A splits over F_s.

(iii) There exists a finite Galois extension K/F such that A splits over K.

(iv) $A \cong M_n(D)$ for some n, where D is a skew field over F of finite degree.

Proof. See [NSW08, Proposition 6.3.1]. □

Proposition 2.3.3. *Let A/F be a CSA. Then $A \otimes_F A^{op} \cong M_n(F)$, where $n = \dim_F A$, and A^{op} is the opposite algebra, i.e., A equipped with the multiplication $a \cdot b = ba$.*

Proof. See [Led05, Proposition 3.3.1]. □

The F-algebra $A^e = A \otimes_F A^{op}$ is sometimes known as the *enveloping algebra* of A. Also, by [Led05, Corollary 3.3.4], the tensor product $A \otimes_F B$ of two central simple F-algebras is again central simple and $\sim$ respects tensor products, so we have a well defined composition on the similarity classes of CSA's over F given by

$$[A][B] = [A \otimes_F B].$$

This is associative, commutative, has identity $1 = [F]$ and $[A]^{-1} = [A^{op}]$, so the similarity classes constitute an abelian group, known as the *Brauer group* $\mathrm{Br}(F)$ of F.

Example 2.3.4. Let K/F be a Galois extension of degree $n = [K : F]$ with Galois group $G = \mathrm{Gal}(K/F)$. Let $x : G \times G \to K^\times$ be a normalized (i.e. $x(\sigma, 1) = x(1, \sigma) = 1$) 2-cocycle and consider the n-dimensional K-vector space

$$K^{(G)} = \bigoplus_{\sigma \in G} K e_\sigma$$

with coordinates indexed by G. Define a multiplication on $K^{(G)}$ by

$$(\sum_\sigma a_\sigma e_\sigma)(\sum_\tau b_\tau e_\tau) = \sum_{\sigma,\tau} a_\sigma \sigma b_\tau x(\sigma, \tau) e_{\sigma\tau}.$$

This multiplication has identity $1 = e_1$ and is associative due to the cocycle relation

$$x(\sigma, \tau)x(\sigma\tau, \rho) = \sigma x(\tau, \rho)x(\sigma, \tau\rho),$$

hence making $K^{(G)}$ an n^2-dimensional F-algebra, which is called the *crossed product* of K and G by x, denoted (K, G, x).

Proposition 2.3.5. *Crossed product algebras have the following properties:*

(i) (K, G, x) *is a central simple* F*-algebra which splits over* K*.*

(ii) The normalized cocycles x *and* y *are cohomologous if and only if* $(K, G, x) \cong (K, G, y)$*.*

(iii) $(K, G, xy) \sim (K, G, x) \otimes_F (K, G, y)$.

(iv) Every central simple F-algebra which splits over K is similar to a crossed product algebra.

Proof. See [NSW08, Proposition 6.3.3]. □

If L/F is a field extension, we have the *restriction* homomorphism

$$res_{L/F} : \mathrm{Br}(F) \to \mathrm{Br}(L), \quad [A] \mapsto [A \otimes_F L].$$

The kernel of $res_{L/F}$ is the *relative Brauer group*, $\mathrm{Br}(L/F)$, which is the group of central simple F-algebras which split over L. If K/F runs through the finite Galois subextensions of F_s/F, then by Proposition 2.3.2(3)

$$\mathrm{Br}(F) = \bigcup_K \mathrm{Br}(K/F).$$

Given a normalized 2-cocycle x, we can associate to the cohomology class $[x] \in H^2(\mathrm{Gal}(K/F), K^\times)$ the class $[(K, G, x)]$ to obtain a map

$$H^2(\mathrm{Gal}(K/F), K^\times) \to \mathrm{Br}(K/F),$$

which, by Proposition 2.3.5, is a group isomorphism. If $F \subseteq K \subseteq L$ are two finite Galois extensions, then the diagram

$$\begin{tikzcd}
H^2(\mathrm{Gal}(L/F), L^\times) \arrow[r] & \mathrm{Br}(L/F) \\
H^2(\mathrm{Gal}(K/F), K^\times) \arrow[r] \arrow[u, "inf"] & \mathrm{Br}(K/F) \arrow[u, hook]
\end{tikzcd}$$

commutes and taking direct limits gives

Theorem 2.3.6. *For every Galois extension K/F we have a canonical isomorphism*

$$H^2(\mathrm{Gal}(K/F), K^\times) \cong \mathrm{Br}(K/F).$$

In particular,

$$H^2(G_F, F_s^\times) \cong \mathrm{Br}(F),$$

so $\mathrm{Br}(F)$ *is a torsion group.*

Proof. See [NSW08, Theorem 6.3.4]. □

We can again consider, for n prime to the characteristic of F, the exact sequence

$$1 \longrightarrow \mu_n \longrightarrow F_s^\times \xrightarrow{a \mapsto a^n} F_s^\times \longrightarrow 1$$

of G_F-modules. The associated exact cohomology sequence, together with Hilbert's Satz 90 and the above theorem, then yields the isomorphism

$$H^2(G_F, \mu_n) \cong \mathrm{Br}_n(F) = \{b \in \mathrm{Br}(F) \mid b^n = 1\}.$$

If K/F is a cyclic extension of degree n with Galois group $C_n = \langle \sigma \rangle$, we have

$$\mathrm{Br}(K/F) \cong H^2(C_n, K^\times) \cong F^\times / N_{K/F}(K^\times),$$

where the class of $a \in F^\times$ corresponds to the similarity class of the algebra $(K, C_n, x) = K[s]$ having relations $s^n = a$ and $sb = \sigma bs$ for $b \in K$. In this case the crossed product algebra (K, C_n, x) is often written (K, σ, a) and is referred to as a *cyclic algebra.*

Example 2.3.7. Let F be a field of characteristic $\neq 2$ and let $K = F(\sqrt{a})$ for some $a \in F^\times \setminus (F^\times)^2$. The cyclic algebra $(K, \sigma, b) = F[i, j]$, where $i = \sqrt{a},\ j^2 = b \in F^\times$, σ generates $C_2 = \mathrm{Gal}(K/F)$ and $ji = \sigma ij = -ij$. This algebra is 4-dimensional over F with basis $\{1, i, j, ij\}$ and is split if and only if b is a norm in K/F.

2.4 Quadratic Forms and Quaternion Algebras

Definition 2.4.1. An algebra Q/F in characteristic $\neq 2$ is called a *quaternion algebra* if Q is generated over F by elements i and j such that $i^2 = a,\ j^2 = b$ and $ji = -ij$ for some $a, b \in F^\times$.

Example 2.4.2. $(F(\sqrt{a}), \sigma, b)$ is a quaternion algebra whenever $a \notin (F^\times)^2$. In fact, for any $a, b \in F^\times$ there is a corresponding quaternion algebra Q, denoted

$$Q = (\frac{a, b}{F}) = (a, b)_F$$

which is a 4-dimensional central simple algebra and is either split or a division algebra.

Quaternion algebras have a close connection to quadratic forms. We briefly recall some of the basic theory and notation.

Let F be a field of characteristic $\neq 2$ and let V be a finite-dimensional F-vector space. A symmetric bilinear form on V is a map $B : V \times V \to F$, such that

1. $B(au + bv, w) = aB(u, w) + bB(v, w)$, and
2. $B(u, v) = B(v, u)$

for all $u, v, w \in V$ and $a, b \in F$. The associated *quadratic form* is the diagonal map

$$q : V \to F, \quad u \mapsto B(u, u).$$

Since $q(u + v) = q(u) + q(v) + 2B(u, v)$, one can recover B from q. The pair (V, q) is called a *quadratic space*.

Example 2.4.3. Let $V = F^n$ and let $a_1, \ldots, a_n \in F$. Then the map

$$V \to F, \quad (x_1, \ldots, x_n) \mapsto a_1 x_1^2 + \cdots + a_n x_n^2$$

is an n-ary quadratic form on F^n, called a *diagonal form* and denoted by $\langle a_1, \ldots, a_n \rangle$.

Given two quadratic spaces (V_1, q_1) and (V_2, q_2) over F, where $q_1 = \langle a_1, \ldots, a_n \rangle$ and $q_2 = \langle b_1, \ldots, b_m \rangle$, one can define the *orthogonal sum* $(V_1 \oplus V_2, q_1 \perp q_2) := (V_1, q_1) \perp (V_2, q_2)$ and *tensor product* $(V_1 \otimes V_2, q_1 \otimes q_2) := (V_1, q_1) \otimes (V_2, q_2)$, where

$$q_1 \perp q_2 := \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$$

and

$$q_1 \otimes q_2 := \langle a_1b_1, \ldots, a_1b_m, \ldots, a_nb_1, \ldots, a_nb_m \rangle.$$

Two n-ary quadratic forms q and q' are said to be *equivalent* ($\sim$) if there exists an invertible matrix $C \in GL_n(F)$ such that $q'(Cv) = q(v)$ and two quadratic spaces (V, q) and (V', q') are said to be *isometric* ($\cong$) if there exists an F-isomorphism $\varphi : V \to V'$ such that $q'(\varphi(v)) = q(v)$. It can be shown that every quadratic form is equivalent to a diagonal form and that there is a one-one correspondence between the equivalence classes of n-ary quadratic forms and the isometry classes of n-dimensional quadratic spaces.

Definition 2.4.4. Let q be an n-ary quadratic form over F and let $a \in F^\times$. We say that q *represents* a if there exist $x_1, \ldots, x_n \in F$ such that $q(x_1, \ldots, x_n) = a$. The set of values in $F^\times$ represented by q, or the *value set* of q, is denoted $D_F(q)$. Note that this set depends only on the equivalence class of q.

Let (V, q) be a quadratic space and let B be the symmetric bilinear form corresponding to q. Two vectors $u, v \in V$ are said to be orthogonal, written $u \perp v$, if $B(u, v) = 0$. If U is a subspace of V, the orthogonal complement of U is the subspace

$$U^\perp = \{v \in V \mid \forall u \in U : u \perp v\}.$$

If $U \cap U^\perp = 0$, we say that U is a *regular* subspace. If $V^\perp = 0$, we say that q is regular or *nonsingular*. We say that a vector v is *isotropic* if $q(v) = 0$ and *anisotropic* otherwise. The quadratic form q is called isotropic, or is said to *represent zero*, if q has a non-zero isotropic vector, otherwise it is called anisotropic. An isotropic form can be regular, for example the binary form $\langle 1, -1 \rangle$.

Theorem 2.4.5. *Let (V,q) be a 2-dimensional quadratic space. The following are equivalent:*

(i) V is regular and isotropic.

(ii) V is isometric to $\langle 1, -1 \rangle$.

(iii) V corresponds to the equivalence class of the binary quadratic form x_1x_2.

Proof. See [Lam05, Theorem I.3.2] □

The isometry class of a 2-dimensional quadratic space satisfying the conditions of Theorem 2.4.5 is called the *hyperbolic plane*, denoted $\mathbb{H}$. An orthogonal sum of hyperbolic planes is called a *hyperbolic space*. E. Witt [Wit37a] showed that any regular quadratic space (V, q) splits into an orthogonal sum $(V_h, q_h) \perp (V_a, q_a)$ where V_h is hyperbolic, V_a is anisotropic and the isometry types of V_h and V_a are uniquely determined.

Definition 2.4.6. The set of equivalence classes of anisotropic nonsingular quadratic forms over a field F, together with the binary operations $\perp$ and $\otimes$, form a commutative ring, known as the *Witt ring* $W(F)$ of F.

Returning now to the quaternion algebra $Q = (a, b)_F$ with basis $\{1, i, j, k = ij\}$, we can make Q into a quadratic space as follows. For an arbitrary quaternion $x = \alpha + \beta i + \gamma j + \delta k \in Q$, we define a map $N : Q \to F$ by $N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2$. Then $N = \langle 1, -a, -b, ab\rangle$ is a quadratic form, referred to as the norm form of Q, and $N(x)$ is called the norm of the quaternion x.

Theorem 2.4.7. *For $a, b, c, d \in F^\times$, the following are equivalent:*

(i) $\langle 1, -a, -b, ab\rangle \sim \langle 1, -c, -d, cd\rangle$.

(ii) $\langle -a, -b, ab\rangle \sim \langle -c, -d, cd\rangle$.

(iii) $(a, b)_F \cong (c, d)_F$.

Proof. See [Sch85, Ch. 2, Theorem 11.9]. □

Hence a quaternion algebra is completely determined by its norm form. This also leads to the following criteria for the splitting of a quaternion algebra.

Corollary 2.4.8. *The following are equivalent:*

(i) $\langle -a, -b, ab\rangle$ *is isotropic.*

(ii) $(a, b)_F$ *is split.*

(iii) The binary form $\langle a, b\rangle$ *represents 1.*

(iv) $b \in N_{K/F}(K)$, *where* $K = F(\sqrt{a})$ *and* $N_{K/F}$ *is the field norm.*

We denote the equivalence class of the quaternion algebra $(a, b)_F$ in $\mathrm{Br}(F)$ by (a, b) and call it a *quaternion class*. We have

Theorem 2.4.9. *Let* $a, a', b, b', x, y \in F^\times$. *Then*

(i) $(a, b) = (b, a)$ *and* $(ax^2, by^2) = (a, b)$.

(ii) $(a, -a) = 1$ *and* $(a, 1 - a) = 1$ *if* $a \neq 1$.

(iii) $(a, a) = (a, -1)$.

(iv) $(aa', b) = (a, b)(a', b)$ *and* $(a, bb') = (a, b)(a, b')$.

Proof. See [Led05, Theorem 3.5.3]. □

Definition 2.4.10. A pairing $f : F^\times \times F^\times \to A$ into a multiplicative abelian group A is said to be a *Steinberg symbol* if f is bimultiplicative and has the *Steinberg property*; $f(a, b) = 1$ whenever $a + b = 1$.

Every such symbol factors through a group $K_2(F)$, called the *second K-group* of the field F, which is defined by

$$K_2(F) = (F^\times \otimes_{\mathbb{Z}} F^\times)/\langle a \otimes b \mid a + b = 1\rangle.$$

The natural pairing $\varphi : F^\times \times F^\times \to K_2(F)$ is then a *universal Steinberg symbol*; i.e. for any arbitrary Steinberg symbol $f : F^\times \times F^\times \to A$ there exists a unique group homomorphism $g : K_2(F) \to A$ such that $f = g\varphi$.

We define the group $k_2(F)$ to be the quotient $K_2(F)/(K_2(F))^2$. Any Steinberg symbol into an abelian group A with $A^2 = 1$ then factors uniquely through $k_2(F)$. Theorem 2.4.9 shows that the quaternion map $(-, -) : F^\times \times F^\times \to \mathrm{Br}(F)$ is a symmetric bilinear form defined on the square classes of $F^\times$, which defines a Steinberg symbol into $\mathrm{Br}_2(F)$. This symbol is induced by the unique group homomorphism $k_2(F) \to \mathrm{Br}_2(F)$ given by $[a] \otimes [b] \mapsto (a, b)$.

Theorem 2.4.11 (Merkurjev)**.** *The map* $k_2(F) \to \mathrm{Br}_2(F)$ *is an isomorphism.*

Proof. See [Mer81]. □

This leads to the notion of a *symbol* for any field F as a multi-multiplicative map

$$F^\times \times \cdots \times F^\times \to A, \quad (a_1, \ldots, a_n) \mapsto [a_1, \ldots, a_n],$$

into a (multiplicatively written) abelian group A such that $[a_1, \ldots, a_n] = 1$ whenever $a_i + a_j = 1$ for some $i \neq j$. Every such symbol factors through a group $K_n^M(F)$, which is the universal target of symbols and is defined as follows.

Definition 2.4.12. The n-th *Milnor K-group* of a field F is the quotient

$$K_n^M(F) = (F^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^\times)/I_n,$$

where I_n is the subgroup generated by the elements $a_1 \otimes \cdots \otimes a_n$ such that $a_i + a_j = 1$ for some $i \neq j$.

The Milnor K-groups have a close connection to Galois cohomology, which arises as follows.

Let $k \in \mathbb{N}$ be prime to the characteristic of F. Recall that the exact sequence

$$1 \longrightarrow \mu_k \longrightarrow F_s^\times \xrightarrow{a \mapsto a^k} F_s^\times \longrightarrow 1$$

gives a surjective homomorphism

$$\delta_F : F^\times \to H^1(G_F, \mu_k)$$

with kernel $(F^\times)^k$. Also, for each $n \geq 1$, we have the cup product

$$H^1(G_F, \mu_k) \times \cdots \times H^1(G_F, \mu_k) \xrightarrow{\cup} H^n(G_F, \mu_k^{\otimes n}),$$

hence a map

$$F^\times \times \cdots \times F^\times \to H^n(G_F, \mu_k^{\otimes n}), \quad (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n)_F := \delta_F a_1 \cup \cdots \cup \delta_F a_n.$$

Theorem 2.4.13 (Tate)**.** *The above map induces a homomorphism*

$$h_F : K_n^M(F) \to H^n(G_F, \mu_k^{\otimes n}),$$

called the Galois symbol (or the norm residue map).

Proof. [NSW08, Theorem 6.4.2] The multiplicativity in each argument follows from the definition. It remains to show that $(a_1, \ldots, a_n)_F = 1$ if $a_i + a_j = 1$ for $i \neq j$ and it suffices to consider the case $n = 2$ since if $n > 2$ and, say $i = 1$, $j = 2$, then $(a_1, \ldots, a_n)_F = (a_1, a_2)_F \cup (a_3, \ldots, a_n)_F$.

Let $n = 2$ and let $a \in F^\times$, $a \neq 1$. Let $X^n - a = \prod_i f_i(X)$ with $f_i(X)$ monic and irrreducible in $F[X]$. For each i, let a_i be a root of $f_i(X)$ and let $F_i = F(a_i)$. Then

$$1 - a = \prod_i f_i(1) = \prod_i N_{F_i/F}(1 - a_i).$$

Hence

$$(1 - a, a)_F = (\prod_i N_{F_i/F}(1 - a_i), a)_F = \prod_i (N_{F_i/F}(1 - a_i), a)_F.$$

The formula $cor(\alpha \cup res\beta) = (cor\alpha) \cup \beta$ together with the fact that cor is the norm on H^0 and commutes with δ gives

$$\begin{aligned}(N_{F_i/F}(1 - a_i), a)_F &= cor(1 - a_i, a)_{F_i} \\ &= cor(1 - a_i, a_i^k) \\ &= cor(1 - a_i, a_i)^k \\ &= 1,\end{aligned}$$

hence $(1 - a, a) = 1$. □

For the Galois symbol we have

Conjecture 2.4.14 (Bloch-Kato)**.** *For every field F and every $k \in \mathbb{N}$ prime to the characteristic of F, the Galois symbol yields an isomorphism*

$$h_F : K_n^M(F)/NK_n^M(F) \xrightarrow{\sim} H^n(G_F, \mu_k^{\otimes n}).$$

This famous conjecture has recently been proved by V. Voevodsky with contributions by M. Rost and C. Weibel. The result is often referred to as the *norm residue isomorphism.*

2.5 The Incidence Algebra and Möbius Functions

Often a set of objects to be counted possesses a natural partial ordering. As a result, many problems of enumeration are closely related to the theory of Möbius functions. In this section we recall some pertinent aspects of that general theory (see [Rot64, BG75, Wal61]).

Consider a partially ordered set $P = (S, \leqq)$, where $\leqq$ is an order relation on the set S. For any $x, y \in P$, the *segment* $[x, y] := \{z \in P \mid x \leqq z \leqq y\}$. A partially ordered set P is *locally finite* if every segment in P is finite.

Let P be a locally finite partially ordered set. The *incidence algebra* of P is defined as follows. Consider the set of all real-valued functions of two variables $f(x, y)$, defined for $x, y \in P$, with the property that $f(x, y) = 0$ if $x \nleqq y$. The sum of two such functions as well as multiplication by scalars are defined as usual. The product $h = fg$ is defined as follows:

$$h(x, y) = \sum_{x \leqq z \leqq y} f(x, z)g(z, y).$$

Since P is locally finite, the sum on the right is well defined. This is an associative algebra over the reals and has an identity element which is the Kronecker delta function, $\delta(x, y)$.

The *zeta function* of P is the element of the incidence algebra of P given by $\zeta(x, y) = 1$ if $x \leqq y$ and $\zeta(x, y) = 0$ otherwise. The function $n(x, y) = \zeta(x, y) - \delta(x, y)$ is called the *incidence function.*

Proposition 2.5.1. *The zeta function of a locally finite partially ordered set P is invertible in the incidence algebra.*

Proof. Let $\mu(x, y)$ be the function defined inductively over the elements in the segment [x,y] as follows. Set $\mu(x, x) = 1$ for all $x \in P$. Now suppose that $\mu(x, z)$ has been defined for all z such that $x \leqq z < y$ and set

$$\mu(x, y) = -\sum_{x \leqq z < y} \mu(x, z).$$

Then

$$\begin{aligned}(\zeta\mu)(x, y) &= \sum_{x \leqq z \leqq y} \zeta(x, z)\mu(z, y) \\ &= \sum_{x \leqq z \leqq y} \mu(z, y) \\ &= \delta(x, y),\end{aligned}$$

and similarly $(\mu\zeta)(x, y) = \delta(x, y)$. The function μ, the inverse of ζ, is called the *Möbius function* of the partially ordered set P. □

Proposition 2.5.2 (Möbius inversion formula I)**.** *Let $f : P \to \mathbb{R}$ be defined for all x in a locally finite partially ordered set P and assume there exists an element $m \in P$ such that $f(x) = 0$ unless $x \geqq m$. Suppose that $g : P \to \mathbb{R}$ is given by*

$$g(x) = \sum_{y \leqq x} f(y).$$

Then

$$f(x) = \sum_{y \leqq x} g(y)\mu(y, x).$$

Proof. Since P is locally finite, $\sum_{y \leqq x} f(y) = \sum_{m \leqq y \leqq x} f(y)$ is a finite sum. Hence the

function g is well-defined. Then

$$\begin{aligned}\sum_{y\leqq x} g(y)\mu(y,x) &= \sum_{y\leqq x}\sum_{z\leqq y} f(z)\mu(y,x)\\ &= \sum_{y\leqq x}\sum_{z} f(z)\zeta(z,y)\mu(y,x)\\ &= \sum_{z} f(z)\sum_{y\leqq x}\zeta(z,y)\mu(y,x)\\ &= \sum_{z} f(z)\delta(z,x)\\ &= f(x).\end{aligned}$$

□

A similar argument establishes

Proposition 2.5.3 (Möbius inversion formula II)**.** *Let $f : P \to \mathbb{R}$ be defined for all x in a locally finite partially ordered set P and assume there exists an element $M \in P$ such that $f(x) = 0$ unless $x \leqq M$. Suppose that $g : P \to \mathbb{R}$ is given by*

$$g(x) = \sum_{y\geqq x} f(y).$$

Then

$$f(x) = \sum_{y\geqq x} \mu(x,y)g(y).$$

Corollary 2.5.4. *The Möbius function μ of a locally finite partially ordered set can be computed recursively by either of the formulae*

$$\mu(x,z) = -\sum_{x\leqq y<z} \mu(x,y), \quad x < z,$$
$$\mu(x,z) = -\sum_{x<y\leqq z} \mu(y,z), \quad x < z,$$

together with $\mu(x,x) = 1$.

Example 2.5.5. [Rot64, Example 1] The classical Möbius function defined on the set

of positive integers is given by $\mu(d) = (-1)^r$ if d is a product of r distinct primes and 0 otherwise. The classical inversion formula, first derived by Möbius in 1832, is:

$$g(m) = \sum_{n|m} f(n); \quad f(m) = \sum_{n|m} g(n)\mu(m/n).$$

The set of positive integers is a locally finite partially ordered set with divisibility as the partial order. In this case the incidence algebra has a distinguished subalgebra consisting of all functions f of the form $f(n,m) = F(m/n)$. The Möbius function of this partially ordered set is $\mu(n,m) = \mu(m/n)$. The product $H = FG$ of two functions in this subalgebra can be written in the simpler form

$$H(m) = \sum_{kn=m} F(k)G(n).$$

If we associate the *formal Dirichlet series* $\hat{F}(s) = \sum_{n=1}^{\infty} F(n)/n^s$ with the element F of this subalgebra, then the above product corresponds to the product of two formal Dirichlet series considered as functions of s, $\hat{H}(s) = \hat{F}(s)\hat{G}(s)$. Under this representation, the zeta function of the partially ordered set is the classical *Riemann zeta function* $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$, and the statement that the Möbius function is the inverse of the zeta function reduces to the classical identity $1/\zeta(s) = \sum_{n=1}^{\infty} \mu(n)/n^s$.

The lattice of subgroups of a finite group G is a locally finite partially ordered set. The theory of Möbius functions in this case is of particular interest in counting Galois extensions. A *subgroup function* from G to $\mathbb{Z}$ is a mapping of the lattice of subgroups of G into $\mathbb{Z}$. The equations

$$\mu_G(G) = 1 \quad \text{and} \quad \sum_{H \leq K} \mu_G(K) = 0 \quad \text{whenever } H < G,$$

define the *Möbius function* μ_G of G; μ_G is a subgroup function from G to $\mathbb{Z}$. Note that if $N \lhd G$, $N \leq H \leq G$, then $\mu_{G/N}(H/N) = \mu_G(H)$.

If two subgroup functions g, h satisfy

$$g(H) = \sum_{K \leq H} h(K)$$

for all $H \leq G$, then by the Möbius inversion formula

$$h(G) = \sum_{H \leq G} \mu_G(H) g(H).$$

An explicit formula for $\mu_G(H)$ can be obtained as follows. Let $M_1, \ldots, M_r$ be the maximal subgroups of G. If $S = \{i_1, \ldots, i_s\}$ is a subset of $I = \{1, \ldots, r\}$, let

$$\begin{aligned} (-1)^S &:= (-1)^s, \\ M_S &:= M_{i_1} \wedge M_{i_2} \wedge \cdots \wedge M_{i_s}; \end{aligned}$$

so $M_\phi = G$, and M_I is the Frattini subgroup $\Phi(G)$ of (G). Let S_H denote the set of indices i such that $H \leq M_i$. Then

$$\begin{aligned} \sum_{H \leq M_S} (-1)^S &= \sum_{S \subseteq S_H} (-1)^S \\ &= \begin{cases} 1 & \text{if } H = G \\ 0 & \text{if } H < G, \end{cases} \end{aligned}$$

so

$$\mu_G(H) = \sum_{M_S = H} (-1)^S.$$

It follows that $\mu_G(H) = 0$ unless H is an intersection of maximal subgroups of G. In particular, $\mu_G(H) = 0$ unless $\Phi(G) \leq H$.

Now consider the case in which G is a p-group. Let $V_n(q)$ be an n-dimensional vector space over the field of q elements and partially order the subspaces of $V_n(q)$ by inclusion. Denote the resulting partially ordered set by $L(V_n(q))$. The Gaussian coefficient $\binom{n}{k}_q$ is

defined to be the number of k-dimensional subspaces of $V_n(q)$. Hence

$$\begin{aligned}\binom{n}{k}_q &= \frac{\#\text{ of sequences of } k \text{ independent vectors in } V_n(q)}{\#\text{ of sequences of } k \text{ independent vectors in } V_k(q)} \\ &= \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} \\ &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.\end{aligned}$$

For any two subspaces S and T of $V_n(q)$, the structure of the sublattice $[S,T]$ of $L(V_n(q))$ depends only on $\dim_{\mathbb{F}_q} T - \dim_{\mathbb{F}_q} S$, so computing the Möbius function of the partially ordered set $L(V_n(q))$ reduces to determining the Möbius function $\mu_k = \mu(0, V_k(q))$ for all $k \leq n$.

Let X be a vector space over $\mathbb{F}_q$ with $|X| = x$. For any subspace $U \in L(V_n(q))$ let $N_=(U)$ be the number of linear transformations $f : V_n(q) \to X$ whose kernel is U and let $N_\geq(U)$ be the number of such maps whose kernel contains U. Then

$$N_\geq(U) = \sum_{U \leq W \in L(V_n(q))} N_=(W),$$

and by Möbius inversion

$$N_=(U) = \sum_{U \leq W \in L(V_n(q))} \mu(U,W) N_\geq(W).$$

The number of injective maps is then

$$N_=(0) = \sum_{W \in L(V_n(q))} \mu(0,W) N_\geq(W).$$

Since any injective map from $V_n(q) \to X$ is specified by giving the image of an ordered basis of $V_n(q)$, the number of such maps is $(x-1)(x-q)\cdots(x-q^{n-1})$. Also, if W has $\mathbb{F}_q$-dimension $d(W)$, then $N_\geq(W) = x^{n-d(W)}$. Hence

$$(x-1)(x-q)\cdots(x-q^{n-1}) = \sum_{W \in L(V_n(q))} \mu_{d(W)} x^{n-d(W)} = \sum_{k=0}^{n} \binom{n}{k}_q \mu_k x^{n-k}.$$

Since this identity is true for infinitely many values of x, it is a polynomial identity. Equating the constant terms gives

$$\mu_n = (-1)(-q)\cdots(-q^{n-1}) = (-1)^n q^{\frac{1}{2}n(n-1)}.$$

Thus we have

Lemma 2.5.6. *If G is a p-group and $H \leq G$ with $[G:H] = p^i$ then*

$$\mu_G(H) = \begin{cases} (-1)^i p^{\frac{1}{2}i(i-1)} & \text{if } G^p[G,G] \leq H \\ 0 & \text{otherwise.} \end{cases}$$

□

This lemma will be important when we consider M. Yamagishi's method for determining the number of Galois p-extensions of certain local fields in section 3.3.4.

Chapter 3

Counting Galois p-Extensions

The goal of this chapter is to illustrate several techniques for enumerating Galois p-extensions of various fields. These numbers are important in the study of quotients and filtrations of absolute Galois groups. In section 3.2 we point out a connection between the number of Galois extensions of a field F having Galois group isomorphic to D_4, the dihedral group of order 8, and a particular small quotient of G_F referred to as the W-group of F.

We turn to the problem of counting D_4-extensions of local fields, beginning, in section 3.3, with a method of constructing extensions of the p-adic numbers, $\mathbb{Q}_p$, due to H. Naito [Nai95]. We then provide an alternative, group-theoretic approach based on knowledge of the W-group as well as a method which utilizes the theory of quaternion algebras. These are new techniques for determining the number of D_4-extensions of $\mathbb{Q}_p$ which are presented as an alternative to the direct construction approach of Naito.

Section 3.3.4 describes a technique, due to M. Yamagishi [Yam95], using the theory of complex characters and Möbius functions to count finite Galois p-extensions of a local field K, where K is a finite extension of $\mathbb{Q}_p$. We illustrate this method in the case of D_4-extensions in example 3.3.6. In [MT14] J. Mináč and N. D. Tân develop a technique to compute the number of $\mathbb{U}_4(\mathbb{F}_p)$-extensions of K using triple Massey products. We closely follow this approach in section 3.3.5, with the necessary modifications, to show that cup products can be used to determine a formula for the number of D_4-extensions of K based on the degree $n = [K : \mathbb{Q}_p]$.

In section 3.4 we consider formally real pythagorean fields. It is interesting to note that in 1900, David Hilbert posed a famous list of twenty-three problems and it was the theory of formally real fields that led Emil Artin, in 1927, to a solution of Hilbert's seventeenth problem. After reviewing the basic theory, we develop, in section 3.4.1, a formula for the number of D_4-extensions of a pythagorean SAP field. In section 3.4.2 we characterize the group $G_F(2)$ for F a pythagorean SAP field or a superpythagorean field. These groups will be considered further when we study dimensions of Zassenhaus filtration subquotients in chapter 4.

3.1 The Inverse Galois Problem

A central problem in modern Galois theory is the inverse Galois problem: given a field F and a group G, is it possible to construct a Galois extension K/F with Galois group isomorphic to G? Such an extension K/F is often referred to as a G-extension. If such a construction is possible, then the closely related question of counting the number of G-extensions of F naturally arises.

The embedding problem in Galois theory generalizes the inverse problem and consists of finding the conditions under which one can construct a Galois extension K/F, with group G, such that K extends a given Galois extension L/F whose Galois group is a quotient of G. If the group G contains a normal subgroup H, then a natural approach to solving the inverse problem for the field F and the group G is to choose an extension L/F with Galois group G/H which can in turn be embedded in an appropriate extension K.

Probably the simplest example of an embedding problem is the following well known result (see, for example [ILF97]), which is also related to the notion of pythagorean fields. We include a proof in order to illustrate that even this case is nontrivial.

Theorem 3.1.1. *Let F be a field with* $\mathrm{char}(F) \neq 2$ *and let $K = F(\sqrt{a})$ be a quadratic extension of F. Then K can be embedded in a cyclic extension L/F of degree 4 if and only if a is a sum of two squares in F.*

Proof. We assume that $-1 \notin F^2$; otherwise every element in F is a sum of two squares in F and $L = F(\sqrt[4]{a})$ is a solution of the embedding problem.

Suppose that L/F is a C_4-extension with $\mathrm{Gal}(L/F) = \langle g \rangle$ and that $K \subseteq L$. Let α be a primitive element of L and let $m = (\alpha - g^2(\alpha))/(g(\alpha) - g^3(\alpha))$. Then m is well defined and $m \neq 0$. Also, $g(m) = (g(\alpha) - g^3(\alpha))/(g^2(\alpha) - \alpha) = -m^{-1}$ and $g^2(m) = -g(m)^{-1} = m$, so $m \in K = F(\sqrt{a})$. If $m = x + y\sqrt{a}$, where $x, y \in F$, then $x^2 - ay^2 = N_{K/F}(m) = mg(m) = -1$, so $y \neq 0$ and $a = (x/y)^2 + (1/y)^2$ is a sum of two squares in F.

Conversely, suppose $a = u^2 + v^2$ with $u, v \in F,\ v \neq 0$ and let $m = (u + \sqrt{a})/v$. Then, if $\bar{g}$ is the automorphism of $K = F\sqrt{a}$ defined by $\sqrt{a} \mapsto -\sqrt{a}$, we have $m\bar{g}(m) = -1$. Now let $\lambda = 1 + m^2$. Then $\lambda \neq 0$ and $\bar{g}(\lambda) = 1 + 1/m^2 = \lambda/m^2$. Let $\theta = \sqrt{\lambda}$, let $L = K(\theta)$ and let g be an automorphism of L extending the automorphism $\bar{g}$ of K. Then $g(\theta)^2 = g(\lambda) = \lambda/m^2 = (\theta/m)^2$, so, up to sign, $g(\theta) = \theta/m$. Hence g is an automorphism of L/F and furthermore,

$$\begin{aligned} g^2(\theta) &= g(\theta)/\bar{g}(m) = \theta/(m\bar{g}(m)) = -\theta; \\ g^3(\theta) &= -\theta/m; \\ g^4(\theta) &= \theta, \end{aligned}$$

so $g^4 = 1$. Therefore $L = K(\theta)$ is normal over F with $\mathrm{Gal}(L/F) = \langle g \rangle \cong C_4$. □

Embedding problems have close connections to Galois cohomology and quadratic forms. They are also of considerable importance in the study of absolute Galois groups. For example, from the Galois correspondence, an affirmative answer to the inverse problem is equivalent to the existence of a closed normal subgroup H of the absolute Galois group G_F of F such that $G_F/H \cong G$. However, absolute Galois groups remain largely mysterious objects and determining which profinite groups are realizable as absolute Galois groups of various fields remains a significant open problem in Galois theory.

One means of approaching this problem is to study small quotients of absolute Galois groups. The structure of these groups is, in turn, closely related to the problem of counting Galois extensions. In the next section, for example, we look at the connection between the number of D_4-extensions of a field F and the W-group of F.

3.2 Dihedral Extensions and W-Groups

We follow [MS96] to define a special Galois extension of a base field F and then summarize results which pertain to the determination of dihedral extensions of F.

We fix the following notation: C_n denotes the cyclic group of order n and D_4 denotes the dihedral group of order 8. We assume that all fields have characteristic different from 2 and we make no distinction between an element a in a field F and and its square class $a(F^\times)^2 \in F^\times/(F^\times)^2$. An extension K of the field F is called a *G-extension* if K/F is Galois with Galois group G.

Let $F^{(2)} = F(\sqrt{a} \mid a \in F^\times)$; the compositum of all quadratic extensions of F, $\Gamma = \{b \in F^{(2)} \mid F^{(2)}(\sqrt{b})/F \text{ is Galois}\}$ and $F^{(3)} = F^{(2)}(\sqrt{b} \mid b \in \Gamma)$; the compositum of all quadratic extensions of $F^{(2)}$ which are Galois over F. Due to its close connection with the Witt ring $W(F)$ of F, the field $F^{(3)}$ has been referred to as the *Witt closure* of F and the group $\mathrm{Gal}(F^{(3)}/F)$ is called the *W-group* of F. Recall that the *quadratic closure* or *maximal 2-extension* of F, denoted $F(2)$, is the smallest extension of F which is closed under taking of square roots, or alternatively, is the compositum of all 2-towers over F (inside a fixed algebraic closure of F). The group $\mathrm{Gal}(F(2)/F)$ is the maximal pro-2 quotient, $G_F(2)$, of the absolute Galois group G_F of F. By [MS96, Proposition 2.1] we see that the W-group of F, $\mathrm{Gal}(F^{(3)}/F) \cong G_F(2)^{[3]}$.

Let $\{a_i \mid i \in I\}$ be a basis of $F^\times/(F^\times)^2$. The automorphisms σ_i given by $\sigma_j(\sqrt{a_i}) = (-1)^{\delta_{ij}}\sqrt{a_i}$, where δ_{ij} is the Kronecker delta function, form a minimal set of generators of $\mathrm{Gal}(F^{(2)}/F)$ and they induce a natural isomorphism $\mathrm{Gal}(F^{(2)}/F) \cong \prod_{i\in I} C_2$. From Kummer theory, $\mathrm{Gal}(F^{(2)}/F)$ is the Pontrjagin dual of the discrete group $F^\times/(F^\times)^2$ under the pairing $(\sigma, a) = \sigma(\sqrt{a})/\sqrt{a}$ with values in $C_2 \cong \{\pm 1\}$.

We now look more closely at the structure of $F^{(3)}$. Recall that quaternion algebras over F are denoted $(a, b)_F$, or simply (a, b) when the field F is clear. By Merkurjev's Theorem [2.4.11], the subgroup of the Brauer group $\mathrm{Br}(F)$ generated by the isomorphism classes of quaternion algebras over F is $\mathrm{Br}_2(F)$, the subgroup generated by elements of order ≤ 2. The operation in $\mathrm{Br}(F)$ will be written multiplicatively, so $(a, b)_F = 1$ means (a, b) splits over F. For $a \in F^\times$, N_a denotes the *norm group* of a, i.e., the group of

values of the quadratic form $\langle 1, -a\rangle$ over F. The norm of an element $y \in F(\sqrt{a})$ for $a \in F^\times \setminus (F^\times)^2$ will be written Ny.

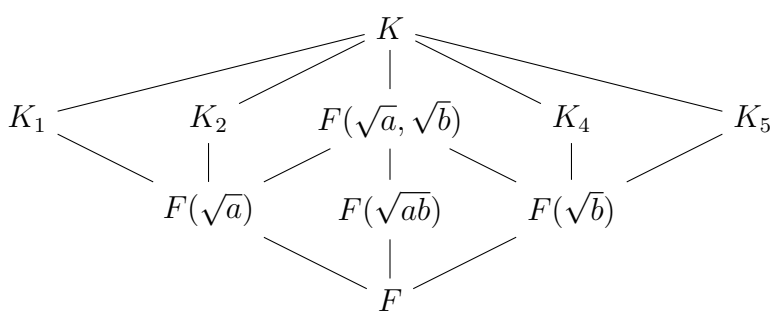
If $a \in F^\times/(F^\times)^2$ then by a C_4^a*-extension* of F we mean a C_4-extension K of F such that $F(\sqrt{a}) \subset K$. For these we have the following well known result (see, for example, [JLY03, Chapter 2, Section 2] or [MS96, Proposition 2.3]).

Proposition 3.2.1. *Let $a \in F^\times/(F^\times)^2$. Then there exists a C_4^a-extension of F if and only if $(a,a)_F = 1$. Furthermore, K is a C_4^a-extension of F if and only if $K = F(\sqrt{a})(\sqrt{y})$ where $y \in F(\sqrt{a})$ is such that $Ny = a \in F^\times/(F^\times)^2$.*

Two elements $a, b \in F^\times$ are called *independent modulo squares* if a and b are linearly independent in $F^\times/(F^\times)^2$. If $a, b \in F^\times$ are independent modulo squares then by a $D_4^{a,b}$*-extension* of F we mean a D_4-extension K of F such that $F(\sqrt{a}, \sqrt{b}) \subset K$ and $\mathrm{Gal}(K/F(\sqrt{ab})) \cong C_4$. This next proposition is also well known (see, for example, [JLY03, Chapter 2, Section 2]). For some history and discussion of more general types of Galois extensions related to these extensions see also [Frö85, 7.7], [Mas87] or [MNQD77].

Proposition 3.2.2. *Let $a, b \in F^\times$ be independent modulo squares. Then there exists a $D_4^{a,b}$-extension of F if and only if $(a,b)_F = 1$. Furthermore, K is a $D_4^{a,b}$-extension of F if and only if $K = F(\sqrt{a}, \sqrt{b})(\sqrt{y})$ where $y \in F(\sqrt{a})$ is such that $Ny = b \in F^\times/(F^\times)^2$.*

The following diagram shows the lattice of subfields of a $D_4^{a,b}$-extension K of F:



J. Mináč and M. Spira have shown that $F^{(3)}$ is the compositum of all quadratic, C_4- and D_4-extensions of F [MS96, Corollary 2.18]. Furthermore, they observe that if $y, z \in F(\sqrt{a})$ both satisfy the statement of Proposition 3.2.1, then $F^{(2)}(\sqrt{y}) = F^{(2)}(\sqrt{z})$, and that a similar remark holds for D_4-extensions. They also show that $F^{(3)}$ can be

described as the Galois closure over F of the compositum of all extensions L of F such that $F \subseteq L \subseteq F(2)$ and $[L : F] \leq 4$ [MS96, Corollary 2.19].

Counting the number of D_4-extensions of a given field F is therefore important in determining the W-group, $\mathrm{Gal}(F^{(3)}/F)$, and thereby gaining a better understanding of the absolute Galois group of F. We now consider various examples of fields F in order to illustrate several methods of counting these extensions.

3.3 Local Fields

3.3.1 Constructing extensions

We begin by considering, as the base field, the field of p-adic numbers, $\mathbb{Q}_p$. One means of determining the number of D_4-extensions of $\mathbb{Q}_p$ is, of course, by actually constructing all such extensions. Following [Nai95], we outline this technique and then look at alternative methods of counting these extensions.

1. The case $\mathbf{p \neq 2}$. Any element $x \in \mathbb{Q}_p$ can be written uniquely in the form $x = up^n$, where u is a unit in $\mathbb{Z}_p$. For p odd, $x = up^n \in \mathbb{Q}_p^\times$ is a square if and only if n is even and the image of u in the residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ is a square mod p. Hence, $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong C_2 \times C_2$ with representatives $\{1, p, u, up\}$ where $(\frac{u}{p}) = -1$.

The lattice of subfields of a D_4-extension $L/\mathbb{Q}_p$ is shown in the following diagram.

$$\begin{tikzcd}
 & & L \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
M_1 \arrow[dr, dash] & M_1' \arrow[d, dash] & M \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & M_2 \arrow[d, dash] & M_2' \arrow[dl, dash] \\
 & \mathbb{Q}_p(\sqrt{p}) \arrow[dr, dash] & \mathbb{Q}_p(\sqrt{u}) \arrow[d, dash] & \mathbb{Q}_p(\sqrt{up}) \arrow[dl, dash] & \\
 & & \mathbb{Q}_p & &
\end{tikzcd}$$

The three quadratic extensions of $\mathbb{Q}_p$ are $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{u})$ and $\mathbb{Q}_p(\sqrt{up})$ and $L/\mathbb{Q}_p$ has four intermediate fields of degree 4 which are not Galois over $\mathbb{Q}_p$. These are the extensions labelled M_1, M_1', M_2, M_2' in the above lattice diagram. For each $n \in \mathbb{N}$, any given local field has exactly one unramified extension of degree n. Since $\mathbb{Q}_p(\sqrt{p})/Q_p$ and

$\mathbb{Q}_p(\sqrt{up})/Q_p$ are ramified, $\mathbb{Q}_p(\sqrt{u})/Q_p$ is unramified. Hence, $M/\mathbb{Q}_p(\sqrt{p})$ and $M/\mathbb{Q}_p(\sqrt{up})$ are also unramified. So $M_i, M_i',\ i = 1, 2$ are totally, and since $(p, 4) = 1$, tamely ramified extensions of $\mathbb{Q}_p$. By Serre's mass formula, $\mathbb{Q}_p$ has exactly four totally and tamely ramified extensions of degree 4. One such extension, say M_1, is $\mathbb{Q}_p(\sqrt[4]{p})/\mathbb{Q}_p$. Hence $L = \mathbb{Q}_p(\sqrt{u}, \sqrt[4]{p})/\mathbb{Q}_p$.

If $p \equiv 1 \bmod 4$, then $\mathbb{Q}_p$ contains the 4th roots of unity, so $\mathbb{Q}_p(\sqrt[4]{p})/\mathbb{Q}_p$ is a Galois extension of degree 4. Hence $\mathbb{Q}_p$ can have no D_4-extension in this case.

If $p \equiv 3 \bmod 4$, then -1 is not a square in $\mathbb{Q}_p$, so $\mathbb{Q}_p(\sqrt[4]{p})/\mathbb{Q}_p$ is not Galois. In this case we see that $\mathbb{Q}_p(\sqrt{-1}, \sqrt[4]{p})$ is a D_4-extension of $\mathbb{Q}_p$.

2. The case $\mathbf{p = 2}$. We now consider the field of 2-adic numbers, $\mathbb{Q}_2$. Let $L/\mathbb{Q}_2$ be a Galois extension of degree 8. The Galois group of L, $\mathrm{Gal}(L/\mathbb{Q}_2) \cong D_4$ if and only if L contains an intermediate field of degree 4 which is not Galois over $\mathbb{Q}_2$. Hence, in order to determine the D_4-extensions of $\mathbb{Q}_2$, it is sufficient to construct all quadratic extensions of K_i which are not Galois over $\mathbb{Q}_2$, where K_i is a quadratic extension of $\mathbb{Q}_2$.

The lattice of subfields of a D_4-extension $L/\mathbb{Q}_2$ is shown below. We denote by K the quadratic extension of $\mathbb{Q}_2$ for which L/K is cyclic of degree 4. The other two quadratic extensions of $\mathbb{Q}_2$ in L are denoted K_1 and K_2. For $i = 1, 2$, M_i and M_i' are the quadratic extensions of K_i in L which are not Galois over $\mathbb{Q}_2$.

$$\begin{tikzcd}
 & & L \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
M_1 \arrow[dr, dash] & M_1' \arrow[d, dash] & M \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & M_2 \arrow[d, dash] & M_2' \arrow[dl, dash] \\
 & K_1 \arrow[dr, dash] & K \arrow[d, dash] & K_2 \arrow[dl, dash] & \\
 & & \mathbb{Q}_2 & &
\end{tikzcd}$$

Let σ be the generator of the Galois group of $K_i/\mathbb{Q}_2$. Then $M_i = K_i(\sqrt{\alpha})$ for an $\alpha \in K_i^\times$ such that $\alpha^\sigma/\alpha \notin (K_i^\times)^2$ and we have $M_i' = K_i(\sqrt{\alpha^\sigma}),\ L = K_i(\sqrt{\alpha}, \sqrt{\alpha^\sigma})$ and $M = K_i(\sqrt{\alpha\alpha^\sigma})$. So we consider a system of representatives of the square class group of K_i and take all pairs (α, α^σ) of the system such that α and α^σ are independent modulo squares, thereby obtaining all D_4-extensions $L/\mathbb{Q}_2$.

An element $x = u2^n \in \mathbb{Q}_2^\times$, where u is a unit in $\mathbb{Z}_2$, is a square if and only if n is even and $u \equiv 1 \bmod 8$. In the group U of units of $\mathbb{Z}_2$, we have $U = \{\pm 1\} \times U_2$, $U_2 \cong \mathbb{Z}_2$ and the set of squares in U_2 is $U_3 = \{a \in \mathbb{Z}_2 \mid a \equiv 1 \bmod 2^3\}$. Then $U/U_3 \cong C_2 \times C_2$ with representatives $\{\pm 1, \pm 5\}$ and $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong C_2 \times C_2 \times C_2$ with representatives $\{\pm 1, \pm 5, \pm 2, \pm 10\}$, so there are exactly seven quadratic extensions of $\mathbb{Q}_2$. Naito considers all cases and thereby constructs 18 D_4-extensions of $\mathbb{Q}_2$.

3.3.2 A group-theoretic approach

In cases in which the W-group of a field F is known, this can provide a group-theoretic alternative to the direct construction method for determining the number of D_4-extensions of F. The following proposition provides an illustration.

Proposition 3.3.1. *Let p be an odd prime. Then $\mathbb{Q}_p$ has a D_4-extension if and only if $p \equiv 3$ mod 4, and this extension is unique.*

Proof. Let $G = G_{\mathbb{Q}_p}(2)$. By [MS96, Proposition 2.1], the W-group of $\mathbb{Q}_p$, $\mathrm{Gal}(\mathbb{Q}_p^{(3)}/\mathbb{Q}_p) \cong G/G^4[G^2, G] = G^{[3]}$ and by [MS96, Corollary 2.18], $\mathbb{Q}_p^{(3)}$ is the compositum of all quadratic, C_4- and D_4-extensions of $\mathbb{Q}_p$.

$\mathbb{Q}_p$ has no D_4-extension if $p \equiv 1 \bmod 4$, since in this case [MS96, Example 4.2] shows that $G^{[3]} \cong C_4 \times C_4$, which has no quotient isomorphic to D_4.

If $p \equiv 3 \bmod 4$, then $\{1, p, -1, -p\}$ is a set of representatives of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ and [MS96, Example 4.3] shows that $G^{[3]} = \langle \sigma_p, \sigma_{-1} \mid [\sigma_p, \sigma_{-1}] = \sigma_p^2 \rangle \cong C_4 \rtimes C_4$, with the semidirect product action given by $\sigma_{-1}^{-1}\sigma_p\sigma_{-1} = \sigma_p^{-1}$. We have the group extension

$$1 \longrightarrow \langle \sigma_p^2, \sigma_{-1}^2 \rangle \cong C_2 \times C_2 \longrightarrow G^{[3]} \longrightarrow \mathrm{Gal}(\mathbb{Q}_p^{(2)}/\mathbb{Q}_p) = \langle \bar{\sigma}_p, \bar{\sigma}_{-1} \rangle \longrightarrow 1.$$

So the existence of a D_4-extension of $\mathbb{Q}_p$ is equivalent to the existence of a subgroup $H \subset \langle \sigma_p^2, \sigma_{-1}^2 \rangle$ such that

$$1 \longrightarrow H \cong C_2 \longrightarrow G^{[3]} \longrightarrow D_4 \cong C_4 \rtimes C_2 \longrightarrow 1$$

and

$$1 \longrightarrow \langle \sigma_p^2, \sigma_{-1}^2 \rangle / H \longrightarrow D_4 \longrightarrow \langle \bar{\sigma}_p, \bar{\sigma}_{-1} \rangle \longrightarrow 1$$

are group extensions.

Since D_4 is non-abelian, $\sigma_p^2 = [\sigma_p, \sigma_{-1}] \neq 1$ in D_4, and since D_4 must have one generator of order 2, $\sigma_p^2 \sigma_{-1}^2 \neq 1$ in D_4. Hence, the only possibility is $H = \langle \sigma_{-1}^2 \rangle$, so $\mathbb{Q}_p$ has exactly one D_4-extension. $\square$

3.3.3 Quaternion algebras

Often, of course, one is dealing with a field F for which the W-group is not known and the goal of counting D_4-extensions of F may be to shed light on the structure of that group. We now describe a technique of enumerating these extensions based on the theory of quaternion algebras, using the example of the field $\mathbb{Q}_p$.

Recall that for p odd, $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong C_2 \times C_2$ with representatives $\{1, p, u, up\}$ where u is not a square mod p. So we consider the quaternion algebras $(a, b)_{\mathbb{Q}_p}$ where $a, b \in \{1, p, u, up\}$ are independent modulo squares. By Proposition 3.2.2, there exists a $D_4^{a,b}$-extension of $\mathbb{Q}_p$ if and only if $(a, b)_{\mathbb{Q}_p} = 1 \in \mathrm{Br}_2(\mathbb{Q}_p)$.

If $p \equiv 1 \bmod 4$, then by [Lam05, Theorem VI.2.2], $(p, u)_{\mathbb{Q}_p}$ is a division algebra. Since -1 is a square in $\mathbb{Q}_p$, we have $(p, u)_{\mathbb{Q}_p} \cong (p, up)_{\mathbb{Q}_p} \cong (u, up)_{\mathbb{Q}_p}$, so $\mathbb{Q}_p$ has no D_4-extension.

If $p \equiv 3 \bmod 4$, we can take $u = -1$. In this case $(p, -p)_{\mathbb{Q}_p}$ splits and by the non-degeneracy of the Hilbert symbol, we see that $\{p, -p\}$ is the only choice for $\{a, b\}$. Now suppose $L_1 = F(\sqrt{a}, \sqrt{b})(\sqrt{y})$ and $L_2 = F(\sqrt{a}, \sqrt{b})(\sqrt{z})$ are two $D_4^{a,b}$-extensions of a field F. It follows from Proposition 3.2.2 that there exists an $f \in F$ such that $z = fy$. When $F = \mathbb{Q}_p$ with $p \equiv 3 \bmod 4$, we have $\sqrt{f} \in \mathbb{Q}_p^{(2)} = \mathbb{Q}_p(\sqrt{p}, \sqrt{-p})$. So

$$L_2 = \mathbb{Q}_p(\sqrt{p}, \sqrt{-p})(\sqrt{z}) = \mathbb{Q}_p(\sqrt{p}, \sqrt{-p})(\sqrt{fy}) = \mathbb{Q}_p(\sqrt{p}, \sqrt{-p})(\sqrt{y}) = L_1.$$

Hence there exists only one D_4-extension $L/\mathbb{Q}_p$ in this case.

The diagram below shows the lattice of subfields of this extension.

$$\begin{tikzcd}
 & & \mathbb{Q}_p(\sqrt[4]{p}, \sqrt{-1}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}_p(\sqrt[4]{p}) \arrow[dr, dash] & \mathbb{Q}_p(\sqrt{-\sqrt{p}}) \arrow[d, dash] & \mathbb{Q}_p(\sqrt{p}, \sqrt{-1}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}_p(\sqrt{-\sqrt{-p}}) \arrow[d, dash] & \mathbb{Q}_p(\sqrt[4]{-p}) \arrow[dl, dash] \\
 & \mathbb{Q}_p(\sqrt{p}) \arrow[dr, dash] & \mathbb{Q}_p(\sqrt{-1}) \arrow[d, dash] & \mathbb{Q}_p(\sqrt{-p}) \arrow[dl, dash] & \\
 & & \mathbb{Q}_p &
\end{tikzcd}$$

Recall that for $p = 2$, $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ is a set of representatives of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. Then by Proposition 3.2.2, there exists a $D_4^{a,b}$-extension of $\mathbb{Q}_2$ for each $\{a, b\} \subset \{-1, \pm 5, \pm 2, \pm 10\}$ such that $a \neq b$ and the quaternion algebra $(a, b)_{\mathbb{Q}_2} = 1 \in \mathrm{Br}_2(\mathbb{Q}_2) \cong \{\pm 1\}$. These are the following pairs:

$$\{-1, 2\},\ \{-1, 5\},\ \{-1, 10\},$$
$$\{2, -2\},\ \{5, -5\},\ \{10, -10\},$$
$$\{-2, -5\},\ \{-2, -10\},\ \{5, -10\}.$$

Consider, for example, the pair $\{2, -2\}$. This pair yields a $D_4^{2,-2}$-extension $L/\mathbb{Q}_2$ such that $\mathbb{Q}_2(\sqrt{2}, \sqrt{-2}) \subset L$ and $\mathrm{Gal}(L/\mathbb{Q}_2(\sqrt{-1})) \cong C_4$.

However, in this case, L is not uniquely determined. We have $y_1 := 5\sqrt{-2} \in \mathbb{Q}_2(\sqrt{-2})$ with $Ny_1 = 2 \cdot 5^2 = 2 \in \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$, so $L_1 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{2})(\sqrt{5\sqrt{-2}})$ is a $D_4^{-2,2}$-extension of $\mathbb{Q}_2$. Similarly, $y_2 := -\sqrt{-2} \in \mathbb{Q}_2(\sqrt{-2})$ has $Ny_2 = 2$, so $L_2 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{2})(\sqrt{-\sqrt{-2}}) = \mathbb{Q}_2(\sqrt{-2}, \sqrt{2})(\sqrt[4]{-2})$ is a $D_4^{-2,2}$-extension of $\mathbb{Q}_2$.

Suppose $L_1 = L_2$. Then $\sqrt{5} = (\sqrt{-2})^{-1}(\sqrt[4]{-2})(\sqrt{5\sqrt{-2}}) \in L_1 = L_2$, implying that this dihedral extension of degree 8 contains $\mathbb{Q}_2(\sqrt{-2}, \sqrt{2}, \sqrt{5})/\mathbb{Q}_2$, an elementary abelian extension of degree 8. Hence $L_1 \neq L_2$. Now let $f \in \mathbb{Q}_2 \setminus \mathbb{Q}_2^2$. If $f \in \{5(\mathbb{Q}_2^\times)^2 \cup -5(\mathbb{Q}_2^\times)^2 \cup 10(\mathbb{Q}_2^\times)^2 \cup -10(\mathbb{Q}_2^\times)^2\}$, then

$$\mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{fy_1}) = \mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{-\sqrt{-2}}) = L_2;$$
$$\mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{fy_2}) = \mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{5\sqrt{-2}}) = L_1.$$

Otherwise, $f \in \{2(\mathbb{Q}_2^\times)^2 \cup -2(\mathbb{Q}_2^\times)^2 \cup -(\mathbb{Q}_2^\times)^2$, in which case

$$\mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{fy_1}) = \mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{5\sqrt{-2}}) = L_1;$$
$$\mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{fy_2}) = \mathbb{Q}_2(\sqrt{2}, \sqrt{-2})(\sqrt{-\sqrt{-2}}) = L_2.$$

Hence, $\mathbb{Q}_2$ has exactly two $D_4^{-2,2}$-extensions. An analogous argument shows that there are exactly two $D_4^{a,b}$-extensions for each of the nine pairs $\{a, b\}$ such that $(a, b)_{\mathbb{Q}_2} = 1$, so $\mathbb{Q}_2$ has 18 D_4-extensions.

3.3.4 Complex characters and Möbius functions

In this section we turn to the more general case of finite Galois p-extensions of a local field K, where K is a finite extension of the p-adic numbers, $\mathbb{Q}_p$. Such a field is sometimes referred to as a local number field. We describe an interesting method of counting these extensions using Möbius functions and complex characters, due to M. Yamagishi [Yam95].

Let K be a field and G a finite group. Let

$$\nu(K, G) := |\{G\text{-extensions of } K\}|.$$

Let $\mathcal{G}$ be a fixed group. Define

$$\alpha_{\mathcal{G}}(G) := |\{\text{homomorphisms } \mathcal{G} \to G\}|$$
$$\beta_{\mathcal{G}}(G) := |\{\text{surjective homomorphisms } \mathcal{G} \twoheadrightarrow G\}|.$$

For any subgroup H of G, assume that $\alpha_{\mathcal{G}}(H)$ is finite. Then

$$\alpha_{\mathcal{G}}(G) = \sum_{H \leq G} \beta_{\mathcal{G}}(H),$$

so by the Möbius inversion formula

$$\beta_{\mathcal{G}}(G) = \sum_{H \leq G} \mu_G(H)\alpha_{\mathcal{G}}(H),$$

where μ_G is the Möbius function on the partially ordered set of all subgroups of G.

There is a 1-1 correspondence between the set of G-extensions of K and the set of surjective homomorphisms from the absolute Galois group of K, $G_K \twoheadrightarrow G$, modulo automorphisms of G. Let p be a prime. If G is a p-group, then G_K can be replaced by $G_K(p)$, the Galois group of the maximal p-extension of K. Also, if K is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, it is well-known that K has only finitely many algebraic extensions of given degree (inside a fixed algebraic closure of K). Hence we have

Theorem 3.3.2. *Let p be a prime, K a finite extension of $\mathbb{Q}_p$, and G a finite p-group. Let the notation be as above, with $\mathcal{G} = G_K(p)$. Then*

$$\nu(K, G) = \frac{1}{|\mathrm{Aut(G)}|} \sum_{H \leq G} \mu_G(H) \alpha_{\mathcal{G}}(H).$$

Proof. See [Yam95, Theorem 1]. □

Example 3.3.3. Let p be a prime. Suppose that G is a p-group and K is a finite extension of $\mathbb{Q}_p$ of degree $n = [K : \mathbb{Q}_p]$ which does not contain a primitive p-th root of unity. I. R. Shafarevich [Sha47] showed that the Galois group $G_K(p)$ of the maximal p-extension of K, is a free pro-p-group of rank $n+1$ and he gave an explicit formula for $\nu(K, G)$ in this case:

$$\nu(K, G) = \frac{1}{|\mathrm{Aut(G)}|} (\frac{|G|}{p^d})^{n+1} \prod_{i=0}^{d-1} (p^{n+1} - p^i),$$

where d is the minimal number of generators of G.

This formula can also be obtained from Theorem 3.3.2 as follows. Let $\mathcal{G} = G_K(p)$. Then $\alpha_{\mathcal{G}}(H) = |H|^{n+1}$ for any p-group H. By Lemma 2.5.6, we need consider only those subgroups $H \leq G$ such that $G^p[G, G] \leq H$. The number of such subgroups is $\binom{d}{i}_p$, where

$$i = \dim_{\mathbb{F}_p} \frac{H}{G^p[G, G]}.$$

Since $[G:H]=p^{d-i}$, Lemma 2.5.6 together with the identity $\binom{d}{i}_p=\binom{d}{d-i}_p$ gives

$$\begin{aligned}\sum_{H\leq G}\mu_G(H)\alpha_{\mathcal{G}}(H) &= \sum_{G^p[G,G]\leq H\leq G}\mu_G(H)\alpha_{\mathcal{G}}(H)\\ &= \sum_{i=0}^{d}\binom{d}{i}_p(-1)^{d-i}p^{\frac{1}{2}(d-i)(d-i-1)}\frac{|G|^{n+1}}{p^{(d-i)(n+1)}}\\ &= \sum_{i=0}^{d}\binom{d}{d-i}_p(-1)^{d-i}p^{\frac{1}{2}(d-i)(d-i-1)}\frac{|G|^{n+1}}{p^{(d-i)(n+1)}}\\ &= \sum_{i=0}^{d}\binom{d}{i}_p(-1)^{i}p^{\frac{1}{2}i(i-1)}\frac{|G|^{n+1}}{p^{i(n+1)}}\\ &= \frac{|G|^{n+1}}{p^{d(n+1)}}\sum_{i=0}^{d}\binom{d}{i}_p(-1)^{i}p^{\frac{1}{2}i(i-1)}(p^{n+1})^{d-i}\end{aligned}$$

Induction on d together with the identity $\binom{d+1}{i}_p=\binom{d}{i-1}_p+p^i\binom{d}{i}_p$ shows that

$$\prod_{i=0}^{d-1}(p^{n+1}-p^i)=\sum_{i=0}^{d}\binom{d}{i}_p(-1)^{i}p^{\frac{1}{2}i(i-1)}(p^{n+1})^{d-i},$$

and the result follows.

If $\mathcal{G}$ is finitely presented as:

$$\mathcal{G}=\langle x_1,x_2,\ldots,x_n \mid r_1=r_2=\cdots=r_m=1\rangle,$$

where each $r_i=r_i(x_1,x_2,\ldots,x_n)$ is a finite word in the symbols $x_1,x_2,\ldots,x_n$, then

$$\alpha_{\mathcal{G}}(G)=|\{(g_1,g_2,\ldots,g_n)\in G^n \mid r_i(g_1,g_2,\ldots,g_n)=1,\ i=1,2,\ldots,m\}|.$$

In particular, $\alpha_{\mathcal{G}}(G)$ and $\beta_{\mathcal{G}}(G)$ are finite. By the column orthogonality relations of irreducible characters

$$\begin{aligned}r_i(g_1,g_2,\ldots,g_n)=1 &\Longleftrightarrow \sum_{\chi}\chi(1)\chi(r_i(g_1,g_2,\ldots,g_n))=|G|,\\ r_i(g_1,g_2,\ldots,g_n)\neq 1 &\Longleftrightarrow \sum_{\chi}\chi(1)\chi(r_i(g_1,g_2,\ldots,g_n))=0,\end{aligned}$$

where χ runs over all irreducible complex characters of G. Hence

$$\alpha_{\mathcal{G}}(G) = \frac{1}{|G|^m} \sum_{(g_1,g_2,\ldots,g_n)\in G^n} \prod_{i=1}^{m} \sum_{\chi} \chi(1)\chi(r_i(g_1,g_2,\ldots,g_n)). \tag{3.1}$$

Now consider the case in which K is a finite extension of the p-adic field $\mathbb{Q}_p$ of degree n and assume that K contains a primitive p-th root of unity ζ_p. Then the Galois group $G_K(p)$ of the maximal p-extension of K is a Demushkin group of rank $n+2$.

Definition 3.3.4. A *Demushkin group* is a pro-p group G which satisfies the following three conditions:

1. $\dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p) < \infty$,
2. $\dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p) = 1$,
3. the cup product $H^1(G,\mathbb{F}_p) \times H^1(G,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$ is a non-degenerate bilinear form.

From the first two conditions, we see that a Demushkin group is a finitely generated pro-p group having a single relation among a minimal set of generators. These groups have been completely classified by S.P. Demushkin, J.-P. Serre, and J. Labute (see [Lab66]). Let q be the maximal power of p such that $\zeta_q \in K$. By the classification theorem of Demushkin groups [Lab66], there exist generators $x_1, x_2, \ldots, x_{n+2}$ such that the unique relation r takes one of the following forms:

(i) if $q \neq 2$ (n is even in this case), then

$$r = x_1^q[x_1,x_2][x_3,x_4]\cdots[x_{n+1},x_{n+2}]; \tag{3.2}$$

(ii) if $q = 2$ and n is odd, then

$$r = x_1^2x_2^4[x_2,x_3][x_4,x_5]\cdots[x_{n+1},x_{n+2}]; \tag{3.3}$$

(iii) if $q = 2$ and n is even, then either

$$r = x_1^{2+2^f}[x_1, x_2][x_3, x_4] \cdots [x_{n+1}, x_{n+2}], \tag{3.4}$$

where f is an integer ≥ 2 or ∞, or

$$r = x_1^2[x_1, x_2]x_3^{2^f}[x_3, x_4] \cdots [x_{n+1}, x_{n+2}], \tag{3.5}$$

where f is an integer ≥ 2.

Substituting the explicit forms of r into equation 3.1 and using the identity

$$\sum_{b,c \in G} \chi(a[b,c]) = (\frac{|G|}{\chi(1)})^2 \chi(a), \text{ for all } a \in G,$$

Yamagishi proves

Lemma 3.3.5. *Let p be a prime, K be a finite extension of $\mathbb{Q}_p$ containing a primitive p-th root of unity ζ_p, and G a finite p-group. Let $\mathcal{G} = G_K(p)$. Then*

$$\alpha_{\mathcal{G}}(G) = \begin{cases} |G|^n \sum_\chi \frac{1}{\chi(1)^n} \sum_{g \in G} \chi(g^{q-1})\chi(g) & (\textit{Case } 3.2) \\ |G|^{n-1} \sum_\chi \frac{1}{\chi(1)^{n-1}} \sum_{g,h \in G} \chi(g^2h^3)\chi(h) & (\textit{Case } 3.3) \\ |G|^n \sum_\chi \frac{1}{\chi(1)^n} \sum_{g \in G} \chi(g^{2^f+1})\chi(g) & (\textit{Case } 3.4) \\ |G|^{n-1} \sum_\chi \frac{1}{\chi(1)^{n-1}} \sum_{g,h \in G} \chi(g)\chi(gh^{2^f-1})\chi(h) & (\textit{Case } 3.5), \end{cases}$$

where $n = [K : \mathbb{Q}_p]$, q is the maximal power of p such that $\zeta_q \in K$, and χ runs over all irreducible complex characters of G.

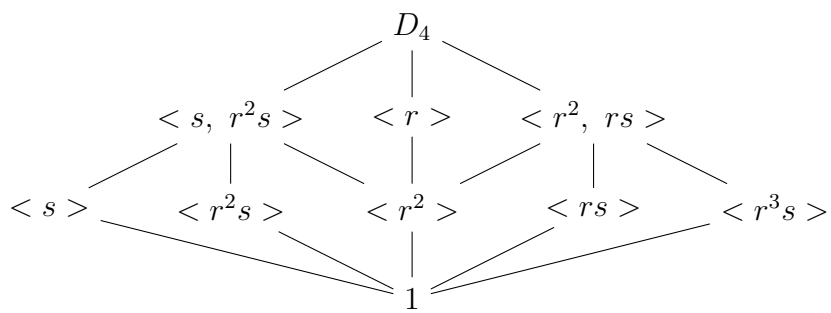
Proof. See [Yam95, Lemma 1.8]. □

Using this result, Yamagishi then derives a formula for $\nu(K, G)$ in the special cases in which G is a non-abelian group of order p^3 or is a dihedral or generalized quaternion group of order 2^m, $m \geq 3$.

Example 3.3.6. Let K be a finite extension of $\mathbb{Q}_2$ which does not contain a primitive 4-th root of unity and assume $n = [K : \mathbb{Q}_2]$ is odd. Then $\mathcal{G} := G_K(2)$ is a Demushkin group with $q = 2$ in which the unique relation among a minimal set of generators takes the form given in (3.3). Let $G = D_4$ be the dihedral group of order 8.

$$D_4 := \langle r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} \rangle,$$

with lattice of subgroups



The Frattini subgroup $\Phi(D_4) =< r^2 >$, so for $H \leq G = D_4$, Lemma 2.5.6 gives

$$\mu_G(H) = \begin{cases} 1 & \text{if } H = D_4 \\ -1 & \text{if } H =< s, r^2 s >,\ < r > \text{ or } < r^2, rs > \\ 2 & \text{if } H =< r^2 > \\ 0 & \text{otherwise} \end{cases}$$

The conjugacy classes of D_4 are $\{1\}$, $\{r^2\}$, $\{s, r^2 s\}$, $\{r, r^3\}$ and $\{rs, r^3 s\}$. The character table is shown below.

D_4	1	s	rs	r	r^2
χ_1	1	1	1	1	1
χ_{ρ_2}	1	-1	-1	1	1
χ_{ρ_3}	1	1	-1	-1	1
χ_{ρ_4}	1	-1	1	-1	1
χ_{σ_1}	2	0	0	0	-2

From Lemma 3.3.5 and the above character table, we obtain

$$\alpha_{\mathcal{G}}(D_4) = 8^{n+1}(4 + \frac{1}{2^n}).$$

If $H \leq G$ is abelian, then in order to calculate $\alpha_{\mathcal{G}}(H)$, one need consider only maps

$$\mathcal{G}/[\mathcal{G}, \mathcal{G}] \cong \mathbb{Z}_2^{n+1} \times \mathbb{Z}_2/q\mathbb{Z}_2 \to H,$$

which gives

$$\alpha_{\mathcal{G}}(H) = |H|^{n+1} \cdot |\{h \in H \mid h^q = 1\}|.$$

Hence

$$\alpha_{\mathcal{G}}(H) = \begin{cases} 4^{n+1} \cdot 4 & \text{if } H =< s, r^2 s > \text{ or } < r^2, rs > \\ 4^{n+1} \cdot 2 & \text{if } H =< r > \\ 2^{n+1} \cdot 2 & \text{if } H =< r^2 > . \end{cases}$$

So for $G = D_4$, Theorem 3.3.2 gives

$$\begin{aligned} \nu(K, G) &= \frac{1}{|\mathrm{Aut(G)}|} \sum_{H \leq G} \mu_G(H) \alpha_{\mathcal{G}}(H) \\ &= \frac{1}{2^3}(8^{n+1}(4 + \frac{1}{2^n}) - 4^{n+1} \cdot 4 - 4^{n+1} \cdot 4 - 4^{n+1} \cdot 2 + 2(2^{n+1} \cdot 2)) \\ &= 2^n(2^{n+1} - 1)^2. \end{aligned}$$

In the case $K = \mathbb{Q}_2$, we once again obtain $\nu(\mathbb{Q}_2, D_4) = 18$.

3.3.5 Cup products in cohomology

In this section, we again consider the case in which K is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers and for a finite group G, we use the notation $\nu(K, G)$ to denote the number of G-extensions of K. We describe a technique based on Galois cohomology to count the number of D_4-extensions of K.

In [MT14] J. Mináč and N. D. Tân use triple Massey products to compute $\nu(K, G)$ for $G = \mathbb{U}_4(\mathbb{F}_p)$, the group of unipotent four by four matrices over $\mathbb{F}_p$. Closely following their

approach, but using cup products instead of triple Massey products, a similar method can be employed to calculate $\nu(K, \mathbb{U}_3(\mathbb{F}_p))$.

Let G be a profinite group and p a prime. We consider the finite field $\mathbb{F}_p$ as a trivial discrete G-module. Let $\mathcal{C}^\bullet = (C^\bullet(G, \mathbb{F}_p), \delta, \cup)$ be the differential graded algebra of inhomogeneous continuous cochains of G with coefficients in $\mathbb{F}_p$ [NSW08, §I.2]. The cohomology groups are written $H^i(G, \mathbb{F}_p)$. We denote by $Z^1(G, \mathbb{F}_p)$ the subgroup of $C^1(G, \mathbb{F}_p)$ consisting of all 1-cocycles. Since G acts trivially on the coefficients $\mathbb{F}_p$, $Z^1(G, \mathbb{F}_p) = H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p)$.

Definition 3.3.7. A *weak embedding problem* $\mathcal{E} := \mathcal{E}(G, f\colon U \to \bar{U}, \varphi\colon G \to \bar{U})$ for a profinite group G is a diagram

$$\mathcal{E} := \begin{tikzcd} & G \arrow[d, "\varphi"] \\ U \arrow[r, "f"] & \bar{U} \end{tikzcd}$$

consisting of profinite groups U and $\bar{U}$ and homomorphisms $\varphi\colon G \to \bar{U}$, $f\colon U \to \bar{U}$ with f being surjective. If φ is also surjective, we call $\mathcal{E}$ an *embedding problem.*

A *weak solution* of $\mathcal{E}$ is a homomorphism $\psi\colon G \to U$ such that $f\psi = \varphi$. If ψ is surjective, the solution is said to be *proper*. We call $\mathcal{E}$ a *finite* weak embedding problem if U is finite. The *kernel* of $\mathcal{E}$ is defined to be $M := \ker(f)$. We denote by $\mathrm{Sol}(\mathcal{E})$ the set of weak solutions of $\mathcal{E}$.

Example 3.3.8. A proper solution of the embedding problem

$$\begin{tikzcd} & G_F^{[3,2]} \arrow[d, "\varphi"] \\ C_4 \arrow[r, "f"] & C_2 \end{tikzcd}$$

corresponds to a C_4-extension of F.

Suppose $\mathcal{E}(G, f\colon U \to \bar{U}, \varphi\colon G \to \bar{U})$ is a weak embedding problem with abelian kernel M. The conjugation action of U on M is trivial while restricting to $M \subseteq U$. Hence this induces a $\bar{U}$-module structure on M. We consider M to be a G-module via φ and the conjugation action of $\bar{U}$ on M. We denote this G-module by M_φ.

Lemma 3.3.9. *Let $\mathcal{E}(G, f, \varphi)$ be a weak embedding problem with finite abelian kernel M which has a weak solution. Then $\mathrm{Sol}(\mathcal{E})$ is a principal homogeneous space over the group of 1-cocycles $Z^1(G, M_\varphi)$.*

In particular, any weak solution θ of $\mathcal{E}$ induces a bijection

$$\mathrm{Sol}(\mathcal{E}) \simeq Z^1(G, M_\varphi).$$

Proof. See [NSW08, Proposition 3.5.11]. □

The group $\mathbb{U}_n(\mathbb{F}_p)$ of unipotent, $n \times n$ matrices over $\mathbb{F}_p$ is the multiplicative group of all upper-triangular $n \times n$ matrices over $\mathbb{F}_p$ which agree with the identity matrix along the diagonal. Let $Z_n(\mathbb{F}_p)$ be the subgroup of $\mathbb{U}_n(\mathbb{F}_p)$ consisting of matrices with all off-diagonal entries being zero except at position $(1, n)$, together with the identity matrix. Then $Z_n(\mathbb{F}_p)$ lies in the center of $\mathbb{U}_n(\mathbb{F}_p)$ and is isomorphic to the additive group of $\mathbb{F}_p$. The quotient group $\bar{\mathbb{U}}_n(\mathbb{F}_p) = \mathbb{U}_n(\mathbb{F}_p)/Z_n(\mathbb{F}_p)$ can be identified with the group of all upper-triangular unipotent $n \times n$ matrices over $\mathbb{F}_p$ with the $(1, n)$ entry omitted.

A representation $\rho\colon G \to \mathbb{U}_n(\mathbb{F}_p)$ is given by a component array $\rho_{ij},\ 1 \le i \le n,\ i < j \le n$, of set maps $G \to \mathbb{F}_p$ which satisfy the identities

$$\rho_{ij}(g_1 g_2) = \rho_{ij}(g_1) + \rho_{ij}(g_2) + \sum_{k=i+1}^{j-1} \rho_{ik}(g_1)\rho_{kj}(g_2), \quad g_1, g_2 \in G.$$

The maps of the form $\rho_{i,i+1}$, called the *near-diagonal components* of ρ, are then group homomorphisms $G \to \mathbb{F}_p$, and hence cohomology classes in $H^1(G, \mathbb{F}_p)$. Similarly, a representation $\rho\colon G \to \bar{\mathbb{U}}_n(\mathbb{F}_p)$ has near-diagonal components in $H^1(G, \mathbb{F}_p)$.

Dwyer [Dwy75] demonstrated a close connection between n-fold Massey products of elements in $H^1(G, \mathbb{F}_p)$ and representations $\rho\colon G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$. In particular, for the case $n = 2$, if $\rho\colon G \to \bar{\mathbb{U}}_3(\mathbb{F}_p)$ is a group homomorphism given by the components $-\rho_1, -\rho_2$, it follows from [Dwy75, Theorem 2.4] that ρ can be lifted to a group homomorphism $G \to \mathbb{U}_3(\mathbb{F}_p)$ if and only if the cup product $\rho_1 \cup \rho_2 = 0$ in $H^2(G, \mathbb{F}_p)$.

Lemma 3.3.10. *Let G be a pro-p-group. Let $\chi_1, \ldots, \chi_n$ be elements in $H^1(G, \mathbb{F}_p)$. Then*

the homomorphism

$$\varphi := (\chi_1, \ldots, \chi_n) \colon G \to \mathbb{F}_p \times \cdots \times \mathbb{F}_p$$

is surjective if and only if $\chi_1, \ldots, \chi_n$ *are* $\mathbb{F}_p$*-linearly independent in* $H^1(G, \mathbb{F}_p)$*.*

Proof. We set $H := \mathbb{F}_p \times \cdots \times \mathbb{F}_p$. Then $\varphi \colon G \to H$ is surjective if and only if the induced homomorphism $\varphi^* \colon H^1(H, \mathbb{F}_p) \to H^1(G, \mathbb{F}_p)$ is injective ([NSW08, Proposition 1.6.14 (ii)]). We have an (non-canonical) isomorphism

$$H \to H^1(H, \mathbb{F}_p), a = (a_1, \ldots, a_n) \mapsto \chi_a,$$

where χ_a is defined by $\chi_a(h_1, \ldots, h_n) = \sum_{i=1}^n a_i h_i$. Then for each $a = (a_1, \ldots, a_n) \in H$,

$$(\varphi^*(\chi_a))(g) = \sum_{i=1}^n a_i \chi_i(g), \ \forall g \in G.$$

Therefore φ^* is injective if and only if $\chi_1, \ldots, \chi_n$ are $\mathbb{F}_p$-linearly independent. □

Now consider the following exact sequence of finite groups

$$1 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{U}_3(\mathbb{F}_p) \xrightarrow{(a_{12}, a_{23})} \mathbb{F}_p \times \mathbb{F}_p \longrightarrow 1, \tag{3.6}$$

where $a_{ij} \colon \mathbb{U}_3(\mathbb{F}_p) \to \mathbb{F}_p$ is the map sending a matrix to its (i, j)-coefficient.

Let $\mathrm{CP}(G, \mathbb{F}_p)$ be the set of $(x, y) \in H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p)$ such that $x \cup y = 0$ and $x,\ y$ are $\mathbb{F}_p$-linearly independent in $H^1(G, \mathbb{F}_p)$. For two profinite groups G and H, let $\mathrm{Epi}(G, H)$ be the set of all continuous surjective homomorphisms from G to H.

Proposition 3.3.11. *Let the notation be as above. Assume that both* $\mathrm{CP}(G, \mathbb{F}_p)$ *and* $Z^1(G, \mathbb{F}_p)$ *are finite. Then*

$$|\mathrm{Epi}(G, \mathbb{U}_3(\mathbb{F}_p))| = \sum_{\varphi \in \mathrm{CP}(G, \mathbb{F}_p)} |Z^1(G, \mathbb{F}_p)|.$$

Proof. Let $\varphi = (x, y) \in \mathrm{CP}(G, \mathbb{F}_p)$. Then φ induces a homomorphism $G \to \bar{\mathbb{U}}_3(\mathbb{F}_p) \cong \mathbb{F}_p \times \mathbb{F}_p,\ g \mapsto (x(g), y(g))$ which, by Lemma 3.3.10 is surjective, since x, y are $\mathbb{F}_p$-linearly

independent in $H^1(G, \mathbb{F}_p)$. This gives an embedding problem

$$\begin{tikzcd} & G \arrow[d, "\varphi"] \\ \mathbb{U}_3(\mathbb{F}_p) \arrow[r, "f"] & \bar{\mathbb{U}}_3(\mathbb{F}_p) \end{tikzcd}$$

with kernel $\mathbb{F}_p$ which, by [Dwy75, Theorem 2.4], has a solution since $x \cup y = 0$. Hence by Lemma 3.3.9, the embedding problem has $|Z^1(G, \mathbb{F}_p)|$ solutions. Since the kernel has order p, each solution is a proper solution, so the result follows. □

Lemma 3.3.12. *Let G be a profinite group, and let $G(p)$ be its maximal pro-p-quotient. Then* $\mathrm{Epi}(G, \mathbb{U}_3(\mathbb{F}_p)) \cong \mathrm{Epi}(G(p), \mathbb{U}_3(\mathbb{F}_p))$.

Proof. This follows from the fact that $\mathbb{U}_3(\mathbb{F}_p)$ is a finite p-group. □

Assume that K is a finite extension of $\mathbb{Q}_p$. Recall that if K contains a primitive pth root of unity, then the group $G := G_K(p)$ is a Demushkin group, which is a pro-p group having the following properties:

1. $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,
2. $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$,
3. the cup product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is a non-degenerate bilinear form.

Note that since $a \cup b = -b \cup a$ for $a, b \in H^1(G, \mathbb{F}_p)$, the bilinear form $(\cdot, \cdot)\colon H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p) \cong \mathbb{F}_p$ induced by the cup product is skew-symmetric. Let $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$. Then G has a minimal presentation $G = S/R$ where S is a free pro-p-group of rank $d = d(G)$ on generators $x_1, x_2, \ldots, x_d$, and $R = \langle r \rangle$ is the closed normal subgroup of S generated by an element $r \in S^p[S, S]$. Let $q = q(G)$ be the maximal power of p such that $\zeta_q \in K$ (and by convention, $p^\infty = 0$). Recall from section 3.3.4 that the relation r takes one of the following forms:

(i) if $q \neq 2$ (d is even in this case), then

$$r = x_1^q [x_1, x_2][x_3, x_4] \cdots [x_{d-1}, x_d]; \tag{3.7}$$

(ii) if $q = 2$ and d is odd, then

$$r = x_1^2 x_2^{2^f} [x_2, x_3][x_4, x_5] \cdots [x_{d-1}, x_d], \tag{3.8}$$

where f is an integer ≥ 2 or ∞;

(iii) if $q = 2$ and d is even, then either

$$r = x_1^{2+2^f} [x_1, x_2][x_3, x_4] \cdots [x_{d-1}, x_d], \tag{3.9}$$

where f is an integer ≥ 2 or ∞, or

$$r = x_1^2 [x_1, x_2] x_3^{2^f} [x_3, x_4] \cdots [x_{d-1}, x_d], \tag{3.10}$$

where f is an integer ≥ 2.

Proposition 3.3.13. *Let G be a Demushkin group and let*

$$(\cdot, \cdot) \colon H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \xrightarrow{\cup} H^2(G, \mathbb{F}_p) \cong \mathbb{F}_p$$

be the non-degenerate skew-symmetric bilinear form induced by the cup product. Let $d = d(G)$ and $q = q(G)$.

1. *If $q \neq 2$, there exists an $\mathbb{F}_p$-basis $v_1, v_2, \ldots, v_d$ of $H^1(G, \mathbb{F}_p)$ such that $(v_i, v_i) = 0$ for every $1 \leq i \leq d$.*

2. *If $q = 2$, there exists an $\mathbb{F}_p$-basis $v_1, v_2, \ldots, v_d$ of $H^1(G, \mathbb{F}_p)$ such that $(v_1, v_1) = 1$, and that $(v_i, v_i) = 0$ for every $2 \leq i \leq d$.*

Proof. Let

$$1 \longrightarrow R \longrightarrow S \longrightarrow G \longrightarrow 1,$$

be a minimal presentation of G, with minimal system of generators $x_1, x_2, \ldots, x_d$.

By [NSW08, Proposition 3.9.12], there exists an $\mathbb{F}_p$-basis $v_1, v_2, \ldots, v_d$ of $H^1(S, \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$ such that $v_i(x_j) = \delta_{ij}$, where δ is the Kronecker delta function.

Suppose $q = p^k \neq 2$. If $p > 2$ then $(v_i, v_i) = 0$ for every $i = 1, 2, \ldots, d$ since a skew-symmetric bilinear form on a vector space over a field of characteristic $\neq 2$ is alternating. From [NSW08, Proposition 3.9.13] applied to the descending 2-central series $(S^{(i)})$ of S, if the defining relation r of G is such that

$$r \equiv \prod_{j=1}^{d} x_j^{2a_j} \cdot \prod_{1 \leq l < m \leq d} (x_l, x_m)^{a_{lm}} \mod S^{(3)}, \quad a_j, a_{lm} \in \mathbb{F}_2,$$

then $(v_j, v_j) = a_j$. If $q = 2^k$ with $k \geq 2$, then r takes the form shown in equation (3.7) above, so $(v_i, v_i) = a_i = 0$ for all $i = 1, 2 \ldots, d$. This establishes part 1.

Now suppose $q = 2$. Then r takes the form shown in equation (3.8), (3.9) or (3.10) above. In each of these cases, $(v_1, v_1) = a_1 = 1$ and $(v_i, v_i) = a_i = 0$ for all $i = 2, 3, \ldots, d$, which establishes part 2. □

When G is a Demushkin group, the following result, based on linear algebra, provides a means of calculating $|\mathrm{CP}(G, \mathbb{F}_p)|$ from $d(G)$ and $q(G)$.

Lemma 3.3.14. *Let V be an $\mathbb{F}_p$-vector space of dimension $d \geq 3$ with with basis $v_1, v_2, \ldots, v_d$. Let $(\cdot, \cdot)\colon V \times V \to \mathbb{F}_p$ be a non-degenerate skew-symmetric bilinear form on V. Let N be the number of pairs $(x, y) \in V \times V$ such that $(x, y) = 0$ and that x, y are $\mathbb{F}_p$-linearly independent.*

1. *If $(v_i, v_i) = 0$ for every $1 \leq i \leq d$, then*

$$N = (p^d - 1)(p^{d-1} - p).$$

2. *If $(v_1, v_1) = 1$ and $(v_i, v_i) = 0$ for every $2 \leq i \leq d$, then*

$$N = (2^{d-1} - 1)(2^{d-1} - 2) + 2^{d-1}(2^{d-1} - 1).$$

Proof. For each $y \in V \setminus \{0\}$, let

$$y^{\perp} = \{x \in V \mid (x, y) = 0\}.$$

Then $y^\perp$ is an $\mathbb{F}_p$-vector space, and $\dim y^\perp = \dim V - 1 = d - 1$ since the bilinear form $(\cdot,\cdot)$ is non-degenerate. Let

$$\begin{aligned} C(y) :&= \{x \in V \mid (x,y) = 0 \text{ and } x, y \text{ are } \mathbb{F}_p\text{-linearly independent}\} \\ &= \{x \in y^\perp \mid x, y \text{ are } \mathbb{F}_p\text{-linearly independent}\}. \end{aligned}$$

Case 1. Let $y = \sum_{i\in I} a_i v_i$, $a_i \in \mathbb{F}_p$, $I \subseteq \{1, 2, \ldots, d\}$. Then

$$\begin{aligned} (y,y) &= (\sum_{i\in I} a_i v_i, \sum_{j\in I} a_j v_j) = \sum_{i,j\in I} a_i a_j (v_i, v_j) \\ &= \sum_{i\in I} a_i^2 (v_i, v_i) + \sum_{\substack{i<j,\\ i,j\in I}} a_i a_j ((v_i, v_j) + (v_j, v_i)) \\ &= 0, \end{aligned}$$

since $(\cdot,\cdot)$ is skew-symmetric and, by assumption, $(v_i, v_i) = 0$ for $1 \le i \le d$. So $y \in y^\perp$. Hence

$$|C(y)| = (p^{d-1} - p).$$

This gives

$$N = \sum_{y\in V\setminus\{0\}} |C(y)| = (p^d - 1)(p^{d-1} - p).$$

Case 2. In this case $p = 2$. Let $y = \sum_{i\in I} v_i$, $I \subseteq \{1, 2, \ldots, d\}$. There are two possibilities to consider:

(i) $1 \notin I$. Then $(v_i, v_i) = 0$ for all $i \in I$, so by the same argument as Case 1 above, $y \in y^\perp$. Hence

$$|C(y)| = (2^{d-1} - 2).$$

(ii) $1 \in I$. Let $I' := I \setminus \{1\}$. Then $(v_i, v_i) = 0$ for all $i \in I'$, so

$$\begin{aligned}(y, y) &= (v_1 + \sum_{i \in I'} v_i, v_1 + \sum_{i \in I'} v_i) \\ &= (v_1, v_1) + (v_1, \sum_{i \in I'} v_i) + (\sum_{i \in I'} v_i, v_1) + (\sum_{i \in I'} v_i, \sum_{i \in I'} v_i) \\ &= (v_1, v_1) \\ &= 1,\end{aligned}$$

since $(\cdot, \cdot)$ is skew-symmetric, and $(\sum_{i \in I'} v_i, \sum_{i \in I'} v_i) = 0$ by part (i). So $y \notin y^\perp$. Hence,

$$|C(y)| = |y^\perp \setminus \{0\}| = (2^{d-1} - 1).$$

Combining the two possibilities gives

$$\begin{aligned}N &= \sum_{y \text{ in case (i)}} |C(y)| + \sum_{y \text{ in case (ii)}} |C(y)| \\ &= (2^{d-1} - 1)(2^{d-1} - 2) + 2^{d-1}(2^{d-1} - 1).\end{aligned}$$

□

Let K be a finite extension of degree n of $\mathbb{Q}_p$ and assume that K contains a primitive p-th root of unity. Then the Galois group $G := G_K(p)$ of the maximal p-extension of K is a Demushkin group of rank $n+2$. Recall that the number of $\mathbb{U}_3(\mathbb{F}_p)$-extensions of K is given by

$$\nu(K, \mathbb{U}_3(\mathbb{F}_p)) = \frac{|\mathrm{Epi}(G_K, \mathbb{U}_3(\mathbb{F}_p))|}{|\mathrm{Aut}(\mathbb{U}_3(\mathbb{F}_p))|},$$

where G_K is the absolute Galois group of K. Since $|Z^1(G, \mathbb{F}_p)| = |H^1(G, \mathbb{F}_p)| = p^{n+2}$, Proposition 3.3.11 together with Lemma 3.3.12 gives

$$|\mathrm{Epi}(G_K, \mathbb{U}_3(\mathbb{F}_p))| = |\mathrm{Epi}(G, \mathbb{U}_3(\mathbb{F}_p))| = \sum_{\varphi \in \mathrm{CP}(G, \mathbb{F}_p)} |Z^1(G, \mathbb{F}_p)| = |\mathrm{CP}(G, \mathbb{F}_p)| \cdot p^{n+2}.$$

Since G is a Demushkin group, the cup product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \xrightarrow{\cup} H^2(G, \mathbb{F}_p) \cong \mathbb{F}_p$ is a non-degenerate skew-symmetric bilinear form. If $q = q(G)$ is the q-invariant of G,

then by Lemma 3.3.14

$$|\mathrm{CP}(G,\mathbb{F}_p)| = \begin{cases} (p^{n+2}-1)(p^{n+1}-p) & \text{if } p>2, \\ (2^{n+2}-1)(2^{n+1}-2) & \text{if } p=2 \text{ and } q>2, \\ (2^{n+1}-1)(2^{n+1}-2)+2^{n+1}(2^{n+1}-1) & \text{if } p=2 \text{ and } q=2. \end{cases}$$

Note also that

$$|\mathrm{Aut}(\mathbb{U}_3(\mathbb{F}_p))| = \begin{cases} p^3(p^2-1)(p-1) & \text{if } p>2, \\ 8 & \text{if } p=2. \end{cases}$$

Therefore

$$\nu(K,\mathbb{U}_3(\mathbb{F}_p)) = \frac{|\mathrm{CP}(G,\mathbb{F}_p)|\cdot p^{n+2}}{|\mathrm{Aut}(\mathbb{U}_3(\mathbb{F}_p))|} = \begin{cases} \dfrac{p^n(p^{n+2}-1)(p^n-1)}{(p^2-1)(p-1)} & \text{if } p>2, \\ 2^n(2^n-1)(2^{n+2}-1) & \text{if } p=2 \text{ and } q>2, \\ 2^n(2^{n+1}-1)^2 & \text{if } p=2 \text{ and } q=2. \end{cases}$$

3.4 Formally Real Pythagorean Fields

Definition 3.4.1. A field F is called *pythagorean* if every sum of two squares (hence any number of squares) in F is a square. For any field F, the set of elements of F that can be expressed as a sum of squares will be denoted $\sum F^2$. If F is pythagorean then $\sum F^2 = F^2$.

Definition 3.4.2. A field F is *formally real* if F satisfies the following (equivalent) conditions:

1. -1 is not a sum of squares in F.

2. For any $n \in \mathbb{N}$, the quadratic form $n\langle 1\rangle = \langle 1,\ldots,1\rangle$ is anisotropic over F.

Otherwise, F is said to be *nonreal*.

If F is a nonreal pythagorean field then for any $a \in F$, there exist $x,\ y,\ z \in F$ such that

$$a = x^2 - y^2 = x^2 + z^2y^2 \in F^2,$$

so F is quadratically closed. Hence, our interest will be in formally real pythagorean fields.

Definition 3.4.3. Let F be a field. A subset P of F is called a *preordering* of F if

$$P + P \subseteq P, \quad P \cdot P \subseteq P, \quad -1 \notin P, \quad \sum F^2 \subseteq P.$$

A preordering of a field F is an *ordering* if in addition

$$P \cup -P = F, \quad P \cap -P = 0.$$

An *ordered field* is a pair consisting of a field F and an ordering P of F. If P is an ordering of F, the elements of $P^\times = P \setminus \{0\}$ are called *positive*, the elements of $-P^\times$ are called *negative* (with respect to P). An element $b \in F^\times$ is said to be *totally positive* if it is positive with respect to all orderings on F. The set of all orderings of F will be denoted X_F.

Artin and Schreier, in the 1920's, developed much of the algebraic theory of formally real fields and studied the relationship between formally real fields and fields with orderings. We have the following important results.

Theorem 3.4.4 (Artin-Schreier Criterion, [AS27])**.** *A field F is formally real if and only if F possesses at least one ordering.*

Theorem 3.4.5 ([Sch85, Chapter 3, Theorem 1.6])**.** *Let F be a formally real field and P a preordering of F. Then $P = \cap R$, where the intersection is taken over all orderings R containing P.*

Theorem 3.4.6 (Artin's Theorem, [Art27])**.** *For a field F of characteristic $\neq 2$, an element $b \in F^\times$ is totally positive if and only if $b \in \sum F^2$.*

We now wish to consider formally real pythagorean fields with a view toward counting their dihedral extensions. We begin with

Lemma 3.4.7. *Let F be a formally real pythagorean field with set of orderings X_F and let $a \in F^\times \setminus (F^\times)^2$. Then*

$$D_F\langle 1, -a\rangle = \bigcap_{P \in X_F, -a \in P} P^\times.$$

Proof. Consider the set $F^2 - aF^2 = \{x^2 - ay^2 \mid x, y \in F\}$. Since F is pythagorean, $\sum F^2 = F^2$, so this set is closed under addition and multiplication. If $-1 = x^2 - ay^2$, then $y \neq 0$ so $a = (x/y)^2 + (1/y)^2 \in F^2$, a contradiction. Hence $F^2 - aF^2$ is a preordering of F. Also, if $P \in X_F$, then since $F^2 \subseteq P$, we have $F^2 - aF^2 \subseteq P$ if and only if $-a \in P$. So by Theorem 3.4.5,

$$D_F\langle 1, -a\rangle \cup \{0\} = F^2 - aF^2 = \bigcap_{P \in X_F, -a \in P} P.$$

□

Lemma 3.4.8. *Let $n \in \mathbb{N}$ and let F be a formally real pythagorean field with set of orderings X_F. If $|F^\times/(F^\times)^2| = 2^n$, then $n \leq |X_F| \leq 2^{n-1}$.*

Proof. For any $P \in X_F$, $P^\times$ is a subgroup of index 2 in $F^\times$. The map

$$F^\times \to \prod_{P \in X_F} F^\times/P^\times, \quad a \mapsto (a \mod P)_{P \in X_F}$$

has kernel $\bigcap_{P \in X_F} P^\times$, which is $\sum (F^\times)^2 = (F^\times)^2$ by Artin's Theorem and the fact that F is pythagorean. So we have an injective map

$$F^\times/(F^\times)^2 \hookrightarrow \prod_{P \in X_F} \{\pm 1\}.$$

Hence $2^n = |F^\times/(F^\times)^2| \leq 2^{|X_F|}$, so $n \leq |X_F|$.

Since F is formally real, we can choose a basis $\{-1, a_1, \ldots, a_{n-1}\}$ of $F^\times/(F^\times)^2$. For any $P \in X_F$, $-1 \notin P$ and for each $i = 1, \ldots, n-1$, we have exactly one of $a_i \in P$ or $-a_i \in P$. Each ordering P could be labelled accordingly, so F can have at most 2^{n-1} orderings. □

3.4.1 Extensions of SAP fields

In this section, we develop a method for counting D_4-extensions of a formally real pythagorean field having the minimal number of orderings.

Definition 3.4.9. A formally real pythagorean field F with finite square class group $F^\times/(F^\times)^2$ is said to have the *Strong Approximation Property* (or to be *SAP*) if for any subset $\{P_1, \dots P_s\}$ of orderings of F, there exists $a \in F^\times$ such that

$$a \in \bigcap_{i=1}^{s} P_i, \quad a \notin P \text{ for all } P \neq P_i,\ i = 1, \dots, s.$$

Recall from sections 2.2, 2.3 and 2.4 that for a field F with $\mathrm{char}(F) \neq 2$, we have the maps

$$F^\times/(F^\times)^2 \cong H^1(G_F, \mathbb{F}_2) = H^1(G_F(2), \mathbb{F}_2), \quad a \mapsto (a),$$

and

$$F^\times/(F^\times)^2 \times F^\times/(F^\times)^2 \to H^2(G_F, \mathbb{F}_2) \cong \mathrm{Br}_2(F), \quad (a, b) \mapsto (a) \cup (b) \mapsto (a, b)_F.$$

Lemma 3.4.10. *Let F be a formally real pythagorean SAP field with finite square class group of cardinality 2^n. There exists a basis $\mathcal{B} = \{a_1, \dots, a_n\}$ for $F^\times/(F^\times)^2$ such that for all $a, b \in F^\times/(F^\times)^2$, $(a) \cup (b) = 0$ if and only if there is no common basis element $a_i \in \mathcal{B}$ entering the expressions for both a and b.*

Proof. Let F be a formally real pythagorean SAP field with $|F^\times/(F^\times)^2| = 2^n$ and let X_F be the set of orderings of F. Since F is SAP, for each $P_i \in X_F$ we can choose

$$a_i \in \bigcap_{P \in X_F,\ P \neq P_i} P \setminus P_i.$$

Suppose $a_{i_1} \cdots a_{i_r} = 1$ in $F^\times/(F^\times)^2$, where $i_j \neq i_k$ if $j \neq k$. Then since $a_{i_2}, \dots, a_{i_r} \in P_{i_1}$, we have $a_{i_1} = a_{i_2} \cdots a_{i_r} \in P_{i_1}$, a contradiction. Hence the a_i's are independent mod $(F^\times)^2$ which implies $|X_F| \leq n$. Then, by Lemma 3.4.8, $|X_F| = n$, so $\mathcal{B} = \{a_1, \dots, a_n\}$ is a basis of $F^\times/(F^\times)^2$.

Now for all $i \neq j$, we have

$$\begin{aligned} D_F < 1, -a_i >: &= \{x^2 - a_i y^2 \mid x, y \in F\} \setminus \{0\} \\ &= \bigcap_{P \in X_F,\ -a_i \in P} P^\times \\ &= \bigcap_{P \in X_F,\ a_i \notin P} P^\times \\ &= P_i^\times. \end{aligned}$$

Hence $a_j \in D_F < 1, -a_i >$, which implies $(a_i) \cup (a_j) = 0$ in $H^2(G_F(2), \mathbb{F}_2)$.

Working modulo squares, any given $a, b \in F^\times$ can be expressed in the basis $\{a_1, \ldots, a_n\}$. Let $c = \prod a_i$, where the product is taken over all elements a_i which occur in the expression for both a and b. From the bilinearity of the cup product and the fact that $(a_i) \cup (a_j) = 0$ if $i \neq j$, we have $(a) \cup (b) = (c) \cup (c)$. The quaternion algebra $(c, c)_F \cong (c, -1)_F$ and $(c, -1)_F$ splits if and only if c is a sum of squares in F. Since F is pythagorean, the result follows. □

Now let $K = F(\sqrt{a}, \sqrt{b}),\ a, b \in F^\times$ be a V_4-extension and recall that K/F embeds into a D_4-extension L/F if and only if $(a) \cup (b) = 0$, and in that case, the possible extensions are

$$L = K(\sqrt{f\gamma}),\ \text{where } f \in F^\times,\ \gamma \in F(\sqrt{a}) \text{ with } N_{F(\sqrt{a})/F}(\gamma) = b.$$

Lemma 3.4.11. *Let* $\mathcal{S} = \{(a, b) \in F^\times/(F^\times)^2 \times F^\times/(F^\times)^2 \mid (a) \cup (b) = 0,\ a, b \neq 1\}$. *Then*

$$|\mathcal{S}| = 3^n - 2^{n+1} + 1.$$

Proof. Suppose a is expressed as a product of elements of the basis $\mathcal{B}$ of Lemma 3.4.10, and similarly for b. That is, $a = a_{i_1} \cdots a_{i_r},\ b = a_{j_1} \cdots a_{j_s}$. Since $(a) \cup (b) = 0$, there is no element of $\mathcal{B}$ common to the expression of both a and b. So $2 \leq k = r + s \leq n$. Now choose a subset $\mathcal{A}$ of $\mathcal{B}$ of size k and consider all subsets $\mathcal{C}$ of $\mathcal{A}$ such that $\mathcal{C} \neq \varnothing$ and $\mathcal{C} \neq \mathcal{A}$. There are $2^k - 2$ such subsets $\mathcal{C}$. We take a to be the product of the elements of $\mathcal{C}$ and b the product of the elements of $\mathcal{A} \setminus \mathcal{C}$. This gives $\sum_{k=2}^{n} \binom{n}{k}(2^k - 2)$ ordered pairs

(a, b). Using the binomial identity $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ gives

$$\begin{aligned}
|\mathcal{S}| &= \sum_{k=2}^{n} \binom{n}{k} (2^k - 2) \\
&= \sum_{k=2}^{n} \binom{n}{k} 2^k - 2 \sum_{k=2}^{n} \binom{n}{k} \\
&= \sum_{k=0}^{n} \binom{n}{k} 2^k - 2 \sum_{k=0}^{n} \binom{n}{k} + 1 \\
&= 3^n - 2^{n+1} + 1.
\end{aligned}$$

□

Putting everything together we have

Theorem 3.4.12. *Let F be a formally real pythagorean SAP field with $|F^\times/(F^\times)^2| = 2^n$, $n \geq 2$ and let $\mathcal{N}$ be the number of D_4-extensions of F. Then*

$$\mathcal{N} = 2^{n-3}(3^n - 2^{n+1} + 1).$$

Proof. Using the notation of the previous lemma and preceding discussion, the number of biquadratic extensions $K = F(\sqrt{a}, \sqrt{b})$ which embed into a D_4-extension L/F is given by the number of unordered pairs $\{a, b\}$ such that $(a) \cup (b) = 0$. For each such pair, there is a $1-1$ correspondence between $\{L/F \mid K/F \subset L/F,\ Gal(L/F) \cong D_4\}$ and $\{f \mid f \in F^\times/((F^\times)^2 \cup a(F^\times)^2 \cup b(F^\times)^2 \cup ab(F^\times)^2)\}$. Hence

$$\begin{aligned}
\mathcal{N} &= (\frac{1}{2}|\mathcal{S}|)(2^{n-2}) \\
&= 2^{n-3}(3^n - 2^{n+1} + 1).
\end{aligned}$$

□

Examples 3.4.13. We have the following results for the first few values of n.

$$\begin{array}{ll} n=2 & \mathcal{N}=1 \\ n=3 & \mathcal{N}=12 \\ n=4 & \mathcal{N}=100 \\ n=5 & \mathcal{N}=720 \\ n=6 & \mathcal{N}=4816 \\ n=7 & \mathcal{N}=30912 \\ n=8 & \mathcal{N}=193600 \end{array}$$

Now consider the extension field $K = F(\sqrt{-1})$ and its quadratic closure $K(2)$. We will show that Lemma 3.4.10 is useful not only in allowing us to count extensions of F, but also in elucidating the structure of the subgroup $G_K(2)$ of $G_F(2)$. First, we recall the following lemma due to Bass and Tate.

Lemma 3.4.14. *Let p be a prime. If E is a field which has no nontrivial finite extensions of degree less than p and L/E is an extension of degree p, then $K_2(L)$ is generated by the symbols (e,l) with $e \in E^\times$, $l \in L^\times$.*

Proof. See [Sri95, Lemma 8.6] □

Proposition 3.4.15. *Let F be a formally real pythagorean SAP field with $|F^\times/(F^\times)^2| = 2^n$ and let $K = F(\sqrt{-1})$. Then $G_K(2)$ is a free pro-2 group of rank 2^{n-1}.*

Proof. Let $a \in F^\times$ and $b \in K^\times$. The corestriction map

$$cor : H^2(G_K(2), \mathbb{F}_2) \longrightarrow H^2(G_F(2), \mathbb{F}_2)$$

is given by $cor((a) \cup (b)) = (a) \cup (N_{K/F}(b))$. Since F is pythagorean, $N_{K/F}(b) = (1)$ and $cor((a) \cup (b)) = 0$. By Lemma 3.4.14 and Merkurjev's Theorem, $H^2(G_K(2), \mathbb{F}_2)$ is generated by the cup products $((f) \cup (k))$ with $f \in F^\times$, $k \in K^\times$. Hence cor is the zero map.

From Arason's long exact sequence [Ara75] we obtain

$$0 \longrightarrow F^\times/(F^\times)^2 \xrightarrow{\bullet\cup(-1)} H^2(G_F(2),\mathbb{F}_2) \xrightarrow{res} H^2(G_K(2),\mathbb{F}_2) \longrightarrow 0.$$

Once again working modulo squares, any given $e, f \in F^\times$ can be expressed in the basis $\mathcal{B} = \{a_1, \ldots, a_n\}$ of Lemma 3.4.10. Let $c = \prod a_i$, where a_i enters the expression for both e and f. Then by the bilinearity of the cup product and Lemma 3.4.10 we have

$$\begin{aligned} res((e)\cup(f)) &= res((c)\cup(c)) \\ &= res((-1)\cup(c)) \\ &= 0. \end{aligned}$$

So by Merkurjev's Theorem, $res : H^2(G_F(2),\mathbb{F}_2) \twoheadrightarrow H^2(G_K(2),\mathbb{F}_2)$ is the zero map. Hence $G_K(2)$ is a free pro-2 group.

From the short exact sequence

$$0 \longrightarrow \{(F^\times)^2 \bigcup -(F^\times)^2\} \longrightarrow F^\times/(F^\times)^2 \longrightarrow K^\times/(K^\times)^2$$

$$\xrightarrow{0} N(K^\times)/(F^\times)^2 \longrightarrow 0$$

we see that $|K^\times/(K^\times)^2| = 2^{n-1}$. So the rank of $G_K(2)$ is $n-1$. □

In the next section we go on to consider the group $G_F(2)$ for the case in which F is a formally real pythagorean SAP field and also the case in which F is a superpythagorean field.

3.4.2 The group $G_F(2)$

Theorem 3.4.16. *Let F be a field with $|F^\times/(F^\times)^2| = 2^{d+1}$, $d \geq 0$. Then F is a formally real pythagorean SAP field if and only if $G_F(2) \cong C_2 * \cdots * C_2$, the free product of $d+1$ copies of C_2.*

Proof. Suppose F is a formally real pythagorean SAP field with space of orderings X_F.

Then $|X_F| = d+1$ and by [Lam83, Theorem 17.4], a decomposition of X_F into its connected components is given by $X_F = \bigoplus_{i=1}^{d+1} X_i$ where $|X_i| = 1$ for each $i = 1, \ldots, d+1$. It then follows from [Min86] that $G_F(2)$ is isomorphic to the free product of $d+1$ copies of C_2.

Conversely, suppose that $G_F(2) \cong C_2 * \cdots * C_2$ ($d+1$ copies). Then $G_F(2)$ is generated by $d+1$ involutions, so F is pythagorean and formally real. Hence $\langle 1, 1\rangle_F$ is not universal. In this case, R. Ware [War79] showed that $G_F(2)$ determines the Witt ring $W(F)$ of F. By [MS96, Theorem 3.8] and [MS90, Corolllary 2.10], the Witt ring $W(F)$ determines the space of orderings X_F of F. It then follows from the "only if" part that $|X_F| = d+1$, so F is an SAP field. □

Corollary 3.4.17. *Let F be any pythagorean field, and let K be a pythagorean SAP field. Assume that $|F^\times/(F^\times)^2| = |K^\times/(K^\times)^2| = 2^{d+1}$. Then there exists an epimorphism $G_K(2) \cong C_2 * \cdots * C_2 \twoheadrightarrow G_F(2)$.*

Proof. By Lemma 3.4.8, F has at least $d+1$ orderings, and we can choose $d+1$ involutions $\sigma_1, \ldots, \sigma_{d+1}$ in $G_F(2)$ which minimally generate $G_F(2)$. The statement then follows from the previous theorem. □

We now wish to look at the case in which F is a superpythagorean field. Recall that a formally real pythagorean field F with $|F^\times/(F^\times)^2| = 2^{d+1} < \infty$ is called superpythagorean if F admits exactly 2^d orderings. We consider the group $G := \mathbb{Z}_2^d \rtimes C_2 = H \rtimes \langle x\rangle$, where the semidirect product action of C_2 on $H := \mathbb{Z}_2^d$ is given by $xyx = y^{-1}$, for all $y \in H$.

Proposition 3.4.18. *Let F be a pythagorean field with $|F^\times/(F^\times)^2| = 2^{d+1}$, $d \geq 0$. Then there exists an epimorphism $G_F(2) \twoheadrightarrow G = \mathbb{Z}_2^d \rtimes C_2$.*

Proof. Choose any ordering P in F and an $\mathbb{F}_2$-basis $[a_1], \ldots, [a_d]$ of $P^\times/(F^\times)^2$. By [Bec74] there exists a field E, called the Euclidean closure of F with respect to P, such that $F(2) = E(\sqrt{-1})$, E is a formally real field and $E^2 \cap F = P$. For each a_i, $i = 1, \ldots, d$, there exists a sequence

$$\sqrt{a_i}, \sqrt[4]{a_i}, \ldots, \sqrt[2^n]{a_i}, \ldots,$$

such that $\sqrt[2^n]{a_i} \in E^\times$ for all $n \in \mathbb{N}$. Indeed, by induction on n, we may assume that $\sqrt[2^n]{a_i} \in E^\times$. Then since $E^\times = (E^\times)^2 \cup -(E^\times)^2$, we can choose $\sqrt[2^{n+1}]{a_i} \in (E^\times)^2$. Now let

$$\tilde{M} := \bigcup_{n=1}^{\infty} F(\sqrt[2^n]{a_1}, \ldots, \sqrt[2^n]{a_d}).$$

Then $\tilde{M}$ is formally real since $\tilde{M}$ is a subfield of E. For each $n \in \mathbb{N}$, $F(\sqrt{-1})$ contains a primitive 2^n-th root of unity ζ_{2^n} (see [Bec78, Chapter II, Theorem 8]) and we may also assume that $\zeta_{2^{n+1}}^2 = \zeta_{2^n}$. Let $M := \tilde{M}(\sqrt{-1})$. Then M/F is a Galois extension.

We now show that $\mathrm{Gal}(M/F\sqrt{-1})$ is isomorphic to $\mathbb{Z}_2^d$. This follows from Kummer theory. Let $\tau_1, \ldots, \tau_d$ be elements in $\mathrm{Gal}(M/F(\sqrt{-1})$ such that for each $i = 1, \ldots, d$,

$$\tau_i(\sqrt[2^n]{a_i}) = \zeta_{2^n} \sqrt[2^n]{a_i} \text{ and } \tau_i(\sqrt[2^n]{a_j}) = \sqrt[2^n]{a_j}, \ \forall j \neq i.$$

Then $\mathrm{Gal}(M/F(\sqrt{-1})) = \prod_{i=1}^d \langle \tau_i \rangle \cong \mathbb{Z}_2^d$.

The restriction of a nontrivial element of $\mathrm{Gal}(E(\sqrt{-1})/E)$ to M gives a nontrivial element $\sigma \in \mathrm{Gal}(M/\tilde{M})$. Thus we have a splitting

$$\mathrm{Gal}(M/F) \cong \mathrm{Gal}(M/F\sqrt{-1}) \rtimes \langle \sigma \rangle,$$

where $\langle \sigma \rangle \cong C_2$, and the action of C_2 on $\mathrm{Gal}(M/F\sqrt{-1})$ is by involution.

The natural projection

$$G_F(2) = \mathrm{Gal}(F(2)/F) \to \mathrm{Gal}(M/F) \cong \mathbb{Z}_2^d \rtimes C_2$$

gives the desired epimorphism. □

Corollary 3.4.19. *Let F be a a field with $|F^\times/(F^\times)^2| = 2^{d+1}$. Then F is a superpythagorean field if and only if $G_F(2)$ is isomorphic to the group $G = \mathbb{Z}_2^d \rtimes C_2$.*

Proof. Assume that F is a superpythagorean field with $|F^\times/(F^\times)^2| = 2^{d+1}$. Let the notation be as in the previous proposition. Then $\mathrm{Gal}(M/F) \cong G = \mathbb{Z}_2^d \rtimes C_2$. On the other hand, from [War78, Example 3.8, (ii)] (see also [Bec78, Chapter III, Theorem 1]), we know that $\mathrm{Gal}(M/F)$ is equal to $G_F(2)$. Hence $G_F(2) \cong \mathbb{Z}_2^d \rtimes C_2$.

The converse direction is proved in a similar fashion to the proof of the "if" part in Theorem 3.4.16. □

Corollary 3.4.20. *Let F be any Pythagorean field, and let K be a superpythagorean field. Assume that $|F^\times/(F^\times)^2| = |K^\times/(K^\times)^2| = 2^{d+1}$. Then there exists an epimorphism $G_F(2) \twoheadrightarrow G_K(2) \cong \mathbb{Z}_2^d \rtimes C_2$.*

Proof. This follows from the previous proposition and corollary. □

We will consider these groups further in sections 4.3 and 4.4 when we look at dimensions of Zassenhaus filtration subquotients.

Chapter 4

Dimensions of Zassenhaus Filtration Subquotients

Central filtrations of profinite groups have a close connection with Galois theory. In 1947, Shafarevich [Sha47] observed that for certain fields not containing primitive p-th roots of unity, one could show the Galois groups of their maximal p-extensions were free pro-p groups by looking at the cardinality of filtration quotients.

Early work by Witt [Wit37b] established a correspondence between free Lie rings and the higher commutator groups of free groups. This idea has subsequently been very fruitful in the study and classification of pro-p groups, one example being the important work of Labute on Demushkin groups [Lab66] and mild pro-p groups [Lab06].

Recall that for a group G and a prime number p, the descending central series (G_n) of G is defined inductively by

$$G_1 = G, \quad G_{n+1} = [G_n, G]$$

and the Zassenhaus (p-)filtration $(G_{(n)})$ of G is defined inductively by

$$G_{(1)} = G, \quad G_{(n)} = G^p_{(\lceil n/p \rceil)} \prod_{i+j=n} [G_{(i)}, G_{(j)}],$$

[0]A version of this chapter is to appear in the Israel Journal of Mathematics [MRT15].

where $\lceil n/p \rceil$ is the least integer which is greater than or equal to n/p.

Given a free Lie ring L on d generators and a free group S on d generators, Witt showed that there is an isomorphism between the additive group of the homogeneous elements of degree n in L and the multiplicative group S_n/S_{n+1}.

Our focus in this chapter will be primarily on the Zassenhaus filtration. We will develop a method for determining the $\mathbb{F}_p$-dimension of subquotients of this filtration in the case of finitely generated pro-p groups and derive an explicit formula for these subquotient dimensions for various families of groups, including free pro-p groups, Demushkin groups and free pro-2 products of finitely many copies of the cyclic group of order 2. Galois theory provides much of the underlying motivation as many of these groups are realizable as Galois groups of maximal p-extensions of certain fields, including local fields and formally real pythagorean fields.

In section 4.1 we define, for a finitely generated pro-p group G,

$$c_n(G) := \dim_{\mathbb{F}_p}(G_{(n)}/G_{(n+1)})$$

and note that $c_n(G)$ is finite for every $n \geq 1$. We show in Lemma 4.2.1 that the numbers $c_n(G)$ are sufficient to characterize finitely generated free pro-p groups in the family of all finitely generated pro-p groups. In Remarks 4.2.4 and 4.4.4, we observe that in some interesting cases, the two numbers $c_1(G)$ and $c_2(G)$ alone are sufficient to determine G. We also observe that if G is a free pro-p group or a Demushkin group, the minimal number of topological generators of $G_{(n)}$ can be calculated from the dimensions $c_n(G)$. In section 4.2 an interesting connection between these dimensions and the Kernel Unipotent Conjecture is also explored.

4.1 The Hilbert-Poincaré Series

The Hilbert-Poincaré series is an important tool which allows us to study filtrations of profinite groups from the group algebra standpoint.

Definition 4.1.1. Let R be a unital commutative ring and $V = \bigoplus_{i=0}^{\infty} V_n$ a graded free

R-module. V is called *locally finite* if $\mathrm{rank}_R(V_n) < \infty$ for all $n \geq 0$. For such a graded free R-module V, the *Hilbert-Poincaré series* $P_V(t) \in \mathbb{Z}[[t]]$ of V is the formal power series

$$P_V(t) = \sum_{n=0}^{\infty} \mathrm{rank}_R(V_n) t^n.$$

We recall also the following definitions from the theory of Lie algebras.

Definition 4.1.2. A Lie algebra L over a commutative ring R is an R-module equipped with a bilinear composition $(x, y) \to [xy]$ that satisfies the two conditions

$$[xx] = 0 \quad \text{and} \quad [[xy]z] + [[yz]x] + [[zx]y] = 0.$$

By an R-algebra we mean an associative ring with identity, containing R as a subring. Any R-algebra A defines a Lie algebra A_L having the same R-module structure as that of A with the Lie product given by $[xy] := xy - yx$. A 'Lie subalgebra of A' means a Lie subalgebra of A_L.

Given any Lie algebra L over R, we can construct the *universal enveloping algebra* $U(L)$ of L as follows. Form the tensor algebra $T(L)$ for the R-module L, $T(L) = R \oplus L \oplus L \otimes L \oplus \cdots$ and let $U(L) = T(L)/I$, where I is the ideal in $T(L)$ generated by all elements of the form

$$[xy] - x \otimes y + y \otimes x, \quad x, y \in L.$$

If u is the restriction to L of the canonical homomorphism of $T(L)$ onto $U(L)$, then u is a homomorphism of the Lie algebra L into $U(L)_L$.

The pair $(U(L), u)$ has the following universal property. If A is any R-algebra and g is a homomorphism of L into A_L, then there exists a unique R-algebra homomorphism $\hat{g} : U(L) \to A$, such that the following diagram of Lie algebra homomorphisms commutes

$$\begin{tikzcd} L \arrow[r, "u"] \arrow[dr, "g"'] & U(L)_L \arrow[d, "\hat{g}"] \\ & A_L \end{tikzcd}$$

Definition 4.1.3. Let k be a field of characteristic p. Let A be a k-algebra and let L be

a Lie subalgebra of A. Then L is said to be *restricted* if for each element $a \in L$, $a^p \in L$.

More generally, a Lie algebra L over k, with an additional unary operation $[p]$, is called a *restricted Lie algebra* if there exist a k-algebra A and a Lie algebra monomorphism $\theta : L \to A_L$ such that $\theta(a^{[p]}) = \theta(a)^p$ for all $a \in L$. In this case A is called a *restricted enveloping algebra* of L. A Lie algebra homomorphism between two restricted Lie algebras is called *restricted* if it preserves the operation $[p]$.

A restricted enveloping algebra U of L is *universal* if it has the following universal property: for any restricted Lie algebra homomorphism $\varphi : L \to B_L$, where B is a k-algebra, there exists a unique k-algebra homomorphism $\hat{\varphi} : U \to B$ such that the following diagram of restricted Lie algebra homomorphisms commutes

$$\begin{tikzcd} L \arrow[r, "\theta"] \arrow[dr, "\varphi"'] & U_L \arrow[d, "\hat{\varphi}"] \\ & B_L \end{tikzcd}$$

Now let G be a finitely generated pro-p group. Recall that $(I^n(G))_{n\geq 0}$ is the filtration of the completed group algebra $\mathbb{F}_p[[G]]$ of G over $\mathbb{F}_p$ by powers of the augmentation ideal, where $I^0(G) = \mathbb{F}_p[[G]]$. There are two graded $\mathbb{F}_p$-algebras associated to G and $\mathbb{F}_p[[G]]$ respectively which are defined by

$$\mathrm{gr}(G) := \bigoplus_{n\geq 1} G_{(n)}/G_{(n+1)} \quad \text{and} \quad \mathrm{gr}(\mathbb{F}_p[[G]]) := \bigoplus_{n\geq 0} I^n(G)/I^{n+1}(G).$$

Since G is finitely generated, it follows from [Koc02, Lemma 7.10 and Theorem 7.11] that the graded algebras $\mathrm{gr}(\mathbb{F}_p[[G]])$ and $\mathrm{gr}(G)$ are locally finite. We define $a_n(G) := \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$ and $c_n(G) := \dim_{\mathbb{F}_p} G_{(n)}/G_{(n+1)}$.

The following theorem is a consequence of a beautiful theory of Jennings and Lazard [DSMS99, Chapters 11 and 12], viewing the Zassenhaus filtration subgroups $G_{(n)}$ as dimension subgroups. (See also [Qui68].)

Theorem 4.1.4 (Jennings-Lazard)**.** *Let the notation be as above.*

(i) The graded algebra $\mathrm{gr}(G)$ *is a restricted Lie algebra.*

(ii) The graded algebra $\mathrm{gr}(\mathbb{F}_p[[G]])$ *is a universal restricted enveloping algebra of* $\mathrm{gr}(G)$.

(iii) We have

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \sum_{n=0}^{\infty} a_n(G)t^n = \prod_{n=1}^{\infty} \left(\frac{1-t^{np}}{1-t^n}\right)^{c_n(G)}. \tag{4.1}$$

Proof. (i) See [DSMS99, Theorem 12.8(i)].

(ii) See [DSMS99, Theorem 12.8(iii)].

(iii) See [DSMS99, Theorem 12.16] (see also [Ers11, Proposition 2.3]). □

We have a similar result relating the descending central series of G to the filtration $(J^n(G))_{n\geq 0}$ of the completed group algebra $\mathbb{Z}_p[[G]]$ by powers of the augmentation ideal. There are two graded $\mathbb{Z}_p$-algebras associated to G and $\mathbb{Z}_p[[G]]$ respectively which are defined by

$$\mathrm{gr}_\gamma(G) = \bigoplus_{n\geq 1} G_n/G_{n+1} \quad \text{and} \quad \mathrm{gr}(\mathbb{Z}_p[[G]]) = \bigoplus_{n\geq 0} J^n(G)/J^{n+1}(G).$$

Lemma 4.1.5. *Let G be a finitely generated pro-p-group. Assume that the graded algebra* $\mathrm{gr}_\gamma(G) = \bigoplus_{n\geq 1} G_n/G_{n+1}$ *is torsion free. Let* $e_n(G) = \mathrm{rank}_{\mathbb{Z}_p} G_n/G_{n+1}$.

(i) The graded algebra $\mathrm{gr}(\mathbb{Z}_p[[G]])$ *is a universal enveloping algebra of* $\mathrm{gr}_\gamma(G)$.

(ii) $J^n(G)/J^{n+1}(G)$ *is a free module over* $\mathbb{Z}_p$ *of finite rank* $d_n(G)$, *and*

$$P_{\mathrm{gr}(\mathbb{Z}_p[[G]])}(t) = \sum_{n=0}^{\infty} d_n(G)t^n = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{e_n(G)}}.$$

Proof. (i) This follows from [Har90, Theorem 1.3] and Corollary 2.1.12.

(ii) This follows from (a) and [Lab06, Proposition 2.5]. □

Example 4.1.6. If $G = C_p$ is the cyclic group of order p then since $\mathrm{gr}(C_p) = C_p$ and $\mathrm{gr}(\mathbb{F}_p[[C_p]]) = \mathrm{gr}(\mathbb{F}_p[C_p]) \cong \mathbb{F}_p[x]/(x^p)$, we have

$$P_{\mathrm{gr}(\mathbb{F}_p[[C_p]])}(t) = 1 + t + \cdots + t^{p-1}.$$

The following lemma is an important technical tool which relies on a fundamental result of Lichtman and also on a simple but remarkable formula which can be traced back to the work of Lemaire in [Lem74, Chapter 5].

Lemma 4.1.7. *Let G_1 and G_2 be two finitely generated pro-p-groups. Let $G = G_1 * G_2$ be the free product of G_1 and G_2 in the category of pro-p-groups. Then*

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = (P^{-1}_{\mathrm{gr}(\mathbb{F}_p[[G_1]])}(t) + P^{-1}_{\mathrm{gr}(\mathbb{F}_p[[G_2]])}(t) - 1)^{-1}.$$

Proof. By [Lic80, Theorem 1], the graded $\mathbb{F}_p$-algebra $\mathrm{gr}(\mathbb{F}_p[[G]])$ is a free product (i.e., a categorical coproduct) of $\mathrm{gr}(\mathbb{F}_p[[G_1]])$ and $\mathrm{gr}(\mathbb{F}_p[[G_2]])$. The statement then follows from [PP05, Equation (1.2), page 56]. □

Example 4.1.8. If $G = C_2 * \cdots * C_2$ is a free product of $d+1$ copies of C_2 the cyclic group of order 2, then by the previous example, Lemma 4.1.7 and induction on d it follows that

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1+t}{1-dt}.$$

Our aim is to use these results to develop a formula for $c_n(G)$ for various families of pro-p groups G. We proceed as follows. Given a power series $P(t) = 1 + \sum_{n\geq 1} a_n t^n \in \mathbb{Z}[[t]]$, we define $c_n,\ n = 1, 2, \ldots$ by

$$P(t) = 1 + \sum_{n\geq 1} a_n t^n = \prod_{n=1}^{\infty} \left(\frac{1-t^{np}}{1-t^n}\right)^{c_n}.$$

Now write $\log P(t) = \sum_{n\geq 1} b_n t^n$. We will derive a formula for c_n using the values $b_1, \ldots, b_n$.

Taking logarithms and using $\log(\frac{1}{1-t}) = \sum_{\nu=1}^{\infty} \frac{1}{\nu} t^\nu$ gives

$$\sum_{n=1}^{\infty} b_n t^n = \sum_{m=1}^{\infty} c_m \sum_{\nu=1}^{\infty} \frac{1}{\nu}(t^{m\nu} - t^{mp\nu}).$$

Equating the coefficients of t^n, we have

$$b_n = \sum_{m\nu=n} \frac{1}{\nu} c_m - \sum_{mp\nu=n} \frac{1}{\nu} c_m.$$

Hence

$$nb_n = \sum_{m|n} mc_m - \sum_{mp|n} mpc_m.$$

We now define a new sequence $w_n,\ n = 1, 2, \ldots$ by

$$w_n = \frac{1}{n} \sum_{m|n} \mu(n/m) m b_m,$$

where μ is the Möbius function: for a positive integer d,

$$\mu(d) = \begin{cases} (-1)^r & \text{if } d \text{ is a product of } r \text{ distinct prime numbers,} \\ 0 & \text{otherwise.} \end{cases}$$

Then by the Möbius inversion formula,

$$nb_n = \sum_{m|n} mw_m.$$

Remark 4.1.9. From the definition of w_n we see that

$$P(t) = 1 + \sum_{n\geq 1} a_n t^n = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{w_n}}.$$

Lemma 4.1.10. *If* $(n, p) = 1$ *then* $c_n = w_n$.

Proof. Assume that $(n, p) = 1$. Then we have

$$nb_n = \sum_{m|n} mc_m.$$

Hence by the Möbius inversion formula,

$$c_n = \frac{1}{n}\sum_{m|n} \mu(n/m) m b_m = w_n. \qquad \square$$

Lemma 4.1.11. *If p divides n, then*

$$c_n = c_{n/p} + w_n.$$

Proof. The proof is by induction on n. Clearly $c_p - c_1 = \dfrac{pb_p - b_1}{p} = w_p$, hence the statement is true for $n = p$. Assume now that $n > p$ and $p \mid n$. Assume also that the statement is true for every m such that $p \mid m \mid n$, $m \neq n$.

Then

$$\begin{aligned}
nb_n &= \sum_{m|n} mc_m - \sum_{pm|n} pmc_m \\
&= \sum_{m|n} mc_m - \sum_{p|m|n} mc_{m/p} \\
&= \sum_{m|n,(m,p)=1} mc_m + \sum_{p|m|n} m(c_m - c_{m/p}) \\
&= \sum_{m|n,(m,p)=1} mw_m + \sum_{p|m|n,m\neq n} mw_m + n(c_n - c_{n/p}) \\
&= \sum_{m|n,m\neq n} mw_m + n(c_n - c_{n/p}).
\end{aligned}$$

Combining this with

$$nb_n = \sum_{m|n} mw_m,$$

gives $c_n - c_{n/p} = w_n$. Hence the statement is true for all n. $\square$

Proposition 4.1.12. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n = w_m + w_{pm} + \cdots + w_{p^k m}.$$

Proof. This follows from the previous two lemmas. $\square$

Theorem 4.1.13. *Let G be a finitely generated pro-p-group. Write*

$$\log P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \sum_{n\geq 1} b_n t^n \in \mathbb{Q}[[t]],$$

and define $w_n(G)$ by

$$w_n(G) := \frac{1}{n}\sum_{m|n} \mu(n/m) m b_m.$$

Let $n = p^k m$ with $(m,p) = 1$. Then

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{p^k m}(G).$$

Proof. This follows from Theorem 4.1.4 and Proposition 4.1.12. □

The following proposition points out that in certain cases there is a close relationship between the quantities $c_n(G) := \dim_{\mathbb{F}_p} G_{(n)}/G_{(n+1)}$ and $e_n(G) := \mathrm{rank}_{\mathbb{Z}_p} G_n/G_{n+1}$.

Proposition 4.1.14. *Let G be a finitely generated pro-p-group and keep the same notation as in Lemma 4.1.5 and Theorem 4.1.13. Assume that the graded algebra $\mathrm{gr}_\gamma(G) = \bigoplus_{n\geq 1} G_n/G_{n+1}$ is torsion free. The following are equivalent.*

(i) $\mathrm{rank}_{\mathbb{Z}_p} J^n(G)/J^{n+1}(G) = \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$ *for all* $n \geq 1$.

(ii) $w_n(G) = \mathrm{rank}_{\mathbb{Z}_p} G_n/G_{n+1}$ *for all* $n \geq 1$.

Proof. (i) ⇒ (ii): Assume that $\mathrm{rank}_{\mathbb{Z}_p} J^n(G)/J^{n+1}(G) = \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$ for all n. Then by Theorem 4.1.4, Remark 4.1.9 and Lemma 4.1.5, we have

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{w_n(G)}} = P_{\mathrm{gr}(\mathbb{Z}_p[[G]])}(t) = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{e_n(G)}}.$$

Therefore $w_n(G) = e_n(G)$ for all $n \geq 1$.

(ii) ⇒ (i): Assume that $w_n(G) = e_n(G)$ for all $n \geq 1$. Then by Theorem 4.1.4, Remark 4.1.9 and Lemma 4.1.5, we have

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = P_{\mathrm{gr}(\mathbb{Z}_p[[G]])}(t).$$

Therefore $\operatorname{rank}_{\mathbb{Z}_p} J^n(G)/J^{n+1}(G) = \dim_{\mathbb{F}_p} I^n(G)/I^{n+1}(G)$ for all $n \geq 1$. $\square$

Remark 4.1.15. We shall see in the next sections that both a free finitely generated pro-p-group and a Demushkin group with a relation of the form $r = [x_1, x_2] \cdots [x_{d-1}, x_d]$ satisfy the equivalent statements in Proposition 4.1.14.

4.2 Free Pro-p Groups

Throughout this section we assume that S is a free pro-p-group on a finite set of generators $x_1, \ldots, x_d$. Recall that the Magnus homomorphism from the completed group algebra $\mathbb{F}_p[[S]]$ to the $\mathbb{F}_p$-algebra $\mathbb{F}_p\langle\langle X_1, \ldots, X_d\rangle\rangle$ of formal power series in d non-commuting variables $X_1, \ldots, X_d$ over $\mathbb{F}_p$ is given by

$$\psi\colon \mathbb{F}_p[[S]] \to \mathbb{F}_p\langle\langle X_1, \ldots, X_d\rangle\rangle, x_i \mapsto 1 + X_i.$$

The $\mathbb{F}_p$-algebra $\mathbb{F}_p\langle\langle X_1, \ldots, X_d\rangle\rangle$ is equipped with a natural valuation v given by

$$v(\sum a_{i_1,\ldots,i_k} X_{i_1} \cdots X_{i_k}) = \inf\{k \mid a_{i_1,\ldots,i_k} \neq 0\} \in \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

making it a compact topological $\mathbb{F}_p$-algebra and by Theorem 2.1.25 the Magnus homomorphism is a (topological) isomorphism.

Lemma 4.2.1. *A finitely generated pro-p group S is free of rank d if and only if the Hilbert-Poincaré series*

$$P_{\mathrm{gr}(\mathbb{F}_p[[S]])}(t) = \frac{1}{1 - dt}.$$

Proof. ($\Rightarrow$) Via the Magnus homomorphism, the augmentation ideal $I(S)$ is mapped to the ideal $I = (X_1, \ldots, X_d)$ of $\mathbb{F}_p\langle\langle X_1, \ldots, X_d\rangle\rangle$. Hence

$$a_n(S) := \dim_{\mathbb{F}_p}(I^n(S)/I^{n+1}(S)) = \dim_{\mathbb{F}_p}(I^n/I^{n+1}),$$

which is equal to the number of non-commutative monomials of degree n in d variables $X_1, \ldots, X_d$. Hence $a_n(S) = d^n$. The result then follows.

($\Leftarrow$) Let S be a finitely generated free pro-p group of rank d and suppose G is a finitely generated pro-p group with

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1-dt}.$$

Then

$$\log(\frac{1}{1-dt}) = \sum_{\nu=1}^{\infty} \frac{1}{\nu}(dt)^{\nu},$$

so by Theorem 4.1.13,

$$w_n(G) = w_n(S) := \frac{1}{n}\sum_{m|n} \mu(m) d^{n/m}$$

and $c_n(G) = c_n(S)$ for all $n \geq 1$. Since $c_1(G) = w_1(G) = d$, which is equal to the minimal number of topological generators of G, there exists a minimal presentation of G:

$$1 \to R \to S \to G \to 1.$$

Then for all $n \geq 1$, $c_n(G) = c_n(S)$ implies $|S/S_{(n)}| = |G/G_{(n)}|$ and hence the natural epimorphism

$$S/S_{(n)} \twoheadrightarrow G/G_{(n)}$$

is an isomorphism. This implies that $R \subseteq S_{(n)}$ for all $n \geq 1$, so by [Koc02, Theorem 7.11], $R = 1$. Hence $G \cong S$. $\square$

Defining $w_n(S)$ by

$$w_n(S) = \frac{1}{n}\sum_{m|n} \mu(m) d^{n/m},$$

Theorem 4.1.13 immediately implies the following result.

Proposition 4.2.2. *If $n = p^k m$ with $(m,p) = 1$, then*

$$c_n(S) = w_m(S) + w_{pm}(S) + \cdots + w_{p^k m}(S). \quad \square$$

Remark 4.2.3. Let (S_n) be the lower central series of S. Then by Witt's result, S_n/S_{n+1} is a free $\mathbb{Z}_p$-module of finite rank $w_n(S)$.

Remarks 4.2.4. (1) If a finitely generated pro-p-group G is known to be realizable as the Galois group of a maximal p-extension of a field F containing a primitive p-th root of unity, then we need only $c_1(G) = c_1(S)$ and $c_2(G) = c_2(S)$, for some finitely generated free pro-p-group S, to establish that G is isomorphic to S.

Indeed, as $c_1(S) = c_1(G)$ we have a short exact sequence

$$1 \to R \to S \xrightarrow{\pi} G \to 1.$$

Since $c_1(S) = c_1(G)$ and $c_2(S) = c_2(G)$, we have $|S/S_{(3)}| = |G/G_{(3)}|$. Thus the natural epimorphism

$$S/S_{(3)} \twoheadrightarrow G/G_{(3)}$$

is in fact an isomorphism. Hence by [EM11a, Theorem C] (see also [CEM12, Theorem D] for the case $p = 2$) we see that $\pi\colon S \to G$ is an isomorphism.

(2) Observe that the numbers $c_n(S)$, $n = 1, 2, \ldots$, also detect the minimal number of generators of $S_{(n)}$. Indeed by the pro-p version of Schreier's formula, for each open subgroup T of S we have the following expression for the minimal number of generators $d(T)$ of T:

$$d(T) = [S : T](d(S) - 1) + 1.$$

Therefore

$$d_n(S) := d(S_{(n)}) = p^{\sum_{i=1}^{n-1} c_i(S)}(d - 1) + 1.$$

Example 4.2.5. Let S be a free pro-p-group of finite rank d. We have

$$c_1(S) = d,$$

$$c_2(S) = \begin{cases} \frac{d^2-d}{2} \text{ if } p \neq 2, \\ \frac{d^2+d}{2} \text{ if } p = 2, \end{cases}$$

$$c_3(S) = \begin{cases} \frac{d^3-d}{3} \text{ if } p \neq 3, \\ \frac{d^3+2d}{3} \text{ if } p = 3, \end{cases}$$

$$c_4(S) = \begin{cases} \frac{d^4-d^2}{4} \text{ if } p \neq 2, \\ \frac{d^4+d^2+2d}{4} \text{ if } p = 2, \end{cases}$$

$$c_5(S) = \begin{cases} \frac{d^5-d}{5} \text{ if } p \neq 5, \\ \frac{d^5+4d}{5} \text{ if } p = 5. \end{cases}$$

We can look at this example in more detail. For any minimal presentation

$$1 \to R \to S \to G \to 1,$$

$$d = c_1(S) = \dim_{\mathbb{F}_p} \frac{S}{S^p[S,S]} = \dim_{\mathbb{F}_p} \frac{G}{G^p[G,G]} = c_1(G),$$

so $c_1(G)$ is an important invariant which gives the minimal number of generators of G.

If $p \neq 2$ then

$$\begin{aligned} c_2(S) &= \dim_{\mathbb{F}_p} \frac{S_{(2)}}{S_{(3)}} \\ &= \dim_{\mathbb{F}_p} \frac{S^p[S,S]}{S^p[[S,S],S]} \\ &= \dim_{\mathbb{F}_p} < \overline{[x_i, x_j]} \mid 1 \leq i < j \leq d > \\ &= \binom{d}{2} \\ &= \frac{d^2-d}{2} \\ &= w_2(S). \end{aligned}$$

Recall that

$$\mathrm{gr}(\mathbb{F}_p[[S]]) = \mathbb{F}_p \oplus \frac{I(S)}{I^2(S)} \oplus \frac{I^2(S)}{I^3(S)} \oplus \cdots$$

is the universal restricted enveloping algebra of the restricted Lie algebra

$$\mathrm{gr}(S) = \mathbb{F}_p \oplus \frac{S}{S_{(2)}} \oplus \frac{S_{(2)}}{S_{(3)}} \oplus \cdots$$

This leads to the equation

$$\begin{aligned}
&(1 + t + t^2 + \cdots + t^{p-1})^{c_1(S)} \\
&\cdot (1 + t^2 + t^{2\cdot 2} + \cdots + t^{2(p-1)})^{c_2(S)} \\
&\cdot (1 + t^3 + t^{3\cdot 2} + \cdots + t^{3(p-1)})^{c_3(S)} \\
&\cdots \\
&= 1 + a_1(S)t + a_2(S)t^2 + a_3(S)t^3 + \cdots \\
&= 1 + dt + d^2t^2 + d^3t^3 + \cdots
\end{aligned}$$

Equating coefficients of t gives $c_1(S) = d$, which reflects the fact that $\overline{X}_1 = \overline{x_1 - 1}, \ldots, \overline{X}_d = \overline{x_d - 1}$ is a basis of $I(S)/I^2(S)$. Equating coefficients of t^2 gives $d^2 = d + \binom{d}{2} + c_2(S)$, so $c_2(S) = \frac{d^2-d}{2}$.

If $p = 2$ then $p-1 < 2$, so the above equation gives $d^2 = \binom{d}{2} + c_2(S)$ or $c_2(S) = \frac{d(d+1)}{2}$, which reflects the fact that, in this case, a basis of $S_{(2)}/S_{(3)}$ also contains the squares of generators.

Similarly, considering the case $p \geq 5$ and looking at coefficients of t^3, we find

$$\begin{aligned}
&(1 + dt + (\binom{d}{2} + d)t^2 + (\binom{d}{3} + d(d-1) + d)t^3 + \ldots) \\
&\cdot (1 + \frac{d^2 - d}{2}t^2 + \mathcal{O}(t^4)) \\
&\cdot (1 + c_3(S)t^3 + \mathcal{O}(t^6)) \\
&\cdots \\
&= 1 + dt + d^2t^2 + d^3t^3 + \cdots
\end{aligned}$$

which gives $c_3(S) = \frac{d^3-d}{3}$.

We can give an explicit $\mathbb{F}_p$-basis for $S_{(n)}/S_{(n+1)}$, for each n in terms of Hall commutators, which we now describe. We note that an $\mathbb{F}_p$-basis for $S_{(n)}/S_{(n+1)}$ is also given in [Gär11].

Definition 4.2.6. Let S be the free group generated by $\{x_1, \ldots, x_d\}$. The set C_n of *Hall commutators of weight* n together with a total order $<$ is inductively defined as follows:

1. $C_1 = \{x_1, \ldots, x_d\}$ with the ordering $x_1 > \cdots > x_d$.

2. Assume $n > 1$ and that the Hall commutators have been defined and simply ordered for all weights $< n$ so that commutators of weight k are greater than all commutators of weight $< k$. Then C_n is the set of all commutators $[c_1, c_2]$ where $c_1 \in C_{n_1}, c_2 \in C_{n_2}$ such that $n_1 + n_2 = n$, $c_1 > c_2$ and if $c_1 = [c_3, c_4]$ then we also require that $c_2 \geq c_4$. The set C_n is ordered lexicographically, i.e., $[c_1, c_2] < [c_1', c_2']$ if and only if $c_1 < c_1'$, or $c_1 = c_1'$ and $c_2 < c_2'$.

The following theorem was proved by M. Hall in the discrete case. The extension of his theorem to the pro-p case follows from Corollary 2.1.12.

Theorem 4.2.7 ([Hal50, Theorem 4.1])**.** *The Hall commutators of weight n represent a basis of S_n/S_{n+1} as a free $\mathbb{Z}_p$-module. In particular, $w_n(S) = |C_n|$.*

The following theorem relating the Zassenhaus filtration to the descending central series is due to Lazard.

Theorem 4.2.8 (Lazard)**.** *For each n, one has*

$$G_{(n)} = \prod_{ip^j \geq n} G_i^{p^j}.$$

Proof. See [DSMS99, Theorem 11.2]. □

Corollary 4.2.9. *Let us write $n = p^k m$ with $(m, p) = 1$. Then a basis of the $\mathbb{F}_p$-vector space $S_{(n)}/S_{(n+1)}$ can be represented by the following set*

$$C_m^{p^k} \bigsqcup C_{pm}^{p^{k-1}} \bigsqcup \cdots \bigsqcup C_{p^{k-1}m}^{p} \bigsqcup C_n.$$

Proof. By Lazard's theorem, the above set defines a set of generators for the $\mathbb{F}_p$-vector space $S_{(n)}/S_{(n+1)}$. Now by Theorem 4.1.13 and a counting argument, we see that this set defines a basis for the $\mathbb{F}_p$-vector space $S_{(n)}/S_{(n+1)}$. □

With this basis in mind, we revisit the calculation of $c_3(S)$ for $p \neq 3$. As pointed out in [Gär11], $C_3 = \{[[x_i, x_j], x_k] \mid 1 \leq i < j \leq d, k \leq j\}$ and

$$\begin{aligned} |C_3| &= 2\binom{d+1}{3} \\ &= \frac{d^3 - d}{3}. \end{aligned}$$

We now consider an interesting, purely group theoretical corollary of our formula for $c_n(S)$ which is closely related to the Kernel n-Unipotent Conjecture formulated by J. Mináč and N. D. Tân in [MT13]. Recall that $\mathbb{U}_n(\mathbb{F}_p)$ is the group of all upper-triangular unipotent $n \times n$ matrices with entries in $\mathbb{F}_p$.

Definition 4.2.10. Let G be a pro-p group and let $n \geq 1$ be an integer. We say that G has the *kernel n-unipotent property* if

$$G_{(n)} = \bigcap \ker(\rho : G \to \mathbb{U}_n(\mathbb{F}_p)),$$

where ρ runs through the set of all representations (continuous homomorphisms) $G \to \mathbb{U}_n(\mathbb{F}_p)$.

Conjecture 4.2.11 (Kernel n-Unipotent Conjecture)**.** *Let F be a field containing a primitive p-th root of unity and let $G = G_F(p)$. Let $n \geq 3$ be an integer. Then G has the kernel n-unipotent property.*

Lemma 4.2.12. *Let n be a positive integer. If $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = 1$, then $c_n(S) = 0$ for every free pro-p-group S.*

Proof. Let S be a free pro-p-group. Assume that $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = 1$. Then for any (continuous) representation $\rho : S \to \mathbb{U}_{n+1}(\mathbb{F}_p)$, we have $\rho(S_{(n)}) \subseteq \mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = 1$. Hence

$$S_{(n+1)} \subseteq S_{(n)} \subseteq \bigcap \ker(\rho\colon S \to \mathbb{U}_{n+1}(\mathbb{F}_p)),$$

where ρ runs over the set of all representations (continuous homomorphisms) $G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$. On the other hand, we know that S has the kernel n-unipotent property for all n (see [Efr14b], and also [Efr14a], [MT13]). This means that we have

$$S_{(n+1)} = \bigcap \ker(\rho\colon S \to \mathbb{U}_{n+1}(\mathbb{F}_p)).$$

Therefore, $S_{(n+1)} = S_{(n)}$, so $c_n(S) = 0$. □

Corollary 4.2.13. *Let n be a positive integer. Then $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} \simeq \mathbb{F}_p$ and*

$$n = \max\{h \mid \mathbb{U}_{n+1}(\mathbb{F}_p)_{(h)} \neq 1\}.$$

Proof. We first observe that if S is a free pro-p-group of rank $d > 1$, then all numbers $w_n(S)$, $n = 1, 2, \ldots$, are positive. Therefore from Proposition 4.2.2 we see that $c_n(S) \neq 0$ for all $n \in \mathbb{N}$. Hence by Lemma 4.2.12, $\mathbb{U}_{(n+1)}(\mathbb{F}_p)_{(n)} \neq 1$.

On the other hand, it is well-known that $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n+1)} = 1$. Hence $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} \subseteq Z(\mathbb{U}_{n+1}(\mathbb{F}_p)) \simeq \mathbb{F}_p$, where $Z(\mathbb{U}_{n+1}(\mathbb{F}_p))$ is the center of $\mathbb{U}_{n+1}(\mathbb{F}_p)$. Therefore

$$\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n)} = Z(\mathbb{U}_{n+1}(\mathbb{F}_p)) \simeq \mathbb{F}_p,$$

and the second assertion is also clear. □

4.3 Free Products of Cyclic Groups

Let d be a non-negative integer. Let $G = C_p * \cdots * C_p$ be a free product in the category of pro-p-groups of $d+1$ copies of C_p, where C_p is the cyclic group of order p. By Example 4.1.6, Lemma 4.1.7 and induction on d, the Hilbert-Poincaré series of $\mathrm{gr}(\mathbb{F}_p[[G]])$ is

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1 + t + \cdots + t^{p-1}}{1 - dt - \cdots - dt^{p-1}}.$$

Due to the close connection with formally real pythagorean fields, we will focus on the case in which $p = 2$.

4.3.1 Free products of cyclic groups of order 2

Let d be a non-negative integer. Let $G = C_2 * \cdots * C_2$ be a free product in the category of pro-2-groups of $d+1$ copies of C_2, where C_2 is the group of order 2.

Recall from Theorem 3.4.16 that G plays an important role as the maximal pro-2 quotient of the absolute Galois group of a formally real pythagorean SAP field. Also it is interesting to observe that if G is such a Galois group, then G is already determined by its quotient $G/G_{(3)}$. More precisely, assume that H is another pro-2-group which is realizable as the Galois group of the maximal 2-extension of a field F, and that $H/H_{(3)} \simeq G/G_{(3)}$, then $H \simeq G$. (See [MS90, MS96, Min86].)

The Hilbert-Poincaré series of $\mathrm{gr}(\mathbb{F}_2[[G]])$ is

$$P_{\mathrm{gr}(\mathbb{F}_2[[G]])}(t) = \frac{1+t}{1-dt}.$$

We have

$$\log P_{\mathrm{gr}(\mathbb{F}_2[[G]])}(t) = \log(\frac{1}{1-dt}) - \log(\frac{1}{1+t}) = \sum_{n\geq 1} \frac{1}{n}(d^n - (-1)^n)t^n.$$

Now we define the sequence $w_n(G), n = 1, 2, \ldots$ by

$$w_n(G) = \frac{1}{n}\sum_{m|n} \mu(n/m)(d^m - (-1)^m).$$

Proposition 4.3.1. *If $n = 2^k m$ with $(m, 2) = 1$, then*

$$c_n(G) = w_m(G) + w_{2m}(G) + \cdots + w_{2^k m}(G). \quad \square$$

4.3.2 Free products of cyclic groups of order 2 as semidirect products

We again let $G = C_2 * \cdots * C_2$ be the free product in the category of pro-2 groups of $d+1$ copies of C_2. Our goal in this subsection is to show that G is isomorphic to a semidirect

product $H \rtimes C_2$ of a free pro-2 group H and C_2. We also provide a relation between $G_{(n)}$ and $H_{(n)}$.

Define the numbers ϵ_n, $n = 1, 2, \ldots$ by

$$\epsilon_n = \frac{1}{n} \sum_{m|n} \mu(n/m)(-1)^m.$$

Then by the Möbius inversion formula,

$$(-1)^n = \sum_{m|n} m\epsilon_m. \tag{*}$$

Lemma 4.3.2. *We have $\epsilon_1 = -1$, $\epsilon_2 = 1$ and $\epsilon_n = 0$ for $n \geq 3$.*

Proof. The equation (*) determines ϵ_n, $n \in \mathbb{N}$, uniquely. But $\epsilon_1 = -1$, $\epsilon_2 = 1$ and $\epsilon_n = 0$ for $n \geq 3$ work as for these numbers

$$\sum_{m|n} m\epsilon_m = \begin{cases} -1 & \text{if } n \text{ is odd,} \\ -1 + 2 = 1 & \text{if } n \text{ is even.} \end{cases} \quad \square$$

Now write

$$G = C_2 * C_2 * \cdots * C_2 = \langle x_0 \mid x_0^2 \rangle * \langle x_1 \mid x_1^2 \rangle * \cdots * \langle x_d \mid x_d^2 \rangle.$$

For ease of notation, we consider $x_0, x_1, \ldots, x_d$ as elements of G. We consider a continuous homomorphism $\varphi : G \to C_2 = \langle x \mid x^2 \rangle$ defined by $x_i \mapsto x$ for all $i = 0, 1, \ldots, d$. For each $i = 1, \ldots, d$, we set $y_i = x_0 x_i \in G$ and let H be the closed subgroup of G generated by $y_1, \ldots, y_d$.

Lemma 4.3.3. *Let the notation be as above.*

(i) $\ker \varphi = H$.

(ii) $G \simeq H \rtimes C_2$, *where the action of C_2 on H is given by $xy_ix = y_i^{-1}$.*

(iii) *H is a free pro-2 group of rank d.*

Proof. (i) For each $i = 1, \ldots, d$, $y_i \in \ker \varphi$, hence $H \subseteq \ker \varphi$. Now consider any element $\gamma \in \ker \varphi$. For each open neighborhood U of γ in G, there exists an element $g = x_{i_1} \cdots x_{i_r} \in U$, $i_1, \ldots, i_r \in \{1, \ldots, d\}$ such that $1 = \varphi(g) = x^r$. Hence $r = 2s$ is even. Since $x_0 y_i x_0 = y_i^{-1}$, we obtain

$$g = x_0 y_{i_1} \cdots x_0 y_{i_r} = y_{i_1}^{-1} y_{i_2} \cdots y_{i_{r-1}}^{-1} y_{i_r}.$$

Thus $g \in H$. Therefore $\gamma \in H$ and $H = \ker \varphi$.

(ii) This follows by observing that $\psi \colon C_2 = \langle x \mid x^2 \rangle \to G$ which maps x to x_0, is a section of φ.

(iii) By Theorem 3.4.16, we can view G as the Galois group $G_F(2)$ of the maximal 2-extension of a formally real pythagorean SAP field F having square class group of cardinality 2^{d+1}. There is a bijective correspondence between the set $\{x_0, x_1, \ldots, x_d\}$ and the set of orderings $X_F = \{P_0, P_1, \ldots, P_d\}$ of F given by

$$P_i = \{f \in F^\times \mid x_i(\sqrt{f}) = \sqrt{f}\}.$$

Let K be the fixed field of H. For all $i = 0, \ldots, d$, we have $-1 \notin P_i$, so $x_i(\sqrt{-1}) = -\sqrt{-1}$. Hence for all $i = 1, \ldots, d$, $y_i = x_0 x_i$ acts trivially on $\sqrt{=1}$. So $F(\sqrt{-1}) \subseteq K$. Since $[G : H] = 2$, we have $K = F(\sqrt{-1})$ and $H = G_K(2)$. Then by Proposition 3.4.15, H is a free pro-2 group of rank d. □

The following proposition and corollary are remarkable properties of the pair $\{H, G\}$.

Proposition 4.3.4. *We have $c_1(H) = d = c_1(G) - 1$ and $c_n(H) = c_n(G)$ for all $n \geq 2$.*

Proof. It is clear that $c_1(H) = w_1(H) = d$ and $c_1(G) = w_1(G) = d + 1$. Hence $c_1(H) = d = c_1(G) - 1$. We shall show that $c_n(H) = c_n(G)$ for any $n \geq 2$.

We note that

$$w_n(H) - w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m)(-1)^m = \epsilon_n.$$

By Lemma 4.3.2, one has $w_2(H) = w_2(G) + 1$ and $w_n(H) = w_n(G)$ for every $n \geq 3$.

If $n > 1$ is odd, then

$$c_n(H) = w_n(H) = w_n(G) = c_n(G).$$

If n is even, then by writing $n = 2^k m$ with m odd, we have

$$\begin{aligned} c_n(H) &= w_m(H) + w_{2m}(H) + w_{4m}(H) + \cdots + w_{2^k m}(H) \\ &= w_m(G) + w_{2m}(G) + w_{4m}(G) + \cdots + w_{2^k m}(G) = c_n(G). \end{aligned}$$

(Note that we always have $w_m(H) + w_{2m}(H) = w_m(G) + w_{2m}(G)$ for every $m \geq 1$ odd.) □

Corollary 4.3.5. *Let $n \geq 2$ be an integer.*

(i) $H_{(n)} = H \cap G_{(n)}$.

(ii) $G/G_{(n)} \simeq H/H_{(n)} \rtimes C_2$, *where the action of C_2 on H is given by $\bar{x}\bar{y}_i\bar{x} = \bar{y}_i^{-1}$.*

Proof. (i) Clearly $H_{(n)} \subseteq H \cap G_{(n)}$. We proceed by induction on n that $H_{(n)} = H \cap G_{(n)}$. First consider the case $n = 2$. We have an exact sequence

$$1 \to H/H \cap G_{(2)} \to G/G_{(2)} \to C_2 \to 1.$$

This implies that $[H : H \cap G_{(2)}] = [G : G_{(2)}]/2 = 2^d = [H : H_{(2)}]$. Hence $H_{(2)} = H \cap G_{(2)}$. Assume that $H_{(n)} = H \cap G_{(n)}$ for some $n \geq 2$. Then from the exact sequence

$$1 \to H/H \cap G_{(n)} \to G/G_{(n)} \to C_2 \to 1,$$

we obtain $[H : H_{(n)}] = [H : H \cap G_{(n)}] = [G : G_{(n)}]/2$. From a similar exact sequence we obtain

$$\begin{aligned} [H : H \cap G_{(n+1)}] &= \frac{1}{2}[G : G_{(n+1)}] = \frac{1}{2}[G : G_n][G_{(n)} : G_{(n+1)}] \\ &= [H : H_{(n)}][H_{(n)} : H_{(n+1)}] = [H : H_{(n+1)}]. \end{aligned}$$

Here the equality $[G_{(n)} : G_{(n+1)}] = [H_{(n)} : H_{(n+1)}]$ follows from Proposition 4.3.4. Therefore $H_{(n+1)} = H \cap G_{(n+1)}$.

(ii) This follows from (i). □

4.4 Another Semidirect Product

In this section we consider an example in which G is the semidirect product $G : \mathbb{Z}_2^d \rtimes C_2 = H \rtimes \langle x \rangle$, where the action of C_2 on $H = \mathbb{Z}_2^d$ is given by $xyx = y^{-1}$, for all $y \in H$. Recall from Corollary 3.4.19 that this group is realizable as the maximal pro-2 quotient of the absolute Galois group of a superpythagorean field.

Lemma 4.4.1. *Let $G = H \rtimes \langle x \rangle = \mathbb{Z}_2^d \rtimes C_2$ be as above. Let $n \geq 2$ be an integer, and let $s = \lceil \log_2 n \rceil$. Then $G_{(n)} = H^{2^s}$.*

Proof. We proceed by induction on n. We first observe that $[y, x] = y^{-1}x^{-1}yx = (y^{-1})^2$ and $(yx)^2 = 1$, for every $y \in H$. Hence

$$G_{(2)} = G^2[G, G] = G^2 = H^2,$$

so the lemma is true for $n = 2$. Now assume that the lemma is true for j with $2 \leq j < n$. Then

$$\begin{aligned} G_{(n)} &= G^2_{(\lceil n/2 \rceil)} \prod_{i+j=n} [G_{(i)}, G_{(j)}] \\ &= G^2_{(\lceil n/2 \rceil)} [G, G_{(n-1)}] \\ &= (H^{2^{s-1}})^2 = H^{2^s}. \end{aligned}$$

Here we use the fact that $G_{(n-1)} \subseteq H^{2^{s-1}}$, and hence $[G, G_{(n-1)}] \subseteq H^{2^s}$. □

An immediate consequence of the above lemma is the following result.

Corollary 4.4.2. *Let $n \geq 1$ be an integer. We have*

$$c_n(G) = \begin{cases} d+1 & \text{if } n = 1, \\ d & \text{if } n = 2^s \text{ for some } 1 \leq s \in \mathbb{Z}, \\ 1 & \text{if } n \text{ is not a power of 2.} \end{cases}$$

Corollary 4.4.3. *We have*

$$P_{\mathrm{gr}(\mathbb{F}_2[[G]])}(t) = \frac{1+t}{(1-t)^d} \prod_{i=1}^{\infty} \frac{1}{1-t^{2i+1}}.$$

Proof. We write $\log P_{\mathrm{gr}(\mathbb{F}_2[[G]])} = \sum_{n\geq 1} b_n(G)t^n$, and let

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m) m b_m(G).$$

By Lemma 4.1.10, if n is odd then $w_n(G) = c_n(G)$. In particular, $w_1(G) = c_1(G) = d+1$, and $w_{2i+1}(G) = c_{2i+1}(G) = 1$ for $i \geq 1$.

By Lemma 4.1.11, $w_2(G) = c_2(G) - c_1(G) = d - (d+1) = -1$.

We claim that $w_n(G) = 0$ if n is even and $n \geq 4$. Indeed, if $n = 2^s$ with $s \geq 2$, then by Lemma 4.1.11,

$$w_{2^s}(G) = c_{2^s}(G) - c_{2^{s-1}}(G) = d - d = 0.$$

Now if $n = 2m$, where m is not a power of 2, then also by Lemma 4.1.11,

$$w_{2m}(G) = c_{2m}(G) - c_m(G) = 1 - 1 = 0.$$

The corollary then follows from Remark 4.1.9. □

Remarks 4.4.4. It is interesting that $c_1(G)$ and $c_2(G)$ can be sufficient to determine G itself within some large families of pro-p-groups. The example of free pro-p groups was mentioned in Remarks 4.2.4 (1). Here are two other instances.

(1) Suppose that K is a formally real pythagorean SAP field with $|K^\times/(K^\times)^2| = 2^{d+1}$. Then $G_K(2) = C_2 * \cdots * C_2$, the free product of $d+1$ copies of C_2. By Proposition 4.3.1, one has

$$c_1(G_K(2)) = d+1 \text{ and } c_2(G_K(2)) = \frac{d(d+1)}{2}.$$

Now let F be a formally real pythagorean field F with $|F^\times/(F^\times)^2| < \infty$. We assume that $c_1(G_F(2)) = d+1$ and that $c_2(G_F(2)) = d(d+1)/2$ for some integer $d \geq 0$.

Claim. F is an SAP field with exactly $d+1$ orderings.

Proof. Since $c_1(G_F(2)) = d+1$, we see that $G_F(2)$ has $d+1$ minimal generators, and therefore $|F^\times/(F^\times)^2| = 2^{d+1}$. Now choose any formally real pythagorean SAP field K with $|K^\times/(K^\times)^2| = 2^{d+1}$. By Corollary 3.4.17, there exists an epimorphism $\varphi\colon G_K(2) \twoheadrightarrow G_F(2)$. We have

$$\begin{aligned}|G_K(2)/G_K(2)_{(3)}| &= c_1(G_K(2)) + c_2(G_K(2))\\ &= d + \frac{d(d+1)}{2}\\ &= c_1(G_F(2)) + c_2(G_F(2))\\ &= |G_F(2)/G_F(2)_{(3)}|.\end{aligned}$$

This implies that the induced epimorphism $G_K(2)/G_K(2)_{(3)} \twoheadrightarrow G_F(2)/G_F(2)_{(3)}$ is an isomorphism. By [CEM12, Theorem D], $\varphi\colon G_K(2) \to G_F(2)$ is an isomorphism. This implies that F is a SAP field by Theorem 3.4.16. □

So, quite remarkably, within the family of formally real pythagorean fields with finitely many square classes, the numbers $c_1(G_F(2))$ and $c_2(G_F(2))$ above suffice to characterize SAP fields F.

(2) Suppose that K is a superpythagorean field with $|K^\times/(K^\times)^2| = 2^{d+1} < \infty$. By Corollary 4.4.2, one has

$$c_1(G_K(2)) = d+1 \text{ and } c_2(G_K(2)) = d.$$

Now let F be a formally real pythagorean field F with $|F^\times/(F^\times)^2| < \infty$. We assume that $c_1(G_F(2)) = d+1$, $c_2(G_F(2)) = d$ for some integer $d \geq 0$.

Claim. F is a superpythagorean field.

Proof. Choose any superpythagorean field K with $|K^\times/(K^\times)^2| = 2^{d+1}$. By Corollary 4.4.3, we have an epimorphism $\varphi\colon G_F(2) \twoheadrightarrow G_K(2)$. Then

$$\begin{aligned}|G_F(2)/G_F(2)_{(3)}| &= c_1(G_F(2)) + c_2(G_F(2))\\ &= d+1+d\\ &= c_1(G_K(2)) + c_2(G_K(2))\\ &= |G_K(2)/G_K(2)_{(3)}|.\end{aligned}$$

This implies that the induced epimorphism $G_F(2)/G_F(2)_{(3)} \twoheadrightarrow G_K(2)/G_K(2)_{(3)}$ is an isomorphism. By [CEM12, Theorem D], $\varphi\colon G_F(2) \to G_K(2)$ is an isomorphism. This implies that F is a superpythagorean field by Corollary 3.4.19. $\square$

So within the family of formally real pythagorean fields with finitely many square classes, the numbers $c_1(G_F(2))$ and $c_2(G_F(2))$ above, also suffice to characterize superpythagorean fields F.

4.5 Demushkin Groups

Recall that a pro-p-group G is said to be a Demushkin group if

1. $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,
2. $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$,
3. the cup product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is a non-degenerate bilinear form.

By the work of [Dem61, Dem63], [Ser63] and [Lab66], we now have a complete classification of Demushkin groups.

Let G be a Demushkin group of rank $d = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$. Let $c_n = c_n(G)$. Then by [Lab06, Theorem 5.1 (g)] (see also [For11, Gär11, LM11]), the Hilbert-Poincaré series

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1 - dt + t^2}.$$

We write $1 - dt + t^2 = (1 - at)(1 - bt)$ so that $a + b = d$ and $ab = 1$. Then

$$\log P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \log(\frac{1}{1 - at}) + \log(\frac{1}{1 - bt}) = \sum_{n \geq 1} \frac{1}{n}(a^n + b^n).$$

We define the sequence $w_n(G), n = 1, 2, \ldots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(m)(a^{n/m} + b^{n/m}) = \frac{1}{n} \sum_{m|n} \mu(n/m)(a^m + b^m).$$

Remark 4.5.1. The numbers $w_n(G)$ are given by the formula

$$w_n(G) = \frac{1}{n}\sum_{m|n}\mu(n/m)\left[\sum_{0\le i\le[m/2]}(-1)^i\frac{m}{m-i}\binom{m-i}{i}d^{m-2i}\right].$$

(See [Lab70, Proof of Proposition 4].)

Proposition 4.5.2. *If $n = p^k m$ with $(m,p) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{p^k m}(G).$$

Example 4.5.3. Let G be a Demushkin pro-p-group of finite rank d. We have

$$c_1(G) = d,$$

$$c_2(G) = \begin{cases} \frac{d^2-d-2}{2} & \text{if } p \neq 2, \\ \frac{d^2+d-2}{2} & \text{if } p = 2, \end{cases}$$

$$c_3(G) = \begin{cases} \frac{d^3-4d}{3} & \text{if } p \neq 3, \\ \frac{d^3-d}{3} & \text{if } p = 3, \end{cases}$$

$$c_4(G) = \begin{cases} \frac{d^4-5d^2+4}{4} & \text{if } p \neq 2, \\ \frac{d^4-3d^2+2d}{4} & \text{if } p = 2, \end{cases}$$

$$c_5(G) = \begin{cases} \frac{d^5-5d^3+4d}{5} & \text{if } p \neq 5, \\ \frac{d^5-5d^3+9d}{5} & \text{if } p = 5. \end{cases}$$

Observe that our numbers $c_n(G)$, $n = 1, 2, \ldots$, also detect the minimal numbers of generators of $G_{(n)}$. Indeed by the remarkable result of I. V. Andožskii and independently by J. Dummit and J. Labute for each open subgroup T of the Demushkin group G, we have the following expression for the minimal number of generators $d(T)$ of T:

$$d(T) = [G : T](d(G) - 2) + 2.$$

(See [NSW08, Theorem 3.9.15].) Therefore

$$d_n(G) := d(G_{(n)}) = p^{\sum_{i=1}^{n-1} c_i(G)}(d-2)+2.$$

From now on we assume that $G = F/\langle r\rangle$, where F is a free pro-p-group on generators $x_1, x_2, \ldots, x_d$, and

$$r = [x_1, x_2][x_3, x_4]\cdots[x_{d-1}, x_d].$$

Then we extract from [Lab70] the following fact.

Lemma 4.5.4. *For every n, $w_n(G) = \mathrm{rank}_{\mathbb{Z}_p} G_n/G_{n+1}$.*

Proof. This follows from [Lab70, Theorem and proof of Proposition 4] and Corollary 2.1.12. □

Corollary 4.5.5. *Assume that for each n, B_n represents a $\mathbb{Z}_p$-basis of G_n/G_{n+1}. Let us write $n = p^k m$ with $(m,p) = 1$. Then a basis of the $\mathbb{F}_p$-vector space $G_{(n)}/G_{(n+1)}$ can be represented by the following set*

$$B_m^{p^k} \bigsqcup B_{pm}^{p^{k-1}} \bigsqcup \cdots \bigsqcup B_{p^{k-1}m}^{p} \bigsqcup B_n.$$

4.6 Some Other Groups

4.6.1 Free products of a finite number of Demushkin groups and free pro-p-groups

Let G be a free pro-p product of r Demushkin groups of ranks $d_1, \ldots, d_r$ and of a free pro-p-group of rank e. The Hilbert-Poincaré series of $\mathrm{gr}(\mathbb{F}_p[[G]])$ is

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1}{1-(d_1+\cdots+d_r+e)t+rt^2} =: \frac{1}{(1-at)(1-bt)}.$$

We define the sequence $w_n(G), n = 1, 2, \ldots$ by

$$w_n(G) = \frac{1}{n}\sum_{m|n}\mu(m)(a^{n/m}+b^{n/m}) = \frac{1}{n}\sum_{m|n}\mu(n/m)(a^m+b^m).$$

Proposition 4.6.1. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{p^k m}(G).$$

4.6.2 A free product of a cyclic group of order 2 and a free pro-2-group

We first consider the case of $p = 2$ because this is the case of interest in Galois theory (of 2-extensions), and because this case is a bit simpler than the general case of any prime p. This latter case will be covered in the next subsection.

Let $G = C_2 * S$ be a free pro-2 product of the cyclic group C_2 of order 2 and a free pro-2-group of rank d. The Hilbert-Poincaré series of $\mathrm{gr}(\mathbb{F}_2[[G]])$ is

$$P_{\mathrm{gr}(\mathbb{F}_2[[G]])}(t) = (\frac{1}{1+t} - dt)^{-1} = \frac{1+t}{1-dt-dt^2} =: \frac{1+t}{(1-at)(1-bt)}.$$

We define the sequence $w_n(G), n = 1, 2, \ldots$ by

$$w_n(G) = \frac{1}{n} \sum_{m|n} \mu(n/m)(a^m + b^m - (-1)^m).$$

Proposition 4.6.2. *If $n = 2^k m$ with $(m, 2) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{2^k m}(G).$$

4.6.3 A free product of a cyclic group of order p and a free pro-p-group

Let $G = C_p * S$ be a free pro-p product of the cyclic group C_p of order p and a free pro-p-group of rank d. We shall find a formula for $c_n(G)$. The Hilbert-Poincaré series of $\mathrm{gr}(\mathbb{F}_p[[G]])$ is

$$P_{\mathrm{gr}(\mathbb{F}_p[[G]])}(t) = \frac{1+t+\cdots+t^{p-1}}{1-dt-dt^2-\cdots-dt^p} =: \frac{(1-\xi_1 t)\cdots(1-\xi_{p-1}t)}{(1-a_1 t)\cdots(1-a_p t)}.$$

We define the sequence $w_n(G), n = 1, 2, \ldots$ by

$$w_n(G) = \frac{1}{n}\sum_{m|n} \mu(n/m)(a_1^m + \cdots + a_p^m - (\xi_1^m + \cdots + \xi_{p-1}^m)).$$

Proposition 4.6.3. *If $n = p^k m$ with $(m, p) = 1$, then*

$$c_n(G) = w_m(G) + w_{pm}(G) + \cdots + w_{p^k m}(G).$$

Remark 4.6.4. Note that

$$\xi_1^n + \cdots + \xi_{p-1}^n = \begin{cases} -1 \text{ if } (n,p) = 1, \\ p - 1 \text{ if } p \mid n. \end{cases}$$

We shall compute $a_1^n + \cdots + a_p^n$. From

$$\frac{1}{(1 - a_1 t)\cdots(1 - a_p t)} = \frac{1}{1 - (dt + dt^2 + \cdots + dt^p)},$$

taking logarithms of both sides, we obtain

$$\begin{aligned}
&\sum_{n\geq 1} \frac{1}{n}(a_1^n + \cdots + a_p^n)t^n = \sum_{n\geq 1} \frac{1}{n}(dt + dt^2 + \cdots + dt^p)^n \\
&= \sum_{n\geq 1} \frac{1}{n} \sum_{\substack{k_1+\cdots+k_p=n,\\ k_i\geq 0}} \binom{n}{k_1, \ldots, k_p} (dt)^{k_1}(dt^2)^{k_2}\cdots(dt^p)^{k_p} \\
&= \sum_{M} \sum_{\substack{k_1+2k_2+\cdots+pk_p=M,\\ k_i\geq 0}} \\
&\qquad \left[\frac{1}{M - k_2 - \cdots - (p-1)k_p} \binom{M - k_2 - \cdots - (p-1)k_p}{k_1, \ldots, k_p} d^{M-k_2-\cdots-(p-1)k_p}\right] t^M.
\end{aligned}$$

Finally comparing the coefficients of t^n gives us the required formula for $a_1^n + \cdots + a_p^n$,

$$\begin{aligned}
&a_1^n + \cdots + a_p^n \\
&= \sum_{\substack{k_1+2k_2+\cdots+pk_p=n,\\ k_i\geq 0}} \frac{n}{n - k_2 - \cdots - (p-1)k_p} \binom{n - k_2 - \cdots - (p-1)k_p}{k_1, \ldots, k_p} d^{n-k_2-\cdots-(p-1)k_p}.
\end{aligned}$$

Chapter 5

Relations in Pro-p Galois Groups

As we have seen, Demushkin groups are pro-p groups which play an important role in Galois theory. These groups have a single defining relation among a finite set of generators and appear as Galois groups of maximal p-extensions of local fields containing a primitive p-th root of unity. The study of relations in Demushkin groups has a long and interesting history and we saw in section 3.3.4 that the unique relation among generators of a Demushkin group can take one of only four rather special forms. One example of a specific Demushkin relation is

$$r = x_1^p[x_1, x_2][x_3, x_4] \cdots [x_{d-1}, x_d].$$

The question arises as to whether other pro-p Galois groups have similar restrictions on the shape of relations. That is, if G is a pro-p group which is realizable as the Galois group $G_F(p)$ of the maximal p-extension of a field F, must the relations in G take on only certain forms?

In this chapter we begin to explore that question and will see that even considering only small abelian extensions of F can provide insight into necessary restrictions on relations in pro-p Galois groups. Further work to extend these results and thereby provide a better understanding of the structure of absolute Galois groups is in progress.

5.1 The Case $\zeta_{p^2} \in F$

In this section we assume that p is a prime and F is a field containing a primitive p^2-th root of unity ζ_{p^2}.

Theorem 5.1.1. *Let p be a prime and F a field containing a primitive p^2-th root of unity ζ_{p^2}. There is no relation $r = x_1^p x_2^p s \in R$, where $S =< x_1, x_2, \ldots >$ is a free pro-p group, $s \in [S, S]$ and*

$$1 \longrightarrow R \longrightarrow S \xrightarrow{\pi} G_F(p) \longrightarrow 1$$

is a minimal presentation of $G_F(p)$.

Proof. Suppose such an r exists and consider the field $L = F(\sqrt[p^2]{a} \mid a \in F^\times)$. By Kummer theory, $\mathrm{Gal}(L/F)$ is the Pontrjagin dual $(F^\times/(F^\times)^{p^2})^*$ of $F^\times/(F^\times)^{p^2} \cong (\bigoplus_J C_p) \bigoplus (\bigoplus_I C_{p^2})$ [Kap69, p. 17, Theorem 6]. Since $\zeta_{p^2} \in F$, every cyclic extension $F(\sqrt[p]{a})/F$ of degree p embeds into a cyclic extension $K = F(\sqrt[p^2]{a})/F$ of degree p^2, so $J = \phi$ and

$$\begin{aligned} \mathrm{Gal}(L/F) &\cong (\textstyle\bigoplus_I C_{p^2})^* \\ &= \textstyle\prod_I C_{p^2}. \end{aligned}$$

Let σ_i be the image of $\pi(x_i),\ i = 1, 2$ under the restriction map

$$S \xrightarrow{\pi} G_F(p) \xrightarrow{res} \mathrm{Gal}(L/F).$$

Then

$$\begin{aligned} 1 &= res(\pi(r)) \\ &= res(\pi(x_1)^p \pi(x_2)^p \pi(s)) \\ &= (res\ \pi(x_1))^p (res\ \pi(x_2))^p \\ &= \sigma_1^p \sigma_2^p \\ &= (\sigma_1 \sigma_2)^p. \end{aligned}$$

However, since

$$1 \longrightarrow R \longrightarrow S \xrightarrow{\pi} G_F(p) \longrightarrow 1$$

is a minimal presentation of $G_F(p)$, it follows that $\pi(x_1)$ and $\pi(x_2)$ are independent modulo the Frattini subgroup $\Phi(G_F(p))$. So $\sigma_1\sigma_2$ has order p^2 in $\mathrm{Gal}(L/F)$, which is a contradiction. □

Theorem 5.1.2. *Let p be a prime and F a field containing a primitive p^2-th root of unity ζ_{p^2}. There is no relation $r = x_1^p s \in R$, where $S =< x_1, x_2, \ldots >$ is a free pro-p group, $s \in [S, S]$ and*

$$1 \longrightarrow R \longrightarrow S \xrightarrow{\pi} G_F(p) \longrightarrow 1$$

is a minimal presentation of $G_F(p)$.

Proof. As in the proof of Theorem 5.1.1, consider the field $L = F(\sqrt[p^2]{a} \mid a \in F^\times)$ with Galois group $\mathrm{Gal}(L/F) \cong \prod_I C_{p^2}$. If σ is the image of $\pi(x_1)$ under the restriction map

$$S \xrightarrow{\pi} G_F(p) \xrightarrow{res} \mathrm{Gal}(L/F),$$

then

$$\begin{aligned} 1 &= res(\pi(r)) \\ &= res(\pi(x_1)^p \pi(s)) \\ &= (res\ \pi(x_1))^p \\ &= \sigma^p. \end{aligned}$$

But since $\pi(x_1) \notin \Phi(G_F(p))$, σ generates a cyclic subgroup of $\mathrm{Gal}(L/F)$ of order p^2, so this is a contradiction. □

5.2 The Case $\zeta_p \in F,\ \zeta_{p^2} \notin F$

In this section we assume that p is an odd prime and F is a field which contains a primitive p-th root but not a primitive p^2-th root of unity.

In addition to the dihedral group D_4, other small nonabelian p-groups also play a fundamental role in the theory of Galois p-extensions. The modular group M_{p^3} is the unique nonabelian group of order p^3 and exponent p^2 given, in terms of generators and

relations, by

$$M_{p^3} = \langle x, y \mid x^{p^2} = y^p = 1,\ yxy^{-1} = x^{1+p} \rangle = \langle x \rangle \rtimes \langle y \rangle.$$

Theorem 5.2.1. *Let p be an odd prime and let F be a field containing a primitive p-th root of unity ζ_p, but no primitive p^2-th root of unity. Let $S =< x_1, x_2, \ldots >$ be a free pro-p group such that*

$$1 \longrightarrow R \longrightarrow S \xrightarrow{\pi} G_F(p) \longrightarrow 1$$

is a minimal presentation of $G_F(p)$. Then there is no relation of the form $r = x_1^p s \in R$, where $s \in [S, S]$ is such that any commutator of the form $[x_i, x_j]$ appearing in the expression for s has $i \neq 1$ and $j \neq 1$.

Proof. Suppose there is such a relation r. For $k = 2, 3$, choose a primitive p^k-th root of unity such that $\zeta_{p^k}^p = \zeta_{p^{k-1}}$. Consider the field $K = F(\zeta_{p^3})$. Then $\pi(x_1)(\zeta_{p^2}) = \zeta_{p^2}$; otherwise $\rho(\pi(x_1))$ would generate the entire Galois group $\mathrm{Gal}(K/F) \cong C_{p^2}$, contradicting

$$\rho(\pi(x_1))^p = \rho(\pi(x_1)^p \pi(s)) = \rho(r) = 1,$$

where $\rho : G_F(p) \twoheadrightarrow \mathrm{Gal}(K/F)$ is the restriction map.

Since the presentation

$$1 \longrightarrow R \longrightarrow S \xrightarrow{\pi} G_F(p) \longrightarrow 1$$

is minimal, $\pi(x_1) \notin \Phi(G_F(p))$. Hence there exists an element $a \in F \setminus F^p$ such that $\pi(x_1)(\sqrt[p]{a}) \neq \sqrt[p]{a}$.

The polynomial $x^{p^2} - a$ is irreducible over $F(\zeta_{p^2})$ so the extension $L := F(\zeta_{p^2}, \sqrt[p^2]{a})$ is Galois over F. Define automorphisms $\sigma, \tau \in \mathrm{Gal}(L/F)$ by

$$\tau : \sqrt[p^2]{a} \mapsto \zeta_{p^2} \sqrt[p^2]{a} \quad \text{and} \quad \tau : \zeta_{p^2} \mapsto \zeta_{p^2};$$

$$\sigma : \sqrt[p^2]{a} \mapsto \sqrt[p^2]{a} \quad \text{and} \quad \sigma : \zeta_{p^2} \mapsto \zeta_p \zeta_{p^2} = \zeta_{p^2}^p \zeta_{p^2} = \zeta_{p^2}^{p+1}.$$

So

$$\sigma\tau\sigma^{-1}(\zeta_{p^2}) = \zeta_{p^2} \quad \text{and}$$
$$\sigma\tau\sigma^{-1}(\sqrt[p^2]{a}) = \sigma\tau(\sqrt[p^2]{a}) = \sigma(\zeta_{p^2}\sqrt[p^2]{a}) = \zeta_{p^2}^{1+p}\sqrt[p^2]{a} = \tau^{1+p}(\sqrt[p^2]{a}).$$

Thus, τ has order p^2, σ has order p and $\sigma\tau\sigma^{-1} = \tau^{1+p}$, so

$$\mathrm{Gal}(L/F) = \langle \sigma, \tau \mid \tau^{p^2} = \sigma^p = 1,\ \sigma\tau\sigma^{-1} = \tau^{1+p} \rangle \cong M_{p^3}.$$

Now let $res : G_F(p) \twoheadrightarrow \mathrm{Gal}(L/F)$ be the restriction map. Since $\pi(x_1)(\zeta_{p^2}) = \zeta_{p^2}$ and $\pi(x_1)(\sqrt[p]{a}) \neq \sqrt[p]{a}$, it follows that $res(\pi(x_1))$ generates $\mathrm{Gal}(L/F(\zeta_{p^2}))$. Then, since no commutator $[x_i, x_j]$ in the expression for s involves x_1, we have

$$\begin{aligned} 1 &= res(\pi(r)) \\ &= res(\pi(x_1)^p \pi(s)) \\ &= res(\pi(x_1))^p \\ &= \tau^p, \end{aligned}$$

which is a contradiction, since τ has order p^2 in $\mathrm{Gal}(L/F)$. $\square$

We see that for a field F containing a p-th root of unity, the presence or absence of a p^2-th root of unity in F is already enough to place certain restrictions on the relations among a set of generators of the Galois group of the maximal p-extension of F. We look forward to the results of further research in this direction.

Chapter 6

Conclusion

In our quest for a deeper understanding of absolute Galois groups we are led to the study of small quotients and central filtrations of these large and largely mysterious objects. By developing techniques to count Galois p-extensions and calculate filtration subquotient dimensions we can, in turn, shed more light on these underlying structures. Answers to these Galois theoretic problems also have important ramifications in other areas of mathematics.

We have described several known techniques for counting finite Galois p-extensions of local fields. While actually constructing small 2-extensions of the p-adic integers is feasible, this would rapidly become unwieldy for local fields with larger square class groups. A technique involving complex characters and Möbius functions used by Yamagishi to enumerate the Galois extensions of a local field having a given Galois group G requires knowledge of the character table of G as well as its subgroups. This also becomes a significant obstacle as the order of G increases.

With these limitations in mind, we have explored other approaches and shown that by using some deeper results from Galois cohomology and the theory of quadratic forms and quaternion algebras one can develop more efficient combinatorial techniques. For example, we find that the number $\mathcal{N}$ of Galois extensions of a formally real pythagorean SAP field with square class group of cardinality 2^n having Galois group the dihedral

group of order 8 is given by the simple formula

$$\mathcal{N} = 2^{n-2} \sum_{k=2}^{n} \tbinom{n}{k}(2^{k-1} - 1).$$

Our main results pertain to the Zassenhaus filtration of finitely generated pro-p groups. Building on a remarkable theory of Jennings and Lazard, we have developed a method for determining the $\mathbb{F}_p$-dimension of subquotients of this filtration and derived explicit formulas applicable to various families of groups, including free pro-p groups, Demushkin groups and free pro-2 products of finitely many copies of the cyclic group of order 2.

These subquotient dimensions, $c_n(G)$, provide an important contribution to our knowledge of group theory and Galois theory. For example, in several significant cases they determine the minimal number of generators of the Zassenhaus subgroups of G, and if F is a pythagorean SAP field or a superpythagorean field, only two of these dimensions, $c_1(G_F(2))$ and $c_2(G_F(2))$ are needed in order to determine the Galois group of the maximal p-extension of F.

They are also of considerable interest in current Galois theory research, such as that involving the Kernel Unipotent Conjecture. If G is isomorphic to the maximal pro-p quotient $G_F(p)$ of the absolute Galois group G_F of a field F and if $F_{(n)}$ denotes the fixed field of $G_F(p)_{(n)}$, then $|\mathrm{Gal}(F_{(n)}/F)| = p^{\sum_{i=1}^{n-1} c_i(G)}$. If the Kernel Unipotent Conjecture is true, we would obtain a characterization of $G_F(p)_{(n)}$, $n \geq 3$, as the intersection of the kernels of all Galois representations $\rho : G_F(p) \to \mathbb{U}_n(\mathbb{F}_p)$. In the case when $G_F(p)$ is finitely generated, knowledge of $|\mathrm{Gal}(F_{(n)}/F)|$ would be useful in order to check whether the intersection of the kernels of given representations is in fact $G_F(p)_{(n)}$.

Another interesting area of research is the investigation of the shape of relations in pro-p Galois groups, which is closely related to detailed knowledge of small quotients of these groups. Further work is planned in this direction.

Certainly, much progress has been made since the time of Évariste Galois and much remains to be done. The journey so far has been fascinating and we look forward to the many miles not yet travelled.

Bibliography

[Ara75] J. K. Arason. Cohomologische invarianten quadratischen Formen. *J. Algebra*, 36:448–491, 1975.

[Art27] E. Artin. Über die Zerlegung definiter Funktionen in Qadrate. *Abh. Math. Sem. Univ. Hamburg*, 5:100–115, 1927.

[AS27] E. Artin and O. Schreier. Algebraische Konstruktion reeller Körper. *Abh. Math. Sem. Univ. Hamburg*, 5:85–99, 1927.

[Bec74] E. Becker. Euklidische Körper und euklidische Hüllen von Körpern. *J. Reine Angew. Math.*, 268/269:41–52, 1974.

[Bec78] E. Becker. *Hereditarily-Pythagorean fields and orderings of higher level*. Number 29 in Monografias de matemática. IMPA Lecture Notes, 1978.

[BG75] E. A. Bender and J. R. Goldman. On the applications of Möbius inversion in combinatorial analysis. *The American Mathematical Monthly*, 82:789–803, 1975.

[CEM12] S. K. Chebolu, I. Efrat, and J. Mináč. Quotients of absolute Galois groups which determine the entire Galois cohomology. *Math. Ann.*, 352(1):205–221, 2012.

[Dem61] S. P. Demushkin. The group of the maximal p-extension of a local field. *Izv. Akad. Nauk. SSSR Ser. Mat.*, 25:329–346, 1961. (Russian).

[Dem63] S. P. Demushkin. On 2-extensions of a local field. *Mat. Sibirsk Z.*, 4:951–955, 1963. (Russian).

[DSMS99] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*. Number 61 in Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2nd edition, 1999.

[Dwy75] W. G. Dwyer. Homology, Massey products and maps between groups. *J. Pure Appl. Algebra*, 6:177–190, 1975.

[Efr14a] I. Efrat. Filtrations of free groups as intersections. *Arch. Math. (Basel)*, 103:411–420, 2014.

[Efr14b] I. Efrat. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Adv. Math.*, 263:389–411, 2014.

[EM11a] I. Efrat and J. Mináč. Galois groups and cohomological functors. *arXiv: 1103.1508*, 2011. To appear in the Transactions of the American Mathematical Society.

[EM11b] I. Efrat and J. Mináč. On the descending central sequence of absolute Galois groups. *American J. Math.*, 133:1503–1532, 2011.

[Ers11] M. Ershov. Kazhdan quotients of Golod-Shafarevich groups. *Proc. Lond. Math. Soc. (3)*, 102(4):599–636, 2011.

[For11] P. Forré. Strongly free sequences and pro-p groups of cohomological dimension 2. *J. Reine Angew. Math.*, 658:173–192, 2011.

[Frö85] A. Fröhlich. Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants. *J. Reine Angew. Math.*, 360:84–123, 1985.

[Gär11] J. Gärtner. *Mild pro-p groups with trivial cup product.* PhD thesis, Universität Heidelberg, 2011.

[Hal50] M. Hall. A basis for free Lie rings and higher commutators in free groups. *Proc. Amer. Math. Soc.*, 1:575–581, 1950.

[Har90] D. Haran. Closed subgroups of $g(\mathbb{Q})$ with involutions. *J. Algebra*, 129(2):393–411, 1990.

[ILF97] V. V. Ishkhanov, B. B. Luré, and D. K. Faddeev. *The Embedding Problem in Galois Theory*, volume 165 of *Translations of Mathematical Monographs.* American Mathematical Society, 1997.

[JLY03] C. U. Jensen, A. Ledet, and N. Yui. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, volume 45 of *Mathematical Sciences Research Institute Publications.* Cambridge University Press, 2003.

[Kap69] I. Kaplansky. *Infinite Abelian Groups.* University of Michigan Press, 1969.

[Koc02] H. Koch. *Galois theory of p-extensions.* Springer Monographs in Mathematics. Springer-Verlag, 2002.

[Lab66] J. Labute. Classification of Demushkin groups. *Canadian J. Math.*, 19:106–132, 1966.

[Lab70] J. Labute. On the descending central series of groups with a single defining relation. *J. Algebra*, 14:16–23, 1970.

[Lab06] J. Labute. Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$. *J. Reine Angew. Math.*, 596:155–182, 2006.

[Lam83] T. Y. Lam. *Orderings, valuations and quadratic forms*. Number 52 in CBMS Regional Conference Series in Mathematics. American Mathematical Society, 1983.

[Lam05] T. Y. Lam. *Introduction to Quadratic Forms over Fields*. American Mathematical Society, 2005.

[Led05] A. Ledet. *Brauer Type Embedding Problems*. Fields Institute Monographs. American Mathematical Society, 2005.

[Lem74] J.-M. Lemaire. *Algèbres connexes et homologie des espaces de lacets*. Number 422 in Lecture Notes in Mathematics. Springer-Verlag, 1974.

[Lic80] A. I. Lichtman. On Lie algebras of free products of groups. *J. Pure Appl. Algebra*, 18(1):67–74, 1980.

[LM11] J. Labute and J. Mináč. Mild pro-2 groups and 2-extensions of $\mathbb{Q}$ with restricted ramification. *J. Algebra*, 332:136–158, 2011.

[Mas87] R. Massy. Construction de p-extensions galoisiennes d'un corps de caractéristique différent de p. *J. Algebra*, 109(2):508–535, 1987.

[Mer81] A. Merkurjev. On the norm residue symbol of degree 2. *Soviet Math. (Doklady)*, 24:546–551, 1981.

[Min86] J. Mináč. Galois groups of some 2-extensions of ordered fields. *C. R. Math. Rep. Acad. Sci. Canada*, 8(2):103–108, 1986.

[MNQD77] R. Massy and T. Nguyen-Quang-Do. Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3: étude locale-globale. *J. Reine Angew. Math.*, 291:149–161, 1977.

[MRT15] J. Mináč, M. Rogelstad, and N. D. Tân. Dimensions of Zassenhaus filtration subquotients of some pro-p groups. *arXiv: 1405.6980v2*, 2015. To appear in the Israel Journal of Mathematics.

[MS90] J. Mináč and M. Spira. Formally real fields, pythagorean fields, C-fields and W-groups. *Math. Z.*, 205(4):519–530, 1990.

[MS96] J. Mináč and M. Spira. Witt rings and Galois groups. *Ann. of Math.*, 144(1):35–60, 1996.

[MT13] J. Mináč and N. D. Tân. Triple Massey products and Galois theory. *arXiv: 1307.6624*, 2013. To appear in the Journal of the European Mathematical Society.

[MT14] J. Mináč and N. D. Tân. Counting Galois $\mathbb{U}_4(\mathbb{F}_p)$-extensions using Massey products. *arXiv: 1408.2586*, 2014.

[MT15] J. Mináč and N. D. Tân. The Kernel Unipotent Conjecture and Massey products on an odd rigid field. *Adv. Math.*, 273:242–270, 2015. (with an appendix by I. Efrat, J. Mináč and N. D. Tân).

[Nai95] H. Naito. Dihedral extensions of degree 8 over the rational p-adic fields. *Proc. Japan Acad. Ser. A. Math. Sci.*, 71, 1995.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Number 323 in A Series of Comprehensive Studies in Mathematics. Springer-Verlag, second edition, 2008.

[PP05] A. Polishchuk and L. Positselski. *Quadratic algebras*. Number 37 in University Lecture Series. American Mathematical Society, 2005.

[Qui68] D. G. Quillen. On the associated graded ring of a group ring. *J. Algebra*, 10:411–418, 1968.

[Rot64] G.-C. Rota. On the foundations of combinatorial theory. *Z. Wahrscheinlichkeitstheorie*, 2:340–368, 1964.

[Sch85] W. Scharlau. *Quadratic and Hermitian Forms*. Number 270 in A Series of Comprehensive Studies in Mathematics. Springer-Verlag, 1985.

[Ser02] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer, 2002. Corrected second printing.

[Ser63] J.-P. Serre. Structures de certain pro-p groups. In *Sém. Bourbaki, exposé 252*, 1962/63.

[Sha47] I. R. Shafarevich. On p-extensions. *Math. Sb.*, 20:351–363, 1947. (Russian).

[Sri95] V. Srinivas. *Algebraic K-theory*. Birkhäuser, second edition, 1995.

[Wal61] G. E. Wall. Some applications of the Eulerian functions of a finite group. *J. Austral. Math. Soc.*, 2:35–59, 1961.

[War78] R. Ware. When are Witt rings group rings? II. *Pacific J. Math.*, 76(2):541–564, 1978.

[War79] R. Ware. Quadratic forms and profinite 2-groups. *J. Alg.*, 58:227–237, 1979.

[Wit37a] E. Witt. Theorie der quadratischen Formen in beliebigen Körpern. *J. Reine Angew. Math.*, 176:31–44, 1937.

[Wit37b] E. Witt. Treue Darstellung Liescher Ringe. *J. Reine Angew. Math.*, 177:152–160, 1937.

[Yam95] M. Yamagishi. On the number of Galois p-extensions of a local field. *Proc. Amer. Math. Soc.*, 123(8):2373–2380, August 1995.

[Zas40] H. Zassenhaus. Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Characteristic p zuzuordnen. *Abh. Mat. Sem. Univ. Hamburg*, 13:200–207, 1940.

CURRICULUM VITAE

Name:	Michael L. Rogelstad	
Post-secondary Education and Degrees:	The University of Western Ontario London, Ontario, Canada	
	M.D. (cum laude)	1983
	FRCSC Ophthalmology	1988
	M.Sc. Physics	1996
	B.Sc. Honors Mathematics	2005
	M.Sc. Mathematics	2010
	Ph.D. Mathematics	2015
Honours and Awards:	UWO Board of Governors Scholarship	1977-1981
	J.A.F. Stevenson Memorial Scholarship	1982
	Horner Medal in Ophthalmology	1983
	Angela Armitt Gold Medal	2004
	Western Graduate Research Scholarship	2009
	Ontario Graduate Scholarship	2010-2012
	NSERC Alexander Graham Bell Canada Graduate Scholarship D	2012-2014
Related Work Experience:	Teaching Assistant The University of Western Ontario	2009-2013

Publications:

- F. B. Yousif, J. B. A. Mitchell, M. Rogelstad, A. Le Paddelec, A. Canosa, and M. I. Chibisov (1994). *Dissociative recombination of HeH^+: a re-examination.* Phys. Rev. A 49, 4610-4615.

- F. B. Yousif, M. Rogelstad, and J. B. A. Mitchell. *Rydberg state formation in H_3^+ recombination,* in Proceedings of the Fourth U.S.-Mexico Symposium on Atomic and Molecular Physics, 343-351. World Scientific, 1995.

- M. L. Rogelstad, F. B. Yousif, T. J. Morgan, and J. B. A. Mitchell (1997). *Stimulated radiative recombination of H^+ and He^+.* J. Phys. B: At. Mol. Opt. Phys. 30, 3913-3931.

- J. Mináč, M. Rogelstad, and N. D. Tân. *Dimensions of Zassenhaus filtration subquotients of some pro-p groups.* arXiv: 1405.6980v2, 2015. To appear in the Israel Journal of Mathematics.