Applications of representation theory and K-theory to problems in algebraic number theory

Submitted by Fabio Ferri, to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Mathematics, June 2022.

I certify that all material in this thesis which is not my own work has been identified and that any material that has previously been submitted and approved for the award of a degree by this or any other University has been acknowledged.

Signature .....

Abstract

> Has the verb "to dream" a present tense? How does a person learn to use this?
>
> Ludwig Wittgenstein

In this thesis we consider three main problems: the Galois module structure of rings of integers in wildly ramified extensions of $\mathbb{Q}$; Leopoldt's conjecture; and non-commutative Fitting ideals and the non-abelian Brumer-Stark conjecture. For each of these problems, which correspond to each main chapter, we will review and use tools from representation theory and algebraic K-theory.

In the first main chapter, we will prove new results concerning the additive Galois module structure of certain wildly ramified finite non-abelian extensions of $\mathbb{Q}$. In particular, when $K/\mathbb{Q}$ is a Galois extension with Galois group G isomorphic to A_4, S_4 or A_5, we give necessary and sufficient conditions for the ring of integers $\mathcal{O}_K$ to be free over its associated order in the rational group algebra $\mathbb{Q}[G]$.

In the second main chapter, we will work on Leopoldt's conjecture. Let p be a rational prime and let L/K be a Galois extension of number fields with Galois group G. Under certain hypotheses, we show that Leopoldt's conjecture at p for certain proper intermediate fields of L/K implies Leopoldt's conjecture at p for L; a crucial tool will be the theory of norm relations in $\mathbb{Q}[G]$. We also consider relations between the Leopoldt defects at p of intermediate extensions of L/K.

Finally, we will investigate new properties of (non-commutative) Fitting ideals in integral group rings, with the general idea of reducing to simpler abstract groups (such as abelian groups) that can emerge as subquotients. As an application we will provide a direct proof of the (non-abelian) Brumer-Stark conjecture in certain cases, by reducing to the abelian case as recently proved by Dasgupta and Kakde. The direct approach avoids use of technical machinery such as the equivariant Tamagawa number conjecture.

Acknowledgements

First of all I wish to express my deepest gratitude to my supervisor Henri Johnston for his constant support, competence and patience throughout my PhD and for the friendly vibe we created. I have been very lucky to work in such a stimulating number theory group at Exeter; in particular, I would also like to thank Julio Andrade, Nigel Byott, Valentina Di Proietto, Oli Gregory, Andreas Langer, Filippo Nuccio for their further guidance and enrichment of my experience.

Outside Exeter, I am grateful to Cornelius Greither for encouraging me to start this journey back in 2018. I would also like to thank Ilaria Del Corso and Davide Lombardo for having continued fruitful collaborations and for having made me keep the spirit of the number theory environment of Pisa alive in me, as well as Lorenzo Stefanello for having co-organised such a fun workshop about Galois modules. I also wish to thank Andreas Nickel for his kindness and guidance over the last few years and Tim Dokchitser for welcoming me into a new journey at the University of Bristol.

I do not regret anything about living in this tiny city for almost four years. I still feel there is a lot to discover here and even today I often still meet such interesting characters who make this place so magical. I wish to thank all the friends I made and who contributed to my spiritual growth and to making my time in Devon so enjoyable, all in the non-mutually exclusive categories of academics, musicians and creative hippies: in particular, Alberto Corato, Andrea Ceni, Andy Corbett, David Reinstein, Doug Coates, Emanuele Tovazzi, Eugenio Sabatino, Giulia Murtas, Helen Louise, James Madell, James Storm, Joe MacMillan, Jonathan Segar, Kevin Smith, Matt Chivers, Silvia Filippi, Surabhi Desai, Taddy Berry, Valentina Todino. To these I would like to add all the members of the bands I have been part of: Tarab, EUJO, DEFM Jazz Combo, Trikkeballakke, Deems Experiment.

In my very last list I want to thank my old friends I remained in contact with: Aluna Rizzoli, Antonio Camerlengo, Dario Rancati, Emanuele Tron, Enrico Merlin, Francesco Ballini, Gianluigi Di Giacomo, Giovanni Pederiva, Guglielmo Nocera, Lorenzo Benedini, Luca Minutillo Menga, Luigi Pagano.

Finally, I wish to thank my family for never ending support, warmth and understanding.

Contents

Chapter 1

Introduction

This thesis, written under the supervision of Henri Johnston, collects three main works, each corresponding to a separate chapter. We will be using tools from abstract algebra, in particular from representation theory, in order to tackle problems and conjectures in algebraic number theory. A common idea in these three works is that purely algebraic arguments combined with the knowledge of some basic cases allow us to deduce our results in much more complex situations. We will give more details in the introduction to each of the chapters.

We will start with the following example: suppose we have a Galois extension $K/\mathbb{Q}$ with Galois group G isomorphic to A_4. We will see that an important question is whether its ring of integers $\mathcal{O}_K$ is a free module over the so called *associated order* $\mathfrak{A}_{K/\mathbb{Q}}$, which is a particular $\mathbb{Z}$-algebra without torsion that spans $\mathbb{Q}[G]$. Specifically, using the structure of K as a $\mathbb{Q}[G]$-module coming from Galois theory, we define

$$\mathfrak{A}_{K/\mathbb{Q}} = \{x \in \mathbb{Q}[G] : x\mathcal{O}_K \subseteq \mathcal{O}_K\}.$$

Note that we always have $\mathfrak{A}_{K/\mathbb{Q}} \supseteq \mathbb{Z}[G]$. We will see that it suffices to us to just focus on the problem of *local freeness*, that is, asking if $\mathcal{O}_{K,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q},p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathfrak{A}_{K/\mathbb{Q}}$ for every prime number p. If we focus on $p = 3$ and we denote by F the subfield of K fixed by the 2-Sylow of A_4, which is normal of index 3, we will see that $\mathfrak{A}_{K/\mathbb{Q},3}$ can be written as a product of $\mathfrak{A}_{F/\mathbb{Q},3}$ and a maximal order. We will omit the details here, but we remark that in a local setting 'a lattice over a maximal order is free', so that our problem is reduced to studying whether in a much simpler extension, namely the Galois cubic extension $F/\mathbb{Q}$, the ring of integers is free over the associated order. Using abstract algebra (more precisely, the theory of *hybrid orders*) we are able to derive properties for A_4-extensions from C_3-extensions, whose behaviour is already well-known in the literature (in particular, here Leopoldt's theorem applies). We summarise the three main theorems of §2.

Theorem 1.0.1. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if 2 is tamely ramified or has full decomposition group.*

Theorem 1.0.2. *Let $K/\mathbb{Q}$ be a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if one of the following conditions on $K/\mathbb{Q}$ holds:*

(i) 2 *is tamely ramified;*

(ii) 2 *has decomposition group equal to the unique subgroup of* G *of order* 12*;*

(iii) 2 *is wildly and weakly ramified and has full decomposition group; or*

(iv) 2 *is wildly and weakly ramified, has decomposition group of order* 8 *in* G*, and has inertia subgroup equal to the unique normal subgroup of order* 4 *in* G*.*

Theorem 1.0.3. *Let* $K/\mathbb{Q}$ *be a Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$*. Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if all three of the following conditions on* $K/\mathbb{Q}$ *hold:*

(i) 2 *is tamely ramified;*

(ii) 3 *is tamely ramified or is weakly ramified with ramification index* 6*; and*

(iii) 5 *is tamely ramified or is weakly ramified with ramification index* 10*.*

Now we consider Leopoldt's conjecture (not to be confused with the aforementioned Leopoldt's theorem). For its statement and basic properties we refer to §3.2.1. Let L/K be a Galois extension of number fields with Galois group G and let p be a prime number. Assuming the existence of *norm relations*, which only depends on the structure of G as an abstract group, or even just using more basic properties coming from representation theory, we will be able to derive Leopoldt's conjecture at p for L ($\mathrm{Leo}(L,p)$ for short) from the validity on certain intermediate fields of L/K. For instance, validity for an S_3-extension of $\mathbb{Q}$ will be implied from its validity for two simpler fields: the quadratic subfield of L and a cubic subfield. Since the former is an abelian extension of $\mathbb{Q}$, we already know that Leopoldt's conjecture holds, so that the problem reduces to studying a cubic subfield (which is non-Galois). We state some of the results of §3.

Theorem 1.0.4. *Let* L/K *be a Galois extension of number fields with Galois group* G*. Let* p *be a prime number. If* $\mathrm{Leo}(L^H,p)$ *holds for every subgroup* H *of* G *which is the kernel of an irreducible complex character, then also* $\mathrm{Leo}(L,p)$ *holds.*

Corollary 1.0.5. *Let* L/K *be an abelian extension of number fields. Let* p *be a prime number. If* $\mathrm{Leo}(F,p)$ *holds for every intermediate field* F *such that* F/K *is cyclic, then also* $\mathrm{Leo}(L,p)$ *holds.*

Theorem 1.0.6. *Let* ℓ *be an odd prime number and let* L/K *be a dihedral extension of order* 2ℓ*, where* K *is* $\mathbb{Q}$ *or an imaginary quadratic field. Let* p *be a prime number. If* $\mathrm{Leo}(F,p)$ *holds for one (indeed, every) intermediate field* F *such that* $[F:K]=\ell$*, then we also have* $\mathrm{Leo}(L,p)$*.*

In the following $\delta(L,p)$ will denote the *Leopoldt defect* of the number field L at p, which roughly measures the failure of L from satisfying Leopoldt's conjecture at p (in particular, $\mathrm{Leo}(L,p)$ holds if and only if $\delta(L,p)=0$).

Theorem 1.0.7. *Let* L/K *be a Galois extension of number fields with Galois group* G *and let* p *be a prime number. Let* H *be a non-cyclic subgroup of* G*. Then we have the relation*

$$\sum_{I \leq H} |I|\ \mu(I,H)\ \delta(L^I,p) = 0,$$

where $\mu(I,H) := \sum_{I=H_0 \lneq \cdots \lneq H_n = H} (-1)^n$*.*

Theorem 1.0.8. *Let L be a finite Galois extension of $\mathbb{Q}$ or of an imaginary quadratic field with Galois group G. Let p be a prime number. Let $1 < d_1 < \cdots < d_s$ be the possible dimensions of the non-linear irreducible complex characters of G. Then we can write $\delta(L,p) = \sum_{i=1}^{s} k_i d_i$ with coefficients $k_i \in \mathbb{N}$. In particular either $\delta(L,p) = 0$ or $\delta(L,p) \geq d_1$.*

Theorem 1.0.9. *Let $\mathcal{A}$ be a finite set of prime numbers. Then there exists an infinite family $\mathcal{L}$ of real S_3-extensions of $\mathbb{Q}$ such that $\mathrm{Leo}(L,p)$ holds for every $L \in \mathcal{L}$ and $p \in \mathcal{A}$.*

In §4 we will discuss (non-commutative) Fitting ideals, stating some properties and studying them using or taking inspiration from algebraic K-theory. The main arithmetic motivation is the Brumer-Stark conjecture. In the recent groundbreaking preprint [DK20], Dasgupta and Kakde proved the (abelian) Brumer-Stark conjecture outside the prime 2. Our algebraic techniques will permit us to deduce the non-abelian Brumer-Stark conjecture for large families of Galois extensions using their result, in a very direct way that does not pass through, for instance, the technical setting of the equivariant Tamagawa number conjecture.

The following is the main algebraic result.

Theorem 1.0.10. *Let G be a finite group, let $\mathcal{H}$ be a family of subquotients of G and let p be a prime number. Suppose that*

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}}\left(\mathbb{Z}_p[H]\cap\zeta(\mathbb{Q}_p[H])^\times\right)\right)\subseteq\mathbb{Z}_p[G], \tag{1.0.1}$$

where ζ denotes the centre of a ring and

$$f_{\mathcal{H}}=\prod_{H\in\mathcal{H}}f_H:\zeta(\mathbb{Q}_p[G])^\times\longrightarrow\prod_{H\in\mathcal{H}}\zeta(\mathbb{Q}_p[H])^\times$$

is a certain map defined functorially. Let $\theta \in \zeta(\mathbb{Q}_p[G])^\times$ and let M be a finitely presented R-torsion $\mathbb{Z}_p[G]$-module with quadratic presentation. Let M_H be the image of M via composition of restriction and quotient (see the end of §4.4). If $f_H(\theta) \in \mathrm{Fitt}_{\mathbb{Z}_p[H]}(M_H)$ for every $H \in \mathcal{H}$, then $\theta \in \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M)$.

Theorem 1.0.10 can be applied to provide a more direct proof of some cases of the non-abelian Brumer-Stark conjecture than what we already find in literature (although none of the actual results will be new).

Theorem 1.0.11. *Let p be an odd prime number. Let L/K be a Galois CM-extension of number fields with Galois group G such that $p \nmid |G'|$ and let $\mathcal{H}$ be a family of abelian subquotients of G. Suppose that the complex conjugation j belongs to G_1 for every $G_1/G_2 \in \mathcal{H}$. Let S and T be two admissible sets of primes. Suppose that we have the containment (1.0.1) and that $\mathrm{Cl}(L)^T(p)$ has a quadratic presentation. Then the p-part of the strong Brumer-Stark conjecture for L/K holds.*

It will be important to assume that $\mathrm{Cl}(L)^T(p)$ has a quadratic presentation. However, using the tool of hybrid orders, we will be able to deduce the Brumer-Stark conjecture without such an assumption; this applies for instance to $A_4 \times C_2$-extensions at $p = 3$.

Note that if $p \nmid |G|$ we automatically have quadratic presentation (see Proposition 4.7.2).

Notation and conventions

All rings are assumed to have an identity element and all modules are assumed to be left modules unless otherwise stated. We denote certain finite groups as follows:

- D_{2n} is the dihedral group of order $2n$;
- Q_8 is the quaternion group of order 8;
- A_n is the alternating group on n letters;
- S_n is the symmetric group on n letters.

Chapter 2

Leopoldt-type theorems for non-abelian extensions of $\mathbb{Q}$

2.1 Introduction

This chapter is essentially the same as the arXiv preprint [Fer21].

Let K/F be a finite Galois extension of number fields or p-adic fields and let $G = \mathrm{Gal}(K/F)$. The classical normal basis theorem says that K is free of rank 1 as a module over the group algebra $F[G]$. A much more difficult problem is that of determining whether the ring of integers $\mathcal{O}_K$ is free of rank 1 over an appropriate $\mathcal{O}_F$-order in $F[G]$. The natural choice of such an order is the so-called associated order

$$\mathfrak{A}_{K/F} := \{\lambda \in F[G] : \lambda \mathcal{O}_K \subseteq \mathcal{O}_K\},$$

since this is the only $\mathcal{O}_F$-order in $F[G]$ over which $\mathcal{O}_K$ can possibly be free.

It is clear that the group ring $\mathcal{O}_F[G]$ is contained in $\mathfrak{A}_{K/F}$. In fact, $\mathfrak{A}_{K/F} = \mathcal{O}_F[G]$ if and only if K/F is at most tamely ramified. It is in this setting that by far the most progress has been made and we say that K/F has a normal integral basis if $\mathcal{O}_K$ is free over $\mathcal{O}_F[G]$. The celebrated Hilbert-Speiser theorem says that if $K/\mathbb{Q}$ is a tamely ramified finite abelian extension, then it has a normal integral basis. Leopoldt removed the assumption on ramification to obtain the following generalisation of this result.

Theorem 2.1.1. *[Leo59] Let $K/\mathbb{Q}$ be a finite abelian extension. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Leopoldt also specified a generator and the associated order; Lettl [Let90] gave a simplified and more explicit proof of the same result. We also have the following result of Bergé.

Theorem 2.1.2. *[Ber72] Let p be a prime and let $K/\mathbb{Q}$ be a dihedral extension of degree $2p$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Now let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8. Suppose that $K/\mathbb{Q}$ is tamely ramified. Martinet [Mar71] gave two examples of such extensions, one without and one with a normal integral basis. Moreover, Fröhlich

[Frö72] showed that both possibilities occur infinitely often. By contrast, in the case that $K/\mathbb{Q}$ is wildly ramified, we have the following result of Martinet.

Theorem 2.1.3. *[Mar72] Let $K/\mathbb{Q}$ be a wildly ramified Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong Q_8$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

In this chapter, we prove other Leopoldt-type theorems for certain non-abelian extensions of $\mathbb{Q}$. An important notion is that of local freeness, which we now review.

For the rest of the introduction, let $K/\mathbb{Q}$ be a finite Galois extension and let $G = \mathrm{Gal}(K/\mathbb{Q})$. We recall that $\mathcal{O}_K$ is said to be locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at a prime number p if $\mathcal{O}_{K,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K$ is free as an $\mathfrak{A}_{K/\mathbb{Q},p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathfrak{A}_{K/\mathbb{Q}}$-module. We say that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ if this holds for all prime numbers p.

Suppose that $K/\mathbb{Q}$ is tamely ramified. Then $\mathcal{O}_K$ is locally free over $\mathbb{Z}[G]$. Moreover, the problem of determining whether $K/\mathbb{Q}$ has a normal integral basis is well understood thanks to Taylor's proof of Fröhlich's conjecture [Tay81]: he determined the class of $\mathcal{O}_K$ in the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ in terms of Artin root numbers of the irreducible symplectic characters of G (see [Frö83, I] for an overview). In particular, if G has no irreducible symplectic characters (this is the case, for instance, if G is abelian, dihedral or of odd order), then $K/\mathbb{Q}$ has a normal integral basis.

If $K/\mathbb{Q}$ is wildly ramified, then the situation becomes much more difficult, not least because $\mathcal{O}_K$ need not even be locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. For instance, Bergé [Ber79] gave examples of wildly ramified dihedral extensions of $\mathbb{Q}$ without the local freeness property.

Let N/M be a finite Galois extension of p-adic fields. One can consider the analogous problem of whether $\mathcal{O}_N$ is free over $\mathfrak{A}_{N/M}$. Indeed, this is the case when N/M is unramified, tamely ramified or weakly ramified, or $M = \mathbb{Q}_p$ and $N/\mathbb{Q}_p$ is abelian or dihedral of order 2ℓ for some prime ℓ (see §2.3.1 for a detailed overview of such results). However, freeness in this situation does not relate to the aforementioned notion of local freeness in the way one might expect. More precisely, if $K/\mathbb{Q}$ is wildly ramified and non-abelian, p is a prime number, $\mathfrak{P}$ a prime of K above p, and $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$, then it is not necessarily the case that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at p (here $K_\mathfrak{P}$ denotes the completion of K at $\mathfrak{P}$). This is an important obstacle that needs to be overcome in the proofs of the main results of the present article.

We consider the question of whether $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ in the case that the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial and $\mathbb{Z}[G]$ has the so-called locally free cancellation property (in fact, the latter condition holds whenever the former holds). In this situation, it is also the case that $\mathrm{Cl}(\mathfrak{A}_{K/\mathbb{Q}})$ is trivial and $\mathfrak{A}_{K/\mathbb{Q}}$ has the locally free cancellation property. Hence it is straightforward to show that the question reduces to whether $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.

We now briefly describe a straightforward application of this strategy. Suppose that G is dihedral of order $2p^n$ for some prime p and some positive integer n. In this situation, Keating [Kea74] gave sufficient conditions for $\mathrm{Cl}(\mathbb{Z}[G])$ to be trivial and Bergé [Ber79] gave necessary and sufficient conditions for $\mathcal{O}_K$ to be locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. As a consequence we obtain the following result.

Theorem 2.1.4. *Let n be a positive integer and let $p \geq 5$ be a regular prime number*

such that the class number of $\mathbb{Q}(\zeta_{p^n})^+$ *is* 1. *Let* $K/\mathbb{Q}$ *be a dihedral extension of degree* $2p^n$. *Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if the ramification index of* p *in* $K/\mathbb{Q}$ *is coprime to* p *or is a power of* p.

Here $\mathbb{Q}(\zeta_{p^n})^+$ denotes the maximal totally real subfield $\mathbb{Q}(\zeta_{p^n})$. Using the class number computations of Miller [Mil14] we obtain the following corollary.

Corollary 2.1.5. *Let* $K/\mathbb{Q}$ *be a dihedral extension of degree* $2p^n$ *where* (p, n) *is* $(5, 2)$, $(5, 3)$, $(7, 2)$ *or* $(11, 2)$. *Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if the ramification index of* p *in* $K/\mathbb{Q}$ *is coprime to* p *or is a power of* p.

Similar but more complicated results hold when $p = 2$ or 3 (see Theorem 2.5.2 for the full statement and proof).

If G is non-abelian and non-dihedral such that $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial, then a result of Endô and Hironaka [EH79] shows that G is isomorphic to A_4, S_4 or A_5; the converse was already shown by Reiner and Ullom [RU74]. The main results of the present chapter will be necessary and sufficient conditions for $\mathcal{O}_K$ to be free over $\mathfrak{A}_{K/\mathbb{Q}}$ when G is isomorphic to A_4, S_4 or A_5. The discussion above shows that the main work is in determining when $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. A key ingredient is the notion of hybrid p-adic group rings, introduced by Johnston and Nickel [JN16]; using this tool it is straightforward to show that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $p = 3$ when G is isomorphic to A_4 or S_4.

The statements of the following theorems will depend on certain primes of K having given decomposition or inertia subgroups up to conjugation. We remark that such properties will not depend on which prime of K we choose above a given prime number. For example, saying that a prime number p is tamely ramified will mean that some, and hence every, prime of K above p is (at most) tamely ramified in $K/\mathbb{Q}$. We shall henceforth abbreviate 'at most tamely ramified' to 'tamely ramified'.

The following result is Theorem 2.8.1.

Theorem 2.1.6. *Let* $K/\mathbb{Q}$ *be a Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$. *Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if* 2 *is tamely ramified or has full decomposition group.*

The proof of the 'if' direction of this result involves the aforementioned tools. To prove the converse, we show that if 2 is wildly ramified and has decomposition group of order 2 or 4 then $\mathcal{O}_K$ is not locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $p = 2$. This reduces to showing that the lattice $\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} := \mathbb{Z}_2[G] \otimes_{\mathbb{Z}_2[D]} \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$, where $\mathfrak{P}$ is a fixed prime above 2 and D is its decomposition group. The main theorem used here is Hattori's result [Hat65] that commutative orders are 'clean' (see §2.6.2).

The following two results are Theorem 2.8.3 and Theorem 2.8.6, respectively.

Theorem 2.1.7. *Let* $K/\mathbb{Q}$ *be a Galois extension with* $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$. *Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if one of the following conditions on* $K/\mathbb{Q}$ *holds:*

(i) 2 *is tamely ramified;*

(ii) 2 *has decomposition group equal to the unique subgroup of* G *of order* 12*;*

(iii) 2 *is wildly and weakly ramified and has full decomposition group; or*

(iv) 2 *is wildly and weakly ramified, has decomposition group of order* 8 *in* G*, and has inertia subgroup equal to the unique normal subgroup of order* 4 *in* G*.*

Theorem 2.1.8. *Let* $K/\mathbb{Q}$ *be a Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$*. Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if all three of the following conditions on* $K/\mathbb{Q}$ *hold:*

(i) 2 *is tamely ramified;*

(ii) 3 *is tamely ramified or is weakly ramified with ramification index* 6*; and*

(iii) 5 *is tamely ramified or is weakly ramified with ramification index* 10*.*

In contrast to the proof of Theorem 2.1.6, the proofs of Theorems 2.1.7 and 2.1.8 use the (updated) implementation in Magma [BCP97] of the algorithms developed by Bley and Johnston [BJ08] and by Hofmann and Johnston [HJ20].

Notation and conventions

Let K be a number field. By a prime of K, we mean a non-zero prime ideal of $\mathcal{O}_K$. If $\mathfrak{P}$ is a prime of K, we let $K_{\mathfrak{P}}$ denote the completion of K at $\mathfrak{P}$. We say that a prime is tamely ramified if it is at most tamely ramified.

Let H be a subgroup of a finite group G. We denote by $\mathrm{ncl}_G(H)$ the normal closure of H in G, defined as the smallest normal subgroup of G containing H or, equivalently, the subgroup generated by all the conjugates of H in G.

2.2 Associated orders and reduction to the study of local freeness

2.2.1 Lattices and orders

For further background, we refer the reader to [Rei03] or [CR81]. Let R be a Dedekind domain with field of fractions F. An R-lattice M is a finitely generated torsion-free R-module, or equivalently, a finitely generated projective R-module. Note that any R-submodule of an R-lattice is again an R-lattice. For any finite-dimensional F-vector space V, an R-lattice in V is a finitely generated R-submodule M in V. We define a F-vector subspace of V by

$$FM := \{\alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_r m_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in F, m_i \in M\}$$

and say that M is a full R-lattice in V if $FM = V$. We may identify FM with $F \otimes_R M$.

Let A be a finite-dimensional F-algebra. An R-order in A is a subring Λ of A (so in particular has the same unity element as A) such that Λ is a full R-lattice in A. A Λ-lattice is a Λ-module which is also an R-lattice. For Λ-lattices M and N, a homomorphism of Λ-modules $f : M \to N$ is called a homomorphism of Λ-lattices.

The following well-known lemma follows from [CR81, Exercise 23.2].

Lemma 2.2.1. *Let* $\Lambda \subseteq \Gamma$ *be two* R*-orders in* A*. Let* M *and* N *be* Γ*-lattices and let* $f : M \to N$ *be a homomorphism of* Λ*-lattices. Then* f *is a homomorphism of* Γ*-lattices.*

2.2.2 Associated orders

Let Λ be an R-order in a finite-dimensional F-algebra A. Let M be a full R-lattice in a free A-module of rank 1 (thus $FM \cong A$ as A-modules). The *associated order* of M is defined to be

$$\mathfrak{A}(A, M) = \{\lambda \in A : \lambda M \subseteq M\}.$$

Note that $\mathfrak{A}(A, M)$ is an R-order (see [Rei03, §8]). In particular, it is the largest order Λ over which M has a structure of Λ-module. The following well-known result says that $\mathfrak{A}(A, M)$ is the only R-order in A over which M can possibly be free.

Proposition 2.2.2. *Let Λ be an R-order in A and let M be a free Λ-lattice of rank 1. Then FM is a free A-module of rank 1 and $\Lambda = \mathfrak{A}(A, M)$.*

Proof. By hypothesis there exists $\alpha \in M$ such that $M = \Lambda\alpha$ is a free Λ-module. Thus $FM = A\alpha$ is free over A. Let $x \in \mathfrak{A}(A, M)$. Then $x\alpha \in M = \Lambda\alpha$, so $x\alpha = y\alpha$ for some $y \in \Lambda$. Since FM is freely generated by α, we must have $x = y$. Hence $\mathfrak{A}(A, M) \subseteq \Lambda$. The reverse inclusion is trivial and therefore $\Lambda = \mathfrak{A}(A, M)$. □

Remark 2.2.3. Suppose Λ is an R-order in A. Then clearly $\Lambda \subseteq \mathfrak{A}(A, \Lambda)$. Moreover, $\mathfrak{A}(A, \Lambda)1_A \subseteq \Lambda$ and so $\mathfrak{A}(A, \Lambda) \subseteq \Lambda$. Therefore $\mathfrak{A}(A, \Lambda) = \Lambda$.

2.2.3 Completion and local freeness

Let $\mathfrak{p}$ be any maximal ideal of R. Let $F_\mathfrak{p}$ denote the completion of F with respect to a valuation defined by $\mathfrak{p}$ and let $R_\mathfrak{p}$ be the corresponding valuation ring. For any R-module M we write $M_\mathfrak{p}$ for $R_\mathfrak{p} \otimes_R M$ and $V_\mathfrak{p} = F_\mathfrak{p} \otimes_F V$ for any F-vector space V. These two notations are consistent as the map $\lambda \otimes_{\mathcal{O}_F} v \mapsto \lambda \otimes_F v$ ($v \in V$, $\lambda \in \mathcal{O}_{F_\mathfrak{p}}$) is an isomorphism (see [FT93, p. 93]).

Let Λ be an R-order and let M be a Λ-lattice in some A-module V. Then $\Lambda_\mathfrak{p}$ is an $R_\mathfrak{p}$-order in $A_\mathfrak{p}$ and $M_\mathfrak{p}$ is a $\Lambda_\mathfrak{p}$-lattice in $V_\mathfrak{p}$. We say that M is *locally free* over Λ if $M_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$ for every $\mathfrak{p}$.

Let G be a finite group and let M be a full $R[G]$-lattice in a free A-module of rank 1. Then $R[G] \subseteq \mathfrak{A}(F[G], M)$ and $R_\mathfrak{p}[G] \subseteq \mathfrak{A}(F_\mathfrak{p}[G], M_\mathfrak{p}) \cong \mathfrak{A}(F[G], M)_\mathfrak{p}$. Moreover, M is locally free over $\mathfrak{A}(F[G], M)$ if $M_\mathfrak{p}$ is free over $\mathfrak{A}(F_\mathfrak{p}[G], M_\mathfrak{p})$ for every $\mathfrak{p}$.

2.2.4 Associated orders of rings of integers

Let K/F be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/F)$. We consider the behaviour of the associated order $\mathfrak{A}_{K/F} := \mathfrak{A}(F[G], \mathcal{O}_K)$ with respect to localisation and induction.

Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$. Then we have decompositions

$$K_\mathfrak{p} := F_\mathfrak{p} \otimes_F K \cong \prod_{\mathfrak{P}'|\mathfrak{p}} K_{\mathfrak{P}'} \quad \text{and} \quad \mathcal{O}_{K,\mathfrak{p}} := \mathcal{O}_{F_\mathfrak{p}} \otimes_{\mathcal{O}_F} \mathcal{O}_K \cong \prod_{\mathfrak{P}'|\mathfrak{p}} \mathcal{O}_{K_{\mathfrak{P}'}},$$

where $\{\mathfrak{P}' \mid \mathfrak{p}\}$ consists of the primes of $\mathcal{O}_K$ above $\mathfrak{p}$ (see [FT93, p. 109]). Fix a prime $\mathfrak{P}$ above $\mathfrak{p}$ and let D be its decomposition group in G. Then as G acts transitively on

$\{\mathfrak{P}' \mid \mathfrak{p}\}$ we have

$$K_{\mathfrak{p}} \cong \prod_{s \in G/D} sK_{\mathfrak{P}} \quad \text{and} \quad \mathcal{O}_{K,\mathfrak{p}} \cong \prod_{s \in G/D} s\mathcal{O}_{K_{\mathfrak{P}}},$$

where the products run over a system of representatives of the left cosets G/D. Hence

$$\mathcal{O}_{K,\mathfrak{p}} \cong \mathrm{Ind}_D^G \mathcal{O}_{K_{\mathfrak{P}}} := \mathcal{O}_{F_{\mathfrak{p}}}[G] \otimes_{\mathcal{O}_{F_{\mathfrak{p}}}[D]} \mathcal{O}_{K_{\mathfrak{P}}},$$

and

$$\mathfrak{A}_{K/F,\mathfrak{p}} = \mathfrak{A}(F[G], \mathcal{O}_K)_{\mathfrak{p}} \cong \mathfrak{A}(F_{\mathfrak{p}}[G], \mathrm{Ind}_D^G \mathcal{O}_{K_{\mathfrak{P}}}),$$

where the last isomorphism follows from [CR81, Exercise 24.2], for instance. Thus $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/F}$ at $\mathfrak{p}$ if and only if $\mathrm{Ind}_D^G \mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}(F_{\mathfrak{p}}[G], \mathrm{Ind}_D^G \mathcal{O}_{K_{\mathfrak{P}}})$.

In §2.6 we will consider the relationship between $\mathfrak{A}(F_{\mathfrak{p}}[G], \mathrm{Ind}_D^G \mathcal{O}_{K_{\mathfrak{P}}})$ and $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}$, as well as conditions under which the implication 'if $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}$ then $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/F}$ at $\mathfrak{p}$' holds.

Notation

We henceforth consider the isomorphism $\mathfrak{A}_{K/F,\mathfrak{p}} \cong \mathfrak{A}(F_{\mathfrak{p}}[G], \mathcal{O}_{K,\mathfrak{p}})$ as an identification. In particular, we consider $\mathfrak{A}_{K/F,\mathfrak{p}}$ as an $\mathcal{O}_{F,\mathfrak{p}}$-order in $F_{\mathfrak{p}}[G]$.

2.2.5 Reduction to the study of local freeness

Definition 2.2.4. Let R be a Dedekind domain with quotient F and let Λ be an R-order. The *locally free class group* $\mathrm{Cl}(\Lambda)$ is the abelian group generated by the symbols $[M]$, where M is a locally free Λ-lattice, modulo the relations coming from *stable isomorphism*: two Λ-lattices M and N are stably isomorphic if there exist non-negative integers r and s such that

$$M \oplus \Lambda^r \cong N \oplus \Lambda^s.$$

Sum is given by direct sum of lattices.

Remark 2.2.5. The locally free class group $\mathrm{Cl}(\Lambda)$ always has finite order by the Jordan-Zassenhaus Theorem [CR81, Theorem (24.1)]. Moreover, as representatives for $\mathrm{Cl}(\Lambda)$ we can consider locally free Λ-lattices of rank 1 by [CR81, Corollary (31.7)] (see also the beginning of [CR87, §49]). We have that $\mathrm{Cl}(\Lambda)$ is naturally a subgroup of $K_0(\Lambda)$, see for instance [CR87, Definition (39.12)] and [CR87, (39.13)] (for an introduction to K-theory see §4.3). Further background material can be found in [CR87, §49].

The following proposition underpins the proofs of all the new theorems stated in the introduction.

Proposition 2.2.6. *Let G be a finite group such that $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial and let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Proof. One implication is trivial. By [CR87, (49.25)] the inclusion $\mathbb{Z}[G] \subseteq \mathfrak{A}_{K/\mathbb{Q}}$ induces a surjection $\mathrm{Cl}(\mathbb{Z}[G]) \twoheadrightarrow \mathrm{Cl}(\mathfrak{A}_{K/\mathbb{Q}})$, and so $\mathrm{Cl}(\mathfrak{A}_{K/\mathbb{Q}})$ is also trivial. Moreover, by [EH79] the triviality of $\mathrm{Cl}(\mathbb{Z}[G])$ implies that G must be abelian, dihedral, or isomorphic to A_4, S_4 or A_5 (see also [CR87, (50.29)]). In each of these cases, $\mathbb{Q}[G]$ is isomorphic to a finite direct product of matrix rings over number fields. Hence by [CR87, (51.2)] $\mathbb{Q}[G]$ satisfies the Eichler condition (see [CR87, (45.4) or §51A]). Thus the Jacobinski cancellation theorem [Jac68] (see also [CR87, (51.24)]) implies that $\mathfrak{A}_{K/\mathbb{Q}}$ has the locally free cancellation property. The non-trivial implication now follows easily. □

Corollary 2.2.7. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4, S_4$ or A_5. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. In each case $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial, as shown in [RU74]. □

2.3 Review of results relating to local freeness

2.3.1 Freeness results for Galois extensions of p-adic fields

Many of the results and definitions of this subsection also hold for local fields of positive characteristic, but for simplicity we restrict to the case of p-adic fields. We fix a prime number p.

Theorem 2.3.1. *Let K/F be a tamely ramified finite Galois extension of p-adic fields and let $G = \mathrm{Gal}(K/F)$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F} = \mathcal{O}_F[G]$.*

Remark 2.3.2. Theorem 2.3.1 is usually attributed to Emmy Noether [Noe32]. In fact, as noted in [Cha96], she only stated and proved the result in the case that $p \nmid |G|$. Complete proofs can be found in [Frö83], [Kaw86] and [Cha96].

Theorem 2.3.3. *[Let98] Let K/F be an extension of p-adic fields such that $K/\mathbb{Q}_p$ is a finite abelian extension. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F}$.*

Theorem 2.3.4. *[Ber72] Let $K/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong D_{2\ell}$, where ℓ is a prime number. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}_p}$.*

Theorem 2.3.5. *[Mar72] Let $K/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong Q_8$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}_p}$.*

Remark 2.3.6. Theorem 2.3.5 is not explicitly stated in [Mar72]. However, the proof of Theorem 2.1.3 given in loc. cit. also works essentially unchanged in the setting of Theorem 2.3.5. Alternatively, note that Theorem 2.3.5 is implied by Theorem 2.1.3 because for every Q_8-extension $L/\mathbb{Q}_2$ there exists a Q_8-extension $K/\mathbb{Q}$ such that $K_{\mathfrak{P}} = L$, where $\mathfrak{P}$ is the unique prime of K above 2; this can be checked using databases of p-adic and number fields such as [JR06] and [LMF19]. Note that unlike Theorem 2.1.3, it is not necessary to assume that the extension in question is wildly ramified, thanks to Theorem 2.3.1.

Theorem 2.3.7. *[Jau81] Let p, n and r be positive integers such that p is an odd prime, n divides $p-1$ and r is a primitive nth root modulo p. Let G be the metacyclic group*

with the following structure:

$$G = \langle x, y : x^p = 1, y^n = 1, yxy^{-1} = x^r \rangle \cong C_p \rtimes C_n. \tag{2.3.1}$$

Let $K/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}_p}$.

Remark 2.3.8. In the special case $n = 2$, the group G of (2.3.1) is dihedral of order $2p$.

Let K/F be a Galois extension of p-adic fields and let $G = \mathrm{Gal}(K/F)$. We recall that for an integer $t \geq -1$ the t-th ramification group is defined to be

$$G_t := \{\sigma \in G : v_K(\sigma(x) - x) \geq t + 1 \ \forall x \in \mathcal{O}_K\},$$

where v_K is the normalized valuation on K (i.e. with image $\mathbb{Z}$). When it is not obvious which extension we are referring to we will use the notation '$G_t(K/F)$' or similar. Thus K/F is unramified if and only if G_0 is trivial and is tamely ramified if and only if G_1 is trivial. We say that the extension is weakly ramified if G_2 is trivial.

Theorem 2.3.9. *[Joh15] Let K/F be a weakly ramified finite Galois extension of p-adic fields and let $G = \mathrm{Gal}(K/F)$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F}$. Moreover, if K/F is both wildly and weakly ramified then $\mathfrak{A}_{K/F} = \mathcal{O}_F[G][\pi_F^{-1}\mathrm{Tr}_{G_0}]$ (that is, the $\mathcal{O}_F[G]$-algebra generated by $\pi_F^{-1}\mathrm{Tr}_{G_0}$, which is an $\mathcal{O}_F$-order), where π_F is a uniformiser of $\mathcal{O}_F$ and $\mathrm{Tr}_{G_0} = \sum_{\gamma \in G_0} \gamma$ is the sum of the elements of the inertia group G_0.*

For a subgroup H of G define $\mathrm{Tr}_H = \sum_{h \in H} h \in F[G]$ and $e_H = \frac{1}{|H|}\mathrm{Tr}_H \in F[G]$. Note that e_H is an idempotent. We say that K/F is almost-maximally ramified if $e_H \in \mathfrak{A}_{K/F}$ for every subgroup H of G such that $G_{t+1} \subseteq H \subseteq G_t$ for some $t \geq 1$.

Theorem 2.3.10. *[Ber79, Proposition 7] Let K/F be a finite dihedral extension of p-adic fields such that $F/\mathbb{Q}_p$ is unramified. Let $G = \mathrm{Gal}(K/F)$. Then $\mathcal{O}_K$ is projective over $\mathfrak{A}_{K/F}$ if and only if $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F}$ if and only if either*

(i) K/F is almost-maximally ramified, in which case $\mathfrak{A}_{K/F} = \mathcal{O}_F[G][\{e_{G_t}\}_{t \geq 1}]$, or

(ii) K/F is not almost-maximally ramified, and the inertia subgroup G_0 is dihedral of order $2p$, in which case $\mathfrak{A}_{K/F} = \mathcal{O}_F[G][2e_{G_0}]$.

Remark 2.3.11. Throughout this chapter, and in particular Theorem 2.3.10, the group $C_2 \times C_2$ is considered to be dihedral of order $2 \cdot 2$.

Remark 2.3.12. Let H be a subgroup of G and let r be a positive integer. We now show how to determine whether $\frac{1}{r}\mathrm{Tr}_H \in \mathfrak{A}_{K/F}$. For example, when $r = |H|$ this can be used to check for almost-maximal ramification. Let M be the subfield of K fixed by H. We denote by $\mathfrak{D}_{K/M}$ the different of the extension K/M (see [Ser79, III§3]) and by $v_p(x)$

the p-adic valuation of an integer x (thus v_p is the restriction of $v_{\mathbb{Q}_p}$ to $\mathbb{Z}$).

$$\begin{aligned}
\frac{1}{r}\mathrm{Tr}_H \in \mathfrak{A}_{K/F} &\iff \frac{1}{r}\mathrm{Tr}_{K/M}(\mathcal{O}_K) \subseteq \mathcal{O}_M \\
&\iff \mathrm{Tr}_{K/M}(\mathcal{O}_K) \subseteq r\mathcal{O}_M \\
&\iff \mathcal{O}_K \subseteq r\mathcal{O}_M\mathfrak{D}_{K/M}^{-1} \text{ by [Ser79, III Proposition 7]} \\
&\iff \mathfrak{D}_{K/M} \subseteq r\mathcal{O}_K \\
&\iff v_K(\mathfrak{D}_{K/M}) \geq e(K/\mathbb{Q}_p)v_p(r) \\
&\iff \sum_{i=0}^{\infty}(|G_i(K/M)| - 1) \geq e(K/\mathbb{Q}_p)v_p(r) \text{ by [Ser79, IV Proposition 4].}
\end{aligned}$$

Remark 2.3.13. From Theorem 2.3.4, Theorem 2.3.10 and Remark 2.3.12 (see also [Ber78, Corollaire to Proposition 3]) we deduce that a dihedral extension $K/\mathbb{Q}_p$ of degree $2p$ is either almost-maximally ramified or is weakly and totally ramified.

2.3.2 Local freeness results for Galois extensions of number fields

Remark 2.3.14. Let K/F be a finite Galois extension of number fields. If $\mathcal{O}_K$ is free over $\mathfrak{A}_{F/K}$ then it is clear that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{F/K}$. In particular, the analogues of Theorems 2.1.1, 2.1.2 and 2.1.3 all hold, with 'locally free' in place of 'free'. Theorems 2.3.16 and 2.3.18 below are generalisations of the first two of these analogues.

Theorem 2.3.15. *Let K/F be a finite Galois extension of number fields. Let $G = \mathrm{Gal}(K/F)$ and let $\mathfrak{p}$ be a prime of F that is tamely ramified in K/F. Then $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}} = \mathcal{O}_{F_\mathfrak{p}}[G]$.*

Theorem 2.3.16. *[Let98] Let K/F be an extension of number fields such that $K/\mathbb{Q}$ is a finite abelian extension. Then $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/F}$.*

Remark 2.3.17. Theorems 2.3.15 and 2.3.16 are well-known consequences of Theorems 2.3.1 and 2.3.3, respectively. See Remark 2.6.4 and Corollary 2.6.7, for instance.

Theorem 2.3.18. *[Jau81] Let $K/\mathbb{Q}$ be a Galois extension such that $\mathrm{Gal}(K/\mathbb{Q})$ is meta-cyclic of type (2.3.1). Then $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Theorem 2.3.19. *[Ber79, Théorème] Let $K/\mathbb{Q}$ be a finite dihedral extension and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let p be an odd prime number that is wildly ramified in $K/\mathbb{Q}$ and let N be the unique cyclic subgroup of G of index 2. Then $\mathcal{O}_{K,p}$ is projective over $\mathfrak{A}_{K/\mathbb{Q},p}$ if and only if $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ if and only if one of the following conditions holds:*

(i) p is almost-maximally ramified in $K/\mathbb{Q}$, in which case

$$\mathfrak{A}_{K/\mathbb{Q},p} = \mathbb{Z}_p[G][\{e_{G_t}\}_{t\geq 1}], \text{ or}$$

(ii) p is not almost-maximally ramified, $|G_0| = 2p$ and $[G : G_0] \mid 2$, in which case

$$\mathfrak{A}_{K/\mathbb{Q},p} = \mathbb{Z}_p[G][e_{G_0}].$$

Remark 2.3.20. In fact, Theorem 2.3.19 is [Ber79, Théorème] specialised to the case that p is odd and the base field is $\mathbb{Q}$; the more general statement is somewhat more complicated.

2.4 Hybrid group rings and applications to local freeness

2.4.1 Hybrid group rings

Let R be a discrete valuation ring with fraction field F and let G be a finite group. Let M be a full $R[G]$-lattice in $F[G]$. Note that $R[G] \subseteq \mathfrak{A}(F[G], M)$.

For a normal subgroup N of G define $e_N = \frac{1}{|N|}\sum_{n\in N} n \in F[G]$ to be the central idempotent associated to N.

Proposition 2.4.1. *If N is a normal subgroup of G such that $|N| \in R^\times$ then*

(i) $R[G] = e_N R[G] \times (1 - e_N)R[G] \cong R[G/N] \times (1 - e_N)R[G]$,

(ii) $e_N M$ *has the structure of a* $e_N R[G] \cong R[G/N]$*-lattice, and*

(iii) $e_N\mathfrak{A}(F[G], M) = \mathfrak{A}(F[G], M) \cap e_N F[G] = \mathfrak{A}(e_N F[G], e_N M) \cong \mathfrak{A}(F[G/N], e_N M)$.

Proof. Since $|N| \in R^\times$ we have $e_N \in R[G]$. Moreover, it is straightforward to show that $e_N R[G] \cong R[G/N]$. Thus we have established (i) and (ii), and it remains to prove (iii).

The last isomorphism of (iii) is immediate from (ii). We now prove the first equality, that is, $e_N\mathfrak{A}(F[G], M) = \mathfrak{A}(F[G], M) \cap e_N F[G]$. Since $e_N \in R[G] \subseteq \mathfrak{A}(F[G], M)$, we easily have that $e_N\mathfrak{A}(F[G], M) \subseteq \mathfrak{A}(F[G], M) \cap e_N F[G]$. The other containment follows from the fact that $e_N^2 = e_N$, hence any element in $\mathfrak{A}(F[G], M) \cap e_N F[G]$, with the harmless multiplication by e_N, can be written as an element in $e_N\mathfrak{A}(F[G], M)$.

We now prove that $\mathfrak{A}(F[G], M) \cap e_N F[G] = \mathfrak{A}(e_N F[G], e_N M)$. Consider

$$e_N x \in \mathfrak{A}(F[G], M) \cap e_N F[G]$$

for a certain $x \in F[G]$; we have to prove that $e_N x$ preserves $e_N M$. Since $e_N M \subseteq M$ and $e_N x \in \mathfrak{A}(F[G], M)$, we have that $e_N x e_N M \subseteq M$. Hence $e_N x e_N M = e_N e_N x e_N M \subseteq e_N M$. Conversely, let us consider an element $e_N x \in \mathfrak{A}(e_N F[G], e_N M)$, thus such that $e_N x e_N M \subseteq e_N M$. We must prove that $e_N x \in \mathfrak{A}(F[G], M)$, which is automatic since $e_N x M = e_N e_N x M = e_N x e_N M \subseteq e_N M \subseteq M$. □

We now recall the notion of hybrid group ring introduced in [JN16, §2] and further developed in [JN18, §2].

Definition 2.4.2. Let N be a normal subgroup of G. We say that $R[G]$ is N-hybrid if $|N| \in R^\times$ and $(1 - e_N)R[G]$ is a maximal R-order in $(1 - e_N)F[G]$.

Remark 2.4.3. The group ring $R[G]$ is a maximal R-order if and only if $|G| \in R^\times$ if and only if $R[G]$ is G-hybrid, where the first equivalence is given by [CR81, (27.1)]. In this situation, $\mathfrak{A}(F[G], M) = R[G]$ and thus M is free over $\mathfrak{A}(F[G], M)$ by [Rei03, (18.10)].

Example 2.4.4. Let $G = A_4$ or S_4 and let N be its unique normal subgroup of order 4. Then $\mathbb{Z}_3[G]$ is N-hybrid as shown in [JN16, Examples 2.16 and 2.18]. Indeed, we have

$$\mathbb{Z}_3[A_4] \cong \mathbb{Z}_3[C_3] \times M_{3\times 3}(\mathbb{Z}_3) \quad \text{and} \quad \mathbb{Z}_3[S_4] \cong \mathbb{Z}_3[S_3] \times M_{3\times 3}(\mathbb{Z}_3) \times M_{3\times 3}(\mathbb{Z}_3),$$

where $M_{3\times 3}(\mathbb{Z}_p)$ is a maximal $\mathbb{Z}_p$-order by [Rei03, (8.7)].

Example 2.4.5. Let n be an odd positive integer and let N_n be the unique subgroup of index 2 in D_{2n}. Then $\mathbb{Z}_2[D_{2n}]$ is N_n-hybrid as shown in [JN16, Example 2.14].

Proposition 2.4.6. *Suppose $R[G]$ is N-hybrid. Then*

$$\mathfrak{A}(F[G], M) = e_N\mathfrak{A}(F[G], M) \times (1 - e_N)R[G] \cong \mathfrak{A}(F[G/N], e_N M) \times (1 - e_N)R[G].$$

Moreover, M is free over $\mathfrak{A}(F[G], M)$ if and only if $e_N M$ is free over $\mathfrak{A}(F[G/N], e_N M)$.

Proof. The first claim follows from Proposition 2.4.1, Definition 2.4.2, and the fact that $R[G] \subseteq \mathfrak{A}(F[G], M)$. Since $(1 - e_N)R[G]$ is a maximal R-order, $(1 - e_N)M$ is free over $(1-e_N)R[G]$ by [Rei03, (18.10)]. The second claim now follows from the decomposition $M \cong e_N M \oplus (1 - e_N)M$. □

2.4.2 Applications to local freeness for extensions of number fields

Proposition 2.4.7. *Let K/F be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/F)$. Let p be a prime number and let $\mathfrak{p}$ be a prime of F above p. Let N be a normal subgroup of G such that $p \nmid |N|$ and let M be the subfield of K fixed by N. Then we have an identification $e_N\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{M,\mathfrak{p}}$. Moreover, via this identification, the structure of $e_N\mathcal{O}_{K,\mathfrak{p}}$ as an $e_N\mathcal{O}_{F_\mathfrak{p}}[G]$-module coincides with the structure of $\mathcal{O}_{M,\mathfrak{p}}$ as an $\mathcal{O}_{F_\mathfrak{p}}[G/N]$-module under the canonical identification $G/N \cong \mathrm{Gal}(M/F)$. In particular,*

$$e_N\mathfrak{A}(F_\mathfrak{p}[G], \mathcal{O}_{K,\mathfrak{p}}) = \mathfrak{A}(F_\mathfrak{p}[G], \mathcal{O}_{K,\mathfrak{p}}) \cap e_N F[G] \cong \mathfrak{A}(F_\mathfrak{p}[G/N], \mathcal{O}_{M,\mathfrak{p}}).$$

Now further suppose that $\mathcal{O}_{F_\mathfrak{p}}[G]$ is N-hybrid. Then

$$\mathfrak{A}_{K/F,\mathfrak{p}} \cong \mathfrak{A}_{M/F,\mathfrak{p}} \times (1 - e_N)\mathcal{O}_{F_\mathfrak{p}}[G],$$

and $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}}$ if and only if $\mathcal{O}_{M,\mathfrak{p}}$ is free over $\mathfrak{A}_{M/F,\mathfrak{p}}$.

Proof. The claims regarding the identifications are clear. The remaining claims are then specialisations of Propositions 2.4.1 and 2.4.6. □

Corollary 2.4.8. *Let $K/\mathbb{Q}$ be a finite Galois extension and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let N be a normal subgroup of G and such that G/N is abelian or metacyclic of type (2.3.1). Let p be a prime number. If $\mathbb{Z}_p[G]$ is N-hybrid, then $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$.*

Proof. Let M be the subfield of K fixed by N. Then $\mathcal{O}_{M,p}$ is free over $\mathfrak{A}_{M/\mathbb{Q},p}$ by Theorem 2.1.1 or Theorem 2.3.18. The result now follows from Proposition 2.4.7. □

Remark 2.4.9. Jaulent [Jau81] developed similar arguments to Corollary 2.4.8, but restricted to the case that G is metacyclic of type (2.3.1).

2.4.3 Preliminary results on A_4 and S_4-extensions of $\mathbb{Q}$

Proposition 2.4.10. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$ or S_4. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$.*

Proof. By Corollary 2.2.7, it suffices to show that $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ for each prime number $p \geq 3$. For $p \geq 5$ this follows from Theorem 2.3.15. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let N be its unique normal subgroup of order 4. By Example 2.4.4 the group ring $\mathbb{Z}_3[G]$ is N-hybrid. Moreover, $G/N \cong C_3$ or S_3 (note that $S_3 \cong D_6$ is metacyclic of type (2.3.1)). Thus by Corollary 2.4.8 we have that $\mathcal{O}_{K,3}$ is free over $\mathfrak{A}_{K/\mathbb{Q},3}$. □

Lemma 2.4.11. *There is a unique Galois extension $L/\mathbb{Q}_2$ with $\mathrm{Gal}(L/\mathbb{Q}_2) \cong A_4$. Moreover, this extension is wildly and weakly ramified, and the inertia subgroup is equal to the unique (normal) subgroup of order 4.*

Proof. This can easily be checked by, for instance, using the database of p-adic fields [JR06] (which is now accessible via the database [LMF19]). Indeed, L is the Galois closure of the extension of $\mathbb{Q}_2$ generated by the polynomial $x^4 + 2x^3 + 2x^2 + 2$. □

Proposition 2.4.12. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$. If 2 is either tamely ramified in $K/\mathbb{Q}$ or has full decomposition group in $\mathrm{Gal}(K/\mathbb{Q})$, then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Proof. By Proposition 2.4.10, it suffices to show that $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$. If 2 is tamely ramified in $K/\mathbb{Q}$ then this follows from Theorem 2.3.15. Now suppose that 2 has full decomposition group in $G := \mathrm{Gal}(K/\mathbb{Q})$. Then 2 is weakly ramified in $K/\mathbb{Q}$ by Lemma 2.4.11. Let $\mathfrak{P}$ be the unique prime of K above 2. Then

$$\mathcal{O}_{K,2} \cong \mathrm{Ind}_G^G \mathcal{O}_{K_\mathfrak{P}} = \mathcal{O}_{K_\mathfrak{P}} \quad \text{and} \quad \mathfrak{A}_{K/\mathbb{Q},2} \cong \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2},$$

so the result now follows from Theorem 2.3.9. □

2.5 Leopoldt-type theorems for certain dihedral extensions of $\mathbb{Q}$

We first recall the following theorem of Bergé stated the introduction to this chapter.

Theorem 2.5.1. *[Ber72] Let p be a prime number and let $K/\mathbb{Q}$ be a dihedral extension of degree $2p$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

In the following theorem and corollaries, we consider other dihedral extensions of $\mathbb{Q}$. For a positive integer m, let $\mathbb{Q}(\zeta_m)^+$ denote the maximal totally real subfield of the mth cyclotomic field $\mathbb{Q}(\zeta_m)$. If m is odd then $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$ and so $\mathbb{Q}(\zeta_{2m})^+ = \mathbb{Q}(\zeta_m)^+$. We recall that we abbreviate 'at most tamely ramified' to 'tamely ramified'.

Theorem 2.5.2. *Let p be a prime and let $n \geq 2$ be an integer. Let $K/\mathbb{Q}$ be a dihedral extension of degree $2p^n$. Suppose that p is a regular prime such that the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ is 1. Consider the following assertions:*

(i) $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$*;*

(ii) $\mathcal{O}_K$ *is locally free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *at* p*;*

(iii) p *is tamely ramified or almost-maximally ramified in the extension* $K/\mathbb{Q}$*;*

(iv) the ramification index of p *in* $K/\mathbb{Q}$ *is coprime to* p *or is a power of* p*.*

Then we have the following conclusions:

(a) (i) *and* (ii) *are equivalent;*

(b) *if* p *is odd, then* (i), (ii) *and* (iii) *are equivalent;*

(c) *if* p *is odd, then* (iv) *implies* (i), (ii) *and* (iii)*;*

(d) *if* $p \geq 5$*, then* (i), (ii), (iii) *and* (iv) *are equivalent.*

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By [Was97, Theorem 10.1] the condition on the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ implies that the class number of $\mathbb{Q}(\zeta_{2p^d})^+$ is 1 for every $d \leq n$. This together with the regularity of p implies that the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial: if p is odd this follows from a special case of the main result of [Kea74, Theorem 1] (see also [CR87, (50.28)]), if $p = 2$ this follows from the results of [FKW74] (see also [CR87, (50.31)] and [CR81, (7.39)]). Therefore $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ by Proposition 2.2.6. Note that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at ℓ for every prime number $\ell \neq 2, p$ by Theorem 2.3.15. Moreover, if p is odd then Example 2.4.5 implies that $\mathbb{Z}_2[G]$ is N-hybrid where N is the unique subgroup of G of index 2, and so $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $\ell = 2$ by Corollary 2.4.8. Thus we have proved claim (a).

Claim (b) now follows from Theorem 2.3.15 and Theorem 2.3.19 (note that case (ii) of Theorem 2.3.19 cannot occur when p is odd and $n \geq 2$). Finally, claims (c) and (d) follow from the definition of tame ramification and the characterization of almost-maximal ramification in dihedral extensions given in [Ber79, Corollaire to Proposition 6]. □

Remark 2.5.3. Let p be a prime and let n be a positive integer. It is well known that p is regular if $p < 37$. Moreover, by the results of [Mil14] the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ is 1 whenever (p, n) is $(2, 6)$, $(3, 4)$, $(5, 3)$, $(7, 2)$, $(11, 2)$, or the same pairs with a smaller choice of $n \geq 2$. Hence the hypotheses of Theorem 2.5.2 hold for these values. In particular, we obtain the following corollaries.

Corollary 2.5.4. *Let* $K/\mathbb{Q}$ *be a dihedral extension of degree* $2 \cdot 3^n$ *where* $n = 2, 3$ *or* 4*. If the ramification index of* 3 *in* $K/\mathbb{Q}$ *is coprime to* 3 *or is a power of* 3 *then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$*.*

Corollary 2.5.5. *Let* $K/\mathbb{Q}$ *be a dihedral extension of degree* $2p^n$ *where* (p, n) *is* $(5, 2)$*,* $(5, 3)$*,* $(7, 2)$ *or* $(11, 2)$*. Then* $\mathcal{O}_K$ *is free over* $\mathfrak{A}_{K/\mathbb{Q}}$ *if and only if the ramification index of* p *in* $K/\mathbb{Q}$ *is coprime to* p *or is a power of* p*.*

Remark 2.5.6. In the proof of Theorem 2.5.2, we could have used [Ber79, Théorème] to establish local freeness at $\ell = 2$ instead of Example 2.4.5 and Corollary 2.4.8.

2.6 Review of results on induction of lattices and associated orders

In this section, we shall give an exposition of Bergé's results contained in [Ber79, §I]. We include some of the proofs for the convenience of the reader. The motivation for this section comes from §2.2.4.

2.6.1 Associated orders and induction

Let R be a Dedekind domain with field of fractions F. Let H be a subgroup of a finite group G and let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$.

We recall that $\mathrm{Ind}_H^G M$ is the induced module $R[G] \otimes_{R[H]} M \cong \bigoplus_{s \in G/H} sM$, where on the right hand side we choose a system of representatives in G of the left cosets G/H and the left $R[G]$-module structure is given by the relation $gs = th$ for some coset representative t and $h \in H$. We wish to understand the relationship between $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ and $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$. Note that these both contain the group ring $R[G]$.

Proposition 2.6.1. *[Ber79, §1.3] We have*

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = \bigcap_{g \in G} g \mathrm{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1}.$$

Proof. Let $x \in \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ and let $g \in G$. We will show that

$$x \in g \mathrm{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1}.$$

Consider a set of representatives $t \in G/H$ such that the identity element is among them. Then $g^{-1}xg \in F[G] = \bigoplus_{t \in G/H} tF[H]$, so that we can write $x = g \left(\sum_{t \in G/H} t a_t \right) g^{-1}$ with $a_t \in F[H]$ for every t. We are done if we show that $a_t \in \mathfrak{A}(F[H], M)$ for every $t \in G/H$. Consider the set of representatives $s = gt$ of G/H, where t runs through the original set of representatives of G/H. Then, as $x \mathrm{Ind}_H^G M \subseteq \mathrm{Ind}_H^G M$ and $\mathrm{Ind}_H^G M \cong \bigoplus_{s \in G/H} sM$, in particular $xsM \subseteq \mathrm{Ind}_H^G M$ for every s. Since the identity is among the representatives indexed by t, we can consider $s = g$ in the last containment. Therefore we obtain

$$xgM = \sum_{t \in G/H} g t a_t M \subseteq \bigoplus_{s \in G/H} sM = \bigoplus_{t \in G/H} gtM.$$

It follows that $a_t \in \mathfrak{A}(F[H], M)$ for every t.

Suppose conversely that $x \in \bigcap_{g \in G} g \mathrm{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1}$. Then, for every $g \in G$, we can write $x = g \left(\sum_{t \in G/H} t a_t \right) g^{-1}$ with $a_t \in \mathfrak{A}(F[H], M)$ for every t. Therefore $xgM \subseteq \bigoplus_{s \in G/H} sM$, which implies that $x \left(\bigoplus_{g \in G/H} gM \right) \subseteq \bigoplus_{s \in G/H} sM$ if we let the g's represent the cosets of G/H. Since $\mathrm{Ind}_H^G M = \bigoplus_{g \in G/H} gM = \bigoplus_{s \in G/H} sM$, this implies $x \in \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$. □

Remark 2.6.2. From the proof of Proposition 2.6.1 one can deduce that, instead of every $g \in G$, we could have taken any system of left coset representatives to index the intersection.

Corollary 2.6.3. $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring if and only if it is equal to* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$.

Proof. If $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring then $g\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)g^{-1} = \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ for all $g \in G$ and thus $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ by Proposition 2.6.1. Conversely, if $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ then the left hand side is a ring since the right hand side is an associated order and thus a ring. □

Remark 2.6.4. In general, $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ need not be a ring. However, it is straightforward to deduce from the above that $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring in the following cases:

(i) there exists a subgroup $K \leq G$ such that $G \cong H \times K$,

(ii) H is contained in the centre of G, or

(iii) $\mathfrak{A}(F[H], M) = R[H]$.

Remark 2.6.5. Proposition 2.6.1 implies that $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$. Hence $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is an $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattice.

Proposition 2.6.6. *If* M *is free over* $\mathfrak{A}(F[H], M)$ *then* $\mathrm{Ind}_H^G M \cong \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *as* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$*-lattices.*

Proof. Since $R[H] \subseteq \mathfrak{A}(F[H], M)$ and M is free (necessarily of rank 1) over $\mathfrak{A}(F[H], M)$, we see that M and $\mathfrak{A}(F[H], M)$ are isomorphic as $R[H]$-lattices. Extension of scalars gives an isomorphism $\mathrm{Ind}_H^G M \cong \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ of $R[G]$-lattices. By Lemma 2.2.1 this is also an isomorphism of $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattices. □

Corollary 2.6.7. *Suppose that* M *is free over* $\mathfrak{A}(F[H], M)$*. If*

(i) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is free over* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$*,*

(ii) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$*, or*

(iii) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring,*

then $\mathrm{Ind}_H^G M$ *is free over* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$*.*

Proof. In case (i) this follows immediately from Proposition 2.6.6. Clearly, (ii) $\Rightarrow$ (i). Moreover, (ii) $\Leftrightarrow$ (iii) by Corollary 2.6.3. □

We now give a partial converse to Corollary 2.6.7(i), for which we will need the following lemmas.

Lemma 2.6.8. *[Ber79, Lemme 1] Let* B *be a ring. A* B*-module* P *is projective if and only if there exists a family* $(x_i)_{i \in I}$ *of elements in* P *and a family* $(f_i)_{i \in I}$ *of* B*-homomorphisms from* P *to* B *such that, for every* $x \in P$*, one has* $x = \sum_{i \in I} f_i(x) x_i$*, where all but a finite number of* $f_i(x)$ *are zero.*

Proof. The condition is equivalent to the fact that there exists a split surjection of $\bigoplus_I B$ onto P, that is, P is a direct summand of a free module. This is equivalent to being projective. □

Lemma 2.6.9. *We have*

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \bigoplus_{t \in H\backslash G} \mathfrak{A}(F[H], M)t,$$

where t runs through a set of right coset representatives of $H \setminus G$.

Proof. We first note that the latter is in fact a direct sum, and that we have

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq F[G] = \bigoplus_{t \in H\backslash G} F[H]t.$$

Let us fix a coset representative $t' \in H \setminus G$. Then the associated order $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ sends $t'^{-1}M \subseteq \mathrm{Ind}_H^G M$ into $\mathrm{Ind}_H^G M = \bigoplus_{s \in G/H} sM$, where we choose the left representatives indexed by s in such a way that t'^{-1} is among them. We now show that the coefficient of t' in each element $x \in \mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \bigoplus_{t \in H\backslash G} F[H]t$ belongs to $\mathfrak{A}(F[H], M)$: in fact, we can write $x = \sum_{t \in H\backslash G} x_t t$ with $x_t \in F[H]$ and, given that if t'' is another representative in $H \setminus G$ and $t''t'^{-1} \in H$ then $t'' = t'$, we have that only $x_{t'}t'$ sends any element of $t'^{-1}M$ to M, and $x_{t'}$ must therefore belong to $\mathfrak{A}(F[H], M)$. This holds for every $t' \in H \setminus G$. □

Proposition 2.6.10. *[Ber79, Proposition 2] If $\mathrm{Ind}_H^G M$ is a projective $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattice, then M is a projective $\mathfrak{A}(F[H], M)$-lattice.*

Proof. Suppose $\mathrm{Ind}_H^G M$ projective over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$. Lemmas 2.6.8 and 2.6.9 give us a collection of $x_i = \sum_{s \in G/H} sx_i^s$ with $x_i^s \in M$ and homomorphisms of $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-modules

$$f_i : \mathrm{Ind}_H^G M \to \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$$

such that $x = \sum_{i \in I} f_i(x)x_i$ for every $x \in \mathrm{Ind}_H^G M$. Note that we can write $f_i = \sum_{t \in H\backslash G} f_i^t t$, with $f_i^t : \mathrm{Ind}_H^G M \to \mathfrak{A}(F[H], M)$, by Lemma 2.6.9. Our strategy is to apply Lemma 2.6.8 again for the module M. Let $y \in M$. Then in particular $y \in \mathrm{Ind}_H^G M$ and we can write

$$y = \sum_{i \in I, t \in H\backslash G, s \in G/H} f_i^t(y)tsx_i^s. \tag{2.6.1}$$

Note that since $y \in M$ we have $\sum_{i \in I, t \in H\backslash G, s \in G/H} f_i^t(y)tsx_i^s = \sum_{i \in I, ts \in H} f_i^t(y)tsx_i^s$ We now show that each $f_i^t|_M : M \to \mathfrak{A}(F[H], M)$ is an $\mathfrak{A}(F[H], M)$-homomorphism. By Lemma 2.2.1 it is sufficient to show that $f_i^t|_M$ is an $R[H]$-homomorphism. Let $y \in M \subseteq \mathrm{Ind}_H^G M$ and $r \in R[H] \subseteq R[G] \subseteq \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$, then

$$\sum_{t \in H\backslash G} f_i^t(ry)t = \left(\sum_{t \in H\backslash G} f_i^t t\right)(ry) = r\left(\sum_{t \in H\backslash G} f_i^t t\right)(y) = \sum_{t \in H\backslash G} r f_i^t(y)t,$$

where we used that $\sum_{t\in H\backslash G} f_i^t t : \mathrm{Ind}_H^G M \to \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ is an $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-homomorphism. This shows that $r f_i^t(y) = f_i^t(ry)$ since the summands are direct summands. Analogously, if $y, z \in M$ then, for every i and t, $f_i^t(y+z) = f_i^t(y) + f_i^t(z)$. So, in order to apply Lemma 2.6.8, as elements we can choose $(tsx_i)_{ts\in H, i\in I}$ and keep the functions f_i^t's. □

Remark 2.6.11. With the same proof as Proposition 2.6.10, we can prove that if Λ is an R-order in $F[H]$, M a Λ-lattice and Γ is an R-order in $F[G]$ such that $\Lambda \subseteq \Gamma \subseteq \bigoplus_{t\in H\backslash G} \Lambda t$, then M is projective over Λ if $\mathrm{Ind}_H^G M$ is projective over Γ. Note that this, together with Swan's theorem [CR81, Theorem (32.1)], can be used to prove that, in a Galois extension K/F of number fields with Galois group G, if $\mathcal{O}_K$ is projective over $\mathcal{O}_F[G]$ then L/K is tamely ramified (here, if we fix a prime $\mathfrak{P}$ of K above the prime $\mathfrak{p}$ of F with decomposition group D, we consider Λ and Γ to be equal to $\mathcal{O}_{F_\mathfrak{p}}[D]$ and $\mathcal{O}_{F_\mathfrak{p}}[G]$, respectively). We also have the opposite direction by Theorem 2.3.15.

If H is normal in G then we define $\mathfrak{A}^*(M) = \bigcap_{g\in G} g\mathfrak{A}(F[H], M)g^{-1}$.

Proposition 2.6.12. *[Ber79, Proposition 3] Suppose that H is normal in G. Then*

(i) $\mathfrak{A}^*(M)$ *is an R-order in $F[H]$,*

(ii) $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = \mathrm{Ind}_H^G \mathfrak{A}^*(M)$, *and*

(iii) $\mathrm{Ind}_H^G M$ *is a projective $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattice if and only if M is a projective $\mathfrak{A}^*(M)$-lattice.*

Proof of Proposition 2.6.12(iii). With the same proof as Lemma 2.6.9, we can show that for every $g \in G$ we have

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \bigoplus_{t\in H\backslash G} \left(g\mathfrak{A}(F[H], M)g^{-1}\right) t,$$

and so

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \bigoplus_{t\in H\backslash G} \mathfrak{A}^*(M)t.$$

Now the 'if' direction follows from Remark 2.6.11. The other direction follows from the functorial properties of the induction (since both $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ and $\mathfrak{A}(M)^*$ are rings and one is induced from the other). □

2.6.2 Clean orders and induction

Let R be a discrete valuation ring with field of fractions F of characteristic zero and suppose that the residue field of R is finite.

Definition 2.6.13. Let Λ be an R-order in a finite dimensional semisimple F-algebra A. Then Λ is said to be *clean* if it has the following property: if M is a projective Λ-lattice such that FM is free over A then M is free over Λ.

Theorem 2.6.14 (Hattori)**.** *Commutative R-orders in finite-dimensional semisimple F-algebras are clean.*

Proof. See [Hat65] or [Rog70, IX Corollary 1.5]. □

Proposition 2.6.15. *[Ber79, Corollaire to Proposition 3] Let H be a normal abelian subgroup of a finite group G and let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$. Then the following are equivalent:*

(i) $\mathrm{Ind}_H^G M$ *is projective over* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$;

(ii) $\mathrm{Ind}_H^G M$ *is free over* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$;

(iii) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring and* $\mathrm{Ind}_H^G M$ *is free over* $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$;

(iv) M *is free over* $\mathfrak{A}(F[H], M)$ *and* $\mathfrak{A}^*(M) = \mathfrak{A}(F[H], M)$.

Proof. (i)⇒(iv). By Proposition 2.6.12(iii), M is projective over $\mathfrak{A}^*(M)$. Moreover, $\mathfrak{A}^*(M)$ is a clean order by Theorem 2.6.14 and thus M is in fact free over $\mathfrak{A}^*(M)$. Hence $\mathfrak{A}^*(M) = \mathfrak{A}(F[H], M)$ by Proposition 2.2.2.

(iv)⇒(iii). We have $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathrm{Ind}_H^G \mathfrak{A}^*(M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$, where the second equality is Proposition 2.6.12(ii). Thus $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring by Corollary 2.6.3. Hence $\mathrm{Ind}_H^G M$ is free over $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ by Corollary 2.6.7(iii).

(iii)⇒(ii). This follows from Corollary 2.6.3.

(ii)⇒(i). This follows from the general fact that every free module is projective. □

2.7 Induction for orders of a certain structure

Let R be a discrete valuation ring with field of fractions F of characteristic zero and suppose that the residue field of R is finite. Let G be a finite group and let H be a subgroup of G. In §2.6 we reviewed some general induction properties of the associated order $\mathfrak{A}(F[H], M)$ (with weaker hypotheses on R for some results). In this section, we prove new results concerning inductions of orders of a certain form and then consider arithmetic applications such as the study of weakly ramified extensions.

Let π be a uniformizer of R. For a subgroup P of G, let $\mathrm{ncl}_G(P)$ denote the normal closure of P in G and let $\mathrm{Tr}_P = \sum_{k \in P} k \in R[G]$.

Theorem 2.7.1. *Let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$. Suppose that there exist a positive integer n and a subgroup P of H such that*

$$\mathfrak{A}(F[H], M) = R[H] + \pi^{-n} R[H] \mathrm{Tr}_P.$$

Then the following statements hold:

(i) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = R[G] + \pi^{-n} R[G] \mathrm{Tr}_P$.

(ii) $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = R[G] + \pi^{-n} R[G] \mathrm{Tr}_{\mathrm{ncl}_G(P)}$.

(iii) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring if and only if P is normal in G.*

(iv) If P is normal in G and M is free over $\mathfrak{A}(F[H], M)$ then $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is free over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$.

(v) If H is abelian and normal in G and $\mathrm{Ind}_H^G M$ is projective over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$, then P is normal in G.

Proof. Note that if h runs through a set of coset representatives of G/H and k runs through a set of coset representatives of H/P, then hk runs through a set of left coset representatives of G/P. Thus we have

$$\begin{aligned}
\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) &= \mathrm{Ind}_H^G \left(R[H] + \left\{ \pi^{-n} \left(\sum_{k \in \{H/P} a_k k \right) : a_k \in R \right\} \cdot \mathrm{Tr}_P \right) \\
&= R[G] + \left\{ \sum_{h \in G/H} \pi^{-n} h \left(\sum_{k \in H/P} a_{h,k} k \right) : a_{h,k} \in R \right\} \cdot \mathrm{Tr}_P \\
&= R[G] + \left\{ \pi^{-n} \left(\sum_{h \in G/H} \sum_{k \in H/P} a_{h,k} hk \right) : a_{h,k} \in R \right\} \cdot \mathrm{Tr}_P \\
&= R[G] + \pi^{-n} R[G] \mathrm{Tr}_P,
\end{aligned}$$

which proves (i). Moreover, we have

$$\begin{aligned}
\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) &= R[G] + \pi^{-n} R[G/P] \mathrm{Tr}_P \\
&= R[G] + \left\{ \pi^{-n} \left(\sum_{h \in G/P} a_h h \right) : a_h \text{ is a representative of } R/(\pi^n) \right\} \cdot \mathrm{Tr}_P \\
&= \pi^{-n} \left\{ \sum_{\gamma \in G} a_\gamma \gamma \in R[G] : \gamma_1^{-1} \gamma_2 \in P \Rightarrow a_{\gamma_1} \equiv a_{\gamma_2} \bmod (\pi^n) \right\}.
\end{aligned}$$

Thus for every $g \in G$, we have

$$\begin{aligned}
g \mathrm{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1} &= R[G] + \pi^{-n} R[G/gPg^{-1}] \mathrm{Tr}_{gPg^{-1}} \\
&= \pi^{-n} \left\{ \sum_{\gamma \in G} a_\gamma \gamma \in R[G] : \gamma_1^{-1} \gamma_2 \in gPg^{-1} \Rightarrow a_{\gamma_1} \equiv a_{\gamma_2} \bmod (\pi^n) \right\}.
\end{aligned}$$

We will now use the following general fact. Let G be a group, let B be any set, let A be a subset of G and let A' be the subgroup of G generated by A. Then from the description of the elements of A' in terms of products of elements of A and their inverses, we have

$$\begin{aligned}
&\left\{ \{a_\gamma\}_{\gamma \in G} \in \textstyle\prod_{\gamma \in G} B : \gamma_1^{-1} \gamma_2 \in A \Rightarrow a_{\gamma_1} = a_{\gamma_2} \right\} \\
&\qquad = \left\{ \{a_\gamma\}_{\gamma \in G} \in \textstyle\prod_{\gamma \in G} B : \gamma_1^{-1} \gamma_2 \in A' \Rightarrow a_{\gamma_1} = a_{\gamma_2} \right\}.
\end{aligned}$$

This said, by Proposition 2.6.1, we have that

$$\begin{aligned}\mathfrak{A}(F[G],\mathrm{Ind}_H^G M) &= \bigcap_{g\in G} g\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)g^{-1}\\ &= \pi^{-n}\left\{\sum_{\gamma\in G} a_\gamma\gamma \in R[G] : \gamma_1^{-1}\gamma_2 \in \bigcup_{g\in G} gPg^{-1} \Rightarrow a_{\gamma_1}\equiv a_{\gamma_2} \bmod (\pi^n)\right\}\\ &= \pi^{-n}\left\{\sum_{\gamma\in G} a_\gamma\gamma \in R[G] : \gamma_1^{-1}\gamma_2 \in \mathrm{ncl}_G(P) \Rightarrow a_{\gamma_1}\equiv a_{\gamma_2} \bmod (\pi^n)\right\}\\ &= R[G] + \pi^{-n}R[G/\mathrm{ncl}_G(P)]\mathrm{Tr}_{\mathrm{ncl}_G(P)},\\ &= R[G] + \pi^{-n}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P)},\end{aligned}$$

which proves (ii).

By Corollary 2.6.3, $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)$ is a ring if and only if it is equal to $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$, which by (i) and (ii) is true if and only if $P=\mathrm{ncl}(P)$. This proves (iii). Part (iv) follows from (iii) and Corollary 2.6.7(iii). Part (v) follows from (iii) and Proposition 2.6.15(i)⇒(iii). □

We have the following application to the understanding of local freeness in weakly ramified extensions of number fields.

Corollary 2.7.2. *Let K/F be a finite Galois extension of number fields with Galois group G and let $\mathfrak{P}|\mathfrak{p}$ be two primes of K/F such that $K_\mathfrak{P}/F_\mathfrak{p}$ is wildly and weakly ramified.*

(i) If the inertia group $G_0 = G_0(\mathfrak{P}|\mathfrak{p})$ is normal in G then $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}}$.

(ii) Suppose that the decomposition group $D = D(\mathfrak{P}|\mathfrak{p})$ is abelian and normal in G. Then $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}}$ if and only if G_0 is normal in G.

Proof. Let π be any uniformizer of $\mathcal{O}_{F_\mathfrak{p}}$. Then by Theorem 2.3.9 we have

$$\mathfrak{A}(F_\mathfrak{p}[D],\mathcal{O}_{K_\mathfrak{P}}) = \mathfrak{A}_{K_\mathfrak{P}/F_\mathfrak{p}} = \mathcal{O}_{F_\mathfrak{p}}[D][\pi^{-1}\mathrm{Tr}_{G_0}] = \mathcal{O}_{F_\mathfrak{p}}[D] + \pi^{-1}\mathcal{O}_{F_\mathfrak{p}}[D]\mathrm{Tr}_{G_0}$$

and $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}(F_\mathfrak{p}[D],\mathcal{O}_{K_\mathfrak{P}})$. Hence claim (i) follows from Theorem 2.7.1(iv). Claim (ii) follows from Theorem 2.7.1(v) for one direction and from claim (i) for the other direction. □

We now prove the following generalisation of Theorem 2.7.1.

Theorem 2.7.3. *Let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$. Suppose that there exist integers $0=n_0<n_1<\cdots<n_r$ and subgroups*

$$\{e\} = P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r \subseteq H \subseteq G$$

such that

$$\mathfrak{A}(F[H],M) = \sum_{i=0}^{r} \pi^{-n_i}R[H]\mathrm{Tr}_{P_i}. \tag{2.7.1}$$

Then the following statements hold:

(i) $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M) = \sum_{i=0}^r \pi^{-n_i}R[G]\mathrm{Tr}_{P_i}$.

(ii) $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M) = \sum_{i=0}^r \pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}$.

(iii) $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)$ *is a ring if and only if* P_i *is normal in* G *for every* i.

(iv) If P_i *is normal in* G *for every* i *and* M *is free over* $\mathfrak{A}(F[H],M)$ *then* $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)$ *is free over* $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$.

(v) If H *is abelian and normal in* G *and* $\mathrm{Ind}_H^G M$ *is projective over* $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$, *then* P_i *is normal in* G *for every* i.

Proof. The proof of part (i) is exactly as for Theorem 2.7.1(i).

We already know from Theorem 2.7.1 that (ii) holds if $r = 1$. So suppose that $r > 1$. Note that, since each $\mathrm{ncl}_G(P_i)$ is normal in G, for each $g \in G$ we have that

$$g^{-1}\pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}g = \pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)} = \mathrm{Tr}_{\mathrm{ncl}_G(P_i)/P_i}\pi^{-n_i}\mathrm{Tr}_{P_i} \in \mathrm{Ind}_H^G\mathfrak{A}(F[H],M),$$

where $\mathrm{Tr}_{\mathrm{ncl}_G(P_i)/P_i}$ is the sum over any fixed choice of coset representatives of $\mathrm{ncl}_G(P_i)/P_i$. Hence for each $g \in G$ we have $\pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)} \in g\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)g^{-1}$. Together with Proposition 2.6.1, this implies that $\pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)} \in \mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$. Therefore

$$\mathfrak{A}(F[G],\mathrm{Ind}_H^G M) \supseteq \sum_{i=0}^r \pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}.$$

It remains to show the reverse containment. First note that

$$\mathfrak{A}(F[G],\mathrm{Ind}_H^G M) \subseteq \mathrm{Ind}_H^G\mathfrak{A}(F[H],M) = \sum_{i=0}^r \pi^{-n_i}R[G]\mathrm{Tr}_{P_i}, \tag{2.7.2}$$

where the containment follows from Remark 2.6.5 and the equality is part (i). Let $\theta \in \mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$. Then we can write $\theta = \sum_{i=0}^r \pi^{-n_i}\theta_i\mathrm{Tr}_{P_i}$, where $\theta_i \in R[G]$ for each i. For each integer j with $0 \le j \le r$, we shall prove that

$$\theta \in \sum_{i=0}^{r-j-1} \pi^{-n_i}R[G]\mathrm{Tr}_{P_i} + \sum_{i=r-j}^{r} \pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}.$$

We proceed by induction on j and first consider the base case $j = 0$. We have that

$$\pi^{n_{r-1}}\theta = \sum_{i=0}^r \pi^{n_{r-1}-n_i}\theta_i\mathrm{Tr}_{P_i} \in R[G] + \pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{P_r}.$$

Also note that for each $g \in G$ we have

$$\begin{aligned} g^{-1}\pi^{n_{r-1}}\theta g &\in g^{-1}\pi^{n_{r-1}}\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)g \\ &= \pi^{n_{r-1}}\mathfrak{A}(F[G],\mathrm{Ind}_H^G M) \\ &\subseteq \pi^{n_{r-1}}\mathrm{Ind}_H^G\mathfrak{A}(F[H],M) \\ &\subseteq R[G] + \pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{P_r}. \end{aligned}$$

Hence

$$\pi^{n_{r-1}}\theta \in \bigcap_{g\in G} g\left(R[G]+\pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{P_r}\right)g^{-1} = R[G]+\pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_r)},$$

where the equality follows from the case $r=1$. Thus there exists $\alpha\in R[G]$ such that

$$\theta-\pi^{-n_r}\alpha\mathrm{Tr}_{\mathrm{ncl}_G(P_r)} \in \pi^{-n_{r-1}}R[G]\cap \mathrm{Ind}_H^G\mathfrak{A}(F[H],M) = \sum_{i=0}^{r-1}\pi^{-n_i}R[G]\mathrm{Tr}_{P_i},$$

where the equality follows from (2.7.2) and the containment $R[G]\mathrm{Tr}_{P_r}\subseteq R[G]\mathrm{Tr}_{P_{r-1}}$, which holds since $\mathrm{Tr}_{P_r}=\mathrm{Tr}_{P_r/P_{r-1}}\mathrm{Tr}_{P_{r-1}}$. This completes the base case $j=0$.

We now proceed with the induction step. Suppose our claim is valid for $j-1$, and let us prove it for j. Using the inductive hypothesis and subtracting an appropriate element of $\sum_{i=j+1}^{r}\pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}$, we can and do assume without loss of generality that

$$\theta=\sum_{i=0}^{r-j}\pi^{-n_i}\theta_i\mathrm{Tr}_{P_i}\in\mathfrak{A}(F[G],\mathrm{Ind}_H^G M),$$

for some $\theta_i\in R[G]$. Hence it remains to show that

$$\theta\in\sum_{i=0}^{r-j-1}\pi^{-n_i}R[G]\mathrm{Tr}_{P_i}+\pi^{-n_{r-j}}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_{r-j})}.$$

As in the base case, for each $g\in G$ we have

$$\begin{aligned} g^{-1}\pi^{n_{r-j-1}}\theta g &\in \pi^{n_{r-j-1}-n_{r-j}}R[G]\cap\pi^{n_{r-j-1}}\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)\\ &\subseteq \pi^{n_{r-j-1}-n_{r-j}}R[G]\cap\pi^{n_{r-j-1}}\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)\\ &\subseteq R[G]+\pi^{n_{r-j-1}-n_{r-j}}R[G]\mathrm{Tr}_{P_{r-j}}, \end{aligned}$$

so, by the result for $r=1$, we have

$$\pi^{n_{r-j-1}}\theta\in R[G]+\pi^{n_{r-j-1}-n_{r-j}}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_{r-j})}.$$

Thus there exists $\alpha\in R[G]$ such that

$$\theta-\pi^{-n_{r-j}}\alpha\mathrm{Tr}_{\mathrm{ncl}_G(P_{r-j})}\in\pi^{-n_{r-j-1}}R[G]\cap\left(\sum_{i=0}^{r-j}\pi^{-n_i}\theta_i\mathrm{Tr}_{P_i}\right)=\sum_{i=0}^{r-j-1}\pi^{-n_i}R[G]\mathrm{Tr}_{P_i}.$$

This concludes the induction step. Therefore we deduce that

$$\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)=\sum_{i=0}^{r}\pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)},$$

which concludes the proof of part (ii).

We easily see with the same methods that

$$\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)=\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$$

precisely when $P_i=\mathrm{ncl}_G(P_i)$ for every i, establishing part (iii). Part (iv) follows from part (iii) and Corollary 2.6.7(iii). Part (v) follows from Proposition 2.6.15(i)⇒(iii). □

Remark 2.7.4. It follows from the proof of Theorem 2.7.3 that the subgroups P_i and the numbers n_i are uniquely determined by $\mathfrak{A}(F[H], M)$. Moreover, P_i is normal in H (a way to see this from what we already proved is the following: $\mathrm{Ind}_H^H \mathfrak{A}(F[H], M) = \mathfrak{A}(F[H], M)$ is a ring, so that we can apply (iii) with $G = H$) and π^{n_i} divides the order of P_i for all i.

2.8 Leopoldt-type theorems for A_4, S_4 and A_5-extensions of $\mathbb{Q}$

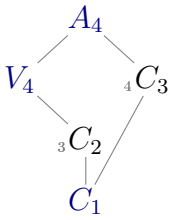
2.8.1 Galois module structure of A_4-extensions of $\mathbb{Q}$

In this subsection, we shall prove the following result, which is Theorem 2.1.6 stated in the introduction to this chapter.

Theorem 2.8.1. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if 2 is tamely ramified or has full decomposition group.*

Remark 2.8.2. After considering computational evidence, in [BJ08, §8] the authors raised the question of whether it is always the case that $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ for every A_4-extension $K/\mathbb{Q}$. Theorem 2.8.1 shows that this is false. Indeed, one can use the database of number fields [LMF19] to verify that every possible decomposition group of 2 of even order can be realised by an A_4-extension $K/\mathbb{Q}$ in which 2 is wildly ramified.

Proof of Theorem 2.8.1. We already showed the 'if' direction in Proposition 2.4.12. Now we prove that if 2 is wildly ramified in $K/\mathbb{Q}$ and does not have full decomposition group then $\mathcal{O}_K$ is not (locally) free (at 2) over $\mathfrak{A}_{K/\mathbb{Q}}$. Let V_4 denote the unique normal subgroup of $G := \mathrm{Gal}(K/\mathbb{Q}) \cong A_4$ of order 4, which is isomorphic to $C_2 \times C_2$. Recall that $A_4 \cong V_4 \rtimes C_3$ and we have the following lattice of the subgroups of A_4 up to conjugacy (see, for instance, the GroupNames database [Dok18]).



Here the subscript on the left denotes the number of conjugate subgroups, and is taken to be 1 when omitted (so that the subgroup is normal).

Let $\mathfrak{P}$ be a prime of K above 2, let $D = D(\mathfrak{P}|2)$ be the decomposition group and let $G_0 = G_0(\mathfrak{P}|2)$ be the inertia group of $K/\mathbb{Q}$. From the subgroup lattice, we see that it suffices to analyse the cases in which 2 is wildly ramified in $K/\mathbb{Q}$ and $D = V_4$ or $D \cong C_2$. More precisely, there are three possibilities for the pair (D, G_0) up to isomorphism: (V_4, V_4), (V_4, C_2) and (C_2, C_2). Since D is abelian in each of these cases, we have that $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ by Theorem 2.3.3. Thus by Proposition 2.6.6 we have that $\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} \cong \mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{P}} \cong \mathcal{O}_{K,2}$ as $\mathfrak{A}_{K/\mathbb{Q},2}$-lattices. Therefore it suffices to show that $\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ in each of the three cases.

First suppose that $D = G_0 = V_4$. Then from the database of p-adic fields [JR06] we see that there are four possible extensions $K_\mathfrak{P}/\mathbb{Q}_2$, each of which has 1 and 3 as (lower) ramification jumps. Let F denote the subfield of $K_\mathfrak{P}$ fixed by G_2. Then by Remark 2.3.12 we have $e_{G_2} \in \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ since

$$\sum_{i=0}^{\infty}(|G_i(K_\mathfrak{P}/F)| - 1) = 1 + 1 + 1 + 1 = 4 \geq 4 = |G_0(K_\mathfrak{P}/\mathbb{Q}_2)| \cdot v_2(|G_2|).$$

Similarly, we have $e_{V_4} = e_{G_1} \in \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ since

$$\sum_{i=0}^{\infty}(|G_i(K_\mathfrak{P}/\mathbb{Q}_2)| - 1) = 3 + 3 + 1 + 1 = 8 \geq 8 = |G_0(K_\mathfrak{P}/\mathbb{Q}_2)| \cdot v_2(|V_4|).$$

Thus $K_\mathfrak{P}/\mathbb{Q}_2$ is almost-maximally ramified, and so by Theorem 2.3.10(i) we have that

$$\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D][e_{G_2}, e_{G_1}] = \mathbb{Z}_2[V_4] + \frac{1}{2}\mathbb{Z}_2[V_4]\mathrm{Tr}_{G_2} + \frac{1}{4}\mathbb{Z}_2[V_4]\mathrm{Tr}_{V_4}.$$

Since $G_2 \cong C_2$ is not normal in G and D is both abelian and normal in G, Theorem 2.7.3(v) implies that $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Hence $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. As an aside, we note that, by Theorem 2.7.3(i)&(ii), in this case we have

$$\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\mathrm{Tr}_{G_2} + \frac{1}{4}\mathbb{Z}_2[G]\mathrm{Tr}_{V_4} \supsetneq \mathbb{Z}_2[G] + \frac{1}{4}\mathbb{Z}_2[G]\mathrm{Tr}_{V_4} = \mathfrak{A}_{K/\mathbb{Q},2}.$$

Now suppose that $D = V_4$ and $G_0 \cong C_2$. Since $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ and $G_0 = G_1$ is not dihedral of order 4, Theorem 2.3.10 implies that

$$\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D][e_{G_0}] = \mathbb{Z}_2[V_4] + \frac{1}{2}\mathbb{Z}_2[V_4]\mathrm{Tr}_{G_0}.$$

(Alternatively, we can use the database of p-adic fields [JR06] to check for almost-maximal ramification as in the previous case; the ramification jump turns out to be 1 or 2). Since D is both abelian and normal in G and G_0 is not normal in G, Theorem 2.7.1(v) implies that $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Hence $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Note that in the next paragraph we shall use the following fact:

$$\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\mathrm{Tr}_{G_0} \supsetneq \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\mathrm{Tr}_{V_4} = \mathfrak{A}_{K/\mathbb{Q},2},$$

which follows from Theorem 2.7.1(i)&(ii).

Finally suppose $D = G_0 \cong C_2$. Then $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is a $\mathbb{Z}_2$-order in $\mathbb{Q}_2[D] \cong \mathbb{Q}_2[C_2]$ strictly containing $\mathbb{Z}_2[D]$. As there is only one such order, we must have

$$\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D] + \frac{1}{2}\mathbb{Z}_2[D]\mathrm{Tr}_D.$$

We cannot directly apply Theorem 2.7.1(iv)&(v) as in the previous cases, as D is not normal in G, but from Theorem 2.7.1(i)&(ii) we have that

$$\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\mathrm{Tr}_D \supsetneq \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\mathrm{Tr}_{V_4} = \mathfrak{A}_{K/\mathbb{Q},2}.$$

Once we fix a copy of C_2 inside G, note that $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$ are exactly the same as in the (V_4, C_2)-case of the previous paragraph, where we already showed that $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Therefore $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. □

2.8.2 Galois module structure of S_4-extensions of $\mathbb{Q}$

In this subsection, we shall prove the following result, which is Theorem 2.1.7 stated in the introduction.

Theorem 2.8.3. *Let $K/\mathbb{Q}$ be a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if one of the following conditions on $K/\mathbb{Q}$ holds:*

(i) 2 *is tamely ramified;*

(ii) 2 *has decomposition group equal to the unique subgroup of G of order* 12*;*

(iii) 2 *is wildly and weakly ramified and has full decomposition group; or*

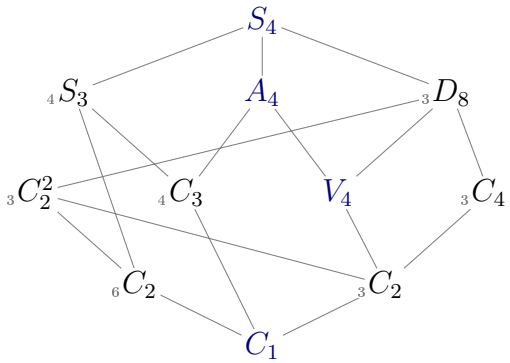
(iv) 2 *is wildly and weakly ramified, has decomposition group of order* 8 *in G, and has inertia subgroup equal to the unique normal subgroup of order* 4 *in G.*

Proof. By Proposition 2.4.10, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$.

We first show that if any of conditions (i)–(iv) hold then $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$. In case (i), this follows from Theorem 2.3.15. In case (ii), Lemma 2.4.11 shows that 2 is wildly and weakly ramified in $K/\mathbb{Q}$ and has inertia group equal to the unique normal subgroup of order 4 in G (note that A_4 is the unique subgroup of S_4 of order 12). Therefore in cases (ii), (iii) and (iv), 2 is wildly and weakly ramified in $K/\mathbb{Q}$ and its inertia group is normal in G, and so the desired result follows from Corollary 2.7.2(i).

It now remains to show that if we are not in any of the cases (i)–(iv) then $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. We shall use the MAGMA implementation of two different algorithms: we use [BJ08, Algorithm 3.1(6)] to verify that in four specific S_4-extensions of $\mathbb{Q}_2$ the ring of integers is not free over its associated order; we use [HJ20, §8.5], which concerns general lattices in group rings, to prove that $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ in cases when we do have freeness in the corresponding 2-adic extension.

We have the following lattice of the subgroups of S_4 up to conjugacy (see, for instance, the GroupNames database [Dok18]).



Here the subscript on the left denotes the number of conjugate subgroups, and is taken to be 1 when omitted (so that the subgroup is normal). In particular, the only normal subgroups are C_1, V_4, A_4 and S_4. (Recall that $V_4 \cong C_2 \times C_2$.)

We fix an isomorphism $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$ and denote by A_4, D_8, S_3, C_2^2, V_4, C_4 a choice of subgroups of G in such a way that whenever there is a containment between choices of conjugates of two such subgroups, one of the subgroups is in fact contained in the other.

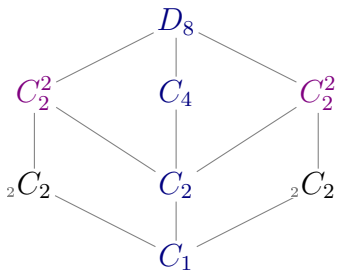
Suppose that $K/\mathbb{Q}$ does not satisfy any of the conditions (i)–(iv). Let $\mathfrak{P}$ be a prime of K above 2 and let $D = D(\mathfrak{P}|2)$ be the decomposition group. In particular, 2 is wildly ramified in $K/\mathbb{Q}$ and so D must be of even order. We cannot have $D = A_4$ as this corresponds to case (ii). Moreover, we cannot have $D = S_3$ since the subgroups of D of order 2 are not normal, but the wild inertia subgroup G_1 must be normal in D.

Suppose that $D = S_4$. Since we are not in case (iii), this implies that 2 is wildly but not weakly ramified in $K/\mathbb{Q}$. From the database of p-adic fields [JR06], we see that there are four possibilities for the completed extension $K_{\mathfrak{P}}/\mathbb{Q}_2$. By using the updated MAGMA implementation of [BJ08, Algorithm 3.1(6)] (see §2.A.1 for details), which is based on that of [BW09, §4.2], we can verify that $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ in any of these cases (for the details on the implementation see §2.A.1). Since the decomposition group is full (i.e. $D = G$), this immediately implies that $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$.

Now suppose that $D \cong D_8$; without loss of generality, we can and do assume that $D = D_8$. We first treat the case in which $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$. Then $\mathcal{O}_{K_{\mathfrak{P}}}$ is not projective over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ by Theorem 2.3.10, and so $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ by Proposition 2.6.10. As an aside, by using the database [JR06], Theorem 2.3.10 and Remark 2.3.12, it is straightforward to check that $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ if and only if the ramification jumps of $K_{\mathfrak{P}}/\mathbb{Q}_2$ are 1, 3 and 5.

Therefore in the remaining cases we can and do assume that $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$, since either D is abelian (in which case we can apply Theorem 2.3.3) or $D = D_8$, in which case the situation in which $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ has already been considered in the previous paragraph. As we wish to show that $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$, by Proposition 2.6.6 it suffices to show that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Our strategy will be to determine the possible ramification groups, use this to understand the structure of $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and then apply Theorem 2.7.3 to obtain explicit descriptions of $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$; we will leave this last step to the end as cases with different D will overlap.

We now return to the case $D = D_8$. We have the following subgroup lattice.



We denote the unique normal subgroup of order 2 in D_8 by V_2, and note that as a subgroup of S_4, this is generated by a double transposition and contained in C_4. (Also note that under D_8-conjugation we have three conjugacy classes of subgroups of order 2 compared to two in the S_4-lattice).

Suppose that $K_\mathfrak{P}/\mathbb{Q}_2$ is almost-maximally ramified. Then by Theorem 2.3.10 we have $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D] + \sum_{t\geq 1}\frac{1}{|G_t|}\mathbb{Z}_2[D]\mathrm{Tr}_{G_t}$ and all quotients of two consecutive different ramification groups are of order 2 (see the database [JR06], for example). We have that V_2 must be among the ramification groups since they are all normal in D_8. Thus if the ramification index of $K_\mathfrak{P}/\mathbb{Q}_2$ is 2, then V_2 is the unique ramification group. Otherwise, there is a ramification group of order 4, which must be one of V_4, C_2^2 or C_4. Moreover, D_8 is a ramification group if and only if the ramification index of $K_\mathfrak{P}/\mathbb{Q}_2$ is 8.

Suppose that $K_\mathfrak{P}/\mathbb{Q}_2$ is not almost-maximally ramified. Then by Theorem 2.3.10 we deduce that $G_0 \cong C_2^2$ and $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D] + \frac{1}{2}\mathbb{Z}_2[D]\mathrm{Tr}_{G_0}$. Moreover, by Remark 2.3.12 we must have that $G_2 = 0$ or $G_2 \cong C_2$ and $G_3 = 0$, but in the latter case the upper ramification jumps are not integral, which is not possible by Hasse-Arf theorem (alternatively just use the database [JR06]); hence $K_\mathfrak{P}/\mathbb{Q}_2$ is weakly ramified. Note that G_0 is not equal to V_4, otherwise we are in case (iv), hence we can assume $G_0 = C_2^2$.

Now suppose that $D \cong C_4$; without loss of generality, we can and do assume that $D = C_4$. If the ramification index of $K_\mathfrak{P}/\mathbb{Q}_2$ is 2, then $G_0 = V_2$ and by Remark 2.3.12 $K_\mathfrak{P}/\mathbb{Q}_2$ is almost-maximally ramified, and hence $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D] + \frac{1}{2}\mathbb{Z}_2[D]\mathrm{Tr}_{G_0}$ (see [Ber78, Corollaire 3 to Théorème 1], for example). If the ramification index is 4, then there must be two ramification jumps; since the upper ramification jumps are integral, Remark 2.3.12 implies that the extension is almost-maximally ramified and so $\frac{1}{2}\mathrm{Tr}_{V_2}$ and $\frac{1}{4}\mathrm{Tr}_D$ belong to $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$. Hence

$$\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \mathbb{Z}_2[D] + \frac{1}{2}\mathbb{Z}_2[D]\mathrm{Tr}_{V_2} + \frac{1}{4}\mathbb{Z}_2[D]\mathrm{Tr}_D,$$

where the containment '$\subseteq$' follows from the fact that the right-hand side is the unique maximal order in $\mathbb{Q}_2[D]$ (see [Ber78, Proposition 5], for example).

Finally, note that in the cases $D \cong C_2^2$ or $D \cong C_2$, we already computed $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ in the proof of Theorem 2.8.1.

We will denote by W_2 a choice of a subgroup of S_4 generated by a transposition and contained in D_8. We fix the following notation: $\langle 1, \frac{1}{2^{n_1}}\mathrm{Tr}_{H_1}, \cdots, \frac{1}{2^{n_k}}\mathrm{Tr}_{H_k}\rangle$ is the lattice

$$\mathbb{Z}_2[G] + \frac{1}{2^{n_1}}\mathbb{Z}_2[G]\mathrm{Tr}_{H_1} + \cdots + \frac{1}{2^{n_k}}\mathbb{Z}_2[G]\mathrm{Tr}_{H_k}.$$

Since we have now determined $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ in all the remaining cases, we can use Theorem 2.7.3(i)&(ii) to determine $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$ as listed in Table 2.1 below. Note that the point of this analysis is to show that no values for $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ other than those listed in Table 2.1 can be realised, and so the reader does not necessarily have to focus on which possible decomposition group(s) and ramification properties correspond to each entry of the table.

Hofmann and Johnston [HJ20, §8.5] described the implementation of an algorithm in Magma that, given a finite group Γ, a prime number p, and $\mathbb{Z}[\Gamma]$-lattices X and Y contained in $\mathbb{Q}[\Gamma]$, determines whether the localisations X_p and Y_p are isomorphic over $\mathbb{Z}_{(p)}[\Gamma]$. Note that by [CR81, Proposition (30.17)], this is equivalent to checking whether the p-adic completions are isomorphic over $\mathbb{Z}_p[\Gamma]$. In present situation, we are interested in understanding whether $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is free over its associated order $\mathfrak{A}_{K/\mathbb{Q},2}$ for each of

Table 2.1

	$\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$	$\mathfrak{A}_{K/\mathbb{Q},2}$
(i)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{G}\rangle$
(ii)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle$	$\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{G}\rangle$
(iii)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{G}\rangle$
(iv)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_4}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{4}\mathrm{Tr}_{G}\rangle$
(v)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{V_4}\rangle$	$\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}\rangle$
(vi)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{4}\mathrm{Tr}_{G}\rangle$
(vii)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{W_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle$	$\langle 1, \frac{1}{4}\mathrm{Tr}_{G}\rangle$
(viii)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2^2}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{G}\rangle$
(ix)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}\rangle$
(x)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{W_2}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{G}\rangle$

the cases in Table 2.1. By Lemma 2.2.1 this condition is equivalent to $\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ being isomorphic to $\mathfrak{A}_{K/\mathbb{Q},2}$ as $\mathbb{Z}_2[G]$-lattices. Since $\mathbb{Z}_2[G] + \frac{1}{2^{n_1}}\mathbb{Z}_2[G]\mathrm{Tr}_{H_1} + \cdots + \frac{1}{2^{n_k}}\mathbb{Z}_2[G]\mathrm{Tr}_{H_k}$ is the completion of $\mathbb{Z}[G] + \frac{1}{2^{n_1}}\mathbb{Z}[G]\mathrm{Tr}_{H_1} + \cdots + \frac{1}{2^{n_k}}\mathbb{Z}[G]\mathrm{Tr}_{H_k}$, a computation using the aforementioned algorithm shows that $\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ in each of the ten cases in Table 2.1 (for the implementation see §2.A.2). □

Remark 2.8.4. Cases (v) and (ix) from Table 2.1 can be tackled using Theorem 2.7.3(v) and cases (vii) and (x) using Theorem 2.7.3(v) combined with Proposition 2.6.10. More precisely:

- for (v) we apply Theorem 2.7.3(v) with $H = V_4$ and $G = S_4$;
- for (vii) we apply Theorem 2.7.3(v) with $H = C_2^2$ and $G = D_8$ and Proposition 2.6.10 inducing from D_8 to $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$;
- for (ix) we apply Theorem 2.7.3(v) with $H = V_4$ and $G = S_4$;
- for (x) we apply Theorem 2.7.3(v) with $H = W_2$ and $G = D_8$ and Proposition 2.6.10 inducing from D_8 to $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$.

Note that here G is not necessarily the Galois group and H is not necessarily one of the decomposition groups.

Remark 2.8.5. The computations in the proof of Theorem 2.8.3 show that each of the lattices considered is free over its associated order if and only if the lattice is a ring if and only if the lattice is equal to its associated order. However, with the algorithm of [HJ20, §8.5] we found that $\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle$ is free over $\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{G}\rangle$ (see §2.A.2 for the implementation).

2.8.3 Galois module structure of A_5-extensions of $\mathbb{Q}$

In this subsection, we shall prove the following result, which is Theorem 2.1.8 stated in the introduction.

Theorem 2.8.6. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if all three of the following conditions on $K/\mathbb{Q}$ hold:*

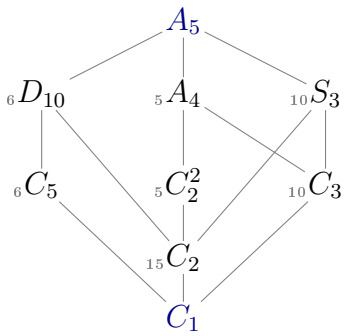
(i) 2 *is tamely ramified;*

(ii) 3 *is tamely ramified or is weakly ramified with ramification index* 6*; and*

(iii) 5 *is tamely ramified or is weakly ramified with ramification index* 10*.*

Proof of Theorem 2.8.6. By Corollary 2.2.7, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ for every prime number p. If p is tamely ramified in $K/\mathbb{Q}$ then $\mathcal{O}_{K,p}$ is indeed free over $\mathfrak{A}_{K/\mathbb{Q},p}$ by Theorem 2.3.15. Thus it remains to consider the situation in which at least one of the primes $p = 2, 3, 5$ is wildly ramified in $K/\mathbb{Q}$.

We have the following lattice of the subgroups of A_5 up to conjugacy (see, for instance, the GroupNames database [Dok18]).



Here the subscript on the left denotes the number of conjugate subgroups. Recall that A_5 is simple and note that the subgroup lattice shows that isomorphic subgroups must be conjugate. Moreover, since A_5 is not soluble, no prime can have full decomposition group. We fix an isomorphism $G := \mathrm{Gal}(K/\mathbb{Q}) \cong A_5$ and denote by A_4, D_{10} etc. a choice of subgroups of G in such a way that whenever there is a containment between choices of conjugates of two such subgroups, one of the subgroups is in fact contained in the other.

Suppose that $p = 2$ is wildly ramified in $K/\mathbb{Q}$. Let $\mathfrak{P}$ be a prime of K above 2 and let $D(2)$ be its decomposition group. Then $D(2)$ must be isomorphic to A_4, C_2^2 or C_2, since for every other subgroup H of A_5 there is no normal non-trivial 2-subgroup in H. Hence in each of these cases $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ (if $D(2) = A_4$, this follows from Lemma 2.4.11 and Theorem 2.3.9; otherwise this follows from Theorem 2.3.3). By Proposition 2.6.6, $\mathrm{Ind}_{D(2)}^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} \cong \mathrm{Ind}_{D(2)}^G \mathcal{O}_{K_\mathfrak{P}} \cong \mathcal{O}_{K,2}$ as $\mathfrak{A}_{K/\mathbb{Q},2}$-lattices. Thus we need to analyse when $\mathrm{Ind}_{D(2)}^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$. In each of the aforementioned possibilities for $D(2)$, we already know the structure of $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ from the proof of Theorem 2.8.1. Using Theorem 2.7.3(i)&(ii) we can write all the possibilities for $\mathrm{Ind}_{D(2)}^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$. We use the following notation: $\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2} \rangle =$

$\mathbb{Z}_2[G]+\frac{1}{2}\mathbb{Z}_2[G]\mathrm{Tr}_{C_2}$ etc. The results are shown in Table 2.2 below (as in the proof of Theorem 2.8.3, the point of the above analysis is to show that no values for $\mathrm{Ind}_{D(2)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ other than those listed in Table 2.2 can be realised).

Table 2.2

	$\mathrm{Ind}_{D(2)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$	$\mathfrak{A}_{K/\mathbb{Q},2}$
(i)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{G}\rangle$
(ii)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle$	$\langle 1, \frac{1}{4}\mathrm{Tr}_{G}\rangle$
(iii)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2^2}\rangle$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{G}\rangle$

As in the proof of Theorem 2.8.3, we can use the MAGMA implementation of the algorithm described in [HJ20, §8.5]. We can hence verify that in none of the above cases $\mathrm{Ind}_{D(2)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} \cong \mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$ (see §2.A.3 for the implementation).

Now suppose that $p = 3$ or 5 and that p is wildly ramified in $K/\mathbb{Q}$. Let $\mathfrak{P}$ be a choice of a prime of K above p and let $D(p)$ be its decomposition group. There is no Galois extension $L/\mathbb{Q}_3$ such that $\mathrm{Gal}(L/\mathbb{Q}_3) \cong A_4$ (since the subgroups of order 3 are not normal in A_4). Hence $D(p)$ must be isomorphic to either D_{2p} or C_p, which implies that $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ by Theorems 2.3.3 and 2.3.4. Thus by Proposition 2.6.6 we have that $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p} \cong \mathrm{Ind}_{D}^{G}\mathcal{O}_{K_\mathfrak{P}} \cong \mathcal{O}_{K,p}$ as $\mathfrak{A}_{K/\mathbb{Q},p}$-lattices, so that our goal is to analyse when $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$. We use the following notation: $\langle 1, \frac{1}{p}\mathrm{Tr}_{C_p}\rangle = \mathbb{Z}_p[G] + \frac{1}{p}\mathbb{Z}_p[G]\mathrm{Tr}_{C_p}$, etc. If $D(p) \cong C_p$ (in which case we can and do assume that $D(p) = C_p$), then as $K_\mathfrak{P}/\mathbb{Q}_p$ is wildly ramified this implies that $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p} = \mathbb{Z}_p[D(p)] + \frac{1}{p}\mathbb{Z}_p[D(p)]\mathrm{Tr}_{D(p)}$, which is the unique maximal order in $\mathbb{Q}_p[D(p)]$. If $D(p) \cong D_{2p}$ (in which case we can and do assume that $D = D_{2p}$), we can use Theorem 2.3.10: in case of almost-maximal ramification, $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p} = \mathbb{Z}_p[D(p)] + \frac{1}{p}\mathbb{Z}_p[D(p)]\mathrm{Tr}_{C_p}$ (which gives the same structure for $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ as when $D(p) = C_p$); otherwise, by Remark 2.3.13, $K_\mathfrak{P}/\mathbb{Q}_p$ is weakly and totally ramified and $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p} = \mathbb{Z}_p[D(p)]+\frac{1}{p}\mathbb{Z}_p[D(p)]\mathrm{Tr}_{D(p)}$. Hence there are two possibilities for $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ and $\mathfrak{A}_{K/\mathbb{Q},p}$, shown in Table 2.3.

Table 2.3

	$\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$	$\mathfrak{A}_{K/\mathbb{Q},p}$
(i)	$\langle 1, \frac{1}{p}\mathrm{Tr}_{C_p}\rangle$	$\langle 1, \frac{1}{p}\mathrm{Tr}_{G}\rangle$
(ii)	$\langle 1, \frac{1}{p}\mathrm{Tr}_{D_{2p}}\rangle$	$\langle 1, \frac{1}{p}\mathrm{Tr}_{G}\rangle$

We used the MAGMA implementation of the algorithm from [HJ20, §8.5] to verify that $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ if and only if we are in case (ii), that is, precisely when $K_\mathfrak{P}/\mathbb{Q}_p$ is weakly ramified or, equivalently, when it is not almost maximally-ramified (see §2.A.3). □

Remark 2.8.7. Note that from the proof of Theorem 2.8.1, we already knew that neither $\mathbb{Z}_2[A_4] + \frac{1}{2}\mathbb{Z}_2[A_4]\mathrm{Tr}_{C_2}$ nor $\mathbb{Z}_2[A_4] + \frac{1}{2}\mathbb{Z}_2[A_4]\mathrm{Tr}_{C_2} + \frac{1}{4}\mathbb{Z}_2[A_4]\mathrm{Tr}_{C_2^2}$ are even projective over their associated orders; induction from A_4 to S_4 and Proposition 2.6.10 permit us to

conclude that $\mathbb{Z}_2[S_4] + \frac{1}{2}\mathbb{Z}_2[S_4]\mathrm{Tr}_{C_2}$ and $\mathbb{Z}_2[S_4] + \frac{1}{2}\mathbb{Z}_2[S_4]\mathrm{Tr}_{C_2} + \frac{1}{4}\mathbb{Z}_2[S_4]\mathrm{Tr}_{C_2^2}$ are not projective over their associated orders. Thus we can treat cases (i) and (ii) from Table 2.2 without using the algorithm.

Remark 2.8.8. Note that for $p = 3$ and $p = 5$ we found that $\langle 1, \frac{1}{p}\mathrm{Tr}_{D_{2p}}\rangle$ is free over $\langle 1, \frac{1}{p}\mathrm{Tr}_G\rangle$ without the two being equal. We also found with the algorithm from [HJ20] that $\langle 1, \frac{1}{2}\mathrm{Tr}_{A_4}\rangle$, which does not come from a ring of integers, is free over $\langle 1, \frac{1}{2}\mathrm{Tr}_G\rangle$ (see §2.A.3).

Appendix

2.A Computer calculations

2.A.1 Determining freeness for S_4-extensions of $\mathbb{Q}_2$

Let $K/\mathbb{Q}$ be an S_4-extension with full decomposition group that is wildly ramified. Here we describe how to use the MAGMA implementation of [BJ08, Algorithm 3.1(6)] to check whether or not $\mathcal{O}_K$ is locally free at 2 over $\mathfrak{A}_{K/\mathbb{Q}}$, or equivalently, whether $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$, where $\mathfrak{P}$ is the unique prime of K above 2. We used the database [LMF19] to find six number fields, each of which has a completion at 2 equal to one of the six wildly ramified S_4-extensions of $\mathbb{Q}_2$ listed in the database of p-adic fields [JR06]. Note that two of these extensions of $\mathbb{Q}_2$ are weakly ramified, and so Corollary 2.7.2(ii) already shows that $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ in both cases, but we include them anyway as an additional check. The files `RelAlgKTheory.m` and `INB.m` referred to below are available on Werner Bley's website `https://www.mathematik.uni-muenchen.de/~bley/pub.php`

We refer to the sample file `sample.m` from the article [BJ08]. Note that here we use the updated file `INB.m` from [BJ11] rather than the original file `ao.m`.

```
Attach("RelAlgKTheory.m");
Attach("INB.m");
P<x> := PolynomialRing(IntegerRing());
Polynomials := [ x^6 + x^4 + x^2 - 1,
x^6 - x^4 + 3*x^2 - 1,
x^6 + 3*x^4 + 11*x^2 + 11,
x^6 + 7*x^4 + 15*x^2 + 11,
x^6 - x^4 - 2*x^3 - x^2 + 1,
x^6 - 2*x^5 + 2*x^4 - 4*x^3 + 4*x^2 - 2*x + 2 ];
for i in [1..6] do
  L := NormalClosure(NumberField(Polynomials[i]));
  G, Aut, h := AutomorphismGroup(L);
  h := map<Domain(h)->Codomain(h) | g:->h(g^-1)>;
  OL := MaximalOrder(L);
  theta := NormalBasisElement(OL, h);
  Ath := ComputeAtheta(OL, h, theta);
  QG := GroupAlgebra(Rationals(), G);
  AssOrd := ModuleConductor(QG, Ath, Ath);
  rho := RegularRep(QG);
```

```
  M := ZGModuleInit(Ath`hnf, rho);
  isfree, w := IsLocallyFree(QG, AssOrd, M, 2);
  if isfree then
    print "we have local freeness at 2";
  else
    print "we do not have local freeness at 2";
  end if;
end for;
we do not have local freeness at 2
we do not have local freeness at 2
we do not have local freeness at 2
we do not have local freeness at 2
we have local freeness at 2
we have local freeness at 2
```

2.A.2 Determining local freeness at 2 for S_4-extensions of $\mathbb{Q}$

Here we describe how to use to use the MAGMA implementation of [HJ20, §8.5] to show that for an S_4-extension $K/\mathbb{Q}$ we have that $\mathcal{O}_K$ is not locally free at 2 over $\mathfrak{A}_{K/\mathbb{Q}}$ if $K/\mathbb{Q}$ does not satisfy any of the conditions (i)–(iv) of Theorem 2.8.3 and $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$, where $\mathfrak{P}$ is a prime of K above 2 (see Table 2.1). Moreover, we also prove the freeness claim of Remark 2.8.5. The files `Iso.m`, `Lattices.m` and `Iso.spec` referred to below are contained in `Iso.zip`, available in the link to [HJ20] on Tommy Hofmann's website `https://www.thofma.com`

```
AttachSpec("Iso.spec");
G := Sym(4);
W2 := sub<G | G!(1, 3)>;
V2 := sub<G | G!(1, 3)(2, 4)>;
C4 := sub<G | G!(1, 2, 3, 4)>;
V4 := sub<G | G!(1, 3)(2, 4),(1, 2)(3, 4)>;
C22 := sub<G | G!(1, 3),(2, 4)>;
D8 := sub<G | G!(1, 2, 3, 4),(1, 3)>;
QG := GroupAlgebra(Rationals(), G);
trW2 := &+[ QG!h : h in W2];
trV2 := &+[ QG!h : h in V2];
trC4 := &+[ QG!h : h in C4];
trV4 := &+[ QG!h : h in V4];
trC22 := &+[ QG!h : h in C22];
trD8 := &+[ QG!h : h in D8];
trG := &+[ QG!h : h in G];
ZG := Order(Integers(), Basis(QG));
M1 := rideal< ZG | 1, trV2/2, trC4/4,trD8/8>;
A1 := rideal< ZG | 1, trV4/2, trG/8>;
IsLocallyIsomorphic(QG, BasisMatrix(M1), BasisMatrix(A1), 2);
false
M2 := rideal< ZG | 1, trV2/2, trV4/4,trD8/8>;
```

```
A2 := rideal< ZG | 1, trV4/4, trG/8>;
IsLocallyIsomorphic(QG, BasisMatrix(M2), BasisMatrix(A2), 2);
false
M3 := rideal< ZG | 1, trV2/2, trC22/4,trD8/8>;
IsLocallyIsomorphic(QG, BasisMatrix(M3), BasisMatrix(A1), 2);
false
M4 := rideal< ZG | 1, trV2/2, trC4/4>;
A4 := rideal< ZG | 1, trV4/2, trG/4>;
IsLocallyIsomorphic(QG, BasisMatrix(M4), BasisMatrix(A4), 2);
false
M5 := rideal< ZG | 1, trV2/2, trV4/4>;
A5 := rideal< ZG | 1, trV4/4>;
IsLocallyIsomorphic(QG, BasisMatrix(M5), BasisMatrix(A5), 2);
false
M6 := rideal< ZG | 1, trV2/2, trC22/4>;
IsLocallyIsomorphic(QG, BasisMatrix(M6), BasisMatrix(A4), 2);
false
M7 := rideal< ZG | 1, trW2/2, trC22/4>;
A7 := rideal< ZG | 1, trG/4>;
IsLocallyIsomorphic(QG, BasisMatrix(M7), BasisMatrix(A7), 2);
false
M8 := rideal< ZG | 1, trC22/2>;
A8 := rideal< ZG | 1, trG/2>;
IsLocallyIsomorphic(QG, BasisMatrix(M8), BasisMatrix(A8), 2);
false
M9 := rideal< ZG | 1, trV2/2>;
A9 := rideal< ZG | 1, trV4/2>;
IsLocallyIsomorphic(QG, BasisMatrix(M9), BasisMatrix(A9), 2);
false
M10 := rideal< ZG | 1, trW2/2>;
IsLocallyIsomorphic(QG, BasisMatrix(M10), BasisMatrix(A8), 2);
false
M11 := rideal< ZG | 1, trV4/4, trD8/8>;
A11 := rideal< ZG | 1, trV4/4, trG/8>;
IsLocallyIsomorphic(QG, BasisMatrix(M11), BasisMatrix(A11), 2);
true -31/4*Id(G) + (1, 4, 3, 2) + 5/4*(1, 3)(2, 4) - 5*(2, 3)
+ 5/4*(1, 2, 4) + 1/4*(1, 4, 3)+ (1, 3, 4, 2) + (2, 4, 3)+ (1, 4, 2, 3)
+ (1, 2, 3) + 5/4*(2, 3, 4) + 1/4*(1, 3, 2) + (2, 4) + 5/4*(1, 2)(3, 4)
+ 1/4*(1, 4)(2, 3)
```

2.A.3 Determining local freeness for A_5-extensions of $\mathbb{Q}$

Here we describe how to use the MAGMA implementation of [HJ20, §8.5] to check local freeness in A_5-extensions of $\mathbb{Q}$ at the wildly ramified primes (see Tables 2.2 and 2.3). Moreover, we also prove the second freeness claim of Remark 2.8.8. The files `Iso.m`, `Lattices.m` and `Iso.spec` referred to below are contained in `Iso.zip`, available in the link to [HJ20] on Tommy Hofmann's website `https://www.thofma.com`

When `IsLocallyIsomorphic(QG, BasisMatrix(M), BasisMatrix(A), 2)` is 'true', we suppress the full output, which includes an element $x \in \mathbb{Q}[G]$ such that $x(\mathbb{Z}_2 \otimes_{\mathbb{Z}} M) = \mathbb{Z}_2 \otimes_{\mathbb{Z}} A$ (whose existence is in our case equivalent to $\mathbb{Z}_2 \otimes_{\mathbb{Z}} M$ being free over $\mathbb{Z}_2 \otimes_{\mathbb{Z}} A$).

```
AttachSpec("Iso.spec");
G:=Alt(5);
C2 := sub<G | G!(1, 2)(3, 4)>;
C22 := sub<G | G!(1, 2)(3, 4),(1, 3)(2, 4)>;
C3 := sub<G | G!(1, 2, 3)>;
D6 := sub<G | G!(1, 2)(4, 5),(1, 2, 3)>;
C5 := sub<G | G!(1, 2, 3, 4, 5)>;
D10 := sub<G | G!(2 ,5)(3, 4),(1, 2, 3, 4, 5)>;
Alt4 := sub<G | G!(1 ,2)(3, 4),(1, 2, 3)>;
QG := GroupAlgebra(Rationals(), G);
trC2 := &+[ QG!h : h in C2];
trC22 := &+[ QG!h : h in C22];
trC3 := &+[ QG!h : h in C3];
trD6 := &+[ QG!h : h in D6];
trC5 := &+[ QG!h : h in C5];
trD10 := &+[ QG!h : h in D10];
trAlt4 := &+[ QG!h : h in Alt4];
trG := &+[ QG!h : h in G];
ZG := Order(Integers(), Basis(QG));
M1 := rideal< ZG | 1, trC2/2>;
A1 := rideal< ZG | 1, trG/2>;
IsLocallyIsomorphic(QG, BasisMatrix(M1), BasisMatrix(A1), 2);
false
M2 := rideal< ZG | 1, trC2/2, trC22/4>;
A2 := rideal< ZG | 1, trG/4>;
IsLocallyIsomorphic(QG, BasisMatrix(M2), BasisMatrix(A2), 2);
false
M3 := rideal< ZG | 1, trC22/2>;
IsLocallyIsomorphic(QG, BasisMatrix(M3), BasisMatrix(A1), 2);
false
M4 := rideal< ZG | 1, trC3/3>;
A4 := rideal< ZG | 1, trG/3>;
IsLocallyIsomorphic(QG, BasisMatrix(M4), BasisMatrix(A4), 3);
false
M5 := rideal< ZG | 1, trD6/3>;
IsLocallyIsomorphic(QG, BasisMatrix(M5), BasisMatrix(A4), 3);
true
M6 := rideal< ZG | 1, trC5/5>;
A6 := rideal< ZG | 1, trG/5>;
IsLocallyIsomorphic(QG, BasisMatrix(M6), BasisMatrix(A6), 5);
false
M7 := rideal< ZG | 1, trD10/5>;
IsLocallyIsomorphic(QG, BasisMatrix(M7), BasisMatrix(A6), 5);
```

```
true
M8 := rideal< ZG | 1, trAlt4/2>;
IsLocallyIsomorphic(QG, BasisMatrix(M8), BasisMatrix(A1), 2);
true
```

Chapter 3

On reduction steps for Leopoldt's conjecture

3.1 Introduction

The work in this chapter is joint with my PhD supervisor Henri Johnston and based on a rough draft of a joint paper.

Let p be a prime number and let K be a number field. It is known that the regulator of K does not vanish. In analogy to this, Leopoldt [Leo62] conjectured that a certain p-adic regulator associated to K and p does not vanish. Due to supporting evidence in its favour and consequences for other conjectures in algebraic number theory, Leopoldt's conjecture has been widely studied and is of great interest.

As explained in [Was97, §5.5] and [NSW08, Chapter X §3], Leopoldt's conjecture, $\mathrm{Leo}(K,p)$ for short, has many different formulations. One of these is as follows. Let K be a number field. For a finite place w of K, let U_{K_w} denote the group of units of the completion K_w and let $U^1_{K_w}$ denote the subgroup of principal units. Let $S_p(K)$ denote the set of places of K above p. For $w \in S_p(K)$, the inclusion $U^1_{K_w} \subseteq U_{K_w}$ induces an isomorphism with the p-adic completion: $U^1_{K_w} \cong \hat{U}_{K_w}$. Therefore, after taking p-adic completions, the diagonal embedding $\mathcal{O}_K^\times \hookrightarrow \prod_{w\in S_p(K)} U_{K_w}$ gives rise to a canonical homomorphism

$$\lambda_{K,p} : \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \longrightarrow \prod_{w\in S_p(K)} U^1_{K_w}. \tag{3.1.1}$$

Leopoldt's conjecture $\mathrm{Leo}(K,p)$ predicts that $\lambda_{K,p}$ is injective.

One of the first important results concerning Leopoldt's conjecture is the following.

Theorem 3.1.1. *[Ax65],[Bru67] Let K be a finite abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field. Then $\mathrm{Leo}(K,p)$ holds for every prime number p.*

Ax reduced the theorem to the fact that the p-adic logarithms of algebraic elements over $\mathbb{Q}$ are $\mathbb{Q}$-independent if and only if they are $\overline{\mathbb{Q}}$-independent, where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}_p$. This is the p-adic analogue of a result by Baker and was proved by Brumer, who therefore completed the proof of Leopoldt's conjecture for abelian extensions of $\mathbb{Q}$ and of imaginary quadratic fields.

Now let L/K be a Galois extension of number fields with Galois group G, and let us fix a prime number p. Several authors (e.g. [Miy82], [EKW84], [Kli90], [Lau89]) already observed that in this case the map $\lambda_{L,p}$ is a map of $\mathbb{Z}_p[G]$-modules, so that the object of our study is the $\mathbb{Z}_p[G]$-module $\ker \lambda_{L,p}$, whose vanishing is equivalent to Leopoldt's conjecture. One strategy is therefore to study the structure of the $M[G]$-module $M \otimes_{\mathbb{Z}_p} \ker \lambda_{L,p}$ for a certain extension $M/\mathbb{Q}_p$ (e.g. $\mathbb{Q}_p$ or $\mathbb{C}_p$). The aforementioned authors used the known $\mathbb{Q}[G]$-structure of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$ when the base field K is $\mathbb{Q}$ or an imaginary quadratic field, which comes from the existence of Minkowski units, to estimate the size of isotypical components of $M \otimes_{\mathbb{Z}_p} \mathrm{im} \lambda_{L,p}$ in order to prove that the isotypical components of $M \otimes_{\mathbb{Z}_p} \ker \lambda_{L,p}$ are zero.

Here we approach the problem from a different point of view. Note that for every prime number p Leopoldt's conjecture at p for a number field implies Leopoldt's conjecture at p for all of its subfields (see Lemma 3.2.6). Now let L/K be a Galois extension of number fields with Galois group G; our purpose is instead to deduce Leopoldt's conjecture at p for L from the validity for some of the intermediate fields of L/K. The key observation is that if H is a subgroup of G then $(\ker \lambda_{L,p})^H = \ker \lambda_{L^H,p}$, where L^H is the field fixed by H and $(\ker \lambda_{L,p})^H$ is the submodule fixed by H, so that if $\ker \lambda_{L^H,p} = 0$ at least one 'component' of $\ker \lambda_{L,p}$ is trivial. The existence of a collection of subgroups $\mathcal{H}$ such that $\ker \lambda_{L,p}$ vanishes if and only if $(\ker \lambda_{L,p})^H$ vanishes for every $H \in \mathcal{H}$ is linked to the existence of a *norm relation*, a property which only depends on G as an abstract group. In §3.3.2 we will review some basic properties of norm relations, which have also been studied by many authors including those in [BFHP22], and show their consequences for equivariant maps and in particular, in §3.4, for Leopoldt's conjecture.

The following result can be proved using norm relations, but in fact also admits a proof just using character theory (see Theorem 3.4.4).

Theorem 3.1.2. *Let L/K be a Galois extension of number fields with Galois group G. Let p be a prime number. If* $\mathrm{Leo}(L^H, p)$ *holds for every subgroup H of G which is the kernel of an irreducible complex character, then also* $\mathrm{Leo}(L, p)$ *holds.*

Note that the statement of Theorem 3.1.2 is non-tautological only when G has no faithful irreducible complex characters: if χ is a faithful irreducible complex character, then by definition χ has trivial kernel and $L^{\ker \chi} = L$.

Corollary 3.1.3. *Let L/K be an abelian extension of number fields. Let p be a prime number. If* $\mathrm{Leo}(F, p)$ *holds for every intermediate field F such that F/K is cyclic, then also* $\mathrm{Leo}(L, p)$ *holds.*

An advantage of using norm relations is that we may combine the consequences derived from their existence to already known results, e.g. from Theorem 3.1.1, and this permits us to study for instance Frobenius groups. One of the consequences is the following result, which is a special case of Corollary 3.4.6.

Theorem 3.1.4. *Let ℓ be an odd prime number and let L/K be a dihedral extension of degree 2ℓ, where K is $\mathbb{Q}$ or an imaginary quadratic field. Let p be a prime number. If* $\mathrm{Leo}(F, p)$ *holds for one (indeed, every) intermediate field F such that $[F : K] = \ell$, then we also have* $\mathrm{Leo}(L, p)$.

Note that none of the results in this chapter depend on the $\mathbb{Q}[G]$-structure of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$,

so that we can obtain in a simpler way some of the results in the literature just knowing basic facts such as Leopoldt's conjecture for abelian extensions of $\mathbb{Q}$. We also remark that in deducing $\mathrm{Leo}(L,p)$ from $\mathrm{Leo}(L^H,p)$ for some subgroups H of G we do not require any assumption on the base field K.

We recall that $\delta(L,p) := \mathrm{rank}_{\mathbb{Z}_p} \ker \lambda_{L,p}$ denotes the Leopoldt defect, which is trivial if and only if $\mathrm{Leo}(L,p)$ holds. In a slightly different approach, using Brauer relations and tools from works such as [Glu81], we are able to prove the following, which is Corollary 3.5.23.

Theorem 3.1.5. *Let L/K be a Galois extension of number fields with Galois group G and let p be a prime number. Let H be a non-cyclic subgroup of G. Then we have the relation*

$$\sum_{I \leq H} |I| \mu(I,H) \delta(L^I,p) = 0,$$

where $\mu(I,H) := \sum_{I=H_0 \lneq \cdots \lneq H_n = H} (-1)^n$.

We will see also that these relations recover the results we obtained via scalar norm relations, which are a particular type of norm relation. For instance, let L/K be an S_3-extension of number fields and let us denote by F one of the intermediate cubic extensions of K and by M the intermediate quadratic field. A consequence of Theorem 3.1.5 is that for every prime number p we have the relation

$$\delta(L,p) + 2\delta(K,p) = \delta(M,p) + 2\delta(F,p).$$

Therefore, if $\delta(M,p) = \delta(F,p) = 0$, then $\delta(L,p) = 0$.

With character theory and our general idea of looking at appropriate intermediate fields we also obtain the following result (see Theorem 3.6.1).

Theorem 3.1.6. *Let L be a finite Galois extension of $\mathbb{Q}$ or of an imaginary quadratic field with Galois group G. Let p be a prime number. Let $1 < d_1 < \cdots < d_s$ be the dimensions of the non-linear irreducible complex characters of G. Then we can write $\delta(L,p) = \sum_{i=1}^{s} k_i d_i$ with coefficients $k_i \in \mathbb{N}$. In particular either $\delta(L,p) = 0$ or $\delta(L,p) \geq d_1 > 1$.*

Using different methods, Khare and Wintenberger proved the following special case of Theorem 3.1.6.

Corollary 3.1.7. *Let $F/\mathbb{Q}$ be a totally real finite Galois extension. Then for every prime p we have $\delta(F,p) \neq 1$.*

In §3.7 we will apply techniques developed by Buchmann and Sands [BS88] to prove Leopoldt's conjecture for an infinite family of totally real non-Galois cubic fields. Combined with Theorem 3.1.4, this will permit us to show that, for every prime p, there is an infinite family of totally real S_3-extensions of $\mathbb{Q}$ which satisfy Leopoldt's conjecture at p. As far as we know no one ever found a non-abelian finite group G, a rational prime p and an infinite family of G-extensions of $\mathbb{Q}$ such that Leopoldt's conjecture at p holds for the whole family. We will use two different approaches: for certain families we can prove Leopoldt's conjecture at the primes different from 3 dividing the linear

coefficients of their defining polynomials; or alternatively, show with a continuity principle that the validity of Leopoldt's conjecture for the whole family descends from the validity for just one basic example. We will see also that the latter strategy applies for some D_8-extensions as well.

For instance we will prove the following, which is Theorem 3.7.12.

Theorem 3.1.8. *Let $\mathcal{A}$ be a finite set of prime numbers. Then there exists an infinite family $\mathcal{L}$ of real S_3-extensions of $\mathbb{Q}$ such that* Leo(L,p) *holds for every $L \in \mathcal{L}$ and $p \in \mathcal{A}$.*

3.2 Review of Leopoldt's conjecture

In this section, we review material concerning Leopoldt's conjecture, the Leopoldt kernel and Leopoldt defects; see also [NSW08, Chapter X, §3] or [Was97, §5.5].

3.2.1 Leopoldt's conjecture

Let p be a prime. For an abelian group A, let

$$\hat{A} := \varprojlim_n A/p^n A$$

be the p-adic completion of A. Observe that $\hat{A}$ is a $\mathbb{Z}_p$-module in a natural way. Moreover, $\hat{A} = \mathbb{Z}_p \otimes_{\mathbb{Z}} A$ if A is a finitely generated $\mathbb{Z}$-module and $\hat{A} = A$ if A is a finitely generated $\mathbb{Z}_p$-module.

Let K be a number field. For a finite place w of K, let U_{K_w} denote the group of units of the completion K_w and let $U^1_{K_w}$ denote the subgroup of principal units. Let $S_p(K)$ denote the set of places of K above p. For $w \in S_p(K)$, the inclusion $U^1_{K_w} \subseteq U_{K_w}$ induces an isomorphism $U^1_{K_w} \cong \hat{U}_{K_w}$. Therefore, after taking p-adic completions, the diagonal embedding $\iota : \mathcal{O}_K^\times \hookrightarrow \prod_{w \in S_p(K)} U_{K_w}$ gives rise to a canonical homomorphism

$$\lambda_{K,p} : \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \longrightarrow \prod_{w \in S_p(K)} U^1_{K_w}. \tag{3.2.1}$$

We say that Lepoldt's conjecture Leo(K,p) holds if $\lambda_{K,p}$ is injective. There are various formulations of Leopoldt's conjecture, for instance see [NSW08, Theorem 10.3.6].

The most important result on Leopoldt's conjecture to date is the following.

Theorem 3.2.1. *If K is a finite abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field then* Leo(K,p) *holds for all primes p.*

Proof. Ax [Ax65] reduced the assertion to a p-adic version of Baker's theorem, which was proved by Brumer [Bru67] (see also [NSW08, Theorem 10.3.16]). □

3.2.2 The Leopoldt Kernel and Leopoldt defect

In this subsection we define some important quantities we will use extensively in the rest of the chapter.

Definition 3.2.2. Let K be a number field and let p be a prime. We define the *Leopoldt kernel* to be $\ker \lambda_{K,p}$, where $\lambda_{K,p}$ is the map defined in (3.2.1). The *Leopoldt defect* $\delta(L,p)$ is defined to be $\operatorname{rank}_{\mathbb{Z}_p} \ker \lambda_{K,p}$.

Note that Leopoldt's conjecture states that the Leopoldt kernel is trivial. We will now show that this is equivalent to saying that the Leopoldt defect is zero.

We set

$$\Lambda_{K,p} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \lambda_{K,p} : \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \longrightarrow \prod_{w \in S_p(K)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{K_w}.$$

Proposition 3.2.3. *Let K be a number field and let p be a prime. We have that $\lambda_{K,p}$ is injective when restricted to the $\mathbb{Z}_p$-torsion submodule of the domain. Moreover, for any field extension $M/\mathbb{Q}_p$, we have*

$$\operatorname{rank}_{\mathbb{Z}_p} \ker \lambda_{K,p} = \dim_M (M \otimes_{\mathbb{Q}_p} \ker \Lambda_{K,p}). \tag{3.2.2}$$

Proof. Note that for every $w \in S_p(K)$ we have $U_{K_w} \cong \langle \zeta_{p^f-1} \rangle \times U^1_{K_w}$, where f is the inertia degree of $K_w/\mathbb{Q}_p$, ζ_{p^f-1} is a primitive (p^f-1)th root of unity and $\langle \zeta_{p^f-1} \rangle$ is the group of roots of unity in K_w of order coprime to p. Let ι be the aforementioned diagonal embedding of units and let

$$\iota' : \mathcal{O}_K^\times \longrightarrow \prod_{w \in S_p(K)} U^1_{K_w}$$

be the map into the completion of the codomain. We will prove that $\ker \iota'$ is the group of roots of unity in K of order coprime to p. Let $x \in \ker \iota'$. Then, fixing a prime w of K above p, $x = \zeta^a_{p^f-1} \cdot y$ in K_w with $y \in U^1_{K_w}$. Since the w-component of $\iota'(x)$ is y, we must have $y = 1$ and so $x \in K \subseteq K_w$ is a root of unity of order coprime to p. The other inclusion is trivial. This easily implies that $\lambda_{K,p}$ is injective on the $\mathbb{Z}_p$-torsion submodule of $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^\times$. Therefore $\ker \lambda_{K,p}$ is a free $\mathbb{Z}_p$-module of finite rank and (3.2.2) follows easily. □

Corollary 3.2.4. *Let K be a number field and let p be a prime. Then $\lambda_{K,p}$ is injective if and only if $\Lambda_{K,p}$ is injective if and only if $\delta(K,p) = 0$.*

Remark 3.2.5. Note that, by Dirichlet's unit theorem, the rank of the domain of $\lambda_{K,p}$ is $r_1 + r_2 - 1$, where r_1 and r_2 denote the number of real and (conjugate pairs of) complex embeddings of K, respectively. Hence we have Leopoldt's conjecture if and only if the image of $\lambda_{K,p}$ has rank $r_1 + r_2 - 1$ (in other words, if the p-adic rank is equal to the rank of the global units); in particular note that we always have $\delta(K,p) \leq r_1 + r_2 - 1$. We will soon see that a much better bound holds.

The following two lemmas are well known. We include their proofs for the convenience of the reader.

Lemma 3.2.6. *Let L/K be an extension of number fields and let p be a prime number. Then $\delta(K,p) \leq \delta(L,p)$. In particular,* $\mathrm{Leo}(L,p) \Rightarrow \mathrm{Leo}(K,p)$.

Proof. We have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times & \xrightarrow{\lambda_{L,p}} & \prod_{w \in S_p(L)} U_{L_w}^1 \\ \uparrow & & \uparrow \\ \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^\times & \xrightarrow{\lambda_{K,p}} & \prod_{v \in S_p(K)} U_{K_v}^1, \end{array} \tag{3.2.3}$$

where the vertical arrows are induced by (diagonal) immersions of units and are injective. Hence the left-hand immersion induces a containment $\ker \lambda_{K,p} \subseteq \ker \lambda_{L,p}$. The conclusion follows. □

Definition 3.2.7. A *CM*-field is a totally imaginary number field which is a quadratic extension of a totally real number field.

Lemma 3.2.8. *Let L be a CM-field and let L^+ be its maximal totally real subfield. Then for every prime number p we have $\delta(L,p) = \delta(L^+,p)$. In particular,* $\mathrm{Leo}(L,p) \Leftrightarrow \mathrm{Leo}(L^+,p)$.

Proof. We will prove that $\mathrm{rank}_{\mathbb{Q}_p} \ker \Lambda_{L,p} = \mathrm{rank}_{\mathbb{Q}_p} \ker \Lambda_{L^+,p}$. Since the unit groups $\mathcal{O}_L^\times$ and $\mathcal{O}_{L^+}^\times$ have the same $\mathbb{Z}$-rank, in the following diagram

$$\begin{array}{ccc} \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times & \xrightarrow{\Lambda_{L,p}} & \prod_{w \in S_p(L)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U_{L_w}^1 \\ \wr\uparrow & & \uparrow \\ \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L^+}^\times & \xrightarrow[\Lambda_{L^+,p}]{} & \prod_{v \in S_p(L^+)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U_{L^+_v}^1 \end{array}$$

the inclusion on the left is an isomorphism. Hence we obtain an identification between $\ker \Lambda_{L^+,p}$ and $\ker \Lambda_{L,p}$. □

From Theorem 3.2.1 and Lemma 3.2.8 we deduce the following well-known result.

Corollary 3.2.9. *Let L be a CM-field whose maximal totally real subfield is abelian over $\mathbb{Q}$. Then we have* $\mathrm{Leo}(L,p)$ *for every prime number p.*

Remark 3.2.10. Note that Corollary 3.2.9 covers cases where L is not itself abelian over $\mathbb{Q}$. For instance we can apply the result if L is a CM Q_8 or D_8-extension of $\mathbb{Q}$.

Remark 3.2.11. Let K be a number field with number of real and (conjugate pairs of) complex places denoted by r_1 and r_2, respectively. Note that whenever $r_1 + r_2 \leq 2$ we have Leopoldt's conjecture at every prime p: if $r_1 + r_2 = 1$ then K is $\mathbb{Q}$ or an imaginary quadratic field, otherwise there exists a global unit which is not a root of unity, which has non-trivial image under $\lambda_{K,p}$ (see the proof of Proposition 3.2.3). This argument also shows that the defect can never be as big as $r_1 + r_2 - 1$.

A classical bound on the defect of any number field is due to Waldschmidt.

Theorem 3.2.12. *[Wal81] Let L be a number field and let p be a prime number. Let r_1 and r_2 be the number of real and (conjugate pairs of) complex embeddings of L, respectively. Then $\delta(L,p) \leq \frac{r_1+r_2-1}{2}$.*

This tells us that Leopoldt's conjecture is at least "half way" to being true.

Waldschmidt's result has recently been generalised.

Theorem 3.2.13. *[Mak22, Theorem 1.1] Let L/K be an extension of number fields and let p be a rational number. Then*

$$\delta(L,p) \leq \delta(K,p) + \frac{r_1(L) + r_2(L) - r_1(K) - r_2(K)}{2}.$$

3.2.3 The Leopoldt kernel as a Galois module

Let L/K be a finite Galois extension of number fields and let $G = \mathrm{Gal}(L/K)$. For a subgroup $H \leq G$, let L^H be the subfield fixed of L by H. Let p be a prime number.

The following result is well known to experts. We include the proof for convenience of the reader.

Lemma 3.2.14. *The map $\lambda_{L,p}$ is a homomorphism of $\mathbb{Z}_p[G]$-modules.*

Proof. Since $\mathcal{O}_L^\times$ is a $\mathbb{Z}[G]$-module, it follows easily that $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$ is a $\mathbb{Z}_p[G]$-module. For a finite place v of K, let $S_v(L)$ denote the places of L above v. Then for each v, we have a canonical isomorphism $L \otimes_K K_v \cong \prod_{w \in S_v(L)} L_w$ of $K_v[G]$-modules. From this, it is straightforward to verify that $\prod_{w \in S_p(L)} U^1_{L_w} = \prod_{v \in S_p(K)} \prod_{w \in S_v(L)} U^1_{L_w}$ inherits the structure of a $\mathbb{Z}_p[G]$-module and that $\lambda_{L,p}$ is G-equivariant. □

It follows immediately that $\Lambda_{L,p}$ is a homomorphism of $\mathbb{Q}_p[G]$-modules and thus $\ker \Lambda_{L,p}$ is also a $\mathbb{Q}_p[G]$-module. For a subgroup $H \leq G$, let $N_H = \sum_{h \in H} h$ denote the associated norm element (note that here we deviate from the notation in §2, where we would have used the notation Tr_H) and for a $\mathbb{Q}_p[G]$-module M, note that

$$N_H M = M^H := \{m \in M \mid hm = m \text{ for all } h \in H\}.$$

Lemma 3.2.15. *Let H be a subgroup of G. Then*

(i) $(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times)^H = \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L^H}^\times$,

(ii) $\left(\prod_{w \in S_p(L)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{L_w}\right)^H = \prod_{t \in S_p(L^H)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{L_t^H}$, *and*

(iii) $(\ker \Lambda_{L,p})^H = \ker \Lambda_{L^H,p}$.

Proof. We will first establish (i). Let $u \in \mathcal{O}_L^\times$; then $N_H u = N_{L/L^H}(u) \in \mathcal{O}_{L^H}^\times$, where we denote by N_{L/L^H} the field norm. Tensoring with $\mathbb{Q}_p$, we obtain that

$$(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times)^H = N_H(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times) \subseteq \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L^H}^\times.$$

On the other hand, it is clear that an element of $\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L^H}^\times$ is fixed by H.

In an analogous way, using the action of H on the set of primes $w \in S_p(L)$ above each $t \in S_p(L_H)$ we obtain (ii) (note that we are using the diagonal embedding of $\prod_{t \in S_p(L^H)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{L_t^H}$ into $\prod_{w \in S_p(L)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{L_w}$).

By the commutative diagram (3.2.3) applied with $K = L^H$, we see that the composition of $\lambda_{L^H,p}$ with the injection $\prod_{t\in S_p(L_H)} U^1_{L_t^H} \hookrightarrow \prod_{w\in S_p(L)} U^1_{L_w}$ corresponds to applying directly $\lambda_{L,p}$, and analogously if we tensor with $\mathbb{Q}_p$. Using the already proved statements (i) and (ii), under the above identification we can see $\Lambda_{L^H,p}$ as the map

$$(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times)^H \longrightarrow \left(\prod_{w\in S_p(L)} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U^1_{L_w}\right)^H$$

obtained by restricting $\Lambda_{L,p}$ to $(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times)^H \subseteq \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$. The conclusion (iii) now follows easily. □

3.3 Triviality of modules over group algebras

Let G be a finite group and let K be a field of characteristic 0. For a subgroup $H \leq G$, let $N_H = \sum_{h\in H} h$ denote the associated norm element. Note that $e_H := |H|^{-1}N_H$ is an idempotent in the group algebra $K[G]$ and is central if and only if H is normal in G. For a $K[G]$-module M, we have

$$e_H M = N_H M = M^H := \{m \in M \mid hm = m \text{ for all } h \in H\}.$$

In this section, we give criteria for the vanishing of a $K[G]$-module M in terms of the vanishing of $e_H M$ for certain subgroups $H \leq G$.

3.3.1 Characters and central idempotents

Let $\mathrm{Irr}_K(G)$ denote the set of characters attached to finite-dimensional K-valued irreducible representations of G. For each character χ, we will denote by $\ker\chi$ the elements of G that map to $\chi(1)$ through χ. For $\chi \in \mathrm{Irr}_K(G)$, let $e_\chi = |G|^{-1}\chi(1)\sum_{g\in G}\chi(g^{-1})g$ denote the central primitive idempotent of G attached to χ.

Proposition 3.3.1. *Let M be a $K[G]$-module. Then the following are equivalent.*

(i) $M = 0$.

(ii) $L \otimes_K M = 0$ *for any field extension* L/K.

(iii) $e_\chi M = 0$ *for all* $\chi \in \mathrm{Irr}_K(G)$.

(iv) $e_{\ker\chi} M = 0$ *for all* $\chi \in \mathrm{Irr}_K(G)$.

(v) $e_{\ker\chi} M = 0$ *for all* $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$.

Proof. The equivalence of (i) and (ii) is clear. The equivalence of (i) and (iii) follows immediately from the decomposition of $K[G]$-modules

$$K[G] = \bigoplus_{\chi\in\mathrm{Irr}_K(G)} e_\chi K[G].$$

We have that (iv) implies (iii) since $e_\chi e_{\ker\chi} = e_\chi$ for each $\chi \in \mathrm{Irr}_K(G)$. Moreover, it is clear that (i) implies (iv). The equivalence of (iv) and (v) follows easily from the

equivalence of (i) and (ii) and the fact that $\{\ker\chi \mid \chi \in \mathrm{Irr}_L(G)\}$ is the same for any field extension L/K such that L contains an algebraic closure of K. □

Corollary 3.3.2. *Suppose that G has no faithful complex irreducible character and let M be a $K[G]$-module. Then $M = 0$ if and only if $e_N M = 0$ for every proper normal subgroup $N \leq G$.*

Remark 3.3.3. If G has a faithful complex irreducible character then its centre $\mathcal{Z}(G)$ must be cyclic; moreover, the converse holds if G is nilpotent, as originally proved in [Fit06] (see also [Isa94, Theorem (2.32), Problem (5.25)]).

Corollary 3.3.4. *Suppose that G is a finite abelian group and let M be a $K[G]$-module. Then $M = 0$ if and only if $e_N M = 0$ for every subgroup $N \leq G$ with cyclic quotient.*

Proof. The non-trivial implication follows from Proposition 3.3.1 since $G/\ker\chi$ is cyclic for all $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$. □

3.3.2 Norm relations

Norm relations have been considered, either implicitly or explicitly, in numerous articles, including [BFHP22], [Bol97], [KR94], [KR89], [MZ87], [Kan85] and [Acc70]. We shall discuss the connection with Brauer relations in §3.5.

Definition 3.3.5. Let $\mathcal{H}$ be a set of non-trivial subgroups of G. A *norm relation* with respect to $\mathcal{H}$ is an equality of the form

$$1 = \sum_{H\in\mathcal{H}} e_H r_H \tag{3.3.1}$$

with $r_H \in \mathbb{Q}[G]$. It is said to be a *scalar norm relation* if $r_H \in \mathbb{Q}$ for all $H \in \mathcal{H}$.

Remark 3.3.6. Definition 3.3.5 is taken from [BFHP22, Definition 2.1], but with two differences. First, we specialise to the case of coefficients in $\mathbb{Q}$. Second, in loc. cit. a norm relation is defined to be of the form

$$1 = \sum_{H\in\mathcal{H}} s_H e_H r_H \tag{3.3.2}$$

with $s_H, r_H \in \mathbb{Q}[G]$. This is essentially equivalent to our definition since $ge_H = e_{gHg^{-1}}g$ for all $g \in G$. The difference is that (3.3.2) allows one to choose $\mathcal{H}$ such that it contains at most one representative of $\{gHg^{-1} : g \in G\}$ for each $H \leq G$, whereas writing all the coefficients r_H on the right as in (3.3.1) is more convenient for our purposes.

Proposition 3.3.7. *Let M be a $K[G]$-module and suppose that G has a norm relation with respect to a set of non-trivial subgroups $\mathcal{H}$. Then $M = 0$ if and only if $e_H M = 0$ for every $H \in \mathcal{H}$.*

Proof. By hypothesis there exists a norm relation of the form $1 = \sum_{H\in\mathcal{H}} e_H r_H$. Suppose that $e_H M = 0$ for every $H \in \mathcal{H}$. Let $x \in M$. Then for every $H \in \mathcal{H}$ we have $e_H r_H x \in e_H M = 0$, so $x = 1 \cdot x = \sum_{H\in\mathcal{H}} e_H r_H x = 0$ and hence $M = 0$. The converse is trivial. □

For $g \in G$ and $H \leq G$, let $H^g = gHg^{-1}$. Note that this is a left action, that is, $(H^{g_1})^{g_2} = H^{g_2 g_1}$ for $g_1, g_2 \in G$. Moreover, we have $ge_H g^{-1} = e_{H^g}$.

Corollary 3.3.8. *Let M be a $K[G]$-module and suppose that G has a norm relation with respect to a set of non-trivial subgroups $\mathcal{H}$. Let $\mathcal{I} \subseteq \mathcal{H}$ be such that for every $H \in \mathcal{H}$ there exist $I \in \mathcal{I}$ and $g \in G$ such that $I^g \subseteq H$. Then $M = 0$ if and only if $e_I M = 0$ for every $I \in \mathcal{I}$.*

Proof. Suppose that $e_I M = 0$ for every $I \in \mathcal{I}$. Let $H \in \mathcal{H}$. Let $g \in G$ and let $I \in \mathcal{I}$ such that $I^g \subseteq H$. Then

$$e_H = \left(\frac{1}{[H : I^g]} \sum_{h \in H/I^g} h \right) g e_I g^{-1},$$

where $\sum_{h \in H/I^g}$ denotes the sum over any set of left coset representatives of I^g in H. Let $x \in M$. Then $e_I g^{-1} x \in e_I M = 0$ and so $e_H x = 0$. Thus $e_H M = 0$. Therefore $e_H M = 0$ for all $H \in \mathcal{H}$, and so $M = 0$ by Proposition 3.3.7. The converse is trivial. □

Remark 3.3.9. Corollaries 3.3.2 and 3.3.4 can both be proved using norm relations, but it is easier and arguably more illuminating to give direct proofs.

3.3.3 Frobenius groups

For further background material on Frobenius groups, including the proof of Theorem 3.3.11 below, we refer the reader to [CR81, §14A].

Definition 3.3.10. A *Frobenius group* is a finite group G with a proper non-trivial subgroup H such that $H \cap H^g = \{1\}$ for all $g \in G \setminus H$, in which case H is called a *Frobenius complement*.

Theorem 3.3.11 (Frobenius)**.** *Let G be a Frobenius group with Frobenius complement H. Then G contains a unique normal subgroup N, called the* Frobenius kernel*, such that $G = NH$ and $N \cap H = \{1\}$.*

Proposition 3.3.12. *Let $G \cong N \rtimes H$ be a Frobenius group. Then the following hold:*

(i) $|N|$ and $|H|$ are coprime;

(ii) every normal subgroup of G either contains or is contained in N;

(iii) for every $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ such that $N \not\subseteq \ker \chi$ we have $\chi = \mathrm{Ind}_N^G \psi$, where $\mathbf{1}_N \neq \psi \in \mathrm{Irr}_{\mathbb{C}}(N)$ (see §3.5.1 for notation in character theory); moreover, all characters of G of this type are irreducible.

Example 3.3.13. Let A be a nontrivial finite abelian group of odd order and let C_2 act on A by inversion. Then the semidirect product $G = A \rtimes C_2$ is a Frobenius group with Frobenius kernel A. In particular, if n is odd then one can take $G = D_{2n}$ and $A = G' \cong C_n$, the subgroup of rotations.

Example 3.3.14. Let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. The group $\mathrm{Aff}(q)$ of affine transformations on $\mathbb{F}_q$ is the group of transformations of the

form $x \mapsto ax + b$ with $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Let $G = \mathrm{Aff}(q)$ and let $N = \{x \mapsto x + b \mid b \in \mathbb{F}_q\}$. Then G is a Frobenius group with Frobenius kernel $N = G' \cong \mathbb{F}_q$ and is isomorphic to the semidirect product $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$ with the natural action. In particular, $\mathrm{Aff}(3) \cong S_3$ and $\mathrm{Aff}(4) \cong A_4$.

Proposition 3.3.15. *Let $G \cong N \rtimes H$ be a Frobenius group with kernel N and complement H. Then G has a scalar norm relation of the form*

$$1 = e_N + \sum_{g \in N} \frac{|H|}{|N|} e_{H^g} - |H| e_G.$$

Proof. This result can be deduced from [Kan85, Remark, p. 324], for example, but we give a direct proof for the convenience of the reader. From the definition of Frobenius complement it follows that $H = H^g$ if and only if $g \in H$. Hence there are $|N|$ distinct subgroups of the form H^g, one for each $g \in N$. Therefore the subgroups N and H^g for $g \in N$ intersect pairwise trivially and by counting elements we obtain

$$G = N \sqcup \bigsqcup_{g \in N} \left(H^g \setminus \{1\}\right),$$

where $\sqcup$ denotes disjoint union. Summing over both sides gives the second equality of

$$|G| e_G = \sum_{g \in G} g = \sum_{n \in N} n + \sum_{g \in N} \sum_{h' \in H^g} h' - |N| = |N| e_N + \sum_{g \in N} |H| e_{H^g} - |N|,$$

and so the desired result follows by multiplying through by $|N|^{-1}$ and rearranging. □

Corollary 3.3.16. *Let $G \cong N \rtimes H$ be a Frobenius group with kernel N and complement H. Let M be a $K[G]$-module. Then $M = 0$ if and only if $e_N M = e_H M = 0$.*

Proof. This follows from Proposition 3.3.15 combined with Corollary 3.3.8. □

3.3.4 Norm relations in a general setting

We list some norm relations that we always have in general. For the convenience of the reader we include the proofs.

Lemma 3.3.17. *[Acc70, Theorem 1][Kan85, Corollary 1] Let G be a finite group and let $\{H_i\}_{i \in 1,\ldots,t}$ be subgroups such that $G = H_1 \cup \ldots \cup H_t$. Then*

$$|G| e_G = \sum_{s=1}^{t} (-1)^{s+1} \sum_{1 \le i_1 \le \cdots \le i_s \le t} |H_{i_1} \cap \ldots \cap H_{i_s}| e_{H_{i_1} \cap \ldots \cap H_{i_s}}.$$

Proof. By the inclusion-exclusion principle, each $g \in G$ appears with coefficient 1 in the expression

$$\sum_{s=1}^{t} (-1)^{s+1} \sum_{1 \le i_1 < \cdots < i_s \le t} \sum_{h \in H_{i_1} \cap \cdots \cap H_{i_s}} h,$$

which is therefore equal to $\sum_{g \in G} g$. This is what we needed to prove. □

Remark 3.3.18. Note that Lemma 3.3.17 can be used to prove Proposition 3.3.15 (where the subgroups have pariwise trivial intersection).

Lemma 3.3.19. *[Kan85, Corollary 2] Let G be a finite group and let $\{H_i\}_{i\in 1,\dots,t}$ be subgroups such that $H_iH_j = H_jH_i$ for every i, j, where H_iH_j denotes the set of products of elements of H_i with elements of H_j, and such that for each $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ there exists i such that $H_i \subseteq \ker\chi$. Then $H_{i_1}\cdots H_{i_s}$ is a subgroup of G for every $1 \le i_1 \le \cdots \le i_s \le t$ and*

$$1 = \sum_{s=1}^{t}(-1)^{s+1} \sum_{1\le i_1\le\cdots\le i_s\le t} e_{H_{i_1}\cdots H_{i_s}}.$$

Proof. Let $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ and let H_i be such that $H_i \subseteq \ker\chi$. Then $e_\chi(1 - e_{H_i}) = 0$. For every i and j in $\{1, ..., t\}$ note that from the hypothesis of commutation H_iH_j is a subgroup of G, isomorphic to a quotient of $H_i \times H_j$ via the natural projection. From this we can easily deduce that the idempotents e_{H_i} commute, as $e_{H_i}e_{H_j} = e_{H_iH_j} = e_{H_jH_i} = e_{H_j}e_{H_i}$. This implies that $e_\chi\prod_{i=1}^{t}(1 - e_{H_i}) = 0$. As this is true for every $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$, then we obtain $\prod_{i=1}^{t}(1 - e_{H_i}) = 0$ by Proposition 3.3.1(iii). As above we can verify that $H_{i_1}\cdots H_{i_s}$ is a subgroup of G for every $1 \le i_1 \le \cdots \le i_s \le t$ and $e_{H_{i_1}\cdots H_{i_s}} = e_{H_{i_1}}\cdots e_{H_{i_s}}$, which leads to the conclusion. □

Remark 3.3.20. Note that Lemma 3.3.19 can be used to prove Corollary 3.3.2.

3.3.5 Characterisation of finite groups that admit norm relations

Theorem 3.3.21. *[BFHP22, Theorem 2.11] A finite group G admits a norm relation if and only if G contains either* (i) *a non-cyclic subgroup of order $\ell_1\ell_2$, where ℓ_1 and ℓ_2 are two not necessarily distinct primes, or* (ii) *a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)$, where $\ell = 2^{2^k} + 1$ is a Fermat prime with $k > 1$.*

Remark 3.3.22. As we shall see in Theorem 3.5.9, finite groups admitting a *scalar* norm relation are precisely those containing a subgroup of type (i). Hence we can see, as already remarked in [BFHP22, Example 2.12], that $\mathrm{SL}_2(\mathbb{F}_{17})$, of order 4896, is the smallest group with a norm relation but without any scalar norm relation.

Remark 3.3.23. For some groups the consequences of having a norm relation are stronger than those that can be obtained from scalar norm relations. In particular, as we will see in Theorem 3.4.4, it is convenient that the groups appearing in norm relations have relatively small index in G; such indices might not be as small if we restrict ourselves to scalar norm relations. For instance for $C_2 \times \mathrm{SU}_3(\mathbb{F}_2)$, of order 432, there is a norm relation involving subgroups with index at most 54, while in each of the scalar norm relations there is at least one subgroup with index greater or equal than 72 (see [BFHP22, Example 2.13]).

3.4 Triviality of Leopoldt kernels

A key point about the results in this section is that they do not require any knowledge of the $\mathbb{Q}[G]$-module structure of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$. All of the proofs in this section only use the fact that $\Lambda_{L,p}$ is equivariant, plus some previously known cases of Leopoldt's conjecture such as Theorem 3.2.1.

Theorem 3.4.1. *Let L/K be a finite Galois extension of number fields and let p be a prime number. Then* $\mathrm{Leo}(L,p)$ *holds if and only if* $\mathrm{Leo}(L^{\ker\chi},p)$ *holds for all* $\chi \in \mathrm{Irr}_{\mathbb{C}}(\mathrm{Gal}(L/K))$.

Proof. This follows from Proposition 3.3.1 and Lemma 3.2.15(iii). □

Corollary 3.4.2. *Let L/K be a finite abelian extension of number fields and let p be a prime number. Then* $\mathrm{Leo}(L,p)$ *holds if and only if* $\mathrm{Leo}(F,p)$ *holds for every intermediate extension F such that F/K is cyclic.*

Proof. This follows from Corollary 3.3.4 and Lemma 3.2.15(iii). □

Remark 3.4.3. Corollary 3.4.2 is a sharpening of [Shi92, Lemma 3.1], which has the additional assumption that $\zeta_p \notin L$ and thus, in particular, requires p to be odd.

Theorem 3.4.4. *Let L/K be a finite Galois extension of number fields and let $G = \mathrm{Gal}(L/K)$. Suppose that $1 = \sum_{H\in\mathcal{H}} e_H r_H$ is a norm relation of G. Let $\mathcal{I}$ be a subset of $\mathcal{H}$ such that for every $H \in \mathcal{H}$ there exist $g \in G$ and $I \in \mathcal{I}$ such that $I^g \subseteq H$. Let p be a prime. Then* $\mathrm{Leo}(L,p)$ *holds if and only if* $\mathrm{Leo}(L^I,p)$ *holds for every $I \in \mathcal{I}$.*

Proof. This follows from Corollary 3.3.8 and Lemma 3.2.15(iii). □

Remark 3.4.5. In particular, Theorem 3.4.4 implies Theorem 3.4.1 and Corollary 3.4.2 using the norm relation provided by Lemma 3.3.19 (where the subgroups considered are the kernels of the irreducible complex characters).

Corollary 3.4.6. *Let L/K be a finite Galois extension of number fields. Suppose that $\mathrm{Gal}(L/K) \cong N \rtimes H$ is a Frobenius group with kernel N and complement H. Let p be a prime. Then* $\mathrm{Leo}(L,p)$ *holds if and only if both* $\mathrm{Leo}(L^N,p)$ *and* $\mathrm{Leo}(L^H,p)$ *hold.*

Proof. This follows from Corollary 3.3.15 and Lemma 3.2.15(iii). □

Corollary 3.4.7. *Let L/K be a finite Galois extension of number fields, where K is either equal to $\mathbb{Q}$ or is an imaginary quadratic field. Suppose that $\mathrm{Gal}(L/K) \cong N \rtimes H$ is a Frobenius group with kernel N and abelian complement H. Let p be a prime. Then* $\mathrm{Leo}(L,p)$ *holds if and only if* $\mathrm{Leo}(L^H,p)$ *holds.*

Proof. Theorem 3.2.1 and the hypotheses on K and H imply that $\mathrm{Leo}(L^N,p)$ holds, and so the desired result follows from Corollary 3.4.6. □

Corollary 3.4.8. *Let $L/\mathbb{Q}$ be a totally imaginary A_4-extension. Then* $\mathrm{Leo}(L,p)$ *holds for every prime p.*

Proof. As seen in Example 3.3.14, $A_4 = \mathrm{Aff}(4)$ is a Frobenius group with kernel $N \cong C_2^2$ and complement $H \cong C_3$. Since L^H is a totally imaginary quartic field, it has unit rank 1, and so $\mathrm{Leo}(L^H, p)$ holds by Remark 3.2.11. Thus the result follows from Corollary 3.4.7. □

Remark 3.4.9. Corollary 3.4.8 was first proved in [EKW84, Théorème 2], the proof of which considers the Galois module structure of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$. By contrast, our proof only uses norm relations and the fact that Leopoldt's conjecture holds for certain proper subfields of L.

Corollary 3.4.10. *Let $L/\mathbb{Q}$ be an S_3-extension and let K be a cubic subextension of L. Let p be a prime. Then $\mathrm{Leo}(L, p)$ holds if and only if $\mathrm{Leo}(K, p)$ holds.*

Proof. As seen in Example 3.3.14, $S_3 = \mathrm{Aff}(3)$ is a Frobenius group. Thus the result follows from Corollary 3.4.7. □

Corollary 3.4.11. *Let L/K be a finite Galois extension of number fields. Suppose that $\mathrm{Gal}(L/K)$ contains either a non-cyclic subgroup of order $\ell_1\ell_2$, where ℓ_1 and ℓ_2 are two not necessarily distinct primes, or a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)$, where $\ell = 2^{2^k} + 1$ is a Fermat prime with $k > 1$. Let p be a prime. Then $\mathrm{Leo}(L, p)$ holds if and only if $\mathrm{Leo}(F, p)$ holds for every proper intermediate field F of L/K.*

Proof. This follows from Theorem 3.3.21, Theorem 3.4.4 and Lemma 3.2.15(iii). □

Example 3.4.12. In this example we will see three of the above results applied. Let $G \cong A \rtimes H$ be a group such that A is a non-cyclic abelian group of odd order and $H \cong C_2$ acts by inversion. Then, by Example 3.3.13, G is a Frobenius group. Let p be a prime number. If L/K is a Galois extension of number fields with Galois group isomorphic to G, by Corollary 3.4.6, $\mathrm{Leo}(L, p)$ holds if $\mathrm{Leo}(L^A, p)$ and $\mathrm{Leo}(L^H, p)$ hold. Note that L^H/K is non-Galois and has only index 2 in L, so that we will instead apply other results in order to involve smaller intermediate fields. By Proposition 3.3.12(iii), all of the irreducible complex characters are either with kernel G or A (hence non-faithful) or $\mathrm{Ind}_A^G \psi$ with $\mathbf{1}_A \neq \psi \in \mathrm{Irr}_{\mathbb{C}}(A)$. Since $\ker \psi$ has cyclic quotient, the character ψ is non-faithful. Using the action of H by inversion, we easily conclude that $\mathrm{Ind}_A^G \psi$ is non-faithful as well. Therefore this is an example where we can apply Theorem 3.4.1: if L/K is a G-extension, in order to conclude $\mathrm{Leo}(L, p)$ it is sufficient to check the fields fixed by the subgroups of A with cyclic quotient in A. Alternatively, note that this is also a consequence of the fact that the subgroup A is abelian, so that we can use instead Corollary 3.4.2 for the extension L/L^A with the same conclusion. For instance, if ℓ is a prime number, $n \geq 2$ and $G \cong C_\ell^n \rtimes C_2$ with action of C_2 by inversion, then we have $\mathrm{Leo}(L, p) \Leftrightarrow \mathrm{Leo}(F, p)$, where F/K is any intermediate field with Galois group isomorphic to $D_{2\ell}$.

3.5 Brauer relations

3.5.1 Review of character theory

We refer to [CR81, §9 & §10] for a good overview.

Let G be a finite group and let K be a field of characteristic 0. We recall that the character associated to a finitely generated K-representation V of G (that is, a finitely generated $K[G]$-module), is the function that assigns to every $g \in G$ the corresponding trace on V. We will denote by $\mathbf{1}_G$ the trivial character of G (corresponding to the trivial representation and independent of the field K).

We will denote by *virtual character* a linear combination of K-characters with coefficients in $\mathbb{Z}$. If a virtual character is zero, namely

$$0 = \sum_i a_i \chi_i$$

as a function, with $a_i \in \mathbb{Z}$, then

$$\sum_{a_i \geq 0} V_{\chi_i}^{a_i} \cong \sum_{a_i < 0} V_{\chi_i}^{-a_i},$$

where V_{χ_i} is a K-representation with character χ_i. Note in fact that the space of virtual K-characters has the set of irreducible K-characters as a $\mathbb{Z}$-basis.

We recall that $\mathrm{Irr}_K(G)$ denotes the set of irreducible K-characters of G. Note that $\mathrm{Irr}_K(G)$ provides a $\mathbb{Q}$-linearly independent set of functions from the set of conjugacy classes of G to K. Moreover, if K is algebraically closed then the cardinality of $\mathrm{Irr}_K(G)$ is equal to the number of conjugacy classes of G.

If H is a subgroup of G and ρ is a K-character attached to a K-representation V of H, we will denote by $\mathrm{Ind}_H^G \rho$ the character of $K[G] \otimes_{K[H]} V$. Note that if ρ is defined over two different fields then in either case we can define the induction and this is independent of the field we choose. For an explicit formula for the induction of a character see [CR81, (10.2)].

If H is a subgroup of G and χ is a K-character of G, then $\mathrm{Res}_H^G \chi$ is the character of H obtained from χ by restriction of scalars.

If N is a normal subgroup of G and φ is a K-character of G/N, then $\mathrm{Infl}_{G/N}^G(\varphi)$ is the character of G obtained via the projection $G \to G/N$.

If χ_1 and χ_2 are two K-characters of G, then we define

$$\langle \chi_1, \chi_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \chi_2(g^{-1}).$$

If V is a K-representation of G with character χ and χ' is an irreducible K-character of G, then $\langle \chi, \chi' \rangle_G$ is the multiplicity of the irreducible component of V with character χ', so that $V = 0$ if and only if $\langle \chi, \chi' \rangle_G = 0$ for every $\chi' \in \mathrm{Irr}_K(G)$. Also note that $\langle \mathbf{1}_G, \chi \rangle_G = \dim_K M^G$.

Let H be a subgroup of G, let χ be a K-character of G and let ρ be a K-character of H. The Frobenius reciprocity theorem tells us that

$$\langle \chi, \mathrm{Ind}_H^G \rho \rangle_G = \langle \mathrm{Res}_H^G \chi, \rho \rangle_H$$

(e.g. see [CR81, p. 233]).

3.5.2 Brauer relations

Definition 3.5.1. Let G be a finite group and let $\mathcal{H}$ be a set of subgroups of G. A *Brauer relation* $\mathcal{R}$ of G with respect to $\mathcal{H}$ is an equality of the form

$$0 = \sum_{H \in \mathcal{H}} a_H \mathrm{Ind}_H^G \mathbf{1}_H,$$

with $a_H \in \mathbb{Q}$, where the expression is taken as a virtual character.

Remark 3.5.2. Brauer relations of finite groups have been completely classified by Bartel and Dokchitser [BD15, BD14].

Proposition 3.5.3. *Let K be a field of characteristic 0 and let M be a finite-dimensional $K[G]$-module. Let $0 = \sum_{H \in \mathcal{H}} a_H \mathrm{Ind}_H^G \mathbf{1}_H$ be a Brauer relation of G. Then*

$$\sum_{H \in \mathcal{H}} a_H \dim_K M^H = 0.$$

Proof. This is essentially [KR94, Lemma 4.1]. We give the proof for the convenience of the reader. Note that we can assume that K is algebraically closed (otherwise we consider an extension of scalars of M to an algebraic closure of K and easily deduce the result for M). Let χ be the character corresponding to M. Then

$$0 = \left\langle \sum_{H \in \mathcal{H}} a_H \mathrm{Ind}_H^G \mathbf{1}_H, \chi \right\rangle_G = \sum_{H \in \mathcal{H}} a_H \langle \mathrm{Ind}_H^G \mathbf{1}_H, \chi \rangle_G = \sum_{H \in \mathcal{H}} a_H \langle \mathbf{1}_H, \mathrm{Res}_H^G \chi \rangle_G,$$

where the last equality comes from Frobenius reciprocity. This is what we wanted to show as $\langle \mathbf{1}_H, \mathrm{Res}_H^G \chi \rangle_G = \dim_K M^H$. □

Proposition 3.5.4. *[BB04, Remark 3.6] Suppose*

$$0 = \sum_{H \in \mathcal{H}} a_H e_H$$

with $a_H \in \mathbb{Q}$. Then we have the following Brauer relation:

$$0 = \sum_{H \in \mathcal{H}} a_H \mathrm{Ind}_H^G \mathbf{1}_H.$$

Proof. Let χ be an irreducible complex character of G. Then by definition $\chi(e_H) = \langle \mathbf{1}_H, \mathrm{Res}_H^G \chi \rangle_H = \langle \mathrm{Ind}_H^G \mathbf{1}_H, \chi \rangle_G$ (where we linearly extended χ from G to $\mathbb{Q}[G]$). Hence

$$\left\langle \sum_{H \in \mathcal{H}} a_H \mathrm{Ind}_H^G \mathbf{1}_H, \chi \right\rangle_G = \chi \left(\sum_{H \in \mathcal{H}} a_H e_H \right) = 0$$

for every χ, which implies that $\sum_{H \in \mathcal{H}} a_H \mathrm{Ind}_H^G \mathbf{1}_H = 0$. □

From now on, let G be a finite group and let L/K be a Galois extension of number fields with Galois group isomorphic to G. Let p be a prime number. If H is a subgroup of G, we will denote by $\delta(H)$ the defect $\delta(L^H, p)$.

Remark 3.5.5. Note that $\delta(H)$ only depends on the conjugacy class of H. In fact, if H and H' are conjugate then L^H and $L^{H'}$ are isomorphic.

Corollary 3.5.6. *In the above setting, suppose* $0 = \sum_{H \leq G} r_H e_H$ *with* $r_H \in \mathbb{Q}$. *Then*

$$\sum_{H \leq G} r_H \delta(H) = 0.$$

Proof. This follows from Proposition 3.5.4, Proposition 3.5.3 with $M = \ker \Lambda_{L,p}$ and Lemma 3.2.15. □

Remark 3.5.7. Corollary 3.5.6 recovers Theorem 3.4.4 when the norm relation is actually a scalar norm relation.

Corollary 3.5.8. *Suppose* $G \cong N \rtimes H$ *is a Frobenius group. Then we have the relation*

$$\delta(1) + |H|\delta(G) = \delta(N) + |H|\delta(H).$$

Proof. This follows from Proposition 3.3.15 and Corollary 3.5.6. □

In particular if we know that $\delta(N) = 0$ (e.g. when H is abelian and K is $\mathbb{Q}$ or an imaginary quadratic field), then Corollary 3.5.8 tells us that $\delta(1) = |H|\delta(H)$. Hence we find that $\delta(1)$ is divisible by $|H|$ (see also Example 3.6.4).

We conclude the subsection with the following.

Theorem 3.5.9. *[Fun79, Theorem 9] A finite group G admits a Brauer relation with non-trivial coefficient for the subgroup $H = 1$ if and only if G contains a non-cyclic subgroup of order $\ell_1\ell_2$, where ℓ_1 and ℓ_2 are two not necessarily distinct primes.*

3.5.3 On a minimal set of Brauer relations

We refer to [CR87, §80] for a good background of the material we present here.

Let G be a finite group.

Definition 3.5.10. The *Burnside ring* $b(G)$ is the commutative ring generated as an abelian group by the symbols $[S]$ for each isomorphism class S of a finite G-set, namely a finite set on which G acts from the left as a group of permutations. The sum is defined by

$$[S] + [T] = [S \sqcup T]$$

and the multiplication by

$$[S] \cdot [T] = [S \times T],$$

where the action of G on disjoint union and product is defined naturally.

Proposition 3.5.11. *Let $\mathcal{H}$ be a full set of nonconjugate subgroups of G. Then $\{[G/H]\}_{H\in\mathcal{H}}$ forms a $\mathbb{Z}$-basis for $b(G)$, where G/H denotes the set of left cosets with the natural left G-action.*

Proof. See [CR87, Corollary (80.6)]. □

Definition 3.5.12. Let K be a field of characteristic 0. We denote by $a(K[G])$ the representation ring of $K[G]$: as an abelian group $a(K[G])$ is generated by the isomorphism classes $[M]$ of finitely generated $K[G]$-modules with sum given by

$$[M] + [N] = [M \oplus N]$$

and multiplication by

$$[M] \cdot [N] = [M \otimes_{K[G]} N].$$

We define $A(K[G]) = \mathbb{Q} \otimes_{\mathbb{Z}} a(K[G])$ and $B(G) = \mathbb{Q} \otimes_{\mathbb{Z}} b(G)$.

Remark 3.5.13. Note that a Brauer relation is an element of the kernel of the map $\phi : B(G) \to A(K[G])$ induced by

$$\begin{aligned} b(G) &\longrightarrow a(K[G]) \\ [G/H] &\longmapsto [K[G/H]]. \end{aligned}$$

In fact, $K[G/H]$ is the representation corresponding to the character $\mathrm{Ind}_H^G \mathbf{1}_H$ (if seen over K). In general a finite G-set S maps to the permutation module $K[S]$.

Remark 3.5.14. If K is algebraically closed, note that $A(K[G])$ has $\mathrm{Irr}_K(G)$ as a $\mathbb{Q}$-basis, which has cardinality the number of conjugacy classes in G.

Proposition 3.5.15. *[CR87, Proposition (80.12)] Let $\mathcal{I} = \{H_1, \ldots, H_m\}$ be a full set of non-conjugate subgroups of G. Let $\alpha : B(G) \to \mathbb{Q}^m$ be the ring homomorphism induced by*

$$[S] \longmapsto \left(|S^{H_1}|, \ldots, |S^{H_m}|\right)$$

for every finite G-set S. Then α is an isomorphism.

Sketch of a proof. We first show that α restricted to $b(G)$ is injective. It is straightforward to verify that $(G/I)^H$ is non-trivial if and only if some conjugate of H is contained in I (see [CR87, (80.9)]). From this, since the elements of the form $[G/I]$ form a basis for $b(G)$, an easy argument shows that the map is injective (see [CR87, Theorem (80.10)]).

Since $b(G)$ is $\mathbb{Z}$-free of rank m, so is the image of α. It follows that the map obtained by tensoring with $\mathbb{Q}$ is an isomorphism. □

It follows that $B(G)$ has a basis of primitive idempotents, corresponding to the elements $\varepsilon_i := (0, \ldots, 1, \ldots, 0)$ in $\mathbb{Q}^m$.

Definition 3.5.16. Let $I \leq H \leq G$ be two subgroups. Then we define

$$\mu(I, H) = \sum_{I=I_0 \lneq \cdots \lneq I_n = H} (-1)^n.$$

We denote by $N_G(H)$ the normaliser of H in G.

Theorem 3.5.17. *[Glu81, Proposition] For every $1 \leq i \leq m$, we have*

$$\alpha^{-1}(\varepsilon_i) = \frac{1}{|N_G(H_i)|} \sum_{I \leq H_i} |I| \mu(I, H_i)[G/I] := \epsilon_{H_i}.$$

The following two statements and proofs are an expansion of [BB04, Theorem 3.3].

Proposition 3.5.18. *If K is algebraically closed and of characteristic 0, then the map $\phi \circ \alpha^{-1} : \mathbb{Q}^m \to A(K[G])$ is completely determined by the components of $\mathbb{Q}^m$ which correspond to the cyclic subgroups in $\mathcal{I}$.*

Proof. It is sufficient to prove the statement looking at a finite G-set S. Since K is algebraically closed, the character χ_S of $\phi([S]) = K[S]$ is an integral linear combination of the irreducible K-characters of G, which are a basis for a space of functions from $\mathcal{I}$ to K and also provide a $\mathbb{Q}$-basis for $A(K[G])$. The character χ_S is completely determined by its valuation at the elements of G, which implies that also the coefficients of its expression as a sum of irreducible characters only depend on the valuation of χ_S at the elements of G. Since $K[S]$ is a permutation representation, we can easily show that $\chi_S(g) = |S^{\langle g \rangle}|$, where $\langle g \rangle$ is the cyclic subgroup of G generated by g. This easily implies the statement by the definition of α. □

Corollary 3.5.19. *Let K be any field of characteristic 0. Then for every $H \in \mathcal{I}$ which is non-cyclic we have that $\phi(e_H) = 0$, that is,*

$$0 = \sum_{I \subseteq H} |I| \ \mu(I, H) \ \mathrm{Ind}_I^G \mathbf{1}_I.$$

Proof. Let $L \supseteq K$ be algebraically closed. We easily see that extension of scalars gives rise to an injection $a(K[G]) \hookrightarrow a(L[G])$ so that we can assume that K is algebraically closed. By Theorem 3.5.17, for every $H_i \in \mathcal{I}$ the idempotent ϵ_{H_i} of $B(G)$ corresponds to $\varepsilon_i \in \mathbb{Q}^m$. By Proposition 3.5.18, each ε_i is mapped through $\phi \circ \alpha^{-1}$ to the image of 0, which is 0. □

Corollary 3.5.20. *Let K be a field of characteristic 0 and let M be a finite-dimensional $K[G]$-module. Let H be a non-cyclic subgroup of G. Then we have the relation*

$$\sum_{I \leq H} |I| \ \mu(I, H) \ \dim_K M^I = 0.$$

Proof. This follows from Corollary 3.5.19 and Proposition 3.5.3. □

Remark 3.5.21. Corollary 3.5.20 is a special case of [BB04, Theorem 1.2], where the authors consider *cohomolgical Mackey functors*. In fact the system $\{M^H\}_{H \leq G}$ forms a cohomological Mackey functor (the proof is straightforward or see [BB04, Example 2.5(d)], noting that M^H is the 0-th H-cohomology group of M). For more on Mackey functors see also [Bol97]. In the present situation, we have focused on a special case which allowed us to have a more direct proof which does not require Mackey functors.

Remark 3.5.22. By Remark 3.5.13, Brauer relations correspond to the kernel of the map $\phi \circ \alpha^{-1} : \mathbb{Q}^m \to A(K[G])$, and what we actually found from the above proofs is that the idempotents ε_i corresponding to non-cyclic subgroups form a basis of $\ker \phi \circ \alpha^{-1}$. Hence Corollary 3.5.20 provides us with a minimal set of possible relations, without dealing with explicit scalar norm relation. Moreover the parameterisation we obtained is quite simple and nice. We also have that relations arising from Lemma 3.3.17 form a basis for Brauer relations, by [BB04, Remark 3.6].

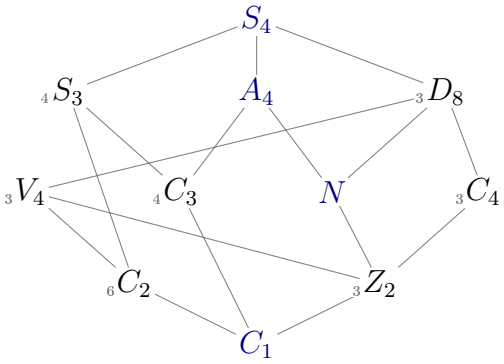
Corollary 3.5.23. *Let L/K be a Galois extension of number fields with Galois group G and let H be a non-cyclic subgroup of G. We recall that $\delta(H)$ is the defect $\delta(L^H, p)$. Then we have the relation*

$$\sum_{I \leq H} |I| \ \mu(I, H) \ \delta(I) = 0.$$

Proof. This follows from Corollary 3.5.20 and Lemma 3.2.15. □

Corollary 3.5.24. *Under the above hypotheses, let H be a non-cyclic subgroup of G such that $\mu(1, H) \neq 0$. Then, if $\mathrm{Leo}(L^I, p)$ holds for every non-trivial subgroup I of H such that $\mu(I, H) \neq 0$, we have $\mathrm{Leo}(L, p)$.*

Example 3.5.25. Let $L/\mathbb{Q}$ be an S_4-extension. Then we can list all the possible relations coming from Corollary 3.5.23. Since the non-cyclic subgroups of S_4 lie in 6 conjugacy classes we can find 6 relations involving the defects of L and its subfields. These relations have already been listed in [BB04, Examples 3.9] (note that there is a typo in their fifth relation). Let us keep their notation: D_8 will be a subgroup isomorphic to the dihedral group of order 8, N the normal Klein-subgroup of order 4, V_4 a choice of a non-normal Klein-subgroup of order 4, Z_2 a subgroup generated by a double transposition, C_2 a subgroup generated by a transposition and A_4, C_4 and C_3 choices of subgroups in their isomorphism classes. See also the lattice of subgroups:



We already know that, with the notation of Corollary 3.5.23, $\delta(S_4) = \delta(A_4) = 0$ (the corresponding fields are $\mathbb{Q}$ or a quadratic field, respectively). Hence by Corollary 3.5.23

we have the following:

$$\begin{aligned}
&\delta(1) + 2\delta(S_3) + 2\delta(D_8) = 2\delta(C_2) + \delta(C_3) + \delta(N)\\
&\delta(1) = 3\delta(C_3) + \delta(N)\\
&\delta(Z_2) + 2\delta(D_8) = \delta(N) + \delta(V_4) + \delta(C_4)\\
&\delta(1) + 2\delta(S_3) = 2\delta(C_2) + \delta(C_3)\\
&\delta(1) + 2\delta(V_4) = 2\delta(C_2) + \delta(Z_2)\\
&\delta(1) + 2\delta(N) = 3\delta(Z_2).
\end{aligned}$$

The subfield L^N is an S_3-extension of $\mathbb{Q}$ and hence its defect is 0 or 2 (by Corollary 3.5.8 and the fact that the defect of the cubic subfield can only be 0 or 1); this is also encoded in the difference between the first and the fourth relation. Hence the second relation tells us that $\delta(1)$ is congruent to 0 or 2 modulo 3. For instance suppose that $\delta(1) = 2$ (note that if L is totally imaginary then $\delta(1)$ cannot be bigger than 2, by [Lau89, Théorème 1]). Then we can show we are able to uniquely determine the defects: the second relation tells us that $\delta(1) = \delta(N) = 2$ and $\delta(C_3) = 0$. Under certain choices of the subgroups inside the conjugacy classes we can assume $L^{S_3} \subseteq L^{C_3}$, therefore by Lemma 3.2.6 we also have that $\delta(S_3) = 0$. From the difference between the first and the fourth relation we find $\delta(D_8) = 1$. Now the first relation gives us $\delta(C_2) = 1$. From the sixth one we get $\delta(Z_2) = 2$, from the fifth one $\delta(V_4) = 1$ and from the third one $\delta(C_4) = 1$. Hence we found the values for the defects of all the subfields. Therefore a possible strategy to prove Leopoldt's conjecture for a certain S_4-extension of $\mathbb{Q}$ could be to exclude that the defect of one of its subfields is equal to one particular value.

3.6 A character-theoretic approach to Leopoldt defects

Theorem 3.6.1. *Let L/K be a non-abelian Galois extension of number fields where either $K = \mathbb{Q}$ or K is an imaginary quadratic extension of $\mathbb{Q}$. Let $1 < d_1 < \cdots < d_s$ be the distinct degrees of the non-linear complex irreducible characters of $\mathrm{Gal}(L/K)$. Let p be a prime. Then $\delta(L,p) = \sum_{i=1}^{s} k_i d_i$ for some $k_i \in \mathbb{Z}_{\geq 0}$. In particular, either $\delta(L,p) = 0$ or $\delta(L,p) \geq d_1 > 1$.*

Proof. We will study $\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p}$ as a $\mathbb{C}_p[G]$-module. Let χ be a linear irreducible complex (or, which is the same, $\mathbb{C}_p$-) character of G. Then $\ker \chi$ is a normal subgroup H of G with cyclic quotient. By Lemma 3.2.15(iii) we have

$$e_H(\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p}) = (\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p})^H = \mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L^H,p} = 0,$$

where we used that $\mathrm{Leo}(L^H, p)$ holds by Theorem 3.2.1. Hence

$$e_\chi(\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p}) \subseteq e_H(\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p}) = 0.$$

Therefore in $\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p}$ there is no χ-isotypical component. The conclusion follows from the decomposition $\mathbb{C}_p \otimes_{\mathbb{Q}_p} \ker \Lambda_{L,p}$, whose dimension only has contributions from non-linear irreducible characters. □

Remark 3.6.2. Using different methods, Khare and Wintenberger [KW14, Proposition A.1] proved that, if $F/\mathbb{Q}$ is a totally real finite Galois extension, then for every prime p we have $\delta(F,p) \neq 1$. The proof was itself a strengthening of an argument of Colmez. Our methods provide a simpler proof that also covers the imaginary case.

Remark 3.6.3. Note that what we actually require in the proof of Theorem 3.6.1 is an extension L/K such that $\mathrm{Leo}(F,p)$ holds for every cyclic intermediate field F/K. The advantage of our approach is that we do not need to know the $\mathbb{Q}[G]$-module structure of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$, which is what was used in previous work such as [EKW84] and [Lau89].

Example 3.6.4. Let $G \cong N \rtimes H$ be a Frobenius group with H abelian and let $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$. By Proposition 3.3.12, if $N \leq \ker\chi$, then χ is lifted from an irreducible complex character of H and hence linear. Otherwise it is an induction from N to G of an irreducible character of N, therefore of dimension a multiple of $|H|$ (exactly $|H|$ if N is abelian, so that χ is necessarily an induction of a linear character of N). Theorem 3.6.1 shows us that in this case the defect would be a multiple of $|H|$, as already noted after Proposition 3.5.8.

3.7 Infinite families of totally real number fields that satisfy Leopoldt's conjecture

We recall that there is no example in the literature of a non-abelian group G and a prime number p such that there exists an infinite family of real G-extensions of $\mathbb{Q}$ which satisfy Leopoldt's conjecture at p. In this section we will see how our techniques permit us to achieve this goal, focusing especially on S_3-extensions. This will be inspired by the ideas of Buchmann and Sands [BS88], via two different methods.

3.7.1 Another formulation of Leopoldt's conjecture

We fix the following notation for the rest of this chapter: L will be a number field, p a prime number, $q = (2,p)\cdot p$, $E_L := \mathcal{O}_L^\times$ with $\mathbb{Z}$-rank r_L, $E_L(q) := \{\alpha \in E_L : \alpha \equiv 1 \pmod q\}$, D a choice of a subgroup of finite index in $E_L(q)$ and $D(p^m) := \{\alpha \in D : \alpha \equiv 1 \pmod{p^m}\}$. For every integer $k \geq 1$ let $\phi_k : D(p^k) \to \mathcal{O}_L/p\mathcal{O}_L$ be the map that sends $1 + p^k\alpha \mapsto \alpha \pmod p$. In [BS87] the authors found another equivalent formulation of Leopoldt's conjecture, summarised in the following proposition.

Proposition 3.7.1. *[BS88, §II] Let L be a number field and let p be a prime number.* $\mathrm{Leo}(L,p)$ *holds if and only if there exists an integer $m \geq 2$ such that one the following equivalent conditions hold:*

(i) $D(p^m) \subseteq D^p$;

(ii) $D(p^m) = D(p^{m-1})^p$;

(iii) $D(p^{m-1})/D(p^m)$ *has dimension r_L as an $\mathbb{F}_p$-vector space;*

(iv) the image of ϕ_{m-1} has rank r_L as an $\mathbb{F}_p$-vector space.

Note that Proposition 3.7.1 does not depend on the choice of the set D. Buchmann and Sands [BS88] used this formulation and an explicit description of units to prove

Leopoldt's conjecture for some infinite families of (non-totally real and non-Galois) number fields. We will see how this can also be applied to exhibit infinite families of totally real non-Galois cubic fields which satisfy Leopoldt's conjecture. This together with Corollary 3.4.10 will lead to an infinite family of real S_3-extensions satisfying Leopoldt's conjecture.

3.7.2 Infinite families of number fields satisfying Leopoldt's conjecture

Buchmann and Sands proved the following theorem about infinite families of quintic number fields.

Theorem 3.7.2. *[BS88, Theorem 3.3 and 3.4] Let $A \geq 1$ (respectively $B \geq 2$) be an integer and let λ be a root of x^5+4A^4x+1 (respectively x^5-B^4x+1). Then $\mathrm{Leo}(\mathbb{Q}(\lambda), p)$ holds whenever $p \neq 5$ and $p \mid 2A$ (respectively $p \mid B$).*

An important ingredient for the proof of Theorem 3.7.2 is the previous research on the description of families of units. We summarize some of the results.

Theorem 3.7.3. *[Mau84, §5 and §6] Let $A \geq 1$ (respectively $B \geq 2$) be an integer and let λ be a root of $x^5 + A^4x + 1$ (respectively $x^5 - B^4x + 1$). Then $L := \mathbb{Q}(\lambda)$ is a quintic extension of $\mathbb{Q}$ with discriminant $5^5 + 4^9A^{20}$ (respectively $5^5 - 4^4B^{20}$) whose Galois closure is an S_5-extension of $\mathbb{Q}$. Moreover the $\mathbb{Z}$-rank of $\mathcal{O}_L^\times$ is 2 (respectively 3) and $\lambda, \lambda^2 - 2A\lambda$ (respectively $\lambda, \lambda + B, \lambda - B$) forms a system of fundamental units of $\mathbb{Z}[\lambda]$; in particular they form a complete system of independent units in $\mathcal{O}_L^\times$ and hence generate a subgroup with finite index.*

Theorem 3.7.4. *[HKS74] Let n and D be natural numbers and let λ be a real root of $x^n - D^n \pm 1$. Then $L := \mathbb{Q}(\lambda)$ has degree n over $\mathbb{Q}$ and $\{\lambda^t - D^t : t \mid D, t \neq n\}$ forms a set of $\tau(n) - 1$ independent units in $\mathcal{O}_L^\times$, where $\tau(n)$ denotes the number of positive divisors of n.*

Buchmann and Sands [BS88] used Theorem 3.7.3 to prove Theorem 3.7.2. A related paper is [Lev92]: the author used Theorem 3.7.4 and the techniques in [BS88] to show that $\{\lambda^t - D^t : t \mid D, t \neq n\}$ forms a system of $\tau(n) - 1$ $\mathbb{Z}_p$-independent units if p is odd, $(p, n) = 1$ and $p \mid D$.

Theorem 3.7.5. *[Ste72] Let r, s be integers such that $2 \leq r \leq s-3$ and let λ be a root of $x(x+r)(x+s) - 1$. Then $L := \mathbb{Q}(\lambda)$ is a totally real cubic extension of $\mathbb{Q}$ such that $\lambda + r, \lambda + s$ forms a system of fundamental units of $\mathbb{Z}[\lambda]$; in particular, they are two independent units in $\mathcal{O}_L^\times$ and hence form a subgroup with finite index.*

In [Ste72] Stender also found a system of independent units in number fields generated by a root of $x(x + kr)(x + ks) - k$ when $k > 1$. Thomas [Tho79] found similar results for other families of cubic fields.

Now we apply these techniques for totally real cubic extensions. As far as we know Theorem 3.7.6 and Proposition 3.7.9 give the first example of a prime p and an infinite family of real S_3 (in particular, non-abelian) extensions of $\mathbb{Q}$ which satisfy Leopoldt's conjecture at p. Note that we can do this for every $p \neq 3$; for $p = 3$ see the alternative approach followed in Example 3.7.11.

Theorem 3.7.6. *Let $t \geq 4$ be an integer which is not a power of 3 and let λ be a root of the polynomial*

$$f_t(x) := x^3 - t^2 x - 1.$$

Then $L := \mathbb{Q}(\lambda)$ is a totally real non-Galois cubic field. Let $p \neq 3$ be a prime number such that $p \mid t$. Then $\mathrm{Leo}(L,p)$ *holds. Moreover, let $\tilde{L}$ be the Galois closure of L over $\mathbb{Q}$, which is a real S_3-extension; then also* $\mathrm{Leo}(\tilde{L},p)$ *holds*

Proof. The discriminant of f_t is $4t^6 - 27$. Note that $4t^6$ is a square and already for $t = 4$ we have $4t^6 - 27 = (2t^3)^2 - 27 > (2t^3 - 1)^2$, so that we always have that $4t^6 - 27$ is a positive non-square. Moreover f_t is always irreducible (in fact, it has no rational root); therefore L is a non-Galois totally real cubic field.

We will now apply Proposition 3.7.1(iv). Let $h \geq 1$ be such that $p^h \parallel t$. Our m will be $2h+1$ and we will now find two units in $D(p^{2h})$ such that their images under ϕ_{2h} are $\mathbb{F}_p$-independent. We will show that we can choose λ^3 and $(\lambda+t)^{3t}$ as such units. First of all they are $\mathbb{Z}$-independent units: λ is a unit as it is a root of f_t which has constant term -1; similarly, $\lambda + t$ is also a unit because it is a root of $x^3 - 3tx^2 + t^2x - 1$. Moreover λ and $\lambda + t$ are $\mathbb{Z}$-independent by Theorem 3.7.5, applied with $s = 2r = 2t$ and $x \mapsto x - t$.

Now let D be the subgroup of $E_L(q)$ generated by λ^3 and $(\lambda+t)^{3t}$. This has finite index in $E_L(q)$ as λ and $\lambda+t$ are $\mathbb{Z}$-independent. We will show that $\phi_{2h}(\lambda^3)$ and $\phi_{2h}((\lambda+t)^{3t})$ are $\mathbb{F}_p$-independent, in order to use Proposition 3.7.1(iv) to prove that $\mathrm{Leo}(L,p)$ holds. We have that $\lambda^3 = 1 + t^2\lambda \in D(p^{2h})$, and so $\phi_{2h}(\lambda^3) = \frac{t^2}{p^{2h}}\lambda \pmod{p}$. Now note that

$$(\lambda+t)^3 = \lambda^3 + 3t\lambda^2 + 3t^2\lambda + t^3 = 1 + t^2\lambda + 3t\lambda^2 + 3t^2\lambda + t^3 = 1 + 3t\lambda^2 + p^{2h}\gamma$$

for some $\gamma \in \mathcal{O}_L$. We can look at the multinomial expansion of $(1 + 3t\lambda^2 + p^{2h}\gamma)^t$: what remains modulo p^{2h+1} is $1 + 3t^2\lambda^2$, so that $\phi_{2h}((\lambda+t)^{3t}) = \frac{3t^2}{p^{2h}}\lambda^2 \pmod{p}$. Note that both $\frac{t^2}{p^{2h}}$ and $\frac{3t^2}{p^{2h}}$ are coprime to p. Therefore, in order to prove that $\phi_{2h}(\lambda^3)$ and $\phi_{2h}((\lambda+t)^{3t})$ are $\mathbb{F}_p$-independent, it remains to show that λ and λ^2 are $\mathbb{F}_p$-independent in $\mathcal{O}_L/p\mathcal{O}_L$. This is true since the discriminant of the minimal polynomial of λ is $4t^6 - 27$, hence coprime to p. More precisely, the discriminant of f_t is also the discriminant of the $\mathbb{Q}$-basis $1, \lambda, \lambda^2$. Therefore $n := [\mathcal{O}_L : \mathbb{Z}[\lambda]]$ is coprime to p and we have $n\mathcal{O}_L \subseteq \mathbb{Z}[\lambda]$. If there exist $\delta \in \mathcal{O}_L$ and $A, B \in \mathbb{Z}$ not both in $p\mathbb{Z}$ such that $A\lambda + B\lambda^2 = p\delta$ (that is, λ and λ^2 are $\mathbb{F}_p$-dependent in $\mathcal{O}_L/p\mathcal{O}_L$), then we have $nA\lambda + nB\lambda^2 = pn\delta$. Since $n\delta \in \mathbb{Z}[\lambda]$ and at least one of nA and nB is not divisible by p, this leads to a non-trivial polynomial in $\mathbb{Z}[x]$ of degree at most 2 which has λ as a solution, which is a contradiction.

The last statement follows from Corollary 3.4.10. □

3.7.3 A continuity principle and a computational application for infinite families of number fields

In this subsection we will use a continuity principle so that Leopoldt's conjecture at a prime p for a field defined by a certain polynomial implies Leopoldt's conjecture at p for another field whose polynomial is p-adically close. This will imply that verifying

Leopoldt's conjecture at p for just one number field is sufficient in order to deduce Leopoldt's conjecture for a certain infinite family, as already observed by Buchmann and Sands for the quintic fields analysed in Theorem 3.7.2. The main result we will use is the following.

Theorem 3.7.7. *[BS88, Theorem 4.1] Let $L = \mathbb{Q}(\alpha)$ be a number field generated by the integer α and let $f(x)$ be the minimal polynomial of α, of degree n. Let p be a prime number such that $p^2 \nmid d_f$, where d_f denotes the discriminant of f. Let $\{\varepsilon_i = \sum_{j=0}^{n-1} a_{i,j}\alpha^j\}_{i=1,\dots,r}$ be a maximal system of independent units of L congruent to 1 modulo $(2,p)\cdot p$ in $\mathbb{Z}[\alpha]$ and let D be the subgroup of $\mathcal{O}_L^\times$ generated by $\{\varepsilon_i\}$. Suppose that $\mathrm{Leo}(L,p)$ holds and let $m \geq 2$ be an integer such that $D(p^m) \subseteq D^p$ (see Theorem 3.7.1). Now let us consider a monic polynomial $g(x)$ of degree n such that its coefficients are congruent to those of $f(x)$ modulo p^m. Let β be a root of $g(x)$ and let $L' = \mathbb{Q}(\beta)$. Suppose that there is a maximal system of independent units $\{\delta_i = \sum_{j=0}^{n-1} b_{i,j}\beta^j\}_{i=1,\dots,r}$ for L' such that $a_{i,j} \equiv b_{i,j} \pmod{p^m}$ $\forall i,j$. Then $\mathrm{Leo}(L',p)$ holds.*

We give a slightly different formulation of Theorem 3.7.7.

Corollary 3.7.8. *Let $I \subseteq \mathbb{Z}$ be a set of indices and let $a_j(t)$ and $s_i(t,z)$ be polynomials in t (respectively in t and z) with coefficients in $\mathbb{Z}$ such that:*

- *$\{f_t = x^n + a_{n-1}(t)x^{n-1} + \cdots + a_1(t)x + a_0(t)\}_{t\in I}$ is a family of irreducible polynomials with coefficients in $\mathbb{Z}$, where we denote by λ_t a choice of a root of f_t and we let $L_t = \mathbb{Q}(\lambda_t)$, with unit rank equal to r (independent of t);*
- *$\{s_i(t,z)\}_{i=1,\dots,r}$ is such that the set $\{s_i(t,\lambda_t)\}_{i=1,\dots,r}$ is a maximal system of independent units in $\mathbb{Z}[\lambda_t] \subseteq \mathcal{O}_{L_t}$ for every $t \in I$.*

Let $t_0 \in I$ and let p be a prime number such that $p^2 \nmid d_{f_{t_0}}$ and $\mathrm{Leo}(L_{t_0},p)$ holds. Then there exists $m \geq 2$ such that if $t' \equiv t_0 \pmod{p^m}$ then we also have $\mathrm{Leo}(L_{t'},p)$.

Proof. Let $N \geq 1$ be an integer such that for every $i = 1,\dots,r$

$$s_i(t_0,\lambda_{t_0})^N \equiv 1 \pmod{(2,p)\cdot p}.$$

Let $D \subseteq \mathbb{Z}[\lambda_{t_0}]^\times$ be the subgroup generated by $\{s_i(t_0,\lambda_{t_0})^N\}_{i=1,\dots,r}$. Then $\mathrm{Leo}(L_{t_0},p)$ implies that there exists $m \geq 2$ such that $D(p^m) \subseteq D^p$. If $t' \equiv t_0 \pmod{p^m}$, then $a_j(t') \equiv a_j(t_0) \pmod{p^m}$ for every $j = 0,\dots,n-1$ and $s_i(t',z) \equiv s_i(t_0,z) \pmod{p^m}$ for every $i = 1,\dots,r$. For every $i = 1,\dots,r$ let us consider the following Euclidean divisions in $\mathbb{Z}[z]$ (since $f_{t_0}(z)$ and $f_{t'}(z)$ are monic):

$$\begin{aligned} s_i(t_0,z)^N &= q_i(z)f_{t_0}(z) + r_i(z) \\ s_i(t',z)^N &= q_i'(z)f_{t'}(z) + r_i'(z), \end{aligned}$$

where $r_i(z)$ and $r_i'(z)$ are polynomials with degree at most $n-1$. Since $f_{t_0}(z) \equiv f_{t'}(z) \pmod{p^m}$ and $s_i(t_0,z)^N \equiv s_i(t',z)^N \pmod{p^m}$, this implies that for every $i = 1,\dots,r$ we also have $r_i(z) \equiv r_i'(z) \pmod{p^m}$. Moreover $s_i(t_0,\lambda_{t_0})^N = r_i(\lambda_{t_0})$ and $s_i(t',\lambda_{t'})^N = r_i'(\lambda_{t'})$. All the hypotheses of Theorem 3.7.7 are satisfied considering the coefficients of $r_i(z)$ and $r_i'(z)$ as $\{a_{i,j}\}$ and $\{b_{i,j}\}$, hence we can conclude that $\mathrm{Leo}(L_{t'},p)$ holds. □

We will see that we can provide infinite families of fields which satisfy Leopoldt's conjecture by combining Corollary 3.7.8 with the following.

Proposition 3.7.9. *In the setting of Corollary 3.7.8 suppose that I is either $\mathbb{Z}$ or of the form $\mathbb{Z}_{\geq d}$ or $\mathbb{Z}_{\leq d}$ with $d \in \mathbb{Z}$. Suppose that d_{f_t} is a non-constant polynomial in $\mathbb{Z}[t]$ which is not a square. Let M and a be two integers and let $J = \{Mx + a\}_{x \in \mathbb{Z}} \cap I$ be an arithmetic progression contained in I. Then $\{L_t\}_{t \in J}$ is an infinite family of number fields.*

Proof. We will prove that there is an infinite number of primes which ramify in at least one element of the family $\{L_t\}_{t \in J}$. First of all we have that

$$d_{f_t} = [\mathcal{O}_{L_t} : \mathbb{Z}[\lambda_t]]^2 \cdot d_{L_t}.$$

Therefore if a prime ℓ divides d_{f_t} with odd exponent for some $t \in J$ it will divide d_{L_t} and hence ramify in L_t. By hypothesis we can write $d_{f_t} = w(t)^2 u(t)$, where $w(t), u(t) \in \mathbb{Z}[t]$ and $u(t)$ is a non-constant polynomial without multiple roots in $\mathbb{C}$.

Let $v(x) = u(Mx+a)$, which is still a non-constant polynomial in $\mathbb{Z}[x]$. The values of x such that $Mx + a \in I$ are in an interval J of the form $\mathbb{Z}_{\geq e}$ or $\mathbb{Z}_{\leq e}$ or $\mathbb{Z}$. We are done if we prove that there is an infinite number of primes ℓ for which there exists $x \in J$ such that ℓ divides exactly $v(x)$. After an easy reparameterisation we can always suppose that $\mathbb{Z}_{\geq 0} \subseteq J$. By a well known fact, if z is a non-constant polynomial then $z(\mathbb{Z}_{\geq 0})$ is divisible by an infinite number of primes (sketch: consider $z(k!a^2)$ for sufficiently large k, where a is the constant term of z), so that $v(\mathbb{Z}_{\geq 0})$ is divisible by an infinite number of primes. Moreover $v(x)$, as a polynomial in $\mathbb{C}[x]$, has no multiple roots, since it is just a linear change of $u(t)$. Thus there exist $a(x), b(x) \in \mathbb{Q}[x]$ such that

$$a(x)v(x) + b(x)v'(x) = 1,$$

where $v'(x)$ denotes the derivative of $v(x)$. This implies that there exist $A(x), B(x) \in \mathbb{Z}[x]$ and $C \in \mathbb{Z}$ such that

$$A(x)v(x) + B(x)v'(x) = C.$$

Now let ℓ be a prime such that $(\ell, C) = 1$ and there exists $x_0 \in \mathbb{N}$ with $\ell \mid v(x_0)$. We claim that we can always find $x_1 \in \mathbb{N}$ such that $\ell \parallel v(x_1)$. Since we have an infinite choice of primes this will prove our statement. If $\ell \parallel v(x_0)$ there is nothing to say. Otherwise note that

$$v(x_0 + \ell) - v(x_0) = v'(x_0)\ell + O(\ell^2).$$

On the other hand, as $\ell \mid v(x_0)$ and $\ell \nmid C$ then $\ell \nmid v'(x_0)$. Therefore $\ell^2 \nmid v(x_0 + \ell)$, so $x_1 = x_0 + \ell$ works. □

Remark 3.7.10. A weaker form of this argument was used in [BS88, Proposition 5.1], which was applied to show that their families of quintic fields are infinite. A similar result when the polynomial has only linear or quadratic factors is contained in [Nag22] (see also the citation in [Nak93, Proof of Lemma 3]).

Buchmann and Sands already applied Theorem 3.7.7 to families of quintic fields, see [BS88, Corollary 4.3, Corollary 4.4 and Remark 4.5]. In the following examples we will study cubic fields (with an S_3-extension as Galois closure) and quartic fields (with a D_8-extension as Galois closure).

Example 3.7.11. Let us consider the polynomials $f_t(x) = x^3 - t^2x - 1$ with $t \geq 3$. As already remarked in the proof of Theorem 3.7.6 each of them defines a non-Galois totally real cubic number field, and by Theorem 3.7.5 for every $t \geq 3$ we can choose a root λ_t of f_t so that $\lambda_t, \lambda_t + t$ is a system of independent units for $L_t = \mathbb{Q}(\lambda_t)$. Hence by Corollary 3.7.8 for every t_0 and prime number p such that $p^2 \nmid 4t_0^6 - 27$ and $\mathrm{Leo}(L_{t_0}, p)$ holds there exists $m \geq 2$ such that for every $t' \equiv t_0 \pmod{p^m}$ we have $\mathrm{Leo}(L_{t'}, p)$ as well. Since $d_{f_t} = 4t^6 - 27$ we conclude that the family considered is infinite by Proposition 3.7.9. For every prime number p, if we are able to verify Leopoldt's conjecture for a certain specific number field, we can finally combine this with Corollary 3.4.10 in order to find an infinite family of real S_3-extensions which satisfy Leopoldt's conjecture at p. For instance for $p = 3$ from [JN20, Theorem A.2] we already know Leopoldt's conjecture at 3 for a wide family of totally real non-Galois cubic fields. We can expect to be able to obtain similar results for other families of cubic fields, e.g. from [Ste72] and [Tho79].

Using the results in §3.7.2 for $p \neq 3$ and in Example 3.7.11 for $p = 3$, with [JN20, Theorem A.2] as already remarked, we can now prove the following.

Theorem 3.7.12. *Let $\mathcal{A}$ be a finite set of prime numbers. Then there exists an infinite family $\mathcal{L}$ of real S_3-extensions of $\mathbb{Q}$ such that $\mathrm{Leo}(L, p)$ holds for every $L \in \mathcal{L}$ and $p \in \mathcal{A}$.*

Proof. If $3 \notin \mathcal{A}$, then it is sufficient to take the Galois closures of the polynomials $x^3 - t^2x - 1$ with t divisible by all the primes in $\mathcal{A}$, by Theorem 3.7.6. Otherwise we first of all find a family of polynomials $x^3 - t^2x - 1$ with t in some arithmetic progression with coefficient a power of 3 which satisfy Leopoldt's conjecture at 3 (see Example 3.7.11); then by the Chinese remainder problem we can extrapolate from this an infinite subfamily such that t is divisible by every other prime of $\mathcal{A}$. □

Example 3.7.13. We now focus on quartic fields. By [Nak93, Proposition 6] we can consider the family $\{f_t = x^4 - tx^3 - x^2 + tx + 1\}_{t \geq 7}$ of totally real quartic fields with Galois closure of Galois group D_8 over $\mathbb{Q}$. Then for every $t \geq 7$ we can choose a root λ_t of f_t so that $\lambda_t - 1, \lambda_t, \lambda_t + 1$ is a system of fundamental units for $L_t = \mathbb{Q}(\lambda_t)$. Hence we can apply Corollary 3.7.8 to conclude that, if for a certain $t_0 \geq 7$ and prime p we have $p^2 \nmid d_{f_{t_0}}$ and $\mathrm{Leo}(L_{t_0}, p)$ holds, then we have $\mathrm{Leo}(L_{t'}, p)$ whenever $t' - t_0$ is divisible by a sufficiently high power of p. Moreover as shown in the same article $d_{f_t} = (t^2 - 4)^2(4t^2 + 9)$, hence we can use Proposition 3.7.9 to guarantee that if t lies in an arithmetic progression we have an infinite family of number fields. That this particular whole family is infinite was already shown in [Nak93] using a result from [Nag22] (c.f. Remark 3.7.10). Now note that, denoting by $\tilde{L}_t$ the Galois closure of L_t, there is a subgroup H of $\mathrm{Gal}(\tilde{L}_t/\mathbb{Q}) \cong D_8$ isomorphic to C_2^2 such that for every subgroup of H of order 2 the fixed field is (in the isomorphism class of) the considered quartic field or abelian over $\mathbb{Q}$ with Galois group isomorphic to C_2^2. By Theorem 3.2.1 and Corollary 3.4.2 applied to the extension $\tilde{L}_t/L^H$, we conclude that $\mathrm{Leo}(\tilde{L}_t, p)$ holds

whenever $\mathrm{Leo}(L_t, p)$ holds. Note that $\tilde{L}_t$ is totally real as well, so that we developed an algorithmic strategy to show Leopoldt's conjecture for an infinite family of real D_8-extensions.

Chapter 4

On Fitting ideals, K-theory and the Brumer-Stark conjecture

4.1 Introduction

Let p be a prime number and G be a finite group such that $p \nmid |G'|$, where G' denotes the commutator of G. In this setting as we will see the group ring $\mathbb{Z}_p[G]$ is a finite product of matrix rings over commutative $\mathbb{Z}_p$-orders (see Theorem 4.2.18). Inspired by the classical notion of (commutative) Fitting ideals, Nickel [Nic10] and then Johnston and Nickel [JN13] defined and studied the properties of certain non-commutative Fitting ideals, which we will define in §4.2.2. If M is a finitely presented $\mathbb{Z}_p[G]$-module, then $\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M)$ will be an ideal in the centre $\zeta(\mathbb{Z}_p[G])$ of $\mathbb{Z}_p[G]$. The advantage of Fitting ideals is that they are contained in the annihilator of M but are much easier to compute.

Now let $\theta \in \zeta(\mathbb{Q}_p[G])^\times$. Finding methods to determine whether $\theta \in \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M)$ is an important question that has applications to several arithmetic conjectures, including the Brumer-Stark conjecture. If $H = G_1/G_2$ is a subquotient of G, then we can define certain quotient and restriction maps

$$\mathrm{res}^G_{G_1} : \zeta(\mathbb{Q}_p[G])^\times \longrightarrow \zeta(\mathbb{Q}_p[G_1])^\times$$

and

$$\mathrm{quot}^{G_1}_H : \zeta(\mathbb{Q}_p[G_1])^\times \longrightarrow \zeta(\mathbb{Q}_p[H])^\times.$$

We define $f_H = \mathrm{quot}^{G_1}_H \circ \mathrm{res}^G_{G_1}$ and we denote by M_H the module obtained by composing the restriction of scalars of M from $\mathbb{Z}_p[G]$ to $\mathbb{Z}_p[G_1]$ with the map obtained from the projection $\mathbb{Z}_p[G_1] \twoheadrightarrow \mathbb{Z}_p[H]$. Our main question will be to understand whether $\theta \in \mathrm{Fitt}_{\mathbb{Z}_p[G]}(M)$ knowing that $f_H(\theta) \in \mathrm{Fitt}_{\mathbb{Z}_p[H]}(M_H)$ for every H in a certain family $\mathcal{H}$, typically of abelian subquotients. We will be particularly interested in the case in which M is a $\mathbb{Z}_p$-torsion $\mathbb{Z}_p[G]$-module with quadratic presentation (that is, it has a presentation such that the two free modules have the same dimension). Let $\mathcal{H}$ be a family of subquotients of G. We consider the map

$$f_{\mathcal{H}} := \prod_{H \in \mathcal{H}} f_H : \zeta(\mathbb{Q}_p[G])^\times \longrightarrow \prod_{H \in \mathcal{H}} \zeta(\mathbb{Q}_p[H])^\times.$$

Our main theorem is the following (see Theorem 4.6.4).

Theorem 4.1.1. *Suppose that*

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}}\left(\mathbb{Z}_p[H]\cap\zeta(\mathbb{Q}_p[H])^\times\right)\right)\subseteq\mathbb{Z}_p[G]. \tag{4.1.1}$$

Let $\theta\in\zeta(\mathbb{Q}_p[G])^\times$ and let M be a finitely presented $\mathbb{Z}_p$-torsion $\mathbb{Z}_p[G]$-module with quadratic presentation. If $f_H(\theta)\in\mathrm{Fitt}_{\mathbb{Z}_p[H]}(M_H)$ for every $H\in\mathcal{H}$, then $\theta\in\mathrm{Fitt}_{\mathbb{Z}_p[G]}(M)$.

Throughout §4.6 we will find several families of groups G and sets $\mathcal{H}$ of subquotients such that (4.1.1) holds. The computations, although not always immediate, will use rather elementary tools.

We will apply our results to the Brumer-Stark conjecture, providing more direct proofs of the (non-abelian) Brumer-Stark conjecture than other proofs in the literature (note that our statements about the Brumer-Stark conjecture will not cover any new case). See §4.10.1 for the statement and overview of the Brumer-Stark conjecture. The key result we are going to use is Dasgupta and Kakde's proof of the abelian Brumer-Stark conjecture outside 2 [DK20]. The strong refinement that they prove predicts that, if L/K is an abelian CM-extension of number fields, S and T are two 'admissible' finite sets of places of K and p is an odd prime number, then a certain Stickelberger element $\theta_S^T(L/K)^\sharp$ is in the Fitting ideal $\mathrm{Fitt}_{\mathbb{Z}_p[G]_-}(\mathrm{Cl}^T(L)^{\vee,-}(p))$; here $\mathrm{Cl}^T(L)^{\vee,-}(p)$ is the p-Sylow of the minus part of the dual of a 'T-corrected' ideal class group and $\mathbb{Z}_p[G]_-$ is the minus part of $\mathbb{Z}_p[G]$. In every (not necessarily abelian) Galois CM-extension of number fields $\theta_S^T(L/K)^\sharp\in\zeta(\mathbb{Q}_p[G]_-)^\times$ is constructed via special values of Artin L-functions (for the definition of CM-fields and extensions see Definition 4.10.3).

The application of Theorem 4.1.1 to the Brumer-Stark conjecture is the following (see Theorem 4.10.18).

Theorem 4.1.2. *Let p be an odd prime number. Let L/K be a Galois CM-extension of number fields with Galois group G such that $p\nmid|G'|$ and let $\mathcal{H}$ be a family of abelian subquotients of G. Suppose that the complex conjugation j belongs to G_1 for every $G_1/G_2\in\mathcal{H}$. Let S and T be two admissible sets of primes (as in the beginning of §4.10.1). Suppose that we have the containment (4.1.1) and that $\mathrm{Cl}(L)^T(p)$ has a quadratic presentation. Then the p-part of the strong Brumer-Stark conjecture for L/K holds.*

We will provide many infinite families and examples of groups G for which Theorem 4.1.2 applies. For instance we have the following applications (see the end of §4.10.3).

Theorem 4.1.3. *Let $G\ncong\mathrm{SL}_2(\mathbb{F}_3)$ be a group of order less than 48, let p an odd prime number such that $p\nmid|G'|$ and let Q be an abelian group such that $p\nmid|Q|$ and each cyclic component has order dividing $p-1$. Let L/K be a CM $G\times Q$-extension. Then, for every pair of admissible sets S and T such that $\mathrm{Cl}(L)^T(p)$ has a quadratic presentation, the p-part of the Brumer-Stark conjecture holds.*

Theorem 4.1.4. *Let L/K be a Galois CM-extension of number fields with Galois group $F\times A$, where F is a Frobenius group and A is an abelian group. Let p be an odd prime number such that $p\nmid|F'|$ and $p\nmid|A|$. Then L/K satisfies the p-part of the Brumer-Stark conjecture.*

This will for instance imply the Brumer-Stark conjecture at 3 in every $A_4 \times C_2$-extension (note that we are not imposing quadratic presentation).

Our approach will also provide a direct proof of the weak Brumer-Stark conjecture for monomial Galois groups (see Corollary 4.10.22).

4.2 Fitting ideals

4.2.1 Commutative Fitting ideals

(Commutative) Fitting ideals were first introduced in [Fit36]. Here we give the basic definitions and summarise some of the main properties.

Definition 4.2.1. Let R be a commutative ring and let M a finitely presented R-module. Let

$$R^n \xrightarrow{h} R^m \longrightarrow M \longrightarrow 0$$

be a presentation of M. By choosing bases for R^n and R^m we may identify h with an $(n \times m)$-matrix C. We define the *Fitting ideal* of M to be

$$\mathrm{Fitt}_R(M) = \begin{cases} 0 & \text{if } n < m \\ \langle \det(B) : B \text{ is an } (m \times m) - \text{submatrix of } C \rangle_R & \text{if } n \geq m. \end{cases}$$

The following proposition tells us that Fitting ideals are well defined.

Proposition 4.2.2. *Definition 4.2.1 does not depend on the presentation of M nor on the choice of bases for the free modules.*

Proof. See [Nor76, Theorem 3.1]. □

Another important object we can attach to an R-module M is the annihilator ideal $\mathrm{Ann}_R(M)$. A key property of the Fitting ideals is the following.

Proposition 4.2.3. *Let R be a commutative ring and let M be a finitely presented R-module. Then*

$$\mathrm{Fitt}_R(M) \subseteq \mathrm{Ann}_R(M).$$

Proof. We follow [Nic10, Theorem 4.2]. We consider a free resolution

$$R^n \xrightarrow{h} R^m \longrightarrow M \longrightarrow 0.$$

The result is trivial if $n < m$, so we assume $n \geq m$. Let C be a matrix corresponding to h and let B be an $m \times m$-submatrix of C. We need to prove that $\det(B) \in \mathrm{Ann}_R(M)$. Let d_{ji} be the determinant of the matrix obtained by removing the j-th row and i-th column from B and let

$$B^* = ((-1)^{i+j} d_{ji})_{1 \leq i,j \leq n}$$

be the adjugate of B, so that $BB^* = B^*B = \det(B)I$. Then we have the following commutative diagram:

$$\begin{array}{ccccccc} R^m & \xrightarrow{B} & R^m & \longrightarrow & \operatorname{coker}(B) & \longrightarrow & 0 \\ & \swarrow^{B^*} & \downarrow{\scriptstyle \det(B)} & & \downarrow{\scriptstyle \det(B)} & & \\ R^m & \xrightarrow{B} & R^m & \longrightarrow & \operatorname{coker}(B) & \longrightarrow & 0, \end{array}$$

which tells us that multiplication by $\det(B)$ is 0 on $\operatorname{coker}(B)$. Since $\operatorname{coker}(B)$ surjects onto $\operatorname{coker}(C) \cong M$, then $\det(B)$ annihilates M. □

The advantage of Fitting ideals as opposed to annihilators is that they can be computed more easily. For instance we have the following.

Proposition 4.2.4. *Let R be a commutative ring and let M_1, M_2 and M_3 be finitely presented R-modules. Then we have the following:*

(i) if there exists a surjection $M_1 \twoheadrightarrow M_2$ then $\operatorname{Fitt}_R(M_1) \subseteq \operatorname{Fitt}_R(M_2)$;

(ii) if $M_2 \cong M_1 \oplus M_3$ then

$$\operatorname{Fitt}_R(M_1) \cdot \operatorname{Fitt}_R(M_3) = \operatorname{Fitt}_R(M_2);$$

(iii) if $M_1 \to M_2 \to M_3 \to 0$ is an exact sequence then

$$\operatorname{Fitt}_R(M_1) \cdot \operatorname{Fitt}_R(M_3) \subseteq \operatorname{Fitt}_R(M_2).$$

The proofs are quite straightforward, see [Nic20, Lemma 1.8] for a sketch.

Definition 4.2.5. Let R be a (not necessarily commutative) ring and let M be a finitely presented R-module. If M admits a presentation

$$R^n \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

for some $n \geq 1$, we will say that M has *quadratic presentation*.

Remark 4.2.6. If R is a commutative ring and M is an R-module with quadratic presentation, then $\operatorname{Fitt}_R(M)$ is principal generated by the determinant of the matrix corresponding to $R^n \to R^n$.

4.2.2 Non-commutative Fitting ideals: the case of matrix rings over commutative orders

We follow [JN13, §2]. Note that some of the results we cite refer to a more general notion of Fitting invariants. See [JN13, Proposition 3.4] and [JN13, (3.5)] for the equivalence between the various definitions.

We start by recalling Morita equivalence. The theory is explained in [Lam99, §17B], [Rei03, Chapter 4] and [CR81, §3D], and we only present the specific special case of matrix rings over commutative rings.

Notation 4.2.7. Let $n \geq 1$ be a natural number. For every $1 \leq i, j \leq n$ we will denote by e_{ij} the matrix with 1 in position (i, j) and 0 otherwise.

Remark 4.2.8. Let $n \geq 1$ be an integer, let Γ be a commutative ring and let M be a $M_{n\times n}(\Gamma)$-module. We can easily show that $e_{ii}M \cong e_{jj}M$ as Γ-modules for every $1 \leq i, j \leq n$ (see [JN13, Lemma 2.1]).

Theorem 4.2.9. *Let Γ be a commutative ring, let $n \in \mathbb{N}$ and let $\Lambda = M_{n\times n}(\Gamma)$. Let $e_{11} \in \Lambda$ be as in Notation 4.2.7. Let ${}_\Gamma\mathfrak{M}$ and ${}_\Lambda\mathfrak{M}$ be the categories of left Γ-modules and left Λ-modules, respectively. Then for every $1 \leq i \leq n$ the following are mutually inverse category equivalences:*

$$\begin{aligned} \mathcal{F} : {}_\Lambda\mathfrak{M} &\longrightarrow {}_\Gamma\mathfrak{M} \\ M &\longmapsto e_{ii}\Lambda \otimes_\Lambda M \end{aligned}$$

and

$$\begin{aligned} \mathcal{G} : {}_\Gamma\mathfrak{M} &\longrightarrow {}_\Lambda\mathfrak{M} \\ N &\longmapsto \Lambda e_{ii} \otimes_\Gamma N. \end{aligned}$$

Proof. See for instance [Lam99, Theorem (17.20)]. □

Remark 4.2.10. The equivalences in Theorem 4.2.9 restrict to the full subcatergories of, for example, projective, injective or finitely generated modules, but not to free modules. In general $\mathcal{F}$ and $\mathcal{G}$ preserve all the possible 'categorical properties' of Λ- and Γ-modules (see [Lam99, Remarks (17.3)]).

Motivated by the explicit Morita equivalence in Theorem 4.2.9, we provide the following definition of non-commutative Fitting ideals, introduced in [JN13].

Definition 4.2.11. Let Γ be a commutative ring, let $n \in \mathbb{N}$ and let $\Lambda = M_{n\times n}(\Gamma)$. Let M be a finitely presented Λ-module. We define

$$\mathrm{Fitt}_\Lambda(M) = \mathrm{Fitt}_\Gamma(e_{11}M).$$

Note that Definition 4.2.11 recovers Definition 4.2.1 when $n = 1$. Also note that Γ is the centre of Λ.

Remark 4.2.12. By Remark 4.2.8, we have an isomorphism $\mathrm{Fitt}_\Gamma(e_{11}M) \cong \mathrm{Fitt}_\Gamma(e_{ii}M)$ for every $1 \leq i \leq n$.

Similarly to Proposition 4.2.3, we have the following (see [JN13, Theorem 2.2(ii)]).

Proposition 4.2.13. *Let Γ be a commutative ring, let $n \in \mathbb{N}$ and let $\Lambda = M_{n\times n}(\Gamma)$. Let M be a finitely presented Λ-module. Then*

$$\mathrm{Fitt}_\Lambda(M) \subseteq \mathrm{Ann}_\Lambda(M).$$

Sketch of a proof. By Remark 4.2.12, we have that $\mathrm{Fitt}_\Lambda(M) = \mathrm{Fitt}_\Gamma(e_{ii}M)$ for every i. We have that $e_{11} + \cdots + e_{nn}$ is the identity matrix and $e_{ii}M \cap e_{jj}M = 0$ for every $i \neq j$, so that

$$M \cong e_{11}M \oplus \cdots \oplus e_{nn}M.$$

By Proposition 4.2.3 we have $\mathrm{Fitt}_\Lambda(M) = \mathrm{Fitt}_\Gamma(e_{ii}M) \subseteq \mathrm{Ann}_\Gamma(e_{ii}M)$ for every i, which implies our statement. □

Remark 4.2.14. Note that $\mathrm{Ann}_\Lambda(M) = M_{n\times n}(\mathrm{Ann}_\Gamma(M))$.

Also in this general setting we have that $\mathrm{Fitt}_\Lambda(M)$ is an easily computable algebraic object. Indeed we have the following (see [JN13, Theorem 2.2]).

Proposition 4.2.15. *Let Γ be a commutative ring, let $n \in \mathbb{N}$ and let $\Lambda = M_{n\times n}(\Gamma)$. Let M_1, M_2, M_3 be finitely presented Λ-modules. Then we have the following:*

(i) if there exists a surjection $M_1 \twoheadrightarrow M_2$ then $\mathrm{Fitt}_R(M_1) \subseteq \mathrm{Fitt}_R(M_2)$;

(ii) if $M_2 \cong M_1 \oplus M_3$ then

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) = \mathrm{Fitt}_R(M_2);$$

(iii) if $M_1 \to M_2 \to M_3 \to 0$ is an exact sequence then

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) \subseteq \mathrm{Fitt}_R(M_2);$$

(iv) we have $\mathrm{Fitt}_\Gamma(M) = \mathrm{Fitt}_\Lambda(M)^n$.

Remark 4.2.16. If M has a quadratic presentation as a Λ-module, then it is straightforward to verify that $e_{11}M$ has a quadratic presentation as a Γ-module (we can see it via Morita equivalence, see Theorem 4.2.9). Hence in this case $\mathrm{Fitt}_\Lambda(M)$ is a principal R-ideal.

Definition 4.2.17. Let Λ be a finite product $\prod_i M_{n_i\times n_i}(\Gamma_i)$, where Γ_i is a commutative ring for every i. Let e_i be the idempotent corresponding to $M_{n_i\times n_i}(\Gamma_i)$. Let M be a finitely presented Λ-module. Then we define $\mathrm{Fitt}_\Lambda(M) = \bigoplus_i \mathrm{Fitt}_{\Lambda_i}(e_iM)$, as an ideal of $\prod_i \Gamma_i$.

We have the following important result (see [DJ83, Corollary on page 390] and [JN13, Proposition 4.4]).

Theorem 4.2.18. *Let R be a complete discrete valuation ring with residue characteristic $p > 0$ and let G be a finite group such that $p \nmid |G'|$, where G' denotes the commutator subgroup of G. Then $R[G]$ is a product of matrix rings over commutative R-orders.*

Lemma 4.2.19. *Let Λ be a finite product of matrix rings over commutative rings and let $e \in \Lambda$ be a central idempotent. Then $e\Lambda$ is a finite product of matrix rings over commutative rings.*

Proof. Let $\Lambda = \prod_i M_{n_i\times n_i}(\Gamma_i)$. Since e is central, we can write $e = \prod_i e_i$ where $e_i \in \Gamma_i$ is a central idempotent. Then for every i we have $e_iM_{n_i\times n_i}(\Gamma_i) = M_{n_i\times n_i}(e_i\Gamma_i)$. Since $e_i\Gamma_i$ is a commutative ring then this implies the statement. □

Remark 4.2.20. From the proof of Lemma 4.2.19, if R is a Dedekind domain and Λ is a finite product of matrix rings over commutative R-orders, then so is $e\Lambda$.

4.3 An introduction to algebraic K-theory

For a good account of algebraic K-theory see [CR87, Chapter 5] and [Bre04, §2].

Let R be a noetherian integral domain of characteristic 0 with field of fractions F. Let A be a finite-dimensional semisimple F-algebra and let Λ be an R-order in A. We denote by $K_0(\Lambda)$ the *Grothendieck group* of the category of finitely generated projective (left) Λ-modules, that is, the abelian group generated by the expressions $[M]$ for each isomorphism class (M) of finitely generated projective Λ-modules, modulo the subgroup generated by $[M \oplus M'] - [M] - [M']$ for all M, M'.

More generally, the Grothendieck group $K_0(\mathcal{C})$ of an abelian category $\mathcal{C}$ is the abelian group generated by the objects of $\mathcal{C}$ modulo the relations coming from short exact sequences (indeed, note that short exact sequences of projective modules split, so that in the definition above direct sums suffice).

We now consider the collection of all ordered pairs (M, μ), where M is a finitely generated projective Λ-module and $\mu \in \mathrm{Aut}_\Lambda(M)$. A morphism $f : (M, \mu) \to (N, \nu)$ is an element $f \in \mathrm{Hom}_\Lambda(M, N)$ for which

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\mu}\downarrow & & \downarrow{\scriptstyle\nu} \\ M & \xrightarrow{f} & N \end{array}$$

commutes. We define

$$0 \longrightarrow (L, \lambda) \xrightarrow{f} (M, \mu) \xrightarrow{g} (N, \nu) \longrightarrow 0 \tag{4.3.1}$$

to be a short exact sequence if f and g are morphisms such that

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

is exact. It follows that $f : (M, \mu) \to (N, \nu)$ is an isomorphism if $f : M \cong N$. We define the *Whitehead group* $K_1(\Lambda)$ to be the abelian group generated by all isomorphism classes of pairs (M, μ), denoted by $[M, \mu]$, modulo $[M, \mu] - [L, \lambda] - [N, \nu]$ whenever we have a short exact sequence as in (4.3.1) and modulo $[M, \mu\mu'] - [M, \mu] - [M, \mu']$ for every $\mu, \mu' \in \mathrm{Aut}_\Lambda(M)$. Alternatively, let $\mathrm{GL}(\Lambda)$ be the general linear group $\varinjlim \mathrm{GL}_n(\Lambda)$, where the direct limit is constructed from the maps

$$\begin{aligned} \mathrm{GL}_n(\Lambda) &\longrightarrow \mathrm{GL}_{n+1}(\Lambda) \\ X &\longmapsto \begin{pmatrix} X & 0 \\ 0 & 1 \end{pmatrix}; \end{aligned}$$

then we can verify that $K_1(\Lambda) = \mathrm{GL}(\Lambda)/\mathrm{GL}'(\Lambda)$, where $\mathrm{GL}'(\Lambda)$ is the commutator subgroup of $\mathrm{GL}(\Lambda)$ (see [CR81, Theorem (40.6)]).

Let K/F be a field extension. Let us consider the classes (M, g, N), where M and N are finitely generated projective Λ-modules and

$$g : K \otimes_R M \longrightarrow K \otimes_R N$$

is an isomorphism of $K\otimes_F A$-modules. A morphism $(M,g,N)\to(M',g',N')$ is a pair of morphisms $\mu: M\to M'$ and $\nu: N\to N'$ such that $g'\circ(\mathrm{id}_{K\otimes_F A}\otimes_R\mu)=(\mathrm{id}_{K\otimes_F A}\otimes_R\nu)\circ g$; it will be an isomorphism if both μ and ν are isomorphisms. In a similar way to (4.3.1), we can define exact sequences. We define $K_0(\Lambda,K)$ to be the abelian group generated by the isomorphism classes $[M,g,N]$ modulo the expressions coming from short exact sequences as above and modulo the expressions $[M,hg,P]-[M,g,N]-[N,h,P]$.

Let A' be another finite-dimensional semisimple F-algebra and let Λ' be an R-order in A'. Suppose we have a ring homomorphism $\varphi:\Lambda\to\Lambda'$. Then the tensor product $\Lambda'\otimes_\Lambda\cdot$ induces a map φ_* from $K_0(\Lambda)$ to $K_0(\Lambda')$, from $K_1(\Lambda)$ to $K_1(\Lambda')$ and from $K_0(\Lambda,K)$ to $K_0(\Lambda',K)$. If Λ' is projective as a Λ-module, then we also obtain a map φ^* in the opposite direction by restriction of scalars.

Analogously, the inclusion $\Lambda\hookrightarrow K\otimes_F A$ induces a map between the Grothendieck groups and between the Whitehead groups.

By [Swa68, Chapter 15], we have the following long exact sequence between the K-groups (we omit the definition of δ):

$$K_1(\Lambda)\longrightarrow K_1(K\otimes_F A)\xrightarrow{\delta} K_0(\Lambda,K)\longrightarrow K_0(\Lambda)\longrightarrow K_0(K\otimes_F A). \tag{4.3.2}$$

Remark 4.3.1. Let A' be another finite-dimensional semisimple F-algebra and let Λ' be an R-order in A'. Let $\varphi:\Lambda\to\Lambda'$ be a ring homomorphism. Suppose that Λ' is projective over Λ (otherwise ignore the first row in the following diagram). Then we can define $K\otimes_R\varphi: K\otimes_R A\to K\otimes_R A'$. We have that the following diagram is commutative (see [Bre04, §2.1.5]):

$$\begin{array}{ccccccccc}
K_1(\Lambda') & \longrightarrow & K_1(K\otimes_F A') & \xrightarrow{\delta} & K_0(\Lambda',K) & \longrightarrow & K_0(\Lambda') & \longrightarrow & K_0(K\otimes_F A') \\
\downarrow{\scriptstyle\varphi^*} & & \downarrow{\scriptstyle(K\otimes_R\varphi)^*} & & \downarrow{\scriptstyle\varphi^*} & & \downarrow{\scriptstyle\varphi^*} & & \downarrow{\scriptstyle(K\otimes_R\varphi)^*} \\
K_1(\Lambda) & \longrightarrow & K_1(K\otimes_F A) & \xrightarrow{\delta} & K_0(\Lambda,K) & \longrightarrow & K_0(\Lambda) & \longrightarrow & K_0(K\otimes_F A) \\
\downarrow{\scriptstyle\varphi_*} & & \downarrow{\scriptstyle(K\otimes_R\varphi)_*} & & \downarrow{\scriptstyle\varphi_*} & & \downarrow{\scriptstyle\varphi_*} & & \downarrow{\scriptstyle(K\otimes_R\varphi)_*} \\
K_1(\Lambda') & \longrightarrow & K_1(K\otimes_F A') & \xrightarrow{\delta} & K_0(\Lambda',K) & \longrightarrow & K_0(\Lambda') & \longrightarrow & K_0(K\otimes_F A').
\end{array}$$

We conclude the subsection with the following result (see [Nic10, §1.0.1] or [CR87, end of §40B]).

Proposition 4.3.2. *The relative K-group $K_0(\Lambda,F)$ is isomorphic to the Grothendieck group of the category of finitely generated R-torsion Λ-modules of finite projective dimension over Λ.*

4.3.1 Reduced norms

We follow [CR81, §7D]. Let F be a field and let A be a separable F-algebra. Let E be a splitting field for A over F (see [CR81, §7B]) and let h be an isomorphism

$$h: E\otimes_F A\cong\prod_i M_{n_i\times n_i}(E).$$

For every $a \in A$, we write $h(1 \otimes a) = \prod_i a_i$, where $a_i \in M_{n_i \times n_i}(E)$ for every i. Let p_i be the characteristic polynomial of the matrix a_i and let $\mathrm{rch}_{A/F} = \prod_i p_i$ be the *reduced characteristic polynomial* of a, which is independent of E and h and has coefficients in F.

Definition 4.3.3. In the above setting, we define the *reduced norm* $\mathrm{nr}_{A/F}$ as the constant term of $\mathrm{rch}_{A/F}$ times $(-1)^m$, where m is the degree of $\mathrm{rch}_{A/F}$.

Notation 4.3.4. Let R be a ring. We denote by $\zeta(R)$ the centre of R.

If A is a simple algebra, we define $\mathrm{nr}_A = \mathrm{nr}_{A/\zeta(A)}$. If more generally $A = \prod_i A_i$ for certain simple algebras A_i, then we define

$$\mathrm{nr}_A = \prod_i \mathrm{nr}_{A_i/\zeta(A_i)} : A \longrightarrow \zeta(A) = \prod_i \zeta(A_i).$$

We have the following.

Theorem 4.3.5. *[CR81, Theorem (7.45)] Let F be the quotient field of a complete discrete valuation ring and let A be a separable F-algebra. Then* $\mathrm{nr}(A^\times) = \zeta(A)^\times$.

We can extend the reduced norm to the Whitehead group. We note that, if $X \in \mathrm{GL}_n(A)$, then

$$\mathrm{nr}_A \begin{pmatrix} X & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{nr}_A(X),$$

so that nr_A is defined on $\mathrm{GL}(A)$. Since $\mathrm{nr}_A(\mathrm{GL}'(A)) = 1$, then nr_A is well defined on $K_1(A)$ (note that we can define the Whitehead group in this generality).

Theorem 4.3.6. *[CR87, Theorem (45.3)] Let F be the quotient field of a complete discrete valuation ring and let A be a separable F-algebra. Then* nr_A *induces an isomorphism*

$$\mathrm{nr}_A : K_1(A) \cong \zeta(A)^\times.$$

Lemma 4.3.7. *Let R be a complete discrete valuation ring with field of fractions F, let A be a separable F-algebra. Let Λ be an R-order in A which is a finite product of matrix rings over commutative R-orders. Then* $\mathrm{nr}_A(K_1(\Lambda)) = \mathrm{nr}_A(\Lambda^\times) = \zeta(\Lambda)^\times$.

Sketch of a proof. We can suppose we are working on a single component $M_{n\times n}(\Gamma)$, with Γ commutative. Then the reduced norm is simply the determinant, which is clearly surjective onto Γ. □

Remark 4.3.8. Let F and K be fields of characteristic zero and let G be a finite group. If $\iota : F \hookrightarrow K$ is an injection of fields, then this easily extends to an injection $F[G] \hookrightarrow K[G]$, which restricts to an injection $\zeta(F[G])^\times \hookrightarrow \zeta(K[G])^\times$, still denoted by ι. Then the following diagram is commutative:

$$\begin{array}{ccc} K_1(F[G]) & \xrightarrow{\mathrm{nr}_{F[G]}} & \zeta(F[G])^\times \\ \downarrow{\scriptstyle \iota_*} & & \downarrow{\scriptstyle \iota} \\ K_1(K[G]) & \xrightarrow{\mathrm{nr}_{K[G]}} & \zeta(K[G])^\times. \end{array}$$

Note that in particular ι_* is injective if F and K are quotient fields of complete discrete valuation rings.

4.4 General functoriality

We recall the following definition (see also Definition 2.6.13) for the convenience of the reader.

Definition 4.4.1. Let R be a Dedekind domain with field of fractions F and let Λ be a finitely generated R-order in the F-algebra A. We will say that Λ is a *clean order* if every projective Λ-lattice that spans a free A-module is free.

We recall the following property.

Proposition 4.4.2. *[Rog70, IX Theorem 1.2] Λ is a clean R-order if and only if $\widehat{\Lambda_P}$ is a clean $\widehat{R_P}$-order for every prime ideal P of R, where $\widehat{\cdot_P}$ denotes the completion at P.*

Theorem 4.4.3 (Hattori)**.** *Suppose R is a discrete valuation ring with finite residue field. Then commutative R-orders in finite-dimensional semisimple F-algebras are clean.*

Proof. See [Hat65] or [Rog70, IX Corollary 1.5]. □

The following is known as Swan's Theorem.

Theorem 4.4.4. *Let R be a discrete valuation ring and let G be a finite group. Then $R[G]$ is clean.*

Proof. See [CR81, Theorem (32.1)]. □

Remark 4.4.5. If Λ is a clean order, we can easily verify that the map $K_0(\Lambda) \to K_0(A)$ is an injection.

Remark 4.4.6. By Remark 4.4.5 and (4.3.2), if Λ is clean then $\delta : K_1(A) \to K_0(\Lambda, F)$ is surjective.

Now let R be a complete discrete valuation ring with residue characteristic $p > 0$ and finite residue field and let G be a finite group such that $p \nmid |G'|$. Suppose that F has characteristic 0. Let $e \in R[G]$ be a central idempotent, let $\Lambda = eR[G]$ and let $A = eF[G]$. Let $H = G_1/G_2$ be a subquotient of G such that $e \in R[G_1]$. Let $\Lambda_{G_1} = eR[G_1]$ and let $A_{G_1} = eF[G_1]$. Let $A_H = eF[H] = eF[G_1/G_2]$ and let $\Lambda_H = eR[G_1/G_2]$ be the image of Λ_{G_1} in A_H.

Lemma 4.4.7. *Under the above hypotheses, Λ is a clean order.*

Proof. By Theorem 4.2.18 and Lemma 4.2.19, Λ is a finite product of matrix rings over commutative R-orders. Hence we can assume $\Lambda = M_{n\times n}(\Gamma)$, where Γ is a commutative R-order. By Theorem 4.2.9 we know that multiplication by e_{11} induces a Morita equivalence between the categories of Λ-modules and Γ-modules. Let M be a Λ-lattice such that $FM \cong A^m \cong M_{n\times n}(B)^m$, where $B = F\Gamma$. Then $Fe_{11}M \cong e_{11}M_{n\times n}(B)^m \cong B^{nm}$.

Since Γ is commutative, hence clean by Theorem 4.4.3, we conclude that $e_{11}M \cong \Gamma^{nm}$. By Morita equivalence we can finally conclude that $M \cong \Lambda^m$. □

Lemma 4.4.8. *We have that Λ is free over Λ_{G_1}.*

Proof. Let $g_1, \ldots, g_r$ be a set of representatives of the right quotient $G_1 \setminus G$. Since $e \in R[G_1]$, we can easily check that these form a basis for $eF[G]$ as an $eF[G_1]$-module. Since Λ_{G_1} is a clean order by Lemma 4.4.7, we deduce that Λ is free over Λ_{G_1}. □

Lemma 4.4.9. *In the above notation and setting, let M be a Λ-module with quadratic presentation. Let M_{G_1} be the Λ_{G_1}-module obtained from M by restriction of scalars and let M_H be the Λ_H-module $e_{G_2}M$. Then M_H, as a Λ_H-module, has a quadratic presentation.*

Proof. Let $H = G_1/G_2$ and let

$$\Lambda^n \longrightarrow \Lambda^n \longrightarrow M \longrightarrow 0$$

be a quadratic presentation. Then the above exact sequence of Λ-modules is also an exact sequence of Λ_{G_1}-modules (as $\Lambda_{G_1} \subseteq \Lambda$). By Lemma 4.4.8 we obtain a presentation of Λ_{G_1}-modules as follows:

$$\Lambda_{G_1}^{rn} \longrightarrow \Lambda_{G_1}^{rn} \longrightarrow M_{G_1} \longrightarrow 0$$

for a certain $r \geq 1$. Multiplying the above with e_{G_2}, we obtain the exact sequence

$$\Lambda_H^{rn} \longrightarrow \Lambda_H^{rn} \longrightarrow M_H \longrightarrow 0.$$ □

As in §4.3, composition of quotient with restriction induces the following maps:

$$\begin{gathered}
{}_{\Lambda}\mathfrak{M} \longrightarrow {}_{\Lambda_H}\mathfrak{M} \\
K_0(\Lambda) \longrightarrow K_0(\Lambda_H) \\
K_1(\Lambda) \longrightarrow K_1(\Lambda_H) \\
K_0(\Lambda, K) \longrightarrow K_0(\Lambda_H, K) \\
{}_{A}\mathfrak{M} \longrightarrow {}_{A_H}\mathfrak{M} \\
K_0(A) \longrightarrow K_0(A_H) \\
K_1(A) \longrightarrow K_1(A_H).
\end{gathered}$$

We will denote all these maps by f_H.

Remark 4.4.10. If we further assume that G_2 is normal in G, then we could instead apply the quotient before the restriction, and the map would be the same as f_H. In fact, if M is a Λ-module, then $f_H(M) = e_{G_2}M$, which is the same module with the same module structure as when we swap the operations. From this, we see that the same principle holds for K-groups as well (and the same over the field F).

4.5 Fitting ideals and K-theory

We start by stating the following result.

Lemma 4.5.1. *[Nic10, p. 2764] Let R be a complete discrete valuation ring with field of fractions F. Suppose F has characteristic 0 and R has finite residue field, with characteristic $p > 0$. Let A be a finitely generated semisimple F-algebra. Let Λ be an R-order in A which is the finite product of matrix rings over commutative R-orders. Let M be a quadratically presented R-torsion Λ-module. Let $x \in K_1(A)$ be such that $\delta(x) = [M] \in K_0(\Lambda, F)$ (see Remark 4.4.6, where $[M]$ is an element of $K_0(\Lambda, F)$ as in Proposition 4.3.2). Then $\mathrm{Fitt}_\Lambda(M) = \langle \mathrm{nr}_A(x) \rangle_{\zeta(\Lambda)}$.*

Proof. Let

$$\Lambda^n \xrightarrow{h} \Lambda^n \longrightarrow M \longrightarrow 0.$$

be a quadratic presentation. Then $F \otimes_R h$ can be seen as an element of $\mathrm{GL}_n(A)$, hence of $K_1(A)$. Since $(F \otimes_R h)(\Lambda^n) \subseteq \Lambda^n$, by [CR87, p. 68] and the fact that $M \cong \Lambda^n / h(\Lambda^n)$ we have that $\delta(F \otimes_R h) = [M]$. At the same time, $\mathrm{Fitt}_\Lambda(M)$ is generated by $\mathrm{nr}(F \otimes_R h)$ by [JN13, Proposition 3.4]. □

Note that the hypotheses of Lemma 4.5.1 imply that Λ is a clean order, with the same proof as Lemma 4.4.7.

Proposition 4.5.2. *Assume the hypotheses of Lemma 4.5.1. Let $\theta \in \zeta(A)^\times$. Then θ generates $\mathrm{Fitt}_\Lambda(M)$ if and only if $[M] - \delta \circ \mathrm{nr}_A^{-1}(\theta) = 0$ in $K_0(\Lambda, F)$.*

Proof. We have the following commutative diagram:

$$\begin{array}{ccccccccc} & & K_1(\Lambda) & \xrightarrow{\iota} & K_1(A) & \xrightarrow{\delta} & K_0(\Lambda, F) & \longrightarrow & 0 \\ & & \downarrow & & \wr\downarrow & & \wr\downarrow & & \\ 0 & \longrightarrow & \zeta(\Lambda)^\times & \longrightarrow & \zeta(A)^\times & \longrightarrow & \zeta(A)^\times/\zeta(\Lambda)^\times & \longrightarrow & 0 \end{array}$$

where the vertical maps are induced by the reduced norm. Note that $SK_1(\Lambda) := \ker \mathrm{nr}_A \,|_{K_1(\Lambda)}$ may not be trivial, but nr_A induces an isomorphism between $\iota(K_1(\Lambda))$ and $\zeta(\Lambda)^\times$ by Lemma 4.3.7. Now, since by definition $[M] - \delta(x) = 0$, we deduce that

$$\begin{aligned} [M] - \delta \circ \mathrm{nr}_A^{-1}(\theta) = 0 &\Leftrightarrow \delta \circ \mathrm{nr}_A^{-1}(\theta) = \delta(x) \Leftrightarrow \delta(x^{-1}\mathrm{nr}_A^{-1}(\theta)) = 0 \\ &\Leftrightarrow x^{-1}\mathrm{nr}_A^{-1}(\theta) \in \iota(K_1(\Lambda)) \Leftrightarrow \mathrm{nr}_A(x)^{-1}\theta \in \zeta(\Lambda)^\times \\ &\Leftrightarrow \theta \in \zeta(\Lambda)^\times \mathrm{nr}_A(x). \end{aligned}$$

This is what we wanted to prove as, by Lemma 4.5.1, $\zeta(\Lambda)^\times \mathrm{nr}_A(x)$ is the set of generators of $\mathrm{Fitt}_\Lambda(M) = \zeta(\Lambda)\mathrm{nr}_A(x)$. □

Notation 4.5.3. Let R be a complete discrete valuation ring with residue characteristic $p > 0$ and finite residue field and let G be a finite group such that $p \nmid |G'|$. Suppose that the field of fractions F of R has characteristic 0. Let $e \in R[G]$ be central idempotent and let $\Lambda = eR[G]$ and $A = eF[G]$. If $\theta \in \zeta(A)^\times$ and H is a subquotient of G, we will identify f_H with $\mathrm{nr}_{A_H} \circ f_H \circ \mathrm{nr}_A^{-1}$ and denote $\theta_H = f_H(\theta)$. Note that $f_H : \zeta(A)^\times \to \zeta(A_H)^\times$ is a homomorphism (since it is so on the K-groups).

By Remark 4.3.1 and Proposition 4.5.2, we have the following.

Corollary 4.5.4. *In the notation and setting of §4.4, suppose that there exists a family $\mathcal{H}$ of subquotients such that*

$$f_{\mathcal{H}} := \prod_{H\in\mathcal{H}} f_H : K_0(\Lambda, F) \longrightarrow \prod_{H\in\mathcal{H}} K_0(\Lambda_H, F)$$

is injective. Let $\theta \in \zeta(A)^\times$. If θ_H generates $\mathrm{Fitt}_{\Lambda_H}(M_H)$ for every $H \in \mathcal{H}$, then θ generates $\mathrm{Fitt}_\Lambda(M)$.

Remark 4.5.5. Let p be an odd prime number. Suppose $\Lambda = \mathbb{Z}_p[G]$ with $p \nmid |G'|$. Then by [Bur04, Theorem 4.1], [GRW99, Lemma 3(i)] and [GRW99, Proposition 9], as a family $\mathcal{H}$ for Corollary 4.5.4 we can consider the set of p-elementary subquotients of G (a p-elementary group is a direct product of a p-group and cyclic group of order coprime to p). If G has a central element j of order 2 and $\Lambda = \mathbb{Z}_p[G]_- := \frac{1-j}{2}\mathbb{Z}_p[G]$, by the proof of [Nic16, Proposition 6.2] we can consider as $\mathcal{H}$ the family of subquotients which either contain j and are p-elementary or are direct products of a p-elementary subquotient and the group of order 2 generated by j. Since the p-Sylow subgroup of G must be abelian, note that in all these cases every $H \in \mathcal{H}$ is abelian.

Notation 4.5.6. Fix a prime number p and a finite group G. We will denote by $\mathrm{Irr}(G)$ the set of irreducible $\mathbb{C}_p$-characters (which are in 1-to-1 correspondence with the set of irreducible complex characters).

Remark 4.5.7. Let G be a finite group and let $H = G_1/G_2$ be a subquotient of G. We have an explicit description of the restriction map f_{G_1}, which we will also denote by $\mathrm{res}^G_{G_1}$ (analogously we will use the expression $\mathrm{quot}^{G_1}_H$ for the quotient). In fact, if we look directly at the groups of units and not at the K-groups, we have the following:

$$\begin{aligned}\mathrm{res}^G_{G_1} : \zeta(\mathbb{C}_p[G])^\times &\longrightarrow \zeta(\mathbb{C}_p[G_1])^\times\\ (\alpha_\chi)_{\chi\in\mathrm{Irr}(G)} &\longmapsto \left(\prod_{\chi\in\mathrm{Irr}(G)} \alpha_\chi^{\langle\chi,\mathrm{Ind}^G_{G_1}\psi\rangle_G}\right)_{\psi\in\mathrm{Irr}(G_1)} = \left(\prod_{\chi\in\mathrm{Irr}(G)} \alpha_\chi^{\langle\mathrm{Res}^G_{G_1}\chi,\psi\rangle_{G_1}}\right)_{\psi\in\mathrm{Irr}(G_1)}\end{aligned} \tag{4.5.1}$$

see for instance [Bre04, Lemma 2.4 and §3.2.2]; for an introduction to character theory and the notation see §3.5.1. Note that if $\mathrm{Ind}^G_{G_1}\psi$ is irreducible then the ψ-component of $\mathrm{res}^G_{G_1}((\alpha_\chi)_{\chi\in\mathrm{Irr}(G)})$ is $\alpha_{\mathrm{Ind}^G_{G_1}\psi}$. By the commutativity stated in Remark 4.3.1 (with $R = F$) together with Remark 4.3.8, we can use (4.5.1) to compute an image θ_H when we work with algebras over smaller fields than $\mathbb{C}_p$ (for instance, $\mathbb{Q}_p$).

If $A = e\mathbb{C}_p[G]$ for a given central idempotent $e \in \mathbb{C}_p[G_1]$, then the corresponding restriction map $\zeta(A)^\times \to \zeta(A_{G_1})^\times$ is compatible with (4.5.1). In fact the following diagram is commutative (see [Bre04, §2.1.5]):

$$\begin{array}{ccc} K_1(\mathbb{C}_p[G]) & \xrightarrow{(e\cdot)_*} & K_1(A) \\ {\scriptstyle f_H}\downarrow & & \downarrow{\scriptstyle f_H} \\ K_1(\mathbb{C}_p[H]) & \xrightarrow{(e\cdot)_*} & K_1(A_H). \end{array}$$

Note that e is the sum of some idempotents associated to characters, and that $(e\cdot)_*$ corresponds to the obvious operation $\zeta(\mathbb{C}_p[G])^\times \to \zeta(A)^\times$.

As concerns $\mathrm{quot}_H^{G_1}$, the map is simply the projection into the components corresponding to the characters lifted from $H = G_1/G_2$, and the same compatibility applies.

Notation 4.5.8. We will denote a generic element of $\zeta(\mathbb{C}_p[G])^\times$ as $\sum_{\chi\in\mathrm{Irr}(G)} \alpha_\chi e_\chi$ or $(\alpha_\chi)_{\chi\in\mathrm{Irr}(G)}$, with $\alpha_\chi \in \mathbb{C}^\times$, depending on what is convenient.

4.6 The case of quadratic presentation

Let R be a complete discrete valuation ring with residue characteristic $p > 0$ and finite residue field and let G be a finite group such that $p \nmid |G'|$. Suppose that the field of fractions F of R has characteristic 0. Let $e \in R[G]$ be a central idempotent and let $\Lambda = eR[G]$ and $A = eF[G]$. Suppose that F has characteristic 0. Note that, by Lemma 4.2.19 and Remark 4.2.20, Λ is a finite product of matrix rings over commutative R-orders.

Definition 4.6.1. Let $\mathcal{H}$ be a family of subquotients of G. Consider the map

$$f_{\mathcal{H}} := \prod_{H\in\mathcal{H}} f_H : \zeta(A)^\times \longrightarrow \prod_{H\in\mathcal{H}} \zeta(A_H)^\times.$$

We will say that the triple $(\Lambda, G, \mathcal{H})$ is *Fitting-detectable* if it satisfies the following containment:

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}} \left(\zeta(\Lambda_H)\cap\zeta(A_H)^\times\right)\right) \subseteq \zeta(\Lambda)\cap\zeta(A)^\times. \tag{4.6.1}$$

Let p be a prime number. We will say that the triple $(p, G, \mathcal{H})$ is *Fitting-detectable* if $(\mathbb{Z}_p[G], G, \mathcal{H})$ is Fitting-detectable.

Remark 4.6.2. The injectivity of $f_{\mathcal{H}}$ in Corollary 4.5.4 can be written as

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}} \left(\zeta(\Lambda_H)^\times\right)\right) \subseteq \zeta(\Lambda)^\times,$$

or, which is the same,

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}} \left(\zeta(\Lambda_H)^\times\cap\zeta(A_H)^\times\right)\right) \subseteq \zeta(\Lambda)^\times\cap\zeta(A)^\times.$$

This is the motivation for the generalisation (4.6.1).

Lemma 4.6.3. *Keep the hypotheses of Definition 4.6.1. Let $e \in \Lambda$ be a central idempotent such that $e \in \Lambda_{G_1}$ for every $G_1/G_2 \in \mathcal{H}$. If $(\Lambda, G, \mathcal{H})$ is Fitting-detectable, then $(e\Lambda, G, \mathcal{H})$ is Fitting-detectable.*

Proof. We need to prove that

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}} \left(\zeta(e\Lambda_H)\cap\zeta(eA_H)^\times\right)\right) \subseteq \zeta(e\Lambda)\cap\zeta(eA)^\times.$$

We recall that the maps are compatible with multiplication by e. The conclusion follows by noting that $\zeta(\Lambda) \cap eA = e\zeta(\Lambda) = \zeta(e\Lambda)$ and $\zeta(eA)^\times = e\zeta(A)^\times$, so that $\zeta(e\Lambda) \cap \zeta(eA)^\times = \zeta(\Lambda) \cap e\zeta(A)^\times$, and analogously after applying f_H. □

The following is the motivation for this section.

Theorem 4.6.4. *Suppose that $(\Lambda, G, \mathcal{H})$ is Fitting-detectable. Let $\theta \in \zeta(A)^\times$ and let M be a finitely presented R-torsion Λ-module with quadratic presentation. If $\theta_H \in \mathrm{Fitt}_{\Lambda_H}(M_H)$ for every $H \in \mathcal{H}$, then $\theta \in \mathrm{Fitt}_\Lambda(M)$.*

Proof. We can write $\theta = z \cdot \mathrm{nr}_A(x)$ for some $z \in \zeta(A)^\times$, where $\mathrm{nr}_A(x)$ is the generator of $\mathrm{Fitt}_\Lambda(M)$ as in Lemma 4.5.1. Then for every $H \in \mathcal{H}$ we have $\theta_H = z_H \cdot \mathrm{nr}_{A_H}(f_H(x))$. Since Λ_H has a quadratic presentation by Lemma 4.4.9, then by Lemma 4.5.1 $\theta_H \in \mathrm{Fitt}_{\Lambda_H}(M_H) = \zeta(\Lambda_H)\mathrm{nr}_{A_H}(f_H(x))$, so necessarily $z_H \in \zeta(\Lambda_H)$. By the containment (4.6.1) we deduce that $z \in \zeta(\Lambda)$, which is what we wanted to prove. □

We will now find infinite families of groups and subquotients with the property of being Fitting-detectable. We will be particularly interested in the situation in which the subquotients are abelian.

4.6.1 On Frobenius groups

For the convenience of the reader, we now recall some definitions and results that were already given at the beginning of §3.3.3.

Definition 4.6.5. A Frobenius group is a finite group G with a proper non-trivial subgroup H, called Frobenius complement, such that $H \cap gHg^{-1} = \{1\}$ for every $g \in G \setminus H$.

We have the following properties. For a full list of references see [JN16, Theorems 2.11&2.12].

Proposition 4.6.6. *Let G be a Frobenius group with complement H. Then there exists a normal subgroup N of G such that $G \cong N \rtimes H$ with a fixed-point-free action of H on N. Moreover if any group G can be written in this way then it is a Frobenius group.*

Proposition 4.6.7. *Let $G \cong N \rtimes H$ be a Frobenius group. Then the following hold:*

(i) $|N|$ and $|H|$ are coprime;

(ii) every normal subgroup of G either contains or is contained in N;

(iii) for every $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ such that $N \nsubseteq \ker \chi$ we have $\chi = \mathrm{Ind}_N^G \psi$, where $\mathbf{1}_N \neq \psi \in \mathrm{Irr}_{\mathbb{C}}(N)$; moreover, all characters of G of this type are irreducible.

Example 4.6.8. The groups $S_3 \cong C_3 \rtimes C_2$ and $A_4 \cong C_2^2 \rtimes C_3$ are examples of Frobenius groups. More generally the affine group $\mathrm{Aff}(\ell^n) := \mathbb{F}_{\ell^n} \rtimes \mathbb{F}_{\ell^n}^\times$ of affine transformations of a finite field is a Frobenius group (see [JN16, Example 2.16]). Also groups isomorphic to $C_\ell \rtimes C_q$, with ℓ prime number and q any natural number dividing $\ell - 1$ with fixed-point-free action of C_q on C_ℓ, are Frobenius groups. Another class of Frobenius groups are groups of the type $A \rtimes C_2$, where A is an abelian group of odd order and the non-trivial

element of C_2 acts by inversion (for instance dihedral groups of order not divisible by 4).

Remark 4.6.9. Note that if $G = N \rtimes H$ is a Frobenius group then $N \subseteq G'$, with equality if and only if H is abelian. Also note that the centre of a Frobenius group $G \cong N \rtimes H$ is trivial: assuming it is not, then there is a central non-trivial element in $g \in N$ by Proposition 4.6.7(ii); this implies that $gHg^{-1} = H$, which contradicts the definition of Frobenius group.

Notation 4.6.10. From now on we will denote by $\mathcal{O}_p$ the ring of integers of $\mathbb{C}_p$, that is, the elements of $\mathbb{C}_p$ of non-negative valuation.

Proposition 4.6.11. *Let $G \cong N \rtimes H$ be a Frobenius group and let p be a prime such that $p \nmid |G'|$. Let $\mathcal{H} = \{N/1, G/N\}$. Then $(p, G, \mathcal{H})$ is Fitting-detectable.*

Proof. In the proof we will identify the subquotient $N/1$ with N and G/N with H. By Proposition 4.6.7(iii), every character of G is either induced from a nontrivial character of N or is lifted from $G/N \cong H$. We claim that

$$\begin{aligned} \mathrm{quot}_H^G : \zeta(\mathbb{C}_p[G])^\times &\longrightarrow \zeta(\mathbb{C}_p[H])^\times \\ (a_\rho)_{\rho\in\mathrm{Irr}(G)} &\longmapsto (a_{\mathrm{Infl}_H^G\lambda})_{\lambda\in\mathrm{Irr}(H)} \end{aligned}$$

and, from (4.5.1),

$$\begin{aligned} \mathrm{res}_N^G : \zeta(\mathbb{C}_p[G])^\times &\longrightarrow \zeta(\mathbb{C}_p[N])^\times \\ (a_\rho)_{\rho\in\mathrm{Irr}(G)} &\longmapsto \left(\prod_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}^{\lambda(1)}, (a_{\mathrm{Ind}_N^G\psi})_{\psi\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}} \right), \end{aligned} \tag{4.6.2}$$

where $\prod_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}^{\lambda(1)}$ is at the position corresponding to $\mathbf{1}_N$. In fact, let $\chi \in \mathrm{Irr}(G)$: if $\chi = \mathrm{Ind}_N^G\psi$ with $\psi \in \mathrm{Irr}(N) \setminus \{\mathbf{1}_N\}$, then

$$\langle \mathrm{Ind}_N^G\psi, \mathrm{Ind}_N^G\mathbf{1}_N\rangle_G = \langle \psi, \mathrm{Res}_N^G\mathrm{Ind}_N^G\mathbf{1}_N\rangle_N = \langle \psi, |H|\mathbf{1}_N\rangle_N = 0$$

(indeed, by [CR81, (10.2)] $\mathrm{Ind}_N^G\mathbf{1}_N(g)$ is $|H|$ if $g \in N$ and 0 otherwise, so that its restriction only has the identity as a component); if $\chi = \mathrm{Infl}_H^G\lambda$ with $\lambda \in \mathrm{Irr}(H)$, then

$$\langle \mathrm{Infl}_H^G\lambda, \mathrm{Ind}_N^G\mathbf{1}_N\rangle_G = \langle \mathrm{Res}_N^G\mathrm{Infl}_H^G\lambda, \mathbf{1}_N\rangle_N = \langle \lambda(1)\mathbf{1}_N, \mathbf{1}_N\rangle_H = \lambda(1),$$

so that the first component of (4.6.2) easily follows from (4.5.1). As for the remaining terms of the image of (4.6.2), it follows from the observation just after (4.5.1), since each $\mathrm{Ind}_N^G\psi$ is irreducible. Note that these remaining terms appear with multiplicity, since a character of G may be induced by more than one character of N.

Let $z = (a_\rho)_{\rho\in\mathrm{Irr}(G)} \in \zeta(\mathbb{Q}_p[G])^\times$. We need to show that if $z_N = \mathrm{res}_N^G(z) \in \mathbb{Z}_p[N]$ and $z_H = \mathrm{quot}_H^G(z) \in \mathbb{Z}_p[H]$, then $z \in \mathbb{Z}_p[G]$. We recall that $\mathcal{O}_p$ is the ring of integers of $\mathbb{C}_p$; note that $\mathbb{Q}_p[G] \cap \mathcal{O}_p[G] = \mathbb{Z}_p[G]$, so that it suffices to show $z \in \mathcal{O}_p[G]$. We will first show that

$$\sum_{\chi=\mathrm{Ind}_N^G\lambda:\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}} a_\chi e_\chi \in \mathcal{O}_p[G].$$

By Remark 4.6.9 and the hypothesis $p \nmid |G'|$ we have $|N| \in \mathbb{Z}_p^\times$. From the expansion $e_\chi = |G|^{-1}\chi(1)\sum_{g\in G}\chi(g)g^{-1}$, what we have to prove is that, for every $g \in G$,

$$\sum_{\chi=\mathrm{Ind}_N^G\lambda:\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}} a_\chi\ \lambda(1)\ \mathrm{Ind}_N^G\lambda(g) \in \mathcal{O}_p.$$

We are done if we show that $a_{\mathrm{Ind}_N^G\lambda}\lambda(1)\mathrm{Ind}_N^G\lambda(g) \in \mathcal{O}_p$ for every $\lambda \in \mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}$. By [CR81, (10.2)], since N is normal in G, we can assume $g \in N$ (otherwise the expression is 0), in which case $\mathrm{Ind}_N^G\lambda(g)$ is an integral linear combination of elements of the form $\lambda(n)$ with $n \in N$. Hence we are done if we show that $a_{\mathrm{Ind}_N^G\lambda}\lambda(1)\lambda(n) \in \mathcal{O}_p$ for every $n \in N$. We have that $z_N \in \mathbb{Z}_p[N]$, that is,

$$\prod_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}^{\lambda(1)} e_{\mathbf{1}_N} + \sum_{\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}} a_{\mathrm{Ind}_N^G\lambda}e_\lambda \in \mathbb{Z}_p[N].$$

Since $e_\lambda \in \mathcal{O}_p[G]$ (as $|N| \in \mathbb{Z}_p^\times$), then for every $\lambda \neq \mathbf{1}_N$ we have $z_N e_\lambda = a_{\mathrm{Ind}_N^G\lambda}e_\lambda \in \mathcal{O}_p[G]$. Coefficient by coefficient we deduce that $a_{\mathrm{Ind}_N^G\lambda}\lambda(1)\lambda(n) \in \mathcal{O}_p$ for every $n \in N$, which is what we wanted to show.

It now remains to show that

$$\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}\ e_{\mathrm{Infl}_H^G\lambda} \in \mathcal{O}_p[G].$$

We will prove that $\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}e_{\mathrm{Infl}_H^G\lambda}$ is actually in $\mathbb{Z}_p[G]$. Note that

$$e_{\mathrm{Infl}_H^G\lambda} = \frac{\lambda(1)}{|G|}\sum_{h\in H}\left(\lambda(h^{-1})\sum_{n\in N}nh\right) = \frac{1}{|N|}\cdot\frac{\lambda(1)}{|H|}\sum_{h\in H}\left(\lambda(h^{-1})\sum_{n\in N}nh\right).$$

Since $|N| \in \mathbb{Z}_p^\times$, coefficient by coefficient we deduce that the relation

$$\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}e_{\mathrm{Infl}_H^G\lambda} \in \mathbb{Z}_p[G]$$

is the same as

$$\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^G\lambda}e_\lambda \in \mathbb{Z}_p[H]$$

(since the coefficients of $e_{\mathrm{Infl}_H^G\lambda}$ are invariant modulo N). This concludes the proof. □

4.6.2 On direct products

In this part we consider direct products of groups.

Proposition 4.6.12. *Let $G = P \times Q$ be a finite group and let p be a prime number such that $p \nmid |Q|$. Suppose that $\mathbb{Q}_p$ is a splitting field for $\mathbb{Q}_p[Q]$ (e.g. if Q is cyclic of order dividing $p-1$). Let $\mathcal{H}'$ be a set of subquotients of P such that $(p, P, \mathcal{H}')$ is Fitting-detectable. Let $\mathcal{H}$ be the set of subquotients $H \times Q$ for every $H \in \mathcal{H}'$. Then $(p, G, \mathcal{H})$ is Fitting-detectable.*

Proof. Let $z \in \zeta(\mathbb{Q}_p[G])^\times$ be such that $z_{H\times Q} \in \mathbb{Z}_p[H\times Q]$ for every $H \in \mathcal{H}'$. We can write it as

$$z = \sum_{\substack{\sigma\in \mathrm{Irr}(P)\\ \chi\in\mathrm{Irr}(Q)}} a_{\sigma,\chi} e_{\sigma\chi}$$

with $a_{\sigma,\chi} \in \mathbb{C}_p^\times$, where $(\sigma\chi)(a,b) = \sigma(a)\chi(b)$. If $\sigma \in \mathrm{Irr}(P)$, then depending on the situation e_σ will denote the idempotent corresponding to σ either in $\mathbb{Q}_p[P]$ or in $\mathbb{Q}_p[G]$ via the inclusion $\mathbb{Q}_p[P] \hookrightarrow \mathbb{Q}_p[G]$, and analogously for e_χ with $\chi \in \mathrm{Irr}(Q)$. Note that $e_{\sigma\chi} = e_\sigma e_\chi$. Hence

$$z = \sum_{\chi\in\mathrm{Irr}(Q)} \left(\sum_{\sigma\in\mathrm{Irr}(P)} a_{\sigma,\chi} e_\sigma \right) e_\chi = \sum_{\chi\in\mathrm{Irr}(Q)} z_\chi e_\chi$$

for certain $z_\chi \in \zeta(\mathbb{C}_p[P])^\times$. Since $\mathbb{Q}_p$ splits $\mathbb{Q}_p[Q]$, then for every χ we have $e_\chi \in \mathbb{Q}_p[Q]$ and so $ze_\chi = z_\chi e_\chi \in \mathbb{Q}_p[G]$. Looking at the coefficient of 1 in $e_\chi \in \mathbb{Q}_p[Q]$, this implies that $z_\chi \in \zeta(\mathbb{Q}_p[P])^\times$.

Since $e_\chi \in \mathcal{O}_p[Q]$ for every χ, then we just need to show that $z_\chi \in \mathcal{O}_p[P]$ for every $\chi \in \mathrm{Irr}(Q)$. Now we use (4.5.1) to compute $z_{H\times Q}$ for every $H \in \mathcal{H}'$. We note that, if we write $H = P_1/P_2$, then $\langle \sigma\chi, \mathrm{Ind}_{P_1\times Q}^{P\times Q}(\sigma'\chi')\rangle_{P\times Q}$ is non-trivial only for $\chi' = \chi$, in which case

$$\langle \sigma\chi, \mathrm{Ind}_{P_1\times Q}^{P\times Q}(\sigma'\chi)\rangle_{P\times Q} = \langle \sigma, \mathrm{Ind}_{P_1}^{P}\sigma'\rangle_P. \tag{4.6.3}$$

Combining restriction with quotient, this easily implies that

$$\mathbb{Z}_p[H\times Q] \ni z_{H\times Q} = \sum_{\chi\in\mathrm{Irr}(Q)} z_{\chi,H} e_\chi, \tag{4.6.4}$$

where $z_{\chi,H}$ is the image of $z_\chi \in \mathbb{Q}_p[P]$ in $\mathbb{Q}_p[H]$. If we fix a certain character χ, then multiplying both sides of (4.6.4) by $e_\chi \in \mathcal{O}_p[Q]$ we obtain that $z_{\chi,H}e_\chi \in \mathcal{O}_p[H\times Q]$. Writing down the idempotent e_χ explicitly, looking at the coefficient of 1 this easily implies that $z_{\chi,H} \in \mathcal{O}_p[H] \cap \mathbb{Q}_p[H] = \mathbb{Z}_p[H]$ for every $H \in \mathcal{H}'$. Since $(p, P, \mathcal{H}')$ is Fitting-detectable, we finally conclude that $z_\chi \in \mathbb{Z}_p[P]$. Therefore $z \in \mathcal{O}_p[G] \cap \mathbb{Q}_p[G] = \mathbb{Z}_p[G]$. □

Proposition 4.6.13. *Let $P \cong N \rtimes H$ be a Frobenius group such that $p \nmid |P'|$. Let Q be a finite group such that $p \nmid |Q'|$. Let $G = P\times Q$ and $\mathcal{H} = \{(N\times Q)/1, (P\times Q)/(N\times 1)\}$. Then $(p, G, \mathcal{H})$ is Fitting-detectable.*

Proof. We will denote the subquotient $(N\times Q)/1$ simply by $N\times Q$ and $(P\times Q)/(N\times 1)$ by $H\times Q$. Let $z \in \zeta(\mathbb{Q}_p[G])^\times$ be such that $z_{N\times Q} \in \mathbb{Z}_p[N\times Q]$ and $z_{H\times Q} \in \mathbb{Z}_p[H\times Q]$. We can write

$$\begin{aligned} z &= \sum_{\substack{\varphi=\mathrm{Ind}_N^P\lambda:\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}\\ \chi\in\mathrm{Irr}(Q)}} a_{\varphi,\chi} e_{\mathrm{Ind}_N^P\lambda\cdot\chi} + \sum_{\substack{\lambda\in\mathrm{Irr}(H)\\ \chi\in\mathrm{Irr}(Q)}} a_{\mathrm{Infl}_H^P\lambda,\chi} e_{\mathrm{Infl}_H^P\lambda\cdot\chi} \\ &= \sum_{\chi\in\mathrm{Irr}(Q)} \left(\sum_{\varphi=\mathrm{Ind}_N^P\lambda:\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}} a_{\varphi,\chi} e_{\mathrm{Ind}_N^P\lambda} \right) e_\chi + \sum_{\chi\in\mathrm{Irr}(Q)} \left(\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^P\lambda,\chi} e_{\mathrm{Infl}_H^P\lambda} \right) e_\chi \end{aligned}$$

with coefficients in $\mathbb{C}_p^\times$. Similarly to the proof of Proposition 4.6.12, we have that

$$z_{H\times Q} = \sum_{\chi\in\mathrm{Irr}(Q)} \left(\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^P\lambda,\chi} e_\lambda \right) e_\chi \in \mathbb{Z}_p[H\times Q].$$

This also implies that

$$\sum_{\chi\in\mathrm{Irr}(Q)} \left(\sum_{\lambda\in\mathrm{Irr}(H)} a_{\mathrm{Infl}_H^P\lambda,\chi} e_{\mathrm{Infl}_H^P\lambda} \right) e_\chi \in \mathbb{Z}_p[P\times Q]$$

as already done in the end of the proof of Proposition 4.6.11. It remains to show that the remaining summand of z is in $\mathbb{Z}_p[P\times Q]$. Swapping the two sums, we will show that

$$\sum_{\varphi=\mathrm{Ind}_N^P\lambda:\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}} \sum_{\chi\in\mathrm{Irr}(Q)} a_{\varphi,\chi} e_\chi e_{\mathrm{Ind}_N^P\lambda} \in \mathcal{O}_p[P\times Q]. \tag{4.6.5}$$

We can write

$$z_{N\times Q} = \sum_{\lambda\in\mathrm{Irr}(N)} z_\lambda e_\lambda \in \mathbb{Z}_p[N\times Q],$$

where by (4.6.2) and (4.6.3) for every $\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}$ we have $z_\lambda = \sum_{\chi\in\mathrm{Irr}(Q)} a_{\mathrm{Ind}_N^P\lambda,\chi} e_\chi$. Since $e_\lambda\in\mathcal{O}_p[N]$, then for every $\lambda\in\mathrm{Irr}(N)\setminus\{\mathbf{1}_N\}$

$$z_{N\times Q} e_\lambda = \sum_{\chi\in\mathrm{Irr}(Q)} a_{\mathrm{Ind}_N^P\lambda,\chi} e_\chi e_\lambda \in \mathcal{O}_p[N\times Q].$$

This implies that for every $n\in N$ we have

$$\sum_{\chi\in\mathrm{Irr}(Q)} \lambda(1)\lambda(n) a_{\mathrm{Ind}_N^P\lambda,\chi} e_\chi \in \mathcal{O}_p[Q].$$

By [CR81, (10.2)] for every $g\in P$ we have that $\mathrm{Ind}_N^P\lambda(g)$ is an integral combination of elements of the type $\lambda(n)$ with $n\in N$ (in particular, 0 if $g\notin N$). We deduce that for every $g\in P$ we have

$$\sum_{\chi\in\mathrm{Irr}(Q)} \lambda(1)\mathrm{Ind}_N^P\lambda(g) a_{\mathrm{Ind}_N^P\lambda,\chi} e_\chi \in \mathcal{O}_p[Q].$$

Summing over the characters of P induced by the non-trivial characters of N, this implies (4.6.5). □

Proposition 4.6.14. *Let Q be a finite group and let p be an odd prime number such that $p\nmid|Q'|$. Let Q_8 be the quaternionic group of order 8, let $H_1\cong C_4$ be a subgroup of Q_8 of order 4 and let $H_2\cong C_2^2$ be the quotient of Q_8 of order 4. Let $G = Q_8\times Q$ and $\mathcal{H} = \{H_1\times Q, H_2\times Q\}$. Then $(p,G,\mathcal{H})$ is Fitting-detectable.*

Proof. As already done in previous proofs, we will identify $H_1\cong C_4$ with C_4 and $H_2\cong C_2^2$ with C_2^2. We start by providing the character table of Q_8.

class	1	2	4A	4B	4C
size	1	1	2	2	2
σ_1	1	1	1	1	1
σ_2	1	1	-1	1	-1
σ_3	1	1	1	-1	-1
σ_4	1	1	-1	-1	1
σ_5	2	-2	0	0	0

Here the subgroup $H_1 \cong C_4$ corresponds to $4A$ in the table and in general we will list by nA, nB etc. the conjugacy classes of groups of order n. Let $z \in \zeta(\mathbb{Q}_p[G])^\times$ be such that $z_{C_4\times Q} \in \mathbb{Z}_p[C_4 \times Q]$ and $z_{C_2^2\times Q} \in \mathbb{Z}_p[C_2^2 \times Q]$. We can write

$$z = \sum_{\substack{\sigma\in \mathrm{Irr}(Q_8)\\ \chi\in\mathrm{Irr}(Q)}} a_{\sigma,\chi} e_{\sigma\chi}$$

with coefficients in $\mathbb{C}_p^\times$. The quotient map to $C_2^2 \times Q$ corresponds to the projection into the four linear characters of Q_8 (times the irreducible complex characters of Q). Hence as in the proof of Proposition 4.6.13 it remains to prove that

$$\sum_{\chi\in\mathrm{Irr}(Q)} a_{\sigma_5,\chi} e_{\sigma_5} e_\chi \in \mathbb{Z}_p[G].$$

Using (4.5.1) we get

$$z_{C_4\times Q} = \sum_{\chi\in\mathrm{Irr}(Q)} (a_{\sigma_1,\chi}a_{\sigma_3,\chi}e_{\rho_1} + a_{\sigma_2,\chi}a_{\sigma_4,\chi}e_{\rho_2} + a_{\sigma_5,\chi}e_{\rho_3} + a_{\sigma_5,\chi}e_{\rho_4})e_\chi \in \mathbb{Z}_p[C_4 \times Q],$$

where ρ_i denote the irreducible complex characters of C_4, where we follow the order of the characters as in the following character table.

class	1	2	4A	4B
size	1	1	1	1
ρ_1	1	1	1	1
ρ_2	1	1	-1	-1
ρ_3	1	-1	$-i$	i
ρ_4	1	-1	i	$-i$

So

$$\mathbb{Z}_p[C_4 \times Q] \ni z_{C_4\times Q}(e_{\rho_3} + e_{\rho_4}) = \sum_{\chi\in\mathrm{Irr}(Q)} a_{\sigma_5,\chi}(e_{\rho_3} + e_{\rho_4})e_\chi.$$

Since $e_{\rho_3} + e_{\rho_4} = e_{\sigma_5}$ (via the inclusion $C_4 \hookrightarrow Q_8$), we are done. □

Proposition 4.6.15. *Let Q be a finite group and let p be an odd prime number such that $p \nmid |Q'|$. Let D_8 be the dihedral group of order 8, let H_1 be the cyclic subgroup of order 4 of D_8 and let H_2 be the quotient of order 4. Let $\mathcal{H}$ be the set of $C_4 \times Q$ and $C_2^2 \times Q$ as subquotients of $G := D_8 \times Q$. Then $(p, G, \mathcal{H})$ is Fitting-detectable.*

Proof. The following is the character table of D_8.

class	1	2A	2B	2C	4
size	1	1	2	2	2
σ_1	1	1	1	1	1
σ_2	1	1	-1	1	-1
σ_3	1	1	1	-1	-1
σ_4	1	1	-1	-1	1
σ_5	2	-2	0	0	0

Since the character tables of D_8 and Q_8 are the same, the proof is essentially the same as that of Proposition 4.6.14. □

4.6.3 On $\mathrm{SL}_2(\mathbb{F}_3)$: a group which is not Fitting-detectable with respect to any set of abelian subquotients

We start with the following definition.

Definition 4.6.16. Let G be a finite group. Then G is *monomial* if every irreducible complex character of G is induced by a linear character.

The class of monomial groups is quite vast; the smallest non-monomial group is $\mathrm{SL}_2(\mathbb{F}_3)$, of order 24.

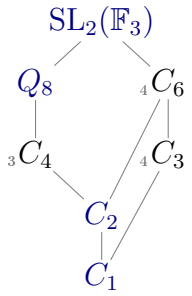
Proposition 4.6.17. *Let G be $\mathrm{SL}_2(\mathbb{F}_3)$ and let $\mathcal{H}$ be a family of abelian subquotients of G. Then $(3, G, \mathcal{H})$ is not Fitting-detectable.*

Proof. We need to exhibit an element $z \in \zeta(\mathbb{Q}_3[G])^\times \setminus \mathbb{Z}_3[G]$ such that $z_H \in \mathbb{Z}_3[H]$ for every abelian subquotient H of G. We will refer to the following character table of $\mathrm{SL}_2(\mathbb{F}_3)$.

class	1	2	3A	3B	4	6A	6B
size	1	1	4	4	6	4	4
ρ_1	1	1	1	1	1	1	1
ρ_2	1	1	ζ_3^2	ζ_3	1	ζ_3^2	ζ_3
ρ_3	1	1	ζ_3	ζ_3^2	1	ζ_3	ζ_3^2
ρ_4	2	-2	-1	-1	0	1	1
ρ_5	2	-2	ζ_6^5	ζ_6	0	ζ_3	ζ_3^2
ρ_6	2	-2	ζ_6	ζ_6^5	0	ζ_3^2	ζ_3
ρ_7	3	3	0	0	-1	0	0

Note that $|G| = 24$, G is not monomial, has a central element of order 2 and $3 \nmid |G'| =$

$|Q_8| = 8$. We recall the following subgroup lattice:



There are 7 irreducible complex characters denoted by $\rho_1, ..., \rho_7$. Let $z \in \zeta(\mathbb{C}_3[G])^\times$ be the element corresponding to $(9, 9, 9, 1, 27, 27, 9)$.

First of all we verify that $z \in \mathbb{Q}_3[G]$. Note that e_{ρ_1}, e_{ρ_4} and e_{ρ_7} are already in $\mathbb{Q}_3[G]$, so may be ignored. It remains to show that $9e_{\rho_2} + 9e_{\rho_3} + 27e_{\rho_5} + 27e_{\rho_6} \in \mathbb{Q}_3[G]$. This holds for both $e_{\rho_2} + e_{\rho_3}$ and $e_{\rho_5} + e_{\rho_6}$, since $\zeta_3 + \zeta_3^2$ and $\zeta_6 + \zeta_6^5$ are in $\mathbb{Q}_3$ (c.f. the character table).

We also have that $z \notin \mathbb{Z}_3[G]$ (although it lies in a maximal order): the coefficient at the identity is

$$\frac{1}{24} \cdot 9 + \frac{1}{24} \cdot 9 + \frac{1}{24} \cdot 9 + \frac{2}{24} + \frac{2}{24} \cdot 27 + \frac{2}{24} \cdot 27 + \frac{3}{24} \cdot 9 \notin \mathbb{Z}_3.$$

Finally we show that at every abelian subquotient the image of z has integral coefficients. Let $H = G_1/G_2$. If $G_1 = G$, then G_2 can only be Q_8 with $H \cong C_3$. Then

$$\begin{aligned} \mathrm{quot}_H^G : (a_1, ..., a_7) &\longmapsto (a_1, a_2, a_3) \\ (9, 9, 9, 1, 27, 27, 9) &\longmapsto (9, 9, 9) \in \mathbb{Z}_3[C_3]. \end{aligned}$$

If $G_1 \cong C_6$ then it is sufficient to consider $\mathrm{res}_{G_1}^G$ (since further quotients would remain integral as well). Under a certain order of the characters of C_6, we have that

$$\begin{aligned} \mathrm{res}_{G_1}^G : (a_1, ..., a_7) &\longmapsto (a_1a_7, a_5a_6, a_2a_7, a_4a_5, a_3a_7, a_4a_6) \\ (9, 9, 9, 1, 27, 27, 9) &\longmapsto (81, 729, 81, 27, 81, 27) \in \mathbb{Z}_3[C_6]. \end{aligned}$$

Analogously, if $G_1 \cong C_3$ and $G_1 \subseteq G_3 \cong C_6$, then under a certain order of the characters we have

$$\begin{aligned} \mathrm{res}_{G_1}^G = \mathrm{res}_{G_1}^{G_3} \circ \mathrm{res}_{G_3}^G : (a_1, ..., a_7) &\longmapsto (a_1a_5a_6a_7, a_3a_4a_6a_7, a_2a_4a_5a_7) \\ (9, 9, 9, 1, 27, 27, 9) &\longmapsto (59049, 2187, 2187) \in \mathbb{Z}_3[C_3]. \end{aligned}$$

If $G_1 \cong Q_8$, then again we consider the case $G_2 = \{1\}$ (note that this is not an abelian subquotient, but this analysis covers all further subquotients):

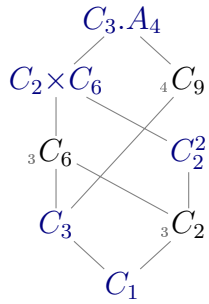
$$\begin{aligned} \mathrm{res}_{Q_8}^G : (a_1, ..., a_7) &\longmapsto (a_1a_2a_3, a_7, a_7, a_7, a_4a_5a_6) \\ (9, 9, 9, 1, 27, 27, 9) &\longmapsto (3^6, 9, 9, 9, 3^6) \in \mathbb{Z}_3[Q_8]. \end{aligned}$$

Since $\mathbb{Z}_3[Q_8]$ is a maximal order and (4.5.1) sends maximal orders to maximal orders, also the restrictions to the subgroups of order 4 or 2 are integral.

We hence proved that $z_H \in \mathbb{Z}_3[G]$ for every abelian subquotient H. □

4.6.4 A further example of a Fitting-detectable triple: on the group $C_3.A_4$

The group $C_3.A_4$ is of order 36 and is labelled as SmallGroup(16,3). We refer to [Dok18] for its properties and notation. We recall the following subgroup lattice:



where $H := C_3.A_4/C_2^2 \cong C_9$. By $C_2 \times C_6$ we will denote the corresponding subgroup of G.

Proposition 4.6.18. *The triple* $(3, C_3.A_4, \{H, C_2 \times C_6\})$ *is Fitting-detectable.*

Proof. We start by providing the character table of $C_3.A_4$.

class	1	2	3A	3B	6A	6B	9A	9B	9C	9D	9E	9F
size	1	3	1	1	3	3	4	4	4	4	4	4
ρ_1	1	1	1	1	1	1	1	1	1	1	1	1
ρ_2	1	1	1	1	1	1	ζ_3^2	ζ_3	ζ_3	ζ_3^2	ζ_3^2	ζ_3
ρ_3	1	1	1	1	1	1	ζ_3	ζ_3^2	ζ_3^2	ζ_3	ζ_3	ζ_3^2
ρ_4	1	1	ζ_3^2	ζ_3	ζ_3	ζ_3^2	ζ_9	ζ_9^5	ζ_9^2	ζ_9^7	ζ_9^4	ζ_9^8
ρ_5	1	1	ζ_3^2	ζ_3	ζ_3	ζ_3^2	ζ_9^7	ζ_9^8	ζ_9^5	ζ_9^4	ζ_9	ζ_9^2
ρ_6	1	1	ζ_3	ζ_3^2	ζ_3^2	ζ_3	ζ_9^2	ζ_9	ζ_9^4	ζ_9^5	ζ_9^8	ζ_9^7
ρ_7	1	1	ζ_3	ζ_3^2	ζ_3^2	ζ_3	ζ_9^8	ζ_9^4	ζ_9^7	ζ_9^2	ζ_9^5	ζ_9
ρ_8	1	1	ζ_3^2	ζ_3	ζ_3	ζ_3^2	ζ_9^4	ζ_9^2	ζ_9^8	ζ_9	ζ_9^7	ζ_9^5
ρ_9	1	1	ζ_3	ζ_3^2	ζ_3^2	ζ_3	ζ_9^5	ζ_9^7	ζ_9	ζ_9^8	ζ_9^2	ζ_9^4
ρ_{10}	3	-1	3	3	-1	-1	0	0	0	0	0	0
ρ_{11}	3	-1	$\frac{-3+3\sqrt{-3}}{2}$	$\frac{-3-3\sqrt{-3}}{2}$	ζ_6	ζ_6^5	0	0	0	0	0	0
ρ_{12}	3	-1	$\frac{-3-3\sqrt{-3}}{2}$	$\frac{-3+3\sqrt{-3}}{2}$	ζ_6^5	ζ_6	0	0	0	0	0	0

Let $z \in \zeta(\mathbb{Q}_3[G])^\times$ be such that $z_H \in \mathbb{Z}_3[C_9]$ and $z_{C_2\times C_6} \in \mathbb{Z}_3[C_2 \times C_6]$. There are 12 characters $\rho_1, ..., \rho_{12}$, so that $z \in \zeta(\mathbb{C}_3[G])^\times$ can be written as $z = \sum_{i=1}^{12} a_i e_{\rho_i}$ (see the character table). Note that the linear characters $\rho_1, ..., \rho_9$ are exactly the ones lifted from the irreducible complex characters $\sigma_1, ..., \sigma_9$ of C_9. Since all the denominators of $e_{\rho_1}, ..., e_{\rho_9}, e_{\sigma_1}, ..., e_{\sigma_9}$ have valuation 2 then $z_H \in \mathbb{Z}_3[C_9]$ implies that $\sum_{i=1}^{9} a_i e_{\rho_i} \in \mathbb{Z}_3[C_9]$. Hence it remains to show that $a_{10}e_{\rho_{10}} + a_{11}e_{\rho_{11}} + a_{12}e_{\rho_{12}} \in \mathbb{Z}_3[G]$.

Now we compute $\mathrm{res}^G_{C_2\times C_6}$. We will refer to the following character table of $C_2 \times C_6$.

class	1	2A	2B	2C	3A	3B	6A	6B	6C	6D	6E	6F
size	1	1	1	1	1	1	1	1	1	1	1	1
λ_1	1	1	1	1	1	1	1	1	1	1	1	1
λ_2	1	−1	1	−1	1	1	1	−1	−1	1	−1	−1
λ_3	1	1	−1	−1	1	1	−1	1	1	−1	−1	−1
λ_4	1	−1	−1	1	1	1	−1	−1	−1	−1	1	1
λ_5	1	1	1	1	ζ_3	ζ_3^2	ζ_3	ζ_3	ζ_3^2	ζ_3^2	ζ_3	ζ_3^2
λ_6	1	−1	1	−1	ζ_3	ζ_3^2	ζ_3	ζ_6^5	ζ_6	ζ_3^2	ζ_6^5	ζ_6
λ_7	1	1	−1	−1	ζ_3	ζ_3^2	ζ_6^5	ζ_3	ζ_3^2	ζ_6	ζ_6^5	ζ_6
λ_8	1	−1	−1	1	ζ_3	ζ_3^2	ζ_6^5	ζ_6^5	ζ_6	ζ_6	ζ_3	ζ_3^2
λ_9	1	1	1	1	ζ_3^2	ζ_3	ζ_3^2	ζ_3^2	ζ_3	ζ_3	ζ_3^2	ζ_3
λ_{10}	1	−1	1	−1	ζ_3^2	ζ_3	ζ_3^2	ζ_6	ζ_6^5	ζ_3	ζ_6	ζ_6^5
λ_{11}	1	1	−1	−1	ζ_3^2	ζ_3	ζ_6	ζ_3^2	ζ_3	ζ_6^5	ζ_6	ζ_6^5
λ_{12}	1	−1	−1	1	ζ_3^2	ζ_3	ζ_6	ζ_6	ζ_6^5	ζ_6^5	ζ_3^2	ζ_3

Using (4.5.1) we find that

$$\begin{aligned}\mathrm{res}^G_{C_2\times C_6} : \zeta(\mathbb{C}_p[G])^\times &\longrightarrow \zeta(\mathbb{C}_p[C_2\times C_6])^\times\\ (a_i)_{i=1,\dots,12} &\longmapsto (a_1a_2a_3, a_{10}, a_{10}, a_{10}, a_6a_7a_9, a_{11}, a_{11}, a_{11}, a_4a_5a_8, a_{12}, a_{12}, a_{12}).\end{aligned}$$

Imposing that the coefficients of $z_{C_2\times C_6}$ at 1 and at every element of $C_2 \times C_6$ of order 2 are in $\mathbb{Z}_3$, we know that

$$\begin{cases} a_1a_2a_3 + a_6a_7a_9 + a_4a_5a_8 + 3(a_{10} + a_{11} + a_{12}) \in 9\mathbb{Z}_3\\ a_1a_2a_3 + a_6a_7a_9 + a_4a_5a_8 - (a_{10} + a_{11} + a_{12}) \in 9\mathbb{Z}_3, \end{cases}$$

which implies $a_{10} + a_{11} + a_{12} \in 9\mathbb{Z}_3$. Now we look at the coefficients at the elements representing the conjugacy classes $3A$ and $6A$ in $C_2 \times C_6$:

$$\begin{cases} a_1a_2a_3 + \zeta_3a_6a_7a_9 + \zeta_3^2a_4a_5a_8 + 3a_{10} + 3\zeta_3a_{11} + 3\zeta_3^2a_{12} \in 9\mathbb{Z}_3\\ a_1a_2a_3 + \zeta_3a_6a_7a_9 + \zeta_3^2a_4a_5a_8 - a_{10} - \zeta_3a_{11} - \zeta_3^2a_{12} \in 9\mathbb{Z}_3, \end{cases}$$

so that $a_{10} + \zeta_3a_{11} + \zeta_3^2a_{12} \in 9\mathbb{Z}_3$. Finally, looking at the elements in the classes $3B$ and $6C$ we get $a_{10} + \zeta_3^2a_{11} + \zeta_3a_{12} \in 9\mathbb{Z}_3$. Combining our formulas we obtain that $a_{10} \in 3\mathbb{Z}_3$ and $a_{11} + \zeta_3a_{12} \in 3\mathbb{Z}_3$. We can therefore deduce the following:

$$\begin{cases} 3a_{10} + 3a_{11} + 3a_{12} \in 3\mathbb{Z}_3\\ -a_{10} - a_{11} - a_{12} \in 3\mathbb{Z}_3\\ 3a_{10} + 2\zeta_3a_{11} + 2\zeta_3^2a_{12} \in 3\mathbb{Z}_3\\ 3a_{10} + 2\zeta_3^2a_{11} + 2\zeta_3a_{12} \in 3\mathbb{Z}_3\\ -a_{10} - \zeta_3^2a_{11} - \zeta_3a_{12} \in 3\mathbb{Z}_3\\ -a_{10} - \zeta_3a_{11} - \zeta_3^2a_{12} \in 3\mathbb{Z}_3, \end{cases}$$

that is, $a_{10}e_{\rho_{10}} + a_{11}e_{\rho_{11}} + a_{12}e_{\rho_{12}} \in \mathbb{Z}_3[G]$ and hence $z \in \mathbb{Z}_3[G]$. □

From all the above classes we considered and the database [Dok18] we deduce the following.

Corollary 4.6.19. *Let p be an odd prime and let G be a finite group such that $p \nmid |G'|$ and $|G| < 48$. Then there exists a family $\mathcal{H}$ of abelian subquotients of G such that $(p, G, \mathcal{H})$ is Fitting-detectable if and only if G is monomial if and only if $G \ncong \mathrm{SL}_2(\mathbb{F}_3)$.*

4.7 Fitting ideals over maximal orders

We now define Fitting ideals of modules over maximal orders. We start with the following.

Lemma 4.7.1. *Let R be a discrete valuation ring of characteristic 0 and let $\mathcal{M}$ be a maximal R-order in a finitely generated semisimple algebra. Then $\mathcal{M}$ is a clean order.*

Proof. This easily follows from the fact that in this setting every lattice over $\mathcal{M}$ is free, by [Rei03, (18.10)]. □

Proposition 4.7.2. *[JN13, Lemma 4.7] Let R be a discrete valuation ring of characteristic 0 with field of fractions F. Let A be a finite-dimensional semisimple F-algebra and let $\mathcal{M}$ be a maximal R-order in A. Let M be an R-torsion finitely generated $\mathcal{M}$-module. Then M admits a quadratic presentation.*

Proof. Let us consider a surjective map $\pi : \mathcal{M}^n \twoheadrightarrow M$. Then $\ker \pi$, since it is a lattice over $\mathcal{M}$, is projective by [CR81, Theorem (26.12)]. By hypothesis we have that $F \otimes_R M = 0$, which implies that $F \otimes_R \ker \pi = A^n$. Since $\mathcal{M}$ is clean by Lemma 4.7.1, then we deduce that $\ker \pi$ is free of rank n. □

Definition 4.7.3. In the hypotheses of Proposition 4.7.2, let

$$\mathcal{M}^n \xrightarrow{h} \mathcal{M}^n \longrightarrow M \longrightarrow 0$$

be a quadratic presentation of M. By choosing a basis for $\mathcal{M}^n$ we may identify h with an $(n \times n)$-matrix C. Then we define

$$\mathrm{Fitt}_{\mathcal{M}}(M) = \langle \mathrm{nr}_{M_{n\times n}(A)}(C) \rangle_{\zeta(\mathcal{M})}.$$

We will be interested in the following types of orders.

Definition 4.7.4. Let R be a complete discrete valuation ring of characteristic 0 with field of fractions F. Let A be a finite-dimensional semisimple F-algebra and let Λ be an R-order in A. We say that Λ is a *nice Fitting order* if Λ is a finite product of a maximal order and matrix rings over commutative orders.

Let $\Lambda = \mathcal{M} \times \prod_i M_{n_i \times n_i}(\Gamma_i)$ be a nice Fitting order, with $\mathcal{M}$ maximal and Γ_i commutative, and let M be a finitely presented Λ-module. Then we define

$$\mathrm{Fitt}_{\Lambda}(M) = \mathrm{Fitt}_{\mathcal{M}}(M) \cdot \mathrm{Fitt}_{\prod_i M_{n_i \times n_i}(\Gamma_i)}(M)$$

as an ideal of $\zeta(\Lambda) = \zeta(\mathcal{M}) \cdot \prod_i \Gamma_i$.

Remark 4.7.5. We can define Fitting ideals (or better, Fitting invariants) without assuming that Λ is a nice Fitting order, but the definition is far more complicated. See [JN13] for the general setting and results about the compatibility between the definitions.

Remark 4.7.6. In the above hypothesis, let Λ be nice and let $e \in \Lambda$ be a central idempotent. Then $e\Lambda$ is nice. In fact, we can work component by component: if Λ is a maximal order then so is $e\Lambda$; if Λ is a matrix over a commutative R-order then so is $e\Lambda$ by Remark 4.2.20.

We have the following results, proved in [JN13].

Proposition 4.7.7. *In the above setting let Λ be a nice Fitting order. Let M_1, M_2, M_3 be finitely presented Λ-modules. Then we have the following:*

(i) $\mathrm{Fitt}_\Lambda(M_1) \subseteq \mathrm{Ann}_{\zeta(\Lambda)}(M_1)$;

(ii) *if there exists a surjection $M_1 \twoheadrightarrow M_2$ then* $\mathrm{Fitt}_R(M_1) \subseteq \mathrm{Fitt}_R(M_2)$;

(iii) *if $M_2 \cong M_1 \oplus M_3$ then*

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) = \mathrm{Fitt}_R(M_2);$$

(iv) *if $M_1 \to M_2 \to M_3 \to 0$ is an exact sequence then*

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) \subseteq \mathrm{Fitt}_R(M_2).$$

If we restrict to group rings the theory of nice Fitting orders reduces to the theory of orders which are products of matrix rings over commutative rings. In fact we have the following ([JN13, Proposition 4.4]).

Theorem 4.7.8. *Let R be a complete discrete valuation ring with residue characteristic $p > 0$ and let G be a finite group. Then $R[G]$ is a nice Fitting order if and only if $p \nmid |G'|$ if and only if $R[G]$ is a product of matrix rings over commutative R-orders.*

We end with the following.

Proposition 4.7.9. *In the above setting, let Λ be a nice Fitting order and let M be a finitely presented Λ-module. Let $e \in \Lambda$ be a central idempotent. Then*

$$e\mathrm{Fitt}_\Lambda(M) = \mathrm{Fitt}_{e\Lambda}(e\Lambda \otimes_\Lambda M).$$

Proof. See [JN13, Theorem 3.1(vi)]. □

4.7.1 Functoriality for modules over maximal orders

In this subsection we generalise concepts and results of §4.4.

Let R be a complete discrete valuation ring with residue characteristic $p > 0$ and let G be a finite group. Suppose that the field of fractions F of R has characteristic 0. Let $e \in R[G]$ be central idempotent and let $\mathcal{M}$ be a maximal order in $eF[G]$. Let $H = G_1/G_2$ be a subquotient of G such that $e \in R[G_1]$. Let $\mathcal{M}_{G_1}$ be a choice

of a maximal order in $eF[G_1]$ contained in $\mathcal{M}$. Let $\mathcal{M}_H$ be the image of $\mathcal{M}_{G_1}$ in $eF[H] = eF[G_1/G_2]$, which is still maximal. Denote by A the algebra $eF[G]$ and define A_{G_1} and A_H as in §4.4.

Lemma 4.7.10. *We have that $\mathcal{M}$ is free over $\mathcal{M}_{G_1}$.*

Proof. This is an easy consequence of Lemma 4.7.1 and the first part of the proof of Lemma 4.4.8. □

Let H be a subquotient of G. Then composition of quotient with restriction induces the following maps:

$$
\begin{aligned}
{}_{\mathcal{M}}\mathfrak{M} &\longrightarrow {}_{\mathcal{M}_H}\mathfrak{M} \\
K_0(\mathcal{M}) &\longrightarrow K_0(\mathcal{M}_H) \\
K_1(\mathcal{M}) &\longrightarrow K_1(\mathcal{M}_H) \\
K_0(\mathcal{M}, K) &\longrightarrow K_0(\mathcal{M}_H, K)
\end{aligned}
$$

We will denote all these maps by f_H. Working factor by factor, we can also define f_H for nice Fitting orders in $eF[G]$, with the usual properties still valid.

As in §4.5, we have the following result.

Lemma 4.7.11. *Let R be a complete discrete valuation ring of characteristic 0 with field of fractions F. Suppose the residue field is finite and has characteristic $p > 0$. Let A be a finite-dimensional semisimple F-algebra and let Λ be a nice Fitting R-order in A. Let M be a quadratically presented R-torsion Λ-module. Let $x \in K_1(A)$ be such that $\delta(x) = [M] \in K_0(\mathcal{M}, F)$. Then $\mathrm{Fitt}_\Lambda(M) = \langle \mathrm{nr}_A(x) \rangle_{\zeta(\Lambda)}$.*

The following has exactly the same proof as Proposition 4.5.2.

Proposition 4.7.12. *In the hypotheses of Lemma 4.7.11, let $\theta \in \zeta(A)^\times$. Then θ generates $\mathrm{Fitt}_\Lambda(M)$ if and only if $[M] - \delta \circ \mathrm{nr}_A^{-1}(\theta) = 0$ in $K_0(\Lambda, F)$.*

Corollary 4.7.13. *Let R be a complete discrete valuation ring with finite residue field of characteristic $p > 0$ and let G be a finite group. Suppose that the field of fractions F of R and has characteristic 0. Let $e \in R[G]$ be a central idempotent and let Λ be a nice Fitting order in $eF[G]$. Suppose that there exists a family $\mathcal{H}$ of subquotients such that*

$$
f_{\mathcal{H}} := \prod_{H \in \mathcal{H}} f_H : K_0(\Lambda, F) \longrightarrow \prod_{H \in \mathcal{H}} K_0(\Lambda_H, F)
$$

is injective. Let $\theta \in \zeta(A)^\times$. If θ_H generates $\mathrm{Fitt}_{\Lambda_H}(M_H)$ for every $H \in \mathcal{H}$, then θ generates $\mathrm{Fitt}_\Lambda(M)$.

4.8 A general reduction step

With the concept of Fitting ideal over a maximal order, we can now obtain the following very general results.

We recall the notion of hybrid group rings, which we already introduced in §2.4.1.

Definition 4.8.1. Let R be a discrete valuation ring with field of fractions F, let G be a finite group and let N be a normal subgroup of G. We say that $R[G]$ is N-hybrid if $|N| \in R^\times$ and $(1-e_N)R[G]$ is a maximal R-order in $(1-e_N)F[G]$.

Remark 4.8.2. The group ring $R[G]$ is a maximal R-order if and only if $|G| \in R^\times$ if and only if $R[G]$ is G-hybrid, where the first equivalence is given by [CR81, (27.1)].

Proposition 4.8.3. *[JN16, Lemma 2.13] Let $G = N \rtimes H$ be a Frobenius group. Then, for every prime p not dividing $|N|$, the group ring $\mathbb{Z}_p[G]$ is N-hybrid.*

Proposition 4.8.4. *[JN16, Lemma 2.9] Let Q be a finite group of order prime to p. If $\mathbb{Z}_p[G]$ is N-hybrid, then $\mathbb{Z}_p[G \times Q]$ is $(N \times 1)$-hybrid.*

Proposition 4.8.5. *Let R be a complete discrete valuation ring with residue characteristic $p > 0$ and field of fractions F with characteristic 0, let G be a finite group and let $e \in R[G]$ be a central idempotent. Let Λ be a nice Fitting order in $eF[G]$. Let N be a normal subgroup of G and suppose that $(1-e_N)\Lambda$ is a maximal R-order (e.g. if $\Lambda \supseteq eR[G]$ and $R[G]$ is N-hybrid). Let M be a finitely generated R-torsion Λ-module. Let $\theta \in \zeta(\Lambda)^\times$ be such that $\theta_{G/N} \in \mathrm{Fitt}_{\Lambda_{G/N}}(M_{G/N})$ and $\theta \in \mathrm{Fitt}_{\mathcal{M}}(\mathcal{M} \otimes_\Lambda M)$, where $\mathcal{M} \supseteq \Lambda$ is a maximal R-order. Then $\theta \in \mathrm{Fitt}_\Lambda(M)$.*

Proof. By Proposition 4.7.9 we know that

$$\mathrm{Fitt}_{\Lambda_{G/N}}(M_{G/N}) = \mathrm{Fitt}_{e_N\Lambda}(e_N M) = e_N \mathrm{Fitt}_\Lambda(M).$$

Hence $e_N\theta = \theta_{G/N} \in e_N\mathrm{Fitt}_\Lambda(M) \subseteq \mathrm{Fitt}_\Lambda(M)$. Moreover, since $(1-e_N)\Lambda$ is maximal,

$$\begin{aligned}(1-e_N)\theta \in (1-e_N)\mathrm{Fitt}_{\mathcal{M}}(\mathcal{M} \otimes_\Lambda M) &= \mathrm{Fitt}_{(1-e_N)\mathcal{M}}((1-e_N)\mathcal{M} \otimes_\Lambda M) \\ &= \mathrm{Fitt}_{(1-e_N)\Lambda}((1-e_N)M) = (1-e_N)\mathrm{Fitt}_\Lambda(M) \subseteq \mathrm{Fitt}_\Lambda(M).\end{aligned}$$

This concludes the proof since $\theta = e_N\theta + (1-e_N)\theta$. □

Example 4.8.6. Let $N \rtimes H$ be a Frobenius group and let p be a prime such that $p \nmid |N|$. Let Q be a group such that $p \nmid |Q|$. Then by Proposition 4.8.3 and Proposition 4.8.4, if $G = (N \rtimes H) \times Q$ then $\mathbb{Z}_p[G]$ is N-hybrid and we can apply Proposition 4.8.5. If Q has even order and $j \in Q \subseteq G$ is central of order 2, then we can apply Proposition 4.8.3 for $\Lambda = \frac{1-j}{2}\mathbb{Z}_p[G]$.

4.9 The case of maximal orders and nice Fitting orders

We start the section by generalising the previous definition of Fitting-detectable triple.

Definition 4.9.1. Let R be a complete discrete valuation ring, let G be a finite group, let $e \in R[G]$ be a central idempotent and let Λ be a nice Fitting order in $A = eF[G]$. Let $\mathcal{H}$ be a family of subquotients of G. Consider the map

$$f_{\mathcal{H}} := \prod_{H \in \mathcal{H}} f_H : \zeta(A)^\times \longrightarrow \prod_{H \in \mathcal{H}} \zeta(A_H)^\times.$$

We will say that the triple $(\Lambda, G, \mathcal{H})$ is *Fitting-detectable* if it satisfies the following containment:

$$f_{\mathcal{H}}^{-1}\left(\prod_{H\in\mathcal{H}}\left(\zeta(\Lambda_H)\cap\zeta(A_H)^\times\right)\right)\subseteq\zeta(\Lambda)\cap\zeta(A)^\times. \tag{4.9.1}$$

The following results have the same proof as in §4.6 (in Lemma 4.9.2, for every H we are choosing a maximal order in $(eA)_H$ as the multiplication by e of the one we choose in A_H, as our definition of $\mathcal{M}_{G_1}$ was arbitrary).

Lemma 4.9.2. *Keep the hypotheses of Definition 4.9.1. Let $e\in\Lambda$ be a central idempotent such that $e\in R[G_1]$ for every $G_1/G_2\in\mathcal{H}$. If $(\Lambda, G, \mathcal{H})$ is Fitting-detectable, then $(e\Lambda, G, \mathcal{H})$ is Fitting-detectable.*

Theorem 4.9.3. *Suppose that $(\Lambda, G, \mathcal{H})$ is Fitting-detectable. Let $\theta\in\zeta(A)^\times$ and let M be a finitely presented R-torsion Λ-module with quadratic presentation. If $\theta_H\in\mathrm{Fitt}_{\Lambda_H}(M_H)$ for every $H\in\mathcal{H}$, then $\theta\in\mathrm{Fitt}_\Lambda(M)$.*

Proposition 4.9.4. *Let G be a finite monomial group and let p be a prime number. Let $\mathcal{H}$ be the set of cyclic subquotients. Let $\mathcal{M}$ be a maximal order in $\mathbb{Q}_p[G]$ containing $\mathbb{Z}_p[G]$. Then $(\mathcal{M}, G, \mathcal{H})$ is Fitting-detectable.*

Proof. We start by noting that for every $H\in\mathcal{H}$ we have that $\mathcal{M}_H$ is a maximal order as well, by definition. Let $z\in\zeta(\mathbb{Q}_p[G])^\times$ be such that $z_H\in\zeta(\mathcal{M}_H)$ for every $H\in\mathcal{H}$; we want to show that $z\in\mathcal{M}$. Since $z\in(\mathbb{C}_p[G])^\times$, we can write $z=\sum_{\chi\in\mathrm{Irr}(G)}a_\chi e_\chi$, with $a_\chi\in\mathbb{C}_p^\times$. As we already know that $z\in\mathbb{Q}_p[G]$, if we show that a_χ is integral over $\mathbb{Z}_p$ for every χ we are done.

Let us fix $\chi\in\mathrm{Irr}(G)$. Since G is monomial, then there exists a subgroup G_1 of G and a linear character $\lambda\in\mathrm{Irr}(G_1)$ such that $\chi=\mathrm{Ind}_{G_1}^G\lambda$; this is the same as saying that we find a cyclic subquotient H of G and a linear character $\mu\in\mathrm{Irr}(H)$ such that $\chi=\mathrm{Ind}_{G_1}^G\mathrm{Infl}_H^{G_1}\mu$. We now compute the λ-coefficient b_λ of $z_{G_1}=\sum_{\psi\in\mathrm{Irr}(G_1)}b_\psi e_\psi$: using (4.5.1), we find that $b_\lambda=a_\chi$. Finally, the coefficient c_μ of $z_H=\sum_{\varphi\in\mathrm{Irr}(H)}c_\varphi e_\varphi$ is equal to a_χ as well (since the quotient corresponds to the projection into the characters of G_1 lifted from H). Since z_H is in a maximal order in $\mathbb{Q}_p[H]$, then $b_\mu=a_\chi$ is integral over $\mathbb{Z}_p$, which is what we wanted to show. □

4.10 On the Brumer-Stark Conjecture

The main arithmetic motivation for our results on Fitting ideals is the Brumer-Stark conjecture. As we will see our approach will provide a rather direct way to deduce in several cases the non-abelian Brumer-Stark conjecture from the abelian Brumer-Stark conjecture, now a theorem outside the prime 2.

4.10.1 Overview of the Brumer-Stark conjecture

Let L/K be a Galois extension of number fields with Galois group G. Let S_∞ be the set of archimedean places of K. Let $S\supseteq S_\infty$ be a finite set of places of K containing the primes which ramify in L. Let χ be a complex irreducible character of G and let

V_χ be a $\mathbb{C}[G]$-module with character χ. For every place v of K, we choose a place w of L above v, with inertia group I_w. We let ϕ_w denote any lifting of the Frobenius in G. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, we define the Artin L-function as

$$L_S(s,\chi) = \prod_{v \notin S} \det\left(1 - N(v)^{-s}\phi_w \mid_{V_\chi^{I_w}}\right)^{-1}$$

and

$$L_S(s) = (L_S(s,\chi))_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \in \zeta(\mathbb{C}[G]),$$

where we used the identification $\zeta(\mathbb{C}[G]) \cong \prod_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}$ and $N(v) \in \mathbb{Z}$ is the norm of v, or, which is the same, the cardinality of the residue field of K at v. The two functions have meromorphic continuation to the whole complex plane $\mathbb{C}$. Let T another finite set of places (indeed, finite primes) of K such that $S \cap T = \emptyset$. Define:

$$\delta_T(s,\chi) = \prod_{v \in T} \det\left(1 - N(v)^{1-s}\phi_w^{-1} \mid_{V_\chi^{I_w}}\right),$$

and

$$\delta_T(s) = (\delta_T(s,\chi))_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \in \zeta(\mathbb{C}[G]),$$

and finally

$$\Theta_{S,T}(s) := \delta_T(s) L_S(s)^\sharp \in \zeta(\mathbb{C}[G]),$$

where $\sharp$ denotes the linear extension to $\mathbb{C}[G]$ of the involution $g \mapsto g^{-1}$. Again these functions have meromorphic continuation to $\mathbb{C}$. From all of this we can define the generalised Stickelberger element $\theta_S^T(L/K) := \Theta_{S,T}(0) \in \zeta(\mathbb{C}[G])$. From a result of Siegel [Sie70], we know that $\Theta_{S,T}(0) \in \zeta(\mathbb{Q}[G])$.

Definition 4.10.1. Let T be a finite sets of (finite) primes of K. We will denote by $\mathrm{Cl}^T(L)$ the group of fractional ideals of L relatively prime to T modulo the principal ideals congruent to 1 modulo every prime of L above a prime in T.

Conjecture 4.10.2 (Abelian Brumer-Stark conjecture)**.** *Let L/K be an abelian Galois extension of number fields with Galois group G, and let S and T be as above. Then*

$$\theta_S^T(L/K) \in \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Cl}^T(L)).$$

Definition 4.10.3. A *CM*-field is a totally imaginary number field which is a quadratic extension of a totally real number field.

Let L be a CM-field. Then every embedding of L into $\mathbb{C}$ defines an automorphism on L obtained by restricting the complex conjugation, which is independent of the embedding into $\mathbb{C}$ (see [Was97, p. 39]). We will typically denote this automorphism by j.

Remark 4.10.4. The Brumer-Stark conjecture can be reduced to the case in which L/K is a Galois CM-extension, that is, a Galois extension where L is CM and K is totally real. For a detailed explanation see [Nic19, Remark 1.1]. Note that if L/K is a Galois CM-extension, then the complex conjugation j fixes K and corresponds to a central element of order 2 in $\mathrm{Gal}(L/K)$. Therefore, a necessary condition for an abstract group G to be isomorphic to the Galois group to a Galois CM-extension is that G contains a central element of order 2.

The following refinement of the Brumer-Stark conjecture was proved in the groundbreaking article [DK20].

Theorem 4.10.5 (Strong abelian Brumer-Stark conjecture outside 2)**.** *Let L/K be an abelian CM-extension of number fields with Galois group G. Let us denote by $j \in G$ be the complex conjugation. Let $\mathbb{Z}[G]_- = \frac{1-j}{2}\mathbb{Z}[\frac{1}{2}][G]$ and, for every $\mathbb{Z}[G]$-module M, let $M^- = \mathbb{Z}[G]_- \otimes_{\mathbb{Z}[G]} M$. Let S and T be as above and let $^\vee$ denote the Pontryagin dual, i.e. $\mathrm{Hom}_{\mathbb{Z}}(\cdot, \mathbb{Q}/\mathbb{Z})$ with G-action given by $g\varphi(x) = \varphi(g^{-1}x)$. Let $^\sharp$ denote the linear extension to $\mathbb{Q}[G]$ of the involution $g \mapsto g^{-1}$. Then*

$$\theta_S^T(L/K)^\sharp \in \mathrm{Fitt}_{\mathbb{Z}[G]_-}(\mathrm{Cl}^T(L)^{\vee,-}).$$

Remark 4.10.6. As summarised in [DK20], the following three observations tell us that Theorem 4.10.5 implies the prime-to-2 part of the abelian Brumer-Stark conjecture: Proposition 4.2.3; the fact that if M is a finite R-module then $\mathrm{Ann}_R(M^\vee) = \mathrm{Ann}_R(M)^\sharp$; the fact that $\theta_S^T(L/K)$ annihilates a $\mathbb{Z}[G]$-module if and only if it annihilates its minus part, as j acts as -1 on $\theta_S^T(L/K)$. Note that we do need to take the dual, as the 'non-dual strong Brumer-Stark property', despite still implying the prime-to-2 part of the Brumer-Stark conjecture, is generally false (as proved in [GK08]).

We note that Theorem 4.10.5 is equivalent to the following.

Theorem 4.10.7. *Assume the notation and setup of Theorem 4.10.5. For every odd prime number p we have*

$$\theta_S^T(L/K)^\sharp \in \mathrm{Fitt}_{\mathbb{Z}_p[G]_-}(\mathrm{Cl}^T(L)^{\vee,-}(p)),$$

where $\cdot(p)$ denotes the p-Sylow subgroup and $\mathbb{Z}_p[G]_- = \frac{1-j}{2}\mathbb{Z}_p[G]$.

Remark 4.10.8. We can indeed notice that $\theta_S^T(L/K)^\sharp$ lives in the minus part, as j acts as -1. It will also be important to keep in mind that $\theta_S^T(L/K)^\sharp \in \zeta(\mathbb{Q}_p[G]_-)^\times$, by the aforementioned result of Siegel.

We now consider the non-abelian generalisation. We refer to [Nic11a] for the definition of $\mathrm{Fitt}_\Lambda^{\max}(M)$. The reader can keep in mind that whenever Λ is a nice Fitting order and M is a finitely-presented Λ-module we have $\mathrm{Fitt}_\Lambda^{\max}(M) = \mathrm{Fitt}_\Lambda(M)$.

Conjecture 4.10.9 (Non-abelian strong Brumer-Stark conjecture)**.** *Let L/K be a Galois CM-extension of number fields and let p be an odd prime number. Let us keep the notation above. Then*

$$\theta_S^T(L/K)^\sharp \in \mathrm{Fitt}^{\max}_{\mathbb{Z}_p[G]_-}(\mathrm{Cl}^T(L)^{\vee,-}(p)).$$

Remark 4.10.10. We now know that the non-abelian Brumer-Stark conjecture at the odd primes is a theorem when $\mathrm{Gal}(L/K)$ has abelian p-Sylow subgroup (which is a generalisation of the condition $p \nmid |\mathrm{Gal}(L/K)'|$). We will outline how the proof goes.

In the recent preprint [BBDS21] the authors provide an unconditional proof of the minus part of the equivariant Tamagawa number conjecture (eTNC for short) in abelian CM-extensions. The eTNC was originally formulated in [BF01], and roughly speaking predicts that, if L/K is a Galois extension of number fields with Galois group G,

then a certain element $T\Omega(L/K,0) \in K_0(\mathbb{Z}[G],\mathbb{R})$ vanishes. If we further assume that $T\Omega(L/K,0) \in K_0(\mathbb{Z}[G],\mathbb{Q})$ (a condition which is equivalent to Stark's conjecture) then the conjecture splits over p-parts. An argument which is essentially the same as Proposition 4.5.2 with [Bur04, Theorem 4.1] and [GRW99, Proposition 9], together with the functorial properties stated in [JN16, Proposition 4.1] (see also [Nic16, Proposition 6.2]), tells us that we can deduce the minus part of the eTNC at p for non-abelian CM-extensions whose Galois groups have abelian p-Sylow subgroups.

By [Nic19, Theorem 4.4] (which refers to [Bur20, Proof of Corollary 3.11(iii)]), the minus part of the eTNC at p implies the (strong) Brumer-Stark conjecture at p. In this section we will focus on providing direct proofs that do not involve the technical machinery of the equivariant Tamagawa number conjecture.

Remark 4.10.11. Let us keep in mind the following setting in which the Brumer-Stark conjecture fits: let R be a complete discrete valuation ring with field of fractions F of characteristic 0 and let Λ be a nice Fitting R-order in the finite dimensional semisimple F-algebra A. Let M be a finitely presented R-torsion Λ-module. We are asking if a certain natural element $\theta \in \zeta(A)^\times$ belongs to $\mathrm{Fitt}_\Lambda(M)$, assuming that this is true whenever Λ is commutative (c.f. Theorem 4.10.7).

We recall that we also have a weak formulation of the Brumer-Stark conjecture (see [Nic11a, §3]), which is now a theorem.

Theorem 4.10.12. *[Nic21, Corollary 1] Let L/K be a Galois CM-extension of number fields and let p be an odd prime number. Let us keep the notation of Theorem 4.10.5. Let $\mathcal{M}$ be a maximal order containing $\mathbb{Z}_p[G]$ and let $\mathcal{M}_-$ be $\frac{1-j}{2}\mathcal{M}$. Then*

$$\theta_S^T(L/K)^\sharp \in \mathrm{Fitt}_{\mathcal{M}_-}(\mathcal{M}_- \otimes_{\mathbb{Z}_p[G]_-} \mathrm{Cl}^T(L)^{\vee,-}(p)).$$

Remark 4.10.13. Note that $\mathcal{M}_-$ is maximal and so we do not need to consider $\mathrm{Fitt}^{\max}$ as originally stated in Nickel's papers.

The proof of Theorem 4.10.12 passes through the p-part of the strong Stark conjecture. C.f. Corollary 4.10.22 for a more direct proof (supposing that the Galois group is monomial).

Corollary 4.10.14. *Let L/K be a Galois CM-extension of number fields and let p be an odd prime number which does not divide $|\mathrm{Gal}(L/K)|$. Then for every pair of admissible sets S and T of places of K we have the Brumer-Stark conjecture at p for L/K.*

In the following subsections our goal is to provide more direct proofs of Brumer-Stark conjecture for some specific cases and families of extensions of number fields. We remark that our results do not cover any new case.

4.10.2 General results on the Brumer-Stark conjecture

In the context of the Brumer-Stark conjecture the functoriality of §4.4 translates as follows. We let $\Lambda = \mathbb{Z}_p[G]_-$ (in the previous notation, we are imposing $e = \frac{1-j}{2}$), $A = \mathbb{Q}_p[G]_-$, $\theta = \theta_S^T(L/K)^\sharp$ and $M = \mathrm{Cl}^T(L)^{\vee,-}(p)$. Let $H = G_1/G_2$ be a subquotient of G corresponding to an intermediate real or CM-extension (that is, j belongs to G_1).

If F/K is a finite extension we denote by $T(F)$ and $S(F)$ the places of F above T and S, respectively. Then in the above notation $M_H = \mathrm{Cl}^{T(L^{G_1})}(L^{G_2})^{\vee,-}(p)$ and $\theta_H = \theta_{S(L^{G_1})}^{T(L^{G_1})}(L^{G_2}/L^{G_1})^\sharp$. The proof for the latter equality is the same as [BB07, Proposition 3.5]. Note that if p is odd and H is an abelian subquotient then $\theta_H \in \mathrm{Fitt}_{\Lambda_H}(M_H)$, by Theorem 4.10.7.

Notation 4.10.15. In all what follows, when we will say that a CM-Galois extension of number fields satisfies the Brumer-Stark conjecture at the prime p, we will implicitly mean that this holds for all admissible sets of places S and T.

After Proposition 4.8.5, and in particular Example 4.8.6, we can now prove the following.

Corollary 4.10.16. *Let L/K be a Galois CM-extension of number fields with Galois group $F \times A$, where F is a Frobenius group and A is an abelian group. Let p be an odd prime number such that $p \nmid |F'|$ and $p \nmid |A|$. Then L/K satisfies the p-part of the Brumer-Stark conjecture.*

Proof. This follows from Proposition 4.8.5 and Proposition 4.8.4. □

Remark 4.10.17. In order for the conditions of Corollary 4.10.16 to be satisfied we need to assume that A has a central element of order 2 as Frobenius groups have no centre (see Remark 4.6.9). For instance, we obtain the Brumer-Stark conjecture at 3 whenever G is isomorphic to $A_4 \times C_2$.

4.10.3 On the Brumer-Stark conjecture assuming quadratic presentation

In the setting of the Brumer-Stark conjecture, if we assume that $\mathrm{Cl}^T(L)^{\vee,-}(p)$ (or equivalently $\mathrm{Cl}(L)^T(p)$) has a quadratic presentation as a $\mathbb{Z}_p[G]_-$-module, we can immediately apply the machinery of §4.6. First of all we have the following consequence of Theorem 4.6.4, Theorem 4.10.7 and Lemma 4.6.3.

Theorem 4.10.18. *Let p be an odd prime number. Let L/K be a Galois CM-extension of number fields with Galois group G such that $p \nmid |G'|$ and let $\mathcal{H}$ be a family of abelian subquotients of G. Suppose that the complex conjugation j belongs to G_1 for every $G_1/G_2 \in \mathcal{H}$. Suppose that $(p, G, \mathcal{H})$ is Fitting-detectable and that $\mathrm{Cl}(L)^T(p)$ has a quadratic presentation. Then L/K satisfies the p-part of the strong Brumer-Stark conjecture.*

Remark 4.10.19. Let p be an odd prime number and let L/K be a Galois CM-extension of number fields with Galois group G. Let S and T have their usual meanings. In [Nic11b, Theorem 1] the author gives sufficient conditions for $\mathrm{Cl}(L)^T(p)$ to be cohomologically trivial (this is equivalent to having a quadratic presentation by [CF67, §IV Theorem 9] and [BPSS04, Proposition 2.2.1]). These conditions include the primes in S above p being either (at most) tamely ramified or with the complex conjugation being in the corresponding decomposition group in G, plus further hypotheses on S and T.

In the following situations, given a finite group G, an odd prime number p, a CM G-extension L/K, and S and T as above, the Brumer-Stark conjecture at p holds if $\mathrm{Cl}(L)^T(p)$ has a quadratic presentation and:

(i) G is of the form $P \times Q$ where $P \cong N \rtimes H$ is a Frobenius group such that $p \nmid |P'|$, N and H are abelian and Q is an abelian group of even order, from Proposition 4.6.13 and Corollary 4.10.18. For instance this applies to $A_4 \times C_6$ at 3 and $S_3 \times C_{10}$ at 5;

(ii) G is of the form $Q_8 \times Q$ with abelian Q (that is, a Hamiltonian group), from Proposition 4.6.14 and Corollary 4.10.18;

(iii) G is of the form $D_8 \times Q$ with abelian Q, from Proposition 4.6.15 and Corollary 4.10.18.

Using the database [Dok18], from the above we deduce the following (c.f. Corollary 4.6.19).

Corollary 4.10.20. *Let L/K be a Galois CM-extension of number fields with degree less than 48. Suppose that the Galois group G is such that $p \nmid |G'|$ and $G \ncong \mathrm{SL}_2(\mathbb{F}_3)$. Assuming that $\mathrm{Cl}(L)^T(p)$ has quadratic presentation, we have the p-part of the Brumer-Stark conjecture.*

Using Proposition 4.6.12 we deduce the following.

Corollary 4.10.21. *Let p be an odd prime number and let $G \ncong \mathrm{SL}_2(\mathbb{F}_3)$ be a finite group such that $p \nmid |G'|$ and $|G| < 48$. Let Q be an abelian group such that $p \nmid |Q|$ and each cyclic component has order dividing $p-1$. Let L/K be a CM $G \times Q$-extension (if for instance Q is even then such an extension is always realisable). Then, assuming that $\mathrm{Cl}(L)^T(p)$ has quadratic presentation, we have the p-part of the Brumer-Stark conjecture.*

We conclude the chapter with the following easier proof of Theorem 4.10.12 (restricting to monomial groups).

Corollary 4.10.22. *Let p be an odd prime number. Let L/K be a Galois CM-extension of number fields with monomial Galois group G. Then L/K satisfies the p-part of the weak Brumer-Stark conjecture as stated in Theorem 4.10.12.*

Proof. Let $\mathcal{H}$ be the family of cyclic subquotients of G and let $\mathcal{H}'$ be the family of abelian subquotients $G_1/G_2 \in \mathcal{H}$ such that $j \in G_1$. Let $\mathcal{M}$ be a maximal order in $\mathbb{Q}_p[G]$. We will prove that $(\mathcal{M}, G, \mathcal{H}')$ is Fitting-detectable, which will suffice by Theorem 4.9.3 and Lemma 4.9.2.

Let $z \in \zeta(\mathbb{Q}_p[G])^\times$ be such that $z_H \in \zeta(\mathcal{M}_H)$ for every $H \in \mathcal{H}'$. We will show that $z_H \in \zeta(\mathcal{M}_H)$ for every $H \in \mathcal{H}$, which will imply that $z \in \zeta(\mathcal{M})$ by Proposition 4.9.4.

Let $H \in \mathcal{H}$. If $j \in H$, then $H \in \mathcal{H}'$ and so automatically $z_H \in \zeta(\mathcal{M}_H)$. Otherwise, we have that $G_1' := \langle G_1, j\rangle \cong G_1 \times \langle j\rangle$ and $H' := G_1'/G_2 \cong H \times \langle j\rangle \in \mathcal{H}'$. We note that $z_H = \mathrm{res}_H^{H\times\langle j\rangle}(z_{H\times\langle j\rangle})$, by Remark 4.4.10. Since $z_{H\times\langle j\rangle} \in \zeta(\mathcal{M}_{H\times\langle j\rangle})$, its coefficients in the character-expansion are integral over $\mathbb{Z}_p$. By (4.5.1), this is also

true for $\mathrm{res}_H^{H\times\langle j\rangle}(z_{H\times\langle j\rangle})$, which is therefore in the corresponding maximal order. This concludes the proof. □

Bibliography

[Acc70] R. D. M. Accola. Two theorems on Riemann surfaces with noncyclic automorphism groups. *Proc. Amer. Math. Soc.*, 25:598–602, 1970.

[Ax65] J. Ax. On the units of an algebraic number field. *Illinois J. Math.*, 9:584–589, 1965.

[BB04] W. Bley and R. Boltje. Cohomological Mackey functors in number theory. *J. Number Theory*, 105(1):1–37, 2004.

[BB07] M. Breuning and D. Burns. Leading terms of Artin L-functions at $s = 0$ and $s = 1$. *Compos. Math.*, 143(6):1427–1464, 2007.

[BBDS21] D. Bullach, D. Burns, A. Daoud, and S. Seo. Dirichlet L-series at $s = 0$ and the scarcity of Euler systems. *arXiv preprint arXiv:2111.14689*, 2021.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BD14] A. Bartel and T. Dokchitser. Brauer relations in finite groups II: Quasi-elementary groups of order $p^a q$. *J. Group Theory*, 17(3):381–393, 2014.

[BD15] A. Bartel and T. Dokchitser. Brauer relations in finite groups. *J. Eur. Math. Soc. (JEMS)*, 17(10):2473–2512, 2015.

[Ber72] A.-M. Bergé. Sur l'arithmétique d'une extension diédrale. *Ann. Inst. Fourier (Grenoble)*, 22(2):31–59, 1972.

[Ber78] A.-M. Bergé. Arithmétique d'une extension galoisienne à groupe d'inertie cyclique. *Ann. Inst. Fourier (Grenoble)*, 28(4):17–44, ix, 1978.

[Ber79] A.-M. Bergé. Projectivite des anneaux d'entiers sur leurs ordres associés. *Astérisque*, 61:15–28, 1979.

[BF01] D. Burns and M. Flach. Tamagawa numbers for motives with (non-commutative) coefficients. *Doc. Math.*, 6:501–570, 2001.

[BFHP22] J.-F. Biasse, C. Fieker, T. Hofmann, and A. Page. Norm relations and computational problems in number fields. *J. Lond. Math. Soc. (2)*, 105(4):2373–2414, 2022.

[BJ08] W. Bley and H. Johnston. Computing generators of free modules over orders in group algebras. *J. Algebra*, 320(2):836–852, 2008.

[BJ11] W. Bley and H. Johnston. Computing generators of free modules over orders in group algebras II. *Math. Comp.*, 80(276):2411–2434, 2011.

[Bol97] R. Boltje. Class group relations from Burnside ring idempotents. *J. Number Theory*, 66(2):291–305, 1997.

[BPSS04] D. Burns, C. Popescu, J. Sands, and D. Solomon. *Stark's conjectures: recent work and new directions: an international conference on Stark's conjectures and related topics, August 5-9, 2002, Johns Hopkins University.* American Mathematical Society, 2004.

[Bre04] M. Breuning. *Equivariant epsilon constants for Galois extensions of number fields and p-adic fields.* PhD thesis, King's College London (University of London), 2004.

[Bru67] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[BS87] J. Buchmann and J. W. Sands. An algorithm for testing Leopoldt's conjecture. *J. Number Theory*, 27(1):92–105, 1987.

[BS88] J. Buchmann and J. W. Sands. Leopoldt's conjecture in parameterized families. *Proc. Amer. Math. Soc.*, 104(1):43–48, 1988.

[Bur04] D. Burns. Equivariant Whitehead torsion and refined Euler characteristics. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 35–59. Amer. Math. Soc., Providence, RI, 2004.

[Bur20] D. Burns. On derivatives of p-adic L-series at $s = 0$. *J. Reine Angew. Math.*, 762:53–104, 2020.

[BW09] W. Bley and S. M. J. Wilson. Computations in relative algebraic K-groups. *LMS J. Comput. Math.*, 12:166–194, 2009.

[CF67] J. W. S. Cassels and A. Fröhlich. *Algebraic number theory: proceedings of an instructional conference.* Academic press, 1967.

[Cha96] R. J. Chapman. A simple proof of Noether's theorem. *Glasgow Math. J.*, 38(1):49–51, 1996.

[CR81] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[CR87] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. II.* John Wiley & Sons, Inc., New York, 1987. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[DJ83] F. R. DeMeyer and G. J. Janusz. Group rings which are Azumaya algebras. *Trans. Amer. Math. Soc.*, 279(1):389–395, 1983.

[DK20] S. Dasgupta and M. Kakde. On the Brumer-Stark conjecture. *arXiv preprint arXiv:2010.00657*, 2020.

[Dok18] T. Dokchitser. Group names. https://people.maths.bris.ac.uk/∼matyd/GroupNames/, 2018. [Online].

[EH79] S. Endô and Y. Hironaka. Finite groups with trivial class groups. *J. Math. Soc. Japan*, 31(1):161–174, 1979.

[EKW84] M. Emsalem, H. H. Kisilevsky, and D. B. Wales. Indépendance linéaire sur $\overline{\mathbf{Q}}$ de logarithmes p-adiques de nombres algébriques et rang p-adique du groupe des unités d'un corps de nombres. *J. Number Theory*, 19(3):384–391, 1984.

[Fer21] F. Ferri. Leopoldt-type theorems for non-abelian extensions of Q. *arXiv preprint arXiv:2112.09525*, 2021.

[Fit06] W. B. Fite. Groups whose orders are powers of a prime. *Trans. Amer. Math. Soc.*, 7(1):61–68, 1906.

[Fit36] H. Fitting. Die Determinantenideale eines Moduls. *Jahresber. Dtsch. Math.-Ver.*, 46:195–228, 1936.

[FKW74] A. Fröhlich, M. E. Keating, and S. M. J. Wilson. The class groups of quaternion and dihedral 2-groups. *Mathematika*, 21:64–71, 1974.

[Frö72] A. Fröhlich. Artin root numbers and normal integral bases for quaternion fields. *Invent. Math.*, 17:143–166, 1972.

[Frö83] A. Fröhlich. *Galois module structure of algebraic integers*, volume 1 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1983.

[FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[Fun79] T. Funakura. On Artin theorem of induced characters. *Comment. Math. Univ. St. Paul.*, 27(1):51–58, 1978/79.

[GK08] C. Greither and M. Kurihara. Stickelberger elements, Fitting ideals of class groups of CM-fields, and dualisation. *Math. Z.*, 260(4):905–930, 2008.

[Glu81] David Gluck. Idempotent formula for the Burnside algebra with applications to the p-subgroup simplicial complex. *Illinois J. Math.*, 25(1):63–67, 1981.

[GRW99] K. W. Gruenberg, J. Ritter, and A. Weiss. A local approach to Chinburg's root number conjecture. *Proc. London Math. Soc. (3)*, 79(1):47–80, 1999.

[Hat65] A. Hattori. Rank element of a projective module. *Nagoya Math. J.*, 25:113–120, 1965.

[HJ20] T. Hofmann and H. Johnston. Computing isomorphisms between lattices. *Math. Comp.*, 89(326):2931–2963, 2020.

[HKS74] F. Halter-Koch and H.-J. Stender. Unabhängige Einheiten für die Körper $K = Q(\sqrt[n]{(D^n \pm d)})$ mit dD^n. *Abh. Math. Sem. Univ. Hamburg*, 42:33–40, 1974.

[Isa94] I. M. Isaacs. *Character theory of finite groups*. Dover Publications, Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423 (57 #417)].

[Jac68] H. Jacobinski. Genera and decompositions of lattices over orders. *Acta Math.*, 121:1–29, 1968.

[Jau81] J.-F. Jaulent. Sur la l-structure galoisienne des idéaux ambiges dans une extension métacyclique de degré nl sur le corps des rationnels. In *Number theory, 1979–1980 and 1980–1981*, Publ. Math. Fac. Sci. Besançon, pages Exp. No. 3, 20. Univ. Franche-Comté, Besançon, 1981.

[JN13] H. Johnston and A. Nickel. Noncommutative Fitting invariants and improved annihilation results. *J. Lond. Math. Soc. (2)*, 88(1):137–160, 2013.

[JN16] H. Johnston and A. Nickel. On the equivariant Tamagawa number conjecture for Tate motives and unconditional annihilation results. *Trans. Amer. Math. Soc.*, 368(9):6539–6574, 2016.

[JN18] H. Johnston and A. Nickel. Hybrid Iwasawa algebras and the equivariant Iwasawa main conjecture. *Amer. J. Math.*, 140(1):245–276, 2018.

[JN20] H. Johnston and A. Nickel. On the p-adic Stark conjecture at $s = 1$ and applications. *J. Lond. Math. Soc., II. Ser.*, 101(3):1320–1354, 2020.

[Joh15] H. Johnston. Explicit integral Galois module structure of weakly ramified extensions of local fields. *Proc. Amer. Math. Soc.*, 143(12):5059–5071, 2015.

[JR06] J. W. Jones and D. P. Roberts. A database of local fields. *J. Symbolic Comput.*, 41(1):80–97, 2006.

[Kan85] E. Kani. Relations between the genera and between the Hasse-Witt invariants of Galois coverings of curves. *Canad. Math. Bull.*, 28(3):321–327, 1985.

[Kaw86] F. Kawamoto. On normal integral bases of local fields. *J. Algebra*, 98(1):197–199, 1986.

[Kea74] M. E. Keating. Class groups of metacyclic groups of order $p^r q$, p a regular prime. *Mathematika*, 21:90–95, 1974.

[Kli90] N. Klingen. Leopoldt's conjecture for imaginary Galois number fields. *J. Symbolic Comput.*, 10(6):531–545, 1990.

[KR89] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[KR94] E. Kani and M. Rosen. Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties. *J. Number Theory*, 46(2):230–254, 1994.

[KW14] C. Khare and J.-P. Wintenberger. Ramification in Iwasawa theory and splitting conjectures. *Int. Math. Res. Not. IMRN*, (1):194–223, 2014.

[Lam99] T. Y. Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[Lau89] M. Laurent. Rang p-adique d'unités et action de groupes. *J. Reine Angew. Math.*, 399:81–108, 1989.

[Leo59] H.-W. Leopoldt. Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers. *J. Reine Angew. Math.*, 201:119–149, 1959.

[Leo62] H.-W. Leopoldt. Zur Arithmetik in abelschen Zahlkörpern. *J. Reine Angew. Math.*, 209:54–71, 1962.

[Let90] G. Lettl. The ring of integers of an abelian number field. *J. Reine Angew. Math.*, 404:162–170, 1990.

[Let98] G. Lettl. Relative Galois module structure of integers of local abelian fields. *Acta Arith.*, 85(3):235–248, 1998.

[Lev92] C. Levesque. $\mathbf{Z}_p$-independent systems of units. *Proc. Japan Acad. Ser. A Math. Sci.*, 68(8):239–241, 1992.

[LMF19] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2019. [Online; accessed 30 October 2019].

[Mak22] A. Maksoud. On Leopoldt's and Gross's defects for Artin representations. *arXiv preprint arXiv:2201.08203*, 2022.

[Mar71] J. Martinet. Modules sur l'algèbre du groupe quaternionien. *Ann. Sci. École Norm. Sup. (4)*, 4:399–408, 1971.

[Mar72] J. Martinet. Sur les extensions à groupe de Galois quaternionien. *C. R. Acad. Sci. Paris Sér. A-B*, 274:A933–A935, 1972.

[Mau84] E. Maus. Zur Arithmetik einiger Serien nichtauflösbarer Gleichungen 5. Grades. *Abh. Math. Sem. Univ. Hamburg*, 54:227–250, 1984.

[Mil14] J. C. Miller. Class numbers of real cyclotomic fields of composite conductor. *LMS J. Comput. Math.*, 17(suppl. A):404–417, 2014.

[Miy82] K. Miyake. On the units of an algebraic number field. *J. Math. Soc. Japan*, 34(3):515–525, 1982.

[MZ87] M. L. Madan and H. G. Zimmer. Relations among Iwasawa invariants. *J. Number Theory*, 25(2):213–219, 1987.

[Nag22] T. Nagel. Zur arithmetik der polynome. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 1, pages 178–193. Springer, 1922.

[Nak93] K. Nakamula. On certain number fields with small regulators. Number 837, pages 130–141. 1993. Interdisciplinary studies on number theory (Japanese) (Kyoto, 1992).

[Nic10] A. Nickel. Non-commutative Fitting invariants and annihilation of class groups. *J. Algebra*, 323(10):2756–2778, 2010.

[Nic11a] A. Nickel. On non-abelian Stark-type conjectures. *Ann. Inst. Fourier (Grenoble)*, 61(6):2577–2608 (2012), 2011.

[Nic11b] A. Nickel. On the equivariant Tamagawa number conjecture in tame CM-extensions. *Math. Z.*, 268(1-2):1–35, 2011.

[Nic16] A. Nickel. Integrality of Stickelberger elements and the equivariant Tamagawa number conjecture. *J. Reine Angew. Math.*, 719:101–132, 2016.

[Nic19] A. Nickel. Conjectures of Brumer, Gross and Stark. In *Spectral structures and topological methods in mathematics*, pages 365–388. Zürich: European Mathematical Society (EMS), 2019.

[Nic20] A. Nickel. Notes on noncommutative Fitting invariants (with an appendix by H. Johnston and A. Nickel). In *Development of Iwasawa theory – the centennial of K. Iwasawa's birth. Proceedings of the international conference "Iwasawa 2017", University of Tokyo, Tokyo, Japan, July 19–28, 2017*, pages 27–60. Tokyo: Mathematical Society of Japan, 2020.

[Nic21] A. Nickel. The strong Stark conjecture for totally odd characters. *arXiv preprint arXiv:2106.05619*, 2021.

[Noe32] E. Noether. Normalbasis bei Körpern ohne höhere Verzweigung. *J. Reine Angew. Math.*, 167:147–152, 1932.

[Nor76] D. G. Northcott. *Finite free resolutions*. Cambridge Tracts in Mathematics, No. 71. Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Rei03] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[Rog70] K. W. Roggenkamp. *Lattices over orders. II*. Lecture Notes in Mathematics, Vol. 142. Springer-Verlag, Berlin-New York, 1970.

[RU74] I. Reiner and S. Ullom. Remarks on class groups of integral group rings. *Symposia Mathematica, Vol. XIII (Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972)*, pages 501–516, 1974.

[Ser79] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Shi92] T. Shimada. Some remarks on Leopoldt's conjecture. *Manuscripta Math.*, 77(4):405–414, 1992.

[Sie70] C. L. Siegel. Über die Fourierschen Koeffizienten von Modulformen. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, 1970:15–56, 1970.

[Ste72] H.-J. Stender. Einheiten für eine allgemeine Klasse total reeller algebraischer Zahlkörper. *J. Reine Angew. Math.*, 257:151–178, 1972.

[Swa68] R. G. Swan. *Algebraic K-theory*. Lecture Notes in Mathematics, No. 76. Springer-Verlag, Berlin-New York, 1968.

[Tay81] M. J. Taylor. On Fröhlich's conjecture for rings of integers of tame extensions. *Invent. Math.*, 63(1):41–79, 1981.

[Tho79] E. Thomas. Fundamental units for orders in certain cubic number fields. *J. Reine Angew. Math.*, 310:33–55, 1979.

[Wal81] M. Waldschmidt. Transcendance et exponentielles en plusieurs variables. *Invent. Math.*, 63(1):97–127, 1981.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.