University of Exeter
Department of Mathematics

Integral Clifford Theory and the Computation of Denominator Ideals

David Watson

May 2018

Supervised by Dr Henri Johnston

Submitted by David Watson, to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Mathematics , May 2018.

This thesis is available for Library use on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

I certify that all material in this thesis which is not my own work has been identified and that no material has previously been submitted and approved for the award of a degree by this or any other University.

(signature) .....

Abstract

Let R be a commutative ring. To each finitely presented R-module M one can associate an ideal, $\mathrm{Fit}_R(M)$, called the (zeroth) Fitting ideal of M. This ideal is always contained within the R-annihilator of M. Now let R be an integrally closed complete Noetherian local ring and let Λ be a (not necessarily commutative) R-order. A. Nickel generalised the notion of the Fitting ideal, providing a definition of the Fitting invariant for finitely presented modules M over Λ. In this case, to obtain the relation between the Fitting invariant of M and the annihilator of M in the centre of Λ, one must multiply the Fitting invariant of M by a certain ideal, $\mathcal{H}(\Lambda)$, of the centre of Λ, called the denominator ideal of Λ. H. Johnston and A. Nickel have formulated several bounds for the denominator ideal and have computed the denominator ideal for certain group rings. In this thesis, we prove a local-global principle for denominator ideals. We build upon the work of H. Johnston and A. Nickel to give improved bounds for the denominator ideal of Λ assuming some structural knowledge of Λ. We also build upon the work of P. Schmid and K. Roggenkamp to determine structural information about certain group rings. Finally, we use this structural information to compute the denominator ideal of group rings $R[G]$, where G is a p-group with commutator subgroup of order p.

Firstly, I would like to thank my supervisor Henri Johnston for his patience and keen eye for detail, without which this thesis would never have been written. I would like to thank to Andreas Nickel for his hospitality in Bielefeld in October 2017.
I would like to thank Kayvan Nejabati Zenouz, Oli Gregory and the other Exeter PhD students for their help and support, and for putting up with my mathematical (and non-mathematical) ramblings. I am also grateful to Chris Ferro and Mitchell Berger for their pastoral support throughout the last three years.
Finally, I would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council.

Contents

1 Preliminaries

1.1 Introduction

Let R be a commutative ring (with identity) and let M be a finitely presented R-module. In [Fit36], H. Fitting introduced the notion of Fitting ideals associated to M. Thanks to several useful properties, Fitting ideals have since become an important tool in commutative algebra. For example, the zeroth Fitting ideal, $\mathrm{Fit}_R(M)$, is always contained within the R-annihilator of M. We will discuss further properties of $\mathrm{Fit}_R(M)$ in Section 1.2.

More recently there has been an effort to generalise the concept of the Fitting invariant to non-commutative rings. In [Sus88] and [Sus89], J. Susperregui considered skewcommutative graded rings and rings of differential operators satisfying the left Ore property. P. Grime [Gri02] considered several cases including matrix rings over commutative rings, certain hereditary orders and (twisted) group rings. Moreover, A. Parker [Par07] defined non-commutative Fitting invariants for modules with quadratic presentation over the rings $\mathbb{Z}[G]$, $\mathbb{Z}_{(p)}[G]$ or $\mathbb{Z}_p[G]$, where G is a finite group and p is a prime number.

Let R be an integrally closed complete local Noetherian domain with field of fractions F, let A be a separable F-algebra, let Λ be an R-order in A and let M be a finitely generated Λ-module. In [Nic10], A. Nickel gave a definition of the Fitting invariant for M. In the same setting, H. Johnston and A. Nickel [JN13] gave an alternative definition. These two notions are used in different contexts and both have useful properties similar to those of the zeroth Fitting ideal. A further discussion of the merits of these methods is given in Section 1.11.

As in the commutative case, the Fitting invariant of a Λ-module M is related to the annihilator of M over the centre of Λ. However, the relationship is not quite as straightforward as in the case of the zeroth Fitting ideal. The denominator ideal, $\mathcal{H}(\Lambda)$, is needed to formulate a relation between the Fitting invariant of M and the annihilator of M over the centre of Λ. In particular, to obtain annihilators of a Λ-module M the Fitting invariant of M must be multiplied by the denominator ideal of Λ. In this thesis, we address the problem of computing or approximating denominator ideals.

Fitting invariants have several applications in number theory. If L/K is a finite Galois extension of number fields with Galois group G then the class group cl_L of L has a natural structure as a $\mathbb{Z}[G]$-module. There are several conjectures on the annihilators of class groups. For example the Brumer-Stark conjecture, first formulated for non-abelian extensions in [Nic11, Conjecture 2.1], predicts annihilators of cl_L using special values of Artin L-functions and the denominator ideal of $\mathbb{Z}[G]$. If p is a prime number then the p-part of the class group $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{cl}_L$ is a module over $\mathbb{Z}_p[G]$ meaning that Fitting invariants may be used to give a bound on the annihilator of the class group. This technique has

been used in [JN16b] to prove special cases of the non-abelian Brumer-Stark conjecture. See [Nic17a] for a survey of results in this direction.

In [Nic11], A. Nickel showed that for a finite group G and a prime number p, the denominator ideal of the group ring $\mathcal{H}(\mathbb{Z}[G])$ is dense in $\mathcal{H}(\mathbb{Z}_p[G])$. In [JN13], H. Johnston and A. Nickel gave several bounds for the denominator ideal in terms of the central conductor of Λ into a maximal order containing Λ. They also showed that $\mathcal{H}(\mathbb{Z}_p[G])$ is the centre of $\mathbb{Z}_p[G]$ when G is a finite group and p is a prime number such that p does not divide the order of the commutator subgroup of G. In [JN16a] and [JN18], the same authors introduced and developed the notion of an N-hybrid p-adic group ring and computed the denominator ideal for such a ring. In particular, they showed that if G is a Frobenius group then for every prime number p not dividing the order of its Frobenius complement N, the group ring $\mathbb{Z}_p[G]$ is N-hybrid. In [JN13] and [JN16a], they provided explicit bounds for $\mathcal{H}(\mathbb{Z}_p[G])$ for certain pairs of groups G and prime numbers p.

In the rest of the present chapter, we will provide a brief introduction to Fitting invariants and we will introduce notation and key results used throughout the thesis. In Chapter 2, we will generalise an idea from [Nic11, Lemma 1.4] to show that a local-global principle holds for denominator ideals. In Chapter 3, we will provide bounds for the denominator ideal of Λ in terms of the structure of Λ, thereby generalising the bounds given in [JN13]. In Chapter 4, we will compute the structure of certain group rings; this may be read independently of the rest of the thesis. Finally in Chapter 5, we will use the structural information found in Chapter 4 and the bounds for the denominator ideals found in Chapter 3 to compute the denominator ideal explicitly for group rings over finite p-groups with commutator subgroup of order p.

Notation and conventions. Throughout this thesis all rings will be assumed to have an identity element and all modules will be assumed to be right modules unless otherwise stated. We fix the following notation.

$A^\times$ is the group of units of a ring A.

$\mathfrak{Z}(A)$ is the centre of a ring A.

$\mathrm{Irr}_F(G)$ is the set of F-valued irreducible characters of a finite group G, where F is a field.

$M_{m\times m}(R)$ is the ring of $m \times m$ matrices with entries in a ring R.

$\det_F(H)$ is the determinant of a matrix $H \in M_{m\times m}(F)$, where F is a field (sometimes the subscript F may be omitted if it is clear from context).

$\mathrm{ch}_F(H)$ is the characteristic polynomial of a matrix $H \in M_{m\times m}(F)$, where F is a field (the subscript F will never be omitted, to avoid confusion with a related term).

$\mathbb{Z}_{>0}$ is the set of positive integers.

$\mathbb{Z}_{\geq 0}$ is the set of non-negative integers.

$\mathbb{F}_q$ is the finite field of order q, where q is a prime power.

$\mathbb{Q}_p$ is the p-adic numbers, where p is a prime number.

$\mathbb{Z}_p$ is the p-adic integers, where p is a prime number.

$\mathbb{Z}_{(p)}$ is the integers localised at the prime number p.

$M_{\mathfrak{p}}$ is the localisation of an R-module M at the prime ideal $\mathfrak{p}$ of R, where R is an integrally closed Noetherian domain.

$\widehat{M_{\mathfrak{p}}}$ is the completion of an R-module M at the prime ideal $\mathfrak{p}$ of R, where R is an integrally closed Noetherian domain.
$Z(G)$ is the centre of a group G.
$[g,h]$ is the commutator $ghg^{-1}h^{-1}$ of elements g,h in a group G.
$[G,A]$ is the subgroup of a group G generated by the commutators $[g,a]$ for $g \in G$ and $a \in A$, where A is a subgroup of G.
G' is the commutator subgroup, $[G,G]$, of a group G.
C_n is the cyclic group of order n for some $n \in \mathbb{Z}_{>0}$.
D_{2n} is the dihedral group of order $2n$ for some $n \in \mathbb{Z}_{>0}$.
$\mathrm{Aff}(q)$ is the affine group $\mathbb{F}_q \rtimes \mathbb{F}_q^{\times}$, where q is a prime power (defined in Example 3.6.6).

1.2 Fitting ideals

Let R be a commutative ring, let M_1 and M_2 be free R-modules of rank b and a, respectively, with $a \leq b$ and let $h\colon M_1 \to M_2$ be an R-module homomorphism. By choosing bases of the free R-modules M_1 and M_2, we may identify h with a $b \times a$ matrix. We define $S_a(h)$ to be the set of $a \times a$ submatrices of h.

Definition 1.2.1. Let R be a commutative ring, let M be a finitely presented R-module and let

$$R^b \xrightarrow{h} R^a \longrightarrow M \longrightarrow 0$$

be a presentation for M, for some $a, b \in \mathbb{Z}_{>0}$. (By writing the free R-modules as R^b and R^a we are implicitly including the choice of bases in the presentation h.) We define the *Fitting ideal* of M to be

$$\mathrm{Fit}_R(M) = \begin{cases} \langle \det(H) \mid H \in S_a(h) \rangle_R & \text{if } a \leq b, \\ 0 & \text{if } a > b. \end{cases}$$

By [Nor76, Theorem 3.1], $\mathrm{Fit}_R(M)$ is independent of the choice of presentation h. Thus $\mathrm{Fit}_R(M)$ is well-defined.

A key reason for the interest in Fitting ideals is the following result.

Theorem 1.2.2. *Let R be a commutative ring. If M is a finitely presented R-module then*

$$\mathrm{Fit}_R(M) \subset \mathrm{Ann}_R(M).$$

Proof. The proof given here is inspired by [Nic10, Theorem 4.2]. Let

$$R^b \xrightarrow{h} R^a \longrightarrow M \longrightarrow 0$$

be a presentation for M. If $a > b$, we note that

$$\mathrm{Fit}_R(M) = 0 \subset \mathrm{Ann}_R(M),$$

proving the result. Otherwise, when $a \leq b$, let $H \in S_a(h)$ and let $H^* \in M_{a\times a}(R)$ be the adjugate matrix of H. We note that multiplication by H^* yields a map $R^a \to R^a$ and that

$HH^* = \det(H)I_a$, where I_a is the $a \times a$ identity matrix. Therefore, there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} R^a & \xrightarrow{H} & R^a & \longrightarrow & \operatorname{coker}(H) & \longrightarrow & 0 \\ & \swarrow^{H^*} & \downarrow{\scriptstyle \det(H)} & & \downarrow{\scriptstyle \det(H)} & & \\ R^a & \xrightarrow{H} & R^a & \longrightarrow & \operatorname{coker}(H) & \longrightarrow & 0. \end{array}$$

This shows that multiplication by $\det(H)$ is the zero map on $\operatorname{coker}(H)$. Since $\operatorname{coker}(H)$ surjects onto M, we see that $\det(H) \in \operatorname{Ann}_R(M)$. As $H \in S_a(h)$ was arbitrary, we see that

$$\operatorname{Fit}_R(M) \subset \operatorname{Ann}_R(M). \qquad \square$$

The Fitting ideal satisfies certain useful properties. Following [Nic17b, Lemma 1.8], we now list some of these properties.

Lemma 1.2.3. *Let R be a commutative ring, and let M_1, M_2 and M_3 be finitely presented R-modules.*

(i) If there is a surjection $\pi\colon M_1 \to M_2$ then $\operatorname{Fit}_R(M_1) \subseteq \operatorname{Fit}_R(M_2)$.

(ii) If $M_2 = M_1 \oplus M_3$ then

$$\operatorname{Fit}_R(M_1)\operatorname{Fit}_R(M_3) = \operatorname{Fit}_R(M_2).$$

(iii) If $M_1 \to M_2 \to M_3 \to 0$ is an exact sequence then

$$\operatorname{Fit}_R(M_1)\operatorname{Fit}_R(M_3) \subseteq \operatorname{Fit}_R(M_2).$$

Proof. For a proof of part (i), let

$$R^b \xrightarrow{h} R^a \xrightarrow{\pi_1} M_1 \to 0$$

be a presentation of M_1. Then one may construct a finite presentation of M_2 given by

$$R^{b+b'} \xrightarrow{(h,*)} R^a \xrightarrow{\pi\circ\pi_1} M_2 \to 0,$$

where $(h, *)$ is the map h extended possibly with extra relations; this proves part (i). Part (ii) follows directly from [Nor76, Exercise 3.3]. Part (iii) follows from [Nor76, Exercise 3.2] on short exact sequences and part (i). $\square$

Example 1.2.4. Let R be a commutative ring. Let $I_1, \ldots, I_n$ be ideals of R. Then $\operatorname{Fit}_R(\bigoplus_{k=1}^n R/I_k) = \prod_{k=1}^n I_k$. This follows from [Nor76, Exercise 3.4].

1.3 Semisimple algebras

We recall the definition of semisimple rings and modules from [CR81].

Definition 1.3.1. Let A be a ring. A right A-module M is called *simple* if $M \neq 0$ and the only submodules of M are 0 and M.

Proposition 1.3.2. *Let M be a right A-module over an arbitrary ring A. The following statements are equivalent.*

(i) $M = \bigoplus_{i\in I} M_i$ *for some family,* $\{M_i\}_{i\in I}$*, of simple submodules of* M*.*

(ii) $M = \sum_{j\in J} M_j$ *for some family,* $\{M_j\}_{j\in J}$*, of simple submodules of* M*.*

(iii) For every submodule $M' \subset M$*, there exists a submodule* $M'' \subset M$ *such that*

$$M = M' \oplus M''.$$

Proof. A proof of this is given in [CR62, Theorem 15.3]. □

Definition 1.3.3. Let A be a ring. A right A-module M satisfying the equivalent conditions of Proposition 1.3.2 is called *semisimple*.

Proposition 1.3.4. *Let A be a ring. The following conditions on A are equivalent.*

(i) Every right A-module is semisimple.

(ii) Every finitely generated right A-module is semisimple.

(iii) The ring A viewed as a right A-module over itself is semisimple and is a direct sum $A = L_1 \oplus \cdots \oplus L_m$ of a finite number of minimal right ideals $\{L_1, \ldots, L_m\}$ of A.

Proof. A proof of this is given in [CR81, Proposition 3.15]. □

Definition 1.3.5. A ring A is called *semisimple* if A satisfies the equivalent conditions of Proposition 1.3.4.

Remark 1.3.6. This definition of a semisimple ring differs from that found in [Rei75, Section 6a] which defines a semisimple ring to be a ring A such that the Jacobson radical $\mathrm{rad}(A)$ of A is 0. If A is an Artinian ring then, by [CR81, Theorem 5.18], A is semisimple if and only if $\mathrm{rad}(A) = 0$. In fact, using Theorem 1.3.12 below, A is semisimple if and only if A is Artinian and $\mathrm{rad}(A) = 0$. Hence, semisimple rings (as defined here) are both Noetherian and Artinian.

Motivation for Definition 1.3.5 comes from group algebras and Theorem 1.3.8 below.

Definition 1.3.7. Let R be a ring and let G be a finite group. The group ring $R[G]$ is defined to be the free R-module

$$R[G] = \bigoplus_{g\in G} Rg$$

with multiplication given by

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h (gh),$$

for some $a_g, b_h \in R$.

Theorem 1.3.8 (Maschke's Theorem)**.** *Let F be a field and let G be a finite group. If either* $\mathrm{char}(F) = 0$ *or* $\mathrm{char}(F) \nmid |G|$ *then the group algebra $F[G]$ is a semisimple ring.*

Proof. A sketch proof is given in [CR81, Theorem 3.14]. □

Definition 1.3.9. A ring A is called *simple* if A has no proper non-zero two-sided ideals.

Definition 1.3.10. Let F be a field and let A be a F-algebra. We call A a *central simple F-algebra* if A is a simple ring, A is finite dimensional over F and $\mathfrak{Z}(A) = F$.

We now recall the definition of a homogeneous component of a semisimple module from [CR81, Definition 3.21].

Definition 1.3.11. Let M be a semisimple right A-module and let $\{M_i\}_{i\in I}$ be a set of representatives of the isomorphism classes of simple right A-submodules of M. For $i \in I$, let

$$H_i = \sum_{\substack{P\cong M_i \\ P\subset M_i}} P.$$

The submodules $\{H_i\}_{i\in I}$ are called the *homogeneous components* of M.

Theorem 1.3.12 (Wedderburn's Decomposition Theorem)**.** *If A is a semisimple ring, then the number of homogeneous components $\{A_i\}$ of A as a right A-module is finite and A is their direct sum:*

$$A = A_1 \oplus \cdots \oplus A_m.$$

Each homogeneous component A_i is a two-sided ideal in A and $A_iA_{i'} = 0$ if $i \neq i'$. Moreover, each A_i is a simple Artinian ring.

Proof. A proof of this is given in [CR81, Theorem 3.22]. □

Remark 1.3.13. By [CR81, Proposition 3.24], every simple Artinian ring is semisimple. Thus if $A = A_1 \times \cdots \times A_m$ where each A_i is a simple Artinian ring then A is semisimple. This shows that the definition of a semisimple ring is independent of taking right or left modules in the definition.

Definition 1.3.14. When A is a semisimple ring we will call the decomposition

$$A = A_1 \times \cdots \times A_m$$

into simple Artinian rings the *Wedderburn decomposition* of A.

1.4 Idempotents

In order to talk about the decomposition of a semisimple ring into components it is useful to introduce the concept of an idempotent.

Definition 1.4.1. Let A be a ring. An element $e \in A$ is called an *idempotent* in A if $e^2 = e$.

Example 1.4.2. If A is a ring then $0^2 = 0$ so 0 is an idempotent in A. If A has an identity element 1_A then $1_A^2 = 1_A$ and so 1_A is an idempotent in A.

Example 1.4.3. Let F be a field. Let $A = M_{2\times 2}(F)$. Then A is a semisimple F-algebra and the matrix $e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is an idempotent in A.

Definition 1.4.4. Let A be a ring. Non-zero idempotents e_1 and e_2 in A are called orthogonal if $e_1e_2 = 0$. A set $\{e_i\}$ of idempotents in A is called a set of orthogonal idempotents in A if the idempotents are pairwise orthogonal.

Definition 1.4.5. A idempotent e in A is called *primitive* if eA is a simple A-module. In other words, $e \neq 0$ and if $e = e' + e''$ for some idempotents e', e'' in A then either e' or e'' is 0.

Definition 1.4.6. Let A be a ring. A *central idempotent* in A is an idempotent e in A such that $e \in \mathfrak{Z}(A)$.

Example 1.4.7. Let A be a ring. We note that 0 and 1_A are central idempotents in A.

Example 1.4.8. Let F be a field of characteristic 0 and let G be a finite group. If H is a subgroup of G then $e_H := \frac{1}{|H|}\operatorname{Tr}_H$ (where $\operatorname{Tr}_H := \sum_{h\in H} h$) is an idempotent of $F[G]$ called the trace idempotent associated to H. If H is a normal subgroup of G then e_H is a central idempotent in $F[G]$.

Let G' be the commutator subgroup of G. Then $e_{G'}$ is the 'largest' central idempotent of $F[G]$ such that $e_{G'}F[G]$ is a commutative ring. More precisely, if e is a central idempotent of $F[G]$ such that $eF[G]$ is a commutative ring then $ee_{G'} = e$. This follows because G' is the minimal normal subgroup of G such that G/G' is commutative. We will generalise this concept to other semisimple algebras in Definition 3.5.1.

Definition 1.4.9. A central idempotent e in A is called *primitive* if $e \neq 0$ and $e = e' + e''$ (for some central idempotents $e', e'' \in A$) implies either $e' = 0$ or $e'' = 0$.

Example 1.4.10. Let F be a field of characteristic 0 and let G be a finite group. Recall that $\operatorname{Irr}_F(G)$ is the set of F-valued irreducible characters of G. If $\chi \in \operatorname{Irr}_F(G)$ then $e_\chi := \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$ is a primitive central idempotent of $F[G]$ called the idempotent associated to χ.

Remark 1.4.11. Let A be a semisimple ring and let $A = A_1 \times \cdots \times A_m$ be the Wedderburn decomposition of A. Then $e_i = 1_{A_i}$ is a primitive central idempotent in A. Conversely, if e is a primitive central idempotent in A then eA is a simple ring contained in A so $eA = A_i$ and $e = e_i$ for some $i \in \{1, \ldots, m\}$. Furthermore, the set $\{e_1, \ldots, e_m\}$ is a set of orthogonal idempotents in A. We also see that $e_1, \ldots, e_m$ are the primitive (central) idempotents in $\mathfrak{Z}(A)$ and we see that $\mathfrak{Z}(e_iA) = e_i\mathfrak{Z}(A)$.

Let e be a central idempotent in A. We see that $e = \sum_{i=0}^{m} ee_i = \sum_{i\in\mathcal{I}} e_i$ for some subset $\mathcal{I}$ of $\{1, \ldots, m\}$. Thus

$$\mathfrak{Z}(eA) = \prod_{i\in\mathcal{I}} \mathfrak{Z}(e_iA) = \prod_{i\in\mathcal{I}} e_i\mathfrak{Z}(A) = e\mathfrak{Z}(A).$$

1.5 Tensor products

Let A be a ring and let M be a right A-module and let N be a left module. Recall the definition of the tensor product $M \otimes_A N$ from [CR81, Section 2B].

Lemma 1.5.1. *Let A be a ring. Let M, M_1 and M_2 be right A-modules and let N, N_1 and N_2 be left A-modules. Then*

(i) if $f\colon M_1 \to M_2$ and $g\colon N_1 \to N_2$ are A-module homomorphism then there is a unique group homomorphism $f \otimes g\colon M_1 \otimes_A N_1 \to M_2 \otimes_A N_2$ such that

$$f \otimes g(m_1 \otimes m_2) = f(m_1) \otimes g(m_2)$$

for $m_1 \in M_1$ and $m_2 \in M_2$,

(ii) there are canonical isomorphisms $A \otimes_A N \cong N$ and $M \otimes_A A \cong M$, and

(iii) there are canonical isomorphisms

$$(M_1 \oplus M_2) \otimes_A N \cong (M_1 \otimes_A N) \oplus (M_2 \otimes_A N)$$

and

$$M \otimes_A (N_1 \oplus N_2) \cong (M \otimes_A N_1) \oplus (M \otimes_A N_2).$$

Proof. For proofs of (i), (ii) and (iii) see [CR62, Theorems 12.10, 12.12 and 12.14], respectively. □

Lemma 1.5.2. *Let A and B be rings. Let L be a right A-module, let M be an (A, B)-bimodule and let N be a left B-module. Then there is an isomorphism of abelian groups*

$$(L \otimes_A M) \otimes_B N \cong L \otimes_A (M \otimes_B N),$$

given by the formula $(l \otimes m) \otimes n \mapsto l \otimes (m \otimes n)$ for $l \in L$, $m \in M$ and $n \in N$.

Proof. A proof of this is given in [CR62, Theorem 12.15]. □

Definition 1.5.3. Let R be a commutative ring and let A and B be R-algebras. Then $A \otimes_R B$ is an R-algebra with multiplication given by

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2).$$

Example 1.5.4. Let R be a commutative ring, and let B be an R-algebra. Then there is an R-algebra isomorphism

$$M_{n\times n}(R) \otimes_R B \xrightarrow{\cong} M_{n\times n}(B),$$

given on the R-spanning set $\{(r_{ij})_{1\leq i,j\leq n} \otimes b \mid r_{ij} \in R, b \in B\}$ by

$$(r_{ij})_{1\leq i,j\leq n} \otimes b \longmapsto (r_{ij}b)_{1\leq i,j\leq n}.$$

By Lemma 1.5.1(iii) the map is a bijection and it is easy to directly check that this map is an R-algebra homomorphism.

Example 1.5.5. Let R be a commutative ring, let S be a commutative R-algebra and let G be a finite group. Then there is an R-algebra isomorphism

$$S \otimes_R R[G] \xrightarrow{\cong} S[G],$$

given on the R-spanning set $\{s \otimes g \mid s \in S, g \in G\}$ of $S \otimes_R R[G]$ by

$$s \otimes g \longmapsto sg.$$

By Lemma 1.5.1(iii) the map is a bijection and it is easy to directly check that this map is an R-algebra homomorphism.

Example 1.5.6. Let R be a commutative ring and let G and H be finite groups. Then there is an R-algebra isomorphism

$$R[G] \otimes_R R[H] \xrightarrow{\cong} R[G \times H],$$

given on the R-basis $\{g \otimes h \mid g \in G, h \in H\}$ of $R[G] \otimes_R R[H]$ by

$$g \otimes h \longmapsto (g, h).$$

By Lemma 1.5.1(iii) the map is a bijection and it is easy to directly check that this map is an R-algebra homomorphism.

1.6 Reduced norms

The start of this section will closely follow [CR81, Section 7D], although we will cite [Rei75] for proofs. Let F be a field and let V be a finite dimensional F-vector space. Some useful tools in the study of linear maps are the concepts of the characteristic polynomial and determinant. For a linear map $H \in \mathrm{End}_F(V)$ we write $\mathrm{ch}_F(H)$ for the characteristic polynomial of H and $\det_F(H)$ for the determinant of H. We will use the same notation for the characteristic polynomial and determinant of a matrix in $M_{n\times n}(F)$.

Let A be a finite dimensional F-algebra and let $H \in A$. We obtain a linear map

$$H_L \colon A \longrightarrow A$$

given by left multiplication by H. We will write

$$\mathrm{ch}_{A/F}(H) = \mathrm{ch}_F(H_L) \quad \text{and} \quad \mathrm{N}_{A/F}(H) = \det_F(H_L).$$

Note that the subscript of $\mathrm{ch}_{A/F}$ is important to distinguish from the usual characteristic polynomial when A is a matrix ring over F. We note that $\mathrm{N}_{A/F}(-H)$ is the constant coefficient of $\mathrm{ch}_{A/F}(H)$.

Consider (for now) the central simple F-algebra $A = M_{n\times n}(F)$. An element $H \in A$ is already a matrix so we may take the determinant and characteristic polynomial of H directly, without the extra work of considering H as a linear map $A \to A$. With this

notation, by [Rei75, Theorem 9.5], we see that

$$\mathrm{ch}_{A/F}(H) = (\mathrm{ch}_F(H))^n$$

and

$$\mathrm{N}_{A/F}(H) = (\det_F(H))^n.$$

This shows that ch_F and $\det_F$ are in some sense 'finer versions' of $\mathrm{N}_{A/F}$ and $\mathrm{ch}_{A/F}$, respectively. We define the reduced characteristic polynomial of $H \in A$ to be

$$\mathrm{rch}_{A/F}(H) = \mathrm{ch}_F(H)$$

and the reduced norm to be

$$\mathrm{nr}_{A/F}(H) = \det_F(H).$$

Remark 1.6.1. We note that $\mathrm{nr}_{A/F}(-H)$ is the constant coefficient of the reduced characteristic polynomial of H. In other words

$$\mathrm{rch}_{A/F}(H)(X) = X^n + \cdots + (-1)^n \mathrm{nr}_{A/F}(H).$$

More generally, let A be any central simple F-algebra. By [Rei75, Theorems 7.4 and 7.15] there is a separable field extension E of F such that there is an E-algebra isomorphism $f\colon A \otimes_F E \to M_{n\times n}(E)$ for some $n \in \mathbb{Z}_{>0}$. We call E a *splitting field* for A over F (we will generalise this notion further in Definition 1.8.7). The reduced characteristic polynomial is defined to be

$$\mathrm{rch}_{A/F}(H) = \mathrm{ch}_E(f(H \otimes_F 1_E))$$

and the reduced norm is defined to be

$$\mathrm{nr}_{A/F}(H) = \det_E(f(H \otimes_F 1_E)).$$

The definitions of the reduced characteristic polynomial and reduced norm may appear to depend on the choice of E-algebra isomorphism $f\colon A \otimes_F E \to M_{n\times n}(E)$. However, if $h\colon A \otimes_F E \to M_{n\times n}(E)$ is any other E-algebra isomorphism, then fh^{-1} is an E-algebra automorphism of $M_{n\times n}(E)$ and thus is inner by the Skolem-Noether Theorem (see [Rei75, Corollary 7.23]). In particular, there exists a matrix $T \in \mathrm{GL}_n(E)$ such that $f(H \otimes_F 1_E) = Th(H \otimes_F 1_E)T^{-1}$. Thus the characteristic polynomials of $f(H \otimes_F 1_E)$ and $h(H \otimes_F 1_E)$ are the same; similarly for the determinants. Therefore the reduced characteristic polynomial and reduced norm do not depend on the choice of E-algebra isomorphism $A \otimes_F E \to M_{n\times n}(E)$.

By [Rei75, Theorem 9.3], $\mathrm{rch}(H)$ lies in $F[X]$ and is independent of the choice of splitting field E. Using Remark 1.6.1, we see that

$$\mathrm{rch}_{A/F}(H)(X) = X^n + \cdots + (-1)^n \mathrm{nr}_{A/F}(H).$$

Hence $\mathrm{nr}_{A/F}(H)$ lies in F and is independent of the choice of splitting field E.

When defining the reduced characteristic polynomial and reduced norm for an arbitrary (not necessarily central) simple F-algebra A we diverge from the definition given in [CR81, Section 7D] or [Rei75, Definition 9.13]. The definitions of the reduced characteristic polynomial and reduced norm given by Curtis and Reiner produce elements of $F[X]$ and F, respectively, whereas we are more interested in producing elements of $\mathfrak{Z}(A)[X]$ and $\mathfrak{Z}(A)$. Suppose that A is a simple F-algebra. We note that $\mathfrak{Z}(A)$ is a finite field extension of F and A is a central simple $\mathfrak{Z}(A)$-algebra. Thus we can and do define the reduced characteristic polynomial and reduced norm of an element $H \in A$ as follows

$$\mathrm{rch}_A(H) = \mathrm{rch}_{A/\mathfrak{Z}(A)}(H) \quad \text{and} \quad \mathrm{nr}_A(H) = \mathrm{nr}_{A/\mathfrak{Z}(A)}(H).$$

We will often drop the A in the notation when it is clear from context.

We are now in a position to define the reduced characteristic polynomial and reduced norm for elements of a finite dimensional semisimple F-algebra A. Since A is finite dimensional semisimple, it may be written as a product

$$A = \prod_{i=1}^{t} A_i,$$

where the A_i are simple F-algebras. Hence any element $H \in A$ can be viewed as a tuple $H = (H_1, \ldots, H_t)$, where $H_i \in A_i$. We defined the reduced characteristic polynomial and reduced norm componentwise,

$$\mathrm{rch}_A(H) = (\mathrm{rch}_{A_1}(H_1), \ldots, \mathrm{rch}_{A_t}(H_t))$$

and

$$\mathrm{nr}_A(H) = (\mathrm{nr}_{A_1}(H_1), \ldots, \mathrm{nr}_{A_t}(H_t)).$$

Again we will often drop the A in the notation when it is clear from context.

Remark 1.6.2. Using Remark 1.6.1, we see that $\mathrm{nr}_A(-H)$ is the constant coefficient of the reduced characteristic polynomial of H.

It is important to note that the reduced characteristic polynomial of an element of A need not be monic, as illustrated by the following example.

Example 1.6.3. Let F be a field and consider the F-algebra $F \times M_{2\times 2}(F)$. The reduced characteristic polynomial of $0 \in F \times M_{2\times 2}$ is $e_2X^2 + e_1X$, where e_1 is the central idempotent corresponding to the F component and e_2 is the central idempotent corresponding to the $M_{2\times 2}(F)$ component.

Remark 1.6.4. Since the definition of the reduced norm of elements of a finite dimensional semisimple algebra is built from the definition of the determinant for matrices over a field, to prove properties of the reduced norm it often suffices to prove them for determinants. In a similar way, to prove properties of the reduced characteristic polynomial of a finite dimensional semisimple algebra it often suffices to prove them for the characteristic polynomial of matrices over a field.

Remark 1.6.5. The reduced characteristic polynomial and reduced norm of a finite dimensional semisimple algebra do not depend on the choices of splitting fields for the simple components because they do not depend on the choice of splitting field in the central simple algebra case.

Lemma 1.6.6. *Let F be a field and let A be a finite dimensional semisimple F-algebra. If $H \in A$ then*

$$\mathrm{rch}(H)(X) = \mathrm{nr}(1_A \otimes_F X - H \otimes_F 1_{F(X)}),$$

where the reduced norm is considered in the finite dimensional semisimple $F(X)$-algebra $A \otimes_F F(X)$ and both sides of the equality are considered as polynomials over X.

Proof. We give a proof in the case that A is a matrix ring over a field. From this one can deduce the more general case by unravelling the definitions; this is a long but straightforward exercise.

Let E be a field and let $n \in \mathbb{Z}_{>0}$. If $H \in M_{n\times n}(E)$ then the definition of the characteristic polynomial of the matrix H is

$$\begin{aligned}\mathrm{ch}_F(H) &= (-1)^n \det_{F(X)}(H - XI_n)\\ &= \det_{F(X)}(-I_n)\det_{F(X)}(H - XI_n)\\ &= \det_{F(X)}(XI_n - H),\end{aligned}$$

where I_n in the $n \times n$ identity matrix in $M_{n\times n}(E)$. □

Lemma 1.6.6 allows us to deduce properties of the reduced characteristic polynomial from properties of the reduced norm.

Lemma 1.6.7. *Let F be a field and let A, B be finite dimensional semisimple F-algebras. If $\varphi\colon A \to B$ is an F-algebra isomorphism then for $H \in A$ we have*

$$\mathrm{rch}_B(\varphi(H)) = \varphi(\mathrm{rch}_A(H))$$

and

$$\mathrm{nr}_B(\varphi(H)) = \varphi(\mathrm{nr}_A(H)),$$

where φ acts on the coefficients of the reduced characteristic polynomial.

Proof. Since the reduced norm is defined componentwise, Lemma 1.6.6 shows that the proof may reduced to the case that A and B are simple F-algebras. Let $\varphi\colon A \to B$ be an isomorphism of simple F-algebras. Let E be a field extension of $\mathfrak{Z}(A)$ that is a splitting field for A over $\mathfrak{Z}(A)$. Viewing E as a field extension of $\mathfrak{Z}(B)$ via $\varphi|_{\mathfrak{Z}(A)}$, the isomorphism φ extends to an E-algebra isomorphism

$$\varphi_E\colon A \otimes_{\mathfrak{Z}(A)} E \longrightarrow B \otimes_{\mathfrak{Z}(B)} E.$$

In particular, E may be viewed as a splitting field for B over $\mathfrak{Z}(B)$. Let $H \in A$. Then $\mathrm{nr}_A(H) = \det_E(H \otimes 1_E)$. Since the reduced norm does not depend on the choice of E-algebra isomorphism $A \otimes_{\mathfrak{Z}(A)} E \to M_{n\times n}(E)$, by applying φ we see that

$$\varphi(\mathrm{nr}_A(H)) = \varphi_E(\det_E(H \otimes 1_E)) = \det_E(\varphi_E(H \otimes 1_E)) = \mathrm{nr}_B(\varphi(H)),$$

where the second equality follows because φ_E is an E-algebra homomorphism. □

1.7 Generalised adjoints

Definition 1.7.1. Let F be a field and let A be a finite dimensional semisimple F-algebra. For $H \in A$ write

$$\mathrm{rch}_A(H)(X) = \sum_{j=0}^{N} a_j X^j$$

and define the *generalised adjoint* of H to be

$$H^* = -\,\mathrm{nr}_A(-1_A) \sum_{j=1}^{N} a_j H^{j-1} \in A.$$

Lemma 1.7.2. *Let F be a field and let $A = M_{n\times n}(F)$ be a central simple F-algebra. If $H \in M_{n\times n}(F)$ then the generalised adjoint of H in A is precisely the adjugate of the matrix H in A.*

Proof. A proof for this may be found in [Gan98, Section IV.4.3]. □

The reduced characteristic polynomial of H has constant term $\mathrm{nr}_A(-H)$. This observation leads to the following result.

Lemma 1.7.3. *Let F be a field and let A be a finite dimensional semisimple F-algebra. If $H \in A$ then*

$$HH^* = H^*H = \mathrm{nr}_A(H)1_A.$$

Proof. Suppose that A is a matrix ring over a field. If $H \in A$ then

$$HH^* - \mathrm{nr}_A(H)1_A = H^*H - \mathrm{nr}_A(H)1_A = -\,\mathrm{nr}_A(-1_A)\,\mathrm{rch}_A(H)(H) = 0,$$

where the last equality follows from the Cayley-Hamilton Theorem (see [Gan98, Theorem IV.2]). This concludes the proof in this case. The more general case follows from this by unravelling the definitions; this is a long but straightforward exercise. □

Remark 1.7.4. By Lemma 1.7.3, if $H \in \mathrm{GL}_n(A)$ then $H^* = \mathrm{nr}(H)H^{-1}$.

Remark 1.7.5. We may write the finite dimensional semisimple algebra A as a product of simple F-algebras $A = \prod_{i=1}^{t} A_i$. Write $H = (H_1, \ldots, H_t)$ where $H_i \in A_i$ and write $\mathrm{rch}_{A_i}(H_i) = \sum_{j=0}^{m_i} \alpha_{i,j} X^j$, where $m_i^2 = \deg_{\mathfrak{Z}(A_i)}(A_i)$. Using that the definition of the reduced characteristic polynomial is built up from the definition on simple F-algebras, we see that

$$H^* = (H_1^*, \ldots, H_t^*), \quad \text{where} \quad H_i^* = (-1)^{m_i+1} \sum_{j=1}^{m_i} \alpha_{i,j} H_i^{j-1}.$$

Here we have used that $\mathrm{nr}_A(-1_A) = ((-1_{A_1})^{m_1}, \ldots, (-1_{A_t})^{m_t})$. Therefore the definition of generalised adjoint given here agrees with the definition in [JN13, Section 3.6].

Example 1.7.6. Let F be a field. We recall the example of an F-algebra $F \times M_{2\times 2}(F)$ from Remark 1.6.3, in which we noted that

$$\mathrm{rch}(0) = e_2X^2 + e_1X,$$

where e_1 is the central idempotent corresponding to the F component and e_2 is the central idempotent corresponding to the $M_{2\times 2}(F)$ component. In this case we note that the generalised adjoint of 0 in $F \times M_{2\times 2}(F)$ is e_1.

Remark 1.7.7. Using an idea from the proof of [JN13, Proposition 4.4], we shall now show that Example 1.7.6 is a special case of a more general result. Let F be a field and let A be a finite dimensional semisimple F-algebra. Using Theorem 1.3.12, write $A = \prod_{i=1}^{t} A_i$ where the A_i are simple F-algebras. Using [Rei75, Theorem 7.4], there are F-algebra isomorphisms $A_i \cong M_{n_i\times n_i}(D_i)$, where D_i is a division ring over F with Schur index s_i. Let $H = 0 \in A$. We may write $H = (H_1, \ldots, H_t)$, where $H_i = 0 \in A_i$. We see that the reduced characteristic polynomial of H_i is $f_i(X) = X^{n_is_i}$. Hence $H_i^* = h_i(0)$ where $h_i(X) = X^{n_is_i-1}$. In other words,

$$H_i^* = \begin{cases} 1_{A_i} & \text{if } n_is_i = 1, \\ 0_{A_i} & \text{otherwise.} \end{cases}$$

We observe that the ring A_i is commutative if and only if $n_is_i = 1$. Therefore $0^* = H^*$ is the 'largest' central idempotent e of A such that eA is commutative. We will make this notion more precise in Definition 3.5.1.

Theorem 1.7.8. *Let F be a field and let A be a finite dimensional semisimple F-algebra. Then the following results hold.*

(i) If B is a finite dimensional semisimple F-algebra and $\varphi\colon A \to B$ is an F-algebra isomorphism then

$$(\varphi(H))^* = \varphi(H^*).$$

(ii) Suppose that B is a commutative finite dimensional semisimple E-algebra where E is a field extension of F such that $A \otimes_F B$ is finite dimensional semisimple E-algebra. If $H \in A$ then, in $A \otimes_F B$, we have

$$(H \otimes 1_B)^* = H^* \otimes 1_B.$$

(iii) If $H_1 \in M_{n\times n}(A)$ and $H_2 \in M_{m\times m}(A)$ then

$$\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}^* = \begin{pmatrix} \mathrm{nr}(H_2)H_1^* & 0 \\ 0 & \mathrm{nr}(H_1)H_2^* \end{pmatrix} \in M_{(n+m)\times(n+m)}(A).$$

(iv) If $H_1, H_2 \in A$ then $(H_1H_2)^* = H_2^*H_1^*$.

Remark 1.7.9. The hypothesis that $A \otimes_F B$ is finite dimensional semisimple E-algebra in part (ii) is due to us only having defined the generalised adjoint for finite dimensional semisimple E-algebras.

Proof of Theorem 1.7.8. Using Lemma 1.6.7 (which tells us that the reduced characteristic polynomial is preserved by the isomorphism φ) and the definition of the generalised adjoint (Definition 1.7.1), we see that (i) holds.

We will give a proof of (ii), (iii) and (iv) in the case that A is a matrix ring over a field; in this setting, by Lemma 1.7.2, the generalised adjoint is the same as the adjugate matrix. These properties are well known for adjugates of matrices over a field and the proofs are routine (though we will provide a proof below for the convenience of the reader). From this one can deduce the more general case by unravelling the definitions; this is a long but straightforward exercise.

Let $H \in M_{n\times n}(F)$ for some $n \in \mathbb{Z}_{>0}$. It is clear that the matrix of cofactors of the matrix H is the same as the matrix of cofactors of $H \otimes 1_B$ viewed as a matrix in $M_{n\times n}(F) \otimes_F B \cong M_{n\times n}(B)$. Therefore, using Lemma 1.7.2 and (i) we see that

$$H^* \otimes 1_B = (H \otimes 1_B)^*$$

and so (ii) holds.

Showing that (iii) holds may be done directly; however here we will provide a more topological proof. The proofs of (iii) and (iv) given here are inspired by the topological proof of the Cayley-Hamilton Theorem.

Note that, by (ii), it suffices to show (iii) and (iv) when F is an algebraically closed field. For $n \in \mathbb{Z}_{>0}$, we may identify $M_{n\times n}(F)$ with the affine variety $\mathbb{A}_F^{n^2}$ by sending the (i,j)-entry of a matrix in $M_{n\times n}(F)$ to the $(i-1)n+j$-coordinate of $\mathbb{A}_F^{n^2}$. By [Har77, Example 1.4.1], affine space over an algebraically closed field is irreducible in the topological sense (that is, non-empty open subsets are dense). Let I be the set of invertible matrices in $M_{n\times n}(F)$. We see that I is the preimage of the open set $F \setminus \{0\}$ under the determinant map (which is continuous because it is a polynomial map in the coefficients of the matrix) and so we see that I is a open subset of $M_{n\times n}(F)$. We also note that I is non-empty so it is a dense subset of $M_{n\times n}(F)$.

Let $n_1, n_2 \in \mathbb{Z}_{>0}$. Let

$$\varphi\colon M_{n_1\times n_1}(F) \times M_{n_2\times n_2}(F) \to M_{(n_1+n_2)\times(n_1+n_2)}(F)$$

be the map given by

$$\varphi(H_1, H_2) = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}^* - \begin{pmatrix} \det(H_2)H_1^* & 0 \\ 0 & \det(H_1)H_2^* \end{pmatrix}$$

for $H_1 \in M_{n_1\times n_1}(F)$ and $H_2 \in M_{n_2\times n_2}(F)$. Then φ is a polynomial map in the entries of the matrices H_1 and H_2 and so (after identifying the matrix rings with affine varieties) φ is a continuous map. Let I_i be the set of invertible elements in $M_{n_i\times n_i}(F)$ for $i = 1, 2$. For $H_1 \in I_1$ and $H_2 \in I_2$, we see that $\left(\begin{smallmatrix} H_1 & 0 \\ 0 & H_2 \end{smallmatrix}\right) \in M_{(n_1+n_2)\times(n_1+n_2)}(F)$ is an invertible matrix

and so

$$\begin{aligned}\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}^* &= \det(H_1)\det(H_2)\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} \det(H_1)\det(H_2)H_1^{-1} & 0 \\ 0 & \det(H_1)\det(H_2)H_2^{-1} \end{pmatrix} \\ &= \begin{pmatrix} \det(H_2)H_1^* & 0 \\ 0 & \det(H_1)H_2^* \end{pmatrix}.\end{aligned}$$

Therefore φ is a continuous map which is the zero map on the dense subset $I_1 \times I_2$ of $M_{n_1\times n_1}(F) \times M_{n_2\times n_2}(F)$. Hence φ is the zero map and so (iii) holds.

Let

$$\varphi\colon M_{n\times n}(F) \times M_{n\times n}(F) \to M_{n\times n}(F)$$

be the map given by $\varphi(H_1, H_2) = (H_1H_2)^* - H_2^*H_1^*$. Then φ is a polynomial map in the entries of the matrices H_1 and H_2 and so (after identifying the matrix rings with affine varieties) φ is a continuous map. Let I be the set of invertible matrices in $M_{n\times n}(F)$. For $H_1, H_2 \in I$, we have

$$\begin{aligned}(H_1H_2)^* &= \det(H_1H_2)(H_1H_2)^{-1} \\ &= \det(H_2)H_2^{-1}\det(H_1)H_1^{-1} \\ &= H_2^*H_1^*,\end{aligned}$$

where the second equality follows because the determinant is multiplicative and has image in F. Therefore φ is a continuous map which is the zero map on the dense subset $I \times I$ of $M_{n\times n}(F) \times M_{n\times n}(F)$. Hence φ is the zero map and so (iv) holds. □

1.8 Separable algebras

Maschke's Theorem (Theorem 1.3.8) can be rephrased as saying that if G is a finite group, F is a field and either $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) \nmid |G|$, then for every field extension E of F the group algebra $E[G] \cong E \otimes_F F[G]$ is a semisimple E-algebra. This leads us to the following theorem/definition.

Theorem 1.8.1. *Let F be a field and let A be a finite dimensional F-algebra. Then the following statements are equivalent.*

(i) The ring $A \otimes_F E$ is a semisimple E-algebra for every field extension E of F (including F itself).

(ii) There exists a finite separable field extension E of F such that $A \otimes_F E$ is a direct product of full matrix algebras over E.

(iii) The ring A is a semisimple F-algebra such that the centre of each simple component of A is a separable field extension of F.

Proof. A proof of this is given in [Rei75, Theorem 7.18] (note that (iii) is given as the definition of a separable algebra in this reference). Another proof is given in [CR81,

Lemmas 7.2 and 7.3] (note that (i) is given as the definition of a separable algebra in this reference). □

Definition 1.8.2. Let F be a field. An F-algebra A is called *separable* if A is a finite dimensional F-algebra and A satisfies the equivalent conditions of Theorem 1.8.1.

Remark 1.8.3. This definition of a separable F-algebra is equivalent to the definitions given in [Rei75, Section 7c] and [CR81, Definition 7.1].

Example 1.8.4. Let F be a field and let G be a finite group. If the characteristic of F is zero or does not divide the order of G then Maschke's Theorem (Theorem 1.3.8) shows that $F[G]$ is a separable F-algebra.

Example 1.8.5. If F is a field of characteristic 0 then, by Wedderburn's Decomposition Theorem (Theorem 1.3.12) and Theorem 1.8.1(ii), every finite dimensional semisimple F-algebra is separable.

Example 1.8.6. Let F be a field and let A be a finite dimensional central simple F-algebra. By [Rei75, Theorems 7.4 and 7.15], there is a finite separable field extension E of F such that $A \otimes_F E$ is isomorphic to a matrix ring over E (this was noted after Remark 1.6.1, where we called E a splitting field for A). In particular, this shows that Theorem 1.8.1(ii) holds. Hence finite dimensional central simple algebras are separable.

For general finite dimensional separable algebras splitting fields are defined in a slightly different way.

Definition 1.8.7. Let F be a field and let A be a separable F-algebra. As in [CR81, Definition 7.12] a *splitting field* of A over F is a field extension E of F such that every simple $A \otimes_F E$-module is absolutely simple. (An $A \otimes_F E$-module M is absolutely simple if $M \otimes_E K$ is a simple $A \otimes_F K$-module for every field extension K of E.)

Remark 1.8.8. Let F be a field and let A be a separable F-algebra. By [CR81, Theorems 3.34 and 3.43], E is a splitting field for A over F if and only if $A \otimes_F E$ is a direct product of full matrix algebras over E. In particular, by Theorem 1.8.1(ii) a finite dimensional F-algebra A is separable if and only if there exists a finite separable field extension E of F such that E is a splitting field for A over F. This also shows that, in the case of central simple algebras, Definition 1.8.7 agrees the definition of splitting fields given in Section 1.6.

Remark 1.8.9. Let F be a field and let A be a separable F-algebra. Remark 1.8.8 shows that a splitting field for a separable F-algebra A is (in some sense) a 'simultaneous splitting field' for all of the homogeneous components of A. To be more precise, let A be a separable F-algebra and let E be a splitting field for A over F. Let $A = \prod_{i=1}^{m} A_i$ be the Wedderburn decomposition of A into simple F-algebras. Then $A \otimes_F E = \prod_{i=1}^{m} (A_i \otimes_F E)$. By [CR81, Corollary 7.6], $L_i := \mathfrak{Z}(A_i)$ is a finite separable field extension of F. Since A_i, L_i and E are (F, L_i)-bimodules, Lemma 1.5.2 shows that there exists an F-algebra isomorphism

$$A_i \otimes_F E \cong A_i \otimes_{L_i} (L_i \otimes_F E).$$

By [Rei75, Theorem 7.16], we see that $L_i \otimes_F E$ is a product of fields. Therefore, using [Rei75, Theorem 7.6] and considering the homogeneous components of $L_i \otimes_F E$, we see that $A_i \otimes_F E$ is a semisimple algebra with centre $L_i \otimes_F E$. Moreover, since E is a splitting field for A, we see that $A_i \otimes_F E$ is a product of matrix rings over E. Therefore $L_i \otimes_F E$ is isomorphic to a finite direct product of copies of E. Hence the field L_i can be viewed as a subfield of E and $A_i \otimes_{L_i} E$ is isomorphic to a matrix ring over E (in other words, E is a splitting field for the central simple L_i-algebra A_i).

Remark 1.8.10. Let F be a field and let A be a separable F-algebra. Computing the reduced characteristic polynomial and reduced norm in A is done over the simple components of A_i. In light of Remark 1.8.9, if E is a splitting field for A then E is also a splitting field for each simple component A_i of A. It would be convenient if computing the reduced characteristic polynomial and reduced norm could be done over $A \otimes_F E$ rather than needing to consider the centres of each simple component. This is indeed the case by Remark 1.8.9 together with the following lemma.

Lemma 1.8.11. *Let F be a field and let A be a separable simple F-algebra with centre L. Let E be a splitting field for A over F. If $H \in A$ then in $A \otimes_F E$ we have*

$$\mathrm{rch}(H) \otimes 1_E = \mathrm{rch}(H \otimes 1_E)$$

and

$$\mathrm{nr}(H) \otimes 1_E = \mathrm{nr}(H \otimes 1_E).$$

Proof. We note that, using the argument in Remark 1.8.9, there is an F-algebra isomorphisms

$$A \otimes_F E \cong M_{n\times n}(L \otimes_F E),$$

for some $n \in \mathbb{Z}_{>0}$. Furthermore, by Lemma 1.5.2, there are F-algebra isomorphisms

$$A \otimes_F E \cong (L \otimes_F A) \otimes_L E \cong L \otimes_F (A \otimes_L E).$$

Hence we see that there is a commutative diagram

$$\begin{array}{ccccc}
A & & \xrightarrow{\quad\mathrm{nr}_A\quad} & & \mathfrak{Z}(A) \\
\downarrow{\scriptstyle -\otimes 1_E} & & & & \downarrow{\scriptstyle -\otimes_L 1_E} \\
A \otimes_L E & \xrightarrow{\cong} & M_{n\times n}(E) & \xrightarrow{\det_E} & E \\
\downarrow{\scriptstyle 1_L\otimes -} & & \downarrow{\scriptstyle 1_L\otimes -} & & \downarrow{\scriptstyle 1_L\otimes_F -} \\
A \otimes_F E & \xrightarrow{\cong} & M_{n\times n}(L \otimes_F E) & \xrightarrow{\det_{L\otimes_F E}} & L \otimes_F E.
\end{array} \tag{1.1}$$

Let H be an element of A. The element $\mathrm{nr}_A(H) \otimes 1_E$ corresponds to computing the determinant in $A \otimes_L E$ and then embedding into $L \otimes_F E$ and the element $\mathrm{nr}_{A\otimes_F E}(H \otimes 1_E)$ corresponds to computing the determinant in $A \otimes_F E$ directly. We note that because the reduced norm is invariant under F-algebra isomorphisms (by Lemma 1.6.7), it does not

matter whether we take determinant over $L \otimes_F E$ or break into simple algebras and then take determinants over E. Therefore, the commutative diagram (1.1) shows that

$$\mathrm{nr}(H) \otimes 1_E = \mathrm{nr}(H \otimes 1_E).$$

The result for reduced characteristic polynomials follows from the result on reduced norms and Lemma 1.6.6 (which tells us that the reduced characteristic polynomial of an element of A can be seen as the reduced norm of an element in $A \otimes_F F(X)$). □

1.9 Lattices and orders

This section follows [Rei75, Section 8].

Definition 1.9.1. Let R be a Noetherian integral domain with field of fractions F and let V be a finite dimensional F-vector space. A *full R-lattice* in V is a finitely generated R-submodule M of V such that

$$FM := \left\{ \sum_{i=1}^{n} \alpha_i m_i \;\middle|\; n \in \mathbb{Z}_{>0}, \alpha_i \in F, m_i \in M \right\} = V.$$

Remark 1.9.2. Let R be a Noetherian integral domain with field of fractions F. Every finite dimensional F-vector space V contains a full R-lattice. In particular, if $v_1, \ldots, v_d$ is an F-basis for V then $M = \sum_{i=1}^{d} Rv_i$ is a full R-lattice in V.

Example 1.9.3. Let R be a Noetherian integral domain with field of fractions F and let G be a finite group. Then $R[G]$ is a full R-lattice in $F[G]$.

Lattices over a Dedekind domain satisfy the following local-global principle.

Theorem 1.9.4. *Let R be a Dedekind domain with field of fractions F, let V be a finite dimensional F-vector space and let M be an R-lattice in V. View M and its localisations $\{M_\mathfrak{p}\}$ as embedded in the F-vector space V. Then*

$$M = \bigcap_{\mathfrak{p}} M_\mathfrak{p},$$

where $\mathfrak{p}$ ranges over all maximal ideals of R.

Proof. For a proof see [Rei75, Theorem 4.21]. □

Definition 1.9.5. Let R be a Noetherian integral domain with field of fractions F and let A be finite dimensional F-algebra. An *R-order* in A is a subring Λ of A (with the same identity element) that is also a full R-lattice in A.

Remark 1.9.6. Let R be a Noetherian integral domain with field of fractions F. We note that R-orders are Noetherian rings as they are finitely generated R-modules over the Noetherian ring R.

Examples 1.9.7. Let R be a Noetherian integral domain with field of fractions F.

(i) The R-algebra $\Lambda = M_{n\times n}(R)$ is an R-order in $M_{n\times n}(F)$.

(ii) If R is a Dedekind domain and L is a finite separable extension of F then the integral closure of R in L is an R-order in L.
(iii) If G is a finite group then $R[G]$ is an R-order in $F[G]$.

Lemma 1.9.8. *Let R be a Noetherian integral domain with field of fractions F, let A be a finite dimensional F-algebra and let Λ be an R-order in A. If e is a central idempotent of A then*
(i) $\mathfrak{Z}(e\Lambda) = (e\Lambda) \cap \mathfrak{Z}(A)$,
(ii) $e\mathfrak{Z}(\Lambda) \subset \mathfrak{Z}(e\Lambda)$ *and*
(iii) $\mathfrak{Z}(e\Lambda) \cap \mathfrak{Z}(\Lambda) = e\mathfrak{Z}(\Lambda) \cap \mathfrak{Z}(\Lambda)$.

Proof. Since $e \in \mathfrak{Z}(A)$ and Λ is an R-order in A, we see that $e\mathfrak{Z}(\Lambda) \subset (e\Lambda) \cap \mathfrak{Z}(A)$ and $\mathfrak{Z}(e\Lambda) \subset (e\Lambda) \cap \mathfrak{Z}(A)$. Since $e\Lambda \subset A$, an element of A which commutes with every element in A commutes with every element in $e\Lambda$ and so we see that $(e\Lambda) \cap \mathfrak{Z}(A) \subset \mathfrak{Z}(e\Lambda)$. This proves (i) and (ii). Let $x \in \mathfrak{Z}(e\Lambda) \cap \mathfrak{Z}(\Lambda)$. Since $x \in e\Lambda$ and $x \in \mathfrak{Z}(\Lambda)$, we see that $x = ex \in e\mathfrak{Z}(\Lambda)$. Therefore,

$$\mathfrak{Z}(e\Lambda) \cap \mathfrak{Z}(\Lambda) \subset e\mathfrak{Z}(\Lambda) \cap \mathfrak{Z}(\Lambda).$$

Now (iii) follows from (ii). □

Example 1.9.9. It is not necessarily true that $e\mathfrak{Z}(\Lambda) = \mathfrak{Z}(e\Lambda)$. For example let p be a prime number and let $A = \mathbb{Q} \times \mathbb{Q} \times M_{2\times 2}(\mathbb{Q})$. Let $e_1 = (1, 0, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right))$, $e_2 = (0, 1, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right))$ and $e_3 = (0, 0, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ be the primitive central idempotents of A. Let $\Gamma = \mathbb{Z} \times \mathbb{Z} \times M_{2\times 2}(\mathbb{Z})$ and let $e_3' = (0, 0, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)) \in \Gamma$. Then Γ is a maximal $\mathbb{Z}$-order in A and e_3' is a primitive idempotent in e_3A. Let

$$\Lambda = 1_\Gamma \cdot \mathbb{Z} + (e_1 + e_3') \cdot \mathbb{Z} + p\Gamma = (e_1 + e_3') \cdot \mathbb{Z} + (e_2 + e_3 - e_3') \cdot \mathbb{Z} + p\Gamma.$$

It is clear that Λ is a $\mathbb{Z}$-lattice in A and since

$$1_\Gamma \cdot \mathbb{Z} \cdot (e_1 + e_3') \cdot \mathbb{Z} = (e_1 + e_3') \cdot \mathbb{Z} \text{ and } (e_1 + e_3') \cdot \mathbb{Z} \cdot p\Gamma \subset p\Gamma,$$

we see that Λ is as $\mathbb{Z}$-order in A. Finally, it is clear that

$$(e_1 + e_2)\mathfrak{Z}(\Lambda) = (e_1 + e_2) \cdot \mathbb{Z} + p(e_1 + e_2) \cdot \mathfrak{Z}(\Gamma) \subsetneq e_1 \cdot \mathbb{Z} + e_2 \cdot \mathbb{Z} = \mathfrak{Z}((e_1 + e_2)\Lambda).$$

Corollary 1.9.10. *Let R be a Noetherian integral domain with field of fractions F, let A be a finite dimensional F-algebra and let Λ be an R-order in A. Let $x \in \mathfrak{Z}(\Lambda)$ and let e be the sum of the central primitive central idempotents e_i of A such that $e_i x \neq 0$. Then $x\mathfrak{Z}(e\Lambda) = x\Lambda \cap \mathfrak{Z}(A)$.*

Proof. From the definition of the idempotent e we see that $ex = x \in (e\mathfrak{Z}(A))^\times$ and so $xe\mathfrak{Z}(A) = e\mathfrak{Z}(A)$. Therefore we see that

$$x\Lambda \cap \mathfrak{Z}(A) = xe\Lambda \cap e\mathfrak{Z}(A) = x(e\Lambda \cap e\mathfrak{Z}(A)) = x\mathfrak{Z}(e\Lambda),$$

where the last equality follows from Lemma 1.9.8(i) for the R-order $e\Lambda$ in eA (and using the fact that $e\mathfrak{Z}(A) = \mathfrak{Z}(eA)$). □

Remark 1.9.11. Let R be a Noetherian integral domain with field of fractions F and let A be a finite dimensional F-algebra. Let M be any full R-lattice in A. We define the *left order* of M to be

$$O_l(M) = \{x \in A \mid xM \subset M\}.$$

We define the *right order* of M to be

$$O_r(M) = \{x \in A \mid Mx \subset M\}.$$

It is relatively easy to verify that these are indeed R-orders in A (see the discussion after [Rei75, Definition 8.1]). Hence every finite dimensional F-algebra A contains an R-order (because every such A contains an R-lattice).

Definition 1.9.12. Let R be a Noetherian integral domain with field of fractions F and let A be a finite dimensional F-algebra. An R-order in A is called *maximal* if it is not properly contained in any other R-order in A.

Example 1.9.13. Let R be an integrally closed Noetherian domain with field of fractions F and let $m \in \mathbb{Z}_{>0}$. By [Rei75, Theorem 8.7], $M_{m\times m}(R)$ is a maximal R-order in $M_{m\times m}(F)$.

Conversely, when R is a principal ideal domain the following result holds.

Lemma 1.9.14. *Let R be a principal ideal domain with field of fractions F. If $m \in \mathbb{Z}_{>0}$ and Λ is a maximal order in $M_{m\times m}(F)$ then $\Lambda \cong M_{m\times m}(R)$.*

Proof. As R is a principal ideal domain, it is integrally closed so the unique maximal R-order in F is R. Let $m \in \mathbb{Z}_{>0}$. By [Rei75, Corollary 27.6], any maximal R-order Λ in $M_{m\times m}(F)$ is isomorphic to an R-algebra

$$\Lambda \cong \begin{bmatrix} R & \cdots & R & J^{-1} \\ \vdots & \ddots & \vdots & \vdots \\ R & \cdots & R & J^{-1} \\ J & \cdots & J & R \end{bmatrix},$$

where J is a non-zero fractional ideal of R. However, as R is a principal ideal domain, the ideal J is principal; that is, $J = aR$ for some $a \in R$. Therefore there is an R-algebra isomorphism

$$\begin{bmatrix} R & \cdots & R & J^{-1} \\ \vdots & \ddots & \vdots & \vdots \\ R & \cdots & R & J^{-1} \\ J & \cdots & J & R \end{bmatrix} \longrightarrow M_{m\times m}(R)$$

$$x \longmapsto TxT^{-1},$$

where

$$T = \begin{pmatrix} a & 0 & \cdots & & 0 \\ 0 & a & & & \\ \vdots & & \ddots & & \vdots \\ & & & a & 0 \\ 0 & & \cdots & 0 & 1 \end{pmatrix}$$

and the inverse of T is taken in $M_{m\times m}(F)$. Therefore there is an R-algebra isomorphism

$$\Lambda \cong M_{m\times m}(R). \qquad \square$$

Remark 1.9.15. Let R be an integrally closed Noetherian integral domain with field of fractions F and let A be a finite dimensional F-algebra. Without the hypothesis that A is a separable F-algebra, it may happen that there are no maximal R-orders in A. In fact, when the Jacobson radical of A is not 0, the discussion in [Rei75, pg. 128] shows that there are no maximal orders in A.

Theorem 1.9.16. *Let R be an integrally closed Noetherian domain with field of fractions F and let A be a separable F-algebra. If Λ is any R-order in A then there is a maximal R-order in A containing Λ.*

Proof. For a proof see [Rei75, Corollary 10.4]. $\square$

Lemma 1.9.17. *Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be a maximal R-order in A. If $H \in \Lambda$ then $\mathrm{rch}_A(H)$ has coefficients in $\mathfrak{Z}(\Lambda)$ and $\mathrm{nr}_A(H) \in \mathfrak{Z}(\Lambda)$.*

Proof. Let $H \in \Lambda$. As A is a finite dimensional semisimple F-algebra we may write $A = \prod_{i=1}^{t} A_i$, where each A_i is a simple F-algebra. As Λ is a maximal R-order in A there is a corresponding decomposition $\Lambda = \prod_{i=1}^{t} \Lambda_i$, where each Λ_i is a maximal R-order in A_i. Thus $H = (H_1, \ldots, H_t) \in \prod_{i=1}^{t} \Lambda_i$. For each $i \in \{1, \ldots, t\}$ we note that $\mathfrak{Z}(\Lambda_i)$ is a maximal R-order in $\mathfrak{Z}(A_i)$, so $\mathfrak{Z}(\Lambda_i)$ is an integrally closed Noetherian domain and we note that A_i is separable over $\mathfrak{Z}(A_i)$. Hence, by [Rei75, Theorem 10.1], for each $i \in \{1, \ldots, t\}$ the coefficients of $\mathrm{rch}_{A_i}(H_i)$ lie in $\mathfrak{Z}(\Lambda_i)$. Therefore

$$\mathrm{rch}_A(H) = (\mathrm{rch}_{A_1}(H_1), \ldots, \mathrm{rch}_{A_t}(H_t)),$$

has coefficients in $\prod_{i=1}^{t} \mathfrak{Z}(\Lambda_i) = \mathfrak{Z}(\Lambda)$. This together with the fact that $\mathrm{nr}_A(H)$ is the constant coefficient of $\mathrm{rch}_A(-H)$ shows that $\mathrm{nr}_A(H) \in \mathfrak{Z}(\Lambda)$. $\square$

Lemma 1.9.18. *Let R be a integrally closed Noetherian domain with field of fractions F. Let A be a commutative finite dimensional F-algebra and let S be an R-order in A. Let V be a finite dimensional F-vector space and let M be an R-lattice in V. If M is a flat R-module then we may identify V with a subset of $V \otimes_F A$ via the map $x \mapsto x \otimes 1_A$ and under this identification $M = (M \otimes_R S) \cap V$. In particular, this holds when R is a Dedekind domain.*

Proof. Noting that $R = S \cap F$ (because R is integrally closed), [Bou89, Chapter I §2.6 Lemma 7] shows that $M = (M \otimes_R S) \cap V$. If R is a Dedekind domain then every torsion free module is flat; in particular, every R-lattice M is flat and $M = (M \otimes_R S) \cap V$. □

Remark 1.9.19. Let E be a finite field extension of F. If S is the integral closure of R in E then [AM69, Proposition 5.12] shows that $FS = E$ (see Definition 1.9.1 for the definition of FS) and so S is an R-order in E. Hence we may view $\Lambda \otimes_R S$ as a subset of $A \otimes_F E$.

Corollary 1.9.20. *Let R be an integrally closed Noetherian domain. Let A be a finite dimensional F-vector space and let Λ be an R-order in A. Let B be a commutative finite dimensional F-algebra and let S be an R-order in B. If Λ is flat as an R-module then $\mathfrak{Z}(\Lambda) = \mathfrak{Z}(\Lambda \otimes_R S) \cap \mathfrak{Z}(A)$. In particular, this holds when R is a Dedekind domain.*

Proof. Using Lemma 1.9.18, we see that $\Lambda = (\Lambda \otimes_R S) \cap A$. Let $x \in \mathfrak{Z}(\Lambda \otimes_R S) \cap \mathfrak{Z}(A)$ and let $y \in (\Lambda \otimes_R S) \cap A$. Since $\Lambda = (\Lambda \otimes_R S) \cap A$ and $\mathfrak{Z}(\Lambda) \subset \mathfrak{Z}(A)$, we have $xy = yx$. Therefore as $y \in (\Lambda \otimes_R S) \cap A$ was arbitrary, we see that $x \in \mathfrak{Z}((\Lambda \otimes_R S) \cap A)$. Thus since $x \in \mathfrak{Z}(\Lambda \otimes_R S) \cap \mathfrak{Z}(A)$ was arbitrary, we see that

$$\mathfrak{Z}(\Lambda \otimes_R S) \cap \mathfrak{Z}(A) \subset \mathfrak{Z}((\Lambda \otimes_R S) \cap A).$$

But $\mathfrak{Z}((\Lambda \otimes_R S) \cap A) = \mathfrak{Z}(\Lambda) \subset \mathfrak{Z}(\Lambda \otimes_R S) \cap \mathfrak{Z}(A)$ because S is commutative. □

1.10 Denominator ideals and auxiliary rings

We now define some auxiliary rings that will be used in the construction of Fitting invariants.

Definition 1.10.1. Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. We define $\mathcal{U}(\Lambda)$ to be the $\mathfrak{Z}(\Lambda)$-submodule of $\mathfrak{Z}(A)$ given by

$$\mathcal{U}(\Lambda) = \langle \mathrm{nr}(H) \mid H \in \mathrm{GL}_b(\Lambda), \forall b \in \mathbb{Z}_{>0} \rangle_{\mathfrak{Z}(\Lambda)}.$$

It is clear that $\mathcal{U}(\Lambda)$ is an R-algebra.

Remark 1.10.2. If R is a local ring then, by [CR81, Proposition 5.28(ii)], Λ is semilocal. Hence, by [CR87, Theorem 40.31], the map $\Lambda^\times \to K_1(\Lambda)$ is surjective. Furthermore, the diagram

$$\begin{array}{ccc} \Lambda^\times & \longrightarrow & K_1(\Lambda) \\ \downarrow{\scriptstyle \mathrm{nr}} & \swarrow{\scriptstyle \mathrm{nr}} & \\ \mathfrak{Z}(A) & & \end{array}$$

commutes. Therefore, $\mathrm{nr}(\Lambda^\times) = \mathrm{nr}(K_1(A)) = \mathrm{nr}(\mathrm{GL}_b(\Lambda))$ for all $b \in \mathbb{Z}_{>0}$. Hence we see that

$$\mathcal{U}(\Lambda) = \langle \mathrm{nr}(H) \mid H \in \Lambda^\times \rangle_{\mathfrak{Z}(\Lambda)}.$$

Definition 1.10.3. Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. We define $\mathcal{I}(\Lambda)$ to be the $\mathfrak{Z}(\Lambda)$-submodule of $\mathfrak{Z}(A)$ given by

$$\mathcal{I}(\Lambda) = \langle \mathrm{nr}(H) \mid H \in M_{b\times b}(\Lambda), \forall b \in \mathbb{Z}_{>0} \rangle_{\mathfrak{Z}(\Lambda)}.$$

It is clear that $\mathcal{I}(\Lambda)$ is an R-algebra.

Remark 1.10.4. It is clear that $\mathfrak{Z}(\Lambda) \subset \mathcal{U}(\Lambda) \subset \mathcal{I}(\Lambda) \subset \mathfrak{Z}(A)$.

Remark 1.10.5. Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a separable F algebra and let Λ be an R-order in A. Suppose that Λ' is a maximal R-order in A containing Λ (this exists by Theorem 1.9.16). With these hypothesis $\mathcal{U}(\Lambda) \subset \mathcal{I}(\Lambda) \subset \mathfrak{Z}(\Lambda') \subset \mathfrak{Z}(A)$. Therefore, using that R is Noetherian, $\mathcal{U}(\Lambda)$ and $\mathcal{I}(\Lambda)$ are R-orders in $\mathfrak{Z}(A)$.

Remark 1.10.6. Let $m \in \mathbb{Z}_{>0}$. It is clear from the definitions that

$$\mathcal{U}(M_{m\times m}(\Lambda)) \subset \mathcal{U}(\Lambda) \quad \text{and} \quad \mathcal{I}(M_{m\times m}(\Lambda)) \subset \mathcal{I}(\Lambda).$$

The reverse inclusions also hold. For $n \in \mathbb{Z}_{>0}$ and $H \in M_{n\times n}(\Lambda)$, we see that

$$\mathrm{nr}_{M_{mn\times mn}(\Lambda)} \begin{pmatrix} H & 0 \\ 0 & I_{(m-1)n} \end{pmatrix} = \mathrm{nr}_{M_{n\times n}(\Lambda)}(H),$$

where $I_{(m-1)n}$ is the identity matrix in $M_{(m-1)n\times(m-1)n}(\Lambda)$. Hence

$$\mathcal{U}(M_{m\times m}(\Lambda)) = \mathcal{U}(\Lambda) \quad \text{and} \quad \mathcal{I}(M_{m\times m}(\Lambda)) = \mathcal{I}(\Lambda).$$

We now recall the definition of the denominator ideal from [JN13, Section 3.6].

Definition 1.10.7. Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. We define the *denominator ideal* of Λ to be

$$\mathcal{H}(\Lambda) = \{x \in \mathfrak{Z}(\Lambda) \mid xH^* \in M_{n\times n}(\Lambda), \forall H \in M_{n\times n}(\Lambda), \forall n \in \mathbb{Z}_{>0}\}.$$

It is clear that $\mathcal{H}(\Lambda)$ is an ideal of $\mathfrak{Z}(\Lambda)$.

Remark 1.10.8. Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a separable F algebra and let Λ be an R-order in A. Suppose that Λ' is a maximal R-order in A containing Λ (this exists by Theorem 1.9.16). With these hypothesis $\mathcal{H}(\Lambda)$ is contained in $\mathfrak{Z}(\Lambda')$. Therefore, using that R is Noetherian, $\mathcal{H}(\Lambda)$ is an R-lattice in $\mathfrak{Z}(A)$.

The following lemma was stated but not proven in [JN13, Section 3.6].

Lemma 1.10.9. *Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. Then $\mathcal{H}(\Lambda)$ is an ideal of $\mathcal{I}(\Lambda)$.*

Proof. Let $x \in \mathcal{H}(\Lambda)$, let $n, m \in \mathbb{Z}_{>0}$, let $H_1 \in M_{n\times n}(\Lambda)$, let $H_2 \in M_{m\times m}(\Lambda)$ and consider the matrix

$$H' = \begin{pmatrix} H_2 & 0 \\ 0 & H_1 \end{pmatrix} \in M_{(n+m)\times(n+m)}(\Lambda).$$

Using Theorem 1.7.8(iii), we see that

$$H'^* = \begin{pmatrix} \operatorname{nr}(H_1)H_2^* & 0 \\ 0 & \operatorname{nr}(H_2)H_1^* \end{pmatrix},$$

and, from the definition of $\mathcal{H}(\Lambda)$, we see that $xH'^* \in M_{(n+m)\times(n+m)}(\Lambda)$. In particular, we see that

$$x \operatorname{nr}(H_1)H_2^* \in M_{m\times m}(\Lambda).$$

Hence, as $m \in \mathbb{Z}_{>0}$ and $H_2 \in M_{m\times m}(\Lambda)$ were arbitrary, we see that $x \operatorname{nr}(H_1) \in \mathcal{H}(\Lambda)$. Therefore, since $x \in \mathcal{H}(\Lambda)$, $n \in \mathbb{Z}_{>0}$ and $H_1 \in M_{n\times n}(\Lambda)$ were arbitrary and $\mathcal{H}(\Lambda)$ is an ideal of $\mathfrak{Z}(\Lambda)$, we see that $\mathcal{H}(\Lambda)$ is an ideal of $\mathcal{I}(\Lambda)$. □

Lemma 1.10.10. *Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. Then $\mathcal{H}(\Lambda) = \mathcal{H}\left(M_{m\times m}(\Lambda)\right)$ for all $m \in \mathbb{Z}_{>0}$.*

Proof. Let $m \in \mathbb{Z}_{>0}$. Using that $M_{n\times n}(M_{m\times m}(\Lambda)) \cong M_{nm\times nm}(\Lambda)$, it is clear that

$$\mathcal{H}(\Lambda) \subset \mathcal{H}(M_{m\times m}(\Lambda)).$$

We note that there is a $\mathfrak{Z}(\Lambda)$-algebra isomorphism

$$\varphi\colon M_{m\times m}\left(M_{n\times n}(\Lambda)\right) \to M_{n\times n}\left(M_{m\times m}(\Lambda)\right).$$

Let $n \in \mathbb{Z}_{>0}$ and let $H \in M_{n\times n}(\Lambda)$. Consider the matrix

$$H' = \begin{pmatrix} H & 0 \\ 0 & I_{(m-1)n} \end{pmatrix} \in M_{m\times m}\left(M_{n\times n}(\Lambda)\right),$$

where $I_{(m-1)n}$ is the identity matrix in $M_{n(m-1)\times n(m-1)}(\Lambda)$. Theorem 1.7.8(iii) shows that

$$H'^* = \begin{pmatrix} H & 0 \\ 0 & I_{(m-1)n} \end{pmatrix}^* = \begin{pmatrix} H^* & 0 \\ 0 & \operatorname{nr}(H)I_{(m-1)n} \end{pmatrix}.$$

Now let $x \in \mathcal{H}\left(M_{m\times m}(\Lambda)\right)$. By Theorem 1.7.8(i), we see that

$$\varphi(xH'^*) = x\varphi(H')^* \in M_{n\times n}\left(M_{m\times m}(\Lambda)\right).$$

Hence, applying φ^{-1}, we see that

$$xH'^* \in M_{m\times m}\left(M_{n\times n}(\Lambda)\right).$$

In particular, we see that $xH^* \in M_{n\times n}(\Lambda)$. As $n \in \mathbb{Z}_{>0}$ and $H \in M_{n\times n}(\Lambda)$ were arbitrary, we have shown that $x \in \mathcal{H}(\Lambda)$. Therefore, as $x \in \mathcal{H}(M_{m\times m}(\Lambda))$ was arbitrary, we have

shown that

$$\mathcal{H}(\Lambda) \supset \mathcal{H}\left(M_{m\times m}(\Lambda)\right). \qquad \square$$

1.11 Non-commutative Fitting invariants

Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra, let Λ be an R-order in A and let M be a finitely presented Λ-module. A naïve approach to generalising the definition of Fitting ideal to the non-commutative ring Λ is to make the same definitions as in the commutative case using the reduced norm in place of the determinant. More precisely, let

$$\Lambda^b \xrightarrow{h} \Lambda^a \longrightarrow M \longrightarrow 0$$

be a presentation for M and assume (for now) that $a \leq b$. (Note that we have implicitly chosen a basis for Λ^a and Λ^b when choosing the presentation h.) We may identify h with a $b \times a$ matrix with entries in Λ. One might define the Fitting invariant of M to be the $\mathfrak{Z}(\Lambda)$-ideal

$$\langle \mathrm{nr}(H) \mid H \in S_a(h)\rangle_{\mathfrak{Z}(\Lambda)},$$

where $S_a(h)$ is the set of $a \times a$ submatrices of h. Unfortunately, there are several problems with this approach.

The first problem is that a different choice of basis for Λ^a in the presentation h yields a new presentation h' for M whose matrix differs from that of H by left multiplication by an element of $\mathrm{GL}_a(\Lambda)$. Over the commutative ring R the determinant gives a map $\mathrm{GL}_a(R) \to R^\times$, so the Fitting ideal of M over R does not depend on the choice of basis of R^a. Unfortunately, without stricter conditions on Λ, the reduced norm of an element in $\mathrm{GL}_a(\Lambda)$ may not lie in $\mathfrak{Z}(\Lambda)^\times$ or even in $\mathfrak{Z}(\Lambda)$. Thus the ideal of $\mathfrak{Z}(\Lambda)$ generated by the reduced norms of submatrices of h may depend of the choice of basis for Λ^a.

There are two approaches to fixing this problem. The first approach (taken in [Nic10, Definition 3.1]) is to define the Fitting invariant of a presentation to be an equivalence class of ideals of $\mathfrak{Z}(\Lambda)$. This has its advantages but as our goal is going to be computing annihilators, a weaker idea suffices. The second approach (taken in [JN13, Section 3.5]) is to instead consider ideals of the slightly larger ring $\mathcal{U}(\Lambda)$. In Remark 1.11.3, we will explain why no information about annihilators is lost when considering ideals over $\mathcal{U}(\Lambda)$.

Definition 1.11.1. Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra, let Λ be an R-order in A and let M be a finitely presented Λ-module with presentation

$$\Lambda^b \xrightarrow{h} \Lambda^a \longrightarrow M \longrightarrow 0,$$

where $a, b \in \mathbb{Z}_{>0}$. We identify h with a $b \times a$ matrix with entries in Λ. We define the *Fitting invariant* of the presentation h to be the $\mathcal{U}(\Lambda)$-ideal

$$\mathrm{Fit}_\Lambda(h) = \begin{cases} \langle \mathrm{nr}(H) \mid H \in S_a(h)\rangle_{\mathcal{U}(\Lambda)} & \text{if } a \leq b, \\ 0 & \text{if } a > b, \end{cases}$$

where $S_a(h)$ is the set of $a \times a$ submatrices of h. We will call $\mathrm{Fit}_\Lambda(h)$ a Fitting invariant of M.

We note that $\mathrm{nr}(\mathrm{GL}_a(\Lambda)) \subset \mathcal{U}(\Lambda)$ so the Fitting invariant does not depend on the choice of basis for Λ^a. However, the Fitting invariant does depend on the choice of presentation. In Definition 1.11.5, we will give a definition which does not depend on the choice of presentation.

One of the aims in generalising the definition of the zeroth Fitting ideal to non-commutative rings is to give an analogue of Theorem 1.2.2. In particular, we wish to show that there is a relation between a Fitting invariant of a module and the annihilator of that module over $\mathfrak{Z}(\Lambda)$. Expecting this relation to be as simple as the commutative case is unrealistic as the Fitting invariant is not even an ideal of $\mathfrak{Z}(\Lambda)$. However, for a presentation $h\colon \Lambda^b \to \Lambda^a$ of M, there is still a relation between $\mathrm{Fit}_\Lambda(h)$ and $\mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M)$. This is given in [Nic10, Theorem 4.2] or [JN13, Theorem 3.3] and is reproduced below.

Theorem 1.11.2. *Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra, let Λ be an R-order in A and let M be a finitely presented Λ-module. If*

$$\Lambda^b \xrightarrow{h} \Lambda^a \longrightarrow M \longrightarrow 0$$

is a presentation for M then

$$\mathcal{H}(\Lambda) \cdot \mathrm{Fit}_\Lambda(h) \subset \mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M).$$

Proof. The proof given here is inspired by [Nic10, Theorem 4.2]. When $a > b$, we note that

$$\mathcal{H}(\Lambda) \cdot \mathrm{Fit}_\Lambda(h) = \mathcal{H}(\Lambda) \cdot 0 = 0 \subset \mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M),$$

proving the result. Otherwise, when $a \leq b$, let $H \in S_a(h)$ and let $x \in \mathcal{H}(\Lambda)$. We see that $xH^* \in M_{a\times a}(\Lambda)$ so multiplication by xH^* gives a map $\Lambda^a \to \Lambda^a$. Using Lemma 1.7.3, we see that $HH^* = \mathrm{nr}(H)I_a$, where I_a is the identity matrix in $M_{a\times a}(\Lambda)$. Therefore we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\Lambda^a & \xrightarrow{H} & \Lambda^a & \longrightarrow & \mathrm{coker}(H) & \longrightarrow & 0 \\
 & \searrow^{xH^*} & \downarrow{\scriptstyle x\,\mathrm{nr}(H)} & & \downarrow{\scriptstyle x\,\mathrm{nr}(H)} & & \\
\Lambda^a & \xrightarrow{H} & \Lambda^a & \longrightarrow & \mathrm{coker}(H) & \longrightarrow & 0.
\end{array}$$

This shows that multiplication by $x\,\mathrm{nr}(H)$ is the zero map on $\mathrm{coker}(H)$. Thus, as $\mathrm{coker}(H)$ surjects onto M, we see that $x\,\mathrm{nr}(H) \in \mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M)$. As $H \in S_a(h)$ and $x \in \mathcal{H}(\Lambda)$ were arbitrary, we see that

$$\mathcal{H}(\Lambda) \cdot \mathrm{Fit}_\Lambda(h) \subset \mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M). \qquad \square$$

Remark 1.11.3. By Lemma 1.10.9, $\mathcal{H}(\Lambda)$ is an ideal of $\mathcal{I}(\Lambda)$. Recalling that $\mathcal{U}(\Lambda) \subset \mathcal{I}(\Lambda)$ and using Theorem 1.11.2, we see that

$$\mathcal{H}(\Lambda) \cdot \mathcal{U}(\Lambda) \cdot \mathrm{Fit}_\Lambda(h) = \mathcal{H}(\Lambda) \cdot \mathrm{Fit}_\Lambda(h) \subset \mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M),$$

so information about the $\mathfrak{Z}(\Lambda)$-annihilator of M is not lost when considering the Fitting invariant as an ideal of $\mathcal{U}(\Lambda)$.

Remark 1.11.4. In [JN13, Section 3.5], R is required to be an integrally closed complete Noetherian local domain and A is required to be a separable F-algebra. Under these stronger conditions one can give a definition of the Fitting invariant that does not depend on the choice of presentation for M.

Let R be an integrally closed complete Noetherian local domain with field of fractions F. Let A be a separable F-algebra, let Λ be an R-order in A and let M be a finitely generated Λ-module. With these assumptions on R we see that M is a finitely presented Λ-module (see [Nic10, Section 2]).

Let $h_1\colon \Lambda^{b_1} \to \Lambda^{a_1}$ and $h_2\colon \Lambda^{b_2} \to \Lambda^{a_2}$ be presentations of M (for $a_1, a_2, b_1, b_2 \in \mathbb{Z}_{>0}$). As R is a complete local ring [Nic10, Theorem 3.2] applies, so the discussion immediately preceding [Nic10, Definition 3.3] shows that there is a presentation $h\colon \Lambda^b \to \Lambda^a$ of M (for $a, b \in \mathbb{Z}_{>0}$) such that $\mathrm{Fit}_\Lambda(h)$ contains both $\mathrm{Fit}_\Lambda(h_1)$ and $\mathrm{Fit}_\Lambda(h_2)$. Hence inclusion turns the set of Fitting invariants of M into a directed set (that is, inclusion is a partial ordering and every pair of elements has an upper bound).

Using that R is an integrally closed Noetherian domain and that A is a separable F-algebra, by Theorem 1.9.16, there is a maximal R-order Λ' in A containing Λ. If $h\colon \Lambda^b \to \Lambda^a$ is any presentation of M then, from the definition of the Fitting invariant, $\mathrm{Fit}_\Lambda(h) \subset \mathcal{U}(\Lambda)$. Also, by Lemma 1.9.17, $\mathcal{U}(\Lambda) \subset \mathfrak{Z}(\Lambda')$. In particular, every Fitting invariant of M is an R-module contained within the finitely generated R-module $\mathfrak{Z}(\Lambda')$. Therefore, as R is Noetherian, there is a (unique) maximal element of the set of Fitting invariants of M.

Definition 1.11.5. Let R be an integrally closed complete Noetherian local domain with field of fractions F. Let A be a separable F-algebra, let Λ be an R-order in A and let M be a finitely generated Λ-module. We define $\mathrm{Fit}_\Lambda^{\max}(M)$ to be the Fitting invariant of M maximal with respect to inclusion among all the Fitting invariants of M.

We note that $\mathrm{Fit}_\Lambda^{\max}(M)$ is a Fitting invariant of M, so by Theorem 1.11.2, an analogue of Theorem 1.2.2 holds.

Theorem 1.11.6. *Let R be an integrally closed complete Noetherian local domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. If M is a finitely generated Λ-module then*

$$\mathcal{H}(\Lambda) \cdot \mathrm{Fit}_\Lambda^{\max}(M) \subset \mathrm{Ann}_{\mathfrak{Z}(\Lambda)}(M).$$

Analogues of Lemma 1.2.3(i) and (iii) also hold (see Lemma 1.11.9). To give an analogue of Lemma 1.2.3(ii), we first must define a quadratic presentation.

Definition 1.11.7. Let R be an integrally closed complete Noetherian local domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. Let M be a finitely presented Λ-module. We say that M admits a *quadratic presentation* h if there is a presentation

$$\Lambda^a \xrightarrow{h} \Lambda^a \longrightarrow M \longrightarrow 0$$

of M.

Remark 1.11.8. Let R be a discrete valuation ring and let G be a finite group. A result of Swan [CR81, Theorem 32.1] may be used to show that every finitely generated R-torsion $R[G]$-module of projective dimension at most 1 admits a quadratic presentation.

Lemma 1.11.9. *Let R be an integrally closed complete Noetherian local domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. Let M, M_1, M_2 and M_3 be finitely presented Λ-modules.*

(i) If there is a surjection $M_1 \to M_2$ then $\mathrm{Fit}_\Lambda^{\max}(M_1) \subseteq \mathrm{Fit}_\Lambda^{\max}(M_2)$.

(ii) If $M_1 \to M_2 \to M_3 \to 0$ is an exact sequence then

$$\mathrm{Fit}_\Lambda^{\max}(M_1)\,\mathrm{Fit}_\Lambda^{\max}(M_3) \subseteq \mathrm{Fit}_\Lambda^{\max}(M_2).$$

(iii) If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence, and M_1 and M_3 admit quadratic presentations, then M_2 admits a quadratic presentation and

$$\mathrm{Fit}_\Lambda^{\max}(M_1)\,\mathrm{Fit}_\Lambda^{\max}(M_3) = \mathrm{Fit}_\Lambda^{\max}(M_2).$$

(iv) The Fitting invariant $\mathrm{Fit}_\Lambda^{\max}(M)$ is an ideal of $\mathcal{I}(\Lambda)$.

(v) If M admits a quadratic presentation h then $\mathrm{Fit}_\Lambda^{\max}(M) = \mathrm{Fit}_\Lambda(h)$.

(vi) If $e \in A$ is a central idempotent then $e\,\mathrm{Fit}_\Lambda^{\max}(M) = \mathrm{Fit}_{e\Lambda}(e\Lambda \otimes_\Lambda M)$.

(vii) Let e be the sum of all primitive central idempotents e_i of A such that $e_i FM \neq 0$. Then $\mathrm{Fit}_\Lambda^{\max}(M) = e\,\mathrm{Fit}_\Lambda^{\max}(M) = \mathrm{Fit}_{e\Lambda}(e\Lambda \otimes_\Lambda M)$.

Proof. For a proof of this see [JN13, Theorem 3.1 and Equation 3.5]. The proof of (v) from this will also require the use of (iv). □

2 The local-global principle for denominator ideals

2.1 Introduction

In this chapter we show that the denominator ideal of an order over a Dedekind domain may be computed locally. The argument presented here generalises the proof of [Nic11, Lemma 1.4] which shows that if G is a finite group then $\mathcal{H}(\mathbb{Z}[G])$ is dense in $\mathcal{H}(\mathbb{Z}_p[G])$ under the p-adic topology (see Example 2.2.3). The results presented in the present chapter are independent of the rest of the thesis and may be skipped on the first reading.

2.2 Lattices and valuations

Definition 2.2.1. Let R be a Dedekind domain with field of fractions F and let $\mathfrak{p}$ be a non-zero prime ideal of R. Let V be a finite dimensional F-vector space and let M be a full R-lattice in V. We define a valuation $v_{M_\mathfrak{p}}$ on $x \in V$ by

$$v_{M_\mathfrak{p}}(x) = \begin{cases} \max\{n \in \mathbb{Z} \mid x \in \mathfrak{p}^n M_\mathfrak{p}\} & \text{if } x \neq 0, \\ +\infty & \text{if } x = 0, \end{cases}$$

where $M_\mathfrak{p}$ is the localisation of M at $\mathfrak{p}$. In particular, we see that

$$M_\mathfrak{p} = \{x \in V \mid v_{M_\mathfrak{p}}(x) \geq 0\}.$$

Example 2.2.2. Let R be a Dedekind domain with field of fractions F and let $\mathfrak{p}$ be a non-zero prime ideal of R. Then $v_{R_\mathfrak{p}}$ is the valuation on R induced by $\mathfrak{p}$, normalised such that $v_{R_\mathfrak{p}}(r) = 1$ for $r \in \mathfrak{p} \setminus \mathfrak{p}^2$. Throughout this chapter we will denote this valuation by $v_\mathfrak{p}$ (omitting R from the notation).

Example 2.2.3. Let G be a finite group and let p be a prime number. We take $R = \mathbb{Z}_p$ in the above definition with ideal $\mathfrak{p} = p\mathbb{Z}_p$ and we consider the $\mathbb{Z}_p$-lattice $M = \mathbb{Z}_p[G]$ in $V = \mathbb{Q}_p[G]$. The valuation $v_{\mathbb{Z}_p[G]}$ on $\mathbb{Q}_p[G]$ is the same as the p-adic valuation on $\mathbb{Q}_p[G]$ defined before [Nic11, Lemma 1.4]. In particular, given an element $x = \sum_{g \in G} a_g g \in \mathbb{Q}_p[G]$ (for some $a_g \in \mathbb{Q}_p$) we have

$$v_{\mathbb{Z}_p[G]}(x) = \min_{g \in G}\{v_p(a_g)\},$$

where v_p is the usual p-adic valuation on $\mathbb{Q}_p$. One way to prove this is to apply Lemma 2.2.4 below.

Lemma 2.2.4. *Let R be a Dedekind domain with field of fractions F. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Let V and V' be finite dimensional F-vector spaces, and let M and M' be full R-lattices in V and V', respectively. If $(x, x') \in V \oplus V'$ then*

$$v_{M_\mathfrak{p} \oplus M'_\mathfrak{p}}(x, x') = \min(v_{M_\mathfrak{p}}(x), v_{M'_\mathfrak{p}}(x')).$$

Proof. Given $n \in \mathbb{Z}$, we see that

$$(x, x') \in \mathfrak{p}^n(M_\mathfrak{p} \oplus M_\mathfrak{p}) \iff x \in \mathfrak{p}^n M_\mathfrak{p} \quad \text{and} \quad x' \in \mathfrak{p}^n M'_\mathfrak{p}.$$

Therefore, for $(x, x') \in V \oplus V'$ we have

$$v_{M_\mathfrak{p} \oplus M'_\mathfrak{p}}(x, x') = \min\left(v_{M_\mathfrak{p}}(x), v_{M'_\mathfrak{p}}(x')\right). \qquad \square$$

Lemma 2.2.5. *Let R be a Dedekind domain with field of fractions F. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Let V be a finite dimensional F-vector space and let M be a full R-lattice in V.*

(i) If $x \in V$ and $f \in F$ then $v_{M_\mathfrak{p}}(fx) = v_\mathfrak{p}(f) + v_{M_\mathfrak{p}}(x)$ (using the convention that $\infty + \infty = \infty + n = n + \infty = \infty$ for any $n \in \mathbb{Z}$).

(ii) If $x, y \in V$ then $v_{M_\mathfrak{p}}(x + y) \geq \min(v_{M_\mathfrak{p}}(x), v_{M_\mathfrak{p}}(y))$. In particular, addition is continuous with respect to the topology on V induced by $v_{M_\mathfrak{p}}$.

Proof. Let $x \in V$ and let $f \in F$. Note that if $x = 0$ or $f = 0$ then (i) follows easily from our conventions on infinity, so in the following we will assume that $x \neq 0$ and $f \neq 0$. We may write $x = em$ for some $m \in M_\mathfrak{p} \setminus \mathfrak{p}M_\mathfrak{p}$ and $e \in F^\times$ and we note that $v_{M_\mathfrak{p}}(x) = v_\mathfrak{p}(e)$. Similarly we see that $v_{M_\mathfrak{p}}(fx) = v_\mathfrak{p}(fe)$. Therefore, using standard properties of valuations (see [FT93, Equation II(2.1.a)]), we see that

$$v_{M_\mathfrak{p}}(fx) = v_\mathfrak{p}(fe) = v_\mathfrak{p}(f) + v_\mathfrak{p}(e) = v_\mathfrak{p}(f) + v_{M_\mathfrak{p}}(x).$$

This proves (i).

Let $x, y \in V$. Given $n, m \in \mathbb{Z}$, if $x \in \mathfrak{p}^n M_\mathfrak{p}$ and $y \in \mathfrak{p}^m M_\mathfrak{p}$ then $x + y \in \mathfrak{p}^{\min(n,m)} M_\mathfrak{p}$ since $\mathfrak{p}$ is an ideal of R. Therefore, for $x, y \in V$, we see that

$$v_{M_\mathfrak{p}}(x + y) \geq \min(v_{M_\mathfrak{p}}(x), v_{M_\mathfrak{p}}(y))$$

(here we use the convention that $+\infty$ is larger than every integer to deduce the cases when x or y is zero). Now endow V with the topology induced by $v_{M_\mathfrak{p}}$. The following argument (to show that addition is continuous) is standard but is included for the convenience of the reader. Let $(x_1, y_1) \in V \times V$ and let $N \in \mathbb{Z}$. If $(x_2, y_2) \in V \times V$ such that $v_{M_\mathfrak{p}}(x_1 - x_2) > N$ and $v_{M_\mathfrak{p}}(y_1 - y_2) > N$, then

$$\begin{aligned} v_{M_\mathfrak{p}}(x_1 + y_1 - (x_2 + y_2)) &= v_{M_\mathfrak{p}}(x_1 - x_2 + y_1 - y_2) \\ &\geq \min(v_{M_\mathfrak{p}}(x_1 - x_2), v_{M_\mathfrak{p}}(y_1 - y_2)) \\ &> N. \end{aligned}$$

This proves that addition in V is continuous, completing the proof of (ii). $\square$

Lemma 2.2.6. *Let R be a Dedekind domain with field of fractions F. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Let V be a finite dimensional F-vector space, and let M and M' be full R-lattices in V. Then the topologies on V induced by $v_{M_\mathfrak{p}}$ and $v_{M'_\mathfrak{p}}$ are the same. In particular, there exists $N \in \mathbb{Z}$ such that $x \in V$ and $v_{M'_\mathfrak{p}}(x) > N$ implies $x \in M_\mathfrak{p}$.*

Proof. Since M and M' are full R-lattices in V there exist non-zero $r, r' \in R$ such that $rM \subset M'$ and $r'M' \subset M$. Let $x \in V$. If $x = 0$ then $v_{M_\mathfrak{p}}(x) = \infty = v_{M'_\mathfrak{p}}(x)$. Otherwise, when $x \neq 0$ we see that

$$rx \in r\mathfrak{p}^{v_{M_\mathfrak{p}}(x)} M_\mathfrak{p} \subset \mathfrak{p}^{v_{M_\mathfrak{p}}(x)} M'_\mathfrak{p}.$$

Thus, by Lemma 2.2.5(i),

$$v_\mathfrak{p}(r) + v_{M'_\mathfrak{p}}(x) = v_{M'_\mathfrak{p}}(rx) \geq v_{M_\mathfrak{p}}(x).$$

In a similar manner, we see that $v_\mathfrak{p}(r') + v_{M_\mathfrak{p}}(x) \geq v_{M'_\mathfrak{p}}(x)$. Since $x \in V$ was arbitrary, we conclude that the topologies on V induced by $v_{M_\mathfrak{p}}$ and $v_{M'_\mathfrak{p}}$ are the same. □

Lemma 2.2.7. *Let R be a Dedekind domain with field of fractions F. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Let V be a finite dimensional F-vector space and let M be a full R-lattice in V. Suppose that V' is a subspace of V and let $M' = V' \cap M$. If $x \in V'$ then $v_{M'_\mathfrak{p}}(x) = v_{M_\mathfrak{p}}(x)$. In particular, endowing V and V' with the topologies induced by $v_{M_\mathfrak{p}}$ and $v_{M'_\mathfrak{p}}$ respectively, we see that V' has the subspace topology.*

Proof. Localising at $\mathfrak{p}$, we may assume without loss of generality that R is a discrete valuation ring. Since R is a discrete valuation ring, $M = M_\mathfrak{p}$, $M' = M'_\mathfrak{p}$ and $\mathfrak{p} = \pi R$ for some $\pi \in R$.

Let $x \in V'$. Since $M' \subset M$, we have $x \in \mathfrak{p}^{v_{M'}(x)} M' \subset \mathfrak{p}^{v_{M'}(x)} M$ and so $v_{M'}(x) \leq v_M(x)$. We also see that $x \in \mathfrak{p}^{v_M(x)} M$, so $x = \pi^{v_M(x)} y$ for some $y \in M$, but $y = x\pi^{-v_M(x)} \in V'$ because $\pi \in R$. Thus $y \in V' \cap M = M'$ and we see that $x \in \mathfrak{p}^{v_M(x)} M'$ meaning that $v_{M'}(x) \geq v_M(x)$. Therefore, we see that $v_{M'}(x) = v_M(x)$. □

Lemma 2.2.8. *Let R be a Dedekind domain with field of fractions F. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. If $x, y \in A$ then*

$$v_{\Lambda_\mathfrak{p}}(xy) \geq v_{\Lambda_\mathfrak{p}}(x) + v_{\Lambda_\mathfrak{p}}(y).$$

In particular, (non-commutative) polynomials with coefficients and variables in A are continuous with respect to the topology induced by $v_{\Lambda_\mathfrak{p}}$.

Proof. Given $n, m \in \mathbb{Z}$, if $x \in \mathfrak{p}^n \Lambda_\mathfrak{p}$ and $y \in \mathfrak{p}^m \Lambda_\mathfrak{p}$ then $xy \in \mathfrak{p}^{n+m} \Lambda_\mathfrak{p}$ (as $\mathfrak{p} \subset \mathfrak{Z}(A)$). Hence, for $x, y \in A$, we see that $v_{\Lambda_\mathfrak{p}}(xy) \geq v_{\Lambda_\mathfrak{p}}(x) + v_{\Lambda_\mathfrak{p}}(y)$.

Now endow A with the topology induced by $v_{\Lambda_\mathfrak{p}}$. The following argument (to show that multiplication is continuous) is standard but is included for the convenience of the reader. Let $(x_1, y_1) \in A \times A$ and let $N \in \mathbb{Z}$. Let $M = \max\big(N - v_{\Lambda_\mathfrak{p}}(x_1), N - v_{\Lambda_\mathfrak{p}}(y_1), N/2\big)$. If

$(x_2, y_2) \in A \times A$ such that $v_{\Lambda_\mathfrak{p}}(x_1 - x_2) > M$ and $v_{\Lambda_\mathfrak{p}}(y_1 - y_2) > M$, then

$$\begin{aligned}
v_{\Lambda_\mathfrak{p}}(x_1y_1 - x_2y_2) &= v_{\Lambda_\mathfrak{p}}(x_1(y_1 - y_2) + (x_1 - x_2)y_2) \\
&\geq \min(v_{\Lambda_\mathfrak{p}}(x_1(y_1 - y_2)), v_{\Lambda_\mathfrak{p}}((x_1 - x_2)y_2)) \\
&\geq \min(v_{\Lambda_\mathfrak{p}}(x_1) + v_{\Lambda_\mathfrak{p}}(y_1 - y_2), v_{\Lambda_\mathfrak{p}}(x_1 - x_2) + v_{\Lambda_\mathfrak{p}}(y_2)) \\
&= \min(v_{\Lambda_\mathfrak{p}}(x_1) + v_{\Lambda_\mathfrak{p}}(y_1 - y_2), v_{\Lambda_\mathfrak{p}}(x_1 - x_2) + v_{\Lambda_\mathfrak{p}}(y_1 + (y_2 - y_1))) \\
&\geq \min(v_{\Lambda_\mathfrak{p}}(x_1) + v_{\Lambda_\mathfrak{p}}(y_1 - y_2), v_{\Lambda_\mathfrak{p}}(x_1 - x_2) + v_{\Lambda_\mathfrak{p}}(y_1), \\
&\qquad\qquad v_{\Lambda_\mathfrak{p}}(x_1 - x_2) + v_{\Lambda_\mathfrak{p}}(y_2 - y_1)) \\
&> \min(v_{\Lambda_\mathfrak{p}}(x_1) + N - v_{\Lambda_\mathfrak{p}}(x_1), N - v_{\Lambda_\mathfrak{p}}(y_1) + v_{\Lambda_\mathfrak{p}}(y_1), N/2 + N/2) \\
&= N.
\end{aligned}$$

Hence multiplication in A is continuous. Therefore, using Lemma 2.2.5(ii) (which shows that addition in A is continuous), we see that (non-commutative) polynomials with coefficients and variables in A are continuous. □

2.3 Continuity of the reduced norm and generalised adjoint

Lemma 2.3.1. *Let R be a Dedekind domain with field of fractions F. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Let A be a separable F-algebra and let Λ be an R-order in A. Endow A with the topology induced by $v_{\Lambda_\mathfrak{p}}$ and endow $\mathfrak{Z}(A)$ with the subspace topology. Then*

(i) the reduced norm $\mathrm{nr}\colon A \to \mathfrak{Z}(A)$ is continuous and

(ii) the generalised adjoint map $\cdot^*\colon A \to A$ is continuous.

Proof. We will first show that it suffices to prove the result when A is a matrix ring over a field, where the proof is relatively straightforward.

If Λ' is a maximal R-order in A containing Λ (this exists by Theorem 1.9.16) then, by Lemma 2.2.6, the topologies on A induced by Λ and Λ' are equivalent. Hence without loss of generality we may assume that Λ is a maximal R-order in A. If A has decomposition $A = \prod_{i=1}^t A_i$ into simple algebras A_i then Λ has decomposition $\Lambda = \bigoplus_{i=1}^t \Lambda_i$, where each Λ_i is a maximal order in A_i. Recall that the reduced norm and generalised adjoint may be defined componentwise and, using Lemma 2.2.4, we see that for

$$x = (x_1, \ldots, x_t) \in A = \prod_{i=1}^t A_i$$

we have $v_{\Lambda_\mathfrak{p}}(x) = \min_i(v_{\Lambda_{i,\mathfrak{p}}}(x_i))$. Therefore, it suffices to prove the result when A is a simple F-algebra.

Recall that the reduced norm and generalised adjoint in the simple F-algebra A are defined after tensoring over the centre of A by a splitting field for A. Let E be finite field extension of $\mathfrak{Z}(A)$ such that E is a splitting field for A over $\mathfrak{Z}(A)$; in particular, $A \otimes_{\mathfrak{Z}(A)} E \cong M_{n\times n}(E)$ for some $n \in \mathbb{Z}_{>0}$. Let S be the integral closure of R in E. Since Λ is a maximal R-order in A, we see that $\mathfrak{Z}(\Lambda)$ is the integral closure of R in the field $\mathfrak{Z}(A)$ so $\mathfrak{Z}(\Lambda)$ is a Dedekind domain. Thus, by Lemma 1.9.18, we see that $\Lambda = (\Lambda \otimes_{\mathfrak{Z}(\Lambda)} S) \cap A$. Hence, by Lemma 2.2.7, for $x \in A$ we have $v_{\Lambda_\mathfrak{p}}(x) = v_{(\Lambda\otimes_{\mathfrak{Z}(\Lambda)}S)_\mathfrak{p}}(x \otimes 1)$. Therefore, after

replacing Λ with $\Lambda \otimes_{\mathfrak{Z}(\Lambda)} S$ and A with $A \otimes_{\mathfrak{Z}(A)} E$, without loss of generality we may assume that Λ is an R-order contained in the simple F-algebra $A = M_{n\times n}(E)$.

Recall from Lemma 2.2.8 that (non-commutative) polynomials in A are continuous. Let $H \in A = M_{n\times n}(E)$. Write

$$\mathrm{rch}(H)(X) = \sum_{i=0}^{N} a_i(H)X^i,$$

for some $N \in \mathbb{Z}_{>0}$, some $a_1(H), \ldots, a_N(H) \in \mathfrak{Z}(A) \cong E$ and some indeterminate X. The coefficients $a_1(H), \ldots, a_N(H)$ are polynomials in the entries of H when viewed as a matrix in $M_{n\times n}(E)$. Let $E_{ij} \in M_{n\times n}(E)$ be the matrix with 1 in the (i,j)-entry and zero everywhere else. We note that $\sum_{i=1}^{n} E_{ki}HE_{il} \in \mathfrak{Z}(A)$ is the (l,k)-entry of the matrix H. Therefore, we see that each $a_i(H)$ is given by a (non-commutative) polynomial in A. Since $a_0(-H) = \mathrm{nr}(H)$, we see that the reduced norm is continuous. We also note that $H^* = \sum_{i=1}^{N} a_i(H)H^{i-1}$; in particular, H^* is given by a (non-commutative) polynomial in A. Hence the generalised adjoint map is continuous. □

2.4 The local-global principle for denominator ideals

Lemma 2.4.1. *Let R be a Dedekind domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Then $\mathcal{H}(\Lambda)_{\mathfrak{p}} = \mathcal{H}(\Lambda_{\mathfrak{p}})$ and $\widehat{\mathcal{H}(\Lambda)}_{\mathfrak{p}} = \mathcal{H}(\widehat{\Lambda}_{\mathfrak{p}})$ for each non-zero prime ideal $\mathfrak{p}$ of R, where $\widehat{M}_{\mathfrak{p}}$ is the completion of the R-module M at $\mathfrak{p}$.*

Proof. Recall the valuation $v_{\Lambda_{\mathfrak{p}}}$ given in Definition 2.2.1. From Lemma 2.2.7, for every $b \in \mathbb{Z}_{>0}$ we have $v_{M_{b\times b}(\Lambda_{\mathfrak{p}})}|_A = v_{\Lambda_{\mathfrak{p}}}$, where A is viewed as a subset of $M_{b\times b}(A)$ via the diagonal embedding. With this in mind, to simplify notation we will write $v_{\Lambda_{\mathfrak{p}}}$ instead of $v_{M_{b\times b}(\Lambda_{\mathfrak{p}})}$.

Firstly, we show that $\mathcal{H}(\Lambda)_{\mathfrak{p}} \subset \mathcal{H}(\Lambda_{\mathfrak{p}})$. Let $b \in \mathbb{Z}_{>0}$ and let $H \in M_{b\times b}(\Lambda_{\mathfrak{p}})$. Recall from Lemma 2.3.1(ii) that the generalised adjoint map $\cdot^*\colon M_{b\times b}(A) \to M_{b\times b}(A)$ is continuous with respect to the topology induced by $v_{\Lambda_{\mathfrak{p}}}$. In particular, there exists $N \in \mathbb{Z}$ such that if $H' \in M_{b\times b}(\Lambda_{\mathfrak{p}})$ and $v_{\Lambda_{\mathfrak{p}}}(H - H') \geq N$, then $H^* - (H')^* \in M_{b\times b}(\Lambda_{\mathfrak{p}})$.

Let $x \in \mathcal{H}(\Lambda)$. Since Λ is dense in $\Lambda_{\mathfrak{p}}$, there is $H' \in M_{b\times b}(\Lambda)$ such that $v_p(H - H') \geq N$. Therefore, as $x \in \mathcal{H}(\Lambda) \subset \mathfrak{Z}(\Lambda)$, we see that

$$xH^* = x(H')^* + x(H^* - (H')^*) \in M_{b\times b}(\Lambda_{\mathfrak{p}}).$$

Hence, because $H \in M_{b\times b}(\Lambda_{\mathfrak{p}})$ and $b \in \mathbb{Z}_{>0}$ were arbitrary, we see that $x \in \mathcal{H}(\Lambda_{\mathfrak{p}})$. Thus, as $x \in \mathcal{H}(\Lambda)$ was arbitrary, we see that $\mathcal{H}(\Lambda) \subset \mathcal{H}(\Lambda_{\mathfrak{p}})$. Therefore, since $\mathcal{H}(\Lambda_{\mathfrak{p}})$ is an $R_{\mathfrak{p}}$-module, we see that $\mathcal{H}(\Lambda)_{\mathfrak{p}} \subset \mathcal{H}(\Lambda_{\mathfrak{p}})$. We note that an identical arguments shows that $\widehat{\mathcal{H}(\Lambda)}_{\mathfrak{p}} \subset \mathcal{H}(\widehat{\Lambda}_{\mathfrak{p}})$.

We now show that $\mathcal{H}(\Lambda_{\mathfrak{p}}) \subset \mathcal{H}(\Lambda)_{\mathfrak{p}}$. We do this following a similar argument to that presented in the proof of [Nic11, Lemma 1.4]. Recall that $\mathcal{H}(\Lambda)$ is a full R-lattice in $\mathfrak{Z}(A)$ contained in $\mathfrak{Z}(\Lambda)$; in particular, there exists $r \in R$ such that $r\mathfrak{Z}(\Lambda) \subset \mathcal{H}(\Lambda)$. Since R is a Dedekind domain, we may write $rR = \mathfrak{a}\mathfrak{p}^m$ for some ideal $\mathfrak{a}$ of R coprime to $\mathfrak{p}$ and some

$m \in \mathbb{Z}_{\geq 0}$. Let $a \in \mathfrak{a} \setminus \mathfrak{p}$ (in particular, $a \in R_{\mathfrak{p}}^{\times}$). Then for each non-zero prime ideal $\mathfrak{q} \neq \mathfrak{p}$ of R we have $aH^* \in M_{b\times b}(\Lambda_{\mathfrak{q}})$, for all $H \in M_{b\times b}(\Lambda)$ and for all $b \in \mathbb{Z}_{>0}$.

We know that $\mathcal{H}(\Lambda)_{\mathfrak{p}}$ and $\mathcal{H}(\Lambda_{\mathfrak{p}})$ are full $R_{\mathfrak{p}}$-lattices in $\mathfrak{Z}(A)$ contained in $\mathfrak{Z}(\Lambda_{\mathfrak{p}})$. Thus there exists $N \in \mathbb{Z}$ such that if $x \in \mathfrak{Z}(A)$ and $v_{\Lambda_{\mathfrak{p}}}(x) \geq N$, then x belongs to both $\mathcal{H}(\Lambda)_{\mathfrak{p}}$ and $\mathcal{H}(\Lambda_{\mathfrak{p}})$.

Let $y \in \mathcal{H}(\Lambda_{\mathfrak{p}})$. Since $\mathfrak{Z}(\Lambda)$ is dense in $\mathfrak{Z}(\Lambda_{\mathfrak{p}})$, there is $x \in \mathfrak{Z}(\Lambda)$ such that $v_{\Lambda_{\mathfrak{p}}}(x-y) \geq N$. Let $b \in \mathbb{Z}_{>0}$ and let $H \in M_{b\times b}(\Lambda)$. We see that

$$xH^* = yH^* + (x-y)H^* \in M_{b\times b}(\Lambda_{\mathfrak{p}}),$$

where $(x-y)H^* \in M_{b\times b}(\Lambda_{\mathfrak{p}})$ follows because $v_{\Lambda_{\mathfrak{p}}}(x-y) \geq N$. Since $a \in \mathfrak{a} \setminus \mathfrak{p} \subset R$ and $x \in \mathcal{H}(\Lambda_{\mathfrak{p}}) \subset \mathfrak{Z}(\Lambda_{\mathfrak{p}})$, we see that

$$axH^* \in M_{b\times b}(\Lambda_{\mathfrak{q}})$$

for all non-zero prime ideals $\mathfrak{q}$ of R. Since R is a Dedekind domain, using Theorem 1.9.4, we see that

$$M_{b\times b}(\Lambda) = \bigcap_{\mathfrak{q}} M_{b\times b}(\Lambda_{\mathfrak{q}}),$$

where $\mathfrak{q}$ runs through all non-zero prime ideals of R. Hence, as $H \in M_{b\times b}(\Lambda)$ and $b \in \mathbb{Z}_{>0}$ were arbitrary, we see that $ax \in \mathcal{H}(\Lambda)$. Therefore, we see that $x = a^{-1}(ax) \in \mathcal{H}(\Lambda)_{\mathfrak{p}}$ because $a \in R_{\mathfrak{p}}^{\times}$. Thus because $v_{\Lambda_{\mathfrak{p}}}(y-x) \geq N$, we have $y \in \mathcal{H}(\Lambda)_{\mathfrak{p}}$. Since $y \in \mathcal{H}(\Lambda_{\mathfrak{p}})$ was arbitrary, we see that $\mathcal{H}(\Lambda_{\mathfrak{p}}) \subset \mathcal{H}(\Lambda)_{\mathfrak{p}}$.

To conclude that $\mathcal{H}(\widehat{\Lambda}_{\mathfrak{p}}) \subset \widehat{\mathcal{H}(\Lambda)}_{\mathfrak{p}}$ a similar argument may be used. However, in place of Theorem 1.9.4 one can use [Rei75, Theorem 5.3(i)] to deduce that

$$M_{b\times b}(\Lambda) = M_{b\times b}(A) \cap \bigcap_{\mathfrak{q}} M_{b\times b}(\widehat{\Lambda}_{\mathfrak{q}}),$$

where $\mathfrak{q}$ runs through all non-zero prime ideals of R. □

Remark 2.4.2. In the proof that $\mathcal{H}(\Lambda_{\mathfrak{p}}) \subset \mathcal{H}(\Lambda)_{\mathfrak{p}}$ above, if we assume that $v_{\Lambda_{\mathfrak{p}}}(a-1) \geq N$ then

$$v_{\Lambda_{\mathfrak{p}}}(ax-y) \geq \min(v_{\Lambda_{\mathfrak{p}}}(x(a-1)), v_{\Lambda_{\mathfrak{p}}}(x-y)) \geq N.$$

This can be used to show that $\mathcal{H}(\Lambda)$ is dense in $\mathcal{H}(\Lambda_{\mathfrak{p}})$ (see the proof of [Nic11, Lemma 1.4] for more details).

Remark 2.4.3. There is a slightly simpler argument to show that $\mathcal{H}(\Lambda_{\mathfrak{p}}) \subset \mathcal{H}(\Lambda)_{\mathfrak{p}}$ (avoiding the approximation step). The key difference is in how one produces $x \in \mathfrak{Z}(\Lambda)$: when $y \in \mathfrak{Z}(\Lambda_{\mathfrak{p}})$ there exists $s \in R \setminus \mathfrak{p} \subset R_{\mathfrak{p}}^{\times}$ such that $x = sy \in \mathfrak{Z}(\Lambda)$. This does not hold for $y \in \mathfrak{Z}(\widehat{\Lambda}_{\mathfrak{p}})$.

Theorem 2.4.4. *Let R be a Dedekind domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. Then*

$$\mathcal{H}(\Lambda) = \bigcap_{\mathfrak{p}} \mathcal{H}(\Lambda_{\mathfrak{p}}) = \mathfrak{Z}(A) \cap \bigcap_{\mathfrak{p}} \mathcal{H}(\widehat{\Lambda}_{\mathfrak{p}}),$$

where $\mathfrak{p}$ *ranges through all the non-zero prime ideals of* R*.*

Proof. By Remark 1.10.8, $\mathcal{H}(\Lambda)$ is a full R-lattice in $\mathfrak{Z}(A)$. By Theorem 1.9.4 and [Rei75, Theorem 5.3(i)], we see that

$$\mathcal{H}(\Lambda) = \bigcap_{\mathfrak{p}} \mathcal{H}(\Lambda)_{\mathfrak{p}} = \mathfrak{Z}(A) \cap \bigcap_{\mathfrak{p}} \widehat{\mathcal{H}(\Lambda)}_{\mathfrak{p}}.$$

The result now follows from Lemma 2.4.1. □

3 Computing denominator ideals

3.1 Introduction

In this chapter we will discuss methods for computing denominator ideals. Let R be a Noetherian integral domain with field of fractions F. Let A be a finite dimensional semisimple F-algebra and let Λ be an R-order in A. We recall that the denominator ideal of Λ is the set

$$\mathcal{H}(\Lambda) := \{x \in \mathfrak{Z}(\Lambda) \mid xH^* \in M_{b\times b}(\Lambda), \forall H \in M_{b\times b}(\Lambda), \forall b \in \mathbb{Z}_{>0}\}.$$

Firstly, in section 3.2 we will explain how denominator ideals behave with respect to extension and restriction of scalars. The bounds found in this section may not be sharp; a counterexample is given in Section 3.10.

Next we will discuss several methods of producing 'lower bounds' for the denominator ideal of Λ. The following lemma is a slight generalisation [JN13, Corollary 6.2 and Proposition 6.3]; one of the main goals of this chapter is to generalise this further.

Lemma 3.1.1. *Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. If Λ' is a maximal R-order in A containing Λ then*

(i) $\mathcal{F}(\Lambda', \Lambda) \subset \mathcal{H}(\Lambda)$ *and*

(ii) $\mathcal{F}(\mathfrak{Z}(\Lambda'), \mathfrak{Z}(\Lambda)) \subset \mathcal{H}(\Lambda)$,

where $\mathcal{F}(\Lambda', \Lambda)$ denotes the central conductor of Λ' into Λ (see Definition 3.3.1).

Proof. When R is an integrally closed complete Noetherian local domain proofs of (i) and (ii) are given in [JN13, Corollary 6.2 and Proposition 6.3], respectively. These proofs still work when R is an integrally closed Noetherian domain. The key point of these proofs is that the generalised adjoint of an element of the maximal order Λ' lies in Λ'. □

In Section 3.4 (in particular, in Theorem 3.4.1), we will generalise the idea from Lemma 3.1.1. In Section 3.5 (in particular, in Theorem 3.5.3), we will use Theorem 3.4.1 to provide an explicit decomposition of the denominator ideal of Λ in terms of the 'commutative part' of Λ. In Section 3.6, we will talk about how these results specialise to group rings and give some examples.

The results after Section 3.6 will not be required later in the thesis, though variations on the techniques used here will be used later in Chapter 5. In Section 3.7, we will generalise Theorem 3.4.1 to slightly improve on the 'lower bound' achieved when there is more than one ring involved. One limitation to the application of Theorem 3.4.1 is that it precludes division rings in the Wedderburn decomposition of A; we will show that this limitation may be removed in Section 3.8. Finally in Section 3.9, we will use Theorem 3.5.3 along

with some general information about central idempotents in A to produce an upper bound for the denominator ideal of Λ.

3.2 Extension and restriction of scalars

Lemma 3.2.1. *Let R be a Dedekind domain with field of fractions F, let A be a separable F-algebra and let Λ be an R-order in A. Suppose that B is a commutative finite dimensional semisimple F-algebra such that $A \otimes_F B$ is semisimple. If Γ is an R-order in B then, under the natural identifications, we have*

$$\mathcal{H}(\Lambda \otimes_R \Gamma) \cap \mathfrak{Z}(A) \subset \mathcal{H}(\Lambda).$$

Remark 3.2.2. We do not always have equality in Lemma 3.2.1; the reverse inclusion

$$\mathcal{H}(\Lambda \otimes_R \Gamma) \cap \mathfrak{Z}(A) \supset \mathcal{H}(\Lambda)$$

does not hold in general. In Section 3.10 we will produce a counterexample to this statement when Γ is the integral closure of R in some finite field extension E of F.

Proof of Lemma 3.2.1. Let $x \in \mathcal{H}(\Lambda \otimes_R \Gamma) \cap \mathfrak{Z}(A)$. Corollary 1.9.20 shows that

$$x \in \mathfrak{Z}(\Lambda \otimes_R \Gamma) \cap \mathfrak{Z}(A) = \mathfrak{Z}(\Lambda).$$

Let $n \in \mathbb{Z}_{>0}$ and let $H \in M_{n\times n}(\Lambda)$. Theorem 1.7.8(ii) shows that

$$x(H^* \otimes 1_\Gamma) = x(H \otimes 1_\Gamma)^* \in M_{n\times n}(\Lambda \otimes_R \Gamma).$$

As $H^* \in M_{n\times n}(A)$ and $x \in \mathfrak{Z}(A)$, we see that

$$xH^* \in M_{n\times n}(\Lambda \otimes_R \Gamma) \cap M_{n\times n}(A) = M_{n\times n}(\Lambda),$$

where the equality of R-orders follows by Lemma 1.9.18. As $n \in \mathbb{Z}_{>0}$ and $H \in M_{n\times n}(\Lambda)$ were arbitrary, we see that $x \in \mathcal{H}(\Lambda)$. □

Lemma 3.2.3. *Let R be an integrally closed Noetherian domain with field of fractions F, let A be a separable F-algebra and let Λ be an R-order in A. Let B be a commutative finite dimensional semisimple F-algebra. If Γ is an R-order in B which is free as an R-module then*

$$\mathcal{H}(\Lambda \otimes_R \Gamma) \subset \mathcal{H}(\Lambda) \otimes_R \Gamma.$$

Proof. The conditions that B is a commutative finite dimensional semisimple F-algebra and that A is a separable F-algebra ensure that $A \otimes_F B$ is a finite dimensional semisimple F-algebra (an argument similar to Remark 1.8.9 can be used to prove this). Thus the denominator ideal of $\Lambda \otimes_R \Gamma$ is defined.

Let $n \in \mathbb{Z}_{>0}$. There is a natural identification of rings

$$M_{n\times n}(\Lambda \otimes_R \Gamma) = M_{n\times n}(\Lambda) \otimes_R \Gamma.$$

Let $\{r_1, \ldots, r_d\}$ be an R-basis for Γ.

Now let $x \in \mathcal{H}(\Lambda \otimes_R \Gamma) \subset \mathfrak{Z}(\Lambda) \otimes_R \Gamma$. Then x may be written uniquely as $\sum_{j=1}^{d} x_j \otimes r_j$, where $x_j \in \mathfrak{Z}(\Lambda)$. If we can show that $x_j \in \mathcal{H}(\Lambda)$ for every j then $x \in \mathcal{H}(\Lambda) \otimes_R \Gamma$, which in turn shows that

$$\mathcal{H}(\Lambda \otimes_R \Gamma) \subset \mathcal{H}(\Lambda) \otimes_R \Gamma.$$

With this in mind, let $H \in M_{n\times n}(\Lambda)$. We see that

$$H \otimes 1 \in M_{n\times n}(\Lambda \otimes_R \Gamma).$$

Since Γ is free as an R-module it is a flat R-module. Hence $\Lambda \otimes_R \Gamma$ can be viewed as a submodule of $A \otimes_F B$ and, using Lemma 1.9.18, under the identification of A as a subset of $A \otimes_F B$ we see that $\Lambda = A \cap (\Lambda \otimes_R \Gamma)$. Now Theorem 1.7.8(ii) shows that $(H \otimes 1)^* = H^* \otimes 1$ and so

$$x(H^* \otimes 1) = x(H \otimes 1)^* \in M_{n\times n}(\Lambda \otimes_R \Gamma)$$

because $x \in \mathcal{H}(\Lambda \otimes_R \Gamma)$. As $\{r_1, \ldots, r_d\}$ is an R-basis for Γ and $x(H^* \otimes 1) \in M_{n\times n}(\Lambda) \otimes_R \Gamma$, we see that $x(H^* \otimes 1)$ may be written uniquely as

$$x(H^* \otimes 1) = \sum_{j=1}^{d} h_j \otimes r_j,$$

where $h_j \in M_{n\times n}(\Lambda)$. However,

$$x(H^* \otimes 1) = \sum_{j=1}^{d} x_j H^* \otimes r_j,$$

so we see that $x_j H^* = h_j \in M_{n\times n}(\Lambda)$. As $H \in M_{n\times n}(\Lambda)$ and $n \in \mathbb{Z}_{>0}$ were arbitrary, we have shown that $x_j \in \mathcal{H}(\Lambda)$. □

3.3 Central conductors

For the convenience of the reader, we now introduce the notion of the left, right and central conductor and talk about some of their properties. These are useful tools for comparing two rings. We have already seen the central conductor in Lemma 3.1.1. The central conductor will appear in other theorems on bounds for denominator ideals.

Definition 3.3.1. Let A be a ring. Let Λ and Γ be rings contained in A with the same addition and multiplication operation but not necessarily the same multiplicative identity. We define

$$(\Gamma, \Lambda)_l = \{x \in \Gamma \mid x\Gamma \subset \Lambda\} = \text{largest right } \Gamma\text{-module in } \Lambda,$$
$$(\Gamma, \Lambda)_r = \{x \in \Gamma \mid \Gamma x \subset \Lambda\} = \text{largest left } \Gamma\text{-module in } \Lambda.$$

We call $(\Gamma, \Lambda)_l$ the *left conductor of* Γ *into* Λ and $(\Gamma, \Lambda)_r$ the *right conductor of* Γ *into* Λ. The *central conductor of* Γ *into* Λ is defined to be

$$\mathcal{F}(\Gamma, \Lambda) = (\Gamma, \Lambda)_l \cap \mathfrak{Z}(\Gamma) = \{x \in \mathfrak{Z}(\Gamma) \mid x\Gamma \subset \Lambda\}.$$

When Γ and Λ are both commutative these definitions coincide and we call them all the *conductor of* Γ *into* Λ.

Remark 3.3.2. This is more general than the definition of conductors in [CR81, Definition 27.2], which is restricted to rings Λ and Γ such that Λ is a subring of Γ.

It is useful to consider how central conductors interact with central idempotents.

Lemma 3.3.3. *Let A be a commutative ring. Let Λ and Γ be rings contained in A with the same addition and multiplication as A but not necessarily the same multiplicative identity. If $1_\Gamma = f_1 + \cdots + f_k$ is a decomposition of unity as a sum of (central) idempotents of Γ then*

$$\mathcal{F}(\Gamma, \Lambda) = \bigoplus_{i=1}^{k} \mathcal{F}(f_i\Gamma, \Lambda).$$

Proof. Let $I = \sum_{i=1}^{k} \mathcal{F}(f_i\Gamma, \Lambda)$. It is clear that $I \subset \Lambda$ and that I is a Γ-module so

$$I \subset \mathcal{F}(\Gamma, \Lambda).$$

Let x be an element of $\mathcal{F}(\Gamma, \Lambda)$. For each f_i, we see that $f_i x \in \mathcal{F}(f_i\Gamma, \Lambda)$, because f_i is a central idempotent of Γ. Thus $x = x1_\Gamma = f_1x + \cdots + f_kx \in I$. Hence, because $x \in \mathcal{F}(\Gamma, \Lambda)$ was arbitrary, we see that $\mathcal{F}(\Gamma, \Lambda) \subset I$. □

Lemma 3.3.4. *Let R be an integrally closed Noetherian domain with field of fractions F, let A be a commutative separable F-algebra and let Λ be an R-order in A. If f is a central idempotent in A then*

$$\mathcal{F}(f\Lambda, \Lambda) = f\Lambda \cap \Lambda.$$

Proof. Let $I = f\Lambda \cap \Lambda$. From the definition of the central conductor we see that

$$\mathcal{F}(f\Lambda, \Lambda) = \{x \in f\Lambda \mid x \cdot f\Lambda \subset \Lambda\} \subset f\Lambda \cap \Lambda = I.$$

Let $x \in I$. Since $x \in f\Lambda$ and f is a central idempotent, we see that $x = fx$. Given $y \in f\Lambda$, we see that $y = fa = af$ for some $a \in \Lambda$, so $yx = afx = ax \in \Lambda$. Therefore, as $x \in I$ was arbitrary, we see that $I \subset \mathcal{F}(f\Lambda, \Lambda)$. □

Lemma 3.3.5. *Let R be a Dedekind domain with field of fractions F, let A be a separable F-algebra and let Λ and Γ be R-orders in A. If E is a finite field extension of F and S is the integral closure of R in E, then under the natural identifications we have*

$$\mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S) \cap \mathfrak{Z}(A) = \mathcal{F}(\Gamma, \Lambda).$$

Proof. Let $x \in \mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S) \cap \mathfrak{Z}(A)$. We see that

$$x \in \mathfrak{Z}(\Gamma \otimes_R S) \cap \mathfrak{Z}(A) = \mathfrak{Z}(\Gamma),$$

where the equality follows from Corollary 1.9.20. Thus $x(\Gamma \otimes_R S) \subset \Lambda \otimes_R S$. For $y \in \Gamma$, since $x \in \mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S)$, we see that $xy \in \Lambda \otimes_R S$ and, since $x \in \mathfrak{Z}(A)$, we see that

$xy \in A$; thus $xy \in (\Lambda \otimes_R S) \cap A = \Lambda$ (by Lemma 1.9.18). Hence, we see that $x\Gamma \subset \Lambda$ and so $x \in \mathcal{F}(\Gamma, \Lambda)$. Since $x \in \mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S) \cap \mathfrak{Z}(A)$ was arbitrary, we see that

$$\mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S) \cap \mathfrak{Z}(A) \subset \mathcal{F}(\Gamma, \Lambda).$$

Let $x \in \mathcal{F}(\Gamma, \Lambda)$. We see that $x \in \mathfrak{Z}(\Gamma) \subset \mathfrak{Z}(\Gamma \otimes_R S)$ such that $x\Gamma \subset \Lambda$. Let $y \in \Gamma \otimes_R S$. We may write $y = \sum_i y_i \otimes s_i$ for some $y_i \in \Gamma$ and $s_i \in S$, so

$$xy = \sum_i xy_i \otimes s_i \in \Lambda \otimes_R S.$$

Since $y \in \Gamma \otimes_R S$ was arbitrary, we see that $x(\Gamma \otimes_R S) \subset \Lambda \otimes_R S$. Since $x \in \mathfrak{Z}(\Gamma) \subset \mathfrak{Z}(A)$, we see that $x \in \mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S) \cap \mathfrak{Z}(A)$. Since $x \in \mathcal{F}(\Gamma, \Lambda)$ was arbitrary, we see that

$$\mathcal{F}(\Gamma, \Lambda) \subset \mathcal{F}(\Gamma \otimes_R S, \Lambda \otimes_R S) \cap \mathfrak{Z}(A). \qquad \square$$

3.4 Lower bounds of denominator ideals

In certain situations it is possible to compute a 'lower bound' for parts of the denominator ideal.

Theorem 3.4.1. *Let R be an integrally closed Noetherian domain with field of fractions F, let A be a separable F-algebra, let Λ be an R-order in A and let f be a central idempotent of A. Suppose that Γ is an R-order in fA isomorphic to a matrix ring over a commutative ring. If $f\Lambda \subset \Gamma$ then*

$$\mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)) \subset \mathcal{H}(\Lambda).$$

Remark 3.4.2. Theorem 3.4.1 deals with a single central idempotent. We may consider a decomposition of unity into central idempotents to achieve a more concise result. Suppose that Γ is an R-order in A containing a decomposition of unity $1_\Gamma = f_1 + \cdots + f_k$ into central idempotents in Γ such that each $f_i\Gamma$ is isomorphic to a matrix ring over a commutative ring. If $\Lambda \subset \Gamma$ then, using Lemma 3.3.3, we see that

$$\mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)) = \bigoplus_{i=1}^{k} \mathcal{F}(\mathfrak{Z}(f_i\Gamma), \mathfrak{Z}(\Lambda)) \subset \mathcal{H}(\Lambda).$$

Proof of Theorem 3.4.1. We follow the proof of [JN13, Proposition 6.3]. Let $b \in \mathbb{Z}_{>0}$. As Γ is isomorphic to a matrix ring over a commutative ring, so is $M_{b\times b}(\Gamma)$. Hence, using that the reduced characteristic polynomial does not depend on the choice of embedding as a matrix ring we see that the reduced characteristic polynomial of any element of $M_{b\times b}(\Gamma)$ has coefficients in $\mathfrak{Z}(\Gamma)$.

Let $H \in M_{b\times b}(\Lambda)$. We see that

$$fH \in M_{b\times b}(f\Lambda) \subset M_{b\times b}(\Gamma),$$

so the reduced characteristic polynomial of fH has coefficients in $\mathfrak{Z}(\Gamma)$. Hence, from the definition of the generalised adjoint (Definition 1.7.1) and Theorem 1.7.8(i), we see that

$$(fH)^* = \sum_{i=0}^{m} \alpha_i (fH)^i,$$

where $m \in \mathbb{Z}_{>0}$ and $\alpha_i \in \mathfrak{Z}(\Gamma)$.

Let $x \in \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda))$. As $x \in \Gamma \subset fA$, we see that $x = fx = xf$ and so

$$xH^* = xfH^* = x(fH)^* = x\sum_{i=0}^{m} \alpha_i (fH)^i = \sum_{i=0}^{m} xf\alpha_i H^i = \sum_{i=0}^{m} x\alpha_i H^i.$$

Since $\alpha_i \in \mathfrak{Z}(\Gamma)$ and $x \in \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda))$ we see that xH^* lies in $M_{b\times b}(\Lambda)$. As $b \in \mathbb{Z}_{>0}$ and $H \in M_{b\times b}(\Lambda)$ were arbitrary, we see that $x \in \mathcal{H}(\Lambda)$. Since $x \in \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda))$ was arbitrary, we have proven that

$$\mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)) \subset \mathcal{H}(\Lambda). \qquad \square$$

Remark 3.4.3. We note that $\Gamma \subset fA$ being a matrix ring over a commutative ring precludes division rings in the Wedderburn decomposition of fA when applying Theorem 3.4.1. In Theorem 3.8.2, we will see that when R is a Dedekind domain this restriction may be weakened.

In the case that $\mathfrak{Z}(\Gamma) = \mathfrak{Z}(f\Lambda)$, using Lemma 3.3.4 (for the R-order $\mathfrak{Z}(\Lambda)$ in $\mathfrak{Z}(A)$), we see that

$$\mathcal{F}(\mathfrak{Z}(f\Lambda), \mathfrak{Z}(\Lambda)) = \mathfrak{Z}(f\Lambda) \cap \mathfrak{Z}(\Lambda),$$

leading us to the following corollary.

Corollary 3.4.4. *Let R be an integrally closed Noetherian domain with field of fractions F, let A be a separable F-algebra, let Λ be an R-order in A and let f be a central idempotent of A. If there is an injective R-algebra homomorphism $f\Lambda \hookrightarrow M_{n\times n}(\mathfrak{Z}(f\Lambda))$ which restricts to the canonical identification on centres and induces an isomorphism of F-algebras after extending scalars, then $\mathfrak{Z}(f\Lambda) \cap \mathfrak{Z}(\Lambda) \subset \mathcal{H}(\Lambda)$.*

Proof. Applying the functor $- \otimes_R F$ to the map $f\Lambda \hookrightarrow M_{n\times n}(\mathfrak{Z}(f\Lambda))$ yields an F-algebra isomorphism

$$fA \cong f\Lambda \otimes_R F \cong M_{n\times n}(\mathfrak{Z}(f\Lambda)) \otimes_R F.$$

The preimage of $M_{n\times n}(\mathfrak{Z}(f\Lambda))$ in $fA \cong f\Lambda \otimes_R F$ is isomorphic to a matrix ring over $\mathfrak{Z}(f\Lambda)$ which contains $f\Lambda$. Hence by Theorem 3.4.1 we have

$$\mathcal{F}(\mathfrak{Z}(f\Lambda), \mathfrak{Z}(\Lambda)) \subset \mathcal{H}(\Lambda)$$

and, using Lemma 3.3.4 (for the R-order $\mathfrak{Z}(\Lambda)$ in $\mathfrak{Z}(A)$), we see that

$$\mathcal{F}(\mathfrak{Z}(f\Lambda), \mathfrak{Z}(\Lambda)) = \mathfrak{Z}(f\Lambda) \cap \mathfrak{Z}(\Lambda). \qquad \square$$

When R is a principal ideal domain we can use this to deduce a special case of Lemma 3.1.1(ii).

Corollary 3.4.5. *Let R be a principal ideal domain with field of fractions F, let A be a separable F-algebra, let Λ be an R-order in A and let f be a central idempotent of A. If*

(i) $fA \cong M_{n\times n}(\mathfrak{Z}(fA))$ for some $n \in \mathbb{Z}_{>0}$ and

(ii) $\mathfrak{Z}(f\Lambda)$ is a maximal R-order in $\mathfrak{Z}(fA)$,

then

$$\mathfrak{Z}(f\Lambda) \cap \mathfrak{Z}(\Lambda) \subset \mathcal{H}(\Lambda).$$

Proof. The fact that there is a ring homomorphism $f\Lambda \hookrightarrow M_{n\times n}(\mathfrak{Z}(f\Lambda))$ follows from Lemma 1.9.14 (which shows that up to isomorphism the only maximal R-order in $M_{n\times n}(F)$ is $M_{n\times n}(R)$). This map induces an isomorphism of F-algebras after extending scalars by hypothesis (i). Thus the result follows from Corollary 3.4.4. □

3.5 The commutative part of the denominator ideal

It is possible to decompose the denominator ideal of an order into the direct sum of a 'commutative part' and a 'non-commutative part'. We will do this in Theorem 3.5.3 below. To produce this decomposition we make the following definition.

Definition 3.5.1. Let F be a field and let A be a separable F-algebra. The *maximal level-1 idempotent of A* is the central idempotent e of A given by the sum of all primitive central idempotents e_i of A such that e_iA is commutative. (We sometimes omit "of A" if A is clear from the context.) In other words, e is the 'largest' central idempotent of A such that eA is commutative.

We will further generalise the idea of Definition 3.5.1 to maximal level-m idempotents in Definition 3.9.2, for some $m \in \mathbb{Z}_{>0}$.

Example 3.5.2. Let F be a field of characteristic 0 and let G be a finite group. Then $e_{G'}$ (the central idempotent in $F[G]$ associated to the commutator subgroup of G) is the maximal level-1 idempotent of $F[G]$ (see Example 1.4.8).

Let e be the maximal level-1 idempotent of A. Since eA is commutative we may apply Corollary 3.4.4 to obtain a lower bound for the denominator ideal of Λ. In fact, we may improve upon Corollary 3.4.4 as follows.

Theorem 3.5.3. *Let R be an integrally closed Noetherian domain with field of fractions F, let A be a separable F-algebra and let Λ be an R-order in A. If e is the maximal level-1 idempotent of A then*

$$\mathcal{H}(\Lambda) = (e\Lambda \cap \Lambda) \oplus (1-e)\mathcal{H}(\Lambda).$$

In particular, we see that $(1-e)\mathcal{H}(\Lambda) \subset \mathcal{H}(\Lambda)$.

Remark 3.5.4. When there are no primitive central idempotents e_i such that e_iA is commutative, Theorem 3.5.3 is the tautology

$$\mathcal{H}(\Lambda) = \mathcal{H}(\Lambda).$$

Proof of Theorem 3.5.3. From the definition of e we see that eA and $e\Lambda$ are commutative. Thus by Corollary 3.4.4 we see that

$$e\Lambda \cap \Lambda \subset \mathcal{H}(\Lambda). \tag{3.1}$$

Since $e\Lambda$ is commutative, Lemma 1.9.8 may be used to show $e\Lambda \cap \Lambda = \mathfrak{Z}(e\Lambda) \cap \mathfrak{Z}(\Lambda)$.

By Remark 1.7.7, we see that $0^* = e$. In particular, if $x \in \mathcal{H}(\Lambda)$ then $xe \in \Lambda$. Since $\mathcal{H}(\Lambda) \subset \mathfrak{Z}(\Lambda) \subset \Lambda$, we see that $xe \in e\Lambda \cap \Lambda$. Hence we have shown that

$$e\mathcal{H}(\Lambda) \subset e\Lambda \cap \Lambda. \tag{3.2}$$

We now show that $\mathcal{H}(\Lambda)$ may be written as a direct sum. Let $x \in \mathcal{H}(\Lambda)$. By (3.1) and (3.2), we see that $xe \in e\mathcal{H}(\Lambda) \subset e\Lambda \cap \Lambda \subset \mathcal{H}(\Lambda)$. As $\mathcal{H}(\Lambda)$ is closed under addition, we have $(1-e)x = x - ex \in \mathcal{H}(\Lambda)$. Using that e is a central idempotent of A, we have $(e\Lambda \cap \Lambda) \cap (1-e)\mathcal{H}(\Lambda) = \{0\}$. Since $x \in \mathcal{H}(\Lambda)$ was arbitrary, we have shown that

$$\mathcal{H}(\Lambda) = (e\Lambda \cap \Lambda) \oplus (1-e)\mathcal{H}(\Lambda). \qquad \square$$

3.6 Denominator ideals of group rings

Let G be a finite group and let F be a field. For simplicity, in this section we will assume that the characteristic of F is 0. However, almost all of the results still hold when F is a field characteristic p, for some prime number p not dividing the order of G. This assumption ensures that the trace idempotents associated to subgroups of G exist in $F[G]$ (see Example 1.4.8 for the characteristic 0 case). In Chapters 4 and 5, we will also assume that our fields have characteristic 0 for similar reasons. One additional advantage of assuming that F has characteristic 0 is that any finitely generated semisimple F-algebra A is necessarily a separable F-algebra (which is one of the conditions in [Rei75, Corollary 10.4] used to prove the existence of maximal orders in A).

Lemma 3.6.1. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and let G be a finite group with normal subgroup N. If e_N is the trace idempotent associated to N in $F[G]$ then*

$$e_N R[G] \cap R[G] = \mathrm{Tr}_N\, R[G]$$

and

$$(1-e_N)R[G] \cap R[G] = \sum_{n \in N} (1-n)R[G].$$

In particular, if G' is the commutator subgroup of G then

$$e_{G'} R[G] \cap R[G] = \mathrm{Tr}_{G'}\, R[G].$$

Proof. To prove the first assertion we follow the idea in the proof of [JN13, Proposition 6.11]. Let $h_1, \ldots, h_r$ be a set of representatives in G of the quotient group G/N; then

$\{e_N h_1, \ldots, e_N h_r\}$ is an R-basis for $e_N R[G]$. Write $N = \{n_1, \ldots, n_s\}$; then $G = \{n_i h_j\}_{i,j}$ is an R-basis for $R[G]$. Let $x \in e_N R[G]$. Then we may write

$$x = \sum_{k=0}^{r} \lambda_k e_N h_k = \sum_{k=0}^{r} \frac{\lambda_k}{|N|} \sum_{i=0}^{s} n_i h_k,$$

for some $\lambda_k \in R$. Hence we see that $x \in R[G]$ if and only if $|N|$ divides each λ_k if and only if $x \in \mathrm{Tr}_N R[G]$. Since $x \in e_N R[G]$ was arbitrary, it follows that $e_N R[G] \cap R[G] = \mathrm{Tr}_N R[G]$.

To prove the second assertion we note that $(1 - e_N)R[N] \cap R[N]$ is precisely the kernel of the augmentation map

$$\begin{aligned} R[N] &\longrightarrow R \\ \sum_{n \in N} a_n n &\longmapsto \sum_{n \in N} a_n. \end{aligned}$$

In particular, $(1 - e_N)R[N] \cap R[N]$ is the augmentation ideal of $R[N]$. Hence, by [Web16, Proposition 6.3.3(2)], we see that

$$(1 - e_N)R[N] \cap R[N] = \sum_{n \in N} (1 - n)R[N].$$

We may view $R[N]$ as an R-subalgebra of $R[G]$ and we see that $R[G]$ is a free as an $R[N]$-module; in particular, $R[G]$ is a flat $R[N]$-module. Therefore, using [Bou89, Chapter I §2.6 Lemma 7] (note that the rings in the referenced lemma are not necessarily commutative), we see that

$$\begin{aligned} (1 - e_N)R[G] \cap R[G] &= ((1 - e_N)R[N] \cap R[N]) \otimes_{R[N]} R[G] \\ &= \left(\sum_{n \in N} (1 - n)R[N] \right) \otimes_{R[N]} R[G] \\ &= \sum_{n \in N} (1 - n)R[G]. \end{aligned}$$

□

Corollary 3.6.2. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and let G be a finite group with commutator subgroup G'. Then*

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1 - e_{G'})\mathcal{H}(R[G]).$$

Proof. We note that $e_{G'}$ is the maximal level-1 idempotent of $F[G]$ (see Definition 3.5.1). Hence Lemma 3.6.1 and Theorem 3.5.3 prove the claim. □

When $\mathfrak{Z}((1 - e_{G'})R[G])$ is maximal we obtain a finer result.

Corollary 3.6.3. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and let G be a finite group with commutator subgroup G'. Suppose that $\mathfrak{Z}((1 - e_{G'})R[G])$ is a maximal R-order in $\mathfrak{Z}((1 - e_{G'})F[G])$. Then*

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus \left(\mathfrak{Z}((1 - e_{G'})R[G]) \cap \mathfrak{Z}(R[G]) \right).$$

Proof. From Corollary 3.6.2 we have

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1 - e_{G'})\mathcal{H}(R[G]).$$

Thus, as $\mathcal{H}(R[G]) \subset \mathfrak{Z}(R[G])$, we see that

$$(1 - e_{G'})\mathcal{H}(R[G]) \subset \mathfrak{Z}((1 - e_{G'})R[G]) \cap \mathfrak{Z}(R[G]).$$

As $\mathfrak{Z}((1 - e_{G'})R[G])$ is a maximal R-order in $\mathfrak{Z}((1 - e_{G'})F[G])$, using Lemmas 3.1.1(ii) and 3.3.4 we see that

$$\mathfrak{Z}((1 - e_{G'})R[G]) \cap \mathfrak{Z}(R[G]) \subset \mathcal{H}(R[G]).$$

Therefore, we have shown that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus \left(\mathfrak{Z}((1 - e_{G'})R[G]) \cap \mathfrak{Z}(R[G])\right). \qquad \square$$

For certain group rings it is possible to compute the denominator ideal explicitly.

Example 3.6.4. Let p be an odd prime number, let G be either of the non-abelian groups of order p^3 and let Z be the centre of G. Then Z is isomorphic to C_p, the cyclic group of order p (otherwise G/Z would be cyclic and G would be abelian) and Z is the commutator subgroup of G (as Z is the smallest normal subgroup of G such that G/Z is abelian). Then $e := e_Z$ is the maximal level-1 idempotent of $\mathbb{Q}[G]$. Let $z \in G$ be a generator of Z.

One can show that $(1-e)\mathbb{Q}[G] \cong M_{p\times p}(\mathbb{Q}(\zeta))$ where ζ is a primitive p-th root of unity. (There are several ways of proving this, one of which is using the character table of G along with a dimension counting argument. The character table of G is computed in [JL01, Theorem 26.6].)

The element $(1-e)z \in \mathfrak{Z}((1-e)\mathbb{Z}[G])$ is a p-th root of unity because $1-e$ is a central idempotent and $z^p = 1$. Moreover, $(1-e)z$ is a primitive p-th root of unity because $(1-e)z = z - e \neq 1 - e$. Hence there is a $\mathbb{Z}$-algebra homomorphism

$$\begin{aligned} \varphi\colon \mathbb{Z}[\zeta] &\longrightarrow \mathfrak{Z}((1-e)\mathbb{Z}[G]) \\ \zeta^i &\longmapsto (1-e)z^i. \end{aligned}$$

Since this map is injective and $\mathbb{Z}[\zeta]$ is a maximal $\mathbb{Z}$-order in $\mathbb{Q}(\zeta)$, it is surjective and so is a $\mathbb{Z}$-algebra isomorphism.

Therefore we see that $\mathfrak{Z}((1-e)\mathbb{Z}[G])$ is a maximal $\mathbb{Z}$-order in $\mathfrak{Z}((1-e)\mathbb{Q}[G]) \cong \mathbb{Q}(\zeta)$. Thus, by Corollary 3.6.3 we have

$$\mathcal{H}(\mathbb{Z}[G]) = \mathrm{Tr}_{G'} \mathbb{Z}[G] \oplus \left(\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G])\right).$$

By Lemma 3.6.1 we see that

$$(1-e)\mathbb{Z}[G] \cap \mathbb{Z}[G] = \sum_{i=0}^{p-1} (1 - z^i)\mathbb{Z}[G] = (1-z)\mathbb{Z}[G],$$

where the last equality follows because $(1-z^i) = (1-z)\sum_{j=0}^{i-1} z^j$. Therefore, we conclude that

$$\begin{aligned}\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G]) &= ((1-e)\mathbb{Z}[G] \cap \mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Q}[G]) \\ &= (1-z)\mathbb{Z}[G] \cap \mathfrak{Z}(\mathbb{Q}[G]) \\ &= (1-z)\mathfrak{Z}((1-e)\mathbb{Z}[G]),\end{aligned}$$

where first equality follows from Lemma 1.9.8 and the last equality follows by Corollary 1.9.10. Therefore we see that

$$\mathcal{H}(\mathbb{Z}[G]) = \mathrm{Tr}_Z\, \mathbb{Z}[G] \oplus (1-z)\mathfrak{Z}((1-e)\mathbb{Z}[G]).$$

In Example 5.1.1 and Remark 5.1.3 we will generalise this to compute $\mathcal{H}(R[G])$ where R is an integrally closed Noetherian domain with field of fractions F of characteristic 0.

Example 3.6.5. Let p be an odd prime number and let

$$G = D_{2p} = \langle x, y \mid x^p = y^2 = 1, yxy^{-1} = x^{-1}\rangle$$

be the dihedral group of order $2p$. Then $\langle x\rangle$ is the commutator subgroup of G and $e := e_{\langle x\rangle}$ is the maximal level-1 idempotent of $\mathbb{Q}[G]$. Moreover, it can be shown that $\{x, x^{-1}\}$ is a conjugacy class in G.

It is known that $(1-e)\mathbb{Q}[G] \cong M_{2\times 2}(\mathbb{Q}(\zeta+\zeta^{-1}))$ where ζ is a primitive p-th root of unity. (There are several ways of proving this, one of which is using the character table of G along with a dimension counting argument. It is also computed more explicitly in [CR81, Example 7.39].)

The element $(1-e)x$ is a p-th root of unity because $1-e$ is a central idempotent and $x^p = 1$. Moreover, $(1-e)x$ is a primitive p-th roof of unity because $(1-e)x = x - e \neq 1-e$. The element $(1-e)(x+x^{-1}) \in (1-e)\mathbb{Z}[G]$ is central as $\{x, x^{-1}\}$ is a conjugacy class in G. Hence there is a $\mathbb{Z}$-algebra homomorphism

$$\begin{aligned}\varphi\colon \mathbb{Z}[\zeta+\zeta^{-1}] &\longrightarrow \mathfrak{Z}((1-e)\mathbb{Z}[G]) \\ \zeta^i + \zeta^{-i} &\longmapsto (1-e)(x^i + x^{-i}).\end{aligned}$$

Since this map is injective and $\mathbb{Z}[\zeta+\zeta^{-1}]$ is a maximal $\mathbb{Z}$-order in $\mathbb{Q}(\zeta+\zeta^{-1})$, it is surjective and so is a $\mathbb{Z}$-algebra isomorphism. Therefore, by Corollary 3.6.3, we have

$$\mathcal{H}(\mathbb{Z}[G]) = \mathrm{Tr}_{G'}\, \mathbb{Z}[G] \oplus \left(\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G])\right).$$

Let $\mathfrak{m} = (2-(\zeta+\zeta^{-1}))\mathbb{Z}[\zeta+\zeta^{-1}]$ be the unique prime ideal over p in $\mathbb{Z}[\zeta+\zeta^{-1}]$. It is clear that

$$\varphi(\mathfrak{m}) = (1-e)(2-(x+x^{-1}))\mathfrak{Z}((1-e)\mathbb{Z}[G])$$

is a maximal ideal in $\mathfrak{Z}((1-e)\mathbb{Z}[G])$. Noting that $ex = e = ex^{-1}$, we see that

$$(1-e)\left(2-(x+x^{-1})\right) = \left(2-(x+x^{-1})\right).$$

This shows that

$$\varphi(\mathfrak{m}) = (2 - (x + x^{-1}))\mathfrak{Z}((1-e)\mathbb{Z}[G]) \subset \mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G]).$$

As $(1-e) \notin \mathfrak{Z}(\mathbb{Z}[G])$, we see that

$$\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G]) \neq \mathfrak{Z}((1-e)\mathbb{Z}[G]).$$

Since the ideal $\varphi(\mathfrak{m})$ is maximal, we have shown that

$$\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G]) = (2 - (x + x^{-1}))\mathfrak{Z}((1-e)\mathbb{Z}[G]).$$

Therefore we see that

$$\mathcal{H}(\mathbb{Z}[G]) = \mathrm{Tr}_{G'}\,\mathbb{Z}[G] \oplus (2 - (x + x^{-1}))\mathfrak{Z}((1-e)\mathbb{Z}[G]).$$

Example 3.6.6. Let p be a prime number, let $q = p^n$ for some $n \in \mathbb{Z}_{>0}$, let

$$G = \mathrm{Aff}(q) = \mathbb{F}_q \rtimes \mathbb{F}_q^\times$$

be the group of affine transformations on $\mathbb{F}_q$ and let G' be the commutator subgroup of G. Then $G' = \mathbb{F}_q \cong (C_p)^n$ and $|G'| = q$. We also see that $e := e_{G'}$ is the maximal level-1 idempotent of $\mathbb{Z}[G]$.

One can show that $(1-e)\mathbb{Q}[G] \cong M_{(q-1)\times(q-1)}(\mathbb{Q})$. (There are several ways of proving this, one of which is using the character table of G along with a dimension counting argument.)

As $\mathbb{Z}$ is the only $\mathbb{Z}$-order in $\mathbb{Q}$, we see that $\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cong \mathbb{Z}$ is a maximal $\mathbb{Z}$-order in $\mathfrak{Z}((1-e)\mathbb{Q}[G]) \cong \mathbb{Q}$. Therefore, by Corollary 3.6.3, we have

$$\mathcal{H}(\mathbb{Z}[G]) = \mathrm{Tr}_{G'}\,\mathbb{Z}[G] \oplus \left(\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G])\right).$$

Recalling that

$$e = e_{G'} = \left|G'\right|^{-1} \mathrm{Tr}_{G'} = q^{-1}\,\mathrm{Tr}_{G'},$$

we see that q is the smallest positive integer m such that $me \in \mathfrak{Z}(\mathbb{Z}[G])$. Because there is a $\mathbb{Z}$-algebra isomorphism $\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cong \mathbb{Z}$, we see that

$$\mathfrak{Z}((1-e)\mathbb{Z}[G]) \cap \mathfrak{Z}(\mathbb{Z}[G]) = q\mathfrak{Z}((1-e)\mathbb{Z}[G]).$$

Therefore we see that

$$\mathcal{H}(\mathbb{Z}[G]) = \mathrm{Tr}_{G'}\,\mathbb{Z}[G] \oplus q\mathfrak{Z}((1-e)\mathbb{Z}[G]).$$

Example 3.6.7. Let A be an abelian group. Let p an odd prime number and let G be one of the following groups:

- a non-abelian group of order p^3 (as in Example 3.6.4),
- D_{2p} (as in Example 3.6.5) or

- $\mathrm{Aff}(q)$, where $q = p^n$ for some $n \in \mathbb{Z}_{>0}$ (as in Example 3.6.6; note that this example also extends to the case when $p = 2$).

We identify $\mathbb{Z}[G \times A]$ with $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[A]$ as in Example 1.5.6. We note that $\mathbb{Z}[A]$ is commutative and, by one of Examples 3.6.4, 3.6.5 or 3.6.6, there exists Γ a $\mathbb{Z}$-order in $\mathbb{Q}[G]$ such that

- $\Gamma \cong e\mathbb{Z}[G] \oplus M_{n\times n}(\mathfrak{Z}((1-e)\mathbb{Z}[G]))$ where $e := e_{G'}$ is the maximal level-1 idempotent of $\mathbb{Q}[G]$ and
- $\mathcal{H}(\mathbb{Z}[G]) = \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\mathbb{Z}[G]))$,

so, by Remark 3.4.2, we see that

$$\mathcal{F}(\mathfrak{Z}(\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}[A]), \mathfrak{Z}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[A])) \subset \mathcal{H}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[A]).$$

By Lemma 3.2.3, we see that

$$\mathcal{H}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[A]) \subset \mathcal{H}(\mathbb{Z}[G]) \otimes_{\mathbb{Z}} \mathbb{Z}[A] = \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\mathbb{Z}[G])) \otimes_{\mathbb{Z}} \mathbb{Z}[A].$$

Now let $x \otimes y \in \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\mathbb{Z}[G])) \otimes_{\mathbb{Z}} \mathbb{Z}[A]$. We have $x\mathfrak{Z}(\Gamma) \subset \mathfrak{Z}(\mathbb{Z}[G])$ so

$$(x \otimes y)(\mathfrak{Z}(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Z}[A]) \subset \mathfrak{Z}(\mathbb{Z}[G]) \otimes_{\mathbb{Z}} \mathbb{Z}[A].$$

Therefore, as $x \otimes y \in \mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\mathbb{Z}[G])) \otimes_{\mathbb{Z}} \mathbb{Z}[A]$ was arbitrary, we see that

$$\mathcal{F}(\mathfrak{Z}(\Gamma), \mathfrak{Z}(\mathbb{Z}[G])) \otimes_{\mathbb{Z}} \mathbb{Z}[A] \subset \mathcal{F}(\mathfrak{Z}(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Z}[A], \mathfrak{Z}(\mathbb{Z}[G]) \otimes_{\mathbb{Z}} \mathbb{Z}[A]).$$

Hence, after identifying $\mathbb{Z}[G \times A]$ with $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[A]$, we see that

$$\begin{aligned}\mathcal{H}(\mathbb{Z}[G \times A]) &= \mathcal{H}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[A]) \\ &= \mathcal{H}(\mathbb{Z}[G]) \otimes_{\mathbb{Z}} \mathbb{Z}[A] \\ &= (e\mathbb{Z}[G \times A] \cap \mathbb{Z}[G \times A]) \oplus (\mathfrak{Z}((1-e)\mathbb{Z}[G \times A]) \cap \mathfrak{Z}(\mathbb{Z}[G \times A])).\end{aligned}$$

3.7 Lower bounds of denominator ideals using multiple rings

The remaining results in this chapter will not be used later in the thesis, but still may be useful in computing denominator ideals.

Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a separable F-algebra, let Λ be an R-order in A and let f be a central idempotent of A such that fA is isomorphic to a matrix ring over a commutative ring. One limitation of Theorem 3.4.1 is that there may be many R-orders Γ in fA containing $f\Lambda$ subject to the condition that Γ is isomorphic to a matrix ring over a commutative ring. Unfortunately, there is no guarantee that there exists a minimal R-order Γ in fA containing $f\Lambda$ which is a matrix ring over a commutative ring. This is because the intersection of two matrix rings over commutative rings is not necessarily a matrix ring over a commutative ring. To address this problem, we adapt the proof of Theorem 3.4.1 to a situation where there are multiple R-orders Γ containing Λ.

Theorem 3.7.1. *Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a separable F-algebra, let Λ be an R-order in A and let f be a central idempotent of A. If $\mathcal{G}$ is a collection of R-orders in fA such that each $\Gamma \in \mathcal{G}$ is isomorphic to a matrix ring over a commutative ring and $f\Lambda \subset \Gamma$, then we have*

$$\mathcal{F}\left(\bigcap_{\Gamma\in\mathcal{G}} \mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)\right) \subset \mathcal{H}(\Lambda).$$

Proof. Given $b \in \mathbb{Z}_{>0}$ and an element $H \in M_{b\times b}(\Lambda)$, the first part of the proof of Theorem 3.4.1 shows that $\mathrm{rch}(H)$ has coefficients in $\mathfrak{Z}(\Gamma)$ for each $\Gamma \in \mathcal{G}$. Therefore, by the second part of the proof of Theorem 3.4.1, we see that

$$\mathcal{F}\left(\bigcap_{\Gamma\in\mathcal{G}} \mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)\right) \subset \mathcal{H}(\Lambda). \qquad \square$$

3.8 Lower bounds of denominator ideals using extension of scalars

Let R be an integrally closed Noetherian domain with field of fractions F. Let A be a separable F-algebra, let Λ be an R-order in A and let f be a central idempotent of A. In Theorem 3.4.1 we assumed that there existed an R-order Γ in fA containing $f\Lambda$ which is isomorphic to a matrix ring over a commutative ring. In Remark 3.4.3, we noted that the condition that Γ is a matrix ring over a commutative ring precludes division rings in the Wedderburn decomposition of fA. One reason that this assumption is needed is to ensure that the degrees of all the matrix rings in the Wedderburn decomposition of fA are the same. To adapt for when there may be division rings in the Wedderburn decomposition we will need take Schur indices into account. This leads us to the following definition.

Definition 3.8.1. Let F be a field, let A be a separable F-algebra and let $m \in \mathbb{Z}_{>0}$. A central idempotent f in A has *level-m* if there exists a finite field extension E of F such that $fA \otimes_F E$ is isomorphic to the matrix ring $M_{m\times m}(\mathfrak{Z}(fA \otimes_F E))$. In this case we call f a *level-m idempotent* of A (or just a level idempotent of A for short). (We sometimes omit "of A" if A is clear from the context.) It should be noted that by transitivity of tensor products it suffices to check this when E is a splitting field of A.

Equivalently, a central idempotent f in A has level-m if for all primitive central idempotents e_i of A such that $e_i f = e_i$ we have $n_i s_i = m$, where $e_i A \cong M_{n_i\times n_i}(D_i)$ with D_i a division ring over K with Schur index s_i.

We are now in a position to strengthen Theorem 3.7.1 to allow for division rings.

Theorem 3.8.2. *Let R be a Dedekind domain with field of fractions F, let A be a separable F-algebra, let Λ be an R-order in A and let f be a level idempotent of A. Suppose that $\mathcal{G}$ is a collection of R-orders in fA and for each $\Gamma \in \mathcal{G}$ there exists a finite field extension E_Γ of F such that $\Gamma \otimes_R S_\Gamma$ is isomorphic to a matrix ring over a commutative ring, where S_Γ is the integral closure of R in E_Γ. If $f\Lambda \subset \Gamma$ for each $\Gamma \in \mathcal{G}$ then we have*

$$\mathcal{F}\left(\bigcap_{\Gamma\in\mathcal{G}} \mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)\right) \subset \mathcal{H}(\Lambda).$$

Proof. Let E be the compositum of all the E_Γ and let S be the integral closure of R in E. (Note that E may not be a finite field extension of F.) It is clear that each $\Gamma \otimes_R S$ is a matrix ring over a commutative ring because each $\Gamma \otimes_R S_\Gamma$ is a matrix ring over a commutative ring. We see that

$$\mathcal{F}\left(\bigcap_{\Gamma\in\mathcal{G}} \mathfrak{Z}(\Gamma), \mathfrak{Z}(\Lambda)\right) = \mathcal{F}\left(\bigcap_{\Gamma\in\mathcal{G}} \mathfrak{Z}(\Gamma \otimes_R S), \mathfrak{Z}(\Lambda \otimes_R S)\right) \cap \mathfrak{Z}(A), \tag{3.3}$$

$$\subset \mathcal{H}\left(\Lambda \otimes_R S\right) \cap \mathfrak{Z}(A), \tag{3.4}$$

$$\subset \mathcal{H}(\Lambda), \tag{3.5}$$

where

- equation (3.3) follows from Lemma 3.3.5,
- equation (3.4) follows from applying Theorem 3.7.1 to $f\Lambda \otimes_R S \subset \Gamma \otimes_R S$ and
- equation (3.5) follows by applying Lemma 3.2.1. □

3.9 Upper bounds of denominator ideals

Let R be a Noetherian integral domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. We recall from Lemma 1.10.9 that $\mathcal{H}(\Lambda)$ is an ideal of the ring

$$\mathcal{I}(\Lambda) := \langle \mathrm{nr}(H) \mid \forall H \in M_{b\times b}(\Lambda), \forall b \in \mathbb{Z}_{>0} \rangle_{\mathfrak{Z}(\Lambda)}.$$

This immediately gives us the following 'upper bound' for the denominator ideal of Λ, remarked upon in [JN13, Remark 6.5].

Lemma 3.9.1. *Let R be a Noetherian integral domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. Then $\mathcal{I}(\Lambda)\mathcal{H}(\Lambda) \subset \mathfrak{Z}(\Lambda)$ and so*

$$\mathcal{H}(\Lambda) \subset \mathcal{F}(\mathcal{I}(\Lambda), \mathfrak{Z}(\Lambda)).$$

Unfortunately, it is not clear that $\mathcal{I}(\Lambda)$ is any easier to compute than $\mathcal{H}(\Lambda)$. An alternative way of obtaining an upper bound for the denominator ideal is Theorem 3.5.3. This shows that

$$\mathcal{H}(\Lambda) = (e\Lambda \cap \Lambda) \oplus (1-e)\mathcal{H}(\Lambda),$$

where e is the maximal level-1 idempotent of A. Hence using the fact that $\mathcal{H}(\Lambda) \subset \mathfrak{Z}(\Lambda)$ and Lemma 1.9.8(iii), we see that

$$e\mathcal{H}(\Lambda) \subset \mathfrak{Z}(e\Lambda) \cap \mathfrak{Z}(\Lambda) \quad \text{and} \quad (1-e)\mathcal{H}(\Lambda) \subset \mathfrak{Z}((1-e)\Lambda) \cap \mathfrak{Z}(\Lambda), \tag{3.6}$$

Now assume that R is a discrete valuation ring (note that this assumption may be weakened using the local-global principle in Theorem 2.4.4). In this section we will generalise the 'upper bounds' in (3.6) to certain other central idempotents of A. In order to do this it is sometimes useful to isolate the level-m part of A, for example the maximal level-1 idempotent of A. With this in mind we make the following definition.

Definition 3.9.2. Let F be a field, let A be a separable F-algebra and let $m \in \mathbb{Z}_{>0}$. The *maximal level-m idempotent* of A is the sum of all the primitive level-m idempotents of A or zero if there are no primitive level-m idempotents. These are called maximal level idempotents of A for short. (We sometimes omit "of A" if A is clear from context.)

Maximal level idempotents of A can be used to compute reduced norms of elements of $\mathfrak{Z}(A)$.

Proposition 3.9.3. *Let F be a field and let A be a separable F-algebra. Let $f_1, \ldots, f_d$ be the non-zero maximal level idempotents of A with levels $m_1, \ldots, m_d$, respectively. If $x \in \mathfrak{Z}(A)$ then*

$$\mathrm{nr}(x) = \sum_{i=1}^{d} (f_i x)^{m_i}.$$

Proof. Let E be a splitting field for A over F. Then

$$(A \otimes_F E) = \prod_{i=1}^{d} f_i(A \otimes_F E),$$

where $f_i(A \otimes_F E) \cong M_{m_i \times m_i}(\prod_{j=1}^{n_i} E)$ for some non-zero $n_i \in \mathbb{Z}_{>0}$. Let $x \in \mathfrak{Z}(A)$ and let $(x_1, \ldots, x_d)$ be the image of x in $\prod_{i=1}^{d} M_{m_i \times m_i}(\prod_{j=1}^{n_i} E)$. The determinant of this element is

$$\det(x_1, \ldots, x_d) \cdot 1_{A \otimes_F E} = \left({x_1}^{m_1}, \ldots, {x_d}^{m_d}\right).$$

Thus, by the definition of the reduced norm, we have

$$\mathrm{nr}(x) = \sum_{i=1}^{d} (f_i x)^{m_i}.$$ □

Corollary 3.9.4. *Let F be a field and let A be a separable F-algebra. Let $f_1, \ldots, f_d$ be the non-zero maximal level idempotents of A with levels $m_1, \ldots, m_d$, respectively. If $H \in \mathfrak{Z}(A)^\times$ then*

$$H^* = \sum_{i=1}^{d} (H f_i)^{m_i - 1}.$$

Proof. If $H \in \mathfrak{Z}(A)^\times$ then

$$H^* = \mathrm{nr}(H) H^{-1} = \sum_{i=1}^{d} (H f_i)^{m_i - 1},$$

where the first equality comes from Remark 1.7.4 and the last equality is Proposition 3.9.3. □

Let R be a discrete valuation ring with field of fractions F, let A be a separable F-algebra and let Λ be an R-order in A. We now give a sketch of a method of producing an 'upper bound' for the denominator ideal of Λ which we will develop into Theorem 3.9.5 below. The homomorphism $R \hookrightarrow \mathfrak{Z}(\Lambda)\colon r \mapsto 1_\Lambda r$ restricts to a group homomorphism $R^\times \hookrightarrow \mathfrak{Z}(\Lambda)^\times$. Let $r \in R^\times$. The generalised adjoint of $1_\Lambda r \in \mathfrak{Z}(\Lambda)^\times$ may be computed explicitly. Furthermore, by the definition of $\mathcal{H}(\Lambda)$ we see that $(1_\Lambda r)^* \mathcal{H}(\Lambda) \subset \Lambda$ (and, since

$(1_\Lambda r)^* \in \mathfrak{Z}(A)$, we have $(1_\Lambda r)^* \mathcal{H}(\Lambda) \subset \mathfrak{Z}(\Lambda))$. Therefore, for each $r \in R^\times$, we have an 'upper bound' for $\mathcal{H}(\Lambda)$ given by

$$\mathcal{H}(\Lambda) \subset \{x \in \mathfrak{Z}(\Lambda) \mid (1_\Lambda r)^* x \in \mathfrak{Z}(\Lambda)\}.$$

With a few more restrictions on R and A, and considering more elements of R we may produce a better 'upper bound' for $\mathcal{H}(\Lambda)$.

Theorem 3.9.5. *Let R be a discrete valuation ring with field of fractions F and residue field k, let A be a separable F-algebra and let Λ be an R-order in A. Let e be the maximal level-1 idempotent of A (we note that e may be 0) and let $f_1, \ldots, f_d$ be all the non-zero maximal level idempotents of $(1-e)A$ with levels $m_1, \ldots, m_d > 1$, respectively. If there exists $g \in k^\times$ such that $g^{m_i} = g^{m_j} \iff i = j$, then for all $i \in \{1, \ldots, d\}$ we have*

$$f_i \mathcal{H}(\Lambda) \subset \mathfrak{Z}(f_i \Lambda) \cap \mathfrak{Z}(\Lambda).$$

In particular, this holds when k is an infinite field.

Before we prove Theorem 3.9.5 we first need a result on bases of free modules.

Proposition 3.9.6. *Let R be a commutative local ring, with residue field k and let $u \in R$ with image $g \in k^\times$. Let $d \in \mathbb{Z}_{>0}$ and $m_1, \ldots, m_d \in \mathbb{Z}_{>0}$. If $g^{m_i} = g^{m_j} \iff i = j$ then the set*

$$X := \{x_i = (u^{im_1}, u^{im_2}, \ldots, u^{im_d}) \mid i \in \{0, \ldots, d-1\}\}$$

is a basis for the free R-module R^d.

Proof. Consider the matrix M with columns given by $x_0, \ldots, x_{d-1}$; in particular, the (i,j)-entry of M is $x^{(i-1)m_j}$. This is a Vandermonde matrix and so has determinant

$$\det(M) = \prod_{1 \le i < j \le d} (u^{m_i} - u^{m_j}).$$

Since $u \in R$ has image $g \in k^\times$ and $g^{m_i} - g^{m_j} \in k^\times$ for $1 \le i < j \le d$, we see that $\det(M) \in R^\times$. Hence $x_0, \ldots, x_{d-1}$ is an R-basis for the free R-module R^d. □

We are now in a position to prove Theorem 3.9.5.

Proof of Theorem 3.9.5. Suppose $g \in k^\times$ has the property that $g^{m_i} = g^{m_j} \iff i = j$. Let u be a lift of g in R. In order to conclude that

$$f_j \mathcal{H}(\Lambda) \subset \mathfrak{Z}(f_j \Lambda) \cap \mathfrak{Z}(\Lambda)$$

for $j = 1, \ldots, d$, we will show that if $x \in \mathfrak{Z}(\Lambda)$ and $x(1_\Lambda u^i)^* \in \Lambda$ for $i = 0, \ldots, d-1$ then $f_j x \in \mathfrak{Z}(\Lambda)$.

We begin by considering the R-module map

$$\begin{aligned} \varphi \colon R^d &\longrightarrow \mathfrak{Z}(A) \\ (y_1, \ldots, y_d) &\longmapsto \sum_{j=1}^{d} f_j y_j. \end{aligned}$$

This has the property that if $e_j \in R^d$ is the j-th standard basis vector then

$$\varphi(e_j) = f_j.$$

If $i \in \{0, \dots, d-1\}$ then, by Corollary 3.9.4, we see that

$$(1_\Lambda u^i)^* = e + \sum_{j=1}^{d} f_j u^{i(m_j-1)},$$

where e is the maximal level-1 idempotent of A, and so

$$\begin{aligned}(1-e)(1_\Lambda u^i)^* &= (1-e)\left(e + \sum_{j=1}^{d} f_j u^{i(m_j-1)}\right)\\ &= \sum_{j=1}^{d} f_j u^{i(m_j-1)}\\ &= \varphi\left(u^{i(m_1-1)}, \dots, u^{i(m_d-1)}\right).\end{aligned}$$

Since $g^{m_i} = g^{m_j} \iff i = j$ and u is a lift of g in R, Proposition 3.9.6 shows that the set

$$\left\{\left(u^{i(m_1-1)}, \dots, u^{i(m_d-1)}\right) \;\middle|\; i \in \{0, \dots, d-1\}\right\}$$

is a basis of R^d. In particular, for each $j \in \{1, \dots, d\}$ there exist $a_0, \dots, a_{d-1} \in R$ such that

$$e_j = \sum_{i=0}^{d-1} a_i \left(u^{i(m_1-1)}, \dots, u^{i(m_d-1)}\right)$$

and so

$$\begin{aligned}f_j &= \varphi(e_j)\\ &= \varphi\left(\sum_{i=0}^{d-1} a_i \left(u^{i(m_1-1)}, \dots, u^{i(m_d-1)}\right)\right)\\ &= \sum_{i=0}^{d-1} (1-e) a_i (1_\Lambda u^i)^*.\end{aligned}$$

Let $j \in \{1, \dots, d\}$. Let $x \in f_j\mathcal{H}(\Lambda)$. Then $x = f_j y$ for some $y \in \mathcal{H}(\Lambda)$. Theorem 3.5.3 shows that

$$(1-e)\mathcal{H}(\Lambda) \subset \mathcal{H}(\Lambda),$$

so $(1-e)y \in \mathcal{H}(\Lambda)$. Therefore, we see that $(1-e)y(1_\Lambda u^i)^* \in \Lambda$ for all $i \in \{0, \dots, d-1\}$. Hence,

$$f_j y = \sum_{i=0}^{d-1} (1-e) a_i y (1_\Lambda u^i)^* \in \Lambda.$$

We know that y and f_j are central, so $x = f_j y \in \mathfrak{Z}(\Lambda)$. As $\mathcal{H}(\Lambda) \subset \mathfrak{Z}(\Lambda)$, we see that $x \in f_j\mathfrak{Z}(\Lambda)$. Therefore $x \in f_j\mathfrak{Z}(\Lambda) \cap \mathfrak{Z}(\Lambda)$ and, because $x \in f_j\mathcal{H}(\Lambda)$ was arbitrary, we have shown that

$$f_j\mathcal{H}(\Lambda) \subset f_j\mathfrak{Z}(\Lambda) \cap \mathfrak{Z}(\Lambda) = \mathfrak{Z}(f_j\Lambda) \cap \mathfrak{Z}(\Lambda),$$

where the last equality is Lemma 1.9.8(iii).

To show the last claim of Theorem 3.9.5 (when k is an infinite field the result always holds) we split into two cases. First, suppose that k is an algebraic extension of $\mathbb{F}_p$ for some prime number p. Since k is an infinite field, the group $k^\times$ contains elements with arbitrarily large orders. In particular, $k^\times$ contains an element g with order greater than $\max\{m_1, \ldots, m_d\}$ which must satisfy

$$g^{m_i} = g^{m_j} \iff m_i = m_j \iff i = j.$$

Otherwise, suppose that k is not an algebraic extension of $\mathbb{F}_p$. In this case k contains an element g of infinite order which must satisfy

$$g^{m_i} = g^{m_j} \iff m_i = m_j \iff i = j.$$

(There are actually two possibilities when k is not an algebraic extension of $\mathbb{F}_p$ for some prime number p. First, if the characteristic of k is p then k contains a transcendental element g over $\mathbb{F}_p$ and g must have infinite order. Otherwise, if the characteristic of k is 0 then $2 \in k^\times$ is an example of an element of infinite order.) □

Using Theorem 3.9.5, after a finite extension, we always have the following 'upper bound' for the denominator ideal.

Corollary 3.9.7 (of Theorem 3.9.5)**.** *Let R be a discrete valuation ring with field of fractions F, let A be a separable F-algebra and let Λ be an R-order in A. Let f be a non-zero maximal level idempotent of A. Then there exists a finite field extension E of F such that*

$$f\mathcal{H}(\Lambda \otimes_R S) \subset \mathfrak{Z}(f\Lambda \otimes_R S) \cap \mathfrak{Z}(\Lambda \otimes_R S),$$

where S is the integral closure of R in E. In particular, if F is a complete local field with finite residue field then E can be taken to be a finite unramified extension of F.

Proof. If f has level-1 then the result follows with $E = F$ from Theorem 3.5.3. For the rest of the proof we will assume that f does not have level-1.

Let k be the residue field of R. If k is an infinite field the result follows with $E = F$ directly from Theorem 3.9.5. Otherwise, k is a finite field. Let e be the maximal level-1 idempotent of A and let $f_1, \ldots, f_d$ be the non-zero maximal level idempotents of $(1-e)A$ with levels $m_1, \ldots, m_d$ respectively. Let k_E be a finite extension of k such that $\left|k_E^\times\right| > m_i$ for all i and let g be a primitive root of k_E. Then

$$g^{m_i} = g^{m_j} \iff m_i = m_j \pmod{\left|k_E^\times\right|} \iff m_i = m_j \iff i = j.$$

Since f does not have level-1, $f = f_i$ for some $i \in \{1, \ldots, d\}$. Hence, by Theorem 3.9.5, an extension E of F with residue field k_E suffices. □

3.10 A counterexample to equality in restriction of scalars

Let R be an Dedekind domain with field of fractions F. Let A be a separable F-algebra and let Λ be an R-order in A. If E is a field extension of F and S is the integral closure

of R in E then the containment

$$\mathcal{H}\left(\Lambda \otimes_R S\right) \cap \mathfrak{Z}(A) \subset \mathcal{H}(\Lambda)$$

(in Lemma 3.2.1) is not necessarily an equality (we noted this in Remark 3.2.2). In this section we will produce an R-order Λ and finite field extension E where equality does not hold.

Let p be a prime number. Let $R = \mathbb{Z}_p$ so $F := \mathrm{Frac}(R) = \mathbb{Q}_p$, let

$$A = \mathbb{Q}_p \times M_{p\times p}(\mathbb{Q}_p) \times M_{p^2\times p^2}(\mathbb{Q}_p)$$

with central idempotents f_1, f_p and f_{p^2} with levels 1, p and p^2, respectively and let

$$\Gamma = \mathbb{Z}_p \times M_{p\times p}(\mathbb{Z}_p) \times M_{p^2\times p^2}(\mathbb{Z}_p) \subset A$$

be a maximal $\mathbb{Z}_p$-order in A. Define the $\mathbb{Z}_p$-order

$$\Lambda = 1_\Gamma \cdot \mathbb{Z}_p + pf_1 \cdot \mathbb{Z}_p + p^2\Gamma \subset \Gamma \subset A.$$

Let E be the unique unramified extension of $\mathbb{Q}_p$ of degree 2 and let S be the integral closure of $\mathbb{Z}_p$ in E.

Proposition 3.10.1. *If Λ, A, and E are as above then*

$$\mathcal{H}\left(\Lambda \otimes_{\mathbb{Z}_p} S\right) \cap \mathfrak{Z}(A) \not\supset \mathcal{H}(\Lambda).$$

Proof. The idea of this proof is to show that the element

$$y := p(f_p + f_{p^2}) = 1_\Gamma p - pf_1 \in \mathfrak{Z}(\Lambda)$$

is in $\mathcal{H}(\Lambda)$ but not $\mathcal{H}\left(\Lambda \otimes_{\mathbb{Z}_p} S\right) \cap \mathfrak{Z}(A)$.

Claim 3.10.2.

$$y = p(f_p + f_{p^2}) \in \mathcal{H}(\Lambda).$$

Proof. We note that $f_p + f_{p^2} = 1_\Gamma - f_1$ so we see that

$$\Lambda = 1_\Gamma \cdot \mathbb{Z}_p + pf_1 \cdot \mathbb{Z}_p + p^2\Gamma = 1_\Gamma \cdot \mathbb{Z}_p + p(f_p + f_{p^2}) \cdot \mathbb{Z}_p + p^2\Gamma.$$

In particular, given $x \in \Gamma$ we see that $yx = p(f_p + f_{p^2})x \in \Lambda$ if and only if there exists $r \in \mathbb{Z}_p$ such that $x \equiv (f_p + f_{p^2})r \pmod{p\Gamma}$.

Let $n \in \mathbb{Z}_{>0}$ and consider $M_{n\times n}(\Lambda) \subset M_{n\times n}(\Gamma)$. We will abuse notation by considering f_1, f_p and f_{p^2} as central idempotents of $M_{n\times n}(\Gamma)$ and by viewing $M_{n\times n}(\mathbb{Z}_p)$ as a subring of $M_{n\times n}(\Gamma)$ via the $\mathbb{Z}_p$-algebra map $\mathbb{Z}_p \hookrightarrow \Gamma$. Then, for $x \in M_{n\times n}(\Gamma)$ we see that

$$yx \in M_{n\times n}(\Lambda) \iff x \equiv (f_p + f_{p^2})r \pmod{p\Gamma} \qquad \text{for some } r \in M_{n\times n}(\mathbb{Z}_p). \tag{3.7}$$

We note that $M_{n\times n}(\Lambda)$ is an $\mathbb{Z}_p$-order contained within the maximal $\mathbb{Z}_p$-order $M_{n\times n}(\Gamma)$. Let $H \in M_{n\times n}(\Lambda)$. By Lemma 1.9.17, $H^* \in M_{n\times n}(\Gamma)$. By the criterion (3.7), showing

that $yH^* \in M_{n\times n}(\Lambda)$ is equivalent to showing that

$$(f_p + f_{p^2})H^* \equiv (f_p + f_{p^2})r \pmod{p\Gamma}, \tag{3.8}$$

for some $r \in M_{n\times n}(\mathbb{Z}_p)$.

We note that reduction modulo p is a $\mathbb{Z}_p$-algebra homomorphism, so taking the characteristic polynomial commutes with reduction modulo p. Write $\overline{H}$ for the image of H in $M_{n\times n}\left(\Gamma/p\Gamma\right)$. We note that $\Lambda/p\Gamma = 1_{\Gamma/p\Gamma} \cdot \mathbb{Z}_p/p\mathbb{Z}_p$ and so $\overline{H} = 1_{M_{n\times n}\left(\Gamma/p\Gamma\right)}\overline{r}$ for some $\overline{r} \in M_{n\times n}(\mathbb{F}_p)$. Now, using Theorem 1.7.8 parts (i) and (iii), one can show that

$$(\overline{f_1 H})^* = \overline{f_1}\overline{r}^*, \qquad (\overline{f_p H})^* = \overline{f_p}\det(\overline{r})^{p-1}\overline{r}^* \quad \text{and} \qquad (\overline{f_{p^2} H})^* = \overline{f_{p^2}}\det(\overline{r})^{p^2-1}\overline{r}^*.$$

Furthermore, as $\overline{r} \in M_{n\times n}(\mathbb{F}_p)$, we see that $\overline{r}^* \in M_{n\times n}(\mathbb{F}_p)$ and $\det(\overline{r}) \in \mathbb{F}_p$. Thus

$$\det(\overline{r})^{p-1} = \begin{Bmatrix} 1 & \text{if } \overline{r} \in \mathrm{GL}_n(\mathbb{F}_p), \\ 0 & \text{otherwise} \end{Bmatrix} = \det(\overline{r})^{p^2-1};$$

in either case this shows that (3.8) holds, which proves that $yH^* \in M_{n\times n}(\Lambda)$. Therefore, as $H \in M_{n\times n}(\Lambda)$ and $n \in \mathbb{Z}_{>0}$ were arbitrary, we see that $y \in \mathcal{H}(\Lambda)$. □

Claim 3.10.3.

$$y \notin \mathcal{H}(\Lambda \otimes_{\mathbb{Z}_p} S) \cap \mathfrak{Z}(A)$$

Proof. Let k_E be the residue field of S (the integral closure of $\mathbb{Z}_p$ in E). Since E is the unramified extension of $\mathbb{Q}_p$ of degree 2, we see that $k_E = \mathbb{F}_{p^2}$. In particular, there exists $g \in k_E$ such that $g^p \neq g$. Hence Theorem 3.9.5 shows that

$$f_p\mathcal{H}(\Lambda \otimes_{\mathbb{Z}_p} S) \subset \mathfrak{Z}(f_p\Lambda \otimes_{\mathbb{Z}_p} S) \cap \mathfrak{Z}(\Lambda \otimes_{\mathbb{Z}_p} S).$$

Recall that

$$\Lambda = 1_\Gamma \cdot \mathbb{Z}_p + pf_1 \cdot \mathbb{Z}_p + p^2\Gamma.$$

In particular,

$$\Lambda \otimes_{\mathbb{Z}_p} S = 1_\Gamma \cdot S + pf_1 \cdot S + p^2(\Gamma \otimes_{\mathbb{Z}_p} S).$$

Hence, it is clear that

$$\mathfrak{Z}(f_p\Lambda \otimes_{\mathbb{Z}_p} S) \cap \mathfrak{Z}(\Lambda \otimes_{\mathbb{Z}_p} S) = p^2 f_p S.$$

Recalling that $y = p(f_p + f_{p^2})$, we see that $f_p y = pf_p \notin p^2 f_p S$. Therefore we see that $y \notin \mathcal{H}(\Lambda \otimes_{\mathbb{Z}_p} S)$. □

These two claims complete the proof of Proposition 3.10.1. □

4 Integral Clifford theory and group rings

4.1 Introduction

This chapter may be read independently of the other chapters, though the results will be used in Chapter 5.

Let G be a finite group with normal subgroup N. Working over a characteristic 0 field F, Clifford's Theorem tells us that the irreducible characters of $F[G]$ can be constructed from the irreducible characters of $F[N]$ (see [CR81, Section 11B] for details when F is a splitting field for G and is a subfield of $\mathbb{C}$). This allows us to compute the structure of the group algebra $F[G]$ using knowledge of the group algebra $F[N]$ and the action of G on $F[N]$. The goal of this chapter is to generalise these ideas to working over certain group rings $R[G]$ where R is an integrally closed Noetherian domain.

Notation and conventions. Throughout this chapter in addition to the notation given in Chapter 1 we will use the following notations and conventions.

- Let G be a finite group.
- Let N be a normal subgroup of G.
- Let F denote a field of characteristic 0. (The characteristic 0 hypothesis is made for the same reason as in Section 3.6.)
- Recall that $\mathrm{Irr}_F(G)$ is the set of F-valued irreducible characters of G. There is a (right) action of G on $\mathrm{Irr}_F(N)$ by conjugation: $\chi^g(n) = \chi(gng^{-1})$, for $\chi \in \mathrm{Irr}_F(N)$, $g \in G$ and $n \in N$.
- For $\chi \in \mathrm{Irr}_F(N)$, let $I_G(\chi) = \{g \in G \mid \chi^g = \chi\} = \mathrm{Stab}_G(\chi)$ be the *inertia group* of χ in G. We note that N acts trivially on $\mathrm{Irr}_F(N)$ so $N \lhd I_G(\chi)$.
- For a ring A, there is a (right) action of G on $A[N]$ by conjugation: $x^g = g^{-1}xg$, where $x \in A[N]$ and $g \in G$.
- For $\chi \in \mathrm{Irr}_F(G)$, recall from Example 1.4.10 that $e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g \in F[G]$ is the primitive central idempotent associated to χ. We note that the action of G on $\mathrm{Irr}_F(N)$ and $F[N]$ are compatible in the following sense. For $\chi \in \mathrm{Irr}_F(N)$ and $g \in G$, we see that $e_{\chi^g} = e_\chi^g$.
- For a central idempotent $e \in F[N]$, let $I_G(e) = \{g \in G \mid e^g = e\} = \mathrm{Stab}_G(e)$; we call this the *inertia group* (or *centralizer*) of e in G. We note that the conjugation action of N on $\mathfrak{Z}(F[N])$ is trivial so $N \lhd I_G(e)$. Also, for $\chi \in \mathrm{Irr}_F(N)$, we see that $I_G(\chi) = I_G(e_\chi)$.

Remark 4.1.1. As in Section 3.6, for many of the results in the present chapter the hypothesis that the characteristic of F is 0 may be weakened. We only consider fields of characteristic 0 for brevity.

The aim of this chapter is prove the following theorem.

Theorem 4.1.2. *Let R be an integrally closed Noetherian domain and let G be a finite group. Suppose that $G = N \rtimes H$ and suppose that $F := \mathrm{Frac}(R)$ is a splitting field for N of characteristic 0. Let $\chi \in \mathrm{Irr}_F(N)$ with associated primitive central idempotent $e_\chi \in F[N]$. Let $e = \sum_{\chi' \in \mathrm{Orb}_G(\chi)} e_{\chi'} \in F[N]$. Suppose that $e_\chi \in R[N]$. If $\chi(1)$ and $|I_G(\chi)/N|$ are coprime and either*

(i) N is an abelian group, or

(ii) R is a principal ideal domain,

then e is a central idempotent of $R[G]$ and

$$eR[G] \cong M_{km \times km}(R[I_G(\chi)/N]),$$

where $k = |\mathrm{Orb}_G(\chi)|$ and $m = \chi(1)$.

Theorem 4.1.2 generalises the following well-known result on the trace idempotent attached to a normal subgroup.

Lemma 4.1.3. *Let R be an integral domain with field of fractions F of characteristic 0. Let G be a finite group with normal subgroup N. If $e := e_N \in F[G]$ is the trace idempotent attached to N, then there is an R-algebra isomorphism $eR[G] \cong R[G/N]$.*

Proof. Let X be a transversal of N in G. We define the R-module homomorphism

$$\varphi \colon R[G/N] \longrightarrow eR[G]$$

on G/N by $\varphi(\overline{x}) = ex$ (for $x \in X$ with image $\overline{x}$ in G/N). This homomorphism is well-defined because, for $n \in N$, we have $en = e$ (this also shows that $eR[N] = eR$). Moreover, φ is an R-algebra homomorphism because e is a central idempotent in $F[G]$.

Recalling that X is a transversal of N in G, we see that $R[G] = \bigoplus_{x \in X} xR[N]$ and $R[G/N] = \bigoplus_{x \in X} \overline{x}R$. Hence, as $e \in F[N]$ is a central idempotent of $F[G]$, we see that

$$eR[G] = \bigoplus_{x \in X} xeR[N] = \bigoplus_{x \in X} exR.$$

Therefore, φ gives a bijection between R-bases of the free R-modules $R[G/N]$ and $eR[G]$ and so is an R-algebra isomorphism. □

Recall the notation of Theorem 4.1.2. In particular, let R be an integrally closed Noetherian domain and let G be a finite group. Suppose that $G = N \rtimes H$ and suppose that $F := \mathrm{Frac}(R)$ is a splitting field for N of characteristic 0. There are at least four results related to Theorem 4.1.2 in the literature.

Firstly, in [Rog92, Theorem XIII.16], Roggenkamp proves a result similar to Theorem 4.1.2 in the case that R is a complete discrete valuation ring of characteristic 0 with residue field of characteristic $p > 0$ (although our result is phrased in terms of central

idempotents of $R[N]$ rather than irreducible $R[N]$-lattices). In [Rog92, Theorem XIII.2], Roggenkamp improves on this result to obtain results in the case that F is a not necessarily a splitting field for N. The references [Rog92, Chapter XIII] and [Rog96, Section 1] are similar; we will cite the former though the same material may be found in the latter.

Secondly, we note that [Rog92, Theorem XIII.16] is a more general version of a result contained within in the proof of [CR87, Theorem 46.24] which holds in the case that R is the valuation ring of a finite extension of $\mathbb{Q}_p$ and $G = N \rtimes P$ where N is a cyclic group with order prime to p and P is an abelian p-group.

Thirdly, in [Sch88a], [Sch83] and [Sch88b], Schmid shows that similar results to Theorem 4.1.2 hold over a finite field and that these results may be lifted to the valuation ring of some finite field extension of $\mathbb{Q}_p$. Schmid does not assume that $\mathrm{Frac}(R)$ is a splitting field for N.

Finally, in [DJ83], DeMeyer and Janusz show that $R[G]$ is a product of matrix rings over commutative rings in the case that R is a complete local ring with residue field of characteristic $p > 0$ such that p does not divide the order of the commutator subgroup of G. The assumptions made on G and k ensure that the Brauer group of k is trivial and $k[G]$ is an Azumaya algebra; this, along with the assumption that R is a complete local ring, is used to deduce that $R[G]$ is a product of matrix rings over commutative rings.

The advantages of Theorem 4.1.2 over the other results are threefold:

- The conditions on the ring R are weaker in some respects: for example the assumption that R is complete is not required at all.
- Unlike the third and fourth approach, the theorem gives an explicit description of the structure of $R[G]$ in terms of the structure of $R[N]$ for some normal subgroup N.
- The proof of the theorem uses idempotents rather than characters or $R[G]$-modules which allows partial results to be achieved when p divides the order of the commutator subgroup. This will be used heavily in Chapter 5.

The idea for proving Theorem 4.1.2 presented here is to construct $eR[G]$ directly by using the structure of $e_\chi R[N]$ and the action of G. This idea is very similar to the proofs of first two similar results in the literature discussed above. The idea can be thought of as a refinement of a proof of Clifford's Theorem over a field (see the proof of [Pas85, Theorem 6.1.9]) to work over an integrally closed Noetherian domain. The proof of Theorem 4.1.2 will be done in two parts: part (i) (when N is an abelian group) is proven in Theorem 4.4.1 and part (ii) (when R is a principal ideal domain) is proven in Theorem 4.9.1.

4.2 Groups with proper inertia group

As in [Pas85, Theorem 6.1.9] the proof of Theorem 4.1.2 proceeds by first reducing to the case $I_G(\chi) = G$. We first recall [Pas85, Lemma 6.1.6].

Lemma 4.2.1. *Let Λ be a ring and let $1 = e_1 + \cdots + e_k$ be a decomposition of unity into a sum of orthogonal idempotents of Λ. Let G be a subgroup of $\Lambda^\times$ and assume that the action of G on $\{e_1, \ldots, e_k\}$ given by conjugation ($e_i^g = g^{-1}e_i g$, for $i \in \{1, \ldots, k\}$ and*

$g \in G$) is transitive. Then there is an isomorphism of rings $\Lambda \cong M_{k\times k}(e_1\Lambda e_1)$, which induces the map

$$\begin{aligned} \mathfrak{Z}(\Lambda) &\longrightarrow \mathfrak{Z}(e_1\Lambda e_1) \\ x &\longrightarrow e_1 x e_1, \end{aligned}$$

on centres.

We give the following generalisation of [Pas85, Lemma 6.1.7].

Theorem 4.2.2. *Let G be a finite group with normal subgroup N. Let R be a commutative ring and let Q be the total ring of fractions of R. Recall that G acts on $Q[N]$ by conjugation ($x^g = g^{-1}xg$, for $x \in Q[N]$ and $g \in G$). If $\{e_1, \ldots, e_k\}$ is a G-orbit of orthogonal central idempotents of $Q[N]$ then $e := e_1 + \cdots + e_k$ is a central idempotent of $Q[G]$ and there is an injection of R-algebras*

$$eR[G] \hookrightarrow M_{k\times k}(e_1 R[I]), \tag{4.1}$$

where $I = I_G(e_1)$. Furthermore, if $e_1 \in R[N]$ then $e \in R[G]$ and (4.1) is an R-algebra isomorphism. In particular (4.1) induces an isomorphism of Q-algebras after extending scalars.

Proof. The proof closely follows that of [Pas85, Lemma 6.1.7], although we note that the assumption that the e_i are primitive central idempotents in $R[N]$ has been replaced by the assumption that the e_i are orthogonal central idempotents in $Q[N]$.

The element e is a central idempotent of $Q[N]$ because the e_i are orthogonal central idempotents in $Q[N]$. The action of G merely permutes the e_i so the action of G fixes e. Therefore e is central in $Q[G]$.

Let $\Lambda = \bigoplus_{i=1}^{k} e_i R[G]$; we view Λ as an R-algebra via multiplication in $Q[G]$. This is the R-algebra generated by $eR[G]$ and $e_1, \ldots, e_k$, so Λ is a ring with identity e and $\overline{G} := \{eg \mid g \in G\}$ is a subgroup of $\Lambda^\times$. By assumption, the action of $\overline{G}$ on $\{e_1, \ldots, e_k\}$ by conjugation is transitive. Furthermore, $e = e_1 + \cdots + e_k$ is a decomposition of unity in the ring Λ. Therefore, by Lemma 4.2.1, there is an isomorphism of rings

$$\Lambda \cong M_{k\times k}(e_1\Lambda e_1),$$

which we note to be an R-algebra isomorphism. Moreover, we have

$$e_1\Lambda e_1 = e_1\left(\bigoplus_{i=1}^{k} e_i R[G]\right)e_1 = e_1 R[G] e_1.$$

It remains to identify this ring.

We note that $e_1R[G]e_1$ is the R-linear span of elements e_1ge_1 for $g \in G$. As the e_i are orthogonal idempotents, we see that

$$e_1 g e_1 = e_1(e_1^{g^{-1}})g = \begin{cases} e_1 g & \text{if } g \in I_G(e_1), \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, $e_1R[G]e_1 \cong e_1R[I_G(e_1)]$ and there is an injection of R-algebras

$$eR[G] \hookrightarrow \Lambda \cong M_{k\times k}(e_1R[I_G(e_1)]).$$

If $e_1 \in R[N]$ then, as G acts transitively on $\{e_1, \ldots, e_k\}$, we see that $e_i \in R[N]$ for $i = 1, \ldots, k$. Therefore, we see that $e = e_1 + \cdots + e_k \in R[G]$ and

$$eR[G] = \bigoplus_{i=1}^{k} e_iR[G] = \Lambda. \qquad \square$$

Remark 4.2.3. It seems plausible that a result similar to Theorem 4.2.2 may be obtained for crossed product orders (for the definition of crossed product orders see Definition 4.6.1). This may be interesting to investigate further in a future project. A result related to this idea is [BW09, Lemma 8.8], where certain crossed product orders are shown to be matrix rings over a 'smaller' crossed product order.

Theorem 4.2.2 is a useful stepping stone in proving Theorem 4.1.2; however, the result has merit in its own right. It may be used to obtain results on Frobenius groups (see Theorem 4.3.3) and we will also build upon this theorem in Chapter 5 to deduce results about the denominator ideals of p-groups. In order deduce results on the denominator ideals of p-groups, we will need to know a little more about the map (4.1). The rest of this section provides more details on this and may be skipped on the first reading if one is not interested in the computation of denominator ideals.

Recall the notation from Theorem 4.2.2 and in addition assume that R is a Dedekind domain with field of fractions $F = Q$. Let f be some central idempotent $f \in F[G]$. When computing lower bounds for denominator ideals of $R[G]$ in Chapter 3 (see, for example, Theorem 3.8.2) we were interested in finding R-orders Γ_i in $fF[G]$ containing $fR[G]$ such that each Γ_i was isomorphic to a matrix ring over commutative ring. We were particularly interested in the intersection of the centres of the Γ_i. It is clear that Theorem 4.2.2 has applications to this. For example, if we were to suppose that I was abelian and we considered Γ the pre-image of $M_{k\times k}(e_1R[I])$ in $F[G]$ under the map

$$eF[G] \longrightarrow M_{k\times k}(e_1F[I]), \tag{4.2}$$

then Γ is an R-order in $eF[G]$ containing $eR[G]$ and Γ is isomorphic to a matrix ring over the commutative ring $e_1R[I]$. For this reason it is useful to consider the pre-image of $\mathfrak{Z}\left(M_{k\times k}(e_1R[I])\right)$ under the map (4.2); Corollary 4.2.4 below gives a way of computing this pre-image.

Corollary 4.2.4. *Recall the notation and results of Theorem 4.2.2. Consider the R-algebra homomorphism*

$$\varphi\colon \mathfrak{Z}(eR[G]) \longrightarrow \mathfrak{Z}(M_{k\times k}(e_1R[I])) \xrightarrow{\cong} \mathfrak{Z}(e_1R[I]),$$

given by composition of the restriction of (4.1) *to centres with the canonical isomorphism*

$\mathfrak{Z}(M_{k\times k}(e_1R[I])) \cong \mathfrak{Z}(e_1R[I])$. *Let T be a left transversal of I in G and consider the map*

$$\begin{aligned}\psi\colon \mathfrak{Z}(e_1R[I]) &\longrightarrow \mathfrak{Z}(eQ[G])\\ x &\longmapsto \sum_{h\in T} x^h.\end{aligned}$$

Then φ and ψ are injections of R-algebras and ψ is the left inverse of φ. Furthermore, if $e_1 \in R[G]$ then φ and ψ are inverses of each other. In particular, this holds when $R = Q$.

Proof. For $x \in \mathfrak{Z}(eR[G])$, the map φ is given by $\varphi(x) = e_1xe_1 = e_1x$ (the last equality follows because $x \in \mathfrak{Z}(eR[G])$). Therefore we see that

$$\psi(\varphi(x)) = \psi(e_1x) = \sum_{h\in T} (e_1x)^h = \sum_{h\in T} e_1^h x^h = \sum_{i=1}^{k} e_ix = x$$

(here the third equality follows because $x \in \mathfrak{Z}(eR[G])$). In particular, we see that ψ is a left inverse of φ. Note that if $e_1 \in R[G]$ then (4.1) is an isomorphism meaning that φ is an isomorphism and so $\psi = \varphi^{-1}$. In particular, since $e_1 \in Q[G]$, the map

$$\psi \otimes Q\colon \mathfrak{Z}(e_1Q[I]) \longrightarrow \mathfrak{Z}(eQ[G])$$

is a Q-algebra isomorphism. It is clear that ψ is the composition of the injection

$$\mathfrak{Z}(e_1R[I]) \longrightarrow \mathfrak{Z}(e_1Q[I])$$

with the isomorphism $\psi \otimes Q$ and so ψ is an injection of R-algebras. □

4.3 Group rings of Frobenius groups

Definition 4.3.1. A Frobenius group G is a transitive permutation group on a finite set X such that no non-trivial element fixes more than one point and at least one non-trivial element fixes a point.

Recall the following theorem from [Gor80, Theorem 7.5].

Theorem 4.3.2 (Frobenius)**.** *Let G be a Frobenius group acting on a set X. Let $H = \mathrm{Stab}_G(x)$ for some $x \in X$. Then the subset N of G consisting of the identity together with those elements of G that fix no element of X form a normal subgroup of G of order $|G\colon H|$. In particular, $G = N \rtimes H$.*

Theorem 4.3.3. *Let $G = N \rtimes H$ be a (finite) Frobenius group and let R be a Dedekind domain with field of fractions F of characteristic 0. Suppose that $|N|$ is invertible in R. Let $e_N \in F[G]$ be the trace idempotent attached to N. Then $e_N \in R[G]$ and there is an R-algebra isomorphism*

$$R[G] \cong R[H] \times \mathcal{M},$$

where $\mathcal{M}$ is a maximal R-order in $(1 - e_N)F[G]$.

Remark 4.3.4. In the case that F is a splitting field for N one may obtain a more explicit description of the maximal R-order $\mathcal{M}$ using equation (4.3) of the proof below. If in addition R is a principal ideal domain then Corollary 4.9.4 provides an explicit description of the group ring $R[G]$. (Note that since G is a Frobenius group, $|N|$ and $|H|$ are coprime see [CR81, Section 14A].)

Proof of Theorem 4.3.3. The trace idempotent $e_N := \frac{1}{|N|}\sum_{n\in N} n$ attached to N lies in $R[N]$ because $|N|$ is invertible in R. Hence, using Lemma 4.1.3, there is an R-algebra isomorphism $e_N R[G] \cong R[G/N] \cong R[H]$.

Let E be a finite field extension of F such that E is a splitting field for N (for example, by [CR81, Theorem 15.16], we can take $E = F(\zeta_k)$ where k is the exponent of N and ζ_k is a primitive k-th root of unity). Let S be the integral closure of R in E. Let χ be a non-trivial irreducible character of N over E. Let $C = \mathrm{Orb}_G(\chi)$ be the orbit of χ in $\mathrm{Irr}_E(N)$ under the action of G by conjugation: $\chi^g(n) = \chi(gng^{-1})$. Note that $e_\chi = \frac{\chi(1)}{|N|}\sum_{n\in N}\chi(n^{-1})n \in S[N]$ as $|N|$ is invertible in R and so in invertible in S. Furthermore, χ is an absolutely irreducible character of N because E is a splitting field for N. Since N is a Frobenius group, [Isa76, Theorem 6.34(a)] and the remarks following it show that

$$I_G(e_\chi) = I_G(\chi) := \{g \in G \mid \chi^g = \chi\} = N.$$

Then, using Theorem 4.2.2, we see that $f := \sum_{\chi'\in C} e_{\chi'}$ is a central idempotent of $S[G]$ and that

$$fS[G] \cong M_{k\times k}(e_\chi S[N]), \tag{4.3}$$

where $k := |C| = |H|$ by the Orbit-Stabilizer Theorem.

Since S is a Dedekind domain and $|N|$ is invertible in $R \subset S$, [Rei75, Theorem 41.1] shows that $S[N]$ is a maximal S-order in $E[N]$. Hence $e_\chi S[N]$ is a maximal S-order in $e_\chi E[N]$. Therefore, by [Rei75, Theorem 8.7], we see that $fS[G]$ is a maximal S-order in $fE[G] \cong M_{k\times k}(e_\chi E[N])$.

Let Δ be the set of primitive central idempotents of $E[N]$. Then $\sum_{\delta\in\Delta\setminus\{e_N\}}\delta = 1 - e_N$ and we see that $(1-e_N)S[G] \cong S \otimes_R (1-e_N)R[G]$ is a maximal S-order in $(1-e_N)E[G]$. Therefore, by Lemma 4.3.5 (below), we see that $(1-e_N)R[G]$ is a maximal R-order in $(1-e_N)F[G]$. □

Lemma 4.3.5. *Let R be a Noetherian integral domain with field of fractions F, let E be a finite field extension of F and let A be an F-algebra. Let $\Lambda \subset A$ and $S \subset E$ be R-orders in A and E respectively. Suppose that either*

1. *S is a free R-module of finite rank, or*
2. *R is integrally closed.*

If $\Lambda \otimes_R S$ is a maximal S-order in $A \otimes_F E$, then Λ is a maximal R-order in A.

Remark 4.3.6. When R is a Dedekind domain, a stronger result than Lemma 4.3.5 may be found in [Jan79, Theorem 7]; this includes conditions for a converse to hold.

Proof. First suppose that S is a free R-module of finite rank. In particular, S is a faithfully flat R-module. Let Λ be a non-maximal R-order in A. Then there exists an R-order Λ' such that $\Lambda \subsetneq \Lambda' \subset A$, so we have a short exact sequence of R-modules

$$0 \longrightarrow \Lambda \longrightarrow \Lambda' \longrightarrow \Lambda'/\Lambda \longrightarrow 0,$$

where $\Lambda'/\Lambda \neq 0$. Since S is faithfully flat as an R-module, applying the functor $- \otimes_R S$ gives a short exact sequence of S-modules

$$0 \longrightarrow \Lambda \otimes_R S \longrightarrow \Lambda' \otimes_R S \longrightarrow (\Lambda'/\Lambda) \otimes_R S \longrightarrow 0,$$

where $(\Lambda'/\Lambda) \otimes_R S \neq 0$. Thus, $\Lambda \otimes_R S$ is a non-maximal S-order. Hence, if $\Lambda \otimes_R S$ is a maximal S-order in $A \otimes_F E$ then Λ is a maximal R-order in A.

Now suppose that R is an integrally closed Noetherian domain. Let Λ be a non-maximal R-order in A. Then there exists an R-order Λ' such that $\Lambda \subsetneq \Lambda' \subset A$. In particular, $\mathrm{Ann}_R(\Lambda'/\Lambda) \subsetneq R$. By [Bou89, Chapter VII §1.3 Theorem 2] R is a Noetherian Krull domain so, using [Bou89, Chapter VII §1.3 Definition $3\mathrm{AK}_{\mathrm{II}}$], we see that $R = \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$ where $\mathfrak{p}$ ranges through all the height 1 prime ideals of R and $R_{\mathfrak{p}}$ is the localisation of R at $\mathfrak{p}$. Hence there exists a height 1 prime ideal $\mathfrak{p}$ of R such that $\mathfrak{p} \not\subset \mathrm{Ann}_R(\Lambda'/\Lambda)$. Localising at $\mathfrak{p}$ we see that $\Lambda_{\mathfrak{p}} \subsetneq \Lambda'_{\mathfrak{p}} \subset A$. Using [Bou89, Chapter VII §1.3 Definition $3\mathrm{AK}_{\mathrm{I}}$], we see that $R_{\mathfrak{p}}$ is a discrete valuation ring. From this, we see that $S_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module of finite rank (since E/F is a finite field extension). By the above argument, this shows that $\Lambda_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{p}} = (\Lambda \otimes_R S)_{\mathfrak{p}}$ is a non-maximal $S_{\mathfrak{p}}$-order and so, by [Rei75, Corollary 11.2], $\Lambda \otimes_R S$ is a non-maximal R-order. Hence, if $\Lambda \otimes_R S$ is a maximal S-order in $A \otimes_F E$ then Λ is a maximal R-order in A. □

4.4 Semidirect products by an abelian group

Before proving the full strength of Theorem 4.1.2, we first prove the special case when the normal subgroup N is abelian.

Theorem 4.4.1. *Let R be an integrally closed Noetherian domain. Let G be a finite group with abelian normal subgroup N. Suppose that $F := \mathrm{Frac}(R)$ is a splitting field for N of characteristic 0. Let $\chi \in \mathrm{Irr}_F(N)$ with associated primitive central idempotent $e_\chi \in F[N]$. Let $I = I_G(e_\chi)$, let $e = \sum_{\chi' \in \mathrm{Orb}_G(\chi)} e_{\chi'} \in F[N]$ and let $k = |\mathrm{Orb}_G(\chi)|$. If $e_\chi \in R[N]$ and I may be written as a semidirect product $I = N \rtimes H$, then e is a central idempotent of $R[G]$ and there is an R-algebra isomorphism*

$$eR[G] \cong M_{k\times k}(R[H]).$$

Remark 4.4.2. If $G = N \rtimes H$ then N is a normal subgroup of I and $N \cap (I \cap H) = 1$ so $I = N \rtimes (H \cap I)$.

Proof of Theorem 4.4.1. Since $e_\chi \in R[N]$, Theorem 4.2.2 shows that e is a central idempotent of $R[G]$ and

$$eR[G] \cong M_{k\times k}(e_\chi R[I]).$$

Thus it suffices to show there is an R-algebra isomorphism $e_\chi R[I] \cong R[H]$.

By the definition of I, the element $e_\chi \in R[N]$ is a central idempotent of $R[I]$. Hence the R-module homomorphism

$$\varphi\colon R[H] \longrightarrow e_\chi R[I],$$

defined on H by $\varphi(h) = e_\chi h$, is an R-algebra homomorphism.

Since F is a splitting field (of characteristic 0) for the abelian group N and $\chi \in \mathrm{Irr}_F(N)$, we see that $e_\chi F[N] \cong F$. We note that $e_\chi R[N]$ is an R-order in $e_\chi F[N] \cong F$ (R-orders are defined because R is a Noetherian integral domain). As R is integrally closed, R is the only R-order in F. Therefore $e_\chi R[N] = e_\chi R = R e_\chi$.

Since $I = N \rtimes H$, we have $R[I] = \bigoplus_{h\in H} hR[N]$. Hence, using that e_χ is a central idempotent of $R[N]$, we see that

$$e_\chi R[I] = \bigoplus_{h\in H} e_\chi h R[N] = \bigoplus_{h\in H} e_\chi h R.$$

Thus φ gives a bijection between R-bases of the free R-modules $R[H]$ and $e_\chi R[I]$ and hence is an R-algebra isomorphism. □

4.5 Group cohomology and the Schur-Zassenhaus Theorem

For the convenience of the reader we will recall the definition of *2-cocycles*, *2-coboundaries* and the *second cohomology group*. This section is inspired by [Rog92, pg. 128] although the reader should note that here we will consider G acting on the right rather than the left. For a more comprehensive survey of group cohomology see [Ser79, Chapter VII] or [CR81, Sections 8B and 8C].

Definition 4.5.1. Let G be a finite group and let A be an abelian group with (right) action of G written as a^g for $a \in A$ and $g \in G$. We will write the group operations of G and A multiplicatively. Any function $\gamma\colon G \times G \to A$ satisfying

$$\gamma(x, yz)\gamma(y, z) = \gamma(xy, z)\gamma(x, y)^z \tag{4.4}$$

is called a *2-cocycle* of G with values in A. Using that A is abelian, one can check that the 2-cocycles of G with values in A form an abelian group under pointwise multiplication; this group is denoted by $Z^2(G, A)$.

Let $\psi\colon G \to A$ be any function. The function $\sigma\colon G \times G \to A$ defined by

$$\sigma(x, y) = \psi(xy)^{-1}\psi(x)^y\psi(y),$$

is called a *2-coboundary* of G with values in A. Using that A is abelian, one can check that the 2-coboundaries of G with values in A form an abelian group under pointwise multiplication; this group is denoted by $B^2(G, A)$. Let σ be a 2-coboundary. For $x, y, z \in G$

we see that

$$\begin{aligned}\sigma(x,yz)\sigma(y,z) &= \psi(xyz)^{-1}\psi(x)^{yz}\psi(yz)\psi(yz)^{-1}\psi(y)^{z}\psi(z)\\ &= \psi(xyz)^{-1}\psi(x)^{yz}\psi(y)^{z}\psi(z)\\ \sigma(xy,z)\sigma(x,y)^{z} &= \psi(xyz)^{-1}\psi(xy)^{z}\psi(z)(\psi(xy)^{-1}\psi(x)^{y}\psi(y))^{z}\\ &= \psi(xyz)^{-1}\psi(xy)^{z}\psi(z)(\psi(xy)^{z})^{-1}\psi(x)^{yz}\psi(y)^{z}\\ &= \psi(xyz)^{-1}\psi(x)^{yz}\psi(y)^{z}\psi(z),\end{aligned} \tag{4.5}$$

where the last equality follows because A is abelian. Therefore we see that

$$\sigma(x,yz)\sigma(y,z) = \sigma(xy,z)\sigma(x,y)^{z}$$

and thus σ is a 2-cocycle. Hence every 2-coboundary is a 2-cocycle.

The *second cohomology group* of G with values in A is an abelian group defined to be the quotient group

$$H^2(G,A) := Z^2(G,A)/B^2(G,A).$$

The following lemma gives information on the orders of elements of the second cohomology group.

Lemma 4.5.2. *If G is a finite group acting on an abelian group A then every element of $H^2(G,A)$ has order dividing $|G|$. Furthermore, if A has finite exponent, $\exp(A)$, then every element of $H^2(G,A)$ has order dividing $\exp(A)$.*

Proof. The proof is identical to that of [CR81, Lemma 8.39]. □

The elements of the second cohomology group appear naturally when considering group extensions. Consider the short exact sequence of groups

$$1 \longrightarrow A \longrightarrow B \longrightarrow G \longrightarrow 1, \tag{4.6}$$

where A is an abelian group (note that we do not require G or B to be abelian) and we view A as a subgroup of B. The group A can be given a structure of a G-module in the following way. Let $x \in G$. We define the action of x on A as follows. For a lift $b_x \in B$ of x, define the map

$$\begin{aligned}A &\longrightarrow A\\ a &\longmapsto a^x := b_x^{-1}ab_x.\end{aligned}$$

This action is well-defined because for any other choice of lift $b'_x \in B$ of x, we can write $b'_x = sb_x$, for some $s \in A$, and so, using that A is abelian, we see that

$${b'_x}^{-1}ab'_x = b_x^{-1}s^{-1}asb_x = b_x^{-1}ab_x.$$

One might ask whether the short exact sequence (4.6) splits. Working set theoretically, every short exact sequence splits. If $f\colon G \to B$ is a set theoretic splitting of (4.6) then $\gamma\colon G \times G \to A$, defined by

$$\gamma(x,y) = f(xy)^{-1}f(x)f(y), \tag{4.7}$$

measures how far away the splitting f is from being a group homomorphism. (We note that $\gamma(x,y)$ lies in A, because the function $B \to G$ is a group homomorphism.) We also note that $f(x) \in B$ is a lift of x, so we have

$$a^x = f(x)^{-1} a f(x) \tag{4.8}$$

for $a \in A$. Finally if f is a group homomorphism then γ is the trivial map.

For $x, y, z \in G$, from associativity in B (and G) and using (4.8), we have

$$\begin{aligned} f(x)(f(y)f(z)) &= f(x)(f(yz)\gamma(y,z)) \\ &= f(x)f(yz)\gamma(y,z) \\ &= f(xyz)\gamma(x,yz)\gamma(y,z), \\ (f(x)f(y))f(z) &= f(xy)\gamma(x,y)f(z) \\ &= f(xy)f(z)f(z)^{-1}\gamma(x,y)f(z) \\ &= f(xy)f(z)\gamma(x,y)^z \\ &= f(xyz)\gamma(xy,z)\gamma(x,y)^z. \end{aligned} \tag{4.9}$$

In particular, γ satisfies the identity (4.4); that is

$$\gamma(x,yz)\gamma(y,z) = \gamma(xy,z)\gamma(x,y)^z$$

and so is a 2-cocycle.

This argument can be reversed: if A is a G-module and $\gamma \in Z^2(G,A)$ then the set $B = G \times A$ with multiplication given by

$$(g,x)(h,y) = (gh, \gamma(g,h)x^h y),$$

is a group which fits in the short exact sequence

$$1 \longrightarrow A \longrightarrow B \longrightarrow G \longrightarrow 1,$$

we call B the extension of G by A corresponding to γ. We note that when γ is the trivial map, B is the semidirect product $G \rtimes A$.

One might ask how the choice of set theoretic splitting $f\colon G \to B$ of (4.6) affects the 2-cocycle. If $f'\colon G \to B$ is another splitting of (4.6) then $\psi\colon G \to A$, defined by

$$\psi(x) = f'(x)^{-1} f(x),$$

measures how different the two splittings f and f' are. (We note that $\psi(x)$ does indeed lie in A because the function $B \to G$ is a group homomorphism which both f and f' split.)

If γ and γ' are the 2-cocycles associated to the splittings f and f', respectively then

we see that

$$\begin{aligned}\gamma(x,y) &= f(xy)^{-1}f(x)f(y)\\ &= \psi(xy)^{-1}f'(xy)^{-1}f'(x)\psi(x)f'(y)\psi(y)\\ &= \psi(xy)^{-1}f'(xy)^{-1}f'(x)f'(y)\psi(x)^y\psi(y)\\ &= \psi(xy)^{-1}\gamma'(x,y)\psi(x)^y\psi(y)\\ &= \gamma'(x,y)\psi(xy)^{-1}\psi(x)^y\psi(y),\end{aligned}$$

where the third equality follows from (4.8) and the last equality follows because A is abelian and $\gamma'(x,y), \psi(xy) \in A$. In particular, γ and γ' differ in $Z^2(G,A)$ by a 2-coboundary.

Suppose that γ and γ' in $Z^2(G,A)$ differ by a 2-coboundary given by $\psi(xy)^{-1}\psi(x)^y\psi(y)$ for $x, y \in G$ and some function $\psi\colon G \to A$. Let B and B' be the extensions of G by A corresponding to γ and γ', respectively. Then there is a group isomorphism

$$\begin{aligned}B &\longrightarrow B'\\ (g,x) &\longmapsto (g,\psi(g)x).\end{aligned}$$

Note that the converse is not true: B and B' being isomorphic extensions of G by A does not imply that the corresponding 2-cocycles differ by a 2-coboundary.

Therefore we have shown that $H^2(G,A)$ classifies the groups B that fit into the short exact sequence

$$1 \longrightarrow A \longrightarrow B \longrightarrow G \longrightarrow 1.$$

This classification along with Lemma 4.5.2 can be used to prove the Schur-Zassenhaus Theorem in the case that the normal subgroup considered is abelian.

Theorem 4.5.3 (Schur-Zassenhaus)**.** *Let G be a finite group with normal subgroup N. If $|N|$ and $|G/N|$ are coprime then G is isomorphic to a semidirect product of N and G/N.*

Proof. Since N is a normal subgroup of G, there is a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1.$$

Assuming that N is an abelian group, the above discussion shows that the structure of G is determined by an element of the group $H^2(G/N,N)$. Assume that $|N|$ and $|G/N|$ are coprime. Then, using Lemma 4.5.2, we see that $H^2(G/N,N)$ is trivial. This means that G must be the semidirect product of N and G/N.

A full proof (when the normal subgroup N is not necessarily abelian) can be achieved by reducing to the case when N is abelian. See [Rob96, Theorem 9.1.2] for a complete proof of this theorem. □

4.6 Crossed product orders

We are now in a position to define crossed product orders. Let G be a finite group and let R be a commutative ring on which G acts trivially. The idea of the construction of the crossed product order is similar to the idea of how the second cohomology group classifies group extensions.

Definition 4.6.1. Let G be a finite group, let R be a commutative ring, and suppose that G acts on R via the trivial action. Suppose that $\gamma\colon G \times G \to R^\times$ is a function such that

$$\gamma(x, yz)\gamma(y, z) = \gamma(xy, z)\gamma(x, y),$$

for $x, y, z \in G$ (in other words, γ is a 2-cocycle). The *crossed product order* of R and G is defined to be the free R-module

$$R *_\gamma G = \bigoplus_{x \in G} u_x R,$$

where the symbols $\{u_x \mid x \in G\}$ form an R-basis for $R *_\gamma G$. And $R *_\gamma G$ is given the structure of an R-algebra with multiplication defined by

$$ru_x = u_x r \quad \text{and} \qquad\qquad u_x u_y = u_{xy}\gamma(x, y), \tag{4.10}$$

for $x, y \in G$ and $r \in R$. Associativity of multiplication in $R *_\gamma G$ follows from the 2-cocycle condition by reversing the argument in (4.9): for all $x, y, z \in G$ and $r, s, t \in R$ we see that

$$\begin{aligned}((u_x r)(u_y s))(u_z t) &= (u_{xy}\gamma(x, y)rs)(u_z t)\\ &= u_{xyz}\gamma(xy, z)\gamma(x, y)rst\\ &= u_{xyz}\gamma(x, yz)\gamma(y, z)rst\\ &= (u_x r)(u_{yz}\gamma(y, z)st)\\ &= (u_x r)((u_y s)(u_z t)).\end{aligned}$$

For more details see [Pas85, Section 1.2] or [CR81, Examples 8.33] (both these references use the terminology "twisted group ring/algebra").

Remark 4.6.2. If R is a Noetherian integral domain with field of fractions F of characteristic 0 then $R *_\gamma G$ is an R-order in $F *_\gamma G$. This is part of the reason for the name crossed product order.

Remark 4.6.3. A similar definition works for crossed products orders when the action of G on R is non-trivial.

Remark 4.6.4. If $\gamma, \gamma' \in Z^2(G, R^\times)$ have the same image in $H^2(G, R^\times)$ then there exists a function $\mu\colon G \to R^\times$ such that

$$\gamma(x, y) = \gamma'(x, y)\mu(xy)^{-1}\mu(x)\mu(y),$$

where $x, y \in G$. This induces an R-module isomorphism $\varphi\colon R *_\gamma G \to R *_{\gamma'} G$ given by $\varphi(u_x) = u'_x\mu(x)$ on the R-basis $\{u_x \mid x \in G\}$ and extended R-linearly. The R-module

isomorphism φ is in fact an R-algebra isomorphism because for $x, y \in G$ we have

$$\begin{aligned}\varphi(u_x)\varphi(u_y) &= u'_x\mu(x)u'_y\mu(y)\\ &= u'_xu'_y\mu(x)\mu(y)\\ &= u'_{xy}\gamma'(x,y)\mu(x)\mu(y)\\ &= u'_{xy}\mu(xy)\gamma'(x,y)\mu(xy)^{-1}\mu(x)\mu(y)\\ &= u'_{xy}\mu(xy)\gamma(x,y)\\ &= \varphi(u_{xy}\gamma(x,y))\\ &= \varphi(u_xu_y).\end{aligned}$$

In this case we say that $R *_\gamma G$ is *diagonally equivalent* to $R *_{\gamma'} G$. Consequently, the R-algebra $R *_\gamma G$ depends, up to isomorphism, only on the image of γ in $H^2(G, R^\times)$.

Remark 4.6.5. If $\gamma\colon G\times G \to R^\times$ is the trivial 2-cocycle (i.e., $\gamma(x,y) = 1$ for all $x, y \in G$) then there is an R-algebra isomorphism $R *_\gamma G \cong R[G]$ defined by $u_x \mapsto x$ for $x \in G$.

4.7 A cohomological description of well-behaved group rings

The following lemma will play a crucial role in the rest of this section.

Lemma 4.7.1. *Let Λ be a ring containing a subset*

$$\{e_{ij} \in \Lambda \mid i, j \in \{1, \dots, m\}\}$$

satisfying $\sum_{i=1}^m e_{ii} = 1_\Lambda$ and

$$e_{ij}e_{rs} = \begin{cases} e_{is} & \text{if } j = r,\\ 0 & \text{otherwise,}\end{cases} \tag{4.11}$$

for $i, j, r, s \in \{1, \dots, m\}$. If S is the centralizer of all these elements then there are ring isomorphisms

$$S \cong e_{11}\Lambda e_{11} \quad \text{and} \qquad \Lambda \cong M_{m\times m}(S).$$

Proof. This is [Pas85, Lemma 6.1.5]. □

Remark 4.7.2. The converse to Lemma 4.7.1 is also true. That is, if Λ and S are rings such that $\Lambda \cong M_{m\times m}(S)$ then there exists a subset $\{e_{ij} \in \Lambda \mid i, j \in \{1, \dots, m\}\}$ of Λ satisfying $\sum_{i=1}^m e_{ii} = 1$ and

$$e_{ij}e_{rs} = \begin{cases} e_{is} & \text{if } j = r,\\ 0 & \text{otherwise,}\end{cases}$$

for $i, j, r, s \in \{1, \dots, m\}$. For example one can take e_{ij} to be the matrix with 1 in position i, j and 0 everywhere else.

Theorem 4.7.3. *Let R be a commutative ring and let G be a finite group with normal subgroup N. Let Q be the total ring of fractions of R. Suppose that $e \in Q[N]$ is a central idempotent of $Q[G]$ such that:*

I *the action of G on $\mathfrak{Z}(eR[N])$ is trivial,*

II *there is an R-algebra isomorphism $eR[N] \cong M_{m\times m}(C)$, where $m \in \mathbb{Z}_{>0}$ and C is a commutative R-algebra, and*

III *there exists a (left) transversal X of N in G and a function $\varphi\colon X \to (eR[N])^\times$ such that $x\varphi(x)$ centralizes $eR[N]$ for all $x \in X$.*

Then there is a 2-cocycle $\gamma\colon G/N \times G/N \to C^\times$ such that

$$eR[G] \cong M_{m\times m}(C *_\gamma G/N).$$

Furthermore, if the inflation map on cohomology

$$\iota\colon H^2(G/N, C^\times) \longrightarrow H^2(G, C^\times) \tag{4.12}$$

is injective then the order of $\overline{\gamma} \in H^2(G/N, C^\times)$ divides m, where $\overline{\gamma}$ is the image of γ in $H^2(G/N, C^\times)$.

Remark 4.7.4. With a little more work Hypothesis I (saying that G acts trivially on $eR[N]$) may be removed. This requires that the definition of crossed product order is generalised to allow for an action of the group on the coefficient ring.

Remark 4.7.5. Suppose that G may be written as a semidirect product $G = N \rtimes H$. (In particular, by the Schur-Zassenhaus Theorem (see Theorem 4.5.3) this is always possible when $|N|$ and $|G/N|$ are coprime.) Then the short exact sequence

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G/N \longrightarrow 1$$

splits and so there is a section $\theta\colon G/N \to G$ such that $\pi \circ \theta$ is the identity on G/N. Moreover, θ induces a map on cohomology

$$\theta^*\colon H^2(G, C^\times) \longrightarrow H^2(G/N, C^\times).$$

and π induces $\pi^* = \iota$, the inflation map on cohomology given in (4.12). Therefore, $\theta^* \circ \iota$ is the identity on $H^2(G/N, C^\times)$ so ι is injective.

Remark 4.7.6. The 2-cocycle γ is defined explicitly in equation (4.16) in the proof below.

Proof of Theorem 4.7.3. The first part of this proof is inspired by [Rog92, Chapter XIII].

Each $g \in G$ may be written uniquely as $g = xn$ for some $x \in X$ and $n \in N$. Using this, we may extend the function $\varphi\colon X \to (eR[N])^\times$ to a function $\psi\colon G \to (eR[N])^\times$ by defining

$$\psi(xn) = n^{-1}\varphi(x).$$

Let $g \in G$; we may write $g = xn$ for some $x \in X$ and $n \in N$. Note ψ and multiplication by elements of N are related as follows: for $n' \in N$ we have

$$\begin{aligned}\psi(gn') = \psi(xnn') &= (nn')^{-1}\varphi(x) = n'^{-1}n^{-1}\varphi(x)\\ &= n'^{-1}\psi(xn) = n'^{-1}\psi(g).\end{aligned} \tag{4.13}$$

We also see that

$$g\psi(g) = xn\psi(xn) = xnn^{-1}\psi(x) = x\psi(x),$$

so $g\psi(g)$ centralizes $eR[N]$ for all $g \in G$ by hypothesis III. Recall that the action of G on $eR[N]$ is given by $\alpha^g = g^{-1}\alpha g$ for $g \in G$ and $\alpha \in eR[N]$. In particular, for $\alpha \in eR[N]$ and $g \in G$ we have

$$\begin{aligned} \alpha^g\psi(g) &= g^{-1}\alpha g\psi(g) \\ &= g^{-1}g\psi(g)\alpha \\ &= \psi(g)\alpha. \end{aligned} \tag{4.14}$$

We now define a function $\mu\colon G \times G \to (eR[N])^\times$ by

$$\mu(g,h) = \psi(gh)^{-1}\psi(h)\psi(g) = \psi(gh)^{-1}\psi(g)^h\psi(h), \tag{4.15}$$

for $g, h \in G$, where the second equality follows from (4.14). We note the similarities between μ and a 2-coboundary; the difference is that $(eR[N])^\times$ is not necessarily commutative. Using (4.14) and (4.15), for $\alpha \in eR[N]$ and $g, h \in G$ we note that

$$\begin{aligned} \mu(g,h)\alpha &= \psi(gh)^{-1}\psi(h)\psi(g)\alpha \\ &= \psi(gh)^{-1}\psi(h)\alpha^g\psi(g) \\ &= \psi(gh)^{-1}\alpha^{gh}\psi(h)\psi(g) \\ &= \alpha^{gh(gh)^{-1}}\psi(gh)^{-1}\psi(h)\psi(g) \\ &= \alpha\mu(g,h). \end{aligned}$$

From this, we see that $\mu(g,h) \in \mathfrak{Z}(eR[N])$ and so the image of μ is contained in $\mathfrak{Z}(eR[N])^\times$ and there is a function $\mu\colon G \times G \to \mathfrak{Z}(eR[N])^\times$.

We now check that μ is a 2-cocycle of G with values in $\mathfrak{Z}(eR[N])^\times$; the proof is similar to the proof that 2-coboundaries are 2-cocycles (see (4.5)). Given $g, h, k \in G$ we see that

$$\begin{aligned} \mu(gh,k)\mu(g,h) &= \psi(ghk)^{-1}\psi(gh)^k\psi(k)\psi(gh)^{-1}\psi(g)^h\psi(h) && \text{by (4.15)} \\ &= \psi(ghk)^{-1}\psi(gh)^k(\psi(gh)^{-1})^k\psi(g)^{hk}\psi(h)^k\psi(k) && \text{by (4.14)} \\ &= \psi(ghk)^{-1}\psi(g)^{hk}\psi(h)^k\psi(k) \\ &= \psi(ghk)^{-1}\psi(g)^{hk}\psi(hk)\psi(hk)^{-1}\psi(h)^k\psi(k) \\ &= \mu(g,hk)\mu(h,k) && \text{by (4.15).} \end{aligned}$$

Therefore, using hypothesis I (the action of G on $C \cong \mathfrak{Z}(eR[N])$ is trivial), μ is a 2-cocycle of G with values in $\mathfrak{Z}(eR[N])^\times$.

We now check that $\mu\colon G \times G \to \mathfrak{Z}(eR[N])^\times$ is constant on cosets of N. For $g, h \in G$

and $n_1, n_2 \in N$ we have

$$\begin{aligned}
\mu(gn_1, hn_2) &= \psi(gn_1hn_2)^{-1}\psi(hn_2)\psi(gn_1) && \text{by (4.15)}\\
&= \psi(gh(n_1)^h n_2)^{-1}\psi(hn_2)\psi(gn_1)\\
&= \psi(gh)^{-1}n_1^h n_2 n_2^{-1}\psi(h)n_1^{-1}\psi(g) && \text{by (4.13)}\\
&= \psi(gh)^{-1}n_1^h\psi(h)en_1^{-1}\psi(g) && \text{as } e = 1_{eR[N]}\\
&= \psi(gh)^{-1}n_1^h(en_1^{-1})^h\psi(h)\psi(g) && \text{by (4.14)}\\
&= \psi(gh)^{-1}\psi(h)\psi(g) && \text{as } e = 1_{eR[N]}\\
&= \mu(g,h) && \text{by (4.15).}
\end{aligned}$$

Therefore, using that $C \cong \mathfrak{Z}(eR[N])$, we see that there is a 2-cocycle γ of G/N with values in $C^\times$ such that under the inflation map $\iota\colon H^2(G/N, C^\times) \to H^2(G, C^\times)$ we have $\iota(\overline{\gamma}) = \overline{\mu'}$ (where μ' is μ composed with the isomorphism $\mathfrak{Z}(eR[N]) \cong C$ and bar denotes taking the image in the cohomology group).

Using that there is an R-algebra isomorphism $eR[N] \cong M_{m\times m}(C)$, computing reduced norms in (4.15) we see that

$$\begin{aligned}
\mu(g,h)^m &= \operatorname{nr}(\mu(g,h))1_{eR[N]}\\
&= \operatorname{nr}(\psi(gh)^{-1})\operatorname{nr}(\psi(g)^h)\operatorname{nr}(\psi(h))1_{eR[N]}\\
&= \operatorname{nr}(\psi(gh))^{-1}\operatorname{nr}(\psi(g))^h\operatorname{nr}(\psi(h))1_{eR[N]},
\end{aligned}$$

where the first equality follows from Proposition 3.9.3. Hence μ'^m (where μ' is μ composed with the isomorphism $\mathfrak{Z}(eR[N]) \cong C$) is a 2-coboundary and so $\iota(\overline{\gamma^m}) = 1_{H^2(G/N,C^\times)}$. If the inflation map ι on cohomology is injective then $\overline{\gamma^m} = 1_{H^2(G/N,C^\times)}$, so the order of $\overline{\gamma}$ in $H^2(G/N, C^\times)$ divides m.

The remainder of this proof follows that of [Pas85, Lemma 6.1.8]. Since there is an R-algebra isomorphism $eR[N] \cong M_{m\times m}(C)$ (hypothesis II), Remark 4.7.2 shows that there is a subset

$$U := \{e_{ij} \in eR[N] \mid i, j \in \{1, \dots, m\}\}$$

of $eR[N]$ such that $\sum_{i=1}^m e_{ii} = e$ and

$$e_{ij}e_{rs} = \begin{cases} e_{is} & \text{if } j = r,\\ 0 & \text{otherwise,}\end{cases}$$

for $i, j, r, s \in \{1, \dots, m\}$. The set U is also a subset of $eR[G]$ so, by Lemma 4.7.1, we have

$$eR[G] \cong M_{m\times m}(e_{11}R[G]e_{11}).$$

It remains to compute $e_{11}R[G]e_{11}$.

We may view $eR[N]$ as a C-algebra via the R-algebra isomorphism $eR[N] \cong M_{m\times m}(C)$. The ring C is the ring of scalars of the matrix ring $M_{m\times m}(C)$ and e_{11} can be thought of as a matrix with 1 in the top left hand corner and 0 everywhere else, so we see that

$e_{11}R[N]e_{11} = e_{11}C$. Because X is a (left) transversal of N in G, we see that

$$R[G] = \bigoplus_{x \in X} xR[N],$$

so, since $e \in Q[N] \cap \mathfrak{Z}(Q[G])$, we see that

$$eR[G] = \bigoplus_{x \in X} xeR[N] = \bigoplus_{x \in X} x\varphi(x)eR[N],$$

where the second equality follows because $\varphi(x)$ is a unit in $eR[N]$. Therefore, as e is a central idempotent of $Q[G]$ such that $e_{11}e = e_{11}$ and $e_{11} \in eR[N]$, we see that

$$\begin{aligned} e_{11}R[G]e_{11} &= \bigoplus_{x \in X} e_{11}x\varphi(x)eR[N]e_{11} \\ &= \bigoplus_{x \in X} x\varphi(x)e_{11}R[N]e_{11} \\ &= \bigoplus_{x \in X} x\varphi(x)e_{11}C. \end{aligned}$$

where the second equality follows from hypothesis III. In particular, $e_{11}R[G]e_{11}$ is a free C-module of rank $|G/N| = |X|$ with basis $\{x\varphi(x)e_{11} \mid x \in X\}$.

Again using that X is a (left) transversal of N in G, by the definition of the crossed product order (see 4.6.1), we see that

$$C *_\gamma G/N = \bigoplus_{x \in X} u_{xN}C,$$

where the symbols $\{u_{xN} \mid x \in X\}$ form a C-basis for $C *_\gamma G/N$. In particular, there is an C-module isomorphism

$$\theta \colon e_{11}R[G]e_{11} \longrightarrow C *_\gamma G/N,$$

given on the C-basis $\{xe_{11} \mid x \in X\}$ by $\theta(x\varphi(x)e_{11}) = u_{xN}$.

We now check that this is a ring homomorphism. Suppose that $x, y, z \in X$ such that $z^{-1}xy \in N$. We see that

$$\begin{aligned} \gamma(xN, yN) &= \mu(x, y) \\ &= \psi(zz^{-1}xy)^{-1}\psi(y)\psi(x) \\ &= \psi(z)^{-1}z^{-1}xy\psi(y)\psi(x) \\ &= \psi(z)^{-1}z^{-1}x\psi(x)y\psi(y) \\ &= \varphi(z)^{-1}z^{-1}x\varphi(x)y\varphi(y), \end{aligned} \tag{4.16}$$

where the last line follows because $x, y, z \in X$. Therefore, we see that

$$\begin{aligned}\theta(x\varphi(x)e_{11})\theta(y\varphi(y)e_{11}) &= u_{xN}u_{yN}\\ &= u_{zN}\gamma(xN, yN)\\ &= \theta(z\varphi(z)e_{11}\gamma(xN, yN))\\ &= \theta(z\varphi(z)e_{11}\psi(z)^{-1}z^{-1}x\psi(x)y\psi(y))\\ &= \theta(x\varphi(x)e_{11}y\varphi(y)e_{11}),\end{aligned}$$

where the forth equality follows from (4.16). Hence θ is a C-algebra isomorphism and so θ is an R-algebra isomorphism. □

Corollary 4.7.7. *Let R be a commutative ring, let G be a finite group and let Q be the total ring of fractions of R. Suppose that $G = N \rtimes H$ and suppose that $e \in Q[N]$ is a central idempotent of $Q[G]$ satisfying hypotheses I, II and III of Theorem 4.7.3. Recall the R-algebra C and $m \in \mathbb{Z}_{>0}$ from hypothesis II. If $|G/N|$ and m are coprime then there is an R-algebra isomorphism*

$$eR[G] \cong M_{m\times m}(C[H]).$$

Proof. Since $G = N \rtimes H$, by Remark 4.7.5, the inflation map

$$H^2(G/N, C^\times) \longrightarrow H^2(G, C^\times)$$

is injective. Therefore, applying Theorem 4.7.3, we see that there is an R-algebra isomorphism

$$eR[G] \cong M_{m\times m}(C *_\gamma G/N),$$

where $\gamma\colon G/N \to G/N \to C^\times$ is a 2-cocycle, with image $\overline{\gamma} \in H^2(G/N, R^\times)$ with order dividing m. By Lemma 4.5.2, we also see that the order of $\overline{\gamma}$ in $H^2(G/N, R^\times)$ divides $|G/N|$. Hence, the order of $\overline{\gamma}$ is 1 and, by Remarks 4.6.4 and 4.6.5, we see that $C *_\gamma G/N$ is diagonally equivalent to $C[G/N] \cong C[H]$. □

4.8 Well-behaved group rings

We will first recall the hypotheses of Theorem 4.7.3 and Corollary 4.7.7. Let R be a commutative ring with total ring of fractions Q and let G be a finite group with normal subgroup N. Suppose that $e \in Q[N]$ is a central idempotent of $Q[G]$ such that:

- I the action of G on $\mathfrak{Z}(eR[N])$ is trivial,
- II there is an R-algebra isomorphism $eR[N] \cong M_{m\times m}(C)$, where $m \in \mathbb{Z}_{>0}$ and C is a commutative R-algebra, and
- III there exists a transversal X of N in G and a function $\varphi\colon X \to (eR[N])^\times$ such that $x\varphi(x)$ centralizes $eR[N]$ for all $x \in X$.

A natural question is: when does a central idempotent $e \in Q[N]$ satisfying these hypotheses exist?

We first check that hypotheses I, II and III of Theorem 4.7.3 are compatible with the results of Theorem 4.4.1 on groups with an abelian normal subgroup.

Lemma 4.8.1. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and let G be a finite group with normal subgroup N. Suppose that F is a splitting field for N and $e \in R[N]$ is a primitive central idempotent of $F[N]$ and lies in $\mathfrak{Z}(R[G])$. If N is an abelian group then hypotheses I, II and III of Theorem 4.7.3 hold.*

Proof. As F is a splitting field of characteristic 0 for the abelian group N and e is a primitive central idempotent of $F[N]$, we see that $eF[N] \cong F$. We know that $eR[N]$ is isomorphic to an R-order in F. Since R is integrally closed, R is the only R-order in F and so $eR[N] \cong R$, which shows that hypotheses I and II of Theorem 4.7.3 hold. Let X be any transversal of N in G. If $\alpha \in eR[N] \cong R$ then $x^{-1}\alpha x = \alpha$ for any $x \in X$ because the action of G on R is trivial. Thus hypothesis III of Theorem 4.7.3 holds. □

We shall see that if the automorphism of $eR[N]$ induced by conjugation by an element of G is inner, then hypothesis III of Theorem 4.7.3 holds. The Skolem-Noether Theorem is a common way of showing that automorphisms of central simple algebras over a field are inner. We now recall a generalised version of the Skolem-Noether Theorem from [Isa80, Corollary 15].

Theorem 4.8.2. *Let R be a unique factorisation domain. If $\Lambda = M_{m\times m}(R)$ for some $m \in \mathbb{Z}_{>0}$ then every R-algebra automorphism of Λ is an inner automorphism.*

Remark 4.8.3. The hypotheses of Theorem 4.8.2 can be weakened. In particular, [AG60, Theorem 3.6] shows that result holds when R is a commutative ring such that every finitely generated projective R-module of rank 1 is free. In particular, this holds whenever R is a commutative local ring.

For a finite group G and commutative ring R we now provide an equivalent condition for the idempotent associated to an irreducible character of G to live in $R[G]$.

Lemma 4.8.4. *Let R be an integrally closed Noetherian domain and let G be a finite group. Suppose that $F := \mathrm{Frac}(R)$ is a splitting field for G of characteristic 0. Let $\chi \in \mathrm{Irr}_F(G)$. Then $e_\chi \in R[G]$ if and only if $\frac{\chi(1)}{|G|} \in R^\times$*

Proof. Clearly $\sum_{g\in G} \chi(g^{-1})g \in R[G]$ so if $\frac{\chi(1)}{|G|} \in R^\times$ then $e_\chi \in R[G]$. It remains to show the forward direction.

For a prime ideal $\mathfrak{p}$ of R, let $R_\mathfrak{p}$ denote the localisation of R at $\mathfrak{p}$. Abusing notation we will write $\mathfrak{p}$ for the unique maximal ideal $\mathfrak{p}_\mathfrak{p}$ of $R_\mathfrak{p}$. We note that R is a Noetherian Krull domain by [Bou89, Chapter VII §1.3 Theorem 2]. If $\frac{\chi(1)}{|G|} \in {R_\mathfrak{p}}^\times$ for all height 1 primes ideals $\mathfrak{p}$ of R then, using [Bou89, Chapter VII §1.3 Definition $3\mathrm{AK}_{\mathrm{II}}$], $\frac{\chi(1)}{|G|} \in R^\times$. Pick a height 1 prime ideal $\mathfrak{p}$ of R. We will consider two cases based on the characteristic of $R_\mathfrak{p}/\mathfrak{p}$.

First suppose that $R_\mathfrak{p}/\mathfrak{p}$ has characteristic 0. Let $s \in \mathbb{Z} \setminus \{0\}$. Since $R_\mathfrak{p}/\mathfrak{p}$ is a field of characteristic 0 there exists $r \in R_\mathfrak{p}$ and $m \in \mathfrak{p}$ such that $sr = 1 + m$. The ideal $\mathfrak{p}$ is the Jacobson radical of $R_\mathfrak{p}$ meaning $1 + m \in R_\mathfrak{p}^\times$, so $s \in {R_\mathfrak{p}}^\times$. This holds for all $s \in \mathbb{Z}$, so $\mathbb{Q}^\times \subset R_\mathfrak{p}^\times$. Therefore we see that $\frac{\chi(1)}{|G|} \in {R_\mathfrak{p}}^\times$.

Otherwise suppose that $R_\mathfrak{p}/\mathfrak{p}$ has characteristic $p > 0$. By [Bou89, Chapter VII §1.3 Definition $3\mathrm{AK}_{\mathrm{I}}$] $R_\mathfrak{p}$ is a discrete valuation ring. This part of the proof is inspired

by [JN16a, Lemma 2.1]. An element $g \in G$ is said to be p-singular if the order of g is divisible by p. Viewing $e_\chi := \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$ as an idempotent in $R_\mathfrak{p}[G]$, by [Kül94, Proposition 5], $\frac{\chi(1)}{|G|}\chi(g^{-1}) = 0$ for every p-singular element $g \in G$. (Note that [Kül94, Proposition 5] is only stated for complete discrete valuation rings. However after considering the embedding $R_\mathfrak{p}$ into its completion the result claimed is clear.) Hence the character χ vanishes on p-singular elements of G. Let P be a Sylow p-subgroup of G. Then χ vanishes on $P \setminus \{1\}$. Hence the multiplicity of the trivial character of P in the restriction χ_P is

$$\langle \chi_P, 1_P\rangle = \frac{\chi(1)}{|P|}.$$

Consequently $\chi(1) = |P|\langle \chi_P, 1_P\rangle$, so $v_\mathfrak{p}(\chi(1)) = v_\mathfrak{p}(|P|) = v_\mathfrak{p}(|G|)$ where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation on $R_\mathfrak{p}$ (this can be assumed to be the same valuation as that given in example 2.2.2). Thus $\frac{\chi(1)}{|G|} \in {R_\mathfrak{p}}^\times$. □

This can be used to deduce information about the structure of group rings.

Lemma 4.8.5. *Let R be a principal ideal domain with field of fractions F of characteristic 0 and let G be a finite group. Suppose that F is a splitting field for G and $e \in R[G]$ is a primitive central idempotent of $F[G]$. Then there is an R-algebra isomorphism $eR[G] \cong M_{m\times m}(R)$ for some $m \in \mathbb{Z}_{>0}$.*

Proof. First, as F has characteristic 0 and is a splitting field for G, we see that

$$eF[G] \cong M_{m\times m}(F)$$

for some $m \in \mathbb{Z}_{>0}$, so $eR[G]$ is isomorphic to an R-order in $M_{m\times m}(F)$. Furthermore, there is a character $\chi\colon G \to F$ such that $e = e_\chi$ and $\chi(1) = m$. As $e \in R[G]$, by Lemma 4.8.4 we see that $\frac{\chi(1)}{|G|} \in R^\times$.

Let Γ be a maximal R-order in $eF[G]$ containing $eR[G]$. By Jacobinski's central conductor formula [Jac66, Theorem 3] (see also [CR81, Theorem 27.13]) we see that

$$e\mathcal{F}(\Gamma, R[G]) = |G|m^{-1}\mathfrak{D}^{-1}(R/R) = R,$$

where $\mathfrak{D}^{-1}(R/R) = R$ is the inverse different of R relative to R and $\mathcal{F}(\Gamma, R[G])$ is the central conductor of Γ into $R[G]$ (as defined in Definition 3.3.1). Therefore we must have

$$eR[G] = \Gamma.$$

Using Lemma 1.9.14, we see that

$$eR[G] = \Gamma \cong M_{m\times m}(R).$$ □

Using Theorem 4.8.2 and Lemma 4.8.5 we obtain a condition on R for hypotheses I, II and III of Theorem 4.7.3 to be satisfied.

Lemma 4.8.6. *Let R be a principal ideal domain with field of fractions F of characteristic 0 and let G be a finite group with normal subgroup N. Suppose that F is a splitting field*

for N and $e \in R[N]$ is a primitive central idempotent of $F[N]$ and lies in $\mathfrak{Z}(R[G])$. Then hypotheses I, II and III of Theorem 4.7.3 hold.

Proof. Since e is a primitive central idempotent of $R[N]$, Lemma 4.8.5 shows that

$$eR[N] \cong M_{m\times m}(R).$$

Moreover, G acts trivially on R by definition of a group ring. Therefore hypotheses I and II of Theorem 4.7.3 are satisfied.

Let X be any transversal of N in G. We define a function $\varphi\colon X \to (eR[N])^\times$ as follows. For $x \in X$ there is an R-automorphism

$$\begin{aligned} eR[N] &\longrightarrow eR[N] \\ \alpha &\longmapsto \alpha^x = x^{-1}\alpha x. \end{aligned}$$

Using Theorem 4.8.2 (for the principal ideal domain R and $eR[N] \cong M_{m\times m}(R)$), this R-automorphism is inner. In particular, there exists $\beta_x \in (eR[N])^\times$ such that

$$\beta_x \alpha {\beta_x}^{-1} = \alpha^x,$$

for all $\alpha \in eR[N]$. Define $\varphi(x) = \beta_x$. We see that

$$x\varphi(x)\alpha = \alpha x\varphi(x)$$

for all $\alpha \in eR[N]$ and so $x\varphi(x)$ centralizes $eR[N]$, showing hypothesis III of Theorem 4.7.3 holds. □

4.9 Integral Clifford theory for semidirect products

Theorem 4.9.1. *Let R be a principal ideal domain and let G be a finite group. Suppose that $G = N \rtimes H$ and suppose that $F := \mathrm{Frac}(R)$ is a splitting field for N of characteristic 0. Let $\chi \in \mathrm{Irr}_F(N)$ with associated primitive central idempotent $e_\chi \in F[N]$. If $e_\chi \in R[N]$ then $e = \sum_{\chi' \in \mathrm{Orb}_G(\chi)} e_{\chi'} \in R[N]$ is a central idempotent of $R[G]$. Furthermore, if $\chi(1)$ and $|I_G(\chi)/N|$ are coprime then there is an R-algebra isomorphism*

$$eR[G] \cong M_{km\times km}(R[I_G(\chi)/N]),$$

where $k = |\mathrm{Orb}_G(\chi)|$ and $m = \chi(1)$.

Remark 4.9.2. The assumptions that G is a semidirect product and that $\chi(1)$ and $|I_G(\chi)/N|$ are coprime may be removed. With this weakened hypothesis, using Theorem 4.7.3, we instead deduce that

$$eR[G] \cong M_{km\times km}(R *_\gamma I_G(\chi)/N).$$

Remark 4.9.3. In certain cases the assumption in Theorem 4.9.1 that R is a principal ideal domain may also be weakened. For example, using the notation from Theorem 4.9.1,

if S (not necessarily a principal ideal domain) is an R-algebra then, by extension of scalars, we see that

$$\begin{aligned} eS[G] &\cong S \otimes_R eR[G] \\ &\cong S \otimes_R M_{km\times km}(R[I_G(\chi)/N]) \\ &\cong M_{km\times km}(S[I_G(\chi)/N]). \end{aligned}$$

Also note that in the case that N is abelian, Theorem 4.4.1 provides a version of Theorem 4.9.1 where R is not a principal ideal domain.

Proof of Theorem 4.9.1. By Theorem 4.2.2, $e := \sum_{\chi' \in \mathrm{Orb}_G(\chi)} e_{\chi'}$ is a central idempotent of $R[G]$ and there is an R-algebra isomorphism

$$eR[G] \cong M_{k\times k}(e_\chi R[I_G(\chi)]).$$

Here we have used that $I_G(\chi) = I_G(e_\chi)$.

The field F has characteristic 0 and is a splitting field for N, and e_χ is a primitive central idempotent of $R[N]$. Therefore, using Lemma 4.8.6, we see that hypotheses I, II and III of Theorem 4.7.3 hold for the group $I_G(\chi)$ with normal subgroup N and $e_\chi \in R[N]$.

Applying Corollary 4.7.7, there is an R-algebra isomorphism

$$e_\chi R[I_G(\chi)] \cong M_{m\times m}(R[I_G(\chi)/N]). \qquad \square$$

In the case that R is a principal ideal domain this gives us a generalisation of Theorem 4.4.1 that works in the case that the normal subgroup is not necessarily abelian.

Corollary 4.9.4. *Let R be a principal ideal domain and let G be a finite group. Suppose that $G = N \rtimes H$, suppose that $F := \mathrm{Frac}(R)$ is a splitting field for N of characteristic 0, and suppose that $|N|$ is invertible in R. If $\chi(1)$ and $|I_G(\chi)/N|$ are coprime, for each $\chi \in \mathrm{Irr}_F(N)$, then there is an R-algebra isomorphism*

$$R[G] \cong \prod_i M_{n_i\times n_i}(R[H_i]),$$

for some $n_i \in \mathbb{Z}_{>0}$ and subgroups H_i of H. In particular, this holds when either N is abelian or $|H|$ and $|N|$ are coprime.

Proof. Consider $\mathrm{Irr}_F(N)$ and recall the action of G given by $\chi^g(n) = \chi(gng^{-1})$ for $g \in G$ and $\chi \in \mathrm{Irr}_F(N)$.

Let $\chi \in \mathrm{Irr}_F(N)$. As $|N|$ is invertible in R, the associated idempotent

$$e_\chi := \frac{\chi(1)}{|N|} \sum_{n\in N} \chi(n^{-1})n$$

is in $R[N]$. By assumption $\chi(1)$ and $|I_G(\chi)/N|$ are coprime. Therefore, by Theorem 4.9.1, there is an R-algebra isomorphism

$$eR[G] \cong M_{km\times km}(R[I_G(\chi)/N]),$$

where $m = \chi(1)$ and $k = |\mathrm{Orb}_G(\chi)|$. Moreover, $I_G(\chi)/N \leq G/N \cong H$.

Taking the direct product over all the G-orbits in $\mathrm{Irr}_F(N)$ completes the proof. □

Remark 4.9.5. In Corollary 4.9.4 the sufficient conditions, that either N is abelian or $|H|$ and $|N|$ are coprime, are not necessary. For example, consider S_4, the symmetric group on four letters, which can be written as the semidirect product of A_4, the alternating group on four letters, and C_2. We note that the degrees of the irreducible complex characters of A_4 are $1, 1, 1$ and 3 which are all coprime to $|S_4/A_4| = 2$. Hence we see that the hypothesis of Corollary 4.9.4 holds, even though A_4 is not abelian and $|A_4| = 12$ is not coprime to $|S_4/A_4| = 2$.

Remark 4.9.6. Corollary 4.9.4 recovers [Rog92, Theorem XIII.16] which holds when R is a complete discrete valuation ring. Here we use that the Schur-Zassenhaus Theorem (see Theorem 4.5.3) implies that when $|G/N|$ and $|N|$ are coprime, G is a semidirect product $N \rtimes H$.

To apply Corollary 4.9.4 it is useful to have a criterion for when G is a semidirect product.

Lemma 4.9.7. *Let p be a prime number. If G is a finite group then the following are equivalent*

(i) p does not divide the order of the commutator subgroup of G,
(ii) $G = N \rtimes P$ where P is an abelian Sylow p-subgroup of G and
(iii) G has abelian Sylow p-subgroup with a normal p-complement.

Proof. Suppose that p does not divide the order of the commutator subgroup G' of G. Let P be a Sylow p-subgroup of G. Then $P \cap G' = \{1\}$ so $P \cong PG'/G'$ is a Sylow p-subgroup of the abelian group G/G'. Therefore

$$G/G' = PG'/G' \times H$$

for some (normal) subgroup H of G/G'. Hence the set $N = \{g \in G \mid gG' \in H\}$ is a normal subgroup of G such that $P \cap N = \{1\}$ and $G = NP$ (because $G/G' = (NG'/G')(PG'/G')$). Therefore $G = N \rtimes P$.

If $G = N \rtimes P$, where P is an abelian Sylow p-subgroup of G, then N is a normal p-complement of P in G.

Suppose that G has abelian Sylow p-subgroup P with a normal p-complement N. Then $G/N \cong P$ is abelian, meaning that $G' < N$. Hence $p \nmid |G'|$ as $p \nmid |N|$. □

Remark 4.9.8. Let p be a prime number, let R be a principal ideal domain and let G be a finite group. Suppose that G has a normal p-complement N and that $|N|$ is invertible in R. Suppose that $F := \mathrm{Frac}(R)$ is a splitting field for N of characteristic 0. Then $G = N \rtimes P$ for some Sylow p-subgroup P of G and, by Corollary 4.9.4,

$$R[G] \cong \prod_i M_{n_i \times n_i}(R[H_i]),$$

for some $n_i \in \mathbb{Z}_{>0}$ and subgroups H_i of P.

One of the corollaries to [DJ83, Theorem 1] shows that if R is a complete discrete valuation ring with residue field of characteristic p and $p \nmid |G'|$ then $R[G]$ is a direct product of matrix rings over commutative rings. In Lemma 4.9.7 we noted that $p \nmid |G'|$ if and only if G has an abelian Sylow p-subgroup P and a normal p-complement N. Therefore, with the extra condition that F is a splitting field for N, we have produced a more refined version of this corollary.

The following result gives a necessary and sufficient condition for the existence of a normal p-complement.

Theorem 4.9.9 (Frobenius)**.** *A finite group G possesses a normal p-complement if and only if one of the following conditions holds:*

1. $N_G(H)/C_G(H)$ is a p-group for every non-identity p-subgroup H of G,

2. $N_G(H)$ has a normal p-complement for every non-identity p-subgroup H of G,

where $C_G(H)$ is the centralizer of H in G and $N_G(H)$ is the normalizer of H in G.

Proof. For a proof of this see [Gor80, Theorem 7.4.5]. □

For $p \neq 2$, a theorem of Glauberman-Thompson [Gor80, Theorem 8.3.1] can be used to give other sufficient conditions for G to have a normal p-complement.

5 Computing denominator ideals using Clifford theory

5.1 Introduction

Throughout this section we let p denote a prime number. The aim of this chapter is to compute denominator ideals of group rings for certain finite p-groups using the results of Chapters 3 and 4. The main idea is that knowing information about the structure of a group ring gives us information about the denominator ideal of said group ring.

Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 (the characteristic 0 hypothesis may be weakened; see Section 3.6 for more details). We will compute denominator ideals for group rings $R[G]$ over several finite p-groups G, culminating in Theorem 5.5.1 which computes the denominator ideal for any group ring $R[G]$ over a finite p-group G with commutator subgroup of order p.

As a motivating example, we first consider the non-abelian p-group of order p^3 and exponent p.

Example 5.1.1. Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and fix a prime number p. Let $G = (Z \times A) \rtimes B$, where $Z = \langle z \mid z^p \rangle$, $A = \langle a \mid a^p \rangle$, $B = \langle b \mid b^p \rangle$ and the action of B on $Z \times A$ is given by $z^b = z$ and $a^b = za$. Then G is the non-abelian group of order p^3 and exponent p, and $G' = Z = Z(G)$

Let e_Z be the trace idempotent of Z in $F[G]$, so e_Z is the maximal level-1 idempotent of $F[G]$. Consider the idempotent $(1 - e_Z)e_A$ in $F[G]$. Let G act on $F[G]$ on the right by conjugation. A calculation (the details of which are given in the proof of Claim 5.2.4) shows that

$$\mathcal{E} := \mathrm{Orb}_G((1 - e_Z)e_A) = \{(1 - e_Z)e_{\langle z^i a \rangle} \mid i = 0, \ldots, p - 1\}$$

is a set of orthogonal idempotents (note that these are non-central in $F[G]$) and

$$\sum_{e \in \mathcal{E}} e = (1 - e_Z).$$

It is easy to check that $\mathrm{Stab}_G((1 - e_Z)e_A) \supset Z \times A$ and so, using the Orbit-Stabilizer Theorem, we see that

$$I := I_G((1 - e_Z)e_A) = \mathrm{Stab}_G((1 - e_Z)e_A) = Z \times A.$$

Therefore, by Theorem 4.2.2, there is an injection of R-algebras given by

$$(1 - e_Z)R[G] \longrightarrow M_{p \times p}((1 - e_Z)e_A R[I]) \tag{5.1}$$

which induces an isomorphism of F-algebras after extending scalars. We will now show that this map restricts to an isomorphism on centres.

On centres (5.1) induces the following injection of R-algebras given by the composition

$$\varphi\colon \mathfrak{Z}((1-e_Z)R[G]) \longrightarrow \mathfrak{Z}\left(M_{p\times p}((1-e_Z)e_AR[I])\right) \cong (1-e_Z)e_AR[I],$$

where the isomorphism follows because I is abelian. Let $x \in (1-e_Z)e_AR[I]$. By Lemma 4.1.3, we see that $e_AR[I] = e_AR[Z\times A] \cong R[Z]$ and so $x = (1-e_Z)e_Ay$ for some $y \in R[Z]$. Let T be a left transversal of I in G. We see that

$$\sum_{h\in T} x^h = \sum_{h\in T} \left((1-e_Z)e_Ay\right)^h = (1-e_Z)\sum_{h\in T} {e_A}^h y = (1-e_Z)y \in \mathfrak{Z}((1-e_Z)R[G]).$$

Hence, the function

$$\begin{aligned}\psi\colon (1-e_Z)e_AR[I] &\longrightarrow \mathfrak{Z}((1-e_Z)R[G])\\ x &\longmapsto \sum_{h\in T} x^h,\end{aligned}$$

is well-defined. Using Corollary 4.2.4, ψ is an injection and ψ is a left inverse of φ. Hence φ and ψ are mutually inverse meaning that (5.1) restricts to an isomorphism on centres. Therefore, Corollary 3.4.4 shows that

$$(1-e_Z)\mathcal{H}(R[G]) \supset \mathfrak{Z}((1-e_Z)R[G]) \cap \mathfrak{Z}(R[G]).$$

By Corollary 3.6.2 we have

$$\mathcal{H}(R[G]) = \mathrm{Tr}_Z\, R[G] \oplus (1-e_Z)\mathcal{H}(R[G]).$$

Thus, as $\mathcal{H}(R[G]) \subset \mathfrak{Z}(R[G])$, we see that

$$(1-e_Z)\mathcal{H}(R[G]) \subset (1-e_Z)\mathfrak{Z}(R[G]) \cap \mathfrak{Z}(R[G]).$$

Therefore we see that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_Z\, R[G] \oplus \left(\mathfrak{Z}((1-e_Z)R[G]) \cap \mathfrak{Z}(R[G])\right).$$

By Lemma 3.6.1, we note that

$$(1-e_Z)R[G] \cap R[G] = \sum_{i=0}^{p-1}(1-z^i)R[G] = (1-z)R[G],$$

where the last equality follows because $(1-z^i) = (1-z)\sum_{j=0}^{i-1} z^j$. Thus, we see that

$$\begin{aligned}\mathfrak{Z}((1-e_Z)R[G]) \cap \mathfrak{Z}(R[G]) &= ((1-e_Z)R[G] \cap R[G]) \cap \mathfrak{Z}(F[G])\\ &= (1-z)R[G] \cap \mathfrak{Z}(F[G])\\ &= (1-z)\mathfrak{Z}((1-e_Z)R[G]),\end{aligned}$$

where the first equality follows from Lemma 1.9.8 and last equality follows by Corollary 1.9.10. In particular, we see that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_Z\, R[G] \oplus (1-z)\mathfrak{Z}((1-e_Z)R[G]).$$

We note that this agrees with the computation of the denominator ideal for $\mathbb{Z}[G]$ in Example 3.6.4. We also note that the subgroup A of G is not special, the same argument applied to each subgroup $\langle a^i b\rangle < G$ leads to an identical result.

Remark 5.1.2. Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and fix a prime number p. Let $n \in \mathbb{Z}_{>0}$ and let $G = (Z \times A) \rtimes B$, where $Z = \langle z \mid z^p\rangle$, $A = \langle a \mid a^p\rangle$, $B = \langle b \mid b^{p^n}\rangle$ and the action of B on A is given by $z^b = z$ and $a^b = za$. Then essentially the same argument as used in Example 5.1.1, with the subgroup A and idempotent $(1-e_Z)e_A$, shows that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_Z\, R[G] \oplus (1-z)\mathfrak{Z}((1-e_Z)R[G]).$$

Remark 5.1.3. Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and fix a prime number p. The method in Example 5.1.1 may also be used to compute the denominator ideal of group rings over the non-abelian p-group of order p^3 and exponent p^2. More explicitly, let $G = A \rtimes B$, where $A = \langle a \mid a^{p^2}\rangle$, $B = \langle b \mid b^p\rangle$ and the action of B on A is given by $a^b = a^{p+1}$. Then essentially the same argument as used in Example 5.1.1, with the subgroup B and idempotent $(1-e_{\langle a^p\rangle})e_B$, shows that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'}\, R[G] \oplus (1-a^p)\mathfrak{Z}((1-e_{G'})R[G]).$$

Again, this agrees with the computation of the denominator ideal for $\mathbb{Z}[G]$ in Example 3.6.4.

Recall the notation in Example 5.1.1. The argument in Example 5.1.1 can be roughly split into three steps.

- The first step is using knowledge of the subgroups A and $Z = [G, A]$ to show that $(1-e_Z)R[G]$ is contained within a $p \times p$ matrix ring over the commutative group ring $(1-e_Z)e_H R[Z \times A]$.
- The second step is showing that

$$\mathfrak{Z}((1-e_Z)e_A R[Z \times A]) = \mathfrak{Z}((1-e_Z)R[G]).$$

- The final step is amalgamating this information and computing the denominator ideal of $R[G]$.

Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and let G be a finite p-group. The first step will be generalised in Lemma 5.2.1, assuming that a subgroup $H < G$ satisfying certain properties can be found. The second step will be generalised in Lemma 5.2.5, requiring the additional assumption that $|G'| = p$. The final step will be generalised in Proposition 5.3.1 and Corollary 5.3.4 using an induction argument. In addition to requiring that $|G'| = p$, Proposition 5.3.1 and Corollary 5.3.4

also require a fairly strict technical condition on the structure of G to ensure that a subgroup H of G exists to which Lemma 5.2.1 may be applied. In Theorem 5.5.1 we remove the technical condition on the structure of G. This will give us a method of computing the denominator ideal of all group rings over finite p-groups with commutator subgroup of order p.

5.2 Lemmas for induction on finite p-groups

Let R be an integrally closed Noetherian domain of characteristic 0 and let G be a finite p-group. The idea of this section is to provide specialised versions of Theorem 4.2.2 and Corollary 4.2.4 that may be applied to certain idempotents in the group ring $R[G]$.

Lemma 5.2.1. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0, fix a prime number p and let G be a finite p-group. Let H be a subgroup of G of order p, let*

$$\Delta = [G, H] = \langle [g, h] \mid g \in G, h \in H \rangle$$

and let $I = I_G((1 - e_\Delta)e_H)$. If $|\Delta| = p$ then $\Delta \leq Z(G)$, $|G : I| = p$ and there is an injection of R-orders

$$(1 - e_\Delta)R[G] \longrightarrow M_{p\times p}((1 - e_\Delta)e_H R[I]),$$

which induces an isomorphism of F-algebras after extending scalars.

Remark 5.2.2. The condition that $|\Delta| = p$ does not always hold. Consider the group

$$G = (Y \times Z \times A_Y \times A_Z) \rtimes B$$

where Y, Z, A_Y, A_Z and B are groups of order p generated by y, z, a_y, a_z and b respectively, and the action of B is given by $[b, y] = [b, z] = 1$, $[b, a_y] = y$ and $[b, a_z] = z$. We note that B is a subgroup of order p with $[G, B] = \langle y, z \rangle$ which has order p^2.

Proof of Lemma 5.2.1. We first prove that $\Delta = [G, H]$ is contained within $Z(G)$. Given $g_1, g_2 \in G$ and $h \in H$ we see that

$$\begin{aligned} g_1[g_2, h]g_1^{-1} &= g_1 g_2 h g_2^{-1} h^{-1} g_1^{-1} = (g_1 g_2)h(g_1 g_2)^{-1} g_1 h^{-1} g_1^{-1} \\ &= ((g_1 g_2)h(g_1 g_2)^{-1} h^{-1})(h g_1 h^{-1} g_1^{-1}) = [g_1 g_2, h][g_1, h]^{-1}. \end{aligned}$$

In particular, this shows that $\Delta = [G, H]$ is normal in G. Hence, by [JL01, Lemma 26.1(1)] (which tells us that the intersection of a non-trivial normal subgroup of a finite p-group with the centre of said p-group is non-trivial), we see that $\Delta \cap Z(G)$ is non-trivial. Thus, because Δ has prime order, we see that $\Delta \leq Z(G)$.

Claim 5.2.3. *Fix a generator h of H. Consider the map $\theta_h \colon G \to \Delta$ given by $g \mapsto [g, h]$ for $g \in G$. Then θ_h is a surjective group homomorphism.*

Proof. Given $g_1, g_2 \in G$ we see that

$$\begin{aligned}[g_1, h][g_2, h] &= g_1 h {g_1}^{-1} h^{-1} [g_2, h] = g_1 [g_2, h] h {g_1}^{-1} h^{-1} \\ &= g_1 g_2 h {g_2}^{-1} h^{-1} h {g_1}^{-1} h^{-1} = [g_1 g_2, h],\end{aligned} \tag{5.2}$$

where the second equality follows because $\Delta \leq Z(G)$. This shows that θ_h is a group homomorphism. By symmetry, given $g \in G$ and $h_1, h_2 \in H$ we see that

$$[g, h_1][g, h_2] = [g, h_1 h_2]. \tag{5.3}$$

Let $\delta \in [G, H]$. First, if $\delta = 1$ then $\delta = [1, h]$. Otherwise $\delta \neq 1$ and there exist $n \in \mathbb{Z}_{>0}$, $g_1, \ldots, g_n \in G$, $h_1, \ldots, h_n \in H$ and $k_1, \ldots, k_n \in \mathbb{Z}$ such that

$$\delta = \prod_{i=1}^{n} [g_i, h_i]^{k_i}.$$

Since h generates H, there exist $m_1, \ldots, m_n \in \mathbb{Z}_{>0}$ such that $h_i = h^{m_i}$ for $i = 1, \ldots, n$. Thus we see that

$$\delta = \prod_{i=1}^{n} [g_i, h^{m_i}]^{k_i} = \prod_{i=1}^{n} [g_i, h]^{m_i k_i} = \left[\prod_{i=1}^{n} g_i^{k_i m_i}, h \right],$$

where the last two equalities follow by (5.3) and (5.2), respectively. This shows that the map θ_h is surjective. This completes the proof of Claim 5.2.3. □

Consider the right action of G on $F[G]$ by conjugation; in particular, for $x \in F[G]$ and $g \in G$, let $x^g = g^{-1} x g$. Let $\mathcal{E} = \mathrm{Orb}_G((1 - e_\Delta) e_H)$. Let h be a generator of H. By Claim 5.2.3, the map θ_h is surjective and so, for each $\delta \in \Delta$, there exists $b_\delta \in G$ such that $[b_\delta, h] = \delta^{-1}$. In particular, a short calculation shows that $(1 - e_\Delta) e_H^{b_\delta} = (1 - e_\Delta) e_{\langle \delta h \rangle}$. Therefore there is a bijection

$$\begin{aligned}\varphi \colon \Delta &\to \mathcal{E} \\ \delta &\mapsto (1 - e_\Delta) e_{\langle \delta h \rangle}.\end{aligned}$$

Claim 5.2.4. *The set $\mathcal{E}$ is a set of (central) orthogonal idempotents in $F[\Delta \times H]$ and*

$$\sum_{e \in \mathcal{E}} e = 1 - e_\Delta.$$

Proof of Claim 5.2.4. It is clear that the elements of $\mathcal{E}$ are idempotents in $F[\Delta \times H]$. Let $\delta_1, \delta_2 \in \Delta$. We see that

$$\begin{aligned}\mathrm{Tr}_{\langle \delta_1 h \rangle} \mathrm{Tr}_{\langle \delta_2 h \rangle} &= \sum_{i,j=0}^{p-1} (\delta_1 h)^i (\delta_2 h)^j = \sum_{i,j=0}^{p-1} \delta_1^i \delta_2^j h^{i+j} = \sum_{i,j=0}^{p-1} \delta_1^i \delta_2^{j-i} h^j \\ &= \sum_{i=0}^{p-1} (\delta_1 \delta_2^{-1})^i \mathrm{Tr}_{\langle \delta_2 h \rangle} = \begin{cases} p \, \mathrm{Tr}_{\langle \delta_2 h \rangle} & \text{if } \delta_1 = \delta_2, \\ \mathrm{Tr}_\Delta \mathrm{Tr}_{\langle \delta_2 h \rangle} & \text{if } \delta_1 \neq \delta_2, \end{cases}\end{aligned}$$

where the third equality follows by relabelling j and the last equality follows because Δ is a group of order p and so is generated by any non-identity element. Noting that $(1-e_\Delta)\operatorname{Tr}_\Delta = 0$, we see that

$$\varphi(\delta_1)\varphi(\delta_2) = \begin{cases} \varphi(\delta_1) & \text{if } \delta_1 = \delta_2, \\ 0 & \text{if } \delta_1 \neq \delta_2. \end{cases}$$

This proves that the idempotents in $\mathcal{E}$ are orthogonal.

We now show that $\sum_{e\in\mathcal{E}} e = (1-e_\Delta)$. We see that

$$\sum_{e\in\mathcal{E}} e = \sum_{\delta\in\Delta} \varphi(\delta) = (1-e_\Delta)\frac{1}{p}\sum_{i=0}^{p-1}\sum_{\delta\in\Delta}\delta^i h^i.$$

Since $\Delta \cong C_p$, for $i \in \{0,\dots,p-1\}$ we see that

$$\sum_{\delta\in\Delta}\delta^i = \begin{cases} \operatorname{Tr}_\Delta & \text{if } i \neq 0, \\ |\Delta| = p & \text{if } i = 0. \end{cases}$$

Recalling that $(1-e_\Delta)\operatorname{Tr}_\Delta = 0$, we see that $\sum_{e\in\mathcal{E}} e = (1-e_\Delta)$. This completes the proof of Claim 5.2.4. □

Using Claim 5.2.4, we may apply Theorem 4.2.2 to see that there is an injection of R-algebras

$$(1-e_\Delta)R[G] \longrightarrow M_{p\times p}((1-e_\Delta)e_H R[I]),$$

where $I = I_G((1-e_\Delta)e_H)$. Furthermore, we note that $I = \operatorname{Stab}_G((1-e_\Delta)e_H)$ so by the Orbit-Stabilizer Theorem

$$|G:I| = |\mathcal{E}| = |\Delta| = p.$$

This completes the proof of Lemma 5.2.1. □

Lemma 5.2.5. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0, fix a prime number p and let G be a finite p-group. Let H be a subgroup of G of order p, let*

$$\Delta = [G,H] = \langle [g,h] \mid g \in G, h \in H\rangle$$

and let $I = I_G((1-e_\Delta)e_H)$. If Δ and G' have order p then the injection of R-orders

$$(1-e_\Delta)R[G] \longrightarrow M_{p\times p}((1-e_\Delta)e_H R[I])$$

from Lemma 5.2.1 restricts to an isomorphism on centres.

Proof. It is clear that $\Delta \leq G'$ so $\Delta = G'$. The injection of R-orders

$$(1-e_\Delta)R[G] \longrightarrow M_{p\times p}((1-e_\Delta)e_H R[I])$$

induces the following R-algebra homomorphism on centres

$$\begin{aligned}\varphi\colon \mathfrak{Z}((1-e_\Delta)R[G]) &\longrightarrow \mathfrak{Z}((1-e_\Delta)e_H R[I])\\ x &\longmapsto e_H x e_H.\end{aligned}$$

Note we have used the canonical isomorphism

$$\mathfrak{Z}(M_{p\times p}((1-e_\Delta)e_H R[I])) \cong \mathfrak{Z}((1-e_\Delta)e_H R[I]).$$

Let $b \in G$ be a lift of a generator of G/I and let $T = \{b^0, b^1, \ldots, b^{p-1}\}$. Using Claim 5.2.3, a quick calculation shows that T is a left transversal of I in G. Hence, by Corollary 4.2.4, we see that φ has left inverse

$$\begin{aligned}\psi\colon \mathfrak{Z}((1-e_\Delta)e_H R[I]) &\longrightarrow \mathfrak{Z}((1-e_\Delta)F[G])\\ x &\longmapsto \sum_{g\in T} x^g.\end{aligned}$$

Thus, $\operatorname{Im}(\psi) \supset \mathfrak{Z}((1-e_\Delta)R[G])$

Let h be a generator of H and let $\delta = [b,h]^{-1} \in \Delta$. Let $\mathcal{C}_I$ be the set of conjugacy classes of I. Let $C \in \mathcal{C}_I$ and let $\operatorname{Tr}_C = \sum_{g\in C} g$. Since $I' \leq G' = \Delta \leq Z(G)$, we see that either $C = g\Delta$ for some $g \in I$ or $C = \{g\}$ for some $g \in I$. In the former case, $(1-e_\Delta)e_H \operatorname{Tr}_C = 0$; in particular, $\psi((1-e_\Delta)e_H \operatorname{Tr}_C) \in \mathfrak{Z}((1-e_\Delta)R[G])$. In the latter case, since $\Delta = G'$, we see that $(\operatorname{Tr}_C)^b = g^b = \delta^r g$ for some $r \in \{0,\ldots,p-1\}$. In particular, we see that

$$\begin{aligned}\sum_{i=0}^{p-1} ((1-e_\Delta)e_H \operatorname{Tr}_C)^{b^i} &= \frac{1}{p}(1-e_\Delta)\sum_{i=0}^{p-1}\delta^{ir} g \sum_{j=0}^{p-1}\delta^{ij}h^j\\ &= \frac{1}{p}(1-e_\Delta)\sum_{j=0}^{p-1} gh^j \sum_{i=0}^{p-1}\delta^{i(r+j)}\\ &= (1-e_\Delta)gh^{-r},\end{aligned}$$

where the last equality follows because

$$\sum_{i=0}^{p-1}\delta^{i(r+j)} = \begin{cases} p & \text{if } j = -r\\ \operatorname{Tr}_\Delta & \text{otherwise.}\end{cases}$$

Therefore, $\psi((1-e_\Delta)e_H \operatorname{Tr}_C) \in \mathfrak{Z}((1-e_\Delta)R[G])$. Since $I' \leq \Delta$ and $H \leq Z(I)$, we see that $\{(1-e_\Delta)e_H \operatorname{Tr}_C \mid C \in \mathcal{C}_I\}$ is a generating set for $\mathfrak{Z}((1-e_\Delta)e_H R[I])$ as an R-module. Therefore, we see that $\operatorname{Im}(\psi) \subset \mathfrak{Z}((1-e_\Delta)R[G])$.

Therefore, $\operatorname{Im}(\psi) = \mathfrak{Z}((1-e_\Delta)R[G])$ and, since ψ is a left inverse to φ, we see that φ is an isomorphism. Thus the map

$$(1-e_\Delta)R[G] \longrightarrow M_{p\times p}((1-e_\Delta)e_H R[I])$$

restricts to an isomorphism on centres. □

5.3 Denominator ideals of group rings over certain finite p-groups with commutator subgroup of order p

Proposition 5.3.1. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0, fix a prime number p and let G be a finite p-group. Suppose that every element of ${}^{G}\!/_{Z(G)}$ has a lift in G of order p. If the commutator subgroup of G has order p then*

$$(1 - e_{G'})\mathcal{H}(R[G]) \supset \mathfrak{Z}((1 - e_{G'})R[G]) \cap \mathfrak{Z}(R[G]).$$

Remark 5.3.2. The condition that every element of ${}^{G}\!/_{Z(G)}$ has a lift in G of order p is stronger than necessary. If one is interested in results on the structure of $R[G]$ then this condition may be weakened (for examples of this see Remarks 5.1.2 and 5.1.3) but not removed entirely (see Example 5.3.5). For the purpose of computing denominator ideals, we will see that this condition may be removed entirely (see Remark 5.3.7 and Theorem 5.5.1).

Proof of Proposition 5.3.1. The idea of this proof is to show that for some $n \in \mathbb{Z}_{>0}$ there is an injection of R-algebras

$$(1 - e_{G'})R[G] \longrightarrow M_{n\times n}(\mathfrak{Z}((1 - e_{G'})R[G])), \tag{5.4}$$

which restricts to the canonical identification on centres and induces an isomorphism of F-algebras after extending scalars. Then Corollary 3.4.4 gives a lower bound for $\mathcal{H}(R[G])$.

For the purposes of this proof we will say that a group G satisfies the lifting condition if every non-identity element of ${}^{G}\!/_{Z(G)}$ has a lift in G of order p. To show that (5.4) holds we will induct on the order of ${}^{G}\!/_{Z(G)}$ using Lemmas 5.2.1 and 5.2.5. We will in fact prove the following slightly stronger claim.

Claim 5.3.3. *Let G be a finite p-group with $|G'| \leq p$ such that G satisfies the lifting condition. Let*

$$f_G = \begin{cases} 1 & \text{if } G \text{ is abelian,} \\ 1 - e_{G'} & \text{otherwise.} \end{cases}$$

Then there exists $n \in \mathbb{Z}_{>0}$ and an injection of R-algebras

$$f_G R[G] \longrightarrow M_{n\times n}(\mathfrak{Z}(f_G R[G])), \tag{5.5}$$

which restricts to the canonical identification on centres and induces an isomorphism of F-algebras after extending scalars.

Proof. For the base case of the induction we note that if G is a finite p-group with $\left|{}^{G}\!/_{Z(G)}\right| = 1$ then G is abelian and (5.5) holds with $n = 1$. Now fix $k > 1$ and assume that if I is a finite p-group with $|I'| \leq p$ such that I satisfies the lifting condition and $\left|{}^{I}\!/_{Z(I)}\right| < k$, then there exists $n \in \mathbb{Z}_{>0}$ and an injection of R-algebras

$$f_I R[I] \longrightarrow M_{n\times n}(\mathfrak{Z}(f_I R[I])),$$

which restricts to the canonical identification on centres and induces an isomorphism of F-algebras after extending scalars.

Let G be a finite p-group with $|G'| = p$ such that G satisfies the lifting condition and $\left|{}^{G}\!/_{Z(G)}\right| = k$. Let $\overline{h}$ be a non-identity element of ${}^{G}\!/_{Z(G)}$ and pick a lift $h \in G$ of $\overline{h}$ with order p. Consider the subgroup $H = \langle h \rangle < G$. Since $h \notin Z(G)$ and $G' \cong C_p$, we see that $[H, G] = G' \cong C_p$. Let $I = I_G((1 - e_{G'})e_H)$. Then, using Lemma 5.2.5, there is an injection of R-algebras

$$(1 - e_{G'})R[G] \longrightarrow M_{p\times p}((1 - e_{G'})e_H R[I]) \tag{5.6}$$

which restricts to an isomorphism on centres and induces an isomorphism of F-algebras after extending scalars. Since $I < G$, we see that $I' \leq G'$ and so because $|G'| = p$ we see that either I is abelian or $I' = G'$; in either case $f_I(1 - e_{G'}) = (1 - e_{G'}) = f_G$ and $|I'| \leq p$.

Since every element of $Z(G)$ commutes with every element of H we see that $Z(G) \leq I$ and so $Z(I) \geq Z(G)$. Hence ${}^{I}\!/_{Z(I)}$ is a quotient of ${}^{I}\!/_{Z(G)}$. Let $g \in I \setminus Z(I)$. Then $gZ(G)$ is a non-identity element of ${}^{I}\!/_{Z(G)}$ so there exists $g' \in G$ of order p such that $gZ(G) = g'Z(G)$. Since $Z(G) \leq I$ we see that $g' \in I$. Therefore, I satisfies the lifting condition.

Furthermore, as $I \lneq G$, we see that ${}^{I}\!/_{Z(G)} \lneq {}^{G}\!/_{Z(G)}$ and so $\left|{}^{I}\!/_{Z(I)}\right| \leq \left|{}^{I}\!/_{Z(G)}\right| < k$ (it can be shown that the first inequality is also strict but this is not needed here). Thus, by the induction hypothesis, for some $n \in \mathbb{Z}_{>0}$ there is an injection of R-algebras

$$f_I R[I] \longrightarrow M_{n\times n}(\mathfrak{Z}(f_I R[I]))$$

which restricts to the canonical identification of centres and induces an isomorphism of F-algebras after extending scalars.

After multiplying by the central idempotent $(1 - e_{G'})e_H$ of $F[I]$ (this is central by the definition of I), we have an injection of R-algebras

$$(1 - e_{G'})e_H R[I] \longrightarrow M_{n\times n}(\mathfrak{Z}((1 - e_{G'})e_H R[I]))$$

which induces an isomorphism of F-algebras after extending scalars. The isomorphism induced on centres from (5.6) gives an R-algebra isomorphism

$$\mathfrak{Z}((1 - e_{G'})R[G]) \cong \mathfrak{Z}((1 - e_{G'})e_H R[I]).$$

Thus, by (5.6), there is an injection of R-algebras

$$f_G R[G] \longrightarrow M_{np\times np}(\mathfrak{Z}(f_G R[G]))$$

which restricts to the canonical identification of centres and induces an isomorphism of F-algebras after extending scalars. This completes the proof of Claim 5.3.3 □

Finally, by Claim 5.3.3 and Corollary 3.4.4, we see that there is a containment

$$(1 - e_{G'})\mathcal{H}(R[G]) \supset \mathfrak{Z}((1 - e_{G'})R[G]) \cap \mathfrak{Z}(R[G]).$$

This completes the proof of Proposition 5.3.1. □

Corollary 5.3.4. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0, fix a prime number p and let G be a finite p-group. Suppose that every element of ${}^{G}\!/_{Z(G)}$ has a lift in G of order p. If the commutator subgroup of G has order p then the denominator ideal of $R[G]$ is given by*

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1-g)\mathfrak{Z}((1-e_{G'})R[G]),$$

for some generator g of G'.

Proof. By Proposition 5.3.1 we have

$$(1-e_{G'})\mathcal{H}(R[G]) \supset \mathfrak{Z}((1-e_{G'})R[G]) \cap \mathfrak{Z}(R[G]).$$

From Corollary 3.6.2 we have

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1-e_{G'})\mathcal{H}(R[G]).$$

Thus, as $\mathcal{H}(R[G]) \subset \mathfrak{Z}(R[G])$, we see that

$$(1-e_{G'})\mathcal{H}(R[G]) \subset (1-e_{G'})\mathfrak{Z}(R[G]) \cap \mathfrak{Z}(R[G]) = \mathfrak{Z}((1-e_{G'})R[G]) \cap \mathfrak{Z}(R[G]),$$

where the last equality is Lemma 1.9.8(iii). Therefore we see that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus \left(\mathfrak{Z}((1-e_{G'})R[G]) \cap \mathfrak{Z}(R[G])\right).$$

Using Lemma 3.6.1, we note that

$$(1-e_{G'})R[G] \cap R[G] = \sum_{i=0}^{p-1}(1-g^i)R[G] = (1-g)R[G]$$

for some generator g of G', where the last equality follows because $(1-g^i) = (1-g)\sum_{j=0}^{i-1} g^j$. Therefore, we conclude that

$$\begin{aligned}\mathfrak{Z}((1-e_{G'})R[G]) \cap \mathfrak{Z}(R[G]) &= ((1-e_{G'})R[G] \cap R[G]) \cap \mathfrak{Z}(F[G]) \\ &= (1-g)R[G] \cap \mathfrak{Z}(F[G]) \\ &= (1-g)\mathfrak{Z}((1-e_{G'})R[G]),\end{aligned}$$

where the first equality follows from Lemma 1.9.8 and last equality follows by Lemma 5.2.1 (showing that $g \in Z(G)$) and Corollary 1.9.10. □

Example 5.3.5. Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and fix a prime number p. Let $A = \langle a \mid a^{p^2}\rangle$, $B = \langle b \mid b^{p^2}\rangle$ and define an action of B on A by $a^b = a^{p+1}$. Consider the group $A \rtimes B$. It is not possible to replicate Remarks 5.1.3 and 5.1.2 for this group as every subgroup of G with order p lies in the centre of G. This means that the method used in Example 5.1.1 does not work for the group ring $R[A \rtimes B]$. Therefore, the condition that every element of ${}^{G}\!/_{Z(G)}$ has a lift in

G of order p in Corollary 5.3.4 cannot be removed entirely without further work. However there is a trick that may be applied to compute the denominator ideal of $R[C_{p^2} \rtimes C_{p^2}]$. To illustrate this trick we will consider the non-abelian group of order p^3 and exponent p^2 in Example 5.3.6 below.

Example 5.3.6. Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and fix a prime number p. Let $G = A \rtimes B$, where $A = \langle a \mid a^{p^2} \rangle$, $B = \langle b \mid b^p \rangle$ and the action of B on A is given by $a^b = a^{p+1}$. Then G is the non-abelian group of order p^3 and exponent p^2. For the purposes of this example we will pretend that Remark 5.1.3 is not applicable and we will instead compute the denominator ideal of $R[G]$ using Proposition 5.3.1.

The idea is to produce a larger group G_1 which satisfies the conditions of Proposition 5.3.1 and then show that there is a relation between $\mathcal{H}(R[G])$ and $\mathcal{H}(R[G_1])$. Let $G_1 = (Y \times A_1) \rtimes B$ where $A_1 = \langle a_1 \mid a_1^p \rangle$, $Y = \langle y \mid y^{p^2} \rangle$ and the action of B on $Y \times A_1$ is given by $y^b = y$ and $a_1^b = y^p a_1$. We see that $Y = Z(G_1)$ and it is clear that each non-identity element of $G_1/Y = \langle a_1 Y, bY \rangle$ has a lift in G_1 of order p. Hence Proposition 5.3.1 shows that

$$(1 - e_Z)\mathcal{H}(R[G_1]) \supset \mathfrak{Z}((1 - e_Z)R[G_1]) \cap \mathfrak{Z}(R[G_1]), \tag{5.7}$$

where $Z = \langle y^p \rangle = G_1'$.

We may consider G as a subgroup of G_1 by identifying $a = ya_1$. Then under this identification $Z = \langle a^p \rangle$ is the commutator subgroup of G. One can show that there is an R-algebra isomorphism

$$\varphi \colon R[G] \otimes_{R[Z]} R[Y] \longrightarrow R[G_1].$$

given on the R generating set $g \otimes y$ of $R[G] \otimes_{R[Z]} R[Y]$ by $\varphi(g \otimes y) = gy$ (the proof of this will be omitted here, for details one can see Lemma 5.4.4).

We note that $R[G]$ is a free $R[Z]$-module, hence using Lemma 1.9.18, we see that $R[G] = R[G_1] \cap F[G]$ and, using Corollary 1.9.20, $\mathfrak{Z}(R[G]) = \mathfrak{Z}(R[G_1]) \cap \mathfrak{Z}(F[G])$. Hence, by Lemma 3.2.1, we see that

$$\mathcal{H}(R[G]) = \mathcal{H}(R[G_1] \cap F[G]) \supset \mathcal{H}(R[G_1]) \cap \mathfrak{Z}(F[G]). \tag{5.8}$$

Putting (5.7) and (5.8) together we see that

$$\begin{aligned}(1 - e_Z)\mathcal{H}(R[G]) &\supset (1 - e_Z)\mathcal{H}(R[G_1]) \cap \mathfrak{Z}(F[G]) \\ &\supset (\mathfrak{Z}((1 - e_Z)R[G_1]) \cap \mathfrak{Z}(R[G_1])) \cap \mathfrak{Z}(F[G]) \\ &= \mathfrak{Z}((1 - e_Z)R[G]) \cap \mathfrak{Z}(R[G]).\end{aligned}$$

Finally, since a^p is a generator for G', using the argument from Corollary 5.3.4 we see that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_Z R[G] \oplus (1 - a^p)\mathfrak{Z}((1 - e_Z)R[G]).$$

Remark 5.3.7. Fix a prime number p. Let G be a finite p-group with commutator subgroup of order p. The method used to produce the larger group G_1 from G in Example 5.3.6 is a central product (see Definition 5.4.1). Using central products to extend the group G

turns out to be very powerful. It will allow us to entirely remove the awkward condition in Corollary 5.3.4 on the lifts of elements of $G/Z(G)$. This will be done in Theorem 5.5.1.

5.4 Central products

To make progress in generalising the idea of Example 5.3.6 we will need to introduce the notion of the central product of groups.

Definition 5.4.1. Let G and H be finite groups and let M a finite abelian group which is identified with a subgroup of $Z(G)$ and a subgroup of $Z(H)$. We define the (outer) *central product* of G and H (with respect to M) to be

$$G \circ_M H = (G \times H)/D,$$

where $D = \{(m, m^{-1}) \mid m \in M\}$ (we note that D is normal in $G \times H$ because it is contained within $Z(G \times H)$) and we identify M with its image in $G \circ_M H$.

Remark 5.4.2. The above definition of the central product may be weakened in several ways. Firstly, a very similar definition works if there is an action of H on G. To do this we would replace $G \times H$ with the semidirect product $G \rtimes H$. The construction used still works when M is identified with a normal subgroup of G and a normal subgroup of H (weakening the requirement that M is identified with a subgroup of $Z(G)$ and a subgroup of $Z(H)$); in this case $G \circ_M H$ is called the *partial semidirect product* of G and H. See [Gor80, Section 2.5] for details.

Lemma 5.4.3. *Let G and H be finite groups and let M a finite abelian group which is identified with a subgroup of $Z(G)$ and a subgroup of $Z(H)$. The central product of G and H with respect to M satisfies the following properties.*

(i) The canonical maps given by the compositions

$$G \longrightarrow G \times H \longrightarrow G \circ_M H \quad \text{and} \quad H \longrightarrow G \times H \longrightarrow G \circ_M H$$

are injections. In this way we identify G and H with normal subgroups of $G \circ_M H$.

(ii) Under the identification of G, H and M as subgroups of $G \circ_M H$ we have $M = G \cap H$.

(iii) We have $Z(G) \circ_M Z(H) = Z(G \circ_M H)$.

(iv) We have $(G \circ_M H)' = G'H'$.

Proof. For a proof of (i) and (ii) see [Gor80, Section 2.5]. Let

$$(g, h)D \in Z(G \circ_M H) = Z\left((G \times H)/D\right),$$

where $D := \{(m, m^{-1}) \mid m \in M\} < Z(G \times H)$. Then for each $g' \in G$, we see that

$$(g'g, h)D = (g', 1_H)D(g, h)D = (g, h)D(g', 1_H)D = (gg', h)D.$$

Hence, there exists $m \in M$ such that $g'g = gg'm$ and $h = hm^{-1}$; in particular, $m = 1$ so $g'g = gg'$ for each $g' \in G$. Thus $g \in Z(G)$. A similar argument shows that $h \in Z(H)$. Hence the map $Z(G) \times Z(H) \to Z(G \circ_M H)$ is a surjection with kernel D and the First

Isomorphism Theorem for groups completes the proof of (iii). Since G and H are subgroups of $G \circ_M H$, we must have $G'H' < (G \circ_M H)'$. However, we see that

$$(G \circ_M H)/G'H' = \Big((G \times H)/D\Big)/\Big((G' \times H')D/D\Big) \cong (G \times H)/(G' \times H')D$$

and so $(G \circ_M H)/G'H'$ is abelian. Since the commutator subgroup of $G \circ_M H$ is the smallest normal subgroup N such that $G \circ_M H/N$ is abelian, we have $G'H' > (G \circ_M H)'$. This proves (iv). □

Let R be a commutative ring. Recall from Example 1.5.6 that for products of finite groups G and H there is an isomorphism $R[G \times H] \cong R[G] \otimes_R R[H]$. A similar property holds for central products.

Lemma 5.4.4. *Let R be a commutative ring. Let G and H be finite groups and let M be a finite abelian group which is identified with a subgroup of $Z(G)$ and a subgroup of $Z(H)$. Then there is an isomorphism*

$$R[G \circ_M H] \cong R[G] \otimes_{R[M]} R[H].$$

Proof. The proof of this lemma is routine, but a proof is provided here for the convenience of the reader. The proof used here is inspired by the mathoverflow answer [Lea18]. Consider the map

$$\begin{aligned} \mu \colon R[G] \times R[H] &\longrightarrow R[G \circ_M H] \\ (g, h) &\longmapsto (g, h)D, \end{aligned}$$

where $D = \{(m, m^{-1}) \mid m \in M\}$. We see that μ is a bilinear map and $\mu(gm, h) = \mu(g, mh)$, for $g \in G$, $h \in H$ and $m \in M$. In particular, since $M \subset Z(G \circ_M H)$, we see that μ induces a unique map

$$\begin{aligned} \mu' \colon R[G] \otimes_{R[M]} R[H] &\longrightarrow R[G \circ_M H] \\ g \otimes h &\longmapsto (g, h)D. \end{aligned}$$

It is clear that μ' is a surjection. Furthermore, in $G \circ_M H$ the elements of G and H commute meaning that μ' is a ring homomorphism. Finally, this map has inverse given by

$$\begin{aligned} R[G \circ_M H] &\longrightarrow R[G] \otimes_{R[M]} R[H] \\ (g, h)D &\longmapsto g \otimes h, \end{aligned}$$

we note that, from the definition of D, this map is well defined. This proves that μ' is a R-algebra isomorphism. □

5.5 Denominator ideals of group rings over any finite p-group with commutator subgroup of order p

Theorem 5.5.1. *Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0, fix a prime number p and let G be a finite p-group. If the commutator subgroup of G has order p then the denominator ideal of $R[G]$ is given by*

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1-g)\mathfrak{Z}((1-e_{G'})R[G]),$$

where g is a generator of G'.

Proof. The idea of this proof is to produce a larger group G_1, where every non-identity element of ${}^{G_1}\!/_{Z(G_1)}$ has a lift in G_1 of order p, in such a way that $R[G_1] \cong R[G] \otimes_{R[M_1]} R[B_1]$ for some $M_1 \leq Z(G)$ and some abelian group B_1. Then Lemma 1.9.18, Proposition 5.3.1, and the proof of Corollary 5.3.4 may be used prove the desired result.

We will produce the group G_1 in the following way. We will first show that ${}^{G}\!/_{Z(G)}$ has exponent p. Next let $\overline{g}$ be a non-identity element of ${}^{G}\!/_{Z(G)}$ and let $g \in G$ be any lift of $\overline{g}$. We see that $g^p \in Z(G)$. If g^p has a "central p-th root" h (in other words, there exists $h \in Z(G)$ such that $h^p = g^p$) then gh^{-1} is a lift of $\overline{g}$ in G with order p. Therefore, to show that an element $\overline{g} \in {}^{G}\!/_{Z(G)}$ has a lift of order p it is sufficient to show that g^p has a "central p-th root". Unfortunately a "central p-th root" of g^p may not exist. We will use a central product to create the larger group G_1 in which all the desired "central p-th roots" exist.

Since G is a non-abelian finite p-group and G' is a non-trivial normal subgroup of G, the subgroup $G' \cap Z(G)$ is non-trivial (see [JL01, Lemma 26.1(1)]). Thus, as $G' \cong C_p$, we see that $G' < Z(G)$. Let $g \in G$. For all $h \in G$, we see that

$$[g^p, h] = [g, h]^p = 1,$$

where the first equality follows because $G' < Z(G)$ (see the proof of Claim 5.2.3 for details of this argument) and the second equality follows because $G' \cong C_p$. In particular, we see that $g^p \in Z(G)$. Therefore, we see that ${}^{G}\!/_{Z(G)}$ has exponent p.

For each non-identity element $\overline{g} \in {}^{G}\!/_{Z(G)}$, fix a lift $g \in G$ and let $\mathcal{G}$ be the set of such lifts. Consider the abelian group $B = \prod_{g \in \mathcal{G}} C_{\mathrm{ord}(g)}$ with generators b_g such that $\mathrm{ord}(b_g) = \mathrm{ord}(g)$. Let $M = \langle b_g^p \mid g \in \mathcal{G} \rangle < B$. Since the element g^p is central for each $g \in \mathcal{G}$ and $\mathrm{ord}(g^p) = \mathrm{ord}(b_g^p)$, there is a group homomorphism $\theta \colon M \to Z(G)$ given on the generators $\{b_g^p \mid g \in \mathcal{G}\}$ of M by $\theta(b_g^p) = g^p$. Let $C = \ker(\theta)$, let $B_1 = {}^{B}\!/_{C}$ and let $M_1 = {}^{M}\!/_{C} < B_1$. Using the First Isomorphism Theorem for groups, we identify M_1 with the subgroup $\langle g^p \mid g \in \mathcal{G} \rangle$ of $Z(G)$ via the map θ and we let $G_1 = G \circ_{M_1} B_1$ be the central product of G and B_1 with respect to M_1. By Lemma 5.4.3(i), we see that G may be identified with a subgroup of G_1.

Let $\overline{g_1}$ be a non-identity element of ${}^{G_1}\!/_{Z(G_1)}$. Using Lemma 5.4.3(iii) and the Third Isomorphism Theorem for groups, we see that

$${}^{G_1}\!/_{Z(G_1)} = \left({}^{(G \times B_1)}\!/_{D_1}\right) \Big/ \left({}^{(Z(G) \times B_1)}\!/_{D_1}\right) \cong {}^{(G \times B_1)}\!/_{(Z(G) \times B_1)} \cong {}^{G}\!/_{Z(G)},$$

where

$$D_1 = \langle (m, m^{-1}) \in G \times B_1 \mid m \in M_1 \rangle.$$

This is the map $(g, bC)D_1Z(G_1) \mapsto gZ(G)$. Thus $\overline{g_1} = (g, b_g^{-1}C)D_1Z(G_1)$ for some $g \in \mathcal{G}$. Note that, in $G \times B_1$, we have $(g, b_g^{-1}C)^p = (g^p, b_g^{-p}C) \in D_1$. Therefore, $(g, b_g^{-1}C)D_1 \in G_1$ is a lift of $\overline{g_1}$ in G_1 with order p. As $\overline{g_1} \in {}^{G_1}\!/_{Z(G_1)}$ was arbitrary, every non-identity element of ${}^{G_1}\!/_{Z(G_1)}$ has a lift in G_1 of order p. Hence, by Proposition 5.3.1, we see that

$$(1 - e_{G_1'})\mathcal{H}(R[G_1]) \supset \mathfrak{Z}((1 - e_{G_1'})R[G_1]) \cap \mathfrak{Z}(R[G_1]). \tag{5.9}$$

Using Lemma 5.4.4, we see that $R[G_1] \cong R[G] \otimes_{R[M_1]} R[B_1]$. We note that $R[G]$ is a free $R[M_1]$-module; in particular, $R[G]$ is a flat $R[M_1]$-module. Therefore, using Lemma 1.9.18, we see that $R[G] = R[G_1] \cap F[G]$ and, using Corollary 1.9.20, we see that $\mathfrak{Z}(R[G]) = \mathfrak{Z}(R[G_1]) \cap \mathfrak{Z}(F[G])$.

Now, using Lemma 3.2.1, we see that

$$\mathcal{H}(R[G]) = \mathcal{H}(R[G_1] \cap F[G]) \supset \mathcal{H}(R[G_1]) \cap \mathfrak{Z}(F[G]). \tag{5.10}$$

Using Lemma 5.4.3(iv), we see that $G' = G_1'$, meaning that $e_{G'} = e_{G_1'}$. Therefore, using (5.9) and (5.10), we see that

$$(1-e_{G'})\mathcal{H}(R[G]) \supset \Big(\mathfrak{Z}((1 - e_{G_1'})R[G_1]) \cap \mathfrak{Z}(R[G_1])\Big) \cap \mathfrak{Z}(F[G]) = \mathfrak{Z}((1-e_{G'})R[G]) \cap \mathfrak{Z}(R[G]).$$

Finally, using an identical proof to Corollary 5.3.4, we see that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1 - g)\mathfrak{Z}((1 - e_{G'})R[G]),$$

where g is a generator of G'. □

Remark 5.5.2. The central product G_1 found in the proof of Theorem 5.5.1 is almost certainly larger than necessary. This is because the proof makes no effort to detect when the required "central p-th roots" already exist. It is possible that more refined structural information of $R[G]$ may be found by making an effort to detect the existing "central p-th roots". However this provides no benefit when computing denominator ideal of $R[G]$.

Example 5.5.3. Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0 and fix a prime number p. Let G be an extraspecial p-group, in other words G is a finite p-group such that $G' = Z(G) = \Phi(G) \cong C_p$ where $\Phi(G)$ is the Frattini subgroup of G. Then by Theorem 5.5.1, we see that

$$\mathcal{H}(R[G]) = \mathrm{Tr}_{G'} R[G] \oplus (1 - g)\mathfrak{Z}((1 - e_{G'})R[G]),$$

where g is a generator of G'. By [Gor80, Theorem 5.2], for every $n \in \mathbb{Z}_{>0}$ there are two extraspecial p-groups of order p^{2n+1}; moreover, these are given by a central product of n non-abelian p-groups of order p^3.

5.6 Where next?

Let R be an integrally closed Noetherian domain with field of fractions F of characteristic 0, let G be a finite group and let p be a prime number. A natural question to ask is: for what groups G do similar results to Theorem 5.5.1 hold? Using the methods of this chapter to obtain an explicit formulation for the denominator ideal for group rings $R[G]$ when G' does not have order p is probably overly ambitious. However the methods in the chapter may still be useful in obtaining 'lower bounds' for the denominator ideal. It seems unlikely that the methods introduced will work for all finite groups, but there are situations for which the arguments show more promise.

Finite p-groups G with abelian commutator subgroup. The step which appears to go wrong is Lemma 5.2.5. It seems unlikely that there exists a subgroup H of G which yields the desired isomorphism on centres, although some progress can be made towards this when $G' \leq Z(G)$. One potential fix for this would be to look at many subgroups H of G and hope that after taking intersections the desired isomorphism on centres holds.

Finite p-groups G with non-abelian commutator subgroup. This runs into the same problems as the abelian commutator subgroup case, but has the added issue that it may be hard to find subgroups H of G such that $[G, H]$ is contained within the centre of G. It is not clear how to proceed if such a group cannot be found.

Finite groups with commutator subgroup of order p, for example a dihedral group D_{2p} (with $p \neq 2$). A version of Lemma 5.2.5 does not hold for dihedral groups in general. However, there may be tricks involving central products and looking at the intersection over many subgroups which lead to a similar result. Considering the result on the structure of $\mathbb{Q}_p[D_{2p}]$ given in [CR81, Example 7.39], it seems plausible that such a method might work.

Finite groups with normal p-complement. Here Remark 4.9.8 shows one can reduce to considering p-groups, where hopefully denominator ideals can be computed.

Iwasawa algebras. In seems plausible that the arguments in this section could be adapted to apply to Iwasawa algebras over certain profinite groups with commutator subgroup of order p.

Bibliography

[AG60] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409. MR 0121392

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802

[Bou89] N. Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1989, Translated from the French, Reprint of the 1972 edition. MR 979760

[BW09] W. Bley and S. M. J. Wilson, *Computations in relative algebraic K-groups*, LMS J. Comput. Math. **12** (2009), 166–194. MR 2564571 (2010k:16013)

[CR62] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962. MR 0144979

[CR81] ———, *Methods of representation theory. Vol. I, With applications to finite groups and orders*, John Wiley & Sons, Inc., New York, 1981, Pure and Applied Mathematics, A Wiley-Interscience Publication. MR 632548 (82i:20001)

[CR87] ———, *Methods of representation theory. Vol. II, With applications to finite groups and orders*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1987, A Wiley-Interscience Publication. MR 892316 (88f:20002)

[DJ83] F. R. DeMeyer and G. J. Janusz, *Group rings which are Azumaya algebras*, Trans. Amer. Math. Soc. **279** (1983), no. 1, 389–395. MR 704622

[Fit36] H. Fitting, *Die determinantenideale eines moduls.*, Jahresbericht der Deutschen Mathematiker-Vereinigung **46** (1936), 195–228.

[FT93] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR 1215934

[Gan98] F. R. Gantmacher, *The theory of matrices. Vol. 1*, AMS Chelsea Publishing, Providence, RI, 1998, Translated from the Russian by K. A. Hirsch, Reprint of the 1959 translation. MR 1657129

[Gor80] D. Gorenstein, *Finite groups*, second ed., Chelsea Publishing Co., New York, 1980. MR 569209

[Gri02] P. Grime, *Fitting ideals and module structure*, Ph.D. thesis, University of Durham, 2002.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[Isa76] I. M. Isaacs, *Character theory of finite groups*, Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976, Pure and Applied Mathematics, No. 69. MR 0460423

[Isa80] ———, *Automorphisms of matrix algebras over commutative rings*, Linear Algebra Appl. **31** (1980), 215–231. MR 570392

[Jac66] H. Jacobinski, *On extensions of lattices*, Michigan Math. J. **13** (1966), 471–475. MR 0204538

[Jan79] G. J. Janusz, *Tensor products of orders*, J. London Math. Soc. (2) **20** (1979), no. 2, 186–192. MR 551444

[JL01] G. James and M. Liebeck, *Representations and characters of groups*, second ed., Cambridge University Press, New York, 2001. MR 1864147 (2002h:20010)

[JN13] H. Johnston and A. Nickel, *Noncommutative Fitting invariants and improved annihilation results*, J. Lond. Math. Soc. (2) **88** (2013), no. 1, 137–160. MR 3092262

[JN16a] ———, *On the equivariant Tamagawa number conjecture for Tate motives and unconditional annihilation results*, Trans. Amer. Math. Soc. **368** (2016), no. 9, 6539–6574. MR 3461042

[JN16b] ———, *On the non-abelian Brumer-Stark conjecture*, arXiv preprint arXiv:1509.00200 (2016).

[JN18] ———, *Hybrid Iwasawa algebras and the equivariant Iwasawa main conjecture*, Amer. J. Math. **140** (2018), no. 1, 245–276. MR 3749195

[Kül94] B. Külshammer, *Central idempotents in p-adic group rings*, J. Austral. Math. Soc. Ser. A **56** (1994), no. 2, 278–289. MR 1261587

[Lea18] T. Leason, *Group rings over central products*, MathOverflow, 2018, URL:https://mathoverflow.net/q/295476 (version: 2018-03-18).

[Nic10] A. Nickel, *Non-commutative Fitting invariants and annihilation of class groups*, J. Algebra **323** (2010), no. 10, 2756–2778. MR 2609173 (2011f:16039)

[Nic11] ———, *On non-abelian Stark-type conjectures*, Ann. Inst. Fourier (Grenoble) **61** (2011), no. 6, 2577–2608 (2012). MR 2976321

[Nic17a] ———, *Conjectures of Brumer, Gross and Stark*, arXiv preprint arXiv:1707.04432v2 (2017).

[Nic17b] ———, *Notes on noncommutative Fitting invariants*, arXiv preprint arXiv:1712.07368v1 (2017).

[Nor76] D. G. Northcott, *Finite free resolutions*, Cambridge University Press, Cambridge-New York-Melbourne, 1976, Cambridge Tracts in Mathematics, No. 71. MR 0460383

[Par07] A. Parker, *Equivariant Tamagawa numbers and non-commutative Fitting invariants*, Ph.D. thesis, Kings College London, 2007.

[Pas85] D. S. Passman, *The algebraic structure of group rings*, Robert E. Krieger Publishing Co., Inc., Melbourne FL, 1985, Reprint of the 1977 original. MR 798076

[Rei75] I. Reiner, *Maximal orders*, vol. 38, Academic press London, 1975.

[Rob96] D. J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR 1357169

[Rog92] K. W. Roggenkamp, *Group rings: units and the isomorphism problem*, Group rings and class groups, DMV Sem., vol. 18, Birkhäuser, Basel, 1992, With contributions by W. Kimmerle and A. Zimmermann, pp. 1–152. MR 1167450

[Rog96] ———, *Clifford theory and a counterexample to the isomorphism problem for infinite groups*, An. Ştiinţ. Univ. Ovidius Constanţa Ser. Mat. **4** (1996), no. 1, 98–123, Representation theory of groups, algebras, and orders (Constanţa, 1995). MR 1407530

[Sch83] P. Schmid, *Lifting modular representations of p-solvable groups*, J. Algebra **83** (1983), no. 2, 461–470. MR 714256

[Sch88a] ———, *Clifford theory of simple modules*, J. Algebra **119** (1988), no. 1, 185–212. MR 971353

[Sch88b] ———, *Extensions of lattices over p-solvable groups*, Arch. Math. (Basel) **50** (1988), no. 6, 492–494. MR 948262

[Ser79] J. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237

[Sus88] J. Susperregui, *On determinantal ideals over certain noncommutative rings*, Ring theory (Granada, 1986), Lecture Notes in Math., vol. 1328, Springer, Berlin, 1988, pp. 269–282. MR 959761

[Sus89] ———, *Fitting invariants for modules over anticommutative graded rings*, Comm. Algebra **17** (1989), no. 8, 2035–2054. MR 1013481

[Web16] P. Webb, *A course in finite group representation theory*, Cambridge University Press, 2016.