National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

University of Alberta

tors of Large Subgroups of General Linear Groups over Group Rings

by

Gregory Thomas Lee ©

submitted to the Faculty of Graduate Studies and Research in partial
lfilment of the requirements for the degree of Master of Science

in

Mathematics.

Department of Mathematical Sciences

Edmonton, Alberta
Fall 1995

National Library of Canada

Acquisitions and Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale du Canada

Direction des acquisitions et des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

THE AUTHOR HAS GRANTED AN IRREVOCABLE NON-EXCLUSIVE LICENCE ALLOWING THE NATIONAL LIBRARY OF CANADA TO REPRODUCE, LOAN, DISTRIBUTE OR SELL COPIES OF HIS/HER THESIS BY ANY MEANS AND IN ANY FORM OR FORMAT, MAKING THIS THESIS AVAILABLE TO INTERESTED PERSONS.

L'AUTEUR A ACCORDE UNE LICENCE IRREVOCABLE ET NON EXCLUSIVE PERMETTANT A LA BIBLIOTHEQUE NATIONALE DU CANADA DE REPRODUIRE, PRETER, DISTRIBUER OU VENDRE DES COPIES DE SA THESE DE QUELQUE MANIERE ET SOUS QUELQUE FORME QUE CE SOIT POUR METTRE DES EXEMPLAIRES DE CETTE THESE A LA DISPOSITION DES PERSONNE INTERESSEES.

THE AUTHOR RETAINS OWNERSHIP OF THE COPYRIGHT IN HIS/HER THESIS. NEITHER THE THESIS NOR SUBSTANTIAL EXTRACTS FROM IT MAY BE PRINTED OR OTHERWISE REPRODUCED WITHOUT HIS/HER PERMISSION.

L'AUTEUR CONSERVE LA PROPRIETE DU DROIT D'AUTEUR QUI PROTEGE SA THESE. NI LA THESE NI DES EXTRAITS SUBSTANTIELS DE CELLE-CI NE DOIVENT ETRE IMPRIMES OU AUTREMENT REPRODUITS SANS SON AUTORISATION.

ISBN 0-612-06496-4

Canada

University of Alberta

Library Release Form

Name of Author: Gregory Thomas Lee

Title of Thesis: Generators of Large Subgroups of General Linear Groups over Group Rings

Degree: Master of Science

Year this Degree Granted: 1995

Permission is hereby granted to the University of Alberta Library to reproduce single copies of this thesis and to lend or sell such copies for private, scholarly or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the thesis, and except as hereinbefore provided neither the thesis nor any substantial portion thereof may be printed or otherwise reproduced in any material form whatever without the author's prior written permission.

(Signed) . . . .

Gregory Thomas Lee
311 Tunis Street
Ingersoll, Ontario
N5C 1W9
Canada

Date: Oct. 5/95 . . . . .

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **Generators of Large Subgroups of General Linear Groups over Group Rings** submitted by Gregory Thomas Lee in partial fulfilment of the requirements for the degree of Master of Science in Mathematics.

S. K. Sehgal

Dr. S. K. Sehgal (Supervisor)

M. Shirvani

Dr. M. Shirvani (Chair & Examiner)

Dr. S. K. Malhotra (External)

Date: Sept. 29, 95

Abstract

Let $\mathbb{Z}G$ be the integral group ring over a finite group, G. This thesis is a discussion of the problem of constructing generators of a subgroup of finite index in $GL_n(\mathbb{Z}G)$, for positive integers n.

First, we consider the unit group, $\mathcal{U}(\mathbb{Z}G)$. We begin by obtaining a result due to Jespers and Leal, which states that if $\mathbb{Q}G$ has no exceptional Wedderburn components, and G has no nonabelian fixed point free homomorphic images, then the Bass cyclic and bicyclic units generate a large subgroup in $\mathcal{U}(\mathbb{Z}G)$. When G is nilpotent, we obtain a result due to Giambruno and Sehgal, which gives generators of a large subgroup of $\mathcal{U}(\mathbb{Z}G)$, provided $\mathbb{Q}G$ has no exceptional components.

Finally, we present a new result. Namely, the elementary matrices over G, together with the matrices bI_n, for Bass cyclic units b, generate a large subgroup in $GL_n(\mathbb{Z}G)$, when $n \geq 3$.

Acknowledgements

I would like to take this opportunity to express my gratitude to my supervisor, Dr. Sudarshan K. Sehgal, both for introducing me to the study of group rings, and for all of his help during the creation of this thesis. His guidance has been invaluable.

In addition, I would like to thank the Natural Sciences and Engineering Research Council and the University of Alberta for their financial support.

Finally, thanks to my family for their ongoing support.

This thesis was typeset using $\mathcal{A}\!\mathcal{M}\!\mathcal{S}$-TEX.

Table of Contents

Chapter 1

Introduction

Let G be a finite group, and $\mathbb{Z}G$ its integral group ring. The unit group of this group ring, $\mathcal{U}(\mathbb{Z}G)$, is our object of study in this thesis.

In [Hi], Higman classified the finite groups for which $\mathcal{U}(\mathbb{Z}G) = \pm G$. In a few other isolated cases, $\mathcal{U}(\mathbb{Z}G)$ has been completely determined. However, in general, the problem of determining $\mathcal{U}(\mathbb{Z}G)$ precisely has proven to be quite intractably difficult. Another problem has arisen, and it is this: can we construct generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$? This is the problem with which we shall concern ourselves.

We will concentrate primarily on nilpotent groups, G. There are two main approaches in the literature. One, which was introduced by Ritter and Sehgal in [RS2], involves establishing results for odd p-groups, and many 2-groups, and then extending these results to the direct product of these groups. Another, which was begun by Ritter and Sehgal in [RS1], and strengthened by Jespers and Leal in [JL2], allows us to obtain a result without the nilpotency assumption. However, if we assume that the group is nilpotent, some strong results can be obtained. The first of these approaches gives results which involve slightly fewer generators, but the second gives results which hold a little more generally. The first of these methods is presented in Chapter 3 of [Se2]. We will focus upon the second method here.

We now present a brief overview of the thesis. We will prove nothing at this time.

Chapter 2 contains some results of a preliminary nature. Various results about Wedderburn decompositions, primitive central idempotents, representations, reduced norms, and the like are presented.

In Chapter 3, we present some results, without requiring that G be nilpotent. We will begin by introducing the Bass cyclic units, which are of the form

$$(1 + x + x^2 + \cdots + x^{i-1})^{\varphi(|G|)} + \frac{1 - i^{\varphi(|G|)}}{|x|}\hat{x},$$

where $x \in G$, $1 < i < |x|$, $(i, |x|) = 1$, $\hat{x} = 1 + x + \cdots + x^{|x|-1}$, and φ is the Euler function. We will make use of a theorem of Bass and Milnor, which states that under the natural map $j : \mathcal{U}(\mathbb{Z}G) \to K_1(\mathbb{Z}G)$, the images of the Bass cyclic units generate a subgroup of finite index in $K_1(\mathbb{Z}G)$, in order to obtain a major reduction in our problem. This result allows us to concentrate our investigations on the elements of $\mathcal{U}(\mathbb{Z}G)$ which map onto subgroups of finite index in the group of invertible matrices of reduced norm one in $M_{n_i}(\mathcal{O}_i)$, where $\mathcal{O}_i$ is an order in

D_i, and $M_{n_i}(D_i)$ is a Wedderburn component of $\mathbb{Q}G$, and which map to the identity matrix in all of the other components. If we can find these units, then combining them with the Bass cyclic units, we will have found generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. It will follow easily that the Bass cyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$, if G is abelian.

Next, we will introduce the bicyclic units, which are of the form

$$1+(1-g)h\hat{g},\ 1+\hat{g}h(1-g)$$

for $g, h \in G$. We will prove that if G has no nonabelian fixed point free homomorphic images, and if $\mathbb{Q}G$ has no exceptional components (that is, components for which the Congruence Subgroup Theorem fails), then the Bass cyclic and bicyclic units will generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

In Chapter 4, we introduce the assumption that G is nilpotent. Under this assumption, we classify all of the possible fixed point free homomorphic images, and discover that these groups are either cyclic, or the direct product of a generalized quaternion group and a cyclic group of odd order. The Wedderburn decompositions of these groups are well-known. It follows that if $\mathbb{Q}G$ has no exceptional components, or components of the form $\mathbb{H}(\mathbb{Q}(\xi_p))$, for odd primes p, then the Bass cyclic and bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. From this, it follows immediately that we need only worry about those nilpotent groups which have nonabelian Sylow 2-subgroups. In particular, the problem has been solved for all nilpotent groups of odd order (or, indeed, all groups whose orders are not divisible by eight). We also present an example of a group, G, of order 16, for which the bicyclic and Bass cyclic units generate a subgroup of infinite index in $\mathcal{U}(\mathbb{Z}G)$.

We then introduce some new units, which were designed by Giambruno and Sehgal to deal with homomorphic images of the form $Q_8 \times C_n$, for odd integers $n > 1$. These units, together with the Bass cyclic and bicyclic units, will generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$, provided that $\mathbb{Q}G$ has no exceptional Wedderburn components.

In Chapter 5, we generalize the problem. Instead of just considering the unit group of $\mathbb{Z}G$, we consider the unit group of $M_n(\mathbb{Z}G)$, namely $GL_n(\mathbb{Z}G)$, for positive integers n. When $n \geq 3$, we can bypass the exceptions to the Congruence Subgroup Theorem. Further, we have a new class of units in this ring. Specifically, we may consider the elementary matrices over $\mathbb{Z}G$. Dropping the nilpotency assumption, we will present a new result. To wit, the units bI_n, for Bass cyclic units b, together with the elementary matrices in $M_n(\mathbb{Z}G)$, will generate a subgroup of finite index in $GL_n(\mathbb{Z}G)$, for any finite group G, and any $n \geq 3$.

In Chapter 6, we mention some open problems in this area, and some related results.

Chapter 2

Preliminaries

In this chapter, we will present some definitions and results from several different areas of mathematics. As all of the results are well-known, we shall simply supply references, except when the proofs are short.

§2.1 Basic Definitions

Let us agree that by a ring, we will mean a ring with identity, and that by a field, we will mean a commutative field. Let us further assume that ring homomorphisms map the identity element to the identity element. Throughout, we reserve the symbols $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ for the integers, the rational numbers, the real numbers, and the complex numbers respectively.

Let G be a group, and R a ring. Then the **group ring**, RG, is defined to be the set of all formal sums

$$\sum_{g\in G} \alpha_g g$$

with $\alpha_g \in R$ for all $g \in G$, and all but finitely many $\alpha_g = 0$, together with the operations

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \alpha'_g g = \sum_{g\in G} (\alpha_g + \alpha'_g) g$$

and

$$(\sum_{g\in G} \alpha_g g) \cdot (\sum_{g\in G} \alpha'_g g) = \sum_{g\in G} (\sum_{h\in G} \alpha_h \alpha'_{h^{-1}g}) g.$$

To express the latter another way,

$$(\sum_{g\in G} \alpha_g g) \cdot (\sum_{g\in G} \alpha'_g g) = \sum_{g\in G} \sum_{h\in G} \alpha_g \alpha'_h gh.$$

It is easily seen that RG is a ring with additive identity $\sum_{g\in G} 0g$ and multiplicative identity $\sum_{g\in G} \delta_g g$, where $\delta_1 = 1$ and $\delta_g = 0$ for all $g \neq 1$. In the case where R is a field, we may also refer to RG as a **group algebra**. We will often drop the terms with zero coefficients, and write the elements of RG as

$$\alpha_1 g_1 + \cdots \alpha_k g_k$$

with $\alpha_i \in R$, $g_i \in G$ for all i. We identify the ring R with the set of elements $\{r1 : r \in R\}$ and the group G with the set $\{1g : g \in G\}$. In this sense, we see that the elements of R commute with the elements of G in RG.

It is easily seen that the map $\epsilon : RG \to R$ defined by $\epsilon(\sum_{g\in G} \alpha_g g) = \sum_{g \in G} \alpha_g$ is a ring homomorphism. We let $\Delta_R(G)$ denote the kernel of this map. We call ϵ the **augmentation map**, and $\Delta_R(G)$ the **augmentation ideal** of RG. We have

Proposition 2.1.1. *The ideal $\Delta_R(G)$ consists precisely of the finite sums of terms of the form $r(g-1)$, $r \in R$, $g \in G$.*

Proof. Certainly $\epsilon(g-1) = 0$ for each $g \in G$, so these elements are all in the kernel. Conversely, take $\alpha \in \Delta_R(G)$. Then $\sum_{g\in G} \alpha_g = 0$, so in particular,

$$\alpha = \alpha - 0 = \sum_{g\in G} \alpha_g g - \sum_{g\in G} \alpha_g,$$

and this is

$$\sum_{g\in G} \alpha_g(g-1)$$

which is of the correct form. □

Similarly, if K is a normal subgroup of G, then the projection $G \to G/K$ extends R-linearly to a ring homomorphism $\epsilon_K : RG \to R(G/K)$. We denote its kernel by $\Delta_R(G,K)$. Note that $\Delta_R(G) = \Delta_R(G,G)$. The proof of the following result is similar to that of the above proposition, and we omit it.

Proposition 2.1.2. *The ideal $\Delta_R(G,K)$ consists of the finite sums of terms of the form $rg(k-1)$, with $r \in R$, $g \in G$ and $k \in K$. Equivalently, it consists of finite sums of terms of the form $r(k-1)g$, $r \in R$, $g \in G$, $k \in K$.*

In any ring R, by a **unit** of R, we mean an element with a two-sided multiplicative inverse. These elements form a group under multiplication, which we denote by $\mathcal{U}(R)$. The group $\mathcal{U}(\mathbb{Z}G)$ will be our primary object of study. We observe that if $g \in G$, then the elements $\pm g \in \mathbb{Z}G$ are units, with inverses $\pm g^{-1}$. We call these the **trivial units.**

We now introduce some basic definitions from representation theory. For more information, see, for instance, [CR1]. Let F be a field, and G a finite group. Then a **representation** of G over F is a homomorphism $T : G \to GL_F(V)$, where $GL_F(V)$ is the group of invertible F-linear transformations of an F-vector space $V \neq 0$. Evidently, the map T extends F-linearly to a ring homomorphism T :

$FG \to End_F(V)$, where $End_F(V)$ denotes the ring of F-linear transformations of V. If we define an operation of FG on V via $\alpha \cdot v = T(\alpha)(v)$, it is plain that V becomes an FG-module.

When V is finite-dimensional over F, say of dimension n, we may identify $End_F(V)$ with $M_n(F)$, the $n \times n$ matrix ring over F, by choosing a basis for V and identifying each linear transformation with its matrix with respect to that basis. We say that two representations T and U (both mapping G to $GL_F(V)$) are **equivalent** if there exist bases X and Y for V such that for each $g \in G$, the matrix corresponding to $T(g)$ with respect to X is the same as the matrix corresponding to $U(g)$ with respect to Y. The representation T is said to be **reducible** if there exists a subspace $0 \neq W \neq V$ such that $T(g)(w) \in W$ for all $g \in G$, $w \in W$. T is **irreducible** if it is not reducible. Finally, we define the **character** χ of a representation via $\chi(g) = \text{trace}(T(g))$. The trace of the matrix does not depend upon the basis which is chosen, so that the character is also independent of this choice. Some easy examples of representations are given in

Example 2.1.3. (a) Let V be the one-dimensional F-vector space. Define T via $T(g)(v) = v$ for all $g \in G$, $v \in V$. This is known as the trivial representation.

(b) Let V=FG. This is a $|G|$-dimensional vector space. Define T via

$$T(g)(\alpha) = g\alpha, \text{ for all } g \in G, \alpha \in FG.$$

This is known as the regular representation.

The last thing we need to define is a nilpotent group. First, if G is a group, and $g, h \in G$, then the **commutator** of g and h is $[g,h] = g^{-1}h^{-1}gh$. If H and K are subgroups of G, we let $[H,K]$ be the subgroup of G generated by all elements of the form $[h,k]$, with $h \in H$ and $k \in K$. Now, let $G_{(1)} = G$. Then, for $i \geq 1$, let $G_{(i+1)} = [G_{(i)}, G]$. We say that G is **nilpotent** if $G_{(i)} = 1$ for some i. The results we need are contained in the following proposition.

Proposition 2.1.4. *(a) Every subgroup and homomorphic image of a nilpotent group is nilpotent.*

(b) A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.

Proof. (a) [Hup, Satz III.2.5a]

(b) [Hun, Proposition II.7.5] □

It follows from the definition that every abelian group is nilpotent, and from part (b) of the above proposition that every p-group is nilpotent.

§2.2 Wedderburn Decompositions and Representations

If F is a field, then by an **F-algebra**, we mean a ring A containing F (or an isomorphic copy thereof) in its centre, with $1_F = 1_A$.

We say that a nonzero ring R is **simple** if its only two-sided ideals are (0) and R. We say that R is left (resp. right) Artinian if there is no infinite, strictly descending sequence of left (resp. right) ideals

$$I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \cdots$$

of R. R is said to be **Artinian** if it is both left and right Artinian. If A is a finite-dimensional F-algebra (for any field F), then it is clear that any left or right ideal is a vector subspace of A. Thus, in any descending sequence as above, we have $\dim_F I_{j+1} < \dim_F I_j$ for all $j \geq 1$. We conclude that we must eventually reach dimension zero; that is, some $I_j = (0)$, at which point the sequence stops. That is, A is Artinian. The structure of simple Artinian algebras is given by

Theorem 2.2.1 (Wedderburn-Artin). *Let A be an Artinian F-algebra. Then F is simple if and only if F is isomorphic to $M_n(D)$, the ring of $n \times n$ matrices over an F-division algebra D. In this case, the natural number n is uniquely determined, and D is uniquely determined up to an F-algebra isomorphism.*

Proof. The first part is [Hun, Theorem IX.1.14]. The uniqueness is [Hun, Proposition IX.1.17ii]. □

If R is any ring and M is an R-module, then M is said to be **simple** if $M \neq 0$ and its only submodules are 0 and M. M is said to be **semisimple** if it is the direct sum of some collection of simple modules. We have the following result, which is Theorem 2.4 in [La].

Proposition 2.2.2. *M is semisimple if and only if for every submodule N of M, there exists a submodule N' of M such that $M = N \oplus N'$.*

A ring R is said to be **semisimple** if the left regular module ${}_RR$ is semisimple. (We should make two observations at this point. First, strictly speaking, this is the definition of a left semisimple ring. However, left semisimplicity and right semisimplicity are equivalent conditions (see, for instance, [La, Corollary 3.7]), so this is not a problem. Second, this definition is not used in all sources. For example, Hungerford's definition (in [Hun]) actually describes a weaker condition, and our semisimple rings would be called semisimple Artinian rings in his terminology. Since we are interested in finite-dimensional algebras, the difference is unimportant, and we follow [La]). The most important result on semisimplicity is

Theorem 2.2.3. *For an F-algebra A, the following are equivalent:*

(1) *A is semisimple;*

(2) *Every left A-module is semisimple;*

(3) *A is isomorphic (as an F-algebra) to $\bigoplus_{i=1}^{r} M_{n_i}(D_i)$ for some natural numbers n_i, and F-division algebras D_i.*

When these conditions hold, the r is uniquely determined, and the $M_{n_i}(D_i)$ are uniquely determined up to order and isomorphism.

Proof. The equivalence of (1) and (2) is [La, Theorem 2.5]. The equivalence of (1) and (3) is [Hun, Theorem IX.3.3]. The uniqueness is [La, Theorem 3.5]. □

The equivalence of (1) and (3) in the above result is known as the Wedderburn-Artin theorem. We call the isomorphism of (3) the **Wedderburn decomposition** of A, and the $M_{n_i}(D_i)$ its **Wedderburn components.** The reason for our interest in semisimple algebras is

Theorem 2.2.4 (Maschke). *If F is a field of characteristic zero and G is a finite group, then FG is a semisimple algebra.*

Proof. We let M be the left FG-module FG, and N any submodule. Clearly, N is an F-subspace of M. Hence, we may take an F-basis $\{x_1, \ldots, x_q\}$ of N, and extend it to an F-basis $\{x_1, \ldots, x_{|G|}\}$ of M. Let $N' = \operatorname{span}\{x_{q+1}, \ldots, x_{|G|}\}$. Then $M = N \oplus N'$ as F-modules. We need to find a complement for N as an FG-module.

We have the F-linear projection map $\pi : M \to N$, corresponding to $M = N \oplus N'$. Define $\tau : M \to N$ via

$$\tau(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot \pi(g \cdot m)$$

where $\cdot$ is the FG-module action on M. Now, τ is certainly F-linear, and if $h \in G$, then

$$\begin{aligned} h\tau(m) &= \frac{1}{|G|} \sum_{g \in G} hg^{-1} \cdot \pi(g \cdot m) \\ &= \frac{1}{|G|} \sum_{k \in G} k^{-1} \cdot \pi(kh \cdot m) \\ &= \tau(hm) \end{aligned}$$

(where $k = gh^{-1}$ runs through G as g does). That is, τ is FG-linear. Further, since $\pi : M \to N$, $\pi(g \cdot m) \in N$ for all g, and N is an FG-module. Hence,

$g^{-1} \cdot \pi(g \cdot m) \in N$. We conclude that τ is an FG-linear map from M to N as promised. Next, if $n \in N$, we have $g \cdot n \in N$, and the projection map π fixes N. Thus, $g^{-1} \cdot \pi(g \cdot n) = n$, and we conclude that $\tau(n) = \frac{1}{|G|}|G|n = n$.

Let $K = \ker\tau$. Since τ is an FG-module homomorphism, K is an FG-submodule of M. Take $m \in M$. Then $\tau(m) \in N$, and $\tau(m - \tau(m)) = \tau(m) - \tau(\tau(m))$. Since τ fixes N, $\tau(\tau(m)) = \tau(m)$, so that $m - \tau(m) \in K$. Thus, $m = \tau(m) + (m - \tau(m)) \in N + K$. That is, $M = N + K$. If $m \in N \cap K$, then since τ fixes N, $\tau(m) = m$. By definition of K, $\tau(m) = 0$. Thus, $m = 0$. We conclude that $M = N \oplus K$ (as FG-modules), and by Proposition 2.2.2, we are done. □

There is an equivalent formulation of Maschke's Theorem, the proof of which is basically identical to the one we have just presented. Namely, every finite-dimensional representation of a finite group, G, over a field, K, of characteristic zero is the direct sum of irreducible representations.

We observe that the restriction on the characteristic of F is needed only to guarantee that $1/|G|$ exists. Thus, the result also holds if the field has a nonzero characteristic which does not divide $|G|$.

Maschke's Theorem tells us that if K is any subfield of $\mathbb{C}$, and G is a finite group, then $KG \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i)$ for some natural numbers n_i and division algebras D_i, which must be finite-dimensional over K, since KG is.

Let us examine these division algebras for a moment. If D is a finite-dimensional K-division algebra, then it is easy to see that its centre, F, is an extension field of K, and D is a finite-dimensional division algebra over F. An important result is

Lemma 2.2.5. *Let D be a finite-dimensional division algebra over its centre, F, a field of characteristic zero. Let E be a maximal subfield of D containing F (which must exist by finiteness of dimension). Then* $\dim_F E = \dim_E D$. *In particular,* $\dim_F D$ *is a perfect square.*

Proof. [CR2, Corollary 7.22] □

We call the value $\dim_F E = \sqrt{\dim_F D}$ the **Schur index** of D, and denote it by $s(D)$. We also call this value the Schur index of a Wedderburn component of the form $M_n(D)$. Of immense value to us will be the following result, whose proof can be found in [CR2, Theorem 27.11].

Theorem 2.2.6. *Let G be a finite group, and let $\mathbb{Q}G \cong \bigoplus M_{n_i}(D_i)$ be the Wedderburn decomposition. Then for each i, $n_i s(D_i)$ divides the order of G.*

It follows, for example, that if G is a group of odd order, then each n_i and each $s(D_i)$ must be an odd number.

We need to explore the connection between the irreducible complex representations of a finite group G, and the Wedderburn components of $\mathbb{Q}G$. If T is an irreducible complex representation of G, and χ is its character, we write $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) : g \in G)$. Recall that $T : \mathbb{C}G \to End_{\mathbb{C}}(V)$ for some vector space V, and observe that $\mathbb{Q}G$ is embedded in $\mathbb{C}G$ in an obvious way. We have

Proposition 2.2.7. *Given G and T as above, if $\mathbb{Q}G = \bigoplus A_i$ is the Wedderburn decomposition of $\mathbb{Q}G$, with each $A_i \cong M_{n_i}(D_i)$, then there exists a unique i such that $T(A_i) \neq 0$. The centre of A_i (which is also the centre of D_i) is isomorphic to $\mathbb{Q}(\chi)$.*

Proof. [Hup, Hilfssatz V.14.7] □

On the other hand, if, for some i, we had $T(A_i) = 0$ for all irreducible complex representations T, then since $A_i \subseteq \mathbb{Q}G \subseteq \mathbb{C}G$, we would have a nonzero element $\alpha \in \mathbb{C}G$ such that $T(\alpha) = 0$ for all irreducible complex representations T. Let ρ be the regular representation of G over $\mathbb{C}$. (See Example 2.1.3(b)). Then $\rho(\alpha)(1) = \alpha \neq 0$. However, by Maschke's Theorem, ρ is the direct sum of some irreducible complex representations T_j. But each $T_j(\alpha) = 0$ by assumption, contradicting the fact that their direct sum is nonzero. Hence, for each i, there exists an irreducible complex representation T such that $T(A_i) \neq 0$. It follows immediately that the next result holds.

Corollary 2.2.8. *If $\mathbb{Q}G \cong \bigoplus M_{n_i}(D_i)$, then the centre of each D_i may be taken to be $\mathbb{Q}(\chi)$, where χ is the character of some irreducible complex representation of G.*

Finally, we say that a complex representation T is **realizable** over a subfield K if under some choice of basis, $T(g) \in M_n(K)$ for all $g \in G$. We conclude with the following celebrated theorem.

Theorem 2.2.9 (Brauer). *Every irreducible complex representation of a finite group is realizable over $\mathbb{Q}(\xi_{|G|})$, where $\xi_{|G|}$ is a primitive $|G|^{\text{th}}$ root of unity.*

Proof. [CR2, Theorem 15.16] □

§2.3 Primitive Central Idempotents

An element e of a ring R is said to be an **idempotent** if $e^2 = e$. Two idempotents e and f are said to be **orthogonal** if $ef = fe = 0$. For example, if e is an idempotent, then $(1-e)^2 = 1 - 2e + e^2 = 1 - e$, and $e(1-e) = e - e^2 = 0 = (1-e)e$, which means that e and $1-e$ are orthogonal idempotents.

If e is a central idempotent in R, we can see that Re is a ring with identity element e. (If R is an F-algebra for some field F, then so is Re). Suppose that a central idempotent e can be written as the sum of orthogonal central idempotents, $e = f + f'$. Then $f = f^2 = f^2 + ff' = f(f + f') = fe$. That is, $f \in Re$ and similarly, $g \in Re$. We say that a nonzero central idempotent $e \in R$ is a **primitive central idempotent** if it cannot be expressed as the sum of two orthogonal central idempotents, unless one of these is 0. We have

Proposition 2.3.1. *If e is a central idempotent of R, and $Re \cong M_n(D)$ for some natural number n and some division ring D, then e is a primitive central idempotent.*

Proof. Suppose this is false. Then write $e = f + g$, with f and g orthogonal central idempotents in R (and hence elements of Re by our earlier remarks). Since f is central in R, it is certainly central in $Re \cong M_n(D)$. That is, $f = zI_n$, a scalar multiple of the identity matrix, for some z in the centre of D. Since $f^2 = f$, we have $z^2 = z$. But in a division ring, this means that $z = 0$ or $z = 1$. Hence, f is the zero element or the identity element of Re, namely e. In the latter case, $e = e + g$ implies $g = 0$. □

Let us take a group algebra KG, with G a finite group, K a field of characteristic zero. Then we have the Wedderburn decomposition $KG = \bigoplus_{i=1}^{r} A_i$, with each $A_i \cong M_{n_i}(D_i)$. If we let e_i be the identity element of A_i, it is immediate that e_i is a central idempotent in KG, and $KGe_i \cong M_{n_i}(D_i)$. By the above result, e_i is a primitive central idempotent. Further $e_ie_j = 0$ for $i \neq j$ (since the sum is direct), and $1_{KG} = e_1 + \cdots + e_r$. Thus, we have written 1 as a sum of pairwise orthogonal primitive central idempotents. This expression is unique, as seen in

Proposition 2.3.2. *Suppose we can write $1 = c_1 + \cdots + c_t$ in a ring R, where the c_i are pairwise orthogonal primitive central idempotents. Then the central idempotents of R are precisely the sums of subsets of $\{c_1, \ldots, c_t\}$, and the only primitive central idempotents of R are $c_1, \ldots, c_t$. In particular, the expression* *of* 1 *as a sum of pairwise orthogonal primitive central idempotents is unique up to order.*

Proof. Let e be a central idempotent in R. Then for each i, ec_i is a central idempotent of R contained in Rc_i. If $0 \neq ec_i \neq c_i$, then we write $c_i = ec_i + (c_i - ec_i)$. Now,

$$ec_i(c_i - ec_i) = ec_i^2 - e^2c_i^2 = ec_i - ec_i = 0,$$

and similarly, $(c_i - ec_i)ec_i = 0$. Further,

$$(c_i - ec_i)^2 = c_i^2 - 2ec_i^2 + e^2c_i^2 = c_i - ec_i.$$

Since c_i and ec_i are central, so is $c_i - ec_i$, and we conclude that ec_i and $c_i - ec_i$ are orthogonal central idempotents summing to e, a contradiction. Thus, for each i, $ec_i = 0$ or $ec_i = c_i$. Hence,

$$e = e(c_1 + \cdots + c_t) = ec_1 + \cdots + ec_t$$

is a sum of a subset of $\{c_1, \cdots, c_t\}$. Since the c_i are pairwise orthogonal, if $j_1, \ldots, j_k$ are distinct values in $\{1, \ldots, t\}$, then

$$(c_{j_1} + \cdots + c_{j_k})^2 = c_{j_1}^2 + \cdots + c_{j_k}^2 = c_{j_1} + \cdots + c_{j_k}$$

and the centrality of each c_i implies the centrality of their sum. Hence, each sum of a subset of $\{c_1, \ldots, c_t\}$ is a central idempotent, completing the proof of the first statement.

Now, if we have $c = c_{j_1} + \cdots + c_{j_k}$, $k \geq 2$, then c_{j_1} and $c_{j_2} + \cdots + c_{j_k}$ are orthogonal central idempotents. We know that $c_{j_1} \neq 0$ by definition, and if $c_{j_2} + \cdots + c_{j_k} = 0$, then

$$0 = 0c_{j_2} = c_{j_2}c_{j_2} + \cdots + c_{j_k}c_{j_2} = c_{j_2}$$

by orthogonality, a contradiction. Thus, c is not primitive central. This gives us the second statement. To get the last part, suppose we have an expression $1 = z_1c_1 + \cdots + z_tc_t$, for non-negative integers z_i. Then for each i,

$$c_i = z_1c_1c_i + \cdots + z_tc_tc_i = z_ic_i$$

by orthogonality. Thus, our expression is $1 = c_1 + \cdots + c_t$. □

Hence, in our group algebra, the primitive central idempotents are precisely the identity elements of the Wedderburn components.

Suppose e is a primitive central idempotent in $\mathbb{Q}G$, for a finite group G. Then e commutes with all elements of G, which means that e is a central idempotent of $\mathbb{C}G$ (but not necessarily primitive central). By Proposition 2.3.2, we may write $e = f_1 + \cdots + f_m$ for some distinct primitive central idempotents $f_1, \ldots, f_m$ of $\mathbb{C}G$. Now, $\mathbb{C}Gf_i$ is a Wedderburn component of $\mathbb{C}G$. Since $\mathbb{C}$ is the only finite-dimensional division algebra over $\mathbb{C}$, we have $\mathbb{C}Gf_i \cong M_n(\mathbb{C})$ for some natural number n. It follows immediately that the map $g \mapsto gf_i \in M_n(\mathbb{C})$ is a complex representation of G. Let χ be its character. Then, by [Ya, p.4],

$$f_i = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

Thus, all coefficients of f_i are in $\mathbb{Q}(\chi)$. Let $\mathcal{G}$ be the Galois group of $\mathbb{Q}(\chi)$ over $\mathbb{Q}$; that is, the group of field automorphisms of $\mathbb{Q}(\chi)$ fixing $\mathbb{Q}$ elementwise. Then [Ya, Proposition 1.1] gives us

Theorem 2.3.3. *Under the above conditions,*

$$e = \frac{\chi(1)}{|G|} \sum_{\sigma \in \mathcal{G}} \sum_{g \in G} \sigma(\chi(g^{-1}))g.$$

This is particularly important to us, in that we may deduce the following result.

Corollary 2.3.4. *Let e be a primitive central idempotent of $\mathbb{Q}G$, and write $e = f_1 + \cdots + f_m$, a sum of primitive central idempotents of $\mathbb{C}G$. If for some $h \in G$, there is an i such that $hf_i = f_i$, then $he = e$.*

Proof. Let χ be the character defined in the discussion preceding Theorem 2.3.3. We write $\alpha_g = \chi(g^{-1})$, $\beta = \chi(1)/|G|$. Then $f_i = \beta \sum_{g \in G} \alpha_g g$. Now, $hf_i = f_i$ implies that

$$\beta \sum_{g \in G} \alpha_g hg = \beta \sum_{g \in G} \alpha_g g.$$

Hence,

$$\beta \sum_{g \in G} \alpha_{h^{-1}g} g = \beta \sum_{g \in G} \alpha_g g.$$

Since $\beta \neq 0$, $\alpha_{h^{-1}g} = \alpha_g$ for all $g \in G$. Therefore, $\sigma(\alpha_{h^{-1}g}) = \sigma(\alpha_g)$ for all $g \in G$, $\sigma \in \mathcal{G}$. That is,

$$\beta \sum_{g \in G} \sigma(\alpha_{h^{-1}g})g = \beta \sum_{g \in G} \sigma(\alpha_g)g.$$

In other words,

$$\beta \sum_{g\in G} \sigma(\alpha_g)hg = \beta \sum_{g\in G} \sigma(\alpha_g)g.$$

That is,

$$h\beta \sum_{g\in G} \sigma(\alpha_g)g = \beta \sum_{g\in G} \sigma(\alpha_g)g.$$

Since e is the sum over $\sigma \in \mathcal{G}$ of these terms, we have $he = e$, as required. □

§2.4 Reduced Norms

For any ring R, and any natural number n, we may consider $GL_n(R) = \mathcal{U}(M_n(R))$, the group of invertible $n \times n$ matrices over R. If R is commutative, we also have $SL_n(R)$, the subgroup of $GL_n(R)$ consisting of matrices of determinant 1. In the noncommutative case, however, determinants do not exist. Since we will be interested in studying $GL_n(D)$ for division rings D, we would like to have an analogue of the determinant.

We assume familiarity with the basic properties of tensor products of algebras over a field. (For instance, let M be a right R-module, and N a left R-module, for some ring R. (When R is a field, R-algebras will suffice. This is the case which interests us.) If K is any abelian group, then a map $\lambda : M \times N \rightarrow K$ is said to be **middle linear** if $\lambda(m_1 + m_2, n_1) = \lambda(m_1, n_1) + \lambda(m_2, n_1)$, $\lambda(m_1, n_1 + n_2) = \lambda(m_1, n_1) + \lambda(m_1, n_2)$, and $\lambda(m_1 r, n_1) = \lambda(m_1, rn_1)$, for all $m_1, m_2 \in M$, $n_1, n_2 \in N$, and $r \in R$. We recall that a middle linear map induces a group homomorphism $\lambda' : M \otimes_R N \rightarrow K$, given by $\lambda'(m \otimes n) = \lambda((m, n))$. (See [Hun, Theorem IV.5.2].))

Recalling that the Schur index $s(D)$ was defined in §2.2, we have

Lemma 2.4.1. *Suppose that D is a division algebra which is finite-dimensional over its centre, F, which is an algebraic number field. Suppose further that E is a maximal subfield of D containing F. Then $D \otimes_F E \cong M_{s(D)}(E)$ as E-algebras.*

Proof. [Re, Theorem 7.15] □

Call this isomorphism $\beta : D \otimes_F E \rightarrow M_{s(D)}(E)$. For a natural number n, we want to define a map $\gamma : M_n(D) \otimes_F E \rightarrow M_{ns(D)}(E)$. Let us regard matrices in $M_{ns(D)}(E)$ as $n \times n$ grids of $s(D) \times s(D)$ matrices. If $\alpha \in M_n(D)$ has entries $\alpha_{i,j}$, then for $e \in E$, we define a map $\eta : M_n(D) \times E \rightarrow M_{ns(D)}(E)$ by letting $\eta((\alpha, e))$ be the matrix whose $(i,j)^{\text{th}}$ $s(D) \times s(D)$ matrix is $\beta(\alpha_{i,j} \otimes e)$. This is clearly a middle linear map, so that we get a homomorphism γ, as required, with $\gamma(\alpha \otimes e)$ being the matrix whose $(i,j)^{\text{th}}$ $s(D) \times s(D)$ matrix is $\beta(\alpha_{i,j} \otimes e)$. It is perfectly straightforward to verify that γ is surjective, so by comparing dimensions, it is injective as well. It is also clear that γ is a homomorphism of E-algebras. In summary,

Proposition 2.4.2. *If D, F, and E are as in Lemma 2.4.1, then*

$$\gamma : M_n(D) \otimes_F E \to M_{ns(D)}(E)$$

is an isomorphism of E-algebras.

Since γ is an isomorphism of E-algebras, we observe that $\gamma(f \otimes 1)$ will be the matrix

$$\begin{pmatrix} f & & \\ & \ddots & \\ & & f \end{pmatrix}$$

for each $f \in F$.

We define the **reduced norm** on $M_n(D)$ via $nr(\alpha) = \det(\gamma(\alpha \otimes 1))$. It is important to state

Proposition 2.4.3. *With the same notations as above, $nr(\alpha) \in F$, for all α in $M_n(D)$.*

Proof. [Re, Theorem 9.3] □

It is clear that the reduced norm preserves multiplication. Thus,

$$nr : GL_n(D) \to F^\times$$

is a group homomorphism, where $F^\times = \mathcal{U}(F)$. We write $SL_n(D)$ for the subgroup of $GL_n(D)$ consisting of matrices of reduced norm one. When D is a field, γ is simply the identity map, and $SL_n(D)$ agrees with our original definition.

§2.5 Algebraic Number Theory

Let A be a $\mathbb{Q}$-algebra. An element $\alpha \in A$ is said to be **integral** over $\mathbb{Z}$, if it satisfies a monic polynomial in $\mathbb{Z}[x]$. A basic result about integrality is

Proposition 2.5.1. *For an element α in a $\mathbb{Q}$-algebra A, the following are equivalent:*

(1) *α is integral over $\mathbb{Z}$;*
(2) *$(\mathbb{Z}[\alpha], +)$ is a finitely generated abelian group;*
(3) *$\mathbb{Z}[\alpha]$ is contained in a subring R of A, where $(R, +)$ is a finitely generated abelian group.*

Proof. [Re, Theorem 1.10] □

When A is a subfield of the complex numbers, the elements which are integral over $\mathbb{Z}$ are called the **algebraic integers.** It is clear that every rational integer is an algebraic integer. We also have the following result, which is [ST, Theorem 2.15].

Proposition 2.5.2. *If K is a subfield of $\mathbb{C}$, then its algebraic integers form a subring, O_K, of K containing $\mathbb{Z}$. If K is an algebraic number field, then O_K has a finite integral basis; that is, a subset $\{x_1, \ldots, x_n\}$ of O_K which is a $\mathbb{Z}$-basis of O_K, and a $\mathbb{Q}$-basis of K.*

The next result is an important one.

Theorem 2.5.3 (Dirichlet's Unit Theorem). *Let $\mathbb{Q}(\alpha)$, $\alpha \in \mathbb{C}$, be an algebraic number field. Let $m(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Let s be the number of real roots of $m(x)$, and let $2t$ be the number of non-real roots. Then the unit group of the ring of algebraic integers of $\mathbb{Q}(\alpha)$ is a finitely generated abelian group which is isomorphic to $C \times F$, where C is a finite cyclic group, and F is free abelian of rank $s + t - 1$.*

Proof. [ST, Theorem 12.6] □

We note that the number of non-real roots of a polynomial in $\mathbb{Q}[x]$ must be even, since if $\beta \in \mathbb{C}$ is a root, then so is its complex conjugate.

We say that a subfield F of $\mathbb{C}$ is an **imaginary quadratic extension of the rationals** if $[F : \mathbb{Q}] = 2$ and $F \not\subseteq \mathbb{R}$. It is easy to see that this holds if and only if $F = \mathbb{Q}(\sqrt{-n})$, for some natural number n. We deduce

Corollary 2.5.4. *Let $F = \mathbb{Q}(\alpha)$ be an algebraic number field, and O_F its ring of algebraic integers. Then $\mathcal{U}(O_F)$ is finite if and only if $F = \mathbb{Q}$, or F is an imaginary quadratic extension of the rationals.*

Proof. Clearly, the group $C \times F$ described in Dirichlet's Unit Theorem is finite if and only if the rank of F is zero. Thus, this is true if and only if either $s = 1, t = 0$, or $s = 0, t = 1$. In the former case, $\alpha \in \mathbb{Q}$; hence, $F = \mathbb{Q}$. In the latter, $[F : \mathbb{Q}] = 2$, and since α is among the roots of $m(x)$, $\alpha \notin \mathbb{R}$, so $F \not\subseteq \mathbb{R}$. □

Suppose, now, that ξ_n is a primitive n^{th} root of unity, in $\mathbb{C}$. Then ξ_n is certainly an algebraic integer, and therefore, $\mathbb{Z}[\xi_n]$ is contained in the ring of algebraic integers of $\mathbb{Q}(\xi_n)$. In fact, more is true, and we give this well-known result, which is [CR1, Theorem 21.13].

Theorem 2.5.5. *The ring of algebraic integers of $\mathbb{Q}(\xi_n)$ is $\mathbb{Z}[\xi_n]$.*

Chapter 3

General Results

In this chapter, our goal is to obtain some units (specifically, the bicyclic and Bass cyclic units) which, under appropriate restrictions on the Wedderburn components of $\mathbb{Q}G$ and the homomorphic images of G, will generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$, for a finite group G.

Here is our plan of attack. In the first section, we will prove some easy (but extremely useful) results about orders in $\mathbb{Q}$-algebras. In the second and third sections, we introduce the Bass cyclic units, and use a result of Bass and Milnor to obtain a reduction in the problem, due to Ritter and Sehgal. In the fourth section, we demonstrate that certain Wedderburn components of $\mathbb{Q}G$ are harmless. We deduce from this that for any abelian group, the Bass cyclic units alone generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. In the fifth and sixth sections, we present the results of Jespers and Leal, which give conditions under which the Bass cyclic and bicyclic units suffice.

§3.1 Orders

We say that a subring R of S is a **unital subring** if $1_R = 1_S$.

Let A be a finite-dimensional $\mathbb{Q}$-algebra. Then a unital subring, Λ, of A, is said to be an **order** (or $\mathbb{Z}$-order), if $(\Lambda, +)$ is a finitely generated group, and $\mathbb{Q}\Lambda = A$. Let us give some easy examples of orders.

Example 3.1.1. (a) If K is an algebraic number field, then its ring of integers is an order in K. This is immediate from the existence of the integral basis, which we pointed out in Proposition 2.5.2.

(b) For any finite group G, $\mathbb{Z}G$ is an order in $\mathbb{Q}G$. No comment is necessary.

In fact, if Λ is an order in A, then $(\Lambda, +)$ is a free abelian group of rank $\dim_{\mathbb{Q}} A$. Indeed, if for some natural number n, and $\lambda \in \Lambda$, we had $n\lambda = 0$, then (working in A), $0 = (1/n)n\lambda = \lambda$. Thus, $(\Lambda, +)$ is torsion-free, and since it is a finitely generated abelian group, it is free of finite rank. Let $\{\lambda_1, \dots, \lambda_n\}$ be a $\mathbb{Z}$-basis for Λ. If $n > \dim_{\mathbb{Q}} A$, then this set is linearly dependent over $\mathbb{Q}$. That is, there exist $q_1, \dots, q_n \in \mathbb{Q}$, not all zero, such that $q_1\lambda_1 + \cdots + q_n\lambda_n = 0$. If t is the least common multiple of the denominators of the q_i, then $tq_1\lambda_1 + \cdots + tq_n\lambda_n = 0$, with each $tq_i \in \mathbb{Z}$, and not all zero. This contradicts freeness. Thus, $n \leq dim_{\mathbb{Q}}A$. But since $\mathbb{Q}\Lambda = A$, $\lambda_1, \ldots, \lambda_n$ generate A as a vector space, so $n \geq dim_{\mathbb{Q}}A$.

Suppose Λ is an order in A. Take $a \in A$. Because $\mathbb{Q}\Lambda = A$, there exist $q_1, \ldots, q_n \in \mathbb{Q}$ and $\lambda_1, \ldots, \lambda_n \in \Lambda$ such that $a = q_1\lambda_1 + \cdots + q_n\lambda_n$. Let t be the least common denominator for the q_i terms. Then, we actually have an expression of the form

$$a = \frac{1}{t}(z_1\lambda_1 + \cdots + z_n\lambda_n)$$

with each $z_i \in \mathbb{Z}$. That is, the expression in brackets on the right hand side is in Λ. Thus, there exist $\mu \in \Lambda$, and a nonzero integer t, with $a = (1/t)\mu$. Conversely, if for every $a \in A$, there exist a nonzero integer t and $\mu \in \Lambda$ with $a = (1/t)\mu$, then the condition $A = \mathbb{Q}\Lambda$ is obviously satisfied. Thus, we may substitute this condition, when it is convenient.

Some obvious facts are given in

Proposition 3.1.2. *(a) If Λ is an order in A, then $M_n(\Lambda)$ is an order in $M_n(A)$, for any natural number n.*

(b) If $\pi : A \to B$ is a homomorphism of $\mathbb{Q}$-algebras, and Λ is an order in A, then $\pi(\Lambda)$ is an order in $\pi(A)$.

(c) If Λ_i is an order in A_i, $1 \leq i \leq n$, then $\Lambda_1 \oplus \cdots \oplus \Lambda_n$ is an order in $A_1 \oplus \cdots \oplus A_n$.

Proof. (a) If the set $\{\lambda_1, \ldots, \lambda_r\}$ generates $(\Lambda, +)$, and if we let $E_{i,j}$ be the $n \times n$ matrix with a 1 in the (i,j) position, and 0 elsewhere, then it is clear that the set $\{\lambda_k E_{i,j} : 1 \leq k \leq r, 1 \leq i,j \leq n\}$ generates $M_n(\Lambda)$. If $\alpha \in M_n(A)$ has coefficients $\alpha_{i,j}$, then by our above remarks, there exist nonzero integers $t_{i,j}$, and $\lambda_{i,j} \in \Lambda$ such that $\alpha_{i,j} = (1/t_{i,j})\lambda_{i,j}$. That is, $t_{i,j}\alpha_{i,j} \in \Lambda$ for each pair (i,j). If we let t be the product of all of the $t_{i,j}$ terms, then t is a nonzero integer, and $t\alpha_{i,j} \in \Lambda$ for each pair (i,j). That is, $t\alpha \in M_n(\Lambda)$. Again, by our above remarks, we have $\mathbb{Q}M_n(\Lambda) = M_n(A)$. We are done.

Parts (b) and (c) are completely trivial. □

As we will be dealing with orders in division algebras, we had better make sure that we are not talking in a vacuum.

Lemma 3.1.3. *Let D be a division algebra, which is finite-dimensional over its centre, F, an algebraic number field. Then D has an order. In fact, this order may be chosen such that it contains the ring of algebraic integers O_F of F.*

Proof. Using the terminology of Lemma 2.4.1, let $\beta : D \otimes_F E \to M_{s(D)}(E)$ be the isomorphism. By Example 3.1.1, the ring of integers O_E of E is an order in E. Thus, by Proposition 3.1.2, $M_{s(D)}(O_E)$ is an order in $M_{s(D)}(E)$. We identify D

with $D\otimes 1 \subseteq D\otimes_F E$. Let $\Lambda = \beta^{-1}(M_{s(D)}(O_E)) \cap (D\otimes 1)$. Since $(M_{s(D)}(O_E), +)$ is a finitely generated abelian group, so is $(\beta^{-1}(M_{s(D)}(O_E)), +)$, and therefore, so is any subgroup, such as $(\Lambda, +)$. If we take $d \in D$, then $\beta(d \otimes 1) \in M_{s(D)}(E)$, which means that there exist a nonzero integer t, and $\alpha \in M_{s(D)}(O_E)$, satisfying $\beta(d \otimes 1) = (1/t)\alpha$. Hence,

$$d \otimes 1 = \beta^{-1}((1/t)\alpha) = (1/t)\beta^{-1}(\alpha)$$

(by $\mathbb{Q}$-linearity). Since $d\otimes 1 \in D\otimes 1$, so is $t(d\otimes 1) = \beta^{-1}(\alpha)$. That is, $\beta^{-1}(\alpha) \in \Lambda$, and $d \otimes 1 = (1/t)\beta^{-1}(\alpha)$ for a nonzero integer t. Therefore, Λ is an order in D.

Now, let Λ be any order in D. If the set $\{\lambda_1, \dots, \lambda_n\}$ generates $(\Lambda, +)$, and $\{\mu_1, \dots, \mu_m\}$ generates $(O_F, +)$, then since O_F centralizes Λ, it is clear that the set $\{\lambda_i\mu_j : 1 \le i \le n, 1 \le j \le m\}$ generates $(\Lambda O_F, +)$, where

$$\Lambda O_F = \{a_1 b_1 + \cdots + a_t b_t : a_i \in \Lambda, b_i \in O_F, t > 0\}.$$

Since $\mathbb{Q}\Lambda = D$, $\mathbb{Q}\Lambda O_F = D$. Again, since O_F centralizes Λ, ΛO_F is easily seen to be a unital subring of D. Therefore, it is an order containing both Λ and O_F. □

Proposition 3.1.4. *Let D be a division algebra which is finite-dimensional over $\mathbb{Q}$. Then for any natural number n, $M_n(D)$ has an order.*

Proof. Combine Lemma 3.1.3 and Proposition 3.1.2(a). □

We will have occasion to use

Proposition 3.1.5. *Every element of an order Λ, in A, is integral over $\mathbb{Z}$.*

Proof. If $\alpha \in \Lambda$, then $\mathbb{Z}[\alpha] \subseteq \Lambda$, where $(\Lambda, +)$ is finitely generated. By Proposition 2.5.1, α is integral over $\mathbb{Z}$. □

Now, suppose Λ_1 and Λ_2 are two orders in A. Then, it is clear that $\Lambda_1 \cap \Lambda_2$ is a unital subring of A, and since $(\Lambda_1, +)$ is finitely generated, so is its subgroup, $(\Lambda_1 \cap \Lambda_2, +)$. If $a \in A$, then we may choose nonzero integers t_1 and t_2, $\lambda_1 \in \Lambda_1$, and $\lambda_2 \in \Lambda_2$, such that

$$a = \frac{1}{t_1}\lambda_1 = \frac{1}{t_2}\lambda_2.$$

That is, $t_1 a \in \Lambda_1$, and $t_2 a \in \Lambda_2$. Thus, $t_1 t_2 a \in \Lambda_1 \cap \Lambda_2$. In other words, there exists $\lambda \in \Lambda_1 \cap \Lambda_2$ satisfying

$$a = \frac{1}{t_1 t_2}\lambda.$$

We have proved

Proposition 3.1.6. *If Λ_1 and Λ_2 are orders in A, then so is $\Lambda_1 \cap \Lambda_2$.*

Perhaps the most useful result of all will be

Theorem 3.1.7. *Let Λ_1 and Λ_2 be two orders in A, with $\Lambda_1 \subseteq \Lambda_2$. Then*
(a) $|\Lambda_2 : \Lambda_1| < \infty$;
(b) $|\mathcal{U}(\Lambda_2) : \mathcal{U}(\Lambda_1)| < \infty$.

Proof. (a) We know that $(\Lambda_2, +)$ and $(\Lambda_1, +)$ are finitely generated abelian groups of the same rank. Thus, the index of one in the other is finite.

(b) From part (a), we may choose a natural number m such that $m\Lambda_2 \subseteq \Lambda_1$. Suppose that $x, y \in \mathcal{U}(\Lambda_2)$ are in different left cosets of $\mathcal{U}(\Lambda_1)$. That is, $x\mathcal{U}(\Lambda_1) \neq y\mathcal{U}(\Lambda_1)$. Suppose, on the other hand, that x and y are in the same coset of $m\Lambda_2$ in Λ_2. That is, $x - y \in m\Lambda_2$. Since $y \in \Lambda_2$, it follows that

$$y^{-1}x - 1 = y^{-1}(x - y) \in m\Lambda_2 \subseteq \Lambda_1.$$

Since $1 \in \Lambda_1$, $y^{-1}x \in \Lambda_1$. Interchanging the roles of x and y, we find out that $x^{-1}y \in \Lambda_1$. Therefore, $x^{-1}y \in \mathcal{U}(\Lambda_1)$, which means that $x\mathcal{U}(\Lambda_1) = y\mathcal{U}(\Lambda_1)$, a contradiction. That is, different left cosets of $\mathcal{U}(\Lambda_1)$ in $\mathcal{U}(\Lambda_2)$ yield different cosets of $m\Lambda_2$ in Λ_2. Thus,

$$|\mathcal{U}(\Lambda_2) : \mathcal{U}(\Lambda_1)| \leq |\Lambda_2 : m\Lambda_2| = m^k < \infty,$$

where k is the rank of $(\Lambda_2, +)$. We are done. □

A final observation is

Proposition 3.1.8. *If $\Lambda_1 \subseteq \Lambda_2$ are orders in A, $u \in \Lambda_1$, and $u \in \mathcal{U}(\Lambda_2)$, then $u \in \mathcal{U}(\Lambda_1)$.*

Proof. Since $u \in \mathcal{U}(\Lambda_2)$, we have $u\Lambda_2 = \Lambda_2$. Thus, $|\Lambda_2 : u\Lambda_1| = |u\Lambda_2 : u\Lambda_1|$. Now, if $x_1, x_2 \in \Lambda_2$, and ux_1, ux_2 are in different cosets of $u\Lambda_1$ in Λ_2 (that is, if $u(x_1 - x_2) \notin u\Lambda_1$), then certainly $x_1 - x_2 \notin \Lambda_1$. Thus,

$$|\Lambda_2 : u\Lambda_1| = |u\Lambda_2 : u\Lambda_1| \leq |\Lambda_2 : \Lambda_1| < \infty$$

(by Theorem 3.1.7(a)). However, $u\Lambda_1 \leq \Lambda_1$ and, therefore,

$$|\Lambda_2 : \Lambda_1| \leq |\Lambda_2 : u\Lambda_1| \leq |\Lambda_2 : \Lambda_1| < \infty.$$

It follows that $u\Lambda_1 = \Lambda_1$, and therefore, $u \in \mathcal{U}(\Lambda_1)$. □

§3.2 The Bass Cyclic Units

For a natural number m, let $\xi_m = e^{2\pi i/m}$, a primitive m^{th} root of unity. Let φ be the Euler function; that is, $\varphi(m)$ is the number of natural numbers, less than or equal to m, which are coprime to m. We begin with a useful lemma.

Lemma 3.2.1. *Let $C_n = \langle x \rangle$ be a cyclic group of order n. Then the $\mathbb{Q}$-algebra homomorphism*

$$\kappa : \mathbb{Q}C_n \to \bigoplus_{d|n} \mathbb{Q}(\xi_d),$$

given by $\kappa(x) = (\xi_d)_{d|n}$ is an isomorphism. In particular, $\bigoplus_{d|n} \mathbb{Q}(\xi_d)$ is the Wedderburn decomposition of $\mathbb{Q}C_n$.

Proof. Suppose κ is not injective. Then there exist $q_1, \ldots, q_n \in \mathbb{Q}$, not all zero, such that

$$0 = \kappa(\sum_{i=0}^{n-1} q_i x^i) = (\sum_{i=0}^{n-1} q_i \xi_d^i)_{d|n}.$$

That is, $\sum_{i=0}^{n-1} q_i \xi_d^i = 0$, for each d dividing n. Now, if $1 \leq r \leq d$, and $(r,d) = 1$, then ξ_d^r is a primitive d^{th} root of unity. Thus, there is a field homomorphism $\alpha : \mathbb{Q}(\xi_d) \to \mathbb{C}$, with $\alpha(\xi_d) = \xi_d^r$, and $\alpha(q) = q$, for all $q \in \mathbb{Q}$. Hence,

$$0 = \alpha(\sum_{i=0}^{n-1} q_i \xi_d^i) = \sum_{i=0}^{n-1} q_i \xi_d^{ri}.$$

Now, if $1 \leq m \leq n$, write $\frac{m}{n} = \frac{s}{t}$, in lowest terms. That is, t divides n, $1 \leq s \leq t$, and $(s,t) = 1$. Thus, taking $d = t$, and $r = s$, we have

$$0 = \sum_{i=0}^{n-1} q_i \xi_t^{si} = \sum_{i=0}^{n-1} q_i \xi_n^{mi},$$

for all natural numbers $m \leq n$. Hence, if we let M be the $n \times n$ matrix whose $(i,j)^{\text{th}}$ entry is $\xi_n^{(i-1)j}$, then M is singular. But M is a Vandermonde matrix, which is always invertible. We have a contradiction; hence, κ is injective.

We further observe that $\dim_{\mathbb{Q}} \mathbb{Q}C_n = n$, and $\dim_{\mathbb{Q}}(\bigoplus_{d|n} \mathbb{Q}(\xi_d)) = \sum_{d|n} \varphi(d) = n$. Thus, κ is surjective as well, as required. That $\bigoplus_{d|n} \mathbb{Q}(\xi_d)$ is the Wedderburn decomposition follows from uniqueness. □

Let $\langle x\rangle$ be a cyclic group of order n. Fix a positive multiple, m, of $\varphi(n)$. Let $1 < i < n$, where i is coprime to n. Then, by Fermat's Little Theorem, we know that $i^m \equiv 1 \pmod{n}$. Henceforth, let us write

$$\hat{x} = 1 + x + x^2 + \cdots + x^{n-1}.$$

Let k be the integer such that $i^m = 1 + kn$. Then the elements of the form

$$(1 + x + x^2 + \cdots + x^{i-1})^m - k\hat{x} \in \mathbb{Z}\langle x\rangle$$

are called **Bass cyclic units**. They were introduced by Bass in [Ba2]. Notice that if $n = 1$ or 2, there are no Bass cyclic units.

It is not transparently obvious that the Bass cyclic units are, indeed, units. We must prove

Proposition 3.2.2. *The Bass cyclic units are in $\mathcal{U}(\mathbb{Z}\langle x\rangle)$.*

Proof. Let $G = \langle x\rangle$. By the definition of κ in Lemma 3.2.1, it is clear that $\kappa(\mathbb{Z}G) \subseteq \bigoplus_{d|n} \mathbb{Z}[\xi_d]$. Now, $\mathbb{Z}[\xi_d]$ is an order in $\mathbb{Q}(\xi_d)$, so Proposition 3.1.2(c) tells us that $\bigoplus_{d|n} \mathbb{Z}[\xi_d]$ is an order in $\bigoplus_{d|n} \mathbb{Q}(\xi_d)$. Since $\mathbb{Z}G$ is an order in $\mathbb{Q}G$, we know that $\kappa(\mathbb{Z}G)$ is also an order in $\kappa(\mathbb{Q}G) = \bigoplus_{d|n} \mathbb{Q}(\xi_d)$. Let

$$u = (1 + x + \cdots + x^{i-1})^m - k\hat{x}.$$

Then, by Proposition 3.1.8, if $\kappa(u)$ is a unit in $\bigoplus_{d|n} \mathbb{Z}[\xi_d]$, it must be a unit in $\kappa(\mathbb{Z}G)$. Since κ is an isomorphism, in this case, u would be a unit in $\mathbb{Z}G$.

Now, $\kappa(u)$ is a unit in $\bigoplus_{d|n} \mathbb{Z}[\xi_d]$ if and only if its projection into each component is a unit. That is, we wish to show that

$$(1 + \xi_d + \xi_d^2 + \cdots + \xi_d^{i-1})^m - k(1 + \xi_d + \cdots + \xi_d^{n-1}) \in \mathcal{U}(\mathbb{Z}[\xi_d]),$$

for each d dividing n. Now, the polynomial $1 + y + y^2 + \cdots + y^{n-1}$ may be rewritten $\frac{1-y^n}{1-y}$. Thus, if $y \neq 1$ satisfies $y^n = 1$, then $1 + y + \cdots + y^{n-1} = 0$. Hence, if $d \neq 1$, then

$$(1+\xi_d+\cdots+\xi_d^{i-1})^m - k(1+\xi_d+\cdots+\xi_d^{n-1}) = (1+\xi_d+\cdots+\xi_d^{i-1})^m = \left(\frac{1-\xi_d^i}{1-\xi_d}\right)^m.$$

Since $(i, n) = 1$, we have $(i, d) = 1$. Thus, there exists an integer h such that $hi \equiv 1 \pmod{d}$. (Since adding multiples of d has no effect, we may assume that $h > 0$). Thus, we have $\xi_d = \xi_d^{hi}$. Hence,

$$\frac{1-\xi_d}{1-\xi_d^i} = \frac{1-\xi_d^{hi}}{1-\xi_d^i} = 1 + \xi_d^i + \xi_d^{2i} + \cdots + \xi_d^{(h-1)i} \in \mathbb{Z}[\xi_d].$$

But this is the inverse of $\frac{1-\xi_d^i}{1-\xi_d}$; hence, $\frac{1-\xi_d^i}{1-\xi_d}$ is invertible in $\mathbb{Z}[\xi_d]$, as required.

When $d = 1$, $(1+1^2+\cdots+1^{i-1})^m - k(1+\cdots+1^{n-1}) = i^m - kn = 1$, which is certainly invertible. We are done. □

For a finite group G, the Bass cyclic units corresponding to each $x \in G$, with $m = \varphi(|G|)$, are called the **Bass cyclic units of $\mathbb{Z}G$**. (We observe that if $x \in G$, $\varphi(|x|)|\varphi(|G|)$, since $|x|\,||G|$). The subgroup of $\mathcal{U}(\mathbb{Z}G)$ generated by these units is denoted $\mathcal{B}_1$. That is,

$$\mathcal{B}_1 = \langle (1+x+\cdots+x^{i-1})^{\varphi(|G|)} + \frac{1-i^{\varphi(|G|)}}{|x|}\hat{x} : x \in G, 1 < i < |x|, (i,|x|) = 1 \rangle.$$

A result of Bass and Milnor, which we present next, involves algebraic K-theory. We shall assume it as the starting point of our investigations, but to understand it, we will need some terminology. We refer the reader to [CR3, Chapter 5] for more information.

For any ring R, and natural number n, we let $GL_n(R)$ be the group of invertible $n \times n$ matrices over R. We see that, if $m < n$, then $GL_m(R)$ is embedded in $GL_n(R)$ under the map

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & I_{n-m} \end{pmatrix},$$

where I_{n-m} is the $(n-m) \times (n-m)$ identity matrix. We let $GL(R)$ (with no subscript) denote the set of equivalence classes of the set $\bigcup_{n=1}^{\infty} GL_n(R)$, where the $m \times m$ matrix A and the $n \times n$ matrix B are in the same equivalence class provided: 1) $m = n$, $A = B$; 2) $m > n$, $A = \begin{pmatrix} B & 0 \\ 0 & I_{m-n} \end{pmatrix}$; or 3) $n > m$, $B = \begin{pmatrix} A & 0 \\ 0 & I_{n-m} \end{pmatrix}$. Clearly, this is an equivalence relation.

Now, $GL(R)$ is a group, where the multiplication of two equivalence classes $[A]$ and $[B]$ is defined as follows. Choose a natural number n such that $[A]$ contains some $n \times n$ matrix A_1, and $[B]$ contains some $n \times n$ matrix B_1. (This is certainly possible, if we take n to be sufficiently large). Then we let $[A][B] = [A_1B_1]$. It is obvious that the choice of n is irrelevant, since adding more ones down the diagonal in each of A_1 and B_1 will simply add more ones down the diagonal in their product. The verification that this is a group operation is entirely trivial.

Now, it is clear that the derived subgroup $[GL(R), GL(R)]$ consists of equivalence classes containing, for some natural number m, an $m \times m$ matrix A in $[GL_m(R), GL_m(R)]$. We define

$$K_1(R) = GL(R)/[GL(R), GL(R)].$$

This is an abelian group, known as the **Whitehead group** of R. If $[A]$ is an equivalence class in $GL(R)$, we will write $[A]^*$ for the element $[A][GL(R), GL(R)]$ of $K_1(R)$.

Now, we identify $\mathcal{U}(R)$ with $GL_1(R)$, and so we may define the **natural homomorphism** $j : \mathcal{U}(R) \to K_1(R)$ via $j(u) = [(u)]^*$. (We may denote this map by j_R, when the ring is in question).

Let R be a unital subring of S. Then, any commutator in $GL_n(R)$ is certainly a commutator in $GL_n(S)$. Thus, the inclusion map $GL_n(R) \to GL_n(S)$ induces a homomorphism $\epsilon_{R,S} : K_1(R) \to K_1(S)$. If we let $\iota_{R,S} : \mathcal{U}(R) \to \mathcal{U}(S)$ be the inclusion map, then it is completely clear that $\epsilon_{R,S} \circ j_R = j_S \circ \iota_{R,S}$.

If R is commutative, then the determinant map is a homomorphism,

$$\det : GL_n(R) \to \mathcal{U}(R),$$

for each natural number n. Since elements of an equivalence class in $GL(R)$ have the same determinant, the map det induces a map

$$\mu : GL(R) \to \mathcal{U}(R),$$

where $\mu([A]) = \det A$. Now, if $A, B \in GL_n(R)$, then

$$\det([A, B]) = (\det A)^{-1}(\det B)^{-1}(\det A)(\det B) = 1,$$

by commutativity. It follows that $[GL(R), GL(R)] \leq \ker \mu$. Thus, μ induces a homomorphism

$$\nu : K_1(R) \to \mathcal{U}(R),$$

where $\nu([A]^*) = \det A$. We define $SK_1(R) = \ker \nu$. Take an equivalence class $[A] \in GL(R)$, and let us say A is $n \times n$, with $\det A = r \in \mathcal{U}(R)$. Then, the $n \times n$ diagonal matrix

$$M = \begin{pmatrix} r & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

also has determinant r, and $[M] = [(r)]$; hence, $[M]^* = [(r)]^* \in j(\mathcal{U}(R))$. Further,

$$\begin{aligned} \nu([M^{-1}A]^*) &= \nu([M^{-1}]^*)\nu([A]^*) \\ &= \nu([(r^{-1})]^*)\nu([A]^*) \\ &= r^{-1}r \\ &= 1. \end{aligned}$$

That is, $[M^{-1}A]^* \in SK_1(A)$. But $[A]^* = [M]^*[M^{-1}A]^*$, implying that $SK_1(R)$ and $j(\mathcal{U}(R))$ together generate $K_1(R)$. It is time to state the results which we will have to assume.

Lemma 3.2.3. *Let $\langle x \rangle$ be a finite cyclic group, and let m be a multiple of $\varphi(|x|)$. Then the Bass cyclic units corresponding to the x^i, $1 \leq i \leq |x|$, using m as the fixed multiple of $\varphi(|x^i|)$, generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}\langle x \rangle)$.*

Proof. See [Ba2, Theorem 4], and the remark which follows it. □

We will also assume the following lemma, which is [Ba2, Theorem 2].

Lemma 3.2.4. *Let G be a finite group. Then the subgroup*

$$\langle \epsilon_{\mathbb{Z}\langle x \rangle, \mathbb{Z}G}(K_1(\mathbb{Z}\langle x \rangle)) : x \in G \rangle$$

of $K_1(\mathbb{Z}G)$, is of finite index in $K_1(\mathbb{Z}G)$.

These results give us

Theorem 3.2.5 (Bass-Milnor). *Let G be a finite group. Then $j(\mathcal{B}_1)$ is of finite index in $K_1(\mathbb{Z}G)$.*

Proof. Take $x \in G$, and let m be any positive multiple of $\varphi(|x|)$. Then, we let $\mathcal{B}_x$ be the group generated by the Bass cyclic units described in Lemma 3.2.3, which is of finite index in $\mathcal{U}(\mathbb{Z}\langle x \rangle)$. By [CR3, Theorem 48.1], $SK_1(\mathbb{Z}\langle x \rangle) = 1$. Thus, by our above remarks,

$$j_{\mathbb{Z}\langle x \rangle}(\mathcal{U}(\mathbb{Z}\langle x \rangle)) = K_1(\mathbb{Z}\langle x \rangle).$$

Therefore, $j_{\mathbb{Z}\langle x \rangle}(\mathcal{B}_x)$ is of finite index in $K_1(\mathbb{Z}\langle x \rangle)$. Let us say that this index is n_x.

By Lemma 3.2.4, the subgroup

$$\langle \epsilon_{\mathbb{Z}\langle x \rangle, \mathbb{Z}G}(K_1(\mathbb{Z}\langle x \rangle)) : x \in G \rangle$$

is of finite index in $K_1(\mathbb{Z}G)$. Let us say that this index is q. Then, since $K_1(\mathbb{Z}G)$ is abelian, it follows that the images under $\epsilon_{\mathbb{Z}\langle x \rangle, \mathbb{Z}G} \circ j_{\mathbb{Z}\langle x \rangle}$ of the various $\mathcal{B}_x$ generate a subgroup of index at most $q \prod_{x \in G} n_x$ in $K_1(\mathbb{Z}G)$; a finite number. Now, if we take $m = \varphi(|G|)$, then all of the Bass cyclic units we have described are among the Bass cyclic units of $\mathbb{Z}G$. Since $\epsilon_{\mathbb{Z}\langle x \rangle, \mathbb{Z}G} \circ j_{\mathbb{Z}\langle x \rangle} = j_{\mathbb{Z}G} \circ \iota_{\mathbb{Z}\langle x \rangle, \mathbb{Z}G}$, the images of the Bass cyclic units of $\mathbb{Z}G$ under $j_{\mathbb{Z}G}$ generate a subgroup of finite index in $K_1(\mathbb{Z}G)$. We are done. □

§3.3 The Main Reduction

Let us establish some notation, which we will keep for some time. For a finite group G, let e_i, $1 \leq i \leq t$, be the primitive central idempotents of $\mathbb{Q}G$. Then $\mathbb{Q}Ge_i \cong M_{n_i}(D_i)$, for some natural number n_i, and some finite-dimensional $\mathbb{Q}$-division algebra D_i. Let $\theta_i : \mathbb{Q}Ge_i \to M_{n_i}(D_i)$ be this isomorphism. Let $\pi_i : \mathbb{Q}G \to M_{n_i}(D_i)$ be the projection map; that is, $\pi_i(\eta) = \theta_i(\eta e_i)$, for all $\eta \in \mathbb{Q}G$. Let F_i be the centre of D_i, which will be an algebraic number field. Let O_i be the ring of algebraic integers of F_i. Let Λ_i be any order in $M_{n_i}(D_i)$, containing $\pi_i(\mathbb{Z}G)$. (For example, taking $\Lambda_i = \pi_i(\mathbb{Z}G)$ will suffice). Let $\mathcal{O}_i$ be any order in D_i which contains O_i. (The existence of such an $\mathcal{O}_i$ is guaranteed by Lemma 3.1.3). Thus, $M_{n_i}(\mathcal{O}_i)$ will be an order in $M_{n_i}(D_i)$. In addition, we name the isomorphism $\tau : \mathbb{Q}G \to \bigoplus M_{n_i}(D_i)$. That is, $\tau(\eta) = (\pi_i(\eta))_i$. Recall that $SL_{n_i}(D_i)$ denotes the group of invertible $n_i \times n_i$ matrices over D_i which have reduced norm one. We write $SL_{n_i}(\mathcal{O}_i) = SL_{n_i}(D_i) \cap GL_{n_i}(\mathcal{O}_i)$.

We should point out that in most of the literature in this area, the orders are assumed to be maximal; that is, not properly contained in any other orders. This assumption is not, however, required. Also, by Proposition 3.1.5, every element of an order is integral over $\mathbb{Z}$. Thus, when D_i is commutative, $\mathcal{O}_i \subseteq O_i$. However, we are assuming that $O_i \subseteq \mathcal{O}_i$. Therefore, in this case, we are forcing the choice $\mathcal{O}_i = O_i$.

Note that for any group or ring $\mathcal{A}$, we denote the centre of $\mathcal{A}$ by $Z(\mathcal{A})$. Let us begin by proving

Lemma 3.3.1. *The group $Z(\mathcal{U}(\mathbb{Z}G))$ is finitely generated.*

Proof. Clearly, $Z(\mathbb{Q}G)$ is a $\mathbb{Q}$-subalgebra of $\mathbb{Q}G$. Since $(\mathbb{Z}G, +)$ is finitely generated, its subgroup $(Z(\mathbb{Z}G), +)$ is finite generated. If $\alpha \in Z(\mathbb{Q}G)$, then there exists a natural number m such that $m\alpha \in \mathbb{Z}G$, and therefore, $m\alpha \in Z(\mathbb{Z}G)$. Thus, $Z(\mathbb{Z}G)$ is an order in $Z(\mathbb{Q}G)$. It follows that $\tau(Z(\mathbb{Z}G))$ is an order in $\tau(Z(\mathbb{Q}G)) = Z(\tau(\mathbb{Q}G)) = \bigoplus Z(M_{n_i}(D_i))$. Now, the centre of $M_{n_i}(D_i)$ consists of scalar multiples of the identity matrix, where the scalar is in $Z(D_i) = F_i$. That is, $\tau(Z(\mathbb{Q}G)) = \bigoplus F_i I_{n_i}$. Since O_i is an order in F_i, Proposition 3.1.2 tells us that $\bigoplus O_i I_{n_i}$ is an order in $\tau(Z(\mathbb{Q}G))$. Therefore, by Proposition 3.1.6, so is $\tau(Z(\mathbb{Z}G)) \cap \bigoplus O_i I_{n_i}$. Now, $\mathcal{U}(\bigoplus O_i I_{n_i}) = \prod \mathcal{U}(O_i) I_{n_i}$, and each $\mathcal{U}(O_i)$ is a finitely generated abelian group, by Dirichlet's Unit Theorem. Thus, $\prod \mathcal{U}(O_i) I_{n_i}$ is a finitely generated abelian group, and so is its subgroup, $\mathcal{U}((\bigoplus O_i I_{n_i}) \cap \tau(Z(\mathbb{Z}G)))$. Therefore, by Theorem 3.1.7,

$$|\mathcal{U}(\tau(Z(\mathbb{Z}G))) : \mathcal{U}(\bigoplus O_i I_{n_i} \cap \tau(Z(\mathbb{Z}G)))| < \infty.$$

Hence, $\mathcal{U}(\tau(Z(\mathbb{Z}G))) = \tau(\mathcal{U}(Z(\mathbb{Z}G)))$ is finitely generated. Since τ is an isomorphism, it follows that $\mathcal{U}(Z(\mathbb{Z}G))$ is finitely generated.

It remains only to show that $\mathcal{U}(Z(\mathbb{Z}G)) = Z(\mathcal{U}(\mathbb{Z}G))$. Suppose that α is in $\mathcal{U}(Z(\mathbb{Z}G))$. Then $\alpha^{-1} \in Z(\mathbb{Z}G)$, which certainly implies that $\alpha \in Z(\mathcal{U}(\mathbb{Z}G))$. If $\beta \in Z(\mathcal{U}(\mathbb{Z}G))$, then β commutes with each $g \in G$. Thus, β commutes with all of $\mathbb{Z}G$, and similarly for β^{-1}. It follows that $\beta \in \mathcal{U}(Z(\mathbb{Z}G))$. □

Another useful fact is

Lemma 3.3.2. *Let A be a subgroup of finite index in $SL_{n_i}(O_i)$. Let B be a subgroup of finite index in $GL_{n_i}(O_i) \cap Z(GL_{n_i}(D_i))$. Then A and B generate a subgroup of finite index in $GL_{n_i}(O_i)$.*

Proof. Let $\alpha \in M_{n_i}(O_i)$. Let γ be the map defined in Proposition 2.4.2. Since $M_{n_i}(O_i)$ is an order in $M_{n_i}(D_i)$, α is integral over $\mathbb{Z}$ (by Proposition 3.1.5). Let $m(x)$ be a monic integral polynomial which is satisfied by α. Since γ is $\mathbb{Q}$-linear, $m(\gamma(\alpha \otimes 1)) = 0$ as well. Therefore, the minimal polynomial, over $\mathbb{C}$, of $\gamma(\alpha \otimes 1) \in M_{ns(D_i)}(E)$, divides $m(x)$. (The notation is taken from Proposition 2.4.2). Since the roots of the characteristic polynomial of $\gamma(\alpha \otimes 1)$ are the same as those of the minimal polynomial, up to multiplicity, all roots of the characteristic polynomial are roots of $m(x)$. But, by definition, the roots of $m(x)$ are algebraic integers. Thus, all roots of the characteristic polynomial, and therefore, all of its coefficients, are algebraic integers. However, the constant term of the characteristic polynomial is $\pm\det(\gamma(\alpha \otimes 1))$. Thus, $nr(\alpha) = \det(\gamma(\alpha \otimes 1))$ is an algebraic integer. By Proposition 2.4.3, $nr(\alpha) \in F_i$. Hence, $nr(\alpha) \in O_i$. If we take $\alpha \in GL_{n_i}(O_i)$, then everything we have just said about α could be said about α^{-1}. Therefore, $nr(\alpha)^{-1} = nr(\alpha^{-1}) \in O_i$. That is, $nr(\alpha) \in \mathcal{U}(O_i)$. Therefore, we have a homomorphism

$$nr : GL_{n_i}(O_i) \rightarrow \mathcal{U}(O_i).$$

Since $\mathcal{U}(O_i)$ is abelian, it has a subgroup $\mathcal{U}(O_i)^{n_i s(D_i)}$. Let

$$\rho : GL_{n_i}(O_i) \rightarrow \mathcal{U}(O_i)/\mathcal{U}(O_i)^{n_i s(D_i)}$$

be the map obtained by applying the reduced norm, and then projecting onto $\mathcal{U}(O_i)/\mathcal{U}(O_i)^{n_i s(D_i)}$.

Suppose $\alpha \in \ker \rho$. Let us say $nr(\alpha) = \omega^{n_i s(D_i)}$, with $\omega \in \mathcal{U}(O_i)$. Then we have the $n_i \times n_i$ matrix

$$\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix} \in GL_{n_i}(O_i) \cap Z(GL_{n_i}(D_i)).$$

Further, since γ is F-linear,

$$\gamma\left(\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix} \otimes 1\right) = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix} \in GL_{n_i s(D_i)}(O_i).$$

Thus,

$$nr\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix} = \omega^{n_i s(D_i)}.$$

Hence,

$$nr\left(\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}^{-1} \alpha\right) = 1;$$

that is,

$$\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}^{-1} \alpha \in SL_{n_i}(\mathcal{O}_i).$$

But

$$\alpha = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}\left(\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}^{-1} \alpha\right),$$

so we conclude that

$$\ker\rho \leq \langle SL_{n_i}(\mathcal{O}_i), GL_{n_i}(\mathcal{O}_i) \cap Z(GL_{n_i}(D_i))\rangle,$$

where we have used the fact that $O_i \subseteq \mathcal{O}_i$ to see that $GL_{n_i}(O_i) \subseteq GL_{n_i}(\mathcal{O}_i)$.

Now, $GL_{n_i}(\mathcal{O}_i)/\ker\rho$ is isomorphic to a subgroup of $\mathcal{U}(O_i)/\mathcal{U}(O_i)^{n_i s(D_i)}$. By Dirichlet's Unit Theorem, $\mathcal{U}(O_i)$ is a finitely generated abelian group. Thus, $\mathcal{U}(O_i)/\mathcal{U}(O_i)^{n_i s(D_i)}$ is finite. We conclude that $GL_{n_i}(\mathcal{O}_i)/\ker\rho$ is finite, and therefore,

$$|GL_{n_i}(\mathcal{O}_i) : \langle SL_{n_i}(\mathcal{O}_i), GL_{n_i}(\mathcal{O}_i) \cap Z(GL_{n_i}(D_i))\rangle| < \infty.$$

Since B is central in $GL_{n_i}(\mathcal{O}_i)$, if $|GL_{n_i}(\mathcal{O}_i) \cap Z(GL_{n_i}(D_i)) : B| = r_1$, and $|SL_{n_i}(\mathcal{O}_i) : A| = r_2$, then

$$|\langle GL_{n_i}(\mathcal{O}_i) \cap Z(GL_{n_i}(D_i)), SL_{n_i}(\mathcal{O}_i)\rangle : \langle A, B\rangle| \leq r_1 r_2.$$

We conclude that $|GL_{n_i}(\mathcal{O}_i) : \langle A, B\rangle| < \infty$. □

Now, we will give a condition under which we get a subgroup of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$.

Lemma 3.3.3. *Let C be a subgroup of $\mathcal{U}(\mathbb{Z}G)$, such that for each i, C contains a subgroup C_i, satisfying $\pi_j(C_i) = 1$, if $i \neq j$, and such that $\pi_i(C_i)$ contains a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$. Then C, together with the Bass cyclic units of $\mathbb{Z}G$, will generate a group containing a subgroup of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$.*

Proof. Take $z \in Z(\mathcal{U}(\mathbb{Z}G))$. Then $j(z) \in K_1(\mathbb{Z}G)$, so by Theorem 3.2.5, there exists a natural number l such that $j(z)^l \in j(\mathcal{B}_1)$. That is, there is a $b \in \mathcal{B}_1$ such that $j(z^l b^{-1}) = 1$. Since we are in $K_1(\mathbb{Z}G)$, this means that there exists a natural number a, such that the $a \times a$ matrix

$$\begin{pmatrix} z^l b^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

is in $[GL_a(\mathbb{Z}G), GL_a(\mathbb{Z}G)]$. Now, we extend the map $\pi_i : \mathbb{Q}G \to M_{n_i}(D_i)$, to a map $\zeta_i : M_a(\mathbb{Q}G) \to M_{an_i}(D_i)$, in the following manner. We regard matrices in $M_{an_i}(D_i)$ as $a \times a$ grids of $n_i \times n_i$ matrices. Then, if $\alpha = (\alpha_{p,q})_{p,q} \in M_n(\mathbb{Q}G)$, we let the $(p,q)^{\text{th}}$ $n_i \times n_i$ matrix of $\zeta_i(\alpha)$ be $\pi_i(\alpha_{p,q})$. Clearly, ζ_i is a $\mathbb{Q}$-algebra homomorphism. We also observe that

$$\zeta_i \begin{pmatrix} z^l b^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} \pi_i(z^l b^{-1}) & & & \\ & I_{n_i} & & \\ & & \ddots & \\ & & & I_{n_i} \end{pmatrix}$$

is in $[GL_{an_i}(D_i), GL_{an_i}(D_i)]$, since the homomorphic image of a commutator is a commutator. Now, $nr : GL_{an_i}(D_i) \to \mathcal{U}(F_i)$. Since $\mathcal{U}(F_i)$ is commutative, the reduced norm of a commutator is 1. That is,

$$nr \begin{pmatrix} \pi_i(z^l b^{-1}) & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = 1.$$

By the definition of the map γ in Proposition 2.4.2, we see that

$$1 = nr \begin{pmatrix} \pi_i(z^l b^{-1}) & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = nr(\pi_i(z^l b^{-1}))1^{a-1} = nr(\pi_i(z^l b^{-1})).$$

That is, $\pi_i(z^l b^{-1}) \in SL_{n_i}(D_i)$, for each i.

We further observe that

$$\pi_i(z^l b^{-1}) \in \pi_i(\mathbb{Z}G) \subseteq \Lambda_i,$$

and similarly, $\pi_i(z^l b^{-1})^{-1} = \pi_i(bz^{-l}) \in \Lambda_i$. Thus, $\pi_i(z^l b^{-1}) \in \mathcal{U}(\Lambda_i)$. Since $M_{n_i}(\mathcal{O}_i)$ and Λ_i are both orders in $M_{n_i}(D_i)$, Proposition 3.1.6 tells us that $M_{n_i}(\mathcal{O}_i) \cap \Lambda_i$ is another order in $M_{n_i}(D_i)$. Therefore, by Theorem 3.1.7,

$$|\mathcal{U}(\Lambda_i) : \mathcal{U}(\Lambda_i \cap M_{n_i}(\mathcal{O}_i))| = r_i < \infty.$$

Let $r = \prod r_i$. Then, $\pi_i(z^l b^{-1})^r \in GL_{n_i}(\mathcal{O}_i)$, which, by centrality of z, means that

$$\pi_i(z^{lr} b^{-r}) \in GL_{n_i}(\mathcal{O}_i) \cap SL_{n_i}(D_i) = SL_{n_i}(\mathcal{O}_i).$$

We are given that $\pi_i(C_i)$ contains a subgroup of finite index, let us say k_i, in $SL_{n_i}(\mathcal{O}_i)$. Let $k = \prod k_i$. We conclude that $\pi_i(z^{klr} b^{-kr}) \in \pi_i(C_i)$. Thus,

$$(1, \dots, 1, \pi_i(z^{klr} b^{-kr}), 1, \dots, 1) \in \tau(C_i),$$

for each i. Multiplying these together for the various i, we get

$$(\pi_1(z^{klr} b^{-kr}), \pi_2(z^{klr} b^{-kr}), \dots) \in \tau(C).$$

That is, $\tau(z^{klr} b^{-kr}) \in \tau(C)$. Since τ is an isomorphism, $z^{klr} b^{-kr} \in C$. Since $b^{kr} \in \mathcal{B}_1$, we have $z^{klr} \in \langle \mathcal{B}_1, C \rangle$. To wit, the group

$$Z(\mathcal{U}(\mathbb{Z}G))/(Z(\mathcal{U}(\mathbb{Z}G)) \cap \langle \mathcal{B}_1, C \rangle)$$

is torsion. By Lemma 3.3.1, $Z(\mathcal{U}(\mathbb{Z}G))$ is a finitely generated abelian group. Therefore, every quotient of the group is finitely generated and abelian. Hence, the group

$$Z(\mathcal{U}(\mathbb{Z}G))/(Z(\mathcal{U}(\mathbb{Z}G)) \cap \langle \mathcal{B}_1, C \rangle)$$

is finite. □

In fact, a much stronger result holds. We will need to use this lemma a couple of times.

Lemma 3.3.4. *Let A be a finite-dimensional $\mathbb{Q}$-algebra. Let W_1 and W_2 be two orders in A. If N is a subgroup of $\mathcal{U}(A)$, and N contains a subgroup which is of finite index in $\mathcal{U}(W_1)$, then N also contains a subgroup which is of finite index in $\mathcal{U}(W_2)$.*

Proof. Let M be the subgroup of N which is of finite index in $\mathcal{U}(W_1)$. Since $W_1 \cap W_2$ is an order in A (by Proposition 3.1.6), it follows from Theorem 3.1.7 that $|\mathcal{U}(W_2) : \mathcal{U}(W_1 \cap W_2)| < \infty$. Now, $\mathcal{U}(W_1 \cap W_2) = \mathcal{U}(W_1) \cap \mathcal{U}(W_2)$. That is, $|\mathcal{U}(W_2) : \mathcal{U}(W_1) \cap \mathcal{U}(W_2)| < \infty$. Furthermore,

$$|\mathcal{U}(W_1) \cap \mathcal{U}(W_2) : M \cap \mathcal{U}(W_2)| \leq |\mathcal{U}(W_1) : M| < \infty.$$

We conclude that $M \cap \mathcal{U}(W_2)$ is of finite index in $\mathcal{U}(W_2)$. □

We are now in a position to give our main reduction.

Theorem 3.3.5 (Ritter-Sehgal). *Let C be a subgroup of $\mathcal{U}(\mathbb{Z}G)$, such that for each i, C contains a subgroup C_i satisfying $\pi_j(C_i) = 1$ if $i \neq j$, and such that $\pi_i(C_i)$ contains a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$. Then $\langle \mathcal{B}_1, C\rangle$ is of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

Proof. By Lemma 3.3.3, $\langle \mathcal{B}_1, C\rangle$ contains a subgroup which is of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$. Therefore, $\tau(\langle \mathcal{B}_1, C\rangle)$ contains a subgroup which is of finite index in $\tau(Z(\mathcal{U}(\mathbb{Z}G)))$. At the end of the proof of Lemma 3.3.1, we demonstrated that $Z(\mathcal{U}(\mathbb{Z}G)) = \mathcal{U}(Z(\mathbb{Z}G))$. Therefore, $\tau(\langle \mathcal{B}_1, C\rangle)$ contains a subgroup of finite index in $\tau(\mathcal{U}(Z(\mathbb{Z}G))) = \mathcal{U}(\tau(Z(\mathbb{Z}G)))$.

Since $Z(\mathbb{Z}G)$ is an order in $Z(\mathbb{Q}G)$, it follows that $\tau(Z(\mathbb{Z}G))$ is an order in

$$\tau(Z(\mathbb{Q}G)) = Z(\tau(\mathbb{Q}G)) = Z(\bigoplus M_{n_i}(D_i)) = \bigoplus Z(M_{n_i}(D_i)).$$

Now, $Z(M_{n_i}(D_i))$ consists of those matrices which are of the form zI_{n_i}, for $z \in Z(D_i) = F_i$. Hence, $\tau(Z(\mathbb{Q}G)) = \bigoplus F_i I_{n_i}$. Since O_i is an order in F_i, Proposition 3.1.2 informs us that $\bigoplus O_i I_{n_i}$ is an order in $\tau(Z(\mathbb{Q}G))$. Therefore, by Lemma 3.3.4, $\tau(\langle \mathcal{B}_1, C\rangle)$ contains a subgroup which is of finite index in $\mathcal{U}(\bigoplus O_i I_{n_i}) = \prod \mathcal{U}(O_i) I_{n_i}$. Hence, $\tau(\langle \mathcal{B}_1, C\rangle)$ contains a subgroup of the form $\prod K_i$, where each K_i is of finite index in $\mathcal{U}(O_i)I_{n_i}$. Now, if $\alpha \in Z(GL_{n_i}(D_i))$, then $A = aI_{n_i}$, for some $a \in Z(\mathcal{U}(D_i)) = \mathcal{U}(Z(D_i)) = \mathcal{U}(F_i)$. If $A \in GL_{n_i}(\mathcal{O}_i)$ as well, then $a \in \mathcal{U}(\mathcal{O}_i) \cap \mathcal{U}(F_i) = \mathcal{U}(\mathcal{O}_i \cap F_i) \leq \mathcal{U}(O_i)$, by Proposition 3.1.5. Therefore, K_i contains a subgroup of finite index in $GL_{n_i}(\mathcal{O}_i) \cap Z(GL_{n_i}(D_i))$. Further, by our choice of C_i, each $\pi_i(C_i)$ contains a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$. Therefore, by Lemma 3.3.2, $\tau(\langle \mathcal{B}_1, C\rangle)$ contains a subgroup of finite index in $\prod GL_{n_i}(\mathcal{O}_i) = \mathcal{U}(\bigoplus M_{n_i}(\mathcal{O}_i))$. Since $\bigoplus M_{n_i}(\mathcal{O}_i)$ is an order in $\bigoplus M_{n_i}(D_i)$, and so is $\bigoplus \Lambda_i$, it follows from Lemma 3.3.4 that $\tau(\langle \mathcal{B}_1, C\rangle)$ contains a subgroup of finite index in $\mathcal{U}(\bigoplus \Lambda_i)$.

However, we know that

$$\tau(\mathcal{U}(\mathbb{Z}G)) = \mathcal{U}(\tau(\mathbb{Z}G)) \subseteq \mathcal{U}(\bigoplus \pi_i(\mathbb{Z}G)) \subseteq \mathcal{U}(\bigoplus \Lambda_i).$$

Since $\tau(\langle \mathcal{B}_1, C\rangle)$ is of finite index in the unit group of the larger order, it is certainly of finite index in the unit group of the smaller order. Therefore, $\tau(\langle \mathcal{B}_1, C)$ is of finite index in $\tau(\mathcal{U}(\mathbb{Z}G))$. Since τ is an isomorphism, we are done. □

It is, perhaps, worth mentioning that in certain cases, the Bass cyclic units are extraneous. In fact, we can see immediately that they were only required to obtain a subgroup of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$. We deduce

Corollary 3.3.6. *Let C satisfy the same conditions as in Theorem 3.3.5. Suppose further that $Z(\mathcal{U}(\mathbb{Z}G))$ is finite. Then C is of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

Going a little further, we obtain

Corollary 3.3.7. *Let C satisfy the same conditions as in Theorem 3.3.5. Suppose that each F_i is either $\mathbb{Q}$, or an imaginary quadratic extension of the rationals. Then C is of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

Proof. The assumption assures us that $Z(\mathcal{U}(\mathbb{Z}G))$ is finite, and the result follows from Corollary 3.3.6. □

§3.4 The Trivial Case

In general, Wedderburn components of $\mathbb{Q}G$ which are division rings (that is, components where $n_i = 1$), will cause us a lot of trouble. In fact, the problem of finding a finite set of generators for $SL_1(\mathcal{O}_i)$, where $\mathcal{O}_i$ is an order in a division algebra, remains open. However, there are certain cases in which we will discover that $SL_1(\mathcal{O}_i)$ is finite. Clearly, in this case, we may take $C_i = 1$ in Theorem 3.3.5. Thus, we need not worry about such components. We adopt the same notation that we introduced at the beginning of §3.3.

The following result is obvious, but it must be stated.

Lemma 3.4.1. *If $n_i = 1$, and D_i is a field, then $SL_{n_i}(\mathcal{O}_i) = SL_1(\mathcal{O}_i) = 1$.*

Proof. When D_i is commutative, the reduced norm is simply the determinant. In the 1×1 case, the determinant is the identity map. □

We have presented all of the machinery which is necessary to prove

Theorem 3.4.2 (Bass-Milnor). *Let G be a finite abelian group. Then we have $|\mathcal{U}(\mathbb{Z}G) : \mathcal{B}_1| < \infty$.*

Proof. Since $\mathbb{Q}G$ is commutative, every Wedderburn component must be commutative. That is, each $n_i = 1$, and each D_i is a field. By Lemma 3.4.1, we may take $C = 1$ in Theorem 3.3.5. □

As an application of Corollary 3.3.7, let us find some groups G such that $\mathbb{Z}G$ has only trivial units. In the following lemma, let us denote the trace of a matrix M by tr M.

Lemma 3.4.3 (Berman-Higman). *Let G be a finite abelian group, and suppose that $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{Z}G$ satisfies $\alpha^n = 1$, for some natural number n. Then $\alpha = \pm g$, for some $g \in G$.*

Proof. Let T be the regular representation of G over $\mathbb{C}$. That is, $T(x)(y) = xy$, for all $x, y \in \mathbb{C}G$. Now, $\mathbb{C}G$ has G as a basis. If $g \in G$, the matrix of $T(g)$ with respect to this basis will have exactly one 1 in each column, and zeroes elsewhere. In particular, the position of the 1, in the column corresponding to $y \in G$, will be the position corresponding to $gy \in G$. If $g \neq 1$, then $gy \neq y$, for all $y \in G$. Thus, the 1 will never occur on the diagonal of $T(g)$. Therefore, tr $T(g) = 0$, if $g \neq 1$. However, tr $T(1) =$ tr $I_{|G|} = |G|$.

Now, $\alpha^n = 1$. Therefore, since T is a homomorphism, $T(\alpha)^n = 1$. Thus, the minimal polynomial of $T(\alpha)$ divides $x^n - 1$. Since the roots of this polynomial are distinct, $T(\alpha)$ is diagonalizable. Thus, $T(\alpha)$ is similar to a matrix

$$\begin{pmatrix} \xi_n^{i_1} & & \\ & \ddots & \\ & & \xi_n^{i_{|G|}} \end{pmatrix},$$

for a primitive n^{th} root of unity ξ_n, and integers $i_1, \ldots, i_{|G|}$. (The diagonal elements must be n^{th} roots of unity, since $T(\alpha)^n = 1$). Since the trace function is invariant under change of basis, we observe that tr $(T(\alpha)) = \sum_{j=1}^{|G|} \xi_n^{i_j}$, and tr $(T(\alpha)) = \sum_{g\in G} \alpha_g$ tr $T(g) = \alpha_1|G|$, by our above remarks. Thus, $\alpha_1|G| = \sum_{j=1}^{|G|} \xi_n^{i_j}$.

Let us suppose that $\alpha_1 \neq 0$. Then, since $\alpha_1 \in \mathbb{Z}$, $|\alpha_1|G|| \geq |G|$. But

$$|\sum_{j=1}^{|G|} \xi_n^{i_j}| \leq \sum_{j=1}^{|G|} |\xi_n^{i_j}| = \sum_{j=1}^{|G|} 1 = |G|,$$

with equality holding if and only if all of the $\xi_n^{i_j}$ are equal. Thus, $T(\alpha)$ is similar to

$$\begin{pmatrix} \xi_n^{i} & & \\ & \ddots & \\ & & \xi_n^{i} \end{pmatrix},$$

for some integer i. This matrix is central in $M_n(\mathbb{C})$, so it follows that

$$T(\alpha) = \begin{pmatrix} \xi_n^{i} & & \\ & \ddots & \\ & & \xi_n^{i} \end{pmatrix}.$$

This means that $\alpha y = \xi_n^i y$, for all $y \in G$. In particular, $\alpha = \alpha 1 = \xi_n^i$. However, $\alpha \in \mathbb{Z}G$. Thus, $\alpha = \pm 1$.

In general, since $\alpha \neq 0$, we may take $h \in G$, satisfying $\alpha_h \neq 0$. Then, since G is abelian,

$$(\alpha h^{-1})^{n|G|} = \alpha^{n|G|} h^{-|G|n} = 1^{|G|} 1^n = 1.$$

From the result we have just shown, either $(\alpha h^{-1})_1 = 0$, or $\alpha h^{-1} = \pm 1$. But $(\alpha h^{-1})_1 = \alpha_h \neq 0$. Therefore, $\alpha h^{-1} = \pm 1$, which means that $\alpha = \pm h$. □

This allows us to prove

Proposition 3.4.4 (Higman). *Let G be a finite abelian group of exponent $1, 2, 3, 4$, or 6. Then $\mathbb{Z}G$ has only trivial units.*

Proof. As we pointed out in the proof of Theorem 3.4.2, the Wedderburn components of $\mathbb{Q}G$ are algebraic number fields, F_i. Recalling that π_i is the projection $\mathbb{Q}G \to F_i$, we see that F_i is generated, as a field, by $\mathbb{Q}$ and the elements $\pi_i(g)$, for $g \in G$. Since $\pi_i(G)$ is a finite subgroup of $F_i^\times$, $\pi_i(G)$ must be cyclic. Thus, $F_i = \mathbb{Q}(\pi_i(h))$, for some $h \in G$. Now, $h^{\exp G} = 1$; hence, $\pi_i(h)$ is also an $(\exp G)^{\text{th}}$ root of unity. We conclude that $\pi_i(h)$ is a primitive k^{th} root of unity, for $k = 1, 2, 3, 4$, or 6. Now, if $k = 1$ or 2, then $F_i = \mathbb{Q}$. If $k = 3, 4$, or 6, then $[\mathbb{Q}(\xi_k) : \mathbb{Q}] = \varphi(k) = 2$. Thus, since $\xi_k \notin \mathbb{R}$, F_i is an imaginary quadratic extension of the rationals. Therefore, by Corollary 3.3.7, we do not need the Bass cyclic units. By Lemma 3.4.1, we do not need any other units. That is, $\mathcal{U}(\mathbb{Z}G)$ is finite. By Lemma 3.4.3, the torsion units of $\mathbb{Z}G$ are trivial. Thus, $\mathcal{U}(\mathbb{Z}G) = \pm G$. □

There is another type of division ring which will yield a finite $SL_1(\mathcal{O}_i)$, and we will introduce it now. A subfield, K, of $\mathbb{C}$, is said to be **totally real** if $\sigma(K) \subseteq \mathbb{R}$, for all embeddings $\sigma : K \to \mathbb{C}$. An element $\alpha \in K$, where K is totally real, is said to be **totally positive** if $\sigma(\alpha) > 0$ for all embeddings $\sigma : K \to \mathbb{C}$. Let D be a finite-dimensional algebra over its centre, K, which is an algebraic number field. Then D is called a **totally definite quaternion algebra** provided K is totally real, and there exist $x, y \in D$, such that the elements of D are uniquely of the form $\alpha_1 + \alpha_2 x + \alpha_3 y + \alpha_4 xy$, with each $\alpha_i \in K$, and the following operational rules are satisfied: 1) $x^2 = -a$, for a totally positive element a of K; 2) $y^2 = -b$, for a totally positive element b of K; and 3) $xy = -yx$. We write $D = K \dot{+} Kx \dot{+} Ky \dot{+} Kxy$.

It is clear that the centre of D is, indeed, K. Further, if

$$0 \neq \alpha_1 + \alpha_2 x + \alpha_3 y + \alpha_4 xy \in D,$$

then

$$\frac{1}{\alpha_1^2+\alpha_2^2a+\alpha_3^2b+\alpha_4^2ab}(\alpha_1-\alpha_2x-\alpha_3y-\alpha_4xy)(\alpha_1+\alpha_2x+\alpha_3y+\alpha_4xy)=1.$$

(The fact that $\alpha_1^2+\alpha_2^2a+\alpha_3^2b+\alpha_4^2ab \neq 0$ is guaranteed by the total reality of K, and the total positivity of a and b). Thus, D is a division algebra. It is clear that $\dim_K D = 4$, and that the Schur index of D is 2. We also observe that $E = K \dot{+} Kx$ is a maximal subfield of D. We wish to compute the reduced norm on D. To do this, we must construct the isomorphism $\beta : D \otimes_K E \to M_2(E)$. We define a map $\lambda : D \times E \to M_2(E)$ via

$$\begin{aligned}&\lambda((\alpha_1+\alpha_2x+\alpha_3y+\alpha_4xy, \alpha_5+\alpha_6x))\\ &=\begin{pmatrix}\alpha_1+\alpha_2x & \alpha_3+\alpha_4x\\ -b\alpha_3+b\alpha_4x & \alpha_1-\alpha_2x\end{pmatrix}\begin{pmatrix}\alpha_5+\alpha_6x & 0\\ 0 & \alpha_5+\alpha_6x\end{pmatrix}.\end{aligned}$$

This map is easily seen to be middle linear. Hence, it induces a map $\beta : D \otimes_K E \to M_2(E)$, namely

$$\begin{aligned}&\beta((\alpha_1+\alpha_2x+\alpha_3y+\alpha_4xy)\otimes(\alpha_5+\alpha_6x))\\ &=\begin{pmatrix}\alpha_1+\alpha_2x & \alpha_3+\alpha_4x\\ -b\alpha_3+b\alpha_4x & \alpha_1-\alpha_2x\end{pmatrix}\begin{pmatrix}\alpha_5+\alpha_6x & 0\\ 0 & \alpha_5+\alpha_6x\end{pmatrix}.\end{aligned}$$

A straightforward (albeit, messy) computation is all that is required to verify that β is an E-algebra homomorphism. To see that β is onto, let us take $\alpha_1, \alpha_2 \in K$. Then

$$\beta(\frac{\alpha_1}{2}\otimes 1-\frac{\alpha_1}{2a}x\otimes x)=\begin{pmatrix}\frac{\alpha_1}{2} & 0\\ 0 & \frac{\alpha_1}{2}\end{pmatrix}-\begin{pmatrix}\frac{\alpha_1}{2a}x & 0\\ 0 & -\frac{\alpha_1}{2a}x\end{pmatrix}\begin{pmatrix}x & 0\\ 0 & x\end{pmatrix}=\begin{pmatrix}\alpha_1 & 0\\ 0 & 0\end{pmatrix}.$$

Similarly,

$$\beta(\frac{\alpha_2}{2}\otimes x+\frac{\alpha_2}{2}x\otimes 1)=\begin{pmatrix}\frac{\alpha_2}{2} & 0\\ 0 & \frac{\alpha_2}{2}\end{pmatrix}\begin{pmatrix}x & 0\\ 0 & x\end{pmatrix}+\begin{pmatrix}\frac{\alpha_2}{2}x & 0\\ 0 & -\frac{\alpha_2}{2}x\end{pmatrix}=\begin{pmatrix}\alpha_2x & 0\\ 0 & 0\end{pmatrix}.$$

Thus,

$$\begin{pmatrix}\alpha_1+\alpha_2x & 0\\ 0 & 0\end{pmatrix}\in \mathrm{im}\,\beta.$$

In a similar fashion, we can put arbitrary entries of E in the other four positions in the matrix. That is, β is surjective. Since $\dim_K(D\otimes_K E) = \dim_K(M_2(E)) = 8$, β is an isomorphism. Therefore,

$$\begin{aligned}nr(\alpha_1+\alpha_2x+\alpha_3y+\alpha_4xy) &= \det\beta((\alpha_1+\alpha_2x+\alpha_3y+\alpha_4xy)\otimes 1)\\ &=\det\begin{pmatrix}\alpha_1+\alpha_2x & \alpha_3+\alpha_4x\\ -b\alpha_3+b\alpha_4x & \alpha_1-\alpha_2x\end{pmatrix}\\ &=\alpha_1^2+\alpha_2^2a+\alpha_3^2b+\alpha_4^2ab.\end{aligned}$$

At this point, we shall prove

Proposition 3.4.5. *Let D be a totally definite quaternion algebra. Let its centre be $K = \mathbb{Q}(\eta)$. If $\mathcal{O}$ is any order in D, then $SL_1(\mathcal{O})$ is finite.*

Proof. If Λ is another order in D, then $|\mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathcal{O} \cap \Lambda)| < \infty$, by Proposition 3.1.6 and Theorem 3.1.7. Thus,

$$|SL_1(\mathcal{O}) : SL_1(\mathcal{O} \cap \Lambda)| = |\mathcal{U}(\mathcal{O}) \cap SL_1(D) : \mathcal{U}(\mathcal{O} \cap \Lambda) \cap SL_1(D)| < \infty.$$

Therefore, it will be sufficient if we show that $SL_1(\Lambda)$ is finite. We observe that it makes no difference if we replace x or y in the definition of D by nx or ny, respectively, for some natural number n. (We see that $nxy = -ynx$, and $(nx)^2 = n^2x^2 = -n^2a$. If $\sigma : K \to \mathbb{C}$, then $\sigma(n^2a) = n^2\sigma(a) > 0$, since $\sigma(a) > 0$. The proof for ny is similar.) Let O be the ring of algebraic integers in K. Since $a \in K$, and O is an order in K, there exists a natural number n_1, such that $n_1a \in O$. Similarly, there is a natural number n_2 such that $n_2b \in O$. Thus, we will assume that $a, b \in O$. Under this assumption, it is easy to see that $\Lambda = O \dot{+} Ox \dot{+} Oy \dot{+} Oxy$ is an order in D.

Suppose $\alpha \in SL_1(\Lambda)$. Let us say that $\alpha = \alpha_1 + \alpha_2x + \alpha_3y + \alpha_4xy$, with each $\alpha_i \in O$. Then

$$1 = nr(\alpha) = \alpha_1^2 + \alpha_2^2a + \alpha_3^2b + \alpha_4^2ab.$$

Hence, for each $\sigma : K \to \mathbb{C}$, we have

$$1 = \sigma(1) = \sigma(\alpha_1)^2 + \sigma(\alpha_2)^2\sigma(a) + \sigma(\alpha_3)^2\sigma(b) + \sigma(\alpha_4)^2\sigma(a)\sigma(b).$$

Now, since K is totally real, each $\sigma(\alpha_i)^2 \geq 0$. Since a and b are totally positive, each of $\sigma(a), \sigma(b)$, and $\sigma(a)\sigma(b)$ is positive. Thus, we conclude that each of the summands in the above equation is at least zero. It follows that, for each σ, $\sigma(\alpha_1)^2 \leq 1$, $\sigma(\alpha_2)^2 \leq 1/\sigma(a)$, $\sigma(\alpha_3)^2 \leq 1/\sigma(b)$, and $\sigma(\alpha_4)^2 \leq 1/(\sigma(a)\sigma(b))$. Let $M = \max\{1, \sigma(a), \sigma(b), \sigma(a)\sigma(b) | \sigma : K \to \mathbb{C}\}$. Then, for each i, and each $\sigma : K \to \mathbb{C}$, we have $\sigma(\alpha_i)^2 \leq M$. Thus, since $M \geq 1$, $|\sigma(\alpha_i)| \leq \sqrt{M} \leq M$.

Let $m(x)$ be the minimal polynomial of α_i over $\mathbb{Q}$. Let $k(x)$ be the minimal polynomial of η over $\mathbb{Q}(\alpha_i)$. Then, the roots of $m(x)$ are precisely $\tau(\alpha_i)$, for the various embeddings $\tau : \mathbb{Q}(\alpha_i) \to \mathbb{C}$. Let L be a splitting field for $k(x)$ over $\mathbb{Q}(\alpha_i)$, which we may choose so that it contains K. Then, by a basic property of splitting fields (see, for instance, [Hun, Theorem V.3.8]), τ extends to an embedding $\rho : L \to \mathbb{C}$. Thus, letting σ be the restriction of ρ to K, we have an embedding $\sigma : K \to \mathbb{C}$ extending τ. Thus, the roots of $m(x)$ are of the form $\sigma(\alpha_i)$, for embeddings $\sigma : K \to \mathbb{C}$. Let n be the degree of $m(x)$. Then the coefficient of x^l, for $0 \leq l < n$, in $m(x)$ will be the sum of $\binom{n}{l}$ products of $n - l$ roots of $m(x)$ (up to sign). Thus, the magnitude of this coefficient is at most $\binom{n}{l}M^{n-l} \leq n^nM^n$ (since $M \geq 1$). Now, $\alpha_i \in K$, which means that $\deg m \leq [K : \mathbb{Q}]$. Thus, the magnitude of any coefficient of $m(x)$ is at most $([K : \mathbb{Q}]M)^{[K:\mathbb{Q}]}$, a fixed number. The coefficients of $m(x)$ are rational integers (see, for instance, [ST, Lemma 2.12]). There are only finitely many integral polynomials of degree at most $[K:\mathbb{Q}]$, with coefficients of bounded magnitude. Each of these polynomials has only finitely many roots. Therefore, there are only finitely many choices for each α_i. □

Thus, we may feel free to ignore any Wedderburn components of $\mathbb{Q}G$ which are commutative, or totally definite quaternion algebras. An example of a totally definite quaternion algebra, which we will encounter is

Example 3.4.6. Let K be an algebraic number field. Then, if we create two symbols, x and y, and let

$$D = K \dot{+} Kx \dot{+} Ky \dot{+} Kxy,$$

with $x^2 = y^2 = -1$, $xy = -yx$, and let x and y commute with the elements of K, then it is easily seen that D is an algebra over K. It is known as the **(Hamiltonian) quaternion algebra over** K, and is denoted $\mathbb{H}(K)$. In general, it need not be a division ring. (If we take $K = \mathbb{Q}(\sqrt{-1})$, then it is easy to see that $\mathbb{H}(K)$ will have zero divisors). However, if K is totally real, then since 1 is totally positive, $\mathbb{H}(K)$ is a totally definite quaternion algebra.

§3.5 Exceptional Components and Another Reduction

Let R be any ring. Working inside $M_n(R)$, let $E_{i,j}$ be the $n \times n$ matrix which has a 1 in the $(i,j)^{\text{th}}$ position, and zeroes elsewhere. By an **elementary matrix** over R, we will mean a matrix which differs from the identity matrix by one non-diagonal entry; that is, a matrix of the form $I_n + rE_{i,j}$, with $i \neq j$, $0 \neq r \in R$. It is easy to see that such a matrix is invertible, with inverse $I_n - rE_{i,j}$. In fact, observing that $E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$, we obtain

Lemma 3.5.1. *Take $r, s \in R$. Then*

(a) If $j \neq i \neq k$, then $(I_n + rE_{i,j})(I_n + sE_{i,k}) = I_n + rE_{i,j} + sE_{i,k}$. Similarly, $(I_n + rE_{j,i})(I_n + sE_{k,i}) = I_n + rE_{j,i} + sE_{k,i}$.

(b) If i, j, and k are pairwise distinct, then $[I_n + rE_{i,j}, I_n + sE_{j,k}] = I_n + rsE_{i,k}$.

Proof. Part (a) is trivial. For part (b), we write

$$\begin{aligned}[I_n + rE_{i,j}, I_n + sE_{j,k}] &= (I_n - rE_{i,j})(I_n - sE_{j,k})(I_n + rE_{i,j})(I_n + sE_{j,k}) \\ &= I_n + rE_{i,j} + sE_{j,k} + rsE_{i,k} - rE_{i,j} \\ &\quad - rsE_{i,k} - sE_{j,k} + rsE_{i,k} \\ &= I_n + rsE_{i,k}. \quad \square\end{aligned}$$

We write $E_n(R)$ for the subgroup of $GL_n(R)$ generated by all elementary matrices over R. If W is an ideal of R, then we call a matrix **W-elementary** if it is of the form $I_n + wE_{i,j}$, for some $0 \neq w \in W$, $i \neq j$. The subgroup of $GL_n(R)$ generated by these matrices is denoted by $E_n(W)$. We denote by $\tilde{E}_n(W)$ the normal closure of $E_n(W)$ in $E_n(R)$; that is, $\tilde{E}_n(W)$ is the smallest normal subgroup of $E_n(R)$ containing $E_n(W)$.

Let us suppose that our ring is an order, $\mathcal{O}$, in a finite-dimensional $\mathbb{Q}$-division algebra D. Then, we claim that any elementary matrix over $\mathcal{O}$ has reduced norm one. Indeed, any such matrix, α, obviously satisfies $(x-1)^2 = 0$. Thus, if we let γ be the map defined in Proposition 2.4.2, we have $(\gamma(\alpha \otimes 1) - 1)^2 = 0$. That is, the minimal polynomial of $\gamma(\alpha \otimes 1)$ divides $(x-1)^2$. Since the characteristic polynomial has the same roots as the minimal polynomial, up to multiplicity, the characteristic polynomial is $(x-1)^m$, for some m. Thus, its constant term is $(-1)^m$. However, the constant term of the characteristic polynomial is $(-1)^m \det(\gamma(\alpha \otimes 1))$. That is, $\det(\gamma(\alpha \otimes 1)) = 1$. Hence, $nr(\alpha) = 1$. Therefore, $E_n(\mathcal{O}) \leq SL_n(\mathcal{O})$. It will be necessary for us to make use of a celebrated theorem, known as the **Congruence Subgroup Theorem.** It was first established, in the commutative case, by Bass, Milnor, and Serre, in [BMS], and later extended to the noncommutative case. We refer the reader to [Se2, Theorem 19.32].

Theorem 3.5.2 (Bass-Milnor-Serre-Vaserstein). *Let $n \geq 3$, with D and $\mathcal{O}$ as above. Let W be any nonzero ideal in $\mathcal{O}$. Then $|SL_n(\mathcal{O}) : \tilde{E}_n(W)| < \infty$.*

In fact, we need to strengthen this result slightly. A lemma is required.

Lemma 3.5.3 (Vaserstein). *Let D, $\mathcal{O}$, W, and n be as in Theorem 3.5.2. Then $\tilde{E}_n(W^{2^{4n-2}}) \leq E_n(W)$.*

Proof. Let Q be any ideal in $\mathcal{O}$. Suppose $B \in GL_n(\mathcal{O})$ is of the form

$$B = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix},$$

where $A \in GL_{n-1}(\mathcal{O})$. Then, we claim that $B^{-1}E_n(Q^2)B \subseteq E_n(Q)$. It will suffice if we can show this for the generators of $E_n(Q^2)$; namely, matrices of the form $C = I_n + q_1 q_2 E_{i,j}$, with $q_1, q_2 \in Q$, $1 \leq i \neq j \leq n$. If $i = n$, then

$$B^{-1}C = \begin{pmatrix} A^{-1} & 0 \\ 0 & 1 \end{pmatrix} + q_1 q_2 E_{n,j},$$

implying that

$$\begin{aligned}B^{-1}CB &= I_n + q_1q_2E_{n,j}B \\ &= I_n + \sum_{k=1}^{n-1} q_1q_2a_kE_{n,k} \\ &= \prod_{k=1}^{n-1}(I_n + q_1q_2a_kE_{n,k}) \in E_n(Q^2),\end{aligned}$$

where a_k is the (j,k) entry of A, and each $q_1q_2a_k \in Q^2$, since $Q^2 \triangleleft \mathcal{O}$. In the same manner, it is easy to see that if $j = n$, then $B^{-1}CB \in E_n(Q^2)$. Otherwise, i, j, and n are pairwise distinct. In this case, Lemma 3.5.1 tells us that

$$C = [I_n + q_1E_{i,n}, I_n + q_2E_{n,j}].$$

Thus, $B^{-1}CB = [B^{-1}(I_n + q_1E_{i,n})B, B^{-1}(I_n + q_2E_{n,j})B]$. Taking Q in place of Q^2 in the argument which we have just made, we see that each of the terms of this commutator is in $E_n(Q)$. Therefore, $B^{-1}CB \in E_n(Q)$, for all $C \in E_n(Q^2)$, and all B of the appropriate form.

Now, examining this argument, it is clear that the only condition which was required of B was that the n^{th} row and n^{th} column contain zeroes, except in the (n,n) position, where we have a 1. However, the n^{th} row and column are not distinguished. Let $I_n + xE_{i,j}$ be an elementary matrix in $E_n(\mathcal{O})$. Since $n \geq 3$, we may choose k such that $1 \leq k \leq n$, and $i \neq k \neq j$. Then the k^{th} row and column of $I_n + xE_{i,j}$ contain zeroes, except for a 1 in the (k,k) position. Thus, we conclude that for any $x \in \mathcal{O}$, and $1 \leq i \neq j \leq n$, we have $(I_n - xE_{i,j})E_n(Q^2)(I_n + xE_{i,j}) \subseteq E_n(Q)$.

We will need to make use of a well-known result due to Bass. Specifically, $\mathcal{O}$ has stable range 2. That is, if, for some $r > 2$, and some $y_1, \ldots, y_r \in \mathcal{O}$, we have $\mathcal{O}y_1 + \cdots + \mathcal{O}y_r = \mathcal{O}$, then there exist $x_1, \ldots, x_{r-1} \in \mathcal{O}$ such that

$$\mathcal{O}(y_1 + x_1y_r) + \mathcal{O}(y_2 + x_2y_r) + \cdots + \mathcal{O}(y_{r-1} + x_{r-1}y_r) = \mathcal{O}.$$

(See [CR3, Theorem 41.22]).

Take $M \in GL_n(\mathcal{O})$, and let the last column of M be

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

If the bottom row of M^{-1} is $(l_1 \cdots l_n)$, then $l_1m_1 + \cdots + l_nm_n = 1$. Thus, $\mathcal{O}m_1 + \cdots + \mathcal{O}m_n = \mathcal{O}$. Hence, we may choose $b_2, \ldots, b_n \in \mathcal{O}$ such that

$$\mathcal{O}(m_2 + b_2m_1) + \mathcal{O}(m_3 + b_3m_1) + \cdots + \mathcal{O}(m_n + b_nm_1) = \mathcal{O}.$$

Let $\tau_1 = I_n + \sum_{i=2}^n b_i E_{i,1}$. Then the last column of $\tau_1 M$ is

$$\begin{pmatrix} m_1 \\ m_2 + b_2 m_1 \\ m_3 + b_3 m_1 \\ \vdots \\ m_n + b_n m_1 \end{pmatrix}.$$

Since $\mathcal{O}(m_2 + b_2 m_1) + \cdots + \mathcal{O}(m_n + b_n m_1) = \mathcal{O}$, let us choose $c_2, \ldots, c_n \in \mathcal{O}$ such that $c_2(m_2 + b_2 m_1) + \cdots + c_n(m_n + b_n m_1) = 1$. For each i, let $d_i = (m_n + b_n m_1 - m_1 - 1)c_i$. Let $\tau_2 = I_n + \sum_{i=2}^n d_i E_{1,i}$. Then, the last column of $\tau_2 \tau_1 M$ is

$$\begin{aligned} \begin{pmatrix} m_1 + \sum_{i=2}^n d_i(m_i + b_i m_1) \\ m_2 + b_2 m_1 \\ \vdots \\ m_n + b_n m_1 \end{pmatrix} &= \begin{pmatrix} m_1 + m_n + b_n m_1 - m_1 - 1 \\ m_2 + b_2 m_1 \\ \vdots \\ m_n + b_n m_1 \end{pmatrix} \\ &= \begin{pmatrix} m_n + b_n m_1 - 1 \\ m_2 + b_2 m_1 \\ \vdots \\ m_n + b_n m_1 \end{pmatrix}. \end{aligned}$$

Let $\tau_3 = I_n - E_{n,1}$. Clearly, the last column of $\tau_3 \tau_2 \tau_1 M$ is

$$\begin{pmatrix} m_n + b_n m_1 - 1 \\ m_2 + b_2 m_1 \\ \vdots \\ m_{n-1} + b_{n-1} m_1 \\ 1 \end{pmatrix}.$$

Now, let $\tau_4 = I_n + (\sum_{i=2}^{n-1}(-m_i - b_i m_1)E_{i,n}) - (m_n + b_n m_1 - 1)E_{1,n}$. We see that the last column of $\tau_4 \tau_3 \tau_2 \tau_1 M$ is

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Therefore, let us write

$$\tau_4 \tau_3 \tau_2 \tau_1 M = \begin{pmatrix} N & 0 \\ \mu & 1 \end{pmatrix},$$

for some $N \in GL_{n-1}(\mathcal{O})$, and a $1 \times (n-1)$ vector, μ, over $\mathcal{O}$. Now, $-\mu N^{-1}$ is a $1 \times (n-1)$ vector. Let

$$\tau_5 = \begin{pmatrix} I_{n-1} & 0 \\ -\mu N^{-1} & 1 \end{pmatrix}.$$

Then, we have

$$\tau_5\tau_4\tau_3\tau_2\tau_1 M = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix},$$

or, in other words,

$$M = \tau_1^{-1}\tau_2^{-1}\tau_3^{-1}\tau_4^{-1}\tau_5^{-1} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}.$$

Now, $\tau_1^{-1} = \prod_{i=2}^{n}(I_n - b_i E_{i,1})$, a product of $n-1$ elementary matrices (where we allow I_n to be an elementary matrix). Similarly, τ_2^{-1} and τ_4^{-1} are products of $n-1$ elementary matrices. Further, $\tau_3^{-1} = I_n + E_{n,1}$ is elementary, and if we write $\mu^{-1}N = (\lambda_1 \cdots \lambda_{n-1})$, then $\tau_5^{-1} = \prod_{i=1}^{n-1}(I_n + \lambda_i E_{n,i})$, which is a product of $n-1$ elmentary matrices. We conclude that M is a product of $4n-2$ matrices, each of which is elementary, or of the form

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix},$$

with $N \in GL_{n-1}(\mathcal{O})$.

Take any $\gamma \in E_n(W^{2^{4n-2}})$, and any $\beta \in E_n(\mathcal{O}) \leq GL_n(\mathcal{O})$. Write $\beta = \beta_1\beta_2\cdots\beta_{4n-2}$, where each β_i is of one of the two types of matrices discussed above. Then, as we pointed out earlier in this proof,

$$\begin{aligned}
\beta^{-1}\gamma\beta &= \beta_{4n-2}^{-1}\cdots\beta_2^{-1}(\beta_1^{-1}\gamma\beta_1)\beta_2\cdots\beta_{4n-2} \\
&\in \beta_{4n-2}^{-1}\cdots\beta_3^{-1}(\beta_2^{-1}E_n(W^{2^{4n-3}})\beta_2)\beta_3\cdots\beta_{4n\ 2} \\
&\subseteq \beta_{4n-2}^{-1}\cdots\beta_3^{-1}E_n(W^{2^{4n-4}})\beta_3\cdots\beta_{4n-2} \\
&\subseteq \cdots \subseteq \beta_{4n-2}^{-1}E_n(W^2)\beta_{4n-2} \\
&\subseteq E_n(W).
\end{aligned}$$

The elements $\beta^{-1}\gamma\beta$ generate $\tilde{E}_n(W^{2^{4n-2}})$, which means that $\tilde{E}_n(W^{2^{4n-2}}) \leq E_n(W)$. □

Thus, for any ideal W in $\mathcal{O}$, we know that $\tilde{E}_n(W^{2^{4n-2}})$ is of finite index in $SL_n(\mathcal{O})$, and $\tilde{E}_n(W^{2^{4n-2}}) \leq E_n(W)$. Therefore, we obtain

Theorem 3.5.4 (Bass-Milnor-Serre-Vaserstein). *Let D be a finite-dimensional $\mathbb{Q}$-division algebra, and $\mathcal{O}$ any order in D. Let $0 \neq W$ be an ideal in $\mathcal{O}$, and let $n \geq 3$. Then $|SL_n(\mathcal{O}) : E_n(W)| < \infty$.*

When $n = 2$, the situation is not quite as good. In general, the index of $E_2(W)$ in $SL_2(\mathcal{O})$ may be infinite. However, there is a partial recovery. We refer the reader to the main theorem of [Va1] for the proof.

Theorem 3.5.5 (Vaserstein). *Let K be an algebraic number field, and O its ring of integers. Let W be a nonzero ideal in O. If K is neither $\mathbb{Q}$ nor an imaginary quadratic extension of the rationals, then $|SL_2(O) : E_2(W)| < \infty$.*

(We should, perhaps, point out that Vaserstein's criterion is that $\mathcal{U}(O)$ must be infinite. By Corollary 2.5.4, the criterion in the above result is correct.) Let us adopt the same notation that we introduced at the beginning of §3.3. The Wedderburn components which will cause us problems are those which are not covered by the above results. We say that a Wedderburn component, $M_{n_i}(D_i)$ of $\mathbb{Q}G$ is **exceptional** if

(1) $n_i = 1$, and D_i is neither commutative, nor a totally definite quaternion algebra; or,

(2) $n_i = 2$, and D_i is $\mathbb{Q}$, an imaginary quadratic extension of the rationals, or a noncommutative division algebra.

Otherwise, the component is said to be **nonexceptional.** (The reason for excluding fields and totally definite quaternion algebras should be obvious from the results in §3.4).

Now, let R be a ring. A set of elements $\{e_{i,j} : 1 \leq i,j \leq n\}$ in R, for some natural number n, is said to be a set of **matrix units** if $e_{i,j}e_{k,l} = \delta_{j,k}e_{i,l}$, for all i,j,k,l, and $\sum_{i=1}^{n} e_{i,i} = 1$. The obvious example is the set $\{E_{i,j} : 1 \leq i,j \leq n\}$ in $M_n(R)$.

Lemma 3.5.6. *Let $\{e_{i,j} : 1 \leq i,j \leq n\}$ be a set of matrix units in R. Let B be the subring of R consisting of those elements which centralize all of the matrix units. Then, the elements of R can be expressed uniquely in the form $\sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}e_{i,j}$, with $b_{i,j} \in B$. Further, the map $\psi : R \to M_n(B)$, given by $\psi(\sum_i \sum_j b_{i,j}e_{i,j}) = \sum_i \sum_j b_{i,j}E_{i,j}$ is an isomorphism. Also, $B \cong e_{1,1}Re_{1,1}$.*

Proof. Take $r \in R$. For any i and j, let $b_{i,j} = \sum_{k=1}^{n} e_{k,i}re_{j,k}$. Then, for any l and m, we have $b_{i,j}e_{l,m} = e_{l,i}re_{j,m} = e_{l,m}b_{i,j}$. Thus, each $b_{i,j} \in B$, and $\sum_i \sum_j b_{i,j}e_{i,j} = \sum_i e_{i,i}(r(\sum_j e_{j,j})) = r$. That is, every element of R may be expressed in the form $\sum_i \sum_j b_{i,j}e_{i,j}$. Suppose this expression is not unique. Then there exist $c_{i,j} \in B$, not all zero, such that $\sum_i \sum_j c_{i,j}e_{i,j} = 0$. Then

$$0 = \sum_k e_{k,p} \sum_i \sum_j c_{i,j}e_{i,j}e_{q,k} = c_{p,q},$$

for any p and q. This gives us uniqueness.

Now, the map ψ is well-defined by the uniqueness which we have just shown, and it is obviously a ring homomorphism. It is easily seen to have an inverse map, namely $\sum_i \sum_j b_{i,j}E_{i,j} \mapsto \sum_i \sum_j b_{i,j}e_{i,j}$. Thus, it is an isomorphism. To verify the last assertion, we observe that since elements of R are of the form $\sum_i \sum_j b_{i,j} e_{i,j}$, the elements of $e_{1,1} R e_{1,1}$ are of the form $\sum_i \sum_j e_{1,1} b_{i,j} e_{i,j} e_{1,1}$. Since elements of B commute with the $e_{i,j}$, this equals $\sum_i \sum_j b_{i,j} e_{1,1}$. That is, $e_{1,1} R e_{1,1} \subseteq B e_{1,1}$. Evidently, the reverse inclusion holds, so that $e_{1,1} R e_{1,1} = B e_{1,1}$. Since the expression of elements in the form $b e_{1,1}$, $b \in B$, is unique, we have $B e_{1,1} \cong B$, under the map $b e_{1,1} \mapsto b$. □

Note that if R is a $\mathbb{Q}$-algebra, then so is B, and the isomorphisms may be taken to be $\mathbb{Q}$-algebra isomorphisms.

We will assume familiarity with some basic facts about modules over division rings, and their similarities to vector spaces over fields. We need to know that a finitely generated module over a division ring is free of finite rank (and therefore has a finite basis). Further, the rank of such a module is well-defined. (For proofs of these results, see Theorems IV.2.4 and IV.2.7 in [Hun]). Also, suppose we let M be a free left D-module of rank n. Then, choosing a basis for M, we may identify M with the set of $1 \times n$ vectors over D. Thus, to every D-endomorphism, α, of M, there corresponds a matrix in $M_n(D)$. The action of α on M corrresponds to right multiplication by this matrix. Conversely, right multiplication by an element of $M_n(D)$ constitutes a D-endomorphism. In addition, two matrices X and Y in $M_n(D)$ correspond to the same D-endomorphism, over different bases of M, if and only if there exists $P \in GL_n(D)$, such that $P^{-1} X P = Y$. (See [Hun, Corollary VII.1.7]).

The following lemma is taken from [JL2], but the proof is a variation due to Sehgal (in [Se2]).

Lemma 3.5.7. *Let e_i be a primitive central idempotent of $\mathbb{Q}G$, such that $\mathbb{Q}Ge_i \cong M_{n_i}(D_i)$, with $n_i \geq 2$. Suppose f_i is an idempotent in $\mathbb{Q}Ge_i$, with $0 \neq f_i \neq e_i$. Then there exist matrix units $\{e_{j,k} : 1 \leq j,k \leq n_i\}$ in $\mathbb{Q}Ge_i$, such that $f_i = e_{1,1} + \cdots + e_{l,l}$, $0 < l < n_i$. Further, we may take D_i to be the centralizer of all of the $e_{j,k}$ in $\mathbb{Q}Ge_i$, and the isomorphism $\theta_i : \mathbb{Q}Ge_i \to M_{n_i}(D_i)$ to be given by $\theta_i(\sum_j \sum_k d_{j,k} e_{j,k}) = \sum_j \sum_k d_{j,k} E_{j,k}$.*

Proof. Since θ_i is an isomorphism, $\theta_i(f_i)$ is an idempotent in $M_{n_i}(D_i)$, satisfying $0 \neq \theta_i(f_i) \neq I_{n_i}$. We let M be the left D_i-module consisting of $1 \times n_i$ vectors over D_i. Let $M_1 = M\theta_i(f_i)$, and $M_2 = M(I_{n_i} - \theta_i(f_i))$. These are D_i-submodules of M. Clearly, if $\alpha \in M$, then $\alpha = \alpha\theta_i(f_i) + \alpha(I_{n_i} - \theta_i(f_i))$, which means that $M = M_1 + M_2$. If $\alpha\theta_i(f_i) + \beta(I_{n_i} - \theta_i(f_i)) = 0$, for $\alpha, \beta \in M$, then multiplying on the right by $\theta_i(f_i)$, we get $\alpha f_i = 0$. Multiplying on the right by $(I_{n_i} - \theta_i(f_i))$, we get $\beta(I_{n_i} - \theta_i(f_i)) = 0$. Thus, $M = M_1 \oplus M_2$. The action of $\theta_i(f_i)$ on M is clearly the identity function, as $\alpha\theta_i(f_i)\theta_i(f_i) = \alpha\theta_i(f_i)$. The action of $\theta_i(f_i)$ on M_2 is to send everything to zero, since $\alpha(I_{n_i} - \theta_i(f_i))\theta_i(f_i) = 0$. Thus, if we choose a basis $\{\lambda_1, \ldots, \lambda_l\}$ for M_1, and a basis $\{\lambda_{l+1}, \ldots, \lambda_m\}$ for M_2, then we have $\lambda_r\theta_i(f_i) = \lambda_r$, if $r \leq l$; otherwise, $\lambda_r\theta_i(f_i) = 0$. Now, $\{\lambda_1, \dots, \lambda_m\}$ is a basis for M. Thus, $m = n_i$, and the matrix of the D_i-endomorphism to which $\theta_i(f_i)$ corresponds, in this new basis, will be

$$A = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Hence, there exists $P \in GL_{n_i}(D_i)$ such that $P^{-1}\theta_i(f_i)P = A$. Since $\theta_i(f_i) \neq 0$, we cannot have $M_1 = 0$. Therefore, $l \geq 1$. Since $\theta_i(f_i) \neq I_{n_i}$, we have $I_{n_i} - \theta_i(f_i) \neq 0$. Thus, $M_2 \neq 0$, which means that $l < n_i$. That is,

$$P^{-1}\theta_i(f_i)P = E_{1,1} + \cdots + E_{l,l},$$

with $0 < l < n_i$. Hence,

$$\theta_i(f_i) = PE_{1,1}P^{-1} + \cdots + PE_{l,l}P^{-1}.$$

Now, we can see immediately that $\{PE_{j,k}P^{-1} : 1 \leq j,k \leq n_i\}$ is another set of matrix units in $M_{n_i}(D_i)$. Since θ_i is an isomorphism,

$$\{\theta_i^{-1}(PE_{j,k}P^{-1}) : 1 \leq j,k \leq n_i\}$$

is a set of matrix units in $\mathbb{Q}Ge_i$. Let $e_{j,k} = \theta_i^{-1}(PE_{j,k}P^{-1})$, for each j and k. Then, we observe that

$$f_i = \theta_i^{-1}(\theta_i(f_i)) = \theta_i^{-1}(PE_{1,1}P^{-1} + \cdots + PE_{l,l}P^{-1}) = e_{1,1} + \cdots + e_{l,l},$$

with $0 < l < n_i$. Applying Lemma 3.5.6, the only thing left to verify is that B, the centralizer of the $e_{j,k}$, is isomorphic to D_i. By Lemma 3.5.6,

$$\begin{aligned} B &\cong e_{1,1}\mathbb{Q}Ge_ie_{1,1} \cong \theta_i(e_{1,1})\theta_i(\mathbb{Q}G)\theta_i(e_{1,1}) \\ &= PE_{1,1}P^{-1}M_{n_i}(D_i)PE_{1,1}P^{-1} = PE_{1,1}M_{n_i}(D_i)E_{1,1}P^{-1} \\ &= P\begin{pmatrix} D_i & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}P^{-1} \cong \begin{pmatrix} D_i & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \cong D_i. \end{aligned}$$

We are done. □

Of course, if $\mathbb{Q}Ge_i \cong M_{n_i}(D_i)$, and $n_i \geq 2$, there is always an idempotent other than 0 or e_i (the identity element of $\mathbb{Q}Ge_i$), namely the element $E_{1,1}$ of $M_{n_i}(D_i)$. Thus, for any Wedderburn component $\mathbb{Q}Ge_i$, with $n_i \geq 2$, we may choose such an f_i. Since $f_i \in \mathbb{Q}G$, there is a natural number n_{f_i} such that $n_{f_i}f_i \in \mathbb{Z}G$. Thus, for any $g \in G$, we have $1 + n_{f_i}^2 f_i g(1 - f_i) \in \mathbb{Z}G$. Since $(1 - f_i)f_i = 0$, it follows immediately that the inverse of this element is $1 - n_{f_i}^2 f_i g(1 - f_i) \in \mathbb{Z}G$. Thus, $1 + n_{f_i}^2 f_i g(1 - f_i) \in \mathcal{U}(\mathbb{Z}G)$. Similarly, $1 + n_{f_i}^2(1 - f_i)gf_i \in \mathcal{U}(\mathbb{Z}G)$. Let

$$H_{f_i} = \langle 1 + n_{f_i}^2 f_i g(1 - f_i), 1 + n_{f_i}^2(1 - f_i)gf_i : g \in G\rangle.$$

For the remainder of this section, we will assume that D_i is as described in Lemma 3.5.7, and assume the other notations from §3.3.

The major reduction in this section is

Theorem 3.5.8 (Jespers-Leal). *Let G be a finite group, and e_i a primitive central idempotent of $\mathbb{Q}G$, such that $\mathbb{Q}Ge_i \cong M_{n_i}(D_i)$, with $n_i \geq 2$. Suppose $\mathbb{Q}Ge_i$ is a nonexceptional component. Then H_{f_i} contains a subgroup K, such that $\pi_j(K) = 1$, for $j \neq i$, and $\pi_i(K)$ is of finite index in $SL_{n_i}(\mathcal{O}_i)$.*

Proof. For $g, h \in G$, and $z \in \mathbb{Z}$, we have

$$(1 + n_{f_i}^2 f_i g(1 - f_i))^z = 1 + n_{f_i}^2 f_i z g(1 - f_i),$$

and

$$(1 + n_{f_i}^2 f_i z g(1 - f_i))(1 + n_{f_i}^2 f_i h(1 - f_i)) = 1 + n_{f_i}^2 f_i(zg + h)(1 - f_i).$$

It follows that $1 + n_{f_i}^2 \mathbb{Z}G(1 - f_i) \subseteq H_{f_i}$. Similarly $1 + n_{f_i}^2(1 - f_i)\mathbb{Z}Gf_i \subseteq H_{f_i}$. Since $e_i \in \mathbb{Q}G$, we may choose a natural number r_i such that $r_ie_i \in \mathbb{Z}G$. Then, $1 + n_{f_i}^2 f_i\mathbb{Z}Gr_ie_i(1 - f_i) \subseteq H_{f_i}$. Since e_i is central in $\mathbb{Q}G$ (and certainly, so is any integer), we may write

$$1 + r_in_{f_i}^2 f_i\mathbb{Z}G(1 - f_i)e_i \subseteq H_{f_i}.$$

Similarly,

$$1 + r_in_{f_i}^2(1 - f_i)\mathbb{Z}Gf_ie_i \subseteq H_{f_i}.$$

Now, if $\alpha \in \mathbb{Z}G$, we have

$$\pi_j(1 + r_in_{f_i}^2 f_i\alpha(1 - f_i)e_i) = I_{n_j} + \theta_i(r_in_{f_i}^2\alpha(1 - f_i)e_ie_j),$$

for each j. If $j \neq i$, then $e_ie_j = 0$. Therefore, $\pi_j(1 + r_in_{f_i}^2 f_i\alpha(1 - f_i)e_i) = I_{n_j}$. Similarly $\pi_j(1 + r_in_{f_i}^2(1 - f_i)\alpha f_ie_i) = I_{n_j}$, for all $j \neq i$. Thus, it will be sufficient if we can show that

$$H = \pi_i(\langle 1 + r_in_{f_i}^2 f_i\mathbb{Z}G(1 - f_i)e_i, 1 + r_in_{f_i}^2(1 - f_i)\mathbb{Z}Gf_ie_i\rangle)$$

contains a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$.

Take any $\omega \in \mathcal{O}_i$. Let $1 \leq u \leq l$, and $l < v \leq n_i$. Then, using the definitions from Lemma 3.5.7, we have

$$f_i\omega e_{u,v}(1-f_i) = (e_{1,1} + \cdots + e_{l,l})\omega e_{u,v}(1 - e_{1,1} - \cdots - e_{l,l}).$$

Since $\omega \in D_i$, which centralizes the $e_{j,k}$, we have

$$\begin{aligned} f_i\omega e_{u,v}(1-f_i) &= \omega(e_{1,1} + \cdots + e_{l,l})e_{u,v}(1 - e_{1,1} - \cdots - e_{l,l}) \\ &= \omega e_{u,v}(1 - e_{1,1} - \cdots - e_{l,l}) \\ &= \omega e_{u,v}, \end{aligned}$$

since $v > l$. Therefore, $f_i\mathcal{O}_ie_{u,v}(1-f_i) = \mathcal{O}_ie_{u,v}$. Now, $(\mathcal{O}_i, +)$ is a finitely generated subgroup of $(\mathbb{Q}G, +)$, and therefore, so is $(\mathcal{O}_ie_{u,v}, +)$. Let us say that it is generated by $\{d_1, \ldots, d_a\}$. Since each $d_s \in \mathbb{Q}G$, we may choose natural numbers z_s, such that each $z_sd_s \in \mathbb{Z}G$. Let $q_{u,v} = \prod_s z_s$. Then, we have $q_{u,v}\mathcal{O}_ie_{u,v} \subseteq \mathbb{Z}G$. We also observe that since $e_{u,v} \in \mathbb{Q}Ge_i$, which has identity element e_i, we have $e_{u,v}e_i = e_{u,v}$. Therefore,

$$\begin{aligned} r_in_{f_i}^2q_{u,v}\mathcal{O}_ie_{u,v} &= r_in_{f_i}^2q_{u,v}\mathcal{O}_ie_{u,v}e_i \\ &= r_in_{f_i}^2f_iq_{u,v}\mathcal{O}_ie_{u,v}(1-f_i)e_i \\ &\subseteq r_in_{f_i}^2f_i\mathbb{Z}G(1-f_i)e_i. \end{aligned}$$

Similarly, for any $\omega \in \mathcal{O}_i$, we observe that

$$\begin{aligned} (1-f_i)\omega e_{v,u}f_i &= (1 - e_{1,1} - \cdots - e_{l,l})\omega e_{v,u}(e_{1,1} + \cdots + e_{l,l}) \\ &= \omega(1 - e_{1,1} - \cdots - e_{l,l})e_{v,u} \\ &= \omega e_{v,u}. \end{aligned}$$

Thus, $(1-f_i)\mathcal{O}_ie_{v,u}f_i = \mathcal{O}_ie_{v,u}$. Proceeding as above, we obtain natural numbers $q_{v,u}$ such that

$$r_in_{f_i}^2q_{v,u}\mathcal{O}_ie_{v,u} = r_in_{f_i}^2(1-f_i)q_{v,u}\mathcal{O}_ie_{v,u}f_ie_i \subseteq r_in_{f_i}^2(1-f_i)\mathbb{Z}Gf_ie_i.$$

Let q_i be the product of all of the $q_{u,v}$ and all of the $q_{v,u}$, with $1 \leq u \leq l < v \leq n_i$. Then, we know that

$$r_in_{f_i}^2q_i\mathcal{O}_ie_{u,v} \subseteq r_in_{f_i}^2f_i\mathbb{Z}G(1-f_i)e_i$$

and

$$r_in_{f_i}^2q_i\mathcal{O}_ie_{v,u} \subseteq r_in_{f_i}^2(1-f_i)\mathbb{Z}Gf_ie_i.$$

Take an arbitrary $\omega \in \mathcal{O}_i$. Then

$$\pi_i(1 + r_i n_{f_i}^2 q_i \omega e_{u,v}) \in \pi_i(1 + r_i n_{f_i}^2 f_i \mathbb{Z}G(1 - f_i)e_i) \subseteq H.$$

But, by Lemma 3.5.7,

$$\begin{aligned}\pi_i(1 + r_i n_{f_i}^2 q_i \omega e_{u,v}) &= I_{n_i} + \theta_i(r_i n_{f_i}^2 q_i \omega e_{u,v} e_i) \\ &= I_{n_i} + r_i n_{f_i}^2 q_i \omega E_{u,v}\end{aligned}$$

(where e_i maps to the identity matrix). Similarly,

$$\pi_i(1 + r_i n_{f_i}^2 q_i \omega e_{v,u}) \in \pi_i(1 + r_i n_{f_i}^2 (1 - f_i)\mathbb{Z}G f_i e_i) \subseteq H,$$

and

$$\pi_i(1 + r_i n_{f_i}^2 q_i \omega e_{v,u}) = I_{n_i} + r_i n_{f_i}^2 q_i \omega E_{v,u}.$$

We still have to deal with the restrictions on u and v. Suppose that $1 \leq u, v \leq l$, and $u \neq v$. Then, since $l < n_i$, we have

$$I_{n_i} + r_i^2 n_{f_i}^4 q_i^2 \omega E_{u,v} = [I_{n_i} + r_i n_{f_i}^2 q_i \omega E_{u,n_i}, I_{n_i} + r_i n_{f_i}^2 q_i E_{n_i,v}] \in H.$$

If $l < u, v \leq n_i$, with $u \neq v$, then since $1 \leq l$, we have

$$I_{n_i} + r_i^2 n_{f_i}^4 q_i^2 \omega E_{u,v} = [I_{n_i} + r_i n_{f_i}^2 q_i \omega E_{u,1}, I_{n_i} + r_i n_{f_i}^2 q_i E_{1,v}] \in H.$$

Thus, for all u and v, with $u \neq v$, and any $\omega \in \mathcal{O}_i$, we have

$$I_{n_i} + r_i^2 n_{f_i}^4 q_i^2 \omega E_{u,v} \in H.$$

That is, $E_{n_i}(r_i^2 n_{f_i}^4 q_i^2 \mathcal{O}_i) \leq H$, where $r_i^2 n_{f_i}^4 q_i^2 \mathcal{O}_i$ is a nonzero ideal in $\mathcal{O}_i$. Thus, by Theorems 3.5.4 and 3.5.5, H contains a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$, as required. □

We conclude this section by stating

Corollary 3.5.9. *Let G be a finite group, such that $\mathbb{Q}G$ does not have any exceptional Wedderburn components. For each Wedderburn component $M_{n_i}(D_i)$, with $n_i \geq 2$, we create an H_{f_i} as above. Then all of the H_{f_i}, together with $\mathcal{B}_1$, generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

Proof. We wish to apply Theorem 3.3.4. By Theorem 3.5.8, we obtain the appropriate subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$, when $n_i \geq 2$. By the results of §3.4, no units at all are required when $n_i = 1$, and D_i is commutative or a totally definite quaternion algebra. Any other Wedderburn components are forbidden, by assumption. We are done. □

§3.6 The Bicyclic Units

While Corollary 3.5.9 is a very useful result, it is not our ultimate goal. We wish to compute the generators explicitly, not in terms of idempotents inside Wedderburn components, which can be difficult to determine.

Henceforth, if g is an element of a finite group G, we will write

$$\hat{g} = 1 + g + g^2 + \cdots + g^{|g|-1}.$$

We observe that $\hat{g}(1-g) = 0$, and $\hat{g}^2 = |g|\hat{g}$. In particular, $\frac{1}{|g|}\hat{g}$ is an idempotent in $\mathbb{Q}G$.

Let G be a finite group. If $g, h \in G$, it is clear that $1 + \hat{g}h(1-g)$ is a unit in $\mathbb{Z}G$, with inverse $1 - \hat{g}h(1-g)$. Similarly, $1 + (1-g)h\hat{g}$ has inverse $1 - (1-g)h\hat{g}$. We call the units of this type the **bicyclic units**. We write

$$\mathcal{B}_2 = \langle 1 + \hat{g}h(1-g), 1 + (1-g)h\hat{g} : g, h \in G \rangle.$$

The bicyclic units were introduced by Ritter and Sehgal, and their usefulness was explored in a series of papers (see, for instance, [RS1] and [RS2]). We should note that in these papers, and in [Se2], only the units of the form $1 + (1-g)h\hat{g}$ are called bicyclic units, and some of the results we will obtain for nilpotent groups can be deduced without using the units of the form $1 + \hat{g}h(1-g)$. We will call the units of the form $1 + (1-g)h\hat{g}$, the **one-sided bicyclic units**. Our goal will be to show that, under favourable circumstances, the groups H_{f_i} defined in the last section may be chosen in such a way that they lie within $\mathcal{B}_2$.

A finite-dimensional representation of a finite group, G, over a field, K, is said to be **fixed point free** if for all $1 \neq g \in G$, $T(g)$ does not have 1 as an eigenvalue. A finite group, G, is said to be a **fixed point free group** provided it has a fixed point free, irreducible complex representation. We will now present some basic facts about fixed point free groups.

Lemma 3.6.1. *Let G be a finite group. Then*

(a) G is fixed point free if and only if G has a (not necessarily irreducible) fixed point free complex representation.

(b) If G has a fixed point free representation over $\mathbb{Q}$, then G is fixed point free.

Proof. (a) To prove sufficiency, suppose T is a fixed point free complex representation of G. By Maschke's Theorem, we may write T as the direct sum of irreducible complex representations of G, $T = T_1 \oplus \cdots \oplus T_k$. If, for some $1 \neq g \in G$, $T_1(g)$ has 1 for an eigenvalue, then certainly, so does $T(g)$, contradicting the choice of T. Thus, T_1 is an irreducible fixed point free complex representation of G. Necessity is tautological.

(b) Let T be a fixed point free representation over $\mathbb{Q}$, say $T : G \to End_{\mathbb{Q}}(V)$, for a $\mathbb{Q}$-vector space V. Choose a basis for V. Then, we have $T : G \to M_n(\mathbb{Q})$ for some n. We define $U : G \to M_n(\mathbb{C})$ via $U(g) = T(g)$. Then U is a complex representation of G. If, for some $g \in G$, $U(g)$ has 1 as an eigenvalue, then 1 is a root of the characteristic polynomial of $U(g)$. But $U(g) = T(g)$, which means that the characteristic polynomial of $U(g)$ is that of $T(g)$. Thus, $T(g)$ has 1 as an eigenvalue, forcing $g = 1$. Hence, U is a fixed point free complex representation of G. Now apply part (a). □

Proposition 3.6.2 (Amitsur). *Let D be a division algebra which is finite-dimensional over $\mathbb{Q}$. Let G be a finite subgroup of $D^\times = \mathcal{U}(D)$. Then G is fixed point free.*

Proof. We regard D as a $\mathbb{Q}$-vector space. Let us define $T : G \to End_{\mathbb{Q}}(D)$ via $T(g)d = gd$, for all $g \in G$, and all $d \in D$. This is obviously a finite-dimensional representation of G over $\mathbb{Q}$. Suppose there exists $g \in G$ such that $T(g)$ has 1 as an eigenvalue. Then $gd = d$ for some $0 \neq d \in D$. Thus, $(g-1)d = 0$. Now, this is a computation inside D, which has no zero divisors. Since $d \neq 0$, we must have $g = 1$. Thus, T is a fixed point free representation of G over $\mathbb{Q}$. Apply Lemma 3.6.1. □

This result is useful to us in the following form: if e_i is a primitive central idempotent of $\mathbb{Q}G$, and $\mathbb{Q}Ge_i \cong D_i$, a division ring, then Ge_i is a fixed point free group. Let us describe a condition under which $H_{f_i} \subseteq \mathcal{B}_2$. We assume the same notations as in the last section.

Lemma 3.6.3. *Let G be a finite group, and e_i a primitive central idempotent of $\mathbb{Q}G$, such that Ge_i is not fixed point free. Then there exists some $g \in G$ such that $\frac{1}{|g|}\hat{g}e_i$ is an idempotent in $\mathbb{Q}Ge_i$, with $0 \neq \frac{1}{|g|}\hat{g}e_i \neq e_i$. In this case, if we take $f_i = \frac{1}{|g|}\hat{g}e_i$, then we may assume that $H_{f_i} \subseteq \mathcal{B}_2$.*

Proof. Since we observed earlier that $\frac{1}{|g|}\hat{g}$ is always an idempotent, and e_i is a central idempotent, it is clear that for any $g \in G$, $\frac{1}{|g|}\hat{g}e_i$ is an idempotent in $\mathbb{Q}Ge_i$. The difficulty lies in finding a g such that this idempotent is neither 0 nor e_i.

In §2.3, we pointed out that e_i is a central idempotent in $\mathbb{C}Ge_i$, and that we may write $e_i = e'_1 + \cdots + e'_r$, where $e'_1, \ldots, e'_r$ are primitive central idempotents of $\mathbb{C}G$, contained in $\mathbb{C}Ge_i$. That is, $\mathbb{C}Ge_i = \mathbb{C}Ge'_1 \oplus \cdots \oplus \mathbb{C}Ge'_r$. Now, if all of the $\mathbb{C}Ge'_j$ are commutative, then so is $\mathbb{C}Ge_i$, and therefore, $\mathbb{Q}Ge_i$ is commutative. That is, $\mathbb{Q}Ge_i \cong D_i$, for a $\mathbb{Q}$-division algebra D_i. But, in this case, Ge_i is fixed point free, a contradiction. Thus, some $\mathbb{C}Ge'_j$ is noncommutative. Since $\mathbb{C}Ge'_j \cong M_n(\mathbb{C})$, for some natural number n, we must have $n \geq 2$. Let $\lambda : \mathbb{C}Ge'_j \to M_n(\mathbb{C})$ be this isomorphism.

Since $e'_j \in \mathbb{C}Ge_i$, we have $e_i e'_j = e'_j$. Thus, the map $T : Ge_i \to M_n(\mathbb{C})$, which we define via right multiplication by e_j; namely, $T(ge_i) = \lambda(ge'_j)$, is a complex representation of Ge_i. Since Ge_i is not fixed point free, there exists some $h \in G$ such that $he_i \neq e_i$, and $T(he_i)$ has 1 as an eigenvalue. Now, $(he_i)^{|h|} = h^{|h|}e_i = e_i$, since e_i is a central idempotent. Thus, $T(he_i)^{|h|} = I_n$. Therefore, the minimal polynomial of $T(he_i)$, over $\mathbb{C}$, divides $x^n - 1$. The roots of this polynomial are distinct, which means that $T(he_i)$ is diagonalizable over $\mathbb{C}$. Since $T(he_i)^{|h|} = I_n$, the diagonal entries must be $|h|^{\text{th}}$ roots of unity. Let us assume that we are using the appropriate basis, and write

$$T(he_i) = \begin{pmatrix} \xi_{|h|}^{a_1} & & \\ & \ddots & \\ & & \xi_{|h|}^{a_n} \end{pmatrix},$$

where $\xi_{|h|}$ is a primitive $|h|^{\text{th}}$ root of unity, and each a_k is an integer satisfying $0 \leq a_k < |h|$. Since $T(he_i)$ has 1 as an eigenvalue, at least one of the diagonal entries is 1. Further, if $T(he_i) = I_n$, then this means that $\lambda(he'_j) = I_n$. But λ is an isomorphism, so $he'_j = e'_j$. By Corollary 2.3.4, $he_i = e_i$, a contradiction. Thus, at least one of the diagonal entries of $T(he_i)$ is not 1. Without loss of generality, let us say $a_1 = 0$ and $a_n \neq 0$.

Now, each of the entries $\xi_{|h|}^{a_k}$ is a root of the polynomial $x^{|h|} - 1$. Thus, if $a_k \neq 0$, it also satisfies $\frac{x^{|h|-1}}{x-1} = x^{|h|-1} + x^{|h|-2} + \cdots + 1$. That is,

$$1 + \xi_{|h|}^{a_k} + \xi_{|h|}^{2a_k} + \cdots + \xi_{|h|}^{(|h|-1)a_k} = 0.$$

If $a_k = 0$, then, of course,

$$1 + \xi_{|h|}^{a_k} + \xi_{|h|}^{2a_k} + \cdots + \xi_{|h|}^{(|h|-1)a_k} = |h|.$$

We observe that, for any natural number p, we have

$$T(h^p e_i) = T(he_i)^p = \begin{pmatrix} \xi_{|h|}^{a_1 p} & & \\ & \ddots & \\ & & \xi_{|h|}^{a_n p} \end{pmatrix}.$$

Thus,

$$T(\hat{h}e_i) = \begin{pmatrix} 1+\xi_{|h|}^{a_1}+\cdots+\xi_{|h|}^{(|h|-1)a_1} & & \\ & \ddots & \\ & & 1+\xi_{|h|}^{a_n}+\cdots+\xi_{|h|}^{(|h|-1)a_n} \end{pmatrix}.$$

Therefore, we conclude that

$$T(\frac{1}{|h|}\hat{h}e_i) = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix},$$

where each d_k is either 0 or 1, and we know that $d_1 = 1$, and $d_n = 0$. However, $T(0) = 0$, and $T(e_i) = \lambda(e_j') = I_n$. Thus, $0 \neq \frac{1}{|h|}\hat{h}e_i \neq e_i$, as required. Let $f_i = \frac{1}{|h|}\hat{h}e_i$.

For any $g_1, g_2, g_3 \in G$, and any $z \in \mathbb{Z}$, we have

$$(1+\hat{g}_1g_2(1-g_1))^z(1+\hat{g}_1g_3(1-g_1)) = 1+\hat{g}_1(zg_2+g_3)(1-g_1).$$

Thus, $1+\hat{g}\mathbb{Z}G(1-g) \subseteq \mathcal{B}_2$, for all $g \in G$. Similarly, $1+(1-g)\mathbb{Z}G\hat{g} \subseteq \mathcal{B}_2$, for all $g \in G$. Choose a natural number n_{e_i} satisfying $n_{e_i}e_i \in \mathbb{Z}G$. It is easy to see that $|h|n_{e_i}f_i \in \mathbb{Z}G$, so we set $n_{f_i} = |h|n_{e_i}$. Now, for any natural number q, we have $1-h^q = (1+h+h^2+\cdots+h^{q-1})(1-h) \in \mathbb{Z}G(1-h)$. Therefore,

$$|h| - \hat{h} = \sum_{q=0}^{|h|-1}(1-h^q) \in \mathbb{Z}G(1-h).$$

Hence, $n_{e_i}^2 e_i\mathbb{Z}G(|h|-\hat{h}) \subseteq \mathbb{Z}G(1-h)$, which means that

$$1+\hat{h}n_{e_i}^2e_i\mathbb{Z}G(|h|-\hat{h}) \subseteq \mathcal{B}_2.$$

Now, $e_i = e_i^2$, and e_i is central. Thus, we may write

$$1+n_{e_i}^2\hat{h}e_i\mathbb{Z}Ge_i(|h|-\hat{h}) \subseteq \mathcal{B}_2.$$

Since $\hat{h}e_i = |h|f_i$, we have

$$1+|h|n_{e_i}^2f_i\mathbb{Z}G|h|(1-f_i) \subseteq \mathcal{B}_2.$$

That is,

$$1+n_{f_i}^2f_i\mathbb{Z}G(1-f_i) \subseteq \mathcal{B}_2.$$

Similarly, $1+n_{f_i}^2(1-f_i)\mathbb{Z}Gf_i \subseteq \mathcal{B}_2$. Hence, $H_{f_i} \subseteq \mathcal{B}_2$, as required. □

This allows us to complete our goal for this chapter. Specifically, we wanted to find some conditions on the Wedderburn components of $\mathbb{Q}G$, and on the homomorphic images of G, under which $\langle \mathcal{B}_1, \mathcal{B}_2 \rangle$ will be of finite index in $\mathcal{U}(\mathbb{Z}G)$. Let us give these conditions now.

heorem 3.6.4 (Jespers-Leal). *Let G be a finite group, such that $\mathbb{Q}G$ does ɔt have any Wedderburn components which are 2×2 matrix rings over $\mathbb{Q}$, an naginary quadratic extension of the rationals, or a noncommutative division 'gebra. Suppose that G does not have any nonabelian, fixed point free homomor- ɦic images. Then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$.*

roof. If, for any i, $\mathbb{Q}Ge_i \cong D_i$, a division algebra, then by Proposition 3.6.2, e_i is fixed point free. But Ge_i is a homomorphic image of G (under the map $\mapsto ge_i$), forcing Ge_i to be abelian. Thus, $\mathbb{Q}Ge_i$ is commutative. Therefore, $\mathbb{Q}G$ ɔes not have any exceptional Wedderburn components. By Corollary 3.5.9, $\mathcal{B}_1$ ıd all of the H_{f_i} together generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. Since ɔne of the Ge_i can be fixed point free, except in the case where $\mathbb{Q}Ge_i$ is a field, emma 3.6.3 tells us that each $H_{f_i} \subseteq \mathcal{B}_2$. □

Actually, if the order of G is odd, then by Theorem 2.2.6, $\mathbb{Q}G$ cannot possibly ave any 2×2 matrix rings among its Wedderburn components. Thus, in this ıse, we have a rather strong condition.

'orollary 3.6.5. *Let G be a group of odd order which has no nonabelian fixed ɔint free homomorphic images. Then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$.*

Chapter 4

Nilpotent Groups

In this chapter, we will restrict our attention to group rings over nilpotent groups. The results which we presented in the last chapter will have strong consequences in this case.

In the first section, we will show that the fixed point free nilpotent groups have very nice forms. In the second section, we will present some facts about Wedderburn decompositions. Combining this information, and the results in the last chapter, the third section will give some conditions on the Wedderburn components of G, under which the Bass cyclic and bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. In the fourth section, we will show that that this property does not hold for all nilpotent groups. In the fifth and sixth sections, we will introduce some new units, and give a result due to Giambruno and Sehgal. This result will tell us that if $\mathbb{Q}G$ has no exceptional Wedderburn components, then these new units, together with the Bass cyclic and bicyclic units, generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

§4.1 Fixed Point Free Nilpotent Groups

From the results in §3.6, it is evident that a classification of all fixed point free groups would be useful. In fact, such a classification was completed by Zassenhaus, in [Za]. (For a discussion of this work, see Chapters 5 and 6 of [Wo]). In general, the structure of these groups can be fairly complicated. However, we will obtain a very strong condition on the Sylow subgroups of fixed point free groups. This will lead to a strong condition on nilpotent fixed point free groups. Here is a useful reduction.

Lemma 4.1.1. *Let G be a fixed point free group. If p and q are (not necessarily distinct) primes, and H is a subgroup of G such that H has order pq, then H is cyclic.*

Proof. Let $T : G \to GL_{\mathbb{C}}(V)$ be a fixed point free, complex irreducible representation of G, where V is some nonzero complex vector space. If $1 \neq K$ is a subgroup of G, then the restriction of T to K is a fixed point free representation of K. Take $1 \neq k_0 \in K$. Then, if $v \in V$, we have

$$\sum_{k\in K} T(k)v = \sum_{k\in K} T(k_0k)v = T(k_0)\sum_{k\in K} T(k)v.$$

Therefore, if $\sum_{k\in K} T(k)v \neq 0$, then $T(k_0)$ has 1 as an eigenvalue, contradicting the assumption on T. Thus, $\sum_{k\in K} T(k)v = 0$, for all $v \in V$.

Suppose that H is a subgroup of G, such that $|H| = pq$, but H is not cyclic. Let us suppose that the subgroups of H are $\{1, H, H_1, \dots, H_r\}$. Now, if $p \neq q$, then H has a Sylow p-subgroup and a Sylow q-subgroup. If $p = q$, then since H is not cyclic, H must be the direct product of two cyclic groups of order p. Thus, either way, H has more than one proper subgroup. That is, $r \geq 2$. Now, each H_i must have order p or q. Since distinct groups, each of prime order, must intersect trivially, each $1 \neq h \in H$ is in at most one of the H_i. However, H is not cyclic, which means that $\langle h \rangle = H_i$, for some i. Thus, each $1 \neq h \in H$ is in exactly one H_i. Hence,

$$\sum_{i=1}^{r} \sum_{g\in H_i} T(g)v = (\sum_{1\neq h\in H} T(h)v) + rT(1)v.$$

Further, we demonstrated that $\sum_{g\in H_i} T(g)v = 0$ for each i. Thus,

$$(\sum_{1\neq h\in H} T(h)v) + rT(1)v = 0.$$

Also,

$$\sum_{h\in H} T(h)v = 0.$$

Subtracting, we find that $(r-1)T(1)v = 0$, for all $v \in V$. Since $r \geq 2$, we may divide by $r - 1$. Since $T(1) = 1$, we conclude that $v = 0$. That is, $V = 0$, which is not permitted. □

In particular, every subgroup of order p^2 in a fixed point free group is cyclic. This is clearly a condition on the Sylow p-subgroups of the group. Therefore, we will concentrate on p-groups. We will assume that the reader is acquainted with the basic properties of finite p-groups. In particular, they have nontrivial centres, and if $H \leq K \leq G$ are finite p-groups, then there exist subgroups $H_1, \dots, H_r$ of K, such that $H = H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_r = K$, with each H_i of index p in H_{i+1}. In particular, a maximal subgroup of a finite p-group is normal. (See [Su, Theorems 2.1.4 and 2.1.9]).

We denote the cyclic group of order n by C_n. We have

Lemma 4.1.2. *Let $1 \neq G$ be a p-group, and assume that every subgroup of order p^2 is cyclic. Then G has exactly one subgroup of order p, and it is central.*

Proof. Since $Z(G) \neq 1$, and $Z(G)$ is a p-group, we may take $g \in Z(G)$ such that g has order p. Now, if $h \in G$ has order p, then since g and h commute, either h is a power of g, or $\langle g, h\rangle \simeq C_p \times C_p$. The latter is not permitted, so we conclude that $\langle g\rangle$ is the only subgroup of order p. □

Some general facts are contained in

Lemma 4.1.3. *Let G be a group, satisfying $G' = [G,G] \leq Z(G)$. Take $g, h \in G$, and a natural number n. Then*
(a) $[g^n, h] = [g,h]^n$.
(b) $(gh)^n = [h,g]^{n(n-1)/2} g^n h^n$.

Proof. (a) Our proof is by induction on n. When, $n = 1$, there is nothing to do. Assume that $[g^{n-1}, h] = [g,h]^{n-1}$, for some $n \geq 2$. Then

$$[g^n, h] = g^{-n}h^{-1}g^n h = g^{-1}(g^{1-n}h^{-1}g^{n-1}h)g(g^{-1}h^{-1}gh) = g^{-1}[g^{n-1},h]g[g,h].$$

Since $G' \leq Z(G)$,

$$[g^n, h] = [g^{n-1},h][g,h] = [g,h]^{n-1}[g,h] = [g,h]^n,$$

by our inductive hypothesis.

(b) Once again, our proof is by induction on n. When $n = 1$, there is nothing to prove. Suppose that $(gh)^{n-1} = [h,g]^{(n-1)(n-2)/2} g^{n-1}h^{n-1}$, for some $n \geq 2$. Then

$$\begin{aligned}(gh)^n &= (gh)^{n-1}(gh)\\ &= [h,g]^{(n-1)(n-2)/2} g^{n-1}h^{n-1}gh\\ &= [h,g]^{(n-1)(n-2)/2} g^{n-1}gh^{n-1}[h^{n-1},g]h.\end{aligned}$$

Since $G' \leq Z(G)$, this means that

$$(gh)^n = [h,g]^{(n-1)(n-2)/2}[h^{n-1},g]g^n h^n.$$

By part (a), this implies that

$$(gh)^n = [h,g]^{(n-1)(n-2)/2}[h,g]^{n-1}g^n h^n = [h,g]^{n(n-1)/2}g^n h^n,$$

as required. □

Let us recall the definition of the **generalized quaternion group**,

$$Q_{2^m} = \langle g, h \mid g^{2^{m-2}} = h^2, h^4 = 1, h^{-1}gh = g^{-1}\rangle,$$

for $m \geq 3$. This is a group of order 2^m. (When $m = 3$, this is just the quaternion group, Q_8).

The last in our series of lemmata is

Lemma 4.1.4. *Let G be a finite p-group such that every subgroup of order p^2 is cyclic. Suppose that G has distinct cyclic subgroups, H and K, each of index p in G. Then $p = 2$, and $G \simeq Q_8$.*

Proof. Let $B = H \cap K$. Since H and K are maximal subgroups, they are normal in G. Therefore, B is normal in G. Further, since H and K are distinct maximal subgroups, $G = HK$. Thus,

$$|G| = |HK| = \frac{|H||K|}{|H \cap K|} = \frac{(|G|/p)(|G|/p)}{|B|},$$

which means that $|G : B| = p^2$. In particular, G/B is abelian. Therefore, $G' \leq B$. Since H and K are cyclic, let us write $H = \langle x \rangle$, $K = \langle y \rangle$. Again, since $G = HK$, the elements of G are of the form $x^i y^j$, for integers i and j. If $b \in B$, then $b = x^r = y^s$, for integers r and s. Thus, b commutes with every element of the form $x^i y^j$. That is, $B \leq Z(G)$. Since $G' \leq B$, Lemma 4.1.3 is in effect. Let us take any $g_1, g_2 \in G$. Since $|G : H| = |G : K| = p$, we have $g_1^p \in H \cap K = B$, and $g_2^p \in B$. Thus, g_1^p is central, which implies that $[g_1^p, g_2] = 1$. By Lemma 4.1.3, $[g_1, g_2]^p = 1$.

Suppose that p is an odd prime. Then p divides $p(p-1)/2$, which means that

$$(g_1 g_2)^p = [g_2, g_1]^{p(p-1)/2} g_1^p g_2^p = g_1^p g_2^p.$$

Thus, the map $\rho : G \to B$, given by $\rho(g) = g^p$, is a homomorphism. Its kernel consists of elements of order 1 and p. By Lemma 4.1.2, there are precisely p such elements. That is, $|G/\ker \rho| = \frac{|G|}{p} > |B|$. Since $\operatorname{im} \rho \leq B$, this is impossible. Therefore, $p = 2$.

In this case, Lemma 4.1.3 tells us that $(g_1 g_2)^4 = [g_2, g_1]^6 g_1^4 g_2^4 = g_1^4 g_2^4$, since $[g_2, g_1]^2 = 1$. Thus, the map $\sigma : G \to B$, given by $\sigma(g) = g^4$, is a homomorphism. Let f be an element of maximal order in G. Suppose that $f^2 = f_1^4$, for some $f_1 \in G$. Let us say that the order of f_1 is 2^l. with $l \geq 0$. If $l \geq 2$, then $1 = f_1^{2^l} = f^{2^{l-1}}$, contradicting the maximality of the order of f. Thus, $|f| = 1$ or 2. If $|f| = 1$, then $G = 1$. If $|f| = 2$, then the exponent of G is 2, forcing $G \simeq C_2 \times \cdots \times C_2$. Since G has just one element of order 2 (by Lemma 4.1.2), $G \simeq C_2$. Either way, G does not have two cyclic subgroups of index 2, contrary to our assumption. Thus, f^2 is not a fourth power in G. We demonstrated above that $f^2 \in B$, but we now know that $f^2 \notin \operatorname{im} \sigma$. Thus, σ is not surjective. Therefore, $|G/\ker \sigma| < |B| = \frac{|G|}{4}$. Hence, $|\ker \sigma| > 4$. Let g be the element of order 2 in G (which must be inside $\ker \sigma$, by definition of σ). Then the elements of $\ker \sigma$, aside from 1 and g, have order 4. Take $a \in \ker \sigma$, with $1 \neq a \neq g$. Then $\langle a \rangle = \{1, a, g, ag\}$. Since $|\ker \sigma| > 4$, let us take $b \in \ker \sigma$, with $b \notin \langle a \rangle$. Then $\langle a \rangle$ and $\langle b \rangle$ are distinct subgroups of G which have order 4.

Suppose $|H| \geq 8$. Then $|B| \geq 4$; therefore, B contains a subgroup of order 4. That is, we might as well take $a \in B$. Since $B \leq Z(G)$, a and b commute. As

$a^2 = b^2$, we must have $\langle a\rangle\langle b\rangle \simeq C_4 \times C_2$. This group has two elements of order 2, contradicting Lemma 4.1.2. Thus, $|H| \leq 4$, which means that $|G| \leq 8$. Of the 2-groups of order at most 8, the only one with two cyclic subgroups of index 2, and such that every subgroup of order 4 is cyclic, is Q_8. □

This allows us to present a strong condition which must be satisfied by the Sylow subgroups of a fixed point free group.

Theorem 4.1.5. *Let G be a finite p-group, such that every subgroup of G which has order p^2 is cyclic. If p is odd, then G is cyclic. If $p = 2$, then either G is cyclic, or $G \simeq Q_{2^m}$, for some $m \geq 3$.*

Proof. Let us dispense with the case where p is odd. Let $|G| = p^n$, and proceed by induction on n. If $n = 0$ or 1, there is nothing to do. Let H be a subgroup of index p in G. Every subgroup of H which has order p^2 is cyclic, so by our inductive hypothesis, H is cyclic. Since H is a maximal subgroup of G, H is normal in G. Since $|G/H| = p$, G/H is cyclic. Let $H = \langle h\rangle$, and let g be an element of G which is not in H. Then, $\langle g, h\rangle = G$. If $\langle gh\rangle \neq G$, then taking a chain of subgroups, $\langle gh\rangle = G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r \triangleleft G_{r+1} = G$, with each G_{i+1}/G_i having order p, we have $\langle gh\rangle \leq G_r$, with $|G/G_r| = p$. By our inductive hypothesis, G_r is cyclic. By Lemma 4.1.4, G has only one cyclic subgroup of index p. Thus, $H = G_r$, forcing gh to be inside H. But $h \in H$, hence $g \in H$, contradicting the choice of g. Thus, $G = \langle gh\rangle$.

Therefore, we may assume that $p = 2$. Let K be a maximal abelian normal subgroup of G. If K is not cyclic, then the Fundamental Theorem of Finite Abelian Groups tells us that K must contain at least two elements of order 2, contradicting Lemma 4.1.2. Thus, K is cyclic. Further, it is well-known that under these conditions, the centralizer of K, $C_G(K)$, is actually K. (See, for instance, [Su, p.91]).

If G is cyclic, there is nothing to prove. Otherwise, $G \neq K$, so since G/K is a 2-group, let us take $g \in G$ such that $gK \in G/K$ has order 2. Then $g^2 \in K$. Let $K = \langle k\rangle$. Suppose $k = g^i$ for some i. In this case, g and k would commute. Thus, $g \in C_G(K) = K$, a contradiction. Therefore, $k \notin \langle g\rangle$. Hence, $\langle g^2\rangle \lneq K$, which means that there exists K_1, such that $\langle g^2\rangle \lneq K_1 \leq K$, with $|K_1 : \langle g^2\rangle| = 2$. Since K is cyclic, so is every subgroup of K. Thus, we write $K_1 = \langle k^r\rangle$, for some r. Since K_1 is a nontrivial cyclic 2-group, it has exactly one subgroup of index 2. That is, $\langle g^2\rangle = \langle k^{2r}\rangle$. Let $H = \langle g, K_1\rangle$. We claim that the elements of H are of the form k^{ar}, or $k^{ar}g$, for various integers a. Indeed, all such elements are certainly inside H, and, in fact, they generate H. Hence, it will be enough if we can show that these elements form a group. First, $k^{a_1r}k^{a_2r} = k^{(a_1+a_2)r}$, which is of the correct form. It follows that $k^{a_1r}k^{a_2r}g = k^{(a_1+a_2r)}g$, which is of the correct form. Next, $k^{a_1r}gk^{a_2r} = k^{a_1r}(gkg^{-1})^{a_2r}g$. Since $K \triangleleft G$, $gkg^{-1} = k^b$, for some b. Thus, $k^{a_1 r} g k^{a_2 r} = k^{(a_1+ba_2)r} g$, which is of the correct form. It follows that $k^{a_1 r} g k^{a_2 r} g = k^{(a_1+ba_2)r} g^2$. Since $g^2 \in \langle k^{2r} \rangle$, this is of the correct form. Thus, these elements form a set which is closed under multiplication. Since they are contained in a finite group, G, they form a subgroup, as required. Therefore, $|H : K| = 2$. Further, $H = \langle g \rangle \cup k^r \langle g \rangle$, implying that $|H : \langle g \rangle| = 2$. Now, $g \notin K$, so $\langle g \rangle \neq K_1$. Thus, H has two distinct cyclic subgroups of index 2. By Lemma 4.1.4, $H \simeq Q_8$.

Let us say that the order of k is 2^{m-1}, for a natural number m. Now, $g^2 \in K$, so let us say $g^2 = k^v$, with $v \geq 0$. Since $|H| = 8$, we have $|\langle g \rangle| = 4$, which means that the order of k^v is 2. The only element of $\langle k \rangle$ which has order 2 is $k^{2^{m-2}}$. Hence, $g^2 = k^{2^{m-2}}$. Further, if $kg \in K$, then $g \in K$, which is a contradiction. Thus, $kg \notin K$, and $(kg)^2 = kgkg = k(gkg^{-1})g^2$. Since K is normal in G, each of k, gkg^{-1}, and g^2 is in K. Thus, $(kg)^2 \in K$. That is, kgK has order 2 in G/K. This means that we could have taken kg in place of g, to begin with. Hence, $(kg)^2 = k^{2^{m-2}} = g^2$. Therefore, $kgkg^{-1} = 1$, and $g^{-1}kg = k^{-1}$. That is,

$$\langle K, g \rangle \simeq \langle g, k \,|\, k^{2^{m-1}} = g^2, g^4 = 1, g^{-1}kg = k^{-1} \rangle = Q_{2^m}.$$

Suppose we take another element $g_1 \in G$, such that $g_1 K \in G/K$ has order 2. Then, repeating our argument, we find that $\langle K, g_1 \rangle \simeq Q_{2^m}$. It follows that $g^{-1}kg = k^{-1} = g_1^{-1}kg_1$. That is, $gg_1^{-1}k = kgg_1^{-1}$; that is, gg_1^{-1} centralizes K. Since $C_G(K) = K$, $gg_1^{-1} \in K$. Thus, $g_1 \in \langle K, g \rangle$, and $gK = g_1 K$. That is, gK is the only element of order 2 in G/K. Now, if $f \in G$, but $f \notin K$, then since G/K is a 2-group, some power of fK has order 2, implying that gK is a power of fK. Let us point out a well-known (and easily verified) result. Namely, for any group X, and subgroup X_1, if N is the normalizer of X_1 in X, and C is the centralizer of X_1 in X, then we have a homomorphism $\eta : N \to Aut(X_1)$. We define η via $\eta(n)(x_1) = nx_1n^{-1}$, for all $n \in N$, and all $x_1 \in X_1$. The kernel of η is C. We take $X = G$, and $X_1 = K$. Then $N = G$, and $C = K$. Thus, η induces a monomorphism $\lambda : G/K \to Aut(K)$. Further, $\eta(g)(k^i) = gk^ig^{-1} = (gkg^{-1})^i = k^{-i}$, for all i. Thus, $\lambda(gK)(k^i) = k^{-i}$, for all i. Therefore, $\lambda(gK)(\lambda(gK)(k^i)) = \lambda(gK)(k^{-i}) = k^i$, for all i. Hence, $\lambda(gK)$ has order 2. It follows that every element of $\operatorname{im}\lambda$ (except the identity) has $\lambda(gK)$ among its powers. Thus, either $|G/K| = 2$, or there exists $g' \in G$, such that $\lambda(g'K)^2 = \lambda(gK)$. Suppose the latter holds. Then, since $\lambda(g'K)(k) = k^j$, for some j, we must have $\lambda(gK)(k) = k^{j^2}$. Therefore, $j^2 \equiv -1 \pmod{2^{m-1}}$. Since $|K_1| = 4$, we know that $4 | 2^{m-1}$. Thus, $j^2 \equiv 3 \pmod 4$, an impossibility. Hence, $|G/K| = 2$. Therefore, $G = \langle K, g \rangle \simeq Q_{2^m}$. □

Thus, if G is a fixed point free group, then by Lemma 4.1.1 and Theorem 4.1.5, the Sylow subgroups of G are cyclic or, in the case where $p = 2$, possibly generalized quaternion groups. If G is nilpotent, then it is the direct product of its Sylow subgroups. Recalling that the direct product of finitely many cyclic groups of pairwise relatively prime order is cyclic, we obtain

Corollary 4.1.6. *A fixed point free nilpotent group is either cyclic, or isomorphic to $Q_{2^m} \times C_n$, for some $m \geq 3$, and some odd natural number n.*

§4.2 Some Wedderburn Decompositions

Let us gather together some useful facts about the Wedderburn components of various group algebras. We begin with a basic result.

Lemma 4.2.1. *Let G and H be finite groups, and let K be any field. Then $KG \otimes_K KH \cong K(G \times H)$.*

Proof. Let us define a map $\mu : KG \times KH \to K(G \times H)$, via

$$\mu((\sum_{g\in G} \alpha_g g, \sum_{h\in H} \beta_h h)) = \sum_{g\in G}\sum_{h\in H} \alpha_g\beta_h(g,h).$$

This map is obviously middle linear, so it induces a map $\nu : KG \otimes_K KH \to K(G \times H)$, which is given by

$$\nu((\sum_{g\in G} \alpha_g g) \otimes (\sum_{h\in H} \beta_h h)) = \sum_{g\in G}\sum_{h\in H} \alpha_g\beta_h(g,h).$$

This is clearly a K-algebra homomorphism. It is also entirely obvious that ν is onto. Since $\dim_K(KG \otimes_K KH) = |G||H| = \dim_K(K(G \times H))$, it follows that ν is an isomorphism. □

Let us make a couple of observations about this result. First, we can see that we are free to extend it, by induction, to the direct product of finitely many groups. Second, if we identify G with $\{(g,1) : g \in G\}$, and H with $\{(1,h) : h \in H\}$, then the map ν is given by $\nu(\alpha \otimes \beta) = \alpha\beta$, for all $\alpha \in KG$, $\beta \in KH$. In particular, if the direct product of G and H is internal, then this is the case.

Some more useful information is contained in

Lemma 4.2.2. *Let G and H be finite groups, such that $(|G|,|H|) = 1$. Suppose that $M_n(D)$ is a Wedderburn component of $\mathbb{Q}G$, and $M_m(D')$ is a Wedderburn component of $\mathbb{Q}H$, for natural numbers m and n, and $\mathbb{Q}$-division algebras D and D'. Then, for any natural numbers a and b, $M_a(D) \otimes_{\mathbb{Q}} M_b(D')$ is a simple algebra.*

Proof. Let F be the centre of D, and F' the centre of D'. (Of course, F and F' are algebraic number fields). By [CR2, Theorem 3.60], the ideals of $M_a(D) \otimes_{\mathbb{Q}} M_b(D')$ are in one-to-one correspondence with the ideals of $F \otimes_{\mathbb{Q}} F'$. In particular, $M_a(D) \otimes_{\mathbb{Q}} M_b(D')$ is simple if and only if $F \otimes_{\mathbb{Q}} F'$ is simple. Since $F \otimes_{\mathbb{Q}} F'$ is commutative, this holds if and only if $F \otimes_{\mathbb{Q}} F'$ is a field. Let us write $F = \mathbb{Q}(\alpha)$, and $F' = \mathbb{Q}(\beta)$, with $\alpha, \beta \in \mathbb{C}$. By Corollary 2.2.8, $F = \mathbb{Q}(\chi)$, where χ is the character of some irreducible complex representation of G. Call this representation T. By Theorem 2.2.9, T is realizable over $\mathbb{Q}(\xi_{|G|})$, where $\xi_{|G|}$ is a primitive $|G|^{\text{th}}$ root of unity. Since characters are invariant under a change of basis, we must have $\mathbb{Q}(\chi) \leq \mathbb{Q}(\xi_{|G|})$. That is, $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\xi_{|G|})$. Similarly, $\mathbb{Q}(\beta) \leq \mathbb{Q}(\xi_{|H|})$.

Now, since $(|G|,|H|) = 1$, $\xi_{|G|}\xi_{|H|}$ is a primitive $(|G||H|)^{\text{th}}$ root of unity. Thus, if we let φ be the Euler function, then $\mathbb{Q}(\xi_{|G|}, \xi_{|H|}) = \mathbb{Q}(\xi_{|G||H|})$, and

$$\dim_{\mathbb{Q}}(\mathbb{Q}(\xi_{|G||H|})) = \varphi(|G||H|) = \varphi(|G|)\varphi(|H|) = \dim_{\mathbb{Q}}(\mathbb{Q}(\xi_{|G|}))\dim_{\mathbb{Q}}(\mathbb{Q}(\xi_{|H|})).$$

We define a map $\eta : \mathbb{Q}(\alpha) \times \mathbb{Q}(\beta) \to \mathbb{Q}(\alpha, \beta)$, via $\eta((y_1, y_2)) = y_1 y_2$, for all $y_1 \in \mathbb{Q}(\alpha)$, $y_2 \in \mathbb{Q}(\beta)$. It is clear that η is middle linear; hence, it induces a map $\lambda : \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta) \to \mathbb{Q}(\alpha, \beta)$, which is given by $\lambda(y_1 \otimes y_2) = y_1 y_2$, for all $y_1 \in \mathbb{Q}(\alpha)$, and all $y_2 \in \mathbb{Q}(\beta)$. It is also clear that λ is a $\mathbb{Q}$-algebra homomorphism, and that it is surjective. Thus, to show that $\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta)$ is a field, and thereby complete the proof, it suffices to show that $\dim_{\mathbb{Q}}\mathbb{Q}(\alpha, \beta) = \dim_{\mathbb{Q}}\mathbb{Q}(\alpha) \dim_{\mathbb{Q}}\mathbb{Q}(\beta)$. Or, writing this in terms of the degrees of field extensions, we must show that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$. We will have to use this basic fact several times: if $K_1 \leq K_2 \leq K_3$ are fields, and $z \in K_3$, then $[K_2(z) : K_2] \leq [K_1(z) : K_1]$. (This is obvious, since the minimal polynomial of z over K_1 is a polynomial over K_2 which is satisfied by z). Thus,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\beta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Now, $\mathbb{Q}(\beta) \leq \mathbb{Q}(\xi_{|H|})$, which means that $[\mathbb{Q}(\beta, \alpha) : \mathbb{Q}(\beta)] \geq [\mathbb{Q}(\xi_{|H|}, \alpha) : \mathbb{Q}(\xi_{|H|})]$. Suppose that $[\mathbb{Q}(\xi_{|H|}, \alpha) : \mathbb{Q}(\xi_{|H|})] < [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then

$$[\mathbb{Q}(\xi_{|H|}, \alpha) : \mathbb{Q}] = [\mathbb{Q}(\xi_{|H|}, \alpha) : \mathbb{Q}(\xi_{|H|})][\mathbb{Q}(\xi_{|H|}) : \mathbb{Q}] < [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\xi_{|H|}) : \mathbb{Q}].$$

Thus, in this case,

$$\begin{aligned}
[\mathbb{Q}(\xi_{|H|}, \xi_{|G|}) : \mathbb{Q}] &= [\mathbb{Q}(\xi_{|H|}, \xi_{|G|}) : \mathbb{Q}(\xi_{|H|}, \alpha)][\mathbb{Q}(\xi_{|H|}, \alpha) : \mathbb{Q}] \\
&< [\mathbb{Q}(\xi_{|H|}, \xi_{|G|}) : \mathbb{Q}(\xi_{|H|}, \alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\xi_{|H|}) : \mathbb{Q}] \\
&\leq [\mathbb{Q}(\xi_{|G|}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\xi_{|H|}) : \mathbb{Q}] \\
&= [\mathbb{Q}(\xi_{|G|}) : \mathbb{Q}][\mathbb{Q}(\xi_{|H|}) : \mathbb{Q}],
\end{aligned}$$

a contradiction. Therefore, $[\mathbb{Q}(\xi_{|H|},\alpha) : \mathbb{Q}(\xi_{|H|})] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Thus,

$$\begin{aligned}[\mathbb{Q}(\beta,\alpha) : \mathbb{Q}] &= [\mathbb{Q}(\beta,\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]\\ &\geq [\mathbb{Q}(\xi_{|H|},\alpha) : \mathbb{Q}(\xi_{|H|})][\mathbb{Q}(\beta) : \mathbb{Q}]\\ &= [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}].\end{aligned}$$

We already showed that $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$, so we are done. □

A consequence of fundamental importance is

Proposition 4.2.3. *Let G and H be finite groups of relatively prime orders. Let the primitive central idempotents of $\mathbb{Q}G$ be e_i, $1 \leq i \leq d$, and let $\mathbb{Q}G = \bigoplus_i \mathbb{Q}Ge_i \cong \bigoplus_i M_{n_i}(D_i)$ be the Wedderburn decomposition of $\mathbb{Q}G$. Let the primitive central idempotents of $\mathbb{Q}H$ be e'_j, $1 \leq j \leq d'$, and let $\mathbb{Q}H = \bigoplus_j \mathbb{Q}He'_j \cong \bigoplus_j M_{n_j}(D'_j)$ be the Wedderburn decomposition of $\mathbb{Q}H$. Then the Wedderburn decomposition of $\mathbb{Q}(G \times H) \cong \mathbb{Q}G \otimes_{\mathbb{Q}} \mathbb{Q}H$ is*

$$\bigoplus_i \bigoplus_j (\mathbb{Q}Ge_i \otimes_{\mathbb{Q}} \mathbb{Q}He'_j) \cong \bigoplus_i \bigoplus_j (M_{n_i}(D_i) \otimes_{\mathbb{Q}} M_{n_j}(D'_j)).$$

In particular, if we identify G and H with the sets of elements $\{(g,1) : g \in G\}$ and $\{(1,h) : h \in H\}$ respectively, then the primitive central idempotents of $\mathbb{Q}(G \times H)$ are $\{e_ie'_j : 1 \leq i \leq d, 1 \leq j \leq d'\}$.

Proof. We have

$$\mathbb{Q}(G\times H) \cong \mathbb{Q}G\otimes_{\mathbb{Q}}\mathbb{Q}H \cong (\bigoplus_i \mathbb{Q}Ge_i)\otimes_{\mathbb{Q}}(\bigoplus_j \mathbb{Q}He'_j) \cong \bigoplus_i \bigoplus_j (\mathbb{Q}Ge_i\otimes_{\mathbb{Q}}\mathbb{Q}He'_j).$$

By Lemma 4.2.2, each $\mathbb{Q}Ge_i \otimes \mathbb{Q}He'_j$ is simple, so this is the Wedderburn decomposition. The primitive central idempotents are the elements which map to the identity element of each $\mathbb{Q}Ge_i \otimes \mathbb{Q}Ge'_j$ (namely, $e_i \otimes e'_j$). But under the isomorphism $\nu : \mathbb{Q}G\otimes_{\mathbb{Q}}\mathbb{Q}H \to \mathbb{Q}(G \times H)$, which was defined in Lemma 4.2.1, we have $e_i \otimes e'_j \mapsto e_ie'_j$. Thus, $e_ie'_j$ maps to $e_i \otimes e'_j$, under the inverse isomorphism, as required. □

Once again, this result can be extended to a direct product of finitely many groups. However, if we drop the assumption that $(|G|, |H|) = 1$, then this result may fail. (Take $G = H = C_4$. Then, by Lemma 3.2.1, $\mathbb{Q}C_4 \cong \mathbb{Q}(i) \oplus \mathbb{Q} \oplus \mathbb{Q}$, where $i = \sqrt{-1}$. If the result held in this case, then $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i)$ would be a simple algebra. Since it is commutative, it would be a field. But $\{1, i\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(i)$, so that $\{1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i)$.

Thus, $1\otimes i+i\otimes 1\neq 0\neq 1\otimes i-i\otimes 1$. However, $(1\otimes i+i\otimes 1)(1\otimes i-i\otimes 1)=0$, a contradiction.)

Clearly, when G is nilpotent, this allows us to deduce the Wedderburn decomposition of $\mathbb{Q}G$ from the Wedderburn decompositions of $\mathbb{Q}S_i$, where the S_i are the Sylow subgroups of G.

For any subgroup, K, of a group G, let us write $\hat{K}=\sum_{k\in K}k$. (Then $\widehat{\langle g\rangle}=\hat{g}$, for any $g\in G$). The results of §3.6 show us that the homomorphic images of a group are of particular interest. Thus, we state

Proposition 4.2.4. *Let G be a finite group, and K a normal subgroup of G. Let $H=G/K$. Let $\bar{e}$ be a central idempotent of $\mathbb{Q}H$. If $\rho:\mathbb{Q}G\to\mathbb{Q}H$ is the natural homomorphism, then let e be any preimage of $\bar{e}$ under ρ. Then $e\frac{\hat{K}}{|K|}$ is a central idempotent of $\mathbb{Q}G$, and ρ restricts to an isomorphism $\rho:\mathbb{Q}Ge\frac{\hat{K}}{|K|}\to\mathbb{Q}H\bar{e}$. If $\bar{e}$ is a primitive central idempotent of $\mathbb{Q}H$, then $e\frac{\hat{K}}{|K|}$ is a primitive central idempotent of $\mathbb{Q}G$. In particular, if $M_n(D)$ is a Wedderburn component of $\mathbb{Q}H$, then it is also a Wedderburn component of $\mathbb{Q}G$.*

Proof. Since $\hat{K}^2=|K|\hat{K}$, it follows that $\frac{\hat{K}}{|K|}$ is an idempotent in $\mathbb{Q}G$. Further, since K is normal in G, $g^{-1}Kg=K$; hence, $g^{-1}\hat{K}g=\hat{K}$, for all $g\in G$. Thus, $\frac{\hat{K}}{|K|}$ is a central idempotent in $\mathbb{Q}G$. Now, $\rho(e)^2=\bar{e}^2=\bar{e}=\rho(e)$, which means that e^2-e is in $\Delta_{\mathbb{Q}}(G,K)$, where this notation was defined in §2.1. By Proposition 2.1.2, e^2-e is a sum of terms of the form $qg(k-1)$, with $q\in\mathbb{Q}$, $g\in G$, and $k\in K$. But, for any $k\in K$, $k\hat{K}=\hat{K}$, which means that $qg(k-1)\hat{K}=0$. Thus, $(e^2-e)\frac{\hat{K}}{|K|}=0$, which means that $(e\frac{\hat{K}}{|K|})^2=e\frac{\hat{K}}{|K|}$. Further, if $g\in G$, then $g^{-1}(e\frac{\hat{K}}{|K|})g=g^{-1}eg\frac{\hat{K}}{|K|}$, by the centrality of $\hat{K}$. Now, $\rho(g^{-1}eg)=\rho(g)^{-1}\bar{e}\rho(g)=\bar{e}=\rho(e)$, by the centrality of $\bar{e}$ in $\mathbb{Q}H$. That is, $g^{-1}eg-e\in\Delta_{\mathbb{Q}}(G,K)$. Once again, applying Proposition 2.1.2, we have $g^{-1}eg\frac{\hat{K}}{|K|}=e\frac{\hat{K}}{|K|}$. That is, $e\frac{\hat{K}}{|K|}$ is a central idempotent in $\mathbb{Q}G$.

Now, we have $\rho(e)=\bar{e}$, and $\rho(\frac{\hat{K}}{|K|})=1$. Thus, $\rho:\mathbb{Q}Ge\frac{\hat{K}}{|K|}\to\mathbb{Q}H\bar{e}$ is a homomorphism of $\mathbb{Q}$-algebras. Since $\rho(ge\frac{\hat{K}}{|K|})=gK\bar{e}$, for each $g\in G$, the map is surjective. Suppose that we have $\alpha\in\mathbb{Q}G$ such that $\rho(\alpha e\frac{\hat{K}}{|K|})=0$. Then $\rho(\alpha e)=0$, which means that $\alpha e\in\Delta_{\mathbb{Q}}(G,K)$. Thus, $\alpha e\frac{\hat{K}}{|K|}=0$. Therefore, $\rho:\mathbb{Q}Ge\frac{\hat{K}}{|K|}\to\mathbb{Q}H\bar{e}$ is an isomorphism. If $\bar{e}$ is a primitive central idempotent, then $\mathbb{Q}H\bar{e}$ is a simple algebra, and therefore, so is $\mathbb{Q}Ge\frac{\hat{K}}{|K|}$. By Proposition 2.3.1, $e\frac{\hat{K}}{|K|}$ is a primitive central idempotent. The last statement of the theorem is an immediate corollary. □

We need to compute some Wedderburn decompositions explicitly. In particular, recalling that

$$Q_{2^m} = \langle g, h \,|\, g^{2^{m-2}} = h^2, h^4 = 1, h^{-1}gh = g^{-1}\rangle,$$

we state

Proposition 4.2.5. *We have*

$$\mathbb{Q}Q_8 = \mathbb{Q}Q_8(\frac{1-g^2}{2}) \oplus \mathbb{Q}Q_8(\frac{1+g^2}{2}) \cong \mathbb{H}(\mathbb{Q}) \oplus 4\mathbb{Q}$$

(where $4\mathbb{Q}$ *means* $\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}$*), and* $\mathbb{H}(\mathbb{Q})\oplus4\mathbb{Q}$ *is the Wedderburn decomposition of* $\mathbb{Q}Q_8$.

Proof. Since g^2 is a central element of order 2, it is clear that $(1-g^2)/2$ and $(1+g^2)/2$ are orthogonal central idempotents which sum to 1. Thus,

$$\mathbb{Q}Q_8 = \mathbb{Q}Q_8((1+g^2)/2) \oplus \mathbb{Q}Q_8((1-g^2)/2).$$

Now, $1+g^2 = \widehat{\langle g^2\rangle}$. Since g^2 is central, $\langle g^2\rangle$ is normal. Thus, taking $G = Q_8$, $K = \langle g^2\rangle$, and $\bar{e} = 1$ in Proposition 4.2.4, we have $\mathbb{Q}Q_8((1+g^2)/2) \cong \mathbb{Q}(Q_8/\langle g^2\rangle)$. It is easy to see that $Q_8/\langle g^2\rangle \simeq C_2 \times C_2$. Now, by Lemma 4.2.1, $\mathbb{Q}(C_2 \times C_2) \cong \mathbb{Q}C_2 \otimes_{\mathbb{Q}} \mathbb{Q}C_2$. By Lemma 3.2.1, this is isomorphic to $(\mathbb{Q}\oplus\mathbb{Q}) \otimes_{\mathbb{Q}} (\mathbb{Q}\oplus\mathbb{Q})$, which is isomorphic to $4\mathbb{Q}$.

Let us write $\mathbb{H}(\mathbb{Q}) = \mathbb{Q}\dot{+}\mathbb{Q}x\dot{+}\mathbb{Q}y\dot{+}\mathbb{Q}xy$. We define a map $\delta : \mathbb{Q}Q_8 \to \mathbb{H}(\mathbb{Q})$, by letting $\delta(g) = x$ and $\delta(h) = y$. It is clear that this uniquely defines a homomorphism of $\mathbb{Q}$-algebras. Now,

$$\delta((1-g^2)/2) = (1-x^2)/2 = (1+1)/2 = 1.$$

Hence, restricting δ, we get $\delta : \mathbb{Q}Q_8((1-g^2)/2) \to \mathbb{H}(\mathbb{Q})$. Since $\delta((1-g^2)/2) = 1$, $\delta(g(1-g^2)/2) = x$, $\delta(h(1-g^2)/2) = y$, and $\delta(gh(1-g^2)/2) = xy$, it follows that this map is surjective. Now, $\dim_{\mathbb{Q}}Q_8 = 8$, and $\dim_{\mathbb{Q}}4\mathbb{Q} = 4$, implying that $\dim_{\mathbb{Q}}Q_8((1-g^2)/2) = 4$. Since $\dim_{\mathbb{Q}}\mathbb{H}(\mathbb{Q}) = 4$, we conclude that

$$\mathbb{Q}Q_8((1-g^2)/2) \cong \mathbb{H}(\mathbb{Q}).$$

Now, $\mathbb{Q}$ is a field, and $\mathbb{H}(\mathbb{Q})$ is a totally definite quaternion algebra, which is necessarily a division ring. Thus, each of these is a simple $\mathbb{Q}$-algebra, which means that we have found the Wedderburn decomposition. □

We need another Wedderburn decomposition. Let

$$D_8 = \langle \sigma, \tau \,|\, \sigma^4 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1}\rangle,$$

the dihedral group of order 8. Then, we have

Lemma 4.2.6. *The Wedderburn decomposition of* $\mathbb{Q}D_8$ *is* $M_2(\mathbb{Q}) \oplus 4\mathbb{Q}$, *where the projection* $\mathbb{Q}D_8 \longrightarrow M_2(\mathbb{Q})$ *is given by*

$$\sigma \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proof. Since σ^2 is a central element of order 2 in D_8, it follows that

$$\mathbb{Q}D_8 \cong \mathbb{Q}D_8((1-\sigma^2)/2) \oplus \mathbb{Q}D_8((1+\sigma^2)/2).$$

Now, $1+\sigma^2 = \widehat{\langle\sigma^2\rangle}$. Thus, if we take $G = D_8$, $K = \langle\sigma^2\rangle$, and $\bar{e} = 1$ in Proposition 4.2.4, then we find that $\mathbb{Q}D_8((1+\sigma^2)/2) \cong \mathbb{Q}(D_8/\langle\sigma^2\rangle)$. Clearly, $D_8/\langle\sigma^2\rangle \simeq C_2 \times C_2$. Just as in the proof of Proposition 4.2.5, we obtain

$$\mathbb{Q}D_8((1+\sigma^2)/2) \cong (2\mathbb{Q}) \otimes_{\mathbb{Q}} (2\mathbb{Q}) \cong 4\mathbb{Q}.$$

We define a map $\delta : \mathbb{Q}D_8 \longrightarrow M_2(\mathbb{Q})$ as described in the statement of the lemma. It is easy to verify that this definition uniquely determines a $\mathbb{Q}$-algebra homomorphism. Further,

$$\delta((1-\sigma^2)/2) = \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix} - \begin{pmatrix} -1/2 & 0 \\ 0 & -1/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore, restricting δ, we obtain a homomorphism $\delta : \mathbb{Q}D_8((1-\sigma^2)/2) \longrightarrow M_2(\mathbb{Q})$. It is also easy to see that this map is surjective. (If $q \in \mathbb{Q}$, then

$$\delta((\frac{q}{2}\tau - \frac{q}{2}\sigma^2)((1-\sigma^2)/2)) = \begin{pmatrix} q/2 & 0 \\ 0 & -q/2 \end{pmatrix} - \begin{pmatrix} -q/2 & 0 \\ 0 & -q/2 \end{pmatrix} = \begin{pmatrix} q & 0 \\ 0 & 0 \end{pmatrix}.$$

Similarly, we can put arbitrary elements of $\mathbb{Q}$ in each matrix position.) Now, $\dim_{\mathbb{Q}}\mathbb{Q}D_8((1-\sigma^2)/2) = \dim_{\mathbb{Q}}\mathbb{Q}D_8 - \dim_{\mathbb{Q}}\mathbb{Q}D_8((1+\sigma^2)/2) = 8-4 = 4$. Since $\dim_{\mathbb{Q}}M_2(\mathbb{Q}) = 4$, it follows that $\mathbb{Q}D_8((1-\sigma^2)/2) \cong M_2(\mathbb{Q})$. Since $\mathbb{Q}$ and $M_2(\mathbb{Q})$ are simple $\mathbb{Q}$-algebras, we have found the Wedderburn decomposition. □

We should point out that D_8 is not particularly interesting to us, *per se*. It is, however, a homomorphic image of some groups which are interesting to us. We have

Proposition 4.2.7. *For all* $m \geq 4$, *the group algebra* $\mathbb{Q}Q_{2^m}$ *has* $M_2(\mathbb{Q})$ *among its Wedderburn components.*

Proof. Let $\kappa : Q_{2^m} \longrightarrow D_8$ be defined via $\kappa(g) = \sigma$, $\kappa(h) = \tau$. Since $\sigma^4 = 1 = \tau^2$, and $\tau^{-1}\sigma\tau = \sigma^{-1}$, κ is a homomorphism. Clearly, κ is surjective. Thus, by Lemma 4.2.6 and Proposition 4.2.4, we are done. □

One last result is required.

Proposition 4.2.8. *Let G be a finite group, and let e be a primitive central idempotent of $\mathbb{Q}G$. Let K be the kernel of the homomorphism from G to Ge, given by $g \mapsto ge$. Let $H = G/K$. Let $\bar{e}$ be the image of e under the natural map $\mathbb{Q}G \to \mathbb{Q}H$. Then $\bar{e}$ is a primitive central idempotent of $\mathbb{Q}H$, and the induced map $\mathbb{Q}Ge \to \mathbb{Q}H\bar{e}$ is an isomorphism. In particular, if $\mathbb{Q}Ge \cong M_n(D)$, then $M_n(D)$ is a Wedderburn component of $\mathbb{Q}H$. Further, the map $h \mapsto h\bar{e}$, for $h \in H$, is injective.*

Proof. Let $\eta : \mathbb{Q}G \to \mathbb{Q}H$ be the natural homomorphism. Since $\bar{e}^2 = \eta(e^2) = \eta(e) = \bar{e}$, we know that $\bar{e}$ is an idempotent. Further, if $\alpha \in \mathbb{Q}G$, then since $\alpha e = e\alpha$, we have $\eta(\alpha e) = \eta(e\alpha)$, which means that $\eta(\alpha)\bar{e} = \bar{e}\eta(\alpha)$. Since η is surjective, $\bar{e}$ is central in $\mathbb{Q}H$. It is clear that the restriction $\eta : \mathbb{Q}Ge \to \mathbb{Q}H\bar{e}$ is an epimorphism. We must show that this map is injective. Suppose that $\eta(\alpha e) = 0$, for some $\alpha \in \mathbb{Q}G$. Then, by the definition of $\Delta_{\mathbb{Q}}(G, K)$, we have $\alpha e \in \Delta_{\mathbb{Q}}(G, K)$. Thus, by Proposition 2.1.2, αe is a sum of terms of the form $qg(k-1)$, with $q \in \mathbb{Q}$, $g \in G$, and $k \in K$. It follows immediately that $\alpha e\frac{\hat{K}}{|K|} = 0$. However, $ke = e$, for each $k \in K$, which means that $\hat{K}e = |K|e$. Thus, $\alpha e = 0$. Therefore, $\mathbb{Q}Ge \cong \mathbb{Q}H\bar{e}$. Since $\mathbb{Q}Ge$ is simple, Proposition 2.3.1 tells us that $\bar{e}$ is a primitive central idempotent of $\mathbb{Q}H$. Now, suppose that $h\bar{e} = \bar{e}$, for some $h \in H$. Writing $h = gK$, with $g \in G$, we have $\eta(ge) = h\bar{e} = \bar{e} = \eta(e)$. That is, $ge - e \in \Delta_{\mathbb{Q}}(G, K)$. Thus, $(ge - e)\frac{\hat{K}}{|K|} = 0$, and by our previous argument, $ge = e$. Therefore, $g \in K$, which means that $h = 1$. □

§4.3 Cases Where the Bicyclic and Bass Cyclic Units Suffice

At this point, we have the pleasant task of drawing some conclusions from the results in previous sections. In fact, the results of §§3.6 and 4.1 are sufficient to give us a rather surprisingly strong result.

Theorem 4.3.1 (Ritter-Sehgal). *Let G be a finite nilpotent group of odd order. Then the Bass cyclic and bicyclic units of $\mathbb{Z}G$ generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

Proof. By Corollary 3.6.5, we need only show that G has no nonabelian fixed point free homomorphic images. By Corollary 4.1.6, the only nonabelian fixed point free nilpotent groups are of the form $Q_{2^m} \times C_n$, where $m \geq 3$, and n is an odd natural number. Since any homomorphic image of a nilpotent group is nilpotent, any fixed point free nonabelian homomorphic image of G is of the form $Q_{2^m} \times C_n$. No such group can be the homomorphic image of a group of odd order. We are done. □

However, we can obtain a stronger result. Perhaps the simplest condition on the Wedderburn components of $\mathbb{Q}G$, under which the Bass cyclic and bicyclic units will suffice, is given in

Theorem 4.3.2 (Jespers-Leal). *Let G be a finite nilpotent group. Suppose that $\mathbb{Q}G$ does not have any Wedderburn components of the following types:*

(1) $\mathbb{H}(\mathbb{Q})$;

(2) *a 2×2 matrix ring over $\mathbb{Q}$, an imaginary quadratic extension of the rationals, or a noncommutative division algebra.*

Then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$.

Proof. By Theorem 3.6.4, it will be sufficient if we can show that G has no nonabelian fixed point free homomorphic images. Since G is nilpotent, any such homomorphic image would be nilpotent. Thus, by Corollary 4.1.6, G would have a homomorphic image of the form $Q_{2^m} \times C_n$, for some $m \geq 3$, and some odd number n. Thus, G would have $\mathbb{Q}_{2^m}$ as a homomorphic image, for some $m \geq 3$. If $m \geq 4$, then by Proposition 4.2.7, $\mathbb{Q}Q_{2^m}$ has $M_2(\mathbb{Q})$ as a Wedderburn component. By Proposition 4.2.4, it follows that $\mathbb{Q}G$ has $M_2(\mathbb{Q})$ as a Wedderburn component. This is forbidden. Thus, we may assume that G has $\mathbb{Q}_8$ as a homomorphic image. By Proposition 4.2.5, $\mathbb{Q}Q_8$ has $\mathbb{H}(\mathbb{Q})$ as a Wedderburn component. Therefore, Proposition 4.2.4 tells us that $\mathbb{Q}G$ has $\mathbb{H}(\mathbb{Q})$ as a Wedderburn component, which is not permitted. □

It seems, somehow, a little strange that the absence of a totally definite quaternion algebra as a Wedderburn component should be a determining condition, since the results of §3.4 show that this component is innocuous. In fact, we can deduce a slightly stronger result, namely

Theorem 4.3.3. *Let G be a finite nilpotent group. Suppose that $\mathbb{Q}G$ does not have any Wedderburn components of the following types:*

(1) $\mathbb{H}(\mathbb{Q}(\xi_p))$, *for some odd prime p, and a primitive p^{th} root of unity, ξ_p;*

(2) *a 2×2 matrix ring over $\mathbb{Q}$, an imaginary quadratic extension of the rationals, or a noncommutative division algebra.*

Then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$.

Proof. We wish to apply Corollary 3.5.9. To do so, we must verify that $\mathbb{Q}G$ has no exceptional Wedderburn components. Since 2×2 exceptional components are forbidden, let us suppose that e_i is a primitive central idempotent of $\mathbb{Q}G$, and $\mathbb{Q}Ge_i \cong D_i$, where D_i is some division algebra. By Proposition 3.6.2, Ge_i is fixed point free. Since Ge_i is the homomorphic image of a nilpotent group, it is nilpotent. By Corollary 4.1.6, either Ge_i is cyclic, in which case $\mathbb{Q}Ge_i$ is commutative, and therefore nonexceptional, or $Ge_i \simeq Q_{2^m} \times C_n$, for some $m \geq 3$, and some odd number n. If $m \geq 4$, then just as in the proof of Theorem 4.3.2, we discover that $\mathbb{Q}G$ has $M_2(\mathbb{Q})$ as a Wedderburn component, which is not allowed.

Suppose $Ge_i \simeq Q_8 \times C_n$, where $n \geq 3$. Then, if p is any prime dividing n, we know that C_n projects onto C_p. Therefore, G has $Q_8 \times C_p$ as a homomorphic image. Now, by Proposition 4.2.5, $\mathbb{Q}Q_8$ has $\mathbb{H}(\mathbb{Q})$ as a Wedderburn component. By Lemma 3.2.1, $\mathbb{Q}C_p$ has $\mathbb{Q}(\xi_p)$ as a Wedderburn component. It follows from Proposition 4.2.3 that $\mathbb{Q}(Q_8 \times C_n)$ has $\mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_p) \cong \mathbb{H}(\mathbb{Q}(\xi_p))$ as a Wedderburn component. This is unacceptable.

Thus, we must conclude that $Ge_i \simeq Q_8$. By Proposition 4.2.8, $\mathbb{Q}Q_8$ has $\mathbb{Q}Ge_i$ as a Wedderburn component. By Proposition 4.2.5, this Wedderburn component must be $\mathbb{Q}$ or $\mathbb{H}(\mathbb{Q})$, neither of which is exceptional. Therefore, $\mathbb{Q}G$ has no exceptional Wedderburn components. Thus, the H_{f_i} defined in §3.5, together with $\mathcal{B}_1$, generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

By Lemma 3.6.3, we may assume that $H_{f_i} \leq \mathcal{B}_2$, provided Ge_i is not fixed point free. We just finished showing that if Ge_i is fixed point free, then $Ge_i \simeq Q_8$, and then Ge_i is a division algebra. The H_{f_i} are only defined when the Wedderburn component is not a division algebra. Thus, we may always assume that $H_{f_i} \leq \mathcal{B}_2$. Hence, $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$. □

A special case of this result allows us to improve Theorem 4.3.1.

Corollary 4.3.4. *Let G be a finite nilpotent group. Suppose that the Sylow 2-subgroup of G is abelian. Then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$.*

Proof. By Theorem 4.3.2, it will be sufficient if we can show that the Wedderburn components of $\mathbb{Q}G$ do not include any noncommutative division rings, or any 2×2 matrix rings. Let S_1 be the Sylow 2-subgroup of G, and let S_2 be the direct product of all of the other Sylow subgroups. Thus, $G \simeq S_1 \times S_2$. Since S_1 is abelian, $\mathbb{Q}S_1$ is commutative, which means that its Wedderburn decomposition is a direct sum of fields, $\mathbb{Q}S_1 \cong \bigoplus_j F_j$. Now, S_2 has odd order. Thus, applying Theorem 2.2.6, the Wedderburn decomposition of $\mathbb{Q}S_2$ is $\bigoplus_i M_{n_i}(D_i)$, for various division algebras D_i, and odd numbers n_i. By Proposition 4.2.3, the Wedderburn components of $\mathbb{Q}G$ are of the form $F_j \otimes_{\mathbb{Q}} M_{n_i}(D_i)$. By Lemma 4.2.2, $F_j \otimes_{\mathbb{Q}} D_i$ is a simple algebra. Thus, $F_j \otimes_{\mathbb{Q}} D_i \cong M_k(D)$, for some natural number k and division algebra D. That is, $F_j \otimes_{\mathbb{Q}} M_{n_i}(D_i) \cong M_{kn_i}(D)$. If $kn_i \leq 2$, then $n_i \leq 2$. Since n_i must be odd, $n_i = 1$. Now, if e_i' is a primitive central idempotent of $\mathbb{Q}S_2$ such that $\mathbb{Q}S_2 e_i' \cong D_i$, then Proposition 3.6.2 tells us that $S_2 e_i'$ is fixed point free. That is, $S_2 e_i'$ is a fixed point free nilpotent group, which is a homomorphic image of S_2. If $S_2 e'_i$ is nonabelian, then $S_2 e'_i \simeq Q_{2^m} \times C_n$, for some $m \geq 3$, and some odd number n, which is impossible for a group of odd order. Therefore, $S_2 e'_i$ is abelian, forcing $\mathbb{Q}S_2 e'_i$ to be a field, F. It follows that $F_j \otimes_{\mathbb{Q}} F$ is commutative. We are done. □

Since the 2-groups of order less than 8 are abelian, we have

Corollary 4.3.5. *Let G be a finite nilpotent group. If the order of G is not divisible by 8, then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$.*

Remark 4.3.6. In fact, the work of Ritter and Sehgal, in [RS2], tells us that Theorem 4.3.1, and Corollaries 4.3.4 and 4.3.5 remain true if we substitute the one-sided bicyclic units for the bicyclic units. It is not presently known whether or not Theorem 4.3.3 would hold with the one-sided bicyclic units.

§4.4 A Counterexample

Unfortunately, there are nilpotent groups, G, which do not satisfy

$$|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty.$$

For the remainder of this section, let

$$G = \langle g, h \,|\, g^4 = h^4 = 1, h^{-1}gh = g^{-1} \rangle.$$

This a well-known group of order 16, and exponent 4. Since $h^2 \in Z(G)$, we know that $\langle h^2 \rangle$ is a normal subgroup of G. Further,

$$G/\langle h^2 \rangle \simeq \langle \bar{g}, \bar{h} | \bar{g}^4 = \bar{h}^2 = 1, \bar{h}^{-1}\bar{g}\bar{h} = \bar{g}^{-1} \rangle = D_8.$$

By Lemma 4.2.6, $\mathbb{Q}D_8$ has $M_2(\mathbb{Q})$ as a Wedderburn component. Therefore, Proposition 4.2.4 tells us that $\mathbb{Q}G$ has $M_2(\mathbb{Q})$ as a Wedderburn component. Thus, the results of §4.3 do not apply. This is not, however, sufficient to guarantee that $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle|$ is infinite, since D_8 has an exceptional component, but $|\mathcal{U}(\mathbb{Z}D_8) : \langle \mathcal{B}_1, \mathcal{B}_2 \rangle| < \infty$. (See [Se2, Theorem 23.1]). However, in [RS2], Ritter and Sehgal showed that the Bass cyclic and one-sided bicyclic units generate a subgroup of infinite index in $\mathcal{U}(\mathbb{Z}G)$. It turns out that the inclusion of all of the Bass cyclic units does not improve our situation at all, as we shall prove at this time.

Let us begin by eliminating the Bass cyclic units from consideration.

Lemma 4.4.1. *The Bass cyclic units of $\mathbb{Z}G$ are all equal to* 1.

Proof. Take $x \in G$. Proposition 3.2.2 tells us that the Bass cyclic units corresponding to x are in $\mathcal{U}(\mathbb{Z}\langle x\rangle)$. Since the exponent of G is 4, Proposition 3.4.4 tells us that these Bass cyclic units are in $\pm\langle x\rangle$. Further, the augmentation of any Bass cyclic unit is easily seen to be 1, which means that these Bass cyclic units are in $\langle x\rangle$. Now, if $|x| = 1$ or 2, there are no Bass cyclic units. Thus, we may assume that $|x| = 4$. In the definition of these units, from §3.2, the only possible value for i is 3. Since we take $m = \varphi(|G|) = 8$, our Bass cyclic unit can only be

$$u = (1 + x + x^2)^8 - k\hat{x},$$

for a suitable integer k. Let $i = \sqrt{-1}$. Then, let $\rho : \mathbb{Q}\langle x\rangle \to \mathbb{Q}(i)$ be the usual projection, given by $x \mapsto i$. We have

$$\rho(u) = (1 + i - 1)^8 - k(1 + i - 1 - i) = i^8 = 1.$$

However, $\rho(x) = i$, $\rho(x^2) = -1$, and $\rho(x^3) = -i$, which means that we can only have $u = 1$. □

For any $x, y \in G$, let us write

$$u_{x,y} = 1 + (1 - x)y\hat{x}, \text{ and } u'_{x,y} = 1 + \hat{x}y(1 - x),$$

for the bicyclic units of $\mathbb{Z}G$. For any $\bar{x}, \bar{y} \in D_8$, we will write

$$v_{\bar{x},\bar{y}} = 1 + (1 - \bar{x})\bar{y}\hat{\bar{x}}, \text{ and } v'_{\bar{x},\bar{y}} = 1 + \hat{\bar{x}}\bar{y}(1 - \bar{x}),$$

for the bicyclic units of $\mathbb{Z}D_8$. Let $\eta : \mathbb{Q}G \to \mathbb{Q}D_8$ be the usual map induced from the projection $G \to D_8$. (Thus, $\eta(x) = \bar{x}$, for all $x \in G$). We observe that $\eta(u_{x,y}) = 1 + (1 - \bar{x})\bar{y}\eta(\hat{x})$. We note that $\eta(\hat{x})$ is not necessarily equal to $\hat{\bar{x}}$, since the order of x in G need not be the order of $\bar{x}$ in D_8. Certainly, the latter divides the former. Thus, $\eta(\hat{x}) = \frac{|x|}{|\bar{x}|}\hat{\bar{x}}$. Therefore,

$$\eta(u_{x,y}) = 1 + (1 - \bar{x})\bar{y}\frac{|x|}{|\bar{x}|}\hat{\bar{x}} = (v_{\bar{x},\bar{y}})^{|x|/|\bar{x}|}.$$

Similarly, $\eta(u'_{x,y}) = (v'_{\bar{x},\bar{y}})^{|x|/|\bar{x}|}$. Taking $\bar{x}, \bar{y} \in D_8$, it easy to see that if $\bar{y}$ normalizes the subgroup $\langle\bar{x}\rangle$, then $v_{\bar{x},\bar{y}} = 1$. Since $\langle\bar{g}^k\rangle$ is normal in D_8, for all integers k, we may assume that $\bar{x} = \bar{g}^k\bar{h}$, for some k. The order of any such element $\bar{x}$ is 2, whereas the order of any x satisfying $\eta(x) = \bar{x}$ is 4. (These are the elements of the form g^kh^j, $0 \le k \le 3$, $j = 1$ or 3). Thus,

$$\eta(\mathcal{B}_2) \le \langle(v_{\bar{x},\bar{y}})^2, (v'_{\bar{x},\bar{y}})^2 : \bar{y} \in D_8, \bar{x} = \bar{g}^k\bar{h}, 0 \le k \le 3\rangle.$$

Further, we observe that for any natural numbers j and k, we have

$$\begin{aligned} v_{\bar{g}^k\bar{h},\bar{g}^j\bar{h}} &= 1 + (1-\bar{g}^k\bar{h})\bar{g}^j\bar{h}(1+\bar{g}^k\bar{h}) \\ &= 1 + (1-\bar{g}^k\bar{h})\bar{g}^{j-k}(\bar{g}^k\bar{h}(1+\bar{g}^k\bar{h})) \\ &= 1 + (1-\bar{g}^k\bar{h})\bar{g}^{j-k}(\bar{g}^k\bar{h}+1) \\ &= v_{\bar{g}^k\bar{h},\bar{g}^{j-k}}. \end{aligned}$$

Similarly, we obtain

$$\begin{aligned} v'_{\bar{g}^k\bar{h},\bar{g}^j\bar{h}} &= 1 + (1+\bar{g}^k\bar{h})\bar{g}^j\bar{h}(1-\bar{g}^k\bar{h}) \\ &= 1 + ((1+\bar{g}^k\bar{h})\bar{g}^k\bar{h})\bar{g}^{k-j}(1-\bar{g}^k\bar{h}) \\ &= v'_{\bar{g}^k\bar{h},\bar{g}^{k-j}}. \end{aligned}$$

Since 1 and $\bar{g}^2$ are central, we have

$$v_{\bar{x},1} = v_{\bar{x},\bar{g}^2} = v'_{\bar{x},1} = v'_{\bar{x},\bar{g}^2} = 1,$$

for all $\bar{x} \in D_8$. It follows that

$$\eta(\mathcal{B}_2) \leq \langle (v_{\bar{x},\bar{y}})^2, (v'_{\bar{x},\bar{y}})^2 : \bar{x} = \bar{g}^k\bar{h}, 0 \leq k \leq 3, \bar{y} = \bar{g} \text{ or } \bar{g}^3 \rangle.$$

Let us write

$$X = \langle v_{\bar{x},\bar{y}}, v'_{\bar{x},\bar{y}} : \bar{x} = \bar{g}^k\bar{h}, 0 \leq k \leq 3, \bar{y} = \bar{g} \text{ or } \bar{g}^3 \rangle,$$

and

$$Y = \langle (v_{\bar{x},\bar{y}})^2, (v'_{\bar{x},\bar{y}})^2 : \bar{x} = \bar{g}^k\bar{h}, 0 \leq k \leq 3, \bar{y} = \bar{g} \text{ or } \bar{g}^3 \rangle.$$

We wish to compute $T(X)$ and $T(Y)$, where $T : \mathbb{Q}D_8 \to M_2(\mathbb{Q})$ is the projection which we defined in Lemma 4.2.6. That is,

$$T(\bar{g}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T(\bar{h}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Since $T(\bar{g}^2) = -I_2$, it follows that

$$T(v_{\bar{x},\bar{g}^3}) = T(1 + (1-\bar{x})\bar{g}^3\hat{\bar{x}}) = T(1 - (1-\bar{x})\bar{g}\hat{\bar{x}}) = T(v_{\bar{x},\bar{g}})^{-1},$$

for any $\bar{x} \in D_8$. Similarly, $T(v'_{\bar{x},\bar{g}^3}) = T(v'_{\bar{x},\bar{g}})^{-1}$, for any $\bar{x} \in D_8$. Thus,

$$T(X) = \langle T(v_{\bar{x},\bar{g}}), T(v'_{\bar{x},\bar{g}}) : \bar{x} = \bar{g}^k\bar{h}, 0 \leq k \leq 3 \rangle,$$

and

$$T(Y) = \langle T(v_{\bar{x},\bar{g}})^2, T(v'_{\bar{x},\bar{g}})^2 : \bar{x} = \bar{g}^k\bar{h}, 0 \leq k \leq 3 \rangle.$$

Some simple computations tell us that

$$T(v_{\bar{h},\bar{g}}) = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}, T(v'_{\bar{h},\bar{g}}) = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix},$$

$$T(v_{\bar{g}\bar{h},\bar{g}}) = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}, T(v'_{\bar{g}\bar{h},\bar{g}}) = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix},$$

$$T(v_{\bar{g}^2\bar{h},\bar{g}}) = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} = T(v'_{\bar{h},\bar{g}}), T(v'_{\bar{g}^2\bar{h},\bar{g}}) = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} = T(v_{\bar{h},\bar{g}}),$$

$$T(v_{\bar{g}^3\bar{h},\bar{g}}) = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} = T(v'_{\bar{g}\bar{h},\bar{g}}), \text{ and } T(v'_{\bar{g}^3\bar{h},\bar{g}}) = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} = T(v_{\bar{g}\bar{h},\bar{g}}).$$

Therefore,

$$T(X) = \langle \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} \rangle,$$

and

$$T(Y) = \langle \begin{pmatrix} 1 & 0 \\ -8 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -3 & 4 \\ -4 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ -4 & -3 \end{pmatrix} \rangle,$$

where these are, of course, subgroups of $SL_2(\mathbb{Z})$.

A little terminology is required. We write $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\langle \pm I_2 \rangle$. For any integer $n \geq 2$, we define

$$\Gamma(n) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \langle \pm I_2 \rangle \in PSL_2(\mathbb{Z}) : a \equiv d \equiv \pm 1 \pmod{n}, b \equiv c \equiv 0 \pmod{n} \}.$$

It is clear that $\Gamma(n)$ is a normal subgroup of $PSL_2(\mathbb{Z})$. Further, it is well-known that $\Gamma(2)$ is a free group of rank 2, for the proof of which we refer the reader to [Ne, p. 149].

Let us suppose that $|\mathcal{U}(\mathbb{Z}G) : \mathcal{B}_2| < \infty$. Then, since $\mathbb{Z}G$ is an order in $\mathbb{Q}G$, $T(\eta(\mathbb{Z}G))$ is an order in $T(\eta(\mathbb{Q}G)) = M_2(\mathbb{Q})$, and $T(\eta(\mathcal{B}_2))$ is of finite index in the unit group of this order. However, $M_2(\mathbb{Z})$ is another order in $M_2(\mathbb{Q})$. By Lemma 3.3.4, $T(\eta(\mathcal{B}_2))$ contains a subgroup of finite index in $GL_2(\mathbb{Z})$. We showed above that $T(\eta(\mathcal{B}_2)) \leq SL_2(\mathbb{Z})$. Thus, $T(\eta(\mathcal{B}_2))$ is of finite index in $SL_2(\mathbb{Z})$. Therefore, $T(\eta(\mathcal{B}_2))\langle \pm I_2 \rangle / \langle \pm I_2 \rangle$ is of finite index in $PSL_2(\mathbb{Z})$. In fact, since

$$T(\eta(\mathcal{B}_2))\langle \pm I_2 \rangle / \langle \pm I_2 \rangle \leq T(Y)\langle \pm I_2 \rangle / \langle \pm I_2 \rangle \leq \Gamma(2),$$

it follows that $T(Y)\langle \pm I_2 \rangle / \langle \pm I_2 \rangle$ is of finite index in $\Gamma(2)$. Let us say that this index is m. Now, Schreier's Theorem tells us that if F is a free group of finite rank a, and F_1 is a subgroup of F of index $b < \infty$, then F_1 is a free group of rank $ab - b + 1$. (See [Su, p. 185]). Thus, $T(Y)\langle \pm I_2 \rangle / \langle \pm I_2 \rangle$ is free of rank $m + 1$. But this group is generated by four elements. Therefore, $m \leq 3$. Now, we have

$$T(Y)\langle \pm I_2 \rangle / \langle \pm I_2 \rangle \leq T(X)\langle \pm I_2 \rangle / \langle \pm I_2 \rangle \leq \Gamma(2).$$

Suppose that any two of these three groups are the same. Then, taking the groups generated by each of these groups, together with $\Gamma(4)$, we would still have identical groups. Now, it is obvious that $T(Y)\langle \pm I_2\rangle/\langle \pm I_2\rangle \leq \Gamma(4)$. However, $T(X)\langle \pm I_2\rangle/\langle \pm I_2\rangle$ contains the element $\left(\begin{smallmatrix} -1 & 2 \\ -2 & 3 \end{smallmatrix}\right)\langle \pm I_2\rangle$, which is not in $\Gamma(4)$.

Let us suppose that

$$\langle T(X)\langle \pm I_2\rangle/\langle \pm I_2\rangle, \Gamma(4)\rangle = \Gamma(2).$$

Then, modulo $\Gamma(4)$, these groups are still the same. However, modulo $\Gamma(4)$, we have

$$T(X)\langle \pm I_2\rangle/\langle \pm I_2\rangle = \langle \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\rangle\langle \pm I_2\rangle/\langle \pm I_2\rangle.$$

Thus, this group does not contain $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)\langle \pm I_2\rangle/\langle \pm I_2\rangle$. It follows that

$$T(Y)\langle \pm I_2\rangle/\langle \pm I_2\rangle \lneqq T(X)\langle \pm I_2\rangle/\langle \pm I_2\rangle \lneqq \Gamma(2).$$

Thus, the index of each group in the next is at least 2. Therefore, the index of $T(Y)\langle \pm I_2\rangle/\langle \pm I_2\rangle$ in $\Gamma(2)$ is at least 4, a contradiction.

In summary, we state

Theorem 4.4.2 (Ritter-Sehgal). *There are finite nilpotent groups (indeed, 2-groups), G, such that $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2\rangle| = \infty$. Indeed,*

$$\langle g, h \,|\, g^4 = h^4 = 1, h^{-1}gh = g^{-1}\rangle$$

is such a group.

§4.5 Fixed Point Free Homomorphic Images

For this section, let us write $i = \sqrt{-1}$. In Theorem 4.3.3, we had to exclude Wedderburn components of the form $\mathbb{H}(\mathbb{Q}(\xi_p))$, for odd primes p. However, these components need not be exceptional, since they need not be division algebras. Proposition 4.2.5 tells us that the Wedderburn decomposition of $\mathbb{Q}Q_8$ is $\mathbb{H}(\mathbb{Q}) \oplus 4\mathbb{Q}$. Lemma 3.2.1 informs us that the Wedderburn decomposition of $\mathbb{Q}C_n$ is $\bigoplus_{d|n} \mathbb{Q}(\xi_d)$, for any integer n. Thus, by Proposition 4.2.3, it follows that for any odd number n, the Wedderburn decomposition of $\mathbb{Q}(Q_8 \times C_n)$ is

$$(\bigoplus_{d|n} \mathbb{H}(\mathbb{Q}(\xi_d))) \oplus (\bigoplus_{d|n} 4\mathbb{Q}(\xi_d)).$$

In particular, $\mathbb{H}(\mathbb{Q}(\xi_n))$ is a simple $\mathbb{Q}$-algebra. Clearly, it is 4-dimensional over its centre, $\mathbb{Q}(\xi_n)$. Any 3×3 or larger matrix ring would be at least 9-dimensional over its centre, and $M_2(D)$ is 4-dimensional over its centre, if and only if D is commutative. That is, either $\mathbb{H}(\mathbb{Q}(\xi_n))$ is a division ring, or $\mathbb{H}(\mathbb{Q}(\xi_n)) \cong M_2(\mathbb{Q}(\xi_n))$. We have

Lemma 4.5.1. *Let n be an odd natural number. Then $\mathbb{H}(\mathbb{Q}(\xi_n)) \cong M_2(\mathbb{Q}(\xi_n))$ if and only if there exist $\alpha, \beta, \gamma \in \mathbb{Q}(\xi_n)$ such that $\alpha^2 + \beta^2 + \gamma^2 = -1$.*

Proof. Suppose there exist $\alpha, \beta, \gamma \in \mathbb{Q}(\xi_n)$ such that $\alpha^2 + \beta^2 + \gamma^2 = -1$. Then, writing $\mathbb{H}(\mathbb{Q}(\xi_n)) = \mathbb{Q}(\xi_n) \dot{+} \mathbb{Q}(\xi_n)x \dot{+} \mathbb{Q}(\xi_n)y \dot{+} \mathbb{Q}(\xi_n)xy$, we have

$$(\alpha + \beta x + \gamma y + xy)(\alpha - \beta x - \gamma y - xy) = \alpha^2 + \beta^2 + \gamma^2 + 1 = 0.$$

A division algebra has no zero divisors; hence, $\mathbb{H}(\mathbb{Q}(\xi_n)) \cong M_2(\mathbb{Q}(\xi_n))$. Suppose that $\mathbb{H}(\mathbb{Q}(\xi_n)) \cong M_2(\mathbb{Q}(\xi_n))$. For any $\delta_1, \delta_2, \delta_3, \delta_4 \in \mathbb{Q}(\xi_n)$, we have

$$(\delta_1 + \delta_2 x + \delta_3 y + \delta_4 xy)(\delta_1 - \delta_2 x - \delta_3 y - \delta_4 xy) = \delta_1^2 + \delta_2^2 + \delta_3^2 + \delta_4^2.$$

Thus, if $\delta_1^2 + \delta_2^2 + \delta_3^2 + \delta_4^2 \neq 0$, except when all of the δ_j are 0, then every nonzero element of $\mathbb{H}(\mathbb{Q}(\xi_n))$ is a unit, contrary to our assumption. Thus, there is a nontrivial solution to $\delta_1^2 + \delta_2^2 + \delta_3^2 + \delta_4^2 = 0$ in $\mathbb{Q}(\xi_n)$. Without loss of generality, let us say that $\delta_1 \neq 0$. Then, taking $\alpha = \delta_2\delta_1^{-1}$, $\beta = \delta_3\delta_1^{-1}$, and $\gamma = \delta_4\delta_1^{-1}$, we have the desired solution. □

It is clear that it would be helpful to know the minimum number of squares which sum to -1 in a given field, K. We will denote this value by $\mathcal{S}(K)$, when it exists. (If, for instance, $K \leq \mathbb{R}$, then we are definitely not going to find any number of squares summing to -1). In fact, this problem has been solved for the cyclotomic fields. Evidently, if $4|n$, then $i \in \mathbb{Q}(\xi_n)$, which means that $\mathcal{S}(\mathbb{Q}(\xi_n)) = 1$. If n is even, but not a multiple of 4, then $-\xi_{n/2}$ is a primitive n^{th} root of unity; hence, $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{n/2})$. Thus, the following result is reduced to the case where n is odd. The proof of that case is given in [Mo, Théorème 1]. Let us observe that if $n > 1$ is an odd number, then by the order of 2 mod n, we mean the order of 2 as an element of $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.

Lemma 4.5.2 (Moser). *Let $n > 2$ be a natural number.*

(a) If $4|n$, then $\mathcal{S}(\mathbb{Q}(\xi_n)) = 1$.

(b) If $n \equiv 2 \pmod 4$, then $\mathcal{S}(\mathbb{Q}(\xi_n)) = \mathcal{S}(\mathbb{Q}(\xi_{n/2}))$.

(c) If n is odd, then $\mathcal{S}(\mathbb{Q}(\xi_n)) = 2$ if the order of 2 mod n is even; otherwise, $\mathcal{S}(\mathbb{Q}(\xi_n)) = 4$.

Combining these two results, we obtain

Proposition 4.5.3. *Let $n > 1$ be an odd natural number. The following are equivalent:*

(1) $\mathbb{H}(\mathbb{Q}(\xi_n)) \cong M_2(\mathbb{Q}(\xi_n))$;

(2) *there exist* $\alpha, \beta \in \mathbb{Q}(\xi_n)$ *such that* $\alpha^2 + \beta^2 = -1$;

(3) *the order of* 2 mod n *is even.*

Let $\langle d \rangle$ be a cyclic group of order n. If $\gamma = \sum_{a=0}^{n-1} \gamma_a d^a \in \mathbb{C}\langle d \rangle$, then we write $\Re(\gamma) = \sum_{a=0}^{n-1} \mathrm{Re}(\gamma_a) d^a$, and $\Im(\gamma) = \sum_{a=0}^{n-1} \mathrm{Im}(\gamma_a) d^a$. We will denote complex conjugation by a bar; thus, $\bar{\gamma} = \sum_{a=0}^{n-1} \overline{\gamma_a} d^a$.

Some technical facts are contained in

Lemma 4.5.4. *Take* $\gamma, \delta \in \mathbb{C}\langle d \rangle$, *where* $\langle d \rangle$ *is cyclic of order* $n < \infty$. *Then*

(1) $\bar{\gamma} + \bar{\delta} = \overline{\gamma + \delta}$,

(2) $\bar{\gamma}\bar{\delta} = \overline{\gamma\delta}$,

(3) $\Re(\gamma + \delta) = \Re(\gamma) + \Re(\delta)$,

(4) $\Im(\gamma + \delta) = \Im(\gamma) + \Im(\delta)$,

(5) $\gamma + \bar{\gamma} = 2\Re(\gamma)$,

(6) $\gamma - \bar{\gamma} = 2i\Im(\gamma)$, *and*

(7) $\gamma\bar{\gamma} = (\Re(\gamma))^2 + (\Im(\gamma))^2$.

Proof. Given that these properties hold for the coefficients, all of the parts except for (7) are trivial to verify. Let us write $\gamma = \sum_{i=0}^{n-1} \gamma_a d^a$. For any k, we have

$$\begin{aligned}(\gamma_k d^k)\overline{(\gamma_k d^k)} &= \gamma_k \overline{\gamma_k} d^{2k} \\ &= ((\mathrm{Re}(\gamma_k))^2 + (\mathrm{Im}(\gamma_k))^2) d^{2k} \\ &= (\Re(\gamma_k d^k))^2 + (\Im(\gamma_k d^k))^2.\end{aligned}$$

Proceeding by induction, let us assume that

$$(\sum_{a=0}^{j-1} \gamma_a d^a)\overline{(\sum_{a=0}^{j-1} \gamma_a d^a)} = (\Re(\sum_{a=0}^{j-1} \gamma_a d^a))^2 + (\Im(\sum_{a=0}^{j-1} \gamma_a d^a))^2,$$

for some j, with $1 \leq j < n$. Then we have

$$\begin{aligned}(\sum_{a=0}^{j}\gamma_a d^a)\overline{(\sum_{a=0}^{j}\gamma_a d^a)} &= ((\sum_{a=0}^{j-1}\gamma_a d^a)+\gamma_j d^j)(\overline{(\sum_{a=0}^{j-1}\gamma_a d^a)}+\overline{\gamma_j}d^j) \\ &= (\Re(\sum_{a=0}^{j-1}\gamma_a d^a))^2+(\Im(\sum_{a=0}^{j-1}\gamma_a d^a))^2+ \\ &\qquad (\overline{\gamma_j}d^j)(\sum_{a=0}^{j-1}\gamma_a d^a)+\overline{(\overline{\gamma_j}d^j)(\sum_{a=0}^{j-1}\gamma_a d^a)}+\gamma_j\overline{\gamma_j}d^{2j} \\ &= (\Re(\sum_{a=0}^{j-1}\gamma_a d^a))^2+(\Im(\sum_{a=0}^{j-1}\gamma_a d^a))^2+ \\ &\qquad 2\Re((\overline{\gamma_j}d^j)(\sum_{a=0}^{j-1}\gamma_a d^a))+\gamma_j\overline{\gamma_j}d^{2j}.\end{aligned}$$

Now, $\overline{\gamma_j}d^j = (\mathrm{Re}(\gamma_j) - i\mathrm{Im}(\gamma_j))d^j$, which tells us that

$$\Re((\overline{\gamma_j}d^j)(\sum_{a=0}^{j-1}\gamma_a d^a)) = (\mathrm{Re}(\gamma_j)d^j)(\Re(\sum_{a=0}^{j-1}\gamma_a d^a))+(\mathrm{Im}(\gamma_j)d^j)(\Im(\sum_{a=0}^{j-1}\gamma_a d^a)).$$

It follows that $(\sum_{a=0}^{j}\gamma_a d^a)\overline{(\sum_{a=0}^{j}\gamma_a d^a)}$ is equal to

$$\begin{aligned}&(\Re(\sum_{a=0}^{j-1}\gamma_a d^a))^2+(\Im(\sum_{a=0}^{j-1}\gamma_a d^a))^2+(2\mathrm{Re}(\gamma_j)d^j)(\Re(\sum_{a=0}^{j-1}\gamma_a d^a))+ \\ &\qquad (2\mathrm{Im}(\gamma_j)d^j)(\Im(\sum_{a=0}^{j-1}\gamma_a d^a))+\gamma_j\overline{\gamma_j}d^{2j}.\end{aligned}$$

On the other hand,

$$(\Re(\gamma))^2+(\Im(\gamma))^2 = (\Re(\sum_{a=0}^{j-1}\gamma_a d^a)+\mathrm{Re}(\gamma_j)d^j)^2+(\Im(\sum_{a=0}^{j-1}\gamma_a d^a)+\mathrm{Im}(\gamma_j)d^j)^2.$$

Expanding this, and comparing with our computations above, it remains only to verify that $((\mathrm{Re}(\gamma_j))^2+(\mathrm{Im}(\gamma_j))^2)d^{2k} = \gamma_j\overline{\gamma_j}d^{2k}$. But this is obvious. □

Given this result, we would like to find solutions to the equation $x^2+y^2 = -1$.

Proposition 4.5.5. *Let p be an odd prime, such that the order of* 2 mod p *is* $2m$*, for some natural number* m*. Then* $2^m \equiv -1 \pmod{p}$*. Let* $C_p = \langle d \rangle$ *be a cyclic group of order* p*. Let*

$$\gamma = \prod_{a=0}^{m-1} (1 + id^{2^a}) \in \mathbb{Z}[i]C_p.$$

Let $\alpha = d\Re(\gamma)$*, and* $\beta = d\Im(\gamma)$*. Then,* $\alpha, \beta \in \mathbb{Z}C_p$*, and if* $\rho : \mathbb{Q}C_p \to \mathbb{Q}(\xi_p)$ *is the usual epimorphism, given by* $d \mapsto \xi_p$*, then* $\rho(\alpha^2 + \beta^2 + 1) = 0$*.*

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the only square roots of 1 are ± 1. It follows that $2^m \equiv -1 \pmod{p}$. Since $\gamma \in \mathbb{Z}[i]C_p$, it follows immediately that $\alpha, \beta \in \mathbb{Z}C_p$. Then, by Lemma 4.5.4(7), it follows that

$$\alpha^2 + \beta^2 = d^2((\Re(\gamma))^2 + (\Im(\gamma))^2) = d^2(\gamma\bar{\gamma}).$$

By Lemma 4.5.4(2), we have

$$\bar{\gamma} = \overline{\prod_{a=0}^{m-1} (1 + id^{2^a})} = \prod_{a=0}^{m-1} (1 - id^{2^a}).$$

Therefore,

$$\alpha^2 + \beta^2 = d^2(\prod_{a=0}^{m-1} (1 + id^{2^a})(1 - id^{2^a})) = d^2(\prod_{a=0}^{m-1} (1 + d^{2^{a+1}})).$$

Hence,

$$\begin{aligned}(1 - d^2)(\alpha^2 + \beta^2) &= d^2(1 - d^2)(1 + d^2)(1 + d^4) \cdots (1 + d^{2^m}) \\ &= d^2(1 - d^4) \cdots (1 + d^{2^m}) \\ &= \cdots = d^2(1 - d^{2^{m+1}}).\end{aligned}$$

Now, $2^{m+1} = 2(2^m) \equiv -2 \pmod{p}$. Thus,

$$(1 - d^2)(\alpha^2 + \beta^2) = d^2(1 - d^{-2}) = d^2 - 1.$$

Hence, $(1 - d^2)(\alpha^2 + \beta^2 + 1) = d^2 - 1 + 1 - d^2 = 0$. Since $\alpha^2 + \beta^2 + 1 \in \mathbb{Z}\langle d \rangle$, let us write $\alpha^2 + \beta^2 + 1 = \sum_{i=0}^{n-1} z_i d^i$, for various integers z_i. Then, since

$$\alpha^2 + \beta^2 + 1 = d^2(\alpha^2 + \beta^2 + 1),$$

it follows that $\sum_{i=0}^{n-1} z_i d^i = \sum_{i=0}^{n-1} z_i d^{i+2}$, which means that $z_0 = z_2 = \cdots = z_{n-3} = z_{n-1} = z_1 = z_3 = \cdots = z_{n-2}$. That is, $\alpha^2 + \beta^2 + 1 = z\hat{d}$, for some $z \in \mathbb{Z}$. Hence, $\rho(\alpha^2 + \beta^2 + 1) = z\rho(\hat{d}) = z(1 + \xi_p + \cdots + \xi_p^{p-1}) = 0$. □

Since we will be interested in homomorphic images of the form $Q_8 \times C_n$, for odd numbers $n > 1$, let us write

$$Q_8 \times C_n = \langle \bar{g}, \bar{h}, \bar{c} \,|\, \bar{g}^2 = \bar{h}^2, \bar{g}^4 = 1, \bar{c}^n = 1, \bar{h}^{-1}\bar{g}\bar{h} = \bar{g}^{-1}, [\bar{g}, \bar{c}] = [\bar{h}, \bar{c}] = 1 \rangle.$$

Then, recalling that we have already given the Wedderburn decomposition of $\mathbb{Q}(Q_8 \times C_n)$, for an odd number $n > 1$, we have

Proposition 4.5.6. *The primitive central idempotent of* $\mathbb{Q}(Q_8 \times C_n)$ *corresponding to the component* $\mathbb{H}(\mathbb{Q}(\xi_n))$ *is* $((1-\bar{g}^2)/2)\prod(1-\widehat{(\bar{c}^{n/p})}/p)$, *where the product is over all of the distinct primes* p *which divide* n. *If* f *is any other primitive central idempotent of* $\mathbb{Q}(Q_8 \times C_n)$, *then there exists* $1 \neq \gamma \in Q_8 \times C_n$, *satisfying* $\gamma f = f$. *Thus, if* G *is a finite group, and* e *is a primitive central idempotent of* $\mathbb{Q}G$ *such that* $Ge \simeq Q_8 \times C_n$, *then* $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_n))$. *Let* K *be the kernel of the map* $G \to Ge$, *and let* $\tau : G/K \to Q_8 \times C_n$ *be an isomorphism. Then, let* $\lambda : \mathbb{Q}G \to \mathbb{Q}(Q_8 \times C_n)$ *be the map obtained by following the obvious epimorphism* $\mathbb{Q}G \to \mathbb{Q}(G/K)$ *with the isomorphism* $\mathbb{Q}(G/K) \to \mathbb{Q}(Q_8 \times C_n)$ *induced by* τ. *If* μ *is any preimage of* $((1-\bar{g}^2)/2)\prod(1-\widehat{(\bar{c}^{n/p})}/p)$ *under* λ, *then* $e = \frac{\hat{K}}{|K|}\mu$.

Proof. By Proposition 4.2.3, the primitive central idempotent corresponding to $\mathbb{H}(\mathbb{Q}(\xi_n))$ is the product of the primitive central idempotent of $\mathbb{Q}Q_8$ corresponding to $\mathbb{H}(\mathbb{Q})$, and the primitive central idempotent of $\mathbb{Q}C_n$ corresponding to $\mathbb{Q}(\xi_n)$. By Proposition 4.2.5, the first of these is $(1-\bar{g}^2)/2$. To determine the other, we know that it will be the element which projects onto the identity element in $\mathbb{Q}(\xi_n)$, and to the zero element in each of the other Wedderburn components of $\mathbb{Q}C_n$. These projections are given in Lemma 3.2.1. If $d|n$, but $d \neq n$, then let us say that $p|\frac{n}{d}$, for some prime p. Thus, $\xi_d^{n/p} = 1$, which means that, under the map $\bar{c} \mapsto \xi_d$, the element $1 - \widehat{(\bar{c}^{n/p})}/p$ gets mapped to 0. Thus, $\prod(1 - \widehat{(\bar{c}^{n/p})}/p) \mapsto 0$, in all components except for $\mathbb{Q}(\xi_n)$. In this component

$$1 - \frac{\widehat{\bar{c}^{n/p}}}{p} \mapsto 1 - \frac{1 + \xi_n^{n/p} + \xi_n^{2n/p} + \cdots + \xi_n^{(p-1)n/p}}{p}.$$

But $\xi_n^{n/p}$ is a primitive p^{th} root of unity. Thus, $1 + \xi_n^{n/p} + \cdots + \xi_n^{(p-1)n/p} = 0$, which means that $1 - \widehat{(\bar{c}^{n/p})}/p$ gets mapped to 1, for each p. Therefore, their product gets mapped to 1, and this is the primitive central idempotent.

Again, by Proposition 4.2.3, f will be the product of primitive central idempotents f_1 of $\mathbb{Q}Q_8$, and f_2 of $\mathbb{Q}C_n$. Given the restriction on f, we must have $f_1 \neq (1-\bar{g}^2)/2$, or $f_2 \neq \prod(1-\widehat{(\bar{c}^{n/p})}/p)$. In the first case, $f_1 \in \mathbb{Q}Q_8((1+\bar{g}^2)/2)$. Now, $\bar{g}^2(1+\bar{g}^2)/2 = (1+\bar{g}^2)/2$, forcing $\bar{g}^2 f_1 = f_1$, and therefore, $\bar{g}^2 f = f$. In the second case, we know that $\bar{c}^r f_2 = f_2$ if and only if the projection of $\bar{c}^r$ into the corresponding component is the identity element. Since that component is $\mathbb{Q}(\xi_d)$, for some $d|n$, with $d \neq n$, if we let $p|\frac{n}{d}$, for a prime p, then $\bar{c}^{n/p} \mapsto \xi_d^{n/p} = 1$. Thus, $\bar{c}^{n/p} f_2 = f_2$, implying that $\bar{c}^{n/p} f = f$. Therefore, if $Ge \simeq Q_8 \times C_n$, then Proposition 4.2.8 tells us that $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_n))$.

It is clear that we must have $\lambda(e) = ((1-\bar{g}^2)/2)\prod(1-\widehat{(\bar{c}^{n/p})}/p)$. Since $\lambda(\frac{\hat{K}}{|K|}) = 1$, it is obvious that $\mu\frac{\hat{K}}{|K|}$ satisfies this property. Further, by Proposition 4.2.4, $e = \mu\frac{\hat{K}}{|K|}$ is a primitive central idempotent of $\mathbb{Q}G$. Suppose that e' is another primitive central idempotent of $\mathbb{Q}G$, such that $\lambda(e') = \lambda(e)$. Then $e' - e \in \ker\lambda = \Delta_{\mathbb{Q}}(G,K)$. Since e' is a sum of terms of the form $qg(k-1)$, with $q \in \mathbb{Q}$, $g \in G$, and $k \in K$ (by Proposition 2.1.2), it follows that $(e'-e)\frac{\hat{K}}{|K|} = 0$. Now, $e = \mu\frac{\hat{K}}{|K|}$. Since $\frac{\hat{K}}{|K|}$ is a central idempotent (because K is normal in G), we have $e\frac{\hat{K}}{|K|} = e$. Hence, $e = e'\frac{\hat{K}}{|K|}$. Thus, $e \in \mathbb{Q}Ge'$. However, $\mathbb{Q}Ge \cap \mathbb{Q}Ge' = 0$, a contradiction. Thus, e is the only primitive central idempotent of $\mathbb{Q}G$ such that $\lambda(e)$ has the appropriate value. Our proof is complete. □

The time has come to introduce our new units, which were discovered by Giambruno and Sehgal, in [GS]. Let G be a finite group. Suppose that $G/K \simeq Q_8 \times C_n$, for some odd number n, where n has a prime divisor p', such that the order of 2 mod p' is even. Let $\tau_K : G/K \to Q_8 \times C_n$ be this isomorphism, and let $\lambda_K : \mathbb{Q}G \to \mathbb{Q}(Q_8 \times C_n)$ be the epimorphism obtained by applying the obvious map $\mathbb{Q}G \to \mathbb{Q}(G/K)$, and then the isomorphism $\mathbb{Q}(G/K) \to \mathbb{Q}(Q_8 \times C_n)$ induced by τ_K. Let μ_K be a preimage of $((1-\bar{g}^2)/2)\prod(1-\widehat{(\bar{c}^{n/p})}/p)$ under λ_K. (In particular, since the denominator of any coefficient of $((1-\bar{g}^2)/2)\prod(1-\widehat{(\bar{c}^{n/p})}/p)$ divides $2\prod p$ which, in turn, divides $|G/K| = 8n$, we may choose μ_K such that $|G/K|\mu_K$ is in $\mathbb{Z}G$). Let $e_K = \mu_K\frac{\hat{K}}{|K|}$. Let p' be some prime divisor of n such that the order of 2 mod p' is even. Then $\langle\bar{c}^{n/p'}\rangle \simeq C_{p'}$. Let $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}\langle\bar{c}^{n/p'}\rangle$ be the elements which we created in Proposition 4.5.5. Thus, under the map $\bar{c}^{n/p'} \mapsto \xi_{p'}$, we have $\bar{\alpha}^2 + \bar{\beta}^2 + 1 \mapsto 0$. Let $g, h, c \in G$ be preimages of $\bar{g}, \bar{h}$, and $\bar{c}$ respectively, under the projection $G \to G/K \simeq Q_8 \times C_n$. Let $x, y \in \mathbb{Z}G$ be preimages of $\bar{x}$ and $\bar{y}$, respectively, under λ_K.

By Proposition 4.2.4, e_K is a primitive central idempotent of $\mathbb{Q}G$. Further,

$$\lambda_K((\alpha^2 + \beta^2 + 1)e_K) = (\bar{\alpha}^2 + \bar{\beta}^2 + 1)(\prod(1-\widehat{(\bar{c}^{n/p})}/p))((1-\bar{g}^2)/2).$$

Since $\bar{\alpha}^2 + \bar{\beta}^2 + 1 \mapsto 0$, under the map $\bar{c}^{n/p'} \mapsto \xi_{p'}$, which extends to the map $\bar{c} \mapsto \xi_n$, it follows that the projection of $\bar{\alpha}^2 + \bar{\beta}^2 + 1$ into the Wedderburn component $\mathbb{Q}(\xi_n)$, of $\mathbb{Q}C_n$, is zero. Thus,

$$(\bar{\alpha}^2 + \bar{\beta}^2 + 1)\prod(1 - (\widehat{\bar{c}^{n/p}})/p) = 0,$$

which means that

$$(\bar{\alpha}^2 + \bar{\beta}^2 + 1)(\prod(1 - (\widehat{\bar{c}^{n/p}})/p))((1 - \bar{g}^2)/2) = 0.$$

Hence, $(\alpha^2+\beta^2+1)e_K \in \Delta_{\mathbb{Q}}(G, K)$. But then, as we have seen a few times before, $(\alpha^2 + \beta^2 + 1)e_K \frac{\hat{K}}{|K|} = 0$. Since $e_K \frac{\hat{K}}{|K|} = e_K$, it follows that $(\alpha^2 + \beta^2 + 1)e_K = 0$.

Let

$$\eta_K = |G|(\beta g + h + \alpha g h)e_K, \text{ and } \eta'_K = |G|(\beta g - h + \alpha g h)e_K.$$

Each of α, β, g, and h is in $\mathbb{Z}G$. Further, we have $e_K = \mu_K \frac{\hat{K}}{|K|}$. We chose μ_K such that $|G/K|\mu_K \in \mathbb{Z}G$. Thus, $|G|e_K \in \mathbb{Z}G$, which means that $\eta_K, \eta'_K \in \mathbb{Z}G$. We recall that e_K is a primitive central idempotent in $\mathbb{Q}G$. Since $\bar{\alpha}$ and $\bar{\beta}$ are central, it follows that, for any $\sigma \in \mathbb{Q}G$, we have $\alpha\sigma - \sigma\alpha \in \Delta_{\mathbb{Q}}(G, K)$. Hence, $(\alpha\sigma - \sigma\alpha)\frac{\hat{K}}{|K|}$, which means that $\alpha\sigma e_K = \sigma\alpha e_K$. Similarly, since $\bar{g}^2 = \bar{h}^2$, we have $g^2 e_K = h^2 e_K$. Write $g^2 = \nu$. Since $\bar{g}^2$ is central, it follows that νe_K is central in $\mathbb{Q}Ge_K$. Further $\bar{g}^4 = 1$ implies that $\bar{g}^4 e_K = e_K$. In addition, since $\bar{h}\bar{g} = \bar{g}^{-1}\bar{h}$, we obtain $hge_K = g^{-1}he_K = \nu g h e_K$. Therefore,

$$\begin{aligned}
\eta_K^2 &= |G|^2(\beta^2\nu + \beta g h + \alpha\beta\nu h + \beta h g + \nu + \alpha h g h + \alpha\beta g h g + \alpha\nu g + \alpha^2 g h g h)e_K \\
&= |G|^2(\alpha\beta h(1+\nu) + \beta(1+\nu)gh + \alpha g(1+\nu) + (\alpha^2+\beta^2+1)\nu)e_K.
\end{aligned}$$

Now, we already know that $(\alpha^2 + \beta^2 + 1)e_K = 0$. We also have

$$\lambda_K((1+\nu)e_K) = ((1+\bar{g}^2)/2)((1-\bar{g}^2)/2)\prod(1 - (\widehat{\bar{c}^{n/p}})/p) = 0.$$

Thus, $\eta_K^2 = 0$. Similarly,

$$\begin{aligned}
\eta_K'^2 &= |G|^2(\beta^2\nu - \beta g h + \alpha\beta\nu h - \beta h g + \nu - \alpha h g h + \alpha\beta g h g - \alpha\nu g + \alpha^2 g h g h)e_K \\
&= |G|^2(\alpha\beta h(1+\nu) - \beta(1+\nu)gh - \alpha g(1+\nu) + (\alpha^2+\beta^2+1)\nu)e_K = 0.
\end{aligned}$$

Therefore, for any $x \in G$, we have $1 + \eta_K x \eta_K \in \mathcal{U}(\mathbb{Z}G)$, with inverse $1 - \eta_K x \eta_K$. Similarly, $1 + \eta'_K x \eta'_K \in \mathcal{U}(\mathbb{Z}G)$. Our new units are

$$\mathcal{B}_3 = \langle 1 + \eta_K x \eta_K, 1 + \eta'_K x \eta'_K : x \in G, \text{ all } K\rangle,$$

where we take one η_K and one η'_K for each normal subgroup K of G such that $G/K \simeq Q_8 \times C_n$, where n is an odd number having a prime divisor p, such that the order of 2 mod p is even.

These units will be used in the next section.

§4.6 The Solution to the Case Without Exceptional Components

In this section, we combine much of our previous work to find generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$, provided G is a finite nilpotent group and $\mathbb{Q}G$ has no exceptional Wedderburn components. All of the notations which we introduced in §§3.3, 3.5 and 4.5 are in effect. The units that we introduced in the last section are exploited in

Lemma 4.6.1. *Let G be a finite group, and let e_i be a primitive central idempotent of $\mathbb{Q}G$, such that $Ge_i \simeq Q_8 \times C_n$, where n is some odd number having a prime divisor p', such that the order of 2 mod p' is even. If K is the kernel of the map $G \to Ge_i$, with η_K and η'_K as before, then let*

$$B_K = \langle 1 + \eta_K x \eta_K, 1 + \eta'_K x \eta'_K : x \in G \rangle.$$

Then, for each $j \neq i$, $\pi_j(B_K) = 1$. Further, $\mathbb{Q}Ge_i \cong M_2(\mathbb{Q}(\xi_n))$, and we may define π_i such that $\pi_i(B_K)$ contains $E_2(a\mathbb{Z}[\xi_n])$, for some natural number a.

Proof. By the definitions of η_K and η'_K, we can see that $\eta_K, \eta'_K \in \mathbb{Q}Ge_K$. Proposition 4.5.6 tells us that $e_i = e_K$. That is, $\eta_K, \eta'_K \in \mathbb{Q}Ge_i$. For any $j \neq i$, we have $\pi_j(e_i) = \theta_j(e_i e_j) = 0$, which means that $\pi_j(B_K) = 1$.

It follows from Proposition 4.5.6 that $\mathbb{Q}Ge_i \cong \mathbb{H}(\mathbb{Q}(\xi_n))$. If the order of 2 mod n is odd, then let us say that $2^r \equiv 1 \pmod{n}$, with r odd. Then $2^r \equiv 1 \pmod{p'}$, a contradiction. Hence, Proposition 4.5.3 informs us that $\mathbb{Q}Ge_i \cong M_2(\mathbb{Q}(\xi_n))$. Let us construct the projection π_i. As we pointed out in Proposition 4.5.6, the primitive central idempotent of $\mathbb{Q}(Q_8 \times C_n)$, which corresponds to $\mathbb{H}(\mathbb{Q}(\xi_n))$ is $((1-\bar{g}^2)/2)\prod(1-(\widehat{\bar{c}^{n/p}})/p)$. Let us define a map $T : \mathbb{Q}(Q_8 \times C_n) \to M_2(\mathbb{Q}(\xi_n))$, via

$$T(\bar{g}) = \begin{pmatrix} \rho(\bar{\alpha}) & \rho(\bar{\beta}) \\ \rho(\bar{\beta}) & -\rho(\bar{\alpha}) \end{pmatrix}, T(\bar{h}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T(\bar{c}) = \begin{pmatrix} \xi_n & 0 \\ 0 & \xi_n \end{pmatrix},$$

where ρ, $\bar{\alpha}$, and $\bar{\beta}$ are the various things which we defined in Proposition 4.5.5. Since $\rho(\bar{\alpha}^2 + \bar{\beta}^2 + 1) = 0$, it is easy to verify that T is a homomorphism of $\mathbb{Q}$-algebras. Further,

$$T((1-\bar{g}^2)/2) = \frac{1}{2}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} \rho(\bar{\alpha}^2+\bar{\beta}^2) & 0 \\ 0 & \rho(\bar{\alpha}^2+\bar{\beta}^2) \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Also, for any prime divisor p of n, we have

$$T(\widehat{\bar{c}^{n/p}}) = \begin{pmatrix} 1+\xi_n^{n/p}+\cdots+\xi_n^{(p-1)n/p} & 0 \\ 0 & 1+\xi_n^{n/p}+\cdots+\xi_n^{(p-1)n/p} \end{pmatrix} = 0,$$

since $\xi_n^{n/p}$ is a primitive p^{th} root of unity. Thus, $T(\prod(1-(\widehat{\bar{c}^{n/p}})/p)) = 1$, which means that restricting T, we have a $\mathbb{Q}$-algebra homomorphism

$$T : \mathbb{Q}(Q_8 \times C_n)((1-\bar{g}^2)/2)\prod(1-(\widehat{\bar{c}^{n/p}})/p) \to M_2(\mathbb{Q}(\xi_n)).$$

Since $\mathbb{Q}(Q_8 \times C_n)((1-\bar{g}^2)/2)\prod(1-(\widehat{\bar{c}^{n/p}})/p)$ is a simple $\mathbb{Q}$-algebra, this map is injective. Since it is isomorphic to $M_2(\mathbb{Q}(\xi_n))$, by comparing dimensions, this map is an isomorphism. If $\tau_K : G/K \to Q_8 \times C_n$ is an isomorphism, then by Proposition 4.2.4, we have an isomorphism

$$\psi : \mathbb{Q}Ge_K \to \mathbb{Q}(Q_8 \times C_n)((1-\bar{g}^2)/2)\prod(1-(\widehat{\bar{c}^{n/p}})/p),$$

which is defined via

$$ge_K \mapsto \tau(gK)((1-\bar{g}^2)/2)\prod(1-(\widehat{\bar{c}^{n/p}})/p),$$

for all $g \in G$. Thus, we may define $\pi_i : \mathbb{Q}G \to M_2(\mathbb{Q}(\xi_n))$ via $\pi_i(\zeta) = T(\psi(\zeta e_K))$, for all $\zeta \in \mathbb{Q}G$.

Since $\eta_K^2 = 0 = (\eta'_K)^2$, it follows that for any $x_1, x_2 \in G$, and any $b_1, b_2 \in \mathbb{Z}$, we have

$$(1+\eta_K x_1 \eta_K)^{b_1}(1+\eta_K x_2 \eta_K)^{b_2} = 1 + \eta_K(b_1 x_1 + b_2 x_2)\eta_K.$$

(And, similarly for η'_K). Thus,

$$\langle 1+\eta_K \mathbb{Z}G\eta_K, 1+\eta'_K\mathbb{Z}G\eta'_K\rangle \leq B_K.$$

Since $\mathbb{Z}G$ is an order in $\mathbb{Q}G$, it follows that $\pi_i(\mathbb{Z}G)$ is an order in $M_2(\mathbb{Q}(\xi_n))$. As $M_2(\mathbb{Z}[\xi_n])$ is another order,

$$|M_2(\mathbb{Z}[\xi_n]) : M_2(\mathbb{Z}[\xi_n]) \cap \pi_i(\mathbb{Z}G)| < \infty.$$

(See Theorem 3.1.7). Let us say that this order is l. Then, for any $\omega \in \mathbb{Z}[\xi_n]$, we have

$$\begin{pmatrix} 0 & l\omega \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ l\omega & 0 \end{pmatrix} \in \pi_i(\mathbb{Z}G).$$

Now,

$$\begin{aligned}\pi_i(\eta_K) &= |G|\pi_i(\beta g + h + \alpha g h)\\ &= |G|T(\bar\beta\bar g + \bar h + \bar\alpha\bar g\bar h)\\ &= |G|\Bigg(\begin{pmatrix}\rho(\bar\beta) & 0\\ 0 & \rho(\bar\beta)\end{pmatrix}\begin{pmatrix}\rho(\bar\alpha) & \rho(\bar\beta)\\ \rho(\bar\beta) & -\rho(\bar\alpha)\end{pmatrix} + \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} +\\ &\qquad \begin{pmatrix}\rho(\bar\alpha) & 0\\ 0 & \rho(\bar\alpha)\end{pmatrix}\begin{pmatrix}\rho(\bar\alpha) & \rho(\bar\beta)\\ \rho(\bar\beta) & -\rho(\bar\alpha)\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\Bigg)\\ &= |G|\left(\begin{pmatrix}\rho(\bar\alpha\bar\beta) & \rho(\bar\beta^2)\\ \rho(\bar\beta^2) & -\rho(\bar\alpha\bar\beta)\end{pmatrix} + \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + \begin{pmatrix}-\rho(\bar\alpha\bar\beta) & \rho(\bar\alpha^2)\\ \rho(\bar\alpha^2) & \rho(\bar\alpha\bar\beta)\end{pmatrix}\right)\\ &= \begin{pmatrix}0 & 0\\ -2|G| & 0\end{pmatrix},\end{aligned}$$

since $\rho(\bar\alpha^2 + \bar\beta^2 + 1) = 0$. Similarly,

$$\pi_i(\eta'_K) = \begin{pmatrix}0 & -2|G|\\ 0 & 0\end{pmatrix}.$$

Thus,

$$\begin{aligned}&\begin{pmatrix}1 & 0\\ 4|G|^2 l\omega & 1\end{pmatrix}\\ &= I_2 + \begin{pmatrix}0 & 0\\ -2|G| & 0\end{pmatrix}\begin{pmatrix}0 & l\omega\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ -2|G| & 0\end{pmatrix} \in \pi_i(1 + \eta_K\mathbb{Z}G\eta_K) \le B_K,\end{aligned}$$

and

$$\begin{aligned}&\begin{pmatrix}1 & 4|G|^2 l\omega\\ 0 & 1\end{pmatrix}\\ &= I_2 + \begin{pmatrix}0 & -2|G|\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ l\omega & 0\end{pmatrix}\begin{pmatrix}0 & -2|G|\\ 0 & 0\end{pmatrix} \in \pi_i(1 + \eta'_K\mathbb{Z}G\eta'_K) \le B_K.\end{aligned}$$

Taking $a = 4|G|^2 l$, we are done. □

(We could conclude immediately that we get a subgroup of finite index in $SL_2(\mathbb{Z}[\xi_n])$, except that if $n = 3$, then $\mathbb{Q}(\xi_n)$ is an imaginary quadratic extension of the rationals; hence, $M_2(\mathbb{Q}(\xi_n))$ is an exceptional component).

This allows us to prove

Theorem 4.6.2 (Giambruno-Sehgal). *Let G be a finite nilpotent group. Suppose that for every odd prime p which divides $|G|$, the order of* $2 \bmod p$ *is even. Suppose further that $\mathbb{Q}G$ has no Wedderburn components which are 2×2 matrix rings over $\mathbb{Q}$, an imaginary quadratic extension of the rationals, or a noncommutative division algebra. Then*

$$|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \rangle| < \infty.$$

Proof. We wish to apply Theorem 3.3.5. Let e_i be a primitive central idempotent of $\mathbb{Q}G$. If $\mathbb{Q}Ge_i$ is not a division ring, then since exceptional 2×2 matrix rings are forbidden, the units H_{f_i} which we defined in §3.5 will give us a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$, by Theorem 3.5.8. If Ge_i is not fixed point free, then we may assume that $H_{f_i} \leq \mathcal{B}_2$, by Lemma 3.6.3. Thus, we are left with the cases where Ge_i is fixed point free, or $\mathbb{Q}Ge_i$ is a division ring. By Proposition 3.6.2, the latter case is contained in the former. Therefore, let us assume that Ge_i is fixed point free.

Since Ge_i is a homomorphic image of a nilpotent group, it is nilpotent. By Corollary 4.1.6, $Ge_i \simeq Q_{2^m} \times C_n$, for some $m \geq 3$, and some odd number n. If $m \geq 4$, then G has Q_{2^m} as a homomorphic image. By Proposition 4.2.7, $\mathbb{Q}Q_{2^m}$ has $M_2(\mathbb{Q})$ as a Wedderburn component. Thus, by Proposition 4.2.4, $\mathbb{Q}G$ has $M_2(\mathbb{Q})$ as a Wedderburn component, which is forbidden. Therefore, $m = 3$. If $n = 1$, then by Proposition 4.2.8, $\mathbb{Q}Q_8$ has $\mathbb{Q}Ge_i$ as a Wedderburn component. By Proposition 4.2.5, $\mathbb{Q}Ge_i$ is either $\mathbb{Q}$ or $\mathbb{H}(\mathbb{Q})$. The results of §3.4 tell us that no units at all are required to deal with these components. Therefore, we will assume that $n > 1$. Given the restriction on the order of G, for every prime divisor p, of n, the order of $2 \bmod p$ must be even. By Lemma 4.6.1, $\mathbb{Q}Ge_i \cong M_2(\mathbb{Q}(\xi_n))$, and $\mathcal{B}_3$ contains a subgroup B_K such that $\pi_j(B_K) = 1$, if $j \neq i$, and $\pi_i(B_K)$ contains $E_2(a\mathbb{Z}[\xi_n])$, for some natural number a. By Theorem 2.5.5, the ring of algebraic integers of $\mathbb{Q}(\xi_n)$ is $\mathbb{Z}[\xi_n]$. Since exceptional 2×2 components are not permitted, $E_2(a\mathbb{Z}[\xi_n])$ is of finite index in $SL_2(\mathbb{Z}[\xi_n])$. We are done. □

It is now easy to obtain

Theorem 4.6.3. *Let G be a finite nilpotent group. Assume that $\mathbb{Q}G$ has no Wedderburn components of the following types:*

(1) *a division algebra of the form $\mathbb{H}(\mathbb{Q}(\xi_p))$, for some odd prime p, such that the order of* $2 \bmod p$ *is odd; or,*

(2) *a 2×2 matrix ring over $\mathbb{Q}$, an imaginary quadratic extension of the rationals, or a noncommutative division algebra.*

Then $|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \rangle| < \infty$.

Proof. We follow the same proof as in Theorem 4.6.2, up to the point where we assume that $Ge_i \simeq Q_8 \times C_n$, for some odd number $n > 1$. Suppose that, for some prime divisor p, of n, the order of 2 mod p is odd. Since C_n has C_p as a homomorphic image, it follows that G has $Q_8 \times C_p$ as a homomorphic image. Now, we already know that $\mathbb{Q}(Q_8 \times C_p)$ has $\mathbb{H}(\mathbb{Q}(\xi_p))$ as a Wedderburn component. Therefore, by Proposition 4.2.4, so does $\mathbb{Q}G$, which is a contradiction. The remainder of the proof is the same. □

Our desired conclusion is a particular case of this result. Since $\mathbb{Q}(\xi_n)$ is not real, for an odd natural number $n > 1$, it follows that $\mathbb{H}(\mathbb{Q}(\xi_n))$ is not a totally definite quaternion algebra. Therefore, we are only excluding exceptional components in the above result. Hence, we obtain

Corollary 4.6.4. *Let G be a finite nilpotent group, such that $\mathbb{Q}G$ has no exceptional Wedderburn components. Then*

$$|\mathcal{U}(\mathbb{Z}G) : \langle \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \rangle| < \infty.$$

We should, perhaps, perform one concrete example of the construction of $\mathcal{B}_3$, in order to show that it can be done easily, and, for groups of reasonable size, by hand.

Example 4.6.5. Let $G = Q_8 \times C_2 \times C_5$. Since G is the direct product of its Sylow subgroups, it is nilpotent. Further, by Proposition 4.2.5, $\mathbb{Q}Q_8 \cong 4\mathbb{Q} \oplus \mathbb{H}(\mathbb{Q})$. By Lemma 3.2.1, $\mathbb{Q}C_2 \cong 2\mathbb{Q}$. Thus, by Lemma 4.2.1, $\mathbb{Q}(Q_8 \times C_2) \cong \mathbb{Q}Q_8 \otimes_{\mathbb{Q}} \mathbb{Q}C_2 \cong 2\mathbb{H}(\mathbb{Q}) \oplus 8\mathbb{Q}$. Since $\mathbb{H}(\mathbb{Q})$ and $\mathbb{Q}$ are simple algebras, this is the Wedderburn decompostion of $\mathbb{Q}(Q_8 \times C_2)$. By Lemma 3.2.1, the Wedderburn decomposition of $\mathbb{Q}C_5$ is $\mathbb{Q} \oplus \mathbb{Q}(\xi_5)$. Hence, by Proposition 4.2.3, the Wedderburn decomposition of $\mathbb{Q}G$ is

$$2\mathbb{H}(\mathbb{Q}) \oplus 8\mathbb{Q} \oplus 2\mathbb{H}(\mathbb{Q}(\xi_5)) \oplus 8\mathbb{Q}(\xi_5).$$

Since the order of 2 mod 5 is 4, Proposition 4.5.3 tells us that this decomposition is actually

$$2\mathbb{H}(\mathbb{Q}) \oplus 8\mathbb{Q} \oplus 2M_2(\mathbb{Q}(\xi_5)) \oplus 8\mathbb{Q}(\xi_5).$$

Since $[\mathbb{Q}(\xi_5) : \mathbb{Q}] = 4$, all of these components are nonexceptional. Thus, Corollary 4.6.4 applies here.

Let us write

$$Q_8 = \langle g, h \,|\, g^2 = h^2, h^4 = 1, h^{-1}gh = g^{-1} \rangle, C_2 = \langle b \,|\, b^2 = 1 \rangle, C_5 = \langle c \,|\, c^5 = 1 \rangle.$$

To construct $\mathcal{B}_3$, we must find all of the normal subgroups K, of G, such that $G/K \simeq Q_8 \times C_n$, for odd integers $n > 1$. Since $|G| = 80$, the only possible value for n is 5. Thus, $|K| = 2$. Therefore, $K = \langle k \rangle$, for some central element of order 2 in G. The elements of order 2 will be of the form (x, y, z), where x, y, and z are each of order 1 or 2 in Q_8, C_2, and C_5 respectively, and not all of x, y, z are 1. This forces $z = 1$, $y = 1$ or b, and $x = 1$ or g^2. Now, it is easy to see that $G/\langle (g^2, 1, 1)\rangle \simeq (Q_8/\langle g^2\rangle) \times C_2 \times C_5 \simeq C_2 \times C_2 \times C_2 \times C_5$. This is abelian, and therefore, not isomorphic to $Q_8 \times C_5$. It is also easy to see that $G/\langle (1, b, 1)\rangle \simeq Q_8 \times C_5$ under the map $(x, y, z)\langle (1, b, 1)\rangle \mapsto (x, z)$, for all $x \in Q_8$, $y \in C_2$, and $z \in C_5$. Also, $G/\langle (g^2, b, 1)\rangle \simeq Q_8 \times C_5$, under the map given by

$$(x, 1, z)\langle (g^2, b, 1)\rangle \mapsto (x, z), \quad (x, b, z)\langle (g^2, b, 1)\rangle \mapsto (xg^2, z),$$

for all $x \in Q_8$, $z \in C_5$.

Let us construct $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}C_5$. We have

$$\gamma = \prod_{a=0}^{1}(1 + i\bar{c}^{2^a}) = (1 + i\bar{c})(1 + i\bar{c}^2) = 1 + i\bar{c} + i\bar{c}^2 - \bar{c}^3.$$

Therefore, $\bar{\alpha} = \bar{c}\Re(\gamma) = \bar{c} - \bar{c}^4$, and $\bar{\beta} = \bar{c}\Im(\gamma) = \bar{c}^2 + \bar{c}^3$. Let $K_1 = \langle (1, b, 1)\rangle$. Then $(g, 1, 1)$ is a preimage of $\bar{g}$, $(h, 1, 1)$ is a preimage of $\bar{h}$, and $(1, 1, c)$ is a preimage of $\bar{c}$ under the map $(x, y, z) \mapsto (x, z)$. Further, our α will be $(1, 1, c) - (1, 1, c^4)$, and our β will be $(1, 1, c^2) + (1, 1, c^3)$. Since μ_{K_1} is a preimage of $((1 - \bar{g}^2)/2)\prod(1 - (\hat{\bar{c}})/5)$, let us take

$$\mu_{K_1} = (\frac{1}{2}(1, 1, 1) - \frac{1}{2}(g^2, 1, 1))((1, 1, 1) - \frac{1}{5}\widehat{(1, 1, c)}).$$

Then, by definition, $e_{K_1} = \mu_{K_1}(1/2)((1, 1, 1) + (1, b, 1))$. Therefore,

$$\eta_{K_1} = 4(((1, 1, c^2) + (1, 1, c^3))(g, 1, 1) + (h, 1, 1) + ((1, 1, c) - (1, 1, c^4))(gh, 1, 1))\cdot$$
$$((1, 1, 1) - (g^2, 1, 1))(5(1, 1, 1) - \widehat{(1, 1, c)})((1, 1, 1) + (1, b, 1)).$$

Similarly,

$$\eta'_{K_1} = 4(((1, 1, c^2) + (1, 1, c^3))(g, 1, 1) - (h, 1, 1) + ((1, 1, c) - (1, 1, c^4))(gh, 1, 1))\cdot$$
$$((1, 1, 1) - (g^2, 1, 1))(5(1, 1, 1) - \widehat{(1, 1, c)})((1, 1, 1) + (1, b, 1)).$$

Now, let $K_2 = \langle (g^2, b, 1)\rangle$. Under the map defined by $(x, 1, z) \mapsto (x, z)$, $(x, b, z) \mapsto (xg^2, z)$, our preimages of $\bar{g}$, $\bar{h}$, $\bar{c}$, $\bar{\alpha}$, and $\bar{\beta}$ still work. Further, we may take $\mu_{K_2} = \mu_{K_1}$. However, $e_{K_2} = \mu_{K_2}(\widehat{K_2})/2$, and $\widehat{K_2} = (1, 1, 1) + (g^2, b, 1)$. Therefore, we obtain

$$\eta_{K_2} = 4(((1, 1, c^2) + (1, 1, c^3))(g, 1, 1) + (h, 1, 1) + ((1, 1, c) - (1, 1, c^4))(gh, 1, 1))\cdot$$
$$((1, 1, 1) - (g^2, 1, 1))(5(1, 1, 1) - \widehat{(1, 1, c)})((1, 1, 1) + (g^2, b, 1)).$$

Similarly,

$$\eta'_{K_2} = 4(((1, 1, c^2) + (1, 1, c^3))(g, 1, 1) - (h, 1, 1) + ((1, 1, c) - (1, 1, c^4))(gh, 1, 1))\cdot$$
$$((1, 1, 1) - (g^2, 1, 1))(5(1, 1, 1) - \widehat{(1, 1, c)})((1, 1, 1) + (g^2, b, 1)).$$

Using these values, we can easily write down the generators, $1 + \eta_{K_r} x \eta_{K_r}$, and $1 + \eta'_{K_r} x \eta'_{K_r}$, $r = 1$ or 2, $x \in G$, of $\mathcal{B}_3$. Thus, we have explicitly obtained generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

Chapter 5

Units in Matrix Rings over Group Rings

In this chapter, we consider a problem which is slightly more general than the one which we have studied up to this point. Specifically, we want to compute generators of a subgroup of finite index in $GL_n(\mathbb{Z}G)$, for finite groups G, and natural numbers n. In fact, we will solve the problem, provided $n \geq 3$. (We will not even require G to be nilpotent). The advantages of working in higher dimensions are twofold: first, we have more room in which to construct units; second, we will not have to worry about the exceptions to the Congruence Subgroup Theorem.

In the first section, we will give a reduction which is analagous to the reduction which we presented in §3.3. In the second section, we will present some new units, and give our main theorem.

§5.1 A Reduction

The problem to be considered in this chapter is

Problem. *Let G be a finite group. Find a finite set of generators for a subgroup of finite index in $GL_n(\mathbb{Z}G)$, for a natural number n.*

Obviously, the problem with which we have been dealing is simply the $n = 1$ case of the above problem.

The following notation will be used for the remainder of this chapter. Let G be a finite group, and e_i the primitive central idempotents of $\mathbb{Q}G$. Let us say $\theta_i : \mathbb{Q}Ge_i \cong M_{n_i}(D_i)$, where D_i is a division ring with centre F_i, an algebraic number field whose ring of integers we denote O_i. Let $\pi_i : \mathbb{Q}G \rightarrow M_{n_i}(D_i)$ be the projection map. That is, $\pi_i(\eta) = \theta_i(\eta e_i)$, for $\eta \in \mathbb{Q}G$. Let Λ_i be an order in $M_{n_i}(D_i)$ containing $\pi_i(\mathbb{Z}G)$. Let $\mathcal{O}_i$ be an order in D_i containing O_i. Then, of course, $M_{n_i}(\mathcal{O}_i)$ is an order in $M_{n_i}(D_i)$.

Now, let $m \geq 3$. Then $M_m(\Lambda_i)$ is an order in $M_{mn_i}(D_i)$, and so is $M_{mn_i}(\mathcal{O}_i)$. We have

$$\begin{aligned} M_m(\mathbb{Q}G) = M_m(\bigoplus \mathbb{Q}Ge_i) &\cong M_m(\bigoplus M_{n_i}(D_i)) \\ &\cong \bigoplus M_m(M_{n_i}(D_i)) = \bigoplus M_{mn_i}(D_i) \end{aligned}$$

where the first isomorphism is simply the application of θ_i in each component, and in each matrix position, and the second isomorphism is simply the action of performing the operations in separate summands separately. To wit, the net effect of these operations is to map $\alpha = (\alpha_{p,q})_{p,q} \in M_m(\mathbb{Q}G)$ to $((\pi_i(\alpha_{p,q}))_{p,q})_i$. Call this isomorphism $\tau : M_m(\mathbb{Q}G) \to \bigoplus M_m(M_{n_i}(D_i))$. The notations GL, SL, and E have their usual meanings.

Lemma 5.1.1. *Let C be a subgroup of $GL_m(\mathbb{Z}G)$ such that for each i, C contains a subgroup C_i satisfying $\tau(C_i) = 1$ in every component except for the i^{th}, and in the i^{th} component, $\tau(C_i)$ contains $E_{mn_i}(q\mathcal{O}_i)$ for some natural number q. Then the elements of C, together with $\mathcal{B}_1 I_m$, the subgroup of $GL_m(\mathbb{Z}G)$ generated by bI_m, for all Bass cyclic units, b, of $\mathbb{Z}G$, generate a group containing a subgroup of finite index in $Z(GL_m(\mathbb{Z}G))$.*

Proof. Let $z \in Z(\mathcal{U}(\mathbb{Z}G))$. Then, just as in the proof of Lemma 3.3.3, it follows that there exist a natural number l and $b \in \mathcal{B}_1$ (the subgroup of $\mathcal{U}(\mathbb{Z}G)$ generated by the Bass cyclic units) such that for each i, the reduced norm $nr(\pi_i(z^l b^{-1})) = 1$. Thus,

$$nr\begin{pmatrix} \pi_i(z^l b^{-1}) & & \\ & \ddots & \\ & & \pi_i(z^l b^{-1}) \end{pmatrix} = 1^m = 1$$

where this matrix is an $m \times m$ grid of $n_i \times n_i$ matrices. That is,

$$\begin{pmatrix} \pi_i(z^l b^{-1}) & & \\ & & \\ & & \pi_i(z^l b^{-1}) \end{pmatrix} \in SL_{mn_i}(D_i).$$

Further, $\pi_i(z^l b^{-1}) \in \pi_i(\mathbb{Z}G) \subseteq \Lambda_i$, and similarly, $(\pi_i(z^l b^{-1}))^{-1} = \pi_i(bz^{-l}) \in \Lambda_i$. Therefore, $\pi_i(z^l b^{-1}) \in \mathcal{U}(\Lambda_i)$. Since $M_{n_i}(\mathcal{O}_i)$ and Λ_i are both orders in $M_{n_i}(D_i)$,

$$|\mathcal{U}(\Lambda_i) : \mathcal{U}(\Lambda_i \cap M_{n_i}(\mathcal{O}_i))| = r_i < \infty.$$

Let $r = \prod r_i$. Then $\pi_i(z^l b^{-1})^r \in GL_{n_i}(\mathcal{O}_i)$, which implies that

$$\begin{pmatrix} \pi_i(z^{lr} b^{-r}) & & \\ & \ddots & \\ & & \pi_i(z^{lr} b^{-r}) \end{pmatrix} \in SL_{mn_i}(D_i) \cap GL_{mn_i}(\mathcal{O}_i) = SL_{mn_i}(\mathcal{O}_i).$$

Now, $mn_i \geq 3$, and therefore, by Theorem 3.5.4,

$$|SL_{mn_i}(\mathcal{O}_i) : E_{mn_i}(q\mathcal{O}_i)| = k_i < \infty.$$

Let $k = \prod k_i$. We now conclude that

$$\begin{pmatrix} \pi_i(z^{klr}b^{-kr}) & & \\ & \ddots & \\ & & \pi_i(z^{klr}b^{-kr}) \end{pmatrix} \in E_{mn_i}(q\mathcal{O}_i).$$

Therefore, by assumption,

$$\left(1,\dots,1, \begin{pmatrix} \pi_i(z^{klr}b^{-kr}) & & \\ & \ddots & \\ & & \pi_i(z^{klr}b^{-kr}) \end{pmatrix}, 1,\dots,1\right) \in \tau(C)$$

for each i. Multiplying these together for the various components, we find that

$$\left(\begin{pmatrix} \pi_1(z^{klr}b^{-kr}) & & \\ & \ddots & \\ & & \pi_1(z^{klr}b^{-kr}) \end{pmatrix}, \begin{pmatrix} \pi_2(z^{klr}b^{-kr}) & & \\ & \ddots & \\ & & \pi_2(z^{klr}b^{-kr}) \end{pmatrix}, \dots\right)$$

is an element of $\tau(C)$. That is,

$$\tau\begin{pmatrix} z^{klr}b^{-kr} & & \\ & \ddots & \\ & & z^{klr}b^{-kr} \end{pmatrix} \in \tau(C),$$

and since τ is an isomorphism,

$$\begin{pmatrix} z^{klr}b^{-kr} & & \\ & \ddots & \\ & & z^{klr}b^{-kr} \end{pmatrix} \in C.$$

Hence,

$$\begin{pmatrix} z^{klr} & & \\ & \ddots & \\ & & z^{klr} \end{pmatrix} \in \langle C, \mathcal{B}_1 I_m \rangle$$

(where we have simply multiplied by b^{kr} times the identity matrix, which is in $\mathcal{B}_1 I_m$).

Thus, for each $z \in Z(\mathcal{U}(\mathbb{Z}G))$, and hence for each

$$\begin{pmatrix} z & & \\ & \ddots & \\ & & z \end{pmatrix} \in Z(GL_m(\mathbb{Z}G)),$$

there exists a natural number v such that

$$\begin{pmatrix} z & & \\ & \ddots & \\ & & z \end{pmatrix}^v \in \langle \mathcal{B}_1 I_m, C\rangle.$$

That is, $Z(GL_m(\mathbb{Z}G))/(Z(GL_m(\mathbb{Z}G)) \cap \langle \mathcal{B}_1 I_m, C\rangle)$ is torsion. However, we know that $Z(GL_m(\mathbb{Z}G))$ is a finitely generated abelian group. (It consists simply of the matrices u times the identity matrix, for $u \in Z(\mathcal{U}(\mathbb{Z}G))$, and by Lemma 3.3.1, $Z(\mathcal{U}(\mathbb{Z}G))$ is finitely generated). Thus, any quotient of $Z(GL_m(\mathbb{Z}G))$ is finitely generated, so we conclude that

$$|Z(GL_m(\mathbb{Z}G)) : (Z(GL_m(\mathbb{Z}G)) \cap \langle \mathcal{B}_1 I_m, C\rangle)| < \infty$$

which was our desired conclusion. □

Proposition 5.1.2. *Let C satisfy the same condition as in the lemma. Then, in fact, $\langle \mathcal{B}_1 I_m, C\rangle$ is a subgroup of finite index in $GL_m(\mathbb{Z}G)$.*

Proof. We know that $M_m(\mathbb{Z}G)$ is an order in $M_m(\mathbb{Q}G)$; hence, $\tau(M_m(\mathbb{Z}G))$ is an order in $\tau(M_m(\mathbb{Q}G)) = \bigoplus M_m(M_{n_i}(D_i))$. Further, $\bigoplus M_m(\Lambda_i)$ is an order in $\bigoplus M_m(M_{n_i}(D_i))$ containing $\bigoplus M_m(\pi_i(\mathbb{Z}G))$, which contains $\tau(M_m(\mathbb{Z}G))$, by definition of τ. Thus,

$$|\prod GL_m(\Lambda_i) : \mathcal{U}(\tau(M_m(\mathbb{Z}G)))| = |\prod GL_m(\Lambda_i) : \tau(GL_m(\mathbb{Z}G))| < \infty.$$

Hence,

$$|\prod GL_m(\Lambda_i) \cap Z(\prod GL_{mn_i}(D_i)) : \tau(GL_m(\mathbb{Z}G)) \cap Z(\prod GL_{mn_i}(D_i))| < \infty.$$

Now, $\tau(GL_m(\mathbb{Z}G)) \cap Z(\bigoplus GL_{mn_i}(D_i)) \subseteq Z(\tau(GL_m(\mathbb{Z}G))) = \tau(Z(GL_m(\mathbb{Z}G)))$, implying that $\tau(Z(GL_m(\mathbb{Z}G)))$ contains a subgroup of finite index in

$$\bigoplus GL_m(\Lambda_i) \cap Z(\bigoplus GL_{mn_i}(D_i)).$$

By Lemma 5.1.1, $\langle \mathcal{B}_1 I_m, C\rangle$ contains a subgroup of finite index in $Z(GL_m(\mathbb{Z}G))$. Hence, $\tau(\langle \mathcal{B}_1 I_m, C\rangle)$ contains a subgroup of finite index in $\tau(Z(GL_m(\mathbb{Z}G)))$, and therefore, in $\prod GL_m(\Lambda_i) \cap Z(\prod GL_{mn_i}(D_i))$ which may also be written $\prod(GL_m(\Lambda_i) \cap Z(GL_{mn_i}(D_i)))$.

Since the index of the unit group of one order in another is finite, we see that $|GL_{mn_i}(\mathcal{O}_i) : \mathcal{U}(M_m(\Lambda_i) \cap M_{mn_i}(\mathcal{O}_i))| < \infty$. Therefore,

$$|GL_{mn_i}(\mathcal{O}_i) \cap Z(GL_{mn_i}(D_i)) : \mathcal{U}(M_m(\Lambda_i) \cap M_{mn_i}(\mathcal{O}_i)) \cap Z(GL_{mn_i}(D_i))| < \infty.$$

We conclude that $\tau(\langle \mathcal{B}_1 I_m, C\rangle)$ contains a subgroup of finite index in

$$\prod (GL_{mn_i}(\mathcal{O}_i) \cap Z(GL_{mn_i}(D_i))).$$

Hence, $\tau(\langle \mathcal{B}_1 I_m, C\rangle)$ contains a subgroup $\prod K_i$, with K_i a subgroup of finite index in $GL_{mn_i}(\mathcal{O}_i) \cap Z(GL_{mn_i}(D_i))$. By our choice of C, $\tau(C)$ contains

$$(1, \dots, 1, E_{mn_i}(q\mathcal{O}_i), 1, \dots, 1).$$

Since $mn_i \geq 3$, it follows from Theorem 3.5.4 that this group is of finite index in $(1, \dots, 1, SL_{mn_i}(\mathcal{O}_i), 1, \dots, 1)$. Since $O_i \subseteq \mathcal{O}_i$, Lemma 3.3.2 informs us that $\tau(\langle \mathcal{B}_1 I_m, C\rangle)$ contains a subgroup of finite index in

$$(1, \dots, 1, GL_{mn_i}(\mathcal{O}_i), 1, \dots, 1).$$

Taking the product over the various components, we get a subgroup of finite index in $\prod GL_{mn_i}(\mathcal{O}_i)$.

Once again, because the unit groups of orders have finite index in each other,

$$|\prod GL_m(\Lambda_i) : \prod \mathcal{U}(M_m(\Lambda_i) \cap M_{mn_i}(\mathcal{O}_i))| < \infty.$$

Thus, we know that $\tau(\langle \mathcal{B}_1 I_m, C\rangle)$ contains a subgroup which is of finite index in $\prod GL_m(\Lambda_i)$. We also know that $\langle \mathcal{B}_1 I_m, C\rangle$ is contained in $GL_m(\mathbb{Z}G)$, which means that $\tau(\langle \mathcal{B}_1 I_m, C\rangle) \subseteq \tau(GL_m(\mathbb{Z}G))$, which is contained in $\prod GL_m(\Lambda_i)$. Since the units $\tau(\langle \mathcal{B}_1 I_m, C\rangle)$ form a subgroup of finite index in the unit group of the larger order, they certainly form a subgroup of finite index in the smaller one, so that $|\tau(GL_m(\mathbb{Z}G)) : \tau(\langle \mathcal{B}_1 I_m, C\rangle)| < \infty$. Since τ is an isomorphism, $|GL_m(\mathbb{Z}G) : \langle \mathcal{B}_1 I_m, C\rangle| < \infty$. □

§5.2 The Main Result

To present our main result, we shall require several different sorts of matrix units. (That is, the matrices with a 1 in one position and zeroes elsewhere, and not the more general objects which we defined in §3.5). We should give them different notations. First, the (p, q) matrix unit in $M_m(\mathbb{Z}G)$, we shall denote $E_{p,q}$. Next, the (p, q) matrix unit in $M_{n_i}(D_i)$ shall be denoted $E^*_{p,q}$. Now, if we regard $M_{mn_i}(D_i)$ as an $m \times m$ grid of $n_i \times n_i$ blocks, we denote by $E'_{p,q}$ the matrix which is the $n_i \times n_i$ identity matrix in the (p, q) block, and zero elsewhere. (This is not, strictly speaking, a matrix unit, but it serves a purpose). Finally, in $M_{mn_i}(D_i)$ (ignoring the above block structure), we write the (p, q) matrix unit as $E''_{p,q}$. We now present the main result.

Theorem 5.2.1. *Let G be a finite group, and $m \geq 3$. Let C be the subgroup of $GL_m(\mathbb{Z}G)$ generated by the elementary matrices $1 + gE_{p,q}$ for $g \in G$, $p \neq q$. Then $\langle \mathcal{B}_1 I_m, C\rangle$ is a subgroup of finite index in $GL_m(\mathbb{Z}G)$.*

Proof. Fix $p \neq q$. We observe that, for $g, h \in G$, $u, v \in \mathbb{Z}$, we have

$$(1 + gE_{p,q})^u(1 + hE_{p,q})^v = 1 + (ug + vh)E_{p,q},$$

and therefore, $\langle \mathcal{B}_1 I_m, C\rangle$ contains $1 + \alpha E_{p,q}$ for all $\alpha \in \mathbb{Z}G$. For any i, choose a natural number k_i such that $k_i e_i \in \mathbb{Z}G$. Certainly, then, $\langle \mathcal{B}_1 I_m, C\rangle$ contains $1 + k_i\alpha e_i E_{p,q}$ for all $\alpha \in \mathbb{Z}G$. Now, the j^{th} component of $\tau(1 + k_i\alpha e_i E_{p,q})$ is, by definition, $1 + \pi_j(k_i\alpha e_i)E'_{p,q}$ which is $1 + \theta_j(k_i\alpha e_i e_j)E'_{p,q}$. If $i \neq j$, then $e_i e_j = 0$, so this is 1. If $i = j$, then this is

$$1 + \theta_i(k_i\alpha e_i)E'_{p,q} = 1 + \pi_i(k_i\alpha)E'_{p,q} = 1 + k_i\pi_i(\alpha)E'_{p,q}.$$

Let $C_{i,p,q}$ be the subgroup of C consisting of the elements $1 + k_i\alpha e_i E_{p,q}$, for $\alpha \in \mathbb{Z}G$. Then we have just observed that

$$\tau(C_{i,p,q}) = (1, \dots, 1, 1 + k_i\pi_i(\mathbb{Z}G)E'_{p,q}, 1, \dots, 1).$$

Now, $\pi_i(\mathbb{Z}G)$ is an order in $M_{n_i}(D_i)$ and so is $M_{n_i}(\mathcal{O}_i)$, implying that

$$|M_{n_i}(\mathcal{O}_i) : M_{n_i}(\mathcal{O}_i) \cap \pi_i(\mathbb{Z}G)| = t_i < \infty.$$

Thus, if $A \in M_{n_i}(\mathcal{O}_i)$, we have $t_i A \in \pi_i(\mathbb{Z}G)$. Hence, $k_i t_i A \in k_i\pi_i(\mathbb{Z}G)$. In particular, $(1, \dots, 1, 1 + k_i t_i A E'_{p,q}, 1, \dots, 1) \in \tau(C_{i,p,q})$. Thus, if we take $\omega \in \mathcal{O}_i$, and any r, s with $1 \leq r, s \leq n_i$, then letting $A = \omega E^*_{r,s}$, we have

$$(1, \dots, 1, 1 + k_i t_i \omega E^*_{r,s} E'_{p,q}, 1, \dots, 1) \in \tau(C_{i,p,q}).$$

At this point, we pause to discuss the meaning of this last statement. By "$E^*_{r,s}E'_{p,q}$", we mean "put the $n_i \times n_i$ matrix with a 1 in the (r, s) position and zeroes elsewhere, in the (p, q) block in the $m \times m$ grid, and zeroes in all other such blocks." In other words, this is actually a matrix unit in $M_{mn_i}(D_i)$. There are no restrictions on r or s, so we may move this 1 freely about any such block. We may also vary p and q, subject to the restriction that $p \neq q$. In other words, the $E^*_{r,s}E'_{p,q}$ can give us any matrix unit in $M_{mn_i}(D_i)$, except those which correspond to a (p, p) block.

Thus, letting C_i be the subgroup of C generated by all $C_{i,p,q}$ for $p \neq q$, we have that $\tau(C_i)$ contains $(1, \dots, 1, 1 + k_i t_i \omega E''_{r,s}, 1, \dots, 1)$ for all $\omega \in \mathcal{O}_i$, and all pairs (r, s), $1 \leq r, s \leq mn_i$ which do not correspond to a (p, p) block.

We claim, however, that the pairs (r, s) with $r \neq s$, corresponding to a (p, p) block, come to us *gratis*. Indeed, suppose that the pair (r, s) corresponds to a (p, p) block. That is, there exists an integer w, $1 \leq w \leq m$, such that

$$(w - 1)n_i + 1 \leq r, s \leq wn_i.$$

Since $m \geq 3$, it is easy to choose an integer y, $1 \leq y \leq mn_i$, such that y does not fall between $(w-1)n_i + 1$ and wn_i. (There are at least $2n_i$ values outside this range). Then for any $\omega \in \mathcal{O}_i$, we see that $(1, \dots, 1, 1 + k_i t_i \omega E''_{r,y}, 1, \dots, 1)$ and $(1, \dots, 1, k_i t_i E''_{y,s}, 1, \dots, 1)$ are in $\tau(C_i)$. Therefore, so is their commutator, namely

$$\begin{aligned}&(1, \dots, 1, [1 + k_i t_i \omega E''_{r,y}, 1 + k_i t_i E''_{y,s}], 1, \dots, 1)\\ =&(1, \dots, 1, 1 + k_i^2 t_i^2 \omega E''_{r,s}, 1, \dots, 1),\end{aligned}$$

by Lemma 3.5.1.

Thus, for all pairs $r \neq s$, we have

$$(1, \dots, 1, 1 + k_i^2 t_i^2 \omega E''_{r,s}, 1, \dots, 1) \in \tau(C_i)$$

for all $\omega \in \mathcal{O}_i$. Taking $q = \prod_i k_i^2 t_i^2$, we find that $\tau(C_i)$ contains

$$(1, \dots, 1, E_{mn_i}(q\mathcal{O}_i), 1, \dots, 1).$$

Apply Proposition 5.1.2 to complete the argument. □

The important thing in this result is that the number of generators is finite. However, it is always desirable to eliminate any extraneous generators. In an effort to do so, it should be noted that $\{1 + gE_{p,q} : g \in G, p \neq q\}$ is by no means a minimal set of generators for the group which it generates. Indeed, suppose we start with the elements $1 + E_{1,q}$ and $1 + E_{p,1}$, for $p \neq 1 \neq q$. Then we have, for 1, p, and q pairwise distinct, $[1 + E_{p,1}, 1 + E_{1,q}] = 1 + E_{p,q}$. Thus, we have $1 + E_{p,q}$ for all $p \neq q$. Suppose we also allow $1 + gE_{1,2}$ for $g \in G$. Then if 1, 2, and q are pairwise distinct, we have $[1 + gE_{1,2}, 1 + E_{2,q}] = 1 + gE_{1,q}$, so that we have these matrices for all $q \neq 1$. Then, if 1, p, and q are pairwise distinct, we get $[1 + E_{p,1}, 1 + gE_{1,q}] = 1 + gE_{p,q}$. Therefore we have all such matrices subject to the condition $p \neq q \neq 1$. So, given $p \neq 1$, choose q distinct from both 1 and p (which can be done since $m \geq 3$). Then we have $[1 + gE_{p,q}, 1 + E_{q,1}] = 1 + gE_{p,1}$. In other words, we now have all of our generators of C. A slightly sharper version of our theorem is, then,

Corollary 5.2.2. *Let C' be the subgroup of $GL_m(\mathbb{Z}G)$ generated by $1 + gE_{1,2}$, $g \in G$, and by $1 + E_{1,p}$, $p > 2$, and by $1 + E_{q,1}$, $q > 1$. Then $\langle \mathcal{B}_1 I_m, C' \rangle$ is a subgroup of finite index in $GL_m(\mathbb{Z}G)$.*

We may also observe that the only place the Bass cyclic units were needed was to get a subgroup of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$. Given that, our next result is obvious.

Corollary 5.2.3. *If $Z(\mathcal{U}(\mathbb{Z}G))$ is finite, then we may omit the units $\mathcal{B}_1 I_m$ in both Theorem 5.2.1 and Corollary 5.2.2.*

In fact, just as in §3.3, we may deduce

Corollary 5.2.4. *If each F_i is either $\mathbb{Q}$, or an imaginary quadratic extension of the rationals, then we may omit the units $\mathcal{B}_1 I_m$ in both Theorem 5.2.1 and Corollary 5.2.2.*

It seems appropriate that we should comment upon the $m = 2$ case, if only to explain why our proof breaks down. In fact, the proof of Theorem 5.2.1 works perfectly well, but the sufficiency of the units $(1, \dots, 1, E_{2n_i}(q\mathcal{O}_i), 1, \dots, 1)$ cannot be guaranteed. In effect, our technique changes the Wedderburn components of the form $M_{n_i}(D_i)$ into $M_{mn_i}(D_i)$. Thus, when $m = 2$, we find that exceptional 2×2 matrix rings become 4×4 matrix rings. However, certain perfectly harmless division rings become exceptional 2×2 components. The reason why we were able to get things done in $\mathcal{U}(\mathbb{Z}G)$, is that for many groups G, $\mathbb{Q}G$ does not have any exceptional components. However, let us take $K = G$ in Proposition 4.2.4. Then, since the Wedderburn component of $\mathbb{Q}1 = \mathbb{Q}$, is $\mathbb{Q}$, we discover that $\mathbb{Q}G$ has $\mathbb{Q}$ as a Wedderburn component, for any finite group G. Therefore, some $M_{mn_i}(D_i)$ will be $M_2(\mathbb{Q})$, and the Congruence Subgroup Theorem fails here. Thus, if any progress is to be made on the $m = 2$ case, some new technique will have to be found.

Chapter 6

Conclusion

Let us bring this thesis to a close by briefly mentioning some related work which has been done in this area, and the work which is still to be done.

We will restrict our attention to finite nilpotent groups, for the moment. Evidently, if G is such a group, then the problem which remains is to deal with Wedderburn components $M_{n_i}(D_i)$ which are exceptional, and those components for which $Ge_i \simeq Q_{2^m} \times C_n$, where $m \geq 4$, and n is an odd number. (The remaining fixed point free nilpotent groups are of the form $Q_8 \times C_n$, and we have dealt with all of these except when $n > 1$, and the order of 2 mod n is odd, but in this case, the Wedderburn component is already exceptional). Two things need to be done in these cases. First, generators of a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$ must be found. Second, we must discover enough information about the projection map $\pi_i : \mathbb{Q}G \to M_{n_i}(D_i)$, that we might find elements of $\mathcal{U}(\mathbb{Z}G)$ which map onto these generators.

In some cases, the first of these tasks is the cause of many difficulties. In particular, this is true when the Wedderburn component is a noncommutative division algebra (other than a totally definite quaternion algebra). For example, we know from §4.5, that if the order of 2 mod m is odd, (for an odd integer $m \geq 3$), then

$$\mathbb{H}(\mathbb{Q}(\xi_m)) = \mathbb{Q}(\xi_m) \dotplus \mathbb{Q}(\xi_m)x \dotplus \mathbb{Q}(\xi_m)y \dotplus \mathbb{Q}(\xi_m)xy$$

is a division ring. Its centre is $\mathbb{Q}(\xi_m)$, whose ring of integers is $\mathbb{Z}[\xi_m]$ (by Theorem 2.5.5). Thus, an obvious order in $\mathbb{H}(\mathbb{Q}(\xi_m))$, containing $\mathbb{Z}[\xi_m]$, is $\mathbb{Z}[\xi_m] \dotplus \mathbb{Z}[\xi_m]x \dotplus \mathbb{Z}[\xi_m]y \dotplus \mathbb{Z}[\xi_m]xy$. In this case, we can actually compute reduced norms explicitly. (As we pointed out in §3.4,

$$nr(\alpha + \beta x + \gamma y + \delta xy) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2,$$

for all $\alpha, \beta, \gamma, \delta \in \mathbb{Q}(\xi_m)$). Even so, no finite set of generators of a subgroup of finite index in $SL_1(\mathbb{Z}[\xi_m] \dotplus \mathbb{Z}[\xi_m]x \dotplus \mathbb{Z}[\xi_m]y \dotplus \mathbb{Z}[\xi_m]xy)$ is known.

In other cases, generators of a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$ are known, but inconvenient. A good example would be the exceptional component $M_2(\mathbb{Q})$. Here, it is well-known (see [Se2, Lemma 19.4]) that $SL_2(\mathbb{Z}) = E_2(\mathbb{Z})$. Thus,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

are generators of a subgroup of finite index in $SL_2(\mathbb{Z})$. The problem is that, in general, we cannot hope to have elements of $\mathcal{U}(\mathbb{Z}G)$ mapping onto these particular generators. The best we could expect is that for some natural number n, we could find elements $\alpha, \beta \in \mathcal{U}(\mathbb{Z}G)$, such that

$$\pi_i(\alpha) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \quad \pi_i(\beta) = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}.$$

Since $M_2(\mathbb{Q})$ is an exception to the Congruence Subgroup Theorem, this is not sufficient. However, it is also known that the normal closure of $E_2(q\mathbb{Z})$ in $SL_2(\mathbb{Z})$ is of finite index in $SL_2(\mathbb{Z})$, for $1 \leq q \leq 5$ (see [Se2, Theorem 22.2]). Again, in general, this will not be sufficient, but for particular groups, this has been a great deal of help. We showed, in Lemma 4.2.6, that $\mathbb{Q}D_8$ has $M_2(\mathbb{Q})$ among its Wedderburn components. Each D_{2^k}, $k \geq 3$, is easily seen to have D_8 as a homomorphic image. Thus, by Proposition 4.2.4, each $\mathbb{Q}D_{2^k}$ has $M_2(\mathbb{Q})$ as a Wedderburn component. Nevertheless, Ritter and Sehgal have managed to prove that the Bass cyclic and one-sided bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}D_{2n})$, for all $n \geq 3$ (including the dihedral groups which are not nilpotent). The proof relies upon the fact that the projection maps π_i are known in this case. When $n = 2^k$, the proof involves finding elements of $\mathcal{U}(\mathbb{Z}D_{2^k})$ which map onto the normal closure of $E_2(4\mathbb{Z})$ in $SL_2(\mathbb{Z})$. We refer the reader to [Se2, Theorem 23.1].

A reduction of the problem was made in a recent paper by Jespers and Leal ([JL3]). In this paper, all of the possible exceptional components $M_{n_i}(D_i)$ which can occur in $\mathbb{Q}G$, for a finite nilpotent group G, are listed, and the structures of the various Ge_i, where $\mathbb{Q}Ge_i$ is such an exceptional component, are almost completely classified. In fact, we discover that the only exceptional division rings, which occur in this way, are those which we have already mentioned; namely, $\mathbb{H}(\mathbb{Q}(\xi_n))$, where n is an odd number, and the order of 2 mod n is odd. Of course, we have already seen that $M_2(\mathbb{Q})$ is a Wedderburn component of $\mathbb{Q}Q_{2^m}$, for $m \geq 4$. The only 2×2 matrix rings over imaginary quadratic extensions of the rationals which can occur are $M_2(\mathbb{Q}(\sqrt{-1}))$, $M_2(\mathbb{Q}(\sqrt{-2}))$, and $M_2(\mathbb{Q}(\xi_3))$. Finally, the only 2×2 matrix rings over noncommutative division algebras which can be obtained are $M_2(\mathbb{H}(\mathbb{Q}(\xi_{2^n} + \xi_{2^n}^{-1})))$, $n \geq 2$, and $M_2(\mathbb{H}(\mathbb{Q}(\xi_m)))$, where m is odd, and the order of 2 mod m is odd. Further, the groups which can occur in the form Ge_i, in an exceptional component $\mathbb{Q}Ge_i$, are generally well-known. The only classification which remains to be done is the following. Let L be a 2-group having a subgroup, H, of index 2, where $L = H \cup Hl$. Suppose that H has a nontrivial normal subgroup, N, such that $N \cap lNl^{-1} = 1$, and $H/N \simeq Q_{2^m}$, for some $m \geq 3$. All such groups L must be classified.

Given this information, an algorithm is presented which allows one to lift units. That is, if $\mathbb{Q}Ge_i \cong M_{n_i}(D_i)$, then by Proposition 4.2.8, $\mathbb{Q}(Ge_i)$ has $M_{n_i}(D_i)$ as a Wedderburn component. If we can compute generators of a subgroup of finite index in $\mathcal{U}_1(\mathbb{Z}(Ge_i)) = \mathcal{U}(\mathbb{Z}(Ge_i)) \cap (1 + \Delta_\mathbb{Z}(Ge_i))$, then these units can be lifted to a set of units X in $\mathcal{U}(\mathbb{Z}G)$, and we will have $\pi_j(X) = 1$, if $j \neq i$, and $\pi_i(X)$ will contain a subgroup of finite index in $SL_{n_i}(\mathcal{O}_i)$. For some of the groups of the form Ge_i, such generators are known. However, there are other groups (including those of the form $Q_8 \times C_n$, where $n > 1$ is odd and the order of 2 mod n is odd), where this is not the case. Additionally, when Ge_i is fixed point free, one can use the same algorithm to lift the units up to $\mathcal{U}(\mathbb{Z}G)$.

Two problems remain. First, there are, unfortunately, infinitely many groups among the Ge_i which fall inside an exceptional component $\mathbb{Q}Ge_i$, for which the generators of large subgroups of $\mathcal{U}(\mathbb{Z}(Ge_i))$ are yet to be found. Second, we will have to define carefully what we mean by "explicitly" constructing the units. This algorithm will certainly give the units explicitly, but its running time is a problem. The smallest groups for which it would be useful would be those of order 32, and even here, the algorithm would take trillions of years to run on a fast computer. Clearly, a clever implementation of this algorithm would be a worthy goal.

Considering the fact that the bicyclic units have such a nice form, another question arises. We know that these units, together with the Bass cyclic units, generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ for many, but not all, nilpotent groups G. It would be nice to obtain a classification of all of the groups for which this holds. Also, it is not currently known whether or not the one-sided bicyclic units can always be substituted for the bicyclic units in our results. We mentioned in §4.3 that they suffice to give us a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$, when G is nilpotent of odd order, but for some other groups the problem remains open.

Another problem to consider is this: what happens if we drop the nilpotency assumption? The results of Chapter 3 do not depend upon the group G being nilpotent. However, the general structure of fixed point free groups is not as nice as in the nilpotent case. Even if we require the group G to be solvable, the structure of these groups can still be complicated. (See [Wo, Theorem 6.1.11]). Also, the possibilities for exceptional components expand quite a bit. A few classes of groups which are not nilpotent have been dealt with, as well as a number of isolated groups. For example, we have already mentioned the dihedral groups, and the problem has also been solved for the symmetric groups. (See [Se2, Theorem 27.8]).

Finally, the author would personally be interested in seeing a solution to the 2-dimensional version of the problem which we considered in Chapter 5.

Bibliography

[Am] Amitsur, S.A., *Finite Subgroups of Division Rings*, Trans. Amer. Math. Soc. **80** (1955), 361–386.

[Ba1] Bass, H., *K-Theory and Stable Algebra*, Publ. Math. Inst. Hautes Études Sci. **22** (1964), 5–60.

[Ba2] Bass, H., *The Dirichlet Unit Theorem, Induced Characters, and Whitehead Groups of Finite Groups*, Topology **4** (1966), 391–410.

[Ba3] Bass, H., *Algebraic K-Theory*, Benjamin, New York, 1968.

[BMS] Bass, H., Milnor, J., Serre, J.-P., *Solution of the Congruence Subgroup Problem for $SL_n (n \geq 3)$ and $Sp_{2n} (n \geq 2)$*, Publ. Math. Inst. Hautes Études Sci. **33** (1967), 59–137.

[CR1] Curtis, C.W., Reiner, I., *Representation Theory of Finite Groups and Associative Algeras*, Wiley-Interscience, New York, 1962.

[CR2] Curtis, C.W., Reiner, I., *Methods of Representation Theory, Vol. I*, Wiley-Interscience, New York, 1981.

[CR3] Curtis, C.W., Reiner, I., *Methods of Representation Theory, Vol. II*, Wiley-Interscience, New York, 1987.

[GS] Giambruno, A., Sehgal, S.K., *Generators of Large Subgroups of Units of Integral Group Rings of Nilpotent Groups*, J. Algebra **174** (1995), 150-156.

[Hi] Higman, G., *The Units of Group-Rings*, Proc. London Math. Soc. **46** (1940), 231–248.

[Hun] Hungerford, T.W., *Algebra*, Springer-Verlag, New York, 1974.

[Hup] Huppert, B., *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[Ja] Jacobson, N., *Structure of Rings*, American Mathematical Society, Providence, RI, 1968.

[JL1] Jespers, E., Leal, G., *Describing Units of Integral Group Rings of Some 2-groups*, Comm. Algebra **19** (1991), 1809–1827.

[JL2] Jespers, E., Leal, G., *Generators of Large Subgroups of the Unit Group of Integral Group Rings*, Manuscripta Math. **78** (1993), 303–315.

[JL3] Jespers, E., Leal, G., *Degree* 1 *and* 2 *Representations of Nilpotent Groups and Applications to Units of Group Rings*, Manuscripta Math. **86** (1995), 479–498.

[La] Lam, T.Y., *A First Course in Noncommutative Rings*, Springer-Verlag, New York, 1991.

[Mo] Moser, C., *Représentation de* -1 *Comme Somme de Carrés dans un Corps Cyclotomique Quelconque*, J. Number Theory **5** (1973), 139–141.

[Ne] Newman, M., *Integral Matrices*, Academic Press, New York, 1972.

[Re] Reiner, I., *Maximal Orders*, Academic Press, London, 1975.

[RS1] Ritter, J., Sehgal, S.K., *Generators of Subgroups of* $U(ZG)$, Contemp. Math. **93** (1989), 331–347.

[RS2] Ritter, J., Sehgal, S.K., *Construction of Units in Integral Group Rings of Finite Nilpotent Groups*, Trans. Amer. Math. Soc. **324** (1991), 603–621.

[Se1] Sehgal, S.K., *Topics in Group Rings*, Marcel Dekker, New York, 1978.

[Se2] Sehgal, S.K., *Units in Integral Group Rings*, Longman, New York, 1993.

[ST] Stewart, I.N., Tall, D.O., *Algebraic Number Theory, Second Edition*, Chapman and Hall, London, 1987.

[Su] Suzuki, M., *Group Theory I*, Springer-Verlag, Berlin, 1982.

[Va1] Vaserstein, L.N., *On the Group* SL_2 *Over Dedekind Rings of Arithmetic Type*, Math. USSR Sbornik **18** (1972), 321–332.

[Va2] Vaserstein, L.N., *The Structure of Classical Arithmetic Groups of Rank Greater Than One*, Math. USSR Sbornik **20** (1973), 465–492.

[Wo] Wolf, J.A., *Spaces of Constant Curvature, Fifth Edition*, Publish or Perish, Wilmington, DE, 1984.

[Ya] Yamada, T., *The Schur Subgroup of the Brauer Group*, Springer-Verlag, Berlin, 1974.

[Za] Zassenhaus, H., *Über Endliche Fastkörper*, Abh. Math. Sem. Hamburg. **11** (1935), 187–220.

[Ya] Yamada, T., *The Schur Subgroup of the Brauer Group*, Springer-Verlag, Berlin, 1974.

[Za] Zassenhaus, H., *Über Endliche Fastkörper*, Abh. Math. Sem. Hamburg. **11** (1935), 187–220.

END

11-03-96

FIN