UNITS OF INTEGRAL SEMIGROUP RINGS

DUZHONG WANG

Units of Integral Semigroup Rings

by

©Duzhong Wang

A thesis submitted to the

School of Graduate Studies

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

Department of Mathematics and Statistics

Memorial University of Newfoundland

May 1995

St. John's Newfoundland Canada

Abstract

In this thesis, we study the unit group $\mathcal{U}(\mathbf{Z}S)$ of the integral semigroup ring $\mathbf{Z}S$ of a finite semigroup S. Throughout, we assume that $\mathbf{Z}S$ has an identity, and, unless mentioned otherwise, it is assumed that $\mathbf{Q}S$ is a semisimple Artinian ring.

In the first part, we study large subgroups of $\mathcal{U}(\mathbf{Z}S)$. First, two types of units are introduced: the Bass cyclic units and the bicyclic units. These are appropriate generalizations of the analogous group ring case. In the main theorem, it is shown that, as in the case of integral group rings, both the Bass cyclic units and bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbf{Z}S)$, for a large class of integral semigroup rings. Because the proof ultimately relies on the celebrated congruence theorems, one has to exclude some semigroups which have some specific Wedderburn simple components of degree 1 or 2 over $\mathbf{Q}$.

In chapter 3, we deal with some examples. We consider the class of semigroups S that are monoid extensions of elementary Rees semigroups. An algorithm is given to compute generators for the full unit group $\mathcal{U}(\mathbf{Z}S)$. The algorithm is then applied to a specific example.

Finally, we classify the semigroups such that the unit group $\mathcal{U}(\mathbf{Z}S)$ is either finite or has a free subgroup of finite index. The former extends Higman's result to the case of semigroup rings.

Acknowledgements

I am deeply indebted to Dr. Eric Jespers, my supervisor, who has always been concerned about my working on the Ph. D programme, especially this thesis. He has been very generous with his time and ideas. I would say that, without his great encouragement, supervision, assistance and financial support, this work could not have been completed within these three years.

I would like to acknowledge my indebtedness to Dr. E. G. Goodaire, the past Department Head, Chair of my comprehensive examination committee and an internal examiner of my final oral examination. He has been concerned about many aspects of my study and my life during the three year study in this department. He gives me a lot of encouragement, advice, assistance and financial support.

I am grateful to Dr. Bruce Watson, the present Department Head, Dr. P. P. Narayanaswami and Dr. Peter Booth, other members of my supervisory committee. Especially, Dr. P. P. Narayanaswami gave me great help during preparation of my Ph.D. comprehensive examinations. He is always freely accessible for discussions and for providing assistance.

I would like to thank Dr. Mike Parmenter for his instructions in the algebra seminar, his careful reading of the thesis and his valuable comments as an internal examiner of my final oral examination.

Thanks are also due to Dr. Guilherme Leal, the external examiner of my final oral examination, for his influence, helpful suggestions and comments. I would like to express my appreciation to Dr. Michael Clase, my previous colleague, for his help during his study at Memorial University.

I would like to thank the Department of Mathematics and Statistics in general, in particular for providing me with the facilities that I needed and a friendly atmosphere in which to work.

I am grateful to the School of Graduate Studies and the Department of Mathematics and Statistics for supporting me with a Memorial University Fellowship and a Teaching Assistantship.

Finally, I would like to express my sincere appreciation to my wife Ling and my son Xin for their understanding, support, encouragement, and welcome distractions from mathematics.

Contents

Abstract ii

Acknowledgement iii

1 Semigroups and Integral Semigroup Rings 4

1.1 Basic semigroup definitions 4

1.2 Structure of finite semigroups 6

1.3 Semigroup rings and Munn Algebras 9

1.4 Orders and reduced norms 13

2 Large subgroups of unit groups of Integral Semigroup Rings 17

2.1 Introduction 17

2.2 Constructing Units 19

2.3 Semigroup Rings of Completely 0-Simple Semigroups 22

2.4 The Main Theorem 35

3 Full Unit Groups: A Class of Examples 43

3.1 General Method 44

3.2 A Specific Example 49

4 Semigroups with $\mathcal{U}(\mathbf{Z}S)$ finite or having a free subgroup of finite index 58

4.1 Finite Unit Group $U(\mathbf{ZS})$ 58

4.2 $\mathcal{U}(\mathbf{Z}S)$ having a free subgroup of finite index 59

References 72

Introduction

The unit group $\mathcal{U}(R)$ of a ring R is a fascinating object at the cross roads of several mathematical topics, such as group theory, representation theory, number theory and ring theory. Some of the important and best known examples for which this group has been investigated are the ring of algebraic integers $\mathcal{O}_K$ of a number field K of finite degree and the integral group ring $\mathbf{Z}G$ of a finite group G. The unit group $\mathcal{U}(\mathcal{O}_K)$ is described by the classical Dirichlet unit theorem. It is a direct product of the finite group of roots of unity of $\mathcal{O}_K$ (the trivial units) and a free abelian group of rank $r_1 + r_2 - 1$, where r_1 and r_2 are such that $dim_{\mathbf{Q}}K = r_1 + 2r_2$ and K has r_1 real and $2r_2$ complex embeddings. It is still an open problem to describe free generators of this free abelian group, even for cyclotomic fields. In the latter case, however, the cyclotomic units generate a subgroup of finite index.

In case G is a finite abelian group, Higman showed an analogue of the Dirichlet unit theorem: $\mathcal{U}(\mathbf{Z}G) = \pm G \times F$, where F is a free abelian group of rank $\frac{1}{2}(|G| + 1 + n_2 - 2c)$, where n_2 is the number of cyclic subgroups of G of order 2 and c is the number of cyclic subgroups of G. Again, in general, free generators for F are unknown, but one can obtain a large subgroup of $\mathcal{U}(\mathbf{Z}G)$. Bass and Milnor constructed finitely many generators for a subgroup of finite index in $\mathcal{U}(\mathbf{Z}G)$. These units are called the Bass cyclic units and are closely related to the cyclotomic units. In case G is nonabelian much less is known on the structure of the unit group $\mathcal{U}(\mathbf{Z}G)$. Recently, Jespers and Leal have constructed, in terms of some non-central idempotents, a finite set of generators of a subgroup of finite index of $\mathcal{U}(\mathbf{Z}G)$ for all groups satisfying some restrictions on the Wedderburn simple components of degree 1 or 2 over $\mathbf{Q}$ of the rational group algebra $\mathbf{Q}G$. The restrictions are such that the celebrated congruence theorems hold for the maximal orders in these simple components. For many groups, such as nilpotent groups of odd order, it then turns out that the Bass cyclic units together with the bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbf{Z}G)$. The bicyclic units are all the units of the type $1+(1-g)h\hat{g}$ and $1+\hat{g}h(1-g)$, where $g, h \in G$ and $\hat{g}=\sum_{i=1}^{n} g^{i}$, n the order of g. These results are a continuation of the work started by Ritter and Sehgal. We refer the reader to a recent survey on the topic by Sehgal [37]; note that, in the latter, only the units of the type $1+(1-g)h\hat{g}$ are called bicyclic units. Earlier surveys on the topic can also be found in [18], [27] and [36].

The ring of algebraic integers in a number field of finite degree and the integral group ring of a finite group both are $\mathbf{Z}$-orders in a semisimple Artinian ring. In this thesis, we study the unit group of the integral semigroup ring $\mathbf{Z}S$ of a finite semigroup S. Unless otherwise stated, we assume that $\mathbf{Z}S$ is a $\mathbf{Z}$-order in a semisimple Artinian ring, that is, we assume that $\mathbf{Z}S$ has an identity and $\mathbf{Q}S$ is semisimple Artinian. Munn showed that the latter is equivalent with S having a principal series with completely 0-simple factors such that the respective sandwich matrices are invertible over the group algebras of maximal subgroups.

In Chapter 1, we introduce the basic definitions and notations. We also recall some essential results from the theory of (semi-)groups, (semi-)group rings and orders.

In chapter 2, we study subgroups of finite index of the unit group $\mathcal{U}(\mathbf{Z}S)$. First, two types of units are introduced: the Bass cyclic units and the bicyclic units. These are appropriate generalizations of their analogues in the group ring case. To define these units, it is sufficient to note that, essentially, all that is needed is a finite cyclic subgroup in S. In the main theorem, it is then shown that, as in the group case, under some restrictions, both the Bass cyclic units and the bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbf{Z}S)$. Again, because of the celebrated congruence theorems, the restrictions are such that certain Wedderburn simple components of $\mathbf{Q}S$ of degree 1 or 2 over $\mathbf{Q}$ have to be excluded. The main outline of the proof is as follows. First one shows that the group generated by the proposed units contains a subgroup of finite index in the centre of $\mathcal{U}(\mathbf{Z}S)$. In some sense, it will be shown that the Bass cyclic units "exhaust" the centre. Second one shows that, for every simple Wedderburn component $M_n(D)$ of $\mathbf{Q}S$, $2 \leq n$, D a division ring, the group generated by the Bass cyclic units and the bicyclic units contains a subgroup of finite index in the special linear group $SL(n, \mathcal{O})$, where $\mathcal{O}$ is a maximal order in D. To prove the former part is "hardest"; we will make use of the fact that the result is known for integral group rings. The proof of the second part is, in some sense, easier than in the group ring case, because there are more idempotents in semigroups than in groups, and thus there are many more bicyclic units. Hence, making use of the methods developed by Jespers and Leal, this proof will follow rather immediately.

In Chapter 3, we investigate some examples. We consider the class of semigroups that are monoid extensions of elementary Rees semigroups. These are in some sense the "easiest" semigroups not previously dealt with concerning units. An algorithm is given to compute generators for the unit group $\mathcal{U}(\mathbf{Z}S)$ of such semigroups. The algorithm is then applied to a special example.

In the last chapter we classify the semigroups such that the unit group $\mathcal{U}(\mathbf{Z}S)$ is either finite or has a free subgroup of finite index. In particular, we extend Higman's result to the case of semigroup rings.

Chapter 1

Semigroups and Integral Semigroup Rings

Our study of the unit group of the integral semigroup ring of a finite semigroup is in the first place based on the structure theory of finite semigroups and on the characterization of semisimple Artinian rational semigroup rings of finite semigroups. A second important, though elementary, fact is that to study large subgroups of $\mathbf{Z}-orders$, one may often replace one $\mathbf{Z}-order$ by another.

In this first chapter, we therefore collect the basic definitions, notations, and the structure theory for finite semigroups. The characterization of semisimple Artinian integral semigroup rings is recalled. And finally we include some background on unit groups of $\mathbf{Z}-orders$.

We try to keep the same notations and terminologies as in [4], [23] and [29].

1.1 Basic semigroup definitions

A *semigroup* S is a non-empty set with an associative operation. We will denote this operation multiplicatively. If, moreover, S has an identity 1 then it is called a *monoid* and $\mathcal{U}(S) = \{s \in S \mid sr = rs = 1 \ for\ some\ r \in S\}$ is called the group of invertible elements of S. A monoid S with $S = \mathcal{U}(S)$ is called a *group.*

If S is a semigroup without an identity, we can adjoin one simply by adding a new element 1 and extending the multiplication by defining $1s = s1 = s$ for all $s \in S \cup \{1\}$. We denote this new semigroup by S^1. If S has an identity already, then we agree that $S^1 = S$.

An element z of semigroup S is a *zero* of S if it is a left and right zero, that is $zs = z = sz$ for all $s \in S$. If S has a zero element, it will usually be denoted by $\mathit{0}$ or $\mathit{0}_S$. A *null* semigroup is one in which the product of any two elements is the zero element $\mathit{0}$ (so a null semigroup must have a zero). In a very similar way to adjoining an identity, we can always adjoin a zero element $\mathit{0}$, and we write $S^0 = S \cup \{\mathit{0}\}$ for this new semigroup. Adjoining zeroes often simplifies arguments.

A *subsemigroup* of a semigroup S is a non-empty subset which is closed under multiplication. A *subgroup* G of S is a subsemigroup which is a group. Note that the identity of G need not be the identity of S (indeed S need not even have an identity). We will denote the union of all subgroups of S by $GR(S)$.

For a semigroup S, the subset $Z(S) = \{x \mid xs = sx \ for\ all\ s \in S\}$ is called the centre of S. It is a commutative subsemigroup of S, that is, any two elements commute with each other.

An element e of semigroup S which satisfies $e = e^2$ is called an *idempotent*. We write $E(S)$ for the set of idempotent elements of a semigroup S. The set $E(S)$ can be partially ordered by $e \leq f$ if and only if $ef = fe = e$. If $e \in E(S)$, then $eSe = \{ese \mid s \in S\}$ is a submonoid of S. Note that $eSe = \{s \in S \mid es = se = s\}$, the set of elements of S for which e is an identity element. Let $H_e = \mathcal{U}(eSe)$, the group of units of the monoid eSe. Then H_e is a subgroup of S and it is the largest subgroup for which e is the identity element. Such subgroups are called the *maximal* subgroups of S. Since e is the unique idempotent element of H_e, there is a one-to-one correspondence between idempotents and maximal subgroups. Note that distinct maximal subgroups are disjoint.

For a non-empty subset A of a semigroup S, we write $\langle A \rangle$ for the subsemigroup generated by A. If A is finite, say $A = \{a_1, a_2, \ldots, a_n\}$, we often write $\langle a_1, a_2, \ldots, a_n \rangle$ instead of $\langle A \rangle$. A semigroup S is *cyclic* if $S = \langle s \rangle$ for some $s \in S$. An element s of a semigroup S is a *periodic element* if $\langle s \rangle$ is finite. A finite cyclic semigroup always contains an idempotent.

A *homomorphism* of semigroups is a function $f: S \to T$ from a semigroup S to a semigroup T such that $f(st) = f(s)f(t)$ for all $s, t \in S$.

A non-empty subset I of S is said to be a *left* (*right*) ideal of S if it is closed under *left* (*right*) multiplication by elements of S. A non-empty subset I of S is said to be an *ideal* of S if it is both a left and right ideal of S. If S has a zero element 0, then $\{0\}$ is always an ideal of S. The ideal generated by a is $S^1 a S^1 = SaS \cup Sa \cup aS \cup \{a\}$.

If I is an ideal of S, the Rees factor semigroup S/I is the set $(S \setminus I) \cup \{0\}$ subject to the multiplication " $\circ$ " defined by the formula

$$s \circ t = \begin{cases} st & \text{if } st \notin I \\ 0 & \text{if } st \in I \end{cases}$$

1.2 Structure of finite semigroups

The basic building blocks of the structure theory of finite semigroups are the simple and 0-simple semigroups.

Let S be a semigroup. We say that S is a *simple semigroup* if it has no ideals other than S itself. This definition is not very interesting if S has a zero element 0, for in that case $\{0\}$ is always an ideal of S. So we say that a semigroup S with a zero is a *$0-$simple semigroup* if (i) $S^2 \neq \{0\}$ and (ii) $\{0\}$ is the only proper ideal of S.

A semigroup S is a *completely $0-$simple semigroup* if it is 0-simple and it contains a *primitive idempotent*, that is, a minimal non-zero idempotent with respect to the earlier defined partial ordering.

Proposition 1.2.1 *[4, Lemma 2.26, p.67] Let S be a semigroup with a zero 0 such that $\{0\}$ is the only proper ideal of S. Then either S is 0-simple or S is the null semigroup of order 2.*

Note that if S does not have a zero and S is simple, then S^0 is 0-simple. This means that any results about 0-simple semigroups can be easily applied to simple semigroups. For this reason, we will usually restrict our attention to 0-simple semigroups.

Let S be a semigroup with a zero. A strictly decreasing series

$$S = S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \{0\}$$

is a *principal series* if each S_i is an ideal of S and there are no ideals of S strictly between S_i and S_{i+1}, that is ,each S_i/S_{i+1} is either the null semigroup of order 2 or a 0-simple semigroup.

Note that our definition of principal series differs slightly from that of [4]. Our series ends with the zero ideal rather than the empty set. Of course, this restricts our definition to semigroups with zeroes, so we will always adjoin a zero before considering principal series.

Proposition 1.2.2 *Finite semigroups always have principal series.*

Note that the analogue for semigroups of the Jordan Holder-Schreier Theorem asserts that the principal factors of any two principal series are isomorphic (in some order).

To describe the structure of completely 0-simple semigroups, we need to introduce more notations.

Let G be a group, n_1 and n_2 positive integers, and let P be a $n_2 \times n_1$ matrix with entries from G^0. For $g \in G^0$, $i \in \{1, 2, \ldots, n_1\}$, and $j \in \{1, 2, \ldots, n_2\}$, write $(g)_{ij}$ for the $n_1 \times n_2$ matrix with (i, j)-entry g and all other entries equal to $\mathit{0} = \mathit{0}_{G^0}$. Let $\mathcal{M}^0(G; n_1, n_2; P)$ be the set whose elements are all such $(g)_{ij}$, with all $(\mathit{0})_{ij}$ identified, and define a multiplication on this set by

$$AB = A \circ P \circ B,$$

where $A, B \in \mathcal{M}^0(G; n_1, n_2; P)$ and '$\circ$' denotes ordinary multiplication of matrices. So, $(y)_{ij}(h)_{kl} = (yp_{jk}h)_{il}$, where p_{ij} is the (i, j)-entry of the matrix $P = (p_{ij})$. The set $\mathcal{M}^0(G; n_1, n_2; P)$ endowed with this operation is a semigroup, called a *Rees matrix* semigroup. Its zero element will also be denoted simply by $\mathit{0}$. The matrix P is called the *sandwich* matrix. Also, P is called regular if it has at least one non-zero entry in every row and column. A Rees matrix semigroup of the form $\mathcal{M}^0(\{1\}; n_1, n_2; P)$, where $\{1\}$ is the trivial group, is called an *elementary Rees matrix semigroup*. Clearly these semigroups have only trivial subgroups.

Theorem 1.2.1 *[4, Theorem 3.5, p.94] A finite semigroup is completely 0-simple if and only if it is isomorphic with a Rees matrix semigroup $\mathcal{M}^0(G; n_1, n_2; P)$, where P is a regular sandwich matrix and G is a finite group.*

The following is now easily verified (see for example [23, p.7])

Lemma 1.2.1 *If $S = \mathcal{M}^0(G; n_1, n_2; P)$ is a completely 0-simple semigroup with sandwich matrix $P = (p_{ij})$, then*

(i) $\{(p_{ji}^{-1})_{ij} \in S \mid p_{ji} \neq 0\}$ is the set of non-zero idempotents of S;

(ii) for any i, j, if $p_{ji} \neq 0_G$, then

$$S_{(i)}^{(j)} \to G^0 : (x)_{ij} \to xp_{ji}$$

is an isomorphism, where

$$S_{(i)}^{(j)} = \{(g)_{ij} \in S \mid g \in G^0\};$$

(iii) the maximal subgroups of S are all $G_{ij} = S_{(i)}^{(j)} \setminus \{0\}$, with $p_{ji} \neq 0$.

1.3 Semigroup rings and Munn Algebras

Definition 1.3.1 *Let R be an associative ring with an identity and let S be a (semi-)group. Then the set RS consisting of all formal sums of the form*

$$\alpha = \sum_{s \in S} a_s s$$

with only finitely many nonzero coefficients $a_s \in R$, is called the (semi-)group ring of the (semi-)group S over the ring R when it is equipped with the following addition, *multiplication and scalar multiplication (only needed when defining a (semi-) group algebra):*

$$\alpha+\beta=\left(\sum_{s\in S}a_s s\right)+\left(\sum_{s\in S}b_s s\right)=\sum_{s\in S}(a_s+b_s)s$$

and

$$\alpha\beta=\left(\sum_{s\in S}a_s s\right)\left(\sum_{t\in S}b_t t\right)=\sum_{s,t\in S}a_s b_t st=\sum_{z\in S}c_z z$$

$$r\alpha=r\left(\sum_{s\in S}a_s s\right)=\sum_{s\in S}(ra_s)s$$

where $\alpha=\sum_{s\in S}a_s s$, $\beta=\sum_{t\in S}b_t t\in RS$, *and* $r\in R$,

$$c_z=\begin{cases}\sum_{st=z}a_s b_t & \textit{if } A(z)\neq\emptyset\\ 0 & \textit{if } A(z)=\emptyset\end{cases}$$

and $A(z)=\{(s,t)\in S\times S \mid st=z\}$.

In particular, $\mathbf{Q}S$ and $\mathbf{Z}S$ are the rational and integral (semi-) group rings, where $\mathbf{Q}$ and $\mathbf{Z}$ denote the rational field and the ring of integers respectively.

Similar to the centre of a semigroup; we denote by $Z(R)$ the centre of ring R; that is, $x\in Z(R)$ if and only if $xr=rx$ for all $r\in R$.

Let S be a semigroup with zero θ. By the contracted semigroup algebra S over R, denoted by R_0S, we mean the factor algebra $RS/R\theta$. Thus, R_0S may be identified with the set of finite sums $\sum\alpha_s s$ with $\alpha_s\in R$, $s\in S\setminus\{\theta\}$, subject to the componentwise addition and multiplication given by the rule

$$s\circ t=\begin{cases}st & \text{if } st\neq\theta\\ 0 & \text{if } st=\theta\end{cases}$$

defined on the basis $S\setminus\{\theta\}$. If S has no zero element, then we put $R_0S=RS$.

From the definition it follows directly that, for any semigroup S, we have $R_0S^0\cong RS^0/R\theta\cong RS$. We will often use the following extension of this fact.

Proposition 1.3.1 *[23, Lemma 7, p.38] Let I be an ideal of a semigroup S. Then $R_0(S/I) \cong RS/RI$.*

Proposition 1.3.2 *[23, Corollary 9, p.38] Assume that S has a zero element. Then $RS = R0 \oplus RS(1-0) \cong R0 \oplus R_0S \cong R \oplus R_0S$.*

This and the fact that, for any S, $RS^0 \cong R \oplus R_0S^0 \cong R \oplus RS$, will allow us to switch from one of the algebras RS, R_0S to the other whenever convenient. Also, it is clear that RS is semisimple if and only if R_0S is semisimple.

Now, we describe an important class of (contracted) semigroup algebras, called Munn algebras, arising from completely 0-simple semigroups. The construction of a Munn algebra is rather similar to that of a Rees matrix semigroup. Again n_1 and n_2 are positive integers, but instead of a group G, we now consider a *K-algebra* A, where K is a commutative ring. Let P be an $n_2 \times n_1$ matrix with entries in A. The *Munn algebra* $R = \mathcal{M}(A; n_1, n_2; P)$ is the set of all $n_1 \times n_2$-matrices with entries in A. Addition and scalar multiplication by elements of K are defined component-wise. Matrices multiply by insertion of the sandwich matrix P; that is, if X and Y are two elements of R, then the product of X and Y is

$$XY = X \circ P \circ Y,$$

where 'o' again denotes the ordinary matrix multiplication. In case $n_1 = n_2$ and P is the identity matrix I, then $R = \mathcal{M}(A; n_1, n_1; I)$ is the classical matrix ring over A. We denote this ring by $M_{n_1}(A)$. So matrix rings are examples of contracted semigroup algebras.

Note that if $S = \mathcal{M}^0(G; m, m; P)$ is a completely 0-simple semigroup, then we will often consider S in a natural way as a subsemigroup of the Munn algebra $\mathcal{M}(RG; m, m; P)$, for any commutative ring R. In particular, under this identification, the zero $0 \in S$ is identified with the zero element $0 \in \mathcal{M}(RG; m, m; P)$.

The Lemma below([4, p.162-163]) is very important for our investigations in chapter 2. The notation $M \cong^{iso} N$ indicates that the algebras M and N are isomorphic under the isomorphism *iso*.

Lemma 1.3.1 *Let m and l be two natural numbers. Let $T = \mathcal{M}^0(G; m, l; P)$ be a finite completely 0-simple semigroup. Then $\mathbf{Q}T$ is semisimple Artinian if and only if $m = l$ and P is invertible in $M_m(\mathbf{Q}G)$. As a consequence, if $\mathbf{Q}T$ is semisimple Artinian, then*

(i) $\mathbf{Q}_0 T \cong^{\eta} \mathcal{M}(\mathbf{Q}G; m, m; P)$, *where η is the natural mapping;*

(ii) the mapping $f_P : \mathcal{M}(\mathbf{Q}G; m, m; P) \to M_m(\mathbf{Q}G) : A \to A \circ P$ is a ring isomorphism; in particular, P^{-1} is the identity of $\mathcal{M}(\mathbf{Q}G; m, m; P)$;

(iii) if $P^{-1} \in \mathcal{M}(\mathbf{Z}G; m, m; P)$, then

$$f_P(\mathcal{M}(\mathbf{Z}G; m, m; P)) = M_m(\mathbf{Z}G).$$

Often in this thesis, we skip the matrix multiplication symbol '$\circ$'. This will not create confusion as it will be clear from the context which product has to be taken.

Generally, we have that (see for example [4, Corollary 5.34, p.174] or [23, Theorem 24, p. 173])

Theorem 1.3.1 *Let*

$$S^0 = S_0 \supset S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \{0_S\}$$

be a principal series of a finite semigroup $S^0 = S \cup \{\theta\}$. *Then* $\mathbf{Q}S$ *is semisimple Artinian if and only if* $S_i/S_{i+1} \cong^{\eta_i} \mathcal{M}^0(G_i; m_i, m_i; P_i)$, G_i *a group,* $i = 0, 1, \ldots, n$, *and each* P_i *is invertible in* $M_{m_i}(\mathbf{Q}G_i)$. *Further, if* $\mathbf{Q}S$ *is semisimple Artinian, then*

$$\mathbf{Q}S^0 \cong^{\psi} \bigoplus_{i=0}^{n} \mathbf{Q}_0(S_i/S_{i+1}) \bigoplus \mathbf{Q}\theta_S \cong^{\oplus\eta_i} \bigoplus_{i=0}^{n} \mathcal{M}(\mathbf{QG}_i; m_i, m_i; P_i) \oplus \mathbf{Q}\theta_S$$

$$\cong^{\oplus(f_{P_i}, \eta_i)} \bigoplus_{i=0}^{n} M_{m_i}(\mathbf{Q}G_i) \oplus \mathbf{Q}\theta_S,$$

where each η_i, f_{P_i} *is defined as in Lemma 1.3.1, and* ψ *is the natural isomorphism.*

Note that if $\mathbf{Z}S$ has an identity $\mathbf{1}$ and $\mathbf{Q}S$ is semisimple Artinian, then the identity $\mathbf{1}$ is "known": it is determined by the inverses of the matrices $P_i^{\prime}s$. In general, determining when $\mathbf{Z}S$ has an identity for any arbitrary semigroup S is difficult.

1.4 Orders and reduced norms

In this section, we recall some elementary facts about orders, norms and reduced norms.

Let A be a finite dimensional $\mathbf{Q}$-algebra with identity 1. A subring $\mathcal{O}$ of A, $1 \in \mathcal{O}$, is said to be a $(\mathbf{Z})-order$ in A if it is a finitely generated $\mathbf{Z}-module$ such that $\mathbf{Q}\mathcal{O} = A$. Further, an order $\mathcal{O}$ in A is said to be *maximal* if it is not properly contained in a bigger order. Every order in A is contained in a maximal order (see for example, [37, Lemma (4.4), p.18]).

Clearly, the ring $\mathcal{O}_K$ of algebraic integers of an algebraic number field K is an order in K and the integral group ring $\mathbf{Z}G$ of a finite group G is an order in $\mathbf{Q}G$. Similarly, $\mathbf{Z}S$ is an order in $\mathbf{Q}S$ if S is a finite semigroup such that $\mathbf{Z}S$ has an identity.

It is easily verified that the intersection $\mathcal{O}_1 \cap \mathcal{O}_2$ of two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in A is again an order in A. Also if $\mathcal{O}$ is an (maximal) order in A then $M_n(\mathcal{O})$ is an (maximal) order in $M_n(A)$ (see for example, [37, Lemma (4.2), p.17] and [29, (8.7) Theorem, p.110]).

Lemma 1.4.1 *[37, Lemma (4.5), p.18] Let A be a semisimple finite dimensional* $\mathbf{Q}$*-algebra with Wedderburn decomposition*

$$A = \oplus e_i A = \oplus A_i$$

into simple algebras A_i where e_i are the primitive central idempotents. A_i is a full matrix ring $M_{m_i}(D_i)$ over the division ring D_i.

(i) Let Λ be a maximal order in A. Then $\Lambda = \oplus \Lambda_i$, $\Lambda_i = e_i \Lambda$. Moreover, Λ_i is a maximal order of A_i.

(ii) Any maximal order in A_i contains $\mathcal{O}_i$, where $\mathcal{O}_i$ is the ring of integers of the algebraic number field Z_i, the centre of D_i.

The following proposition shows that the unit groups of orders are in some sense closely related. Because this fact is crucial to our investigation, we include a proof.

Lemma 1.4.2 *[37, Lemma (4.6), p.19] Suppose that $\mathcal{O}_1 \subseteq \mathcal{O}_2$ are two orders in A. Then*

(a) the index of their unit groups $[\mathcal{U}(\mathcal{O}_2) : \mathcal{U}(\mathcal{O}_1)]$ is finite;

(b) if $u \in \mathcal{O}_1$ is invertible in $\mathcal{O}_2$, then $u^{-1} \in \mathcal{O}_1$.

Proof. (a) Since $\mathcal{O}_2$ and $\mathcal{O}_1$ are two $\mathbf{Z}-$ *orders*, they have the same rank as $\mathbf{Z}-$ *modules*. Thus the index of additive groups $[\mathcal{O}_2 : \mathcal{O}_1] = l < \infty$. Consequently,

$l\mathcal{O}_2 \subseteq \mathcal{O}_1$. Suppose we have $x, y \in \mathcal{U}(\mathcal{O}_2)$ such that $x + l\mathcal{O}_2 = y + l\mathcal{O}_2$. Then $x^{-1}y - 1 \in l\mathcal{O}_2 \subseteq \mathcal{O}_1$. It follows that $x^{-1}y \in \mathcal{O}_1$. Similarly, $y^{-1}x \in \mathcal{O}_1$. It follows that $[\mathcal{U}(\mathcal{O}_2) : \mathcal{U}(\mathcal{O}_1)] \leq [\mathcal{O}_2 : l\mathcal{O}_2] < \infty$.

(b) We observe that the index of additive groups

$$[\mathcal{O}_2 : u\mathcal{O}_1] = [u\mathcal{O}_2 : u\mathcal{O}_1] \leq [\mathcal{O}_2 : \mathcal{O}_1],$$

which implies that $u\mathcal{O}_1 = \mathcal{O}_1$ as required. □

Let K be a field, and A a finite dimensional K-algebra. Each $\alpha \in A$ determines a $K-linear$ transformation α_L on A, by left multiplication. Define $char.pol._K\alpha = char.pol._K\alpha_L$, where $char.pol._K\alpha_L$ indicates the characteristic polynomial of α_L. Then, it is known that [7, p.366]

$$char.pol._K\alpha = det(XI - (a_{ij}))$$

$$= X^m - (T_{A/K}\alpha)X^{m-1} + \cdots + (-1)^m N_{A/K}\alpha,$$

where we suppose that $A = \oplus_{i=1}^m K u_i$, and

$$\alpha u_j = \sum_{i=1}^{m} a_{ij}u_i, \; a_{ij} \in A, \; 1 \leq j \leq m.$$

We call $T_{A/K}\alpha$ the *trace* map, and $N_{A/K}\alpha$ the *norm* map. The trace and norm have the following properties:

$$T(r\alpha + s\beta) = rT(\alpha) + sT(\beta) \quad, N(\alpha\beta) = N(\alpha)N(\beta), \; N(r\alpha) = r^m N(\alpha),$$

for $r, s \in K, \alpha, \beta \in A$.

Now assume A is a central simple K *– algebra*, that is, A is a simple K – *algebra* with centre K, such that $(A : K)$ is finite. For $a \in A$, define its *reduced* characteristic polynomial as in [29, p.112-113]

$$red.char.pol._{A/K}a = char.pol.h(1 \otimes a),$$

where h is the isomorphism $E \otimes_K A \cong M_n(E)$, $(A : K) = n^2$, and E is a splitting field extension field of K. Further, if

$$red.char.pol._{A/K}a = X^n - tr(a)X^{n-1} + \cdots + (-1)^n nr(a), \ a \in A.$$

Then we call $tr(a)$ the *reduced trace* of a, and nr(a) the *reduced norm* of a.

For a (maximal) order $\mathcal{O}$, we will write $GL(m, \mathcal{O})$ for the unit group of $M_m(\mathcal{O})$ and $SL(m, \mathcal{O})$ for the subgroup in $GL(m, \mathcal{O})$ that consists of all elements having reduced norm one.

Chapter 2

Large subgroups of unit groups of Integral Semigroup Rings

2.1 Introduction

The ultimate aim in studying the unit group $\mathcal{U}(\mathbf{Z}S)$ of the integral semigroup ring $\mathbf{Z}S$ of a finite semigroup S is of course to obtain a full algebraic description of this group, in particular, to obtain a presentation for this group. But, as explained in the introduction of this thesis, that is, in general, an extremely hard problem. Even for commutative groups, this is unsolved. So, as a compromise, we look for generators of a subgroup of finite index. In the case of integral group rings $\mathbf{Z}G$, many nice results have been achieved in the last decade (see for example [3],[31], [32], and so on). The main result of this development has recently been improved by Jespers and Leal ([11]) and ([12]), for many groups G. To be more precise, generators for a subgroup of finite index of $\mathcal{U}(\mathbf{Z}G)$ are given for all finite groups G which are such that every non-abelian homomorphic image is not fixed point free , and furthermore, the rational group algebra $\mathbf{Q}G$ has no simple components of the following types

(i) a 2×2-matrix ring over the rationals;

(ii) a 2×2-matrix ring over a quadratic imaginary extension of the rationals;

(iii) a 2×2-matrix ring over a noncommutative division algebra.

Recall that a group G is said to be fixed point free (see for example [32]) if it has a complex irreducible representation ρ such that for every nonidentity element g of G, $\rho(g)$ has all eigenvalues different from one. These groups were characterised in a fundamental paper [39] and are well known. Also see [8, p.73] and [26, p.96 and 204].

The reason we exclude these types of simple rings is that the congruence subgroup theorems for 2×2-matrix rings over maximal orders in the respective division rings fail.

To prove the above mentioned results, it is essential that $\mathbf{Z}G$ is a $\mathbf{Z}$-order in the semisimple Artinian ring $\mathbf{Q}G$. A natural question therefore is to investigate if the results on group rings can be extended to other $\mathbf{Z}$-orders in semisimple Artinian rings. In this chapter, we consider this question for the integral semigroup ring $\mathbf{Z}S$ (with identity) of a finite semigroup S such that $\mathbf{Q}S$ is a semisimple Artinian ring (Theorem 1.3.1), that is, S^0 has a principal series

$$S^0 = S_0 \supset S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \{\theta_S\},$$

where, for $i = 0, 1, \ldots, n$, each principal factor $S_i/S_{i+1} \cong \mathcal{M}^0(G_i; m_i, m_i; P_i)$ is a completely 0-simple Rees matrix semigroup with regular sandwich matrix P_i (here, G_i is a group, and m_i is a positive integer), and moreover, the matrix P_i is invertible in the classical matrix ring $M_{m_i}(\mathbf{Q}G_i)$. In the first part of the chapter, we will therefore mainly deal with the semigroup ring of a completely 0-simple semigroup. In the second part, we then consider the general case. However, for the same reasons as in the group ring case, we need to exclude the existence of certain simple components of $\mathbf{Q}S$.

We begin this chapter by introducing two types of generators: the Bass-cyclic units and bicyclic units. They are the obvious generalizations of the group ring notions. The hardest part of this chapter is to prove that the Bass cyclic units "exhaust" the central units. The second type of units is needed to generate subgroups of finite index in certain special linear groups. Since completely 0-simple semigroups often contain many idempotents, the latter will be "easy" by making use of the methods developed by Jespers and Leal in [11].

2.2 Constructing Units

Throughout the chapter, S is a finite semigroup such that its integral semigroup ring $\mathbf{Z}S$ has an identity. Its unit group is denoted by $\mathcal{U}(\mathbf{Z}S)$.

To introduce the first type of units, we need some notations. Recall that $GR(S)$ denotes the union of all subgroups of S. For $a \in S$, note that $\langle a \rangle$ is a cyclic group if $a \in GR(S)$. In the latter case, we write $\hat{a} = \sum_{j=1}^{n} a^j$, where n is the order of a, i.e. the order of $\langle a \rangle$. Note that $n^{-1}\hat{a}$ is an idempotent in $\mathbf{Q}S$.

Definition 2.2.1 *Let $\mathbf{Z}S$ be a semigroup ring with identity $\mathbf{1}$. A Bass cyclic unit of $\mathbf{Z}S$ is an element of the form*

$$u = (\mathbf{1} + \sum_{j=1}^{i-1} a^j)^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{a},$$

where $a \in GR(S)$, n is the order of $\langle a \rangle$, ϕ is the Euler function; $1 < i < n$, and $(i, n) = 1$.

By B_S we denote the set of all Bass cyclic units of $\mathbf{Z}S$. Further, if S has a zero element, then the natural image of B_S in the contracted semigroup algebra $\mathbf{Q}_0S$ is denoted by B_S^0.

Let us first show that such an element u is indeed a unit of $\mathbf{Z}S$. This can easily be done using the group ring results and the Wedderburn decomposition of $\mathbf{Z}(\langle a\rangle)$. However, we will give an elementary proof by describing explicitly the inverse of a Bass cyclic unit. Since $(i,n) = 1$, there exist two integers, say k and l, such that $ik + ln = 1$. Further, we can assume that $1 < k < n$. Indeed, write $k = nn' + k'$ for some integers n' and k' with $0 \leq k' < n$, then $k' \neq 0$ since $ik + ln = 1$, and $ik' + n(l + in') = 1$ with $1 \leq k' < n$. As $1 < i < n$ it follows easily that $1 < k'$, hence showing the claim. It is obvious that then $l < 0$. Let

$$v = (\mathbf{1} + a^i + \cdots + a^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\hat{a}.$$

Then $uv = X + Y + W + T$, where

$$\begin{aligned}
X &= ((\mathbf{1} + a + \cdots + a^{i-1})(\mathbf{1} + a^i + \cdots + a^{i(k-1)}))^{\phi(n)} \\
&= (\mathbf{1} + a + a^2 + \cdots + a^{i-1} + a^i + a^{i+1} + \cdots + a^{2i-1} + \cdots + a^{ik-1})^{\phi(n)} \\
&= (\mathbf{1} + (a + a^2 + \cdots + a^{n-1} + a^n) + a^n(a + a^2 + \cdots + a^n) \\
&\quad + \cdots + a^{(-l-1)n}(a + a^2 + \cdots + a^n))^{\phi(n)} \\
&= (\mathbf{1} - l\hat{a})^{\phi(n)};
\end{aligned}$$

and

$$\begin{aligned}
Y &= (1 + a + a^2 + \cdots + a^{i-1})^{\phi(n)}(\frac{1 - k^{\phi(n)}}{n})\hat{a} \\
&= (\frac{(\mathbf{1} + a + a^2 + \cdots + a^{i-1})\hat{a}}{n})^{\phi(n)}(1 - k^{\phi(n)})
\end{aligned}$$

$$= \frac{\hat{a}}{n} i^{\phi(n)}(1 - k^{\phi(n)});$$

Similarly,

$$W = (\mathbf{1} + a^{i} + \cdots + a^{i(k-1)})^{\phi(n)}(\frac{1 - i^{\phi(n)}}{n})\hat{a} = \frac{\hat{a}}{n} k^{\phi(n)}(1 - i^{\phi(n)}).$$

Finally,

$$T = (\frac{1 - i^{\phi(n)}}{n})\hat{a}(\frac{1 - k^{\phi(n)}}{n})\hat{a} = (1 - i^{\phi(n)})(1 - k^{\phi(n)})\frac{\hat{a}}{n}.$$

So,

$$Y + W + T = (1 - (ki)^{\phi(n)})\frac{\hat{a}}{n},$$

and

$$uv = (\mathbf{1} - l\hat{a})^{\phi(n)} + (1 - (ki)^{\phi(n)})\frac{\hat{a}}{n}.$$

Consequently

$$uv(\mathbf{1} - \frac{\hat{a}}{n}) = (\mathbf{1} - l\hat{a} - \frac{\hat{a}}{n} + l\frac{(\hat{a})^2}{n})^{\phi(n)} = (\mathbf{1} - \frac{\hat{\mathbf{a}}}{\mathbf{n}})^{\phi(\mathbf{n})} = \mathbf{1} - \frac{\hat{\mathbf{a}}}{\mathbf{n}}$$

and

$$\begin{aligned} uv\frac{\hat{a}}{n} &= (\frac{\hat{a}}{n} - l\frac{(\hat{a})^2}{n})^{\phi(n)} + (1 - (ki)^{\phi(n)})\frac{\hat{a}}{n} \\ &= (\frac{\hat{a}}{n} - l\hat{a})^{\phi(n)} + (1 - (ki)^{\phi(n)})\frac{\hat{a}}{n} \\ &= \frac{\hat{a}}{n}((1 - nl)^{\phi(n)} + 1 - (ki)^{\phi(n)}) \\ &= \frac{\hat{a}}{n}((ik)^{\phi(n)} + 1 - (ik)^{\phi(n)}) \\ &= \frac{\hat{a}}{n}. \end{aligned}$$

Therefore, $uv = \mathbf{1}$. Since u and v commute, we have shown u is a unit.

Important in the construction of the Bass cyclic units is that $a \in R$,where R is a ring with identity 1, and that a generates a finite subgroup (possibly with identity different from 1). Hence, in this way one can define a Bass cyclic unit in any ring R with identity $\mathbf{1}$. It is convenient for further computations to introduce the following notation. Let $x \in R$ be an element for which the subsemigroup $\langle x \rangle$ generated by x is a finite group. Let n be the order of $\langle x \rangle$, $(i, n) = 1$, and $1 < i < n$. Write

$$u_R(x, i) = (\mathbf{1} + \sum_{j=1}^{i-1} x^j)^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{x},$$

where $\hat{x} = \sum_{j=1}^{n} x^j \in R$. So, in particular, a Bass cyclic unit in $\mathbf{Z}S$ can be denoted by $u_{\mathbf{Z}S}(a, i)$. It is clear that if f is a ring isomorphism from R to R' then $f\left(u_R(x, i)\right) = u_{R'}\left(f(x), i\right)$.

We now introduce the second type of units.

Definition 2.2.2 *A bicyclic unit of* $\mathbf{Z}S$ *is an element of the form* $u = \mathbf{1} + (\mathbf{1} - a)s\hat{a}$*, or* $u = \mathbf{1} + \hat{a}s(\mathbf{1} - a)$*, where* $s \in S$*, and* $a \in GR(S)$*.*

Note that these elements are indeed units as they are of the form $\mathbf{1} + \alpha$ with $\alpha^2 = 0$. We decided to call both units of the latter type bicyclic units. In the case of group rings, only the elements of the former type were called so in [30] and [37]; however, this will not create any confusion.

For the remainder of this chapter, we always assume that $\mathbf{Q}S$ is semisimple Artinian, and it is now devoted to showing that the Bass cyclic units and the bicyclic units generate a subgroup of finite index, for many semigroups S.

2.3 Semigroup Rings of Completely 0-Simple Semigroups

Throughout this section, T denotes a finite completely 0-simple semigroup of the type $T = \mathcal{M}^0(G; m, m; P)$, where G is a group with identity e and the sandwich matrix P is regular. Further, we assume that $m > 1$, and that P is invertible in $M_m(\mathbf{Q}G)$.

Since P is regular, for any $i = 1, 2, \ldots, m$, we fix a $j_i \in \{1, 2, \ldots, m\}$ such that $p_{j_i i} \neq 0_T$. As before, let $G_{kl} = T_{(k)}^{(l)} \setminus \{0_T\}$. Then $GR(T) = \cup_{p_{lk} \neq 0_T} G_{kl}$, and $\cup_{i=1}^{n} f_P(G_{ij_i}) \subseteq f_P(GR(T)) = \cup_{p_{ji} \neq 0_G} f_P(G_{ij}) = \cup_{p_{ji} \neq 0_G} G_{ij} P$ (here we refer the reader to Lemma 1.3.1 for the definition of f_P).

In the first part of this section we investigate what a Bass cyclic unit looks like in a matrix format. To do so, we first need the following Lemmas. Further, for $\alpha \in \mathbf{Z}G$, $A = (a_{ij}) \in M_m(\mathbf{Z}G)$, we denote by $\alpha A = (\alpha a_{ij})$.

Lemma 2.3.1 *Let I be the identity of $M_m(\mathbf{Z}G)$, that is*

$$I = \begin{bmatrix} e & 0 & \cdots & 0 \\ 0 & e & \cdots & 0 \\ \vdots & \vdots & & 0 \\ 0 & 0 & \cdots & e \end{bmatrix}.$$

Let $A = (a_{qc}) \in M_m(\mathbf{Z}G)$ be a matrix with all entries zero except possibly those in the ith row. Then, for any positive integer n, $A^n = a_{ii}^{n-1} A$, and

$$(I + A)^n = I + B$$

where

$$B = \sum_{h=0}^{n-1} (e + a_{ii})^h A.$$

Proof. We prove the first part by induction on n; the case $n = 1$ being clear. Assume $A^n = a_{ii}^{n-1} A$. Then $A^{n+1} = A^n A = a_{ii}^{n-1} A^2$. But, $A^2 = a_{ii} A$. Hence, $A^{n+1} = a_{ii}^{n-1} a_{ii} A = a_{ii}^{n} A$. We also prove the second part by induction. It is clear for $n = 1$. Now assume that, for n larger than or equal to 1,

$$(I+A)^n = I + sA, \text{ where } s = \textstyle\sum_{h=0}^{n-1}(e+a_{ii})^h.$$

Then

$$\begin{aligned}(I+A)^{n+1} &= (I+A)^n(I+A)\\ &= (I+sA)(I+A)\\ &= I+A+sA+sA^2\\ &= I+(e+s)A+sa_{ii}A\\ &= I+(e+s+sa_{ii})A.\end{aligned}$$

But

$$\begin{aligned}e+s+sa_{ii} &= e+s(e+a_{ii})\\ &= e+\sum_{h=0}^{n-1}(e+a_{ii})^{h+1}\\ &= e+\sum_{h=1}^{n}(e+a_{ii})^{h}\\ &= \sum_{h=0}^{(n+1)-1}(e+a_{ii})^{h}.\end{aligned}$$

Hence the result follows. □

Corollary 2.3.1 *Given $p_{j_i i} \neq 0_G$, then $G_{ij_i}P$ is a subgroup of $M_m(\mathbf{Z}G)$ with identity $(p_{j_i i}^{-1})_{ij_i}P$; the orders of $(g)_{ij_i} \in G_{ij_i}$, $A = (g)_{ij_i}P \in G_{ij_i}P$ and $gp_{j_i i} \in G$ are the same. Furthermore, for any positive integer n*

$$(I+A)^n = I + B,$$

where

$$B = \sum_{h=0}^{n-1}(e+gp_{j_i i})^h A.$$

Proof. That $G_{ij_i}P$ is a subgroup with identity $(p_{j_i i}^{-1})_{ij_i}P$ of the multiplicative semigroup $M_m(\mathbf{Z}G)$ and that $(g)_{ij_i}$ and $(g)_{ij_i}P$ have the same order follow from Lemma 1.5.1. By Lemma 2.3.1, for any natural number n, $A^n = (gp_{j_i i})^{n-1}A$. Since $(p_{j_i i}^{-1})_{ij_i}P$ is the identity of group $G_{ij_i}P$, it is easily verified that $A^n = (p_{j_i i}^{-1})_{ij_i}P$ if and only if $(gp_{j_i i})^n = e$, the identity of G.

The second part follows at once from Lemma 2.3.1. □

In the following Lemma we describe the matrix representation, under the mapping f_P, of the Bass cyclic units defined via the elements of the group G_{ij_i}.

Lemma 2.3.2 *Let $(g)_{ij_i} \in G_{ij_i}$ be of order l, and let d be an integer with $1 < d < l$, and $(d,l) = 1$. Then*

$$f_P(u_{\mathbf{Z}_0T}((g)_{ij_i}, d)) = u_{M_m(\mathbf{Z}G)}(f_P((g)_{ij_i}), d)$$

$$= u_{M_m(\mathbf{Z}G)}((g)_{ij_i}P, d) = I + B$$

where $B = (u-e)(p_{j_i i}^{-1})_{ij_i}P$ and $u = u_{\mathbf{Z}G}(gp_{j_i i}, d)$.

Proof. Let $A = (g)_{ij_i}P = (a_{ij})$ and let $A' = (a'_{qc})$ be the matrix $\sum_{r=1}^{d-1} A^r$. By Lemma 2.3.1, $A' = \sum_{h=0}^{d-2}(gp_{j_i i})^h A$, and thus $a'_{ic} = \sum_{h=0}^{d-2}(gp_{j_i i})^h a_{ic}$, and $a'_{qc} = 0$ for $q \neq i$. So, again by Lemma 2.3.1, $(I+A')^{\phi(l)} = I+B$, where $B = \sum_{h=0}^{\phi(l)-1}(e+a'_{ii})^h A' = (b_{qc})$. Thus

$$\begin{aligned} b_{ic} &= \sum_{h=0}^{\phi(l)-1} (e + a'_{ii})^h a'_{ic} \\ &= \left(\sum_{h=0}^{\phi(l)-1} \left(e + \sum_{k=0}^{d-2} (gp_{j_i i})^k a_{ii} \right)^h \right) \left(\sum_{k=0}^{d-2} (gp_{j_i i})^k a_{ic} \right) \end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{h=0}^{\phi(l)-1}\left(e+\sum_{k=0}^{d-2}(gp_{j_i i})^k a_{ii}\right)^h\right)\left(\left(-e+\left(e+\sum_{k=0}^{d-2}(gp_{j_i i})^k a_{ii}\right)\right)a_{ii}^{-1}a_{ic}\right)\\
&= \sum_{h=0}^{\phi(l)-1}\left(e+\sum_{k=0}^{d-2}(gp_{j_i i})^k a_{ii}\right)^{h+1} a_{ii}^{-1}a_{ic} - \sum_{h=0}^{\phi(l)-1}\left(e+\sum_{k=0}^{d-2}(gp_{j_i i})^k a_{ii}\right)^{h} a_{ii}^{-1}a_{ic}\\
&= \left(\left(e+\sum_{k=0}^{d-2}(gp_{j_i i})^k a_{ii}\right)^{\phi(l)} - e\right)a_{ii}^{-1}a_{ic}\\
&= \left(\left(\sum_{k=0}^{d-1}(gp_{j_i i})^k\right)^{\phi(l)} - e\right)p_{j_i i}^{-1}p_{j_i c},
\end{aligned}
$$

and $b_{qc} = 0$ for $q \neq i$. Therefore

$$(I+A')^{\phi(l)} = I + \left(\left(\sum_{k=0}^{d-1}(gp_{j_i i})^k\right)^{\phi(l)} - e\right)(p_{j_i i}^{-1})_{ij_i}P.$$

Now, by Corollary 2.3.1, A has order l, and thus

$$
\begin{aligned}
\hat{A} &= (p_{j_i i}^{-1})_{ij_i}P + \sum_{h=1}^{l-1}A^h\\
&= (p_{j_i i}^{-1})_{ij_i}P + \sum_{h=0}^{l-2}(gp_{j_i i})^h A\\
&= (p_{j_i i}^{-1})_{ij_i}P + \sum_{h=0}^{l-2}(gp_{j_i i})^h (g)_{ij_i}P\\
&= (p_{j_i i}^{-1})_{ij_i}P + \sum_{h=0}^{l-2}(gp_{j_i i})^h (gp_{j_i i})(p_{j_i i}^{-1})_{ij_i}P\\
&= \sum_{h=0}^{l-1}(gp_{j_i i})^h (p_{j_i i}^{-1})_{ij_i}P
\end{aligned}
$$

Hence by the previous and Corollary 2.3.1 again

$$
\begin{aligned}
u_{M_m(\mathbf{Q}G)}((g)_{ij_i}P, d) &= I + \left(\left((\sum_{h=0}^{d-1}(gp_{j_i i})^h)^{\phi(l)} - e\right) + \frac{1-d^{\phi(l)}}{l}\sum_{h=0}^{l-1}(gp_{j_i i})^h\right)(p_{j_i i}^{-1})_{ij_i}P\\
&= I + (u_{\mathbf{Z}G}(gp_{j_i i}, d) - e)\,(p_{j_i i}^{-1})_{ij_i}P.
\end{aligned}
$$

□

Remark: Recall that

$$u_{\mathbf{Z}_0T}\left((g)_{ij_i}, d\right)^{-1} = u_{\mathbf{Z}_0T}\left(\left((g)_{ij_i}\right)^d, q\right),$$

where $1 < q < l$, $(q, l) = 1$, and $dq + kl = 1$. Hence we obtain that

$$\begin{aligned} & f_P\left(u_{\mathbf{Z}_0T}((g)_{ij_i}, d)\right)^{-1} \\ & \qquad = u_{M_m(\mathbf{Z}G)}\left(\left((g)_{ij_i}\right)P, d\right)^{-1} \\ & \qquad = u_{M_m(\mathbf{Z}G)}\left(\left((g)_{ij_i}P\right)^d, q\right) \\ & \qquad = u_{M_m(\mathbf{Z}G)}\left(\left((g)_{ij_i}\right)^d P, q\right) \\ & \qquad = I + C \end{aligned}$$

where $C = (v - e)(p_{j_i i}^{-1})_{ij_i}P$, and $v = u_{\mathbf{Z}G}((gp_{j_i i})^d, q) = u^{-1}$, with u as in the Lemma 2.3.2.

We now give a series of three lemmas to show that the projection on a simple component of the group generated by the Bass cyclic units and bicyclic units contains a "nice" set of diagonal matrices.

Lemma 2.3.3 *Let G be a finite group and let n be a positive integer. There exists a positive number r such that for any $u \in \mathcal{U}(\mathbf{Z}G)$ and any positive integer v:*

$$\sum_{i=0}^{vr-1} \bar{u}^i = \bar{0},$$

where u and $\bar{0}$ denote the images of u and 0 under the natural map from $\mathbf{Z}G$ to $\mathbf{Z}_nG$. We denote the smallest such number r by $b(G, n)$.

Proof. Let $u \in \mathcal{U}(\mathbf{Z}G)$ and let v be a positive integer. Since $|\mathcal{U}(\mathbf{Z}_n(G))| = d < \infty$ we obtain that $\bar{u}^d = \bar{1}$. Thus

$$\sum_{i=0}^{nvd-1} \bar{u}^i = \sum_{i=0}^{d-1} \bar{u}^i(\bar{1} + \bar{u}^d + \cdots + \bar{u}^{(vn-1)d}) = \sum_{i=0}^{d-1} u^i vn = 0.$$

Taking $r = nd$, the result follows. □

Lemma 2.3.4 *Let $P_T = \{I + gPsP(I - gP) \mid s, g \in T, g^2 = g\}$. Then the group $< P_T >$ generated by P_T contains the following elements:*

$$\{I + gP\alpha(I - gP) \mid \alpha \in f_P(\eta(\mathbf{Z}_0T))\},$$

where $\eta(\mathbf{Z}_0T) = \mathcal{M}(\mathbf{Z}G; m, m; P)$.

Proof. Note that $(gP)^2 = gP$. Hence, for any $k, l \in \mathbf{Z}; s, s' \in T$,

$$(I + gPsP(I - gP))^k(I + gPs'P(I - gP))^l$$

$$= (I + gPksP(I - gP))(I + gPls'P(I - gP))$$

$$= I + gP(ks + ls')P(I - gP).$$

Hence the result follows. □

Throughout we denote by $E_{ij}, 1 \leq i, j \leq m$, the classical matrix units of $M_m(\mathbf{Z}G)$.

Lemma 2.3.5 *Let $(g)_{ij_i} \in G_{ij_i}$ be an element of order l, and let d be an integer with $1 < d < l$, $(d, l) = 1$. Let $V = f_P(u_{\mathbf{Z}_0T}((g)_{ij_i}, d))$, $u = u_{\mathbf{Z}G}(gp_{j_i i}, d)$, and $t = (p_{j_i i}^{-1})_{ij_i}$. Then, for any positive integer r, V^r has a decomposition $V^r = D^r F$, with*

$$D^r = I + (u^r - e)E_{ii},$$

and

$$F = I + tP(u^{-r} - e)E_{ii}(I - tP).$$

Furthermore, if r is a multiple of $b(G, m(P))$, where $m(P)$ is a positive integer such that $m(P)P^{-1} \in M_m(\mathbf{Z}G)$ (such an element always exists), then $F \in < P_T >$, where P_T is as defined in Lemma 2.3.4.

Proof. By Lemma 2.3.2, $V = I + B$, where

$$B = (b_{qc}) = (u - e)(p^{-1}_{j,i})_{ij_i} P.$$

Note that $b_{ii} = (u - e)$. So by Lemma 2.3.1,

$$V^r = (I + B)^r = I + \sum_{h=0}^{r-1} (e + (u - e))^h B$$

$$= I + \sum_{h=0}^{r-1} u^h B = I + \sum_{h=0}^{r-1} u^h (u - e)tP = I + (u^r - e)tP.$$

Let D^r and F be defined as in the statement of the theorem. Note that if r is a multiple of $b(G, m(P))$ then each integral coefficient of $(u^{-r} - e) = (u^{-1} - e)((u^{-1})^{r-1} + \ldots + u^{-1} + e)$ is a multiple of $m(P)$ by Lemma 2.3.3. Hence $\beta = (u^{-r} - e)E_{ii}P^{-1}$ is a matrix with entries in $\mathbf{Z}G$, and thus $(u^{-r} - e)E_{ii} = \beta P$ with $\beta \in \eta(\mathbf{Z}_0 T) = \mathcal{M}(\mathbf{Z}G; m, m; P)$. Therefore, $F \in \langle P_T \rangle$ by Lemma 2.3.4.

Finally, we check that $D^r F$ is really a decomposition of V^r as claimed. Since

$$\begin{aligned} F &= I + tP(u^{-r} - e)E_{ii}(I - tP) \\ &= I + tPE_{ii}(u^{-r} - e)(E_{ii} - tP) \\ &= I + E_{ii}(u^{-r} - e)(E_{ii} - tP) \\ &= I + (u^{-r} - e)(E_{ii} - tP). \end{aligned}$$

We obtain indeed that

$$\begin{aligned} D^rF &= I+(u^r-e)E_{ii}+(u^{-r}-e)(E_{ii}-tP)+(u^r-e)E_{ii}(u^{-r}-e)(E_{ii}-tP) \\ &= I+[(u^r-e)+(u^{-r}-e)+(u^r-e)(u^{-r}-e)]E_{ii} \\ &\quad -[(u^{-r}-e)+(u^r-e)(u^{-r}-e)]tP \\ &= I+(u^r-e)tP=V^r \end{aligned}$$

This finishes the proof. □

Lemma 2.3.6 *With notations as in Lemma 2.3.5, let r be a multiple of $b(G,m(P))$, where $m(P)$ is such that $m(P)P^{-1}\in M_m(\mathbf{Z}G)$. Then the group generated by $f_P(B_T^0)$ and $<P_T>$ contains the subset*

$$D(P)=\{\sum_{i=1}^{m}u_{ii}^rE_{ii}\mid u_{ii}\in B_G, i=1,2,\dots,m\},$$

where B_G is the set of Bass cyclic units of $\mathbf{Z}G$ and B_T^0 the set of the natural images in $\mathbf{Z}_0T$ of the Bass cyclic units of $\mathbf{Z}T$.

Proof. Let r be as in the statement of the Lemma and let $V\in f_P(B_T^0)$. Because of Lemma 2.3.5, $D^r=V^rF^{-1}\in<f_P(B_T^0),P_T>$. Hence, as $\sum_{i=1}^{m}u_{ii}^rE_{ii}$ (with each $u_{ii}\in B_G$) is a product of m such D^r's, the result follows. □

In the remainder of this section, we show that the group generated by B_T^0 and the images in $\mathbf{Z}_0T$ of bicyclic units of $\mathbf{Z}T$ is a subgroup of finite index in the unit group of the ring $\mathbf{Z}_0T+\mathbf{Z}f$, where f is the identity of $\mathbf{Q}_0T$.

First we need to introduce some more notations. Since $\mathbf{Q}G$ is semisimple, write

$$\mathbf{Q}G=\bigoplus_{j=1}^{t}\mathbf{Q}Ge_j,$$

where each e_j is a primitive central idempotent of $\mathbf{Q}G$, $j = 1, 2, \cdots, t$. Let $\mathbf{Q}Ge_j = M_{n_j}(D_j)$, D_j is a division ring, $j = 1, 2, \ldots, t$. Then

$$M_m(\mathbf{Q}G) = \bigoplus_{j=1}^{t} M_{mn_j}(D_j) = \bigoplus_{j=1}^{t} M_m(\mathbf{Q}G)f_j,$$

where $f_j = e_j I_m$ is a primitive central idempotent of $M_m(\mathbf{Q}G)$, $M_m(\mathbf{Q}G)f_j = M_{mn_j}(D_j)$, $j = 1, 2, \cdots, t$. Furthermore, let

$$\Lambda = \bigoplus_{j=1}^{t} \Lambda_j$$

where Λ_j is a maximal $\mathbf{Z}$-order in $M_m(\mathbf{Q}G)f_j$ containing $M_m(\mathbf{Z}G)f_j$. Let $\mathcal{O}_j$ be some maximal $\mathbf{Z}$-order in D_j, $j = 1, 2, \ldots, t$. Then $M_{mn_j}(\mathcal{O}_j)$ is a second maximal order in $M_m(\mathbf{Q}G)f_j$. We will write GL_j for $GL(mn_j, \mathcal{O}_j)$, its group of units, and SL_j for $SL(mn_j, \mathcal{O}_j)$. We will several times abuse notations by identifying in the natural way SL_j with a subgroup of $\mathcal{U}(\oplus_j M_{mn_j}(\mathcal{O}_j))$.

Proposition 2.3.1 *The centre $Z(\mathcal{U}(\mathbf{Z}G))$ of $\mathcal{U}(\mathbf{Z}G)$ is finitely generated.*

Proof. Let K_j be the centre of D_j which is an algebraic number field whose ring of integers we denote by $\mathcal{O}_j$. Then $\mathcal{O}_j$ is an order in K_j, and $\prod_j \mathcal{O}_j$ is an order in $\prod_j K_j$. First by [18, Proposition 1.10, p.14], the centre $Z(\mathbf{Z}G)$ is an order in $Z(\mathbf{Q}G)$. Since $Z(\mathbf{Q}G) = \prod_j Z(\mathbf{Q}Ge_j) = \prod_j Z(M_{n_j}(D_j)) \cong \prod_j K_j$, $[\mathcal{U}(Z(\mathbf{Z}G)) : \mathcal{U}((\prod_j \mathcal{O}_j) \cap Z(\mathbf{Z}G))] < \infty$ and $[\mathcal{U}(\prod_j \mathcal{O}_j) : \mathcal{U}((\prod_j \mathcal{O}_j) \cap Z(\mathbf{Z}G))] < \infty$ from Lemma 1.4.2. By the Dirichlet's unit theorem (see for example [18, Proposition 2.11, p.5]), $\mathcal{U}(\prod_j \mathcal{O}_j)$ is finitely generated, and thus $\mathcal{U}((\prod_j \mathcal{O}_j) \cap Z(\mathbf{Z}G))$ is a finitely generated Abelian group. It follows that $\mathcal{U}(Z(\mathbf{Z}G)) = Z(\mathcal{U}(\mathbf{Z}G))$ is finitely generated. □

Lemma 2.3.7 *Let J be a subgroup of $\mathcal{U}(M_m(\mathbf{Z}G))$ which contains a subgroup $\prod_{j=1}^{t} J_j$, where J_j is a subgroup of finite index in SL_j, $j = 1, 2, \cdots, t$. Then the group $\langle f_P(B_T^0), J, P_T \rangle$ contains a subgroup of finite index in the centre of $\mathcal{U}(M_m(\mathbf{Z}G))$.*

Proof. Let r be a multiple of $b(G, m(P))$, and let w denote the natural map from $\mathcal{U}(\mathbf{Z}G)$ to $K_1(\mathbf{Z}G)[2]$. Further, denote by π_j the projection of $\mathbf{Q}G$ onto $\mathbf{Q}Ge_j = M_{n_j}(D_j)$, $j = 1, 2, \ldots, t$. It is well known that the group generated by $w(B_G)$ is of finite index in $K_1(\mathbf{Z}G)$ [2].

Clearly

$$Z = Z(\mathcal{U}(M_m(\mathbf{Z}G))) = \mathcal{U}(Z(M_m(\mathbf{Z}G))) = \{\sum_{i=1}^{m} zE_{ii} \mid z \in Z(\mathcal{U}(\mathbf{Z}G))\}.$$

Write $\bar{z} = \sum_{i=1}^{m} zE_{ii} = zI_m \in Z$. Since $[\mathcal{U}(\mathbf{Z}G) : \mathcal{U}(\mathbf{Z}G \cap \prod M_{n_j}(\mathcal{O}_j))] = l < \infty$ from Lemma 1.4.2, $z^l \in \mathcal{U}(\mathbf{Z}G \cap \prod M_{n_j}(\mathcal{O}_j))$, for all $z \in Z(\mathcal{U}(\mathbf{Z}G))$. So there exists a positive integer k (k is independent of z, for example, choosing the index of $w(\langle B_G \rangle)$ in $K_1(\mathbf{Z}G)$) such that $w(z^{lk}) = w(b_z) \in w(\langle B_G \rangle)$, where $b_z \in \langle B_G \rangle$, that is $w(z^{lk}b_z^{-1}) = 1$. This means that a suitable matrix

$$\begin{bmatrix} z^{lk}b_z^{-1} & & & & \\ & 1 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & 1 \end{bmatrix}$$

is a commutator. Therefore, $\pi_j(z^{lk}b_z^{-1}) \in M_{n_j}(\mathcal{O}_j)$ and $\pi_j(z^{lk}b_z^{-1})$ as well as $\pi_j(z^{rlk}b_z^{-r})I_m$ have reduced norm one. So, by the assumptions, there exists a natural number v (independent on z) such that $\pi_j(z^{rlkv}b_z^{-rv})I_m \in J_j$, $j = 1, 2, \ldots, t$. Note that since $K_1(\mathbf{Z}G)$ is abelian, we may assume that b_z^{rv} is a product of rv-th powers of Bass cyclic units. Because of Lemma 2.3.6 $\bar{b}_z^{\,rv} = b_z^{rv} I_m \in \langle f_P(B_T^0), P_T \rangle$. Hence

$$\bar{z}^{rlkv} \bar{b}_z^{\,-rv} = \sum_{j=1}^{t} \pi_j (z^{rlkv} b_z^{-rv}) I_m \in \prod_{j=1}^{t} J_j \subseteq J$$

Therefore $z^{rlkv} \in \langle f_P(B_T^0), P_T, J \rangle$. Then the result follows since $rlkv$ is a constant and Z is finitely generated. □

Lemma 2.3.8 *Under the assumptions of Lemma 2.3.7*

$$\langle f_P(B_T^0), P_T, J \rangle$$

is of finite index in $\mathcal{U}(M_m(\mathbf{Z}G))$.

Proof. Since $I = \sum f_j$, $\Lambda = \bigoplus \Lambda_j$, and $M_m(\mathbf{Z}G) f_j \subseteq \Lambda_j$,

$$M_m(\mathbf{Z}G) \subseteq \sum M_m(\mathbf{Z}G) f_j \subseteq \sum \Lambda_j = \Lambda.$$

Then by Lemma 1.4.2, $[\mathcal{U}(\Lambda) : \mathcal{U}\left(M_m(\mathbf{Z}G)\right)] < \infty$. It is easy to check

$$Z\left(\mathcal{U}(\Lambda)\right) \cap \mathcal{U}\left(M_m(\mathbf{Z}G)\right) = Z\left(\mathcal{U}\left(M_m(\mathbf{Z}G)\right)\right).$$

Hence

$$[Z\left(\mathcal{U}(\Lambda)\right) : Z\left(\mathcal{U}\left(M_m(\mathbf{Z}G)\right)\right)] < \infty.$$

Lemma 2.3.7 yields that $\langle f_P(B_T^0), P_T, J \rangle$ contains a subgroup V such that $[Z\left(\mathcal{U}\left(M_m(\mathbf{Z}G)\right)\right) : V] < \infty$. So $[Z\left(\mathcal{U}(\Lambda)\right) : V] < \infty$. Furthermore, since $Z\left(\mathcal{U}(\Lambda)\right) = \prod Z\left(\mathcal{U}(\Lambda_j)\right)$, we obtain $[Z\left(\mathcal{U}(\Lambda_j)\right) : V \cap Z\left(\mathcal{U}(\Lambda_j)\right)] < \infty$. Now $V \supseteq \prod V \cap Z(\mathcal{U}(\Lambda_j))$, so it follows that $\langle f_P(B_T^0), P_T, J \rangle$ contains a subgroup $K = \prod K_j$, where each $K_j = V \cap Z(\mathcal{U}(\Lambda_j)) \cap Z(GL_j)$ is of finite index in $Z(GL_j)$.

Clearly, K_jJ_j is of finite index in GL_j and thus $\langle f_P(B^0_T), P_T, J\rangle$ contains a subgroup of finite index in the unit group of the order $\prod M_{mn_j}(\mathcal{O}_j)$. Hence it also contains a subgroup of finite index in $\mathcal{U}(\Lambda)$. Since $\langle f_P(B^0_T), P_T, J\rangle \subseteq \mathcal{U}(M_m(\mathbf{Z}G)) \subseteq \mathcal{U}(\Lambda)$ the result follows. □

Next, we construct a finite set of generators for a group J with the properties as in Lemma 2.3.7.

Lemma 2.3.9 *Let t be a nonzero idempotent in T (recall that $1 < m$). Then tPf_j is a non-central idempotent of $M_m(\mathbf{Q}G)f_j = M_m(\mathbf{Q}Ge_j)$, for $j = 1, 2, \ldots, t$.*

Proof. For the sake of simplicity and convenience, we may assume that $t = (e)_{11}$ (see for example [4, Corollary 3.12, page 106]). Now $Z(M_m(\mathbf{Q}Ge_j)) = \{\sum_{i=1}^{m} cE_{ii} \mid c \in Z(\mathbf{Q}Ge_j)\}$. It follows that $(e)_{11}Pf_j = eE_{11}\sum_{k,l} p_{kl}e_jE_{kl} = \sum_{l=1}^{m} p_{1l}e_jE_{1l} = ee_jE_{11} + \sum_{l=2}^{m} p_{1l}e_jE_{1l} \neq 0$, and $(e)_{11}Pf_j \notin Z(M_m(\mathbf{Q}G))$ since $m > 1$. Hence the result follows. □

Lemma 2.3.10 *Assume that $m > 2$ and let t be a nonzero idempotent in T. Let $J_{tP} \subseteq M_m(\mathbf{Z}G)$ be the group generated by the elements:*

$$I + tPsP(I - tP)$$

and

$$I + (I - tP)sPtP,$$

where $s \in T$. Then J_{tP} contains a subgroup of finite index in $SL_j = SL(mn_j, \mathcal{O}_j)$, $j = 1, 2, \ldots, t$.

Proof. By Lemma 2.3.9, tPf_j is a non-central idempotent of $M_m(\mathbf{Q}G)f_j$. Therefore the result is proved as in Proposition 3.2 in [11]. □

Note that the assumption $m > 2$ ensures that the assumptions of Proposition 3.2 in [11] are satisfied; in particular, one can make use of the congruence theorems.

Proposition 2.3.2 *Assume that* $m > 2$. *Then the group generated by* B_T^0 *and*

$$\{f + ts(f - t), f + (f - t)st \mid s, t \in T, \text{ and } t^2 = t \neq \theta_T\}$$

is of finite index in the unit group of the ring $\mathbf{Z}_0T + \mathbf{Z}f$, *where* f *is the identity of* $\mathbf{Q}_0T$.

Proof. From Lemma 2.3.8 and Lemma 2.3.10, it follows that the group generated by $f_P(B_T^0)$ and the units $I + tPsP(I - tP)$ and $I + (I - tP)sPtP$, $t = t^2 \neq \theta_T$, $s \in T$, is a subgroup of finite index in the unit group of $M_m(\mathbf{Z}G)$, and hence in $\sum_{s \in T} \mathbf{Z}sP + \mathbf{Z}I_m$. So the result follows from Lemma 1.3.1. □

2.4 The Main Theorem

We are now in a position to prove our main result. Recall that S is a finite semigroup such that $\mathbf{Q}S$ is a semisimple ring and such that $\mathbf{Z}S$ contains an identity $\mathbf{1}$.

Before the proof of the main theorem, we need the following fact in group theory.

Lemma 2.4.1 *Let* A_i, $1 \leq i \leq n$, *be groups with identities* e_i, *and* $\mathcal{U}_i$, $1 \leq i \leq n$ *be subgroups of the product* $A = \prod_{i=1}^{n} A_i$ *such that, for each* i, $\pi_i(\mathcal{U}_i)$ *is a finite index subgroup of* A_i *and* $\pi_j(\mathcal{U}_i) = e_i$ *for* $j < i$, *where* π_i *is the natural projection of* A *onto* A_i. *Then, the group generated by* $\bigcup_i \mathcal{U}_i$ *is a finite index subgroup of* A.

Proof. We prove the Lemma by induction on n. It is clear for $n = 1$. Now assume that the Lemma is true for n $(1 \leq n)$. Thus if $A = \prod_{i=1}^{n+1} A_i$, then $A = (\prod_{i=1}^{n} A_i) \times A_{n+1} = C \times A_{n+1}$ with $C = \prod_{i=1}^{n} A_i$. Let $\pi_C : A \to C$ be the natural projection. The group generated by $\pi_C(\bigcup_{i=1}^{n} \mathcal{U}_i)$ is a finite index subgroup of C because we can apply the induction hypothesis to the groups $\pi_C(\mathcal{U}_i)$, $1 \leq i \leq n$. Therefore, it is sufficient to prove the Lemma in case $n = 2$. So let $A = A_1 \times A_2$, and write $A_1 = \cup_q \pi_1(\mathcal{U}_1)a_{1q}$ and $A_2 = \cup_k \pi_2(\mathcal{U}_2)a_{2k}$, each a disjoint union of finitely many cosets. Then we claim that $A = \cup_{q,k}\langle \mathcal{U}_1, \mathcal{U}_2\rangle(a_{1q}, a_{2k})$, where $\langle \mathcal{U}_1, \mathcal{U}_2\rangle$ denotes the group generated by $\mathcal{U}_1$ and $\mathcal{U}_2$. Indeed, for any $(a_1, a_2) \in A$, write $a_1 = \pi_1(u_1)a_{1q}, a_2 = \pi_2(u_2)a_{2k}$, for some $u_1 \in \mathcal{U}_1, u_2 \in \mathcal{U}_2$. By assumption $\pi_1(\mathcal{U}_2) = 1$. Hence $(a_1, a_2) = (\pi_1(u_2u_1)a_{1q}, \pi_2(u_2u_1u_1^{-1})a_{2k}) = u_2u_1(a_{1q}, \pi_2(u_1^{-1})a_{2k})$. But $\pi_2(u_1^{-1})a_{2k} \in A_2$, so it can be written as $\pi_2(u_2^{'})a_{2k'}$ for some $u_2^{'} \in \mathcal{U}_2$. Thus

$$(a_1, a_2) = u_2u_1\left(\pi_1(u_2^{'})a_{1q}, \pi_2(u_2^{'})a_{2k'}\right) = u_2u_1u_2^{'}(a_{1q}, a_{2k'}).$$

This shows the claim, and hence the result follows. □

Theorem 2.4.1 *Assume that if S^0 has a principal factor*

$$S_i/S_{i+1} \cong \mathcal{M}^0(G_i; m_i, m_i; P_i)$$

with $m_i = 1$ then G_i does not have a non-abelian homomorphic image which is fixed point free. Further suppose $\mathbf{Q}S$ does not have simple components of the following type:

(i) a non-commutative division algebra other than a totally definite quaternion algebra;

(ii) a 2×2 matrix ring over the rationals;

(iii) a 2×2 matrix ring over a quadratic imaginary extension of the rationals;

(iv) a 2×2 matrix ring over a non-commutative division algebra.

Then the group generated by the following elements is of finite index in $\mathcal{U}(\mathbf{Z}S)$:

(i) the Bass cyclic units B_S of $\mathbf{Z}S$;

(ii) the bicyclic units $\{1+\hat{g}s(1-g), 1+(1-g)s\hat{g} \mid s \in S, g \in GR(S)\}$.

Proof. Note that if S does not have a zero element, then $\mathbf{Z}S^0 \cong \mathbf{Z}S \oplus \mathbf{Z}\theta_S$ (a direct product of rings). Hence to prove the result we may assume that S has a zero element θ_S.

We know that

$$\mathbf{Q}S \cong^{\psi} \oplus_{i=0}^{n} \mathbf{Q}_0(S_i/S_{i+1}) \oplus \mathbf{Q}\theta_S.$$

Further let π_i denote the projection of the latter ring onto the i-th summand. Let f_i be the identity of $\mathbf{Q}_0(S_i/S_{i+1})$. Then

$$\psi(\mathbf{Z}S) \subseteq (\oplus_{i=0}^{n} \mathbf{Z}_0(S_i/S_{i+1}) + \mathbf{Z}f_i) \oplus \mathbf{Z}\theta_S.$$

Let $\mathcal{U}_i$ be the subgroup of $\mathcal{U}(\mathbf{Z}S)$ generated by B_{S_i} and $\{1+\hat{g}s(1-g), 1+(1-g)s\hat{g} \mid s \in S_i, g \in GR(S_i)\}$. Then, in case $m_i \geq 3$, from Proposition 2.3.2 it follows that $\pi_i(\psi(\mathcal{U}_i))$ is of finite index in $\mathcal{U}\left(\mathbf{Z}_0(S_i/S_{i+1}) + \mathbf{Z}f_i\right)$. In case $m_i = 1$, the same holds because of the results in [11] (note that $\pi_i(\psi(\mathbf{Z}S))$ is a group ring). Finally note that for each i and $u_i \in \mathcal{U}_i$, $\pi_j(\psi(u_i)) = f_j$ for $j < i$. By Lemma 2.4.1, the group generated by $\psi(\bigcup_i \mathcal{U}_i)$ is of finite index in $\mathcal{U}\left(\oplus_i(\mathbf{Z}_0(S_i/S_{i+1}) + \mathbf{Z}f_i) \oplus \mathbf{Z}\theta_S\right)$. Hence the result follows. □

It is worth mentioning that recently Jespers and Leal in [12] described precisely when a simple component of the rational group algebra $\mathbf{Q}G$ of a finite nilpotent group is of the exceptional type mentioned in Theorem 2.4.1. As an immediate consequence one can also classify when an exceptional simple component occurs in semisimple Artinian rational semigroup algebras of finite nilpotent semigroups.

Recall that a semigroup S is said to be *nilpotent of class* n, a notion introduced by Malcev [20] (see also [17]), if S satisfies the identity $X_n = Y_n$ and n is the least positive integer with this property. Here we say the identity $X_n = Y_n$ is satisfied in S if $x_n = y_n$ for all $x, y \in S$ and $w_1, w_2, \ldots \in S$ with the following definitions of x_n and y_n:

$$x_0 = x, \ \ y_0 = y,$$

and, for $0 \leq n$,

$$x_{n+1} = x_n w_{n+1} y_n, \ \ y_{n+1} = y_n w_{n+1} x_n.$$

By [17, Lemma 2.1, p.986], $S = \mathcal{M}^0(G; m, m; P)$ is nilpotent if and only if G is nilpotent and S is an inverse semigroup. Furthermore, if S is a nilpotent semigroup (not necessarily completely 0-simple), then any subsemigroup of S itself is a nilpotent semigroup.

Before we state our result, we need some notations of [12].

$\mathcal{Q}_{2m} = \langle g, h \mid g^m = 1, h^2 = g^{m/2}, hgh^{-1} = g^{-1} \rangle$, $m > 2, 2|m$, the quaternion group of order $2m$,

$\mathbf{H}(F)$, *the quaternion algebra over a field* F,

ξ_n, *a primitive* $n-th$ *root of unity*,

$C_n = \langle g \mid g^n = 1 \rangle$, *cyclic group of order* n,

$\mathcal{D}_{2m} = \langle g, h \mid g^m = 1, h^2 = 1, hgh^{-1} = g^{-1} \rangle$, $m > 2$, *the dihedral group of order* $2m$,

$\mathcal{S}_{2^{m+1}} = \langle g, h \mid g^{2^m} = 1, h^2 = 1, hgh^{-1} = g^{-1+2^{m-1}} \rangle$, $3 \leq m$,

$\mathcal{D} = \langle a, b, c \mid a^2 = b^2 = c^4 = 1, ac = ca, bc = cb, ba = c^2ab \rangle$,

$\mathcal{D}^+ = \langle a, b, c \mid a^4 = 1, b^2 = 1, c^4 = 1, ac = ca, cb = bc, ba = ca^3b \rangle$,

$\mathcal{D}^+_{16} = \langle a, b \mid a^8 = b^2 = 1, ba = a^5b \rangle$,

$\mathcal{D}^-_{16} = \mathcal{S}_{16}$,

$G \mathcal{Y} H$, the central product of groups G and H with some central subgroups identified (cf. [38, 4.16]), but it will be clear from the context which central groups these are.

Now, corresponding to Theorems 2.2 and 2.3 of [12], we have

Theorem 2.4.2 *Let S be a finite nilpotent semigroup such that $\mathbf{Q}S$ is a semisimple Artinian ring. Further, let*

$$S^0 = S_0 \supset S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \{\theta_S\}$$

be a principal series of $S^0 = S \cup \{\theta\}$, and $S_i/S_{i+1} \cong \mathcal{M}^0(G_i; m_i, m_i; P_i)$, G_i a group, $P_i^{-1} \in M_{m_i}(\mathbf{Q}G_i)$, $i = 0, 1, \ldots, n$,

$$\mathbf{Q}S^0 \cong \bigoplus_{i=0}^{n} M_{m_i}(\mathbf{Q}G_i) \oplus \mathbf{Q}\theta_S.$$

Finally, let e be a primitive central idempotent of $\mathbf{Q}S$.

(i) *If $\mathbf{Q}Se$ is a noncommutative division ring, then there exists some $m_i = 1$, and there exists a primitive central idempotent e_i in $\mathbf{Q}G_i$ such that if G_ie_i is a 2-group, $G_i/G_ie_i \cong \mathcal{Q}_{2^n}$, $3 \leq n$, and $\mathbf{Q}Se \cong \mathbf{Q}G_ie_i \cong \mathbf{H}(\mathbf{Q}(\xi_{2^n-1} + \xi_{2^n-1}^{-1}))$; If G_ie_i is not a 2-group, $G_i/G_ie_i \cong \mathcal{Q}_8 \times \mathcal{C}_n$, n odd, $\mathbf{Q}Se \cong \mathbf{Q}G_ie_i \cong \mathbf{H}(\mathbf{Q}(\xi_n))$, and the order of 2 modulo n is odd.*

(ii) *If* $\mathbf{Q}Se \cong M_2(F)$, *and* $dim_{\mathbf{Q}}(F) \leq 2$, F *a field, then there exists some* $m_i = 1$, *or* $m_i = 2$, *and there exists a primitive central idempotent* e_i *in* $\mathbf{Q}G_i$ *such that if* $m_i = 1$ *and* G_ie_i *is a 2-group, then one of the following situations occurs:*

- *(a)* $\mathbf{Q}G_ie_i \cong F = \mathbf{Q}$ *and* $G_i/G_ie_i \cong \mathcal{D}_8$;
- *(b)* $\mathbf{Q}G_ie_i \cong F = \mathbf{Q}(\sqrt{2})$ *and* $G_i/G_ie_i \cong \mathcal{D}_{16}$;
- *(c)* $\mathbf{Q}G_ie_i \cong F = \mathbf{Q}(\sqrt{-2})$ *and* $G_i/G_ie_i \cong \mathcal{D}_{16}^-$;
- *(d)* $\mathbf{Q}G_ie_i \cong F = \mathbf{Q}(i)$ *and* $G_i/G_ie_i \cong \mathcal{D}_{16}^+$, $\mathcal{D}$, *or* $\mathcal{D}^+$;

If $m_i = 1$ *and* G_ie_i *is not 2-group, then* $\mathbf{Q}G_ie_i \cong F = \mathbf{Q}(\xi_3)$ *and* $G_i/G_ie_i \cong \mathcal{D}_8 \times \mathcal{C}_3$, *or* $\mathcal{Q}_8 \times \mathcal{C}_3$; *Finally, if* $m_i = 2$, *then* $\mathbf{Q}G_ie_i \cong \mathbf{Q}(\xi_{q_i})$ *and* $G_ie_i \cong C_{q_i}$, *where* $q_i = 1, 2, 3, 4$ *or* 6.

(iii) *If* $\mathbf{Q}Se \cong M_2(D)$, *with* D *a noncommutative division ring, then there exists some* $m_i = 1$ *or* $m_i = 2$, *and there exists a primitive central idempotent* e_i *in* $\mathbf{Q}G_i$ *such that if* $m_i = 1$, *and* G_ie_i *is a 2-group, then* $\mathbf{Q}G_ie_i \cong D \cong \mathbf{H}(\mathbf{Q}(\xi_{2^{n-1}} + \xi_{2^{n-1}}^{-1}))$ *and one of the following situations occurs:*

- *(a)* $G_i/G_ie_i \cong \mathcal{D}_8 \ \mathcal{Y} \ \mathcal{Q}_{2^n}$;
- *(b)* $G_i/G_ie_i \cong H \cup Hg$ *where* H *is a normal subgroup of index 2 in* G_i/G_ie_i *such that* H *contains a non-trivial normal subgroup* N *with* $N \cap gNg^{-1} = \{1\}$ *and* $H/N \cong \mathcal{Q}_{2^n}$;

If $m_i = 1$ *and* G_ie_i *is not a 2-group, then* $\mathbf{Q}G_ie_i \cong D \cong \mathbf{H}(\mathbf{Q}(\xi_n))$ *and* $G_i/G_ie_i \cong \mathcal{S} \times \mathcal{C}_n$, n *an odd number such that the order of 2 modulo* n *is odd, and* $\mathcal{S}$ *is one of the following groups:*

(a) $\mathcal{D}_8 \; \mathcal{Y} \; \mathcal{Q}_8$;

(b) $(\mathcal{Q}_8 \times \mathcal{Q}_8) \rtimes \mathcal{C}_2$, *the semidirect product;*

(c) $\langle a, b, c, g \mid a^4 = b^4 = 1, ab = ba, c^2 = a^2b^2, cac^{-1} = a^{-1}, cbc^{-1} = b^{-1}, g^2 = 1, gag^{-1} = b, gbg^{-1} = a, gc = cg \rangle$;

(d) $\langle a, b, c, g \mid a^4 = b^4 = 1, ab = ba, c^2 = a^2b^2, gag^{-1} = b, gbg^{-1} = a^{-1}, g^2 = c \rangle$;

(e) $\langle a, b, c, g \mid a^2 = b^2, a^4 = 1, ba = a^3b, c^2 = 1, ca = ac, cb = bc, g^2 = 1, ga = ag, gbg^{-1} = cab, gcg^{-1} = a^2c \rangle$;

(f) $\langle a, b, c, g \mid a^2 = b^2, a^4 = 1, ba = a^3b, c^2 = 1, ca = ac, cb = bc, g^2 = a, gbg^{-1} = b^3c, gcg^{-1} = b^2c \rangle$;

(g) $\langle a, b, c, g \mid a^2 = b^2, a^4 = 1, ba = a^3b, c^2 = 1, ca = ac, cb = bc, g^2 = a, bg^{-1} = gb^3, gcg^{-1} = b^2c \rangle$

Finally, if $m_i = 2$ *and* G_ie_i *is a 2-group,* $G_i/G_ie_i \cong \mathcal{Q}_{2^n}$, $3 \leq n$, *and* $\mathbf{Q}Se \cong M_2(\mathbf{Q}G_ie_i) \cong M_2(\mathbf{H}(\mathbf{Q}(\xi_{2^{n-1}} + \xi_{2^{n-1}}^{-1})))$; *If* $m_i = 2$ *and* G_ie_i *is not a 2-group,* $G_i/G_ie_i \cong \mathcal{Q}_8 \times \mathcal{C}_n$, n *odd,* $\mathbf{Q}Se \cong M_2(\mathbf{Q}G_ie_i) \cong M_2(\mathbf{H}(\mathbf{Q}(\xi_n)))$, *and the order of* 2 *modulo* n *is odd.*

Proof: The results are very clear from Theorems 2.2 and 2.3 of [12] except the last part of (ii) with respect to the possibilities of q_i. Now if $QGe_i \cong F$ is a field, then the subgroup Ge_i of F is a cyclic group, say generated by ge_i and say of order q_i. Hence $\mathbf{Q}Ge_i$ is a cyclotomic extension of order q_i of $\mathbf{Q}$. Since F is of dimension at most 2 over $\mathbf{Q}$, $\phi(q_i) = 1$ or 2 (see for example [7, Proposition 8.3, p.299]). It is easy to see that $\phi(q_i) = 1$ implies $q_i = 1$ or 2 and that $\phi(q_i) = 2$ implies $q_i = 4$ or

6. Indeed, let $q_i = p_1^{x_1} p_2^{x_2} \ldots p_l^{x_l}$, where $p_j, 1 \leq j \leq l$, are different prime numbers with $p_1 < p_2 < \ldots < p_l$, and $x_j, 1 \leq j \leq l$, are non-negative integers. Then basic properties of the ϕ tell us that $\phi(q_i) = \prod_{1 \leq j \leq l} \phi(p_j^{x_j}) = \prod_{1 \leq j \leq l} (p_j^{x_j} - p_j^{x_j - 1})$. Clearly $\phi(q_i) = 1$ or 2 implies $l \leq 3$. If $l = 1, q_i = p_1^{x_1}$, then $\phi(q_i) = 1$ implies $x_1 = 0$ (i.e., $q_i = 1$) or $p_1 = 2, x_1 = 1$ (i.e., $q_i = 2$); $\phi(q_i) = 2$ implies $p_1 \leq 3$. If $p_1 = 2$ then $x_1 = 2$, so $q_i = 4$, while if $p_1 = 3$, then $x_1 = 1$, so $q_i = 3$. Similarly, one can check that if $l = 2$, $q_i = p_1^{x_1} p_2^{x_2}$, then $\phi(q_i) = 2$ implies $p_1 = 2$, $p_2 = 3$ and $x_1 = x_2 = 1$, i.e., $q_i = 6$. Finally, one also could check that if $l = 3$, $q_i = p_1^{x_1} p_2^{x_2} p_3^{x_3}$, and $x_1 \neq 0, x_2 \neq 0, x_3 \neq 0$ then $\phi(q_i) > 2$. Therefore, the possibilities of q_i are 1, 2, 3, 4, or 6. □

Chapter 3

Full Unit Groups: A Class of Examples

In the previous chapter, finitely many generators are constructed for a subgroup of finite index of $\mathcal{U}(\mathbf{Z}S)$ for a large class of finite semigroups with $\mathbf{Q}S$ semisimple Artinian. The problem to describe the full unit groups remains open. However we are able to describe these unit groups for concrete examples of finite semigroups S. In case $\mathbf{Z}S$ is the direct product of the contracted integral semigroup rings $\mathbf{Z}_0(S_i/S_{i+1})$ of the principal factors $S_i/S_{i+1} \cong \mathcal{M}^0(G_i; m_i, m_i; P_i)$ (that is the sandwich matrices P_i are invertible in $M_{m_i}(\mathbf{Z}G_i)$), then $\mathcal{U}(\mathbf{Z}S) \cong \prod GL(m_i, \mathbf{Z}G_i)$. Hence the problem is reduced to matrices over group rings. Now recently (see for example [10], [13], [14], [15], [16], [25]) the unit group $\mathcal{U}(\mathbf{Z}G)$ has been described for several classes of finite groups G. With the same methods one can also describe $GL(n, \mathbf{Z}G)$ for several concrete examples of groups G. More examples of full unit groups can be found in [1], [6], [18], [19], [21], [24], [28], [30], [33], [34].

In this chapter, we compute $\mathcal{U}(\mathbf{Z}S)$ for some examples of finite semigroups S. We do this for the "easiest" class of semigroups that does not fall in the above mentioned classes of examples. More specially, we consider the class of semigroups that are monoid extensions of elementary Rees matrix semigroups $\mathcal{M}^0(\{1\}; n, n; P)$; and we are interested in the case P is not invertible in $M_n(\mathbf{Z})$.

3.1 General Method

Let $S = \mathcal{M}^0(\{1\}; n, n; P)$ be an elementary Rees matrix semigroup and assume that sandwich matrix P is invertible in $M_n(\mathbf{Q})$. Put $T = S^1$. Clearly, $\mathbf{Z}T$ has an identity and, because of Lemma 1.3.1, $\mathbf{Q}S$ is semisimple Artinian.

Write

$$\mathbf{Q}T = \mathbf{Q}T\theta \oplus \mathbf{Q}T(\mathbf{1} - E) \oplus \mathbf{Q}T(E - \theta),$$

and note that

$$\mathbf{Z}T \subseteq \mathbf{Z}T\theta \oplus \mathbf{Z}T(\mathbf{1} - E) \oplus \mathbf{Z}T(E - \theta)$$

where E is the identity of $\mathbf{Q}S$. We denote $\mathbf{Z}T$, $\mathbf{Z}T\theta$, $\mathbf{Z}T(1 - E)$, $\mathbf{Z}T(E - \theta)$ by R, R_1, R_2, R_3, respectively, and denote the sum of R_1, R_2, R_3 by R'. So $R \subseteq R_1 \oplus R_2 \oplus R_3 = R'$. Since R and R' are $\mathbf{Z}-$*orders* of $\mathbf{Q}T$, we know, from Lemma 1.4.2, if $\alpha \in R$ and $\alpha \in \mathcal{U}(R')$, then $\alpha \in \mathcal{U}(R)$. In particular, $\alpha \in \mathcal{U}(R)$ if and only if $\alpha\theta \in \mathcal{U}(R_1)$, $\alpha(1 - E) \in \mathcal{U}(R_2)$, $\alpha(E - \theta) \in \mathcal{U}(R_3)$. For an element α of R, we have a close look at its decomposition in R'. Write

$$\alpha = l\mathbf{1} + m\theta + \sum_{i,j} n_{ij}(1)_{ij},$$

$l, m, n_{ij} \in \mathbf{Z}$, $i, j = 1, 2, \cdots, n$. Then,

$$\alpha = \alpha\theta + \alpha(\mathbf{1} - E) + \alpha(E - \theta),$$

where

$$\begin{aligned} \alpha 0 &= (l + m + \sum_{i,j} n_{ij})0, \\ \alpha(\mathbf{1} - E) &= \alpha - \alpha E \\ &= \alpha - lE - m0 - \sum_{i,j} n_{ij}(1)_{ij} \\ &= l(\mathbf{1} - E), \end{aligned}$$

and

$$\alpha(E - 0) = l(E - 0) + \sum_{i,j} n_{ij}(1)_{ij}(E - 0).$$

Further, we know that

$$\mathbf{Q}S = \mathbf{Q}0 \oplus \mathbf{Q}S(E - 0), \quad h(\mathbf{Q}S(E - 0)) = \mathbf{Q}_0 S$$

and

$$\mathbf{Q}_0 S \cong^{\eta} \mathcal{M}(\mathbf{Q}; n, n; P) \cong^{f_P} M_n(\mathbf{Q}),$$

where h is the natural homomorphism from $\mathbf{Q}S$ to $\mathbf{Q}_0 S$. Thus,

$$\begin{aligned} f_P(\eta(h(\alpha(E - 0)))) &= f_P\left(\eta\left(h(l(E - 0) + \sum_{i,j} n_{ij}(1)_{ij}(E - 0))\right)\right) \\ &= f_P(\eta(h(l(E - 0)))) + f_P\left(\eta\left(h(\sum_{i,j} n_{ij}(1)_{ij}(E - 0))\right)\right) \\ &= l f_P(\eta(h(E - 0)))) + f_P\left(\eta\left(h(\sum_{i,j} n_{ij}(1)_{ij}(E - 0))\right)\right) \\ &= lI + f_P\left(\eta\left(h(\sum_{i,j} n_{ij}(1)_{ij})h(E - 0)\right)\right) \\ &= lI + f_P\left(\eta\left(h(\sum_{i,j} n_{ij}(1)_{ij})\right)\right) f_P(\eta(h(E - 0))) \end{aligned}$$

$$
\begin{aligned}
&= lI + f_P\left(\eta\left(h(\sum_{i,j} n_{ij}(1)_{ij})\right)\right) \\
&= lI + \sum_{i,j} n_{ij}(1)_{ij}P \\
&= lI + (n_{ij})P = lI + AP
\end{aligned}
$$

where I is the identity of the full matrix ring $M_n(\mathbf{Z})$, and $A = (n_{ij}) \in M_n(\mathbf{Z})$. It follows that $\mathcal{U}(R_1) = \{\pm\theta\}$, $\mathcal{U}(R_2) = \{\pm(\mathbf{1} - E)\}$, and $\alpha \in \mathcal{U}(R)$ if and only if $l = \pm 1$, $l+m+\sum_{i,j} n_{ij} = \pm 1$, and $\pm I + AP \in \mathcal{W}$, where $\mathcal{W} = (\pm I + M_n(\mathbf{Z})P) \cap GL_n(\mathbf{Z})$. In particular, $\mathcal{W}$ is an image of the group $\mathcal{U}(R)$, and thus $\mathcal{W}$ itself is a group.

Let $\mathcal{V} = (I + M_n(\mathbf{Z})P) \cap GL_n(\mathbf{Z})$, and $\mathcal{V}_+ = (I + M_n(\mathbf{Z})P) \cap SL_n(\mathbf{Z})$. It is clear that $\mathcal{V}$ and $\mathcal{V}_+$ are groups since $\mathcal{W}$ is a group. Put $d_P = det\ P$, the determinant of P. Then $\mathcal{W} = \pm\mathcal{V}$, and $\mathcal{V}_+ \supseteq \Gamma(d_P) = \{u = I + d_P M_n(\mathbf{Z}) \mid det\ u = 1\}$ because $I + d_P M_n(\mathbf{Z}) = I + d_P M_n(\mathbf{Z})(P^{-1}P) = I + M_n(\mathbf{Z})(d_P P^{-1})P \subseteq I + M_n(\mathbf{Z})P$. So $\frac{\mathcal{V}_+}{\Gamma(d_P)} \subseteq \frac{SL_n(\mathbf{Z})}{\Gamma(d_P)} \cong SL_n(\mathbf{Z}_{d_P})$ [22, Theorem VII.6, p.109], where $\mathbf{Z}_{d_P} = \frac{\mathbf{Z}}{d_P\mathbf{Z}}$.

We first show the following.

Lemma 3.1.1 *Let* $\mathcal{U}_1(R) = \mathcal{U}(\{\mathbf{1} + m\theta + \sum_{i,j} n_{ij}(1)_{ij} \mid m, n_{ij} \in \mathbf{Z}, 1 \leq i,j \leq n\})$. *Then*

$$\frac{\mathcal{U}_1(R)}{\{\mathbf{1}, \mathbf{1} - 2\theta\}} \cong \mathcal{V}$$

Proof: From the above, we know that the map

$$\phi : \mathcal{U}_1(R) \to \mathcal{V} : \mathbf{1} + m\theta + \sum_{i,j} n_{ij}(1)_{ij} \to I + (n_{ij})P$$

is a group homomorphism. If $I + (n_{ij})P \in \mathcal{V}$, then with $m = -\sum_{i,j} n_{ij}$, $\alpha = \mathbf{1} + m\theta + \sum_{i,j} n_{ij}(1)_{ij} \in \mathcal{U}_1(R)$, $\phi(\alpha) = I + (n_{ij})P$. Thus ϕ is onto. We claim that

$\ker \phi = \{\mathbf{1}, \mathbf{1} - 2\theta\}$. Indeed, let $\phi(\alpha) = 1$, then $n_{ij} = 0, i, j = 1, 2, \ldots, n$, and thus $\alpha = \mathbf{1} + m\theta$. Further, $\alpha \in \mathcal{U}_1(R)$ implies that $m = \pm 1 - 1 = 0$ *or* -2. □

Note that since $\Gamma(d_P) \subseteq \mathcal{V}_+$, the group $\mathcal{V}_+$ is of finite index in $SL_n(\mathbf{Z})$. Let $\{y_1, \cdots, y_r\}$ be a transversal for $\mathcal{V}_+$ in $SL_n(\mathbf{Z})$.

We need the following two theorems to carry on our discussion. A proof for the first one can be found in [22, Theorem VII.7, p.24].

Theorem 3.1.1 *If R is a Euclidean ring which is not of characteristic 2, then $SL_n(R)$ is generated by*

$$x_1 = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ (-1)^{n-1} & 0 & 0 & \cdots & 0 \end{bmatrix}$$

and

$$x_2(u) = \begin{bmatrix} 1 & u & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix},$$

where $u \in R$. In particular, $SL_n(\mathbf{Z})$ is generated by $x_1, x_2 = x_2(1)$.

The next theorem is well known. Since it is essential for our further calculations, we include a proof (taken from [27, Lemma 1.7, p.117]).

Theorem 3.1.2 *Let G be a group generated by $x_1, x_2, \ldots, x_t$, and let H be a subgroup of finite index with right transversal $\{y_1, y_2, \ldots, y_m\}$ in G. Then H is generated by* *the elements h_{ij}, $1 \leq j \leq m$, $1 \leq i \leq t$, which are such that $y_jx_i = h_{ij}y_{j'}$, for some $j' \in \{1, 2, \ldots, m\}$.*

Proof. For fixed i, right multiplication by x_i permutes the right cosets of H , and we have $Hy_jx_i = Hy_{j'}$ for some $j' \in \{1, 2, \ldots, m\}$ depending on i, j. Hence there exists $h_{ij} \in H$ with $y_jx_i = h_{ij}y_{j'}$. Let $H_0 = \langle h_{ij} \mid j = 1, 2, \ldots, m; i = 1, 2, \ldots, t\rangle$. We show that $H = H_0$.

Set $C = \cup_1^m H_0y_j$. Then for each fixed i

$$Cx_i = \cup_1^m H_0y_jx_i = \cup_1^m H_0h_{ij}y_{j'} = \cup_1^m H_0y_{j'}$$

because $h_{ij} \in H_0$. Thus $Cx_i = C$, because for fixed i, the map $j \to j'$ is a permutation of the subscripts. Now $G = \langle x_1, x_2, \ldots, x_t\rangle$ yields $CG = C$, and hence because $C \neq \emptyset$, we have $C = G$. Suppose, finally, that y_1 is the unique coset representative contained in H. Then H is disjoint from all H_0y_j for $j \neq 1$ and $H \subseteq G = \cup_1^m H_0y_j$ so that $H \subseteq H_0y_1$. This yields $H = H_0$. □

We now apply the previous theorem to the subgroup $\mathcal{V}_+$ of $SL_n(\mathbf{Z})$. It follows that $\mathcal{V}_+ = \langle u_{ij} \mid i = 1, 2; j = 1, 2, \cdots, r\rangle$, where $u_{ij} \in \mathcal{V}_+$ is such that $y_jx_i = u_{ij}y_{j'}$, for some $j' \in \{1, 2, \cdots, r\}$, for $i = 1, 2; j = 1, 2, \cdots, r$.

Since $[GL_n(\mathbf{Z}) : SL_n(\mathbf{Z})] = 2$, $[\mathcal{V} : \mathcal{V}_+] \leq 2$. Let $\frac{\mathcal{V}}{\mathcal{V}_+} = \{\mathcal{V}_+, z\mathcal{V}_+\}$, where z is the identity of $\mathcal{V}$ if $[\mathcal{V} : \mathcal{V}_+] = 1$; otherwise, choose $z \in \mathcal{V}$, and $z \notin \mathcal{V}_+$. Then $\mathcal{V} = \langle u_{ij}, z \mid i = 1, 2; j = 1, 2, \cdots, r\rangle$. Write $z = I + (n_{kl}^0)P$, and $u_{ij} = I + (n_{kl}^{ij})P$, *i.e* $(n_{kl}^{ij}) = (u_{ij} - I)P^{-1}$, $i = 1, 2$; $j = 1, 2, \cdots, r$. Let

$$m_{ij} = \pm 1 - 1 - \sum_{k,l} n_{kl}^{ij}, \quad m_0 = \pm 1 - 1 - \sum_{k,l} n_{kl}^0,$$

and let

$$U_{ij} = \mathbf{1} + m_{ij}\theta + \sum_{k,l} n_{kl}^{ij}(1)_{kl},$$

$$Z_0 = \mathbf{1} + m_0\theta + \sum_{k,l} n_{kl}^{0}(1)_{kl},$$

$$Z_1 = \mathbf{1} - 2\theta.$$

It is clear that Z_1 belongs to the centre of $\mathcal{U}(R)$, and $\phi(U_{ij}) = u_{ij}, \phi(Z_0) = z$ (where ϕ is the homomorphism stated in the proof of Lemma 3.1.1).

Proposition 3.1.1

$$\mathcal{U}(\mathbf{Z}T) = \pm\mathcal{U}_1(\mathbf{Z}T) = \pm\langle U_{ij}, Z_k \mid i = 1,2;\ j = 1,2,\cdots,w; k = 0,1\rangle.$$

Proof: For any $\alpha \in \mathcal{U}_1(R)$, $\alpha = \alpha\theta + \alpha(\mathbf{1} - E) + \alpha(E - \theta)$, and

$$\phi(\alpha) = f_P(\eta(h(\alpha(E - \theta)))) \in \mathcal{V} = \langle u_{ij}, z \mid i = 1,2; j = 1,2,\cdots,r\rangle.$$

So, $\alpha(E - \theta) \in \langle U_{ij}(E - \theta), Z_0(E - \theta) \mid i = 1,2; j = 1,2,\cdots,r\rangle$, and thus , by Lemma 3.1.1, $\alpha \in \langle U_{ij}, Z_0, Z_1 \mid i = 1,2; j = 1,2,\ldots,r\rangle$. □

3.2 A Specific Example

Note that the generators constructed in the previous section depend on the matrix P. We now apply the explained general method to compute $\mathcal{U}(\mathbf{Z}T)$ for a very concrete semigroup T.

Let

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Let $S = \mathcal{M}^0(\{1\}; 3, 3; P)$, and $T = S^1$. Then, $T \supseteq S \supseteq \{\theta\}$ is a principal series of T.

Clearly $d_P = det\ P = 2$ and

$$P^{-1} = \frac{1}{2}\begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{bmatrix}.$$

Therefore, $\mathcal{V} = (I + M_3(\mathbf{Z})P) \cap GL_3(\mathbf{Z}) \supseteq (I + M_3(\mathbf{Z})P) \cap SL_3(\mathbf{Z}) = \mathcal{V}_+ \supseteq (I + 2M_3(\mathbf{Z})) \cap SL_3(\mathbf{Z}) = \Gamma(2)$. Further, $\mathcal{W} = (\pm I + M_3(\mathbf{Z})P) \cap GL_3(\mathbf{Z}) = \mathcal{V}$ since $-I + M_3(\mathbf{Z})P = I - 2I + M_3(\mathbf{Z})P = I - 2P^{-1}P + M_3(\mathbf{Z})P = I + (-2P^{-1} + M_3(\mathbf{Z}))P \subseteq I + M_3(\mathbf{Z})P$. Also, $\frac{SL_3(\mathbf{Z})}{\Gamma(2)} \cong SL_3(\mathbf{Z}_2)$, where $\mathbf{Z}_2 = \{0, 1\}$, and

$$\mid SL_3(\mathbf{Z}_2) \mid = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168\ ([35, p.156 - 157]).$$

In order to calculate $\mathcal{V}_+$, since

$$\mathcal{V}_+/\Gamma(2) = \bar{\mathcal{V}}_+ = \{\bar{I} + \bar{A}\bar{P} \in SL_3(\mathbf{Z}_2) \mid \bar{A} \in M_3(\mathbf{Z}_2)\},$$

we first calculate $\bar{\mathcal{V}}_+$.

Let $X_0 = I + (x_{ij}) = I + X \in SL_3(\mathbf{Z}_2)$. Assume that X_0 has a decomposition of the form: $X_0 = I + \bar{A}\bar{P}$, for some $I + AP \in \mathcal{V}_+$, with $A = (a_{ij}) \in M_3(\mathbf{Z})$, $A = (\bar{a}_{ij}) \in M_3(\mathbf{Z}_2)$, where "-" indicates the natural map from $SL_3(\mathbf{Z})$ to $SL_3(\mathbf{Z}_2)$ and also from $\mathbf{Z}$ to $\mathbf{Z}_2$. We here denote both the identity of $SL_3(\mathbf{Z}_2)$ and the identity of $SL_3(\mathbf{Z})$ by I without causing any confusion. We should then have $(\bar{a}_{ij})P = (x_{ij})$.

So, the $a'_{ij}s$ are a solution of the following linear system:

$$\begin{array}{ccccccccccccccccccc}
a_{11} & & & + & \bar{a}_{13} & & & & & & & & & & & & & = & x_{11} \\
\bar{a}_{11} & + & \bar{a}_{12} & & & & & & & & & & & & & & & = & x_{12} \\
& & \bar{a}_{12} & + & \bar{a}_{13} & & & & & & & & & & & & & = & x_{13} \\
& & & & & \bar{a}_{21} & & & + & \bar{a}_{23} & & & & & & & & = & x_{21} \\
& & & & & \bar{a}_{21} & + & \bar{a}_{22} & & & & & & & & & & = & x_{22} \\
& & & & & & & \bar{a}_{22} & + & \bar{a}_{23} & & & & & & & & = & x_{23} \\
& & & & & & & & & & \bar{a}_{31} & & & + & \bar{a}_{33} & & & = & x_{31} \\
& & & & & & & & & & \bar{a}_{31} & + & \bar{a}_{32} & & & & & = & x_{32} \\
& & & & & & & & & & & & \bar{a}_{32} & + & \bar{a}_{33} & & & = & x_{33}
\end{array}$$

Adding the first three equations together gives 0 on the left hand side, and similarly with equations 4-6 and 7-9. We conclude that each non zero row of X has exactly two non zero entries. There are 64 matrices of this type. Hence there are at most 64 possibilities for X_0. If we further restrict $X_0 \in SL_3(\mathbf{Z}_2)$, then there are only 24 possibilities of such $X_0's$. It is then easily verified that $\mid \frac{\mathcal{V}_+}{\Gamma(2)} \mid = 24$.

It follows that

$$[SL_3(\mathbf{Z}) : \mathcal{V}_+] = \frac{[SL_3(\mathbf{Z}) : \Gamma(2)]}{[\mathcal{V}_+ : \Gamma(2)]} = \frac{168}{24} = 7.$$

Furthermore, it is easily verified that

$$SL_3(\mathbf{Z}) = \cup_{i=1}^{7} y_i \mathcal{V}_+,$$

where

$$y_1 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \quad y_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad y_3 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$y_4 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad y_5 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad y_6 = \begin{bmatrix} -1 & -1 & 0 \\ -1 & 0 & -1 \\ -1 & -1 & -1 \end{bmatrix},$$

$y_7 = I$, $y_i \in SL_3(\mathbf{Z}), i = 1, 2, \ldots, 7$.

From the previous section,

$$\mathcal{V}_+ = \langle u_{ij} \mid i = 1, 2;\ j = 1, 2, 3, 4, 5, 6, 7 \rangle,$$

where u_{ij} is an element of $\mathcal{V}_+$, such that, for given y_j, x_i, there exists $j' \in \{1, 2, 3, 4, 5, 6, 7\}$,

$$y_j x_i = u_{ij} y_{j'} \qquad \cdots\cdots\cdots (2)$$

Note that j' is uniquely determined by j and i.

Equivalently

$$y_j x_i y_{j'}^{-1} = u_{ij} \in \mathcal{V}_+ \qquad \cdots\cdots\cdots (3)$$

or

$$\bar{y}_j \bar{x}_i \bar{y}_{j'}^{-1} = I + X_{ij} \bar{P} \qquad \cdots\cdots\cdots (4)$$

for some $X_{ij} \in M_3(\mathbf{Z}_2)$, and $I + X_{ij}\bar{P} \in \bar{\mathcal{V}}_+$. One can verify that

$$X_{11} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_6;$$

$$X_{12} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_5;$$

$$X_{13} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_2;$$

$$X_{14} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad \bar{y}_{j'} = y_1;$$

$$X_{15} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_3;$$

$$X_{16} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_4;$$

$$X_{17} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_7;$$

$$X_{21} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_1;$$

$$X_{22} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_7;$$

$$X_{23} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_4;$$

$$X_{24} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_3;$$

$$X_{25} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_5;$$

$$X_{26} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_6;$$

$$X_{27} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \bar{y}_{j'} = \bar{y}_2.$$

Hence, we obtain that

$$u_{11} = y_1 x_1 y_6^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & -1 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix};$$

$$u_{12} = y_2 x_1 y_5^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix};$$

$$u_{13} = y_3 x_1 y_2^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & -1 \end{bmatrix};$$

$$u_{14} = y_4 x_1 y_1^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix};$$

$$u_{15} = y_5 x_1 y_3^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ -1 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{bmatrix};$$

$$u_{16} = y_6 x_1 y_4^{-1} = \begin{bmatrix} -1 & -1 & 0 \\ -1 & 0 & -1 \\ -1 & -1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & -1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix};$$

$$u_{17} = y_7 x_1 y_7^{-1} = x_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix};$$

$$u_{21} = y_1 x_2 y_1^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix};$$

$$u_{22} = y_2 x_2 y_7^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 0 \end{bmatrix};$$

$$u_{23} = y_3 x_2 y_4^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & -1 \end{bmatrix};$$

$$u_{24} = y_4 x_2 y_3^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ -1 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 1 & 1 \\ -1 & 2 & 2 \\ -2 & 3 & 2 \end{bmatrix};$$

$$u_{25} = y_5 x_2 y_5^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{bmatrix};$$

$$u_{26} = y_6 x_2 y_6^{-1} = \begin{bmatrix} -1 & -1 & 0 \\ -1 & 0 & -1 \\ -1 & -1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & -1 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{bmatrix};$$

$$u_{27} = y_7 x_2 y_2^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Finally, we describe a finite set of generators of $\mathcal{U}_1(R) = \mathcal{U}_1(\mathbf{Z}T)$. From above, since $z = -I \in \mathcal{V}, z \notin \mathcal{V}_+$, $[\mathcal{V} : \mathcal{V}_+] = 2$. Hence $\mathcal{V} = \langle u_{ij}, -I \mid i = 1,2; j = 1,2,3,4,5,6,7\rangle$. So, from Proposition 3.1.1, we are left with the problem of writing the generators $u_{ij}, z = -I$ as semigroup ring elements U_{ij}, Z_0. Clearly $z = -I = I - 2I = I - 2P^{-1}P$, and thus $(n_{kl}^0) = -2P^{-1}$. Further note that

$$(n_{kl}^{11}) = (u_{11} - I)P^{-1} = \begin{bmatrix} 0 & 0 & -1 \\ -1 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix}; \quad (n_{kl}^{12}) = (u_{12} - I)P^{-1} = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix};$$

$$(n_{kl}^{13}) = (u_{13} - I)P^{-1} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 2 & -1 & -1 \end{bmatrix}; \quad (n_{kl}^{14}) = (u_{14} - I)P^{-1} = \begin{bmatrix} -1 & 2 & -1 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix};$$

$$(n_{kl}^{15}) = (u_{15} - I)P^{-1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix}; \quad (n_{kl}^{16}) = (u_{16} - I)P^{-1} = \begin{bmatrix} -2 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 0 \end{bmatrix};$$

$$(n_{kl}^{17}) = (u_{17} - I)P^{-1} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix}; \quad (n_{kl}^{21}) = (u_{21} - I)P^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 1 & -1 & 0 \end{bmatrix};$$

$$(n_{kl}^{22}) = (u_{22} - I)P^{-1} = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \end{bmatrix}; \quad (n_{kl}^{23}) = (u_{23} - I)P^{-1} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 2 & -1 & -1 \end{bmatrix};$$

$$(n_{kl}^{24}) = (u_{24} - I)P^{-1} = \begin{bmatrix} -1 & 2 & -1 \\ -1 & 2 & 0 \\ 0 & 3 & -2 \end{bmatrix}; \quad (n_{kl}^{25}) = (u_{25} - I)P^{-1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{bmatrix};$$

$$(n_{kl}^{26}) = (u_{26} - I)P^{-1} = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}; \quad (n_{kl}^{27}) = (u_{27} - I)P^{-1} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix}.$$

Consequently, $U_{ij} = \mathbf{1} + m_{ij}\boldsymbol{\theta} + \sum_{k,l} n_{kl}^{ij}(1)_{kl}$, $Z_0 = \mathbf{1} + m_0\boldsymbol{\theta} + \sum_{k,l} n_{kl}^{0}(1)_{kl}$, and $Z_1 = \mathbf{1} - 2\boldsymbol{\theta}$, where $m_{ij} = \pm 1 - 1 - \sum_{k,l} n_{kl}^{ij}$, $m_0 = \pm 1 - 1 + \sum_{k,l} n_{kl}^{0}(1)_{kl}$, $i = 1, 2$; $j = 1, 2, 3, 4, 5, 6, 7$. It follows that, from Proposition 3.1.1

$$\mathcal{U}(\mathbf{Z}T) = \pm\mathcal{U}_1(\mathbf{Z}T) = \mathcal{U}_1(\mathbf{Z}T) = \langle U_{ij}, Z_k \mid i = 1, 2; j = 1, 2, 3, 4, 5, 6, 7;\ k = 0, 1\rangle.$$

Chapter 4

Semigroups with $\mathcal{U}(\mathbf{Z}S)$ finite or having a free subgroup of finite index

4.1 Finite Unit Group U(ZS)

We first study the conditions under which the unit group $\mathcal{U}(\mathbf{Z}S)$ is finite. Here we will only assume that S is a finite semigroup such that $\mathbf{Z}S$ contains an identity $\mathbf{1}$.

In order to state the first theorem, we recall some terminology. A group G is said to be a Hamiltonian group if G is non-Abelian and all its subgroups are normal. It is well known (see M. Hall [5]) that a Hamiltonian group can be written as $A \times E \times K_8$, where K_8 is the quaternion group of order 8, A is Abelian with every element of odd order, and E is an elementary Abelian 2-group.

Theorem 4.1.1 *Let S be a finite semigroup such that $\mathbf{Z}S$ contains an identity. Then the order of unit group $\mathcal{U}(\mathbf{Z}S)$ is finite if and only if S is an inverse semigroup which is a union of disjoint groups which are either abelian of exponent 1, 2, 3, 4 or 6 or Hamiltonian 2-groups.*

Proof. First, assume the order $| \mathcal{U}(\mathbf{Z}S) | < \infty$. Then it is easy (and well known) to show that $\mathbf{Q}S$, and thus also $\mathbf{Z}S$ have no non-zero nilpotent elements. Indeed, let $x \in \mathbf{Z}S$, and assume $n \geq 2$ is such that $y = x^{n-1} \neq 0, x^n = 0$. Since $y^2 = 0$

$$(\mathbf{1} - zy)(\mathbf{1} + zy) = \mathbf{1},$$

for any $z \in \mathbf{Z}$. Hence we have an infinite set $\{1 + zy \mid z \in \mathbf{Z}\}$ of units, a contradiction. This proves the claim and hence $\mathbf{Q}S$ is a semisimple Artinian ring . Thus Theorem 1.3.1 implies that S^0 has a principal series

$$S^0 = S_0 \supset S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \{\theta_S\},$$

where each principal factor $S_i/S_{i+1} \cong G_i^0$, each G_i a group, $1 \leq i \leq n$. The isomorphisms used in Theorem 1.3.1 yield that

$$\mathbf{Z}S^0 \cong \bigoplus_{i=0}^{n} \mathbf{Z}G_i \oplus \mathbf{Z}\theta_S.$$

Thus from $\mathcal{U}(\mathbf{Z}S^0) \cong \prod_{i=0}^{n} \mathcal{U}(\mathbf{Z}G_i) \times \mathcal{U}(\mathbf{Z})$ we obtain that each $| \mathcal{U}(\mathbf{Z}G_i) | < \infty$. Consequently by [36, p.59, Corollary 5.4], each G_i is either abelian of exponent 1, 2, 3, 4 or 6 or G_i is a Hamiltonian 2-group.

Conversely, assume S is an inverse semigroup which is a union of such groups. By using the same method as above, we obtain $\mathbf{Z}S^0 \cong \bigoplus_{i=0}^{n} \mathbf{Z}G_i \oplus \mathbf{Z}\theta_S$. Hence $\mathcal{U}(\mathbf{Z}S^0) \cong \prod_{i=0}^{n} \mathcal{U}(\mathbf{Z}G_i) \times \mathcal{U}(\mathbf{Z}$;. The result then follows again by using [36, page 57, Theorem 4.1]. □

4.2 $\mathcal{U}(\mathbf{Z}S)$ having a free subgroup of finite index

For finite groups, E. Jespers has proved that there are only four groups G such that $\mathcal{U}(\mathbf{Z}G)$ has a nonabelian free subgroup of finite index:

Theorem 4.2.1 *[9] Let G be a finite group. Then $\pm G$ has a non-Abelian free subgroup of finite index in $\mathcal{U}(\mathbf{Z}G)$ if and only if G is isomorphic with either S_3, D_8, T, P, where*

(i) $S_3 = \langle a, b \mid a^3 = 1, b^2 = 1, ba = a^{-1}b\rangle$, the symmetric group of degree 3;

(ii) $D_8 = \langle a, b \mid a^4 = 1, b^2 = 1, ba = a^{-1}b\rangle$, the dihedral group of order of 8;

(iii) $T = \langle a, b \mid a^6 = 1, b^2 = a^3, ba = a^5 b\rangle$, the dicyclic group of order 12;

(iv) $P = \langle a, b \mid a^4 = 1, b^4 = 1, aba^{-1}b^{-1} = a^2\rangle$, a group of order 16.

In this section, we study the analogous problem for the integral semigroup ring $\mathbf{Z}S$ of a finite semigroup. Again we assume that $\mathbf{Q}S$ is semisimple Artinian and that $\mathbf{Z}S$ contains an identity. So, S^0 has a principal series

$$S^0 = S_0 \supset S_1 \supset \cdots \supset S_n \supset S_{n+1} = \{\mathit{0}_S\}$$

and

(i) $S_i/S_{i+1} \cong^{\eta_i} \mathcal{M}^0(G_i; m_i, m_i; P_i), i = 0, 1, \cdots, n$

(ii) $\mathbf{Q}S^0 \cong^{\oplus f_{P_i}\eta_i} \oplus_{i=0}^{n} M_{m_i}(\mathbf{Q}G_i) \oplus \mathbf{Q}\mathit{0}_S$ (**)

where each G_i is a finite group, m_i is a positive integer, and each sandwich matrix P_i is invertible in $M_{m_i}(\mathbf{Q}G_i)$, $i = 0, 1, \cdots, n$. We prove two theorems in this Chapter, one of which is as follows.

Theorem 4.2.2 *Under the above assumptions, $\mathcal{U}(\mathbf{Z}S)$ has a non-trivial free subgroup of finite index if and only if there exists $0 \leq i_0 \leq n$ such that, for $i \neq i_0, m_i = 1$, and G_i is either an Abelian group with $G_i^4 = \{e_i\}$ or $G_i^6 = \{e_i\}$, or a Hamiltonian 2-group and, furthermore, one of the following three conditions is satisfied:*

(i) $m_{i_0} = 2, G_{i_0} = \{e_{i_0}\}$*;*

(ii) $m_{i_0} = 1$*, and* G_{i_0} *is one of* $S_3, D_8, T, or P$*;*

(iii) $m_{i_0} = 1$*, and* G_{i_0} *is cyclic of order 5, 8 or 12.*

Recall that for a finite Abelian group A of order n, $\mathcal{U}(\mathbf{Z}A) = \pm A \times F$, where F is a free Abelian group of rank $r = \frac{1}{2}(n + 1 + n_2 - 2c)$, c the number of cyclic subgroups of A and n_2 the number of elements of order 2 in A. It follows then easily that $\mathbf{Z}A$ has only trivial units, i.e., r = 0, if and only if A has exponent 1, 2, 3, 4 or 6, i.e., $A^4 = \{e\}$ *or* $A^6 = \{e\}$. This shows the first fact of the well known Higman Theorem :

Proposition 4.2.1 *(see for example [36, Theorem 4.1, p.57]) Suppose* G *is a finite group. Then* $\mathcal{U}(\mathbf{Z}G) = \pm G$ *if and only if* G *is either*

(i) an Abelian group with $G^4 = \{1\}$*; or*

(ii) an Abelian group with $G^6 = \{1\}$*; or*

(iii) a Hamiltonian 2-group.

In order to prove Theorem 4.2.2, we need to show that $r = 1$ in the above if and only if A is cyclic of order 5, 8 or 12. In fact, we show more generally that:

Theorem 4.2.3 *Let* G *be a finite group. Then* $\mathcal{U}(\mathbf{Z}G)$ *has a rank one free subgroup of finite index if and only if* G *is cyclic of order 5, 8, or 12.*

In the remainder of this section, we prove Theorems 4.2.2 and 4.2.3. We begin with the following lemma, which is proved in [9] for group rings. We often make use of the fact that if $\mathcal{U}(\mathbf{Z}S)$ has free subgroup of finite index then it does not contain a free Abelian subgroup of rank two. Indeed, suppose the contrary, there exists a free Abelian subgroup F of rank two in $\mathcal{U}(\mathbf{Z}S)$ with a free subgroup N of finite index, say x and y are the generators of F. Then, there will exist a positive integer m such that the subgroup $\langle x^m, y^m\rangle$ generated by x^m and y^m contains in N, and thus $\langle x^m, y^m\rangle$ is a free and Abelian group. Therefore, it is a cyclic infinite order group and there must exist a positive integer n such that $x^{mn} = y^{mn}$. This is a contradiction.

Lemma 4.2.1 *If $\mathcal{U}(\mathbf{Z}S)$ has a free subgroup of finite index, then $\mathbf{Q}S$ has at most one simple Wedderburn component which is not a division ring. Furthermore, if such a component M exists, then it is isomorphic to $M_2(\mathbf{Q})$, a two-by-two matrix ring over $\mathbf{Q}$.*

Proof: Let M be a simple component of $\mathbf{Q}S$. We first show that if $M \cong M_n(D)$, D a division ring and $2 \leq n$, then $n = 2$. If $3 \leq n$, let $E_{ij}, 1 \leq i, j \leq n$ be a set of classical matrix units of M (so, E_{ij} is a matrix which has 1 at the (i,j)-entry and zeroes elsewhere). Since $E_{ij} \in \mathbf{Q}S$, there exists a positive integer m_{ij} such that $m_{ij}E_{ij} \in \mathbf{Z}S$. As furthermore, $(m_{12}E_{12})^2 = (m_{1n}E_{1n})^2 = 0$, it follows easily that $1 + m_{12}E_{12}$ and $1 + m_{1n}E_{1n}$ generate a free abelian group of rank two contained in $\mathbf{Z}S$, a contradiction. Thus $n = 2$.

Next, we show that $\mathbf{Q}S$ has at most one simple Wedderburn component which is not a division ring; i.e., which is isomorphic to $M_2(D)$, for some division ring D. Suppose that there are two components M_1 and M_2 which are not division rings. As above, in each $M_i \cap \mathbf{Z}T$ there exists $\alpha_i \neq 0$ with $\alpha_i^2 = 0, i = 1, 2$. It again follows that $1+\alpha_1$ and $1+\alpha_2$ generate a free abelian group of rank two, a contradiction.

Third, we show that if $M \cong M_2(D)$, D a division ring, is a simple component of $\mathbf{Q}S$, then $D = \mathbf{Q}$. If not, let $d \in D, d \notin \mathbf{Q}$, then with the above notation, let m be a positive integer such that $mE_{12}, mdE_{12} \in \mathbf{Z}S$. The units $1+mE_{12}$, and $1+mdE_{12}$ generate a free abelian group of rank two, again yielding a contradiction. □

Lemma 4.2.2 *Let H be a group and F a subgroup of finite index such that F is a free group of rank one. Then every non-trivial free subgroup of H has rank one.*

Proof: The assumption implies that for any two non-periodic elements $x, y \in H$, there exist positive integers k, l such that $x^k, y^l \in F$ since F is of finite index in H. Then there must be another two positive integers m, n such that $x^{km} = y^{ln}$ since F is a free group of rank one. It follows that H can not contain any free subgroup with rank more than one. □

Lemma 4.2.3 *If $\mathcal{U}(\mathbf{Z}S)$ has a free subgroup of finite index, then any element of a subgroup of S, which is isomorphic to a subgroup of $\mathcal{U}(\mathbf{Z}S)$, has order 1, 2, 3, 4, 5, 6, 8, or 12.*

Proof: Let G be a subgroup of S, which is isomorphic to a subgroup of $\mathcal{U}(\mathbf{Z}S)$, and let $g \in G$. Since $\mathcal{U}(\mathbf{Z}\langle g\rangle)$ does not contain any free Abelian subgroup of rank two, it follows from Higman's result that the rank r of the free Abelian complement of the trivial units in $\mathcal{U}(\mathbf{Z}\langle g\rangle)$ is

$$r = \frac{1}{2}(n+1+n_2-2c) = 0 \text{ or } 1,$$

where n is the order of g, c is the number of cyclic subgroups of $\langle g\rangle$ and n_2 is the number of elements of order 2 in $\langle g\rangle$. The case $r = 0$ yields n=1, 2, 3, 4, or 6.

Assume now r=1, i.e.,

$$n + n_2 - 2c - 1 = 0. \quad (*)$$

Let p be a prime number with $p^\alpha \mid n$ and $1 \leq \alpha$. If $p \neq 2, 3$, then the order of g^{n/p^α} is not 2, 3, 4, and 6, and the above applied to the element g^{n/p^α} yields

$$p^\alpha - 2(\alpha + 1) - 1 = 0$$

and thus $p^\alpha = 2\alpha + 3$. Writing p as $1 + (p - 1)$, it follows that.

$$1 + \alpha(p-1) + \cdots + (p-1)^\alpha = 2\alpha + 3$$

$$\alpha(p-1) + \cdots + (p-1)^\alpha = 2\alpha + 2$$

Since $4 \leq p - 1$, we have $4\alpha \leq 2\alpha + 2$, and therefore $\alpha \leq 1$. Thus $\alpha = 1$, and it follows that $p = p^\alpha = 5$.

Therefore, $n = 5^x 2^y 3^z$, where $x \leq 1, y, z$ are non-negative integers. Under the condition (*), we show the possible values of each x, y, z in the following . We will repeatedly use the result that, for a finite cyclic group H, there is a one-to-one correspondence between its subgroups and the divisors of the order of H. Further, if m is the order of H, and $m = p_1^{x_1} p_2^{x_2} \ldots p_t^{x_t}$, where $p_i, 1 \leq i \leq t$, are prime numbers, then the number of divisors of m is $(x_1 + 1)(x_2 + 1) \ldots (x_t + 1)$. In particular, if m is an odd number, then G does not contain any element of order 2, and if m is an even number, then G has only one element of order 2.

Case 1: Let $x = 1, 1 \leq y$. Then, $n = 5 \times 2^y 3^z$, $n_2 = 1$, and $c = (1+1)(y+1)(z+1)$. Thus, from condition (*), $5 \times 2^y 3^z + 1 - 2(1+1)(y+1)(z+1) - 1 = 0$; i.e.,

$5 \times 2^y 3^z = 4(y+1)(z+1)$. However, it is easy to show that $4(y+1)(z+1) < 5 \times 2^y 3^z$. Thus case 1 is not possible.

Case 2: Let $x = 1, y = 0, 1 \leq z$, then $5 \times 3^z + 0 - 2(1+1)(z+1) - 1 = 0$ from (*), i.e., $5 \times 3^z = 1 + 4(z+1)$. Again since $5 \times 3^z > 5(z+1) = 4(z+1) + z + 1 > 4(z+1) + 1$, case 2 is not possible.

Case 3: Let $x = 0, 3 \leq y, 1 \leq z$, then $2^y 3^z + 1 - 2(y+1)(z+1) - 1 = 0, i.e., 2^y 3^z = 2(y+1)(z+1), 2^{y-1} 3^z = (y+1)(z+1)$. But $y + 1 \leq 2^{y-1}$ for $3 \leq y$ and $z + 1 < 3^z$ for $1 \leq z$. Thus case 3 is not possible.

Case 4: Let $x = 0, 3 \leq y, z = 0$, then $2^y + 1 - 2(y+1) - 1 = 0, 2^{y-1} = y + 1$. Thus $y = 3$ otherwise $y + 1 < 2^{y-1}$.

Case 5: Let $x = 0, y = 2, 1 \leq z$, then if $2^2 3^z + 1 - 2(2+1)(z+1) - 1 = 0, i.e., 4 \times 3^z = 2 \times 3(z+1), 2 \times 3^{z-1} = z+1$. Thus $z = 1$, otherwise it is not possible since $z+1 \leq 3^{z-1}$, for $2 \leq z$, and $z + 1 < 2 \times 3^{z-1}$.

Case 6: Let $x = 0, y = 1, 1 \leq z$, then $2 \times 3^z + 1 - 2(1+1)(z+1) - 1 = 0, i.e., 3^z = 4(z+1)$. It is not possible.

Case 7: Let $x = 0, y = 0, 2 \leq z$, then if $3^z - 2(z+1) - 1 = 0, 3(3^{z-1} - 1) = 2z$. It is impossible since $z < 3^{z-1}$.

Therefore, the possibilities of n are only 1, 2, 3, 4, 5, 6, 8 or 12. □

Proposition 4.2.2 *[36, Theorem 1.17, p.172] The rational group algebra* $\mathbf{Q}G$ *of a finite group* G *has no non-zero nilpotent elements if and only if one of the following* *is satisfied*

(i) G is Abelian;

(ii) G is Hamiltonian of order $2^n m$, m odd, such that the multiplicative order of 2 mod m is odd.

We also recall the following fact.

Lemma 4.2.4 *[22, p. 149] Let*

$$x = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad y = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

Then the group $\langle x, y \rangle = \left\{ u \mid u = \begin{bmatrix} 2m+1 & 2n \\ 2l & 2k+1 \end{bmatrix}_{\det\ u=1}, m, n, l, k \in \mathbf{Z} \right\}$ *is non-trivial freely generated and of finite index in $SL_2(\mathbf{Z})$.*

Corollary 4.2.1 *Let $\mathcal{U}(\mathbf{Z}S)$ have a non-trivial free subgroup F of finite index. Then there exists $0 \leq i_0 \leq n$ such that, for $i \neq i_0, m_i = 1$, and G_i is either an Abelian group with $G_i^4 = \{e_i\}$ or $G_i^6 = \{e_i\}$, or a Hamiltonian 2-group. Furthermore,*

(i) If F is non-Abelian, then all simple components of $\mathbf{Q}S$ are division rings, except one which is $M_2(\mathbf{Q})$.

(ii) If F is Abelian, then $\mathbf{Q}S$ is a direct sum of division rings, G_{i_0} is Abelian and $\mathcal{U}(\mathbf{Z}G_{i_0}) = \pm G_{i_0} \times F_{i_0}$, where F_{i_0} is a free group of rank one.

Proof: First let F be Abelian. Then the rank of F must be one. Thus every free subgroup of $\mathcal{U}(\mathbf{Z}S)$ has rank one from Lemma 4.2.2. From Lemma 4.2.1, $\mathbf{Q}S$ either has a unique simple component M which is isomorphic to $M_2(\mathbf{Q})$ or is a direct sum of division rings. Let us assume that $\mathbf{Q}S$ has a simple component M which is isomorphic to $M_2(\mathbf{Q})$. According to Lemma 4.2.4, the group $\langle x, y\rangle$ is a rank two free subgroup of $GL(2, \mathbf{Z})$. If we identify M and $M_2(\mathbf{Q})$, then we could choose an order $\mathcal{O}$ of $\mathbf{Q}S$, which contains $M_2(\mathbf{Z})$ up to isomorphism, and thus $\langle x, y\rangle \subset \mathcal{U}(\mathcal{O})$. Since $\mathbf{Z}S$ is another order of $\mathbf{Q}S$, it follows that $[\mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathcal{O} \cap \mathbf{Z}S)] < \infty$ from Lemma 1.4.2. Therefore, there are two positive numbers k, l such that $x^k, y^l \in \mathcal{U}(\mathbf{Z}S)$, and thus there are another two positive numbers m, n such that $x^{km} = y^{ln} \in F$, a contradiction. Therefore, $\mathbf{Q}S$ is a direct sum of division rings.

Second assume F is non-Abelian. We will prove that $\mathbf{Q}S$ is not a sum of division rings. Suppose the contrary. Then $\mathbf{Q}S$ has no nilpotent elements. Hence all $m_i = 1$,

$$\mathbf{Q}S^0 = \oplus_{i=0}^{n} \mathbf{Q}G_i \oplus \mathbf{Q}\theta_S,$$

and each $\mathbf{Q}G_i$ is a direct sum of division rings. In particular, S is an inverse semigroup which is a disjoint union of the groups G_i and $\{\theta_S\}$. It follows that

$$\mathbf{Z}S^0 \cong \oplus_{i=0}^{n} \mathbf{Z}G_i \oplus \mathbf{Z}\theta_S$$

and

$$\mathcal{U}(\mathbf{Z}S^0) = \prod_{i=0}^{n} \mathcal{U}(\mathbf{Z}G_i) \times \mathcal{U}(\mathbf{Z}\theta_S).$$

Since $\mathbf{Q}G_i$ has no non-zero nilpotent elements, Proposition 4.2.2 implies that G_i is either Abelian or Hamiltonian of order $2^{l_i}k_i$, k_i odd such that the multiplicative order of 2 modulo k_i is odd, $i = 0, 1, \cdots, n$.

If G_i is Abelian, then $\mathcal{U}(\mathbf{Z}G_i) = \pm G_i \times F_i$, where F_i is a finitely generated free Abelian group. Since, by assumption, $\mathcal{U}(\mathbf{Z}S)$, and thus $\mathcal{U}(\mathbf{Z}G_i)$ do not contain a free

Abelian subgroup of rank 2, the rank of F_i is at most 1, and there exists at most one such group G_i.

Now assume that G_i is a Hamiltonian group. Recall that G_i contains an element of order p if p is a prime divisor of the order of G_i. Thus, we know that the possible prime divisors of k_i are only 3 or 5 from Lemma 4.2.3. Hence $k_i = 3^x5^y$ for some non-negative integers x and y. If $k_i \neq 1$, then $x \neq 0$ or $y \neq 0$. So, $\mathbf{Z}/(3^x5^y) \supseteq \mathbf{Z}/(3)$ if $x \neq 0$ and $\mathbf{Z}/(3^x5^y) \supseteq \mathbf{Z}/(5)$ if $y \neq 0$. However, the multiplicative order of 2 modulo 3 or 5 is 2 or 4 respectively. Therefore, the multiplicative order of 2 modulo k_i is even in any case. This is a contradiction. Hence, k_i must be 1 and G_i is a Hamiltonian 2-group. Therefore $\mathcal{U}(\mathbf{Z}G_i)$ is trivial by Proposition 4.2.1.

So, we have shown that there is at most one i such that $\mathcal{U}(\mathbf{Z}G_i)$ has non-trivial unit group, and that it has a cyclic subgroup of finite index. It follows that $\mathcal{U}(\mathbf{Z}S) = \prod_{i=0}^{n} \mathcal{U}(\mathbf{Z}G_i) \times \mathcal{U}(\mathbf{Z}\theta_S)$ has a cyclic subgroup of finite index. This is in contradiction with the assumption that $\mathcal{U}(\mathbf{Z}S)$ has a non-Abelian free subgroup of finite index. Hence our assumption that $\mathbf{Q}S$ is a direct sum of division rings is false. Therefore, $\mathbf{Q}S$ must have one simple component which is isomorphic to $M_2(\mathbf{Q})$.

The other claims are clear from the proof. □

Applying Corollary 4.2.1 to the case when S is a group, it follows that

Corollary 4.2.2 *Let G be a finite group. If $\mathcal{U}(\mathbf{Z}G)$ has an infinite cyclic subgroup of finite index, then G must be an Abelian group.*

In the following, we first show the proof of Theorem 4.2.3, and in the proof we will use these examples:

Example 1 Let $G = \langle c \mid c^5 = 1\rangle \times \langle d \mid d^5 = 5\rangle$.Then $\mathcal{U}(\mathbf{Z}G) = \pm G \times F$, where the rank of the free Abelian group F is 7. In fact, G has no element of order 2 and 6 cyclic subgroups. Thus $r = \frac{1}{2}(25 + 1 + 0 - 2 \times 7) = 6$.

Example 2 Let $G = \langle c \mid c^8 = 1\rangle \times \langle d \mid d^2 = 1\rangle$. Then G has 3 elements of order 2, and 7 cyclic subgroups. Thus $r = \frac{1}{2}(16 + 1 + 3 - 2 \times 8) = 2$.

Example 3 Let $G = \langle c \mid c^{12} = 1\rangle \times \langle d \mid d^2 = 1,\ or\ d^3 = 1\rangle$. Then if $d^2 = 1$, G has 3 elements of order 2 and 11 cyclic subgroups, thus $r = \frac{1}{2}(24 + 1 + 3 - 2 \times 11) = 3$; if $d^3 = 1$, G has 1 element of order 2 and 14 cyclic subgroups, thus $r = \frac{1}{2}(36 + 1 + 1 - 2 \times 14) = 5$.

The **Proof of Theorem 4.2.3**

Assume $\mathcal{U}(\mathbf{Z}G)$ has a rank one free subgroup of finite index. Then G is Abelian from Corollary 4.2.2. From Lemma 4.2.3, it follows that any element of G has order 1,2,3,4,5,6,8, or 12. Further, if G contains an element x of order 5, then G can not contain any element whose order is a multiple of 2 or 3, since otherwise G contains an element of order 10 or 15. Furthermore, by Example 1, G does not contain any subgroup which is a product of two cyclic groups of order 5. Hence $G = \langle x\rangle$ is of order 5. Similarly, if G contains an element y of order 8, then G can not contain any element whose order is a multiple of 3 or 5. Thus $G = \langle y\rangle$ by Example 2 since there can not exist $a \in G, a \notin \langle y\rangle$, such that the order of a is a multiple of 2. Finally, if G does not contain any element of order 5 or 8, then any element of G has order 1,2,3,4,6, or 12. Hence $G = \langle z\rangle$, z an element of order 12, by Example 3.

Conversely, it is easily verified that the rank of the free Abelian complement is 1 when G is a cyclic group of order 5, 8, or 12. □

Now we can give the **proof of Theorem 4.2.2** as follows:

Proof: Assume that $\mathcal{U}(\mathbf{Z}S)$ has a non-trivial free subgroup F of finite index. From Corollary 4.2.1, it follows that there exists i_0 such that for all $i \neq i_0$, $m_i = 1$ and G_i is either an Abelian group with $G_i^4 = \{e_i\}$ or $G_i^6 = \{e_i\}$, or a Hamiltonian 2-group. Now recall that, for a non-trivial group G, $\mathbf{Q}G$ always has a proper ideal, for example, the augmentation ideal of $\mathbf{Q}G$ [36, p.2], and thus $M_2(\mathbf{Q}G)$ can not be a simple ring. Therefore, if F is non-Abelian, then either $m_{i_0} = 2$, and $G_{i_0} = \{e_{i_0}\}$, or $m_{i_0} = 1$, and $\mathcal{U}(\mathbf{Z}G_{i_0})$ has a non-Abelian free subgroup of finite index. It then follows from Theorem 4.2.1 that, G_{i_0} is one of S_3, D_4, T or P. If F is Abelian, then again from Corollary 4.2.1, G_{i_0} is Abelian with $\mathcal{U}(\mathbf{Z}G_{i_0}) = \pm G_{i_0} \times F_{i_0}$, where F_{i_0} is a free group of rank one. Further, from Theorem 4.2.3, G_{i_0} is a cyclic group of order 5, 8 or 12.

Conversely, if (i) holds then (**) becomes

$$\mathbf{Q}S^0 \cong \oplus_{i\neq i_0}\mathbf{Q}G_i \oplus M_2(\mathbf{Q}) \oplus \mathbf{Q}\mathit{0}.$$

If (ii), or (iii) holds then (**) becomes

$$\mathbf{Q}S^0 \cong \oplus_{i=0}^{n}\mathbf{Q}G_i \oplus \mathbf{Q}\mathit{0}.$$

Let $\mathcal{O} = \oplus_{i\neq i_0}\mathbf{Z}G_i \oplus \mathcal{O}_{i_0} \oplus \mathbf{Z}\mathit{0}$, where $\mathcal{O}_{i_0} = M_2(\mathbf{Z})$, or $= \mathbf{Z}G_{i_0}$. Then, up to isomorphism, $\mathcal{O}$ is an order of $\mathbf{Q}S^0$, and $[\mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathbf{Z}S^0 \cap \mathcal{O})] < \infty$, $[\mathcal{U}(\mathbf{Z}S^0) :$

$\mathcal{U}(\mathbf{Z}S^0 \cap \mathcal{O})] < \infty$ from Lemma 1.4.2. On the other hand,

$$\mathcal{U}(\mathcal{O}) = \prod_{i \neq i_0} \mathcal{U}(\mathbf{Z}G_i) \times \mathcal{U}(\mathcal{O}_{i_0}) \times \mathcal{U}(\mathbf{Z}\theta),$$

and under assumption (i), (ii), or (iii), $\mathcal{U}(\mathcal{O})$ has a free subgroup F_0 of finite index from Theorem 4.2.1, Proposition 4.2.1, Lemma 4.2.4, and Theorem 4.2.3. Since any subgroup of a free group is also free (see for example [35, Theorem 11.23, p.258]), $\mathcal{U}(\mathbf{Z}S^0) \cap F_0$ is free and $[\mathcal{U}(\mathbf{Z}S^0) \cap \mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathbf{Z}S^0) \cap F_0] < \infty$. Therefore $[\mathcal{U}(\mathbf{Z}S^0) : \mathcal{U}(\mathbf{Z}S^0) \cap F_0] < \infty$. So, $\mathcal{U}(\mathbf{Z}S^0) \cap F_0$ is a free subgroup of finite index of $\mathcal{U}(\mathbf{Z}S^0)$. Finally, since $\mathcal{U}(\mathbf{Z}S^0) \cong \pm\mathcal{U}(\mathbf{Z}S)$, $\mathcal{U}(\mathbf{Z}S)$ itself has a free subgroup of finite index. □

Bibliography

[1] P.J. Allen and C.Hobby, A characterization of the units in $\mathbf{Z}[A_4]$, J. Algebra 66, 534-543 (1980).

[2] H.Bass, The Dirichlet unit theorem, induced characters and whitehead groups of finite groups, Topology 4, 391-410(1966).

[3] A. K. Bhandari, On the generators of subgroups of unit groups of group rings, Bol. Soc. Brasil. Mat. N.S. 20, 87-93 (1990).

[4] A. H. Clifford and G. B. Preston, The Algebraic Theory of Semigroups, Vol.1, Amer. Math. Soc., Providence, 1961.

[5] M. Hall, The theory of groups, MacMillan, New York, 1959.

[6] I. Hughes, K.R. Pearson, The group of units of the integral group ring $\mathbf{Z}S_3$, Canad. Math. Bull. 15, 529-534 (1972).

[7] T. W. Hungerford, Algebra, Springer-Verlag, New York, 1974.

[8] N.Ito, Frobenius and Zassenhaus groups, Lecture Notes, University of Illinois at Chicago Circle, 1969.

[9] Eric Jespers, Free Normal Complements and the Unit Group of Integral Group Rings, Proc. Amer. Math. Soc. 122(1), 59-66 (1994).

[10] ———, Bicyclic units in some integral group rings, Can. Math. Bull. Vol.38 (1), 80-86 (1995).

[11] E. Jespers and G. Leal, Generators of large subgroups of the unit group of integral group rings, Manuscripta Math. 78, 303-315 (1993).

[12] ————, Degree 1 and 2 representations of nilpotent groups and applications to units of group rings, Manuscripta Math, to appear.

[13] ————, Units of integral group rings of Hamiltonian groups, Comm. Algebra 23(2),623-628 (1995).

[14] ————————, Describing units of integral group rings of some 2-groups, Commun. in Algebra 19(6), 1809-1827 (1991).

[15] E.Jespers, M. M. Parmenter, Bicyclic units in $\mathbf{Z}S_3$, Bull. Belg. Math. Soc. 44, 141-146 (1992).

[16] ————————, Units of group rings of groups of order 16, Glasgow Math. J. 35, 367-379 (1993).

[17] E. Jespers and J. Okninski, Nilpotent semigroups and semigroup algebras, J. Algebra 169, 984-1011 (1994).

[18] Gregory Karpilovsky, Unit groups of group rings, Longman Scientific & Technical, New York, 1989.

[19] E. Kleinert, A theorem on units of integral group rings, J. Pure Appl. Algebra 49, 161 - 171 (1987).

[20] A.I.Malcev, Nilpotent semigroups, Uc. Zap. Ivanovsk.Ped.Inst. 4, 107-111 (1953).

[21] C. Polcino Milies, The units of the integral group ring $\mathbf{Z}D_4$, Bol. Sci. Brasil. Mat. 4, 85-92 (1973).

[22] M. Newman, Integral Matrices, Academic Press, New York and London, 1972.

[23] J. Okninski, Semigroup Algebras, Marcel Dekker, New York and Basel, 1991.

[24] M. M. Parmenter, Free torsion-free normal complements in integral group rings, Commun. in Algebra 21 (10), 3611-3617 (1993).

[25] ————————, Torsion-free normal complements in unit groups of integral group rings, C.R. Math. Rep. Acad. Soc. Canada 12(4), 113-118 (1990).

[26] D.S.Passman, Permutation groups, Benjamin, New York, 1968.

[27] D.S. Passman, The Algebraic Structure of Group Rings, A Wiley-Interscience Publication, John Wiley & Sons, New York, London, Sydney, Toronto, 1977.

[28] D.S. Passman, P.F. Smith, Units in integral group rings, J. Algebra 69, 213-239 (1981).

[29] I. Reiner, Maximal Orders, Academic Press, New York, 1975.

[30] J. Ritter and S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, Trans. Amer. Math. Soci. 324(2), 603-621(1991).

[31] ——————, Certain normal subgroups of units in groups, J.Reine Angew. Math. 381, 214-220 (1987).

[32] ——————, Generators of subgroups of $\mathcal{U}(\mathbf{Z}G)$, Contemp. Math. 93, 331-347 (1989).

[33] ——————, Construction of units in group rings of monomial and symmetric groups, J. Algebra 142, 511-526 (1991).

[34] ——————, Units of group rings of solvable and Frobenius groups over large rings of cyclotomic integers, J. Algebra 158, 116-129 (1993).

[35] Joseph J. Rotman, The Theory of Groups, Allyn and Bacon Inc., 1973.

[36] S.K. Sehgal, Topic in Group Rings, Marcel Dekker, New York and Basel, 1978.

[37] S.K. Sehgal, Units in integral group rings, Longman Scientific and Technical, Essex, 1993.

[38] M.Suzuki, Group Theory, Springer-Verlag, New York, 1982.

[39] H.Zassenhaus, Uber endliche Fastkorper, Hamburg Abh. 11, 187-220 (1935).